

HANDBUCH

Martin R. Schulz (Hrsg.)

Compliance Management im Unternehmen

Grundlagen, Erfolgsfaktoren und
praktische Umsetzung

3. Auflage

RECHT WIRTSCHAFT STEUERN

Compliance Management im Unternehmen

Grundlagen, Erfolgsfaktoren und praktische Umsetzung

Herausgegeben von

Prof. Dr. Martin R. Schulz, LL.M. (Yale)

Mit Beiträgen von

Wolfram Bartuschka; Philipp Becker; Carsten Beisheim;
Prof. Dr. Daniel Benkert; Dr. Viola Bensinger; Florian Block;
Prof. Dr. Benjamin von Bodungen, LL.M. (Auckland); Dietmar Böhlke, MBA
(Warwick); Dr. Marcus Böttger; Dr. Bernd Federmann, LL.M.; Armin Fladung;
Prof. Dr. Kai Förstl; Melanie Frankenberger; Dr. Ulrich Hagel;
Prof. Dr. Katharina Hastenrath; Dominik Heske, LL.M.; Sven Jacobs;
Dr. Joachim Kaetzler; Prof. Dr. Oliver Keßler; Martin T. Knopp; Till Komma;
Marcel Moussaoui; Dr. Oliver Mross; Dr. Manfred Rack; Dr. Christian Rau,
LL.M. (Georgetown); Hartmut T. Renz; Frank Romeike; Charlotte Salathé;
Dr. Christian Scherer; Prof. Dr. Martin C. Schleper; Prof. Dr. Martin R. Schulz,
LL.M. (Yale); Dr. Tobias Schwartz; Prof. Dr. Daniela Seeliger; Nina Seydel;
Dr. Thomas Sonnenberg; Prof. Dr. Christopher Stehr; Dr. Thomas Uhlig;
Dr. Benjamin Ullrich, M.Jur. (Oxford); Klaus G. Walter; Dr. Florian Wettner;
Michael Wiedmann

3., aktualisierte und wesentlich erweiterte Auflage 2025

Alle im Buch verwendeten Begriffe verstehen sich geschlechterneutral. Aus Gründen der besseren Lesbarkeit wird auf eine geschlechtsspezifische Differenzierung verzichtet – entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat lediglich redaktionelle Gründe und beinhaltet keine Wertung.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.de> abrufbar.

I S B N 978-3-8005-1931-6

dfv' Mediengruppe

© 2025 Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft,
Mainzer Landstr. 251, 60326 Frankfurt am Main, buchverlag@ruw.de
www.ruw.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Satzkonvertierung: Lichtsatz Michael Glaese GmbH, 69502 Hemsbach

Druck und Verarbeitung: Beltz Bad Langensalza GmbH, 99947 Bad Langensalza

Printed in Germany

Vorwort zur 3. Auflage

Wie wenig andere Themenbereiche ist Compliance durch eine anhaltende Dynamik geprägt, die aus vielfältigen Aktivitäten des Gesetzgebers und der Gerichte sowie durch neue Entwicklungen in Rechtswissenschaft und Unternehmenspraxis resultiert. Dies gilt insbesondere für neue und wachsende Anforderungen im Bereich der sog. „ESG-Compliance“, für größer werdende Compliance-Herausforderungen im Zuge der Digitalisierung (insbesondere im Zusammenhang adäquater „Cyber-Security“) sowie für gestiegene Risiken bei grenzüberschreitender Geschäftstätigkeit (Stichwort „Sanctions Compliance“). Zugleich zeigen neuere Entwicklungen der „Lieferketten-Compliance“, dass sich die Reichweite bestimmter Compliance-Pflichten über den eigenen Unternehmensbereich hinaus erweitert. Die Notwendigkeit für ein Compliance Management im Sinne wirksamer organisatorischer Vorkehrungen zur Verhinderung von Regelverstößen, zur Aufdeckung und Sanktionierung von „Non-Compliance“ sowie zur regelmäßigen Aktualisierung der etablierten Strukturen und Maßnahmen wird dadurch immer größer. Für die Geschäftsleiter stellt sich die erfolgreiche und dauerhafte Implementierung eines wirksamen Compliance Managements daher dauerhaft als eine zentrale und zugleich anspruchsvolle Führungsaufgabe dar.

Mit der Neuauflage greifen wir aktuelle Entwicklungen in Gesetzgebung, Rechtsprechung und Rechtswissenschaft auf und zeigen am Beispiel zentraler Compliance-Fragen, welchen Anforderungen ein erfolgreiches Compliance Management genügen sollte und wie eine dauerhafte Implementierung gelingen kann. Mit vielfältigen Perspektiven und Handlungsempfehlungen unserer Autorinnen und Autoren aus Praxis und Wissenschaft wollen wir auch mit der Neuauflage wieder dazu beitragen, ein wirkungsvolles Compliance Management zu etablieren und aktuell zu halten.

Mein herzlicher Dank gilt allen Autorinnen und Autoren, welche ihr umfassendes Know-how und ihre langjährigen Erfahrungen in diese Neuauflage eingebracht haben. Mein besonderer Dank gilt ferner Frau Nadine Grüttner, die als Lektorin das Manuskript, ebenso wie bei den Voraufgaben, umsichtig und umfassend betreut hat. Herrn Verlagsleiter Patrick Orth danke ich herzlich für wertvolle redaktionelle Hinweise.

Frankfurt am Main, im November 2024

Martin R. Schulz

Verzeichnis der Autorinnen und Autoren

Wolfram Bartuschka, Wirtschaftsprüfer und Steuerberater, ist als Partner für PwC in München tätig und berät seit über 25 Jahren Mandanten bei der Umsetzung von Anforderungen in den Bereichen (Tax) Compliance, Governance, interne Kontrollsysteme insbesondere beim Einsatz neuer Technologien. Darüber hinaus prüft er im Rahmen von Jahresabschluss- und Sonderprüfungen Corporate Governance Systeme. Er publiziert und hält Vorträge zu diesen Themen und betreut vor allem mittelständische und Familienunternehmen.

Philipp Becker ist Senior Legal Counsel im Bereich Litigation und Investigation bei der Zurich Insurance Company Ltd. Sein Dienstsitz ist Zürich. Zuvor war er Principal Associate in den Bereichen IP/IT und Dispute Resolution bei der Rechtsanwaltskanzlei Freshfields Bruckhaus Deringer LLP in Köln. Er veröffentlicht und spricht regelmäßig zu den Themen Datenschutz, Compliance und Investigation.

Carsten Beisheim ist Rechtsanwalt und Partner bei GvW Graf von Westphalen. Er berät industrieübergreifend insbesondere auf den Gebieten Compliance, ESG bzw. Nachhaltigkeit sowie in Fragen der IT Governance. Aus seinen früheren Tätigkeiten für eine internationale Wirtschaftskanzlei sowie als General Counsel und Chief Compliance Officer in namhaften Konzernen (börsennotiertes Finanzkonglomerat und Mischkonzern in Familienbesitz) verfügt er über umfangreiche Kenntnisse und Erfahrungen in der Rechts- und Compliance-Beratung sowie auf den Gebieten der Nachhaltigkeit und Informationssicherheit. Das Deutsche Rechnungslegungs Standards Committee (DRSC), den deutschen Standardsetzer im Bereich der Bilanzierung, unterstützt Carsten Beisheim im Fachausschuss ESG-Reporting.

Prof. Dr. Daniel Benkert ist Rechtsanwalt und Gründungspartner der international ausgerichteten Frankfurter Wirtschaftssozietät METIS Rechtsanwälte PartG mbB. Zuvor war er acht Jahre lang für die Großkanzlei Freshfields Bruckhaus Deringer LLP tätig. Er ist Fachanwalt für Arbeitsrecht und berät in allen Fragen von Arbeitsrecht, Konfliktlösung und Compliance. Zudem hat Benkert bereits zahlreiche Transaktionen und Umstrukturierungen arbeitsrechtlich begleitet. Benkert ist unter anderem Mitautor eines Standardkommentars zum Kündigungsschutzgesetz und hält In-house-Schulungen zu Compliance-Standards ab.

Dr. Viola Bensinger ist Partnerin der Kanzlei Greenberg Traurig und leitet in Deutschland den Bereich Technologie. Sie ist außerdem Co-Chair der globalen Praxisgruppen IP & Technology sowie Data, Privacy & Cyber Security. Sie berät deutsche und internationale Internet-, Technologie- und Gesundheitsunternehmen, insbesondere in den Bereichen Digitalisierung, E-Commerce, digitale Zahlungsdienstleistungen, Lizenzierungen und Vertrieb, Compliance, Insolvenzen, Datenschutz, Cloud Computing sowie Outsourcing. Bensinger veranstaltet

interdisziplinäre Schulungen für Cyber Crisis-Situationen und ist Herausgeberin und Autorin zahlreicher Publikationen zum IT- und Internetrecht.

Florian Block ist Rechtsanwalt und Partner bei CMS in Deutschland, München, im Bereich Compliance & Forensic Services. Er verfügt über umfassende Erfahrung beim Auf- oder Ausbau von Compliance-Strukturen und bei der Einrichtung von europa- und weltweiten Hinweisgebersystemen. Florian Block ist für eine Vielzahl von Unternehmen als Meldestellenbeauftragter bzw. Ombudsmann tätig. Er hat zudem große Erfahrung in der Aufarbeitung von Compliance-Verstößen und unterstützt Unternehmen bei internen Ermittlungen, behördlichen Untersuchungen und der Rückgewinnung von Vermögenswerten sowie der außergerichtlichen und gerichtlichen Durchsetzung von Schadensersatzansprüchen.

Prof. Dr. Benjamin von Bodungen, LL.M. (Auckland), ist Partner der internationalen Anwaltssozietät Bird & Bird LLP in Frankfurt am Main und gehört dort der Praxisgruppe Finanzierung und Finanzregulierung sowie der Sektorgruppe Automotive an. Ein Schwerpunkt seiner Praxis liegt im Bereich grenzüberschreitender Finanzierungen, insbesondere was die Finanzierung mobiler Ausrüstungsgegenstände wie Luftfahrzeuge, Eisenbahnrollmaterial und Schiffe anbelangt. Ebenso berät er Mandanten zum nationalen und internationalen Transport-, Verkehrs- und Logistikrecht, wobei ein besonderer Schwerpunkt auf den zulassungs- und haftungsrechtlichen Aspekten des autonomen Fahrens liegt.

Dietmar Böhlke, MBA (Warwick), ist Rechtsanwalt und Leiter der deutschen Rechtsabteilung der CGI Deutschland B.V. & Co. KG. In dieser Funktion berät er die Gesellschaft und den Datenschutzbeauftragten auch datenschutzrechtlich. Zuvor war er zwölf Jahre lang für die Media-Saturn-Holding GmbH und die Ceconomy AG u. a. als Konzerndatenschutzbeauftragter und Bereichsleiter der Rechtsabteilung tätig. Weitere berufliche Stationen waren davor die Kanzlei SKW Schwarz sowie die T-Systems International GmbH. Er veröffentlicht und spricht regelmäßig zu den Themen IT-Recht und Datenschutz.

Dr. Marcus Böttger ist Rechtsanwalt und Fachanwalt für Strafrecht. Als Gründungspartner der Kanzlei VBB Rechtsanwälte (Düsseldorf · Essen · Karlsruhe) ist er ausschließlich in den Bereichen Wirtschafts- und Steuerstrafrecht sowie in der Compliance-Beratung tätig. Neben seiner Tätigkeit als Dozent z.B. für die German Graduate School of Management and Law (GGS), das Bundeskriminalamt oder die Deutsche AnwaltAkademie war er bis 2017 Richter am Amtsgericht des Landes Nordrhein-Westfalen. Er veröffentlicht regelmäßig in den Bereichen Wirtschaftsstrafrecht und Compliance.

Dr. Bernd Federmann, LL.M., seit 2007 Rechtsanwalt bei KPMG Law. Er ist Partner der Kanzlei, leitet deren Stuttgarter Standort und ist EMA Head of Compliance sowie Global Legal Sector Head of Industrial Manufacturing von KPMG Law. Er berät Unternehmen beim Auf- und Ausbau ihrer Governance-

Systeme und unterstützt sie in deren Regelbetrieb. Bernd Federmann ist Mitautor zahlreicher Veröffentlichungen im Governance- und Compliance-Kontext.

Armin Fladung ist Gründer und Geschäftsführer des CAD-Institut für Compliance, Arbeitsrecht und Datenschutz. Seit über 20 Jahren unterstützt er als Rechtsanwalt, Compliance-Officer und Datenschutzbeauftragter vor allem Unternehmen, Verbände sowie Stiftungen bei der Einführung von Compliance- und Datenschutz-Managementsystemen auch hinsichtlich arbeitsrechtlicher Herausforderungen. Armin Fladung ist zudem zertifizierter KI-Manager (DFKI) und Autor zahlreicher Fachveröffentlichungen.

Prof. Dr. Kai Förstl ist Professor für Supply Chain Management an der EBS Business School und Leiter der EBS Executive School. Er promovierte an der EBS Universität für Wirtschaft und Recht und war anschließend als Postdoc am Fraunhofer Center for Applied Research on Supply Chain Services. Vor seiner Rückkehr an die EBS war er in seiner vorherigen Position Professor für Supply Chain Management und Logistik an der German Graduate School of Management and Law (GGS), Heilbronn. Er ist Autor und Gutachter diverser internationaler Fachzeitschriften und seine Forschungsinteressen umfassen Global Sourcing, Reshoring und Insourcing, Supply Chain Management Teams und nachhaltiges Supply Chain Management.

Melanie Frankenberger ist Rechtsanwältin in Frankfurt am Main und seit 2016 Syndikusrechtsanwältin und Compliance Counsel bei der Commerzbank AG, Global Markets Compliance. Ihr Fokus liegt auf dem Bereich Wertpapiergeschäft. In der Commerzbank AG verantwortet sie insbesondere das Thema Mitarbeitergeschäfte und erstellt u. a. weltweit gültige Arbeitsanweisungen. Darüber hinaus befasst sie sich mit der Durchführung und Weiterentwicklung der globalen, konzernweiten Risikoanalyse im Hinblick auf das Wertpapiergeschäft. Vor ihrer Tätigkeit bei der Commerzbank AG war sie als Compliance-Beauftragte für mehrere Volks- und Raiffeisenbanken tätig und Rechtsanwältin bei einer amerikanischen Wirtschaftskanzlei im Bereich Bankaufsichtsrecht und Compliance.

Dr. Ulrich Hagel ist Rechtsanwalt, Wirtschaftsmediator und Partner bei HWCL in Berlin. Er war über 25 Jahre in Unternehmen tätig, zuletzt als Chief Compliance & Security Officer eines Weltmarktführers in der Bahnindustrie. Er berät Unternehmen, Verbände und öffentliche Auftraggeber in allen Compliance-Fragen und im Bereich der Konfliktbeilegung (Dispute Resolution). Er unterstützt und berät beim Aufbau und der Weiterentwicklung von Compliance- und Risiko-Managementsystemen, Beschwerdemechanismen und internen Untersuchungen. Bei der Konfliktbeilegung agiert Ulrich Hagel als neutraler Wirtschaftsmediator und Schiedsrichter, bei Mediationsverfahren auch als Parteivertreter (Mediationsanwalt). Ulrich Hagel ist Vorstandsvorsitzender des Europäischen Instituts für Konfliktmanagement (EUCON), Beirat der Deutschen Institution für Schiedsgerichtsbarkeit (DIS) und Mitglied der Arbeitskreise Menschenrechte und Exportkontrolle des Deutschen Instituts für Compliance (DICO).

Prof. Dr. Katharina Hastenrath ist Expertin im Bereich Governance, Compliance und ESG. Sie berät global tätige Unternehmen in vorgenannten Themen. Daneben hält sie eine diesbezügliche Professur an der Züricher Hochschule für Angewandte Wissenschaften (ZHAW) und leitet dort u.a. einen Weiterbildungsmaster in Compliance. Zuvor war sie für drei Unternehmen als Compliance Counsel bzw. Chief Compliance Officerin tätig. Hastenrath ist Dozentin an weiteren renommierten Hochschulen im In- und Ausland, Fachbeirätin und Chefredakteurin des Compliance-Fachjournals „Recht relevant für Compliance Officers“ in der Schweiz.

Dominik Heske, LL.M. (Compliance), ist Rechtsanwalt und seit 2016 Syndikusrechtsanwalt bei der HUGO BOSS AG. Als Compliance & Human Rights Officer leitet er die Compliance Abteilung. Zuvor war er unter anderem als Rechtsanwalt bei CMS in Stuttgart tätig. Der Beitrag stellt ausschließlich die persönliche Auffassung des Verfassers dar.

Sven Jacobs arbeitet als Senior Legal Counsel und EMEA Data Strategy Lead für Cisco Systems im Bereich IT-Lizenzverträge, Datenrecht und regulatorische Marktzugangsbedingungen. Es ist darüber hinaus Lehrbeauftragter für Immaterialgüter- und KI-Recht an der Hector School des Karlsruhe Institute of Technology und Autor diverser Bücher und Aufsätze zu den Themen IT-Compliance, Legal Tech und Datenschutz/Datenrecht.

Dr. Joachim Kaetzler ist Rechtsanwalt und Partner bei CMS in Deutschland, Frankfurt am Main. Seit 1999 berät er Unternehmen innerhalb und außerhalb des Finanzsektors in Compliance-Fragen, insbesondere zur Geldwäsche- und Korruptionsprävention. Er begleitet aktuelle rechtliche Entwicklungen seit vielen Jahren durch Publikationen, Vorträge und Lehrtätigkeit an verschiedenen Hochschulen sowie Bildungseinrichtungen.

Prof. Dr. Oliver Keßler ist Professor für Wirtschaftsrecht an der Hochschule Karlsruhe (HKA). Zuvor hat er über 20 Jahre lang als Rechtsanwalt und Partner führender internationaler Wirtschaftskanzleien Finanzinstitute und Unternehmen bei der Strukturierung und Nutzung von Finanz- und Kapitalmarktprodukten sowie den damit verbundenen Risikomanagement- und Compliance-Themen beraten. Keßler befasst sich heute schwerpunktmäßig mit interdisziplinärer Risikoforschung an der Schnittstelle von Recht und Wirtschaft und publiziert regelmäßig hierzu.

Martin T. Knopp, LL.M., CCP, CAP, CORM, CFE, arbeitet seit 2020 bei einem deutschen Handelsunternehmen, das zu den führenden Unternehmen im Lebensmitteleinzelhandel in Deutschland und Europa zählt. Als Senior Consultant im Bereich HR Compliance International befasst er sich insbesondere mit der konzeptionellen Ausgestaltung und Weiterentwicklung des CMS-Programms HR sowie der Betreuung, Beratung und Unterstützung der Landesgesellschaften bei der Implementierung. Dabei wirkt er maßgeblich bei der Gestaltung und Entwicklung der Methodik zur Durchführung von HR

Compliance-Risikoanalysen mit. Zuvor war er als wissenschaftlicher Mitarbeiter am Institut für Compliance und Unternehmensrecht (ICU) der German Graduate School of Management & Law (GGS) in Heilbronn tätig.

Till Komma ist Rechtsanwalt bei CMS in Deutschland, Frankfurt am Main. Dort berät er Unternehmen im Bereich des Wirtschaftsstrafrechts sowie zu Compliance-Angelegenheiten. Er ist auf die unternehmensinterne Prävention von Geldwäsche, Korruption und Betrug sowie die Durchführung von internen Untersuchungen spezialisiert. Darüber hinaus begleitet er Mandanten bei der Entwicklung, Einführung und Verbesserung von Compliance-Management-Programmen.

Marcel Moussaoui ist Rechtsanwalt und Senior Associate bei CMS in Deutschland, Frankfurt am Main. Er ist spezialisiert auf den Bereich Compliance. Er berät nationale und internationale Unternehmen des Finanz- und des Nichtfinanzsektors zu Rechtsfragen im Bereich Anti-Financial Crime (Geldwäscheprevention, Prävention von Verstößen gegen Finanzsanktionen). Zudem begleitet er Unternehmen bei allen compliance-relevanten Fragestellungen im Tagesgeschäft. Er verfügt zudem über umfangreiche Erfahrung bei der Durchführung von internen Untersuchungen.

Dr. Oliver Mross, Rechtsanwalt, ist Leiter des Compliance Office bei der HELLA GmbH & Co. KGaA, Lippstadt. Zu seinem Aufgabenbereich gehören die Bereiche Kartellrecht und Korruptionsprävention sowie das bereichsübergreifende Compliance-Management-System. Vor seiner Tätigkeit bei HELLA war er als Rechtsanwalt für eine internationale Wirtschaftskanzlei mit Schwerpunkt Kartellrecht tätig.

Dr. Manfred Rack ist Rechtsanwalt und Notar bei Rack Rechtsanwälte, Frankfurt am Main. Seine Arbeitsschwerpunkte liegen im Compliance- und Risikomanagement. Er ist Herausgeber des EDV-gestützten Managementsystems „Recht im Betrieb“: Umwelt- und arbeitsschutzrechtliche Betriebsorganisation, Bank- und Kapitalmarktrecht, Pflichtenmanagement für Vorstand, Geschäftsführer und Aufsichtsrat. Er publiziert regelmäßig zu den Themen Risikomanagement und Organisationsrecht in der Zeitschrift „Compliance Berater“.

Dr. Christian Rau, LL.M. (Georgetown), verfügt über langjährige Erfahrungen im In- und Ausland, als Rechtsanwalt, In-House Counsel, Manager und Dozent, vor allem in den Bereichen Governance, Compliance, Risk, M&A und US-Litigation. 2007 übernahm er, nach beruflichen Stationen bei Freshfields in Berlin und Johnson & Johnson in Brüssel und New Jersey, den globalen Konzernbereich Recht und Compliance beim Dax-Konzern Linde AG in München. Seit 2018 verantwortet er als Chief Compliance Officer und Head of GRC EMEA beim japanischen Medizintechnikunternehmen Olympus die Bereiche Governance, Risk, Compliance, Datenschutz und Information Security. Dr. Rau absolvierte seine juristische Ausbildung in Freiburg, Genf, Washington D.C. und Berlin. Er lebt und arbeitet in Hamburg.

RA Hartmut T. Renz ist Partner Regulatory, Risk & Compliance Advisory bei der STRATECO GmbH sowie Co-CEO der TRECCERT GmbH, Hannover. Er war zuvor in verantwortlichen (Chief-)Compliance Officer- und weiteren Leitungsfunktionen unter anderem bei der DZ Bank AG, Helaba, LBBW und Citigroup tätig. Ferner ist er Dozent an der Universität Zürich, Schweiz, der Universität Vaduz, Liechtenstein, sowie der Frankfurt School of Finance and Management, Frankfurt am Main, Deutschland, und war Dozent an der Universität St. Gallen, Schweiz.

Frank Romeike ist Gründer und geschäftsführender Gesellschafter des Kompetenzzentrums RiskNET – The Risk Management Network. In seiner beruflichen Vergangenheit war er Chief Risk Officer bei der IBM Central Europe. Er hat u. a. ein wirtschaftswissenschaftliches und mathematisches Studium abgeschlossen. Im Anschluss hat er Politikwissenschaften, Psychologie und Philosophie studiert. Außerdem hat er ein exekutives Masterstudium im Bereich Risiko- und Compliance Management abgeschlossen.

Charlotte Salathé ist Rechtsanwältin und Counsel bei CMS in Deutschland, Frankfurt am Main. Sie berät nationale und internationale Unternehmen des Finanz- und des Nichtfinanzsektors umfassend bei compliance-bezogenen Fragestellungen. Ihr Fokus liegt auf den Bereichen Geldwäsche-, Korruptions- und Betrugsprävention sowie auf Fragen des Außenwirtschaftsrechts. Sie begleitet Mandanten bei der Konzeption und Durchführung von Compliance-Risikoplanalysen sowie der Entwicklung, Überarbeitung und Implementierung von Compliance-Management-Systemen, der Durchführung von internen Untersuchungen und unterstützt Mandanten bei allen compliance-relevanten Fragestellungen im Tagesgeschäft.

Dr. Christian Scherer ist Fachanwalt für Vergaberecht und für Verwaltungsrecht sowie Partner bei CMS in Deutschland, Köln. Er verfügt über reichhaltige Erfahrung mit der Beratung von Bietern und öffentlichen Auftraggebern zum Vergaberecht, einschließlich der Vertretung in Vergabenachprüfungsverfahren. Zu seinen Tätigkeitsschwerpunkten gehört die Begleitung von Unternehmen in Vergabeverfahren zur Vermeidung von Vergabefehlern und Entwicklung von Strategien bei Compliance-Verstößen genauso wie die Unterstützung von Vergabestellen bei der Strukturierung und Durchführung von Beschaffungen.

Prof. Dr. Martin C. Schleper ist Professor für Supply Chain Management und Nachhaltigkeit an der NEOMA Business School in Reims, Frankreich. Nach seiner Promotion und Projektleitung an der EBS Universität für Wirtschaft und Recht in Wiesbaden arbeitete er an der German Graduate School of Management & Law (GGS) in Heilbronn, an der University of Nottingham, UK und an der University of Sussex, UK. Er ist Autor und Gutachter diverser internationaler Fachzeitschriften und In seiner Forschung untersucht er nachhaltiges und ethisches Supply Chain Management, Aspekte des Risikomanagements und der Resilienz in Lieferketten sowie Käufer-Lieferanten-Beziehungen im Allgemeinen.

Prof. Dr. Martin R. Schulz, LL.M (Yale), ist Rechtsanwalt und Counsel bei CMS in Deutschland, Frankfurt am Main. Ferner ist er Professor für Wirtschaftsrecht an der IU Internationale Hochschule, Erfurt. Seine Publikations- und Tätigkeitsschwerpunkte sind Gesellschaftsrecht, Compliance Management im Unternehmen sowie Wissensmanagement für Juristen. Im Fokus stehen dabei die erfolgreiche Umsetzung von Compliance-Maßnahmen im Unternehmen, Compliance-Fragen in Lieferketten sowie die Implementierung von Wissens- und Innovationsmanagement in Kanzleien. Zu diesen Themen hat Martin Schulz zahlreiche Beiträge in deutscher und englischer Sprache veröffentlicht.

Dr. Tobias Schwartz ist Rechtsanwalt, Fachanwalt für Steuerrecht und Partner bei Flick Gocke Schaumburg in Bonn. Seine Kompetenzfelder liegen insbesondere in der Beratung von Unternehmen in Fragen der Tax Compliance sowie des Steuerstraf- und Wirtschaftsstrafrechts. Er ist Lehrbeauftragter für Steuerstrafrecht an der Universität Bayreuth und veröffentlicht daneben regelmäßig zu den Themen Tax Compliance und Steuerstrafrecht.

Prof. Dr. Daniela Seeliger ist Partnerin im Fachbereich Kartellrecht & Investitionskontrolle bei Linklaters LLP in Düsseldorf. Sie hat umfangreiche Expertise im Rahmen kartellrechtlicher Untersuchungen und der Umsetzung von Compliance-Programmen. Sie ist Non-Governmental Advisor im International Competition Network (ICN) und war Mitglied der Kommission „Wettbewerbsrecht 4.0“ des Bundesministeriums für Wirtschaft und Klimaschutz. Seit Dezember 2018 ist sie im Vorstand der Studienvereinigung Kartellrecht e. V. vertreten.

Nina Seydel, Rechtsanwältin, ist als Associate im Bereich Kartellrecht & Investitionskontrolle bei Linklaters LLP in Düsseldorf tätig. Sie ist spezialisiert auf das Investitionskontrollrecht sowie europäisches und deutsches Kartellrecht, mit einem besonderen Fokus auf Kartellverfahren, Compliance, Missbrauchsaufsicht und Fusionskontrolle. Sie vertritt dabei Mandanten vor der Europäischen Kommission und dem Bundeskartellamt sowie vor europäischen und deutschen Gerichten.

Dr. Thomas Sonnenberg ist seit 2016 Rechtsanwalt und Partner bei CMS in Deutschland, Köln. Seine Beratungsschwerpunkte sind Corporate Governance, Compliance und M&A. Vor seiner Tätigkeit für CMS war er fast 25 Jahre lang in Rechtsabteilungen bekannter Unternehmen tätig, so u.a. als Chefsyndikus der Privatbank Sal. Oppenheim jr. & Cie. und der Ferrostaal AG sowie als Group General Counsel und Group Compliance Officer der Hochtief AG und schließlich als Head of Governance für den Private Equity Fonds Triton. Die EU-Hinweisgeberrichtlinie und das deutsche Umsetzungsgesetz hat er von Beginn an mit Vorträgen und Veröffentlichungen intensiv begleitet.

Prof. Dr. Christopher Stehr studierte Politik- und Wirtschaftswissenschaften an der Universität von München. 2003 gründete er die Unternehmensbera-

tung Polymundo, welche den Fokus Globalisierungsthemen, strategische Beratung und Coaching hat. Zwischen 2003 und 2009 war er Habilitand/Assistent an der Fakultät für Mathematik und Wirtschaftswissenschaften der Universität Ulm im Institut für Unternehmensplanung. Später wurde er Professor für Internationales und Interkulturelles Management sowie Studiengangsleiter International Business an der Karlsruhochschule International University. Von Oktober 2010 bis Dezember 2020 war Stehr Professor für Internationales Management an der German Graduate School of Management and Law (GGS) in Heilbronn. Seitdem ist er bei der von ihm gegründeten Unternehmung Polymundo AG Aufsichtsrat und an verschiedenen Universitäten und Hochschulen (u.a. in Rio de Janeiro, Budapest) als Gastdozent tätig. 2012 initiierte er zudem die sog. Heilbronner Erklärung, eine freiwillige Selbstverpflichtung mit dem Schwerpunkt CSR zwischen aktuell acht Unternehmen der Region Heilbronn-Franken. Seine Forschungsschwerpunkte sind: Internationalisierung von KMU, CSR und Nachhaltigkeit sowie Interkulturelle Kompetenz.

Dr. Thomas Uhlig ist seit 2010 Rechtsanwalt bei KPMG Law. Er ist Partner der Kanzlei und leitet den Bereich Allgemeines Wirtschaftsrecht und Handelsrecht. Er hat langjährige Erfahrung bei der Beratung international tätiger Unternehmen in den Schwerpunkten Compliance- und Governance-Organisation, Produkt-Compliance sowie Lieferketten-Compliance. In diesen Kontext hat er zahlreiche nationale und internationale Projekte geleitet.

Dr. Benjamin Ullrich, M.Jur (Oxford), ist Rechtsanwalt und Partner der Sozietät YPOG in Berlin. YPOG ist eine Spezialkanzlei für Steuern, Fonds, Gesellschaftsrecht (einschließlich Transaktionen und Litigation), Compliance und Banking + Finance. Benjamin Ullrich ist spezialisiert auf Corporate Compliance sowie M&A- und Venture-Capital-Transaktionen. Im JUVE-Handbuch Wirtschaftskanzleien wird er als „stark in Transaktionen“ ausgezeichnet und die Wirtschaftswoche führt ihn als einen der führenden M&A-Anwälte des Landes.

Klaus G. Walter, Rechtsanwalt und Fachanwalt für Strafrecht, berät in Frankfurt am Main mit seiner Kanzlei FM Strafrecht bundesweit Einzelpersonen und Unternehmen in Wirtschaftsstrafsachen zu allen Aspekten laufender Strafverfahren, aber auch präventiv in strafrechtlichen Compliance-Fragen. Zuvor war er als Wirtschaftsstrafrechtsexperte lange Jahre in der Kanzlei Kempf & Dannefeldt tätig. Walter verteidigt und berät seine Mandanten schwerpunktmäßig im Korruptionsstrafrecht sowie im Bankenstrafrecht, einige von ihnen in öffentlich bekannt gewordenen Gerichtsverfahren.

Dr. Florian Wettner ist Rechtsanwalt und Partner der Sozietät METIS Rechtsanwälte PartG mbB. Er ist spezialisiert auf nationale und internationale Prozessführung und Schiedsgerichtsbarkeit. Florian Wettner verfügt über umfangreiche Erfahrung in der Aufarbeitung komplexer Schadens- und Haftungsfälle und deren versicherungsrechtlicher Begleitung (insbesondere im Bereich

D&O- und sonstiger Vermögensschaden-Haftpflichtversicherungen) und berät Unternehmen und deren Organe im Rahmen von Compliance-Untersuchungen.

Michael Wiedmann, Maître en Droit (Poitiers), ist Rechtsanwalt und Partner bei HWCL in Essen und war über 25 Jahre in Unternehmen der Rohstoff- und Automobilindustrie sowie im Handel tätig, zuletzt als Chief Compliance Officer. Er berät Unternehmen aus unterschiedlichen Branchen in allen Compliance-Fragen, insbesondere hinsichtlich Nachhaltigkeitspflichten und ethischer Unternehmensführung. Er unterstützt und berät beim Aufbau und der Weiterentwicklung von Compliance- und Risiko-Managementsystemen, Hinweisgebersystemen und internen Untersuchungen sowie bei Compliance Due Dilligence und der Kommunikation mit Aufsichtsbehörden. Michael Wiedmann ist seit 2019 Co-Leiter des Arbeitskreises Menschenrechte in Unternehmen des Deutschen Instituts für Compliance (DICO).

Inhaltsverzeichnis

Vorwort	V
Verzeichnis der Autorinnen und Autoren	VII
Abkürzungsverzeichnis	LIII

Teil 1

Grundlagen, Erfolgsfaktoren und Handlungsstrategien

1. Kapitel

Compliance Management – Grundlagen, Orientierungshilfen und Erfolgsfaktoren

(Schulz)

I. Grundlagen und Zusammenhänge	1
1. Anhaltende Bedeutung von Compliance und Compliance Management	1
2. Compliance Management als Inbegriff regelkonformer Unternehmensorganisation	5
3. Risiken und Nachteile von Regelverletzungen und „Non-Compliance“	7
4. Funktionen von Compliance und Compliance Management.	9
5. Compliance Management als Daueraufgabe im dynamischen Umfeld	10
6. Compliance als Basis für „Good Corporate Governance“	12
7. Compliance und Reputationsmanagement	14
II. Vorgaben und Orientierungshilfen für das Compliance Management	15
1. Grundlagen der Compliance-Pflicht – Regelungsbeispiele	16
2. Compliance-Pflicht als rechtsformübergreifende Ausprägung der Leitungsverantwortung	20
3. Rechtsprechung zur Compliance-Pflicht.	21
4. Compliance-Anforderungen anderer Rechtsordnungen.	23
a) UK Bribery Act (Vereinigtes Königreich)	24
b) Leitfaden des Department of Justice (USA)	24
5. Deutscher Corporate Governance Kodex	26
6. Erkenntnisse des Risikomanagements	26
a) Besonderheiten von Compliance-Risiken	27
b) Mögliche Berücksichtigung integrativer Perspektiven	28
7. Compliance-Standards als Orientierungshilfe (Beispiel IDW PS 980)	29

III. Erfolgsfaktoren für ein wirksames Compliance Management	30
1. Individuelle Konzeption auf Basis des Compliance-Risikoprofils	30
2. Entwicklung einer passenden Compliance-Strategie	31
a) Wahl eines unternehmensspezifischen Organisationsmodells	32
b) Klärung von Zuständigkeiten und Delegationsfragen	32
c) Fokussierung und Prioritätensetzung bei Compliance-Maßnahmen.	33
d) Berücksichtigung des besonderen Compliance-Risikoprofils	35
aa) Systematische Identifikation von Compliance-Risiken	36
bb) Analyse und Bewertung.	37
cc) Implementierung von Risikosteuerungsmaßnahmen	38
dd) Berichterstattung zu Compliance-Risiken	38
ee) Durchführung regelmäßiger Compliance-Audits.	38
3. Förderung und Incentivierung von Regeltreue (Compliance-Kultur)	39
aa) Compliance Commitment durch die Unternehmens- und Verbandsleitung	40
bb) Akzeptanz als Grundlage der Regelbefolgung	41
cc) Kommunikation von Werten und Umgang mit „Regelungslücken“	43
4. Verfassung von Regeln, Richtlinien und Werten.	44
5. Unabhängige Positionierung der Compliance Officer	45
6. Verständliche Schulungen und Fortbildungsprogramme	46
a) Bedarfsanalyse und Zielgruppenorientierung	46
b) Positionierung von Compliance als „Business Enabler“	47
c) Regelmäßige Anpassung der Fortbildungsformate	47
d) Aktive Einbeziehung der Stakeholder	47
7. Integration von Compliance-Themen in die Geschäftsprozesse	48
8. Koordination der Zusammenarbeit mit anderen Unternehmensfunktionen	49
9. Einrichtung von wirksamen Kontrollen und Feedback-Prozessen	49
10. Aufklärung von Verstößen und Betrieb von Hinweisgebersystemen.	50
11. Konsequente Sanktionierung von regelwidrigem Verhalten.	50
12. „Legal Monitoring“ und regelmäßige Aktualisierung	51
13. Angemessene Dokumentation	51
IV. Vorteile eines effektiven Compliance Managements	51
1. Prävention und Reduzierung der Kostenrisiken und Nachteile von „Non-Compliance“	52
2. Schutz von Unternehmen, Leitungsorganen und Unternehmensangehörigen	52
3. Sicherung der Reputation und Vertrauenserhalt der Stakeholder	52
4. Eröffnung und Wahrung rechtlicher Chancen und Gestaltungsoptionen	53

5. Vorteile beim Marketing und im Wettbewerb.	53
6. Verteidigungsmöglichkeiten bei „Non-Compliance“	54
7. Verbesserung von Strukturen und Prozessen	55
V. Zusammenfassung und Empfehlungen	55

2. Kapitel

Compliance Management und Strafrecht

(Böttger)

I. Einführung in die Criminal Compliance	59
II. Strafrechtliche Grundlagen der Compliance-Verpflichtung	67
III. Typische strafrechtliche Compliance-Risiken	72
1. Korruption	74
a) Vorteilsgewährung (§ 333 StGB)	77
b) Bestechung (§ 334 StGB)	84
c) Bestechung von Mandatsträgern (§ 108e StGB)	86
d) Bestechung im geschäftlichen Verkehr (§ 299 Abs. 2 StGB) ..	89
e) Bestechlichkeit im geschäftlichen Verkehr (§ 299 Abs. 1 StGB)	93
f) Bestechung im Gesundheitswesen (§ 299b StGB)	94
g) Auslandskorruption	96
h) Korruptionsdelikte im weiteren Sinne	100
2. Untreue (§ 266 StGB)	102
a) Generierung von Bestechungsgeld	103
b) Zahlung von Bestechungsgeld	104
3. Steuerverkürzung (§§ 370 ff. AO)	105
IV. Strafrechtliche Risiken der Non-Compliance für die Verantwortlichen des Unternehmens	109
1. Originäre strafrechtliche Verantwortlichkeit	109
a) Verantwortlichkeit der Geschäftsleitung	110
b) Gremienentscheidungen	111
c) Delegation von Verantwortungsbereichen	112
d) Verantwortlichkeit des Compliance Officers	114
e) Aufsichtsrat	116
2. Innerbetriebliche Anweisungen/Täterschaft kraft Organisationsherrschaft	118
3. Fahrlässigkeitshaftung (sog. Organisationsverschulden)	119
4. Verletzung der Aufsichtspflicht in Betrieben und Unternehmen (§ 130 OWiG)	120

V. Strafrechtliche Risiken der Non-Compliance für das Unternehmen	123
1. (Unternehmens-)Strafrecht	123
a) Überblick	123
b) Einziehung	124
c) Das Unternehmen als Nebenbeteiligter im Strafverfahren	127
2. Ordnungswidrigkeitenrecht	127
a) Verbandsgeldbuße gem. § 30 OWiG	127
b) Das Unternehmen als Nebenbeteiligter im Verfahren wegen § 30 OWiG	130
c) Einziehung (§ 29a OWiG)	130
VI. Sonstige Risiken für das Unternehmen und seine Verantwortlichen	131
1. Blacklisting und Vergabesperren	131
a) Registereintragungen	131
aa) Bundeszentralregister	131
bb) Gewerbezentralregister	131
cc) Vergabe- bzw. Wettbewerbsregister	132
dd) Sonstige Register	134
b) Vergaberechtliche Konsequenzen	135
2. Inhabilität (§§ 70 StGB, 6 GmbHG, 76 AktG)	136
3. Aufsichtsrechtliche Konsequenzen	138
VII. Strafrechtliche Risiken innerhalb des Compliance-Prozesses („Failed Compliance“)	138

3. Kapitel

Compliance Management als Schnittstellenaufgabe – Überlegungen und Empfehlungen zur erfolgreichen Zusammenarbeit mit anderen Unternehmensfunktionen

(Rau)

I. Einleitung	143
II. Unternehmensfunktionen und ihre Interaktion im Sinne der Compliance	144
1. Geschäftsleitung	145
2. Aufsichtsrat	149
3. Rechtsabteilung	151
4. Personalabteilung	154
5. Betriebsrat	155
6. Finanzfunktion	157
7. Innenrevision	158
8. Wirtschaftsprüfer	160
9. Unternehmenskommunikation	161
10. Andere	163

11. Von Compliance zu GRC – der Weg zu einer integrierten Governance-, Risiko- und Compliance-Funktion und die Herausforderungen durch ESG	164
12. Fallbeispiel	165
III. Fazit	167

4. Kapitel

Einführung eines „Code of Conduct“

(Benkert)

I. Einleitung	171
II. Ausgestaltung	172
1. Erscheinungsformen	172
2. Typische Regelungen	175
III. Einführung eines „Code of Conduct“	177
1. Individualvertragliche Umsetzung	178
a) Weisungsrecht des Arbeitgebers	178
b) Vertragliche Vereinbarung	180
c) Änderungskündigung	182
2. Betriebsvereinbarung	182
IV. Datenschutzrechtliche Implikation	185
V. Mitbestimmungsrecht des Betriebsrats	186

5. Kapitel

Hinweisgebersysteme – Aufbau und Management

(Block/Sonnenberg)

I. Einleitung	191
1. Begriffsbestimmung	193
2. Gründe für die Einführung eines Hinweisgebersystems („Whistleblowing-Systems“)	193
3. Aktuelle Rechtliche Rahmenbedingungen	195
a) Internationale Anforderungen	195
aa) Sarbanes-Oxley Act (SOX) (USA)	196
bb) Dodd-Frank Act (USA)	196
cc) UK Bribery Act (Großbritannien)	197
dd) OECD-Übereinkommen vom 17.12.1997	198
b) Rechtslage in Deutschland	199
aa) Gesellschaftsrechtliche Vorgaben	200
bb) Ordnungswidrigkeitenrechtliche Vorgaben	200
cc) Vorgaben des Deutschen Corporate Governance Kodex ..	201
dd) Vorgaben aus der Rechtsprechung	201

II. Die Vorgaben des deutschen Hinweisgeberschutzgesetzes	202
1. Ziel des Gesetzes	202
2. Überblick über den Inhalt des Hinweisgeberschutzgesetzes	203
3. Sachlicher Anwendungsbereich	203
4. Persönlicher Anwendungsbereich des Hinweisgeberschutz- gesetzes	204
5. Voraussetzungen für den Schutz von Hinweisgebern	205
a) Gemeinsame Schutzvoraussetzungen	206
b) Besonderheiten in Abhängigkeit vom Meldeweg	207
aa) Interne Meldungen gemäß § 17 HinSchG	207
bb) Externe Meldungen gemäß § 27 HinSchG	208
cc) Offenlegung gemäß § 32 HinSchG	209
6. Pflicht zur Einrichtung eines internen Hinweisgebersystems.	210
a) Unternehmen des privaten Sektors	210
b) Juristische Personen des öffentlichen Sektors	211
7. Gesetzliche Anforderungen an ein internes Hinweisgebersystem	211
a) Wahrung der Vertraulichkeit	211
b) Meldewege	212
c) Interne Meldestelle	213
d) Exkurs: Interne Meldestellen im Konzern	214
e) Bearbeitung der eingehenden Meldungen	215
f) Dokumentation und Datenschutz	216
8. Pflicht zur Einrichtung externer Meldestellen	217
9. Schutzmaßnahmen	219
a) Verbot von Repressalien und Schutz von Hinweisgebern	219
b) Sanktionen bei Verstößen	221
III. Aufbau/Einführung eines Hinweisgebersystems im Unternehmen .	221
1. Entscheidungen hinsichtlich der konkreten Ausgestaltung.	221
a) Organisation	221
b) Ausgestaltungsmöglichkeiten	222
aa) Kreis der Hinweisgeber	222
bb) Zentrale Meldestelle vs. lokale Meldestellen	223
cc) Meldekanäle	224
dd) Arten der meldbaren Verstöße	227
ee) Anonyme Meldungen	227
ff) Regelungen zur Einführung eines Hinweisgebersystems .	228
2. Kommunikation	229
3. Datenschutzrechtliche Regelungen	230
IV. Die praktische Arbeit mit einem Hinweisgebersystem	232
1. Schutz des Hinweisgebers vor Nachteilen	232
2. Schutz des Betroffenen	233
3. Datenschutzkonformer Umgang mit eingegangenen Hinweisen .	234
V. Fazit	235

6. Kapitel

**Kommunikationsmanagement und Schulungen
(analog und remote)***(Hastenrath)*

I. Einleitung	237
II. Grundzüge zur Kommunikation in der Unternehmenspraxis	238
1. Relevanz der Kommunikation im Unternehmen und bei Compliance	238
2. Kommunikationsmodelle	240
a) Modell zu Konfliktarten als Grundlage für die Kommunikation	240
b) Praxisrelevantes Beispiel	242
III. Ausgewählte Instrumente der Compliance-Kommunikation	245
1. Tone from the Top	245
2. Persönlicher Kontakt mit dem Compliance Officer	246
3. Zusammenarbeit des Compliance Officers mit Schlüsselfunktionen im Unternehmen	246
4. Schriftliche Informationen an die Mitarbeiter	247
5. Compliance im firmeneigenen Intranet	247
IV. Schulungen	248
1. Persönliche Schulungen durch die Compliance-Funktion	248
2. Schulungen mit klassischem E-Learning	249
3. Digitale Schulungen: Schulungen mit Webinaren, Podcasts, Livestreams oder vertonten Präsentationen	250
4. Unterstützung dezentraler Compliance-Funktionen: das Schulungshandbuch	263
V. Die „Top 5 Stolpersteine“ in der Compliance-Kommunikation und Lösungsvorschläge	265
1. Fehlende, verspätete oder missverständliche Information	265
a) Problemstellung	265
b) Lösungsvorschlag	266
2. Mangelnde Authentizität („Nicht gelebte Hochglanzaussagen“).	267
a) Problemstellung	267
b) Lösungsvorschlag	267
3. Fehler im Kommunikationsmanagement: Budget- und Ressourcenmangel	268
a) Problemstellung	268
aa) Unzureichende Übersetzung eines Code of Conduct (CoC)	269
bb) Unzureichendes Schulungsbudget	270
b) Lösungsvorschlag	271

4. Probleme mit der Technik	271
a) Problemstellung	271
b) Lösungsvorschlag	272
5. Fehler im Kommunikationsmanagement von Compliance aufgrund von Kulturunterschieden	274
a) Problemstellung	274
b) Lösungsvorschlag	275
VI. Fazit zur Compliance-Kommunikation	276

7. Kapitel

Auswirkungen des ISO-Standards 37301 auf die Prüfung von Compliance-Management-Systemen nach IDW PS 980 und Vergleich mit ISO 31022

(Uhlig/Federmann)

I. Einleitung	279
II. Zielsetzung und Zielgruppe	280
1. Ausgangslage	280
2. Zielsetzung des IDW PS 980	281
3. Zielsetzung des ISO 37301:2021	281
4. Vergleich	282
III. Unterschiedliche Regelungstiefe zur Ausgestaltung des CMS	282
1. CMS-bezogene Regelungsinhalte des IDW PS 980	282
2. Regelungsinhalte des ISO 37301	283
IV. ISO 37301 als geeignetes, angemessenes Rahmenkonzept für ein CMS	286
1. Anforderungen des IDW PS 980 an ein Rahmenkonzept	286
2. Vergleich ISO 37301 Anforderungen mit IDW PS 980-Grundelementen	287
V. Zwischenergebnis	289
VI. Die Legalitätskontrolle als Bindeglied zwischen Risiko- und Compliance-Management?	289
1. Zielsetzung des ISO 31022	291
2. Regelungsinhalte des ISO 31022	291
3. Vergleich zum Compliance-Risiko/Vergleich zur ISO 37301 ...	292
4. Zwischenergebnis	292
VII. Argumente für eine Ausrichtung des CMS nach ISO 37301	293
1. Basis für Ermessensentscheidung und Compliance-Richtlinie ..	293
2. Beurteilung der angemessenen Einrichtung eines wirksamen CMS	295
VIII. Zusammenfassung	296

8. Kapitel

Management interner Untersuchungen*(Wettner/Walter)*

I. Einleitung	299
II. Entscheidung über die Durchführung interner Untersuchungen	300
1. Entscheidungsbefugte Stellen	301
2. Pflicht zur Aufklärung konkreter Verdachtsfälle	301
3. Interne Untersuchung oder externe Ermittlung?	302
a) Bereits laufendes behördliches Verfahren	303
b) (Noch) kein behördliches Verfahren	304
III. Vornahme von Eilmaßnahmen	305
1. Einrichtung einer zentralen Koordinierungsstelle	306
2. Maßnahmen der Daten- und Beweissicherung	306
3. Arbeitsrechtliche Maßnahmen	307
4. Beachtung von Informations- und Berichtspflichten	307
IV. Planung der internen Untersuchung	308
1. Grundlagen der Planung	308
a) Beachtung von Recht- und Verhältnismäßigkeit	308
b) Beachtung von Risiken und Folgen der internen Untersuchung	309
2. Festlegung des Untersuchungsgegenstands	310
3. Bestimmung des Untersuchungsteams und der Verantwortlichkeiten	311
a) Auswahl von Mitarbeitern und externen Beratern	311
b) Festlegung von Verantwortlichkeiten und Berichtswegen	312
4. Bestimmung und Vorbereitung der Informationsquellen	313
a) Relevante Informationsquellen	313
aa) Dokumente	313
bb) Elektronische Daten und E-Mails	313
cc) (Ehemalige) Mitarbeiter	314
b) Notwendige Abstimmung der geplanten Untersuchungsmaßnahmen	315
aa) Beteiligung von Betriebsrat oder Sprecherausschuss	315
bb) Abstimmung mit Ermittlungs- und Aufsichtsbehörden...	315
c) Einrichtung eines Datenraums oder eines „Projektportals“ ...	316
5. Sicherung der Vertraulichkeit	317
a) Zugriffsmöglichkeiten Dritter	317
aa) Beschlagnahme durch Ermittlungsbehörden	317
bb) Herausgabe von Unterlagen an Versicherer	319
b) Begrenzung der E-Mail- und sonstigen schriftlichen Kommunikation	319

c) Kennzeichnung und Aufbewahrung geschützter Kommunikation	320
6. Erstellen eines Untersuchungsplans	321
V. Durchführung der internen Untersuchung	321
1. Allgemeine Untersuchungsgrundsätze	321
2. Dokumentation der Untersuchung	322
3. Erhebung und Auswertung von Dokumenten	323
4. Erhebung und Auswertung von elektronischen Daten	324
5. Befragung von Mitarbeitern	324
6. Auswertung und Aufarbeitung der Untersuchungsergebnisse ...	326
VI. Fazit	328

Teil 2

Übergreifende Themen und Herausforderungen

Abschnitt 2.1

Risiko und Governance

9. Kapitel

Risiko- und Chancenmanagement – Erfolgsfaktoren für eine wirksame Umsetzung

(Romeike)

I. Corporate Governance und das Management von Chancen und Risiken	331
1. Grundlagen und Einführung	331
2. Die Odyssee und der Umgang mit Risiken	333
3. Risikomanagement als zentraler Erfolgsfaktor	335
4. Überblick über aktuelle regulatorische Entwicklungen	335
5. Krisenfrüherkennung gemäß Unternehmensstabilisierungs- und -restrukturierungsgesetz (StaRUG)	336
6. FISG fordert Internes Kontrollsystem und Risikomanagement- system	338
II. Abgrenzung des Risiko- und Chancenbegriffs	339
III. Nutzen eines wirksamen Chancen- und Risikomanagements	342
IV. Unterscheidung von Ursachen – Risiken – Wirkungen	344
V. Verknüpfung von Risikomanagement und Strategie	347
VI. Der Risikomanagement-Prozess als Regelkreis	349

VII. Methoden zur Risikoidentifikation und -bewertung	353
VIII. Aggregation von Risiken	356
IX. Maßnahmen zur Risikosteuerung	357
X. Unterschiedliche Reifegrade im Risikomanagement	360
XI. Fazit und Ausblick	361

10. Kapitel

Auditverfahren: Compliance als Dauerpflcht

(Rack)

I. Einleitung	367
II. Die Dauerpflcht zur Sicherstellung der dauerhaften Wirksamkeit des CMS nach DIN und EMAS	367
III. Die Beweislast für Vorstände und Geschäftsführer	369
IV. Die Unvorhersehbarkeit von Rechtsverstößen als Grund für Compliance als Dauerpflcht	369
V. Zertifikate sind bloße Momentaufnahmen ohne Nachweis dauerhafter Wirksamkeit eines CMS	369
VI. Das Stichprobenargument in Rechtsprechung und Literatur	370
VII. Der erfolglose Entlastungsversuch durch den Hinweis auf Regeln ohne Anwendung	372
VIII. Die Haftung von Vorständen und Geschäftsführern für fehlende und fehlerhafte CMS nach der Rechtsprechung	375
IX. Die Haftung von Auditoren und Umweltgutachtern gegenüber dem zertifizierten Unternehmen nach der Expertenhaftung	375
X. Die Expertenhaftung von Auditoren und Umweltgutachtern gegenüber Dritten	377
XI. Aufsicht und Sanktionen von Behörden gegen Umweltgutachter und Auditoren für falsche Zertifikate nach dem Auditverfahren ...	378
XII. Der Gesetzeszweck des UAG	378
XIII. Die Zulassung	378
XIV. Die Aufsicht	379

XV. Die Konkretisierung des UAG durch Richtlinien des Umweltgutachterausschusses.	379
XVI. Mehr Risiken durch Anordnungen, Untersagungen und Widerruf der Zulassung für Umweltgutachter und Auditoren durch Hinweise auf Rechtsverstöße nach dem Hinweisgeberschutzgesetz.	380
XVII. Mehr Risiken für Umweltgutachter und Auditoren durch den erweiterten Kreis der Hinweisgeber außerhalb der Unternehmensbelegschaft.	381
XVIII. Fazit.	382

11. Kapitel

Governance, Risk und Compliance im Mittelstand – Zusammenhänge und Abhängigkeiten

(Bartuschka)

I. Einleitung – Die Notwendigkeit der Einrichtung von Instrumenten zur Überwachung von Unternehmen.	383
II. Das System der Unternehmensüberwachung.	386
1. Überblick über das Gesamtsystem.	386
2. Externe Komponenten der Unternehmensüberwachung.	386
3. Interne Komponenten der Unternehmensüberwachung.	388
III. Die Verknüpfung der einzelnen Elemente der Unternehmensüberwachung.	389
1. Der GRC-Ansatz.	389
2. Das interne Kontrollsystem und die anderen Elemente der Überwachung des Unternehmens.	390
3. Compliance- und Risikomanagement.	391
4. Risikomanagement und Controlling.	392
5. Interne Revision, Compliance und Risikomanagement.	393
6. Fazit.	393
IV. Grundkonzept für die Ausgestaltung eines integrierten Systems der Überwachung für mittelständisch geprägte Unternehmen.	394
1. Bestimmung der Zielgruppe der Unternehmen.	394
2. Zielstellung für die Einführung eines integrierten Systems der Überwachung.	394
3. Vorgehensweise.	394
a) Risikoanalyse.	395
b) Analyse bestehender Strukturen.	396
c) Ermittlung des Anpassungsbedarfs.	396
d) Umsetzung.	397
4. Fazit.	399

Abschnitt 2.2

Datenschutz und IT-Security

12. Kapitel

Datenschutz im Compliance Management

(Becker/Böhlke/Fladung)

I. Einleitung	401
II. Der konzeptionelle Schutz personenbezogener Daten	405
1. Gesetzliche Grundlagen	405
a) Datenschutzgrundverordnung	405
b) Bundesdatenschutzgesetz	406
c) Landesdatenschutzgesetz	406
d) Europäische Richtlinien und Verordnungen	407
e) Weitere Gesetze mit datenschutzrechtlichen Vorgaben.	408
2. Zentrale Grundsätze	409
a) Verbot mit Erlaubnisvorbehalt	409
b) Prinzip der Verhältnismäßigkeit	412
c) Datensparsamkeit	412
d) Transparenz	413
e) Zweckbindung	413
3. Grundbegriffe	413
a) Personenbezogene Daten	414
b) Verantwortliche Stelle	415
c) Umgang mit personenbezogenen Daten	415
aa) Erheben	416
bb) Speichern	416
cc) Verändern	416
dd) Übermitteln	416
d) Auftragsverarbeitung	419
III. Betrieblicher Datenschutz	420
1. Pragmatischer Ansatz: Wo fange ich an?	420
2. Beratungspraxis	425
a) Der betriebliche Datenschutzbeauftragte	428
b) Prozess der Datenschutzberatung	430
c) Praxisrelevante Beispiele	433
3. Implementierung	435
4. Zusammenarbeit mit Behörden	438
IV. Instrumente der datenschutzrechtlichen Compliance	439
1. Tone from the Top	439
2. Interne Richtlinien	439
a) Datenschutzrichtlinie	440

b) IT-Nutzungsrichtlinie	440
c) E-Mail-Policy	441
d) Social-Media und Messaging-Dienste	442
e) IT-Datenschutzmanagement-Richtlinie (Datenschutzmanagementkonzept)	442
f) Archivierungs- und Löschungsrichtlinie	443
3. Verzeichnis von Verarbeitungstätigkeiten	444
4. Interne Kommunikation und Awareness	445
a) Der Datenschutz-Newsletter	445
b) Intranet	446
c) Der „Datenschutz-Tag“ und Fachtagungen	446
5. Schulungen	446
a) Persönliche Schulungen	447
b) E-Learning/Webinars	448
c) Unterstützung dezentraler Compliance-Funktionen	449
V. Effektive Datenschutzüberwachung	450
1. Audits und Maßnahmenpläne/Quick Self-Assessment	450
2. IT-Infrastruktur-Reviews und Koordinierung mit IT-Security ...	452
3. Incident- und Regel-Reporting aus den Betrieben	452
4. Der Datenschutzjahresbericht	453
5. Bericht an Aufsichtsrat/Compliance-Bericht/Audit Committee .	453
6. Zusammenarbeit mit dem Compliance Officer, IT-Security und Revision	454
VI. Beschäftigtendatenschutz	457
1. Bedeutung des Beschäftigtendatenschutzes für Compliance	457
2. Rechtsgrundlagen für den Umgang mit Mitarbeiterdaten	461
a) Kollektivvereinbarungen zur Nutzung von Mitarbeiterdaten .	461
b) Rechtfertigende Einwilligung des Mitarbeiters	463
c) Arbeitsvertragliche Regelungsmöglichkeiten	464
d) Gesetzliche Erlaubnistatbestände	466
e) Internationaler Datenverkehr mit Beschäftigtendaten	469
3. Risiken beim Umgang mit Beschäftigtendaten	470
a) Phase 1: Begründung des Arbeitsverhältnisses/ „Boarding-Phase“	471
b) Phase 2: Durchführung des Arbeitsverhältnisses/ „On Board-Phase“	471
c) Phase 3: Beendigung des Arbeitsverhältnisses/ „Off Boarding-Phase“	472
4. Zusammenarbeit mit dem Betriebsrat	473
5. Personalleiter und Betriebsrat als Teil des Datenschutz- und Compliance-Teams	475
6. Hinweise, Muster und Beispielsfall	476
a) Hinweise zur Regelung der Nutzung von Beschäftigtendaten	476

b) Hinweise zur Regelung der Nutzung von Internet und E-Mail	478
c) Beispielsfall zur Kontrolle bei Verdacht gegen Mitarbeiter...	481
d) Beispielsfall zum Auskunftsrecht eines Mitarbeiters bei Untersuchungen von Compliance-Verstößen	483
VII. Fazit.....	485

13. Kapitel

IT-Compliance – Software-Lizenzmanagement, Blockchain und Nutzung von Daten

(Jacobs)

I. Rechtliche Herausforderungen der fortschreitenden Digitalisierung und Vernetzung	487
II. Software-Lizenzmanagement.....	487
1. Rechtliche Grundlagen der Nutzung von Computerprogrammen	488
2. Besondere Arten von Software, insbesondere Open-Source-Software	489
3. Software-Lizenzmanagement im Rahmen verantwortungs- bewusster Unternehmensführung	490
4. Rechtsfolgen einer Unterlizenzierung.....	491
III. Software-Lizenzmanagement im Rahmen von Cloud-Diensten	491
1. Nutzungshandlungen beim Cloud Computing.....	491
a) Recht der öffentlichen Zugänglichmachung der Software	492
b) Recht zur Vervielfältigung der Software	493
2. Lizenzmanagement im Zusammenhang mit Cloud Computing- Diensten.....	493
IV. Rechtsrahmen von Softwarelizenz-Audits.....	494
1. Rechtliche Grundlagen für einen Softwarelizenz-Audit	495
2. Vertragliche Ausgestaltung eines Softwarelizenz-Audits	496
V. Rechte an und Zugang zu nicht-personenbezogenen Daten.....	497
1. Regelungsinhalt und Struktur des Data Act	499
2. Datenweitergabe unter dem Data Act	500
a) Allgemeine Pflichten	501
b) Erfasste Datenkategorien	502
c) Datenzugriffsrechte für Nutzer	502
d) Recht der Nutzer auf Datenweitergabe an Dritte	503
3. Verhältnis zum Datenschutzrecht	504
4. Nutzung durch und Weitergabe von Daten durch den Dateninhaber.....	504
5. Missbräuchliche Vertragsklauseln	506
6. Sanktionen.....	506

VI. Wechsel von Datenverarbeitungsdiensten.....	507
VII. Blockchain und Smart Contracts	508
VIII. Implementierung eines IT-Compliance-Systems.....	509

14. Kapitel

Cybersecurity, IT-Sicherheit und Krisenmanagement

(Bensinger)

I. Analyse	511
1. Ziele der IT-Sicherheit	511
2. Cybercrime im Wandel	512
a) Ideelle Hintergründe	513
b) Materielle Hintergründe	516
3. Entwicklungen bei Schutzmaßnahmen.....	516
II. Vorbeugende Maßnahmen	517
1. Adressaten	518
a) KRITIS-Betreiber	518
b) Anbieter von Telemediendiensten	520
c) Anbieter von Telekommunikationsdiensten	521
d) Bank- und Finanzwesen	522
e) Energiewirtschaft.....	522
f) Geschäftsführung von Aktiengesellschaften und GmbHs	523
2. Inhalt der gesetzlichen Verpflichtungen	523
a) BSIG.....	525
aa) Pflichten der KRITIS-Betreiber.....	525
bb) Befugnisse des BSI.....	527
b) KRITIS-Dachgesetz	528
c) DSGVO	529
d) BDSG.....	535
e) TTDSG und TKG.....	535
aa) TTDSG.....	535
bb) TKG.....	535
cc) Verhältnis zur DSGVO	536
f) KWG, ZAG, MaRisk etc.....	537
aa) MaRisk (Mindestanforderungen an das Risikomanagement).....	538
bb) ZAG.....	542
cc) § 27 Abs. 1 ZAG	544
dd) DORA.....	544
ee) Konkurrenz zum BSIG	545
g) EnWG.....	545
h) NIS-Richtlinien	546

i) §§ 76, 91, 93 AktG	547
aa) Ausgestaltung des IT-Risikomanagementsystems	548
bb) Anforderungen nach DSGVO	551
cc) Verantwortungsverteilung innerhalb der Geschäftsleitung	552
dd) Dokumentationspflicht	553
3. Unternehmensinterne Vorkehrungen	553
a) Interne Vorgaben	553
b) Aktuelle technisch-organisatorische Schutzmaßnahmen	554
III. Der Krisenfall	556
1. Hacker-Angriffe erkennen	556
2. Rechtliche Konsequenzen und Handlungsoptionen	556
a) Melde- und Informationspflichten	556
aa) DSGVO	556
(1) Meldung an die Aufsichtsbehörde (Art. 33 DSGVO)	557
(2) Meldung an die Betroffenen (Art. 34 DSGVO)	559
(3) Sanktionen	562
bb) BDSG	562
cc) BSIG	562
dd) ZAG	564
ee) Meldepflichten für Energiewirtschaftsunternehmen	566
ff) TMG	566
gg) TKG	567
hh) Sonstige Informationspflichten	568
b) Werkzeuge zur Abwehr von Cyberangriffen	568
3. Interne und externe Kommunikation	570
4. Mittel- und längerfristige Maßnahmen	570
IV. Ausblick	571

Abschnitt 2.3

ESG und Governance

15. Kapitel

Corporate Social Responsibility und Corporate Compliance – Entwicklungslinien gesellschaftlicher und juristischer Verantwortung von Unternehmen

(Stehr/Knopp)

I. Einleitung	573
1. „Shareholder Value“ und „Stakeholder Value“ – eine „Mission Impossible“ für Unternehmen?	573
2. CSR und Unternehmensführung – Auswirkungen auf die Unternehmen?	575
3. CSR und Unternehmensführung – Wechselwirkungen mit dem Compliance Management	576

II. Grundlagen	577
1. Corporate Social Responsibility	577
a) Bedeutungswandel des Begriffsverständnisses	577
b) Konzeptionen und Modelle	577
c) Definitionen	579
2. Corporate Governance	581
a) Begriffsverständnis	581
b) Corporate Governance und Corporate Social Responsibility ..	581
c) Gesellschaftsrecht und Deutscher Corporate Governance Kodex	583
3. Corporate Compliance	585
a) Begriffsverständnis	585
b) Corporate Compliance und Corporate Governance	586
c) Corporate Compliance als Organisationspflicht	587
d) Aktuelle gesetzliche Entwicklungen in Deutschland und der Europäischen Union	588
III. Corporate Social Responsibility und Regulierungsebenen	590
1. Einführung in die CSR-Regulierung	590
a) Regulierungsebenen	590
b) Regulierungsansätze	590
c) Rechtsqualität	591
d) Reputationsmanagement	592
2. Beispiele für CSR-Regulierung	592
a) Globale Regulierungsebene	592
aa) OECD-Leitsätze für multinationale Unternehmen	592
bb) GRI-Berichtsstandards	593
cc) UN Global Compact	594
dd) ISO 26000	595
b) Internationale Regulierungsebene	596
c) Supranationale bzw. europäische Regulierungsebene	597
d) Nationale bzw. deutsche Regulierungsebene	597
3. CSR-Normenflut als Herausforderung für Unternehmen	599
IV. Corporate Social Responsibility und Corporate Compliance	601
1. Einführung	601
2. Allgemeine Relevanz von CSR-Normen für die Corporate Compliance	603
3. Konkrete Relevanz von CSR-Normen sowie sonstiger CSR-Themen für die Corporate Compliance	604
a) CSR-Normen und CSR-Themen im Compliance- Risikomanagementprozess	605
aa) Schritt 1: Definition der Compliance-Risiken	605
bb) Schritt 2: Identifikation der Compliance-Risiken	605

cc) Schritt 3: Analyse und Bewertung der Compliance-Risiken.....	606
dd) Schritt 4: Berichterstattung der Compliance-Risiken	607
ee) Schritt 5: Steuerung der Compliance-Risiken	607
ff) Schritt 6: Monitoring der Compliance-Risiken.....	608
b) Verknüpfung von CSR- und Compliance-Risiken	608
V. Zusammenfassung	608

16. Kapitel

„ESG-Compliance“: Herausforderungen des Nachhaltigkeitsreportings (Beisheim)

I. Einleitung: Nachhaltigkeit, Corporate Governance und die Rolle von Compliance.....	611
II. Status quo und bald Historie: Die CSR-Richtlinie und das CSR-Richtlinie-Umsetzungsgesetz von 2017.....	614
1. Zielsetzungen der CSR-Richtlinie und des CSR-Richtlinie-Umsetzungsgesetzes	614
2. Neuausrichtung des Nachhaltigkeitsreportings	615
a) Bereits vor dem CSR-RUG vorhandene nichtfinanzielle Berichtspflichten im deutschen Bilanzrecht	616
b) Sog. Soft-Law-Ansätze als Rahmenwerke für das CSR-Reporting	617
c) Paradigmenwechsel	618
3. Adressaten der CSR-Berichtspflichten nach dem CSR-RUG....	619
4. Berichtsanforderungen im Rahmen des Reportings nach der bislang geltenden CSR-Richtlinie	621
a) Berichtsvarianten: Die nichtfinanzielle Erklärung und der gesonderte Bericht	621
b) Inhalte, Relevanzmaßstab und Methodik des CSR-Reportings	623
c) Muster: Struktur und Ansätze zur Gestaltung des CSR-Reportings	626
d) Die Möglichkeit der Verwendung von Rahmenwerken	629
5. Nichtangaben, unrichtige Angaben und ihre Folgen.....	631
a) Der „Comply or Explain“-Grundsatz	631
b) Ein Sonderfall: Das (vorübergehende) Weglassen nachteiliger Angaben	632
c) Prüfungen.....	633
d) Verstöße, Säumnisse und Sanktionen	635
III. Die CSRD: Neue Anforderungen im Nachhaltigkeitsreporting	636
1. Adressaten und Konzernprivileg.....	640

2. Überblick über die ESRS	642
a) Regelungsinhalte des Set 1 der ESRS	643
b) Der Grundsatz der doppelten Wesentlichkeit und weitere Verfahrensvorgaben	647
c) Verortung im Lagebericht und Prüfung	651
d) Erleichterungen im Rahmen der Implementierung des Reportings	652
IV. Der Referentenentwurf zum CSRD-Umsetzungsgesetz und ein weitergehender Ausblick	653

17. Kapitel

Compliance im Kontext nachhaltigen Supply Chain Managements – Die betriebswirtschaftliche Perspektive

(Schleper/Förstl)

I. Einleitung	659
II. Nachhaltiges Lieferantenmanagement	661
1. Lieferantenbewertung	661
2. Lieferantenentwicklung	662
3. Lieferantenauswahl	663
4. Lieferantenmonitoring	663
III. Unterschiede entlang der Lieferkette	664
IV. Menschenrechtsprobleme und Due Diligence – „beyond compliance“	666
V. Praxisrelevanz	669
VI. Fazit	670

18. Kapitel

Lieferkettensorgfaltspflichtengesetz (LkSG) – Einführung und praktische Hinweise zur Umsetzung der Sorgfaltspflichten im Unternehmen

(Heske)

I. Wesentliche Regelungen des LkSG im Überblick	671
1. Entstehung, Zielsetzung und Anwendungsbereich	671
2. Definition der Lieferkette	672
a) Lieferkette nach § 2 Abs. 5 LkSG	672
b) Erfasste Handlungsbereiche im Rahmen der Lieferkette	673
3. Menschenrechtliche und umweltbezogene Risiken und Pflichten	675
a) Menschenrechtliche Risiken	676
b) Umweltbezogene Risiken	676
c) Menschenrechtsbezogene und umweltbezogene Pflichten ...	677

II. Praktische Hinweise zur Umsetzung der Sorgfaltspflichten im Unternehmen	677
1. Verantwortlichkeiten im Rahmen der Einhaltung der Sorgfaltspflichten.....	677
2. Sorgfaltspflichten im Unternehmen nach dem LkSG.....	678
a) Synergien erkennen – Compliance-Management-System nutzen	679
b) Umsetzungsprojekt: Vorüberlegungen zur Implementierung der Sorgfaltspflichten.....	679
c) Die Sorgfaltspflichten im Überblick.....	681
aa) Angemessenes und wirksames Risikomanagement (§ 3 Abs. 1 Nr. 1 LkSG)	682
bb) Festlegung einer betriebsinternen Zuständigkeit (§ 3 Abs. 1 Nr. 2 LkSG)	684
cc) Risikoanalyse (§ 3 Abs. 1 Nr. 3 LkSG)	685
(1) Ziele der Risikoanalyse	685
(2) Bedeutung der Risikoanalyse und Vorüberlegungen	685
(3) Umfang und Inhalt der Risikoanalyse.....	686
(4) Regelmäßige und anlassbezogene Risikoanalyse	689
(5) Unternehmensinterne Kommunikation der Risikoanalyse.....	690
dd) Abgabe einer Grundsatzerklärung (§ 3 Abs. 1 Nr. 4 LkSG)	690
ee) Verankerung von Präventionsmaßnahmen (§ 3 Abs. 1 Nr. 5 LkSG)	692
(1) Präventionsmaßnahmen im eigenen Geschäftsbereich (§ 6 Abs. 3 LkSG)	692
(2) Präventionsmaßnahmen gegenüber unmittelbaren Zulieferern (§ 6 Abs. 4 LkSG)	693
(3) Wirksamkeit und Aktualisierung der Präventionsmaßnahmen (§ 6 Abs. 5 LkSG).....	696
ff) Abhilfemaßnahmen (§ 3 Abs. 1 Nr. 6 LkSG).....	696
(1) Abhilfemaßnahmen im eigenen Geschäftsbereich (§ 7 Abs. 1 LkSG)	696
(2) Abhilfemaßnahmen bei einem unmittelbaren Zulieferer (§ 7 Abs. 2 LkSG).....	697
(3) Wirksamkeit und Aktualisierung der Abhilfemaßnahmen (§ 7 Abs. 4 LkSG).....	698
gg) Einrichtung eines Beschwerdeverfahrens (§ 3 Abs. 1 Nr. 7 LkSG)	698
hh) Risiken bei mittelbaren Zulieferern (§ 3 Abs. 1 Nr. 8 LkSG)	700

(1) Substantiierte Kenntnis (§ 9 Abs. 3 LkSG)	700
(2) Maßnahmen nach Erlangung von substantiierter Kenntnis (§ 9 Abs. 3 LkSG)	701
ii) Dokumentation und Berichterstattung (§ 3 Abs. 1 Nr. 9 LkSG)	702
(1) Dokumentationspflichten (§ 10 Abs. 1 LkSG)	702
(2) Berichtspflicht (§ 10 Abs. 2 LkSG)	702
III. Das BAFA als zuständige Behörde für die Kontrolle und Durchsetzung der Regelungen des LkSG	703
1. FAQs, Handreichungen und sonstige Informationsquellen	703
2. Berichtspflicht und Kontrollen	704
a) Elektronische Berichtspflicht der Unternehmen	704
b) Kontrollbefugnisse des BAFA	705
c) Anordnungen und Maßnahmebefugnisse des BAFA	706
IV. Sanktionen	706
1. Bußgeld und Bemessungsgrundlage	707
2. Ausschluss von der Vergabe öffentlicher Aufträge	707
V. Zivilrechtliche Haftung und Prozessstandschaft	708
VI. Auswirkungen der europäischen Lieferkettenregelung (CSDDD) – Anpassung des LkSG	708

19. Kapitel

Menschenrechtsbeauftragte und Beschwerdebeauftragte nach dem LkSG

(Hagel/Wiedmann)

I. Einleitung	711
II. Menschenrechtsbeauftragte	711
1. Begrifflichkeiten und gesetzliche Grundlagen	711
2. Überwachungsaufgaben	713
3. Anforderungen an Menschenrechtsbeauftragte	715
a) Qualifikation	715
b) Unparteilichkeit, Unabhängigkeit und Weisungsungebundenheit	716
c) Verschwiegenheit	717
4. Ernennung	718
5. Stellung im Unternehmen	718
6. Arbeitsrechtlicher Schutz	721
7. Auslagerung der Funktion	721
8. Haftung	722

III. Beschwerdebeauftragte	723
1. Begrifflichkeiten und gesetzliche Grundlagen	723
2. Aufgaben	724
3. Anforderungen an Beschwerdebeauftragte	726
a) Qualifikation	726
b) Unparteilichkeit, Unabhängigkeit und Weisungsungebundenheit	727
c) Verschwiegenheit	728
4. Ernennung	728
5. Stellung im Unternehmen	728
6. Arbeitsrechtlicher Schutz	729
7. Haftung	729
8. Abgrenzung zum Meldestellenbeauftragten nach HinSchG	729
IV. Verhältnis Menschenrechts- zu Beschwerdebeauftragtem	730
V. Fazit	731

Teil 3

Besondere Aufgaben und Anwendungsfelder

20. Kapitel

Die Compliance-Funktion in einem Kreditinstitut

(Renz/Frankenberger)

I. Einleitung: Was ist die Bedeutung des Begriffs Compliance?	733
II. Welche Compliance-Funktionen gibt es in einem Kreditinstitut? ..	734
1. Kapitalmarkt-Compliance	735
2. Zentrale Stelle/sonstige strafbare Handlungen (inkl. Geldwäscheprävention) sowie Finanzsanktionen und Embargo (Anti-Financial Crime (AFC))	739
3. MaRisk-Compliance	742
4. Hinweisgebersystem (Whistleblowing)	744
5. Datenschutz	746
6. Auslagerung der Compliance-Funktion oder von einzelnen Compliance-Tätigkeiten	748
III. Inhalt und Aufgabe einer modernen Compliance-Funktion	749
IV. Das Compliance-Management-System (CMS)	750
V. Schnittstellen zu anderen Funktionen	754
1. Fachbereiche	755
2. Rechtsbereich	755
3. Risikocontrolling-Funktion	757
4. Interne Revision	757

VI. Compliance als Teil des IKS eines Kreditinstituts.	759
VII. Übertragung der Struktur/des Ansatzes auf andere Industriesäulen – und umgekehrt	764
VIII. Fazit/Ausblick.	766

21. Kapitel

Produktbezogenes Compliance- und Risikomanagement im Treasury

(Keßler)

I. Einleitung	767
II. Finanz- und Kapitalmarktprodukte; Risiken	768
1. „Einfache“ Produkte	768
2. „Komplexe“ Produkte.	769
a) Überblick	769
b) Risiken im Einzelnen	772
III. Rechtliche Anforderungen an das Risikomanagement- und Compliance-System	774
1. Anforderungen an Finanzinstitute	774
a) Aufsichtsrechtliche Anforderungen	774
b) „Best Practice“ und praktische Ausgestaltung.	776
aa) Risikomanagement.	776
(1) Risikomanagementstrategie	777
(2) Risikotragfähigkeitskonzept.	777
(3) Interne Kontrollverfahren	778
(4) Personelle und technische Ausstattung.	778
(5) Notfallkonzept.	778
(6) Nachhaltiges Vergütungssystem	778
bb) Compliance	779
(1) MaRisk BA-Compliance.	779
(2) MaComp-Compliance	780
2. Anforderungen an Unternehmen	780
a) Normativer Rahmen und Übertragbarkeit.	780
b) Grenzen	783
IV. Ausgestaltung des Risikomanagement- und Compliance-Systems im Unternehmensbereich	783
1. Finanzproduktbezogenes Risikomanagement und Compliance – Überblick	783
2. Die Ausgestaltung der wichtigsten ICRM-Komponenten im Einzelnen	785
a) Rechtliche Einzelfallprüfung: Covenant-Tool	785
b) Kreditrisiko-Tool	786

c) Marktrisiko-Tool	787
d) Liquiditätsrisiko-Tool	788
3. Delegation des Risikomanagements und Compliance	788
V. Haftungsfragen	790
1. Verstoß gegen die Pflicht zum Risikomanagement	790
2. Verstoß gegen die Pflicht zur Compliance	792
3. Einsatz von Künstlicher Intelligenz	792
VI. Fazit	793

22. Kapitel

Der Geldwäschebeauftragte – Stellung und Aufgaben

(Kaetzler)

I. Der Geldwäschebeauftragte	795
1. Warum eigentlich ein Geldwäschebeauftragter? – Geschichte einer besonderen Funktion	796
2. Verpflichtete Unternehmen	804
a) Qua Gesetz	804
b) Freistellungsmöglichkeit (§ 7 Abs. 2 GwG)	806
c) Anordnung der Behörden	807
3. Anforderungen an den Geldwäschebeauftragten und Bestellung	808
4. Kompetenzen und Stellung im Unternehmen	810
5. Aufgaben des Geldwäschebeauftragten	814
a) Risikoanalyse	815
b) Sicherungsmaßnahmen	815
c) Antizipation und Implementierung neuer rechtlicher und verwaltungspraktischer Vorschriften	816
d) Kontinuierliche Überwachung von Geschäftsbeziehungen/ „Monitoring“	817
e) Verdachtsfälle und Verdachtsmeldewesen/Unstimmigkeits- meldungen	817
f) Berichtswesen, Bericht an Geschäftsleitung und Aufsichtsorgan	819
g) Mitarbeiterschulungen	819
6. Arbeitsrechtlicher Schutz des Geldwäschebeauftragten und Teilausnahme vom Direktionsrecht des Arbeitgebers	820
a) Sonderkündigungsschutz	820
b) Benachteiligungsverbot	821
c) Ausnahme vom Direktionsrecht	822
7. Auslagerung der Funktion	822
8. Haftung	824
9. Der Geldwäschebeauftragte – gefangen zwischen hoheitlicher und unternehmerischer Tätigkeit?	825

23. Kapitel

Geldwäsche-Compliance in Industrie und Handel

(Komma)

I. Einführung in die Geldwäscheprävention	827
1. Begriff und Methoden der Geldwäsche	827
2. Die Geldwäschebekämpfung	829
a) Geldwäschebekämpfung auf internationaler Ebene: FATF ...	829
b) Geldwäschebekämpfung in der deutschen Gesetzgebung	830
3. Geldwäscherisiken für Industrie- und Handelsunternehmen	832
II. Industrie- und Handelsunternehmen im GwG:	
Der Begriff des Güterhändlers	834
III. Die Pflichten der Güterhändler im GwG	835
1. Die privilegierte Verpflichtetenstellung von Güterhändlern	836
a) Praktische Umsetzung des Bargeldausschlusses	836
b) Konsequenzen bei Einführung einer Bargeldbeschränkung ..	838
2. Risikomanagement	839
a) Risikoanalyse	839
b) Interne Sicherungsmaßnahmen	841
aa) Richtlinie zur Prävention von Geldwäsche	842
bb) Überprüfung von Geschäftspartnern	842
cc) Überwachung von Zahlungseingängen	842
c) Gruppenweite Pflichten	843
3. Kundensorgfaltspflichten	844
a) Auslösetatbestände der Sorgfaltspflichten für Güterhändler ..	844
b) Ausgewählte Aspekte der allgemeinen Sorgfaltspflichten ...	846
c) Ausgewählte Aspekte der vereinfachten und verstärkten Sorgfaltspflichten	847
4. Pflicht zur Abgabe von Verdachtsmeldungen	848
a) Verdachtsfall und typische Verdachtsmomente	848
b) Folgen einer Verdachtsmeldung	850
aa) Strafbefreiende Wirkung	850
bb) Transaktionssperrfrist § 46 GwG	851
cc) Verbot der Informationsweitergabe (Tipping Off-Verbot)	851
IV. Fazit	852

24. Kapitel

Sanktions-Compliance als Teil eines effektiven

Compliance-Management-Systems

(Salathé/Moussaoui)

I. Einleitung	855
1. Terminologien und Begriffsverständnis	856

2. Sanktionen: Historie, Gründe und Ziele	857
II. Rechtsrahmen	858
1. UN-Sanktionen	858
2. EU-Sanktionen	859
a) Anwendungsbereich	859
b) Grundlage der EU-Sanktionen	861
c) Auslegung der EU-Sanktionen	862
3. Aufbau der EU-Sanktionen	863
a) Listenprinzip	863
b) Finanzsanktionen	864
aa) Begriffsdefinitionen	864
(1) Gelder	865
(2) Wirtschaftliche Ressourcen	865
(3) Einfrieren von Geldern und wirtschaftlichen Ressourcen	866
(4) Eigentum und Besitz	867
(5) Halten und Kontrollieren	867
bb) Bereitstellungsverbot	869
(1) Bereitstellung	869
(2) Mittelbare Bereitstellung	870
cc) Einfriergebot	871
dd) Ausnahmen	872
4. Deutschland	873
a) Außenwirtschaftsgesetz und Außenwirtschaftsverordnung	873
b) Sanktionsdurchsetzungsgesetze	874
5. Ausblick: Deutschland und EU	876
6. US-Sanktionen	877
a) Grundlagen	877
b) Anwendungsbereich	878
aa) Primärsanktionen	878
bb) Sekundär-Sanktionen	879
c) Funktionsweise der US-Sanktionen	880
7. Anti-Boykott-Regelungen	881
a) EU-Blocking-Verordnung	881
aa) Hintergrund der EU-Blocking-Verordnung	881
bb) Regelungen der EU-Blocking-Verordnung	882
b) § 7 AWV	883
8. Weitere Sanktionen anderer Staaten und Organisationen	884
III. Konsequenzen und Haftung	885
1. Straf- und ordnungswidrigkeitsrechtliche Folgen	885
a) § 17 AWG	885
b) § 18 AWG	885
c) § 19 AWG	886

d) Vermeidung von Verstößen	887
2. Zivilrechtliche Folgen	887
3. Schadensersatz	889
4. Sonstige Folgen	889
IV. Maßnahmen zur Umsetzung eines Sanktions-Compliance- Management-Systems	890
1. Risikobewertung	891
2. Know Your Business Partner/Know Your Customer/ Risikoanalyse	892
a) Phase 1: Informationsbeschaffung	893
b) Phase 2: Überprüfung	894
c) Phase 3: Risikoeinschätzung	895
d) Phase 4: Entscheidung	895
3. Interne Meldeprozesse und Ablauforganisation	895
4. Tone from the Top und Guidance	896
5. Mitarbeiterzuverlässigkeit	897
6. Schulungen	898
7. Überprüfung	898
8. Rechtliche Unterstützung	899
9. Einsatz von IT-Hilfen/Technik	899
10. Dokumentation und Aufbewahrung	899
V. Checkliste	900

25. Kapitel

Exportkontrolle und Compliance

(v. Bodungen)

I. Einleitung	903
II. Rechtsgrundlagen der Exportkontrolle in Deutschland	904
1. Supranationale Vorgaben	904
2. Nationale Vorgaben	906
3. Relevanz ausländischen Exportkontrollrechts	906
a) Allgemeines	906
b) Insbesondere: US-Re-Exportkontrolle	906
III. Exportkontrollrechtliche Genehmigungspflichten	908
1. Allgemeines	908
2. Genehmigungspflichten bei Ausführen in Länder außerhalb der EU	908
a) Gelistete Güter	908
b) Nicht gelistete Güter	909
3. Genehmigungspflichten bei Verbringungen	910
a) Verbringungen bei Endverbleib in der EU	910

b) Verbringungen mit anschließender Ausfuhr	910
4. Sonstige Genehmigungspflichten	911
a) Handels- und Vermittlungsgeschäfte	911
b) Technische Unterstützung	911
IV. Exportkontrollrechtliches Genehmigungsverfahren	912
1. Zuständigkeit des BAFA	912
2. Ablauf des Genehmigungsverfahrens	913
3. Genehmigungstypen	914
4. Sanktionen bei exportkontrollrechtlichen Verstößen	915
V. Exportkontrollrechtliche Compliance-Strukturen	916
1. Allgemeines	916
2. Der Ausfuhrverantwortliche	918
3. Modell eines innerbetrieblichen Exportkontrollsystems	919
a) Überblick über die relevanten Strukturelemente	920
b) Umsetzung im Einzelfall	922
VI. Zusammenfassung und Ausblick	924

26. Kapitel

Compliance in M&A-Transaktionen

(Ullrich)

I. Einleitung	927
II. Prozessuale M&A-Compliance – Einhaltung von Rechtsvorschriften im M&A-Verfahren	928
1. Strukturierung der Transaktion	928
a) Auktions- und Einzelbieterverfahren	928
b) Transaktionsgegenstand	929
2. Offenlegung von Informationen	929
a) Offenlegungs- und Aufklärungspflichten des Veräußerers	929
b) Rechtliche Grenzen der Offenlegung von Informationen	931
aa) Gesellschaftsrechtliche Zulässigkeit der Offenlegung von Informationen gegenüber Dritten	931
bb) Vertraulichkeitsbestimmungen in Verträgen mit Dritten	933
cc) Datenschutzrechtliche Anforderungen für die Offenlegung von personenbezogenen Daten	934
3. Kartellrechtliche M&A-Compliance – Vollzugsverbot, Marktmachtmissbrauch und Informationsaustausch	936
a) Anmeldepflicht und Vollzugsverbot	936
b) Informationsaustausch	939
4. Kapitalmarktrechtliche M&A-Compliance	942
a) Informationsweitergabe im Rahmen der Due Diligence	942
b) Ad-hoc-Pflicht	943

c) Übernahmerechtliche M&A-Compliance	944
5. Pflicht zur Durchführung einer rechtlichen Due Diligence	945
a) Regelfall	945
b) Besonders gelagerte Fälle	946
c) Nachgelagerte Due Diligence (Post-Closing Due Diligence) ..	948
6. (Abbruch der) Vertragsverhandlungen	948
7. Zustimmungserfordernisse	950
a) Zustimmung von Aufsichtsgremien und/oder der Gesellschafter	950
b) Zustimmung von Ehegatten oder Lebenspartnern	954
8. Vereinbarung von Wettbewerbsverboten im Unternehmens- kaufvertrag	956
III. Materielle M&A-Compliance – Prüfung von/Umgang mit Compliance in der Zielgesellschaft	957
1. Due Diligence	957
a) Erfordernis einer Compliance-Due Diligence	957
aa) Einführung unter besonderer Beachtung von ESG/CSR .	957
bb) Erfordernis der Durchführung einer Compliance-Due Diligence	959
cc) (Eigen-)Interesse der Geschäftsleitung (Business Judgement Rule)	961
dd) Normative Kraft des Faktischen	962
b) Vorgehensweise: Abgestufte, risikobasierte Compliance-Due Diligence	962
aa) Rechtlicher Rahmen	962
bb) Ermittlung des Risikoprofils der Zielgesellschaft	963
cc) Risikobewertung und Dokumentation	964
dd) Eigentliche Due Diligence	964
c) Due Diligence nach Vollzug	964
2. Umgang mit bekannten/bekanntgewordenen Compliance- Verstößen/-Risiken	965
a) Risikobewertung	965
b) Umgang mit bekannten/entdeckten Compliance-Risiken	966
IV. Zusammenfassung	969

27. Kapitel

Kartellrechts-Compliance

(Seeliger/Mross/Seydel)

I. Überblick über die Kartellrechts-Risiken	971
1. Einleitung	971
2. Kartellrechts-Risikokategorien	973
a) Das Verbot wettbewerbsbeschränkender Vereinbarungen: Absprachen mit anderen Unternehmen	974

aa) Vereinbarung, abgestimmtes Verhalten oder Beschluss ..	974
bb) Bezweckte oder bewirkte Wettbewerbsbeschränkung	975
cc) Sehr hohe Risiken	976
(1) „Hardcore-Kartelle“	976
(2) Ausschreibungen	977
(3) Informationsaustausch	978
(4) Verbandsarbeit	980
(5) Preisbindungen und Preisempfehlungen	981
(6) Marktaufteilungen beim Vertrieb	982
(7) Internet-Behinderungen	983
(8) Boykott	986
(9) Personalbereich	986
dd) Weniger hohe Risiken	987
(1) Horizontale Kooperationen	987
(2) Vertriebsbeschränkungen	991
(3) Wettbewerbsverbote (Markenzwang); Alleinbezugsverpflichtungen	993
b) Machtmissbrauch (einseitige Handlungen)	994
aa) Allgemeine Voraussetzungen	994
(1) Marktbeherrschende Stellung	995
(2) Missbräuchliche Ausnutzung	996
bb) Sehr hohe Risiken	996
(1) Behinderung/Ausgrenzung von Wettbewerbern	996
(2) Kundenbindung, Treuerabatte	997
(3) Squeeze-out von Wettbewerbern, Kosten-Preis- Schere	997
(4) Kopplung von Angeboten	997
cc) Weniger hohe Risiken	998
(1) Ausbeutungsmissbrauch, Kundenpreis- differenzierung	998
(2) Niedrigpreisstrategien	998
(3) Lieferverweigerung; wesentliche Einrichtungen („Essential Facilities“)	999
(4) Ausschließlichkeitsbindungen	999
(5) Diskriminierung abhängiger Unternehmen	999
(6) Behinderung von kleineren Wettbewerbern; Verkauf unter Einstandspreis	1000
3. Haftungssubjekte (Wer haftet für wen?)	1000
a) Unternehmenshaftung	1000
b) Persönliche Haftung	1001
c) Haftung im Konzern („Wirtschaftliche Einheit“)	1002
d) Haftung bei Gemeinschaftsunternehmen	1003
e) Haftung für Beauftragte	1003
f) Haftung bei Rechtsnachfolge	1004

4. Art und Umfang der Haftung	1005
a) Strafrechtliche Sanktionen	1005
b) Bußgelder	1006
aa) EU-Recht	1006
bb) Deutsches Recht	1007
c) Schadensersatz	1009
aa) Individualansprüche	1009
bb) Kollektiver Rechtsschutz	1011
cc) Schadensausgleich im Innenverhältnis	1012
d) Sonstige Nachteile	1012
II. Management der Kartellrechtsrisiken in der Praxis	1013
1. Risikoanalyse: Identifizierung und Bewertung	1015
a) Kartellrechtliches Risikoprofil	1015
b) Geschäftstätigkeit und Geschäftsbeziehungen	1015
c) Risikokategorisierung und Risikobewertung	1016
d) Einführung eines Top-down-Ansatzes	1017
2. Präventive Maßnahmen	1017
a) Richt- und Leitlinien zum Kartellrecht	1018
b) Schulungen (Präsenzs Schulungen und Webinars/E-Learning) ..	1021
3. Maßnahmen zur Kontrolle/Aufdeckung	1023
III. Behördliche Untersuchungen	1025
1. Durchsuchungen der EU-Kommission	1026
a) Zuständigkeit	1026
b) Befugnisse	1027
c) Elektronische Durchsuchung	1028
d) Typischer Ablauf	1029
2. Durchsuchungen des Bundeskartellamts	1030
a) Zuständigkeit	1030
b) Befugnisse	1031
c) Elektronische Durchsuchung	1033
d) Typischer Ablauf	1034
3. Verhaltensregeln für die Unternehmen	1034
a) Vor der Durchsuchung	1034
b) Während der Durchsuchung	1035
c) Nach der Durchsuchung	1037

28. Kapitel

Compliance-Anforderungen im Wettbewerb um öffentliche Aufträge

(Scherer)

I. Einleitung	1039
II. Anforderungen an Unternehmen in Vergabeverfahren	1040

III. Ausschlussgründe	1042
1. Zwingende Ausschlussgründe	1042
a) Straftatbestände	1042
b) Steuer- und Abgabentatbestände	1043
2. Fakultative Ausschlussgründe	1044
a) Verstoß gegen umwelt-, sozial- oder arbeitsrechtliche Verpflichtungen	1044
b) Insolvenz und Liquidation	1045
c) Schwere Verfehlung im Rahmen beruflicher Tätigkeit	1045
d) Wettbewerbsbeschränkende Vereinbarungen oder abgestimmte Verhaltensweisen	1046
e) Interessenkonflikt	1047
f) Vorbefassung	1047
g) Mangelhafte Leistung bei Ausführung früherer Aufträge	1048
h) Schwerwiegende Täuschung bei Eignungsprüfung	1048
i) Unzulässige Einflussnahme	1049
IV. Wettbewerbsregister	1050
1. Einrichtung des Wettbewerbsregisters	1050
2. Eintragung von Rechtsverstoßen	1050
3. Einbindung in das Vergabeverfahren	1051
4. Löschung von Eintragungen	1052
5. Rechtsbehelfe	1053
V. Selbstreinigung	1053
1. Selbstreinigung im Vergabeverfahren	1053
a) Prüfung durch Vergabestelle	1053
b) Prüfung durch Wettbewerbsregister	1054
2. Kriterien der Selbstreinigung	1054
a) Ausgleich des Schadens	1054
b) Zusammenarbeit zur Aufklärung	1055
c) Technische, organisatorische und personelle Maßnahmen	1056
VI. Ausschlussfristen	1058
1. Fristenregelung bei zwingenden Ausschlussgründen	1058
2. Fristenregelung bei fakultativen Ausschlussgründen	1058
3. Ermessensausübung	1059

29. Kapitel

Tax Compliance

(Schwartz)

I. Einleitung	1061
II. Steuerliche Pflichten	1063

1. Allgemeine steuerliche Pflichten	1063
2. Spezifische materiell-rechtliche Problemschwerpunkte	1068
a) Lohnsteuer und Sozialabgaben	1068
b) Umsatzsteuer	1069
c) Verdeckte Gewinnausschüttungen	1070
d) Anzeigepflicht nach § 153 AO	1071
e) Tochtergesellschaften und Betriebstätten im Ausland	1074
f) Internationale Verrechnungspreise	1075
g) Versagung des Betriebsausgabenabzugs nach § 160 AO	1075
h) Betriebsausgabenabzugsverbot nach § 4 Abs. 5 Satz 1 Nr. 10 EStG	1076
III. Risiken mangelnder Tax Compliance	1078
1. Steuerliche Haftungsrisiken	1078
2. Steuerstrafrechtliche und steuerordnungswidrigkeitenrechtliche Risiken	1080
a) Sanktionen gegen Organe und Mitarbeiter	1080
aa) Steuerhinterziehung und leichtfertige Steuerverkürzung (§§ 370, 378 AO)	1080
(1) Täter	1080
(2) Objektiver Tatbestand	1081
(3) Subjektiver Tatbestand	1085
(4) Strafe	1086
bb) Verletzung der Aufsichtspflicht (§ 130 OWiG)	1087
b) Sanktionen gegen das Unternehmen	1088
aa) Verbandsgeldbuße (§ 30 OWiG)	1088
bb) Einziehung (§ 29a OWiG)	1090
IV. Tax Compliance-System	1091
1. Risikoanalyse	1091
2. Ausgestaltung eines Tax Compliance-Systems	1092
a) Zuständigkeit für Tax Compliance	1092
b) Zuständigkeit und Verantwortlichkeit bzgl. der steuerlichen Pflichten	1092
c) Berichtswege/Berichtspflichten	1093
d) Prozessbeschreibung Deklarationswesen	1095
e) Kontroll- und Überwachungsmaßnahmen	1095
f) Umgang mit Betriebsprüfungen	1096
g) Schulungen	1098
h) Dokumentation	1098
3. Prüfungserleichterungen nach Art. 97 § 38 EGAO	1099
a) Tatbestandsvoraussetzungen	1099
b) Rechtsfolgen	1101
V. Zertifizierung des Tax Compliance-Systems durch Dritte	1102

VI. Berichtigung von Steuererklärungen	1104
1. Korrekturvorschrift	1104
2. Selbstanzeige im Unternehmen (§§ 371, 378 Abs. 3 AO)	1105
a) Person des Anzeigerstatters	1105
b) Positive Wirksamkeitsvoraussetzungen des § 371 AO	1106
c) Negative Wirksamkeitsvoraussetzungen des § 371 AO (Sperrgründe)	1108
d) Absehen von Verfolgung nach § 398a AO	1111
e) Bußgeldbefreiende Selbstanzeige nach § 378 Abs. 3 AO	1112
VII. Fazit	1112
Literaturverzeichnis	1113
Sachregister	1157

Abkürzungsverzeichnis

a. A./A. A.	andere(r) Ansicht
a. a. O.	am angegebenen Ort
Abb.	Abbildung
ABC-Waffe	atomare, biologische und chemische Waffe
AbgG	Abgeordnetengesetz in der Fassung der Bekanntmachung vom 21. Februar 1996 (BGBl. I S. 326), zuletzt geändert durch Artikel 1 des Gesetzes vom 8. Oktober 2021 (BGBl. I S. 4650) geändert
ABl.	Amtsblatt
Abs.	Absatz
ABS	Asset Backed Securities
a. E.	am Ende
AEAO	Anwendungserlass zur Abgabenordnung in der Fassung des BMF-Schreibens vom 31.1.2014 (BStBl. I S. 290), zuletzt geändert durch das BMF-Schreiben vom 23.5.2016 (BStBl. I S. 490)
AEUV	Vertrag über die Arbeitsweise der Europäischen Union, konsolidierte Fassung, ABl. EG Nr. C 115 vom 9.5.2008, zuletzt geändert mit ABl. EU L 112/21 vom 24.4.2012
a. F.	alte Fassung
AG	Aktiengesellschaft/Die Aktiengesellschaft (Zeitschrift)
AGB	Allgemeine Geschäftsbedingung
AGG	Allgemeines Gleichbehandlungsgesetz vom 14. August 2006 (BGBl. I S. 1897), zuletzt geändert durch Artikel 15 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 414)
AktG	Aktiengesetz vom 6. September 1965 (BGBl. I S. 1089), zuletzt geändert durch Artikel 13 des Gesetzes vom 11. Dezember 2023 (BGBl. 2023 I Nr. 354)
AktG-E	Aktiengesetz-Entwurf
allg.	allgemein(e)
AMG	Arzneimittelgesetz in der Fassung der Bekanntmachung vom 12. Dezember 2005 (BGBl. I S. 3394), zuletzt geändert durch Artikel 7 des Gesetzes vom 27. März 2024 (BGBl. 2024 I Nr. 109)
ÄndG	Änderungsgesetz
Anh.	Anhang
Anm.	Anmerkung(en)
AO	Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), zuletzt geändert durch Artikel 14 des Gesetzes vom 27. März 2024 (BGBl. 2024 I Nr. 108)

Abkürzungsverzeichnis

App	Applikation (Anwendungsprogramm, -software)
AR	Aufsichtsrat
ArbG	Arbeitsgericht
Art.	Artikel
AStBV (St)	Anweisungen für das Straf- und Bußgeldverfahren (Steuer)
AStG	Außensteuergesetz vom 8. September 1972 (BGBl. I S. 1713), zuletzt geändert durch Artikel 10 des Gesetzes vom 27. März 2024 (BGBl. 2024 I Nr. 108)
AT	amtlicher Teil/allgemeiner Teil
AuA	Arbeit und Arbeitsrecht (Zeitschrift)
Aufl.	Auflage
Ausschussdrucks.	Ausschussdrucksache
AW-Prax.	Außenwirtschaftliche Praxis (Zeitschrift)
AWG	Außenwirtschaftsgesetz vom 6. Juni 2013 (BGBl. I S. 1482), zuletzt geändert durch Artikel 2 des Gesetzes vom 27. Februar 2024 (BGBl. 2024 I Nr. 71)
AWV	Außenwirtschaftsverordnung vom 2. August 2013 (BGBl. I S. 2865), zuletzt geändert durch Artikel 3 des Gesetzes vom 27. Februar 2024 (BGBl. 2024 I Nr. 71)
Az.	Aktenzeichen
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAG	Bundesarbeitsgericht
BAnz.	Bundesanzeiger
BayObLG	Bayerisches Oberstes Landesgericht
BB	Betriebs-Berater (Zeitschrift)
BBG	Bundesbeamtengesetz vom 5. Februar 2009 (BGBl. I S. 160), zuletzt geändert durch Artikel 6 des Gesetzes vom 20. Dezember 2023 (BGBl. 2023 I Nr. 389)
BCBS	Basel Committee on Banking Supervision
Bd.	Band
BDI	Bundesverband der Deutschen Industrie e. V.
BDSG	Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), zuletzt geändert durch Artikel 7 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149)
BeckOK	Beck'scher Onlinekommentar herausgegeben von Rof/s/Gie-
Arbeitsrecht	sen/Meßling/Udsching
BeckOK BGB	Beck'scher Onlinekommentar herausgegeben von Hau/ Poseck
BeckOK Daten- schutzrecht	Beck'scher Onlinekommentar herausgegeben von Wolff/ Brink
BeckOK Geld- wäschegesetz	Beck'scher Onlinekommentar herausgegeben von Fromm/ Nordemann

BeckOK GmbHG	Beck'scher Onlinekommentar herausgegeben von Ziemons/ Jaeger/Pöschke
BeckOK HinSchG	Beck'scher Onlinekommentar herausgegeben von Colneric/ Gerdemann
BeckOK LkSG	Beck'scher Onlinekommentar herausgegeben von Henn/Jahn
BeckOK OWiG	Beck'scher Onlinekommentar herausgegeben von Graf
BeckOK StGB	Beck'scher Onlinekommentar herausgegeben von Heint- schel-Heinegg/Kudlich
BeckOK Vergaberecht	Beck'scher Onlinekommentar herausgegeben von Gabriel/ Mertens/Prieß/Stein
BeckRS	Beck-online Rechtsprechung
Begr.	Begründung
Beil.	Beilage
Bek.	Bekanntmachung
BetrVG	Betriebsverfassungsgesetz in der Fassung der Bekanntma- chung vom 25. September 2001 (BGBl. I S. 2518), zuletzt geändert durch Artikel 6d des Gesetzes vom 16. September 2022 (BGBl. I S. 1454)
Beschl.	Beschluss
BFH	Bundesfinanzhof
BFH/NV	Sammlung der Entscheidungen des Bundesfinanzhofs, die nicht veröffentlicht wurden (Zeitschrift)
BGB	Bürgerliches Gesetzbuch in der Fassung der Bekanntma- chung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Artikel 1 des Gesetzes vom 24. Juni 2024 (BGBl. 2024 I Nr. 212)
BGBI.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungssammlung des Bundesgerichtshofes in Straf- sachen
BGHZ	Entscheidungssammlung des Bundesgerichtshofes in Zivil- sachen
BHO	Bundeshaushaltsordnung
BImSchG	Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge (Bundes-Immissionsschutzgesetz) in der Fassung der Bekanntmachung vom 17. Mai 2013 (BGBl. I S. 1274; 2021 I S. 123), zuletzt geändert durch Artikel 1 des Gesetzes vom 3. Juli 2024 (BGBl. 2024 I Nr. 225)
BAK	Bundeskriminalamt
BKartA	Bundeskartellamt
BKR	Zeitschrift für Bank- und Kapitalmarktrecht (Zeitschrift)
BMF	Bundesministerium der Finanzen
BMI	Bundesministerium des Inneren

Abkürzungsverzeichnis

BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BOARD	Zeitschrift für Aufsichtsräte in Deutschland (Zeitschrift)
BpO	Betriebsprüfungsordnung
BR-Drs.	Bundesratsdrucksache
BRAK	Bundesrechtsanwaltskammer
BRAO	Bundesrechtsanwaltsordnung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 303-8, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 1 des Gesetzes vom 17. Januar 2024 (BGBl. 2024 I Nr. 12)
BremGbl.	Gesetzblatt der Freien Hansestadt Bremen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982)
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung) vom 22. April 2016 (BGBl. I S. 958), zuletzt geändert durch Artikel 1 der Verordnung vom 29. November 2023 (BGBl. 2023 I Nr. 339)
bspw.	beispielsweise
BStBl.	Bundessteuerblatt
BT	Besonderer Teil
BT-Drs.	Bundestagsdrucksache
BUrlG	Mindesturlaubsgesetz für Arbeitnehmer (Bundesurlaubsgesetz) in der im Bundesgesetzblatt Teil III, Gliederungsnummer 800-4, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 3 Absatz 3 des Gesetzes vom 20. April 2013 (BGBl. I S. 868)
BV	Betriebsvereinbarung
BvD-News	Zeitschrift des Berufsverband der Datenschutzbeauftragten Deutschlands (Zeitschrift)
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgericht, Entscheidungssammlung
BVMed	Bundesverband Medizintechnologie
bzgl.	bezüglich
BZRG	Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz) in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, 1985 I S. 195), zuletzt geändert durch Artikel 7 des Gesetzes vom 19. Juni 2024 (BGBl. 2024 I Nr. 206)
bzw.	beziehungsweise
ca.	circa
CB	Compliance Berater (Zeitschrift)

LVI

CCO	Chief Compliance Officer
CCZ	Corporate Compliance Zeitschrift (Zeitschrift)
CD	Compact Disk (Datenträger)
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CMS	Compliance-Management-System
COO	Chief Operating Officer
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CR	Computer & Recht (Zeitschrift)
CRi	Computer Law Review International (Zeitschrift)
CSDDD	Corporate Sustainability Due Diligence Directive
CSR	Corporate Social Responsibility
CSRD	Corporate Sustainability Reporting Directive
CSV	Creating Shared Value
D&O- Versicherung	Directors-and-Officers-Versicherung (Organ- oder Manager-Haftpflichtversicherung)
dass.	dasselbe
DAX	Deutscher Aktienindex
DB	Der Betrieb (Zeitschrift)
DCGK	Deutscher Corporate Governance Kodex
DDR	Deutsche Demokratische Republik
ders.	derselbe
d. h.	das heißt
d. i.	das ist
dies.	dieselbe(n)
Diss.	Dissertation
DJT	Deutscher Juristentag
DMS	Datenschutzmanagementsystem
DNK	Deutscher Nachhaltigkeitskodex
DÖV	Die Öffentliche Verwaltung (Zeitschrift)
Dr.	Doktor
DRS	Deutsche Rechnungslegungs Standards
DRSC	Deutsche Rechnungslegungs Standards Committee
DRV	Deutscher Rahmenvertrag für Finanztermingeschäfte
DSB	Datenschutzbeauftragte(r)
DSGVO	Datenschutzgrundverordnung
DSRITB	Deutsche Stiftung für Recht und Informatik – Tagungsband (Zeitschrift)
DStR	Deutsches Steuerrecht (Zeitschrift)
DStRE	Deutsches Steuerrecht – Entscheidungsdienst (Zeitschrift)
DtZ	Deutsch-Deutsche Rechts-Zeitschrift (Zeitschrift)

Abkürzungsverzeichnis

DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVD	Digital Versatile Disc (Datenträger)
EBA	European Banking Authority (Europäische Bankenaufsichtsbehörde)
EBITDA	Earnings before Interests, Taxes, Depreciation and Amortisation (Ergebnis vor Zinsen, Steuern und Abschreibungen)
EBRG	Europäische Betriebsräte-Gesetz in der Fassung der Bekanntmachung vom 7. Dezember 2011 (BGBl. I S. 2650), zuletzt geändert durch Artikel 6f des Gesetzes vom 16. September 2022 (BGBl. I S. 1454)
E-Commerce	Elektronischer Handel/Internethandel
EDV	Elektronische Datenverarbeitung
EFZG	Gesetz über die Zahlung des Arbeitsentgelts an Feiertagen und im Krankheitsfall (Entgeltfortzahlungsgesetz) vom 26.5.1994 (BGBl. I S. 1014, 1065), zuletzt geändert durch Gesetz vom 22.11.2019 (BGBl. I S. 1746)
EG	Europäische Gemeinschaft
EGAO	Einführungsgesetz zur Abgabenordnung vom 14.12.1976 (BGBl. I S. 3341; 1977 I S. 667), zuletzt geändert durch Artikel 4 des Gesetzes vom 23.10.2024 (BGBl. 2024 I Nr. 323)
EGMR	Europäischer Gerichtshof für Menschenrechte
EIOPA	European Insurance and Occupational Pensions Authority (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung)
EL	Ergänzungslieferung
E-Learning	electronic learning (elektronisch unterstütztes Lernen)
EMIR	European Market Infrastructure Regulation (Verordnung [EU] Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4.7.2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister)
EMRK	Europäische Menschenrechtskonvention
endg.	endgültig
EnergieStG	Energiesteuergesetz vom 15. Juli 2006 (BGBl. I S. 1534; 2008 I S. 660, 1007), zuletzt geändert durch Artikel 3 des Gesetzes vom 27. März 2024 (BGBl. 2024 I Nr. 107)
EnWG	Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz) vom 7. Juli 2005 (BGBl. I S. 1970, 3621), zuletzt geändert durch Artikel 26 des Gesetzes vom 15. Juli 2024 (BGBl. 2024 I Nr. 236)
ErbStG	Erbschaftsteuer- und Schenkungsteuergesetz in der Fassung der Bekanntmachung vom 27. Februar 1997 (BGBl. I S. 378), zuletzt geändert durch Artikel 28 des Gesetzes vom 27. März 2024 (BGBl. 2024 I Nr. 108)

ErfK ArbR	Erfurter Kommentar zum Arbeitsrecht herausgegeben von Müller-Glöge/Preis/Gallner/Schmidt
ErwG	Erwägungsgrund
ESEF	European Single Electronic Format
ESG	Environmental, Social und Governance
ESMA	European Securities and Markets Authority (Europäische Wertpapier- und Marktaufsichtsbehörde)
ESRS	European Sustainability Reporting Standards
ESt	Einkommenssteuer
ESTG	Einkommensteuergesetz in der Fassung der Bekanntmachung vom 8. Oktober 2009 (BGBl. I S. 3366, 3862), zuletzt geändert durch Artikel 6 des Gesetzes vom 27. März 2024 (BGBl. 2024 I Nr. 108)
et al.	et alii (und andere)
etc.	et cetera
EU	Europäische Union
EUBestG	EU-Bestechungsgesetz vom 10.9.1998 (BGBl. 1998 II S. 2340), zuletzt geändert durch Artikel 2 des Gesetzes vom 20.11.2015 (BGBl. I S. 2025)
EuG	Gericht der Europäischen Union
EuGH	Gerichtshof der Europäischen Union
EuR	Europarecht (Zeitschrift)
EUR	Euro
EURIBOR	Euro Interbank Offered Rate (Referenzzinssatz für Termingelder in Euro im Interbankengeschäft)
EUROPOL	Europäisches Polizeiamt
e. V.	eingetragener Verein
EWR	Europäischer Wirtschaftsraum
EuZW	Europäische Zeitschrift für Wirtschaftsrecht (Zeitschrift)
f./ff.	folgende
F&E	Forschung und Entwicklung
FAQ	Frequently Asked Questions
FATF	Financial Action Task Force on Money Laundering
FCPA	Foreign Corrupt Practices Act
FG	Finanzgericht
FGO	Finanzgerichtsordnung in der Fassung der Bekanntmachung vom 28.3.2001 (BGBl. I S. 442, 2262; 2002 I S. 679), zuletzt geändert durch Gesetz vom 12.7.2024 (BGBl. I S. 234)
FISG	Finanzmarktintegritätsstärkungsgesetz
FIU	Financial Intelligence Unit

Abkürzungsverzeichnis

FKVO	Verordnung (EG) Nr. 139/2004 des Rates vom 20.1.2004 über die Kontrolle von Unternehmenszusammenschlüssen („EG-Fusionskontrollverordnung“)
Fn.	Fußnote
FS	Festschrift
GA	Goltdammer's Archiv für Strafrecht (Zeitschrift)
GbR	Gesellschaft bürgerlichen Rechts
GewO	Gewerbeordnung in der Fassung der Bekanntmachung vom 22. Februar 1999 (BGBl. I S. 202), zuletzt geändert durch Artikel 5 des Gesetzes vom 17. Januar 2024 (BGBl. 2024 I Nr. 12)
GewSt	Gewerbsteuer
GewStG	Gewerbsteuergesetz in der Fassung der Bekanntmachung vom 15. Oktober 2002 (BGBl. I S. 4167), zuletzt geändert durch Artikel 19 des Gesetzes vom 27. März 2024 (BGBl. 2024 I Nr. 108)
GF	Geschäftsführer
GG	Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 1 des Gesetzes vom 19. Dezember 2022 (BGBl. I S. 2478)
ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GmbH & Co KG	Gesellschaft mit beschränkter Haftung & Compagnie Kommanditgesellschaft
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4123-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 9 des Gesetzes vom 22. Februar 2023 (BGBl. 2023 I Nr. 51)
GmbHR	GmbH-Rundschau (Zeitschrift)
GRC	Governance, Risikomanagement & Compliance
GRI	Global Reporting Initiative
GrEStG	Grunderwerbsteuergesetz in der Fassung der Bekanntmachung vom 26. Februar 1997 (BGBl. I S. 418, 1804), zuletzt geändert durch Artikel 30 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 411)
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
GRUR-RR	Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungs-Report (Zeitschrift)
GSSt	Großer Senat für Strafsachen
GVOBl.	Gesetz- und Verordnungsblatt

LX

GWB	Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bekanntmachung vom 26. Juni 2013 (BGBl. I S. 1750, 3245), zuletzt geändert durch Artikel 3 des Gesetzes vom 12. Juni 2024 (BGBl. 2024 I Nr. 190)
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz) vom 23. Juni 2017 (BGBl. I S. 1822), zuletzt geändert durch Artikel 34 Absatz 21 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 411)
GWR	Gesellschafts- und Wirtschaftsrecht (Zeitschrift)
Hdb.	Handbuch
HGB	Handelsgesetzbuch in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 2 des Gesetzes vom 11. April 2024 (BGBl. 2024 I Nr. 120)
HGB-E	HGB-Entwurf
HinschG	Gesetz für einen besseren Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz) vom 31. Mai 2023 (BGBl. 2023 I Nr. 140)
h. L.	herrschende Lehre
h. M.	herrschende Meinung
HmbGVBl.	Hamburgisches Gesetz- und Verordnungsblatt
HR	Human Resources
HRRS	Online-Zeitschrift für Höchstrichterliche Rechtsprechung im Strafrecht (Online-Zeitschrift)
Hrsg.	Herausgeber
IBR	Immobilien & Baurecht (Zeitschrift)
ICRM	Integrierter Compliance- und Risikomanagement
i. d. F.	in der Form
i. d. R.	in der Regel
i. e. S.	im engeren Sinne
i. H. v.	in Höhe von
IKS	Internes Kontrollsystem
Inc.	Incorporated (Amerikanische Gesellschaftsform)
inkl.	inklusive
insb.	insbesondere
InsO	Insolvenzordnung vom 5. Oktober 1994 (BGBl. I S. 2866), zuletzt geändert durch Artikel 36 des Gesetzes vom 12. Juli 2024 (BGBl. 2024 I Nr. 234)

Abkürzungsverzeichnis

InstitutsVergV	Verordnung über die aufsichtsrechtlichen Anforderungen an Vergütungssysteme von Instituten (Institutsvergütungsverordnung) vom 16. Dezember 2013 (BGBl. I S. 4270), zuletzt geändert durch Artikel 1 der Verordnung vom 14. Februar 2023 (BGBl. 2023 I Nr. 41)
IntBestG	Gesetz zu dem Übereinkommen vom 17. Dezember 1997 über die Bekämpfung der Bestechung ausländischer Amtsträger im internationalen Geschäftsverkehr (Gesetz zur Bekämpfung internationaler Bestechung) vom 10.9.1998 (BGBl. 1998 II S. 2327), zuletzt geändert durch Artikel 5 des Gesetzes vom 20.11.2015 (BGBl. I S. 2025)
INTERPOL	Internationale kriminalpolizeiliche Organisation
InvG	Investmentgesetz, aufgehoben durch Artikel 2a des Gesetzes vom 4.7.2013 (BGBl. I S. 1981)
i. S. d.	im Sinne des/im Sinne der
i. S. e.	im Sinne einer/im Sinne eines
i. S. v.	im Sinne von
IT	Informationstechnik
ITRB	Der IT-Rechts-Berater (Zeitschrift)
i. V. m.	in Verbindung mit
KAGB	Kapitalanlagegesetzbuch vom 4. Juli 2013 (BGBl. I S. 1981), zuletzt geändert durch Artikel 34 Absatz 20 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 411)
Kap.	Kapitel
KG	Kommanditgesellschaft
KMU	kleine und mittlere Unternehmen
Komm.	Kommission der Europäischen Union/Kommentar
KOM (2011) 366 endg.	Kommission der Europäischen Gemeinschaften – GRÜNBUCH – Europäische Rahmenbedingungen für die soziale Verantwortung der Unternehmen vom 18.7.2001
KOM (2011) 206 endg.	Mitteilung der Europäischen Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Binnenmarktakte – vom 13.4.2011
KOM (2011) 681 endg.	Mitteilung der Europäischen Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Neue Strategie für soziale Verantwortung der Unternehmen (CSR) – vom 25.10.2011
KölnKomm- AktG	Kölner Kommentar AktG hrsg. von Zöllner/Noack
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich vom 27.4.1998 (BGBl. I S. 786)

KorrBekG	Gesetz zur Bekämpfung der Korruption vom 13.8.1997 (BGBl. I 1997, S. 2038) und vom 20.11.2015 (BGBl. I S. 2025)
KRITIS-Betreiber	Betreiber kritischer Infrastrukturen
KrWaffKontrG	Ausführungsgesetz zu Artikel 26 Abs. 2 des Grundgesetzes (Gesetz über die Kontrolle von Kriegswaffen) in der Fassung der Bekanntmachung vom 22. November 1990 (BGBl. I S. 2506), zuletzt geändert durch Artikel 25 des Gesetzes vom 19. Dezember 2022 (BGBl. I S. 2606)
KSchG	Kündigungsschutzgesetz in der Fassung der Bekanntmachung vom 25. August 1969 (BGBl. I S. 1317), zuletzt geändert durch Artikel 2 des Gesetzes vom 14. Juni 2021 (BGBl. I S. 1762)
KSt	Körperschaftsteuer
KStG	Körperschaftsteuergesetz in der Fassung der Bekanntmachung vom 15. Oktober 2002 (BGBl. I S. 4144), zuletzt geändert durch Artikel 18 des Gesetzes vom 27. März 2024 (BGBl. 2024 I Nr. 108)
KSzW	Kölner Schrift zum Wirtschaftsrecht (Zeitschrift)
KWG	Gesetz über das Kreditwesen (Kreditwesengesetz) in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), zuletzt geändert durch Artikel 6 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 411)
KWKG	Gesetz für die Erhaltung, die Modernisierung und den Ausbau der Kraft-Wärme-Kopplung vom 21. Dezember 2015 (BGBl. I S. 2498), zuletzt geändert durch Artikel 9 des Gesetzes vom 20. Dezember 2022 (BGBl. I S. 2512)
KYC	Know Your Customer
LAG	Landesarbeitsgericht
LCO	Local Compliance Officer
LG	Landgericht
lit.	littera (Buchstabe)
LkSG	Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten (Lieferkettensorgfaltspflichtengesetz) vom 16. Juli 2021 (BGBl. I S. 2959)
LK-StGB	Laufhütte/R. Rissing-van Saan/K. Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, 12. Aufl. 2006 ff.
LohnSt	Lohnsteuer

Abkürzungsverzeichnis

LPartG	Gesetz über die Eingetragene Lebenspartnerschaft (Lebenspartnerschaftsgesetz) vom 16. Februar 2001 (BGBl. I S. 266), zuletzt geändert durch Artikel 5 Absatz 3 des Gesetzes vom 11. Juni 2024 (BGBl. 2024 I Nr. 185)
M&A	Mergers and Acquisitions
MaComp	Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach dem Wertpapierhandelsgesetz für Wertpapierdienstleistungsunternehmen (Verwaltungsanweisungen, von der Bundesanstalt für Finanzdienstleistungsaufsicht in Form eines Rundschreibens erlassen)
MAD	Market Abuse Directive (Richtlinie 2003/6/EG des europäischen Parlaments und des Rates vom 28.1.2003 über Insider-Geschäfte und Marktmanipulation [Marktmissbrauch])
MAH	Münchener Anwaltshandbuch
MAR	Market Abuse Regulation (Verordnung [EU] Nr. 596/2014 des Europäischen Parlaments und des Rates vom 16.4.2014)
MaRisk	Mindestanforderungen an das Risikomanagement (Verwaltungsanweisungen, von der Bundesanstalt für Finanzdienstleistungsaufsicht in Form eines Rundschreibens erlassen)
m. E.	meines Erachtens
MiFID II	Markets in Financial Instruments Directive (Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15.5.2014)
MiLoG	Gesetz zur Regelung eines allgemeinen Mindestlohns (Mindestlohngesetz) vom 11. August 2014 (BGBl. I S. 1348), zuletzt geändert durch Artikel 2 des Gesetzes vom 28. Juni 2023 (BGBl. 2023 I Nr. 172)
Min.	Minute(n)
Mio.	Million(en)
MMR	Multimedia und Recht (Zeitschrift)
Mrd.	Milliarde(n)
MschrKrim	Monatsschrift für Kriminologie und Strafrechtsreform (Zeitschrift)
MünchKomm-AktG	Münchener Kommentar zum Aktiengesetz herausgegeben von Goette/Habersack/Kalss (Hrsg.),
MünchKomm-BGB	Münchener Kommentar zum Aktiengesetz herausgegeben von Goette/Habersack
MünchKomm-GmbH	Münchener Kommentar zum GmbHG herausgegeben von Fleischer/Goette
MünchKomm-Wettbewerbsrecht	Münchener Kommentar zum Wettbewerbsrecht herausgegeben von Säcker/Ganske/Knauff

MünchKomm-StGB	Münchener Kommentar zum Strafgesetzbuch herausgegeben von Joecks/Miebach
m. w. N.	mit weiteren Nachweisen
m. W. v.	mit Wirkung vom
n. F.	neue Fassung
NGO	Non-Governmental Organisation (Nichtregierungsorganisation)
NIS-RL	EU-Richtlinie zur Verbesserung der Netz- und Informationssicherheit
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NJW-RR	Neue Juristische Wochenschrift Rechtsprechungs-Report (Zeitschrift)
NK-StGB	Nomos-Kommentar zum Strafgesetzbuch herausgegeben von Kindhäuser/Neumann/Paeffgen/Saliger
Nr.	Nummer
NRW	Nordrhein-Westfalen (Bundesland)
NStZ	Neue Zeitschrift für Strafrecht (Zeitschrift)
NStZ-RR	Rechtssprechungsreport Strafrecht (Zeitschrift)
n. v.	nicht veröffentlicht
NWB	Steuer- und Wirtschaftsrecht (Zeitschrift)
NZA	Neue Zeitschrift für Arbeitsrecht (Zeitschrift)
NZA-RR	Rechtsprechungs-Report Arbeitsrecht (Zeitschrift)
NZG	Neue Zeitschrift für Gesellschaftsrecht (Zeitschrift)
NZKart	Neue Zeitschrift für Kartellrecht (Zeitschrift)
NZWiSt	Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (Zeitschrift)
o. Ä.	oder Ähnlich(e/es)
OECD	Organization for Economic Co-operation and Development (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung)
OFAC	Office of Foreign Asset Control
o. g.	oben genannte(r)
OHG	Offene Handelsgesellschaft
OLG	Oberlandesgericht
OWiG	Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), zuletzt geändert durch Artikel 10 des Gesetzes vom 12. Juli 2024 (BGBl. 2024 I Nr. 234)
p. a.	per anno (pro Jahr)

Abkürzungsverzeichnis

PartG	Gesetz über die politischen Parteien (Parteiengesetz) in der Fassung der Bekanntmachung vom 31. Januar 1994 (BGBl. I S. 149), zuletzt geändert durch Artikel 1 des Gesetzes vom 27. Februar 2024 (BGBl. 2024 I Nr. 70)
PC	Personal Computer
PEP	Politisch exponierte Person
PR	Public Relations (Öffentlichkeitsarbeit)
PSR	Personal Social Responsibility
PStR	Praxis Steuerstrafrecht (Zeitschrift)
PublG	Gesetz über die Rechnungslegung von bestimmten Unternehmen und Konzernen (Publizitätsgesetz) vom 15. August 1969 (BGBl. I S. 1189), zuletzt geändert durch Artikel 59 des Gesetzes vom 10. August 2021 (BGBl. I S. 3436)
RA	Rechtsanwalt
RAin	Rechtsanwältin
RDV	Recht der Datenverarbeitung (Zeitschrift)
RegE	Regierungsentwurf
RGBL	Deutsches Reichsgesetzblatt
RGSt	Entscheidungen des Reichsgerichts in Strafsachen
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
RL	Richtlinie
RMS	Risikomanagementsystem
Rn.	Randnummer
RNE	Rat für Nachhaltige Entwicklung
Rspr.	Rechtsprechung
S.	Seite
SAR	Suspicious Activity Reporting
SDN	Specially Designated Nationals
SE	Societas Europaea (Europäische Gesellschaft)
Sec.	Section
SEPA	Single Euro Payments Area (Einheitlicher Euro-Zahlungsverkehrsraum)
SGB IV	Das Vierte Buch Sozialgesetzbuch – Gemeinsame Vorschriften für die Sozialversicherung – in der Fassung der Bekanntmachung vom 12. November 2009 (BGBl. I S. 3710, 3973; 2011 I S. 363), zuletzt geändert durch Artikel 2 des Gesetzes vom 30. Mai 2024 (BGBl. 2024 I Nr. 173)
SGB V	Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), zuletzt geändert durch Artikel 3 des Gesetzes vom 30. Mai 2024 (BGBl. 2024 I Nr. 173)
SIEM-System	Security, Information and Event-Management-System

Slg.	Sammlung der Rechtsprechung des Gerichtshofs und des Gerichts der Europäischen Union
SMEs	small and medium-sized entities
SMS	Short Message Service
s. o.	siehe oben
sog.	sogenannt/sogenannte(r/s)
SOX	Sarbanes Oxley Act
Stbg	Die Steuerberatung (Zeitschrift)
StGB	Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 1 des Gesetzes vom 24. Juni 2024 (BGBl. 2024 I Nr. 213)
StPO	Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Artikel 1 des Gesetzes vom 12. Juli 2024 (BGBl. 2024 I Nr. 234)
StraFo	StrafverteidigerForum (Zeitschrift)
StromStG	Stromsteuergesetz vom 24. März 1999 (BGBl. I S. 378; 2000 I S. 147), zuletzt geändert durch Artikel 13 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 412)
st. Rspr.	ständige Rechtsprechung
s.u.	siehe unten/siehe unter
StV	Strafverteidiger (Zeitschrift)
TK	Telekommunikation
TKG	Telekommunikationsgesetz vom 23. Juni 2021 (BGBl. I S. 1858), zuletzt geändert durch Artikel 35 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) g
TMG	Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch das Gesetz zur Änderung des Telemediengesetzes vom 19. November 2020 (BGBl. I S. 2456); zum 14.5.2024 außer Kraft getreten
Tz.	Textziffer
u.	und
u. a.	unter anderem/und andere
u. a. m.	und andere(s) mehr
UAG	Umweltauditgesetz in der Fassung der Bekanntmachung vom 4. September 2002 (BGBl. I S. 3490), das zuletzt durch Artikel 17 des Gesetzes vom 10. August 2021 (BGBl. I S. 3436) geändert worden ist
Ubg	Die Unternehmensbesteuerung (Zeitschrift)
ugs.	umgangssprachlich
UKBA	UK Bribery Act

Abkürzungsverzeichnis

UmwG	Umwandlungsgesetz vom 28. Oktober 1994 (BGBl. I S. 3210; 1995 I S. 428), zuletzt geändert durch Artikel 34 Absatz 16 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 411) g
UN	United Nations (Vereinte Nationen)
UNO	United Nations Organization (Organisation der Vereinten Nationen)
Unterabs.	Unterabsatz
UrhG	Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), zuletzt geändert durch Artikel 25 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858)
Urt.	Urteil
USA	United States of America
USD	US-Dollar
USt	Umsatzsteuer
UStG	Umsatzsteuergesetz in der Fassung der Bekanntmachung vom 21. Februar 2005 (BGBl. I S. 386), zuletzt geändert durch Artikel 23 des Gesetzes vom 27. März 2024 (BGBl. 2024 I Nr. 108)
usw.	und so weiter
u. U.	unter Umständen
UVgO	Verfahrensordnung für die Vergabe öffentlicher Liefer- und Dienstleistungsaufträge unterhalb der EU-Schwellenwerte (Unterschwellenvergabeordnung)
v.	von, vom
VAG	Gesetz über die Beaufsichtigung der Versicherungsunternehmen (Versicherungsaufsichtsgesetz) vom 1.4.2015 (BGBl. I S. 434), geändert durch Artikel 3 Absatz 6 des Gesetzes vom 26.7.2016 (BGBl. I S. 1824)
verb.	verbunden
VersR	Versicherungsrecht (Zeitschrift)
VersStG	Gesetz über die Beaufsichtigung der Versicherungsunternehmen (Versicherungsaufsichtsgesetz) vom 1. April 2015 (BGBl. I S. 434), zuletzt geändert durch Artikel 3 des Gesetzes vom 11. April 2024 (BGBl. 2024 I Nr. 119)
VG	Verwaltungsgericht
vgl.	vergleiche
VgV	Verordnung über die Vergabe öffentlicher Aufträge (Vergabeverordnung)
v. H.	von Hundert
VK	Vergabekammer
VO	Verordnung
VOB/A	Vergabe- und Vertragsordnung für Bauleistungen – Teil A

vs.	versus
VVG	Versicherungsvertragsgesetz vom 23. November 2007 (BGBl. I S. 2631), zuletzt geändert durch Artikel 4 des Gesetzes vom 11. April 2024 (BGBl. 2024 I Nr. 119)
VW	Volkswagen (Automobilhersteller)
Webinar	Web-Seminar (Seminar, das über das Internet abgehalten wird)
WM	Zeitschrift für Wirtschafts- und Bankrecht (Zeitschrift)
WP	Wirtschaftsprüfer
WpDVerOV	Verordnung zur Konkretisierung der Verhaltensregeln und Organisationsanforderungen für Wertpapierdienstleistungsunternehmen (Wertpapierdienstleistungs-, Verhaltens- und Organisationsverordnung) vom 17. Oktober 2017 (BGBl. I S. 3566), zuletzt geändert durch Artikel 1 der Verordnung vom 30. September 2022 (BGBl. I S. 1603)
WpHG	Wertpapierhandelsgesetz in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2708), zuletzt geändert durch Artikel 19 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149)
WpHGMAAnzV	Verordnung über den Einsatz von Mitarbeitern in der Anlageberatung, als Vertriebsmitarbeiter, in der Finanzportfolioverwaltung, als Vertriebsbeauftragte oder als Compliance-Beauftragte und über die Anzeigepflichten nach § 87 des Wertpapierhandelsgesetzes (WpHG-Mitarbeiteranzeigeverordnung) vom 21. Dezember 2011 (BGBl. I S. 3116), zuletzt geändert durch Artikel 1 der Verordnung vom 24. November 2017 (BGBl. I S. 3810)
WpÜG	Wertpapiererwerbs- und Übernahmegesetz vom 20. Dezember 2001 (BGBl. I S. 3822), zuletzt geändert durch Artikel 8 des Gesetzes vom 11. Dezember 2023 (BGBl. 2023 I Nr. 354)
WReG	Gesetz zur Einrichtung und zum Betrieb eines Registers zum Schutz des Wettbewerbs um öffentliche Aufträge und Konzessionen (Wettbewerbsregistergesetz) vom 18. Juli 2017 (BGBl. I S. 2739), zuletzt geändert durch Artikel 12 des Gesetzes vom 28. Juni 2023 (BGBl. 2023 I Nr. 172)
WRP	Wettbewerb in Recht und Praxis (Zeitschrift)
WuW	Wirtschaft und Wettbewerb (Zeitschrift)
WuW/E	Wirtschaft und Wettbewerb, Entscheidungssammlung

Abkürzungsverzeichnis

ZAG	Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdiensteaufsichtsgesetz) vom 17. Juli 2017 (BGBl. I S. 2446; 2019 I S. 1113), zuletzt geändert durch Artikel 11 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 411)
z. B.	zum Beispiel
ZCG	Zeitschrift für Corporate Governance (Zeitschrift)
ZD	Zeitschrift für Datenschutz (Zeitschrift)
ZHR	Zeitschrift für das gesamte Handels- und Wirtschaftsrecht (Zeitschrift)
Ziff.	Ziffer
ZIP	Zeitschrift für Wirtschaftsrecht (Zeitschrift)
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik (Zeitschrift)
ZJS	Zeitschrift für das Juristische Studium (Zeitschrift)
ZKG	Gesetz über die Vergleichbarkeit von Zahlungskontoentgelten, den Wechsel von Zahlungskonten sowie den Zugang zu Zahlungskonten mit grundlegenden Funktionen (Zahlungskontengesetz) vom 11. April 2016 (BGBl. I S. 720), zuletzt geändert durch Artikel 26 des Gesetzes vom 11. Dezember 2023 (BGBl. 2023 I Nr. 354)
ZGR	Zeitschrift für Unternehmens- und Gesellschaftsrecht (Zeitschrift)
ZRFC	Risk, Fraud & Compliance (Zeitschrift)
z. T.	zum Teil
ZUM	Zeitschrift für Urheber- und Medienrecht (Zeitschrift)
ZWH	Zeitschrift für Wirtschaftsstrafrecht und Haftung im Unternehmen (Zeitschrift)

Teil 1

Grundlagen, Erfolgsfaktoren und Handlungsstrategien

1. Kapitel

Compliance Management – Grundlagen, Orientierungshilfen und Erfolgsfaktoren

I. Grundlagen und Zusammenhänge

1. Anhaltende Bedeutung von Compliance und Compliance Management

Die rechtliche Bedeutung von Compliance für Unternehmen und Verbände¹ geht über den Wortsinn einer Regelbefolgung bzw. Regelkonformität weit hinaus.² Wenngleich es nach wie vor an einer einheitlichen Definition fehlt, wird mit Compliance häufig die Summe derjenigen Maßnahmen bezeichnet, die der Einhaltung aller an Unternehmen gerichteten Gesetze und Regeln dienen.³ Im Mittelpunkt stehen damit **organisatorische Vorkehrungen** zur Verhinderung von Regelverstößen, zur Kontrolle der eingeleiteten Maßnahmen, zur Aufdeckung von „Non-Compliance“, zur angemessenen Reaktion bzw. Sanktionierung von Regelverletzungen sowie zur regelmäßigen Aktualisierung der etablierten Strukturen und Maßnahmen (**Compliance Management**).⁴

Primär verantwortlich für das Compliance Management sind die Mitglieder der **Leitungsorgane**, die für normgerechtes Verhalten im Unternehmen und durch das Unternehmen sorgen müssen.⁵ Soweit die Geschäftsleiter nicht schon selbst

1 Die Begriffe „Unternehmen“ und „Verband“ werden nachfolgend synonym verwendet.

2 Zur Herkunft und Begriffsentwicklung von Compliance siehe *Moosmayer/Lösler*, in: *Moosmayer/Lösler, Corporate Compliance*, § 1 Rn. 2 ff.; *Klopp*, *Der Compliance-Beauftragte*, S. 21 ff.; *Kutschelis*, *Korruptionsprävention und Geschäftsleiterpflichten im nationalen und internationalen Unternehmensverbund*, S. 90 f.; *Jenne*, *Die Überprüfung und Zertifizierung von Compliance-Management-Systemen*, S. 32 ff.; *Balke*, in: *Born/Ghassemi-Tabar/Gehle* (Hrsg.) *MHdBGesRVII*, § 104 Rn. 2.

3 *Klopp*, *Der Compliance-Beauftragte*, S. 22 f. m. w. N.; ferner *Leley*, *Compliance im Arbeitsrecht*, S. 9 ff.; *Schmidt*, *Compliance in Kapitalgesellschaften*, S. 18 ff.; v. *Marnitz*, *Compliance-Management für mittelständische Unternehmen*, S. 1 ff.; *Balke*, in: *Born/Ghassemi-Tabar/Gehle* (Hrsg.), *MHdBGesRVII*, § 104 Rn. 2.

4 Vgl. *Jenne*, *Die Überprüfung und Zertifizierung von Compliance-Management-Systemen*, S. 34 ff.; *Balke*, in: *Born/Ghassemi-Tabar/Gehle* (Hrsg.) *MHdBGesRVII*, § 104 Rn. 2 sowie *Rodewald/Unger*, *BB* 2006, 113; *Hoffmann/Schieffer*, *NZG* 2017, 401 sowie *Schulz*, *BB* 2017, 1475 m. w. N. sowie *Michael/Weckmann*, in: *Erdmann/Diehl/Schradin*, *BeckOK VAG* (Stand: 1.9.2023), § 29 Rn. 9 (für Versicherungsunternehmen): „Die Compliance ... muss vor allem organisationsrechtlich begriffen werden.“

5 Siehe *Moosmayer*, *Compliance*, § 1 ff.; *Merkt*, *ZIP* 2014, 1705, 1706; *Jenne*, *Zur Überprüfung und Zertifizierung von Compliance-Management-Systemen*, S. 34 f.

und höchstpersönlich für die Erfüllung bestimmter Rechtspflichten verantwortlich sind (z.B. im Zusammenhang mit steuer- und sozialversicherungsrechtlichen Anforderungen, datenschutzrechtlichen Vorgaben oder Pflichten im Zusammenhang mit einer Insolvenz),⁶ müssen sie entsprechende organisatorische Maßnahmen treffen, um rechtskonformes Verhalten der Unternehmensangehörigen sicherzustellen und Regelverletzungen möglichst zu vermeiden.⁷ Darüber hinaus zeigen neuere Entwicklungen im Bereich der „**Lieferketten-Compliance**“ (siehe unter → Rn. 4f.), dass sich die Reichweite bestimmter Compliance-Anforderungen über den eigenen Unternehmensbereich erweitert. Der **Organisationsauftrag**⁸ der Geschäftsleitung umfasst sowohl die Entscheidung über die Einführung von Compliance-Maßnahmen als auch über die wesentlichen Strategie- und Strukturentscheidungen bezüglich des Compliance Managements.⁹ Dieses Kernbestandes an Organisationsaufgaben kann sich die Unternehmensleitung nicht entäußern bzw. durch Delegation vollständig entziehen.¹⁰

- 3 Compliance und das damit erforderliche Compliance Management sind durch eine anhaltende **Dynamik des rechtlichen Rahmens** geprägt, die durch vielfältige Aktivitäten des Gesetzgebers und der Gerichte sowie durch neue Entwicklungen in Rechtswissenschaft und Unternehmenspraxis bedingt sind. Dies gilt insbesondere für wachsende Anforderungen im Bereich der sog. „**ESG-Compliance**“,¹¹ für die besonderen Compliance-Herausforderungen im Zuge der **Digitalisierung**¹² sowie für gestiegene Risiken bei dem Verstoß gegen Sanktionsregelungen („**Sanctions Compliance**“).
- 4 Neben den (vormals überwiegend freiwillig zu erfüllenden) Anforderungen der **Corporate Social Responsibility (CSR)** werden Unternehmen und ihre Leitungsorgane zunehmend mit neuen Compliance-Pflichten zu **ESG-Themen**, also den Themenfeldern „**Environment**“ (u. a. Klimaschutz, nachhaltige Naturnutzung, Tierschutz), „**Social**“ (u. a. Schutz von Menschenrechten, Verhinderung von Ausbeutung, faire Arbeitsbedingungen) und „**Governance**“ (u. a. gute Unternehmensführung, Korruptionsbekämpfung, Ermöglichung von Melde-

6 Vgl. am Beispiel der GmbH *Stephan/Tieves*, in: MünchKomm-GmbHG, § 37 Rn. 26 f.

7 Vgl. *Schulz/Galster*, in: Bürkle/Hauschka/Schieffer, Der Compliance Officer, § 3 Rn. 9; *Kort*, GmbHR 2013, 566 ff.

8 *Haouache*, Unternehmensbeauftragte und Gesellschaftsrecht der AG und GmbH, S. 53.

9 Vgl. *Karbaum*, AG 2013, 863, 870.

10 Vgl. *Groß*, Chief Compliance Officer, S. 59 m. w. N. Zum Kernbereich der Compliance-Pflicht siehe auch *Gomer*, Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft, S. 160 ff.

11 Siehe hierzu etwa *Engelmann/Lescher*, in: Beisel/Andreas, Beck'sches Mandatshandbuch Due Diligence, § 39 Rn. 1 ff.

12 Vgl. etwa *Müller/Dittrich*, in: Dittrich/Dochow/Ippach, Rechtshandbuch Cybersicherheit im Gesundheitswesen, 18. Kap. sowie *Weihe*, CCZ 2024, 85.

systemen), konfrontiert.¹³ Prominente Beispiele für die zunehmende **ESG-Compliance-Regulierung** sind das seit dem 1.1.2023 geltende Lieferkettensorgfaltspflichtengesetz (**LkSG**)¹⁴ und die am 25.7.2024 in Kraft getretene EU-Lieferkettenrichtlinie (**CSDDD**).¹⁵ Erforderten Compliance-Risiken im Rahmen arbeitsteiliger (häufig internationaler) Wertschöpfungsnetzwerke bei vielen Unternehmen bereits in der Vergangenheit eine sorgfältige Auswahl und Kontrolle von Geschäftspartnern (Stichwort: „**Business Partner Control**“¹⁶), müssen Unternehmen nun im Anwendungsbereich von **LkSG** und **CSDDD** besondere **Sorgfaltspflichten** in Bezug auf Menschenrechte und bestimmte Umweltbelange in einem sanktionsbewehrten Rechtsrahmen erfüllen. Dazu zählen die Einrichtung eines Risikomanagements, die Durchführung von **Risikoanalysen**, das Ergreifen von **Präventions- und Abhilfemaßnahmen**, die Einrichtung eines **Melde- bzw. Beschwerdeverfahrens** sowie **Berichts- und Dokumentationspflichten**.¹⁷ Bei nicht unerheblichen Unterschieden zwischen LkSG und CSDDD resultieren aus beiden Normierungen für die betroffenen Unternehmen erweiterte und teilweise neue Anforderungen an das Compliance Management.¹⁸ Bei der Umsetzung der LkSG-Anforderungen zeigt sich zudem bereits ein sog. „**Trickle down**“-Effekt, wonach Unternehmen die Sorgfaltspflichten durch Vertragsgestaltung auch an Unternehmen weiterreichen, die nicht im unmittelbaren Anwendungsbereich des LkSG sind.¹⁹ Dadurch wird der Anwendungsbereich faktisch erheblich ausgeweitet.

Neben diesen neuen Sorgfaltspflichten in Lieferketten und **Wertschöpfungsnetzwerken** werden viele Unternehmen (je nach Geschäftsmodell und geschäftlichen Aktivitäten) mit zahlreichen weiteren **ESG-Compliance-Vorgaben** konfrontiert, beispielsweise im Zusammenhang mit der EU-Entwaldungsverord-

5

13 Zu den vielfältigen mit „ESG“ verknüpften Themen siehe *Altenbach*, in: Semler/v. Schenck/Wilsing, *Arbeitshandbuch für Aufsichtsratsmitglieder*, § 7 Rn. 21 ff.; zu den wachsenden Anforderungen der „ESG-Compliance“ siehe *Schmigale*, in: Andrejewski/Krause/von Hesberg, *Praxishandbuch ESG*, § 11 B.; *Geier/Meringdal/Stille*, *ESG-Compliance*, § 8; *Engelmann/Lescher*, in: Beisel/Andreas, *Beck'sches Mandatshandbuch Due Diligence*, § 39 Rn. 1 ff.

14 Richtlinie (EU) 2024/1760 des Europäischen Parlaments und des Rates vom 13. Juni 2024 über die Sorgfaltspflichten von Unternehmen im Hinblick auf Nachhaltigkeit und zur Änderung der Richtlinie (EU) 2019/1937, ABl. L vom 5.7.2024, S. 1.

15 Vgl. sowie hierzu *Vitt*, CB 2024, 365.

16 Zu Compliance-Fragen im Rahmen des sog. „Supply Chain Management“ aus Management-sicht siehe → *Schleper/Förstl*, Kap. 17.

17 Zu den LkSG-Sorgfaltspflichten → *Heske*, Kap. 18 sowie *Hagel/Wiedmann* → Kap. 19. Vgl. ferner *Schröder/Schulz*, *Praxisleitfaden Supply Chain Compliance*, Rn. 52 ff.; *Hettich/Scharnitzky*, in: Kubis/Tödtmann, *Arbeitshandbuch für Vorstandsmitglieder*, § 14 Rn. 256 ff.

18 Vgl. *Hettich/Scharnitzky*, in: Kubis/Tödtmann, *Arbeitshandbuch für Vorstandsmitglieder*, § 14 Rn. 256 ff.; *Schröder/Schulz*, *Praxisleitfaden Supply Chain Compliance*, Rn. 52 ff.

19 Vgl. *Schröder/Schulz*, *Praxisleitfaden Supply Chain Compliance*, Rn. 1, 491 sowie *Spießhofer*, in: Moosmayer/Lösler, *Corporate Compliance*, § 16 Rn. 42 f.

nung (**EU-Deforestation Regulation, EUDR**),²⁰ der EU-Zwangsarbeiterverordnung (**EU Forced Labor Prevention Regulation, FLPR**)²¹ oder der **EU-Konfliktmineralien-Verordnung**.²² Neue Anforderungen hinsichtlich der Compliance-Berichterstattung folgen aus der **Corporate Sustainability Reporting Directive (CSRD)**²³ und ihrer Umsetzung in nationales Recht.²⁴

- 6 Ein weiteres Beispiel für die Herausbildung neuer Compliance-Risiken und daraus folgender komplexer Anforderungen an das Compliance Management ist der Bereich **IT-Compliance** und **Cyber-Security**.²⁵ Cyber-Angriffe haben sich zu einem erheblichen Risiko für Unternehmen entwickelt und können nicht nur deren Infrastruktur beeinträchtigen, sondern auch erhebliche Haftungsgefahren für die Unternehmen und ihre Leitungsorgane mit sich bringen.²⁶ Zugleich steigt die Regulierungsdichte auch bei der **IT-Compliance** immer weiter an, besondere Compliance-Pflichten ergeben sich beispielsweise aus der **DSGVO**, dem Gesetz zum Schutz von Geschäftsgeheimnissen (**GeschGehG**), dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (**BSIG**)²⁷ und seinen geplanten Neuregelungen, dem Digital Operational Resilience Act (**DORA**)²⁸

20 Verordnung (EU) 2023/1115 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über die Bereitstellung bestimmter Rohstoffe und Erzeugnisse, die mit Entwaldung und Waldschädigung in Verbindung stehen, auf dem Unionsmarkt und ihre Ausfuhr aus der Union sowie zur Aufhebung der Verordnung (EU) Nr. 995/2010, ABl. L 150 vom 9.6.2023, S. 206.

21 Legislative Entschließung des Europäischen Parlaments vom 23. April 2024 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ein Verbot von in Zwangsarbeit hergestellten Produkten auf dem Unionsmarkt (COM(2022)0453 – C9-0307/2022 – 2022/0269(COD)), P9_TA(2024)0309. Die EUFLR legt Sorgfaltspflichten nicht fest, sondern setzt sie voraus.

22 Verordnung (EU) 2017/821 des Europäischen Parlaments und des Rates vom 17. Mai 2017 zur Festlegung von Pflichten zur Erfüllung der Sorgfaltspflichten in der Lieferkette für Unionseinführer von Zinn, Tantal, Wolfram, deren Erzen und Gold aus Konflikt- und Hochrisikogebieten, ABl. L 130 vom 19.5.2017, S. 1 (Konfliktmineralienverordnung).

23 Zur CSRD und den neuen Anforderungen an die Nachhaltigkeitsberichterstattung ausführlich → *Beisheim*, Kap. 16 sowie *Schmigale*, in: Andrejewski/Krause/von Hesberg, Praxishandbuch ESG, § 11 B., Rn. 14 ff.

24 Zu den neuen Herausforderungen des „Nachhaltigkeitsreportings“ → *Beisheim*, Kap. 16.

25 Siehe → *Bensinger*, Kap. 14 sowie *Müller/Dittrich*, in: Dittrich/Dochow/Ippach, Rechtshandbuch Cybersicherheit im Gesundheitswesen, 18. Kap.

26 Vgl. etwa *Müller/Dittrich*, in: Dittrich/Dochow/Ippach, Rechtshandbuch Cybersicherheit im Gesundheitswesen, 18. Kap. sowie *Weihe*, CCZ 2024, 85.

27 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz, BSIG) v. 14.8.2009, BGBl. I, S. 2821. Vgl. hierzu *Müller/Dittrich*, in: Dittrich/Dochow/Ippach, Rechtshandbuch Cybersicherheit im Gesundheitswesen, 18. Kap. Rn. 28 ff. sowie → *Bensinger*, Kap. 14.

28 Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011, ABl. L 333/1, 27.12.2022 sowie hierzu → *Bensinger*, Kap. 14, Rn. 81 ff.

sowie den Regelungen zur Umsetzung der Richtlinie zur Verbesserung der Netz- und Informationssicherheit (**NIS-Richtlinie**).²⁹

Für grenzüberschreitend tätige Unternehmen sind ferner die besonderen Anforderungen des **Exportkontrollrechts** und des Außenhandelsrechts zu beachten, erhebliche Risiken können auch aus der Nichtbeachtung oder Umgehung von **Sanktionsregelungen** resultieren.³⁰ Angesichts zunehmender internationaler Konflikte sind diverse neue Sanktionsregelungen geschaffen worden.³¹ Unternehmen und ihre Leitungsorgane müssen daher sorgfältig prüfen, ob der Anwendungsbereich dieser Regelungen für sie oder ihre **Geschäftspartner** eröffnet ist, um die relevanten Sorgfaltspflichten (insbesondere auch beim Umgang mit ihren Geschäftspartnern) zu erfüllen.³² 7

Die genannten Entwicklungen zeigen exemplarisch, dass Inhalt und Umfang des Compliance Managements durch ein dynamisches regulatorisches Umfeld immer mehr erweitert werden.³³ Sowohl für die Geschäftsleiter als auch für diejenigen, die im Rahmen wirksamer Delegation mit Compliance-Aufgaben betraut sind, erweist sich Compliance-Management somit als **Daueraufgabe in einem dynamischen Umfeld** (siehe unter → Rn. 16 ff.). 8

2. Compliance Management als Inbegriff regelkonformer Unternehmensorganisation

Im Fokus der anhaltenden Diskussion um Compliance in Unternehmen und ihrer Sicherstellung durch Compliance Management in Form effektiver Strukturen, Prozesse und Systeme stehen folgende **Fragen der Unternehmensorganisation**: 9

- Wie lassen sich die vielfältigen Risiken und Nachteile aus Regelverletzungen („Non-Compliance“) bestmöglich verhindern oder reduzieren?³⁴

29 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik Europäische Kommission, NIS2-Richtlinie, <https://digital-strategy.ec.europa.eu/de/node/10361/printable/pdf> (zuletzt abgerufen am 30.9.2024) sowie hierzu → *Bensinger*, Kap. 14, Rn. 84 ff.

30 Zu Exportkontrolle und Compliance siehe → *von Bodungen*, Kap. 25. Zur sog. „Sanctions Compliance“ siehe → *Salathé/Moussaoui*, Kap. 24 sowie *Voss*, CCZ 2024, 198 zum 14. Russland-Sanktionspaket der EU.

31 Zum 14. Russland-Sanktionspaket der EU siehe *Voss*, CCZ 2024, 198 sowie → *Salathé/Moussaoui*, Kap. 24.

32 Siehe die Beispiele bei *Voss*, CCZ 2024, 198, 203 f.

33 Siehe in Bezug auf ESG-Themen *Engelmann/Lescher*, in: Beisel/Andreas, Beck'sches Mandatshandbuch Due Diligence, § 39 Rn. 1.

34 Vgl. *Merk*, ZIP 2014, 1705, 1706; v. *Marnitz*, Compliance-Management für mittelständische Unternehmen, S. 1 ff.; *Jenne*, Zur Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 34 f. Zu diesem Organisationsaspekt vgl. bereits *Schneider*, ZIP 2003, 645; *Hauschka*, ZIP 2004, 877, sowie *Spindler*, WM 2008, 905. Ähnlich *Meyer*, DB 2014, 1063: „Compliance [...] als die Verpflichtung, jederzeit die vollumfängliche Einhaltung aller für das Unternehmen in sämtlichen Tätigkeitsregionen relevanten Rechtsvorschriften dokumentiert sicherzustellen.“

- Wie, durch wen und mit welchen Ressourcen lässt sich regelkonformes Verhalten im Unternehmen erreichen und gewährleisten?
- Welche Kernelemente sollte ein effizientes und effektives Compliance Management haben?
- Wie weit reicht die Verantwortung der Leitungsorgane und in welchem Umfang können sie Aufgaben delegieren?
- Welchen Beitrag können unterschiedliche Unternehmensfunktionen leisten?
- Wie können Unternehmen und Verbände aus aufgedeckten Regelverstößen lernen?³⁵

10 Diese **Grundfragen einer rechtskonformen Unternehmensorganisation**³⁶ betreffen grundsätzlich alle Unternehmen, von der börsennotierten Aktiengesellschaft und der mittelständischen GmbH bis hin zum Start-up-Unternehmen.³⁷ Denn sämtliche Unternehmen und ihre Leitungsorgane müssen bei ihrer Tätigkeit eine Vielzahl von Normen und rechtlichen Vorgaben von Gerichten und Behörden beachten.³⁸ Zahlreiche aktuelle Fälle von „Non-Compliance“ bei Unternehmen und Verbänden aus ganz unterschiedlichen Branchen, mit unterschiedlichen Geschäftsmodellen und mit unterschiedlicher Größe und Struktur³⁹

35 Vgl. zu diesem Lernprozess ausführlich *Nothelfer*, CCZ 2013, 23 ff.

36 Vgl. *Spindler*, WM 2008, 905; ähnlich bereits *Schneider*, ZGR 1996, 225, 230 ff.

37 Zur Relevanz von Compliance für sog. Start-up-Unternehmen siehe *Nothelfer*, CCZ 2016, 64; zur Relevanz für kleinere und mittelständische Unternehmen siehe u. a. *Merkt*, ZIP 2014, 1705 ff. Zur Bedeutung von Compliance für die AG siehe etwa *Harbarth*, ZHR 179 (2015), 136, sowie *Fleischer*, in: BeckOGK AktG, Stand: 1.2.2024, § 91 Rn. 62 ff.

38 Siehe bereits *Schneider*, ZGR 1996, 225, 227 in Bezug auf öffentlich-rechtliche Gebote und Verbote.

39 Zu prominenten Fällen von „Non-Compliance“ und damit verbundener Nachteile und Kosten siehe. Zu aktuellen Compliance-Fällen → *Stehr/Knopp*, Kap. 15 Rn. 70. Siehe ferner *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 21 ff.; *Gomer*, Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft, S. 73 ff. Aus der Vielzahl in den Medien gemeldeter (Verdachts-)Fälle von „Non-Compliance“ vgl. beispielsweise die Meldungen zum Fall „Wirecard“: <https://www.rnd.de/wirtschaft/wirecard-skandal-was-passierte-wann-die-chronologie-des-versagens-Q52XQE2S6VHQ3JKPGFQKWWMS4.html>; zur „Cum-Ex-Thematik“: <https://www.handelsblatt.com/finanzen/banken-versicherungen/cum-ex/vom-renditeturbo-zum-karrierekiller-cum-ex-deals-die-chronik/13033390.html>; zum sog. „Dieselskandal“ u. a.: <https://www.rnd.de/wirtschaft/chronologie-des-dieselskandals-das-schmutzigste-kapitel-der-vw-geschichte-PZZDQRN5LRELVB35C2KDU6K7Y.html>; zu den sog. „Panama Papers“: <https://www.sueddeutsche.de/politik/eine-enthuellung-und-ihre-folgen-panama-papers-chronik-der-ermittlungen-1.3373248>; sowie den „Paradise Papers“: <https://projekte.sueddeutsche.de/paradisepapers/politik/das-ist-das-leak-e229478/>, 24.9.2020; zum „Libor Skandal“: <https://www.spiegel.de/thema/libor-skandal/>. Siehe ferner Meldungen zu Geldwäsche-Delikten: [https://www.capital.de/wirtschaft-politik/der-unglaubliche-230-milliarden-skandal-zum-sog.-Sommermärchen-\(DFB\):](https://www.capital.de/wirtschaft-politik/der-unglaubliche-230-milliarden-skandal-zum-sog.-Sommermärchen-(DFB):) <https://www.br.de/nachrichten/sport/das-sommermaerchen-chronologie-der-wm-affaere-RsLldza>; und zu Versäumnissen im Zusammenhang mit Schadsoftware „Wanna Cry“: <https://www.spiegel.de/netzwelt/web/wannacry-attacke-fakten-zum-globalen-cyberangriff-a-1147523.html>. Compliance-Verstöße sind häufig auch Gegenstand von Kartellverfahren der EU-Kommission, siehe etwa: <https://www.spiegel.de/wirtschaft/unternehmen/>

zeigen, dass die Beantwortung dieser Fragen offenbar für viele Unternehmen nach wie vor eine Herausforderung bis hin zu einer kaum lösbaren Aufgabe darstellt.⁴⁰ Dies gilt trotz der Tatsache, dass inzwischen viele Verbände und Unternehmen über Compliance-Programme bzw. ein Compliance-Management-System (CMS) verfügen.⁴¹

3. Risiken und Nachteile von Regelverletzungen und „Non-Compliance“

Die Relevanz eines wirksamen Compliance Managements für alle Unternehmen und Verbände wird durch die Risiken, Nachteile und Kosten aus aufgedeckten Fällen von Regelverletzungen („Non-Compliance“) belegt. Diese sind vielfältig und können existenzbedrohende Ausmaße annehmen.⁴² Die Nachteile umfassen unter anderem:⁴³

- strafrechtliche Sanktionen gegen die Geschäftsleiter, sonstige Verantwortliche und involvierte Unternehmensangehörige;
- strafrechtliche Sanktionen gegen das Unternehmen bzw. den Verband;⁴⁴
- Bußgelder gegen das Unternehmen selbst und die Geschäftsleiter;⁴⁵
- Entzug der Betriebserlaubnis bzw. Lizenz bis hin zur Zwangsliquidation;
- Nachzahlung von Steuern bzw. Strafzuschlägen;⁴⁶
- Verpflichtung zum Schadensersatz;
- Einziehung von Vermögenswerten bei rechtswidrigen Geschäften (nach dem „Brutto-Prinzip“);⁴⁷
- Unwirksamkeit von Transaktionen, Nichtigkeit bzw. Anfechtbarkeit von Verträgen und sonstigen Rechtsgeschäften;

bmw-daimler-und-vw-unter-kartellverdacht-eu-kommission-verschaerft-ermittlungen-a-12-28660.html; oder: <https://www.spiegel.de/wirtschaft/unternehmen/wilke-wurst-behoerden-bericht-zeigt-zustande-nach-fabrikschliessung-a-1293802.html> (alle Quellen zuletzt abgerufen am 24.9.2024).

40 Vgl. etwa Schulz, CB 08/2017, I (Editorial). Zu aktuellen Fällen von Non-Compliance siehe → Stehr/Knopp, Kap. 15 Rn. 70.

41 Vgl. Neufang, IRZ 2017, 249.

42 Vgl. etwa Kremer, in: Kremer u. a., Deutscher Corporate Governance Kodex, DCGK, Grundsatz 5, Rn. 36 ff.; Schockenhoff, ZHR 180 (2016), 197, 203 f.

43 Zu strafrechtlichen Sanktionen bei Non-Compliance siehe → Böttger, Kap. 2 Rn. 143. Zum Spektrum der Compliance-Risiken allgemein etwa Leisch/Lohner, M&A Review 2009, 133, 134.

44 Siehe auch → Böttger, Kap. 2 Rn. 143 sowie → Schwartz, Kap. 29 Rn. 59.

45 Zu den kartellrechtlichen Risiken bei Non-Compliance siehe → Seeliger/Mross/Seydel, Kap. 27; zum Risiko drastischer Bußgelder bei Kartellrechtsverstößen Trüg/Ruppert, ZWeR 2020, 69 ff. sowie bereits Schockenhoff, ZHR 180 (2016), 197, 204 f. mit zahlreichen Beispielen.

46 Beispiele bei Schockenhoff, ZHR 180 (2016), 197, 204 f. Zur Tax Compliance siehe → Schwartz, Kap. 29.

47 Siehe → Böttger, Kap. 2 Rn. 146 ff.

Teil 1 Grundlagen, Erfolgsfaktoren und Handlungsstrategien

- Ausschluss von der Auftragsvergabe;⁴⁸
- Ausschluss von (Verwaltungs-)Verfahren;
- Entfall der „Zuverlässigkeit“ und damit verbundenen verfahrensrechtlichen Erleichterungen;
- Imageverlust und Reputationsschäden;
- Vertrauensverlust bei relevanten Bezugsgruppen (u. a. Mitarbeiter, Kunden, Lieferanten, Investoren);
- Verschlechterung der Kreditwürdigkeit und des Ratings;
- höhere (Re-)Finanzierungskosten;
- Delisting;
- Nachteile bei Personalgewinnung und Mitarbeiterbindung;
- hohe Rechtsberatungskosten.⁴⁹

- 12 Dieses umfangreiche Spektrum zeigt, dass die Risiken, **Nachteile und Kosten von „Non-Compliance“** für Unternehmen und Verbände gravierend sind und (auch durch ihre Verknüpfung bzw. Kumulation) unternehmerische Aktivitäten und Geschäftsmodelle erheblich beeinträchtigen oder sogar vollständig vernichten können. Dies wird durch viele prominente Fälle von „Non-Compliance“ bei Unternehmen und Verbänden aus unterschiedlichen Branchen, mit unterschiedlichen Geschäftsmodellen und mit unterschiedlicher Größe und Struktur belegt.⁵⁰ Dabei beruhen Regelverletzungen einerseits auf **vorsätzlichem Fehlverhalten** bzw. kriminellen Aktivitäten von Personen (z. B. in Fällen von Korruptionsvergehen oder Kartellrechtsverstößen).⁵¹ In anderen Fällen ist die Ursache von „Non-Compliance“ **fahrlässiges Verhalten** durch Verletzung von Sorgfaltspflichten oder aufgrund unzureichender Kenntnis von Regeln und Geboten.⁵² Normative Vorgaben werden zum Teil nicht richtig eingeschätzt oder ihre dynamische (Weiter-)Entwicklung wird nicht hinreichend beachtet.⁵³

48 Zur Bedeutung von Compliance im Vergabeverfahren siehe → *Scherer*, Kap. 28.

49 Hohe Rechtsberatungskosten können insbesondere im Zusammenhang mit einer internen Untersuchung anfallen, zu letzterer siehe → *Wettner/Walter*, Kap. 8.

50 Vgl. zu aktuellen Fällen → *Stein/Knopp*, Kap. 15 Rn. 70. Zu prominenten Fällen von „Non-Compliance“ in der Vergangenheit siehe etwa die Darstellung von *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 21 ff.

51 Zu den diversen Straftatbeständen im Bereich der Korruption vgl. → *Böttger*, Kap. 2 Rn. 36 ff. Zum Umgang mit Korruptionsrisiken in M&A-Transaktionen siehe → *Ullrich*, Kap. 26 Rn. 77. Zu den diversen Formen kartellrechtswidrigen Verhaltens siehe → *Seeliger/Mross/Seydel*, Kap. 27.

52 Vgl. *Heißner*, Erfolgsfaktor Integrität, S. 114; *Busmann*, CCZ 2016, 50 ff.; *Preusche/Würz*, Compliance, S. 30 f.

53 Vgl. *Wagner/Rutloff/Miederhoff*, CCZ 2020, 1. Zur Notwendigkeit fortlaufender Beobachtung der Rechtsentwicklung und regelmäßiger Aktualisierung der Compliance-Maßnahmen siehe unter → Rn. 89.

4. Funktionen von Compliance und Compliance Management

Die dargestellten Risiken und Nachteile aus „Non-Compliance“ zeigen, dass wirksame Compliance-Maßnahmen für alle Unternehmen und Verbände aktuell und relevant sind.⁵⁴ Die **proaktive Vermeidung bzw. Reduzierung von Regelverstößen** ist damit nicht nur eine Pflicht der Leitungsorgane, sondern eine wichtige Führungs- und Organisationsaufgabe (siehe dazu unter → Rn. 36 f., 54 ff.).⁵⁵ Compliance Management erfüllt dabei die folgenden **Funktionen**.⁵⁶ Compliance Management dient sowohl dem **Schutz** des Verbands vor zivilrechtlicher Haftung und strafrechtlichen Sanktionen als auch der Prävention bzw. Reduzierung persönlicher zivil- und strafrechtlicher Haftungsrisiken der Mitglieder der Leitungsorgane und der Mitarbeiter.⁵⁷ Darüber hinaus zielen Compliance-Maßnahmen auch auf den Schutz vor Angriffen auf das Unternehmen sowie den Schutz der Unternehmensposition im Wettbewerb.⁵⁸ Ferner dient Compliance dem Schutz der **Reputation** und des **Vertrauens der Stakeholder** in eine ordnungsgemäße und rechtskonforme Geschäftstätigkeit.⁵⁹

Neben dieser präventiven **Schutzfunktion** ist auch die **Risikomanagementfunktion** wichtig, denn zwischen Compliance Management und Risikomanagement besteht ein enger Zusammenhang.⁶⁰ Das Risikomanagement mit seinen Methoden und Verfahren ist eine wichtige Erkenntnisquelle für die Identifikation und systematische Erfassung von Compliance-Risiken.⁶¹

54 Vgl. etwa *Harbarth/Brechtel*, ZIP 2016, 241, sowie etwa die umfassenden Darstellungen von *Wieland/Steinmeyer/Grüninger* (Hrsg.), *Handbuch Compliance-Management 2020*; *Hauschka/Moosmayer/Lösler* (Hrsg.), *Corporate Compliance*, siehe ferner *Moosmayer*, *Compliance*, 3. Aufl. 2015, S. VII.

55 Ähnlich *Dittmers*, *Werteorientiertes Compliance-Management*, S. 29 m. w. N.; *Klopp*, *Der Compliance-Beauftragte*, S. 22 f. („Managementfunktion“) m. w. N., sowie *Kutschelis*, *Korruptionsprävention und Geschäftsleiterpflichten im nationalen und internationalen Unternehmensverbund*, S. 88 f., 98. Zur Bedeutung des sog. *Corporate Reputation Management* ausführlich *Seibt*, DB 2015, 171.

56 Zu den Funktionen von Compliance siehe *Michael/Weckmann*, in: *Erdmann/Diehl/Schradin*, *BeckOK VAG*, 22. Edition (Stand: 10.9.2023), VAG § 29 Internes Kontrollsystem, Rn. 38 ff. sowie ausführlich *Gomer*, *Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft*, S. 73 ff.

57 Vgl. *Gößwein/Hohmann*, BB 2011, 963, 964 sowie *Gomer*, *Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft*, S. 73.

58 Vgl. *Gößwein/Hohmann*, BB 2011, 963, 964; zu sog. „Cyber Risks“ als neuem Brennpunkt der Managerhaftung siehe *Schmidt-Versteyl*, NJW 2019, 1637.

59 Vgl. *Gößwein/Hohmann*, BB 2011, 963, 964.

60 Vgl. *Schulz/Galster*, in: *Bürkle/Hauschka*, *Der Compliance Officer*, § 4 Rn. 12 ff. Zum Zusammenhang zwischen Compliance- und Risikomanagement siehe ausführlich *Kark*, *Compliance-Risikomanagement*, 3. Aufl. 2024.

61 Vgl. *Kark*, *Compliance-Risikomanagement*, 3. Aufl. 2024, Rn. 634 ff.

- 15 Das Compliance Management erfüllt ferner eine wichtige **Informations- und Beratungsfunktion**,⁶² welche sowohl die Beratung der Unternehmensleitung zur Steuerung von Compliance-Risiken durch organisatorische Maßnahmen⁶³ als auch die Organisation der Beratung aller Unternehmensangehörigen in allen relevanten Compliance-Fragen umfasst.⁶⁴ Da zu den notwendigen organisatorischen Maßnahmen auch die kontinuierliche Überwachung und Kontrolle relevanter Normen und Regeln und deren Durchsetzung zählt,⁶⁵ erfüllt Compliance ferner eine **Monitoring-Funktion**.⁶⁶ Durch die systematische Erfassung von Rechts- und Compliance-Risiken, die kontinuierliche Beobachtung neuer rechtlicher Entwicklungen und deren Auswirkungen auf das Compliance-System hat das Compliance Management im Unternehmen zudem eine **Qualitätssicherungs- und Innovationsfunktion**.⁶⁷ Indem ein wirksames Compliance Management dazu beiträgt, Normverstöße zu verhindern bzw. zu reduzieren, fördert es die Glaubwürdigkeit des Unternehmens bei seinen Mitarbeitern, Kunden, Geschäftspartnern und sonstigen Stakeholdern und erfüllt damit eine **Marketing-Funktion**.⁶⁸

5. Compliance Management als Daueraufgabe im dynamischen Umfeld

- 16 Die Flut der rechtlichen Vorgaben und Anforderungen betrifft alle Unternehmensbereiche und speist sich aus allen Quellen des Zivilrechts, des öffentlichen Rechts und des Strafrechts.⁶⁹ Die Sicherstellung rechtskonformer Tätigkeit durch Compliance Management ist anspruchsvoll, denn mit jeder Art unternehmerischer Aktivität sind vielfältige rechtliche Anforderungen verbunden. Das gilt für steuerrechtliche sowie arbeits- und sozialversicherungsrechtliche Erfordernisse, ebenso wie für besondere Pflichten im Falle von Zahlungsunfähigkeit und Insolvenz.⁷⁰ Auch **Korruption** und **Kartellrechtsverstöße** zählen für viele Unternehmen zu den zentralen Compliance-Risiken ihrer Geschäftstätigkeit.⁷¹

62 Vgl. Inderst, in: Inderst/Bannenberg/Poppe, S. 136 f.; Lösler, NZG 2005, 104, 105; sowie Gomer, Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft, S. 75 f.

63 Vgl. Schulz/Renz, BB 2012, 2511.

64 Vgl. Klopp, Der Compliance-Beauftragte, S. 57.

65 Vgl. Klopp, Der Compliance-Beauftragte, S. 57 f. Zum Aspekt der Legalitätsthroughsetzungspflicht siehe Bürkle, in: Moosmayer/Lösler, Corporate Compliance, § 52 Rn. 29.

66 Vgl. Lösler, NZG 2005, 104, 105.

67 Vgl. Hauschka, Compliance im Gesellschaftsrecht, 103, 111; sowie Gomer, Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft, 2020, 77 f.

68 Vgl. Lösler, NZG 2005, 104, 105; Klopp, Der Compliance-Beauftragte, S. 58 f.; Gomer, Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft, S. 78 f.

69 Schulz, Rechtliches Risikomanagement und Compliance im Mittelstand, in: Kessler, Unternehmensfinanzierung Mittelstand, § 6 Rn. 4. Ferner Schmidt, Compliance in Kapitalgesellschaften, S. 17 mit dem Hinweis auf Schätzungen, wonach (bereits 2010) durchschnittlich 900 Vorschriften pro Unternehmen zu beachten sein sollten.

70 Vgl. Kark, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 55 ff.

71 Vgl. Schockenhoff, ZHR 180 (2016), 197, 204; Trüg/Ruppert, ZWeR 2020, 69 ff.

Darüber hinaus bestehen in vielen Bereichen der Unternehmensfinanzierung komplexe Rechts- und Compliance-Risiken.⁷² Wie oben exemplarisch dargestellt, kommen ständig neue bzw. erweiterte Rechtspflichten aus neuen Gesetzen und Regelungsvorhaben hinzu. So hatte bereits die **Datenschutzgrundverordnung (DSGVO)**⁷³ das für alle Unternehmen geltende Pflichten- (und Sanktions-)Spektrum in Bezug auf die Beachtung und Umsetzung datenschutzrechtlicher Vorgaben erheblich erweitert.⁷⁴ Über die typischen Erfordernisse des Datenschutzrechts hinausgehend wirft die **Digitalisierung** zahlreiche weitere Rechtsfragen und damit verbundene besondere Compliance-Risiken auf, insbesondere im Hinblick auf die regelkonforme Entwicklung sowie den rechtssicheren Einsatz digitaler Geschäftsmodelle.⁷⁵ Die dynamischen Entwicklungen rund um „AI Act“ und „Data Act“ zeigen, dass sich ein neuer Bereich der „**KI-Compliance**“ entwickelt.⁷⁶ Wie angeführt, stellt die Gewährleistung einer funktionierenden IT-Sicherheitsstruktur und der Schutz vor **Cyber-Angriffen** aller Art eine komplexe und anspruchsvolle Daueraufgabe des Compliance Managements dar, die einerseits durch zunehmende Cyber-Kriminalität, andererseits durch zahlreiche neue KI- bzw. Cyber-(Security)Regulierungen geprägt wird.⁷⁷ Die Organisation einer nachhaltigen **Cyber-Security** hat sich zu einer Kernaufgabe des Compliance Managements entwickelt.⁷⁸ Auch die Prävention und Kontrolle von **Geldwäsche-Risiken** (nicht zuletzt im Zusammenhang mit virtuellen Währungen) ist von anhaltender Bedeutung und reicht längst über den Finanzdienstleistungssektor hinaus.⁷⁹ Die Erfüllung der damit verbundenen umfangreichen ge-

72 Vgl. *Schulz*, Rechtliches Risikomanagement und Compliance im Mittelstand, in: Kessler, Unternehmensfinanzierung Mittelstand, § 6 Rn. 23.

73 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), L 119/1 vom 4.5.2016. Zu Fragen des Datenschutzrechts beim Compliance Management ausführlich → *Becker/Böhlke/Fladung*, Kap. 12.

74 Siehe hierzu ausführlich *Becker/Böhlke/Fladung*, Kap. 12.

75 Siehe hierzu auch die Beispiele bei *Sassenberg/Faber* (Hrsg.), Rechtshandbuch Industrie 4.0 und Internet of Things; *Schulz*, Digitale Transformation – Herausforderung und Chance für Rechtsanwälte, in: *Schulz/Hartung* (Hrsg.), Recht 2030 – Legal Management in der Digitalen Transformation, Kap. 2 Rn. 29 ff., sowie *Jacobs*, in: *Schulz/Hartung* (Hrsg.), a. a. O., Kap. 22 Rn. 1 ff.

76 Siehe zu „AI Act“ und „Data Act“ → *Becker/Böhlke/Fladung*, Kap. 12 Rn. 1, 22, 98 sowie zum „Data Act“ ausführlich *Jacobs*, Kap. 13, Rn. 33 ff.

77 Siehe → *Bensinger*, Kap. 14. Ferner *Schulz*, BB 2019, 579. Zur Cyber-Security und IT-Compliance siehe auch *Daghles*, DB 2018, 2289 ff.; *Mehrbrey/Schreibauer*, MMR 2016, 75, sowie *Jacobs*, CB 2017, 299.

78 Zu Cyber Risks und Cyber-Security ausführlich → *Bensinger*, Kap. 14. Zu „Cyber Risks“ als Brennpunkt der Managerhaftung *Schmidt-Versteyl*, NJW 2019, 1637.

79 Siehe → *Komma*, Kap. 23 sowie *Krais*, Geldwäsche für Industrie und Handel. Zu Stellung und Aufgabe des Geldwäschebeauftragten ausführlich → *Kaetzler*, Kap. 22.

setzlichen Compliance-Pflichten erfasst über den Finanzdienstleistungssektor hinaus auch sog. Güterhändler.⁸⁰

- 17 Wie ausgeführt, ergeben sich aus vielfältigen Regelungen unter dem Oberbegriff der „**ESG-Compliance**“ zahlreiche neue Pflichten und Haftungsrisiken für Unternehmen und deren Leitungsorgane. Das LkSG als prominentes Beispiel der ESG-Regulierung zeigt exemplarisch, dass bestehende Compliance-Programme um einen Bereich der **Supply-Chain-Compliance** (insbesondere in Bezug auf Menschenrechte und Umweltbelange) erweitert werden müssen.⁸¹
- 18 Rechts- und Compliance-Risiken sind ferner bei Wachstumsstrategien, etwa beim Erwerb von Unternehmen und Restrukturierungsmaßnahmen oder beim Eintritt in Joint Ventures zu beachten („**Compliance Due Diligence**“).⁸² Wie die zunehmende Regulierung von Lieferketten und Wertschöpfungsnetzwerken zeigt, gewinnt dabei die proaktive Compliance-Kontrolle von Geschäftspartnern, Vertriebsmittlern und sonstigen Intermediären immer größere Bedeutung („**Business Partner Compliance**“).⁸³
- 19 Exportorientierte Unternehmen müssen bei Eintritt in neue Märkte zudem neue Vorgaben des **Exportkontrollrechts** und des **Außenwirtschaftsrechts** sowie im anwendbaren Umfang auch die Normen anderer Rechtsordnungen beachten.⁸⁴ Hinzu kommen neue Embargo-Bestimmungen und sonstige **Sanktionsrechts**-regelungen.⁸⁵

6. Compliance als Basis für „Good Corporate Governance“

- 20 Wie die anhaltende Diskussion um die „ESG-Compliance“ zeigt, tragen zur wachsenden Bedeutung von Compliance Management auch neue, umfangreiche Regulierungen und Gesetzesvorhaben (insbesondere mit Bezug auf den Schutz von Umweltbelangen und Menschenrechten) sowie höhere Ansprüche der Stakeholder in Bezug auf **verantwortungsvolle Unternehmensführung** und „**Good Governance**“ bei.⁸⁶ Unternehmen werden dadurch nicht nur mit höheren Anforderungen ihrer Mitarbeiter, Kunden, Lieferanten, Investoren und der Öffentlichkeit im Hinblick auf ein verantwortungsvolles, d.h. integrires und

80 Siehe → *Komma*, Kap. 23.

81 Vgl. *Schröder/Schulz*, Praxisleitfaden Supply Chain Compliance, Rn. 9 ff.

82 Zum Compliance Management bei M&A-Transaktionen ausführlich → *Ullrich*, Kap. 26.

83 Vgl. *Bicker/Stoklasa*, BB 2018, 519 m. w. N.

84 Siehe oben → Rn. 7 sowie zu Compliance-Fragen bei der Export-Kontrolle → *von Bodungen*, Kap. 25.

85 Vgl. *Wiedmann/Greubel*, CCZ 2019, 88, 93. Zur sog. „Sanctions Compliance“ ausführlich → *Salathé/Moussaoui*, Kap. 24.

86 Zum Zusammenhang zwischen Compliance und CSR siehe → *Stehr/Knopp*, Kap. 15. Zum Konzept der „Good Governance“ siehe *Jakob*, in: *Jakob/Orth/Stopper*, Praxishandbuch Vereins- und Verbandsrecht, 2021, § 2 Rn. 827.

ethisch einwandfreies Geschäftsverhalten konfrontiert.⁸⁷ Vielmehr zeigen das LkSG und die CSDDD als prominente Beispiele von ESG-Gesetzen, dass Unternehmen und ihre Leitungsorgane zunehmend die Erfüllung neuer und sanktionsbewehrter Sorgfaltspflichten erfüllen bzw. organisieren müssen.⁸⁸ Hieraus folgt die Notwendigkeit, bestehende Compliance-Systeme anzupassen und um den Bereich der ESG-Compliance zu erweitern.⁸⁹

Die Diskussion um verantwortungsvolle Unternehmensführung, Corporate Social Responsibility und „Good Corporate Citizenship“ mit einem Fokus auf Umwelt und Sozialbelange zeigt sich auch in der neuen Fassung des **Deutschen Corporate Governance Kodex (DCGK)** von 2022.⁹⁰ So wurde in der Präambel die Bedeutung von Sozial- und Umweltfaktoren für den Unternehmenserfolg um den Zusatz erweitert, dass die Tätigkeiten des Unternehmens Auswirkungen auf Mensch und Umwelt haben.⁹¹ Damit geht es nicht mehr allein um die Auswirkungen von Sozial- und Umweltbelangen auf den Unternehmenserfolg („Outside-in-Perspektive“), vielmehr sind nunmehr auch die Auswirkungen der Unternehmenstätigkeit auf Menschen und Umwelt zu berücksichtigen („**Inside-out-Perspektive**“).⁹² Vorstand und Aufsichtsrat müssen **Sozial- und Umweltfaktoren** bei der Führung des Unternehmens bzw. Überwachung der Unternehmenstätigkeit im Rahmen des Unternehmensinteresses berücksichtigen.⁹³ **21**

Nach **A. (Leitung und Überwachung) I.** (Geschäftsführungsaufgaben des Vorstands), **Grundsatz 5 des DCGK** hat der Vorstand für die Einhaltung der gesetzlichen Bestimmungen und der internen Richtlinien zu sorgen und wirkt auf deren Beachtung im Unternehmen hin (**Compliance**). Das interne Kontrollsystem und das Risikomanagementsystem umfassen auch ein an der Risikolage des Unternehmens ausgerichtetes **Compliance Management System**. Nach der Empfehlung und Anregung A. 4 soll Beschäftigten und auch Dritten ferner auf geeig- **22**

⁸⁷ Vgl. *Spießhofer*, Unternehmerische Verantwortung, S. 25 ff., 34 f.; *Vetter*, ZGR 2018, 338, 360 ff.; *Siedenbiedel*, Corporate Compliance, S. 48 f.

⁸⁸ Zur Erweiterung der Compliance-Pflicht durch das LkSG siehe *Schröder/Schulz*, Praxisleitfaden Supply Chain Compliance, Rn. 7 ff.

⁸⁹ Zur „Verrechtlichung“ von (vormals freiwilligen) Anforderungen der Corporate Social Responsibility (CSR) siehe *Spießhofer*, Unternehmerische Verantwortung, S. 574 ff. Zur Bedeutung des sog. Reputationsmanagements näher unten → Rn. 21 f. Zum Zusammenhang von Compliance und CSR siehe auch → *Stehr/Knopp*, Kap. 15.

⁹⁰ Vgl. Deutscher Corporate Governance Kodex, Fassung vom 28.4.2022 https://www.dcgk.de/files/dcgk/usercontent/de/download/kodex/220627_Deutscher_Corporate_Governance_Kodex_2022.pdf (zuletzt abgerufen am 24.9.2024) und hierzu *von der Linden*, DStR 2022, 1765. Zur Bedeutung des „Good Corporate Citizenship“ siehe auch → *Böttger*, Kap. 2 Rn. 25.

⁹¹ Vgl. *Kremer u. a.*, Deutscher Corporate Governance Kodex, DCGK Präambel, Rn. 10, 30 ff.

⁹² Vgl. *Schmeing*, in: Ghassemi-Tabar, Deutscher Corporate Governance Kodex, Präambel, Rn. 7 ff.

⁹³ Vgl. DCGK, A. I, Empfehlung A.1 sowie *Schmeing*, in: Ghassemi-Tabar, Deutscher Corporate Governance Kodex, Präambel, Rn. 9.

nete Weise die Möglichkeit eingeräumt werden, geschützt **Hinweise auf Rechtsverstöße** im Unternehmen zu geben.⁹⁴

7. Compliance und Reputationsmanagement

- 23 Wie die aktuelle Diskussion zum Zusammenhang zwischen Compliance, Governance und ESG zeigt, wird der unternehmerische Verantwortungsbereich durch zahlreiche Normen und Vorgaben für verantwortliches gesellschaftliches Handeln immer mehr erweitert.⁹⁵ Zu bereits existierenden und oben exemplarisch skizzierten umfangreichen Rechtspflichten tritt ein genereller Trend der „**Verrechtlichung**“ unterschiedlicher Anforderungen des „**Soft Law**“ hinzu, wie dies insbesondere die neuen Sorgfaltspflichten in der Lieferkette,⁹⁶ die Pflicht zur CSR-Berichterstattung,⁹⁷ besondere Compliance-Maßnahmen nach der EU-Konfliktmineralien-Verordnung⁹⁸ und weitere neue Compliance-Pflichten zeigen.⁹⁹ So hat sich inzwischen ein neuer Bereich der „CSR-Compliance“ bzw. „ESG-Compliance“ entwickelt.¹⁰⁰
- 24 Die Erfüllung neuer Sorgfaltspflichten und Anforderungen der ESG-Compliance dienen auch der Sicherung der Unternehmensreputation, die als bedeutender immaterieller Vermögensgegenstand gilt.¹⁰¹ Die sog. **Image- und Reputationschäden** sind häufig schwer zu beziffern, sie können aber zu erheblichen Verlusten und Nachteilen und bei börsennotierten Unternehmen bis hin zu einem Einbruch des Börsenwerts führen.¹⁰² Der Schutz der Reputation durch ein wirksames Compliance Management spielt daher eine zentrale Rolle, das positive Image des Unternehmens in der Öffentlichkeit und bei den maßgeblichen Bezugsgruppen (Mitarbeiter, Kunden, Lieferanten, Investoren etc.) kann durch „Non-Compliance“ nachhaltig beeinträchtigt oder ganz zerstört werden.¹⁰³ Reputationsrisiken und „**Reputationsmanagement**“ haben sich daher zu wichtigen Themen für das Compliance- und Risikomanagement entwickelt.¹⁰⁴

94 DCGK, A. I, Empfehlung und Anregung A. 4.

95 Vgl. *Spießhofer*, in: Moosmayer/Lösler, Corporate Compliance, § 16 Rn. 17 ff.

96 Zum LkSG siehe ausführlich → *Heske*, Kap. 18.

97 Zu „CSR-Reporting“ siehe ausführlich → *Beisheim*, Kap. 16.

98 Siehe <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32017R0821> (zuletzt abgerufen am 24.9.2024) sowie hierzu *Teicke*, CCZ 2018, 274.

99 Umfassend *Spießhofer*, in: Moosmayer/Lösler, Corporate Compliance, § 16 sowie *Spießhofer*, Unternehmerische Verantwortung, S. 311 ff., 415 ff.

100 So ausdrücklich → *Beisheim*, Kap. 16.

101 Vgl. *Kröger*, Korruptionsschäden, Unternehmensgeldbußen und Imageschäden, S. 261 f.; *Simons*, ZGR 2018, 316; *Spindler*, in: Goette/Habersack/Kalss, AktG, 5. Aufl. 2019, Rn. 114.

102 Vgl. *Kröger*, Korruptionsschäden, Unternehmensgeldbußen und Imageschäden, S. 256 f.

103 Vgl. *Hauschka*, Compliance im Gesellschaftsrecht, in: Hadding/Hopt/Schimansky, Verbraucherschutz im Kreditgeschäft – Compliance in der Kreditwirtschaft, S. 103, 106.

104 Siehe *Seibt*, DB 2015, 171 ff.; sowie *Seibt*, in: Schmidt/Lutter (Hrsg.), AktG, § 76 Rn. 42; *Inderst*, Compliance Organisation und praktische Umsetzung, in: Inderst/Bannenberg/Poppe, Compliance, S. 127, 140 f.; *Seibt*, DB 2015, 171 ff.

Da die Missachtung ethischer Verhaltenserwartungen der Stakeholder ebenso zu Imageschäden und Reputationseinbußen führen kann wie die Missachtung rechtlicher Vorgaben,¹⁰⁵ sollte die Unternehmensleitung zum **Schutz vor Reputationsverlusten** im Einzelfall erwägen, bei legalen, aber ethisch fragwürdigen Geschäften auf eine Gewinnoptimierung zu verzichten. **25**

II. Vorgaben und Orientierungshilfen für das Compliance Management

Für die Compliance-Pflicht im Sinne einer **Pflicht zur Organisation und Kontrolle der Einhaltung rechtlicher Vorgaben** gibt es eine Reihe relevanter Normen, die als Grundlage oder als Erkenntnisquelle für eine allgemeinen Compliance-Pflicht herangezogen werden können.¹⁰⁶ Grundsätzlich enthält das deutsche Recht kaum besondere Vorgaben für das Compliance Management – eine Ausnahme bilden etwa die oben erwähnten neuen Gesetze im Bereich der **Supply-Chain-Compliance** (wie das LkSG), die teilweise in das Ausgestaltungsermessen der Geschäftsleiter hinsichtlich der Compliance-Maßnahmen eingreifen.¹⁰⁷ Ferner enthalten diverse Rechtsnormen allgemeine Vorgaben und Grundsätze, die bei der Erfüllung der Compliance-Pflicht durch organisatorische Maßnahmen zu berücksichtigen sind oder jedenfalls als Orientierung für die Ausgestaltung des Compliance Managements dienen können.¹⁰⁸ Diese Vorgaben sind durch die Gerichte fallbezogen präzisiert sowie durch Rechtswissenschaft und Rechtspraxis kommentiert worden und bilden damit ein **Muster organisatorischer (Mindest-)Anforderungen** für eine regelkonforme Unternehmensführung.¹⁰⁹ Für bestimmte Branchen bestehen darüber hinaus (teils selbst geschaffene) Regelwerke und Verhaltenskodizes, in denen ebenfalls zentrale Compliance-Fragen behandelt und hierzu Handlungsempfehlungen entwickelt werden.¹¹⁰ Ferner ist das Thema Compliance seit längerem Regelungsgegenstand verschiedener Standardisierungsorganisationen, zu nennen sind

¹⁰⁵ Schmidt, Compliance in Kapitalgesellschaften, S. 22 f.

¹⁰⁶ Vgl. den Überblick bei *Kremer*, in: *Kremer u. a.*, Deutscher Corporate Governance Kodex, DCGK, Grundsatz 5, Rn. 16 ff.; *Müller/Dittrich*, in: *Dittrich/Dochow/Ippach*, Rechtshandbuch Cybersicherheit im Gesundheitswesen, 18. Kap.

¹⁰⁷ Siehe *Seibt/Vesper-Gräse*, CB 2021, 357, 362 ff.; *Schröder/Schulz*, Praxisleitfaden Supply Chain Compliance, Rn. 140 ff. Zum LkSG siehe *Heske* → Kap. 18 sowie *Hagel/Wiedmann* → Kap. 19.

¹⁰⁸ Vgl. *Klahold/Lochen*, in: *Moosmayer/Lösler*, Corporate Compliance, § 13 Rn. 4 ff.; *Theuvsinger/Jung*, in: *Römermann*, Münchener Anwaltshandbuch GmbH-Recht, § 24 Rn. 7 ff.

¹⁰⁹ Zu den Mindestanforderungen an eine Compliance-Organisation ausführlich *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 121 ff. m. w. N.

¹¹⁰ Exemplarisch sind zu nennen der Verhaltenskodex des Gesamtverbandes der Deutschen Versicherungswirtschaft für den Vertrieb von Versicherungsprodukten, <https://www.gdv.de/gdv/service/verhaltenskodex-fuer-den-vertrieb> (zuletzt abgerufen am 16.10.2024) sowie der vom Verein „Freiwillige Selbstkontrolle für die Arzneimittelindustrie“ (FSA) veröffentlichte „FSA-Transparenzkodex“ zur Transparenz bei der Zusammenarbeit mit den Angehörigen

insbesondere der in der Praxis verbreitete Prüfungsstandard des Instituts der Wirtschaftsprüfer (**IDW PS 980**)¹¹¹ die **ISO 37301** (Compliance-Management-Systeme)¹¹² sowie die **ISO 37001** (Anti-Korruptions-Management-Systeme).¹¹³ Diese Regelwerke und Standards sind nicht rechtsverbindlich,¹¹⁴ auch sie können aber nützliche Empfehlungen und Leitlinien für die Gestaltung des Compliance Managements enthalten.¹¹⁵

1. Grundlagen der Compliance-Pflicht – Regelungsbeispiele

- 27** Besondere (**aufsichts-)**rechtliche Pflichten für die Einrichtung einer Compliance-Organisation bestehen für Kredit- und Finanzdienstleistungsunternehmen, für Wertpapierhandelsunternehmen, Wertpapierinstitute sowie für Versicherungsunternehmen.¹¹⁶ So muss gemäß **§ 25a KWG** ein Institut über eine **ordnungsgemäße Geschäftsorganisation** verfügen, welche die Einhaltung der vom Institut zu beachtenden gesetzlichen Bestimmungen und der betriebswirtschaftlichen Notwendigkeiten gewährleistet. Eine ordnungsgemäße Geschäftsorganisation im Sinne dieser Vorschrift muss ein angemessenes und wirksames Risikomanagement umfassen, auf dessen Basis ein Institut die Risikotragfähigkeit laufend sicherzustellen hat. Das Risikomanagement umfasst insbesondere die Festlegung einer auf die nachhaltige Entwicklung gerichteten Geschäftsstrategie und einer damit konsistenten Risikostrategie (§ 25a Abs. 1 Nr. 1 KWG), Verfahren zur Ermittlung und Sicherstellung der Risikotragfähigkeit (§ 25a Abs. 1 Nr. 2 KWG) sowie die Einrichtung interner Kontrollverfahren mit einem internen Kontrollsystem (1. und 2. Verteidigungslinie) und einer Internen Revision (3. Verteidigungslinie, vgl. § 25a Abs. 1 Nr. 3 KWG).¹¹⁷
- 28** Für **Wertpapierhandelsunternehmen** und Wertpapierinstitute werden diese Organisationspflichten insbesondere durch die Verpflichtung erweitert, eine

rigen der Fachkreise und medizinischen Einrichtungen, siehe <http://www.fsa-pharma.de/kodizes/transparenzkodex/inhaltsubersicht> (zuletzt abgerufen am 16.10.2024).

111 Zu Entwicklung und aktuellem Stand des IDW-Prüfungsstandard „Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen“ (IDW PS 980) siehe → *Uhlig/Federmann*, Kap. 7.

112 Zum Vergleich von IDW PS 980 und ISO 37301 ausführlich → *Uhlig/Federmann*, Kap. 7.

113 Zur ISO 37001 siehe *Kayser*, CB 2015, 441.

114 Vgl. *Schulz*, in: Bay/Hastentrath, Compliance-Management-Systeme, 2. Aufl. 2016, sowie *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 47 f.

115 Ausführliche Darstellung und Nachweise bei *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 121 ff.

116 Vgl. *Balke*, in: Born/Ghassemi-Tabar/Gehle (Hrsg.) MHBGesR VII, § 104 Rn. 9; siehe auch → *Renz/Frankenberger*, Kap. 20.

117 Zum Modell der drei (Verteidigungs-)Linien („Three Lines-Modell“) siehe → *Renz/Frankenberger*, Kap. 20 Rn. 76 ff. siehe zum Zusammenspiel von Compliance, Risikomanagement und Interner Revision auch → *Bartuschka*, Kap. 11 Rn. 76 ff.

dauerhafte, unabhängige und wirksame **Compliance-Funktion** einzurichten.¹¹⁸ Diese stellt einen wesentlichen Bestandteil des **internen Kontrollsystems** des Wertpapierdienstleistungsunternehmens im Sinne des § 25a Abs. 1 Satz 3 Nr. 1 KWG dar.¹¹⁹ Die Geschäftsleitung muss einen (Kapitalmarkt-)Compliance-Beauftragten bestellen, der wie die sonstigen Mitarbeiter der Compliance-Abteilung seine Aufgaben unabhängig wahrnehmen muss und nur der Unternehmensleitung unterstellt ist.¹²⁰ Neben Auslegungshinweisen seitens der Bundesanstalt für Finanzdienstleistungsaufsicht (**BaFin**) zur Konkretisierung der organisatorischen Anforderungen haben kapitalmarktorientierte Unternehmen weitere Vorschriften bzw. aufsichtsbehördliche Empfehlungen zu beachten.¹²¹

Versicherungsunternehmen haben die Vorgaben des § 29 VAG zu beachten. 29 Gemäß § 29 Abs. 1 VAG müssen Versicherungsunternehmen über ein wirksames **internes Kontrollsystem** verfügen, das mindestens Verwaltungs- und Rechnungslegungsverfahren, einen internen Kontrollrahmen, eine angemessene unternehmensinterne Berichterstattung auf allen Unternehmensebenen sowie eine Funktion zur Überwachung der Einhaltung der Anforderungen (**Compliance-Funktion**) umfasst. Zu den Aufgaben der Compliance-Funktion gehört gemäß § 29 Abs. 2 VAG die Beratung des Vorstands in Bezug auf die Einhaltung der Gesetze und Verwaltungsvorschriften, die für den Betrieb des Versicherungsgeschäfts gelten. Außerdem hat die Compliance-Funktion die möglichen Auswirkungen von Änderungen des Rechtsumfeldes für das Unternehmen zu beurteilen und das mit der Verletzung der rechtlichen Vorgaben verbundene Risiko (Compliance-Risiko) zu identifizieren und zu beurteilen.

Besondere Vorgaben für die Compliance-Pflicht können aus diversen weiteren speziellen Normierungen folgen, wie etwa aus dem Geldwäschegesetz (**GwG**),¹²² der **DSGVO**,¹²³ dem Gesetz zum Schutz von Geschäftsgeheimnissen (**GeschGehG**)¹²⁴ oder aus besonderen Regulierungen der IT-Sicherheit.¹²⁵ Hinzu kommen die oben erwähnten besonderen Anforderungen des Lieferkettensorg-

118 Siehe Art. 22 Delegierte Verordnung (EU) 217/565 i.V.m. BT 1 der MaComp, siehe → *Renz/Frankenberger*, Kap. 20 Rn. ff.

119 Zu Funktion und Bedeutung von Compliance als Teil des IKS siehe → *Renz/Frankenberger*, Kap. 20 Rn. 70 ff.

120 Daneben sind sogenannte MaRisk-Compliance Funktionen einzurichten (gem. MaRisk AT 4.4.2), die darauf hinwirken sollen, alle für das Institut wesentlichen (aufsichts-)rechtlichen Anforderungen umgesetzt zu wissen. Siehe auch → *Renz/Frankenberger*, Kap. 20 Rn. 7 ff.

121 Siehe → *Renz/Frankenberger*, Kap. 20.

122 Siehe § 9 GwG. Zum Compliance-Management von Geldwäscherisiken siehe → *Kaetzler*, Kap. 22 sowie → *Komma*, Kap. 23.

123 Siehe → *Becker/Böhlke/Fladung*, Kap. 12.

124 Vgl. *Müller/Dittrich*, in: *Dittrich/Dochow/Ippach*, Rechtshandbuch Cybersicherheit im Gesundheitswesen, 18. Kap. Rn. 23 ff.

125 Zur Regulierung von Cyber Risiken und IT-Sicherheit → *Bensinger*, Kap. 14 sowie *Müller/Dittrich*, in: *Dittrich/Dochow/Ippach*, Rechtshandbuch Cybersicherheit im Gesundheitswesen, 18. Kap. Rn. 28 ff.

faltspflichtengesetzes (**LkSG**) in Bezug auf Menschenrechte und bestimmte Umweltbelange.¹²⁶

- 31 Bei den genannten Normen handelt es sich allerdings jeweils um **spezielle Regelungen** im Hinblick auf die besonderen Risiken bestimmter Branchen oder Themenkomplexe, an die der Gesetzgeber besondere rechtliche Anforderungen stellt. Daher besteht weitgehend Konsens, dass diese besonderen Anforderungen und Maßstäbe nicht einfach auf das Compliance Management in Unternehmen außerhalb dieser Branchen und Themenkomplexe übertragen werden können.¹²⁷ Ebenso wenig ergibt sich die Verpflichtung zu einer Compliance-Organisation im Wege einer Gesamtanalogie zu diesen (und ausgewählten weiteren) Vorschriften.¹²⁸
- 32 Dem steht es allerdings nicht entgegen, die genannten (Sonder-)Regelungen (und dazu vorhandene Rechtsprechung und Literatur) als **Erkenntnisquelle und Orientierungshilfe** für die Fragen der Ausgestaltung des Compliance Managements zu nutzen. Zwar können beispielsweise die besonderen Compliance-Pflichten nach KWG, WpHG und VAG nicht auf andere Wirtschaftssektoren übertragen werden, doch lassen sich aus diesen Regelungen zahlreiche **Orientierungspunkte** für allgemeine Fragen des Compliance Managements gewinnen, etwa im Zusammenhang mit der Gesamtverantwortung der Unternehmensleitung, der eindeutigen Zuordnung von Verantwortungsbereichen oder der Einrichtung einer dauerhaften und unabhängig agierenden Compliance-Funktion.¹²⁹
- 33 Diverse Regelungen, die als Grundlage der Compliance-Pflicht erörtert werden, finden sich ferner im Gesellschaftsrecht und insbesondere im Aktiengesetz. So soll nach einer Ansicht die Vorschrift des **§ 91 Abs. 2 AktG (Früherkennung bestandsgefährdender Risiken)** als Grundlage der Compliance-Pflicht des Vorstands dienen.¹³⁰ Nach dieser Norm hat der Vorstand als Gesamtorgan für eine Organisation zu sorgen, welche die Erkennung von bestandsgefährdenden Entwicklungen sicherstellt.¹³¹ Bestandsgefährdende Risiken können dabei auch aus „Non-Compliance“ resultieren, etwa bei sehr hohen Geldstrafen bzw. Bußgeldern (z. B. im Zusammenhang mit Kartellrechtsverstößen) oder beim Aus-

126 Siehe oben → Rn. 4 f. sowie → *Heske*, Kap. 18 sowie *Hagel/Wiedmann* → Kap. 19.

127 Vgl. *Seeliger/Mross*, in: *Jaeger/Kokott/Pohlmann/Schroeder/Seeliger*, Frankfurter Kommentar zum Kartellrecht, 109. EL 9/2024, E. Kartellrechts-Compliance, Rn. 13 f., jeweils m. w. N.

128 Vgl. etwa *Harbarth*, ZHR 179 (2015), 137, 139; *Seeliger/Mross*, in: *Jaeger/Kokott/Pohlmann/Schroeder/Seeliger*, Frankfurter Kommentar zum Kartellrecht, 109. EL 9/2024, E. Kartellrechts-Compliance, Rn. 13 m. w. N.

129 Vgl. *Fleischer*, in: BeckOGK AktG, Stand: 1.2.2024, § 91 Rn. 80.

130 Vgl. *Tödtmann/Winstel*, in: *Kubis/Tödtmann*, Arbeitshandbuch für Vorstandsmitglieder, § 13 Rn. 7 ff. sowie die Nachweise bei *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 37.

131 Vgl. *Liese*, BB-Special Compliance 2008, 17, 18 m. w. N.

schluss von Projekten öffentlicher Auftraggeber.¹³² Andererseits ist zu berücksichtigen, dass die Risiken und Nachteile von „Non-Compliance“ in einigen Fällen, nicht aber in allen Fällen bestandsgefährdend sind. Damit wäre durch § 91 Abs. 2 AktG nur ein Ausschnitt der vielfältigen Compliance-Risiken erfasst. Zum anderen reicht die Compliance-Pflicht über die Risikoprävention hinaus und umfasst zahlreiche weitere Maßnahmen (etwa im Zusammenhang mit der Aufklärung und Sanktionierung von Regelverstößen).¹³³ Zudem ist die Übertragung der Pflicht aus § 91 Abs. 2 AktG auf andere Verbandsformen problematisch, bei denen vergleichbare Regelungen fehlen.¹³⁴

Für **börsennotierte Aktiengesellschaften** hat der Gesetzgeber mit dem am 1.7.2021 in Kraft getretenen Gesetz zur Stärkung der Finanzmarktintegrität (**FISG**) in **§ 91 AktG** einen neuen **Abs. 3** eingeführt, wonach der Vorstand einer börsennotierten Aktiengesellschaft (über die Pflichten des Abs. 2 hinausgehend) ein im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames **internes Kontrollsystem** und Risikomanagementsystem einzurichten hat.¹³⁵ Da Bestandteil des internen Kontrollsystems (**IKS**) auch die „Sicherung der Einhaltung der maßgeblichen rechtlichen Vorschriften“ ist, folgt hieraus die Compliance-Pflicht des Vorstands einer börsennotierten AG.¹³⁶

Auch in den Regelungen des Ordnungswidrigkeitenrechts zur **Haftung von Aufsichtspflichtigen** (§§ 130, 9 OWiG) und zur Haftung des Unternehmens bei Verletzung von Aufsichtspflichten (§§ 30, 130, 9 OWiG) wird eine zentrale Rechtsgrundlage für Compliance gesehen.¹³⁷ Die Vorschrift des § 130 OWiG gilt rechtsformübergreifend für alle Verbände.¹³⁸ Nach § 130 OWiG handelt ordnungswidrig, wer als Inhaber eines Betriebs oder Unternehmens vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem

132 Vgl. *Kark*, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 55 ff. Zu Bußgeldern und sonstigen Risiken wegen Kartellrechtsverstößen ausführlich → *Seeliger/Mross/Seydel*, Kap. 27.

133 Ähnlich *Tödtmann/Winstel*, in: Kubis/Tödtmann, Arbeitshandbuch für Vorstandsmitglieder, § 13 Rn. 8.

134 *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 37, 51 ff.

135 Vgl. *Koch*, AktG, § 76 Rn. 19; *Tödtmann/Winstel*, in: Kubis/Tödtmann, Arbeitshandbuch für Vorstandsmitglieder, § 13 Rn. 8 sowie *Fischer/Schuck*, NZG 2021, 534.

136 Vgl. *Koch*, AktG, § 91 Rn. 28 ff., § 76 Rn. 19; *Tödtmann/Winstel*, in: Kubis/Tödtmann, Arbeitshandbuch für Vorstandsmitglieder, § 13 Rn. 8 sowie *Fischer/Schuck*, NZG 2021, 534.

137 Vgl. *Moosmayer*, NJW 2012, 3013; *ders.*, Compliance, 11 ff.; ähnlich *Rodewald*, CB 2013, 70, 72 („Mutter“ aller Compliance-Vorschriften). Ferner → *Böttger*, Kap. 2 Rn. 29.

138 Vgl. *Moosmayer*, NJW 2012, 3013; *Koch*, WM 2009, 1013, 1015; *Schmidt*, Compliance in Kapitalgesellschaften, S. 69, 71, sowie die Nachweise bei *Rönnau*, ZGR 2016, 277, 293. Siehe ferner *Rodewald*, Gesetzestreue als Organisationsproblem – Compliance richtig managen, in: *Maschmann*, Corporate Compliance und Arbeitsrecht, S. 31, 37: „Urmutter“ des Corporate Compliance-Gedankens.

Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist. Der Normadressat hat seine **Aufsichtspflichten** dabei so zu erfüllen, dass grundsätzlich sämtliche betriebsbezogene Pflichten eingehalten werden.¹³⁹ Die Gerichte haben in langjähriger Entscheidungspraxis die relevanten Pflichten nach § 130 OWiG konkretisiert.¹⁴⁰ Daraus folgt zwar bislang keine ausdrückliche Verpflichtung zu einer bestimmten Compliance-Organisation, wohl aber ergeben sich konkrete Anforderungen an die Erfüllung der geforderten Aufsichtspflichten, etwa hinsichtlich der sorgfältigen **Auswahl** und Bestellung von Aufsichtspersonen, ihrer **Instruktion** und **Überwachung** sowie hinsichtlich der Untersuchung, Aufklärung und Sanktionierung von Verstößen.¹⁴¹ Die hier entwickelten Grundsätze spielen eine maßgebliche Rolle, bei der **Delegationsfrage**, welche Compliance-Maßnahmen die Geschäftsleiter auf nachgeordnete Personen (wie einen Compliance Officer) übertragen dürfen und welche Erfordernisse in Bezug auf Auswahl, Einweisung und Kontrolle der beauftragten Person dabei rechtlich zu beachten sind.¹⁴² Auch aus den genannten Regelungen des Ordnungswidrigkeitenrechts und dazu erfolgten Konkretisierungen durch die Gerichte lassen sich daher allgemeine Anforderungen für das Compliance Management ableiten.¹⁴³

2. Compliance-Pflicht als rechtsformübergreifende Ausprägung der Leitungsverantwortung

- 36** Die Compliance-Pflicht im Sinne einer **Pflicht zur Organisation, Kontrolle und Durchsetzung der Einhaltung rechtlicher Vorgaben** und der Verhinderung regelwidrigen Verhaltens im Unternehmen gilt mittlerweile weitgehend als geklärt.¹⁴⁴ Unabhängig von besonderen Vorschriften folgt die Compliance-Pflicht der Geschäftsleiter nach verbreiteter Ansicht aus der organschaftlichen

¹³⁹ Liese/Schulz, BB 2011, 1347, 1350.

¹⁴⁰ Siehe die Beispiele und Rechtsprechungsnachweise bei Theusinger/Jung, Corporate Compliance, in: Römermann, Münchener Anwaltshandbuch GmbH-Recht, § 24 Rn. 15 ff.; Liese/Schulz, BB 2011, 1347, 1350.

¹⁴¹ Siehe die Beispiele bei Theusinger/Jung, Corporate Compliance, in: Römermann, Münchener Anwaltshandbuch GmbH-Recht, § 24 Rn. 29 ff.

¹⁴² Siehe zu Delegationsfragen im Compliance-Management unter → Rn. 56 f.

¹⁴³ Theusinger/Jung, Corporate Compliance, in: Römermann, Münchener Anwaltshandbuch GmbH-Recht, § 24 Rn. 15 ff.; siehe ferner → Böttger, Kap. 2 Rn. 29 f. Im Unterschied zu den zuvor genannten Normen des Gesellschaftsrechts, bei Compliance-Verstößen eine Innenhaftung der Geschäftsleiter ggü. dem Unternehmen auslösen können (vgl. etwa § 93 Abs. 2 AktG, § 43 Abs. GmbHG) begründet eine Verletzung von §§ 130, 9 OWiG eine sog. Außenhaftung, vgl. Kremer, in: Kremer u. a., Deutscher Corporate Governance Kodex, DCGK, Grundsatz 5, Rn. 17.

¹⁴⁴ Vgl. Koch, AktG, § 76 Rn. 19; Fleischer, in: BeckOGK AktG, Stand: 1.2.2024, § 91 Rn. 62 ff. (in Bezug auf den Vorstand der AG).

Leitungsverantwortung.¹⁴⁵ Daraus folgt die Pflicht, sich nicht nur selbst rechtmäßig zu verhalten, sondern vielmehr auch das rechtmäßige Verhalten aller Unternehmensangehörigen zu organisieren, zu kontrollieren und sicherzustellen (**Legalitätspflicht bzw. Legalitätskontrollpflicht sowie Legalitätsdurchsetzungspflicht**).¹⁴⁶ Compliance ist somit eine rechtsform-, struktur- und größenunabhängige Pflichtaufgabe eines jeden Geschäftsleiters,¹⁴⁷ denn jedes Unternehmen ist so zu organisieren, dass Rechts- und Regelverstöße möglichst verhindert werden.¹⁴⁸

Wie eingangs ausgeführt (siehe unter → Rn. 1), müssen die Geschäftsleiter organisatorische Maßnahmen treffen, um rechtskonformes Verhalten der Unternehmensangehörigen sicherzustellen und Regelverletzungen möglichst zu vermeiden.¹⁴⁹ Dieser umfassende **Organisationsauftrag**¹⁵⁰ der Geschäftsleitung umfasst sowohl die Entscheidung über die Einführung von Compliance-Maßnahmen als auch über die wesentlichen Strategie- und Strukturentscheidungen bezüglich des Compliance Managements.¹⁵¹ Bei Haftungsfragen in Fällen von „Non-Compliance“ steht daher häufig die Verletzung rechtlicher Organisationsanforderungen an die Geschäftsleitung im Mittelpunkt.¹⁵² **37**

3. Rechtsprechung zur Compliance-Pflicht

Anhaltspunkte für eine nähere **Konturierung der Compliance-Pflicht** liefert auch die Rechtsprechung. Denn die Gerichte schaffen bzw. erweitern kontinuierlich ein umfangreiches rechtliches Pflichtenspektrum für Unternehmen und deren Leitungsorgane.¹⁵³ Die Haftung von Geschäftsleitern für Fehlverhalten (sog. **38**

145 Siehe die ausführliche dogmatische Herleitung bei *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 36 ff., 68 m. w. N. sowie *Merkt*, ZIP 2014, 1705, 1707.

146 Vgl. auch *Merkt*, ZIP 2014, 1705, 1706; *Grigoleit*, AktG, § 76 Rn. 44.

147 So wörtlich und zutreffend *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 68.

148 *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 68 f.; ähnlich *Balke*, in: Born/Ghassemi-Tabar/Gehle (Hrsg.) MHBGRes VII, § 104 Rn. 6.

149 Vgl. *Moosmayer*, Compliance, Rn. 11, 63; *Kort*, GmbHR 2013, 566 ff.

150 *Haouache*, Unternehmensbeauftragte und Gesellschaftsrecht der AG und GmbH, S. 53.

151 Vgl. *Karbaum*, AG 2013, 863, 870. Zum Kernbereich der Compliance-Pflicht ausführlich *Gomer*, Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft, 2020, 123 ff., 160 ff.

152 Vgl. bereits *Meyer*, DB 2014, 1063. Nach der Leitentscheidung des Landgerichts München vom 10.12.2013 muss das Vorstandsmitglied einer AG im Rahmen seiner Legalitätspflicht dafür sorgen, dass ein Unternehmen so organisiert wird, dass keine Gesetzesverletzungen erfolgen, vgl. LG München I, 10.12.2013 – 5 HK O 1387/10, CB 2014, 167 ff. m. CB-Komm. *Kränzlin/Weller* sowie ausführlich *Fleischer*, NZG 2014, 321 ff.

153 Zu den damit verbundenen Haftungsrisiken siehe etwa *Moosmayer/Lösler*, in: *Moosmayer/Lösler*, Corporate Compliance, § 1 Rn. 13 ff.

Organhaftung) wurde kontinuierlich ausgeweitet,¹⁵⁴ die Gerichte haben teilweise weitreichende Anforderungen auf der Basis sogenannter **Unternehmensorganisationspflichten**, Verkehrssicherungspflichten und Garantenpflichten entwickelt.¹⁵⁵ Die Reichweite dieser Pflichten und ihre Anwendung im jeweiligen Einzelfall sind für Unternehmer und Geschäftsleiter einerseits nicht immer eindeutig vorhersehbar, andererseits stellt die Verletzung dieser Pflichten ein dauerhaftes Risiko unternehmerischer Tätigkeit dar.¹⁵⁶

- 39 Bei Haftungsfragen in Fällen von „Non-Compliance“ steht häufig die Verletzung rechtlicher Organisationsanforderungen durch die **Geschäftsleitung** im Mittelpunkt, deren Kriterien die Rechtsprechung in mehreren Entscheidungen konkretisiert hat: Nach der Leitentscheidung des **Landgerichts München vom 10.12.2013** muss das Vorstandsmitglied einer AG im Rahmen seiner Legalitätspflicht dafür sorgen, dass ein Unternehmen so organisiert wird, dass keine Gesetzesverletzungen erfolgen.¹⁵⁷ Seine **Organisationspflicht zur Verhinderung von Rechtsverletzungen** erfüllt der **Vorstand einer AG** nach Ansicht des Gerichts, „wenn er eine auf Schadensprävention und Risikokontrolle angelegte Compliance-Organisation einrichtet“, die der jeweiligen Gefährdungslage entspricht.¹⁵⁸ Die Ausführungen des Gerichts zur Compliance-Verantwortung des Vorstands als Kollegialorgan und zur Compliance-Verantwortung der einzelnen Vorstandsmitglieder lassen sich in den Kontext der Organisationspflichten im Unternehmen einordnen.¹⁵⁹ Dabei orientierte sich das Gericht an den Leitlinien zur Compliance-Verantwortung der Unternehmensleitung, welche Wissenschaft und Praxis formuliert haben.¹⁶⁰
- 40 Das **OLG Nürnberg** hat hinsichtlich der **Haftung des Geschäftsführers einer GmbH** nach § 43 Abs. 2 GmbHG am **30.3.2022** entschieden, dass die **Schaffung von Compliance-Strukturen** zur gehörigen **Überwachung von Mitarbeitern** zu den Pflichten eines Geschäftsführers im Rahmen der internen Unter-

154 Vgl. *Lutter/Krieger/Schneider*, Entwicklung der Organpflichten und der Organhaftung, in: *Krieger/Schneider*, Handbuch Managerhaftung, § 1.

155 Zur Entwicklung von Verkehrssicherungspflichten sowie Unternehmensorganisationspflichten umfassend Spindler, Unternehmensorganisationspflichten, 2001; *Matusche-Beckmann*, Das Organisationsverschulden, S. 37 ff. Vgl. ferner *Rack*, CB 2014, 104 sowie *ders.* (im Zusammenhang mit den Sorgfaltspflichten des LkSG) CB 2022, 1. Zum Konzept der strafrechtlichen Garantenpflichten siehe → *Böttger*, Kap. 2 Rn. 114 ff.

156 Vgl. *Schulz*, Rechtliches Risikomanagement und Compliance im Mittelstand, in: Kessler, Unternehmensfinanzierung Mittelstand, § 6 Rn. 4.

157 Vgl. LG München I, 10.12.2013 – 5 HK O 1387/10, CB 2014, 167 ff. m. CB-Komm. *Kränzlin/Weller* sowie ausführlicher Besprechung von *Fleischer*, NZG 2014, 321 ff.

158 Vgl. LG München I, Urt. v. 10.12.2013 – 5 HK O 1387/10, CB 2014, 167 ff. und hierzu *Fleischer*, NZG 2014, 321 ff.; *Meyer*, DB 2014, 1063 ff. Der Rechtsstreit endete durch Vergleich, das Urteil enthält jedoch grundlegende Aussagen zu allgemeinen Anforderungen an ein wirksames Compliance Management.

159 *Schulz/Held*, juris Praxis Report Compliance 1/2014; *Rack*, CB 2014, 104.

160 Vgl. *Fleischer*, in: Spindler/Stilz, AktG, 4. Aufl. 2019, § 91 Rn. 47 ff.; *Hauschka/Moosmayer/Lösler*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 1 Rn. 29 ff.

nehmensorganisation gehöre.¹⁶¹ Aus der Legalitätspflicht folge die Verpflichtung des Geschäftsführers zur Einrichtung eines Compliance-Management-Systems, also zu organisatorischen Vorkehrungen, die die Begehung von Rechtsverstößen durch die Gesellschaft oder deren Mitarbeiter verhindern. Dabei sei der Geschäftsführer nicht nur verpflichtet, den Geschäftsgang so zu überwachen oder überwachen zu lassen, dass er unter normalen Umständen mit einer ordnungsgemäßen Erledigung der Geschäfte rechnen könne; er müsse vielmehr weitergehend sofort eingreifen, wenn sich Anhaltspunkte für ein Fehlverhalten zeigten. Eine Pflichtverletzung liege schon dann vor, wenn durch unzureichende **Organisation, Anleitung bzw. Kontrolle** Mitarbeitern der Gesellschaft Straftaten oder sonstige Fehlhandlungen ermöglicht oder auch nur erleichtert würden.¹⁶² Die Entscheidung belegt einerseits die Erstreckung der Compliance-Pflicht auf andere Verbandsformen als der Aktiengesellschaft; andererseits verdeutlicht sie die durchaus strengen Anforderungen der Gerichte in Bezug auf die Organisation und Kontrolle von Compliance-Maßnahmen durch die Geschäftsleiter sowie damit einhergehende persönliche Haftungsrisiken.

Auch über spezielle Fälle von „Non-Compliance“ hinausgehend, ist die Rechtsprechung zu den sog. **Unternehmensorganisationspflichten** eine Fundgrube für Kriterien zur Konkretisierung der Compliance-Pflicht: Die Gerichte haben auf der Basis deliktsrechtlicher Verkehrssicherungs- und Organisationspflichten sowie strafrechtlicher Garantenpflichten¹⁶³ in vielen Einzelfällen umfangreiche Anforderungen entwickelt, für deren Verletzung die Unternehmen (sowie unter bestimmten Umständen auch die Geschäftsleiter persönlich) haften.¹⁶⁴ In einer umfangreichen Kasuistik wurden zahlreiche Organisationspflichten statuiert, u. a. Pflichten zu ordnungsgemäßer Betriebsorganisation, Informationsversorgung, Risikoermittlung und -steuerung, Delegation, Instruktion, Überwachung und Kontrolle, Dokumentation und Aktualisierung.¹⁶⁵ 41

4. Compliance-Anforderungen anderer Rechtsordnungen

Wie oben ausgeführt (siehe unter → Rn. 7) können sich für international tätige Unternehmen besondere Anforderungen und Vorgaben für die Erfüllung der Compliance-Pflicht auch aus anderen Rechtsordnungen ergeben. Dies gilt insbesondere für **Compliance-Anforderungen des anglo-amerikanischen** 42

161 Vgl. OLG Nürnberg, 30.3.2022 – 12 U 1520/19, CB 2022, 493 m. CB-Komm. *Johnson*, CB 2022, 502.

162 Vgl. OLG Nürnberg, 30.3.2022 – 12 U 1520/19, CB 2022, 493.

163 Zu den strafrechtlichen Garantenpflichten ausführlich → *Böttger*, Kap. 2 Rn. 122 ff.

164 Umfassend *Spindler*, Unternehmensorganisationspflichten, sowie *Matusche-Beckmann*, Das Organisationsverschulden; zu den diversen Pflichten vgl. ferner *Rack*, CB 2013, 14; *ders.*, CB 2014, 104; *ders.*, CB 2014, 279.

165 Die Rechtsprechung zum Organisationsverschulden und ihren Bezug erläutert ausführlich *Rack*, CB 2022, 1 (im Kontext des LkSG) mit Nachweis zur Rspr. sowie bereits *ders.*, CB 2014, 104.

Rechts,¹⁶⁶ da dessen extraterritoriale Geltung häufig bereits bei geringfügiger (Geschäfts-)Verbindung mit anderen Rechtsordnungen eintritt. Die erforderliche Berücksichtigung der Compliance-Erfordernisse der jeweils anwendbaren Rechtsordnung erhöht einerseits die Komplexität der Konzeption und Ausgestaltung des Compliance Managements. Andererseits können die Vorgaben anderer Rechtsordnungen jedoch auch als wertvolle Orientierungshilfen dienen.

a) UK Bribery Act (Vereinigtes Königreich)

- 43 Ein Beispiel bietet der **UK Bribery Act**,¹⁶⁷ dessen Strafandrohung für Korruptionsdelikte sich auf alle Unternehmen erstreckt, die im **Vereinigten Königreich** geschäftstätig sind.¹⁶⁸ Durch diesen weiten Anwendungsbereich werden auch zahlreiche deutsche Unternehmen mit relevanter Geschäftsbeziehung erfasst. Gleichzeitig zeigt das Beispiel, dass Unternehmen im Umgang mit dem britischen Korruptionsstrafgesetz bestimmte Leitlinien und Empfehlungen der Behörden für die Ausgestaltung der erforderlichen Compliance-Maßnahmen nutzen können: So können die Unternehmen im Anwendungsbereich des UK Bribery Acts einer Sanktion dann entgehen, wenn sie die **Umsetzung angemessener Maßnahmen (adequate procedures) zur Korruptionsverhinderung** nachweisen.¹⁶⁹ Als angemessene Maßnahmen gelten nach der „Guidance“ des „Ministry of Justice“ ein eindeutiges Bekenntnis der Unternehmensleitung zur Korruptionsbekämpfung, die unternehmensweite Einführung von Antikorruptionsmaßnahmen, effektive Risikomanagement-Prozesse sowie die fortlaufende Prüfung des Korruptionsrisikos.¹⁷⁰

b) Leitfaden des Department of Justice (USA)

- 44 Eine weitere nützliche Orientierungshilfe für die Ausgestaltung und weitere Optimierung des Compliance Managements bietet der **Leitfaden des US-amerikanischen Justizministeriums (US DOJ) zur Bewertung von Compliance-Programmen (Evaluation of Corporate Compliance Programs)**, der 2023 in aktualisierter Form veröffentlicht wurde.¹⁷¹ In den USA gibt es diverse Leitfäden

166 Siehe *Hauschka/Moosmayer/Lösler*, Corporate Compliance, 3. Aufl. 2016, § 1 Rn. 73 ff.; *Kark*, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 1172 ff.

167 Siehe http://www.legislation.gov.uk/ukpga/2010/23/pdfs/ukpga_20100023_en.pdf (zuletzt abgerufen am 30.9.2024). Zum UK Bribery Act siehe auch *Moosmayer*, Compliance, Rn. 31 ff.; *Kark*, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 1289 ff.

168 Vgl. *Teicke/Mohssen*, BB 2012, 911, 914; *Timmerbeil/Spachmüller*, DB 2013, 2133.

169 Siehe <https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf> (zuletzt abgerufen am 30.9.2024) sowie *Kark*, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 1289 ff.

170 Zu diesen Elementen eines adäquaten Compliance-Programms in der Ausführungsregelung durch das britische Justizministerium *Moosmayer*, Compliance, Rn. 31 ff.; *Teicke/Mohssen*, BB 2012, 911, 915 ff.; *Timmerbeil/Spachmüller*, DB 2013, 2133, 2135 ff.

171 U.S. Department of Justice Criminal Division, Evaluation of Corporate Compliance Programs (Updated March 2023), <https://www.justice.gov/criminal-fraud/page/file/937501/download> (zuletzt abgerufen am 30.9.2024).

und Empfehlungen zur Evaluierung von Compliance-Maßnahmen; Compliance-Maßnahmen werden von den Behörden bei Regelverstößen regelmäßig im Rahmen der Strafzumessung berücksichtigt.¹⁷² Voraussetzung für eine Sanktionsmilderung ist allerdings stets die **Wirksamkeit** („effectiveness“) der implementierten **Compliance-Strukturen und -Maßnahmen**.¹⁷³ Hinsichtlich der Konkretisierung dieses Wirksamkeitserfordernisses legt der Leitfaden des US-amerikanischen Justizministeriums unter anderem fest, nach welchen Maßstäben vorhandene Compliance-Maßnahmen berücksichtigt werden können.¹⁷⁴ Danach ist anhand von **drei zentralen Kernfragen** die Wirksamkeit¹⁷⁵ der Compliance-Maßnahmen (sowohl zum Zeitpunkt der Tat als auch zum Zeitpunkt der Sanktionierung) zu bewerten.¹⁷⁶ So ist erstens zu prüfen, ob das Compliance-System **gut konzipiert** ist:¹⁷⁷ Dabei wird untersucht, ob ein Compliance-Risikomanagement besteht, Compliance-Richtlinien und -Schulungen etabliert sind, Hinweisgebersysteme bestehen, eine Kontrolle von Geschäftspartnern erfolgt und ob Compliance-Aspekte bei M&A-Transaktionen berücksichtigt wurden.¹⁷⁸ Zweitens ist zu untersuchen, ob das Compliance-System auch **ernsthaft und in gutem Glauben umgesetzt** wurde (was heißt, dass es mit adäquaten Ressourcen ausgestattet wurde).¹⁷⁹ Hier liegt der Fokus auf dem Commitment des oberen und mittleren Managements, auf den Themen Ressourcenausstattung und Autonomie sowie auf Anreizstrukturen für ein regelkonformes Verhalten einerseits und Sanktionierung von Non-Compliance andererseits. Drittens ist zu überprüfen, ob das Compliance-System auch tatsächlich **in der Praxis funktioniert**.¹⁸⁰ Relevante Kriterien hierfür sind, ob regelmäßige Überprüfungen und kontinuierliche Verbesserungen des Compliance-Systems erfolgen, ob ein Untersuchungsprogramm zur Aufklärung von Non-Compliance existiert und ob eine Analyse und Behebung aufgedeckter Fehlentwicklungen erfolgt.

Die genannten Kriterien und **Leitfragen** im Leitfaden des US-amerikanischen Justizministeriums sind teilweise etwas redundant, im Hinblick auf die geforderten Maßnahmen aber sehr detailliert formuliert. Unabhängig von seiner jeweiligen Anwendbarkeit auf deutsche Unternehmen bietet der Leitfaden hinsichtlich

45

172 Siehe die ausführliche Darstellung des US-Rechts bei *Kark*, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 1176, 1245 ff.; *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 161 ff. sowie v. *Busekist/Beneke*, WPg 2020, 61, 63 f.

173 US DOJ, S. 13 ff.

174 Vgl. JM 9-28.300 No. 7; *Jenne*, CB 2019, 327; *Schulz/Block*, CCZ 2020, 49; *Grützner/Güngör*, CCZ 2019, 189.

175 JM § 9-28.8000; US DOJ, S. 1.

176 US DOJ, S. 1.

177 US DOJ, S. 1 ff.

178 US DOJ, S. 1 ff. Siehe auch *Moosmayer*, Compliance, Rn. 17 ff.; *Schulz*, in: Bay/Hastenrath, Compliance-Management-Systeme, § 8 Rn. 28 ff. Zu Compliance bei M&A-Transaktionen siehe → *Ullrich*, Kap. 26.

179 US DOJ, S. 9 ff.

180 US DOJ, S. 2, 14 ff.

der praktischen Umsetzung vieler Compliance-Themen eine nützliche Grundlage für die **Optimierung des Compliance Managements**.¹⁸¹

5. Deutscher Corporate Governance Kodex

- 46 Auch der Deutsche Corporate Governance Kodex (DCGK) enthält diverse Hinweise für das Compliance Management im Unternehmen. Wie ausgeführt, nimmt auch die Kodexfassung von 2022 ausdrücklich auf die Compliance-Verantwortung des Vorstands Bezug: Die in **A. I., Grundsatz 5** DCGK angesprochene **Compliance-Verantwortung des Vorstands** ist auch in der Fassung von 2022 unverändert geblieben: Der Vorstand hat danach für die Einhaltung der gesetzlichen Bestimmungen und der internen Richtlinien zu sorgen und wirkt auf deren Beachtung im Unternehmen hin (Compliance). Das **interne Kontrollsystem** und das Risikomanagementsystem umfassen auch ein an der Risikolage des Unternehmens ausgerichtetes **Compliance-Management-System**.¹⁸²

6. Erkenntnisse des Risikomanagements

- 47 Zwischen Compliance Management und Risikomanagement besteht ein enger Zusammenhang,¹⁸³ weshalb sich auch aus den Erkenntnissen des Risikomanagements wertvolle Impulse für die Ausgestaltung des Compliance Managements ergeben können. Dabei sollten allerdings unter anderem folgende Besonderheiten berücksichtigt werden.
- 48 Bei der Steuerung von Compliance-Risiken geht es stets um den **Umgang mit menschlichem (Fehl-)Verhalten**, welches einer juristischen Bewertung bedarf. Die rechtliche Bewertung durch Gerichte und Behörden ist ein dynamischer Prozess und in unterschiedlichen Rechtsordnungen unterschiedlich ausgeprägt – eine rein rechnerische Betrachtung von Compliance-Risiken erscheint daher nicht angebracht.¹⁸⁴ Eine weitere Besonderheit von Compliance-Risiken folgt aus dem Verständnis von Compliance Management als Organisationspflicht zur systematischen Prävention regelwidrigen Verhaltens. Denn bei Compliance Verstößen steht regelmäßig der Vorwurf fehlender bzw. unzureichender präventiver Maßnahmen im Mittelpunkt.¹⁸⁵ Dieses Risiko unzureichender Unternehmensorganisation ist aufgrund des oben dargestellten dynamischen rechtlichen Umfelds

181 US DOJ, S. 13 ff.

182 DCGK, A. I, Grundsatz 5 sowie hierzu *Kremer* u. a., Deutscher Corporate Governance Kodex, Grundsatz 5, Rn. 1 ff.

183 Zum Compliance-Risikomanagement umfassen *Kark*, Compliance-Risikomanagement, 3. Aufl. 2024; *Moosmayer*, Compliance-Risikoanalyse.

184 Zur Analyse und Bewertung der Compliance-Risiken *Kark*, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 742 ff.

185 Siehe hierzu die Ausführungen des LG München I, Urt. v. 10.12.2013 – 5 HK O 1387/10, CB 2014, 167 ff.; siehe auch *Moosmayer*, Compliance, Rn. 1 ff., 11 ff.; *Schulz*, Rechtliches Risikomanagement und Compliance im Mittelstand, in: Kessler, Unternehmensfinanzierung Mittelstand, § 6 Rn. 10; *Nietsch/Hastenrath*, CB 2015, 177, 178.

hoch – wie ausgeführt, haben die Geschäftsleiter eine Pflicht zur Organisation, Kontrolle und Durchsetzung der Einhaltung rechtlicher Vorgaben (siehe → unter Rn. 36). Diese Legalitätskontrollpflicht schließt die Verantwortung für das rechtmäßige Verhalten der Unternehmensangehörigen ein.¹⁸⁶ Zu den besonderen Merkmalen von „Non-Compliance“-Fällen zählen ferner besondere Image- und Reputationsrisiken; ihre Vermeidung bzw. Minimierung steht oft im Mittelpunkt von Compliance-Maßnahmen.¹⁸⁷

a) Besonderheiten von Compliance-Risiken

Eine wesentliche Besonderheit von Compliance-Risiken und Compliance Management besteht zudem darin, dass der staatliche **Rechtsdurchsetzungsanspruch** grundsätzlich keine wirtschaftliche Risikoabwägung kennt¹⁸⁸ – sog. „**nützliche Pflichtverletzungen**“ werden rechtlich nicht toleriert und sind regelmäßig Compliance-Verstöße.¹⁸⁹ Wie das oben erwähnte Urteil des Landgerichts München bestätigt hat (siehe → Rn. 39), können insbesondere regionale Geschäftsgepflogenheiten in anderen Ländern in keinem Fall Bestechungshandlungen rechtfertigen.¹⁹⁰ Die Leitgedanken dieser Entscheidung – **Organisationspflicht zur Vermeidung von Rechtsverstößen** in Abhängigkeit von dem jeweiligen Compliance-Risikoprofil – lassen sich grundsätzlich auf alle Unternehmen und Verbände übertragen.¹⁹¹ Es empfiehlt sich daher, auf Basis der vielfältigen Organisationsanforderungen der Rechtsordnung¹⁹² eine **unternehmensspezifische Risikoinventur** als Ausgangspunkt für das Compliance Management zu wählen (siehe unter → Rn. 60 ff.) und dabei die Besonderheiten von Compliance-Risiken zu beachten.¹⁹³

49

186 Vgl. *Verse*, ZHR 175 (2011), 401, 403; *Grigoleit*, AktG, § 76 Rn. 44 ff.

187 Vgl. *Staub*, CCZ 2009, 121, 129 ff.; *Schulz*, Rechtliches Risikomanagement und Compliance im Mittelstand, in: Kessler, Unternehmensfinanzierung Mittelstand, § 6 Rn. 11; zur Bedeutung von Reputations- und Imageschäden siehe ausführlich *Kröger*, Korruptionsschäden, Unternehmensgeldbußen und Imageschäden, S. 255 ff.; zum „Corporate Reputation Management“ siehe *Seibt*, DB 2015, 171.

188 *Preusche/Würz*, Compliance, S. 46; ähnlich *Kark*, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 114 ff.

189 Vgl. *Kort*, in: Hirte/Mülbert/Roth, AktG, § 91 Rn. 183; *Bosse*, NWB 51/2013, 4056, 4057.

190 Vgl. LG München I, Urt. v. 10.12.2013 – 5 HK O 1387/10, CB 2014, 167 ff., sowie hierzu *Fleischer*, NZG 2014, 321, 322.

191 Vgl. *Rack*, CB 2014, 104 zur Einordnung der Entscheidung in die Rechtsprechung zum sog. Organisationsverschulden, sowie *Passarge*, in: Martinek/Semler/Flohr, Handbuch des Vertriebsrechts, § 79 Rn. 90 hinsichtlich der Relevanz der Entscheidung für die GmbH.

192 Zur Entwicklung der sog. Unternehmensorganisationspflichten umfassend *Spindler*, Unternehmensorganisationspflichten; *Matusche-Beckmann*, Das Organisationsverschulden; vgl. ferner *Rack*, CB 2014, 104; zum Konzept der strafrechtlichen Garantenpflichten siehe *Spindler*, Handbuch Vorstandsrecht, sowie → *Böttger*, Kap. 2.

193 Die Bewertung wird u. a. durch Spielräume bei der Strafzumessung, zum Teil in unterschiedlichen Jurisdiktionen, Einzelfallentscheidungen von Gerichten und Behörden, möglichen Zurechnungen von Fehlverhalten in der Lieferkette etc. erschwert.

b) Mögliche Berücksichtigung integrativer Perspektiven

- 50 Hilfreich für die Konzeption und Weiterentwicklung des Compliance Managements kann auch die Berücksichtigung ganzheitlicher bzw. integrativer Perspektiven sein, durch die neben der Compliance-Funktion weitere Funktionen wie insbesondere Risikomanagement, Revision und Governance-Funktionen einbezogen werden. So wurde in der Betriebswirtschaftslehre seit Längerem ein Ansatz entwickelt, der ein ganzheitliches Management der Governance-, Risiko- und Compliance-Funktionen ermöglichen soll (**Governance, Risk und Compliance**, sog. **GRC-Ansatz**).¹⁹⁴ In Kreditinstituten ist die Compliance-Funktion ferner Teil des **Internen Kontrollsystems (IKS)** gemäß § 25a Abs. 1 Nr. 3 KWG, welches der Gesetzgeber mit der Einführung von § 91 Abs. 3 AktG im Jahr 2021 auch als Steuerungsinstrument für börsennotierte Aktiengesellschaften etabliert hat.¹⁹⁵ Die für Kreditinstitute durch den Gesetzgeber vorgeschriebene „ordnungsgemäße Geschäftsorganisation“ erfordert ausdrücklich die Einrichtung interner Kontrollverfahren mit einem internen Kontrollsystem und einer Internen Revision, wobei die Compliance-Funktion integraler Systembestandteil des **IKS** neben dem Risikomanagement ist.¹⁹⁶ Aufgrund des engen Zusammenhangs zwischen den genannten Funktionen wird dafür plädiert, ihre Instrumente und Prozesse sorgfältig aufeinander abzustimmen und miteinander zu verzahnen.¹⁹⁷ Dadurch sollen insbesondere Lücken bei der Risikoerfassung, -bewertung und -steuerung vermieden werden.¹⁹⁸ Einen ähnlichen Ansatz wie dieses Modell einer „**Combined-Assurance**“¹⁹⁹ verfolgt auch das „**Three-Lines-Modell**“.²⁰⁰ Danach sind Compliance-Fragen in erster Linie durch die operativen Unternehmenseinheiten zu adressieren, die zweite Linie bilden dann das Risikomanagement, das Controlling und die Compliance Funktion, welche die operativen Einheiten durch Beratung und geeignete Prozesse (z.B. Richtlinien, Schulungen) sowie deren Überwachung unterstützen; in dritter Linie werden die Risikomaßnahmen und ihre Wirkung dann durch die interne Revision als objektive und unabhängige Prüfungsinstanz überprüft.²⁰¹ Zwar verfügen nicht alle Unternehmen

194 Siehe hierzu → *Bartuschka*, Kap. 11; zur Verknüpfung von Internem Kontrollsystem (IKS), Risikomanagementsystem (RMS) und Compliance-Management-System (CMS) siehe *Ghassemi-Tabar*, in: *Ghassemi-Tabar*, Deutscher Corporate Governance Kodex, DCGK G5 Grundsatz 5, Rn. 59 ff.

195 Vgl. → *Renz/Frankenberger*, Kap. 20 Rn. 70 ff. m. w. N.

196 Vgl. § 25a Abs. 1 Nr. 3 KWG sowie → *Renz/Frankenberger*, Kap. 20 Rn. 70 ff. m. w. N.

197 *Ghassemi-Tabar*, in: *Ghassemi-Tabar*, Deutscher Corporate Governance Kodex, DCGK G5 Grundsatz 5, Rn. 59 ff.

198 *Ghassemi-Tabar*, in: *Ghassemi-Tabar*, Deutscher Corporate Governance Kodex, DCGK G5 Grundsatz 5, Rn. 59 ff.

199 Zum Modell einer „Integrated Assurance“ ausführlich *Moosmayer/Lösler*, in: *Moosmayer/Lösler*, Corporate Compliance, § 1 Rn. 44 ff.; zum Modell einer integrierten GRC-Organisation siehe *Wilms*, in: *Bürkle/Hauschka/Schieffer*, Der Compliance Officer, § 5 Rn. 34 ff.

200 Siehe hierzu *Klahold/Lochen*, in: *Moosmayer/Lösler*, Corporate Compliance, § 13 Rn. 22 ff. sowie → *Renz/Frankenberger*, Kap. 20 Rn. 76.

201 Siehe hierzu → *Renz/Frankenberger*, Kap. 20 Rn. 76 ff.

über eigenständige Kontroll-, Risikomanagement- und Compliance-Funktionen, die genannten Modelle sind entweder durch den Gesetzgeber vorgegeben oder für größere Unternehmen konzipiert. Gleichwohl erscheint es in jedem Fall sinnvoll, über eine wirkungsvolle **Verknüpfung der** durch diese Funktionen institutionalisierten **Prozesse** nachzudenken.²⁰² Aus diesen Modellen lässt sich die Notwendigkeit eines differenzierten und abgestuften Prozesses für die Steuerung von Compliance-Risiken ableiten und insbesondere die Notwendigkeit einer Einbettung von Compliance-Maßnahmen in die relevanten Geschäftsprozesse (siehe hierzu unter → Rn. 83).

7. Compliance-Standards als Orientierungshilfe (Beispiel IDW PS 980)

Compliance steht zudem seit geraumer Zeit auch im Blickfeld diverser Organisationen und Verbände, die Standards und Leitlinien zu Compliance bzw. zu Compliance-Management-Systemen (CMS) veröffentlicht haben. In der Praxis ist insbesondere der vom **Institut der Wirtschaftsprüfer** in Deutschland (IDW) 2011 veröffentlichte und 2022 in einer Neufassung verabschiedete Standard „Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen“ (**IDW PS 980**) stark verbreitet, welcher sog. „Grundelemente“ eines CMS formuliert hat.²⁰³ Dazu zählen nach wie vor die **Compliance-Kultur** als Grundlage für die Angemessenheit und Wirksamkeit des CMS und die von den gesetzlichen Vertreter festgelegten **Compliance-Ziele**. Unter Berücksichtigung der Compliance-Ziele werden die **Compliance-Risiken** festgestellt, die Verstöße gegen einzuhaltende Regeln und damit eine Verfehlung der Compliance-Ziele zur Folge haben können. Basierend auf der Beurteilung der Compliance-Risiken wird ein **Compliance-Programm** eingeführt, das auf die Begrenzung der Compliance-Risiken und die Vermeidung von Compliance-Verstößen ausgerichtet ist. Das Management regelt die Aufbau- und Ablauforganisation und stellt die notwendigen Ressourcen zur Verfügung (**Compliance-Organisation**). Die betroffenen Mitarbeiter und Dritte sind über das Compliance-Programm zu informieren (**Compliance-Kommunikation**). Angemessenheit und Wirksamkeit des CMS sollen in geeigneter Weise überwacht werden (**Compliance-Überwachung und -Verbesserung**). Voraussetzung hierfür ist eine ausreichende Dokumentation des CMS. Die gesetzlichen Vertreter sorgen ferner für die Durchsetzung des CMS, die Beseitigung der Mängel und die Verbesserung des Systems. Diese Grundelemente eines CMS entsprechen weitgehend denjenigen

51

202 Dieser Ansatz liegt mittlerweile auch global geltenden Standards wie beispielsweise der ISO 37301 (Compliance Management Systeme) zu Grunde.

203 IDW-Prüfungsstandard „Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen“ (IDW PS 980) v. 11.3.2011, aktuelle Version v. 09.2022, siehe zur Neufassung *Jonas*, in: Minn/Stick/Laber, Personallexikon, Edition 42 2024, Compliance – IDW PS 980; sowie zur Vorläuferversion *Balke*, in: Born/Ghassemi-Tabar/Gehle (Hrsg.) MHBGesR VII, § 104 Rn. 14 ff. sowie *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 131 ff. Zur Rolle von IDW-Standards ferner umfassend *Schülke*, IDW-Standards und Unternehmensrecht, 2014.

Elementen und Anforderungen, die auch in Rechtspraxis und Rechtswissenschaft als Kernbestandteile eines wirksamen Compliance Managements angesehen werden.²⁰⁴ Allerdings empfiehlt es sich, bei der Gestaltung des Compliance Management insbesondere diejenigen Grundanforderungen und Kernelemente zu berücksichtigen, die in der Rechtsprechung (unter Begleitung der rechtswissenschaftlichen Literatur) als maßgeblich angesehen werden.²⁰⁵ Denn im Falle eines Regelverstößes ist die entscheidende Frage, ob vorhandene Compliance-Strukturen und Maßnahmen zu einer Minderung von Sanktionen und weiteren Kosten der Non-Compliance führen können. Die Antwort darauf hängt entscheidend davon ab, wie Gerichte und Behörden im jeweiligen Einzelfall die bestehenden Compliance-Maßnahmen beurteilen.²⁰⁶

III. Erfolgsfaktoren für ein wirksames Compliance Management

1. Individuelle Konzeption auf Basis des Compliance-Risikoprofils

- 52** Ein zentraler Erfolgsfaktor für ein wirksames Compliance Management liegt in seiner passenden („maßgeschneiderten“) Konzeption, die genau auf den spezifischen Bedarf und das **individuelle** Risikoprofil des Unternehmens abgestimmt ist. Als relevant für die Bestimmung des individuellen **Compliance-Risikoprofils** gelten insbesondere die folgenden Kriterien:

- Branche bzw. Industriesektor;
- regulatorisches Umfeld;
- Unternehmensgröße und Struktur;
- Kapitalmarktzugang;
- Geschäftsmodell (insbesondere Vertriebsstruktur);
- internationale Präsenz bzw. Auslandsaktivitäten;
- Compliance-Verstöße in der Vergangenheit („Compliance-Historie“);
- Wahrscheinlichkeit einer Normverletzung.

Abgesehen von besonderen gesetzlichen Organisationsvorgaben (siehe unter → Rn. 27 ff.) kann sich der Organisationsgrad des Compliance Managements nach oben genannten Kriterien richten.

204 Zu den Grundelementen und Mindestanforderungen vgl. *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 121 ff.; *Moosmayer*, Compliance, Rn. 144 ff.; *Kremer/Klahold*, ZGR 2010, 113, 122 ff.; *Klopp*, Der Compliance-Beauftragte, S. 81 ff.; *Schulz/Renz*, BB 2012, 2511, 2512 f., sowie speziell für die GmbH *Theusinger/Jung*, in: Römermann, Münchener Anwaltshandbuch GmbH-Recht, § 24 Rn. 40 ff.

205 Vgl. hierzu die umfangreichen Nachweise bei *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 121 ff.

206 Siehe insbesondere die Anforderungen an Compliance-Maßnahmen durch LG München I, Urt. v. 10.12.2013 – 5 HK O 1387/10, CB 2014, 167 ff. und hierzu *Fleischer*, NZG 2014, 321 ff. sowie durch OLG Nürnberg, 30.3.2022 – 12 U 1520/19, CB 2022, 493. Siehe ferner die instruktiven Ausführungen des VRiBGH a.D. *Rolf Raum*, Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten in: Hastenrath, Compliance-Kommunikation, S. 31 ff.

Grundsätzlich haben die Geschäftsleiter bei der Ausgestaltung des Compliance Managements ein Handlungsermessen nach den Grundsätzen der sog. „Business Judgment Rule“²⁰⁷ hinsichtlich der Einführung geeigneter Compliance-Strukturen, Prozesse und Systeme.²⁰⁸ Dieses Auswahlermessen umfasst etwa die Frage, ob die Geschäftsleitung die Compliance-Pflicht in vollem Umfang selbst erfüllt, oder ob sie bestimmte Compliance-Aufgaben an andere Unternehmenseinheiten (wie etwa die Compliance- oder Rechtsabteilung) oder an Externe delegiert.²⁰⁹ In jedem Fall sind hierbei jedoch einerseits die Zulässigkeit einer Delegation von Compliance-Maßnahmen ebenso wie Delegationsgrenzen zu beachten (dazu unter → Rn. 56 f.).

53

2. Entwicklung einer passenden Compliance-Strategie

Es sollte das Ziel jeder Geschäftsleitung sein, eine geeignete und auf das Unternehmen abgestimmte Strategie für ein regelkonformes Verhalten der Stakeholder zu organisieren. Die Compliance-Strategie sollte dabei alle wesentlichen konzeptionellen Fragen und Strukturentscheidungen adressieren, denn diese fallen regelmäßig in den Zuständigkeitsbereich der Unternehmensleitung als Gesamtorgan.²¹⁰ Wie nachfolgend im Einzelnen erläutert wird, bedarf es hierzu der Wahl eines unternehmensspezifischen Organisationsmodells, der Klärung von Zuständigkeiten und Delegationsfragen, einer Fokussierung und Prioritätensetzung bei den Compliance-Maßnahmen sowie eines systematischen Managements des individuellen Compliance-Risikoprofils. Die Compliance Strategie sollte ferner die Förderung einer Compliance-Kultur²¹¹ adressieren sowie ein Compliance-Regelwerk vorsehen, welches mittels verständlicher Schulungsprogramme an die Stakeholder vermittelt sowie regelmäßig dokumentiert, kontrolliert und aktualisiert wird.

54

207 Vgl. *Fleischer*, in: MünchKomm-GmbHG, § 43 Rn. 79 ff. Zur Business Judgment Rule umfassend *Fischer*, Die Business Judgment Rule als typübergreifendes Institut.

208 Vgl. *Rodewald*, Gesetzestreue als Organisationsproblem – Compliance richtig managen, in: Maschmann, Corporate Compliance und Arbeitsrecht, S. 32, 38; *Hauschka/Moosmayer/Lösler*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 1 Rn. 22 ff., 33; *Balke*, in: Born/Ghassemi-Tabar/Gehle (Hrsg.) MHD BGesR VII, § 104 Rn. 12 f. sowie in Bezug auf die GmbH *Bosse*, NWB 2013, 4056, 4060.

209 Zur Notwendigkeit eines „Schnittstellen-Managements“ siehe → Rn. 85. Zur Zusammenarbeit der Compliance-Abteilung mit anderen Funktionen ausführlich → *Rau*, Kap. 3.

210 Vgl. auch *Karbaum*, AG 2013, 863, 870.

211 Vgl. *Wieland*, Integritäts- und Compliance Management als Corporate Governance – konzeptionelle Grundlagen und Erfolgsfaktoren, in: Wieland/Steinmeyer/Grüniger, Handbuch Compliance-Management, S. 15, 23 ff.; *Grüniger*, Grundlagen einer wertorientierten Compliance, ebenda, S. 41 ff., 57 ff. Zur Compliance-Strategie ferner *Itzen*, BB-Spezial 2008, 12 ff.; *Bergmoser/Theusinger/Gushurst*, BB-Spezial 2008, 1, 9 ff.

a) Wahl eines unternehmensspezifischen Organisationsmodells

- 55 Entsprechend der Vielfalt unternehmerischer Aktivitäten gibt es für Compliance Management ganz **unterschiedliche Organisationsmodelle**.²¹² In kleineren und mittelständischen Unternehmen wird die Compliance-Verantwortung meist vom Inhaber bzw. Gesellschafter-Geschäftsführer selbst wahrgenommen (soweit die betreffenden Personen die Notwendigkeit von Compliance Management erkannt haben),²¹³ oder die Verantwortlichen beauftragen externe Anbieter (wie Rechtsanwälte oder Wirtschaftsprüfer) mit der Ausführung von Compliance-Aufgaben.²¹⁴ Dagegen sind in größeren Unternehmen häufig nachgeordnete Unternehmenseinheiten wie die Rechtsabteilung, das Risikomanagement oder die Interne Revision mit Compliance-Aufgaben betraut. In großen Unternehmen und Konzernen werden bestimmte Compliance-Aufgaben oft einem zentralen „**Chief Compliance Officer (CCO)**“ zugewiesen, welcher dann bestimmte Compliance-Aufgaben an weitere Compliance Officer in den einzelnen Geschäftseinheiten delegiert.²¹⁵ In dem – ebenfalls in größeren Unternehmen zu findenden – Modell einer sog. **Matrix-Organisation** wird die Compliance-Funktion durch ein besonderes Gremium (z.B. durch ein sog. „**Compliance Committee**“) koordiniert, dem die Repräsentanten anderer Unternehmenseinheiten wie etwa Rechtsabteilung, Revision, Finanzen, Personalabteilung sowie die Fachbereiche angehören.²¹⁶ Mit Ausnahme spezialgesetzlicher Organisationserfordernisse liegt die Ausgestaltung der organisatorischen Einzelheiten im **Gestaltungsermessen** der Geschäftsleiter.²¹⁷ Entscheidend ist jeweils die genaue Abstimmung der Compliance-Maßnahmen auf die individuelle Unternehmenssituation und die Anpassung an die jeweils verfolgte **Unternehmensstrategie**.

b) Klärung von Zuständigkeiten und Delegationsfragen

- 56 Wie oben ausgeführt, ist die Compliance-Pflicht eine besondere Ausprägung der Leitungssorgfaltspflicht der Geschäftsleiter (siehe oben → Rn. 36).²¹⁸ Compli-

212 Siehe ausführlich *Moosmayer*, Compliance, Rn. 105 ff., welcher zwischen einer sog. autonomen Compliance-Organisation und einer „Matrix-Organisation“ unterscheidet; *ders.*, in: Rotsch (Hrsg.), *Criminal Compliance*, S. 203 ff.; vgl. ferner *Gößwein/Hohmann*, BB 2011, 963 ff.; *Groß*, Chief Compliance Officer, S. 61 f.; *Behringer*, in: *Behringer*, Compliance kompakt, 367 ff.; *Cauers/Haas/Jakob/Kremer/Schartmann/Welp*, DB 2008, 2717 ff.; *Favocia/Richter*, AG 2010, 137, 138; *Kraft/Winkler*, CCZ 2009, 29, 31.

213 Vgl. *Nietsch/Hastenrath*, CB 2015, 177, 178.

214 Zum „Outsourcing“ von Compliance-Aufgaben auf Externe siehe *Bürkle/Kinzl*, in: *Moosmayer/Lösler*, Corporate Compliance, § 12 Rn. 72 ff.; *Schmidt*, Compliance in Kapitalgesellschaften, S. 163 ff.

215 Zu diesem mehrstufigen System von Compliance-Beauftragten ausführlich *Bürkle*, in: *Hauschka/Moosmayer/Lösler*, Corporate Compliance; *Bürkle/Kinzl*, in: *Moosmayer/Lösler*, Corporate Compliance, § 12; *Moosmayer*, in: *Rotsch (Hrsg.)*, *Criminal Compliance*, S. 205.

216 Vgl. *Moosmayer*, Compliance, Rn. 108 ff.; *Gößwein/Hohmann*, BB 2011, 963, 966 f.

217 Vgl. *Bürkle/Kinzl*, in: *Moosmayer/Lösler*, Corporate Compliance, § 12 Rn. 11 ff.

218 Vgl. auch *Merkt*, ZIP 2014, 1705.

ance ist „Chefsache“²¹⁹ – dementsprechend verbleibt ein unveräußerlicher **Kernbereich der Compliance-Pflicht** stets bei der Geschäftsleitung.²²⁰ In diesem Rahmen muss sie dafür sorgen, dass eindeutige Zuständigkeiten, Verantwortungsbereiche und Berichtswege für Compliance-Maßnahmen bestehen.²²¹ Während etwa in der kleinen und mittelständischen GmbH mit einem (Allein-)Geschäftsführer dieser meist höchstpersönlich die Compliance-Verantwortung wahrnimmt, werden in größeren Unternehmen Compliance-Aufgaben an eines von mehreren Geschäftsleitungsmitgliedern übertragen (sog. **horizontale Delegation**).²²² In großen Unternehmen und Konzernen werden Compliance-Aufgaben häufig an sog. Compliance Officer oder andere Unternehmenseinheiten (wie Rechtsabteilung, Risikomanagement oder Interne Revision) delegiert (sog. **vertikale Delegation**).²²³

In jedem Fall sind die allgemeinen rechtlichen **Anforderungen an eine wirksame Delegation** zu beachten: Danach führt eine Delegation von Aufgaben nicht zu einer vollständigen Pflichtbefreiung der übertragenden Personen, vielmehr wandelt sich ihre Pflicht in eine **Kontroll- und Überwachungspflicht** um: Bei einer horizontalen Delegation an einzelne Geschäftsführungsmitglieder müssen die übrigen Geschäftsführungsmitglieder die Aufgabenwahrnehmung ihrer Kollegen beobachten und sind verpflichtet, im Fall von Compliance-Verstößen zu intervenieren.²²⁴ Im Fall der vertikalen Delegation von Compliance-Aufgaben (z. B. an Compliance Officer) verbleiben bei den Auftraggebern bestimmte **Auswahl-, Instruktions- und Überwachungspflichten**, d.h. die jeweiligen Auftragnehmer müssen sorgfältig ausgewählt, eingearbeitet und kontrolliert werden.²²⁵ 57

c) Fokussierung und Prioritätensetzung bei Compliance-Maßnahmen

Im Hinblick auf eine systematische Prävention von Regelverletzungen und Fehlverhalten²²⁶ sollte es das Ziel jeder Geschäftsleitung sein, geeignete und auf das Unternehmen abgestimmte Rahmenbedingungen für ein regelkonformes Ver- 58

219 Siehe *Fleischer*, CCZ 2008, 1, 3.

220 So ausdrücklich und zutreffend *Inderst*, Compliance-Programm und praktische Umsetzung, in: *Inderst/Bannenberg/Poppe*, Compliance, S. 142; siehe ferner *Seibt*, in: Schmidt/Lutter (Hrsg.), AktG, § 76 Rn. 31 ff. sowie ausführlich *Gomer*, Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft, S. 123 ff., 160 ff.

221 Vgl. LG München I, Urt. v. 10.12.2013 – 5 HK O 1387/10, CB 2014, 167 ff., vgl. hierzu *Fleischer*, NZG 2014, 321 ff.; siehe ferner *Balke*, in: Born/Ghassemi-Tabar/Gehle (Hrsg.) MHBGesRVII, § 104 Rn. 26 ff.

222 *Schulz*, CB 2015, 309, 315; zur horizontalen Delegation etwa *Kort*, GmbHR 2013, 566 f.

223 Vgl. zur vertikalen Delegation etwa *Kort*, GmbHR 2013, 566, 567.

224 Dies folgt aus dem Grundsatz der Gesamtverantwortung der Geschäftsführungsmitglieder, vgl. *Kort*, GmbHR 2013, 566 f.

225 Vgl. *Kark*, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 100; *Klopp*, Der Compliance-Beauftragte, S. 186 ff. m. w. N.

226 Vgl. *Raum*, Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten, in: Hastenrath, Compliance-Kommunikation, S. 31, 48 f.

halten der Verbandsangehörigen zu organisieren. Dabei ist zu beachten, dass die Compliance-Maßnahmen regelmäßig unter dem **Vorbehalt der Erforderlichkeit und der Zumutbarkeit**, je nach den Besonderheiten des Unternehmens, variiert.²²⁷ Dies erlaubt in vielen Fällen eine Fokussierung bzw. **Prioritätensetzung** bei der Einführung bzw. Aktualisierung der Compliance-Maßnahmen. Ein Schwerpunkt sollte auf der **Wirksamkeit der Compliance-Maßnahmen** liegen, denn Gesetzgebung und Rechtsprechung zeigen immer wieder normative Anreize für ein wirksames Compliance Management: So spielte die positive Wirkung von Compliance-Maßnahmen eine wichtige Rolle in dem (vorerst gescheiterten) **Regierungsentwurf eines Gesetzes zur Stärkung der Integrität der Wirtschaft (Verbandssanktionengesetz – VerSanG-E)**.²²⁸ Dieser Regierungsentwurf hatte ausdrücklich das Ziel verfolgt, Compliance-Maßnahmen zu fördern und hierfür normative **Anreize** zu setzen.²²⁹ Allerdings wurde aus der Begründung des Entwurfs deutlich, dass eine Wertschätzung nur hätte erfolgen können, wenn die Compliance-Maßnahmen wirksam sind und funktionieren.²³⁰

- 59 In eine ähnliche Richtung scheint die Rechtsprechung zu tendieren, wie sich aus einer Entscheidung des Bundesgerichtshofes vom 9.5.2017²³¹ ergibt. Im Rahmen der Entscheidung über ein Bußgeld für ein Unternehmen wegen der zurechenbaren Straftat einer Leitungsperson (§§ 30, 130 OWiG) führte der BGH im Wege eines obiter dictum Folgendes aus: Für die Bemessung der Geldbuße sei auch von Bedeutung, inwieweit das Unternehmen „seiner Pflicht, Rechtsverletzungen aus der Sphäre des Unternehmens zu unterbinden, genügt und ein **effizientes Compliance Management** installiert hat, das auf die **Vermeidung von Rechtsverstößen** ausgelegt sein muss. Dabei kann auch eine Rolle spielen, ob die Nebenbeteiligte in der Folge dieses Verfahrens entsprechende Regelungen optimiert und ihre betriebsinternen Abläufe so gestaltet hat, dass vergleichbare Normverletzungen zukünftig jedenfalls deutlich erschwert werden.“²³² Zwar hat der BGH die Kriterien für ein „effizientes Compliance Management“ in dieser

227 Vgl. *Merk*, ZIP 2014, 1705, 1711; *Verse*, ZHR 175 (2011), 401, 403, 406 f., sowie *Bürkle*, BB 2005, 565, 569; *ders.*, BB 2007, 1797, 1798; *Bachmann*, Compliance – Rechtsgrundlagen und offene Fragen, in: Schriftenreihe der Gesellschaftsrechtlichen Vereinigung (Hrsg.), Gesellschaftsrecht in der Diskussion, S. 65, 78 f.; *Reichert*, ZIS 2011, 113, 115.

228 Regierungsentwurf „Entwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft vom 16.6.2020, https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Staerkung_Integritaet_Wirtschaft.pdf;jsessionid=26E814AC76746EB88778F4B4D103B8BE.2_cid334?__blob=publicationFile&v=2 (zuletzt abgerufen am 24.9.2020). Siehe ferner den Regierungsentwurf vom 21.10.2020 mit der Gegenäußerung der Bundesregierung zur Stellungnahme des Bundesrates, BT-Drs. 19/23568, <https://dip21.bundestag.de/dip21/btd/19/235/1923568.pdf>.

229 Vgl. Regierungsentwurf „Entwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft“, I, 55 f., 95 f. Siehe auch → *Böttger*, Kap. 2 Rn. 143 ff.

230 Vgl. Regierungsentwurf „Entwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft“, 95 f.

231 Vgl. BGH, Urt. v. 9.5.2017 – 1 StR 265/16 = CB 2017, 330, Ls. 3.

232 Vgl. BGH, Urt. v. 9.5.2017 – 1 StR 265/16 = CB 2017, 330, Ls. 3.

Entscheidung nicht näher konkretisiert. Im Zusammenhang der Entscheidungsbegründung und weiteren Stellungnahmen²³³ ist denkbar, dass das Gericht weniger auf die **Effizienz** als vielmehr auf die Effektivität des Compliance Managements abstellen wollte.²³⁴ Denn im Unterschied zur Effizienz (Beziehung zwischen erbrachter Leistung und Ressourceneinsatz) bezeichnet **Effektivität** die Beurteilung der Zielerreichung, also in welchem Ausmaß die geplanten Ziele auch tatsächlich erreicht worden sind.²³⁵ Diese Beurteilung dürfte auch für das Compliance Management entscheidend sein, da dessen Zweck in der (bestmöglichen) Vermeidung von Regelverletzungen besteht.²³⁶ Für eine positive Berücksichtigung von Compliance-Maßnahmen durch Gerichte und Behörden kommt es regelmäßig darauf an, dass die Compliance Maßnahmen tatsächlich „gelebt“, also konsequent angewandt und regelmäßig aktualisiert werden.²³⁷ Denn nur so kann das Compliance Management seinen primären Zweck einer bestmöglichen **Vermeidung von Rechtsverstößen** erfüllen und erscheint nicht nur als bloßes Lippenbekenntnis.²³⁸ Insofern lohnt sich die strategische Fokussierung auf effektive Compliance-Maßnahmen.

d) Berücksichtigung des besonderen Compliance-Risikoprofils

Aufgrund des Zusammenhangs zwischen Compliance Management und Risikomanagement ist die Entwicklung eines Konzepts zur systematischen Steuerung relevanter Rechts- und Compliance-Risiken ein weiterer zentraler Bestandteil der Compliance-Strategie.²³⁹ Die **Compliance-Risikostrategie** bildet die Basis für die Identifizierung, Bewertung und Überwachung der Compliance-Risiken sowie die Konzeption adäquater Maßnahmen.²⁴⁰ Sie ist als Bestandteil der Leitungssorgfaltspflicht nicht delegierbar.²⁴¹ Das Eingehen von Risiken ist Bestandteil jeder unternehmerischen Aktivität, auch ein umfassendes Compliance Management kann die Risiken der „Non-Compliance“ nicht völlig ausschließen.

60

233 Vgl. *Raum*, Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten in: Hastenrath, Compliance-Kommunikation, S. 31, 48 f.

234 Vgl. *Schulz/Block*, CCZ 2020, 49, 50 f.

235 Vgl. *Thommen/Achleitner/Gilbert/Hachmeister/Jarchow/Kaiser*, Allgemeine Betriebswirtschaftslehre, S. 47, 48.

236 Vgl. *Schulz/Block*, CCZ 2020, 49, 51.

237 *Schulz/Block*, CCZ 2020, 49, 51.

238 *Raum*, Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten, in: Hastenrath, Compliance-Kommunikation, S. 31, 45, spricht von „Umsetzungsernsthaftigkeit“.

239 Vgl. *Kark*, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 13: „Das Compliance-Risikomanagement ist der Schlüssel, der den Zugang für ein wirksames Compliance-Programm eröffnet.“ Ähnlich von *Busekist/Schlitt*, CCZ 2012, 86.

240 Zur (Compliance)-Risikostrategie vgl. *Philippi*, in: Bay/Hastenrath, Compliance-Management-Systeme, § 3, Rn. 30 ff.; *Kark*, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 550 ff.; *Merk*, ZIP 2014, 1705 ff.; *Balke*, in: Born/Ghassemi-Tabar/Gehle (Hrsg.) MHD BGesRV VII, § 104 Rn. 17 ff.

241 *Klingenstein*, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, Rn. 99; *Pauthner/Stephan*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 16 Rn. 73 ff.

Aus Sicht eines wirksamen Compliance Managements kommt es jedoch darauf an, die Gefahren aus vorsätzlichem oder fahrlässigem Fehlverhalten der Unternehmensangehörigen so weit wie möglich zu reduzieren.²⁴² Wie ausgeführt (siehe oben unter → Rn. 47 ff.), ist dabei die Einbeziehung von Methoden und Verfahren des Risikomanagements hilfreich,²⁴³ die Besonderheiten der Compliance-Risiken sind jedoch stets zu beachten.²⁴⁴ Die Einzelheiten des Compliance-Risikomanagements richten sich nach den unternehmensindividuellen Besonderheiten, Ausgangspunkt ist das oben beschriebene **Compliance-Risikoprofil** des Unternehmens.²⁴⁵

aa) Systematische Identifikation von Compliance-Risiken

- 61** Rechts- und Compliance-Risiken können sich zunächst aus dem **rechtlichen Umfeld** des Unternehmens ergeben. Zur **Identifikation** relevanter Compliance-Risiken ist daher eine sorgfältige Analyse des jeweiligen Unternehmens ebenso erforderlich wie eine genaue Prüfung des Umfelds, in dem sich das Unternehmen bewegt. Dazu zählt eine Bestandsaufnahme von Vorgaben des rechtlichen Umfelds, d.h. sämtlicher für das Unternehmen einschlägiger **Normen und Rechtspflichten**.²⁴⁶ Diese kann je nach **Wettbewerbsumfeld, Branche und Geschäftsmodell** ganz unterschiedlich ausfallen, gleichwohl gibt es zahlreiche Compliance-Risiken, die alle Unternehmen und Verbände betreffen. Dazu gehören etwa Risiken im Zusammenhang mit arbeitsrechtrechtlichen, datenschutzrechtlichen und steuerrechtlichen Pflichten, weitere besondere Risiken ergeben sich für viele Unternehmen etwa im Zusammenhang mit dem Wettbewerbs- und Kartellrecht, dem Außenwirtschaftsrecht oder Antikorruptionsvorschriften (siehe oben → Rn. 3 ff.).²⁴⁷ Hinzu kommen **neue regulatorische Wachstumsbereiche** wie „**ESG-Compliance**“ und **IT-Compliance** bzw. „**KI-Compliance**“.²⁴⁸ Je nach Branchenzugehörigkeit, Größe, und geographischer Präsenz können weitere Risiken hinzukommen, etwa aus der Nichtbeachtung von Vorschriften des internationalen oder ausländischen Rechts. Zur systematischen Erfassung empfiehlt sich, die einschlägigen Normen und Rechtspflichten in einem digitalen **Bestandsverzeichnis** zu archivieren und zu dokumentieren. Die Ana-

242 Vgl. *Raum*, Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten, in: Hastenrath, Compliance-Kommunikation, S. 31, 44 ff.

243 Siehe hierzu ausführlich → *Romeike*, Kap. 9.

244 Vgl. *Staub*, CCZ 2009, 121, 125 ff., sowie *Kark*, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 105.

245 Vgl. *Kark*, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 103 ff.

246 Vgl. *von Busekist/Schlitt*, CCZ 2012, 86, 88 f.

247 Zu typischen Compliance-Risiken auch *Kark*, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 55 ff.

248 Siehe oben → Rn. 4 ff.

lyse des Umfelds sollte neben Rechts- und Compliance-Risiken ferner besondere länder- und branchenspezifische Risiken einbeziehen.²⁴⁹

Die Analyse des rechtlichen Umfelds des Unternehmens sollte mit einer sorgfältigen **Analyse des individuellen Geschäftsmodells** des Unternehmens und seiner Unternehmenseinheiten verknüpft werden.²⁵⁰ So sind etwa bestimmte Abteilungen wie etwa **Einkauf** und **Vertrieb** besonders anfällig für „Non-Compliance“ durch Korruption oder Verletzungen des Wettbewerbsrechts.²⁵¹ Grundsätzlich sollte jede Abteilung und Unternehmensfunktion eine „**Risiko-Inventur**“ durchführen, unter Zusammenarbeit der jeweiligen Leiter mit dem Compliance Officer, der Rechtsabteilung oder externen Rechtsberatern. 62

bb) Analyse und Bewertung

Die ermittelten Compliance-Risiken sind in einem weiteren Schritt zu analysieren und zu bewerten, maßgebliche Kriterien sind dabei das potenzielle **Schadensausmaß** sowie die **Eintrittswahrscheinlichkeit**. Allerdings besteht ein wichtiger Unterschied zum allgemeinen Risikomanagement darin, dass es nicht nur um eine rechnerische Betrachtung geht, sondern vielmehr um die **Bewertung menschlichen Verhaltens** im Hinblick auf mögliche Regelverstöße.²⁵² Ein weiterer gravierender Unterschied besteht darin, dass die Geschäftsleitung nicht aus Opportunitätserwägungen heraus Rechtsvorschriften missachten sollte, auch sog. „**nützliche Pflichtverletzungen**“ sind regelmäßig Compliance-Verstöße.²⁵³ Allerdings besteht Konsens dahingehend, dass Compliance-Maßnahmen unter den Aspekten der **Erforderlichkeit** und **Zumutbarkeit** zu beurteilen sind.²⁵⁴ Daher erscheint es beispielsweise zulässig, dass sich die Unternehmensleitung in einem ersten Schritt auf die wichtigsten Risiken (z. B. Korruption, Kartellrechtsverstöße) konzentriert. Im Hinblick auf die oben aufgezeigten vielfältigen Rechts- und Compliance-Risiken sollte diese **Schwerpunktsetzung** jedoch nie isoliert erfolgen, sondern Bestandteil eines ganzheitlichen Risikomanagements für das Unternehmen sein. Der Erfassung, Analyse und Steuerung der schwerwiegendsten Risiken sollten umgehend auch die sonstigen Compliance-Risiken folgen. 63

249 Vgl. Kark, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 61.

250 Vgl. Theusinger/Jung, in: Römermann, Münchener Anwaltshandbuch GmbH-Recht, § 24 Rn. 36, sowie ausführlich Staub, CCZ 2009, 121, 127 mit einem Risiko-Suchmatrix anhand der „value chain“ des Unternehmens.

251 Vgl. ausführlich Staub, CCZ 2009, 121, 127 mit einer Risiko-Suchmatrix anhand der „value chain“ des Unternehmens; ferner Theusinger/Jung, in: Römermann, Münchener Anwaltshandbuch GmbH-Recht, § 24 Rn. 36.

252 Siehe oben → Rn. 48.

253 Vgl. auch Kark, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 118.

254 Vgl. auch Bachmann, Compliance – Rechtsgrundlagen und offene Fragen, in: Schriftenreihe der Gesellschaftsrechtlichen Vereinigung (Hrsg.), Gesellschaftsrecht in der Diskussion, S. 65, 78 f.

cc) Implementierung von Risikosteuerungsmaßnahmen

- 64 Nach der Analyse und Bewertung der Rechts- und Compliance-Risiken folgt die Konzeption von **Maßnahmen der Risikosteuerung**, die sich nach dem jeweiligen Risiko richten. So kann die Analyse im Ergebnis etwa zu einer **Risikovermeidungsmaßnahme** dahingehend führen, dass sich das Unternehmen aus einem bestimmten Markt vollständig zurückzieht bzw. einen bestimmten neuen Markt gar nicht betritt.²⁵⁵ Andere – weniger radikale – Risikosteuerungsmaßnahmen betreffen die Konzeption spezifischer **Schulungen** zur Risikovermeidung (etwa im Zusammenhang mit Vertriebsstrukturen). Dabei kann ein zuvor erstelltes Rechtspflichten-Verzeichnis als Ausgangspunkt für spezielle Schulungsmaßnahmen dienen, mit denen die Unternehmensangehörigen hinsichtlich relevanter Rechts- und Compliance-Risiken in ihren Einheiten sensibilisiert und geschult werden.²⁵⁶
- 65 Im Hinblick auf ein integriertes und effektives Integritäts- und Compliance Management ist bei Konzeption und Durchführung passender Risikosteuerungsmaßnahmen die aktive **Einbeziehung von Führungskräften und Mitarbeitern** der relevanten Fachabteilungen und Unternehmenseinheiten wünschenswert – diese kennen regelmäßig das Risikoprofil ihrer Umgebung und können als „**Process Owner**“²⁵⁷ ihrer Geschäftsabläufe wertvolle Hinweise zur Risikosteuerung geben. Zudem kann durch die aktive Einbeziehung der Geschäftseinheiten die **Akzeptanz** des Compliance Managements erhöht werden, denn zur Vermeidung von Compliance-Risiken ist eine **Compliance-Kultur** erforderlich, in der ein entsprechendes Risikoverhalten nicht toleriert wird.²⁵⁸

dd) Berichterstattung zu Compliance-Risiken

- 66 Die Konzeption einer Compliance-Risikostrategie umfasst auch die Einführung eines entsprechenden **Reportings** bzw. die Integration dieser Berichte über Compliance-Risiken in die allgemeine Risikoberichterstattung, sofern diese im Unternehmen bereits existiert.²⁵⁹

ee) Durchführung regelmäßiger Compliance-Audits

- 67 Die ständige Veränderung des Umfelds für Unternehmen erfordert eine regelmäßige **Überprüfung** der Compliance-Maßnahmen sowie die **Anpassung** des

255 Vgl. Staub, CCZ 2009, 121, 130. Weitere Beispiele zur Compliance-Risikosteuerung bei Kark, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 829 ff.

256 Siehe hierzu am Beispiel von Kartellrechtsrisiken → Seeliger/Mross/Seydel, Kap. 27 Rn. 133 ff.

257 Siehe → Rn. 83. Vgl. auch Pauthner-Stephan, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 16 Rn. 49 ff.

258 Zur Relevanz der Risiko-/Compliance-Kultur siehe auch Kark, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 352 ff, 1309 ff.

259 Vgl. Kark, Compliance-Risikomanagement, 3. Aufl. 2024, Rn. 810 ff.

Compliance-Risikomanagements an veränderte Umstände. Frequenz und Umfang der sog. „Compliance Audits“ richten sich nach den jeweiligen Besonderheiten des Unternehmens. So folgt aus § 91 Abs. 2 AktG, § 317 Abs. 4 HGB für börsennotierte Aktiengesellschaften, dass eine Prüfung der Einhaltung und der Wirksamkeit des Compliance Managements mindestens einmal jährlich erfolgen sollte.²⁶⁰ Da das System nach § 91 Abs. 2 AktG zumindest teilweise mit einem Compliance-Verfahren identisch ist, sind Teilaspekte des Compliance Managements so zu aktualisieren, dass sie nicht bei der jährlichen Prüfung durch den Wirtschaftsprüfer beanstandet werden können.²⁶¹ Bei kleineren Gesellschaften kann dagegen eine Überprüfung in größeren Abständen ausreichend sein, etwa wenn das Umfeld des Unternehmens keinen größeren Änderungen unterworfen ist und es auch in der Vergangenheit nicht zu Fällen von „Non-Compliance“ im Unternehmen gekommen ist.²⁶² Für alle Unternehmen können sich allerdings besondere Anforderungen an ein Compliance-Audit aus einzelnen Rechtsgebieten ergeben, beispielsweise erfordert der Datenschutz eine Folgeabschätzung und ein spezielles Audit.²⁶³

3. Förderung und Incentivierung von Regeltreue (Compliance-Kultur)

Für den Erfolg von Compliance-Maßnahmen und Compliance-Management-Systemen gilt die sog. **Compliance-Kultur** als wichtiger Erfolgsfaktor.²⁶⁴ Auch der vom Institut der Wirtschaftsprüfer veröffentlichte IDW PS 980²⁶⁵ nennt die Compliance-Kultur als erstes Grundelement für die Bewertung der Angemessenheit und Wirksamkeit eines CMS.²⁶⁶ Die Compliance-Kultur behandelt die Frage, inwieweit Rechtstreue bzw. Regelbefolgung als Wert von allen Organisationsangehörigen akzeptiert, geachtet und getragen wird.²⁶⁷ Sie indiziert die **Bereitschaft zu regelkonformem und integrem Verhalten** ebenso wie die Tole-

68

260 Nach diesen Vorschriften unterliegt das Verfahren zur Erkennung existenzgefährdender Risiken einer Aktiengesellschaft der jährlichen Prüfung durch einen Wirtschaftsprüfer, *Liese/Schulz*, BB 2012, 1347, 1352.

261 *Liese/Schulz*, BB 2011, 1347, 1352.

262 *Liese/Schulz*, BB 2011, 1347, 1352.

263 Zum Datenschutz im Compliance Management vgl. → *Becker/Böhlke/Fladung*, Kap. 12.

264 Vgl. *Gösswein*, CCZ 2017, 43; *Moosmayer*, Compliance, 3. Aufl. 2015, Rn. 144 ff.; *Schulz/Muth*, CB 2014, 265; *Bode*, Compliance-Kultur, in: Bay/Hastenrath (Hrsg.), Compliance-Management-Systeme, 2. Aufl. 2016, Rn. 1 ff.

265 IDW-Prüfungsstandard „Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen“ (IDW PS 980), WPg Supplement 2/2011, 78 ff.

266 Vgl. IDW PS 980, Tz. 23, und hierzu *Bergmann*, Elemente eines wirksamen Compliance-Management-Systems, in: KPMG AG (Hrsg.), Das wirksame Compliance-Management-System, 1. Aufl. 2014, S. 11 ff.

267 *Schulz/Muth*, CB 2014, 265; ähnlich *Siedenbiedel*, Corporate Compliance, S. 251 ff.; *Bode*, Compliance-Kultur, in: Bay/Hastenrath, Compliance-Management-Systeme, Rn. 1 ff., sowie *Wendt*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 49 Rn. 24 ff.

ranz oder Indifferenz gegenüber Regelverstößen.²⁶⁸ Die Beachtung und Einhaltung von Regelungen steht in engem Zusammenhang mit der Unternehmenskultur als der Gesamtheit gemeinsamer Werte, Normen, Traditionen und Einstellungen, welche die Entscheidungen und das Verhalten der Organisationsmitglieder prägen.²⁶⁹ Die Prägung der **Unternehmenskultur** wird als zentrales Element des sogenannten „normativen Managements“ angesehen und ist Teil der Unternehmensstrategie.²⁷⁰ Im Hinblick auf die Compliance-Kultur kommt es dementsprechend darauf an, die richtigen Rahmenbedingungen und **Anreize** für ein regelkonformes Verhalten der Unternehmensangehörigen zu setzen.²⁷¹

aa) Compliance Commitment durch die Unternehmens- und Verbandsleitung

- 69 Es besteht Konsens, dass die Compliance-Kultur maßgeblich durch die **Grundeinstellungen** und **Verhaltensweisen** der Mitglieder der **Leitungsorgane** (Geschäftsleitung und ggf. Aufsichtsorgan) geprägt wird.²⁷² Für den Erfolg des Compliance Managements ist daher ausschlaggebend, dass die Unternehmensleitung selbst von Sinn und Notwendigkeit der Compliance-Maßnahmen überzeugt ist. Diese Überzeugung muss in jeder Kommunikation, aber auch im Verhalten eines jeden Mitglieds der Unternehmensleitung ihren Ausdruck finden („**Tone at the Top**“).²⁷³ Für die Entwicklung einer Compliance-Kultur ist es so dann wichtig, dass die Mitglieder der Geschäftsleitung die eigene **Überzeugung** von Sinn und Notwendigkeit des Compliance Managements in das Unternehmen transportieren – „gelebte Compliance“ bedeutet insoweit vor allem „**vorgelebte Compliance**“. So sollte die Bedeutung von Compliance konsequent an alle Unternehmensangehörigen (Führungskräfte und Mitarbeitende) vermittelt, aber auch an sonstige Bezugsgruppen (Mitarbeitende, Kunden, Lieferanten, Investoren) eindeutig und unmissverständlich kommuniziert werden („**Tone from the**

268 Vgl. Schulz/Muth, CB 2014, 265; Bergmann, Elemente eines wirksamen Compliance-Management-Systems, in: KPMG AG (Hrsg.), Das wirksame Compliance-Management-System, 1. Aufl. 2014, S. 11.

269 Zur Unternehmenskultur grundlegend Schein, Organisationskultur; vgl. ferner Waxenberger, Integritätsmanagement, S. 152 f.; Dillerup/Stoi, Unternehmensführung, S. 135; Siedenbiedel, Corporate Compliance, S. 252; Helisch, CB 2014, 225 ff.

270 Vgl. Hungenberg, Strategisches Management in Unternehmen, S. 23 ff.; Eichler, ZCG 2010, 57, 60 ff.

271 Vgl. für kartellrechtliche Compliance-Programme van Vormizeele, CCZ 2009, 41, 42, sowie allgemein Moosmayer, Compliance, Rn. 1 ff., 144 ff.

272 Vgl. Clodius, Grundlagen zu Compliance Management Systemen, in: Umnuß, Corporate Compliance Checklisten, § 4, Rn. 11; Pauthner-Seidel/Stephan, in: Hauschka/Moosmayer/Lösler, Corporate, Compliance, § 27 Rn. 59; Bode, Compliance-Kultur, in: Bay/Hastenrath, Compliance-Management-Systeme, Rn. 1 ff.

273 Vgl. zum sog. „Tone at the Top“ und zur Vorbildfunktion der Führungskräfte etwa Johannes Dittrich/Matthey, in: Moosmayer/Lösler, Corporate Compliance, § 24 Rn. 53; Rieder/Falge, Grundlagen für Compliance, in: Inderst/Bannenberg/Poppe, Compliance, Rn. 48; Bode, Compliance-Kultur, in: Bay/Hastenrath, Compliance-Management-Systeme, Rn. 1, 5 ff.

Top“.²⁷⁴ Das authentische „**Commitment**“ zu Compliance und Integrität, also ein ausdrücklich formuliertes und kommuniziertes Bekenntnis der Unternehmensleitung, bildet ein zentrales Element zur Förderung einer Compliance-Kultur.²⁷⁵ Für die Glaubwürdigkeit ist entscheidend, dass Regeltreue und Integrität auch und insbesondere in Zweifelsfällen stets den Vorrang genießen und nicht aus Opportunitätsgründen anderen Interessen geopfert werden. Hinzukommen sollte die **Selbstverpflichtung** der Unternehmensleitung, Regelverletzungen keinesfalls tatenlos hinzunehmen, sondern festgestellte Verstöße ausnahmslos und angemessen zu sanktionieren.²⁷⁶ Umgekehrt sollte regelkonformes und integrires Verhalten der Unternehmensangehörigen, das sich in Konfliktsituationen bewährt, besonders honoriert werden – die Geschäftsleitung sollte hierfür ein entsprechendes **Anreizsystem** konzipieren.²⁷⁷ Insgesamt sollte deutlich werden, dass im Interesse eines regelkonformen und integren Verhaltens im Zweifelsfall auch wirtschaftliche Einbußen in Kauf genommen werden müssen.²⁷⁸

Eine Chance, das besondere Compliance Commitment zu verdeutlichen, liegt in der Formulierung des Unternehmensleitbilds („**Mission Statement**“) etwa in der Weise, dass der unternehmerische Erfolg stets auf der Achtung rechtlicher Vorgaben und integrem Geschäftsverhalten basiert – das Leitbild dient der schriftlichen Fixierung der Unternehmensmission, welche Unternehmensziele, Unternehmenswerte, Unternehmenskultur und Unternehmensverfassung zusammenfasst.²⁷⁹ Es empfiehlt sich, ausgewählte Vertreter (Führungskräfte, Delegierte von Abteilungen etc.) bei der Entwicklung und Formulierung des Leitbildes einzubeziehen, um Verständnis und **Akzeptanz** bei den Unternehmensangehörigen zu erreichen.²⁸⁰ **70**

bb) Akzeptanz als Grundlage der Regelbefolgung

Die Wirksamkeit von Compliance-Maßnahmen hängt dabei auch von der Bereitschaft der Betroffenen ab, die Regeln und Maßnahmen zu befolgen.²⁸¹ Untersu- **71**

274 Vgl. Moosmayer, Compliance, Rn. 144 ff.; Johannes Dittrich/Matthey, in: Moosmayer/Lösler, Corporate Compliance, § 24 Rn. 52 ff.

275 Vgl. Moosmayer, Compliance, Rn. 144; Johannes Dittrich/Matthey, in: Moosmayer/Lösler, Corporate Compliance, § 24 Rn. 52 ff.

276 Vgl. Volz, Praxisbericht Compliance, in: Teichmann (Hrsg.), Compliance, S. 1, 4 f.

277 Zur Schaffung positiver Anreize für integrires Verhalten vgl. Heißner, Erfolgsfaktor Integrität, S. 137 f.; Schaupensteiner, NZA-Beil. 2011, 8, 12; Bussmann, CCZ 2016, 50, 55; Hastenrath/Müller, CB 2017, 154.

278 Vgl. Itzen, BB-Special Compliance 2008, 12, 14; Schaupensteiner, NZA-Beil. 2011, 8, 12.

279 Vgl. Dillerup/Stoi, Unternehmensführung, S. 160 ff. Das „Mission Statement“ dient dazu, das in der Vision verkörperte Zukunftsbild des Unternehmens in Unternehmensgrundsätze und Leitlinien umzusetzen, vgl. etwa Hungenberg, Strategisches Management in Unternehmen, S. 26 f.

280 Vgl. Schulz/Muth, CB 2014, 265; Bode, Compliance-Kultur, in: Bay/Hastenrath, Compliance-Management-Systeme, Rn. 1 ff.

281 Zu Regelbefolgung und Integrität als Bestandteile der sog. „Compliance-Kultur“ siehe Wieland, Wittenberg – Prozess, CSR und Compliance – Die Zukunftsfähigkeit der sozialen

chungen haben gezeigt, dass ein **integrierter Ansatz** von Compliance- und Integritätsmanagement insofern erfolgsversprechender erscheint als ein rein regel- und kontrollbasierter Compliance-Ansatz, der allein auf die Umsetzung juristischer Vorgaben gerichtet ist.²⁸² In anderen Rechtsordnungen zählt die Kombination von Compliance und Ethikprogrammen bereits seit Längerem explizit zu denjenigen Kriterien, mit deren Nachweis Organisationen den Vorwurf mangelnder Compliance ausräumen können.²⁸³

- 72 Regelverletzungen beruhen einerseits auf **vorsätzlichem Fehlverhalten** bzw. kriminellen Aktivitäten von Personen (z. B. bei Korruptionsvergehen oder Kartellrechtsverstößen),²⁸⁴ in anderen Fällen resultieren sie aus **Fahrlässigkeit** aufgrund der Verletzung von Sorgfaltspflichten oder auch nur unzureichender Kenntnis von Regeln und Geboten.²⁸⁵ Die erforderlichen Compliance-Maßnahmen umfassen daher sowohl die Aufdeckung und Sanktionierung von regelwidrigem Verhalten als auch Aufklärungs- und Schulungsmaßnahmen, insbesondere die **Erklärung** und Übersetzung **juristischer Regeln** und Zusammenhänge in eine allgemeinverständliche Sprache und mit einem konkreten Bezug zu aktuellen Fragen der Unternehmenspraxis.²⁸⁶ Die Beachtung und Einhaltung von Regeln steht in einem engen **Zusammenhang mit den Werten**, denen sich die Organisationsangehörigen verpflichtet fühlen.²⁸⁷ Im Hinblick auf die Verhinderung

Marktwirtschaft, in: Wieland/Schack, Soziale Marktwirtschaft: Verantwortungsvoll gestalten, S. 14, 17. Ähnlich *Busmann*, CCZ 2016, 50, 53; *Bonenberger*, Wertemanagement, in: Jäger/Rödl/Campos Nave, Praxishandbuch Corporate Compliance, S. 419 ff. Vgl. ferner *Schaupensteiner*, NZA-Beilage 2011, 8, 12; *Busmann*, CCZ 2016, 50, 54 ff. Im Zusammenhang mit der Einführung eines Code of Conduct siehe → *Benkert*, Kap. 4.

- 282 Vgl. *Claussen*, Compliance- oder Integrity-Management, S. 187, 401 bzgl. des Vergleichs von Antikorruptionsprogrammen diverser deutscher Unternehmen. In dieselbe Richtung weisen die Ergebnisse diverser US-amerikanischer Untersuchungen von Compliance-Programmen, dargestellt bei *Pape*, CCZ 2009, 233 ff.; vgl. ferner *Faust*, Compliance und Korruptionsbekämpfung, S. 22 ff.; *Herb*, Handelsblatt Journal 2015, 17, sowie ausführlich *Wieland*, Integritäts- und Compliance-Management als Corporate Governance – konzeptionelle Grundlagen und Erfolgsfaktoren, in: Wieland/Steinmeyer/Grüniger, Handbuch Compliance-Management, S. 15 ff.
- 283 Siehe *Wieland*, Governancestrukturen des Gemeinwohls – Eine wirtschaftsethische Skizze, in: v. Kempf/Lüderssen/Volk (Hrsg.), Gemeinwohl im Wirtschaftsstrafrecht, S. 45, 51 ff. sowie *Hopson*, CCZ 2008, 208. Zur Relevanz kombinierter Compliance- und Integritätsansätze im US-amerikanischen Recht ausführlich *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 161 ff. sowie *Faber*, Anreizbasierte Regulierung von Corporate Compliance, S. 187 ff.
- 284 Zu den diversen Straftatbeständen im Bereich der Korruption vgl. → *Böttger*, Kap. 2 Rn. 36 ff. Zum Umgang mit Korruptionsrisiken in M&A-Transaktionen siehe → *Ullrich*, Kap. 26 Rn. 77. Zu den diversen Formen kartellrechtswidrigen Verhaltens siehe → *Seeliger/Mross/Seydel*, Kap. 27 Rn. 8 ff.
- 285 Vgl. *Heißner*, Erfolgsfaktor Integrität, S. 114; *Busmann*, CCZ 2016, 50 ff.; *Preusche/Würz*, Compliance, S. 30.
- 286 Vgl. *Moosmayer*, Compliance, Rn. 175 ff.; *Siedenbiedel*, Corporate Compliance, S. 57.
- 287 Vgl. *Wieland*, Integritäts- und Compliance-Management als Corporate Governance – konzeptionelle Grundlagen und Erfolgsfaktoren, in: Wieland/Steinmeyer/Grüniger, Handbuch

bzw. Reduzierung abweichenden Verhaltens und der Förderung von Regeltreue empfiehlt sich daher, die Compliance-Maßnahmen durch ein begleitendes **Integritätsmanagement** zu untermauern.²⁸⁸

cc) Kommunikation von Werten und Umgang mit „Regelungslücken“

Für eine Fundierung der Compliance-Maßnahmen durch ein begleitendes Integritätsmanagement spricht ferner, dass eine lückenlose Regelung jeglichen (Fehl-)Verhaltens faktisch unmöglich ist (ebenso wie deren Kontrolle). Soweit Regelungen verabschiedet werden – etwa in Form eines Code of Conduct²⁸⁹ –, sind die Aussagen nicht immer eindeutig oder selbsterklärend oder sie erfassen nicht alle Fallkonstellationen.²⁹⁰ Selbst bei regelmäßiger Erläuterung der Inhalte im Rahmen von Compliance-Schulungen²⁹¹ können Zweifelsfragen bestehen bleiben, die Erfüllung sämtlicher Rechtspflichten im operativen Geschäft ist stets eine Herausforderung.²⁹² Für diese Fälle hilft eine Orientierung, wie sich Unternehmensangehörige bei unklaren Sachlagen oder in sog. „Graubereichen“ verhalten sollten. Diese Orientierung kann durch ein begleitendes Integritäts- und Wertemanagement erfolgen, mit dem die Unternehmensangehörigen über Sinn und Zweck der Compliance-Maßnahmen und insbesondere deren Schutzfunktion für das Unternehmen und alle seine Stakeholder informiert werden.²⁹³ Die Formulierung von Werten gibt den Unternehmensangehörigen dabei eine wichtige Hilfestellung für diejenigen Fragen und Fallkonstellationen, die (noch) nicht bzw. nicht eindeutig durch Regeln erfasst bzw. geklärt sind.²⁹⁴ Dies befähigt die Unternehmensangehörigen in solchen Zweifelsfällen entweder zu einer selbstständigen Einschätzung²⁹⁵ oder es fungiert als eine Art Kompass, der in

73

Compliance-Management, S. 15 ff.; *Siedenbiedel*, Corporate Compliance, S. 251; *Bode*, Compliance-Kultur, in: *Bay/Hastenrath*, Compliance-Management-Systeme, Rn. 1 ff.; *Heißner*, Erfolgsfaktor Integrität, S. 174 f.

288 Zur Verknüpfung von Compliance- und Integritätsmanagements siehe *Wieland*, Integritäts- und Compliance-Management als Corporate Governance – konzeptionelle Grundlagen und Erfolgsfaktoren, in: *Wieland/Steinmeyer/Grüniger*, Handbuch Compliance-Management, S. 15 ff.

289 Zu den Wirksamkeitsvoraussetzungen und typischen Inhalten siehe ausführlich → *Benkert*, Kap. 4.

290 Vgl. *Wieland*, Integritäts- und Compliance-Management als Corporate Governance – konzeptionelle Grundlagen und Erfolgsfaktoren, in: *Wieland/Steinmeyer/Grüniger*, Handbuch Compliance-Management, S. 15.

291 Zu den Anforderungen an effektive Compliance-Schulungen ausführlich → *Hastenrath*, Kap. 6, sowie im Kontext der Kartellrechts-Compliance → *Seeliger/Mross/Seydel*, Kap. 27 Rn. 133 ff.

292 Vgl. *Bussmann*, CCZ 2009, 132, 137.

293 Siehe hierzu insbesondere *Wieland*, Integritäts- und Compliance-Management als Corporate Governance – konzeptionelle Grundlagen und Erfolgsfaktoren, in: *Wieland/Steinmeyer/Grüniger*, Handbuch Compliance-Management, S. 15 ff.; *ders.*, CCZ 2008, 15, 17.

294 Vgl. *Göbel*, Unternehmensethik, S. 263 ff.

295 Zur Orientierungsfunktion ethischer Prinzipien siehe *Waxenberger*, Integritätsmanagement, S. 52 ff., 111 ff.; *Göbel*, Unternehmensethik, S. 263 ff.

Zweifelsfällen auf eine Klärung der Frage durch den Compliance Officer verweist.

- 74 Die Fundierung der Compliance-Maßnahmen durch ein Integritäts- und Wertemanagement²⁹⁶ bietet zugleich die Chance einer höheren Akzeptanz von Compliance-Maßnahmen. So verabschieden beispielsweise viele Unternehmen im Rahmen ihrer Anti-Korruptions-Maßnahmen sog. „Geschenke-Richtlinien“ zur Regelung der Gewährung und Annahme von Vergünstigungen. Die Prävention von Korruptionsrisiken jedoch dürfte besser gelingen, wenn gleichzeitig Unbestechlichkeit und faires Wettbewerbsverhalten als Werte durch die Unternehmensleitung und die Führungskräfte kommuniziert werden. Denn mit dieser Verankerung erhöht sich die Chance, dass Vergünstigungen jeder Art kritisch geprüft werden – auch unabhängig von der Frage, ob die jeweilige Zuwendung im Einzelfall durch die „Geschenke-Richtlinie“ geregelt ist.
- 75 Zur Förderung der Compliance-Kultur ist auch zu erwägen, positive Anreize für regeltreues und integrires Verhalten zu schaffen.²⁹⁷ Hierfür gibt es zahlreiche Möglichkeiten, wie die Aufnahme von Compliance-Themen in Leistungs- und Zielvereinbarungen, die Nominierung ausgewählter Unternehmensangehöriger als sog. „Compliance-Botschafter“ oder die Gestaltung besonderer Workshops zu Compliance-Themen.²⁹⁸ Entscheidend ist, dass Mitarbeiter mit einem regelkonformen und integren Verhalten Karriere machen können²⁹⁹ und nicht etwa falsche Anreize bestehen, die Fälle von Non-Compliance begünstigen (etwa im Sinne unreflektierter finanzieller Zielvorgaben).³⁰⁰ Compliance-gerechte und integrierte Verhaltensweisen (sowie deren Wertschätzung durch die Unternehmensleitung) müssen darüber hinaus fester Bestandteil der Aus- und Fortbildung von Unternehmensangehörigen sein.³⁰¹

4. Verfassung von Regeln, Richtlinien und Werten

- 76 Dem Wort in Form eines eindeutigen Bekenntnisses der Unternehmensleitung zu Compliance sollten Taten, u. a. auch durch eine verständliche und praxis-

296 Vgl. *Wieland*, Integritäts- und Compliance-Management als Corporate Governance – konzeptionelle Grundlagen und Erfolgsfaktoren, in: *Wieland/Steinmeyer/Grüniger*, Handbuch Compliance-Management, S. 15, 23 ff. Siehe ferner *Schneider*, ZIP 2003, 645 ff., sowie *Kort*, NZG 2008, 81 ff. Zum Zusammenhang zwischen Compliance und Integrität ferner *Heißner*, Erfolgsfaktor Integrität, S. 113 ff. sowie unter → Rn. 76 ff.

297 Zu Anreizmöglichkeiten für Compliance-gerechtes Verhalten ausführlich *Hastenrath/Müller*, CB 2017, 154 ff.

298 Vgl. *Hastenrath/Müller*, CB 2017, 154 ff.; *Ewelt-Knauer*, Proaktive Gestaltung der Compliance-Kultur, WPg 2016, 597 ff.

299 Vgl. *Bussmann*, CCZ 2016, 50 ff., 55.

300 Vgl. *Schulz*, BB 2018, 1285, 1286; *Gösswein*, CCZ 2017, 43.

301 Vgl. *Nezmeskal-Berggötz*, Integritätsmanagement und Social Compliance bei Deutsche Post DHL Group, in: *Wieland/Steinmeyer/Grüniger*, Handbuch Compliance-Management, S. 709, 720 ff. Zur Gestaltung von Compliance-Schulungen siehe → *Hastenrath*, Kap. 6, sowie im Zusammenhang mit dem Kartellrecht → *Seeliger/Mross/Seydel*, Kap. 27 Rn. 133 ff.

orientierte Formulierung von Compliance-Regeln und Leitwerten folgen.³⁰² Dabei empfiehlt sich die Entwicklung einer Art „Compliance-Verfassung“, in der sämtliche relevanten Regeln, Standards und Werte integriert und aufeinander abgestimmt werden.³⁰³ Als Mittel zur Kommunikation nutzen viele Unternehmen einen sog. „Code of Conduct“.³⁰⁴ Dieser statuiert maßgebliche Regelungen und grundlegende Werte und formuliert die Verhaltensanforderungen, deren Einhaltung von den Unternehmensangehörigen erwartet wird. Typische Inhalte sind unter anderem Regelungen zum respektvollen und fairen Umgang der Unternehmensangehörigen untereinander, zum Schutz vor Diskriminierung, zum Ausschluss von Bestechlichkeits- oder Bestechungsverhalten, Anweisungen zur Wahrung von Vertraulichkeit und Datenschutz, Regelungen zum Ausschluss von Interessenkonflikten, Anweisungen zum Umgang mit Geschenken und Einladungen sowie Prinzipien des fairen Umgangs mit Geschäftspartnern.³⁰⁵

5. Unabhängige Positionierung der Compliance Officer

Angesichts der vielfältigen, weiter wachsenden Rechtspflichten und daraus resultierenden Compliance-Risiken empfiehlt es sich für viele Unternehmen, eine eigene Stelle für Compliance Management bzw. einen Compliance Officer zu etablieren, der die vielfältigen Anforderungen im Rahmen eines eigenständigen Aufgabenbereichs koordiniert.³⁰⁶ Soweit Unternehmen Compliance Officer beschäftigen, spielen diese bei der Einführung und der dauerhaften Implementierung des Compliance Managements eine Schlüsselrolle. Das Aufgabenspektrum der Compliance Officer ist vielfältig,³⁰⁷ dennoch lassen sich einige typische Aufgaben beschreiben, die unabhängig von den Besonderheiten des jeweiligen Unternehmens oder speziellen Branchenvorgaben gelten und sich an den Zielen und Funktionen von Compliance Management orientieren.³⁰⁸ Zu diesen Aufgaben der Compliance Officer gehört die umfassende Beratung der Geschäftsleitung hinsichtlich aller für das Unternehmen relevanter Normen (Gesetze, Richtlinien und Verhaltensstandards) und hinsichtlich der Prävention bzw. Eva-

77

302 Vgl. Lampert, Compliance-Organisation, in: Hauschka, Corporate Compliance, 2. Aufl. 2010, 163 ff., 170 ff.

303 Zu dieser integrierten „Kodifikation“ relevanter Regelungen und Werte ausführlich Grüninger, Werteorientiertes Compliance Management System, in: Wieland/Steinmeyer/Grüninger, Handbuch Compliance-Management, S. 41 ff., 63 f.

304 Zu Grundfragen und Gestaltung eines Code of Conduct siehe ausführlich → Benkert, Kap. 4.

305 Zu Grundfragen und Gestaltung eines Code of Conduct siehe ausführlich → Benkert, Kap. 4. Zu typischen Inhalten siehe ferner Inderst, Compliance Organisation und praktische Umsetzung, in: Inderst/Bannenberg/Poppe, Compliance, S. 130 ff.

306 Zu Funktion und Aufgaben der Compliance Officer siehe Schulz/Galster, in: Bürkle/Hauschka/Schieffer, Der Compliance Officer, § 3; Bürkle/Kinzl, in: Moosmayer/Lösler, Corporate Compliance, § 12.

307 Vgl. Schulz/Galster, in: Bürkle/Hauschka/Schieffer, Der Compliance Officer, § 3 Rn. 30 ff.

308 Zur Rolle der Compliance-Funktion in einem Kreditinstitut siehe ausführlich → Renz/Frankenberger, Kap. 20.

luierung sowie Bewältigung von Compliance-Risiken.³⁰⁹ Eine weitere wichtige Aufgabe besteht in der Steuerung von relevanten Informationsflüssen (**Informations- und Wissensmanagement**).³¹⁰ Der Compliance Officer fungiert dabei als „Informationsschnittstelle“.³¹¹ Dabei sollte der Compliance Officer einerseits alle relevanten Informationen bzw. entsprechende Informationszugriffsrechte in Bezug auf Compliance-Themen erhalten.³¹² Ein funktionierendes Informations- und Wissensmanagement ist auch die Grundlage für die erfolgreiche Kommunikation von Compliance-Themen und entsprechende Schulungsmaßnahmen.³¹³ Zu den Aufgaben der Compliance Officer gehören ferner Überwachungs- und Kontrollpflichten bezüglich compliance-relevanter Vorgaben sowie Berichts- und Dokumentationspflichten hinsichtlich aller Compliance-Themen.³¹⁴

6. Verständliche Schulungen und Fortbildungsprogramme

- 78 Über die Formulierung und Verabschiedung von Compliance-Regeln und Leitwerten (z. B. in Form von Verhaltenskodizes, Compliance Manuals und Richtlinien³¹⁵) hinaus bedarf es weiterer Schritte zur dauerhaften Verankerung bei den Unternehmensangehörigen, die Vermittlung von Compliance und Integrität ist eine Personalführungsaufgabe.³¹⁶

a) Bedarfsanalyse und Zielgruppenorientierung

- 79 Wichtig ist insbesondere ein zielgenaues und fortlaufend aktualisiertes Schulungs- und Fortbildungsprogramm.³¹⁷ Dabei kommt es darauf an, die Unternehmensangehörigen für die Compliance-Risiken des Geschäftsmodells zu sensibilisieren. Denn obwohl Regelverstöße häufig auch auf krimineller Energie einzelner Personen fußen, resultieren andere Fälle der „Non-Compliance“ daraus, dass die Relevanz einschlägiger Regelungen nicht bekannt ist oder nicht verstanden wurde. Daher müssen die Compliance-Risiken und daraufhin entwickelte Compliance-Maßnahmen in verständlicher Sprache erläutert und (insbesondere im Falle juristischer Fachterminologie) in gut nachvollziehbare Formulierungen übersetzt werden.³¹⁸ Hierzu sollten spezielle Aus- und Fortbil-

309 Vgl. *Moosmayer*, Compliance, Rn. 124 ff.; *Groß*, Chief Compliance Officer, S. 75 f. m. w. N.

310 Vgl. *Klopp*, Der Compliance-Beauftragte, S. 94 ff.

311 *Schulz/Renz*, BB 2012, 2511, 2514 ff.

312 *Schulz/Renz*, BB 2012, 2511, 2514 ff.

313 Vgl. *Klopp*, Der Compliance-Beauftragte, S. 87 ff.

314 Vgl. *Klopp*, Der Compliance-Beauftragte, S. 92 ff., 211 ff.

315 Vgl. *Kreßel*, NZG 2018, 841.

316 So wörtlich und zutreffend *Heißner*, Erfolgsfaktor Integrität, S. 114.

317 Zu den Anforderungen an effektive Compliance-Schulungen ausführlich → *Hastenrath*, Kap. 6, *Schulz/Galster*, in: *Bürkle/Hauschka/Schieffer*, Der Compliance Officer, § 3 Rn. 56 ff. sowie im Kontext der Kartellrechts-Compliance → *Seeliger/Mross/Seydel*, Kap. 27 Rn. 133 ff.

318 Vgl. → *Hastenrath*, Kap. 6.

dungsmaßnahmen entwickelt werden, die genau auf das Geschäftsmodell des Unternehmens und sein spezifisches Compliance-Risiko-Profil abgestimmt sind.³¹⁹ Für den Erfolg der Schulungs- und Fortbildungsmaßnahmen ist ferner ausschlaggebend, dass die Formate und Inhalte möglichst genau auf den jeweiligen Bedarf der adressierten Zielgruppen abgestimmt sind.³²⁰

b) Positionierung von Compliance als „Business Enabler“

Bei der Durchführung von Schulungs- und Fortbildungsmaßnahmen ist einerseits auf Verständlichkeit und Praxisnähe zu achten, Juristen sind hier vor allem als „Übersetzer“ komplexer Rechtsthemen in alltagstaugliche und nachvollziehbare Zusammenhänge gefragt. Andererseits ist dringend anzuraten, Compliance nicht pauschal als Funktion der „Geschäftsverhinderung“ darzustellen. In Fällen, in denen Geschäfte und Transaktionen aus Compliance-Gründen nicht durchgeführt werden dürfen, müssen die Gründe daher nachvollziehbar und konsistent erklärt werden.³²¹ Soweit wie möglich sollte ferner eine positive Vorstellung davon vermittelt werden, unter welchen Bedingungen ein abgelehntes Geschäft entweder in eingeschränktem Umfang oder nach inhaltlicher Änderung zulässig sein könnte.³²² **80**

c) Regelmäßige Anpassung der Fortbildungsformate

Aufgrund des oben beschriebenen komplexen und dynamischen regulatorischen Umfelds müssen die Schulungs- und Fortbildungsinhalte regelmäßig aktualisiert und fortlaufend an neue Rechtsentwicklungen angepasst werden. Nur so erhalten die Unternehmensangehörigen die Möglichkeit, sich regelmäßig auf ein geändertes rechtliches Umfeld einzustellen, um Compliance-Risiken erkennen und vermeiden zu können. Zur Erläuterung aktueller Compliance-Themen und der Klärung von Zweifelsfragen trägt ferner die Einrichtung einer Beratungsstelle („Compliance-Helpline“) bei, an die sich alle Unternehmensangehörigen in Compliance-Fragen wenden können.³²³ **81**

d) Aktive Einbeziehung der Stakeholder

Um einen direkten Unternehmensbezug der Compliance-Schulungen und Fortbildungsformate zu gewährleisten, bietet sich die (selektive) Einbeziehung von Unternehmensangehörigen bei der Entwicklung und Durchführung von Schulungsmaßnahmen an.³²⁴ Diese aktive Einbeziehung, etwa durch Repräsentanten unterschiedlicher Unternehmenseinheiten, fördert die Attraktivität und Akzeptanz der Fortbildungsformate, da diese weniger als von „oben verordnet“ als **82**

319 Siehe im Einzelnen hierzu → *Hastenrath*, Kap. 6

320 Vgl. → *Hastenrath*, Kap. 6 m. w. N.

321 *Ritzenhoff/Sonnenberg/Schulz*, CB 2019, 1, 3.

322 *Ritzenhoff/Sonnenberg/Schulz*, CB 2019, 1, 2.

323 Diese Beratungsfunktion nimmt in vielen Unternehmen der Compliance Officer wahr, vgl. *Groß*, Chief Compliance Officer, S. 80 f.

vielmehr als „Eigenentwicklung“ wahrgenommen werden. Die gezielte Beteiligung ausgewählter Mitarbeiter und Führungskräfte an der Entwicklung und Durchführung von Compliance-Schulungen ist gleichzeitig ein wichtiger Beitrag zu Förderung der Compliance-Kultur.

7. Integration von Compliance-Themen in die Geschäftsprozesse

- 83 Ein weiterer Erfolgsfaktor für funktionierendes Compliance Management ist die **Integration** von Compliance-Themen und Maßnahmen in die **Geschäftsprozesse**. In kleineren und mittelständischen Unternehmen ist diese Verankerung von essenzieller Bedeutung, da spezialisierte Funktionen zur Wahrnehmung von Compliance-Aufgaben wie Rechtsabteilung, Risikomanagement oder Revision häufig fehlen. Wie im Zusammenhang mit dem Risikomanagement (und dem GRC-Ansatz) ausgeführt (siehe oben → Rn. 50), ist die proaktive Einbeziehung der operativen Einheiten (als sog. „first line of defense“) wichtig, da die dort tätigen Mitarbeiter als „**Process Owner**“ jeweils über umfangreiches Wissen über die spezifischen Compliance-Risiken verfügen. So kann es sich etwa zur Steuerung der Compliance-Risiken im operativen Betrieb empfehlen, durch spezifische Risikoanalysen und Kontrollen bestimmte Prozesse mit besonderen Compliance-Risiken (z. B. im Einkauf und Vertrieb) systematisch daraufhin zu untersuchen, inwieweit gegen bestehende Regeln verstoßen werden könnte (z. B. bei der Vergabe von Aufträgen im Einkaufsprozess).³²⁵ Je nach Untersuchungsergebnis können dann spezifische Maßnahmen zur Prävention von Fehlverhalten eingeführt werden, wie beispielsweise besondere Kontroll-, Dokumentations- oder Freigabeprozesse.³²⁶ Bei der Zusammenarbeit mit Lieferanten kann es sich anbieten, diese durch einen Auswahlprozess (unter Einbeziehung von Compliance- und Integritätsaspekten) zu selektieren und durch einen separaten Verhaltenskodex auf rechtskonformes Verhalten und bestimmte ethische Grundsätze zu verpflichten.³²⁷
- 84 Auch unabhängig von den besonderen Anforderungen der **Lieferketten-Compliance**³²⁸ empfiehlt sich im Zusammenhang mit den Geschäftspartnern des Unternehmens die Durchführung einer sog. „**Third Party Due Diligence**“ vor Ab-

324 Vgl. Schulz/Galster, in: Bürkle/Hauschka/Schieffer, Der Compliance Officer, § 3 Rn. 57. Zu verschiedenen Schulungsmöglichkeiten und -formaten ausführlich → Hastenrath, Kap. 6.

325 Vgl. Schulz/Muth, CB 2014, 265, 268.

326 Siehe hierzu Bicker/Stoklasa, BB 2018, 519, 521 ff.

327 Zur Kontrolle von (Sub-)Lieferanten siehe → Schleper/Förstl, Kap. 17 sowie Nezmeskal-Berggötz, Integritätsmanagement und Social Compliance bei Deutsche Post DHL Group, in: Wieland/Steinmeyer/Grüninger, Handbuch Compliance-Management, S. 709, 723 f.; Schröder, CCZ 2013, 74 unter Hinweis auf die vom Bundesverband für Materialwirtschaft, Einkauf und Logistik e. V. (BME) formulierten Anforderungen an einen Compliance-/CSR-Prozess im Lieferantenmanagement.

328 Zu den LkSG-Sorgfaltspflichten → Heske, Kap. 18. Vgl. ferner Schröder/Schulz, Praxisleitfaden Supply Chain Compliance, Rn. 52 ff.

schluss von Transaktionen.³²⁹ Dieses besondere Verfahren zur Einschätzung und Steuerung von Compliance-Risiken spielt angesichts der Integration vieler Unternehmen in komplexe Wertschöpfungsketten³³⁰ und damit verbundenen Verantwortungszuweisungen eine immer größere Rolle.

8. Koordination der Zusammenarbeit mit anderen Unternehmensfunktionen

Wie gezeigt, gibt es für die Wahrnehmung von Compliance-Aufgaben kein einheitliches Modell, sondern – je nach Unternehmenssituation – viele unterschiedliche Gestaltungen, bei denen häufig andere Unternehmensfunktionen (z.B. Rechtsabteilung, Risikomanagement und interne Revision) oder Unternehmensbeauftragte (z.B. Datenschutzbeauftragte, Arbeitssicherheitsbeauftragte, Exportkontrollbeauftragte) bestimmte Compliance-Aufgaben (mit-)erfüllen.³³¹ Im Hinblick auf die Wirksamkeit des Compliance Managements ist eine effiziente Koordination der verschiedenen Kompetenzen und Aktivitäten wichtig (sog. „**Schnittstellenmanagement**“).³³² Dabei ist darauf zu achten, dass im Unternehmen vorhandene Erfahrungen und Kompetenzen zu Compliance-Fragen abteilungsübergreifend erfasst und integriert werden.³³³ **85**

9. Einrichtung von wirksamen Kontrollen und Feedback-Prozessen

Um sicherzustellen, dass die relevanten Compliance-Regeln und Prinzipien in allen Unternehmensbereichen und von allen Unternehmensangehörigen tatsächlich eingehalten werden, ist eine **systematische** Überwachung und **Kontrolle** unabdingbar – das Compliance-System ist nur so gut wie seine beste Kontrolle.³³⁴ Dabei ist zunächst zu beachten, dass die primäre Kontroll- und Überwachungspflicht grundsätzlich bei der Geschäftsleitung verbleibt, einzelne Kontroll- und Überwachungsaufgaben können aber an den Compliance Officer delegiert werden.³³⁵ Umfang und Ausgestaltung der erforderlichen Aufgaben und Maßnahmen richten sich wiederum nach den individuellen Besonderheiten **86**

329 Vgl. *Schürle/Olbers*, CCZ 2010, 102, 104 sowie *Bicker/Stoklasa*, BB 2018, 519. Zur Compliance-Due Diligence bei M&A-Transaktionen siehe ausführlich → *Ullrich*, Kap. 26.

330 Zu den komplexen Anforderungen einer „Sustainable Corporate Governance“ siehe *Spießhofer*, in: *Moosmayer/Lösler*, Corporate Compliance, 4. Aufl. 2024, § 16. Zu Compliance im Kontext des sog. Supply Chain Managements siehe → *Schleper/Förstl*, Kap. 17.

331 Vgl. *Moosmayer*, Compliance, Rn. 105 ff.

332 Zum erforderlichen Zusammenwirken unterschiedlicher Unternehmensfunktionen einem „Schnittstellen-Management“ siehe → *Rau*, Kap. 3.

333 Vgl. v. *Marnitz*, Compliance-Management für mittelständische Unternehmen, S. 95; *Schulz*, CB 2015, 309.

334 Vgl. die pointierte Formulierung von *Inderst*, in: *Inderst/Bannenberg/Poppe*, Compliance, S. 148; vgl. ferner *Rieder/Falge*, ebenda, 32 ff.

335 Zur Überwachung und Kontrolle der Compliance als Pflicht der Unternehmensleitung vgl. etwa *Karbaum*, AG 2013, 863, 871; *Schulz/Renz*, BB 2012, 2511, 2514.

des Unternehmens und dessen **Compliance-Risiko-Struktur**.³³⁶ Jedoch ist stets darauf zu achten, dass die entsprechenden Kontrollmaßnahmen regelkonform sind: Bei Kontrollen sind fast immer personenbezogene Daten betroffen, so dass beispielsweise die Vorgaben des Datenschutzrechts zu berücksichtigen sind.³³⁷

10. Aufklärung von Verstößen und Betrieb von Hinweisgebersystemen

- 87 Auch die Aufdeckung und Aufklärung von Compliance-Verstößen ist ein wichtiges Element des Compliance Managements.³³⁸ Denn einerseits gibt es in jedem Unternehmen Fälle vorsätzlicher Regelverletzungen, andererseits kann auch die beste Schulung fahrlässige Regelverstöße nicht absolut ausschließen. Zur **Aufdeckung von Regelverletzungen** nutzen daher bereits vor Inkrafttreten des Hinweisgeberschutzgesetzes viele Unternehmen sog. **Hinweisgebersysteme** (z. B. durch den Einsatz von Ombudspersonen oder durch sog. „Whistleblowing-Systeme“).³³⁹ Hinweisgebersysteme spielen eine wichtige Rolle bei der Aufklärung von „Non-Compliance“, denn dadurch sollen die Unternehmensangehörigen (sowie gegebenenfalls weitere Stakeholder) die Möglichkeit zu (auch anonymen) Hinweisen auf Regelverstöße erhalten.³⁴⁰ Die Ausgestaltung im Einzelnen richtet sich nach den Vorgaben der einschlägigen Vorschriften wie insbesondere des **Hinweisgeberschutzgesetzes**; in jedem Fall ist die Einhaltung relevanter arbeitsrechtlicher und datenschutzrechtlicher Vorgaben zu beachten.³⁴¹

11. Konsequente Sanktionierung von regelwidrigem Verhalten

- 88 Für den Erfolg des Compliance Managements ist die konsequente Sanktionierung festgestellter Regelverletzungen nicht zu unterschätzen. Denn der Umgang mit aufgedeckter „Non-Compliance“ wird von den Unternehmensangehörigen unmittelbar registriert und kann erhebliche Auswirkungen auf die Integritäts- und **Compliance-Kultur** haben.³⁴² Sofern die Geschäftsleitung Regelverstöße toleriert oder nicht mit genügendem Nachdruck verfolgt, kann bei vielen Unter-

336 Vgl. Schulz/Galster, in: Bürkle/Hauschka/Schieffer, Der Compliance Officer, § 3 Rn. 34 f.

337 Zum Datenschutz im Compliance Management vgl. → Becker/Böhlke/Fladung, Kap. 12.

338 Vgl. Rieder/Falge, in: Inderst/Bannenberg/Poppe, Compliance, S. 27 f. sowie Seibt, in: Schmidt/Lutter (Hrsg.), AktG, § 76 Rn. 28 f.

339 Zu Aufbau und Funktion von Whistleblowing-Systemen ausführlich → Block/Sonnenberg, Kap. 5. Zur Beachtung der dabei maßgeblichen datenschutzrechtlichen Vorgaben → Becker/Böhlke/Fladung, Kap. 12 Rn. 185 ff.

340 Zu empirischen Daten für die Aufdeckung von Straftaten durch Hinweisgeber siehe bereits Strauss, ZRfC 2014, 164 m. w. N.

341 Schulz/Galster, in: Bürkle/Hauschka/Schieffer, Der Compliance Officer, § 3 Rn. 66. Zu mitbestimmungsrechtlichen Erfordernissen vgl. Neufeld/Knitter, BB 2013, 821, 822 f.; zu datenschutzrechtlichen Aspekten → Becker/Böhlke/Fladung, Kap. 12 Rn. 185 ff.

342 Zum „ethical leadership“ vgl. Bussmann, CCZ 2016, 50, 54 ff., sowie ähnlich Wieland, Integritäts- und Compliance-Management als Corporate Governance – konzeptionelle Grundlagen und Erfolgsfaktoren, in: Wieland/Steinmeyer/Grüniger, Handbuch Compliance-Management, S. 15 ff.

nehmensangehörigen der fatale Eindruck entstehen, Compliance sei nur ein „Lippenbekenntnis“. Dieser Eindruck kann die konzeptionellen Bemühungen vollständig konterkarieren, da sich manche die Frage stellen werden, ob sich ein regelkonformes Verhalten überhaupt lohnt. Im Compliance Management bestätigt sich damit der Grundsatz, dass sich die Wirksamkeit von Normen auch an der Wahrnehmung ihrer Durchsetzung bemisst.

12. „Legal Monitoring“ und regelmäßige Aktualisierung

Da sich die rechtlichen Rahmenbedingungen unternehmerischen Handelns durch die oben exemplarisch beschriebenen vielfältigen Aktivitäten der Gesetzgeber und Normsetzer auf nationaler und internationaler Ebene sowie durch Vorgaben der Gerichte ständig verändern, besteht für das Compliance Management ein kontinuierlicher **Überprüfungs- und Anpassungsbedarf**.³⁴³ Dies erfordert die kontinuierliche Beobachtung und **Analyse aktueller Rechtsentwicklungen** im Sinne eines „Legal Monitoring“. Im Rahmen sog. „**Compliance Audits**“ ist regelmäßig ferner zu fragen, inwieweit ein Unternehmen hinreichende, d. h. den unternehmensspezifischen Compliance-Risiken angepasste Compliance-Maßnahmen etabliert und umgesetzt hat: Sofern bereits ein Compliance Management etabliert wurde, kann sich dessen mangelnde Eignung zur Einhaltung rechtlicher Vorgaben durch das Unternehmen und dessen Mitarbeiter herausstellen und zu einer Neuausrichtung zwingen.³⁴⁴ Insbesondere aus einem aufgedeckten Regelverstoß resultiert die Pflicht, aber zugleich die Chance, das Compliance Management anzupassen bzw. neue Compliance-Maßnahmen zu entwickeln.³⁴⁵

89

13. Angemessene Dokumentation

Für den Nachweis eines funktionierenden Compliance Managements ist schließlich die sorgfältige Dokumentation der implementierten Compliance-Strukturen, Prozesse und Maßnahmen wichtig.³⁴⁶ Die Dokumentation des Compliance Managements kann der Unternehmensleitung in Fällen von „Non-Compliance“ helfen, die Erfüllung ihrer Organisationspflichten nachzuweisen.³⁴⁷

90

IV. Vorteile eines effektiven Compliance Managements

Gelingt es, mit der Einführung und regelmäßigen Aktualisierung der oben beschriebenen Strukturen, Prozesse und Maßnahmen ein wirksames Compliance

91

343 *Liese/Schulz*, BB 2011, 1347 ff.; *Seibt*, in: Schmidt/Lutter (Hrsg.), AktG, § 76 Rn. 30.

344 *Liese/Schulz*, BB 2011, 1347 ff. Siehe ferner → *Rack*, Kap. 10.

345 Zur Aktualisierung als notwendigem Bestandteil von Compliance Management siehe etwa auch *Fleischer*, in: BeckOGK AktG, Stand: 1.2.2024, § 91 Rn. 75 („Systemprüfungs- und Nachjustierungspflichten“); *Seibt*, in: Schmidt/Lutter (Hrsg.), AktG, § 76 Rn. 30 (in Bezug auf den Vorstand der AG).

346 Vgl. *Klopp*, Der Compliance-Beauftragte, S. 92 ff.

347 Vgl. *Klopp*, Der Compliance-Beauftragte, S. 93 m. w. N.

Management zu schaffen, so hat dies für Unternehmen und Verbände zahlreiche Vorteile.

1. Prävention und Reduzierung der Kostenrisiken und Nachteile von „Non-Compliance“

- 92** Wie ausgeführt, honorieren Gerichte und auch der Gesetzgeber inzwischen ausdrücklich die Existenz von Compliance-Maßnahmen, jedenfalls sofern dadurch das ernsthafte Bemühen zur Prävention von Regelverletzungen zum Ausdruck kommt. Zwar können Regelverletzungen auch durch Compliance Management nicht vollständig verhindert werden. Allerdings lässt sich das Risiko der „Non-Compliance“ durch wirksame Compliance-Maßnahmen erheblich reduzieren. Dadurch leistet ein wirksames Compliance Management einen wesentlichen Beitrag dazu, das immense Kostenrisiko und die sonstigen Nachteile von „Non-Compliance“ einzudämmen.

2. Schutz von Unternehmen, Leitungsorganen und Unternehmensangehörigen

- 93** Zugleich schützt ein wirksames Compliance Management das Unternehmen, seine Leitungsorganen und die Unternehmensangehörigen. Erfasst wird sowohl der Schutz des Unternehmens vor zivilrechtlicher Haftung und strafrechtlichen Sanktionen als auch der Schutz der Geschäftsleiter und Unternehmensangehörigen vor persönlicher zivil- und strafrechtlicher Haftung.³⁴⁸ Erfasst wird ferner der Schutz vor Nachteilen im Geschäftsverkehr und Wettbewerb³⁴⁹ (etwa durch unwirksame Geschäftsmodelle, Transaktionen oder den Ausschluss von Aufträgen) sowie der Schutz gegenüber Angriffen von außen (z. B. durch „Hacker“-Angriffe).³⁵⁰

3. Sicherung der Reputation und Vertrauensserhalt der Stakeholder

- 94** Darüber hinaus fördert bzw. erhält ein wirksames Compliance Management den guten Ruf des Unternehmens und das Vertrauen der Stakeholder. Wie ausgeführt,³⁵¹ kann ein positives Image des Unternehmens bei den maßgeblichen Bezugsgruppen (Mitarbeiter, Kunden, Lieferanten, Investoren etc.) durch Fälle von „Non-Compliance“ schnell beschädigt oder zerstört werden. Umgekehrt sichert ein funktionierendes Compliance Management das Vertrauen der **Stakeholder** in eine rechtskonforme und integre Geschäftstätigkeit und in einen glaubwü-

348 Vgl. Gößwein/Hohmann, BB 2011, 963, 964.

349 Siehe das umfangreiche Spektrum der Nachteile von „Non-Compliance“ unter → Rn. 11.

350 Vgl. Schulz/Galster, in: Bürkle/Hauschka/Schieffer, Der Compliance Officer, § 3 Rn. 14 m. w. N.

351 Siehe oben unter → Rn. 13, 23 ff.

gen Auftritt des Unternehmens in der **Öffentlichkeit**.³⁵² Damit kann auch den (insbesondere im Zusammenhang mit der ESG-Compliance) wachsenden Anforderungen und Erwartungen an verantwortungsvolles unternehmerisches Handeln durch die (stärkere) Berücksichtigung von Reputationsrisiken im Sinne eines „Reputational Risk Management“ bei der Entscheidung über neue Geschäftsmodelle und Transaktionen Rechnung getragen werden (siehe oben unter → Rn. 13, 23 ff.).

4. Eröffnung und Wahrung rechtlicher Chancen und Gestaltungsoptionen

Richtig verstanden erfüllt Compliance Management eine wichtige „**Enabling Function**“ insofern, als rechtlich gesicherte Handlungsoptionen und Gestaltungsmöglichkeiten aufgezeigt werden. Das gilt etwa durch die Verdeutlichung von Optionen für eine vorbeugende **Vertragsgestaltung** oder (steuer-)rechtliche **Strukturierung** im Interesse des Unternehmens,³⁵³ die nicht nur rechtliche Aspekte, sondern auch Reputationsgesichtspunkte berücksichtigt. Ein funktionierendes Compliance Management kann so dazu beitragen, Unternehmenswerte zu schaffen³⁵⁴ und die **Wettbewerbsfähigkeit** des Unternehmens zu sichern. Denn Unternehmen können auch dadurch gefährdet werden, dass Maßnahmen vorausschauender Rechtsgestaltung nicht oder nur unzureichend genutzt werden.³⁵⁵ Wie gezeigt (→ Rn. 13, 23 ff.), sollten bei der Nutzung rechtlicher Gestaltungsmöglichkeiten stets auch die Beziehungen zu maßgeblichen Bezugsgruppen (Mitarbeiter, Kunden, Lieferanten, Investoren etc.) berücksichtigt werden.³⁵⁶

5. Vorteile beim Marketing und im Wettbewerb

Durch ein funktionierendes Compliance Management können zudem positive **Marketing-Effekte** erzielt werden.³⁵⁷ Denn die Unternehmensleitung signalisiert sowohl unternehmensintern als auch im Geschäftsverkehr, dass Normverletzungen systematisch verhindert bzw. geahndet werden. Gelingt es der Unternehmensleitung, Regelkonformität sowie integrires Verhalten glaubwürdig an alle

352 *Schulz/Galster*, in: Bürkle/Hauschka/Schieffer, Der Compliance Officer, § 3 Rn. 14; *Gößwein/Hohmann*, BB 2011, 963, 964.

353 Vgl. *Rodewald*, Gesetzestreue als Organisationsproblem – Compliance richtig managen, in: Maschmann, Corporate Compliance und Arbeitsrecht, S. 31, 32 f.; ähnlich *Theusinger/Jung*, in: Römermann, Münchener Anwaltshandbuch GmbH-Recht, § 24 Rn. 5.

354 *Bürkle*, in: Bürkle, Compliance in Versicherungsunternehmen, § 1 Rn. 77.

355 *Rodewald*, Gesetzestreue als Organisationsproblem – Compliance richtig managen, in: Maschmann, Corporate Compliance und Arbeitsrecht, S. 32 f.; ähnlich *Theusinger/Jung*, in: Römermann, Münchener Anwaltshandbuch GmbH-Recht, § 24 Rn. 5.

356 Zur Notwendigkeit eines „Corporate Reputation Management“ ausführlich *Seibt*, DB 2015, 171 ff., sowie *ders.*, Börsenzeitung Nr. 31 v. 14.2.2015, 9; und *Seibt*, in: Schmidt/Lutter (Hrsg.), AktG, § 76 Rn. 42 ff.

357 Vgl. *Lösler*, NZG 2005, 104, 105; *Klopp*, Der Compliance-Beauftragte, S. 58 f.

Stakeholder zu vermitteln, kann sich das Unternehmen durch ein funktionierendes Compliance Management von Wettbewerbern differenzieren (wirksames **Compliance Management als Wettbewerbsvorteil**).³⁵⁸ Im Wettbewerb um qualifizierten Nachwuchs trägt ein wirksames Compliance Management dazu bei, gute Mitarbeiter zu gewinnen bzw. längerfristig zu halten.³⁵⁹ Denn viele Nachwuchskräfte erwarten von Unternehmen ein gutes Image bzw. ein ihren Vorstellungen entsprechendes regelkonformes Verhalten.³⁶⁰ Die oben genannten positiven Marketingeffekte von Compliance-Maßnahmen setzen allerdings voraus, dass das Compliance Management und die damit verbundenen Maßnahmen regelmäßig überprüft und aktualisiert werden.³⁶¹

6. Verteidigungsmöglichkeiten bei „Non-Compliance“

- 97 Mithilfe von Compliance Management kann die Geschäftsleitung Risiken aus Regelverletzungen reduzieren, jedoch nicht in jedem Fall vollständig ausschließen. Neuere Entwicklungen in Rechtsprechung und Gesetzgebung zeigen, dass Compliance-Maßnahmen für Unternehmen und Verbände positive Wirkungen haben können: Wie der Bundesgerichtshof in seinem Urteil vom 9.5.2017 ausdrücklich festgestellt hat, ist bei Regelverstößen im Rahmen der Bußgeldbemessung von Bedeutung, inwieweit ein Unternehmen seiner Pflicht, Rechtsverletzungen aus der Sphäre des Unternehmens zu unterbinden, genügt und ein „effizientes Compliance-Management“ installiert hat.³⁶² Als zentrales Element eines Compliance-Systems gilt dabei „das präventive Bemühen um eine weitgehende Eindämmung von Rechtsverstößen, die aus dem Unternehmen heraus begangen werden“.³⁶³

358 Zu Compliance Management als Wettbewerbsvorteil siehe *Schertler/Schertler*, Compliance Management aus Sicht der strategischen Unternehmensführung, in: Kaltenbrunner/Urnik, Unternehmensführung, S. 125, 132 f. Zu den verschiedenen Formen der strategischen Positionierung von Compliance-Maßnahmen siehe *Siedenbiedel*, Corporate Compliance, S. 55 f.

359 Vgl. *Rosbach*, CCZ 2008, 101; zu den Vorteilen effektiver Compliance ferner *Poppe*, Begriffsbestimmung Compliance: Bedeutung und Notwendigkeit, in: Inderst/Bannenberg/Poppe, Compliance, S. 1, 11 f. m. w. N.

360 Vgl. *Nezmeskal-Berggötz*, Integritätsmanagement und Social Compliance bei Deutsche Post DHL Group, in: Wieland/Steinmeyer/Grüniger, Handbuch Compliance-Management, S. 709, 710 f. unter Hinweis auf die PWC-Studie „Millennials at work, Reshaping the Workplace“, 2012, <https://www.pwc.com/m1/en/services/consulting/documents/millennials-at-work.pdf> (zuletzt abgerufen am 18.10.2024).

361 Vgl. hierzu *Liese/Schulz*, BB 2011, 1347 ff.

362 BGH, Urt. v. 9.5.2017 – 1 StR 265/16 = CB 2017, 330, Ls. 3: „Für die Bemessung der Geldbuße ist [...] von Bedeutung, inwieweit die Nebenbeteiligte ihrer Pflicht, Rechtsverletzungen aus der Sphäre des Unternehmens zu unterbinden, genügt und ein effizientes Compliance-Management installiert hat.“ Siehe zur Bedeutung dieser Entscheidung für das Compliance-Management etwa *Bürkle*, BB 2018, 525.

363 So ausdrücklich *Raum*, Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten, in: Hastenrath, Compliance-Kommunikation, S. 31, 33.

Wie gezeigt, kann in einem Fall von „Non-Compliance“ der dokumentierte Nachweis eines grundsätzlich existenten Compliance-Management-Systems allerdings zur Verteidigung geltend gemacht werden.³⁶⁴ **98**

7. Verbesserung von Strukturen und Prozessen

Die systematische Beschäftigung mit Compliance-Risiken und die Einführung geeigneter Organisationsmaßnahmen können zu Verbesserungen unternehmensinterner Strukturen und Prozesse beitragen. Dies gilt etwa für die Frage von (neu zu schaffenden oder konkreteren) Zuständigkeiten für Compliance, der besseren Koordination von Informationsflüssen, der Schaffung bzw. Verbesserung von Kommunikationswegen oder des (besseren) Austausches unterschiedlicher Unternehmensfunktionen zu Compliance-Fragen.³⁶⁵ In diesem Zusammenhang lässt sich daher auch ein professionelles Informations- und Wissensmanagement für das Unternehmen etablieren bzw. weiterentwickeln.³⁶⁶ Die für ein effektives Compliance Management erforderliche kontinuierliche Analyse der Veränderungen rechtlicher Vorgaben und Standards erfüllt ferner eine Qualitätssicherungs- und Innovationsfunktion.³⁶⁷ So können sich Hinweise auf Verbesserungsmöglichkeiten bei Geschäftsprozessen oder bei der Behandlung von Compliance-Themen ergeben.³⁶⁸ **99**

V. Zusammenfassung und Empfehlungen

Im Mittelpunkt von Compliance Management stehen organisatorische Vorkehrungen zur Verhinderung von Regelverstößen, zur Kontrolle der eingeleiteten Maßnahmen, zur Aufdeckung von „Non-Compliance“, zur angemessenen Reaktion bzw. Sanktionierung von Regelverletzungen sowie zur regelmäßigen Aktualisierung der etablierten Strukturen und Maßnahmen. Primär verantwortlich für das Compliance Management sind die Geschäftsleiter, die für ein normgerechtes Verhalten im Unternehmen und durch das Unternehmen sorgen müssen. Die sog. **Compliance-Organisationspflicht** betrifft grundsätzlich alle Unternehmen und Verbände, ihre Wahrnehmung zählt zum Kernbestand rechtskonformer Unternehmensführung. **100**

Neuere Entwicklungen zeigen eine erhebliche **Ausweitung der Compliance-Pflicht** und der Anforderungen an ein wirksames Compliance-Management. So **101**

364 Bürkle, in: Bürkle, Compliance in Versicherungsunternehmen, § 1 Rn. 77.

365 Vgl. v. Marnitz, Compliance-Management für mittelständische Unternehmen, S. 74 f.; Schulz/Renz, BB 2012, 2511, 2514.

366 Schulz, CB 2015, 309, 313; siehe auch v. Marnitz, Compliance-Management für mittelständische Unternehmen, S. 75.

367 Vgl. Hauschka, Compliance im Gesellschaftsrecht, in: Hadding/Hopt/Schimansky, Verbraucherschutz im Kreditgeschäft – Compliance in der Kreditwirtschaft, S. 103, 111; Schulz/Galster, in: Bürkle/Hauschka/Schieffer, Der Compliance Officer, § 3 Rn. 19.

368 Hauschka, Compliance im Gesellschaftsrecht, in: Hadding/Hopt/Schimansky, Verbraucherschutz im Kreditgeschäft – Compliance in der Kreditwirtschaft, S. 103, 111.

ist das LkSG ein prominentes Beispiel für „**ESG-Compliance**“, welche die Reichweite bestimmter Compliance-Pflichten in Bezug auf Menschenrechte und bestimmte Umweltbelange über den eigenen Unternehmensbereich erweitert. Eine weitere Ausweitung von Compliance-Anforderungen folgt aus der **Digitalisierung** und dem Einsatz künstlicher Intelligenz und damit verbundenen Herausforderungen im Zusammenhang mit **Cyber-Security** sowie einer „**KI-Compliance**“. Unternehmen müssen ihre Compliance-Strukturen daher systematisch überprüfen und an zahlreiche neue Vorgaben und Herausforderungen anpassen.

- 102** Für die entscheidende Frage der **Wirksamkeit von Compliance Management** fehlt es (abgesehen von besonderen Vorgaben für einzelne Branchen oder Themen) an allgemein verbindlichen Vorgaben. Allerdings lassen sich aus der Entscheidungspraxis der Gerichte, aus Leitlinien von Behörden, aus den von diversen Organisationen entwickelten Standards, aus Leitfäden für Compliance Management aus anderen Rechtsordnungen sowie aus umfangreichen Stellungnahmen der Wissenschaft **bestimmte Kernelemente und Mindestanforderungen** eines effektiven Compliance Managements destillieren. Dazu zählen eine unternehmensspezifische Compliance-Risiko-Strategie, ein unmissverständliches Bekenntnis der Unternehmensleitung zur Regeltreue, ein vorbildliches Verhalten aller Führungskräfte, zielgerichtete und bedarfsorientierte Kommunikations- und Schulungsmaßnahmen, adäquate Berichtswege und Hinweisgebersysteme, systematische Kontrollen sowie die konsequente Aufklärung und Sanktionierung von Regelverletzungen.
- 103** Aufgrund des dynamischen regulatorischen Umfeldes und permanenter neuer rechtlicher Vorgaben (auch durch Gerichte und Behörden) müssen die Compliance-Strukturen und Maßnahmen fortlaufend überprüft und regelmäßig an neue Anforderungen angepasst werden. Dieser Prozess erfordert eine kontinuierliche Beobachtung und **Analyse aktueller Rechtsentwicklungen** („**Legal Monitoring**“).
- 104** Eine Schlüsselrolle für den Erfolg des Compliance Managements spielt die Förderung einer Compliance-Kultur durch vorbildliches Verhalten und positive Kommunikation der Unternehmensleitung und der Führungskräfte. Da eine lückenlose und umfassende Regelung sämtlicher Compliance-Themen unmöglich ist, empfiehlt sich die Fundierung der Compliance-Maßnahmen durch ein **begleitendes Werte- und Integritätsmanagement**. Dies ermöglicht eine Vermeidung von Normverletzungen bei Regelungslücken, in Zweifelsfällen und bei sog. „Graubereichen“. Die Vermittlung der mit den Compliance-Maßnahmen verbundenen Werte fungiert so als **Kompass**, der in Zweifelsfällen zumindest auf eine Klärung von Compliance-Fragen durch den Compliance Officer verweist. Ebenso wichtig für die **Glaubwürdigkeit** des Compliance Managements ist die kompromisslose und angemessene **Sanktionierung von Regelverletzungen**, die keinesfalls als „Kavaliersdelikte“, als „nützliche Pflichtverletzungen“ oder in sonstiger Weise toleriert werden dürfen.

Neben dem Schutz des Unternehmens, seiner Leitungsorgane und seiner Stakeholder dient ein wirksames Compliance Management auch der Sicherung bzw. Verbesserung der **Reputation**, insbesondere vor dem Hintergrund höherer Erwartungen der Stakeholder und der Öffentlichkeit an ein regelkonformes und verantwortungsvolles Auftreten. **105**

Für den langfristigen Erfolg von Compliance Management ist zu empfehlen, das Thema **Compliance als Grundlage erfolgreicher Geschäftstätigkeit** („Business Enabler“) und insbesondere als Möglichkeit zur Nutzung rechtlich gesicherter Gestaltungsoptionen zu vermitteln. Compliance-Aspekte müssen daher stets von Beginn an bei Entwicklung und Ausbau von Geschäftsmodellen berücksichtigt werden. **106**

2. Kapitel

Compliance Management und Strafrecht

I. Einführung in die Criminal Compliance

Die Notwendigkeit sowie die rechtliche Verpflichtung zur Installation eines Compliance Managements entstammt zumindest ursprünglich nicht der Sorge um die strafrechtliche Gesetzmäßigkeit des unternehmerischen Handelns bzw. der Sorge um die Wirkung strafrechtlicher Verfehlungen auf das Unternehmen. In der „Vor-Compliance-Zeit“ (bis 1998)¹ bestand vielmehr ein Zielkonflikt zwischen einer Verpflichtung zu ethischem und damit auch einem strafrechtskonformen Handeln auf der einen Seite sowie der Verpflichtung zur Ertragsoptimierung im Sinne des Shareholder-Value-Gedankens auf der anderen Seite. Hier konnte sogar eine strafrechtliche Grenzüberschreitung als opportun bzw. jedenfalls hinnehmbar in eine Kosten-Nutzen-Abwägung Eingang finden. Je weniger „ehrenrührig“ die strafrechtliche Grenzüberschreitung in den relevanten Kreisen, so etwa der sog. „Deutschland AG“, erschien und je geringer das Entdeckungsrisiko war, desto eher ist ein solches Risiko durch die Unternehmensverantwortlichen in Kauf genommen worden, wenngleich auch seinerzeit bereits penibel darauf geachtet wurde, dass im Falle der Entdeckung eine Verstrickung nicht bis in den Vorstand oder ggf. sogar den Aufsichtsrat nachgewiesen werden konnte.

Gerade im Bereich der heutigen Kern-Compliance-Risiken, etwa der Korruption, der Untreue, der Steuerhinterziehung sowie der Verstöße gegen das Kartell- oder auch Datenschutzrecht, sah die Welt noch völlig anders aus. Bis 1998 waren die Tatbestände der Inlands-Korruption ein relativ stumpfes Schwert, bei der Vorteilsgewährung musste die Justiz den Abschluss einer konkreten Unrechtsvereinbarung nachweisen und die Anforderungen der Rechtsprechung waren hoch, die Auslands-Korruption war schlichtweg in Deutschland noch gar nicht strafbar. Im Gegenteil, der Staat hat die Auslands-Korruption deutscher Unternehmen vielmehr als mögliches Akquisitionsinstrument angesehen und den Einsatz der dafür erforderlichen Mittel, die sog. „nützlichen Aufwendungen“ (NA), steuerlich sogar als Betriebsausgaben anerkannt.²

In diesem Umfeld hat der Gesetzgeber dann im Jahre 1998 durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)³ die für die Compliance als grundlegend angesehene Norm des § 91 Abs. 2 AktG eingeführt, nach der der Vorstand der Aktiengesellschaft „geeignete Maßnahmen“ zu treffen, „insbesondere ein Überwachungssystem einzurichten“ hat, mit dessen Hilfe

1 Erlass des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) v. 27.4.1998, hierzu später ausführlicher.

2 Vgl. BT-Drs. 13/1717 v. 19.6.1995.

3 KonTraG, Gesetz v. 27.4.1998, BGBl. I 1998, S. 786.

„den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt“ werden können. Ein solches Überwachungssystem war bereits von seinem Wortlaut her seinerzeit nur zur Früherkennung *betriebswirtschaftlich* existenzgefährdender Risiken bestimmt. Mit dem Gesetz zur Stärkung der Finanzmarktintegrität vom 3.6.2021⁴ hat der Gesetzgeber zwischenzeitlich § 91 Abs. 3 AktG eingeführt, der den Vorstand einer börsennotierten Gesellschaft ausdrücklich verpflichtet, ein „im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames internes Kontrollsystem und Risikomanagementsystem einzurichten“. Dass sich innerhalb weniger Jahre die Erkenntnis durchsetzen sollte, dass auch strafrechtliche Compliance-Risiken ein existenzgefährdendes Ausmaß für das Unternehmen annehmen könnten, war damals kaum absehbar.

- 4 In den Jahren ab 1998 hat der Gesetzgeber jedoch insbesondere im Strafrecht einen dramatischen Kurswechsel vollzogen, der heute an dem Erfordernis einer insbesondere strafrechtsbasierten Compliance keinen Zweifel mehr lässt.
- 5 Nachdem die bis dato unzureichende Korruptionsbekämpfung im Jahr 1996 Gegenstand des 61. Deutschen Juristentages war, und obwohl die geplanten Maßnahmen dort in hohem Maße umstritten waren, schaffte der Gesetzgeber mit dem Gesetz zur Bekämpfung der Korruption vom 13.8.1997 (KorrBekG)⁵ zunächst einschneidende **Verschärfungen im Korruptionsstrafrecht**, mit welchen die bis dato bestehenden Lücken geschlossen und Verfolgungsprobleme beseitigt werden sollten. Neben einer deutlichen Verschärfung der Strafandrohung für die Korruptionsdelikte des Kernstrafrechts waren die Kernpunkte der Veränderung die Erfassung des sog. „Dritt Vorteils“, also die Strafbarkeit der Zuwendung an einen dem Amtsträger nahestehenden Dritten, sowie die bis heute umstrittene und nachwirkende Lockerung der sog. „Unrechtsvereinbarung“, mithin der inhaltlichen Verknüpfung von Dienstaussübung und Vorteilszuwendung. Schließlich ist der Abschnitt „Straftaten gegen den Wettbewerb“ in das StGB aufgenommen worden, der nicht nur den neu gefassten Straftatbestand des § 298 StGB (wettbewerbsbeschränkende Absprachen bei Ausschreibungen), den ehemaligen „Submissionsbetrug“, umfasst, sondern insbesondere auch die aus dem Nebenstrafrecht (UWG) stammenden Delikte der Nicht-Amtsträger-Bestechung (ugs. Privat-Korruption), der Bestechlichkeit und **Bestechung im geschäftlichen Verkehr** neu gefasst und in das StGB eingefügt hat (§§ 299, 300 StGB). Zwar enthielt § 12 UWG bis dato eine vergleichbare Strafvorschrift, diese war jedoch gem. § 22 UWG a.F. als absolutes Antragsdelikt ausgestaltet und führte dieserhalb eher ein Schattendasein im UWG. Seit der Aufwertung dieses Tatbestands durch Aufnahme in das Kernstrafrecht erfreut sich insbesondere die Regelung des § 299 StGB, also der Bestechlichkeit und Bestechung im geschäftlichen Verkehr, einer stark zunehmenden Beliebtheit bei den Ermitt-

4 Gesetz zur Stärkung der Finanzmarktintegrität vom 3.6.2021, BGBl. I 2021, S. 1534, 1557.

5 KorrBekG, Gesetz v. 13.8.1997, BGBl. I 1997, S. 2038.

lungsbehörden. Durch ein weiteres Gesetz zur Bekämpfung der Korruption⁶ mit Wirkung ab dem 26.11.2015 hat der Gesetzgeber die Vorschrift des § 299 StGB noch einmal erweitert und das sog. Geschäftsherrenmodell in den Tatbestand aufgenommen. Strafbar soll nunmehr auch derjenige sein, der einen Vorteil als Gegenleistung dafür annimmt, dass er bei dem Bezug von Waren oder Dienstleistungen schlichtweg „seine Pflichten gegenüber dem Unternehmen verletzt“. Ziel der durchaus unbestimmten Neuregelung soll, so der Gesetzgeber, ein erweiterter „Schutz der Interessen des Geschäftsherrn an der loyalen und unbeeinflussten Erfüllung der Pflichten durch seine Angestellten und Beauftragten“ sein. Zu befürchten ist jedoch, dass hier mittelfristig auch die Verletzung selbstgesetzter Compliance-Vorgaben des Unternehmens u. U. sogar als strafbarkeitsbegründend angesehen wird.

Sodann hat der Gesetzgeber weitere Spezialtatbestände im Bereich der Korruption neu geschaffen bzw. reformiert. Im Jahr 2014 hat der Gesetzgeber nach über 11 Jahren internationalen Drucks den Tatbestand der **Abgeordnetenbestechung** (§ 108e StGB) reformiert und an die Anforderungen der UN-Konvention angepasst.⁷ Die Neuregelung des § 108e StGB erfasst nunmehr unter dem Titel „Bestechlichkeit und Bestechung von Mandatsträgern“ nicht nur Bundestags- und Landtagsabgeordnete, sondern auch kommunale Mandatsträger.

Im Jahre 2016 hat der Gesetzgeber durch das umstrittene Gesetz zur Bekämpfung von Korruption im Gesundheitswesen vom 14.4.2016⁸ zwei neue Korruptionsvorschriften für die Akteure im Gesundheitswesen erlassen. Die neuen Straftatbestände § 299a StGB (Bestechlichkeit im Gesundheitswesen) und § 299b StGB (Bestechung im Gesundheitswesen) sind der Struktur des § 299 StGB (Bestechlichkeit und Bestechung im geschäftlichen Verkehr) nachgebildet.

Auch international ist seit Jahren – unter dem starken Einfluss der US-amerikanischen Regierung – eine Verstärkung und **Internationalisierung der Korruptionsbekämpfung** zu verzeichnen.⁹ In den USA hat die Korruptionsbekämpfung auch im Rahmen der Auslandsaktivitäten US-amerikanischer Unternehmen bereits eine längere Tradition. Das Auslandsbestechungsgesetz (FCPA) verbietet bereits seit den späten 70er Jahren Zahlungen und Geschenke an ausländische staatliche Amtsträger, die den Zweck haben, einen Geschäftsabschluss zu befördern oder eine Geschäftsbeziehung aufrechtzuerhalten.¹⁰ Auf Basis des OECD-Übereinkommens über die Bekämpfung der Bestechung ausländischer Amtsträ-

⁶ Gesetz zur Bekämpfung der Korruption v. 20.11.2015, BGBl. I 2015, S. 2025.

⁷ 48. Strafrechtsänderungsgesetz vom 23.4.2014, BGBl. I 2014, S. 410 (Geltung ab dem 1.9.2014).

⁸ BGBl. I 2016, S. 1254; in Kraft seit dem 4.6.2016; vgl. BT-Drs. 18/6446; Beschluss des Bundesrates v. 13.5.2016, BR-Drs. 181/16.

⁹ Weiterführend: Böttger, Wirtschaftsstrafrecht, Kap. 5 Rn. 56 m. w. N.

¹⁰ Foreign Corrupt Practices Act (FCPA) von 1977, Title 15 U.S.C. §§ 78dd-1 ff.; vgl. hierzu ausführlich: Rübentahl, NZWiSt 2012, 401.

ger im internationalen Geschäftsbereich vom 17.12.1997 hat dann auch der deutsche Gesetzgeber die internationalen Vorgaben zur Erweiterung der Anwendbarkeit der Korruptionsvorschriften auf den internationalen Bereich umgesetzt und das Gesetz zur Bekämpfung internationaler Bestechung (IntBestG) verabschiedet.¹¹ Durch das IntBestG wurden zahlreiche ausländische Amtsträger (und Richter) unter bestimmten Voraussetzungen den inländischen Amtsträgern gleichgesetzt, darüber hinaus wurde das deutsche Strafrecht unabhängig vom Recht des Tatortes für die Bestechung ausländischer Amtsträger und Abgeordneter im internationalen Geschäftsverkehr für anwendbar erklärt (§ 5 StGB). In Umsetzung des EU-Bestechungsübereinkommens hat der Gesetzgeber mit Schaffung des EU-Bestechungsgesetzes (EUBestG)¹² fast zeitgleich die Anwendbarkeit des Amtsträgerbegriffes auch auf die Amtsträger von EU-Mitgliedsstaaten sowie auf bestimmte Gemeinschaftsbeamte sowie die Mitglieder der Kommission und des Rechnungshofes der europäischen Gemeinschaften ausgeweitet. Des Verweises auf die Vorschriften des IntBestG sowie des EUBestG bedarf es seit November 2015 nicht mehr, da diese zwischenzeitlich – jedenfalls zum größten Teil – in das StGB (§§ 11 Abs. 1 Nr. 2 lit. a, 331 ff., 335a StGB) übernommen wurden.¹³ Der Strafdrohung der deutschen Korruptionsnormen unterliegen damit ausdrücklich auch „Europäische Amtsträger“ (§ 11 Abs. 1 Nr. 2a StGB), also etwa EU-Beamte, Mitglieder der Europäischen Kommission oder auch der EU-Gerichte, sowie „ausländische und internationale Bedienstete“ (§ 335a StGB).¹⁴ Auch die Auslandskorruption ist damit zwischenzeitlich fester Bestandteil des Kernstrafrechts geworden.

- 9 Der Wille, Korruption ernsthaft zu verfolgen, wenngleich diese bis dato von deutschen Unternehmen – jedenfalls im Ausland – als kaum verzichtbares Akquisitionsinstrument angesehen wurde, hat sich dann schließlich auch nicht nur darin niedergeschlagen, dass der Gesetzgeber die steuerliche Absetzbarkeit von im Ausland gezahlten Bestechungsgeldern abgeschafft, sondern er auch diverse faktische Maßnahmen zur Verbesserung der Korruptionsbekämpfung umgesetzt hat. So wurden nicht nur „**Schwerpunktstaatsanwaltschaften zur Korruptionsbekämpfung**“ eingesetzt, die ihr Handwerk wirklich verstehen, sondern auch etwa Hinweisgebersysteme bei den Landeskriminalämtern sowie in einigen Ländern auch **Korruptionsregister** eingeführt. Auf Bundesebene ist die Einführung eines (bundesweiten) Korruptionsregisters zur Vorbereitung von Vergabeentscheidungen, trotz einer jahrelangen Diskussion, jedoch immer wieder gescheitert. In einzelnen Bundesländern gibt es jedoch solche „Korruptionsregister“ oder „Vergaberegister“ teilweise auf Erlassbasis, teilweise auf gesetzli-

11 Gesetz zur Bekämpfung internationaler Bestechung, BGBl. II, S. 2327; III, 450-28, in Kraft getreten am 15.2.1999.

12 Gesetz zu dem Protokoll vom 27.9.1996 zum Übereinkommen über den Schutz der finanziellen Interessen der europäischen Gemeinschaften (EUBestG, BGBl. II 1998, S. 2340, in Kraft getreten am 22.9.1998).

13 Gesetz zur Bekämpfung der Korruption v. 20.11.2015, BGBl. I 2015, S. 2025.

14 Einzelnachweise bei: Böttger, Wirtschaftsstrafrecht, Kap. 5 Rn. 56 ff.

cher Basis, so etwa in NRW bei der Informationsstelle für Vergabeausschlüsse NRW, die beim Finanzministerium NRW geführt wird.¹⁵ Im Jahre 2021 ist darüber hinaus das beim Bundeskartellamt geführte **Wettbewerbsregister** in Betrieb genommen worden, in welchem vergaberechtliche Ausschlussgründe im Sinne der §§ 123 und 124 GWB erfasst und für den Abruf durch öffentliche Auftraggeber bereit gehalten werden.¹⁶

Gab es dieses umfassende strafrechtliche Normengeflecht zwar schon länger, so hat der Gesetzgeber den Ermittlungsbehörden jedoch darüber hinaus zwischenzeitlich ein **Ermittlungsinstrumentarium** an die Hand gegeben, das es ihnen nicht nur ermöglicht, die Einhaltung dieser Vorschriften effektiv zu kontrollieren, sondern auch bei dem Unternehmen als solchem die „Daumenschrauben“ derart anzuziehen, dass das Unternehmen selbst ein überragendes Interesse an der Verhinderung derartiger Straftaten, mithin an Compliance, hat. In der Praxis werden Beweisschwierigkeiten nicht nur regelmäßig mittels einer systematischen Auswertung des gesamten Datenbestands des Unternehmens, insbesondere der E-Mails, dem sog. „e-Search“, sondern auch zunehmend mit dem Instrument der Telekommunikationsüberwachung überwunden. Durch zahlreiche gesetzliche Änderungen wurde die einst dem Bereich der Schwerekriminalität vorbehaltene Telekommunikationsüberwachung auf Bereiche der (vermeintlichen) Wirtschaftskriminalität erstreckt, so insbesondere auf die Tatbestände der Bestechlichkeit und Bestechung, der (schweren) Angestelltenbestechlichkeit und -bestechung sowie neuerdings auch auf den Tatbestand der Bestechung von Mandatsträgern.

Beschränkte sich die Strafverfolgung noch vor einigen Jahren fast ausschließlich auf die Überführung der verantwortlichen Straftäter, so hat sich auch dieses Bild zwischenzeitlich fast um 180° gedreht. Regelmäßig begnügen sich Staatsanwaltschaften nicht mehr mit dem verantwortlichen Mitarbeiter des Unternehmens; regelmäßig versuchen die Staatsanwaltschaften von Anfang an, eine **Verantwortlichkeit der Unternehmensleitung** nachzuweisen, um dann dort – mit dem Ziel der Generalprävention – Schmerzen zu bereiten. So sehen sich die Staatsanwälte der Schwerpunktstaatsanwaltschaften als „Großwildjäger“, die weniger an dem einzelnen Vertriebsmitarbeiter als vielmehr dem Geschäftsführer oder dem Vorstand selbst interessiert sind. Da die staatsanwaltschaftliche Erfahrung zu zeigen scheint, dass die Verantwortlichkeiten regelmäßig in der Unternehmensleitung zusammenlaufen, wird zielorientiert auf die Feststellung entweder positiver Kenntnis der Unternehmensleitung oder jedenfalls eines sog. „Organisationsverschuldens“ hingearbeitet.

15 Gesetz zur Verbesserung der Korruptionsbekämpfung und zur Errichtung und Führung eines Vergaberegisters in Nordrhein-Westfalen (KorruptionsbG NRW) vom 16.12.2004, GV NRW 2005, 8, i. d. F. des ÄndG v. 19.12.2013, GV NRW 2013, 875 ff.

16 Gesetz zur Einrichtung und zum Betrieb eines Registers zum Schutz des Wettbewerbs um öffentliche Aufträge und Konzessionen v. 18.7.2017 (BGBl. I, S. 2739) i.V.m. der Wettbewerbsregisterverordnung v. 16.4.2021 (BGBl. I, S. 809).

- 12** Aber auch die Feststellung individueller strafrechtlicher Verantwortlichkeit bei der Unternehmensleitung reicht den Schwerpunktstaatsanwaltschaften häufig nicht mehr aus. Ziel der Ermittlungsbehörden – dies wird teilweise unverhohlen zugegeben – ist es, das Unternehmen dort zu treffen, wo es „weh tut“, nämlich im finanziellen Bereich. Als Unternehmensvertreter kann man sich häufig des Eindrucks nicht erwehren, dass durchaus auch profiskalische Aspekte hinter einer dahingehenden Forcierung stehen. Teilweise scheint die Ahndung individuellen Verschuldens in den Hintergrund zu treten neben der Absicht, Erträge (häufig) in Millionenhöhe im Wege der Einziehung oder über Unternehmensgeldbußen abzuschöpfen. Da derartige (Millionen-)Erträge dem jeweiligen Landeshaushalt zufließen, entsteht der Eindruck, dass die Staatsanwaltschaften mit teilweise abenteuerlichen Begründungen versuchen, eine dahingehende Kompetenz zu begründen, wo sie vor Jahren noch versucht hätten, entsprechende Zuständigkeiten von sich zu weisen.
- 13** Diese profiskalischen Perspektiven eröffnen sich den Staatsanwaltschaften durch die Instrumente der Einziehung von Taterträgen gemäß § 73 StGB sowie der **Verbandsgeldbuße gemäß § 30 OWiG** (ugs. Unternehmensgeldbuße), die auch im Strafverfahren – neben der persönlichen Schuldfeststellung – Anwendung findet. Kann gem. § 30 Abs. 2 OWiG gegen das Unternehmen bereits eine Geldbuße von bis zu 10 Mio. EUR verhängt werden, so erhöht sich diese bei Vorliegen eines abschöpfungsfähigen Erlöses, der aus der Straftat generiert wurde, gem. § 17 Abs. 4 OWiG schnell auf einen mehrstelligen Millionenbetrag. So hat etwa die Staatsanwaltschaft München I in der Causa Siemens bereits mit Bußgeldbescheid vom 15.12.2008 den Abschöpfungsanteil alleine auf einen Betrag i.H.v. 394.750.000,00 EUR festgesetzt und um einen Ahndungsanteil i.H.v. 250.000,00 EUR erhöht, mithin alleine in diesem Verfahren eine Geldbuße in Höhe von 395 Mio. EUR festgesetzt.¹⁷ Zuvor hatte bereits das LG München I gegen die Siemens AG eine Geldbuße in Höhe von 201 Mio. EUR verhängt. In der sog. „Diesel-Affäre“ hat die Staatsanwaltschaft Braunschweig gegen die Volkswagen AG unter dem 13.6.2018 einen Bußgeldbescheid über eine Verbandsgeldbuße in Höhe von 1 Mrd. EUR erlassen. Das gegen die Volkswagen AG festgesetzte Bußgeld umfasste dabei einen sanktionierenden Teil in Höhe von 5 Mio. und einen vermögensabschöpfenden Teil in Höhe von 995 Mio. EUR. Weitere Verbandsgeldbußen im dreistelligen Millionenbereich sind zwischenzeitlich etwa gegen die Audi AG, die Porsche AG sowie die Daimler AG erlassen worden.
- 14** Durch die zunehmende Europäisierung des Rechts, etwa im Bereich Datenschutz durch die DSGVO, finden auch verstärkt europaweit geltende Sanktionsvorschriften unmittelbare Anwendung.¹⁸ Für bestimmte Verstöße gegen die DSGVO sieht Art. 83 Abs. 5 DSGVO nach deutschem Verständnis ungewöhn-

¹⁷ Die Staatsanwaltschaft hat ihre Zuständigkeit hierbei aus der Ausnahmegvorschrift des § 42 OWiG i.V.m. Nr. 277 RiStBV abgeleitet.

¹⁸ Zur Bedeutung des Datenschutzes für das Compliance Management → *Becker/Böhlke/Fladung*, Kap. 12.

lich (hoch) anmutende Geldbußen von bis zu 20 Mio. EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs vor. Der deutsche Gesetzgeber macht sich eine solche umsatzabhängige Ahndung zunehmend auch zu eigen, so sieht etwa § 24 Abs. 3 LkSG für bestimmte Verstöße eine Ahndung mit einer „Geldbuße bis zu 2 Prozent des durchschnittlichen Jahresumsatzes“ vor.

Aber auch die **Kartellgeldbußen** des Bundeskartellamtes erreichen über das Institut der sog. Mehrerlösgeldbuße gem. § 81 Abs. 4, 5 GWB i.V.m. § 17 Abs. 4 OWiG schnell dreistellige Millionenbeträge.¹⁹ So hat das Bundeskartellamt etwa im Jahre 2014 gegen ein Mitglied des sog. Zuckerkartells eine Einzelgeldbuße in Höhe von 195,5 Mio. EUR verhängt. Die bis dato höchste Einzelkartellgeldbuße des Bundeskartellamtes – 251,5 Mio. EUR – wurde im sog. Grauzementkartell verhängt und vom OLG Düsseldorf sowie dem Bundesgerichtshof später auf 169,9 Mio. EUR bzw. 161,4 Mio. EUR reduziert.²⁰ Noch schmerzhafter aber ebenso compliance-relevant sind die Kartellgeldbußen, die die Europäische Kommission verhängt, die nicht selten die Milliardengrenze überschreiten, wie etwa zuletzt in Höhe von 4,3 Mrd. EUR gegen Google wegen Missbrauchs einer marktbeherrschenden Stellung oder in Höhe von 1,09 Mrd. EUR gegen Daimler im sog. „LKW-Kartell“.

Bei der Sanktionierung von Unternehmen wollte der Gesetzgeber sogar noch einen Schritt weitergehen und den Weg zu einem reinen „Unternehmensstrafrecht“ beschreiten, das die Unternehmen (und sonstigen „Verbände“) einem eigenständigen Sanktionsregime unterworfen hätte. Der von der Bundesregierung unter dem 16.6.2020 vorgelegte Entwurf eines „Gesetzes zur Sanktionierung von verbandsbezogenen Straftaten“, das sog. **Verbandssanktionengesetz** (VerSanG), ist jedoch in der 19. Legislaturperiode nicht mehr verabschiedet worden und damit zumindest vorerst gescheitert. Durch das Gesetzesvorhaben sollte der Weg zu einem „Unternehmensstrafrecht“ beschritten werden, die Unternehmen (und sonstigen „Verbände“) sollten einer eigenständigen Sanktionierung unterliegen. Da Unternehmen jedoch nicht schuldhaft handeln können, sprach man von Unternehmens- bzw. Verbandssanktionen und nicht von „Strafen“, die Wirkung ist jedoch die Gleiche.

Als mögliche Sanktionen sah das Gesetz die „Verbandsgeldsanktion“ sowie die „Verwarnung mit Verbandsgeldsanktionsvorbehalt“ vor. Die Verbandsgeldsanktion sollten ausweislich des Entwurfes bei einer vorsätzlichen Verbandstat bis zu 10 Mio. EUR betragen dürfen, bei einer fahrlässigen Verbandstat bis zu 5 Mio. EUR, bei einem Verband mit einem durchschnittlichen Jahresumsatz von mehr als 100 Mio. EUR sollte die Verbandsgeldsanktion hiervon abweichend sogar bis zu 10 % des durchschnittlichen Jahresumsatzes des betroffenen Unternehmens betragen können. Zugleich wollte der Gesetzgeber mit dem Verbandssank-

19 Zur Relevanz des Kartellrechts für das Compliance Management → *Seeliger/Mross/Seydel*, Kap. 27.

20 Vgl. BGH, Beschl. v. 26.2.2013 – KRB 20/12.

tionengesetz auch die Institutionalisierung der unternehmensinternen Compliance vorantreiben, etwa durch die sanktionsmildernde Berücksichtigung vorhandener Compliance-Strukturen sowie der Schaffung eines Rechtsrahmens für verbandsinterne Untersuchungen. Ob ein Verbandssanktionengesetz in dieser oder in anderer Form in absehbarer Zeit noch einmal angegangen wird, steht aktuell in den Sternen.

- 18 Neben dem aufgezeigten straf- und ordnungsrechtlichen Instrumentarium beherrschen die Schwerpunktstaatsanwaltschaften auch die Klaviatur der Generierung medialer **(Presse-)Öffentlichkeit**. Insbesondere für die betroffenen Unternehmen in hohem Maße etikettierende Durchsuchungs- und Beschlagnahmeaktionen sorgen für eine mediale Aufmerksamkeit und Berichterstattung, die den Verdacht im Bewusstsein der Öffentlichkeit als Tatsache zementiert. In der auflageorientierten Presselandschaft wird der möglicherweise auf dünner Tatsachenbasis angenommene Anfangsverdacht zum Skandal hochgestuft, wodurch weiterer Druck auf das Unternehmen entsteht, den Schaden durch eine „Koope-ration“ mit der Staatsanwaltschaft und möglicherweise durch eine interne Aufklärung zu reduzieren. Versucht das Unternehmen, sich gegen einen bestehenden Anfangsverdacht zu wehren, so ist die Staatsanwaltschaft durchaus in der Lage, offiziell oder inoffiziell die nächste Eskalationsstufe durch Herstellung weiterer Presseöffentlichkeit herbeizuführen. Häufig wird so der einmal angenommene Anfangsverdacht einer Straftat durch die Instrumentarien und die publizistischen Begleitumstände zu einer Art „self fulfilling prophecy“, mithin zu einer Abwärtsspirale, der sich das Unternehmen kaum noch entziehen kann.
- 19 Doch selbst, wenn es im Einzelfall nicht zu einer Einziehung oder der Verhängung einer existenzbedrohenden Verbandsgeldbuße²¹ kommt, sind auch die strafrechtlichen Nebenfolgen, etwa das sog. Blacklisting, nicht außer Acht zu lassen. Eintragungen in bestehende Vergabe- bzw. Korruptionsregister können zu schmerzhaften Vergabeausschlüssen, Eintragungen etwa in das Gewerbezentralregister können zum Entfall der Zuverlässigkeit des Unternehmens und damit zum Entfall zahlreicher Vergünstigungen im amtlichen Verkehr führen.
- 20 Der Einsatz dieser rechtlichen sowie faktischen Instrumentarien, die der Strafjustiz gegen das betroffene Unternehmen zur Verfügung stehen, sowie die erheblichen Konsequenzen, die sowohl das Unternehmen als auch seine Verantwortlichen treffen können, und der erklärte Wille zur rücksichtslosen Anwendung lassen ein Strafverfahren – jedenfalls wegen erheblicherer Vorwürfe – schnell zu einem pekuniären und publizistischen GAU für ein Unternehmen werden. Genau hier zeigt sich, dies war auch durchaus Absicht des Gesetzgebers, dass der Einsatz strafrechtlich-relevanter Methoden im Interesse der Gewinnmaximierung keine Option mehr darstellt. Gewinnstreben und ethisches Verhalten stehen damit nicht mehr in einem Zielkonflikt. Dass sich die Erkenntnis durchgesetzt hat, dass auch strafrechtliche Risiken für das Unternehmen ein existenz-

21 Bzw. nach Inkrafttreten des VerSanG einer „Verbandsgeldsanktion“.

gefährdendes Ausmaß annehmen können, ist daher weniger dem Gedanken der Unternehmensethik oder der Corporate Social Responsibility, denn vielmehr einem dramatischen Kurswechsel des Gesetzgebers im Strafrecht hin zu einem Unternehmenssanktionenrecht geschuldet. Die Vermeidung strafrechtlich relevanter Verhaltensweisen im (vermeintlichen) Unternehmensinteresse muss damit erklärtes Ziel des Unternehmers sein; Mittel zur Umsetzung dieses Ziels ist ein (auch) strafrechtlich basiertes Compliance Management.

Strafrechtliche Compliance-Risiken für das Unternehmen im Überblick

21

- Strafbarkeit der Unternehmensverantwortlichen und deren Inhabilität;
- Anordnung der Verfahrensbeteiligung gem. §§ 424, 444 StPO, 88 OWiG;
- Einziehung von Taterträgen gem. §§ 73 StGB, 29a OWiG;
- Verbandsgeldbuße gem. §§ 30 OWiG, 81 Abs. 4 Satz 2 GWB;
- Mehrerlösabschöpfung gem. §§ 30 Abs. 3, 17 Abs. 4 OWiG; 81 Abs. 4 GWB;
- Eintragung in Wettbewerbs- bzw. Korruptionsregister (Vergabesperren);
- Eintragung in das Gewerbezentralregister (Entfall der Zuverlässigkeit);
- Sonstiges „Blacklisting“ (BaFin, Weltbank etc.);
- Faktische Beeinträchtigungen der Unternehmensabläufe (Durchsuchung, Beschlagnahme etc.);
- Mediale Berichterstattung/Ad-hoc-Publizität (Reduktion des Börsenwertes).

II. Strafrechtliche Grundlagen der Compliance-Verpflichtung

22

Verbindliche gesetzliche Vorschriften zur Implementierung eines Compliance-Systems bzw. zur Durchführung auch nur einzelner Compliance-Maßnahmen finden sich im deutschen Recht bislang lediglich in einigen wenigen Spezialbereichen.²² Konkrete Vorgaben finden sich etwa im Bereich des **Kapitalmarktes**. Neben § 80 WpHG, der allgemeine Organisationspflichten für Wertpapierdienstleistungsunternehmen normiert, und der durch die Richtlinie zur Konkretisierung der Organisationspflichten von Wertpapierdienstleistungsunternehmen gem. § 80 WpHG²³ sowie etwa die Wertpapierdienstleistungs-, Verhaltens- und Organisationsverordnung (WpDVerOV)²⁴ konkretisiert wird, finden sich kon-

22 Grötsch/Scherer, wistra 2024, 139; Ohrtmann, in: Bungenberg/Dutzi/Krebs/Zimmermann, Corporate Compliance und Corporate Social Responsibility, S. 185, 187; Vogelsang/Nahrstedt/Fuhrmann, CCZ 2014, 181, 185. Zur Compliance-Funktion in einem Kreditinstitut → Renz/Frankenberger, Kap. 20.

23 Richtlinie zur Konkretisierung der Organisationspflichten von Wertpapierdienstleistungsunternehmen gem. § 33 Abs. 1 WpHG v. 25.10.1999, BAAnz Nr. 210, 18453 (aufgehoben mit BaFin-Schreiben v. 23.10.2007). § 33 WpHG a. F. entspricht § 80 WpHG.

24 Verordnung zur Konkretisierung der Verhaltensregeln und Organisationsanforderungen für Wertpapierdienstleistungsunternehmen (Wertpapierdienstleistungs-Verhaltens- und Organisationsverordnung – WpDVerOV) vom 20.7.2007 (BGBl. I, S. 1432).

krete Compliance-Vorgaben etwa in § 25a KWG, wonach das erforderliche „angemessene und wirksame Risikomanagement eines Kreditinstituts unter anderem „die Einrichtung interner Kontrollverfahren mit einem internen Kontrollsystem und einer internen Revision“ einschließlich einer „Compliance-Funktion“ zu umfassen hat.²⁵ § 29 Abs. 1 VAG verpflichtet **Versicherungsunternehmen** zum Betrieb eines internen Kontrollsystems, das über eine „Funktion zur Überwachung der Einhaltung der Anforderungen (Compliance-Funktion)“ verfügen muss. Im **Steuerrecht** hat das BMF bereits mit Schreiben vom 23.5.2016 ausgeführt, dass die Existenz eines Tax-Compliance-Management-Systems ein Indiz für einen fehlenden (Hinterziehungs-)Vorsatz darstelle.²⁶ Aufnahme in das Gesetz hat ein solches Tax CMS unter dem Begriff „Steuerkontrollsystem“ allerdings erst durch § 38 EGAO gefunden, wonach im Falle der Existenz eines Steuerkontrollsystems im Rahmen der Betriebsprüfung gewisse Erleichterungen zur Anwendung kommen können. Weitere sektoral geregelte konkrete Compliance-Verpflichtungen existieren beispielsweise im Bereich des **Arzneimittelrechts**, hier bei der sog. Pharmakovigilanz, also der laufenden und systematischen Überwachung der Sicherheit von Fertigarzneimitteln. So verpflichtet etwa § 63 b Abs. 2 Nr. 4 des Arzneimittelgesetzes (AMG) den Inhaber der Zulassung eines Arzneimittels, das zur Anwendung bei Menschen bestimmt ist, „ein Risikomanagement-System für jedes einzelne Arzneimittel zu betreiben“ und die von diesen Arzneimitteln ausgehenden Gefahren detailliert zu überwachen. Auch etwa im Lieferketten Sorgfaltspflichtengesetz (LkSG)²⁷ finden sich dahingehende Ansätze, so fordert § 4 LkSG ausdrücklich die Einrichtung eines angemessenen und wirksamen Risikomanagements zur Einhaltung der Sorgfaltspflichten. Das Risikomanagement müsse in allen maßgeblichen Geschäftsabläufen verankert sein.

- 23 Mit dem Finanzmarktintegritätsstärkungsgesetz vom 3.6.2021 (FISG) hat der Gesetzgeber die Vorschrift des § 91 Abs. 3 AktG geschaffen, die den Vorstand einer börsennotierten Gesellschaft verpflichtet, „ein im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames internes Kontrollsystem und Risikomanagementsystem einzurichten“.²⁸ Auch aus der neuen Vorschrift des § 91 Abs. 3 AktG ergibt sich je-

25 Präzisierung durch das BaFin-Rundschreiben 4/2010 (WA) – MaComp, „Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 31 ff. WpHG für Wertpapierdienstleistungsunternehmen“ vom 7.6.2010, zuletzt geändert am 8.3.2017.

26 BMF-Schreiben v. 23.5.2016 – IV A 3 – S 0324/15/10001, BStBl. I 2016, 490. Zur Tax Compliance → *Schwartz*, Kap. 29.

27 Gesetz über die unternehmerischen Sorgfaltspflichten in Lieferketten (LkSG) v. 16.7.2021, BGBl. I, S. 2959. Zum LkSG → *Heske*, Kap. 18.

28 Gesetz zur Stärkung der Finanzmarktintegrität (Finanzmarktintegritätsstärkungsgesetz – FISG) v. 3.6.2021, BGBl. I, S. 1534.

doch keine ausdrückliche Verpflichtung zur Schaffung (auch) eines reinen Compliance-Management-Systems.²⁹

Eine Verpflichtung zur Compliance erschließt sich insoweit lediglich mittelbar aus der sog. Legalitätspflicht, der Pflicht des Unternehmens, geltende Vorschriften einzuhalten.³⁰ Compliance ist aber gerade nicht begrenzt auf die Einhaltung der gesetzlichen Vorschriften; Compliance bedeutet vielmehr weitergehend, dass Unternehmen, ihre Organe sowie die untergeordneten Mitarbeiter im Einklang nicht nur mit den geltenden Gesetzen, sondern auch mit unternehmensinternen Richtlinien, sonstigen Vorgaben sowie etwa vertraglich vereinbarten Verpflichtungen handeln.³¹ Eine dahingehende Begriffsbestimmung findet dann auch im Deutschen Corporate Governance Kodex (DCGK) Niederschlag, der Compliance gemäß A.I. Grundsatz 5 des Kodex definiert als die „Einhaltung der gesetzlichen Bestimmungen und der internen Richtlinien und das Hinwirken auf deren Beachtung im Unternehmen“.³² Der DCGK verpflichtet den Vorstand in Grundsatz 5 ausdrücklich, für die Einhaltung der gesetzlichen Bestimmungen und der internen nach dem Richtlinien zu sorgen und auf deren Beachtung im Unternehmen hinzuwirken (Compliance). Nach Abschnitt A Grundsatz 5 des DCGK hat das interne Kontrollsystem und das Risikomanagementsystem auch ein an der Risikolage des Unternehmens ausgerichtetes Compliance-Management-System zu umfassen.

Der Betrieb eines Compliance-Management-Systems trägt dafür Sorge, dass Rechtsverstöße entweder gänzlich vermieden werden oder im Falle eines Verstoßes zumindest eine adäquate Reaktion des Unternehmens sichergestellt ist. Ziel des Betriebs eines Compliance-Management-Systems ist es insoweit, die – auch strafrechtliche – Haftung des Unternehmens und der Organe im Falle eines Regelverstoßes auszuschließen oder wenigstens die Konsequenzen zu verringern.³³ Neben dem Ziel der Enthaltung der Gesellschaft oder zumindest der Organe hat sich Compliance zwischenzeitlich aber auch als Wettbewerbsfaktor sowie als

29 Vgl. auch den Referentenentwurf des Finanzmarktintegritätsstärkungsgesetzes, S. 116 (www.bundesfinanzministerium.de).

30 Zur Compliance Pflicht → *Schulz*, Kap. 1.

31 Vgl. *Bock*, in: Rotsch, Wissenschaftliche und praktische Aspekte der nationalen und internationalen Compliance Diskussion, S. 63; *Heuking/von Coelln*, DÖV 2012, 827, 828; *Ohrtmann*, in: Bungenberg/Dutzi/Krebs/Zimmermann, Corporate Compliance und Corporate Social Responsibility, S. 185, 187; *Stanitzek*, Die Bedeutung von Criminal Compliance für das Strafrecht bei der Bekämpfung von Wirtschaftskorruption, S. 29; *Stober*, DVBl. 2012, 391, 391 f.; *Knierim*, in: Wabnitz/Janovsky, Handbuch Wirtschafts- und Steuerstrafrecht, 4. Aufl. 2014, 5. Kap. Rn. 5. Der Deutsche Corporate-Governance Kodex (DCGK) definiert unter A.I. Grundsatz 5 Compliance wie folgt: „Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der internen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmer hin (Compliance).“

32 Deutscher Corporate Governance Kodex i. d. F. v. 28.4.2022.

33 *Stanitzek*, Die Bedeutung von Criminal Compliance für das Strafrecht bei der Bekämpfung von Wirtschaftskorruption, S. 30. Zur Funktion von Compliance Management siehe auch → *Schulz*, Kap. 1 Rn. 13.

fester Bestandteil der Außendarstellung eines Unternehmens im Rahmen der sog. „Corporate Social Responsibility“ als sog. „Good Corporate Citizen“ etabliert.³⁴

- 26** In der Rechtswissenschaft ist es allerdings immer noch streitig, ob sich aus den – wenigen – bestehenden gesetzlichen Vorgaben eine grundsätzliche Compliance-Verpflichtung für Unternehmen bzw. deren Organe erschließt. Der Begriff der Compliance greift in der Gesetzgebung erst langsam Raum, ausgehend, wie gesagt, von einzelnen sektoralen Regelungen, die sich aufgrund internationaler Verknüpfungen anglo-amerikanischen Vorgaben angenähert haben. Zur Begründung einer konkreten Compliance-Verpflichtung wird daher häufig auf strafrechtliche Normen zurückgegriffen, die das Unternehmen – jedenfalls mittlerweile – zumindest faktisch zwingen, compliant am Markt zu agieren, um die schmerzhaften strafrechtlichen Konsequenzen, die das Unternehmen treffen können und die durchaus auch ein existenzgefährdendes Ausmaß annehmen können, abzuwenden.
- 27** Neben den unmittelbaren Folgen strafbaren Verhaltens aus dem Unternehmen heraus und den damit verbundenen persönlichen Konsequenzen für die Verantwortlichen des Unternehmens, also Geld- oder Freiheitsstrafe, der sog. Inhabilität sowie der Belastung des Unternehmens durch das Verfahren als solches und die mit der medialen Berichterstattung verbundenen Konsequenzen sind dies insbesondere die Instrumente der Einziehung gemäß §§ 73 ff. StGB sowie der Verbandsgeldbuße gemäß § 30 OWiG, die auch im Strafverfahren Anwendung findet. Kann gem. § 30 Abs. 2 OWiG gegen das Unternehmen bereits eine Geldbuße von bis zu 10 Mio. EUR verhängt werden, so erhöht sich diese bei Vorliegen eines abschöpfungsfähigen Erlöses, der aus der Straftat generiert wurde, gem. § 17 Abs. 4 OWiG schnell auf einen mehrstelligen Millionenbetrag.³⁵ Auch etwaige Kartellgeldbußen des Bundeskartellamtes erreichen über das Institut der sog. Mehrerlösgeldbuße gem. § 81 Abs. 4, 5 GWB i.V.m. § 17 Abs. 4 OWiG schnell dreistellige Millionenbeträge. Über das Institut der Einziehung gem. § 73 Abs. 1 StGB besteht die Möglichkeit der Abschöpfung illegal erworbener Vermögenswerte, womit dem (Unternehmen als) Täter der wirtschaftliche Anreiz zur Tatbegehung genommen werden soll, ihm sollen keine vermögenswerten Vorteile aus der Tat verbleiben.³⁶
- 28** In diesem Zusammenhang honoriert die Rechtsprechung jedoch ausdrücklich auch die Existenz eines Compliance-Management-Systems. Ausweislich der Rechtsprechung des Bundesgerichtshofs ist für die Bemessung der Verbandsgeldbuße gem. § 30 Abs. 3, § 17 Abs. 4 Satz 1 OWiG von Bedeutung, inwieweit ein Unternehmen seiner Pflicht, Rechtsverletzungen aus der Sphäre des Unternehmens zu unterbinden, genügt und ein effizientes Compliance-Management-

³⁴ Vgl. hierzu ausführlich → *Beisheim*, Kap. 16.

³⁵ Zur Verhängung von Verbandsgeldbußen in „Konzernsachverhalten“ ausführlich: *Böttger*, Verbandsgeldbuße (§ 30 OWiG), in: *Minkoff/Sahan/Wittig*, Konzernstrafrecht, § 12, S. 234 ff.

³⁶ *Kempf/Schilling*, Vermögensabschöpfung, § 1 Rn. 18.

System installiert hat, das auf die Vermeidung von Rechtsverstößen ausgelegt ist. Dabei soll es auch eine Rolle spielen, ob das Unternehmen in der Folge eines Verfahrens entsprechende Regelungen optimiert und seine betriebsinternen Abläufe so gestaltet hat, dass vergleichbare Normverletzungen zukünftig verhindert oder jedenfalls deutlich erschwert werden.³⁷

Als zentrale strafrechtliche Compliance-Norm wird vielfach **§ 130 OWiG** angesehen.³⁸ § 130 Abs. 1 Satz 1 OWiG verpflichtet den Inhaber eines Betriebs oder Unternehmens, Aufsichtsmaßnahmen zu treffen, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist. Sofern der Inhaber vorsätzlich oder fahrlässig die gebotenen Aufsichtsmaßnahmen unterlässt und damit ermöglicht, dass eine Zuwiderhandlung aus dem Unternehmen heraus begangen wird, die durch die Aufsichtsmaßnahmen verhindert oder wesentlich erschwert worden wäre, handelt er ordnungswidrig. Als erforderliche Aufsichtsmaßnahme führt § 130 Abs. 1 Satz 2 OWiG beispielhaft die Bestellung, sorgfältige Auswahl und Überwachung von Aufsichtspersonen auf. Auch hier drohen durchaus existenzbedrohende Sanktionen. Eine derartige Ordnungswidrigkeit kann, wenn die Pflichtverletzung strafbar ist, gem. § 130 Abs. 3 OWiG mit einer Geldbuße von bis zu 1 Mio. EUR sowie im Ausnahmefall über den Verweis gem. § 130 Abs. 3, 30 Abs. 2 Satz 3 OWiG darüber hinaus geahndet werden. Die Ordnungswidrigkeit gem. § 130 OWiG ist zudem Anknüpfungstat für die Verbandsgeldbuße des § 30 OWiG, sodass über diesen Umweg wiederum Geldbußen weit oberhalb der Millionengrenze verhängt werden können.

Unabhängig davon, ob aus den vorbezeichneten Vorschriften nunmehr eine gesetzliche Verpflichtung zur Implementierung eines Compliance-Management-Systems abzuleiten ist oder nicht, dürfte es jedoch unstreitig sein, dass die sog. Non-Compliance jedenfalls faktisch zu einer Haftung des Unternehmens und der Organmitglieder führt, sodass vice versa jedenfalls faktisch eine Pflicht zur Installation eines insbesondere strafrechtsbasierten Compliance-Management-Systems besteht. Da die gelungene Installation sowie der Betrieb eines Compliance-Management-Systems auf der anderen Seite aber durchaus auch zu Vorteilen für die Gesellschaft sowie die Organmitglieder führen kann, etwa bei der Zumessung einer Kartell- oder sonstigen Verbandsgeldbuße sowie bei der Entscheidung über Vergabeausschlüsse oder bei dem sog. Blacklisting, besitzt die Einführung und der Betrieb eines Compliance-Management-Systems jedenfalls, wie es in der Literatur bezeichnet wird, rechtliche Relevanz.³⁹

37 BGH, Urt. v. 9.5.2017 – 1 StR 265/16 („Panzerhaubitze“), Urt. v. 27.4.2022 – 5 StR 278/21, Rn. 118. Siehe hierzu auch → *Schulz*, Kap. 1 Rn. 59.

38 Etwa *Bock*, ZIS 2009, 68.

39 *Rotsch*, Criminal Compliance, § 1 Rn. 20.

III. Typische strafrechtliche Compliance-Risiken

- 31 Die Tatsache, dass insbesondere strafrechtliches Fehlverhalten zu den Kern-Compliance-Risiken in der Unternehmenspraxis zählt, wurde bereits dargestellt. Zugleich ist allerdings so gut wie jeder gesellschaftliche und auch unternehmerische Bereich Gegenstand auch strafrechtlich sanktionierter Verhaltensvorgaben. Die Möglichkeit strafrechtlichen Fehlverhaltens beschränkt sich damit bei Weitem nicht auf die im Strafgesetzbuch normierten Tatbestände des Kernstrafrechts, sondern umfasst insbesondere die diversen Tatbestände des Nebenstrafrechts. Jeder Bereich, der einer spezialgesetzlichen Regelung unterworfen ist, verfügt über flankierende Strafvorschriften, die die Einhaltung des jeweiligen Gesetzes sicherstellen sollen. Die Strafvorschriften des Nebenstrafrechts finden sich in buchstäblich jedem eigenständigen Rechtsgebiet von A bis Z, angefangen von der Abgabenordnung bis zum Zollrecht und finden sich selbst in exotischen Rechtsvorschriften, wie beispielsweise dem Halbleiterschutzgesetz, dem Designgesetz oder etwa auch dem Weingesetz. Strafrechtliche Compliance-Risiken schlummern damit grundsätzlich in jedem Gebiet unternehmerischer Betätigung und müssen insoweit für jedes Unternehmen je nach dem Schwerpunkt seiner Tätigkeit identifiziert werden.
- 32 Auch die ordnungswidrigkeitenrechtlichen Verstöße sind hierbei nicht außer Acht zu lassen, da auch im Falle „lediglich“ der Verwirklichung einer Ordnungswidrigkeit das Risiko der Einziehung gemäß § 29a OWiG und der Verbandsgeldbuße gemäß § 30 OWiG besteht. Darüber hinaus kann auch eine schlichte Ordnungswidrigkeit, wenn sie denn im (vermeintlichen) Unternehmensinteresse begangen wurde, zu einer Eintragung im Gewerbezentralregister sowie der Annahme einer etwaigen Unzuverlässigkeit des Unternehmers mit allen damit verbundenen Konsequenzen führen.
- 33 Ein Compliance-Risiko im engeren Sinne entsteht allerdings in erster Linie bei (vermeintlich) unternehmensnützigen Zuwiderhandlungen, da sich regelmäßig nur dann die straf- bzw. ordnungsrechtlichen Folgen für das Unternehmen einstellen. So ist Voraussetzung für die Einziehung etwa, dass der Täter, in diesem Fall das Unternehmen, etwas aus der Tat „erlangt“ hat. Auch Voraussetzung der Verhängung einer Verbandsgeldbuße gemäß § 30 OWiG ist entweder die Verletzung einer Pflicht, die das Unternehmen trifft, mithin einer betriebsbezogenen Pflicht, oder eine (beabsichtigte) Bereicherung des Unternehmens durch die Pflichtverletzung. Doch selbst im Falle eines eigenmächtigen und eigennützigen Verhaltens eines Mitarbeiters, durch das das Unternehmen möglicherweise sogar geschädigt wird, kann ein Compliance-Risiko für das Unternehmen entstehen. Dies ist etwa dann der Fall, wenn das Verhalten des Mitarbeiters entweder durch eine Aufsichtspflichtverletzung innerhalb des Unternehmens (§ 130 OWiG) ermöglicht wurde oder wenn ein echter „Exzess“ eines Einzeltäters dem Unternehmen zumindest mittelbar, etwa medial, zugerechnet wird mit der Folge, dass das Unternehmen zwar keine strafrechtlichen Folgen trifft, aber ein medialer Schaden entsteht, der zu einem Vertrauensverlust bei der Kundschaft oder gar einem

verminderten Börsenwert des Unternehmens führen kann. Zu denken wäre hier etwa an den Verrat von Geschäftsgeheimnissen eines Kreditinstituts an Dritte (oder gar ausländische Finanzbehörden) oder etwa das Fehlverhalten eines Mitarbeiters in ethisch schwierigen Branchen, bspw. der Chemie- oder der Lebensmittelindustrie. Dass auch Verstöße gegen eher abseitige Rechtsvorschriften zu erheblichen Compliance-Risiken führen können, zeigen etwa die Verstöße von Bankmitarbeitern gegen das aus dem Wertpapierhandelsgesetz folgende Manipulationsverbot, die bereits zu Verbandsgeldbußen in dreistelliger Millionenhöhe geführt haben.⁴⁰

In der Praxis haben sich jedoch einige wenige Bereiche als **Kern-Compliance-Risiken** herauskristallisiert, an erster Stelle die Korruption und die damit verbundenen weiteren strafrechtlichen Risiken. Bei der vermeintlich im Unternehmensinteresse liegenden *aktiven* Korruption besteht ein erhebliches strafrechtliches Risiko aufgrund der möglichen Abschöpfung des „Erlöses“, im Falle der *passiven* Korruption bestehen nicht unerhebliche wirtschaftliche Risiken für das betroffene Unternehmen. Im Falle der aktiven Korruption, also der Korruption aus dem Unternehmen heraus im (vermeintlichen) Unternehmensinteresse, erschließen sich darüber hinaus weitere strafrechtliche Folgerisiken für das Unternehmen. Da Bestechungsgelder üblicherweise nicht aus dem Nettovermögen der Unternehmensverantwortlichen geleistet werden, müssen diese Zuwendungen zunächst im Unternehmen „generiert“ werden, ohne dass dies bei der Abschluss- oder Betriebsprüfung auffällt. Versucht wird dies regelmäßig entweder durch die Schaffung einer „Schwarzen Kasse“ oder durch die Verbrämung des Bestechungsgeldes als „Provision“ oder „Beraterhonorar“. Die Schaffung einer schwarzen Kasse im Unternehmen wird von der Rechtsprechung allerdings per se als Untreuehandlung im Sinne von § 266 Abs. 1 StGB qualifiziert,⁴¹ die Umschreibung eines Bestechungsgeldes zum Zwecke der steuerlichen Geltendmachung (etwa als Beraterhonorar) stellt sich jedoch als Steuerhinterziehung gemäß § 370 Abs. 1 AO dar, da strafrechtlich relevante Zuwendungen gemäß § 4 Abs. 5 Satz 1 Nr. 10 EStG nicht als Betriebsausgaben abzugsfähig sind. Je nach Konstellation im Einzelfall kommt darüber hinaus auch noch eine Umsatzsteuerverkürzung oder eine Bilanzmanipulation im Sinne von § 331 HGB in Betracht. Schlussendlich kann sich der Umgang mit kontaminierten, also aus strafrechtlich relevanten Handlungen genierten Erträgen als Geldwäsche im Sinne von § 261 StGB darstellen.

Aufgrund der Vielzahl der bestehenden strafrechtlichen Compliance-Risiken je nach Betätigungsfeld des betroffenen Unternehmens beschränkt sich der vorliegende Beitrag auf die Darstellung der gerade angesprochenen Kern-Compli- 35

40 Hier hat die EU-Kommission im Jahre 2013 gegen mehrere Banken Geldbußen in Höhe von insgesamt 1,71 Mrd. EUR, die höchsten in der Geschichte der EU, verfügt. Die größte Geldbuße traf die Deutsche Bank mit 725 Mio. EUR.

41 BGH, Urt. v. 29.8.2008 – 2 StR 587/07, BGHSt 52, 323 (durch BVerfGE 126, 170 bestätigt).

ance-Risiken, die auch in der Beraterpraxis den absoluten Schwerpunkt ausmachen.

1. Korruption

- 36** Der Begriff „Korruption“ ist kein Rechtsbegriff, sondern ein aus kriminalpolitischer, kriminalistischer und kriminologischer Perspektive entwickelter Terminus zur Charakterisierung eines regelmäßig wenngleich auch nicht denknotwendig negativ besetzten Verhaltens.⁴² Kriminologisch wird Korruption definiert als Missbrauch eines öffentlichen Amtes, einer Funktion in der Wirtschaft oder eines politischen Mandats zur Erlangung eines Vorteils für sich oder einen Dritten, wobei ein Schaden oder Nachteil nicht bei dem bzw. den Handelnden, sondern lediglich mittelbar bei der Allgemeinheit oder bei einem Unternehmen entsteht. Nach der Definition des Bundesministeriums des Inneren ist Korruption ein Fehlverhalten, das über Jahrtausende in verschiedenen politischen Systemen mehr oder weniger stark ausgeprägt in unterschiedlichen Erscheinungsformen zu verzeichnen ist, in einem demokratischen Rechtsstaat jedoch nicht hinnehmbar ist.⁴³ Eine allgemeingültige Definition für den Begriff Korruption gibt es nicht, im **strafrechtlichen Sinne** umfasst der Begriff der Korruption lediglich die für strafbar erklärten Verhaltensweisen der folgenden Delikte:

- Vorteilsannahme und -gewährung (Amtsträger) gem. §§ 331, 333 StGB;
- Bestechlichkeit und Bestechung (Amtsträger) gem. §§ 332, 334 StGB;
- Bestechlichkeit und Bestechung im geschäftlichen Verkehr gem. §§ 299, 300 StGB;
- Bestechlichkeit und Bestechung im Gesundheitswesen gem. §§ 299a, b StGB;
- Wählerbestechung gem. § 108b StGB;
- Bestechlichkeit und Bestechung von Mandatsträgern gem. § 108e StGB;
- Bestechung ausländischer Abgeordneter gem. § 2 IntBestG;
- Beeinflussung von Betriebsratswahlen gem. § 119 BetrVG;
- Vorteilsgewährung in der Hauptversammlung gem. § 405 Abs. 3 Nr. 7 AktG (OWi).

- 37** Gesellschaftlich und ethisch geht der Begriff der Korruption weit darüber hinaus, so ist etwa an die Beeinflussung journalistischer Berichterstattung über neue Produkte durch ausgiebiges Sponsoring, Einladungen oder auch nur die Verknüpfung journalistischer Berichterstattung mit dem Anzeigenvolumen eines Unternehmens zu denken, die sog. „Schere im Kopf“. Trotz des Bemühens des Gesetzgebers, korruptionsrelevante Strukturen weitestgehend strafrechtlich zu erfassen, drängt sich die Erkenntnis auf, dass die Korruption die dunkle, um nicht zu sagen, inkriminierte Kehrseite einer gesellschaftlichen Vernetzung und eines Systems von Abhängigkeiten darstellt, das wiederum Grundlage der ge-

⁴² Kerner/Rixen, GA 1996, 355, 359 ff., unter Verweis auf die in totalitären Systemen bisweilen lebensrettende Funktion der Korruption; weitere Nachweise bei LK-StGB/Sowada, Vor § 331 Rn. 41.

⁴³ BMI, Texte zur Korruptionsprävention, 1. Einführung, 4.

sellschaftlichen Ordnung ist. Die Überschreitung von Grenzen zum Zwecke der Erlangung eines Vorteils, sei sie strafrechtlich relevant oder nicht, stellt ein globales Phänomen in Staat, Wirtschaft und Gesellschaft dar. So wird die Korruption auch ganz grundsätzlich als „Tausch von Vorteilen unter Regelverstößen“ definiert.

Die Problematik auch des Korruptionsstrafrechts liegt darin, dass die Grenzen zwischen gesellschaftlich erforderlichem und sogar gewünschtem Verhalten im Bereich Beziehungspflege und der strafrechtlich zu beanstandenden inkriminierten Beeinflussung fließend sind. Gerade im internationalen Geschäftsverkehr ist hinlänglich bekannt, dass ohne bestimmte Formen der Zuwendung (sog. „Türöffner“, „Beschleunigungsgelder“, „Bakschisch“⁴⁴ etc.) kaum ein Geschäftsabschluss zustande kommt bzw. kaum eine Amts- oder Diensthandlung zeitnah erfolgt. Die Zahlung nützlicher Aufwendungen, sog. „NA“, durch deutsche Unternehmen im Ausland war bis in das Jahr 1999 sogar steuerlich absetzbar.⁴⁵ Auch in Deutschland war bis in das Jahr 1997 hinein die sog. „Klimapflege“ gegenüber Amtsträgern sowie im politischen Bereich die sog. „Landschaftspflege“ üblich und nicht strafbewehrt. Dies hat sich durch das KorBekG im Jahr 1997 (s. o.) dramatisch geändert. Bis dahin unbeanstandete Formen der Beziehungspflege mit Amtsträgern bis hin zur schlichten Essenseinladung sind nunmehr unter dem Aspekt des „Anfütterns“ strafrechtlich relevant, nach der Rechtsprechung des BGH⁴⁶ reicht bereits die Schaffung des „bösen Anscheins möglicher Käuflichkeit“ für die Verwirklichung des Tatbestands der Vorteilsannahme aus.

Klassische **Compliance-Konflikte** ergeben sich hier insbesondere im Bereich des (internationalen) Vertriebs. Zweifelhafte Zuwendungen werden insbesondere in bestimmten ausländischen Märkten als unverzichtbares Akquisitionsmittel angesehen. Hierbei ist insbesondere zu berücksichtigen, dass sich deutsche Unternehmen, die sich auf vermeintlich (landes-)übliche Praktiken einlassen, im Wettbewerb mit ausländischen Unternehmen befinden, die zwar ausweislich der Vorgaben der OECD unter ähnlichen Strafandrohungen stehen sollten, die jedoch nicht ansatzweise mit ähnlicher Konsequenz wie durch die deutschen Ermittlungsbehörden kontrolliert werden. „Wenn wir’s nicht machen, macht’s der Franzose“, dieser Satz bringt die Verzweiflung des deutschen Wettbewerbers zum Ausdruck, der insbesondere von den deutschen Ermittlungsbehörden streng kontrolliert wird und vermeintlich nur die Wahl zwischen einem rechtskonformen Verhalten (nach deutschem Recht) und dem Verlust des Auftrags an den ausländischen Wettbewerber sieht. Hier offenbart sich, dass zunächst eine ungleich stringente Strafverfolgung⁴⁷ zu einem manifesten Wettbewerbsnachteil

44 Persisch: „Gabe, Geschenk, auch Trinkgeld“.

45 Vgl. BT-Drs. 13/1717 v. 19.6.1995.

46 BGH, NStZ 2005, 334.

47 Dem OECD Progress Report 2013 der Antikorruptionsorganisation Transparency International zufolge versagt die Mehrheit der OECD-Exportnationen bei der aktiven Verfolgung der

mutieren kann, andererseits zeigt sich, dass die deutsche Regierung gut daran tut, im internationalen Bereich auf eine gleichförmige Umsetzung der OECD-Vorgaben und eine entsprechende Strafverfolgung zu drängen. Konsequenterweise wird die Auslandsbestechung insbesondere durch die US-amerikanischen Gesetze geahndet und durch die US-amerikanischen Behörden verfolgt. Zu berücksichtigen ist allerdings auch, dass die US-amerikanischen Behörden „ihren“ Unternehmen im Gegenzug dem Vernehmen nach mit geheimdienstlichen Mitteln Informationen verschaffen, die den Wettbewerbsnachteil der strengen Korruptionsgesetzgebung und deren Umsetzung dadurch quasi kompensieren.⁴⁸ Ebenso bemerkenswert ist der UK Bribery Act 2010, der nicht nur eine Strafbarkeit von Unternehmen für die unterlassene Verhinderung von Bestechung vorsieht (§ 7), sondern die Anwendbarkeit gleich auch auf ausländische, mithin auch deutsche Unternehmen erstreckt, wenn auch nur ein allgemeiner Bezug zu Großbritannien besteht, etwa ein Bevollmächtigter dort gehandelt hat (§ 12 Abs. 5).

- 40 Strukturell sind bei der Korruption zunächst die beiden großen Bereiche der Amtsträgerkorruption (oder auch der „öffentlichen Korruption“) sowie der Bestechung und Bestechlichkeit im geschäftlichen Verkehr („Privatkorruption“) zu unterscheiden. Ist der Vorteilsempfänger ein Amtsträger oder ein für den öffentlichen Dienst besonders Verpflichteter, so finden die weitergehenden und weitestgehend strengen Vorschriften der §§ 331 ff. StGB (Amtsträgerkorruption) Anwendung. Die Amtsträgerkorruption zeichnet sich insbesondere durch eine Vorverlagerung der Strafbarkeit bereits in den Bereich des „Anfütterns“ oder der Klimapflege aus, Voraussetzung der Strafbarkeit ist insofern nur die schlichte Annahme eines Vorteils für die Dienstausübung, die Vereinbarung einer pflichtwidrigen Diensthandlung als Gegenleistung ist im Rahmen der sog. Vorteilsannahme (§ 331 StGB) bzw. der Vorteilsgewährung durch den Vorteilsgeber (§ 333 StGB) nicht erforderlich.
- 41 Wird mit dem Amtsträger darüber hinaus als Gegenleistung für den Vorteil die Erbringung einer pflichtwidrigen Diensthandlung vereinbart, so liegt der Tatbestand der Bestechlichkeit (des Amtsträgers) gem. § 332 StGB bzw. der Bestechung (durch den Vorteilsgeber) gem. § 334 StGB vor, der über ein deutlich erhöhtes Strafmaß (bis zu 10 Jahren Freiheitsstrafe) verfügt. Durch das Gesetz zur Bekämpfung der Korruption vom 20.11.2015 hat der Gesetzgeber durch Aufnahme des **Europäischen Amtsträgers**⁴⁹ in den Gesetzeswortlaut der §§ 331 ff. StGB sowie durch die Erfassung auch ausländischer und internationaler Be diensteter durch § 335a StGB auch formal die bislang nur durch Nebengesetze⁵⁰

Auslandsbestechung. Danach sind Deutschland, die Schweiz, Großbritannien und die USA die einzigen Länder weltweit, in denen eine aktive Verfolgung stattfindet. Zu den wenig aktiven Ländern gehören Frankreich, Schweden, Norwegen oder auch Dänemark. Kaum eine oder keine Verfolgung findet u. a. in Russland, Griechenland, Japan, Polen oder der Türkei statt.

48 Vgl. etwa Süddeutsche Zeitung v. 12.7.2013 „Ausgespäht und ausgenommen“.

49 Die Definition des Europäischen Amtsträgers findet sich in § 11 Abs. 1 Nr. 2 lit. a StGB.

50 IntBestG und EUBestG.

erfassten ausländischen Amtsträger und Bediensteten ausdrücklich in den Geltungsbereich der Amtsträgerkorruption einbezogen.

Hiervon grundsätzlich zu unterscheiden ist der Bereich der Bestechlichkeit und Bestechung im geschäftlichen Verkehr gemäß § 299 StGB, die sog. „Angestellten- oder Beauftragtenkorruption“. Strafbewehrt ist hier die Annahme von Vorteilen durch Angestellte oder Beauftragte eines geschäftlichen Betriebs im geschäftlichen Verkehr. Die schlichte Annahme (oder spiegelbildlich Gewährung) eines Vorteils reicht hier allerdings nicht aus, erforderlich ist hier – anders als bei der Amtsträgerkorruption – der Abschluss einer konkreten Unrechtsvereinbarung, mithin die Erbringung einer konkreten Gegenleistung, die in einer unlauteren Bevorzugung des Vorteilsgebers liegen muss. Seit der Erweiterung des Tatbestands um das sog. „Geschäftsherrenmodell“ im Jahre 2015⁵¹ kann die vereinbarte „Gegenleistung“ neuerdings auch bereits darin liegen, dass der Angestellte oder Beauftragte – im Interesse des Vorteilsgewährenden – seine Pflichten gegenüber dem Unternehmen verletzt. 42

Die Spezialvorschriften der Bestechlichkeit und Bestechung im Gesundheitswesen (§§ 299a, b StGB), der Bestechlichkeit und Bestechung von Mandatsträgern (§ 108e StGB) oder etwa der Beeinflussung von Betriebsratswahlen durch Gewährung von Vorteilen (§ 119 BetrVG) erfassen hierbei bestimmte Empfängerkreise, die weder als Amtsträger noch als Angestellte oder Beauftragte qualifiziert werden können, die aber nach Auffassung des Gesetzgebers einer hohen Korruptionsanfälligkeit unterliegen und deren Unbestechlichkeit eines besonderen Schutzes durch Sondervorschriften bedurfte. 43

a) Vorteilsgewährung (§ 333 StGB)

Der Tatbestand der Vorteilsgewährung (§ 333 StGB) – spiegelbildlich die Vorteilsannahme (§ 331 StGB) – ist dazu bestimmt, das Vertrauen der Allgemeinheit in die Integrität von Trägern staatlicher Funktionen und damit zugleich in die Sachlichkeit staatlicher Entscheidungen zu schützen.⁵² 44

Empfänger des zu gewährenden Vorteils muss damit ein **Amtsträger**, ein Europäischer Amtsträger oder ein für den öffentlichen Dienst besonders Verpflichteter sein. Entscheidend ist, dass der Empfänger des Vorteils zum Zeitpunkt der Tat schon oder noch Amtsträger im Sinne des Gesetzes ist. Der Begriff des Amtsträgers i. S. d. §§ 331 ff. StGB ist in § 11 Abs. 1 Nr. 2 StGB, der des Europäischen Amtsträgers ist in § 11 Abs. 1 Nr. 2 lit. a StGB legal definiert.⁵³ Amtsträger ist demnach, wer nach deutschem Recht Beamter oder Richter ist, wer in einem sonstigen öffentlich-rechtlichen Amtsverhältnis steht oder sonst dazu bestellt ist, einer Behörde oder einer sonstigen Stelle oder in deren Auftrag Aufgaben der öffentlichen Verwaltung unbeschadet der zur Aufgabenerfüllung ge- 45

⁵¹ Gesetz zur Bekämpfung der Korruption v. 20.11.2015, BGBl. I 2015, S. 2025.

⁵² Vgl. BGHSt 49, 214; 43, 370, 377.

⁵³ Aus Gründen der Vereinfachung wird im Weiteren nur von „Amtsträger“ gesprochen.

wählten Organisationsform wahrzunehmen. Die Prüfung, ob es sich bei dem Vorteilsempfänger um einen Amtsträger im Sinne des Gesetzes handelt, ist allerdings hochkomplex und Gegenstand einer äußerst umfangreichen Kasuistik in der Rechtsprechung. Um den Umfang der hiesigen Darstellung nicht zu sprengen, muss insoweit auf die einschlägige Kommentarliteratur oder die insoweit aussagekräftigen Handbücher zum Wirtschaftsstrafrecht verwiesen werden.⁵⁴

- 46 Gerade die Frage, ob es sich bei einem potenziellen Vorteilsempfänger um einen Amtsträger oder einen für den öffentlichen Dienst besonders Verpflichteten handelt, birgt ein erhebliches **Compliance-Risiko**. Zwar liegt die Amtsträgereigenschaft eines Empfängers häufig, insbesondere bei einem bestehenden Beamtenverhältnis, auf der Hand, in einer Vielzahl von Einzelfällen ist aber prima facie, auch für den juristisch geschulten Betrachter, kaum ersichtlich, ob es sich um einen Amtsträger handelt oder nicht. Als Amtsträger angesehen werden beispielsweise Prüferingenieure für Baustatik, Verkehrspiloten, Planungsingenieure, die längerfristig mit Ausschreibungen oder Vergaben der öffentlichen Hand beauftragt sind, oder auch Redakteure der öffentlich-rechtlichen Rundfunkanstalten.⁵⁵ Amtsträger sind auch etwa die Organmitglieder von Landesbanken oder von Sparkassen als Anstalten des öffentlichen Rechts, da auch diese nach den jeweiligen Sparkassengesetzen Aufgaben der öffentlichen Verwaltung wahrnehmen. Angestellte von Kommunalbanken oder Sparkassen sind jedoch regelmäßig nur dann als Amtsträger anzusehen, wenn und soweit die Sparkasse im Rahmen ihrer Tätigkeit als Kommunalbank tätig wird und damit Aufgaben öffentlicher Verwaltung wahrnimmt.⁵⁶ Bei den weniger exponierten Mitarbeitern solcher Kreditinstitute ist darüber hinaus darauf zu achten, dass diese möglicherweise generell „Verpflichtungserklärungen“ im Sinne des Verpflichtungsgesetzes abgegeben haben und damit auch Adressaten der Amtsdelikte geworden sind.

- 47 In hohem Maße problematisch ist auch die Tatsache, dass Amtsträger gemäß § 11 Abs. 1 Nr. 2 lit. c StGB auch ist, wer nach deutschem Recht „sonst dazu bestellt ist, bei einer Behörde oder bei einer sonstigen Stelle oder in deren Auftrag Aufgaben der öffentlichen Verwaltung wahrzunehmen“. Erscheint hier bereits die gesetzliche Definition kaum nachvollziehbar, so überrascht die hierzu ergangene Kasuistik des BGH umso mehr. Bei einer solchen „sonstigen Stelle“ kann es sich nämlich durchaus auch um juristische Personen des Privatrechts handeln, wenn diese etwa Aufgaben der Daseinsvorsorge ausführen und, so der BGH, als „verlängerter Arm des Staates“ erscheinen. In der Praxis werden Aufgaben der Daseinsvorsorge etwa durch Stadtwerke, Verkehrsbetriebe, kommunale Wohnungsbaugesellschaften oder sonstige kommunale Beteiligungsgesellschaften wahrgenommen, die im Rechtsverkehr allerdings als GmbH oder Aktiengesellschaft firmieren und deren Organmitglieder (Geschäftsführer, Vorstände oder

54 Eine detaillierte Übersicht findet sich etwa bei: Böttger, Wirtschaftsstrafrecht, Kap. 5, S. 344 ff.

55 Vgl. BGH, NJW 2010, 784 ff.

56 BGH, Beschl. v. 11.12.2019 – 5 StR 486/19, Rn. 13 ff.

Aufsichtsräte) prima vista natürlich nicht als Amtsträger wahrgenommen werden. Nach der auch hier äußerst unübersichtlichen Kasuistik sind etwa im kommunalen Alleinbesitz befindliche Stadtwerkegesellschaften, sei es in der Rechtsform der GmbH oder der AG, als sonstige Stelle qualifiziert worden, ebenso etwa das Versorgungswerk der Rechtsanwälte, öffentlich-rechtliche Rundfunkanstalten oder auch die Deutsche Bahn Netz AG, nicht jedoch die Deutsche Bahn AG. Gesetzgeberische Absicht war es, das „Vertrauen in die Nicht-Käuflichkeit dienstlichen Handelns“ (BGHSt 47, 295, 303) auch im Rahmen veränderter staatlicher Organisationsformen aufrechtzuerhalten; erkaufte wurde diese Absicht der Erstreckung des Amtsträgerstrafrechts auf privatrechtliche Organisationsformen allerdings durch eine fast grenzenlose Unbestimmtheit des Amtsträgerbegriffs. Aufgrund der Komplexität und Widersprüchlichkeit der Kasuistik in der Rechtsprechung, welche (privatwirtschaftlich organisierte) Gesellschaft eine sonstige Stelle ist und wer bei einer solchen Stelle Amtsträger ist, kann von einer „Vorhersehbarkeit staatlichen Strafens“ hier kaum mehr die Rede sein, das Korruptionsstrafrecht ist insoweit zum „Case Law“ mutiert.

Der Amtsträger muss für die Dienstausbübung einen **Vorteil** entweder für sich oder einen Dritten (sog. Drittvierteil) fordern, sich versprechen lassen oder annehmen. Einen aus compliance-technischer Sicht sicheren Bereich bietet auch das Tatbestandsmerkmal des Vorteils nicht. Unter einem Vorteil ist jede Leistung zu verstehen, auf die der Amtsträger keinen Anspruch hat und die seine wirtschaftliche, rechtliche oder auch nur persönliche Lage objektiv verbessert.⁵⁷ Besser gestellt wird der Amtsträger vor allem durch materielle Zuwendungen jeder Art, aber auch immaterielle Vorteile werden vom Tatbestand erfasst. Als **materielle Vorteile** sind in der Rechtsprechung insbesondere anerkannt:

- Geld⁵⁸ und Sachwerte;⁵⁹
- die Nutzungsmöglichkeit von Gegenständen;⁶⁰
- die Erbringung von Dienst- und Werkleistungen;⁶¹
- die Einräumung von Rabatten und sonstigen Vergünstigungen;⁶²
- die Gewährung von (zinslosen) Darlehen;⁶³
- der Erlass oder die Stundung von Forderungen;⁶⁴
- die Übernahme von Kosten für Urlaubs- und Kongressreisen;⁶⁵
- die Einladung zu entgeltlichen Veranstaltungen (Fußball-WM-Tickets);⁶⁶

⁵⁷ BGHSt 53, 6; 47, 295, 304; BGH, NStZ 2008, 216, 217; NStZ-RR 2007, 309.

⁵⁸ BGHSt 49, 275, 282 m. w. N.

⁵⁹ BGHSt 47, 22, 23; 39, 45, 46.

⁶⁰ BGHSt 15, 239; BGH, NJW 1985, 391.

⁶¹ BGH, NStZ 2004, 565; 1991, 550.

⁶² BGH, NJW 2001, 2558.

⁶³ BGHSt 13, 328; BGH, NStZ 2005, 334, 335.

⁶⁴ BGH, NStZ 1991, 550.

⁶⁵ BGH, NJW 2003, 763, 764; NStZ 2005, 334, 335.

⁶⁶ BGHSt 53, 6, 11.

Teil 1 Grundlagen, Erfolgsfaktoren und Handlungsstrategien

- die Einladung in Gourmet-Restaurants;⁶⁷
 - die Bezahlung sexueller Leistungen durch Prostituierte;⁶⁸
 - die Ausrichtung und Finanzierung von Feiern und sonstigen Veranstaltungen, deren Kosten eigentlich der Amtsträger hätte tragen müssen;⁶⁹
 - die Honorarzahlung für ein (wertloses) Gutachten;⁷⁰
 - Vermittlung eines (Schein-)Beratervertrags;⁷¹
 - erbrechliche Begünstigungen;⁷²
 - Vermittlung einer Nebentätigkeit (z. B. entgeltliche Vorträge), auch wenn diese adäquat vergütet wird (str.).⁷³
- 49** Wertmäßig ist hier eine Begrenzung kaum möglich, auch geringwertige Geschenke fallen unter den Vorteilsbegriff.⁷⁴ Einen „Safe-Harbor“ im Hinblick auf eine zulässige Hingabe von Vorteilen an einen Amtsträger gibt es damit nicht. Insbesondere die Vereinbarung eines adäquaten Austauschverhältnisses mit dem Amtsträger, etwa durch einen Beratervertrag o. Ä., auch wenn dieser von einer Nebentätigkeitsgenehmigung des Beamten gedeckt sein sollte, hilft hier kaum weiter. Nach der Rechtsprechung des BGH soll ein Vorteil nämlich bereits im Abschluss eines solchen Vertrags liegen, wenn dieser Leistungen an den Amtsträger zur Folge hat und zwar selbst dann, wenn diese nur ein angemessenes Entgelt für aufgrund des Vertrages geschuldete Leistungen seien. Andernfalls, so der BGH, könnten die Bestechungstatbestände stets durch die Vereinbarung eines Auftragsverhältnisses zwischen Amtsträger und Leistungsgeber ausgeschlossen werden.⁷⁵
- 50** Für die Erfüllung des Tatbestands ist eine sog. „**Unrechtsvereinbarung**“ erforderlich, die allerdings bereits dann vorliegt, wenn der Vorteilsgeber dem Amtsträger einen Vorteil „für die Amtsausübung“ zuwendet. Eine Gegenleistung, etwa die pflichtwidrige Erteilung einer Genehmigung o. Ä., ist für die Erfüllung des Tatbestands nicht erforderlich, es reicht aus, dass der Vorteil im weitesten Sinne im Hinblick auf die Dienstaussübung des Amtsträgers gewährt wird. Wird mit dem Amtsträger eine pflichtwidrige Gegenleistung für die Hingabe des Vorteils vereinbart, liegt der (Qualifikations-)Tatbestand der Bestechung gemäß § 334 StGB vor, der über einen deutlich erhöhten Strafraum verfügt.
- 51** Durch die Strafdrohung hinsichtlich der schlichten Gewährung eines Vorteils im Hinblick auf die dienstliche Tätigkeit des Amtsträgers wird die Strafbarkeit im

67 BGHSt 47, 22, 23; BGH, NStZ 2000, 90.

68 BGH, NJW 1989, 914, 915.

69 BGHSt 48, 44.

70 BGH, NStZ 1999, 561.

71 BGH, NJW 2001, 3062, 3063.

72 LK-StGB/Sowada, § 331 Rn. 33, unter Bezugnahme auf das Rundschreiben zum Verbot der Annahme von Belohnungen und Geschenken in der Bundesverwaltung vom 8.11.2004.

73 BGHSt 31, 264, 280 m. w. N.; BGH, NStZ-RR 2007, 309, 310.

74 BGH, NStZ 2000, 596, 599; 1998, 194.

75 BGH, Urt. v. 26.5.2011 – 3 StR 492/10; BGHSt 31, 264, 280.

Sinne einer weitestmöglichen Abschreckung nicht nur deutlich vorverlagert, es offenbaren sich auch erhebliche **Compliance-Risiken**. Übliche Formen des gesellschaftlichen Umgangs miteinander sowie der Höflichkeit geraten hier jedenfalls, soweit Amtsträger betroffen sind, in den Bereich der Strafbarkeit. Erklärte Absicht des Gesetzgebers war es, insoweit bereits die Schaffung eines Näheverhältnisses zwischen Amtsträger und Interessent, das sog. „Anfüttern“, die „Klimapflege“ oder die „Schaffung der Allgemeinen Geneigtheit“ einer Strafandrohung zu unterwerfen.⁷⁶ Dem Gesetzgeber wie auch dem BGH ist bewusst, dass der Tatbestand der Vorteilsgewährung – insbesondere nach der Auslegung durch die obergerichtliche Rechtsprechung – im Randbereich kaum mehr trennscharfe Konturen aufweist und im Ergebnis nicht nur zu Beweisschwierigkeiten führen kann, sondern dem Tatrichter vielmehr eine beträchtliche Entscheidungsmacht einräumt.⁷⁷ Der „Preis“ dieser tatbestandlichen Erosion liegt bereits jetzt in einer völligen Verunsicherung der potenziellen Adressaten der Korruptionstatbestände im öffentlich-rechtlichen Wirtschaftsraum, etwa in kommunalen Gebietskörperschaften oder Beteiligungsgesellschaften, die aus Sorge vor unberechenbaren strafrechtlichen Konsequenzen auch wirtschaftlich sinnvolle Entscheidungen für die öffentliche Hand kaum mehr treffen, so etwa im Bereich des Sponsorings im Rahmen sog. PPP-Projekte⁷⁸ oder des Kultursponsorings. Auch die Annahme gesellschaftlich in hohem Maße erwünschter Vorteile durch Amtsträger, wie etwa das Einwerben von Drittmitteln durch Universitätsprofessoren, wird vom Tatbestand des § 331 Abs. 1 StGB erfasst. Nur durch den „Klimmzug“ einer teleologischen Restriktion des Tatbestands ist der BGH zur Straffreiheit des in den Hochschulgesetzen sogar geforderten Verhaltens gekommen. Tatsächlich führt diese Art der „Korruptionsbekämpfung“ durch Gesetzgeber und Gerichte zu ernsthaften Problemen im Bereich der Vorhersehbarkeit staatlichen Strafens bis hin zur Preisgabe der tatbestandlichen Bestimmtheit entgegen Art. 103 Abs. 2 GG und damit auch zu erheblichen Problemen in der Compliance-Beratung.

Ein Versuch einer Strafbarkeitsrestriktion mit dem Ziel, nicht jeglichen gesellschaftlichen Umgang mit einem Amtsträger dem Risiko der Strafbarkeit auszusetzen, findet sich im Bereich der sog. „**Sozialadäquanz**“, deren Grenze jedoch umstritten ist. Unter dem Gesichtspunkt der Sozialadäquanz sind lediglich in gewissem Umfang übliche und deshalb sozialadäquate Vorteile von der Strafbarkeit ausgenommen, etwa wenn diese Vorteile ihren Grund in den Regeln des sozialen Verkehrs oder der Höflichkeit haben.⁷⁹ Als Paradebeispiel für eine sozialübliche Zuwendung ist etwa das weihnachtliche Trinkgeld für die Müllabfuhr oder auch das Trinkgeld an einen Postzusteller oder Spende in die Kaffee-kasse der Station eines Krankenhauses anzusehen. Eine Strafbarkeit entfällt aber nicht etwa grundsätzlich deshalb, weil entsprechende Vorteilsgewährungen in

52

⁷⁶ Vgl. BR-Drs. 298/95, S. 9; BT-Drs. 13/3353, S. 11.

⁷⁷ BGH, 14.10.2008 – 1 StR 260/08, BGHSt 53, 6 = NJW 2008, 3580.

⁷⁸ Public Private Partnership; vgl. hierzu *Bock/Borrmann*, ZJS 2009, 625.

⁷⁹ BGH, NStZ-RR 2002, 272.

bestimmten Bereichen oder Branchen – gar unabhängig von der Höhe der Zuwendung – üblich wären. Auch hier ist die Rechtsprechung des BGH äußerst restriktiv, lediglich geringwertige Aufmerksamkeiten aus gegebenen Anlässen werden vom Tatbestand ausgenommen. Schließlich, so der BGH, lasse sich eine Sozialadäquanz nicht alleine aus einer etwaigen Üblichkeit herleiten, da dies bestehende Strukturen der Korruption vielmehr verfestigen würde. Wichtig sind insoweit natürlich die beamtenrechtlichen Grenzen der Zulässigkeit der Annahme von Vorteilen, die üblicherweise äußerst niedrig liegen; diese stellen zwar keine starre Grenze dar, ab wann eine sozialadäquate Zuwendung nicht mehr vorliegt, sie haben aber für den jeweiligen Regelungsbereich Indizcharakter. Es liegt auf der Hand, dass die Grenzen hierbei fließend sind und sehr stark von dem gesellschaftlichen Umfeld der potenziellen Diensthandlung abhängen. Als strafrechtliche (nicht dienstrechtliche) **Mindestgrenze**, unterhalb derer eine Unrechtsvereinbarung aufgrund Sozialadäquanz regelmäßig nicht vorliegt, ist ein Wert von **50,00 EUR** anzusehen. Zum einen entspricht dies der im Strafrecht allgemein anerkannten Grenze der Geringfügigkeit, zum anderen dürfen gem. **§ 4 Abs. 5 Satz 1 Nr. 1 EStG** Geschenke bis zu einem Wert von 50,00 EUR p.a. steuerlich gewinnmindernd geltend gemacht werden. Fördert der Staat jedoch betrieblich veranlasste Geschenke bis zu einem Wert von 50,00 EUR p.a. auf der einen Seite, so gebietet die Einheitlichkeit der Rechtsordnung, dass er diese Zuwendung auf der anderen Seite nicht als strafrechtlich relevant wertet. Auch hier mag es im Einzelfall Ausnahmen geben, so etwa die Vereinbarung, einem Polizeibeamten als Gegenleistung für das Unterlassen einer Anzeige einen Betrag von 20,00 EUR zuzuwenden. Gibt es keinen Anlass, einem Verkehrspolizisten oder Lebensmittelprüfer Bargeld zuzuwenden oder diesen zu einem Abendessen einzuladen, so entspricht die Erörterung von Sachfragen mit einem Landesbankvorstand oder einem Geschäftsführer einer privatrechtlich organisierten „sonstigen Stelle“ bei einem Arbeitsessen oder im Rahmen einer Repräsentationsveranstaltung durchaus der gesellschaftlichen Üblichkeit.⁸⁰ Im Geschäftsverkehr mit Amtsträgern, insbesondere wenn sich deren Amtsträgereigenschaft aus der Organstellung bei einer sonstigen Stelle ableitet, aber auch bei der Wahrnehmung von Repräsentationsaufgaben, ist der Grenzwert damit (deutlich) höher anzusetzen. So entspricht etwa die Einladung zu einem Arbeitsessen bei einem Wert von bis zu 100,00 EUR oder auch die Einladung zu einem Fußballspiel nicht nur der gesellschaftlichen Üblichkeit, sondern durchaus auch der Sozialadäquanz. Jedenfalls, so der BGH, „handelt es sich bei Zuwendungen im Wert von mehreren Hundert Euro nicht mehr um geringwertige Aufmerksamkeiten“.⁸¹

- 53 Compliance-Risiken** bestehen auch und insbesondere dort, wo die Zusammenarbeit mit der öffentlichen Hand quasi institutionalisiert ist und die öffentliche

80 Zum Aspekt des Arbeitsessens vgl. auch BGH, wistra 2003, 303, 305.

81 BGH, Urt. v. 26.5.2011 – 3 StR 492/10, Rn. 29.

Hand auf eine solche Zusammenarbeit angewiesen ist, wie etwa bei der **Einwerbung von Drittmitteln** für die universitäre Lehre und Forschung oder im Bereich der Wahlkampf- und **Parteispenden**. Auch hier gibt es eine ausgeprägte Judikatur, auf die insoweit lediglich verwiesen werden kann.⁸² Die Angst vor der Überschreitung der von Gesetzgebung und Justiz bewusst schwammig gehaltenen Grenzen hat in vielen Bereichen dazu geführt, dass sich ganze Branchen oder Branchenverbände umfangreiche Kodizes geben, die zumindest Leitlinien für eine Risikoreduktion enthalten („**Best Practice**“), wenngleich die Rechtsprechung solche Richtlinien grundsätzlich nicht als Konkretisierung der einschlägigen Tatbestände akzeptiert, sondern auch diesen lediglich Indizcharakter zumisst. Solche Richtlinien finden sich etwa in der Pharma- und der Medizintechnikbranche, mithin zwei Bereichen, die als habituell korruptionsgefährdet gelten und auch schon schwere Korruptionsskandale durchleiden mussten, erinnert sei insoweit nur an den „ratiopharm-Skandal“ oder an den sog. „Herzklappenkomplex“. In diesen Kodizes, hier dem Pharma Kodex⁸³ und dem Kodex Medizinprodukte,⁸⁴ findet sich eine dezidierte Beschreibung einer für zulässig gehaltenen Sponsoring- und Einladungspraxis, die die jeweiligen Konstellationen bis ins kleinste Detail regelt.

Risiken ergeben sich auch und insbesondere im Bereich des Sport- und Kultursponsorings oder auch im Bereich neuerer Formen der Zusammenarbeit zwischen öffentlichen Stellen und der Privatwirtschaft (sog. **PPP-Projekte**). Zwar mag es denkbar sein, dass ein Amtsträger „gewissermaßen unter dem Deckmantel Sponsoring/Repräsentation“⁸⁵ geneigt gemacht werden kann, ließe man in den Fällen des Sponsorings aber allein den bösen Anschein der Käuflichkeit ausreichen, wäre dies das voraussichtliche Ende des Sport- und Kultursponsorings mit den entsprechenden fiskalischen Folgen für die öffentlichen Stellen. Besondere Vorsicht ist auch im Bereich des sog. „**Fundraising**“ geboten, da die Annahme „geforderter“ Vorteile für den Amtsträger gem. § 331 Abs. 3 StGB nicht genehmigungsfähig ist.⁸⁶

Um den drohenden Rückzug der Sponsoren aus dem **Sport- und Kultursponsoring** zu verhindern und den Unternehmen als Orientierungsrahmen zur Abgrenzung von Kontaktpflege und Gastfreundschaft von Fällen der Korruption zu dienen, hat die Sponsorenvereinigung S20 gemeinsam mit dem Bundesinnenministerium und dem Deutschen Olympischen Sportbund bereits im Jahre 2011

82 Hierzu ausführlich etwa: Böttger, Wirtschaftsstrafrecht, Kap. 5, Rn. 96.

83 Kodex für die Zusammenarbeit der pharmazeutischen Industrie mit Ärzten, Apothekern und anderen Angehörigen medizinischer Fachkreise, herausgegeben von den Mitgliedsunternehmen des Vereins „Freiwillige Selbstkontrolle für die Arzneimittelindustrie e. V.“ (FSA).

84 Kodex Medizinprodukte (2015) des Bundesverbandes Medizintechnologie e. V. (BVMed); noch ausführlicher: „Gemeinsamer Standpunkt zur strafrechtlichen Bewertung der Zusammenarbeit zwischen Industrie, medizinischen Einrichtungen und deren Mitarbeitern“ des BVMed.

85 BGHSt 53, 6 ff. mit weiteren Ausführungen zum Vorteilsbegriff im Bereich „Hospitality“.

86 Bernsmann/Gatzweiler, Verteidigung bei Korruptionsfällen, Rn. 466.

einen Leitfaden „**Hospitality und Strafrecht**“ erstellt.⁸⁷ Der Leitfaden beschreibt typische Einladungskonstellationen (Fachveranstaltungen, gemischte Veranstaltungen sowie Sport- und Unterhaltungsveranstaltungen) und erläutert, worauf der Einladende achten sollte, um strafrechtliche Risiken so gering wie möglich zu halten. Für eine Risikoreduktion ist dieser Leitfaden sicherlich hilfreich, in der Rechtsprechung ist er jedoch bislang ohne Resonanz geblieben.

- 56** Will man nicht jegliche Form des Umgangs und der Kooperation mit Amtsträgern generell unterbinden und als angemessen bewertete Umgangs- bzw. Kooperationsformen beibehalten, so bietet compliance-technisch das Institut der **Genehmigung** der Vorteilsgewährung durch den Dienstherrn des Amtsträgers einen gewissen Handlungsspielraum. Gemäß § 333 Abs. 3 StGB ist die Vorteilsgewährung nicht strafbar, wenn die zuständige Behörde im Rahmen ihrer Befugnisse entweder die Annahme des Vorteils durch den Empfänger vorher genehmigt hat oder diese auf unverzügliche Anzeige des Empfängers genehmigt. Das Vorliegen einer wirksamen Genehmigung stellt strafrechtlich einen Rechtfertigungsgrund für eine etwaige Vorteilsgewährung dar.
- 57** Zu berücksichtigen ist allerdings auch hier, dass eine solche Genehmigung nur dann wirksam ist, wenn die vorgesetzte Stelle sie im Rahmen ihrer gesetzlichen Befugnisse erteilt hat, diese also auch materiell rechtmäßig ist. Es ist mithin darauf zu achten, dass nicht nur die tatsächlich zuständige Behörde⁸⁸ die Genehmigung erteilt, sondern auch dass diese sich im Rahmen der jeweiligen **Genehmigungsgrenzen** bewegt, die sich etwa aus den einschlägigen Beamtengesetzen sowie Verwaltungsvorschriften ergeben. Sehen die jeweiligen Vorschriften hier in einem geringeren Bereich von etwa bis zu 25,00 EUR eine stillschweigend erteilte Zustimmung vor, so sind Zuwendungen im höheren vierstelligen Bereich sicherlich nicht mehr genehmigungsfähig. Auch hier ist im Einzelfall sorgfältig nicht nur die Zuständigkeit, sondern auch die Grenze der Genehmigungsfähigkeit zu ermitteln, um zu verhindern, dass ein zu leichtfertiger Umgang mit einer vermeintlich wirksamen Genehmigung doch zu einer Strafbarkeit des Mitarbeiters führt.

b) Bestechung (§ 334 StGB)

- 58** Wegen Bestechung gemäß § 334 StGB macht sich strafbar, wer einem **Amtsträger**, einem Europäischen Amtsträger oder einem für den öffentlichen Dienst besonders Verpflichteten einen Vorteil für diesen oder einen Dritten als Gegenleistung dafür anbietet, verspricht oder gewährt, dass dieser eine Diensthandlung vorgenommen hat oder künftig vornimmt und dadurch seine Dienstpflicht ver-

⁸⁷ Abrufbar unter: <https://www.s20.de/schwerpunkte-2/> (zuletzt abgerufen am 16.7.2024).

⁸⁸ Die Zuständigkeit der Behörde erschließt sich hierbei prima facie aus den öffentlich-rechtlichen Regelungen des Beamtensrechts (vgl. § 71 Satz 2 BBG für Bundesbeamte). Weitere Zuständigkeitsregelungen finden sich in Verwaltungsvorschriften, Tarifverträgen oder gar Geschäftsverteilungsplänen. Die öffentlich-rechtlichen Vorschriften sind jedoch unvollständig und z. T. sogar widersprüchlich zu den strafrechtlichen Vorgaben.

letzt hat oder noch verletzen würde. Die Bestechung stellt damit einen Qualifikationstatbestand zu dem Grundtatbestand der Vorteilsgewährung dar. Über die bereits oben (→ Rn. 44 ff.) dargestellte Vorteilsgewährung muss der Vorteil hier als **Gegenleistung für eine bestimmte pflichtwidrige Diensthandlung** angeboten, versprochen oder gewährt worden sein, es muss also eine (Unrechts-) Vereinbarung zwischen dem Zuwendendem oder dem Amtsträger geschlossen worden sein, nach der der Amtsträger seine Dienstpflichten unter dem Einfluss der gewährten oder versprochenen Zuwendung verletzt. Als pflichtwidrige Diensthandlungen in Betracht kommen hier bspw. die rechtswidrige Erteilung einer Genehmigung (Baugenehmigung, Fahrerlaubnis pp.), die unrechtmäßige Bewilligung einer Leistung (Subventionen pp.) oder auch die fehlerhafte Einstellung eines Ermittlungsverfahrens gem. § 170 Abs. 2 StPO.⁸⁹

Hinsichtlich der (Grund-)Tatbestandsmerkmale der Amtsträgereigenschaft sowie des Vorteils kann auf die obigen Ausführungen unter → Rn. 44 ff. verwiesen werden. Auch im Hinblick auf die hier erforderliche konkrete Unrechtsvereinbarung ist die Rechtsprechung jedoch „großzügig“. An die Konkretisierung der künftigen pflichtwidrigen Diensthandlung innerhalb der **Unrechtsvereinbarung** sind „keine übertriebenen Anforderungen“ zu stellen,⁹⁰ die einvernehmlich ins Auge gefassten (pflichtwidrigen) Diensthandlungen brauchen ihrem sachlichen Gehalt nach nur in groben Umrissen erkennbar und festgelegt zu sein.⁹¹ Insofern ist es sogar unerheblich, ob die entsprechende pflichtwidrige Diensthandlung tatsächlich vorgenommen wird.⁹² Ebenso unerheblich ist es, dass sich der Täter insgeheim vorbehält, später sachgerecht zu verfahren. Entscheidend ist der von dem Amtsträger nach außen erweckte Eindruck.⁹³ Zeigt sich der Täter zunächst bereit, später seine Pflichten zu verletzen (ob er dies wirklich vor hat oder nicht), so liegt bereits Strafbarkeit vor.⁹⁴

Ein besonderes **Compliance-Risiko** besteht im Falle des Versuchs der Einflussnahme auf eine Ermessensentscheidung des Amtsträgers. Kommt diesem ein Ermessensspielraum zu, handelt er nämlich nach der Rechtsprechung bereits dann pflichtwidrig, wenn er sich nicht ausschließlich von sachlichen Gesichtspunkten leiten, sondern sich auch durch den Vorteil beeinflussen lässt, diesen also lediglich „mit in die Waagschale legt“⁹⁵ und zwar selbst dann, wenn die Entscheidung selbst letztlich sachlich gerechtfertigt ist. Eine solche Feststellung ist nachvollziehbarerweise schnell getroffen.

89 Eine nur schnellere oder sorgfältigere Bearbeitung eines Verfahrens kann pflichtwidrig sein, wenn dadurch die Bearbeitung anderer Sachen beeinträchtigt wird, insb. wenn gegen eine Pflicht zur Bearbeitung in einer bestimmten Reihenfolge verstoßen wird. BGH, 20.5.2008, 5 StR 57/08; BGHSt 15, 350; 16, 37; Fischer, StGB, § 332 Rn. 8.

90 BGHSt 48, 44 ff.; BGH, wistra 1999, 271.

91 BGHSt 48, 44 ff.

92 BGH, wistra 1999, 271.

93 BGHSt 48, 47.

94 Bei dem Amtsträger insoweit gem. § 332 Abs. 3 StGB.

95 BGHSt 15, 88, 92; 15, 239, 242, 247; 48, 44, 47.

- 61 Eine Strafbarkeit wegen (vollendeter) Bestechung liegt gem. § 334 Abs. 3 StGB auch bereits vor, wenn der Täter den Amtsträger zu bestimmen *versucht*, dass dieser als gebundener Beamter durch die Diensthandlung seine Pflichten verletzt (Nr. 1) oder sich als Ermessensbeamter bei der Ermessensausübung durch den Vorteil beeinflussen lässt. Es reicht aus, dass der Amtsträger dieses Angebot zur Kenntnis nimmt.
- 62 Bei der Bestechung sieht das Gesetz zudem eine Strafschärfung für **besonders schwere Fälle** vor. Gem. § 335 StGB ist der Strafraum hier auf Freiheitsstrafe von einem Jahr bis zu zehn Jahren erhöht. Ein besonders schwerer Fall der Bestechung wird von der Rechtsprechung bereits dann angenommen, wenn die Zuwendung ihrem Umfang nach deutlich aus dem Rahmen durchschnittlicher Fälle herausragt.⁹⁶ Die Literatur zieht die Grenze für einen besonders schweren Fall (großes Ausmaß) bei einem Schadensvolumen zwischen 10.000,00 und 25.000,00 EUR.⁹⁷ Ein besonders schwerer Fall liegt auch bei der gewerbs- und bandenmäßigen Begehung vor, die bereits bei deutlich kleineren Beträgen in Betracht kommt. Heikel ist insoweit, dass nach der Rechtsprechung eine Bande bereits beim Zusammenschluss von mehr als zwei Personen angenommen wird, hier also bereits bei einem bestechlichen Amtsträger und zwei Vorteilsgebern vorliegen kann,⁹⁸ was gerade im unternehmerischen Umfeld nicht die Ausnahme sein dürfte.

c) Bestechung von Mandatsträgern (§ 108e StGB)

- 63 Bis in das Jahr 2014 war der Tatbestand der Abgeordnetenbestechung gem. § 108e StGB a. F. ein „stumpfes Schwert“, das nur bestimmte ausgewählte Handlungen erfasste, deshalb so gut wie nicht zur Anwendung gelangte und daher kein großes Compliance-Risiko darstellte. Obwohl sich Deutschland durch die Unterzeichnung des Strafrechtsübereinkommens des Europarates über Korruption vom 27.1.1999⁹⁹ sowie etwa der UN-Konvention gegen Korruption vom 31.10.2003 (UNCAC)¹⁰⁰ bereits längst verpflichtet hatte, eine angemessene Strafdrohung auch für die Korruption von Mandatsträgern einzuführen, ist dies jedoch erst zum 1.9.2014¹⁰¹ erfolgt. Die aktuelle Regelung des § 108e StGB, nunmehr „Bestechlichkeit und Bestechung von Mandatsträgern“, erweitert die Strafbarkeit für die betroffenen Mandatsträger im Vergleich zur alten Regelung zwar erheblich, erfüllt allerdings lediglich die Minimalanforderungen der Kon-

96 BGH, wistra 1991, 106.

97 Fischer, StGB, § 335 Rn. 6 m. w. N.

98 BGH, Beschl. v. 13.12.2012 – 1 StR 522/12, hier: 3,50 EUR für das Einschmuggeln von Mobiltelefonen in die JVA.

99 Criminal Law Convention on Corruption, Council of Europe, European Treaty Series No. 173, <http://conventions.coe.int>; weitere Nachweise bei LK-StGB/Sowada, Vor § 331 Rn. 24.

100 United Nations Convention Against Corruption, A/RES/58/4; Unterzeichnung durch Deutschland am 9.12.2003.

101 48. Strafrechtsänderungsgesetz vom 23.4.2014.

vention, erforderlich für die Strafbarkeit ist der Nachweis einer konkreten Unrechtsvereinbarung, die schlichte Vorteilsannahme wird weiterhin nicht erfasst.

Die Neuregelung des § 108e StGB entspricht der Systematik des Tatbestands der Bestechlichkeit und Bestechung im geschäftlichen Verkehr gem. § 299 StGB. Die passive Bestechlichkeit von Mandatsträgern ist in § 108e Abs. 1 StGB geregelt, die aktive Bestechung von Mandatsträgern in § 108e Abs. 2 StGB. Nach der Neuregelung des § 108e Abs. 2 StGB macht sich wegen der Bestechung von Mandatsträgern strafbar, wer einem „Mitglied einer Volksvertretung des Bundes oder der Länder“ einen „ungerechtfertigten Vorteil“ für diesen oder einen Dritten „als Gegenleistung dafür anbietet, verspricht oder gewährt“, dass er „bei Wahrnehmung seines Mandats eine Handlung im Auftrag oder auf Weisung vornehme oder unterlasse“. Der Tatbestand definiert damit einen neuen, von dem der Amtsträgerkorruption abweichenden Vorteilsbegriff, von der Strafdrohung erfasst wird lediglich ein „ungerechtfertigter Vorteil“, der allerdings gerade *nicht* vorliegt, wenn etwa die Annahme des Vorteils „im Einklang mit den für die Rechtsstellung des Mitglieds maßgeblichen Vorschriften steht“.

Ein **Compliance-Risiko** stellt der Tatbestand aufgrund der **Weite des Empfängerbegriffs** dar. Mandatsträger i. S. d. § 108e Abs. 1 und Abs. 2 StGB ist zwar zunächst einmal nur das „**Mitglied einer Volksvertretung des Bundes oder der Länder**“, mithin des Bundestages, der Landtage, des Abgeordnetenhauses in Berlin sowie der Hamburgischen und Bremischen Bürgerschaft. Gem. § 108e Abs. 3 StGB stehen diesen jedoch die Mitglieder zahlreicher anderer Institutionen gleich. Dies sind Mitglieder einer Volksvertretung einer kommunalen Gebietskörperschaft (Nr. 1), Mitglieder eines in unmittelbarer und allgemeiner Wahl gewählten Gremiums einer für ein Teilgebiet eines Landes oder einer kommunalen Gebietskörperschaft gebildeten Verwaltungseinheit (Nr. 2), Mitglieder der Bundesversammlung (Nr. 3), **Mitglieder des Europäischen Parlaments** (Nr. 4), Mitglieder einer parlamentarischen Versammlung einer internationalen Organisation (Nr. 5) und Mitglieder eines Gesetzgebungsorgans eines ausländischen Staates (Nr. 6). Von besonderer Bedeutung in der Praxis ist die Nr. 1 „Mitglieder einer Volksvertretung der kommunalen Gebietskörperschaften“; dies sind insbesondere Mitglieder der **Stadt- und Gemeinderäte**, aber auch der **Bezirksvertretungen**. Bei diesen ist jeweils zu prüfen, ob sie als Mandatsträger gehandelt haben, (nur) dann kommt eine Strafbarkeit nach § 108e StGB in Betracht, oder ob die Handlung im Rahmen der Betrauung mit konkreten Verwaltungsaufgaben, die über ihre Mandatstätigkeit hinausgehen, erfolgt ist. In einem solchen Fall hätten sie als Amtsträger gehandelt mit der Folge, dass sich eine etwaige Strafbarkeit an den §§ 331 ff. StGB orientiert.¹⁰² Nr. 2 erfasst diejenigen Länder bzw. Stadtstaaten, in denen eine Aufgliederung in Bezirke erfolgt ist, die aber keine Gebietskörperschaften darstellen, wie etwa die Bezirksverordnetenversammlung in Berlin und die Bezirksversammlung in Hamburg.¹⁰³ Inso-

102 Vgl. BGH, NStZ 2006, 389.

103 Vgl. BT-Drs. 18/607, S. 8.

weit wird allerdings auch der **Kreistag** erfasst, der gem. Art. 28 Abs. 1 Satz 2 GG ebenfalls eine aus Wahlen hervorgegangene Volksvertretung ist.

- 66 Der Geber muss dem Mandatsträger oder einem Dritten den ungerechtfertigten Vorteil „als Gegenleistung“ dafür anbieten, versprechen oder gewähren, dass dieser bei Wahrnehmung seines Mandats eine Handlung im Auftrag oder auf Weisung vornehme oder unterlasse, es muss also gerade eine qualifizierte **Unrechtsvereinbarung** geschlossen werden. Der ungerechtfertigte Vorteil muss gerade deshalb zugewendet werden, damit das Mitglied sich in einer bestimmten Weise verhält, also „im Auftrag oder auf Weisung“ des Vorteilsgebers handelt. Der Mandatsträger soll gerade durch den ungerechtfertigten Vorteil dazu verleitet werden, im Auftrag oder nach Weisung des Auftraggebers zu handeln. Für die Strafbarkeit reicht es nicht aus, dass Vorteile nur allgemein für die Mandatsausübung zugewendet werden bzw. das Mitglied wegen der von ihm gemäß seiner inneren Überzeugung vertretenen Positionen einen Vorteil erhält. Die Grenze zur Strafbarkeit wird erst dann überschritten, wenn sich der Mandatsträger durch den Vorteil zu seiner Handlung bestimmen lässt und seine innere Überzeugung den Interessen des Vorteilsgebers unterordnet, er sich also „kaufen“ lässt.
- 67 Von erheblicher Compliance-Relevanz ist § 108e Abs. 4 StGB, der das Merkmal des **ungerechtfertigten Vorteils** mittels einer nicht abschließenden Negativdefinition konkretisiert. Ein ungerechtfertigter Vorteil liegt danach insbesondere **nicht** vor, wenn seine Annahme **im Einklang mit den für die Rechtsstellung des Mandatsträgers maßgeblichen Vorschriften** steht. Mit dem Verweis auf die für die Rechtsstellung maßgeblichen Vorschriften wird für Mitglieder des Deutschen Bundestages auf das Abgeordnetengesetz (AbgG), die Verhaltensregeln für Mitglieder des Deutschen Bundestages (Anlage 1 der Geschäftsordnung des Deutschen Bundestages) sowie die dazu von dem Präsidenten des Deutschen Bundestages erlassenen Ausführungsbestimmungen Bezug genommen. Auch die Landtage haben entsprechende Gesetze und darauf basierende Verhaltensregeln für ihre Mitglieder erlassen. Ebenfalls in den Gemeindeordnungen der Länder finden sich Vorschriften für Mitglieder von Volksvertretungen der Gemeinden und Gemeindeverbände, die ihrerseits innerhalb ihrer Autonomie und entsprechend den Gegebenheiten vor Ort weitere **Verhaltensregeln** festlegen können. Schlussendlich kann damit etwa der Gemeinderat durch die Ausgestaltung der Ehrenordnung oder eines Ehrenkodex,¹⁰⁴ die „für die Rechtsstellung des Mitglieds maßgeblichen Vorschriften“ erlassen und damit die Reichweite des Straftatbestands des § 108e StGB bestimmen. Ebenfalls kraft Gesetzes ausgenommen ist eine nach dem Parteiengesetz oder entsprechenden Gesetzen zulässige **Parteispende** an die Partei oder den Mandatsträger (§ 108e Abs. 4 Satz 2 Nr. 2 StGB).¹⁰⁵ Eine Spende, die allerdings „erkennbar in Erwartung oder als Ge-

104 Vgl. etwa § 43 Abs. 3 Satz 2 GO NRW.

105 Vgl. Nr. 44 des Erläuternden Berichts zu Art. 4 des Strafrechtsübereinkommens des Europarates über Korruption v. 27.1.1999 (Bestechung und Bestechlichkeit von Mitgliedern inländischer öffentlich-rechtlicher Vertretungskörperschaften).

genleistung eines bestimmten wirtschaftlichen oder politischen Vorteils gewährt“ wird, darf bereits nach § 25 Abs. 2 Nr. 7 PartG und § 4 Abs. 4 der Verhaltensregeln nicht angenommen werden und kann damit auch nicht mit den für die Rechtsstellung des Mitglieds maßgebenden Vorschriften in Einklang stehen. Mit dem Zusatz „oder entsprechender Gesetze“ wird ferner mit Blick auf ausländische Mandatsträger klargestellt, dass auch ausländische Gesetze, welche Regelungen über die Zulässigkeit von Parteispenden treffen, zum Ausschluss der Strafbarkeit führen können.

Aufgrund der Vielzahl der Möglichkeiten einer jeweils unterschiedlichen Gestaltung in Bund, Ländern und Kommunen entzieht sich der Tatbestand der Bestechung von Mandatsträgern damit quasi einer Positivliste, in welchen Fällen und in welchem Rahmen Zuwendungen ohne Compliance-Risiko möglich sind, wie sie häufig etwa in einer Antikorruptionsrichtlinie Niederschlag findet. **Best Practice** kann insoweit lediglich äußerste Zurückhaltung und eine dezidierte Prüfung des Bestehens eines Compliance-Risikos im Einzelfall sein. **68**

d) Bestechung im geschäftlichen Verkehr (§ 299 Abs. 2 StGB)

Nach § 299 Abs. 2 StGB ist auch die Bestechung von **Nicht-Amtsträgern**, also Privatpersonen, unter bestimmten Voraussetzungen mit Strafe bedroht. Die Strafbarkeit der Bestechung (und Bestechlichkeit) von Nicht-Amtsträgern ist strafrechtlich allerdings keine neue Entwicklung, sie hat allerdings fast einhundert Jahre lang im Gesetz gegen den unlauteren Wettbewerb (§ 12 UWG a.F.) ein Schattendasein gefristet. Wurde dem § 299 StGB von der Rechtsliteratur noch im Jahr 2008 attestiert, „keine nennenswerte Rolle“¹⁰⁶ zu spielen, so erfreut sich die Anwendung des § 299 StGB in der Rechtswirklichkeit bei den Strafverfolgungsbehörden und Gerichten zwischenzeitlich größter Beliebtheit, verwiesen sei hier nur auf die Urteile des LG Darmstadt¹⁰⁷ und des BGH¹⁰⁸ in dem Auslandsbestechungsverfahren „Siemens/ENEL“, das Verfahren um die „Allianz-Arena“,¹⁰⁹ das sog. ratiopharm-Verfahren sowie auf den Streit in der Rechtsprechung um die Anwendbarkeit des § 299 StGB auf niedergelassene Ärzte als „Beauftragte“ der Krankenkassen.¹¹⁰ **69**

§ 299 Abs. 2 StGB bedroht das Anbieten oder Gewähren von Vorteilen an **Angebotene oder Beauftragte eines Unternehmens** als Gegenleistung für die **unlaut-** **70**

106 Bernsmann/Gatzweiler, Verteidigung in Korruptionsfällen, Rn. 558.

107 LG Darmstadt, 14.5.2007 – 712 Js 5213/04 – 9 KLS – Ss 297/07.

108 BGHSt 52, 323 ff.

109 BGH, Urt. v. 9.8.2006 – 1 StR 50/06, NJW 2006, 3290.

110 Nachdem der Große Strafsenat des BGH mit Beschl. v. 29.3.2012 (BGHSt 57, 202 = NJW 2012, 2530) entschieden hatte, dass niedergelassene Vertragsärzte weder Amtsträger noch Beauftragte der gesetzlichen Krankenkassen i. S. v. § 299 StGB sind, sah sich der Gesetzgeber veranlasst, eine eigenständige Strafnorm zu verabschieden, die im April 2016 in Kraft getretene Vorschrift der Bestechlichkeit und Bestechung im Gesundheitswesen gem. §§ 299a, b StGB.

tere Bevorzugung beim Bezug von Waren oder gewerblichen Dienstleistungen im inländischen oder ausländischen Wettbewerb mit Strafe (das sog. „Wettbewerbsmodell“). Aufgrund einer am 26.11.2015 in Kraft getretenen Erweiterung des § 299 StGB durch das Gesetz zur Bekämpfung der Korruption macht sich nunmehr auch derjenige strafbar, der einem Angestellten oder Beauftragten eines Unternehmens einen Vorteil als Gegenleistung dafür anbietet, dass der Empfänger **seine Pflichten gegenüber dem Unternehmen verletzt** (das sog. „Geschäftsherrenmodell“).

- 71** Als Unternehmen im Sinne der Vorschrift werden nicht nur Handels- oder Gewerbebetriebe, sondern auch gemeinnützige, kulturelle oder soziale Einrichtungen sowie freiberufliche Tätigkeit (str.) erfasst, das Bestehen einer Gewinnerzielungsabsicht ist nicht erforderlich.
- 72** Entscheidend ist jedoch zunächst die Qualifikation des Empfängers als „Angestellter“ oder „Beauftragter“. **Angestellter** i. S. d. § 299 StGB ist, wer in einem mindestens faktischen Dienstverhältnis zum Geschäftsherrn steht und dessen Weisungen unterworfen ist. Eine dauerhafte oder entgeltliche Tätigkeit ist nicht erforderlich, es muss aber ein gewisser Einfluss auf die Geschäftstätigkeit genommen werden können.¹¹¹ Dies sind insbesondere die Mitglieder des Vorstands oder der Geschäftsführung einer Kapitalgesellschaft, Mitarbeiter mit einem bestimmten Handlungsspielraum, etwa im Vertrieb oder im Einkauf, aber auch der gebundene Handelsvertreter.¹¹² Eine rein untergeordnete Tätigkeit, etwa als Hilfskraft, reicht allerdings nicht aus.¹¹³ **Beauftragter** ist, wer, ohne Angestellter oder Inhaber eines Betriebs zu sein, befugtermaßen für einen Geschäftsbetrieb tätig wird und aufgrund seiner Stellung berechtigt (oder verpflichtet) ist, auf Entscheidungen, die den Waren- bzw. Leistungsaustausch des Betriebs betreffen, unmittelbar oder mittelbar Einfluss zu nehmen.¹¹⁴ Der Begriff des Beauftragten bestimmt sich nach den tatsächlichen Verhältnissen,¹¹⁵ ihm kommt daher in der Praxis eine gewisse Auffangfunktion zu. **Nicht** vom Tatbestand erfasst wird lediglich der **Geschäftsherr** bzw. der Betriebsinhaber selbst, da die Annahme eines Vorteils durch den selbstständigen Unternehmer insoweit keine Anreizwirkung für eine unsachliche Entscheidung auslöst.¹¹⁶ Wie beim Amtsträgerbegriff hat sich auch hier in der Rechtspraxis eine beachtliche Kasuistik herausgebildet, auf deren detaillierte Darstellung in der strafrechtlichen Kommentierung verwiesen wird.
- 73** Hinsichtlich des Begriffs des **Vorteils** kann auf die Ausführungen zu den §§ 331 ff. StGB verwiesen werden. Der Tatbestand der Bestechung im geschäft-

¹¹¹ *Fischer*, StGB, § 299 Rn. 14 m. w. N.

¹¹² BGHSt 2, 401.

¹¹³ BayObLG, wistra 1996, 28, 30.

¹¹⁴ BGHSt 57, 202; 2, 396, 402; BGH, GRUR 1968, 587; *Fischer*, StGB, § 299 Rn. 15 m. w. N.

¹¹⁵ NK-StGB/*Dannecker*, 3. Aufl. 2010, § 299 Rn. 22; *Fischer*, StGB, § 299 Rn. 15.

¹¹⁶ BGHSt 57, 202, Rn. 28; „Anteilseigner“ BGH, Beschl. v. 28.7.2021 – 1 StR 506/20, NStZ 2022, 413.

lichen Verkehr erfasst ausdrücklich und uneingeschränkt auch die Zuwendung von Vorteilen an Dritte, sog. **Dritt Vorteile**.¹¹⁷ Dritter kann insoweit auch eine juristische Person oder eine Personengesellschaft sowie eine sonstige Organisation, Behörde oder Partei sein. Erfasst werden daher auch finanzielle Unterstützungen für karitative, kulturelle oder sonst dem Gemeinwohl dienende Institutionen oder Veranstaltungen, medizinische oder wissenschaftliche Forschungsvorhaben sowie Parteispenden.

Der Vorteil muss hier allerdings als konkrete **Gegenleistung** für eine zukünftige **unlautere Bevorzugung im Wettbewerb** (Nr. 1) angeboten oder gewährt werden. Erforderlich ist hierbei die zumindest stillschweigende Übereinkunft, dass die Vorteilszuwendung aufgrund der angestrebten Bevorzugung erfolgt. Nicht ausreichend ist hier – anders als bei der Amtsträgerkorruption – eine Zuwendung zur Herbeiführung lediglich allgemeinen Wohlwollens ohne Bezug zu einer bestimmten Bevorzugung.¹¹⁸ Der Vorteil muss als Gegenleistung für eine **künftige unlautere Bevorzugung** angenommen werden.¹¹⁹ Bleibt zwischen den Beteiligten offen, ob die Zuwendung für eine künftige unlautere Bevorzugung erfolgt (strafbar) oder ob sie aus Dank für eine in der Vergangenheit liegende Bevorzugung erfolgt ist (nicht strafbar), etwa bei der kommentarlosen Zuwendung im Rahmen dauerhafter Geschäftsbeziehungen, so besteht das Risiko, dass Staatsanwaltschaft und Gericht darin allerdings den Abschluss einer erneuten Unrechtsvereinbarung (für die Zukunft) sehen können, wenn eine zukünftige Bevorzugung bereits hinreichend konkretisiert ist.

Die unlautere Bevorzugung muss **im Wettbewerb** erfolgen, also in einem bestehenden wirtschaftlichen Konkurrenzverhältnis. Als **Tathandlungen** kommen etwa in Betracht die Veranlassung einer überhöhten Bezahlung,¹²⁰ das Unterlassen gebotener Mängelbeanstandungen,¹²¹ die Bevorzugung bei der Auftragsvergabe,¹²² der Abschluss eines Alleinvertriebsvertrags,¹²³ das Aufrechterhalten bestehender Geschäftsverbindungen,¹²⁴ das Nichtkündigen einer Geschäftsbeziehung,¹²⁵ die Bekanntgabe Mitbewerber benachteiligender Indiskretionen¹²⁶ sowie sonstige Bevorzugungen bei der Annahme und Prüfung gelieferter Waren.

117 Zur Einschränkung des Dritt Vorteils auf die Fälle einer mittelbaren Besserstellung des Angestellten bzw. Beauftragten vgl. *Fischer*, StGB, § 299 Rn. 11 m. w. N.

118 *Fischer*, StGB, § 299 Rn. 22; *Heine/Eisele*, in: *Schönke/Schröder*, StGB, § 299 Rn. 16.

119 BGH, Beschl. v. 10.7.2013 – 1 StR 532/12, NJW 2013, 3590; BGH, Beschl. v. 14.7.2010 – 2 StR 200/10, wistra 2010, 447.

120 BGHSt 10, 269, 270.

121 *Krick*, in: *MünchKomm-StGB*, § 299 Rn. 25.

122 BGHSt 2, 396, 400 f.

123 BGH, NJW 1968, 1572, 1573.

124 RGSt 66, 16, 18; OLG Stuttgart, WRP 1974, 222, 225.

125 RGSt 68, 70, 76.

126 BGH, BB 1977, 264; BayObLG, NJW 1996, 268, 269.

- 76 Nach der Rechtsprechung genügt es allerdings, wenn die zum Zwecke des Wettbewerbs vorgenommenen Handlungen nach der Vorstellung des Täters **geeignet** sind, seine eigene Bevorzugung oder die eines Dritten im Wettbewerb zu veranlassen; die vereinbarte Bevorzugung muss also tatsächlich nicht einmal eingetreten sein.¹²⁷ § 299 StGB scheidet aber aus, wenn aus Sicht der Beteiligten eine Bevorzugung gar nicht zum Tragen kommen kann, so etwa wenn der Bezug von Waren oder Leistungen von einem Konkurrenzunternehmen nicht mehr möglich ist oder der in Aussicht gestellte Bezug von Waren oder Leistungen eine Privilegierung im Wettbewerb nicht bewirken kann, etwa aufseiten des zu Bevorzugenden ein Monopol besteht.¹²⁸
- 77 In der Alternative des sog. Geschäftsherrenmodells (Nr. 2) muss der Vorteil als Gegenleistung dafür angeboten oder gewährt werden, dass der Empfänger bei dem Bezug von Waren oder Dienstleistungen eine Handlung vornehme oder unterlasse und dadurch **seine Pflichten gegenüber dem Unternehmen verletze**. Ziel der Vorschrift ist hier der Schutz der Interessen des Geschäftsherrn an der loyalen und unbeeinflussten Erfüllung der Pflichten durch seine Angestellten und Beauftragten. Nicht ausreichend für eine solche Pflichtverletzung ist allerdings allein die Annahme des Vorteils oder das bloße Verschweigen der Zuwendung gegenüber dem Geschäftsherrn etwa unter Verstoß beispielsweise gegen interne Compliance-Vorschriften des Unternehmens.¹²⁹ Eine **Genehmigung** der Annahme des Vorteils durch den Geschäftsherrn ist zwar nicht ausdrücklich, wie in § 331 Abs. 3 StGB, geregelt; wenn der Geschäftsherr, der selbst nicht Adressat des § 299 StGB ist, eine Bevorzugung durch einen Angestellten oder Beauftragten jedoch genehmigt, hat dies die gleichen wirtschaftlichen Konsequenzen, lässt die Unlauterkeit entfallen und kann daher nicht anders zu bewerten sein, als wenn der Geschäftsherr selbst unmittelbar handelt. Die Zustimmung bzw. Genehmigung des Geschäftsherrn hat damit tatbestandsausschließende Wirkung.¹³⁰
- 78 In der Praxis sind nicht selten Fallkonstellationen zu beobachten, in der der Zuwendende sich quasi genötigt fühlt, Vorteile zu gewähren, etwa wenn sich ein Unternehmen im Existenzkampf in einer Wettbewerbssituation befindet, in der die Mitbewerber Vorteile gewähren, um Aufträge zu erhalten und ohne Anpassung an eine solche Praxis eine Auftragserteilung gar nicht erst möglich erscheint. Insbesondere ist dieser Aspekt zu berücksichtigen, wenn der über die Vergabe entscheidende Angestellte die Vorteilsgewährung an ihn zur Vorbedingung für die Auftragserteilung macht. Im Einzelfall erscheint es da nicht fernliegend, auch über die Möglichkeit einer Rechtfertigung der Tathandlung, etwa

127 BGH, NJW 2006, 3290 ff. (Allianz-Arena); vgl. auch BGHSt 49, 214, 228; BGH, NJW 2003, 2996, 2997.

128 Weitere Nachweise hierzu bei Fischer, StGB, § 299 Rn. 23 ff.

129 So ausdrücklich die Gesetzesbegründung, BR-Drs. 25/15, S. 21.

130 BGH, Beschl. v. 28.7.2021 – 1 StR 506/20, NSTz 2022, 413; a. A. Fischer, StGB, § 299 Rn. 42; LK-StGB/Tiedemann, § 299 Rn. 55.

über das Vorliegen eines **Nötigungsnotstands** nachzudenken.¹³¹ In der Praxis finden solche Konstellationen jedoch regelmäßig nur im Rahmen der Strafzumessung Berücksichtigung.

Obleich die einfache „Klimapflege“ bei der Bestechung im geschäftlichen Verkehr noch nicht strafbar ist und der Nachweis einer konkret vereinbarten unlauteren Bevorzugung als Gegenleistung schwerfällt, bietet die Bestechung im geschäftlichen Verkehr dennoch erhebliche **Compliance-Risiken**. Gerade im Bereich der wirtschaftlichen Kooperation „privater“ Unternehmen bietet eine solche inkriminierte Einflussnahme auf Entscheidungsträger anderer Unternehmen einen starken „Hebel“, um sich Vorteile im Wettbewerb zu verschaffen. Dazu kommt, dass viele Akteure zwar um die Kartellrechtswidrigkeit etwaiger Absprachen unter Wettbewerbern wissen, die Strafbarkeit der Einflussnahme auf die Vergabeentscheidung außerhalb des öffentlichen Bereichs jedoch häufig nicht bekannt ist und die Unternehmen eine dahingehende Vorsorge durch Compliance-Richtlinien oder Schulungen vernachlässigen. Werden derartige Handlungen dann jedoch aufgedeckt, häufig wiederum durch die steuerliche Betriebsprüfung, stehen die Folgen für das Unternehmen (Einzahlung und Unternehmensgeldbuße) denen für die (harte) Amtsträgerbestechung nur geringfügig nach. Auch die Nichterfassung der schlichten Klimapflege bietet hier nur einen scheinbaren Schutz, da die Staatsanwaltschaften im Falle der Kenntnisnahme von Zuwendungen ab einer gewissen Größenordnung, regelmäßig bereits ab **200,00 EUR**, generell erst einmal einen Anfangsverdacht für das Vorliegen einer Bestechung im geschäftlichen Verkehr sehen und die „Unrechtsvereinbarung“ dann erst im weiteren Verfahren aufklären (wollen). Selbst wenn der Nachweis der unlauteren Bevorzugung dann im Weiteren nicht gelingt, war das Unternehmen dennoch u. U. längere Zeit erst einmal Gegenstand eines Ermittlungsverfahrens mit allen damit verbundenen negativen Konsequenzen.

e) Bestechlichkeit im geschäftlichen Verkehr (§ 299 Abs. 1 StGB)

§ 299 Abs. 1 StGB bedroht die Bestechlichkeit eines Angestellten oder Beauftragten im geschäftlichen Verkehr mit Strafe und erfasst damit spiegelbildlich das entsprechende Fordern, Sich-versprechen-lassen oder Annehmen eines Vorteils als Angestellter oder Beauftragter eines Unternehmens. Im Hinblick auf die Tatbestandsmerkmale kann insoweit auf die Ausführungen zur (aktiven) Bestechung im geschäftlichen Verkehr verwiesen werden, allerdings ist § 299 Abs. 1 StGB ein sog. Sonderdelikt, das nur von einem Angestellten oder Beauftragten eines Unternehmens verwirklicht werden kann. Da eine solche Tat eines Angestellten oder Beauftragten mangels Betriebsnützigkeit oder (beabsichtigter) Bereicherung des eigenen Unternehmens nicht mit dem Risiko der Einziehung oder der Verhängung einer Unternehmensgeldbuße behaftet ist, stellt die (passive) Bestechlichkeit eines Angestellten oder Beauftragten für das betroffene Unternehmen kein Compliance-Risiko im engeren Sinne dar. Dennoch besitzt auch

131 Vgl. *Bernsmann/Gatzweiler*, Verteidigung bei Korruptionsfällen, Rn. 635.

eine solche Strafbarkeit natürlich Compliance-Relevanz, da gerade im Falle der Bestechlichkeit von Angestellten oder Beauftragten, die das Vertrauen der Unternehmensleitung (oder des Gesellschafters) genießen und auf deren Loyalität das Unternehmen angewiesen ist, erhebliche Schäden herbeigeführt werden können. Die Verhinderung und, soweit dies nicht gelingt, Aufdeckung solchermaßen unternehmensschädlicher Straftaten ist damit regelmäßig Ziel und Bestandteil interner Compliance-Management-Systeme.

f) Bestechung im Gesundheitswesen (§ 299b StGB)

- 81** Eine weitere Spezialvorschrift im Bereich der Korruption hat der Gesetzgeber unlängst für die Akteure im als besonders korruptionsanfällig erkannten Gesundheitswesen durch das umstrittene Gesetz zur Bekämpfung von Korruption im Gesundheitswesen vom 14.4.2016¹³² erlassen. Erforderlich geworden war die Spezialvorschrift, nachdem der Bundesgerichtshof in einer Entscheidung aus dem Jahre 2012¹³³ niedergelassene, für die vertragsärztliche Versorgung zugelassene Ärzte bei Wahrnehmung der ihnen in diesem Rahmen übertragenen Aufgaben weder als Amtsträger (§§ 331 ff. StGB) noch als Beauftragte der gesetzlichen Krankenkassen (§ 299 StGB) angesehen hat, mit der Folge dass die Korruptionstatbestände des Strafgesetzbuchs für niedergelassene Vertragsärzte grundsätzlich nicht zur Anwendung kommen konnten. Insofern konnte etwa die Zahlung einer Prämie von einem Pharmaunternehmen an einen Arzt, um damit dessen Verschreibungsverhalten zugunsten eines bestimmten Präparats zu beeinflussen, nicht strafrechtlich geahndet werden. Die insoweit identifizierte Lücke bei der strafrechtlichen Bekämpfung von Korruption im Gesundheitswesen soll durch die Neuregelung der §§ 299a und b StGB geschlossen werden.
- 82** Die relativ neue Korruptionsvorschrift bezieht grundsätzlich alle Heilberufe ein, die für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordern, und gilt für Sachverhalte sowohl innerhalb als auch außerhalb des Bereichs der gesetzlichen Krankenversicherung. Die neuen Straftatbestände § 299a StGB (Bestechlichkeit im Gesundheitswesen) und § 299b StGB (Bestechung im Gesundheitswesen) sind der Struktur des § 299 StGB (Bestechlichkeit und Bestechung im geschäftlichen Verkehr) nachgebildet.
- 83** Nach § 299b StGB wird wegen Bestechung im Gesundheitswesen mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wer einem Angehörigen eines Heilberufs im Sinne des § 299a im Zusammenhang mit dessen Berufsausübung einen Vorteil für diesen oder einen Dritten als Gegenleistung dafür anbietet, verspricht oder gewährt, dass er (1.) bei der Verordnung von Arznei-, Heil- oder Hilfsmitteln oder von Medizinprodukten, (2.) bei dem Bezug von Arznei- oder Hilfsmitteln oder von Medizinprodukten, die jeweils zur unmittelbaren An-

132 BGBl. I 2016, S. 1254; in Kraft seit dem 4.6.2016; vgl. BT-Drs. 18/6446; BR-Drs. 181/16.

133 BGH, Beschl. v. 29.3.2012 – GSSt 2/11; BGHSt 57, 202.

wendung durch den Heilberufangehörigen oder einen seiner Berufshelfer bestimmt sind, oder (3.) bei der Zuführung von Patienten oder Untersuchungsmaterial ihn oder einen anderen im inländischen oder ausländischen Wettbewerb in unlauterer Weise bevorzugen. Geeignete Vorteilsempfänger im Sinne des § 299a StGB sind alle Angehörigen eines Heilberufes, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert.

Die zunächst vorgesehene patientenschutzbezogene Handlungsmodalität eines „Verstoßes gegen berufsrechtliche Pflichten“ ist im Laufe des Gesetzgebungsverfahrens wieder weggefallen mit der Folge, dass der neue § 299b StGB – anders als § 299 Abs. 2 StGB – nur noch wettbewerbsbezogene Handlungen erfasst. Darüber hinaus ist ebenfalls die zunächst vorgesehene Tathandlung der „Abgabe“ von Arzneimitteln oder von Medizinprodukten nicht (mehr) vom Tatbestand erfasst mit der Folge, dass die Berufsgruppe der Apotheker aus dem Anwendungsbereich des Gesetzes herausgefallen ist. **Normadressat** sind damit sowohl die **akademischen Heilberufe**, deren Ausübung eine durch Gesetz und Approbationsordnung geregelte Ausbildung voraussetzt (Ärzte, Zahnärzte, Tierärzte, Psychologische Psychotherapeuten, Kinder- und Jugendpsychotherapeuten), als auch die sogenannten **Gesundheitsfachberufe** wie z.B. Gesundheits- und Krankenpfleger, Ergotherapeuten, Logopäden und Physiotherapeuten, deren Ausbildung ebenfalls gesetzlich geregelt ist.

Vorteile im Sinne der Vorschrift können neben schlichten Zahlungen etwa auch Einladungen zu Kongressen, die Übernahme der Kosten von Fortbildungsveranstaltungen¹³⁴ oder die Einräumung von Vermögens- oder Gewinnbeteiligungen sein. Ein Vorteil kann zudem grundsätzlich auch im Abschluss eines Vertrages liegen, der Leistungen an den Täter zur Folge hat, und zwar selbst dann, wenn diese nur das angemessene Entgelt für die von ihm selbst aufgrund des Vertrags geschuldeten Leistungen sind.¹³⁵ Demnach kann auch in der Verschaffung von Verdienstmöglichkeiten, die beispielsweise in der Teilnahme an einer unangemessen vergüteten Anwendungsbeobachtung (einer sog. Marketingstudie)¹³⁶ und im Abschluss eines Behandlungsvertrages zu sehen sind, ein Vorteil liegen.

Das bloße Anbieten (Versprechen oder Gewähren) ist für die Strafbarkeit allerdings nicht ausreichend, der Täter muss den Vorteil vielmehr als Gegenleistung für eine zumindest intendierte unlautere Bevorzugung im Wettbewerb anbieten, versprechen oder gewähren, erforderlich ist damit eine konkrete **Unrechtsvereinbarung** wie bei der Bestechlichkeit und Bestechung im geschäftlichen Verkehr gem. § 299 StGB. Da im Hinblick auf die neue Vorschrift der Bestechung im Gesundheitswesen gem. § 299b StGB einerseits erhebliche Unsicherheit und damit ein relevantes **Compliance-Risiko** besteht, andererseits der Anwendungs-

134 Vgl. BGH, Urt. v. 23.10.2002 – 1 StR 541/01.

135 Vgl. BGH, Urt. v. 10.3.1983 – 4 StR 375/82.

136 Vgl. hierzu BT-Drs. 360/15, S. 16 m. w. N.

bereich auf die im Gesundheitswesen tätigen Unternehmen beschränkt ist, muss im Hinblick auf die Details auf vertiefende Literatur verwiesen werden.

g) Auslandskorruption

- 87** Wie bereits in der Einführung aufgezeigt, hat die **Internationalisierung der Korruptionsbekämpfung** das nationale Strafrecht erheblich beeinflusst. Der sich aus der offiziellen Strafverfolgungsstatistik¹³⁷ ergebende Eindruck einer nur geringen praktischen Relevanz täuscht. Nicht nur nimmt die Zahl der eingeleiteten Ermittlungsverfahren stetig zu, insbesondere der Umfang der einzelnen Verfahren sowie die Konsequenzen sind erheblich. Ebenso spürbar wächst die Nachfrage im Bereich der **Präventivberatung**, bspw. nach der rechtlichen Bewertung von Korruptionsrisiken beim Abschluss von Agentur- oder Beraterverträgen im Auslandsgeschäft. Dies betrifft keineswegs nur börsennotierte Unternehmen, die gem. § 91 Abs. 2 AktG ohnehin verpflichtet sind, ein entsprechendes Risikomanagement zu betreiben, sondern insbesondere exportorientierte kleine und mittelständische Unternehmen.¹³⁸ Seit einigen Jahren beherrschen allerdings in erster Linie die deutschen Konzerne die Schlagzeilen, die über eine US-amerikanische Börsenzulassung verfügen und insoweit aufgrund internationaler Korruptionspraktiken in das Visier der amerikanischen Behörden geraten sind. Im Bereich der internationalen Korruptionsbekämpfung bekleiden die USA bereits seit Jahren eine Vorreiterrolle, die sie nicht nur über ihre Gesetzgebung und den Einfluss auf die OECD, sondern auch und insbesondere mittels der Durchführung von Korruptionsverfahren gegen internationale Konzerne durchsetzen. Bereits im Jahr 1977 wurde mit dem **Foreign Corrupt Practices Act (FCPA)**¹³⁹ ein Bundesgesetz geschaffen, das es natürlichen Personen wie auch amerikanischen Unternehmen verbietet, geldwerte Vorteile an ausländische staatliche Amtsträger zu erbringen, die den Zweck haben, den Zuschlag für ein Geschäft zu bekommen oder eine Geschäftsbeziehung aufrechtzuerhalten. Darüber hinaus verpflichtet das Gesetz alle in den USA börsennotierten Unternehmen zu einer **den Antikorruptionsregeln des FCPA entsprechenden Buchführung**. Die Antikorruptionsverfahren des Justizministeriums (DOJ) und der Börsenaufsicht (SEC),¹⁴⁰ die bis zum Entzug der Börsenzulassung führen können, werden regelmäßig mit äußerst schmerzhaften **Unternehmensgeldbußen** (sowie der Verpflichtung zur Verbesserung der Compliance) abgeschlossen. Das sog. **Forum Shopping** der USA gerade in Korruptionsverfahren führt mitunter

137 Einen Überblick über die Zahl der Ermittlungsverfahren im Ländervergleich und die bislang geringen Verurteilungszahlen geben die Antwort der Bundesregierung in BT-Drs. 16/8463 sowie etwa der TI-Progress Report 2013 „Assessing Enforcement of the OECD Convention on Combating Foreign Bribery“, www.transparency.org.

138 KfW-Wirtschaftsobserver, Ausgabe 34/2008, Wie international ist der deutsche Mittelstand?, www.kfw.de.

139 Title 15 U.S.C. §§ 78dd-1 ff., www.justice.gov/criminal/fraud/fcpa (zuletzt abgerufen am 25.6.2024).

140 US Securities and Exchange Commission, US-Börsenaufsicht.

dazu, dass ausländische Unternehmen bereits dann der amerikanischen Strafjustiz unterliegen, wenn sie in den USA börsennotiert sind, selbst wenn sämtliche Korruptionshandlungen außerhalb der USA erfolgt sind. Etwa im Fall Daimler hat dies den USA – im Wege eines Vergleichs mit Justizministerium und SEC – Unternehmensgeldbußen i. H. v. 185 Mio. USD in die Kassen gespült. Im Fall Siemens¹⁴¹ hat ein US-Bundesgericht den börsennotierten Konzern im Jahr 2008 zu einer Unternehmensgeldbuße von 450 Mio. USD an das US-Justizministerium und einer Gewinnabschöpfung von 350 Mio. USD an die SEC, mithin einer Gesamtsumme von 800 Mio. USD, verurteilt.¹⁴² In Deutschland hat Siemens wegen seiner (Auslands-)Korruptionspraktiken eine Unternehmensgeldbuße wegen Verletzung der Aufsichtspflicht durch den früheren Gesamtvorstand¹⁴³ von weiteren 395 Mio. EUR akzeptiert, nachdem bereits im Jahr 2007 eine Geldbuße i. H. v. 201 Mio. EUR wegen Verstößen im Geschäftsbereich Communications verhängt worden war. Die zunehmenden Aktivitäten der US-amerikanischen Behörden als „Weltpolizist“ (auch) im Bereich der Korruptionsbekämpfung treffen jedoch zunehmend auf Vorbehalte,¹⁴⁴ wenngleich mittelfristig eine „Amerikanisierung der Korruptionsbekämpfung“ nicht zuletzt aufgrund der profiskalischen Effekte wohl auch in Deutschland zu erwarten ist. Ähnliches gilt auch für das Vereinigte Königreich. Der **UK Bribery Act 2010** weist insoweit nicht nur eine Strafvorschrift für Unternehmen für die unterlassene Verhinderung von Bestechung auf (§ 7), er erklärt eine solche Norm auch auf ausländische, mithin auch deutsche Unternehmen für anwendbar, wenn bei einer Tathandlung auch nur ein allgemeiner Bezug zu Großbritannien besteht, etwa ein Bevollmächtigter dort gehandelt hat (§ 12 Abs. 5).¹⁴⁵

Der deutsche Gesetzgeber hat die internationalen Vorgaben¹⁴⁶ zur Erweiterung der Anwendbarkeit der Korruptionsvorschriften auf den internationalen Bereich umgesetzt mit der Folge, dass die Auslandsbestechung nach deutschem Recht strafbar ist und in Deutschland strafrechtlich verfolgt werden kann und in der Praxis auch wird. Bis in das Jahr 2015 geschah dies durch eine komplizierte Erweiterung des Anwendungsbereiches der Korruptionsvorschriften des StGB durch zwei eigenständige Gesetze, das Gesetz zur Bekämpfung internationaler

88

141 Vgl. Presseerklärung der Siemens AG Corporate Communications/Compliance Communications vom 27.1.2009.

142 Gleichwohl erfolgte die Verurteilung lediglich wegen Rechnungslegungsverstößen und nicht wegen Korruption, um Siemens so die Möglichkeit zu erhalten, öffentliche Aufträge in den USA zu bekommen.

143 §§ 30, 130 OWiG.

144 „SEC-Ermittler als Weltpolizisten gegen Korruption“, Spiegel-Online vom 6.4.2010 m. w. N.; mehrere deutsche Konzerne, etwa E.ON, Infineon sowie Allianz haben zwischenzeitlich wieder auf ihre US-Börsenzulassung verzichtet.

145 UK Bribery Act of 8th April 2010; vgl. <http://www.legislation.gov.uk/ukpga/2010/23/contents> (zuletzt abgerufen am 25.6.2024).

146 So insbes. das OECD-Übereinkommen über die Bekämpfung der Bestechung ausländischer Amtsträger im internationalen Geschäftsbereich vom 17.12.1997.

Bestechung (**IntBestG**)¹⁴⁷ sowie das EU-Bestechungsgesetz (**EuBestG**).¹⁴⁸ Diese Gesetze haben die Anwendbarkeit des Amtsträgerbegriffes auch auf internationale Amtsträger, die Amtsträger von EU-Mitgliedstaaten sowie auf bestimmte Gemeinschaftsbeamte, Mitglieder der Kommission und des Rechnungshofes der europäischen Gemeinschaften ausgeweitet. Des Verweises auf die Vorschriften des IntBestG sowie des EuBestG bedarf es seit November 2015 nicht mehr, da der Gesetzgeber durch das Gesetz zur Bekämpfung der Korruption die Erweiterungen des Amtsträgerbegriffes zwischenzeitlich – jedenfalls zum größten Teil – in das StGB (§§ 11 Abs. 1 Nr. 2 lit. a, 331 ff., 335a StGB) übernommen hat.¹⁴⁹ Gegenstand der Bestechung und auch der Vorteilsgewährung können nunmehr ausweislich des Wortlautes der §§ 331 ff. StGB auch sog. „**Europäische Amtsträger**“ sein. Europäische Amtsträger sind ausweislich der neuen Legaldefinition des § 11 Abs. 1 Nr. 2 lit. a StGB Beamte oder sonstige Bedienstete der Europäischen Union sowie die Mitglieder der Europäischen Kommission, der Europäischen Zentralbank, des Rechnungshofs oder eines Gerichts der Europäischen Union.¹⁵⁰

89 Für die Anwendung der Strafvorschriften über die **Bestechung** (und Bestechlichkeit) – nicht jedoch der schlichten Vorteilsgewährung (s. o.) – stellt **§ 335a Abs. 1 StGB** (n. F.) darüber hinaus nunmehr generell bestimmte „**ausländische und internationale Bedienstete**“ den inländischen Amtsträgern gleich. Ausweislich § 335a Abs. 1 Satz 2 StGB erstreckt sich die Gleichstellung mit einem (deutschen) Amtsträger auf

- a) Bedienstete eines ausländischen Staates (sowie Personen, die beauftragt sind, öffentliche Aufgaben für einen ausländischen Staat wahrzunehmen),
- b) Bedienstete einer internationalen Organisation (sowie Personen, die beauftragt sind, Aufgaben einer internationalen Organisation wahrzunehmen) sowie
- c) Soldaten eines ausländischen Staates und Soldaten, die beauftragt sind, Aufgaben einer internationalen Organisation wahrzunehmen. Für die Beamten und sonstigen Bediensteten ausländischer und internationaler Behörden wird, anders als bisher, nicht mehr der Begriff „Amtsträger“, sondern nur noch der einheitliche Begriff „**Bedienstete**“ verwendet. Ausländische und internationale Beamte sind von dem Begriff „Bedienstete“ allerdings miterfasst.¹⁵¹

147 Gesetz zur Bekämpfung internationaler Bestechung, BGBl. II, S. 2327; III, 450-28.

148 Gesetz zu dem Protokoll vom 27.9.1996 zum Übereinkommen über den Schutz der finanziellen Interessen der europäischen Gemeinschaften (EuBestG), BGBl. II 1998, S. 2340, in Kraft getreten am 22.9.1998.

149 Gesetz zur Bekämpfung der Korruption v. 20.11.2015, BGBl. I 2015, S. 2025.

150 Sowie Beamte oder sonstige Bedienstete einer auf der Grundlage des Rechts der Europäischen Union geschaffenen Einrichtung oder mit der Wahrnehmung von Aufgaben der Europäischen Union oder von Aufgaben einer auf der Grundlage des Rechts der Europäischen Union geschaffenen Einrichtung beauftragte Personen.

151 BT-Drs. 18/4350, S. 24.

Da § 335a Abs. 1 StGB nur die Anwendbarkeit der §§ 332 und 334 StGB (also die Bestechlichkeit und Bestechung) auf Bedienstete ausländischer und internationaler Behörden erstreckt, ist insoweit das Vorliegen einer sog. Unrechtsvereinbarung erforderlich, das Verhalten muss sich also auf eine pflichtwidrige Diensthandlung als Gegenleistung für den gewährten Vorteil beziehen. Gegenüber Bediensteten ausländischer und internationaler Behörden ist damit weiterhin nur die Bestechung i. S. v. § 334 StGB und nicht bereits die einfache Vorteils-gewährung strafbar. Ein neues, nicht zu unterschätzendes **Compliance-Risiko** ergibt sich jedoch daraus, dass die (schlichte) Vorteils-gewährung i. S. v. § 333 StGB, also auch Maßnahmen der sog. Klimapflege, nunmehr auch gegenüber Europäischen Amtsträgern (§ 333 Abs. 1 i. V. m. § 11 Abs. 1 Nr. 2 lit. a StGB)¹⁵² straffbewehrt ist.

Für solche im Ausland begangenen Korruptionsstraftaten gilt das deutsche Strafrecht unabhängig vom Recht des Tatorts, wenn ein besonderer Inlandsbezug besteht. Ein solcher Inlandsbezug besteht gem. § 5 Nr. 15 StGB, wenn der Täter zur Zeit der Tat Deutscher ist, er Europäischer Amtsträger ist und seine Dienststelle ihren Sitz in Deutschland hat oder die Tat gegenüber einem (deutschen) Amtsträger oder einem Europäischen Amtsträger oder einer nach § 335a StGB gleichgestellten Person begangen wird, die zur Zeit der Tat Deutsche ist.

Auch die Anwendbarkeit der Bestechung im geschäftlichen Verkehr gem. § 299 StGB ist auf Auslandssachverhalte erstreckt worden. Bis November 2015 war dies ausdrücklich in **§ 299 Abs. 3 StGB** (Erfassung von Auslandssachverhalten) geregelt, mit Wirkung ab dem 26.11.2015 sieht der (neue) Tatbestand des § 299 StGB als Tathandlung die unlautere Bevorzugung eines anderen „im inländischen oder ausländischen Wettbewerb“ vor. Da der Tatbestand keine Beschränkung auf deutsche Angestellte und Beauftragte sowie auf deutsche Unternehmen enthält, findet er auch bei Taten von ausländischen Angestellten und Beauftragten ausländischer Unternehmen Anwendung. Trotz der Erweiterung des Schutzbereichs des § 299 StGB auf den ausländischen Wettbewerb bleibt die Frage der Anwendbarkeit der Auslandsbestechung im privaten Sektor jedenfalls im Falle von im Ausland begangenen Handlungen im Einzelfall problematisch, eine Anwendungsvorschrift, wie in § 5 Nr. 15 StGB für die §§ 331 ff. StGB vorgesehen, besteht für § 299 StGB nicht. Die allgemeinen Grundsätze der §§ 3 ff. StGB, das sog. **innerstaatliche Strafanwendungsrecht**, bleiben damit im Einzelfall zu berücksichtigen.¹⁵³ Für die Frage der Anwendbarkeit deutschen Rechts ist bei Aus-landstaten gem. § 7 Abs. 1 und 2 StGB daher weiterhin die **jeweilige lokale Rechtslage** zur Strafbarkeit der Korruption im privaten Sektor von Bedeutung.

Compliance-Risiken ergeben sich bei der Auslands-korruption damit nicht nur im Falle der konkreten (Auslands-)Bestechung, für die unzweifelhaft ein Gerichtsstand in Deutschland vorliegt, sondern neuerdings auch aus ehemals – je-

152 Sowie gem. § 335a Abs. 3 StGB gegenüber Soldaten und Bediensteten der in der Bundesrepublik Deutschland stationierten NATO-Truppen.

153 So bereits zur Vorschrift des § 299 Abs. 3 StGB: *Fischer*, StGB, § 299 Rn. 3 m. w. N.

denfalls nach deutschem Recht – im Ausland nicht strafbaren Handlungen, nämlich der Vorteilsgewährung, die mit Wirkung ab dem 26.11.2015 gegenüber einem Europäischen Amtsträger ebenfalls strafbar ist.

- 94 Regelmäßig unter den Tatbestand der (Auslands-)Bestechung subsumiert werden können die im internationalen Geschäft nicht unüblichen sog. **Facilitation Payments** bzw. **Expediting Payments** (Erleichterungs- und Beschleunigungszahlungen), da hier nicht nur Klimapflege betrieben wird, sondern relativ konkret eine pflichtwidrige Gegenleistung, nämlich die bevorzugte Behandlung oder Abfertigung, vereinbart wird. Natürlich gibt es auch Fälle, in denen der (deutsche) Unternehmer Opfer eines Machtmissbrauchs des ausländischen Amtsträgers wird und dieser ihm die Zahlung quasi abpresst. In einem solchen Fall handelt der Zahlende weniger, um sich einen unbilligen Vorteil im internationalen geschäftlichen Verkehr zu verschaffen, sondern um Schaden von seinem Unternehmen abzuwenden, er befindet sich in einer Art Nötigungsnotstand. Zahlt der Vorteilsgeber etwa nicht für die Vornahme einer Diensthandlung, sondern für die Unterlassung einer rechtswidrigen (gar willkürlichen) Diensthandlung, nämlich der verzögerten Abfertigung mangels Zahlung, fehlt es u. U. sogar an einer Unrechtsvereinbarung. Die von § 334 StGB geforderte Pflichtwidrigkeit der (gekauften) Diensthandlung läge hier gerade nicht vor, wenn der ausländische Amtsträger aufgrund der Zahlung eine rechtswidrige Diensthandlung unterlässt, sich also rechtmäßig verhält. Die Vorteilshingabe für eine rechtmäßige Diensthandlung hingegen stellt aber lediglich eine Vorteilsgewährung i. S. v. § 333 StGB dar, die wiederum nur gegenüber europäischen Amtsträgern strafbewehrt ist. Dennoch liegt auf der Hand, dass auch solche Zahlungen ein immenses Compliance-Risiko beinhalten, da das Finanzamt eine solche Zahlung natürlich in Frage stellen würde und eine Staatsanwaltschaft in einem solchen Fall natürlich ermitteln und hier quasi eine Art Beweislastumkehr entstehen würde.

h) Korruptionsdelikte im weiteren Sinne

- 95 Das **Gewähren oder Versprechen von Vorteilen im Zusammenhang mit einer Betriebsratswahl** gem. § 119 Abs. 1 BetrVG kann durchaus als Korruptionsdelikt im weiteren Sinne verstanden werden. Gemäß § 119 Abs. 1 BetrVG¹⁵⁴ wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer eine Wahl des Betriebsrats (sowie weiterer im Gesetz genannter Einrichtungen) behindert oder durch Zufügung oder Androhung von Nachteilen oder durch Gewährung oder Versprechen von Vorteilen beeinflusst (Nr. 1) oder ein Mitglied oder ein Ersatzmitglied des Betriebsrats, des Gesamtbetriebsrats, des Konzernbetriebsrats (und anderer im Gesetz genannter Einrichtungen) um seiner Tätig-

¹⁵⁴ Betriebsverfassungsgesetz i. d. F. d. Bek. vom 25.9.2001, BGBl. I, S. 2518, zuletzt geändert durch Art. 3 Abs. 4 des Gesetzes vom 20.4.2013 (BGBl. I, S. 868); vgl. auch § 44 Abs. 1 Nr. 2 EBRG – Begünstigung eines Mitglieds eines europäischen Betriebsrats.

keit willen benachteiligt oder begünstigt (Nr. 3).¹⁵⁵ § 119 Abs. 1 BetrVG bedroht die Verhaltensweisen mit Strafe, die gem. § 20 Abs. 1 und 2 BetrVG verboten sind. Das Wahlbeeinflussungsverbot des § 20 Abs. 2 BetrVG, das auch den eigentlichen Abstimmungsvorgang vorbereitende Maßnahmen umfasst, bezieht sich auf die Freiheit der inneren Willensbildung der Arbeitnehmer bei der Ausübung ihres Wahlrechts. Insoweit besteht eine „strikte Neutralitätspflicht“ des Arbeitgebers.

Aufmerksamkeit erfuhr die Strafnorm des § 119 Abs. 1 BetrVG nicht zuletzt in dem sog. **„VW-Verfahren“**, in welchem der Konzernbetriebsratsvorsitzende durch das Landgericht Braunschweig im Jahre 2008 wegen Anstiftung zur Begünstigung eines Mitglieds eines Betriebsrats sowie eines Mitglieds eines europäischen Betriebsrats (§ 119 BetrVG, § 26 StGB) in Tateinheit mit Beihilfe zur Untreue zu einer Gesamtfreiheitsstrafe von 2 Jahren und 9 Monaten verurteilt wurde. Der „Vorteilsgeber“, der ehemalige Personalvorstand des VW-Konzerns, war bereits vorab zu einer Freiheitsstrafe verurteilt worden. Das Vorstandsmitglied hatte ohne Kenntnis der weiteren Vorstände Sonderbonuszahlungen an den Betriebsratsvorsitzenden in der Hoffnung veranlasst, damit dessen Wohlwollen zu gewinnen. Darüber hinaus übernahm die VW AG für den Konzernbetriebsratsvorsitzenden in 27 Fällen die Kosten für die Buchung privater Reisen und Hotelaufenthalte, die Übernahme von Telefonkosten, Kosten für Mietfahrzeuge, die Bezahlung eines Maßanzugs und der Dienste von Prostituierten in einem Umfang von rund 230.000,00 EUR. Der BGH hat die Verurteilung wegen Verstoßes gegen § 119 BetrVG wegen Fehlens eines Strafantrags gem. § 119 Abs. 2 BetrVG zwar aufgehoben, die Verurteilung wegen Untreue jedoch bestätigt.¹⁵⁶ Mit Urteil vom 10.1.2023 hat der BGH wiederum in Sachen VW – entgegen der Rechtsprechung des BAG – entschieden, dass auch die Gewährung eines überhöhten Arbeitsentgelts an ein Mitglied des Betriebsrats unter Verstoß gegen das betriebsverfassungsrechtliche Begünstigungsverbot (§ 78 Satz 2 BetrVG) den Tatbestand der Untreue gem. § 266 StGB erfüllt.¹⁵⁷

Praktische Bedeutung erlangt die Strafnorm des § 119 Abs. 1 BetrVG jedoch, auch wenn eine unmittelbare Bestrafung im Regelfall am Fehlen des Strafantrages scheitert, mittelbar für die Frage einer unternehmensnützigen Steuerhinterziehung gem. § 370 AO. Wenn nämlich Zahlungen des Unternehmens an den

155 Die Nr. 2. des § 119 Abs. 1 BetrVG betrifft die Behinderung oder Störung der Tätigkeit des Betriebsrats oder anderer betriebsverfassungsrechtlich relevanter Einrichtungen und ist hier nicht weiter relevant.

156 BGHSt 54, 148 ff.; zur Strafbarkeit der Förderung und des Aufbaus einer unternehmensfreundlichen Aktionsgemeinschaft von Betriebsangehörigen mit dem Ziel der Einflussnahme auf die Zusammensetzung von Betriebsräten und Mitbestimmungsorganen („Arbeitsgemeinschaft Unabhängiger Betriebsangehöriger – AUB e.V.“) durch Verantwortliche der Siemens AG, vgl. LG Nürnberg-Fürth, ArbuR 2010, 35 ff.

157 BGH, Urt. v. 10.1.2023 – 6 StR 133/22. Anm.: Um insoweit aufgetretene „Rechtsunsicherheiten“ zu beseitigen hat die Bundesregierung zwischenzeitlich eine Änderung des § 37 BetrVG in den Bundestag eingebracht (BT-Drs. 20/9469 v. 27.11.2023).

Betriebsrat den Tatbestand des § 119 Abs. 1 Nr. 1 BetrVG erfüllen, handelt es sich bei solchen Zahlungen um die Zuwendung von Vorteilen, die als rechtswidrige Handlungen gem. § 4 Abs. 5 Nr. 10 EStG, § 8 Abs. 1 Satz 1 KStG nicht als Betriebsausgaben abziehbar sind. Ist ein solcher Betriebsausgabenabzug allerdings erfolgt, ist darin unabhängig von der Verfolgbarkeit des Verstoßes gegen § 119 BetrVG, wie etwa im Fall **Siemens/AUB**, möglicherweise eine Steuerhinterziehung zu sehen.¹⁵⁸

- 98** Ebenfalls einen Korruptionstatbestand im weiteren Sinne stellt die in der Praxis wenig bekannte „**Vorteilsannahme und -gewährung**“ in der **Hauptversammlung** dar, die aber immerhin mit einer Geldbuße von bis zu 25.000,00 EUR geahndet werden kann. Gem. **§ 405 Abs. 3 Nr. 6 AktG** handelt ordnungswidrig, wer besondere Vorteile als Gegenleistung dafür fordert, sich versprechen lässt oder annimmt, dass er bei einer Abstimmung in der Hauptversammlung oder in einer gesonderten Versammlung nicht oder in einem bestimmten Sinne stimme (Vorteilsannahme). Gem. **§ 405 Abs. 3 Nr. 7 AktG** handelt ordnungswidrig, wer besondere Vorteile als Gegenleistung dafür anbietet, verspricht oder gewährt, dass jemand bei einer Abstimmung in der Hauptversammlung oder in einer gesonderten Versammlung nicht oder in einem bestimmten Sinne stimme (Vorteilsgewährung). Als besonderes Compliance-Risiko ist auch hier die steuerliche Behandlung derartiger Zuwendungen zu berücksichtigen.

2. Untreue (§ 266 StGB)

- 99** Der Tatbestand der Untreue gem. § 266 Abs. 1 StGB, also die Verletzung einer Vermögensbetreuungspflicht gegenüber dem Treugeber, häufig einem Unternehmen, und die damit verbundene Herbeiführung eines Vermögensschadens, erfolgt im Regelfall im Eigeninteresse des Täters und zum Nachteil des Unternehmens und stellt damit prima vista kein Compliance-Risiko im engeren Sinne für das Unternehmen dar. Gerade im Zusammenhang mit Korruptionsstraftaten stellt sich jedoch häufig auch eine Untreuestrafbarkeit der Unternehmensverantwortlichen ein. Dies liegt daran, dass der Unternehmer, noch weniger der eigenmächtig handelnde Mitarbeiter, das benötigte Bestechungsgeld regelmäßig nicht aus dem (eigenen) versteuerten Einkommen aufwenden möchte. Das zu zahlende Bestechungsgeld muss also insbesondere bei einer beabsichtigten Bestechung aus dem Unternehmen heraus zunächst einmal generiert werden. Bereits diese Generierung des Bestechungsgeldes entweder am Arbeitgeber oder an der Steuer vorbei birgt aber bereits erhebliche strafrechtliche Risiken unter dem Aspekt der Untreue.
- 100** Auf der anderen Seite, der Seite des Bestochenen, steht erhaltenes Bestechungsgeld regelmäßig der vertretenen Institution, etwa dem Unternehmen, zu. Die Einbehaltung des Bestechungsgeldes (um welches der vergebene Auftrag regel-

¹⁵⁸ BGH, Beschl. v. 13.9.2010 – 1 StR 220/09 (Siemens/AUB „Schelsky“) mit grundlegenden Ausführungen zu § 119 BetrVG, BGHSt 55, 288.

mäßig überhöht erteilt wurde) stellt ebenso wie die überteuerte Vergabe des Auftrags eine Treupflichtverletzung dar, die regelmäßig zu einem Vermögensschaden beim Unternehmen und damit zu einer Strafbarkeit des Empfängers wegen Untreue gem. § 266 Abs. 1 StGB zum Nachteil des Treugebers führt.

a) Generierung von Bestechungsgeld

Aufgrund der hohen Kontrolldichte insbesondere bei größeren Kapitalgesellschaften gestaltet sich bereits die unverdächtige Generierung potenzieller Bestechungsgelder, vornehmer umschrieben als „nützliche Aufwendungen“ (NA), innerhalb des Unternehmens als schwierig. Bislang war es nicht unüblich, eine **Vermittlungsprovision** auszukehren oder **Beraterverträge** mit Vermittlern abzuschließen, die keine oder keine adäquate Beratungsleistung erbringen, sondern das Beraterhonorar an den eigentlichen Empfänger weiterleiten. Derartige Vermittlungsprovisionen oder Beraterhonorare wurden als gewinnmindernde und damit steuerreduzierende Betriebsausgaben angesetzt. Diese „althergebrachte“ Methode der Zahlung von Vermittlungsprovisionen oder des Abschlusses von Beraterverträgen führt zwar zunächst zu einem Betriebsausgabenabzug, wird jedoch im Rahmen steuerlicher Betriebsprüfungen zunehmend als korruptionsrelevant erkannt. In der neueren Praxis sind dann alternativ (Rest-)Beträge aus Auslandsaufträgen nicht nach Deutschland, sondern an der offiziellen Buchhaltung vorbei auf Konten, an Treuhänder oder an Stiftungen in üblicherweise rechtshilfeaversen Drittländern (sog. Steueroasen) transferiert worden. Ebenso festzustellen ist die Bestückung solcher schwarzen Kassen über die Einschaltung eines (unnötigen) Zwischenhändlers in derartigen Drittländern, der im Rahmen eines Streckengeschäfts als Kaufpreisempfänger fungiert und den Differenzbetrag zum eigentlichen Kaufpreis entweder aus steuerlichen oder anderen Gründen einbehält. Aus einer solchen verdeckten bzw. **schwarzen Kasse** heraus ist die Bezahlung von nützlichen Aufwendungen, Beschleunigungsgeldern oder auch Kickbacks ohne Kenntnisnahme der deutschen Behörden möglich. Der Tatbestand der **Untreue** kann jedoch durchaus bereits erfüllt sein, wenn Angestellte einer Kapitalgesellschaft dieser ohne wirksame Einwilligung Vermögenswerte entziehen, um sie nach Maßgabe eigener Zwecksetzung, wenn auch möglicherweise im (vermeintlichen) Interesse der Gesellschaft zu verwenden (sog. „Kriegskasse“). Hierbei ist bereits, so die Rechtsprechung,¹⁵⁹ darauf abzustellen, dass es unterlassen wird, die auf verdeckt geführten Konten verborgenen Geldmittel gegenüber dem Unternehmen zu offenbaren, indem sie als Aktiva in die Buchführung eingestellt werden, um den Anforderungen der Bilanzwahrheit zu genügen. Mit Urteil vom 29.8.2008 hat der BGH insoweit wegweisend entschieden, dass das Führen einer verdeckten Kasse nicht nur einen Gefährdungsschaden, sondern einen **endgültigen Vermögensschaden** i. S. v. § 266 Abs. 1 StGB herbeiführt.¹⁶⁰ Im Fall des Führens einer schwarzen Kasse kann die Berechtigte

101

159 BGHSt 55, 266 („Trienekens“); BGHSt 52, 323 („Siemens/ENEL“) = NJW 2009, 89.

160 BGHSt 52, 323, 338 („Siemens/ENEL“); ebenso 55, 266.

(Gesellschaft) auf die verborgenen Vermögenswerte keinen Zugriff nehmen. Die Absicht, die Geldmittel – ganz oder jedenfalls überwiegend – bei späterer Gelegenheit im Interesse der Gesellschaft einzusetzen, insbesondere um durch verdeckte Bestechungszahlungen Aufträge zu akquirieren und der Gesellschaft so mittelbar zu einem Vermögensgewinn zu verhelfen, sei hierfür ohne Belang.

- 102** Eine untreuerelevante Pflichtwidrigkeit kann im Einzelfall allerdings ausgeschlossen sein, wenn eine wirksame **Einwilligung** der Vermögensinhaber vorliegt.¹⁶¹ Bei juristischen Personen tritt an die Stelle des Vermögensinhabers dessen oberstes Willensorgan für die Regelung der inneren Angelegenheiten, im Fall einer **GmbH** also die Gesamtheit ihrer Gesellschafter. Nach der neueren Rechtsprechung des Bundesgerichtshofs kommt jedoch nur dem Einverständnis sämtlicher Gesellschafter einer Kapitalgesellschaft oder einem (Mehrheits-)Beschluss, wenn die Minderheitsgesellschafter jedenfalls gehört worden sind, tatbestandsausschließende Wirkung zu.¹⁶² Bei einer Aktiengesellschaft ist Voraussetzung für ein strafrechtlich bedeutsames Einverständnis, dass es entweder von dem Alleinaktionär oder von der Gesamtheit der Aktionäre durch einen Beschluss der **Hauptversammlung** über die Verwendung des Bilanzgewinns erteilt worden ist, nicht gegen Rechtsvorschriften verstößt oder aus sonstigen Gründen ausnahmsweise als unwirksam zu bewerten ist.¹⁶³ Die Herbeiführung einer rechtswirksamen Einwilligung ist mithin schwierig und stellt compliance-technisch aufgrund der problematischen Verwendungsabsicht ohnehin keine Lösung dar.

b) Zahlung von Bestechungsgeld

- 103** Die Zahlung von Bestechungsgeld, sei es unmittelbar als Barzuwendung oder als Vermittlungsprovision bzw. Beraterhonorar, kann sich ebenfalls als untreuerelevant darstellen. Widerspricht die Hingabe von Vermögenswerten zum Zwecke der Bestechung bereits dem Willen des Vermögensinhabers, liegt unzweifelhaft ein pflichtwidriges Verhalten i. S. v. § 266 StGB vor. Ein solcher entgegenstehender Wille kann sich im Unternehmensbereich insbesondere aus dahingehenden Compliance-Erklärungen (sog. **Compliance Commitments**) ergeben.¹⁶⁴
- 104** Erfolgt die Bestechungshandlung jedoch mit Einwilligung des Vermögensinhabers, ist das Vorliegen einer Pflichtwidrigkeit i. S. v. § 266 StGB zweifelhaft, soweit etwa aufgrund des Einsatzes des Bestechungsgeldes ein gewinnbringender Auftrag generiert wird. Erfolgt die Gegenleistung (der gewinnbringende Auftrag) nicht, liegt ein Vermögensschaden vor. Erfolgt die Gegenleistung jedoch, liegt prima vista zwar kein Vermögensschaden i. S. v. § 266 Abs. 1 StGB vor, die

161 Vgl. *Saliger/Gaede*, HRRS 2008, 57, 69; vgl. auch *Dierlamm*, in: MünchKomm-StGB, § 266 Rn. 143; *Fischer*, StGB, § 266 Rn. 90 ff.

162 BGHSt 55, 266 für die GmbH; 50, 331, 342 für die AG.

163 BGHSt 50, 331; 55, 266.

164 Zur Frage der Ernsthaftigkeit solcher Erklärungen *Ransiek*, StV 2009, 321. Zum Compliance Commitment → *Schulz*, Kap. 1 Rn. 69 f.

Gegenleistung ist dann aber immer noch mit dem Risiko der Anfechtbarkeit und dem Risiko strafprozessualer Maßnahmen, etwa der Einziehung des Erlangten gem. § 73 Abs. 1 Satz 1 StGB, behaftet.¹⁶⁵ Die Gegenleistung ist somit um das Entdeckungsrisiko gemindert.¹⁶⁶ Nicht nur, da diese Rechtsfrage in der Rechtsprechung des BGH sowie des BVerfG in hohem Maße umstritten ist,¹⁶⁷ sondern insbesondere, da eine Konstellation, in der ein Bestechungsgeld nicht der Strafdrohung der §§ 299, 331 ff., 335a StGB unterliegt, kaum mehr denkbar ist, kann ein dahingehendes Einverständnis unter Compliance-Aspekten ohnehin nicht erteilt werden.

Nach der Rechtsprechung des BGH liegt auch bei der Vereinbarung von Schmiergeldzahlungen in Form eines prozentualen Preisaufschlags regelmäßig ein Nachteil i. S. d. § 266 Abs. 1 StGB vor.¹⁶⁸ Diese Rechtsprechung beruht auf der Erwägung, dass jedenfalls mindestens der Betrag, den der Vertragspartner für Schmiergelder aufwendet, auch in Form eines Preisnachlasses dem Geschäftsherrn des Empfängers hätte gewährt werden können.¹⁶⁹ Bei der Auftrags-erlangung durch Bestechung im geschäftlichen Verkehr bildet deshalb der auf den Preis aufgeschlagene Betrag, der lediglich der Finanzierung des Schmiergeldes dient, regelmäßig die Mindestsumme des beim Auftraggeber entstandenen Vermögensnachteils i. S. v. § 266 Abs. 1 StGB. Inwieweit andere Anbieter noch teurere Angebote eingereicht haben, soll, so der BGH, demgegenüber unerheblich sein.¹⁷⁰

Die Erbringung von korruptiven Zahlungen (vulgo: Schmiergeld) stellt sich damit ebenso wie die Entgegennahme von Bestechungsgeld regelmäßig als Treuepflichtverletzung gegenüber dem eigenen Unternehmen dar. In (fast) jedem Korruptionssachverhalt findet sich daher auch eine Untreuestrafbarkeit gem. § 266 Abs. 1 StGB. Die Untreue dient in der Praxis nicht selten als **Auffangtatbestand** in Fällen mangelnder strafrechtlicher Relevanz i. S. d. §§ 331 ff. StGB oder auch in Fällen mangelnder Beweisbarkeit.

3. Steuerverkürzung (§§ 370 ff. AO)

Die Verkürzung von Unternehmenssteuern stellt nicht nur als solche ein erhebliches Compliance-Risiko dar, gerade hier befindet sich das Einfallstor für die

165 Vgl. BGHSt 50, 299 ff.

166 Selbst darin muss aber noch kein Schaden liegen. So verweist *Ransiek* (StV 2009, 321, 322 m. w. N.) auf einen Fall aus dem Bereich Siemens, in dem der Einsatz von 6 Mio. EUR Bestechungsgeld zu einem (Vorsteuer-)Gewinn von über 100 Mio. EUR geführt habe, jedoch „lediglich“ ein Verfall (heute: Einziehung) i. H. v. 38 Mio. EUR angeordnet worden sei.

167 BGHSt 52, 323 ff.; BVerfGE 126, 170; BVerfGE 130, 1, Rn. 174; vertiefend: *Böttger*, Wirtschaftsstrafrecht in der Praxis, 2. Aufl. 2015, S. 331 ff.

168 BGHSt 50, 299 ff.; 47, 295, 298 f.; 49, 317, 332 f.

169 Vgl. *Raum*, in: Wabnitz/Janovsky, Handbuch des Wirtschafts- und Steuerstrafrechts, 4. Aufl. 2014, S. 319 m. w. N.

170 BGHSt 50, 299 ff.; BGH, wistra 2001, 295, 296.

Aufdeckung anderweitiger im Unternehmen schlummernder Compliance-Risiken.

- 108** Im Hinblick auf die Hauptproblemfelder einer Steuerverkürzung im Unternehmensinteresse, mithin dem eigentlichen steuerlichen Compliance-Risiko, so in erster Linie der Umsatzsteuerverkürzung, der Lohnsteuerverkürzung sowie der Körperschaftssteuerverkürzung, kann auf die ausführliche Darstellung im Kapitel 25 **Tax Compliance** verwiesen werden. Die Tatsache, dass die vorsätzliche oder auch nur leichtfertige Verkürzung von Unternehmenssteuern im (vermeintlichen) Unternehmensinteresse per se ein Compliance-Risiko darstellt, dürfte auf der Hand liegen. Im Falle einer vorsätzlich begangenen Steuerhinterziehung droht den Unternehmensverantwortlichen gem. § 370 Abs. 1 AO ein Strafmaß von bis zu fünf Jahren Freiheitsstrafe, in besonders schweren Fällen sogar Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein solcher besonders schwerer Fall liegt in der Regel bereits vor, wenn der Täter Steuern „in großem Ausmaß“ verkürzt oder nicht gerechtfertigte Steuervorteile in entsprechender Höhe erlangt hat (§ 370 Abs. 3 Satz 2 Nr. 1 AO). Ein großes Ausmaß ist nach der Rechtsprechung des BGH mittlerweile bei jeder Steuerhinterziehung über 50.000,00 EUR erreicht.¹⁷¹ Die frühere Unterscheidung zwischen Gefährdung des Steueranspruchs durch Verschweigen steuerpflichtiger Einkünfte und Umsätze (Wertgrenze 100.000,00 EUR) und echtem Vermögensverlust durch Erschleichen ungerechtfertigter Erstattungen (Wertgrenze 50.000,00 EUR) wurde durch den BGH ausdrücklich aufgehoben. Das Erreichen der Schwelle des „großen Ausmaßes“ ist allerdings für jede einzelne Tat im materiellen Sinne, also etwa für jeden Erklärungszeitraum, gesondert zu bestimmen.¹⁷² Infolge der zunehmend restriktiver werdenden Rechtsprechung des BGH in Steuerstrafsachen ist bei Erreichen eines Verkürzungsbetrages von 1 Mio. EUR konsequent auf Freiheitsstrafe nicht unter zwei Jahren zu erkennen mit der Folge, dass dann gem. § 56 Abs. 2 StGB auch eine Strafaussetzung zur Bewährung nur noch sehr ausnahmsweise bei Vorliegen besonders gewichtiger Milderungsgründe in Betracht kommt.¹⁷³ Aufgrund der in der Steuerverkürzung liegenden Verletzung unternehmensbezogener Pflichten und der Absicht der Bereicherung des Unternehmens droht dem Unternehmen neben der (Nach-)Zahlung der verkürzten Steuern, der Hinterziehungszinsen i. H. v. 0,5 % pro Monat¹⁷⁴ und der Bestrafung der Verantwortlichen zusätzlich die Einbeziehung in das Straf- oder Ordnungswidrigkeitenverfahren und die Verhängung einer Unternehmensgeldbuße gem. § 30 OWiG.
- 109** Weniger spektakulär aber umso gefährlicher ist die Aufdeckung weniger offensichtlicher Steuerverkürzungen, die ihrerseits auf andere, nicht-steuerrechtliche Compliance-Verstöße, insbesondere Korruptionssachverhalte, zurückzuführen

¹⁷¹ BGH, NJW 2016, 965.

¹⁷² BGHSt 53, 71.

¹⁷³ BGHSt 57, 123.

¹⁷⁴ §§ 235, 238 AO.

sind. Da Korruptionssachverhalte regelmäßig auf Verdunklung angelegt sind, liegt es nahe, dass die Zahlungswege und Beziehungsgeflechte auch gegenüber den Steuerbehörden nicht offenbart werden sollen, die im Fall ihrer Kenntnisnahme einer Mitteilungspflicht an die Staatsanwaltschaft unterliegen und Amtshilfe leisten würden. Da die Aufwendung von Bestechungsgeldern jedoch bei oberflächlicher Betrachtung als betriebsnützlich angesehen werden kann, wollen Unternehmen jedoch häufig nicht ohne Weiteres auf die steuermindernde Geltendmachung dieser Posten als Betriebsausgaben verzichten. Dies ist jedoch nicht mehr möglich.

Bis 1999 war die steuermindernde Geltendmachung von im Ausland aufgewendeten sog. „Nützlichen Aufwendungen“ (also Bestechungsgeldern) als Betriebsausgaben einkommensteuerrechtlich erlaubt.¹⁷⁵ Da die Auslandsbestechung in Deutschland jedoch bereits seit Inkrafttreten von EUBestG und IntBestG im September 1998 bzw. Februar 1999 strafrechtlich relevant ist, musste dieser Zustand natürlich geändert werden. Durch das Steuerentlastungsgesetz 1999/2000/2002 vom 24.3.1999¹⁷⁶ wurde das EStG dann dahingehend geändert, dass strafrechtlich oder bußgeldrechtlich relevante Zuwendungen nicht mehr absetzbar waren, die Finanzbehörden in solchen Fällen vielmehr sogar verpflichtet sind, die zuständige Staatsanwaltschaft zu informieren.

110

Aufgrund des **Betriebsausgabenabzugsverbots des § 4 Abs. 5 EStG** dürfen bestimmte Betriebsausgaben den Gewinn nicht mindern, so insbesondere nach Nr. 10 die Zuwendung von Vorteilen sowie damit zusammenhängende Aufwendungen, wenn die Zuwendung der Vorteile eine rechtswidrige Handlung darstellt, die den Tatbestand eines Strafgesetzes oder eines Gesetzes verwirklicht, das die Ahndung mit einer Geldbuße zulässt. Das Abzugsverbot betrifft damit jegliche Zahlung von Schmier- und Bestechungsgeldern sowie die damit zusammenhängenden Kosten. Die strafrechtliche Relevanz einer Zuwendung ist damit nunmehr Voraussetzung für die steuerliche Nichtabsetzbarkeit von Betriebsausgaben, die strafrechtliche Bewertung ausschlaggebend für die steuerlichen Konsequenzen.¹⁷⁷ Zwischen Steuerrecht und Strafrecht besteht damit eine Wechselwirkung, in die allerdings auch die sonstigen Regelungen des EStG einfließen. So etwa § 4 Abs. 5 Satz 1 Nr. 1 EStG, wonach Geschenke bis zu einem Wert von 50,00 EUR p.a. abzugsfähig sind, § 4 Abs. 5 Satz 1 Nr. 2 EStG, wonach 70 % der Aufwendungen für die Bewirtung von Personen aus geschäftlichem Anlass, die nach der allgemeinen Verkehrsauffassung als angemessen anzusehen und deren Höhe und betriebliche Veranlassung nachgewiesen sind, absetzbar sind oder etwa die Regelung durch das BMF-Schreiben vom 22.8.2005, demzufolge Kundeneinladungen zu Sportveranstaltungen (VIP-Logen in Sportstätten) auch im

111

¹⁷⁵ Vgl. Fn. 2.

¹⁷⁶ StEntG 1999/2000/2002 vom 24.3.1999, BGBl. I 1999, S. 402.

¹⁷⁷ Zu den Details der Anwendung vgl. BMF-Schreiben, 10.10.2002, IV A 6 – 2245 – 35/02 „Abzugsverbot für die Zuwendung von Vorteilen i. S. d. § 4 Abs. 5 Satz 1 Nr. 10 EStG“.

Fall eines Wertes von über 35,00 EUR vom Einladenden pauschal versteuert werden können und auf eine Empfängerbenennung gem. § 160 AO verzichtet werden kann.¹⁷⁸ Die unentgeltliche Zurverfügungstellung von Plätzen in einer VIP-Loge an Geschäftspartner und Arbeitnehmer kann vom Zuwendenden zudem gem. § 37b EStG pauschal versteuert werden.¹⁷⁹

- 112** Der Versuch, die steuerlichen Vorgaben zu umgehen, indem Bestechungsgelder etwa als Vermittlerprovisionen oder Beraterhonorar getarnt oder sonst als abzugsfähige Betriebsausgaben steuermindernd geltend gemacht werden, stellt eine (versuchte) Steuerhinterziehung gem. § 370 Abs. 1 AO dar. Neben einer Verkürzung der Einkommen- bzw. Körperschaftsteuer kommt, da § 7 Abs. 1 GewStG auf das Abzugsverbot des § 4 Abs. 5 Satz 1 Nr. 10 EStG verweist, auch eine Gewerbesteuerhinterziehung in Betracht. Die in der (versuchten) Geltendmachung von korruptiven Zahlungen als Betriebsausgabe liegende Steuerhinterziehung wird häufig allerdings erst im Rahmen der steuerlichen Betriebsprüfung offenbar und führt dann allerdings nicht nur zur Einleitung eines Steuerstraßverfahrens, sondern zugleich, aufgrund der verpflichtenden Information der Staatsanwaltschaft (§ 4 Abs. 5 Satz 1 Nr. 10 Satz 3 EStG), zur Einleitung eines Korruptionsstraßverfahrens.
- 113** Die erhebliche praktische Relevanz des hier schlummernden **Compliance-Risikos** liegt insbesondere in der profiskalischen Motivation der Betriebsprüfer begründet. Da diese eine Prüfung regelmäßig mit einem „Mehrergebnis“ abschließen wollen, liegt es förmlich auf der Hand, schwerpunktmäßig die häufig nicht optimal dokumentierten Auslandssachverhalte, insbesondere Vermittlungsprovisionen sowie Beraterverträge, zu thematisieren und diesen Ausgaben im Interesse der Feststellung der Nichtabziehbarkeit eine strafrechtliche Relevanz zu unterstellen. Allein eine solche „Arbeitshypothese“ führt jedoch dazu, dass der dahingehende Verdacht gemäß § 4 Abs. 5 Satz 1 Nr. 10 Satz 3 EStG der zuständigen Staatsanwaltschaft gemeldet werden muss. Der dann einmal in Bewegung gesetzte Ermittlungsapparat führt per se bereits zu Kollateralschäden im Unternehmen. Gelingt dann aufgrund der im Steuerverfahren gem. § 90 Abs. 2 AO bestehenden erhöhten Mitwirkungspflicht bei Auslandssachverhalten der Verwendungs- oder Empfängernachweis nicht, so führt dies nicht nur zur Nichtanerkennung der Betriebsausgaben, sondern häufig auch zu erheblichen Schwierigkeiten im Strafverfahren wegen des behaupteten korruptiven Hintergrundes der Zahlungen.

¹⁷⁸ Vgl. BMF-Schreiben, 22.8.2005, IV B 2 – S 2144 – 41/05 „Ertragsteuerliche Behandlung von Aufwendungen für VIP-Logen in Sportstätten“, BStBl. I 2005, 845.

¹⁷⁹ BFH, Urt. v. 23.11.2023 – VI R 15/21.

IV. Strafrechtliche Risiken der Non-Compliance für die Verantwortlichen des Unternehmens

1. Originäre strafrechtliche Verantwortlichkeit

Mangels Existenz eines Unternehmensstrafrechts im engeren Sinne standen historisch immer schon die handelnden natürlichen Personen im Fokus der Strafjustiz. Nach Inkrafttreten des VerSanG wird sich das Verfolgungsinteresse der Staatsanwaltschaften zunächst sicherlich verstärkt auf die Verhängung von Verbandsgeldsanktionen richten, allein aufgrund des Legalitätsprinzips werden die Unternehmensverantwortlichen jedoch auch weiterhin Gegenstand intensiver Befassung bleiben. Die Zeiten, in denen sich die Justiz jedoch mit der Bestrafung der unmittelbar Handelnden im Unternehmen, etwa dem Vertriebsleiter, der einen Beratervertrag geschlossen hat, begnügt hat, sind jedoch längst vorbei. Ziel der Ermittlungen insbesondere bei den Schwerpunktstaatsanwaltschaften sind erklärtermaßen die Verantwortlichen des Unternehmens in der Unternehmensleitung sowie zunehmend auch im Aufsichtsrat, die Staatsanwälte selbst sehen sich quasi als „Großwildjäger“.¹⁸⁰ Gegenstand der Ermittlungen und der Ahndung ist daher zunehmend das **unmittelbare Handeln der Unternehmensleitung**, etwa durch das Treffen konkreter Entscheidungen sowie die Erteilung von Weisungen, das Unterlassen erforderlicher Handlungen, die sog. „**Geschäftsherrenhaftung**“, z.B. durch die Nichtdurchführung eines gebotenen Produktrückrufs, sowie zunehmend auch die Fahrlässigkeitshaftung wegen der Verletzung der im (Geschäfts-)Verkehr erforderlichen Sorgfalt, etwa durch eine unzureichende Pflichtenorganisation, das sog. „**Organisationsverschulden**“.

114

Die unmittelbare Bestrafung der im Unternehmen für die Begehung einer Straftat verantwortlichen Person stellt nicht nur für die unmittelbar handelnden Personen, sondern auch für das Unternehmen als solches ein nicht zu unterschätzendes Compliance-Risiko dar. Aufgrund der teilweise erheblichen Strafen, die bei der Begehung compliance-relevanter Straftaten aus dem Unternehmen heraus sowie im (vermeintlichen) Unternehmensinteresse – auch unter dem Aspekt der Generalprävention – drohen und verhängt werden, im Falle eines besonderen schweren Falles der Bestechung sind dies beispielsweise Freiheitsstrafen von bis zu 10 Jahren, liegt auf der Hand, dass der damit einhergehende „Verlust“ des Führungspersonals jedenfalls für ein mittelständisches Unternehmen erhebliche Auswirkungen haben kann. Aus diesem Grunde haben sich die Unternehmen, die in der Vergangenheit zumindest bereit waren, strafrechtliche Risiken einzugehen, bislang bemüht, die Verantwortlichkeit bei den zuständigen Mitarbeitern zu belassen und möglichst den Nachweis einer Einbeziehung und damit der Verantwortlichkeit der Leitungsorgane zu vereiteln. Ein solches Bemühen verspricht heutzutage jedoch aus zweierlei Gründen keinen Erfolg mehr. Zum einen haben die Ermittlungsbehörden eine derartige Strategie längst erkannt und bemühen sich früh um den Nachweis der Kenntnis und damit der strafrechtlichen

115

180 Vgl. Spiegel Nr. 32/2000 v. 7.8.2000.

Verantwortlichkeit der Leitungsorgane. Die Ermittlungsbehörden halten sich schlichtweg kaum mehr mit den einfachen Mitarbeitern auf, diese werden häufig sogar als „Opfer“ angesehen, mit denen man Nachsicht zeigt, auch weil man sie benötigt, um eine Involvierung der Unternehmensleitung nachzuweisen. Darüber hinaus hat auch die Rechtsprechung den Weg zu einer weitergehenden strafrechtlichen Haftung der Leitungsorgane geebnet.

a) Verantwortlichkeit der Geschäftsleitung

- 116** Die Tatsache, dass das Mitglied der Geschäftsführung oder des Vorstands, das in voller Tatsachenkenntnis höchstpersönlich handelt, entsprechende Anweisungen erteilt oder inkriminierte Handlungen von Untergebenen duldet, strafrechtlich selbst als Täter, Mittäter oder Gehilfe (Anstifter oder Gehilfe) haftet, dürfte keine neue Erkenntnis sein. Rechtlich kompliziert sind jedoch die Grenzfälle, in denen das Mitglied eines mehrköpfigen Führungsorgans entweder keine konkrete Kenntnis von Straftaten seiner Gremienkollegen hat, diese zur Kenntnis nimmt, ggf. innerlich ablehnt, aber nicht verhindert, sich auf die Verantwortung anderer (etwa auch eines Compliance Officers) verlässt oder schlichtweg keine Sorge für hinreichende Organisationsstrukturen trägt und insoweit fahrlässig handelt. Auch die Verletzung der zwischenzeitlich anerkannten Pflicht zur Einrichtung eines auf die Vermeidung strafbarer Handlungen ausgerichteten Compliance-Management-Systems kann insoweit zu einer Pflichtverletzung führen, die, soweit aus dieser Pflichtverletzung ein Schaden resultiert, ihrerseits wiederum zu einer (Fahrlässigkeits-)Strafbarkeit der Unternehmensleitung – das sog. „Organisationsverschulden“ – führt. Es entspricht zwischenzeitlich der wohl überwiegenden Auffassung, dass der Vorstand im Rahmen seiner Legalitätspflicht dafür Sorge zu tragen hat, dass das Unternehmen so organisiert und beaufsichtigt wird, dass keine Gesetzesverstöße wie etwa Schmiergeldzahlungen an Amtsträger oder an Privatpersonen erfolgen. Seiner Organisationspflicht genügt ein Vorstandsmitglied bei entsprechender Gefährdungslage nur dann, wenn er eine auf Schadensprävention und Risikokontrolle angelegte Compliance-Organisation einrichtet. Entscheidend für den Umfang im Einzelnen sind dabei Art, Größe und Organisation des Unternehmens, die zu beachtenden Vorschriften, die geografische Präsenz wie auch Verdachtsfälle aus der Vergangenheit. Die Einhaltung des Legalitätsprinzips und demgemäß die Einrichtung eines funktionierenden Compliance-Systems gehört damit zur Gesamtverantwortung des Vorstands.¹⁸¹ Auch hier kommt neben einer zivilrechtlichen Haftung eine eigenständige strafrechtliche Verantwortlichkeit der Mitglieder der Geschäftsleitung sowie der aufgrund der Delegation beauftragten Mitarbeiter in Betracht.

¹⁸¹ So neuerdings auch die Rspr., BGH, Urt. v. 9.5.2017 – 1 StR 265/16, Rn. 118; Urt. v. 27.4.2022 – 5 StR 278/21; LG München I, Urt. v. 10.12.2013 – 5 HK O 1387/10 (sog. „Neubürger-Urteil“), DB 2014, 766; vgl. hierzu auch → *Schulz*, Kap. 1 Rn. 39.

b) Gremienentscheidungen

Die Entwicklung hin zu einer Gesamtverantwortlichkeit der Leitungsgremien des Unternehmens hat ihren Ausgang in der sog. „**Lederspray-Entscheidung**“ aus dem Jahre 1990 genommen.¹⁸² Die Angeklagten waren hier Geschäftsführer mehrerer (verbundener) Gesellschaften, die sich u.a. mit der Herstellung und dem Vertrieb von Lederspray befassen. Nach Eingang von Meldungen über signifikante Gesundheitsschädigungen nach Gebrauch des Ledersprays hat die mehrköpfige Geschäftsführung in einer extra einberufenen Sitzung zwar eine Veränderung des produktspezifischen Warnhinweises beschlossen, nicht jedoch eine öffentliche Warnung oder gar einen Produktrückruf des vertriebenen Ledersprays. Sowohl das erstinstanzlich zuständige Landgericht Mainz als auch der Bundesgerichtshof sahen in dem weiteren Inverkehrbringen des Ledersprays eine vorsätzliche gefährliche Körperverletzung und in dem Unterlassen des Produktrückrufes eine vorsätzliche gefährliche Körperverletzung durch Unterlassen sämtlicher Geschäftsführer. Obwohl sich einer der Geschäftsführer zunächst sogar für eine Rückrufaktion ausgesprochen hatte, sich jedoch mit seiner Meinung nicht durchsetzen konnte und sich der Mehrheitsmeinung angeschlossen hatte, hat der Bundesgerichtshof jedenfalls in Krisensituationen, in denen das Unternehmen als Ganzes betroffen ist, eine **Gesamtverantwortlichkeit der Geschäftsleitung** angenommen mit der Folge, dass auch im Falle eines (Mehrheits-)Beschlusses eines Kollegialorganes ausschließlich das Gesamtverhalten des Kollegialorganes strafbarkeitsbegründend ist. Unter Anwendung dieses Grundsatzes der **Generalverantwortung und Allzuständigkeit der Geschäftsleitung** hat der Bundesgerichtshof sämtliche an der Abstimmung Beteiligten als Mittäter gemäß § 25 Abs. 2 StGB angesehen. Mit dieser Entscheidung des Bundesgerichtshofs aus dem Jahre 1990 wurde ein Paradigmenwechsel eingeleitet, der im Hinblick auf die Strafbarkeit im Unternehmen unmittelbar bei der Unternehmensleitung ansetzt und insofern zu einer „Top down-Zurechnung“ führt.¹⁸³ Die Rechtsprechung im Unternehmensstrafrecht bewegt sich damit von dem ursprünglichen Grundsatz der individuellen Verantwortlichkeit einer natürlichen Person in Richtung einer Art Kollektivhaftung aller Gremienmitglieder für eine rechtswidrige Entscheidung im Kollegialorgan.

117

War Gegenstand des „Lederspray-Falles“ trotz der Äußerung von Bedenken noch eine einheitliche kollegiale Entscheidung, so musste sich der Bundesgerichtshof im „Mannesmann-Urteil“¹⁸⁴ im Jahre 2005 darüber hinaus mit der Frage der Strafbarkeit einer **Enthaltung** eines Gremienmitgliedes befassen. In dieser Entscheidung hat der BGH die Strafbarkeit eines Mitgliedes eines Kollegialorganes (hier des Aufsichtsrates) angenommen, obwohl dieses sich bei der Fassung des (rechtswidrigen) Beschlusses der Stimme enthalten hat. In Kenntnis der Mehrheitsverhältnisse führe der sich Enthaltende durch seine

118

182 BGHSt 37, 106.

183 Rotsch, Criminal Compliance, § 4 Rn. 5.

184 BGHSt 50, 331 ff.; NSTZ 2006, 214 ff.

Stimmenthaltung vorsätzlich die Wirksamkeit eines Beschlusses herbei, sodass ihm die (strafrechtlich relevante) Mehrheitsentscheidung als Mittäter zuzurechnen ist.

c) Delegation von Verantwortungsbereichen

- 119** Der Grundsatz der Generalverantwortung und Allzuständigkeit der Geschäftsleitung, der auch zu einer strafrechtlichen Verantwortlichkeit des Gesamtorgans führt, gilt jedoch ausweislich der Rechtsprechung zunächst einmal nur in den Situationen, in denen das Unternehmen als Ganzes betroffen ist. Von dem insoweit aus dem Gesellschaftsrecht übertragenen „Prinzip der gemeinschaftlichen Geschäftsführung“¹⁸⁵ gibt es in der Praxis jedoch relevante **Ausnahmen**. So erfolgt in der Praxis allein aus Gründen der Effektivität im Regelfall eine Verteilung der Geschäftsführungsaufgaben auf die Mitglieder der Kollegialorgane. Von dem Prinzip der Gesamtgeschäftsführung abweichende Organisationsformen sind insoweit etwa die Einräumung einer Einzelgeschäftsführungsbefugnis (verbunden mit einem Alleinvertretungsrecht) an einzelne Organmitglieder, die Vereinbarung von Verantwortlichkeiten für einzelne Ressourcen (z. B. Produktion, Vertrieb, Finanzen, HR oder Recht) sowie die Einräumung einer auf bestimmte Sparten des Unternehmens bezogenen Einzelgeschäftsführungsbefugnis.¹⁸⁶ Die Festlegung solcher Abweichungen vom Prinzip der Gesamtgeschäftsführung im Rahmen der Satzung oder der Geschäftsordnung sind gemäß § 77 Abs. 1 Satz 2 AktG auch bei der Aktiengesellschaft zulässig und führen dazu, dass die jeweils geschäftsführungsbefugten Vorstandsmitglieder im Rahmen der ihnen eingeräumten Einzelgeschäftsführungsbefugnis eigenverantwortlich handeln. Eine solche **Geschäftsverteilung oder Ressortaufteilung** auf der Ebene der Geschäftsführung setzt nach der Rechtsprechung des Bundesgerichtshofs¹⁸⁷ jedoch eine klare und eindeutige Abgrenzung der Geschäftsführungsaufgaben aufgrund einer von allen Mitgliedern des Organs mitgetragenen Aufgabenzuweisung voraus, die die vollständige Wahrnehmung der Geschäftsführungsaufgaben durch hierfür fachlich und persönlich geeignete Personen sicherstellt und ungeachtet der Ressortzuständigkeit eines einzelnen Geschäftsführers die Zuständigkeit des Gesamtorgans insbesondere für nicht delegierbare Angelegenheiten der Geschäftsführung wahrt. Eine diesen Anforderungen genügende Aufgabenzuweisung bedarf nicht zwingend einer schriftlichen Dokumentation, wenngleich die schriftliche Dokumentation regelmäßig das naheliegende und geeignete Mittel für eine klare und eindeutige Aufgabenabgrenzung darstellt.¹⁸⁸

¹⁸⁵ § 77 Abs. 1 Satz 1 AktG.

¹⁸⁶ Vgl. hierzu ausführlich: *Knierim*, in: Wabnitz/Janovsky, Handbuch Wirtschafts- und Steuerstrafrecht, 4. Aufl. 2014, Kap. 5 Rn. 36.

¹⁸⁷ BGH, Urt. v. 6.11.2018 – II ZR 11/17, NJW 2019, 1067.

¹⁸⁸ BGH, Urt. v. 6.11.2018, a. a. O., Rn. 17; anders jedoch bei steuerrechtlichen Pflichten gem. § 34 AO, vgl. BFHE 141, 443, 446 f.; 146, 23, 25 f.

Im Hinblick auf die Kernaufgaben der Unternehmensleitung unterliegt eine solche „**horizontale Delegation**“ jedoch bestimmten Grenzen. Nicht zulässig ist die Delegation der grundsätzlichen Planungs- und Steuerungsverantwortung, der Organisationsverantwortung, der Finanzverantwortung sowie nach herrschender Auffassung auch der Verantwortung für die Einrichtung einer Compliance-Organisation, die zu den „unveräußerlichen Leitungsaufgaben des Gesamtvorstandes“ gehört.¹⁸⁹ Unzulässig ist demnach eine vollständige Delegation der vorbezeichneten Aufgaben an einzelne Vorstandsmitglieder oder gar andere Mitarbeiter sowie die Delegation von Einzelaufgaben, die dem Gesamtvorstand etwa konkret durch das Aktiengesetz übertragen sind.¹⁹⁰ Unabhängig von der (zulässigen) Delegation verbleibt es damit bei einer Gesamtverantwortung aller Gremienmitglieder für die ordnungsgemäße und rechtmäßige Gesamtleitung des Unternehmens. Insofern hat das Kollegialorgan sicherzustellen, dass der Gesamtvorstand im Falle der Delegation von dem ressortmäßig zuständigen Mitglied ordnungsgemäß informiert wird und die (delegierte) Einzelverantwortlichkeit kontrolliert und überwacht wird. Um sicherzustellen, dass die Unterrichtungspflicht ordnungsgemäß wahrgenommen wird, ist der Vorstand darüber hinaus verpflichtet, ein System ordnungsgemäßer Berichterstattung einzurichten, das den anderen Kollegialmitgliedern die Wahrnehmung ihrer Kontroll- und Überwachungspflicht ermöglicht. Bestehen Anhaltspunkte für eine sorgfaltswidrige oder nicht rechtmäßige Geschäftsführung durch ein Mitglied eines Kollegialorganes, so hat das Gesamtorgan nicht nur ein Rückholrecht, sondern eine Interventionspflicht, um die Problematik dann im Rahmen einer verbindlichen Kollegialentscheidung zu lösen.

Da die Geschäftsleitung in der Praxis naturgemäß nicht sämtliche Entscheidungen selbst treffen kann, ist auch eine Delegation der Aufgabendurchführung auf untergeordnete Mitarbeiter oder gar externe Dritte, die sog. „**vertikale Delegation**“, geboten und zulässig. Voraussetzung der auch strafrechtlichen Unbedenklichkeit ist allerdings, dass im Rahmen der Delegation der zuständige Mitarbeiter ordnungsgemäß ausgewählt wird, ordnungsgemäß eingewiesen wird, er die zur Erfüllung der delegierten Tätigkeit notwendigen Kompetenzen und Mittel erhält und seine Tätigkeit im Rahmen der bei der Geschäftsleitung verbleibenden Generalverantwortlichkeit überwacht wird. Zur Sicherstellung der ordnungsgemäßen Wahrnehmung der (Rest-)Überwachungspflicht ist insbesondere ein angemessenes Berichtswesen erforderlich, das gewährleistet, dass sämtliche Vorgänge, die eine gewisse Wesentlichkeitsschwelle überschreiten, der Geschäftsleitung vorgelegt werden. Nur dann kann die Geschäftsleitung entsprechend der sog. „Business Judgement Rule“ des § 93 Abs. 1 Satz 2 AktG auf Basis angemessener Informationen entscheiden.¹⁹¹ Ist die Delegation ordnungs-

189 So auch *Knierim*, in: Wabnitz/Janovsky, Handbuch Wirtschafts- und Steuerstrafrecht, 4. Aufl. 2014, Kap. 5 Rn. 38. Siehe zu Umfang und Grenzen der Delegation von Compliance-Maßnahmen auch → *Schulz*, Kap. 1 Rn. 56 f. m. w. N.

190 Vgl. etwa §§ 83, 90, 91, 92, 121 AktG.

191 Vertiefend hierzu: *Schürle*, CCZ 2010, 102.

gemäß erfolgt, verbleibt bei der Geschäftsleitung ein strafrechtliches Risiko sowie das Risiko einer Aufsichtspflichtverletzung gemäß § 130 OWiG nur dann, wenn ein Fall des Auswahlverschuldens, der unzureichenden Einweisung bzw. der unzureichenden Bereitstellung von Kompetenzen und Ressourcen oder ein Überwachungsverschulden vorliegt. Die ordnungsgemäße Delegation, die Festlegung und Abgrenzung von Verantwortungsbereichen sowie die Kompetenzzuweisung und die Überwachung, etwa auch durchlaufende Kontrollen oder sog. „Compliance-Audits“ sowie durch den Erlass von Organisations- und Dienstanweisungen sind Ausfluss der die Unternehmensleitung treffenden (Organisations-)Pflicht zur Einführung eines ordnungsgemäßen Compliance-Management-Systems.

d) Verantwortlichkeit des Compliance Officers

- 122** Soweit der Compliance Officer selbst aktiv handelt oder in strafrechtlich relevante Verhaltensweisen eingebunden ist, liegt auf der Hand, dass auch ihn eine eigenständige strafrechtliche Verantwortlichkeit trifft. Streitig ist jedoch die Frage, ob er sich kraft seiner Funktion auch durch Unterlassen strafbar machen kann, wenn er es etwa unterlässt, als problematisch erkannte Verhaltensweisen im Unternehmen abzustellen, wenngleich er selbst in solche Verhaltensweisen nicht eingebunden ist. Voraussetzung für eine solche Strafbarkeit wegen Unterlassens wäre, dass ihn eine Garantenpflicht zur Abwendung des strafrechtlich relevanten Erfolges trifft. Eine solche Garantenpflicht, etwa die Pflicht, betriebsbezogene Straftaten von Betriebsangehörigen zu unterbinden, trifft originär jedenfalls die Mitglieder des geschäftsführenden Organs. Diese sog. „**Geschäftsherrenhaftung**“ beruht auf dem Gedanken, dass der Geschäftsleiter verantwortlich für das von ihm betriebene Unternehmen als „Gefahrenquelle“ ist und dafür Sorge zu tragen hat, dass von dieser Gefahrenquelle keine Gefahren, etwa typische betriebsbezogene Straftaten, ausgehen. Eine Garantenpflicht besteht jedoch nicht hinsichtlich betriebsuntypischer Straftaten, also allgemeiner Kriminalität von Mitarbeitern ohne Betriebsbezug wie etwa Diebstählen, Beleidigungen oder sexuellen Übergriffen.¹⁹²
- 123** Mit Urteil vom 17.7.2009 hat sich der Bundesgerichtshof im Rahmen eines obiter dictum erstmalig zur Frage der Garantenpflicht eines Compliance Officers geäußert.¹⁹³ Gegenstand des Verfahrens war die Verurteilung des Leiters der Rechtsabteilung und Revision der Berliner Stadtreinigung wegen Beihilfe zum Betrug durch Unterlassen zu einer Geldstrafe von 120 Tagessätzen, da er von überhöhten Gebührenfestsetzungen gewusst habe, ohne sie beim Vorstand zu beanstanden. Der BGH bejahte das Vorliegen einer Garantenstellung aufgrund der Stellung des Angeklagten als Leiter der Rechtsabteilung und der Innenrevision einer Anstalt des öffentlichen Rechts. Die Garantenpflicht folge aus der Überle-

¹⁹² *Knierim*, in: Wabnitz/Janovsky, Handbuch Wirtschafts- und Steuerstrafrecht, 4. Aufl. 2014, Kap. 5 Rn. 52 m. w. N.; vertiefend: *Zimmermann*, BB 2011, 634.

¹⁹³ BGH, Urf. v. 17.7.2009 – 175 StR 394/08 („BSR“), BGHSt 54, 44.

gung, dass denjenigen, dem Obhutspflichten für eine bestimmte Gefahrenquelle übertragen seien, dann auch eine „Sonderverantwortlichkeit“ für die Integrität des von ihm übernommenen Verantwortungsbereichs treffe. Maßgeblich sei die Bestimmung des Verantwortungsbereichs, den der Verpflichtete übernommen habe. Aufgabengebiet eines Compliance Officers sei die Verhinderung von Rechtsverstößen, auch von Straftaten, die aus dem Unternehmen begangen werden. Als „Kehrseite“ dieser gegenüber der Unternehmensleitung übernommenen Pflicht ergebe sich regelmäßig eine strafrechtliche Garantenpflicht im Sinne des § 13 StGB. Die Entscheidung des BGH ist bis heute ebenso umstritten wie die Frage, ob hieraus nun eine originäre, eigenständige Garantenstellung des Compliance Officers abzuleiten ist oder ob hier nur auf eine Selbstverständlichkeit hingewiesen wird, nämlich die Möglichkeit einer „sekundären Garantenpflicht“ aufgrund einer Delegation der den Geschäftsherrn treffenden Garantenpflicht auf den Compliance Officer. In der Literatur wird insoweit differenziert zwischen einerseits „öffentlich-rechtlich überlagerten Zusammenhängen“, in denen den Compliance Officer eine originäre Garantenpflicht treffe, und andererseits einer rein gewerblich-privatwirtschaftlich ausgerichteten Organisation, in der originäre Handlungspflichten nur die Geschäftsleitung selbst treffen.¹⁹⁴

In der **Praxis** kann diese Streitfrage im Regelfall jedoch dahinstehen, da hier regelmäßig originäre Aufsichts- bzw. Garantenpflichten der Geschäftsleitung im Wege der Delegation auf den Compliance Officer übertragen werden, mit der Folge, dass den Compliance Officer insoweit jedenfalls eine abgeleitete sekundäre Garantenpflicht trifft. Voraussetzung hierfür ist allerdings, dass die Geschäftsleitung überhaupt eine (entsprechende) Garantenpflicht trifft und das Organ diese Pflicht wirksam auf den Compliance Officer übertragen hat. Eine solche Delegation einer Garantenpflicht bedarf eines besonderen ausdrücklichen oder jedenfalls konkludenten Übertragungsaktes. Garant wird der Compliance Officer also nur, soweit die Unternehmensleitung ihm entsprechende Aufgaben wirksam übertragen hat. Die Reichweite der Übertragung ergibt sich insoweit nicht nur aus der vertraglichen Gestaltung und der konkreten Beschreibung des übertragenen Aufgabenbereichs, sondern auch aus der Bestimmung der Aufgaben, der Verantwortung und Kompetenz für die Durchsetzung der Regeltreue. Die Vergütung des Compliance Officers ist dagegen kein Beurteilungskriterium für die Entstehung der Garantenpflicht. Erschöpft sich die Funktion des Compliance Officers in der unternehmensinternen Kontrolle und Beratung, so verbleibt die Garantenstellung beim Leitungsorgan. Inhalt der Garanten- bzw. Handlungspflicht des Compliance Officers ist aufgrund seiner Stellung im Unternehmen im Regelfall aber „nur“ die Information der Geschäftsleitung, damit diese die sie treffenden (Geschäftsherren-)Pflichten wahrnehmen kann. Eine vollständige Delegation der Geschäftsherrenpflichten auf den Compliance Officer ist ohnehin nicht möglich, da neben den originären, nicht delegierbaren Garantenpflich-

124

¹⁹⁴ Zum Streitstand: *Knierim*, in: Wabnitz/Janovsky, Handbuch Wirtschafts- und Steuerstrafrecht, 4. Aufl. 2014, Kap. 5 Rn. 50 ff.

ten jedenfalls eine (Rest-)Überwachungspflicht beim Geschäftsherrn verbleibt.¹⁹⁵

e) Aufsichtsrat

- 125** Der Aufsichtsrat hat sowohl personell als auch organisatorisch für einen leistungsfähigen Vorstand zu sorgen und gem. § 111 Abs. 1 AktG dessen Geschäftsführung zu überwachen. Dazu gehört insbesondere auch die Kontrolle der Einrichtung und des ordnungsgemäßen Betriebs des Compliance-Management-Systems durch den Vorstand bzw. die Geschäftsführung. Ausweislich Grundsatz 16 des DCGK hat der Aufsichtsrat sicherzustellen, dass er regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen insbesondere der Strategie, der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und der Compliance informiert wird.¹⁹⁶ Neben dieser Überwachungsfunktion obliegen dem Aufsichtsrat aber in bestimmtem Umfang auch echte Geschäftsleitungspflichten. Dies ist etwa die Vertretung der Gesellschaft gegenüber den Vorstandsmitgliedern bei allen Rechtsgeschäften sowie Rechtsstreitigkeiten jeder Art (§§ 112, 87 Abs. 1, 89 Abs. 1 AktG) bspw. in Fragen der in der jüngeren Vergangenheit umstrittenen Themen der Festsetzung der Vorstandsvergütung bzw. der Prämiengewährung (§ 87 AktG) sowie die Entscheidung über die Geltendmachung von Schadensersatzansprüchen gegenüber Vorstandsmitgliedern. Darüber hinaus trifft den Aufsichtsrat die Pflicht zur Prüfung insbesondere von Jahresabschluss, Lagebericht, Konzernabschluss und Konzernlagebericht (§ 171 AktG) sowie die Pflicht zur Mitwirkung an der Feststellung des Jahresabschlusses (§ 172 AktG). Insoweit treffen Vorstand und Aufsichtsrat für die Aufstellung und Feststellung des Jahresabschlusses gemeinsame Pflichten mit dem Ergebnis, dass insoweit auch eine beiderseitige strafrechtliche Verantwortlichkeit etwa hinsichtlich des Tatbestands der unrichtigen Darstellung gem. § 331 HGB bzw. § 400 AktG in Betracht kommt. Adressat der Strafvorschriften der §§ 331 HGB, 400 AktG, der unrichtigen Darstellung der Verhältnisse der Kapitalgesellschaft, sind ausdrücklich die Mitglieder des vertretungsberechtigten Organs sowie des Aufsichtsrats einer Kapitalgesellschaft.
- 126** Aufgrund der den Aufsichtsrat kraft seiner Organstellung treffenden allgemeinen Verhaltenspflichten, namentlich Loyalitäts-, Verschwiegenheits- und Wahrheitspflichten, bestehen auch hier **originäre strafrechtliche Verantwortlichkeiten** wie etwa im Falle der Verletzung der Geheimhaltungspflicht gem. § 404 AktG.
- 127** Eine eigenständige strafrechtliche Verantwortlichkeit des Aufsichtsrates besteht auch und insbesondere, soweit der Aufsichtsrat in Ausübung seiner Geschäftsführungskompetenzen unternehmerische Entscheidungen trifft, so etwa in den

¹⁹⁵ Vertiefend: *Hastenrath*, CB 2016, 6.

¹⁹⁶ Zu den Compliance-Pflichten des Aufsichtsrates: DICO Standard „S17 – Aufsichtsrat und Compliance“.

Bereichen der Festsetzung der Vorstandsvergütung bzw. der Prämienengewährung (§ 87 AktG) sowie bei der Entscheidung über die Geltendmachung von Schadensersatzansprüchen gegenüber Vorstandsmitgliedern. In diesem Fall richten sich die Anforderungen an den Aufsichtsrat nach § 116 Satz 1 i.V.m. § 93 Abs. 1 AktG und orientieren sich mithin wie beim Vorstand an der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters. Der Bundesgerichtshof hat dies in der sog. „Mannesmann“-Entscheidung am Beispiel von Vergütungsentscheidungen unter Bezugnahme auf §§ 93 Abs. 1, 116 Satz 1 AktG ausdrücklich entschieden.¹⁹⁷ Da der Aufsichtsrat insoweit wie ein Vorstand handelt, verpflichtet der BGH ihn in diesem Sonderbereich damit auch auf das für Geschäftsleiter bei ihren Entscheidungen geltende Pflichtenprogramm. Gleiches gilt für den in der Praxis enorm relevanten Bereich der Pflicht des Aufsichtsrates zur Prüfung und Geltendmachung von Schadensersatzansprüchen gegen Vorstandsmitglieder. Bei Bestehen von dahingehenden Anhaltspunkten hat der Aufsichtsrat ein potenziell haftungsrelevantes Verhalten des Vorstands aufzuklären bzw. fachkundig aufklären zu lassen. Ergibt sich hierbei ein Schadensersatzanspruch, ist der Aufsichtsrat verpflichtet, diesen geltend zu machen, es sei denn, es stehen – ausnahmsweise – übergeordnete Gründe des Unternehmenswohls einer Geltendmachung entgegen. Das vorsätzliche Unterlassen der Geltendmachung bestehender Ansprüche kann daher eine unmittelbare strafrechtliche Haftung der Aufsichtsratsmitglieder nach sich ziehen.¹⁹⁸ Daraus resultiert für Aufsichtsräte insbesondere im Bereich der Untreue gem. § 266 StGB eine nicht unbeträchtliche Steigerung des originären strafrechtlichen Haftungsrisikos.

Umstritten ist jedoch die Frage, inwieweit dem Aufsichtsrat eine **Garantenstellung** für die Ordnungsmäßigkeit der Geschäftsführung durch den Vorstand zukommt, er also für strafrechtlich relevante (Fehl-)Entscheidungen des Vorstands zur Verantwortung gezogen werden kann. Da der Aufsichtsrat im Rahmen seiner überwachenden Tätigkeit keinen eigenen unternehmerischen Entscheidungsprozess durchführt, ist er jedenfalls grundsätzlich auch kein Garant für die Ordnungsmäßigkeit des unternehmerischen Handelns des Vorstands schlechthin und kann dies auch mangels umfassender Entscheidungs- und Beurteilungsgrundlagen nicht sein. Der Aufsichtsrat ist aber Garant für die Verhinderung von gesellschaftsschädlichen Handlungen des Vorstands, die ihm im Rahmen seiner Überwachungstätigkeit bekannt werden.¹⁹⁹ Erfährt der Aufsichtsrat – beispielsweise aus dem Bericht des Wirtschaftsprüfers über die Prüfung des Jahresabschlusses –, dass das Risikomanagement der Gesellschaft mangelhaft ist oder das Risikofrüherkennungssystem ineffektiv, so hat er bei dem Vorstand auf Abhilfe zu drängen. Verschließt sich der Aufsichtsrat diesen Erkenntnissen und bleibt er untätig, so verstößt er gegen seine Garantenpflicht, was beim Hinzutreten der weiteren Tatbestandsmerkmale, so etwa eines Schadenseintrittes, wieder-

128

197 BGH, Beschl. v. 21.12.2005, BGHSt 50, 331, 335.

198 Wegweisend hierzu die sog. „ARAG/Garmenbeck-Entscheidung“, BGHZ 135, 244.

199 Vgl. etwa BGH, NStZ 2002, 322, 324; Krause, NStZ 2011, 57.

rum den Vorwurf der Untreue gem. § 266 StGB nach sich ziehen kann.²⁰⁰ Nichts anderes gilt grundsätzlich auch für die Unterhaltung eines Compliance-Management-Systems. Wird ein solches nicht unterhalten oder besitzt das betriebene System gravierende Mängel, so ist der Aufsichtsrat zum Handeln gegenüber dem Vorstand verpflichtet. Bleibt er untätig oder unterlässt er es, die Einrichtung bzw. Verbesserung des Compliance-Management-Systems zu bewirken, und kommt es hierdurch zu einem unmittelbaren Vermögensnachteil für die Gesellschaft oder etwa auch einem Schadenseintritt, hinsichtlich dessen Abwendung eine Fahrlässigkeitsstrafbarkeit besteht, so kann auch dies eine strafrechtliche Haftung der Aufsichtsratsmitglieder auslösen.

2. Innerbetriebliche Anweisungen/Täterschaft kraft Organisationsherrschaft

- 129** Neben der unmittelbaren Täterschaft eines Mitgliedes eines Leitungsorganes eines Unternehmens, entweder weil das Organmitglied selbst gehandelt hat oder aufgrund der Zurechnung einer Kollegialentscheidung, stellt sich häufig die Frage der Zurechnung von Handlungen der Mitarbeiter am unteren Ende einer hierarchischen Struktur gegenüber dem Geschäftsherrn, der üblicherweise die strategischen und unternehmerischen Entscheidungen selbst trifft. Handelt der Mitarbeiter im Rahmen einer hierarchischen Struktur aufgrund konkreter Arbeitsanweisungen sowie standardisierter Arbeitsabläufe, so ergibt sich eine strafrechtliche Verantwortlichkeit der Unternehmensleitung grundsätzlich nur, wenn die Anweisungen bereits auf ein strafrechtlich relevantes Handeln ausgerichtet waren. In einem solchen Fall kann entweder ein mittäterschaftliches Handeln oder jedenfalls eine Anstiftung durch den Geschäftsherrn vorliegen.²⁰¹
- 130** Schwieriger ist die Annahme einer Täterschaft des Geschäftsherrn jedoch, wenn die Anweisungen zweideutig sind, etwa um gerade einen (auch strafrechtlichen) Haftungsdurchgriff in die Geschäftsleitung zu verhindern, oder wenn der unmittelbare Täter (der Mitarbeiter) in Kenntnis der strafrechtlichen Relevanz seines Tuns auch aus eigenem Interesse, etwa einem Provisionsinteresse, handelt. Hier hat die Rechtsprechung eine weitere Möglichkeit der strafrechtlichen Verantwortlichkeit der Unternehmensleitung entwickelt, die „mittelbare Täterschaft kraft Organisationsherrschaft“. War es lange Zeit so, dass hinter einem vorsätzlich handelnden Täter, etwa einem Vertriebsmitarbeiter des Unternehmens, ein „Hintermann“ lediglich wegen Anstiftung oder Beihilfe belangt werden konnte, so hat der Bundesgerichtshof im Rahmen der sog. „2. Mauerschützen-Entscheidung“ nunmehr jedoch grundlegend entschieden, dass es auch einen „Täter hinter dem Täter“ geben könne, wenn dieser Hintermann durch Organisationsstrukturen bestimmte Rahmenbedingungen mit regelhaften Abläufen ausnutze. Dies, so der BGH, habe es nicht nur bei den Grenztruppen der ehemaligen DDR gegeben, dies komme insbesondere auch bei „unternehmerischen oder geschäftsähn-

²⁰⁰ Weiterführend: Krause, NSTz 2011, 57.

²⁰¹ Vgl. hierzu ausführlich: Schmucker, StraFo 2010, 235.

lichen Organisationsstrukturen“ in Betracht.²⁰² Bei einer solchermaßen begründeten Tatherrschaft des Hintermannes, also hier des Geschäftsführers bzw. Vorstands, kommt es dann auf eine etwaige Gut- oder Bösgläubigkeit des die Tat weisungsgemäß unmittelbar Ausführenden gar nicht mehr an. Hiermit kann innerhalb einer unternehmerischen Struktur eine strafrechtliche Verantwortlichkeit der Unternehmensleitung begründet werden, ohne dass (umständlich) eine vorsätzlich rechtswidrige Handlung des unmittelbar Handelnden bewiesen werden muss. Auf Basis einer solchen Zurechnung kann eine täterschaftliche Verantwortlichkeit nicht nur bei Mitgliedern des Geschäftsführungsorganes, sondern letztlich auch bei jedem anderen Vorgesetzten begründet werden.²⁰³ Konkret auf ein Wirtschaftsunternehmen angewandt hat der Bundesgerichtshof diese Rechtsprechung erstmalig im Jahre 2003 in einem Verfahren wegen der Durchführung sog. Einlagegeschäfte, hier dem Vertrieb von Unternehmensbeteiligungen, über (hier gutgläubige) freie Handelsvertreter.²⁰⁴ Die Täterschaft der Geschäftsführer ergab sich hier aus der Leitungsmacht infolge durchgeführter Schulungen, in deren Rahmen die Geschäftsführer das Verkaufsverhalten und die Art und Weise des Umgangs mit dem Kunden vorgaben, die Handelsvertreter aber gleichzeitig im guten Glauben hielten. Anwendung gefunden hat diese Rechtsprechung unlängst auch in einem Fall des unerlaubten Erbringens von Finanzdienstleistungen.²⁰⁵

3. Fahrlässigkeitshaftung (sog. Organisationsverschulden)

Unter dem aus dem Zivilrecht stammenden Begriff des „Organisationsverschuldens“ versteht man die schuldhafte Unterlassung der Wahrnehmung der die Geschäftsleitung treffenden Organisationspflichten bzw. schuldhaft begangene Fehler bei der Organisation des Unternehmens. Da eine solche Vernachlässigung von Organisationspflichten regelmäßig nicht vorsätzlich begangen wird, führt ein solches Unterlassen im Strafrecht „lediglich“ zu einer Fahrlässigkeitshaftung der Unternehmensleitung, wenn aufgrund einer solchen Fahrlässigkeit ein zum Tatbestand eines Deliktes gehörender „Erfolg“, etwa eine Körperverletzung, ein Todesfall oder ein Umweltschaden eintritt. Zu dem relativ unbestimmten Begriff des Organisationsverschuldens haben sich zwischenzeitlich verschiedene **Fallgruppen** entwickelt, so insbesondere das Auswahlverschulden, das Anweisungsverschulden sowie das Kontroll- bzw. Überwachungsverschulden.

Da es bei den klassischen Compliance-Verstößen, etwa im Bereich der Korruption, der Untreue oder des Betruges, keine Fahrlässigkeitsstrafbarkeit gibt, ist die Begründung einer strafrechtlichen (Fahrlässigkeits-)Haftung über die Rechtsfigur des Organisationsverschuldens hier nicht möglich, eine Zurechnung

131

132

202 BGHSt 40, 218 „Mauerschützen II“, Rn. 79.

203 *Roxin*, Täterschaft und Tatherrschaft, 9. Aufl. 2015, S. 248; *Rotsch*, Criminal Compliance, § 4 Rn. 7.

204 BGHSt 48, 331.

205 BGH, Beschl. v. 27.3.2012 – 3 StR 447/11.

im Unternehmen erfolgt insoweit über die Verletzung der Aufsichtspflicht gem. § 130 OWiG.

4. Verletzung der Aufsichtspflicht in Betrieben und Unternehmen (§ 130 OWiG)

- 133 Ist weder eine unmittelbare vorsätzliche Einbeziehung noch ein strafrechtlich relevantes Organisationsverschulden, also eine Fahrlässigkeitsstrafbarkeit, der Unternehmensleitung festzustellen, so verbleibt – quasi als Auffangtatbestand – das Risiko der Ahndung einer Aufsichtspflichtverletzung durch den Ordnungswidrigkeitentatbestand des § 130 OWiG. Die Sanktionierung der Aufsichtspflichtverletzung soll sicherstellen, dass in Betrieben und Unternehmen ordnungsgemäße und hinreichende Vorkehrungen gegen die Begehung betriebsbezogener Zuwiderhandlungen getroffen werden und dafür Sorge tragen, dass sich etwa aus dem Auseinanderfallen von Entscheidungsträger und unmittelbar Handelndem im Unternehmen keine Strafbarkeitslücke ergibt.²⁰⁶
- 134 § 130 Abs. 1 Satz 1 OWiG verpflichtet den Inhaber eines Betriebs oder Unternehmens, Aufsichtsmaßnahmen zu treffen, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist. Auch wenn es sich lediglich um einen Ordnungswidrigkeitentatbestand handelt, drohen hier durchaus schwerwiegende Sanktionen. Sofern der Inhaber **vorsätzlich oder fahrlässig** die gebotenen **Aufsichtsmaßnahmen unterlässt** und damit ermöglicht, dass eine Zuwiderhandlung aus dem Unternehmen heraus begangen wird, die durch die Aufsichtsmaßnahmen verhindert oder wesentlich erschwert worden wäre, handelt er ordnungswidrig. Als erforderliche Aufsichtsmaßnahme führt § 130 Abs. 1 Satz 2 OWiG beispielhaft die Bestellung, sorgfältige Auswahl und Überwachung von Aufsichtspersonen auf. Der Betriebsinhaber muss die zumutbaren Organisationsmaßnahmen ergreifen, die zur Sicherstellung der Rechtmäßigkeit des Unternehmenshandelns erforderlich und geeignet sind. Hierzu gehören insbesondere Auswahl-, Instruktions-, Überwachungs- sowie Sanktionspflichten, um Compliance-Verstöße für die Zukunft auszuschließen.²⁰⁷ Die Norm des § 130 OWiG ermöglicht es damit, den aufsichtspflichtigen Verantwortlichen des Unternehmens (Organmitglieder, Gesellschafter sowie gem. § 9 Abs. 2 OWiG auch Betriebsleiter oder sonstige Betriebsbeauftragte) auch Handlungen von Mitarbeitern zuzurechnen, obwohl ihnen persönlich im Hinblick auf die Bezugstat kein vorsätzliches oder auch nur fahrlässiges Handeln zur Last gelegt werden kann.
- 135 Eine derartige Ordnungswidrigkeit kann, wenn die Pflichtverletzung strafbar ist, gem. § 130 Abs. 3 OWiG mit einer Geldbuße von bis zu 1 Mio. EUR sowie im Ausnahmefall über den Verweis gem. §§ 130 Abs. 3, 30 Abs. 2 Satz 3 OWiG da-

206 Beck, in: BeckOK OWiG, § 130 Rn. 4.

207 Thoma, in: Göhler, OWiG, § 130 Rn. 10.

rüber hinaus geahndet werden. Im Falle einer fahrlässigen Aufsichtspflichtverletzung ist das Höchstmaß der Geldbuße auf 500.000,00 EUR begrenzt. (§§ 130 Abs. 3, 17 Abs. 2 OWiG). Handelt es sich bei der Bezugstat dagegen lediglich um eine Ordnungswidrigkeit, ist das in dieser Vorschrift angedrohte Höchstmaß der Geldbuße maßgeblich (§ 130 Abs. 3 Satz 2 OWiG).

Die Ordnungswidrigkeit gem. § 130 OWiG ist zudem **Anknüpfungstat für die Verbands Geldbuße des § 30 OWiG**, sodass über diesen Umweg wiederum Geldbußen – gegen das Unternehmen – weit oberhalb der Millionengrenze verhängt werden können. In der Causa Siemens etwa bestand die „Anknüpfungstat“ in der Aufsichtspflichtverletzung des Vorstands i. S. v. § 130 OWiG durch die Nicht-Implementierung eines funktionierenden Compliance-Systems und führte zu der Verhängung einer Geldbuße in Höhe von insgesamt 395 Mio. EUR gegen die Siemens AG gem. §§ 30, 130, 17 IV OWiG mit Bußgeldbescheid der Staatsanwaltschaft München I vom 15.12.2008, wobei sich der Ahndungsanteil lediglich auf 250.000,00 EUR belief, der Abschöpfungsanteil jedoch auf 394.750.000,00 EUR. Aufgrund des Zusammenspiels mit § 30 OWiG wird der Tatbestand der Aufsichtspflichtverletzung gem. § 130 OWiG teilweise als *die* Compliance-Vorschrift angesehen. **136**

Der **Normadressat**, der Inhaber des Betriebs oder Unternehmens, ist die natürliche Person, der die Erfüllung der betrieblichen Pflichten obliegt. Ist „Inhaber“ des Betriebs eine juristische Person, kann § 130 OWiG gemäß § 9 Abs. 1 OWiG nur auf die „vertretungsberechtigten Organe“ als Repräsentanten der Gesellschaft angewandt werden. Die Eigenschaft als Inhaber begründet eine Garantstellung zur Abwendung betriebsbezogener Gefahren. Neben dem Inhaber oder an seiner Stelle kann Täter des § 130 OWiG aber auch sein, auf wen der Inhaber die ihn treffende Aufsichtspflicht ordnungsgemäß delegiert hat, etwa der Betriebsleiter (§ 9 Abs. 2 Satz 1 Nr. 1 OWiG) sowie speziell aufsichtspflichtige Personen, etwa Sicherheitsbeauftragte (§ 9 Abs. 2 Satz 1 Nr. 2) im Rahmen ihres Verantwortungsbereichs. **137**

Materielle Voraussetzung einer Ahndung gemäß § 130 OWiG ist zunächst das Vorliegen einer **betriebsbezogenen Zuwiderhandlung**, also die Begehung einer Straftat oder einer Ordnungswidrigkeit durch einen anderen als den Betriebsinhaber oder die verantwortlichen Gremienmitglieder (§ 9 Abs. 1 OWiG), durch die eine den Betriebsinhaber treffende Pflicht verletzt wird. Diese Zuwiderhandlung darf nur deshalb möglich geworden sein, weil der Betriebsinhaber eine ihn treffende Aufsichtspflicht verletzt hat. **138**

Eine solche **Aufsichtspflicht** kann sich dabei etwa aus dem Gesetz oder aus der Rechtsprechung zur Konkretisierung von Sorgfaltspflichten oder der Begründung von Garantstellungen (Überwachungsgarantenstellung für bestimmte Gefahrenquellen) ergeben. Der Pflichtenkreis des Betriebsinhabers ist hierbei erheblich, wenngleich Unmögliches natürlich nicht verlangt werden kann. Anerkannt sind hierbei insbesondere die Leitungs-, Koordinations-, Organisations- und Kontrollpflichten, die in einem Stufensystem ineinander greifen. Zunächst **139**

hat der Aufsichtspflichtige für eine sorgfältige Auswahl von Mitarbeitern und ggf. von Aufsichtspersonen zu sorgen (1. Stufe). Sodann ist er verpflichtet, eine sachgerechte *Organisation* und Aufgabenverteilung vorzunehmen (2. Stufe). Die Mitarbeiter sind darüber hinaus angemessen über ihre *Aufgaben* und *Pflichten zu instruieren* und *aufzuklären* (3. Stufe). Ferner bedarf es einer ausreichenden *Überwachung* und *Kontrolle* der Mitarbeiter (4. Stufe). Schließlich ist der Aufsichtspflichtige gehalten, *gegen Verstöße einzuschreiten* (5. Stufe), wozu auch eine angemessene Sanktionierung gehört.²⁰⁸ Soweit der Betriebsinhaber seine Aufsichtspflicht selbst delegiert, ist er für die Bestellung, sorgfältige Auswahl und Überwachung auch der bestellten Aufsichtspersonen verantwortlich. Mit deren Bestellung endet die eigene Überwachungspflicht allerdings nicht, sie wird lediglich auf eine (Rest-)Überwachung sowie eine stichprobenweise Kontrolle reduziert. Die im Einzelfall erforderlichen Aufsichtsmaßnahmen können jedoch nicht abstrakt festgelegt werden, sie differieren nach einer Vielzahl von Kriterien. Für den *Umfang der Aufsichtspflicht* sollen „in erster Linie Art, Größe und Organisation des Betriebs, die unterschiedlichen Überwachungsmöglichkeiten, aber auch Vielfalt und Bedeutung der zu beachtenden Vorschriften und die Anfälligkeit des Betriebs für Verstöße gegen diese Bestimmungen (maßgeblich sein), wobei insbesondere solche Fehler eine Rolle spielen können, die bereits in der Vergangenheit gemacht worden sind“.²⁰⁹

- 140** Hierher gehört insbesondere die **Compliance-Verpflichtung** des Unternehmens,²¹⁰ wobei allerdings (noch) streitig ist, ob der Betrieb eines Compliance-Management-Systems bereits eine Rechtspflicht des Unternehmens darstellt oder nur eines von mehreren geeigneten Mitteln zur Wahrnehmung der Aufsichtspflicht ist. Anders sieht es natürlich aus, wenn das Gesetz selbst (vgl. etwa §§ 25a KWG, 80 WpHG, 9, 9a GwG, 29 VAG, 52a ff. BImSchG) Vorgaben für die Einrichtung eines Compliance- oder Risikomanagements macht.²¹¹ Im Hinblick auf die allgemeine Compliance-Verpflichtung des Unternehmens wegweisend sind insoweit die Ausführungen des LG München I in der sog. „Neubürger-Entscheidung“, ausweislich derer die Einhaltung des Legalitätsprinzips und demgemäß die Einrichtung eines funktionierenden Compliance-Systems zur Gesamtverantwortung des Vorstands gehöre.²¹² Ein Vorstandsmitglied habe daher im Rahmen seiner Legalitätspflicht dafür Sorge zu tragen, dass ein Unternehmen so organisiert und beaufsichtigt wird, dass „keine Gesetzesverstöße wie Schmiergeldzahlungen an Amtsträger eines ausländischen Staates oder an aus-

²⁰⁸ Rogall, in: Karlsruher Kommentar zum OWiG, 4. Aufl. 2014, § 130 Rn. 42 m. w. N.

²⁰⁹ Vgl. BGHSt 9, 319, 322 f.; OLG Düsseldorf, wistra 1999, 115; wistra 1991, 39; OLG Zweibrücken, NSTZ-RR 1998, 311 f.; OLG Köln wistra 1994, 315; Rogall, in: Karlsruher Kommentar zum OWiG, 4. Aufl. 2014, § 130 Rn. 43.

²¹⁰ Hierzu grundsätzlich: → Schulz, Kap. 1 Rn. 27 ff.; ders./Block, CCZ 2020, 49.

²¹¹ Vgl. zum Streitstand bei § 130 OWiG: Rogall, in: Karlsruher Kommentar zum OWiG, 4. Aufl. 2014, § 130 Rn. 40.

²¹² LG München I, Urt. v. 10.12.2013 – 5 HK O 1387/10 (sog. „Neubürger-Urteil“), DB 2014, 766; vgl. hierzu auch → Schulz, Kap. 1 Rn. 39.

ländische Privatpersonen“ erfolgen. Seiner Organisationspflicht genüge ein Vorstandsmitglied bei entsprechender Gefährdungslage nur dann, wenn er eine auf Schadensprävention und Risikokontrolle angelegte Compliance-Organisation einrichte, wobei für den Umfang im Einzelnen Art, Größe und Organisation des Unternehmens, die zu beachtenden Vorschriften, die geografische Präsenz wie auch Verdachtsfälle aus der Vergangenheit zu beachten seien.²¹³ Die vom Landgericht München aufgestellten Compliance-Verpflichtungen sind jedoch heftig umstritten und können jedenfalls straf- bzw. ordnungsrechtlich nicht unmittelbar auf die Pflichtenbestimmung i. S. v. § 130 OWiG Anwendung finden.²¹⁴

Eine Darstellung, welche (Aufsichts-)Maßnahmen im Rahmen der Good Corporate Governance unterschiedlicher Unternehmen, die teilweise einem völlig anderen Regelungsregime unterliegen, erforderlich, zulässig und zumutbar und damit „**Best Practice**“ sind, würde den Rahmen dieses Beitrags jedoch sprengen, sodass insoweit auf die unterschiedlichen Kapitel dieses Handbuchs sowie weiterführend auf die Kommentarliteratur zu § 130 OWiG verwiesen werden muss.

Umstritten ist auch die Frage, ob § 130 OWiG in einem **Konzernsachverhalt** im Falle eines Fehlverhaltens der Tochtergesellschaft auch die Verhängung einer Geldbuße gegen die Konzernobergesellschaft ermöglicht. Das Bundeskartellamt bejaht diese Frage, die Rechtsprechung sieht dies allerdings durchaus differenzierter. Das OLG München hat insoweit unlängst befunden, dass eine dahingehende gesellschaftsrechtliche Aufsichtspflicht nur im Falle konkreter Weisungen der Konzernobergesellschaft angenommen werden kann.²¹⁵

V. Strafrechtliche Risiken der Non-Compliance für das Unternehmen

1. (Unternehmens-)Strafrecht

a) Überblick

Nach dem erneuten Scheitern der Schaffung eines echten Unternehmensstrafrechts²¹⁶ durch das sog. Verbandssanktionengesetz (VerSanG), das die Verhängung empfindlicher – im schlimmsten Fall existenzbedrohender – Sanktionen gegen Unternehmen selbst möglich machen sollte, bleibt es bei dem Status quo ante, der allerdings de facto bereits ein effektives „Unternehmensstrafrecht“ i. w. S. darstellt, mittels welchem über die Vorschriften der Verbandsgeldbuße

213 LG München I, Urt. v. 10.12.2013 – 5HK 0 1387/10, BB 2014, 850; vgl. auch BGH, Urt. v. 9.5.2017 – 1 StR 265/16, Rn. 118.

214 Vgl. *Kuhlen*, NZWiSt 2015, 121.

215 OLG München, BB 2015, 2004; weiterführend: *Minkoff*, Unterlassens- und Aufsichtsverantwortlichkeit im Konzern (§ 6), in: *Minkoff/Sahan/Wittig*, Konzernstrafrecht; *Werner*, CB 2016, 167.

216 Vgl. Stn. des Bundesrats v. 18.9.2020, BR-Drs. 440/20; Gesetzentwurf der BReg v. 21.10.2020, BT-Drs. 19/23568, <https://dip21.bundestag.de/dip21/btd/19/235/1923568.pdf> (zuletzt abgerufen am 26.6.2024).

aus § 30 OWiG sowie der Einziehung aus den §§ 73 ff. StGB und § 29a OWiG sowie der Nebenbeteiligung des Unternehmens im Strafverfahren, Unternehmensgeldbußen verhängt und Umsätze aus strafrechtlich bemakelten Geschäften abgeschöpft werden können.

- 144** Mit dem Entwurf des VerSanG sollten allerdings auch ganz konkrete Anreize nicht nur für die Selbstreinigung des Unternehmens durch Aufklärung, sondern auch für die Einführung von **Compliance-Maßnahmen** geschaffen werden.²¹⁷
- 145** Insbesondere wollte der Gesetzgeber mit dem VerSanG einen rechtssicheren Rahmen für **Internal Investigations**, die sog. „verbandsinternen Untersuchungen“, schaffen.²¹⁸ Nach dem Scheitern des Gesetzesvorhabens bleibt zumindest die Schaffung einer Regelung für rechtskonforme Internal Investigations auf der Tagesordnung des Gesetzgebers, absehbar ist die Verabschiedung einer neuen Regelung zum Zeitpunkt der Drucklegung des vorliegenden Handbuchs jedoch nicht.

b) Einziehung

- 146** Gerade in Wirtschaftsstrafverfahren, in denen Straftaten aus dem Unternehmen heraus und im (vermeintlichen) Unternehmensinteresse begangen worden sind, ist es Aufgabe und Ziel der Justiz, strafbare Vermögensverschiebungen zu korrigieren und die von dem oder den Tätern erlangten Vorteile zugunsten des Staates „abzuschöpfen“. Hierzu verfügt die Strafjustiz über ein schlagkräftiges Instrument, die sog. Einziehung gem. §§ 73 ff. StGB.²¹⁹ Die Einziehung ist jedoch weder „Strafe“ noch „Maßregel“, sondern eine **Maßnahme eigener Art**. Eine Vermögensabschöpfung über das Institut der Einziehung ist jedoch von Gesetzes wegen ausdrücklich ausgeschlossen, wenn bereits eine Verbandsgeldbuße verhängt worden ist (§ 30 Abs. 5 OWiG), da die Verbandsgeldbuße bereits den aus der Tat erlangten Vorteil abschöpfen soll (§§ 30 Abs. 3, 17 Abs. 4 OWiG). Seit Inkrafttreten der Neuregelung der Einziehung am 1.7.2017 stehen etwaige Ansprüche eines Verletzten, anders als bislang, der staatlichen Einziehung nicht mehr entgegen.
- 147** Hat der Beteiligte an einer rechtswidrigen Tat durch diese (oder für diese) „etwas“ **erlangt**, ordnet das Gericht gem. § 73 Abs. 1 StGB dessen Einziehung an. Ist der erlangte (Vermögens-)Gegenstand nicht mehr vorhanden, kann das Gericht gem. § 73 Abs. 3 StGB auch das einziehen, was der Täter (oder Teilnehmer) durch Veräußerung des Erlangten oder als Ersatz für dessen Zerstörung, Beschädigung oder Entziehung oder auch aufgrund eines erlangten Rechts erhalten hat, das sog. Surrogat.

²¹⁷ Weiterführend: *Schulz/Block*, CCZ 2020, 49.

²¹⁸ Zu Internal Investigations und deren Management ausführlich → *Wettner/Walter*, Kap. 8.

²¹⁹ Mit Wirkung ab dem 1.7.2017 ersetzt die Einziehung das bisherige Instrument des sog. „Verfalls“.

Hat ein anderer, also etwa das Unternehmen, für das der Täter gehandelt hat, den Vorteil aus einer rechtswidrigen Tat erhalten, so erfolgt die Einziehung gem. § 73b StGB bei dem anderen, also etwa dem Unternehmen. Die Einziehung bei anderen gem. § 73b Abs. 1 StGB erfasst die sog. Vertretungs- und Verschiebungsfälle, in denen die Bereicherung unmittelbar bei dem Vertretenen, also etwa dem Unternehmen eintritt oder in denen der Ertrag auf den Dritten „verschoben“ wurde, etwa durch ein bemakeltes Rechtsgeschäft, um die Tat zu verschleiern oder das Erlangte der Abschöpfung zu entziehen. Voraussetzung der Einziehung im Vertretungsfall, also auch beim Unternehmen, ist, dass der Täter (oder Teilnehmer) „für das Unternehmen“ oder „im Interesse des Unternehmens“ gehandelt hat, das Vorliegen einer förmlichen Beauftragung oder Organstellung des Handelnden ist aber nicht erforderlich. Auch rechtswidrige Handlungen von Angestellten, die nur faktisch oder auch nur vermeintlich im Interesse des Unternehmens erfolgen, sind dem Unternehmen zuzurechnen und führen zur Einziehung des Tatertrages beim Unternehmen. Voraussetzung der Einziehung beim Unternehmen gem. § 73b Abs. 1 Nr. 1 StGB ist darüber hinaus nicht, dass das Unternehmen etwa bösgläubig gewesen wäre, die schlichte Bereicherung reicht aus. In den Verschiebungsfällen gem. § 73b Abs. 1 Nr. 1 StGB erfasst die Einziehung auch sog. „Verschiebungsketten“, in denen der Drittbegünstigte, also auch etwa ein Unternehmen, den Tatertrag aufgrund einer ununterbrochenen Bereicherungskette erlangt hat, selbst wenn sich der Täter bei der Verschiebung eines gutgläubigen Kettenglieds bedient hat.²²⁰ Die Einziehung am Ende der Verschiebungskette ist jedoch gem. § 73b Abs. 1 S. 2 StGB ausnahmsweise ausgeschlossen, wenn das Erlangte zuvor einem gutgläubigen Dritten, der nicht erkannt hat oder hätte erkennen müssen, dass das Erlangte aus einer rechtswidrigen Tat herrührt, „entgeltlich und mit rechtlichem Grund“ übertragen wurde.²²¹

Gegenstand der Einziehung ist das „erlangte Etwas“, also die „Gesamtheit der messbaren wirtschaftlichen Vorteile, die dem Täter oder Teilnehmer durch, aus oder für die Tat zugeflossen sind“. Die Bestimmung des erlangten Etwas erfolgt in einem ersten Schritt grundsätzlich nach dem sog. **Bruttoprinzip**.²²² Durch die Tat erlangt ist damit jeder wirtschaftlich messbare Vorteil im Vermögen des Bereicherten, auch etwa ersparte Aufwendungen. Erst danach erfolgt eine wertende Konkretisierung, ob bzw. in welchem Maße etwaige Aufwendungen oder Gegenleistungen des Täters abzugsfähig sind. Gemäß § 73d Abs. 1 StGB sind bei der Bestimmung des Wertes des Erlangten die Aufwendungen des Täters, Teilnehmers oder des anderen abziehen. Außer Betracht bleibt jedoch das, was für die Begehung der Tat oder für ihre Vorbereitung aufgewendet oder ein-

220 Vgl. hierzu ausführlich: *Mahn*, Vermögensabschöpfung (§ 11), in: Minkoff/Sahan/Wittig, Konzernstrafrecht, S. 205 ff.

221 Der sog. „Erfüllungsfall“, vgl. Gesetzesbegründung, BT-Drs. 18/9525, S. 67.

222 Der Gesetzgeber hat sich insoweit der Rspr. des 1. Strafsenats des Bundesgerichtshofs (BGH, NJW 2006, 925 ff.) angeschlossen; vgl. BT-Drs. 18/9525, S. 62.

gesetzt worden ist. Der Umfang des Erlangten kann gem. § 73d Abs. 2 StGB geschätzt werden.

- 150** Bei **Korruptionsdelikten** ist die Bestimmung des erlangten Etwas aufseiten des Vorteilsgewährenden, insbesondere, wenn dieser für eine juristische Person gehandelt hat, jedoch schwierig. Hat der Täter durch eine Bestechung etwa einen **Auftrag generiert**, so waren einige Instanzgerichte in extensiver Auslegung des Bruttoprinzips zu dem Schluss gekommen, dass im Fall der Korruption der *gesamte* Werklohn für den Auftrag Gegenstand der Einziehung sei.²²³ Ein derartiges Verständnis hat der BGH jedoch zurückgewiesen: Unmittelbar aus einer Bestechung (im geschäftlichen Verkehr) erlangt ein Unternehmer bei der durch Korruption beeinflussten **Auftragsvergabe** lediglich die Auftragserteilung – also den Vertragsschluss selbst –, nicht hingegen den vereinbarten Werklohn. Das Erlangte ist mithin „lediglich“ der Gewinn aus dem Auftrag.²²⁴
- 151** Neben der selbstständigen Einziehung, wenn keine bestimmte Person wegen der Tat verurteilt werden kann (§ 76a Abs. 1 StGB), hat der Gesetzgeber mit der erweiterten selbstständigen Einziehung gem. § 76a Abs. 4 StGB ein gänzlich neues Abschöpfungsinstrument eingeführt. Gleichsam dem US-amerikanischen Institut der „non conviction based confiscation“ kann so Vermögen völlig unklarer Herkunft unabhängig vom Nachweis einer konkreten rechtswidrigen Tat eingezogen werden. Voraussetzung ist lediglich, dass der (Vermögens-)Gegenstand in einem Verfahren wegen einer in § 76a StGB benannten Katalogtat (überwiegend sog. organisierte Kriminalität) beschlagnahmt wurde und dieser aus (irgendeiner) rechtswidrigen Tat herrührt. Da der Straftatenkatalog aber auch die Delikte der Steuerhinterziehung, des Schmuggels und der Geldwäsche enthält, kann auch dieses Institut im Unternehmensbereich durchaus zur Anwendung kommen.
- 152** Um eine Vereitelung der drohenden Einziehung im Rahmen von mitunter jahrelang andauernden Strafverfahren zu verhindern, sichern die Ermittlungsbehörden regelmäßig bereits im laufenden Ermittlungsverfahren entsprechende Vermögenswerte (des Unternehmens) mittels der strafprozessualen Institute der Beschlagnahme (§§ 111b–111d StPO) sowie des Vermögensarrests (§§ 111e–111h StPO) zur Sicherung der späteren Einziehung von Wertersatz. Vollzogen werden derartige Arreste in der Regel durch die Pfändung von (Firmen-)Konten. Bereits hier zeigt sich, dass nicht nur die endgültige Einziehung, sondern auch bereits die vorläufige Pfändung von Unternehmensvermögen zu erheblichen Problemen, sei es wegen der dadurch entstehenden Außenwirkung oder aufgrund einer angespannten Liquiditätslage, führen kann, die existenzgefährdend sein und Worst Case in die Insolvenz wegen Zahlungsunfähigkeit führen können.

223 Vgl. OLG Köln, ZIP 2004, 2013; OLG Jena, wistra 2005, 114.

224 BGH, NJW 2006, 925, 929; BGHSt 47, 369; BGH, NStZ 2000, 480.

Neben der Festsetzung einer **Unternehmensgeldbuße** (§ 30 OWiG) kann eine Einziehung nicht erfolgen (§ 30 Abs. 5 OWiG). Hinsichtlich derselben Tat darf die Einziehung auch nicht etwa kumulativ angeordnet werden, wenn eine Gewinnabschöpfung durch das festgesetzte Bußgeld nicht erfolgt sein sollte.²²⁵ **153**

c) Das Unternehmen als Nebenbeteiligter im Strafverfahren

Da sich das Strafverfahren ausschließlich gegen natürliche Personen richtet, die Einziehung jedoch gemäß §§ 73 ff. StPO regelmäßig auch Unternehmenswerte betrifft, ordnet das Gericht gemäß der §§ 424 ff. StPO an, dass der Dritte (das Unternehmen) an dem Strafverfahren beteiligt wird. Im strafrechtlichen Hauptverfahren entsprechen die Befugnisse des Einziehungsbeteiligten gem. §§ 427 ff. StPO denjenigen des Angeklagten. **154**

Nach den §§ 422 ff. StPO kann die Einziehung auch im **selbstständigen Verfahren** gegen das Unternehmen betrieben werden, wenn wegen der Straftat aus tatsächlichen Gründen (etwa wenn ein Täter nicht ermittelt werden konnte oder sich dem Einfluss der deutschen Justiz entzogen hat) keine bestimmte Person verfolgt oder verurteilt werden kann, ansonsten aber die materiellen Voraussetzungen der Einziehung vorliegen. **155**

2. Ordnungswidrigkeitenrecht

Die in der Praxis größten Compliance-Risiken, jedenfalls die finanziell schmerzhaftesten (abgesehen von der Einziehung gem. § 73 StGB), finden sich de facto im Ordnungswidrigkeitenrecht. Neben der bereits angesprochenen Aufsichtspflichtverletzung gem. § 130 OWiG, die gem. § 130 Abs. 3 OWiG mit einer Geldbuße von bis zu 1 Mio. EUR sowie im Ausnahmefall darüber hinaus geahndet werden kann, ist hier in erster Linie die Verbandsgeldbuße (ugs. auch Unternehmensgeldbuße) gem. § 30 OWiG zu nennen. **156**

a) Verbandsgeldbuße gem. § 30 OWiG

Ist eine Straftat oder eine Ordnungswidrigkeit aus einem Unternehmen heraus oder im Interesse des Unternehmens begangen worden, so kann dies zur Verhängung einer Verbands- bzw. **Unternehmensgeldbuße gem. § 30 OWiG** führen. § 30 OWiG ermöglicht die Festsetzung einer Geldbuße gegen juristische Personen oder Personenvereinigungen unter der Voraussetzung, dass deren Repräsentanten (Organe, Vorstände, Vertreter oder sonstige Leitungspersonen) eine Straftat oder Ordnungswidrigkeit begangen haben, durch die entweder Pflichten des Verbandes (Unternehmens) verletzt worden sind oder die zu dessen Bereicherung geführt haben oder führen sollten. § 30 OWiG umschreibt keinen eigenen Ordnungswidrigkeitentatbestand, sondern knüpft die Folge einer Geldbuße an eine Straftat oder Ordnungswidrigkeit, die sog. **Anknüpfungstat**, des Vertreters einer juristischen Person. Die Anknüpfungstat kann nicht nur eine beliebige **157**

²²⁵ Vgl. hierzu ausführlich BGH, wistra 2007, 222, 224.

Straftat oder Ordnungswidrigkeit sein (durch die wie gesagt allerdings betriebsbezogene Pflichten verletzt wurden oder das Unternehmen bereichert wurde oder werden sollte), sondern auch eine **Aufsichtspflichtverletzung gem. § 130 OWiG**, die damit die Verhängung einer Unternehmensgeldbuße auch dann ermöglicht, wenn die (nicht verhinderte) betriebsbezogene Zuwiderhandlung unterhalb der Organ- oder Vertreterebene begangen worden ist. Die Aufsichtspflichtverletzung selbst muss allerdings der Betriebsinhaber oder ein Vertreter i. S. v. § 9 OWiG begangen haben. Betriebliche Aufsichtspflichtverletzungen können auch dann vorliegen, wenn Korruptionsstraftaten im Unternehmen nicht unterbunden bzw. verhindert werden. Das mangelnde strafrechtliche Risikomanagement, mithin ein unzureichendes Compliance Management des Unternehmens wird damit regelmäßig zu einem Problem i. S. d. §§ 30, 130 OWiG (siehe hierzu ausführlich → Rn. 133 ff.).

- 158** Die **Höhe der Geldbuße** hängt davon ab, ob als Anknüpfungstat eine Straftat oder eine Ordnungswidrigkeit vorliegt (§ 30 Abs. 2 Satz 1 Nr. 1, 2 OWiG). Bei vorsätzlichen Straftaten beträgt die Unternehmensgeldbuße bis zu 10 Mio. EUR, bei fahrlässigen Straftaten „lediglich“ bis zu 5 Mio. EUR. Bei Ordnungswidrigkeiten bestimmt sich das Höchstmaß der Geldbuße grundsätzlich nach dem für die Ordnungswidrigkeit angedrohten Höchstmaß (§ 30 Abs. 2 Satz 2 OWiG), ist also regelmäßig deutlich geringer. Zu beachten ist allerdings, dass zahlreiche Vorschriften des Nebenstrafrechts Ordnungswidrigkeitentatbestände enthalten, die mit ganz erheblichen Bußgeldrahmen ausgestattet sind. So können beispielsweise bestimmte Ordnungswidrigkeiten nach der DSGVO gem. Art. 83 Abs. 5 DSGVO mit einer Geldbuße von bis zu 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs geahndet werden. Die Bußgeldbemessung nach dem Umsatz eines Unternehmens findet zunehmend Eingang in das deutsche Recht, so sieht etwa auch das Lieferkettensorgfaltspflichtengesetz in bestimmten Fällen Geldbußen von bis zu 500.000 EUR oder bei juristischen Personen mit einem durchschnittlichen Jahresumsatz von mehr als 400 Mio. EUR Geldbußen von bis zu 2% des durchschnittlichen Jahresumsatzes vor (§ 24 Abs. 3 LkSG). Für die Bemessung der Höhe der Geldbuße im Falle einer Aufsichtspflichtverletzung i. S. v. § 130 OWiG gilt zunächst § 130 Abs. 3 Satz 1 OWiG (§ 30 Abs. 2 Satz 2 OWiG). Die Geldbuße beträgt demnach bis zu 1 Mio. EUR. Nach § 17 Abs. 2 OWiG kann fahrlässiges Handeln im Höchstmaß nur mit der Hälfte des angedrohten Höchstbetrages der Geldbuße geahndet werden, also mit 500.000,00 EUR.
- 159** § 30 Abs. 3 OWiG erklärt darüber hinaus die Regelung des § 17 Abs. 4 OWiG, die sog. **Mehrerlösabschöpfung**, für entsprechend anwendbar. Danach soll die Geldbuße den wirtschaftlichen Vorteil übersteigen, den das Unternehmen aus der Tat gezogen hat. Zu diesem Zweck darf das gesetzliche Höchstmaß der Geldbuße gem. § 17 Abs. 4 Satz 2 OWiG sogar überschritten werden. Aus diesen gesetzlichen Vorgaben folgt, dass der wirtschaftliche Vorteil, welcher dem Unter-

nehmen aus der Tat zugeflossen ist, rechnerisch die unterste Grenze der Geldbuße darstellt (sog. „**Abschöpfungsanteil**“). Der Begriff des wirtschaftlichen Vorteils bezeichnet dabei die erzielten Erlöse, aber auch mittelbare Vorteile wie Marktvorteile. Zusätzlich ist der Abschöpfungsanteil der Geldbuße um den sog. „**Ahndungsteil**“ zu erhöhen. Zumessungsgrundlage ist hierbei analog § 17 Abs. 3 OWiG die Bedeutung der Straftat, also Gewicht und Ausmaß der Pflichtverletzung, deren Häufigkeit, die Schwere des Schadens und die Auswirkungen des Verstoßes.

Bei der Höhe der Gewinnabschöpfung findet allerdings Berücksichtigung, so etwa in der Causa Siemens, wenn ausländische Behörden, wie etwa die US-amerikanische Börsenaufsicht SEC, das US-Justizministerium Department of Justice (DOJ) oder die britische Finanzaufsicht Financial Conduct Authority (FCA), wegen des gleichen Sachverhalts bereits eine vergleichbare Maßnahme durchgeführt haben oder eine solche noch zu erwarten ist. Dadurch soll ausgeschlossen werden, dass derselbe Gewinn von den beteiligten Behörden mehrfach abgeschöpft wird. Auf exemplarische Fälle der Verhängung von Verbandsgeldbußen wurde bereits in der Einleitung zu diesem Kapitel hingewiesen.

160

Da die Geldbußen gem. § 30 OWiG häufig existenzbedrohende Ausmaße annehmen, haben die betroffenen Unternehmen teilweise bewusst versucht, sich diesen Konsequenzen durch eine gesellschaftsrechtliche Umgestaltung zu entziehen oder unterlagen innerhalb der langen Dauer solcher Verfahren einschneidenden gesellschaftsrechtlichen Veränderungen. Insofern stellte sich rechtlich die Frage der **Sanktionierung des Gesamtrechtsnachfolgers** des betroffenen Unternehmens. Nach der älteren Rechtsprechung des BGH war die Bußgeldhaftung des Rechtsnachfolgers nur möglich, wenn zwischen der früheren und der neuen Gesellschaft nach wirtschaftlicher Betrachtungsweise eine sog. „Nahezu-Identität“ bestand.²²⁶ Diese Rechtsprechung führte allerdings dazu, dass Unternehmen sich einer gegen sie verhängten (Kartell-)Geldbuße entziehen konnten, indem sie eine Form der Umstrukturierung oder Veräußerung des Unternehmens wählten, die die Annahme einer „Nahezu-Identität“ im Sinne der Rechtsprechung ausschloss. Mit Urteil vom 5.3.2015 hat sich dann jedoch der EuGH gegen die Rechtsprechung des BGH gewandt und entschieden, dass die (im Rahmen einer Verschmelzung) aufnehmende Gesellschaft grundsätzlich für Rechtsverstöße der aufgenommenen Gesellschaft haftet.²²⁷ Da dies aber mit dem deutschen Schuldprinzip („nulla poena sine culpa“) nicht vereinbar erscheint, hat der BGH für Altfälle klargestellt, dass eine solche Auslegung des § 30 OWiG contra legem nicht zulässig sei.²²⁸ Für Neufälle hat der Gesetzgeber im Jahre 2013 eine ausdrückliche Regelung in § 30 Abs. 2a OWiG geschaffen,

161

226 BGH, Beschl. v. 10.8.2011 – KRB 55/10, BGHSt 57, 193; Beschl. v. 16.12.2014 – KRB 47/13.

227 EuGH, Urt. v. 5.3.2015 – C-343/13.

228 BGH, Urt. v. 10.8.2011 – KRB 55/10, BGHSt 57, 193.

nach der im Falle der Gesamtrechtsnachfolge die Geldbuße gegen den oder die Rechtsnachfolger festgesetzt werden kann.²²⁹

- 162** In der **Verfolgungspraxis** führen die erheblichen Unternehmensgeldbußen teilweise zu profiskalischen Begehrlichkeiten auch in der Straffjustiz mit der Folge, dass das eigentliche Strafverfahren gegen die persönlich Verantwortlichen nur noch mit geringem Engagement geführt wird und die Straftat (oder Ordnungswidrigkeit) letztlich nur noch als „Aufhänger“ für die beabsichtigte Unternehmensgeldbuße dient. Regelmäßig werden die Verfahren gegen die Unternehmen als Drittbeteiligte abgetrennt und vorgezogen, häufig werden die Verfahren wegen der Anknüpfungstaten dann sogar aus Gründen der „Prozessökonomie“ gem. § 153a StPO bzw. § 47 OWiG eingestellt. Die Verhängung einer Unternehmensgeldbuße, das eigentliche Ziel, bleibt in solchen Fällen im selbstständigen Verfahren gem. § 444 Abs. 3 StPO weiterhin möglich.²³⁰

b) Das Unternehmen als Nebenbeteiligter im Verfahren wegen § 30 OWiG

- 163** Ist im Strafverfahren über die Festsetzung einer Geldbuße gegen ein Unternehmen oder einen Verband i. S. v. § 30 OWiG zu entscheiden, so ordnet das Strafgericht auch hier gem. § 444 Abs. 1 StPO die Beteiligung des Unternehmens oder des Verbands an dem Verfahren an, soweit es die Tat betrifft.²³¹ Gem. § 444 Abs. 2 StPO wird das Unternehmen oder der Verband zur Hauptverhandlung geladen; bleibt der Vertreter des Unternehmens ohne genügende Entschuldigung aus, so kann ohne ihn verhandelt werden. Mit dem Ziel der Verhängung einer Unternehmensgeldbuße ist gem. § 444 Abs. 3 StPO auch die Durchführung eines selbstständigen Verfahrens zulässig. Örtlich zuständig ist in einem solchen Fall (auch) das Gericht, in dessen Bezirk das Unternehmen oder der Verband seinen Sitz oder eine Zweigniederlassung hat.

c) Einziehung (§ 29a OWiG)

- 164** Schlussendlich besteht auch im Ordnungswidrigkeitenverfahren gemäß § 29a OWiG die Möglichkeit, gegen den Täter oder auch das Unternehmen als begünstigten Dritten die Einziehung des Erlangten anzuordnen. Voraussetzung für die Anordnung ist auch hier die rechtswidrige Begehung einer mit Bußgeld bedrohten Handlung, aus der der Täter (oder ein Dritter) einen unmittelbaren Vorteil erlangt, der dann wie bei §§ 73 ff. StGB nach dem „Bruttoprinzip“ abgeschöpft werden kann. Anders als im Strafverfahren ist die Einziehung nach § 29a jedoch ausschließlich auf die Abschöpfung eines Geldbetrags gerichtet und gegen denjenigen ausgeschlossen, gegen den bereits ein Bußgeldbescheid gem. § 30 OWiG erlassen worden ist. Wird gegen den Täter ein Bußgeldverfahren nicht

229 Weiterführend zur Verbandsgeldbuße im Konzern: Böttger, Verbandsgeldbuße (§ 12), in: Minkoff/Sahan/Wittig, Konzernstrafrecht, S. 234 ff.

230 Vgl. Thoma, in: Göhler, OWiG, § 30 Rn. 39.

231 Im Falle einer Ordnungswidrigkeit gem. § 88 OWiG.

eingeleitet oder wird es eingestellt, so kann auch hier die Einziehung gem. § 29a Abs. 4 OWiG selbstständig angeordnet werden.

VI. Sonstige Risiken für das Unternehmen und seine Verantwortlichen

1. Blacklisting und Vergabesperren

a) Registereintragungen

aa) Bundeszentralregister

Rechtskräftige Strafurteile gegen natürliche Personen werden in das vom Bundesamt für Justiz geführte Zentralregister und Erziehungsregister (Bundeszentralregister) eingetragen. Da Auskünfte aus dem Bundeszentralregister auch für öffentliche Stellen jedoch nur sehr restriktiv gewährt werden, etwa für Zwecke der Strafverfolgung, beschränkt sich die Problematik hier auf den Verurteilten selbst, für den sich im Rahmen der unternehmerischen Tätigkeit allerdings die Notwendigkeit ergeben könnte, über etwaige Vorstrafen zu informieren. Öffentliche Stellen erhalten im Falle eines berechtigten Interesses eine Vollauskunft, der Betroffene selbst erhält ein sog. „Führungszeugnis“, das gem. § 32 BZRG jedoch nicht sämtliche Einträge erhält, insbesondere finden dort die Eintragung einer Geldstrafe von nicht mehr als neunzig Tagessätzen oder einer Freiheitsstrafe von nicht mehr als drei Monaten keinen Niederschlag, wenn im Register keine weitere Strafe eingetragen ist. **165**

bb) Gewerbezentralregister

Gemäß § 149 Abs. 1 GewO führt das Bundesamt für Justiz ein Gewerbezentralregister, in das u. a. Entscheidungen über betriebsbedingte Verfehlungen (Straftaten und Ordnungswidrigkeiten) eingetragen werden, wenn die Ahndung eine bestimmte Grenze überschreitet. **166**

Nach § 149 Abs. 2 Nr. 3 GewO werden in das Gewerbezentralregister **Bußgeldentscheidungen** wegen einer Ordnungswidrigkeit eingetragen, die bei oder im Zusammenhang mit der Ausübung eines Gewerbes oder dem Betrieb einer sonstigen wirtschaftlichen Unternehmung oder bei der Tätigkeit in einem Gewerbe oder einer sonstigen wirtschaftlichen Unternehmung von einem Vertreter oder Beauftragten im Sinne des § 9 des Gesetzes über Ordnungswidrigkeiten (OWiG) oder von einer Person, die in einer Rechtsvorschrift ausdrücklich als Verantwortlicher bezeichnet ist, begangen worden ist. In beiden Fällen ist Voraussetzung für die Eintragung, dass die **Geldbuße mehr als 200,00 EUR** beträgt. **167**

Gemäß § 149 Abs. 2 Nr. 4 GewO werden auch rechtskräftige strafgerichtliche Verurteilungen wegen **bestimmter Straftaten**, so nach den §§ 10 und 11 des Schwarzarbeitsbekämpfungsgesetzes, nach den §§ 15 und 15a des Arbeitnehmerüberlassungsgesetzes oder nach § 266a Abs. 1, 2 und 4 StGB, eingetragen, die bei oder im Zusammenhang mit der Ausübung eines Gewerbes oder **168**

dem Betrieb einer sonstigen wirtschaftlichen Unternehmung begangen worden sind, wenn auf **Freiheitsstrafe von mehr als drei Monaten oder Geldstrafe von mehr als 90 Tagessätzen** erkannt worden ist.

- 169** Soweit die Entscheidung eine natürliche Person betrifft, wird diese in das Register eingetragen. Betrifft die (Bußgeld-)Entscheidung eine juristische Person, etwa § 30 OWiG, so besteht ein übergeordnetes ordnungsrechtliches Interesse auch an einer Erweiterung des einzutragenden Personenkreises auf bestimmte abhängig beschäftigte Personen oder Vertretungsberechtigte des Unternehmens, mit der Folge, dass sich der einzutragende Personenkreis auch auf die in § 149 Abs. 2 Nr. 3 lit. b GewO genannten Personen erstreckt. Neben den in § 9 OWiG genannten Personen werden damit auch solche Personen eingetragen, die in einer Rechtsvorschrift ausdrücklich als Verantwortliche bezeichnet sind. Entscheidungen werden also nicht nur beim Gewerbetreibenden, sondern zusätzlich auch bei dem Vertretungsberechtigten einer juristischen Person gem. § 151 Abs. 1 Nr. 1 GewO (z.B. Geschäftsführer und Vorstandsmitglieder) sowie dem mit der Leitung eines Betriebs oder einer Zweigniederlassung Beauftragten gem. § 151 Abs. 1 Nr. 2 GewO (z.B. Prokuristen und Disponenten) im Gewerbezentralregister eingetragen.
- 170** Bei Entscheidungen gemäß 30 OWiG ist auch das **Unternehmen** in das Gewerbezentralregister einzutragen, sofern die Voraussetzungen des § 149 Abs. 2 Nr. 3 GewO gegeben sind, d.h. wenn die Grundlage für die Festsetzung des Bußgeldes die Ordnungswidrigkeit eines Vertreters/Beauftragten des Unternehmens ist, die mit mehr als 200,00 EUR geahndet wurde.
- 171** Eine derartige Eintragung ist unter **Compliance-Aspekten** insbesondere deshalb problematisch, da das Gewerbezentralregister zahlreichen Stellen Auskunft über die Einträge erteilt, so etwa gem. § 150a GewO an öffentliche Stellen zur Vorbereitung von vergaberechtlichen Entscheidungen, und derartige Eintragungen dann tatsächlich zum Vergabeausschluss, zum Entfall der benötigten „Zuverlässigkeit“ oder zum Wegfall bestimmter Vergünstigungen im Verkehr mit öffentlichen Stellen führen können.

cc) Vergabe- bzw. Wettbewerbsregister

- 172** Im Bereich der (öffentlichen) Vergabe sollen nach der Entscheidung des Gesetzgebers compliance-relevante Straftaten, insbesondere Korruptionsstraftaten, Berücksichtigung finden und ggf. sogar zu einem Vergabeausschluss führen.
- 173** Ein bundesweites Vergabe- oder Korruptionsregister hat es lange Zeit nicht gegeben. Ein erster Vorstoß des Gesetzgebers zur Errichtung eines Registers über unzuverlässige Unternehmen ist im Jahre 2002 im Bundesrat gescheitert. Weitere Versuche in den Jahren 2005 und 2009 sind jeweils an der Beendigung der Legislaturperiode vor Verabschiedung des Gesetzes gescheitert; zuletzt im Jahre 2014 hat die Justizministerkonferenz der Bundesländer die Einführung eines bundesweiten Korruptionsregisters beschlossen. Am 29.7.2017 ist dann jedoch

schließlich das **Wettbewerbsregistergesetz** (WRegG) in Kraft getreten. Registerführende Behörde ist das Bundeskartellamt.

Das Wettbewerbsregistergesetz regelt abschließend die zur Eintragung von Unternehmen im Wettbewerbsregister führenden Straftaten und Ordnungswidrigkeiten. Eingetragen werden zum einen rechtskräftige Verurteilungen, Strafbefehle oder bestandskräftige Bußgeldentscheidungen wegen der Delikte, die gemäß § 123 Abs. 1 und 4 GWB zwingend zum Ausschluss aus dem Vergabeverfahren führen (insbesondere Bestechung, Betrug, Geldwäsche, Vorenthalten von Sozialabgaben und Steuerhinterziehung). Zum anderen werden diejenigen fakultativen Ausschlussgründe nach § 124 GWB (Kartellrechtsverstöße und Verstöße gegen bestimmte arbeitsrechtliche Vorschriften) eingetragen, die die Vergabestellen bisher im Gewerbezentralregister abfragen mussten. **174**

Gemäß § 6 Abs. 1 WRegG sind öffentliche Auftraggeber i. S. v. § 99 GWB verpflichtet, vor der Erteilung des Zuschlags in einem Verfahren über die Vergabe öffentlicher Aufträge mit einem geschätzten Auftragswert ab 30.000 EUR bei der Registerbehörde abzufragen, ob im Wettbewerbsregister Eintragungen zu dem Bieter, an den der öffentliche Auftrag vergeben werden soll, vorliegen. **175**

Die Strafverfolgungsbehörden sowie die zur Verfolgung von Ordnungswidrigkeiten berufenen Behörden sind zur (elektronischen) Mitteilung von Informationen über Rechtsverstöße an die Registerbehörde verpflichtet. Unternehmen, die eingetragen werden sollen, werden im Vorfeld von der Registerbehörde angehört und können Einwendungen geltend machen. Die öffentlichen Auftraggeber sind daher zur Prüfung eines etwaigen Vergabeausschlusses nicht mehr auf die in der Mehrzahl der Bundesländer geführten sog. Vergaberegister oder (Anti-)Korruptionsregister angewiesen. **176**

In Berlin, Bremen, Hamburg Nordrhein-Westfalen sowie Schleswig-Holstein ist sind derartige Register auf Gesetzesbasis geführt worden, in anderen Bundesländern auf Erlassbasis.²³² **177**

232 **Gesetze:** **Berlin:** Gesetz zur Einrichtung und Führung eines Registers über korruptionsauffällige Unternehmen in Berlin v. 19.4.2006; **Bremen:** Bremisches Gesetz zur Errichtung und Führung eines Korruptionsregisters v. 17.5.2011, BremGbl. 2011, 365; **Hamburg:** Hamburgisches Gesetz zur Einrichtung und Führung eines Korruptionsregisters v. 18.2.2004, HmbGVBl. 2004, 98 (aufgehoben); **Nordrhein-Westfalen:** § 11 Korruptionsbekämpfungsgesetz NRW (KorrbG) v. 16.12.2004, GVBl. 2005 Nr. 1; Entfall des Vergaberegisters durch Ges. v. 7.3.2022, GV. NRW. 2022, S. 286; **Schleswig-Holstein:** Gesetz zur Einrichtung eines Registers zum Schutz fairen Wettbewerbs v. 13.11.2013, GVOBl. 2013, 405. **Erlasse:** **Baden-Württemberg:** Verwaltungsvorschrift zur Verhütung unrechtmäßiger und unlauterer Einwirkungen auf das Verwaltungshandeln und zur Verfolgung damit zusammenhängender Straftaten v. 19.12.2005; **Bayern:** Richtlinie zur Verhütung und Bekämpfung von Korruption v. 1.5.2004 (für die Bauverwaltung); **Brandenburg:** Richtlinie der Landesregierung zur Korruptionsprävention v. 25.4.2006; **Hessen:** Gemeinsamer Runderlass zum Ausschluss von Bewerbern und Bietern wegen schwerer Verfehlungen, die ihre Zuverlässigkeit infrage stellen v. 13.12.2010; **Mecklenburg-Vorpommern:** Verwaltungsvorschrift zur Bekämpfung von Korruption in der Landesverwaltung v. 11.12.2001; **Rheinland-Pfalz:**

- 178 In das **nordrhein-westfälische Vergaberegister**, das ausdrücklich nicht nur der Vorbereitung und Prüfung von Vergabeentscheidungen öffentlicher Stellen, sondern auch der „Unterstützung von Strafverfolgungsbehörden“ zu dienen bestimmt war, wurden mithin auch Straftaten nach den §§ 331 bis 335, 299 (Bestechung/Bestechlichkeit), 108e StGB (Abgeordnetenbestechung), aber auch nach §§ 261 (Geldwäsche, Verschleierung illegalen Vermögens), 263 (Betrug), 264 (Subventionsbetrug), 265b (Kreditbetrug), 266 (Untreue), 266a (Vorenthalten/Veruntreuen von Arbeitsentgelt), 298 StGB (illegale Absprachen bei Ausschreibungen) sowie nach § 370 AO (Steuerhinterziehung) eingetragen, soweit diese „im Rahmen einer unternehmerischen Betätigung“ begangen worden sind (§ 5 Abs. 1 KorrbG NRW). Einzutragen waren nicht nur **rechtskräftige Verurteilungen**, sondern auch bereits die **Zulassung der Anklage** sowie die **Einstellung des Strafverfahrens gem. § 153a StPO** (§ 5 Abs. 2 Nr. 4 KorrbG NRW).

dd) Sonstige Register

- 179 Neben den deutschen (Antikorruptions-)Registern existieren weitere internationale personenbezogene Antikorruptions- bzw. Sanktionsregister der EU, der UN, der USA, der Weltbank sowie der OECD, die insbesondere der Terrorbekämpfung, aber auch der Unterbindung finanzieller Transaktionen unter Geldwäsche- und Antikorruptionsaspekten dienen sollen. Dies sind etwa:
- Konsolidierte Liste des Sicherheitsrats der Vereinten Nationen, basierend auf der UN-Resolution 1267/1999 vom 15.10.1999 betreffend Al-Qaida und Taliban;
 - Liste der EU, basierend auf der Verordnung (EG) Nr. 2580/2001, mit dem Ziel der Bekämpfung aller Formen der Finanzierung wirtschaftlicher Aktivitäten des internationalen Terrorismus;²³³
 - „Consolidated list of financial sanctions targets“ des Finanzministeriums des Vereinigten Königreichs Großbritannien und Nordirland (Investment Ban);
 - „US Denied Persons List“ (US-DPL) des US Department of Commerce, Bureau of Industry & Security (BIS) betreffend Personen, denen durch das BIS befristet oder unbefristet die Exportprivilegien entzogen worden sind und die mit einer Handelssperre versehen wurden;
 - „World Bank Listing of Ineligible Firms“ (Debarred Firms & Individuals) betreffend Personen und Firmen, die von der Weltbank als betrügerisch oder korrupt eingestuft werden.

Verwaltungsvorschrift zur Bekämpfung der Korruption in der öffentlichen Verwaltung v. 29.4.2003; **Sachsen**: Verwaltungsvorschrift der Sächsischen Staatsregierung zur Korruptionsvorbeugung in der staatlichen Verwaltung des Freistaates Sachsen v. 21.5.2002; **Sachsen-Anhalt**: Verwaltungsvorschrift zur Vermeidung und Bekämpfung der Korruption v. 28.4.2008.

- 233 Verordnung (EG) Nr. 2580/2001 des Rates vom 27. Dezember 2001 über spezifische, gegen bestimmte Personen und Organisationen gerichtete restriktive Maßnahmen zur Bekämpfung des Terrorismus, zuletzt geändert durch die Verordnung (EU) 2024/669 des Rates vom 19. Februar 2024.

b) Vergaberechtliche Konsequenzen

Bei der Vergabe von (öffentlichen) Aufträgen soll auch die Verwirklichung betriebsbezogener Straftaten, mithin insbesondere compliance-relevanter Straftaten, nach dem Willen des Gesetzgebers Berücksichtigung finden. Bei **öffentlichen Ausschreibungen** konnten Unternehmer bereits nach altem Recht, etwa gem. § 8 Nr. 5 Abs. 1 lit. c VOB/A,²³⁴ von der Teilnahme am Wettbewerb ausgeschlossen werden, wenn diese nachweislich eine schwere Verfehlung begangen haben, die ihre Zuverlässigkeit als Bewerber infrage stellt. Neben Verstößen gegen das GWB sind dies natürlich insbesondere **Korruptionsstraftaten**.²³⁵ **180**

Mit der Vergaberechtsreform 2016, die am 18.4.2016 in Kraft getreten ist, hat der Gesetzgeber drei EU-Richtlinien über die Vergabe von öffentlichen Aufträgen und Konzessionen umgesetzt und damit den Rechtsrahmen für die Vergabe öffentlicher Aufträge völlig neu geordnet.²³⁶ Konkrete Vorgaben für Vergabeausschlüsse finden sich nunmehr unmittelbar im Gesetz gegen Wettbewerbsbeschränkungen (GWB). Nach § 122 Abs. 1 GWB werden öffentliche Aufträge (nur) an fachkundige und leistungsfähige (geeignete) Unternehmen vergeben, bezüglich derer keine zwingenden (§ 123 GWB) oder fakultativen Ausschlussgründe (§ 124 GWB) vorliegen. **181**

Ein solcher zwingender **Ausschlussgrund** liegt gem. § 123 GWB aber vor, wenn eine Person, deren Verhalten dem Unternehmen „zurechnen“ ist, wegen bestimmter Straftaten rechtskräftig verurteilt oder dieserhalb gegen das Unternehmen eine Geldbuße nach § 30 OWiG rechtskräftig festgesetzt worden ist. Ausweislich des Kataloges des § 123 Abs. 1 und 4 GWB handelt es sich in erster Linie um schwere Straftaten wie etwa die Bildung krimineller oder terroristischer Vereinigungen, aber auch um compliance-relevante Delikte wie etwa: **182**

- § 263 StGB (Betrug), soweit sich die Straftat gegen den Haushalt der Europäischen Union oder gegen Haushalte richtet, die von der Europäischen Union oder in ihrem Auftrag verwaltet werden;
- § 264 StGB (Subventionsbetrug), soweit sich die Straftat gegen den Haushalt der Europäischen Union oder gegen Haushalte richtet, die von der Europäischen Union oder in ihrem Auftrag verwaltet werden;
- § 266a StGB (Vorenthalten und Veruntreuen von Arbeitsentgelt);
- § 299 StGB (Bestechlichkeit und Bestechung im geschäftlichen Verkehr);
- § 108e StGB (Bestechlichkeit und Bestechung von Mandatsträgern);
- §§ 333 und 334 StGB (Vorteilsgewährung und Bestechung), jeweils auch in Verbindung mit § 335a StGB (Ausländische und internationale Bedienstete);
- Art. 2 § 2 IntBestG (Bestechung ausländischer Abgeordneter im Zusammenhang mit internationalem Geschäftsverkehr);
- § 370 AO (Steuerhinterziehung).

²³⁴ Inhaltsgleich § 7 Abs. 5 lit. c VOL/A.

²³⁵ Vgl. LG Frankfurt am Main, IBR 2004, 530; *Greeve/Dörr*, in: Volk, MAH Wirtschafts- und Steuerstrafsachen, 2. Aufl. 2014, § 20 Rn. 381.

²³⁶ Gesetz zur Modernisierung des Vergaberechts v. 17.2.2016, BGBl. I 2016, S. 203.

- 183 Die **Zurechnung** des Verhaltens einer natürlichen Person, also etwa eines Mitarbeiters des Unternehmens, ist in § 123 Abs. 3 GWB ausdrücklich normiert. Das Verhalten einer rechtskräftig verurteilten Person ist einem Unternehmen danach zuzurechnen, wenn diese Person als für die Leitung des Unternehmens Verantwortlicher gehandelt hat, wozu auch die Überwachung der Geschäftsführung oder die sonstige Ausübung von Kontrollbefugnissen in leitender Stellung gehört.
- 184 Der Nachweis wiederum, dass die in § 123 GWB genannten Ausschlussgründe bei dem Bewerber oder Bieter (nicht) vorliegen, erfolgt gemäß § 48 Abs. 4 der Vergabeverordnung (VgV) über Auszüge aus den einschlägigen **Registern** (s. o.), insbesondere ein Führungszeugnis aus dem Bundeszentralregister oder, in Ermangelung eines solchen, eine gleichwertige Bescheinigung einer zuständigen Gerichts- oder Verwaltungsbehörde des Herkunftslands oder des Niederlassungsstaats des Bewerbers oder Bieters, oder neuerdings auch die sog. Einheitliche Europäische Eigenerklärung (EEE) gem. § 50 VgV.²³⁷
- 185 Ein Unternehmen, bei dem ein zwingender oder ein fakultativer Ausschlussgrund vorliegt, kann den Ausschluss durch geeignete Gegenmaßnahmen jedoch verhindern. Eine derartige „**Selbstreinigung**“ i. S. v. § 125 GWB stellt z. B. die Leistung von Ausgleichszahlungen für durch das Fehlverhalten entstandene Schäden, aber auch die aktive Zusammenarbeit mit Ermittlungsbehörden und dem Auftraggeber zur Aufklärung des Fehlverhaltens dar. Darüber hinaus kann ein Unternehmen einen Vergabeausschluss gem. § 125 Abs. 1 Nr. 3 GWB vermeiden, wenn es „konkrete technische, organisatorische und personelle Maßnahmen ergriffen hat, die geeignet sind, weitere Straftaten oder weiteres Fehlverhalten zu vermeiden“, spricht ein geeignetes **Compliance-Management-System** eingeführt hat. Die von dem Unternehmen ergriffenen Selbstreinigungsmaßnahmen werden von dem öffentlichen Auftraggeber bewertet, wobei auch die Schwere und die besonderen Umstände der Straftat oder des Fehlverhaltens Berücksichtigung finden.

2. Inhabilität (§§ 70 StGB, 6 GmbHG, 76 AktG)

- 186 Ein Compliance-Risiko in erster Linie für das Organmitglied selbst, aber auch für das Unternehmen, stellt die aus einer Verurteilung folgende rechtliche Unfähigkeit dar, weiter Geschäftsführer oder Vorstand zu sein, die sog. Inhabilität.
- 187 Ist der Täter etwa einer Korruptionsstraftat verurteilt worden und hat er diese unter Missbrauch seines Berufs oder Gewerbes oder unter grober Verletzung der mit ihnen verbundenen Pflichten begangen, so kann das Gericht gem. **§ 70 Abs. 1 StGB** ein **Berufsverbot** von einem bis zu 5 Jahren Dauer verhängen.

237 Vgl. Durchführungsverordnung (EU) 2016/7 der Kommission vom 5.1.2016 zur Einführung des Standardformulars für die Einheitliche Europäische Eigenerklärung, ABl. EU Nr. L 3 v. 6.1.2016, 16.

Voraussetzung hierfür ist, dass eine Gesamtwürdigung des Täters und der Tat die Gefahr erkennen lässt, dass er bei weiterer Ausübung des Berufs oder Gewerbes weitere erhebliche rechtswidrige Taten der bezeichneten Art begehen wird, mithin eine Wiederholungsgefahr vorliegt. In Ausnahmefällen kann das Berufsverbot für immer angeordnet werden (§ 70 Abs. 1 Satz 2 StGB). Bei dem Berufsverbot gem. § 70 StGB handelt es sich jedoch um eine Ermessensvorschrift, die in der Praxis relativ selten zur Anwendung kommt.

Deutlich praxisrelevanter sind insoweit die Vorschriften der **§§ 6 GmbHG** sowie **188 76 AktG**, die die Inhabilität der betroffenen Organmitglieder kraft Gesetzes anordnen. Gemäß § 6 Abs. 2 Satz 2 Nr. 3 GmbHG kann Geschäftsführer nicht sein, wer wegen der Begehung bestimmter vorsätzlich begangener Straftaten (rechtskräftig) verurteilt worden ist. Bei den abschließend normierten Delikten, die diese Konsequenz nach sich ziehen, handelt es sich (allerdings nur) um die folgenden Straftaten:

- Insolvenzverschleppung gem. § 15a Abs. 4 InsO;
- Insolvenzstraftaten nach den §§ 283 bis 283d StGB;
- falsche Angaben gem. § 82 GmbH oder § 399 AktG;
- unrichtige Darstellung gem. § 400 AktG, § 331 HGB, § 313 UmwG oder § 17 PublG;
- Straftaten nach den §§ 263 bis 264a oder den §§ 265b bis 266a StGB, also auch Betrug sowie Untreue, soweit auf eine Freiheitsstrafe von mindestens einem Jahr erkannt wurde.

Auch wer nicht als Täter, sondern nur als Teilnehmer einer vorsätzlich begangenen Straftat nach § 6 Abs. 2 Satz 2 Nr. 3 GmbHG rechtskräftig verurteilt worden ist, kann nicht (mehr) Geschäftsführer einer GmbH sein.²³⁸ **189**

Gemäß § 6 Abs. 2 Satz 3 GmbHG gilt dies entsprechend bei einer Verurteilung im Ausland wegen einer Tat, die den oben genannten Taten „vergleichbar“ ist. **190**

Die Inhabilität des Geschäftsführers beginnt unmittelbar mit Rechtskraft des Urteils und gilt für die Dauer von fünf Jahren seit der Rechtskraft des Urteils. Die Dauer einer etwaigen Inhaftierung ist hierbei nicht (!) anzurechnen, die Frist beginnt also erst mit der Entlassung des Betroffenen. Zu beachten ist, dass die Inhabilität kraft Gesetzes **sofort** eintritt, also auch bereits laufende Geschäftsführungsverhältnisse betrifft, und nicht etwa erst im Falle einer neuen Bestellung greift. **191**

Für die Aktiengesellschaft ist die Inhabilität des Vorstands entsprechend in § 76 Abs. 3 AktG geregelt. Gem. § 76 Abs. 3 Satz 2 Nr. 3 AktG kann, wer eine der o.g. Straftaten vorsätzlich begangen hat, auch nicht (mehr) Mitglied des Vorstands sein. **192**

²³⁸ BGH, Beschl. v. 3.12.2019 – II ZB 18/19.

3. Aufsichtsrechtliche Konsequenzen

- 193** Eine sowohl das Unternehmen als auch die Organmitglieder treffende Konsequenz aus strafrechtlichen Verfehlungen kann auch die Verhängung aufsichtsrechtlicher Maßnahmen durch die zuständigen Aufsichtsbehörden sein. Unangenehme persönliche Nebenfolgen einer strafrechtlichen Verurteilung sind nicht nur etwa die Entziehung der Fahrerlaubnis, des Waffenscheins oder der Wegfall einer Fluglizenz, sondern insbesondere der Entfall der erforderlichen beruflichen Zuverlässigkeit als Geschäftsleiter eines Unternehmens.
- 194** Von besonderer Relevanz sind insoweit etwa die Maßnahmen, die die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zur Gefahrenabwehr durchführen kann. Erweist sich etwa der Geschäftsleiter eines Kreditinstituts, eines Finanzdienstleisters oder einer Versicherung aufgrund einer strafrechtlichen Ahndung als nicht hinreichend persönlich zuverlässig, so kann die BaFin gegenüber dem Aufsichtsorgan verlangen, dass dieser Geschäftsleiter abberufen und ersetzt wird. Die BaFin kann auch Mitglieder von Aufsichtsorganen, die nicht über die notwendige Zuverlässigkeit verfügen, abberufen und Befugnisse eines Aufsichtsorgans auf einen Sonderbeauftragten übertragen. Eine solche Beeinträchtigung der erforderlichen persönlichen Zuverlässigkeit ergibt sich häufig aus strafgerichtlichen Verurteilungen aufgrund betriebsbedingter Straftaten und kann im Einzelfall sogar bereits im Falle einer Einstellung eines Strafverfahrens gem. § 153a StPO angenommen werden.
- 195** In einer Vielzahl von Fällen sind es jedoch auch die Unternehmen selbst, die im Falle ihrer Zertifizierung nach unterschiedlichen Vorschriften Vorteile im Geschäftsverkehr in Anspruch nehmen. So existieren etwa im Außenwirtschaftsrecht Vereinfachungen, sog. allgemeine Genehmigungen, für zertifizierte Empfänger, die insbesondere die Zuverlässigkeit des Empfängerunternehmens voraussetzen. Auch etwa der Status des Zugelassenen Wirtschaftsbeteiligten (AEO – Authorised Economic Operator) bringt zollrechtlich erhebliche Vereinfachungen mit sich.²³⁹ Der Vorteil des Unternehmens liegt somit in dem erleichterten Erhalt von Gütern. Vergleichbare Regelungen gibt es in zahlreichen anderen Bereichen auch, so etwa dem Arzneimittelrecht oder auch dem Luftsicherheitsrecht. Darüber hinaus haben die Aufsichtsbehörden im Wirtschaftsverwaltungsrecht im Zusammenhang mit strafrechtlichen Verurteilungen ein weitgehendes Instrumentarium, das im Einzelfall sogar eine Betriebsschließung ermöglicht (§ 20 BImSchG, § 35 GewO, §§ 35 ff. KWG, §§ 61 f. GmbHG, § 396 AktG).

VII. Strafrechtliche Risiken innerhalb des Compliance-Prozesses („Failed Compliance“)

- 196** Auch der Compliance-Prozess als solcher enthält nicht unerhebliche Compliance-Risiken für das Unternehmen und seine Verantwortlichen. Da sich der Geschäftsherr bei der Aufklärung mutmaßlicher Compliance-Verstöße durch in-

²³⁹ Vgl. Art. 73, 95 ff. UZK.

terne Ermittlungen regelmäßig auf der Seite des Rechts wähnt, wird das Risiko, auch im Rahmen des Aufklärungsprozesses strafrechtlich relevante Fehler zu begehen, entweder ausgeblendet oder jedenfalls gering geschätzt. Die im Rahmen der Durchführung interner Ermittlungen begangenen Verstöße, die sog. „**Failed Compliance**“, sind jedoch aufgrund des verfolgten „guten Zwecks“ keinesfalls pauschal gerechtfertigt und werden auch von den Ermittlungsbehörden regelmäßig verfolgt. Tatsächlich besteht hier sogar ein relativ großes Entdeckungsrisiko, da die „Opfer“ derartiger Compliance-Verstöße, etwa der gekündigte Mitarbeiter oder auch der übergangene Betriebsrat aus Gründen der Prävention regelmäßig ein großes Aufklärungsinteresse besitzen und die Verfahren nachhaltig betreiben.²⁴⁰

Bereits bei einer der Standardmaßnahmen interner Ermittlungen, einer Auswertung des elektronischen Datenbestands (sog. „**eSearch**“), können etwa die Straftatbestände des Ausspähens von Daten gemäß § 202a Abs. 1 StGB, der Verletzung des Post- oder Fernmeldegeheimnisses gemäß § 206 Abs. 1 StGB sowie auch und insbesondere der unbefugten Datenverarbeitung gemäß Art. 83 DSGVO i. V. m. § 42 Abs. 2 BDSG verwirklicht werden. Entscheidend ist hierbei die Ausgangsfrage, ob die auszuwertenden elektronischen Daten, etwa der E-Mail-Account des verdächtigen Mitarbeiters, Daten des Unternehmens oder (auch) Daten des Mitarbeiters sind. Nach einer weitverbreiteten Auffassung ist der Arbeitgeber, der seinen Organmitgliedern und Mitarbeitern auch nur die maßvolle private Nutzung der IT-Infrastruktur sowie der Kommunikationsmedien des Unternehmens gestattet oder sie auch nur duldet, als Telekommunikationsanbieter im Sinne des Telekommunikationsgesetzes (TKG) zu qualifizieren und unterliegt damit dem Fernmeldegeheimnis gemäß § 3 Abs. 3 Telekommunikations-Digitale-Dienste-Datenschutz-Gesetz (TDDDG).²⁴¹ Nach § 2 Abs. 2 Nr. 1 TDDDG ist „Anbieter von digitalen Diensten“ jede natürliche oder juristische Person, die eigene oder fremde digitale Dienste erbringt, an der Erbringung mitwirkt oder den Zugang zur Nutzung von eigenen oder fremden digitalen Diensten vermittelt zwar auch dann, wenn das Unternehmen seine Telekommunikationseinrichtungen den Mitarbeitern auch für private und wirtschaftliche Zwecke zur Verfügung stellt. Damit wiederum ist dann der Anwendungsbereich des Straftatbestands des § 206 StGB, der Verletzung des Post- oder Fernmeldegeheimnisses, eröffnet.²⁴²

Die Problematik besteht dann darin, dass eine Rechtfertigung insoweit lediglich aus dem Normengeflecht des TDDDG erfolgen kann, so etwa gemäß § 100 Abs. 1 TKG, wenn der Eingriff zur Beseitigung von Störungen erforderlich ist,

197

198

240 Hierzu ausführlich: Böttger/Kraft, in: Böttger, Wirtschaftsstrafrecht, Kap. 21 – Failed Compliance.

241 Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz – TDDDG) v. 23.6.2021 (BGBl. I, S. 1982; 2022 I, S. 1045); bis 2021: § 88 TKG.

242 OLG Karlsruhe, Beschl. v. 10.1.2005 – 1 Ws 152/07, MMR 2005, 178.

oder gemäß § 12 Abs. 4 TDDDG im Falle des Vorliegens von Anhaltspunkten für eine rechtswidrige Inanspruchnahme eines Telekommunikationsdienstes, etwa im Fall der Leistungerschleichung. Dies ist jedoch im Falle interner Ermittlungen regelmäßig nicht der Fall.

- 199** Die zwischenzeitlich herrschende Auffassung sieht jedoch den Schutzbereich des TDDDG (bzw. des TKG) im Unternehmenskontext als erst gar nicht eröffnet an. Da das TDDDG (ebenso wie bislang § 88 TKG) nur die dynamische Übertragung und nicht etwa (auf dem Unternehmensserver) ruhende Mails erfasse und der Arbeitnehmer auch kein Dritter im Sinne des TDDDG sei, sei der Zugriff auf Arbeitsplatzrechner und/oder E-Mails des Mitarbeiters nicht am Fernmeldegeheimnis, sondern nur an der DSGVO bzw. dem Bundesdatenschutzgesetz zu messen mit der Folge, dass sich eine etwaige Strafbarkeit allenfalls aus § 42 BDSG ergebe.²⁴³
- 200** Da die Auswertung elektronischer Daten im Rahmen eines eSearchs auch eine Datenverarbeitung im Sinne von Art. 5 DSGVO ist, besteht jedoch das Risiko einer Ordnungswidrigkeit bzw. einer **Strafbarkeit gemäß §§ 41 ff. BDSG i.V.m. Art. 83 DSGVO**. Ordnungswidrig handelt insoweit, wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet. Wird eine derartige Handlung dazu „gegen Entgelt“ oder „in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen“, begangen, so stellt dieser Verstoß zudem auch noch eine Straftat dar. Da nur eine *unbefugte* Datenerhebung bzw. -verarbeitung (straf-) rechtlich relevant ist, unterliegt eine derartige Compliance-Maßnahme dem Erfordernis einer Rechtfertigung aus dem Datenschutzrecht. Eine solche Rechtfertigung kann im Einzelfall in einer konkreten Einwilligung im Sinne von Art. 7 DSGVO oder etwa aufgrund einer abgeschlossenen Betriebsvereinbarung bestehen, die Voraussetzungen dieser beiden Einwilligungstatbestände sind jedoch komplex.²⁴⁴ Regelmäßig wird eine Rechtfertigung aus § 26 Abs. 1 S. 1 BDSG bzw. bei der Aufdeckung von Straftaten gemeinsam mit § 26 Abs. 1 S. 2 BDSG erforderlich sein. Die Erfüllung der Anforderungen des § 26 BDSG sind jedoch nicht unerheblich und müssen im Detail geprüft und dokumentiert werden. Probleme entstehen in der Praxis regelmäßig bei der gleichzeitigen Auswertung der Daten nicht verdächtiger Mitarbeiter, bei der nicht hinreichenden Dokumentation des erforderlichen Anfangsverdachts, im Falle der Nichteinhaltung des Mitbestimmungsrechts des Betriebsrates oder auch der Nichtberücksichtigung des Verhältnismäßigkeitsprinzips. Eine konkretere Darstellung würde den Rahmen dieses Kapitels jedoch sprengen, sodass auf die Ausführungen im Kapitel 11 (Datenschutz) verwiesen werden muss.
- 201** Das Risiko einer Strafbarkeit wegen des **Ausspähens von Daten gemäß § 202a Abs. 1 StGB** durch interne Ermittlungen ist regelmäßig gering, da der Tatbe-

243 LAG Berlin-Brandenburg, CB 2016, 175; NZA-RR 2011, 342; LAG Niedersachsen, NZA-RR 2010, 406; VGH Kassel, NJW 2009, 2470.

244 Vgl. hierzu ausführlich: Zoch, in: Böttger, Wirtschaftsstrafrecht, Kap. 17 – Datenschutzstrafrecht, S. 1283 ff.

stand des § 202a Abs. 1 StGB lediglich das Ausspähen von Daten umfasst, die besonders gesichert sind, etwa durch einen Kennwortschutz, wofür die Vergabe eines allgemeinen dienstlichen Nutzerpassworts nicht ausreichend ist.²⁴⁵ Der Tatbestand des § 202a Abs. 1 StGB erfasst in erster Linie das sog. „Hacking“ unter Einsatz von Trojanern oder vergleichbaren Programmen. Werden ausschließlich dienstliche E-Mails „gehackt“, scheidet eine Strafbarkeit gemäß § 202a Abs. 1 StGB bereits deswegen aus, weil derartige E-Mails alleine dem Arbeitgeber zuzuordnen sind.²⁴⁶

Auch bei der **Durchführung von Compliance-Interviews** bestehen strafrechtliche Risiken. Einerseits ist das Beschaffen von Daten auch auf diesem Wege eine Datenerhebung im Sinne von Art. 5 DSGVO mit der Folge, dass auch hier das Risiko eines Verstoßes gegen die §§ 40 ff. BDSG (s.o.) besteht. Andererseits werden in der Praxis im Rahmen der Durchführung von Compliance-Interviews häufig Handlungen vorgenommen, die rechtlich lediglich einem Amtsträger zustehen, etwa die Erteilung einer Belehrung im Sinne von § 136 StPO, die Durchsuchung des Befragten während des Interviews oder die Beschlagnahme mitgebrachter (privater) Gegenstände. Auch wenn der Ermittler sich hierbei nicht als Amtsträger geriert, was allerdings im Falle einer sog. Mock Dawn Raid durchaus vorkommen soll, kann hier der Tatbestand der **Amtsanmaßung gemäß § 132 Var. 2 StGB**, die sog. „Amtshandlungsanmaßung“, erfüllt sein. Nach der Rechtsprechung muss eine derartige Handlung nicht einmal alle Voraussetzungen einer rechtmäßigen Amtshandlung erfüllen, es komme nur darauf an, ob die Handlung einem objektiven Beobachter als hoheitliches Handeln erscheine.²⁴⁷

Auch die Ermittlung und Speicherung privater telefonischer Verbindungsdaten oder gar die Durchführung konkreter **Abhörmaßnahmen** ist in der Compliance-Praxis bereits beobachtet worden. Das insoweit unbefugte Verarbeiten von personenbezogenen (Verbindungs-)Daten verstößt bereits gegen die DSGVO; wird ein solcher Verstoß etwa von einem Dienstleister entgeltlich begangen, so ist auch der Straftatbestand des § 42 BDSG erfüllt. Dass derartige Maßnahmen ebenfalls die Straftatbestände des § 206 StGB sowie der **Verletzung der Vertraulichkeit des Wortes gemäß § 201 Abs. 1 StGB** erfüllen, liegt insoweit auf der Hand.²⁴⁸ Wendet der Geschäftsherr für derartige – strafrechtlich relevante – Maßnahmen dann auch noch Mittel des Unternehmens auf, bezahlt er also mitunter sechsstellige Beträge an externe Dienstleister für eine derartige „Aufklärung“, so besteht darüber hinaus auch noch das Risiko der **Untreue gemäß § 266 Abs. 1 StGB** durch die Bezahlung derart rechtswidriger Ermittlungsmaßnahmen aus dem Unternehmensvermögen.²⁴⁹

245 LAG Köln, NZA-RR 2004, 527.

246 LAG Berlin-Brandenburg, NZA-RR 2011, 342.

247 BGHSt 40, 8; KG, NStZ-RR 2013, 72.

248 BGH, NStZ 2013, 165.

249 BGH, Urt. v. 10.10.2012 – 2 StR 591/11 („DTAG“), NStZ 2013, 165.

3. Kapitel

Compliance Management als Schnittstellenaufgabe – Überlegungen und Empfehlungen zur erfolgreichen Zusammenarbeit mit anderen Unternehmensfunktionen

I. Einleitung

Unter den Unternehmensfunktionen galt Compliance¹ lange als eine Art Nachkömmling. Alle auf Gewinnerzielung angelegten und im Wettbewerb tätigen Unternehmen verfügen, ungeachtet ihrer Größe, schon immer zumindest über eine Unternehmensleitung und eine Finanzfunktion. Letztere hat ein mindestens in Grundzügen organisiertes Rechnungs- und Berichtswesen und ein Controlling. Seit längerem unverzichtbar ist eine IT-Abteilung. Ab einer bestimmten Unternehmensgröße und in Abhängigkeit vom Geschäftsmodell findet man auch weitere organisatorische Untergliederungen, etwa für den Einkauf, die Produktion, den Vertrieb und das Marketing. Hinzu gesellen sich dann typischerweise eine Personalabteilung, eine Rechtsabteilung, eine Innenrevision und manchmal auch eine eigene Unternehmenskommunikation.² Oft haben sich die Mitarbeiter organisiert und einen oder mehrere Betriebsräte gebildet. Größere Unternehmen haben oft einen Beirat oder einen gesetzlich zu bildenden Aufsichts- oder Verwaltungsrat, der seinerseits mitbestimmt sein kann.

All diese angestammten unternehmensinternen „Stakeholder“ haben in den vergangenen Jahren den Aufstieg der Compliance als neuer Unternehmensfunktion miterlebt. Eine nicht abreißende Kette von medienintensiven Skandalen, behördlichen Untersuchungen, empfindlichen Sanktionen und Karrierebrüchen und die sich daraus ergebenden organisatorischen, prozessualen und personellen Konse-

1 Wenn hier von Compliance die Rede ist, ist damit Zweierlei gemeint: Zum einen das Einhalten externer und unternehmensinterner Gesetze, Richtlinien und sonstiger Rechtsregeln. Und zum anderen eine definierte Unternehmensfunktion, deren primäre Aufgabe es ist, Regelverstöße zu vermeiden, sie aufzudecken und in angemessener Weise darauf zu reagieren. Während sich die folgenden Überlegungen schwerpunktmäßig auf Unternehmen beziehen, die für andere Unternehmen oder Verbraucher Erzeugnisse herstellen oder Dienstleistungen anbieten, und bei denen Compliance oft immer noch relativ „neu“ ist oder als neu empfunden wird, wird manches sicherlich auch für Unternehmen in Spezialbranchen von Belang sein, die, wie etwa die Finanzdienstleistungsbranche, schon seit längerer Zeit, wenn auch mit unterschiedlichem Erfolg, mit dem Thema Compliance umgehen. Vgl. hierzu insbesondere → *Renz/Frankenberger*, Kap. 20. Zur Begrifflichkeit siehe auch → *Schulz*, Kap. 1 Rn. 1. Zu einer anschaulichen Darstellung des Compliance-Begriffs im Wege des „Storytelling“ vgl. *Rau*, in: *Bernard-Rau, Sustainability Stories*, Kap. 27, S. 233 ff.

2 Zur Abgrenzung dieser Funktionen und weiterer Funktionen von Compliance vgl. *Bürkle*, in: *Hauschka/Moosmayer/Lösler, Corporate Compliance*, § 36 Rn. 66 ff.; *Schulz/Galster*, in: *Bürkle/Hauschka/Schieffer, Der Compliance Officer*, § 3 Rn. 74 ff.

quenzen haben Compliance eine kaum zu überschätzende Aufmerksamkeit beschert. Die Verstöße sind vielfältig und reichen, um nur einige Beispiele zu nennen, von Preisabsprache-Kartellen über vielfältige Korruptionstatbestände, Geldwäsche, Embargoverletzungen, massenhafte Softwaremanipulation zur Umgehung von Umweltnormen bis hin zu – teilweise massiven – Verstößen gegen Datenschutzregeln.³ Viele Unternehmen haben daher in den letzten 10–15 Jahren Compliance-Abteilungen aufgebaut oder ausgebaut, Compliance-Management-Systeme aus der Taufe gehoben und diese weiterentwickelt.

- 3 Trotz eines gelegentlich als „Compliance-Hype“ kritisierten Überziehens mancher Entwicklungen oder Maßnahmen ist es offenkundig, dass es sich bei Compliance nicht um eine Modeerscheinung handelt, eine jener Initiativen also, mit denen Unternehmenszentralen mehr oder weniger regelmäßig den Gesamtkosmos des Unternehmens beglücken, nur um sie nach einigen Quartalen auslaufen und einen stillen, oft wenig betrauten Tod sterben zu lassen. Compliance hat sich zumindest in der westlichen Wirtschaftshemisphäre fest etabliert und sie wird uns weiterhin begleiten. Zahlreiche Gesetzgebungsakte auf europäischer und nationaler Ebene, zu denen auch das zunächst gescheiterte deutsche „Verbandssanktionengesetz“⁴ zu zählen ist, werden diese Entwicklung weiter stärken (hierzu auch → Rn. 80 ff.).

II. Unternehmensfunktionen und ihre Interaktion im Sinne der Compliance

- 4 Dieses Kapitel befasst sich daher aus Praktikersicht mit Fragen nach einer sinnvollen, effektiven und wertbildenden Interaktion dieser nach wie vor noch „jungen“ Unternehmensfunktion mit ihren angestammten Nachbarinnen. Wie können diese zur Compliance des Unternehmens beitragen? Was kann Compliance von Unternehmensorganen und Nachbarfunktionen lernen, was kann sie von ihnen erwarten? Wie kann eine sinnvolle und nachhaltige Zusammenarbeit gelingen? Und wie kann Compliance den mittlerweile als Substrat sinnvoller Compliance-Risikosteuerung weithin akzeptierten Dreischritt aus präventiver Schadensabwendung („prevent“), Ermittlung von Verstößen („detect“) und kor-

3 Der sachliche Anwendungsbereich von Compliance kann unterschiedlich definiert werden. Bei international tätigen Industrieunternehmen wird jedoch häufig das Kartellrecht, das Wirtschaftsstrafrecht (insbesondere das Recht der Antikorruption), das Außenwirtschaftsrecht und oft auch der Datenschutz der Compliance-Funktion unterstellt. Siehe hierzu auch → v. Bodungen, Kap. 25.

4 Regierungsentwurf zur Sanktionierung von verbandsbezogenen Straftaten (VerSanG) vom 16.6.2020, der im Bundesrat kritisch diskutiert (BR-Drs. 440/20) und schließlich innerhalb der Legislaturperiode bis 2021 nicht mehr verabschiedet wurde, da die damalige Regierungskoalition ihre Unstimmigkeiten nicht überbrücken konnte. Auch wenn die gesetzgeberische Tätigkeit hierzu derzeit nicht mit Hochdruck betrieben wird: Ein deutsches „Unternehmensstrafrecht“ wird wohl über kurz oder lang Wirklichkeit werden.

reaktiver Reaktion von Fehlverhalten („respond“)⁵ im Zusammenwirken mit anderen Unternehmensfunktionen am besten erfüllen und meistern? Im Folgenden werden daher die für den Gedanken der Compliance besonders wichtigen Unternehmensorgane und Unternehmensfunktionen analysiert, um das Management an der „Schnittstelle Compliance“⁶ verbessern zu helfen.

1. Geschäftsleitung

Der Vorstandsvorsitzende eines großen, international operierenden Unternehmens hat auf die Frage seines künftigen Leiters Compliance,⁷ was denn nun von ihm erwartet und woran er gemessen werde, wie folgt geantwortet: „Keine Rechtsverstöße und unfallfreies Fahren!“ Dieser knappe Befehl bringt die Erwartung der Geschäftsleitung an Compliance in verallgemeinerungsfähiger Weise auf den Punkt. Die Compliance-Funktion soll also Regelverstöße verhüten und „Unfälle“ vermeiden. Dabei muss allerdings von vornherein betont werden, dass Compliance nur gelingen kann, wenn sie von allen Unternehmensangehörigen akzeptiert und gelebt wird. Außerdem, und das ist an dieser Stelle maßgeblich, liegt die Letztverantwortung für Compliance stets bei der Unternehmensleitung. Sie ist Ausdruck ihrer Leitungspflicht und mithin „Chefsache“.⁸ Compliance kann daher nicht auf mehr oder minder bequeme Weise „wegdelegiert“ und schon gar nicht ignoriert werden.⁹

Die Geschäftsleitung und insbesondere ihr Vorsitzender müssen also im Rahmen eben dieser grundlegenden Leitungspflicht das Thema Compliance aktiv angehen und vorantreiben: In Abhängigkeit von Geschäftsmodell, Branche, Internationalität, Risikoprofil und Unternehmenskultur muss ein an diese Kriterien angepasstes Compliance-Management-System (CMS) entstehen,¹⁰ will sich das Top-Management im Falle eines Compliance-Verstoßes nicht dem Vorwurf eines Organisationsversagens aussetzen. An Entwicklung, Begleitung und Jus-

5 Vgl. dazu zunächst *Moosmayer*, Compliance, Rn. 43. Sinnvollerweise sollte man jedoch eher von einem „Vierschritt“ sprechen, denn Prävention, Erkennung/Ermittlung von Fehlverhalten und korrektive (Einzel-)Reaktionen werden erst durch stetige, oft auch systemische und tiefgreifende Verbesserung („improve“) wirkungsvoll und nachhaltig. Diese muss zumindest auch von Compliance angestoßen und nachgehalten werden. Vgl. *Galster/Rau*, in: *Bürkle/Hauschka/Schieffer*, Der Compliance Officer, § 2 Rn. 12.

6 Vgl. dazu auch *Schulz/Galster*, in: *Bürkle/Hauschka/Schieffer*, Der Compliance Officer, § 4 Rn. 14 m. w. N.

7 Dieser soll im Weiteren – allein der flüssigeren Lesbarkeit halber in geschlechtsneutraler Form – auch als „Chief Compliance Officer“ oder „CCO“ bezeichnet werden.

8 Prägnant die Beschreibung in Grundsatz 5, S 1 des Deutschen Corporate Governance Kodex (DCGK). Grundlegend die „Siemens-Neubürger“-Entscheidung des LG München I, NZG 2014, 345. Vgl. im Übrigen *Schulz/Galster*, in: *Bürkle/Hauschka/Schieffer*, Der Compliance Officer, § 3 Rn. 21 ff.

9 Zu Delegationsfragen siehe → *Schulz*, Kap. 1 Rn. 56 f. m. w. N.; vgl. auch *Faber*, Anreizbasierte Regulierung von Corporate Compliance, S. 78 ff.

10 Vgl. Grundsatz 5, S 2 DCGK. Vgl. auch → *Schulz*, Kap. 1 Rn. 36 ff. m. w. N.; vgl. des weiteren *Bürkle*, in: *Hauschka/Moosmayer/Lösler*, Corporate Compliance, § 36 Rn. 11 ff.

tierung dieses Compliance-Management-Systems sollte die gesamte Unternehmensleitung tatkräftig und nachhaltig mitwirken und ihr gesamtes Gewicht an Unternehmens- und Branchenkenntnis in die Waagschale werfen. Je mehr sie dabei aktiv mitsteuert und sich nicht nur auf Unternehmensberatungen oder andere Externe verlässt, umso höher ist auch die Chance, sich nicht einen fehl gerichteten oder falsch dimensionierten Fremdkörper „überstülpen“ zu lassen.

- 7 Diese Aufgabe ist nicht einfach und sie birgt auch insofern Konfliktpotenzial, als sie dazu führen kann und wird, die Unternehmensleitung mit Versäumnissen oder „Altlasten“ aus der Vergangenheit zu konfrontieren. Auch ist die Befassung mit komplizierten Rechtsfragen und anspruchsvollen Schulungs-, Hinweisgeber- und Reaktionsprozessen nicht jedermanns Sache. Und dennoch: Compliance ist nun tatsächlich alternativlos. Auch wenn die Unternehmensleitung der Auffassung ist, bisher sei doch immer alles gutgegangen und man könne (und wolle?) ja auch nicht immer alles wissen, sollte sie allerspätstens jetzt „die Flucht nach vorn“ ergreifen und Compliance aktiv annehmen, statt sich von ihr fernzuhalten.
- 8 Das alles nimmt Zeit, Aufmerksamkeit und Geld in Anspruch. Wer nun nur ein-dimensional-kurzfristig fragt oder das gerade geschaffene oder aufgestockte, oft noch etwas unsichere Compliance-Team anherrscht: „Was bringt uns das?“, wird im Allgemeinen keine für ihn befriedigende Antwort erhalten. Gerade die vorsorgende, schulende und den Eintritt von Compliance-Risiken minimierende Compliance-Arbeit ist häufig wenig spektakulär, wird nach außen hin kaum sichtbar und lässt sich oft auch hinsichtlich ihres Wertbeitrags mit herkömmlichen Mitteln nur schwer quantifizieren.
- 9 Was, also, bringt das? Die in Compliance-Schulungen gern landauf, landab gezeigten „Schockfotos“ mit gewaltigen Strafzahlungen, Schadensersatzsummen und Unternehmenslenkern hinter Gittern sind wohl notwendig und entfalten bei manchen auch einen gewissen pädagogischen Effekt. Sie erreichen aber beileibe nicht jeden. Manch einer lässt sich dadurch nicht beeindrucken und lernt tatsächlich nur aus eigenem, höchstpersönlich erlittenem Schaden. Auch greifen die Versuche, die Kosten von Non-Compliance nur im Wege spektakulärer Sanktionen zu illustrieren, zu kurz. Nicht überall ist der Verfolgungsdruck gleich hoch, nicht alle Bußgelder sind drakonisch, nicht immer droht eine Gewinnabschöpfung oder gar der Ausschluss von künftigen Bieterverfahren. Oft liegen die – teilweise diffusen – Kosten von Compliance-Verstößen woanders: Derartige Verstöße und die in ihrer Folge unternommenen internen und externen Untersuchungen, auch die Sanktions- und anderen Reaktionsmaßnahmen können ganze Unternehmensteile über Wochen und Monate lahmlegen. Sie halten von der eigentlichen Arbeit ab, verunsichern die Belegschaft, untergraben Vertrauen und Loyalität und schädigen den guten Ruf des Hauses. Ihre Nachwirkungen klingen oft erst nach Jahren ab.¹¹

¹¹ Einige praxisorientierte Argumentationshilfen zur Frage nach dem Wertbeitrag von Compliance finden sich auch bei *Marimon*, in: Schettgen-Sarcher/Bachmann/Schettgen, *Compliance Officer*, S. 298, 313 f.

Dass also zumindest langfristig diese ganzheitlich verstandenen „Gesamtkosten“ von Non-Compliance jene von Compliance weit übersteigen, sollte auch kühlen Rechnern und auch jenen möglichen Skeptikern in der Unternehmensleitung und den oberen Führungsebenen einleuchten, die sich immer noch mit beleidigter Miene darüber beschwerten, dass Compliance – womöglich in typisch deutscher Übertreibung – den Wettbewerb verzerre und „uns“ das Leben unnötig schwer mache, während anderswo Überwachung, Eingriffe und Sanktionen weiterhin eher lax gehandhabt würden. Der Wirtschaftsstandort Deutschland ist unteilbar: Gut ausgebildete und selbstbewusste Mitarbeiter gehören ebenso dazu wie sozialer Friede, eine verlässliche Infrastruktur, ein funktionierendes Rechtssystem – und eben Compliance. Dessen sollte sich die Unternehmensleitung im Rahmen ihrer Compliance-Anstrengungen bewusst sein. **10**

Was noch kann und sollte sie tun, um Compliance zum Erfolg zu verhelfen? Vor allem muss sie immer wieder und mit allen kommunikativen Möglichkeiten ein unzweideutiges Bekenntnis abgeben, dass Compliance angenommen und ernst genommen wird, dass Rechtsverstöße nicht geduldet werden und dass Compliance im Interesse eines langfristigen Unternehmenserfolgs liegt. Verlautbarungen zu Integrität und Regelbefolgung dürfen keine bloßen „Sonntagsreden“ sein, und einmal im Wege der Selbstverpflichtung aufgestellte Zielvorgaben („Vorreiter in Sachen Compliance“) müssen dann auch konsequent und mit langem Atem verfolgt werden. Hierin zeigt sich der vielbeschworene „Tone at the Top“. Er hat, besonders für die Unternehmensmitarbeiter, prägende Wirkung und wird genau wahrgenommen.¹² **11**

Auch hier zählen Taten natürlich mehr als Worte. Gleichzeitig bietet sich so mit vergleichsweise überschaubarem Aufwand die Gelegenheit zur – weithin sichtbaren – „Führung durch Beispiel“: Wenn also die Geschäftsleitung bei Online-Schulungen mit gutem Beispiel vorangeht, sich als erstes (natürlich selbst) dem computerisierten Fragebogen stellt und die Unternehmensmitarbeiter darüber im Unternehmens-Intranet informiert, wird dies die regelmäßigen Aufrufe zur Compliance unterstützen und dabei helfen, Compliance zur gelebten Unternehmenswirklichkeit werden zu lassen. **12**

Des Weiteren sollte die Geschäftsleitung alles daran setzen, die fachliche Unabhängigkeit und Weisungsfreiheit der Compliance-Organisation zu gewährleisten und zu respektieren.¹³ Dem (Chief) Compliance Officer ist regelmäßiges und im Notfall jederzeitiges Vortragsrecht zu gewähren. Auch ist es klug, den Zugang des CCO zum Aufsichtsrat zu erleichtern, anstatt ihn diesbezüglich „kurz zu halten“ oder sich gar hinter einem – allzu formalen und zu kurz greifenden – Argument zu verstecken, dass ja nur die Geschäftsleitung mit dem Aufsichtsrat kommunizieren dürfe. **13**

12 Zur Bedeutung des „Tone at the Top“ und der sog. „Compliance-Kultur“ siehe → *Schulz*, Kap. 1 Rn. 68 ff. m. w. N.

13 Zu den Aufgaben der Compliance Officer siehe → *Schulz*, Kap. 1 Rn. 77 m. w. N.; *Schulz/Galster*, in: *Bürkle/Hauschka/Schieffer*, *Der Compliance Officer*, § 3 Rn. 30 ff.

- 14** Als eine „Bergetappe“ bei der nachhaltigen Verankerung des Compliance-Gedankens im Unternehmen darf die Mission gelten, compliance-geneigte Anreize bei der Entlohnung und den unternehmensinternen Aufstiegsmöglichkeiten und Karrierewegen zu schaffen. Denn wenn sich erst einmal herumspricht, dass variable Vergütungsbestandteile auch an Compliance-Ziele geknüpft werden und dass, wer aufsteigen will, zumindest eine Zeitlang und zumindest in einer Nebenfunktion (etwa als Compliance-Beauftragter einer Landesgesellschaft oder einer Produktparte) sich um Compliance gekümmert haben muss, so wird dies seine steuernde und bewussteinbildende Wirkung nicht verfehlen. Auch dieser Aufgabe muss sich die Unternehmensleitung stellen, mag sie Umsetzung und Details dann in die bewährten Hände der Personalabteilung legen können.
- 15** Auch den richtigen Chief Compliance Officer zu finden, zu rekrutieren und zu halten, ist ohne Zweifel „Chefsache“. Das ist anspruchsvoll, aber notwendig. Hier zeigt sich auch, aus welchem Holz Geschäftsleitung (und Aufsichtsorgane) geschnitzt sind. Der CCO, eine fachlich starke, menschlich integre, gereifte Persönlichkeit mit Berufs- und Lebenserfahrung¹⁴ darf gerade kein bequemer Zeitgenosse sein. Er muss das Unternehmen gut kennen(lernen), im Zweifel auch „überall dabei sein“ und muss doch stets Abstand wahren.¹⁵ Bei der Kandidatenkür muss hier sicherlich mancher Unternehmensleiter über seinen Schatten springen und den Reflex, im Zweifel dem „pflegeleichteren“ (oder auch etwas jüngeren und vielleicht kostengünstigeren) Bewerber den Vorzug zu geben, überwinden. Im Idealfall wird ihn der Aufsichtsrat hierzu ermutigen und vielleicht sogar darauf bestehen, dass eine Berichtslinie des CCO künftig zum Aufsichtsrat oder dessen Prüfungsausschuss führt.
- 16** Ja, Compliance ist oft der Überbringer eher unschöner Nachrichten. Aber ebenso wie kein vernünftiger Mensch auf die Idee käme, seinen ihn behandelnden Arzt für eine von diesem diagnostizierte Krankheit verantwortlich zu machen, sollte auch die Unternehmensleitung jeden Reflex unterdrücken, die Compliance-Fachleute und ihren Chef moralisch dafür in Haftung nehmen zu wollen, dass sie einen Compliance-Verstoß aufgedeckt haben.
- 17** Im Gegenteil: Früher oder später wird die Unternehmensleitung auch „heiße Eisen“ anpacken müssen und schwierigen Fragen nicht ausweichen können, bevor sich diese eines Tages gegen das Unternehmen richten können: Inwieweit können sich Compliance und Performance ausschließen oder zumindest behindern? Gibt es Staaten, in denen das Unternehmen seine Geschäftstätigkeit einschränken oder gar einstellen sollte, weil ein regelkonformes Wirtschaften dort nicht möglich erscheint? Kommt dem Unternehmen, etwa aufgrund seines Selbstbildes, seiner Tradition, seiner Größe oder Marktstärke vielleicht sogar eine moralische Pflicht zu, sich auch jenseits des unmittelbaren Unternehmenszwecks, also

¹⁴ Vgl. dazu eingehend *Galster/Rau*, in: Bürkle/Hauschka/Schieffler, Der Compliance Officer, § 2.

¹⁵ Zu diesen Anforderungen an die Person des (Chief) Compliance Officer vgl. auch *Galster/Rau*, in: Bürkle/Hauschka/Schieffler, Der Compliance Officer, § 2 Rn. 28 ff.

etwa in Gremien, Vereinigungen oder in der (Fach-)Öffentlichkeit für den Compliance-Gedanken sichtbar stark zu machen und am gelegentlich beschworenen „Kartell der Guten“ aktiv mitzuwirken?

Compliance ist Bestandteil einer guten Unternehmensführung (Good Corporate Governance). Ohne Compliance ist auch eine glaubwürdige Wahrnehmung unternehmerischer Sozialverantwortung, die über das auf Gewinnerzielungsabsicht des Unternehmens ausgerichtete Wirtschaften hinausgeht (Corporate Social Responsibility)¹⁶ nicht denkbar. Im Rahmen der sich für Unternehmen entwickelnden gesetzlichen und faktischen Verpflichtungen im Themenkreis „Environment, Social and Governance (ESG)“ wird die Bedeutung von Compliance noch zunehmen, manche Unternehmen werden gar ihre ESG-Aktivitäten von der Compliance-Funktion koordinieren lassen oder „die ESG“ in die Compliance-Abteilung integrieren (hierzu unten → Rn. 80 ff.).¹⁷ **18**

Es ist richtig, dass Compliance eine Aufgabe für das ganze Unternehmen ist. Doch ebenso gilt: Compliance kann nur mit einer von Compliance überzeugten und im Hinblick auf Compliance überzeugenden Unternehmensleitung gelingen. **19**

2. Aufsichtsrat

Die Bezeichnung „Aufsichtsrat“ ist angenehm klar und sprechend: Er hat eine beaufsichtigende und eine beratende Funktion. Und während die unmittelbare Verantwortung für eine den externen und internen Regeln konforme Leitung des Unternehmens bei Vorstand oder Geschäftsführung liegt, umfasst die Aufsichtspflicht des Aufsichtsrats im Sinne von § 111 Abs. 1 AktG auch die Compliance.¹⁸ **20**

Daher tut der Aufsichtsrat gut daran, sich darüber klar zu werden, in welchem inhaltlichen, zeitlichen und personellen Rahmen er seiner Tätigkeit zur Überwachung der Compliance-Risiken und Compliance-Aktivitäten des beaufsichtigten Unternehmens nachkommen muss und kann.¹⁹ Welche Aufsichtsratsmitglieder verfügen über besondere Kompetenzen im Hinblick auf Compliance? Sind Schulungen erforderlich? Sind die Aufgaben, die Instrumente und die zeitlichen Budgets des häufig²⁰ bestehenden Prüfungsausschusses zu erweitern? Sollte bei besonders risikogeneigten Unternehmen gar über die Bildung eines separaten Compliance-Ausschusses nachgedacht werden? Derartige Fragen sollten sich AR-Vorsitzender und AR-Plenum vorlegen, diese eingehend diskutieren, ihrerseits fachmännischen Rat beiziehen und diese Diskussionen auch in geeigneter Weise dokumentieren. **21**

¹⁶ Siehe → *Stehr/Knopp*, Kap. 15 sowie → *Beisheim*, Kap. 16.

¹⁷ Zur „ESG-Compliance“ siehe die Nachweise bei → *Schulz*, Kap. 1 Rn. 3 ff.

¹⁸ Vgl. *Siepelt/Pütz*, CCZ 2018, 78; *Blassl*, WM 2017, 992.

¹⁹ Vgl. *Siepelt/Pütz*, CCZ 2018, 78, 80 ff.; *Blassl*, WM 2017, 992, 993 ff.

²⁰ Vgl. § 107 Abs. 3 und 4 AktG; Grundsatz 14 DCGK.

- 22** In jedem Fall setzt eine professionelle Aufsichtsratsarbeit eine zeitlich und inhaltlich hinreichende Befassung mit Compliance-Themen voraus. Berichte zu allen Bereichen der Compliance und des Compliance-Management-Systems müssen rechtzeitig vor den Sitzungen verteilt und kritisch gelesen werden. Im Idealfall sollte die Gelegenheit bestehen, bereits im Vorhinein weitere Informationen anzufordern, damit diese dann spätestens in der angesetzten Sitzung zur Verfügung stehen und auch erläutert werden können. Mündliche Vorträge und Erörterungen in der Sitzung brauchen Zeit, insbesondere wenn es um komplexe Sachverhalte, etwa aus dem Bereich von Auslandsrechtsordnungen oder bei Spezialmaterien wie Außenwirtschafts- und Embargorecht geht. Manche Fälle sind sowohl inhaltlich kompliziert als auch menschlich heikel: Wie geht man zum Beispiel mit einem langjährigen Außendienstmitarbeiter um, der sich in einem – sicherlich subjektiven, jedoch für ihn nur schwer überwindbaren – Dilemma zwischen hergebrachten Praktiken, Loyalität zum Unternehmen, Scheu vor dem „Verpfeifen“ eines Kollegen oder gar eines Vorgesetzten einerseits und falscher, nämlich kurzfristig und allein auf Umsatz- und Ertragswachstum orientierter Anreizsysteme andererseits („Wie Sie die Ziele erreichen, ist mir egal, nein, ich will es eigentlich gar nicht wissen ...“) befindet.
- 23** Auch sollte zwischen dem Aufsichtsrat und dem (Chief) Compliance Officer ein reger und vertrauensvoller Austausch stattfinden. Der (Chief) Compliance Officer sollte regelmäßiger Teilnehmer an Aufsichtsratssitzungen sein und dort auch regelmäßig vortragen können. Auch sollte er Gelegenheit haben, zumindest als Zuhörer auch an jenen Tagesordnungspunkten teilzunehmen, die vielleicht nicht zum Kern der ‚Legal Compliance‘ gehören, aber Berührungspunkte dazu aufweisen, wie etwa die finanzielle Risikosteuerung.²¹ Ist ein Prüfungsausschuss gebildet, so gilt das soeben Gesagte in besonderem Maße: Prüfungsausschuss und Chief Compliance Officer sollten in besonders engem Austausch stehen.
- 24** Liegen Compliance-Verstöße vor, so muss zu diesen intensiver berichtet werden – und zwar, wenn dies wegen der Sachnähe geboten erscheint, auch gemeinsam durch den Chief Compliance Officer und den mit dem Fall befassten, spezialisierten Compliance-Mitarbeiter. Unter Umständen kann sich die grundsätzlich bestehende Aufsichtspflicht des Aufsichtsrats dann auch zu einer eigenen Aufklärungspflicht verdichten.²²
- 25** Um die Compliance-Berichterstattung vor dem Aufsichtsrat nicht zu einem leeren Ritual gefälliger Grafiken und inhaltsarmer Power Point Präsentationen erstarren zu lassen, ist es notwendig, Vertrauen aufzubauen und zu pflegen und Zeit und Geduld in die gemeinsame Aufgabe zu investieren. Das gelingt nur dann, wenn der Aufsichtsrat die Compliance-Thematik insgesamt nicht als eine Störung der – oft langjährigen, gut eingespielten und bisweilen erstaunlich we-

²¹ Vgl. Siepelt/Pütz, CCZ 2018, 78, 81 f.; Blassl, WM 2017, 992, 996 f.

²² Vgl. Siepelt/Pütz, CCZ 2018, 78, 80; Blassl, WM 2017, 992, 995, 999 („Nachforschungspflicht“).

nig zeitintensiven – Sitzungen begreift, sondern der teils immer noch als etwas neu empfundenen Funktion und ihren manchmal vielleicht noch nicht ganz sattelfesten Mitarbeitern Interesse, Respekt und eine grundsätzliche Anerkennung entgegenbringt.

Dann kann günstigenfalls im Lauf der Zeit eine Atmosphäre entstehen, in der das so notwendige Nachfragen, Nachhaken und Nachbohren in Aufsichtsratssitzungen und die offene Diskussion eben nicht als peinliche Abweichung von einem sorgsam durchchoreografierten Präsentationsweg verstanden wird, sondern als das, was es sein soll: Das Zurkenntnisnehmen der schwierigen Unternehmensrealität und das ehrliche, gemeinsame Ringen um ein sauberes Wirtschaften im Einklang mit den Regeln und in Fairness zu den Mitarbeitern, den Vertragspartnern und anderen Stakeholdern. Wenn dies gelingt, wird man dann auch einen Umgang mit anderen schwierigen Themen finden, der Frage etwa, ob es eine, wie auch immer geartete Berichtslinie zwischen dem Chief Compliance Officer und dem Aufsichtsrat oder dem AR-Vorsitzenden geben sollte und ob dem CCO das Recht gegeben werden soll, notfalls direkt, also unter Umgehung der Geschäftsleitung, mit dem Aufsichtsrat oder dessen Vorsitzenden zu kommunizieren oder im Aufsichtsrat in Abwesenheit der Geschäftsleitung vorzutragen.²³ **26**

Schließlich gilt auch für den Aufsichtsrat: Je mehr er – wie die Geschäftsleitung – die Unabhängigkeit von Compliance respektiert, ihr Gelegenheit zum Vortrag und zum Vorbringen von Beobachtungen, Ideen und Anregungen gibt und ihr den Rücken stärkt, umso mehr wird er seiner Aufgabe gerecht, im Rahmen des langfristigen Risikomanagements des Unternehmens Rat zu geben und Aufsicht zu sein. **27**

3. Rechtsabteilung

„Compliance, warum Compliance ...?“, mögen sich manche fragen: „Haben wir dafür nicht eine Rechtsabteilung?“ Das ist ein im Kern verständlicher Einwand: Man kann natürlich Schulungen und andere vorbeugende Maßnahmen zur Einhaltung von Gesetzen, unternehmensinternen Richtlinien und anderen Regeln als Aufgabe der Rechtsabteilung ansehen. In manchen Unternehmen wurde und wird dies auch so gehandhabt. Doch wie verhält es sich etwa mit der Prüfung von Zulieferern, Distributoren oder Joint-Venture-Partnern in aller Welt, dem Nachvollziehen von Zahlungsflüssen und Buchungsvorgängen, dem Aufspüren von Regelverstößen oder mit deren Aufklärung und Ahndung, geschweige denn mit der Implementierung von Maßnahmen und Prozessen, um eine Wiederholungsgefahr, zumal systemischer Art, so weit wie möglich auszuschließen? **28**

²³ Zur Frage der Berichtslinien vgl. auch *Schulz/Galster*, in: *Bürkle/Hauschka/Schieffer*, Der Compliance Officer, § 3 Rn. 68 ff. sowie *Willms*, in: *Bürkle/Hauschka/Schieffer*, Der Compliance Officer, § 5 Rn. 44 ff.

- 29** Bei ehrlicher Betrachtung wird man anerkennen müssen, dass diese Leistungen von einer traditionell aufgestellten und ausgerüsteten Rechtsabteilung typischerweise nicht erbracht werden konnten und auch heute nicht können. Eine Bündelung von regulatorischem Spezial-Know-how, vertieftem Wissen um die Vernetzung zwischen Rechtsregeln, Unternehmensabläufen, Geldflüssen und IT-Forensik und das damit einhergehende Projekt- und Prozessmanagement wird man kaum in einer klassischen Rechtsabteilung finden; dies sind im Übrigen auch weder Ausbildungsschwerpunkte eines Unternehmensjuristen, noch entsprechen sie seinem typischen beruflichen Selbstbild.²⁴
- 30** Das heißt umgekehrt aber nicht, dass die Rechtsabteilung eines Unternehmens unverbunden neben der, wie auch immer ausgestalteten, Compliance-Funktion stünde. Im Gegenteil: Man kann die Rechtsabteilung, ebenso wie Compliance, gemäß dem „3 Lines of Defense“-Modell²⁵ zur „2. Verteidigungslinie“ zählen.
- 31** Rechtsregeln aller Art und die Subsumtion realer Unternehmenssachverhalte unter eine Vielzahl internationaler, nationaler, externer, interner, gesetzlicher oder technischer Normen verbinden Recht und Compliance. So ist es naheliegend, dass etwa ein überwiegend mit Unternehmenskäufen oder Wettbewerbsrecht befasster Unternehmensjurist auch Schulungen zum regelkonformen Verhalten mit Wettbewerbern oder zum Umgang mit Betriebsgeheimnissen oder nachvertraglichen Wettbewerbsverboten anbieten kann. Auch kann er z. B. bei der Erstellung einer Richtlinie für die Einkaufsabteilung mitwirken. Der eine oder andere Unternehmensjurist mag auch im Rahmen von unternehmensinternen Untersuchungen, Mitarbeiterbefragungen oder gar Amnestieprogrammen seine fachlichen Stärken, Spezialkenntnisse und juristischen Tugenden ausspielen können. Jedoch werden diese Fähigkeiten allein, zumindest in einem global operierenden Unternehmen und zumal in einer regulierten Industrie oder in einem oligopolistischen Markt, nicht ausreichen. Zur juristischen Expertise müssen sich eben die oben genannten spezifischen Compliance-Kompetenzen gesellen, die finanzielles, informationstechnologisches und forensisches Know-how – und oft auch eine etwas weniger juristische „Denke“ – erfordern.

²⁴ Vgl. → *Renz/Frankenberger*, Kap. 20 Rn. 61 und Rn. 80 f. weisen zu Recht darauf hin, dass für viele „traditionell geprägte“ Unternehmensjuristen, die mit Compliance-Themen konfrontiert werden, auch das Denken in „Produkten“ und „Prozessen“ – statt in Rechtsbereichen und Rechtsproblemen – eher fremd sein und bisweilen auch bleiben kann. Hier kann in der Tat die „Industrie-Compliance“ von der „Finanzdienstleistungs-Compliance“ lernen.

²⁵ Das vom Institute of Internal Auditors (IIA), der Federation of European Risk Management Associations (FERMA) und der European Confederation of Institutes of Internal Auditing (ECIIA) wesentlich entwickelte „Modell der 3 Verteidigungslinien“ ordnet Compliance und die Rechtsabteilung in die 2. Verteidigungslinie ein. Diese spielt eine wesentliche Rolle bei der Steuerung und Überwachung des von der Geschäftsleitung geführten operativen Tagesgeschäfts. Vgl. dazu in deutscher Sprache: <https://www.diir.de/content/uploads/2023/08/Three-Lines-Model-Updated-German.pdf> (zuletzt abgerufen am 1.1.2024).

Man könnte natürlich den Bereich Recht entsprechend „ertüchtigen“ und in ihm eine Spezialabteilung Compliance schaffen oder angliedern, ähnlich wie das manche Rechtsabteilungen zum Beispiel mit Unterabteilungen für M&A, Großprojekte, Unternehmensfinanzierung oder Patente und Marken getan haben. Zwingend ist das jedoch nicht. **32**

Auch jenseits normierter Vorgaben (wie im Finanzdienstleistungs- und Versicherungssektor) spricht manches für eine Trennung von Recht und Compliance, etwa um mögliche Interessenkonflikte schon organisatorisch vermeiden zu helfen.²⁶ **33**

Auch eine „budgetäre Logik“ dürfte eher für ein Nebeneinander als für eine Integration von Compliance und Rechtsfunktion sprechen: Rechtsabteilungen stehen unter erheblichem Kostendruck und werden gern „kurzgehalten“, zumal auch der Wertbeitrag vorsorgender Rechtspflege oft wenig anschaulich ist und sich nur schwer quantifizieren lässt. Jede neue Mitarbeiterstelle, jeder Fortschritt bei der Ausstattung mit Computern, Dokumenten-Software und anderen IT-Arbeitsmitteln muss mühsam erkämpft werden. Compliance profitiert demgegenüber – noch immer und dank ESG auch auf absehbare Zeit – vom Rückenwind des ebenso Neuen wie Unvermeidlichen: Kaum ein Unternehmen, das aufgrund seiner Eigentümerstruktur, seiner Erzeugnisse und Dienstleistungen oder auch aufgrund seines bekannten Namens in der Öffentlichkeit steht, kann es sich leisten, auf die Frage: „Haben Sie eine dem heutigen Standard entsprechende Compliance-Organisation?“ eine ausweichende oder unbefriedigende Antwort zu geben. Mit anderen Worten: Der Weg zu einer personell und materiell schlagkräftigen Compliance-Organisation dürfte sich mit dem Ansatz „getrennt marschieren, aber vereint kämpfen“ oft rascher und besser verwirklichen lassen, als gemeinsam mit einer stets kritisch beäugten, in der Kostenklemme steckenden Rechtsfunktion.²⁷ **34**

Eines jedoch steht außer Zweifel: Auch wenn man Compliance als ein „aliud“²⁸ zum Bereich Recht betrachtet, so handelt es sich doch zumindest um nah beieinander anzusiedelnde Nachbarfunktionen im Unternehmen. Daher ist eine fachlich und menschlich gute und enge Zusammenarbeit unverzichtbar, um mit den zur Verfügung stehenden Ressourcen ein Optimum an Regeltreue, Rechtssicherheit und effizienten unternehmensinternen Prozessen zu erreichen. Auch kann diese Zusammenarbeit Raum für Austausch, Voneinander-Lernen, Job Rotations und „gemischte Karrierewege“ schaffen: Unternehmensjuristen können sich und ihr berufliches Fortkommen in Richtung Compliance weiterentwickeln, für Compliance-Spezialisten können sich da und dort attraktive Entwicklungsmöglichkeiten auch im Bereich „Business Law“ ergeben. **35**

26 Darauf weisen zu Recht *Schulz/Galster*, in: *Bürkle/Hauschka/Schieffer*, *Der Compliance Officer*, § 3 Rn. 78, hin.

27 Instruktiv zum Verhältnis von Recht und Compliance auch *Willms*, in: *Bürkle/Hauschka/Schieffer*, *Der Compliance Officer*, § 5 Rn. 50 ff.

28 Für die Finanzbranche vgl. → *Renz/Frankenberg*, Kap. 20 Rn. 63.

- 36** Wünschenswert ist schließlich eine gute und vertrauensvolle Zusammenarbeit zwischen dem CCO und dem Leiter Recht.²⁹ Für Kompetenzgerangel oder Futterneid sollte kein Platz sein. Es ist – im wahrsten Sinne des Wortes – genug für alle da: genug Arbeit, genug Herausforderungen und genug Gelegenheiten, sich – auch durch Teamwork zwischen Recht und Compliance – auszuzeichnen.

4. Personalabteilung

- 37** Auch die HR-Funktion ist ein wichtiger Träger von Compliance im Unternehmen. Dies beginnt bereits damit, dass sie bei der Schaffung von Stellenbeschreibungen und Personalprofilen und dann im Rahmen von Rekrutierungsprozessen bei der Auswahl von Bewerbern ein besonderes Augenmerk auf „compliance-affine“ Erfahrungen, Grundhaltungen und Verhaltensweisen der Kandidaten legen hilft. Bei Job-Messen, in professionellen sozialen Netzwerken und in Vorstellungsgesprächen trägt sie den „Tone at the Top“ im Hinblick auf Compliance in die Welt der Bewerberinnen und Bewerber – und damit vieler künftiger Multiplikatoren und Meinungsbildner.
- 38** Geeignete und verständliche Compliance-Klauseln in Anstellungsverträgen sollten heute zum Standard gehören. Das Gleiche gilt, im Zusammenwirken mit Compliance, für das Verbreiten von unternehmensinternen Richtlinien, um sicherzustellen, dass – nach dem jeweils geltenden Arbeitsrecht und gerichtsfest – tatsächlich alle Mitarbeiter in zumutbarer Weise über einen neuen compliance-relevanten Standard und die erforderlichen Verhaltensweisen informiert wurden.
- 39** Bei Mitarbeiterschulungen, ob online, hybrid oder im Wege der Präsenzschulung, zeigt sich, wie gut „Personal“ seinen Laden und seine Daten „im Griff hat“. Ist man zum Beispiel in der Lage, „auf Knopfdruck“ sämtliche Mitarbeiter einer Landesgesellschaft zu identifizieren? Wurden die Kontaktdaten auf dem neuesten Stand gehalten? Ist bekannt, wer über einen eigenen Computer verfügt oder wer zumindest Zugang zu einem Terminal hat? Besteht gar die Möglichkeit, die Information: „Hat Computer-Schulung zum Thema *Interessenkonflikte* erfolgreich absolviert“ mit einer automatischen Erinnerungsfunktion zu verknüpfen, um zu vermeiden, dass der gleiche Mitarbeiter nach einer bald anstehenden Versetzung in eine andere Tochtergesellschaft sofort wieder mit der gleichen Schulung beglückt wird? Das erfordert Aufwand und Mehrarbeit, aber im Idealfall wird eine Personalfunktion die sich daraus ergebenden Chancen, ihre Dateien und Prozesse auf den neuesten Stand zu bringen, zu nutzen wissen – im Einklang mit dem Datenschutz, versteht sich.
- 40** Bei der Identifizierung und Förderung von besonders befähigt erscheinenden Nachwuchskräften sollte die Personalfunktion dabei mitwirken, dass neben grundsätzlicher Regeltreue und Integrität auch der Blick des „High Potential“ für Compliance-Risiken und typische Zielkonflikte geschärft wird. In Seminare von Führungskräften und anderen besonders compliance-sensiblen Positionen,

²⁹ Vgl. → *Hastenrath*, Kap. 6 Rn. 4 ff.

etwa im Auslandsgeschäft, im Beschaffungswesen oder im Umgang mit Amtsträgern müssen typische Zielkonflikte als Fallbeispiele eingebaut werden, aus denen deutlich wird, wie rasch sich einzelne Mitarbeiter in einer Spannungslage zwischen Compliance und Performance wiederfinden können. Auch hier sollten die Personalabteilung und die Spezialisten von Compliance Hand in Hand arbeiten.

Im Idealfall wird HR, auf Initiative und mit Billigung der Geschäftsleitung, auch Anreiz- und Vergütungssysteme entwickeln und umsetzen helfen, in denen eben jene schwierige Balance zwischen Compliance und Performance abgebildet wird (vgl. oben → Rn. 14). Wenn es einem Unternehmen mithilfe einer kompetenten und kreativen Personalabteilung gelingt, etwa dem Leiter einer Landesgesellschaft in einem Zukunftsmarkt nicht nur die ihm vertrauten, einer leicht zugänglichen quantitativen Logik folgenden, Wachstums- und Ertragsziele zu setzen, sondern ihn auch nachhaltig dafür zu motivieren, dass er regelmäßige Compliance-Schulungen abhält und dabei sichtbar durch Beispiel führt, oder dass er einen Leistungsträger eine Zeitlang für nebenamtliche Compliance-Aufgaben freistellt, kann dies im Sinne eines „den Compliance-Gedanken in die Organisation Hineintragens“ kaum hoch genug geschätzt werden. **41**

Wenn ein gravierender Compliance-Verstoß sich in einer Personalmaßnahme niederschlägt, ist erneut HR involviert, nun mit einer hoffentlich wohl dosierten Mischung aus arbeitsrechtlicher Expertise, Verfahrenssicherheit und Taktgefühl. Ob es sich um die Anhörung eines Mitarbeiters handelt, ob eine Abmahnung ausgesprochen und attenkundig gemacht werden muss oder ob gar eine außerordentliche Kündigung, womöglich sogar mit sofortiger Freistellung, Sperrung des Computerzugangs und Erteilung eines Hausverbots, ansteht, in all diesen Situationen wird es erneut auf eine enge, reibungslose Zusammenarbeit zwischen den Personalern und der Compliance-Funktion ankommen. **42**

Und selbst in tiefgreifenden oder akuten Compliance-Krisen liegen Chancen, die mithilfe der Personalabteilung genutzt werden können: Auch aus systemischen Fehlern, die dank eines Amnestieprogramms zu Tage treten und sogar aus schmerzhaften Trennungsgesprächen kann ein Unternehmen lernen und Compliance-Lücken in der Zukunft schließen. **43**

Aus dem Vorstehenden wird deutlich, wie wichtig die Personalfunktion bei der gemeinsamen Aufgabe Compliance ist. Dabei ist sie einer der natürlichen Partner von Betriebsräten und anderen Formen von Arbeitnehmervertretungen. **44**

5. Betriebsrat

Betriebsräte sind oft eine seit Jahren oder gar Jahrzehnten etablierte Unternehmensfunktion. Sie kennen ihre Mitwirkungsrechte genau und sorgen dafür, dass diese auch eingehalten werden. Oft haben sie ihr Ohr nah am Puls des Unternehmens und können sowohl bei der Wahrnehmung dessen, was dort geschieht und wie dort gedacht wird, als auch zur Weiterleitung von Informationen in die Tie- **45**

fen des Unternehmensgeflechts einen ausgesprochen nützlichen „Kommunikationskanal“³⁰ darstellen. Eine neue oder erstarkte Compliance-Abteilung tut gut daran, gern nach einer auffrischenden Lektüre einschlägiger mitbestimmungsrechtlicher Normen und Rechtsprechung, frühzeitig und von sich aus den Kontakt zum Betriebsrat zu suchen, am besten zunächst einmal ohne Tagesordnung und unmittelbaren Ergebnisdruck, um zuzuhören und die Unternehmenswirklichkeit durch die Brille langjähriger Unternehmensmitarbeiter zu betrachten.

- 46** Dabei können beide Seiten, neben den ausdrücklich mitbestimmungspflichtigen oder im jeweiligen Unternehmen zumindest „mitbestimmungs- oder kooperationsüblichen“ Feldern,³¹ Anknüpfungspunkte zur weiteren Zusammenarbeit entdecken: Nicht selten sind es die Betriebsräte, die darauf hinweisen, dass manche gut gemeinte, vielleicht unter Zeit- und Handlungsdruck in einer fernen Unternehmenszentrale verfasste Compliance-Richtlinie vor Ort möglicherweise gar nicht angekommen ist oder verstanden wurde oder – aus welchen Gründen auch immer – als nur schwer umsetzbar erscheint. Auch wird die Interaktion mit den Arbeitnehmervertretungen das Empfinden dafür schärfen, dass Compliance-Themen und auch mögliche Compliance-Verstöße in einer von Arbeitsteiligkeit, virtuellen Teams, Matrix-Strukturen und gleichzeitig vorhandenen tatsächlichen wie auch informellen Hierarchieketten geprägten Unternehmens- und Konzernwirklichkeit nicht immer dort angesprochen oder gelöst werden, wo sie hingehören. Manchmal nämlich lassen Vorgesetzte ihre Untergebenen mit derartigen Themen allein oder bescheiden sie, oft unter Hinweis auf Wachstums- oder Sparziele mit der knappen Botschaft: „Wie Sie das schaffen, ist Ihre ‚Challenge‘ ...“. Hier kann die Compliance-Funktion zusammen mit dem Betriebsrat ansetzen, um regelkonformem Verhalten zum Durchbruch zu verhelfen, ohne dass dies allein auf dem Rücken einzelner, möglicherweise aufgrund widerstreitender Vorgaben überforderter Mitarbeiter geschieht.
- 47** Gleichzeitig bleiben freilich systemische Reibungen zwischen Compliance und Arbeitnehmervertretungen unvermeidlich: Wenn beispielsweise Compliance im Namen einer neuen, etwas forschen Vorgabe umfassende Kontrollen oder Rotationen von im Außendienst, der Beschaffung oder der Projektvergabe tätigen Mitarbeitern fordert, könnten angestammte Betriebsräte dies leicht als übertriebenen Versuch interpretieren, langjährige und bewährte Kolleginnen und Kollegen unter Generalverdacht zu stellen oder sie untunlich einzuengen. Doch wird die Diskussion um die entsprechende neue Betriebsvereinbarung wesentlich leichter von der Hand gehen, wenn man sich vorher, gleichsam im „Normalbetrieb“, kennen- und hoffentlich auch schätzen gelernt hat.
- 48** Heikler noch können Diskussionen oder Auseinandersetzungen zu Hinweisgebersystemen verlaufen. Denn während bestimmte – zumal angloamerikanisch beeinflusste – Unternehmenskulturen die Idee des „Whistleblowers“ überwie-

³⁰ Vgl. *Schulz/Galster*, in: Bürkle/Hauschka/Schieffer, *Der Compliance Officer*, § 3 Rn. 84.

³¹ Vgl. dazu *Mengel*, in: Bürkle/Hauschka/Schieffer, *Der Compliance Officer*, § 7 Rn. 13 ff. (14 ff., 33).

gend positiv besetzen und sich dann eher der Frage widmen, wie man ein derartiges „Hotline-Netzwerk“ und die Bearbeitung der eingehenden Meldungen organisatorisch, inhaltlich und für Berichtszwecke bewältigt, wird manchen Arbeitnehmervertretern in diesem Zusammenhang eher das in der deutschen Sprache und Kultur aus leidvoller Vergangenheit durchaus noch präsente Bild des Kollegen vor Augen treten, der einen anderen „verpfeift“ oder gar verpfeifen soll. Mit diesen schwer miteinander zu vereinbarenden Vorstellungen kann der unternehmensseitige Versuch, Mitarbeiter dazu zu motivieren, das Fehlverhalten anderer – womöglich langjähriger, vertrauter und geschätzter – Kollegen zu „melden“, rasch in ein von Unverständnis und Misstrauen geprägtes Abseits geraten.³² Spätestens seitdem die Einrichtung von Hinweisgebersystemen für viele Unternehmen verpflichtend ist,³³ wird auch das produktive Zusammenwirken von Betriebsrat und Compliance umso wichtiger.

Insgesamt sind daher Vertrauen, Professionalität und Sachlichkeit und die Bereitschaft zum Ausgleich unerlässlich, damit aus den durchaus ungleichen Funktionen Betriebsrat und Compliance wertvolle Partner werden können. **49**

6. Finanzfunktion

Unter Leitung des Finanzvorstands oder -geschäftsführers spielen sich im Unternehmen unter anderem das interne Berichtswesen, das Controlling, die Unternehmensfinanzierung und oft auch die generelle Risikoeinschätzung und -steuerung ab.³⁴ Nicht nur in der zuletzt genannten Teilfunktion liegen wiederum organische Anknüpfungspunkte für die Compliance. Das Wissen um Risiken, der Umgang mit ihnen und die traditionelle Vertrautheit mit juristisch-finanziellen Schnittstellenthemen, wie etwa der Frage danach, ob und ggf. welche Beträge für einen größeren Rechtsstreit oder eine behördliche Untersuchung zurückgestellt werden müssen, macht die Finanzfunktion und ihre Leitungsebene zum natürlichen Verbündeten der Compliance-Funktion und des CCO. **50**

Daher sollte dieser, wenn er eine Compliance-Abteilung aufzubauen, auszubauen oder umzubauen hat, beizeiten Fühlung mit den Kollegen aus der Finanzfunktion aufnehmen und deren Rat suchen. Er selbst und seine Mitarbeiter können von den Kollegen aus der Finanzabteilung manches lernen. In dem Maße, in dem dann die Compliance-Abteilung Tiefe gewinnt, wird man die Zusammenar- **51**

32 Weitere Praxisbeispiele und Lösungsvorschläge bei möglichen Konflikten erörtert *Wybitul*, CB 2015, 77.

33 Vgl. die EU-Whistleblower-Richtlinie EU 2019/1937 und das deutsche Hinweisgeberschutzgesetz sowie das deutsche Lieferkettensorgfaltspflichtengesetz.

34 Im Gegensatz zu Kreditinstituten (vgl. dazu → *Renz/Frankenberger*, Kap. 20 Rn. 4 ff.) verfügt beileibe nicht jedes „Produkt-Unternehmen“ über eine eigene, spezifisch ausgewiesene „Risikomanagement“- oder „Risiko-Controlling“-Abteilung. Häufig existieren leider sogar eine Vielzahl von – nicht notwendigerweise harmonisierten oder aufeinander abgestimmten – Risikobegriffen in der Finanzfunktion, der Rechtsabteilung, der Innenrevision, einer möglichen separaten Versicherungsabteilung – und eben bei Compliance.

beit mit den Kollegen von Accounting, Controlling oder Risk Management verstetigen und dann oft auch institutionalisieren, wie etwa bei der Bildung und Beschickung eines unternehmensweiten Compliance Committee oder eines Risk Committee oder bei der Koordination des Informationsaustauschs mit den Wirtschaftsprüfern. Auch gegenseitige Personalentwicklungschancen können sich eröffnen: Accounting oder Risiko-Know-how wird der Compliance-Abteilung gut tun und so tut sich vielleicht für den einen oder anderen „Finanzer“ hier sogar eine attraktive Berufsperspektive auf.

- 52 Was die Überwachungs- und Eingriffskomponente von Compliance angeht, so wird sich auch hier eine enge Zusammenarbeit mit der Finanzfunktion anbieten. Denn deren Mitarbeiter sind, oft im Zusammenwirken mit der Innenrevision, diejenigen, die am besten in der Lage sind, Zahlungsflüsse, Kontenbewegungen, Kassenbestände oder Bargeldverkehr daraufhin zu überprüfen, ob hinter möglichen Auffälligkeiten ein handfester Compliance-Verstoß steckt.
- 53 Möglicherweise stehen in der Finanzfunktion auch IT-Werkzeuge oder IT-Know-how zur Verfügung, die etwa für Compliance-Schulungen, deren Auswertung oder Darstellung genutzt werden können.
- 54 Manchmal mag auch (zumindest) eine Berichtslinie des Chief Compliance Officer zum Chief Financial Officer führen. Dieser wird hoffentlich eine verständige Affinität zum Thema Compliance-Risiken entwickelt haben und es wird ihm – durchaus auch im wohlverstandenen eigenen Interesse eines ordnungsgemäßen Risikomanagements – daran gelegen sein, dass Compliance im Unternehmen systematisch, wirkungsvoll und nachhaltig zum Einsatz kommen kann. Der CFO kann daher auch ein kraftvoller und krisenfester Fürsprecher und Alliierte der Compliance-Abteilung sein und mit dafür sorgen, dass Compliance auch in (vermeintlich) risikoärmeren Phasen oder Zeiten eines konjunkturellen Abschwungs nicht zur „Schönwetterveranstaltung“ mutiert oder Gefahr läuft, das Opfer einer „Compliance nach Kassenlage“ zu werden.

7. Innenrevision

- 55 Ähnlich wie die Paarungen Recht und Compliance und Finanzen und Compliance sollten auch die – der „3. Verteidigungslinie“³⁵ zuzurechnende Innenrevision einerseits und Compliance andererseits ein starkes Tandem bilden.³⁶ Das gilt besonders für den Fall, dass die Compliance-Funktion nicht über ein eigenes forensisches Team verfügt. Die Aufgabe, Unregelmäßigkeiten und Verdachtsmomenten nachzugehen, Dokumente (typischerweise auch E-Mails, soweit das zulässig ist) zu sichten, Zahlungsflüsse zu überprüfen und Untersuchungen auch

35 Vgl. oben → Fn. 25.

36 Zu Möglichkeiten der organisatorischen Zuordnung von Compliance – eingebettet in die Funktion Recht, als eigene Abteilung oder als Teil der Innenrevision – vgl. Daum, in: Bay/Hastenrath, Compliance-Management-Systeme, Kap. 5 Rn. 24 ff.

vor Ort durchzuführen, kann dann gegebenenfalls von der Innenrevision durchgeführt werden.

Denkbar ist auch, dass ein unternehmensinternes Hinweisgebersystem mit „Hotlines“ oder „Helplines“ gemeinsam durch Compliance und Innenrevision organisiert und verantwortet wird. All dies setzt freilich auf Seiten der Innenrevision „Stärke“, vor allem im Sinne fachlicher Kompetenz, hinreichender Personal- und Sachmittel und auch weitestgehender Unabhängigkeit, voraus. Verfügt die Innenrevision neben einer guten Kenntnis des Unternehmens und seiner Branche auch über spezifische forensische Expertise und IT-Expertise? Besteht eine genügende Affinität zu komplexen juristischen Regelungen? Werden fremde Sprachen beherrscht und die dazugehörenden Kulturen verstanden? **56**

Kaum zu überschätzen ist, wie bei allen Unternehmensbereichen, die sich mit Regelverstößen und deren Konsequenzen befassen müssen, auch die Unabhängigkeit der Innenrevision. Sollte etwa ihr Eingriffs- und Einflussbereich vor bestimmten Unternehmensebenen oder Einzelpersonen Halt machen, so ist das kein gutes Zeichen. Derartige systemische Schwächen sind dann oft nur durch externe Wirtschaftsprüfer oder Sonderermittler auszugleichen. **57**

Wichtig ist, dass sich Compliance und Innenrevision sinnvoll ergänzen³⁷ und dass die jeweiligen Zuständigkeiten und Verantwortungsbereiche klar sind, und zwar sowohl im normalen Arbeitsmodus als auch im Krisenmodus. Das wird auf beiden Seiten oft ein gerüttelt Maß an Fingerspitzengefühl erfordern, nicht zuletzt deshalb, weil die Innenrevision möglicherweise in der noch recht neuen, mit Aufmerksamkeit und vielleicht auch Vorschusslorbeeren bedachten Compliance-Funktion einen Rivalen wittern könnte. Doch auch hier gilt: Gegenseitige Teamfähigkeit und uneitler, professioneller Respekt sind unabdingbare Voraussetzungen für eine produktive Zusammenarbeit im Interesse des Unternehmens. Dazu gehört auch, dass die Innenrevision den, vielleicht von großem Tamtam begleiteten, „Newcomer“ Compliance als willkommene Stärkung des Risikomanagements im Unternehmen begreift, statt sich darüber zu ärgern, dass er nun – unverdientermaßen und womöglich mit vermeintlich leichter Hand – die Früchte jenes Weinbergs erntet, in dem die Innenrevision, bisweilen missverstanden und oft eher ungeliebt, seit Jahren ackert. Umgekehrt sollte Compliance, auch bevor es zu sehr die Werbetrommel in eigener Sache rührt, zuhören, verstehen und würdigen, was die Innenrevision geleistet hat und leistet. Sie ist in aller Regel auch eine wichtige Informations- und Erfahrungsquelle mit oft tiefen, ungefilterten Einblicken in die Unternehmenswirklichkeit, besetzt mit – im Idealfall – **58**

37 *Bürkle*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 36 Rn. 73, weist zu Recht darauf hin, dass Compliance idealtypischerweise in Unternehmensprozesse laufend begleitend und überwachend eingebunden ist, während die Innenrevision im allgemeinen ad hoc und zeitlich später, also retrospektivisch Prüfungen vornimmt. Für die Rolle der Innenrevision in Kreditinstituten und ihrer Abgrenzung zur Compliance-Abteilung vgl. → *Renz/Frankenberger*, Kap. 20 Rn. 9, 67 f.

kompetenten, erfahrenen und unerschrockenen Kollegen, die trotz allem das Lächeln nicht verlernt haben.

- 59 Innenrevision und Compliance können sich also durchaus gut ergänzen. Auch hier sind im Rahmen der Mitarbeiterentwicklung attraktive Karrierewege mit Rotationen, Personaltausch und gegenseitiger Weiterbildung denkbar.

8. Wirtschaftsprüfer

- 60 Im Gegensatz zu den anderen besonders compliance-relevanten Unternehmensfunktionen sind Wirtschaftsprüfer „Unternehmensexterne“. Sie sollen hier dennoch Erwähnung finden, auch weil die Zusammenarbeit mit ihnen für Compliance-Verantwortliche im Unternehmen von besonderer Bedeutung sein kann.³⁸
- 61 Hauptaufgabe der Wirtschaftsprüfer ist die Durchführung von betriebswirtschaftlichen Prüfungen, insbesondere von Jahresabschlüssen und Lageberichten. Bei Regelkonformität wird der Bestätigungsvermerk erteilt. Wirtschaftsprüfer kommen außerdem bei Sonderprüfungen oder bei den sogleich zu erwähnenden Zertifizierungen von Compliance-Management-Systemen zum Einsatz. Auch können sie da oder dort bei Compliance-Untersuchungen helfen, wenn etwa eine Innenrevision, gefangen im Korsett ihres Jahresprüfplans, an Grenzen stößt.
- 62 Unabhängigkeit, Gewissenhaftigkeit und Verschwiegenheit gehören zu den gesetzlichen Berufspflichten der Wirtschaftsprüfer. Dazu gesellen sich in aller Regel eine eingehende, manchmal jahrelange Kenntnis des zu prüfenden Unternehmens und nicht selten ein eingespieltes Netzwerk kompetenter, flexibler und teamfähiger Mitarbeiter im In- und Ausland.
- 63 Die meisten Wirtschaftsprüfungsgesellschaften und ihre einem bestimmten Unternehmen zugeordneten Teams sind personell und materiell zufriedenstellend, manchmal vielleicht sogar beneidenswert üppig aufgestellt und verfügen über angestammte Akzeptanz bei Geschäftsleitung und Aufsichtsorganen. Schließlich ist erwähnenswert, dass die Wirtschaftsprüfer – ähnlich wie die oft aus ihren Reihen stammenden Repräsentanten der unternehmensinternen Finanzfunktion und der Innenrevision – über ein ausgeprägtes Verständnis finanzieller und anderer Risiken verfügen. Mehr noch: Das Institut der Wirtschaftsprüfer in Deutschland hat, etwa in Gestalt des Prüfungsstandards 980, maßgeblich die inhaltlichen Anforderungen mitgeprägt, die an ein Compliance-Management-System (CMS) zu stellen sind.³⁹ Ein derartiges CMS kann in bis zu drei Stufen auf Konzeption, Angemessenheit und Implementierung und schließlich auch Wirk-

38 Zur Perspektive und Rolle des Wirtschaftsprüfers siehe → *Bartuschka*, Kap. 11 Rn. 14 sowie → *Uhlig/Federmann*, Kap. 7 Rn. 4, 16 ff. Im Rahmen des „3-Verteidigungslinien-Modells“ (vgl. oben Fn. 25), werden die Wirtschaftsprüfer gelegentlich als „4. Verteidigungslinie“ bezeichnet, so etwa ausdrücklich durch das ICAEW (Institute of Chartered Accountants in England and Wales).

39 Zum Vergleich zwischen den Standards IDW PS 980 und ISO 19600 ausführlich → *Uhlig/Federmann*, Kap. 7.

samkeit untersucht werden. Im Falle eines positiven Befundes erfolgt eine entsprechende Zertifizierung, die, auch im Hinblick auf ein künftiges, wie auch immer ausgestaltetes Verbandssanktionengesetz, das Haftungsrisiko für Geschäftsleitung und Aufsichtsorgane reduzieren helfen kann. Insofern haben die Wirtschaftsprüfer auch in dieser Hinsicht eine inzwischen anerkannte und stark nachgefragte Risikomanagement- und Absicherungsfunktion.

Oft werden die Wirtschaftsprüfer von sich auf den neuen CCO zugehen. Diese ihm entgegengestreckte Hand sollte er freudig ergreifen. Er wird rasch feststellen, dass man eine gemeinsame Sprache spricht und gemeinsame Aufgaben hat. Regelmäßige Treffen zum Informationsaustausch und zur Risikoeinschätzung sollten folgen. Man wird sich in Aufsichtsratssitzungen und Tagungen eines etwa bestehenden Compliance Committee treffen. Das Netzwerk der Wirtschaftsprüfer wird oft, zusätzlich zu anderen Quellen, wertvolle Informationen und Einschätzungen liefern können. **64**

Von der Methodologie der Wirtschaftsprüfer, ihrer Fähigkeit zum Prozess-Management und ihrem wachen, forschenden und nüchternen Blick auf das Unternehmen können viele Compliance-Organisationen lernen. Umgekehrt werden „die WPs“ eine kompetente Compliance-Funktion nach Kräften unterstützen und mit ihr partnerschaftlich zusammenarbeiten. **65**

9. Unternehmenskommunikation

Der gute Ruf eines Unternehmens ist ein ebenso zentraler wie verletzlicher Vermögensgegenstand. Dies gilt umso mehr in einer durch Informationsflut, Kurzatmigkeit, Globalisierung und Skandalisierung geprägten, rund um die Uhr aktiven Kommunikationslandschaft, zu der in den letzten Jahren vor allem die sozialen Netzwerke hinzugetreten sind. Ein dem amerikanischen Unternehmer und Investor *Warren Buffett* zugesprochenes Zitat bringt die daraus resultierende Verletzlichkeit der Unternehmensreputation auf den Punkt: „Für einen guten Ruf muss man 20 Jahre arbeiten, zerstören kann man ihn jedoch in 5 Minuten. Wer das bedenkt, wird bestimmte Dinge etwas anders angehen.“ **66**

Eine professionelle interne wie externe Unternehmenskommunikation ist daher heutzutage wichtiger denn je, um das kostbare Gut der Unternehmensreputation pflegen und schützen zu helfen.⁴⁰ Gleichzeitig kann sie auch entscheidend dazu beitragen, dass ein Unternehmen, das sich die Compliance besonders auf die Fahnen geschrieben hat, als Vorreiter der Compliance im Markt und in der Öffentlichkeit wahrgenommen wird. Daraus können sich dann sogar Wettbewerbsvorteile ergeben. **67**

Nach innen, also „in das Unternehmen hinein“, werden Unternehmenskommunikation und Compliance, zum Beispiel bei der Konzipierung, Formulierung **68**

⁴⁰ Zu Kommunikation als Schlüssel zu erfolgreichem Compliance-Management siehe *Ritzenhoff/Sonnenberg/Schulz*, CB 2019, 1; zu Fragen der Unternehmenskommunikation vgl. → *Hastenrath*, Kap. 6, und hier insbesondere Schulungen im Compliance-Kontext, Rn. 32 ff.

und Verbreitung eines Verhaltenskodex (Code of Conduct), zusammenkommen – und hoffentlich ihre jeweilige Expertise zu bündeln wissen. Im Idealfall paaren sich dann juristisch geschulte Präzision und Prägnanz mit redaktioneller Erfahrung, Augenmaß und adressatengerechter Sprache.

- 69** Der Grundsatz: „Viel hilft viel“ gilt hier gerade nicht, eher „Weniger ist mehr“. Verständlichkeit, Einprägsamkeit und Knappheit zeichnen gute Verhaltenskodizes oder andere, an die breite Unternehmensöffentlichkeit oder auch an externe Vertragspartner gerichtete Veröffentlichungen aus. Dabei sollten die handelnden Personen konsequent der Versuchung widerstehen, einfach mehrere, tatsächlich oder vermeintlich „bewährte“ Verhaltenskodizes anderer Unternehmen aufeinanderzuhäufen oder sich in ausufernden perfektionistisch-ausgeklügelten Formulierungen zu ergehen.
- 70** Eine weitere wichtige Facette der compliance-orientierten Unternehmenskommunikation besteht in der Beförderung, Verstärkung und Wiederholung von Kenntnissen der Unternehmensleitung zur Compliance, dem bereits oben beschriebenen „Tone at the Top“.
- 71** In dem Maße, in dem die Unternehmenskommunikation ihr eigenes Verständnis für die Möglichkeiten aber auch die Grenzen der Compliance vertieft, kann ihr auch eine Art zusätzlicher Wächterfunktion bei der Formulierung von Compliance-Zielen und bei der Sensibilisierung wichtiger Unternehmens-Multiplikatoren zuwachsen. Allzu vollmundige oder sogar gefährliche⁴¹ Verlautbarungsversuche („brutalstmögliche Aufklärung“, „Null Toleranz“) können so noch rechtzeitig eingefangen werden und auch im nie enden wollenden Sisyphus-Kampf um das Begrenzen ebenso markiger wie teilweise rechtswidriger interner Anspruchsziele oder mehr oder weniger gern gehörter missglückter Ehrgeizbekundungen („Wettbewerber vernichten“) kann die Unternehmenskommunikation ein willkommener Mitstreiter sein.
- 72** Die Außendarstellung des Unternehmens und seiner Compliance-Aktivitäten nimmt eine weitere und heutzutage immer wichtigere Rolle der Unternehmenskommunikation ein. Das betrifft die Kommunikation auf der Website des Unternehmens ebenso wie die Vorbereitung und Moderation von Äußerungen des Führungspersonals in der Öffentlichkeit: Ob es nun darum geht, Gesellschafter oder Aktionäre zu informieren, kritische Fragen von Medien oder Nichtregierungsorganisationen zu beantworten oder – im Zusammenwirken mit HR – auf Jobmessen das Compliance-Profil des Unternehmens als attraktiven Arbeitgebers des 21. Jahrhunderts zu schärfen, bei all diesen Aktivitäten sollte Compliance mit der Unternehmenskommunikation „auf Ballhöhe sein“, damit neben überzeugender Präsentation auch Inhalt und Substanz der Information stets einer kritischen Prüfung standhalten, und zwar auch dann, wenn sie verkürzt, zugespitzt oder aus dem Zusammenhang gerissen werden.

41 Vgl. *Bürkle*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 36 Rn. 21 f.

So können Compliance und Unternehmenskommunikation zusammen wachsen. Sie tragen gemeinsam Sorge, dass das „Messaging“ einheitlich, verständlich und juristisch einwandfrei ist. Sie tragen ebenfalls dazu bei, dass Compliance auch in ereignisärmeren Phasen bei der Geschäftsleitung in Erinnerung bleibt und dass sie in wirtschaftlich schwierigen Zeiten nicht unter die Räder kommt („keine Compliance nach Kassen- und Konjunkturlage“). **73**

Dann kann auch die Kommunikation in einer Compliance-Krise gelingen: Behörden fragen an oder lassen gar durchsuchen, Medien belagern das Unternehmen, die Öffentlichkeit verlangt im Stundenrhythmus nach Antworten – und will Opfer sehen. Hier wird sich die vorherige Zusammenarbeit im Normalbetrieb auszahlen, kurze Wege, rasche Absprachen und unbedingtes Vertrauen in die gegenseitigen Einschätzungen und das einander gegebene Wort. **74**

Der gute Draht zur Öffentlichkeit und „das wohlwollende und stets offene Ohr“ der Geschäftsleitung mögen gelegentlich auch manche Versuchung für die Profis der Unternehmenskommunikation in sich tragen. Eine reibungslose Zusammenarbeit mit den vielleicht manchmal als technokratisch, über-juristisch oder wortklaubereich empfundenen Compliance-Experten ist kein Selbstläufer. Wenn aber der Brückenschlag gelingt, können Durchschlagskraft und Ausstrahlungswirkung dieser Allianz aus Compliance und Unternehmenskommunikation beträchtlich sein. **75**

10. Andere⁴²

Auch mit anderen Unternehmensfunktionen bestehen mehr oder weniger markante Berührungspunkte. Beispielhaft sollen die folgenden Drei kurz erwähnt werden: **76**

Zunächst die Einkaufsfunktion, teils auch als „Procurement“ bekannt, deren Einkaufsprozesse und -personal mit hoher Wahrscheinlichkeit von neuen Compliance-Richtlinien maßgeblich beeinflusst werden und daher rechtzeitig von Compliance „ins Boot geholt“ werden müssen, um Abstoßungsreaktionen zu vermeiden, Verständnis für Veränderungen zu erreichen und einen gemeinsamen Sinn für das Machbare zu entwickeln. **77**

Auch mit der Unternehmens-IT wird Compliance, insbesondere im Rahmen von E-Learning und computergestützten Schulungen, zusammenwirken. Jeder, der es einmal unternommen hat, in der zerklüfteten IT-Landschaft eines internationalen Großunternehmens eine erfolgreiche, sauber dokumentierte und wiederholbare Compliance-Schulung per Computer zu konzipieren, gestalten und durchzuführen, wird erkennen, von welcher zentralen Bedeutung dann die Kooperation mit den IT-Kollegen sein wird. **78**

⁴² Vgl. dazu auch *Schulz/Galster* in: *Bürkle/Hauschka/Schieffer*, *Der Compliance Officer*, § 3 Rn. 74 ff.

- 79 Schließlich bringen Eingangskontrollen, mögliche Videoüberwachungen und ähnliche Sicherheitsmaßnahmen zumindest jene Compliance-Abteilung, die sich auch um den Datenschutz zu kümmern hat, nicht nur in Kontakt mit dem Betriebsrat (vgl. oben → Rn. 45 ff.), sondern auch mit der – wie auch immer ausgestalteten – Unternehmenssicherheit. Auch an sie sollte der CCO denken, zumal dann, wenn der Sicherheitschef über eine enge räumliche (und vielleicht auch persönliche) Nähe zum Unternehmensleiter verfügt.

11. Von Compliance zu GRC – der Weg zu einer integrierten Governance-, Risiko- und Compliance-Funktion und die Herausforderungen durch ESG

- 80 In unserer in den letzten Jahren zunehmend von Naturkatastrophen, kriegerischen Auseinandersetzungen, Pandemiefolgen und gesellschaftlichen Spaltungen gezeichneten volatilen, unsicheren, komplexen und mehrdeutigen „VUCA“-Welt⁴³ kommt der Risikosteuerung im Unternehmen eine erneuerte und ständig wachsende Bedeutung zu. Zu den hergebrachten Risikothemen rund um Strategie, Finanzen, Produkte und IT treten neue oder brisanter gewordene Felder wie Lieferketten-Compliance, die auf die Verantwortung des Unternehmens für seine Lieferanten blickt oder „Trade Compliance“, unter der im Allgemeinen das Themenfeld rund um Import und Export-Regeln und -Beschränkungen (einschließlich Embargos) verstanden wird. Um hier den Überblick nicht zu verlieren und um der Segmentierung und Silo-Bildung vorzubeugen, gehen immer mehr Unternehmen dazu über, einen koordinierten oder vereinheitlichten Risikosteuerungsansatz zu verfolgen.
- 81 Durch die Schaffung einer GRC-Organisation sollen, auf der Grundlage einer einheitlichen Risikomethodologie, Risiken⁴⁴ identifiziert, bewertet, dokumentiert und aufbereitet werden, damit Unternehmensleitung und Aufsichtsorgane angemessene, vertretbare und vom Haftungsprivileg der „Business Judgment Rule“⁴⁵ getragene Entscheidungen treffen können. In ihr sollen insbesondere die durch eine rege gesetzgeberische und regulatorische Tätigkeit auf nationaler und internationaler Ebene geschaffenen Normen aus den Bereichen Umwelt, Soziales und Governance (ESG)⁴⁶ in Strukturen und Prozesse umgesetzt und ein ein-

43 Vgl. z. B. die Definition im Gabler-Wirtschaftslexikon: <https://wirtschaftslexikon.gabler.de/definition/vuca-119684/version-384510> (zuletzt abgerufen am 1.3.2024).

44 Und hoffentlich auch Chancen, die ja oft die Kehrseite von Risiken sind! Zum GRC-Ansatz siehe ferner → *Bartuschka*, Kap. 11.

45 Für Deutschland vgl. §§ 93 Abs. 1 Satz 2, 116 Satz 1 AktG.

46 Für Deutschland z. B. durch das am 1.1.2023 in Kraft getretene Lieferkettensorgfaltspflichtengesetz, auf EU-Ebene z. B. durch die Richtlinie 2022/2464 zur Nachhaltigkeitsberichterstattung („CSRD“), die ebenfalls im Januar 2023 in Kraft getreten ist und sukzessive ab dem Geschäftsjahr 2024 für die ersten Unternehmen Anwendung findet. Einen guten Überblick über die vielfältigen Implikationen von ESG geben z. B. die jährlichen Environment-Social-Governance – Sonderhefte der Zeitschrift „Der Betrieb“.

heitlicher Rahmen geschaffen werden, der Governance, Risiko und Compliance bündelt.

Hierdurch werden der Compliance-Funktion in den meisten Unternehmen neue Aufgaben erwachsen, egal ob „GRC“ im Hause Compliance oder anderswo, z. B. in einer eigenen Stabsstelle, angesiedelt wird.⁴⁷ **82**

Viele Unternehmen ringen derzeit mit der Frage, wie eine integrierte GRC-Organisation in optimaler Weise die weiter steigenden ESG-Anforderungen organisatorisch und prozessual angehen und verarbeiten soll. Dafür gibt es kein Patentrezept. Die Lösungen werden, ähnlich wie bei der seinerzeitigen Schaffung eines Compliance-Management-Systems, u. a. von Unternehmensgröße und Unternehmensgegenstand, dem Geschäftsmodell, der Internationalität, dem Grad der Regulierung, dem spezifischen Risikoprofil und auch von dem individuellen „Risikoappetit“ des Unternehmens abhängen. **83**

Offenkundig ist jedoch, dass die Compliance-Funktion davon betroffen sein wird. Es empfiehlt sich daher dringend, auf der Basis des bestehenden Compliance-Management-Systems und dessen Reifegrad zu prüfen, welchen Beitrag die Compliance-Abteilung für Aufbau und Ablauf der sich aus ESG ergebenden Notwendigkeiten realistisch leisten kann.⁴⁸ Auch hierin wird sich die Schnittstellenkompetenz der Compliance erweisen und bewähren müssen. **84**

12. Fallbeispiel

Abschließend soll ein, leicht idealisierter jedoch noch immer realitätsnaher, Fall die in der Überschrift zu diesem 4. Kapitel angesprochene „erfolgreiche Zusammenarbeit“ zwischen Compliance und einigen anderen Unternehmensfunktionen beispielhaft verdeutlichen: **85**

Ein unternehmensinterner, anonymer Hinweisgeber hat über die Unternehmens-Hotline per E-Mail mitgeteilt, dass es bei der Tochtergesellschaft eines global tätigen Herstellers von feinmechanischen Präzisionsinstrumenten seit einiger Zeit zu Unregelmäßigkeiten komme. Der vorgesehene Vertriebsweg durch die dafür zwar nicht exklusiv, aber im Normalfall zuständigen sub-regionalen Außendienstmitarbeiter des Unternehmens werde vor allem gegenüber einem vor etwa 18 Monaten akquirierten Großkunden bewusst umgangen. Die auf diesem Wege getätigten Umsätze würden nicht korrekt verbucht. Außerdem müssten wohl erhebliche Diskrepanzen zwischen dem in den „elektronischen Büchern“ verzeichneten Warenbestand und dem Ist-Bestand im Zentrallager vorliegen. **86**

⁴⁷ Zu Fragen einer integrierten GRC-Organisation vgl. auch → *Bartuschka*, Kap. 11 sowie *Willms*, in: Bürkle/Hauschka/Schieffer, *Der Compliance Officer*, § 5 Rn. 34 ff.

⁴⁸ Vgl. hierzu etwa die hilfreichen Handreichungen des Deutschen Instituts für Compliance (DICO), Stand Juni 2023, https://www.dico-ev.de/wp-content/uploads/2023/06/DICO_Positionspapier_ESG_final_29062023.pdf (zuletzt abgerufen am 1.3.2024).

- 87** Das Hinweisgebersystem funktioniert. Das für die Bearbeitung derartiger Meldungen im Unternehmen gebildete Gremium, in dem unter der Leitung von Compliance unter anderem auch die Personalabteilung und die Innenrevision vertreten sind, stuft die Information als hinreichend substantiiert ein und beauftragt umgehend einen Compliance-Experten mit der Bearbeitung des Falles. Dieser zieht eine Kollegin aus der Innenrevision bei und ermittelt, auch unter Zuhilfenahme eines verlässlichen Compliance-Beauftragten bei der örtlichen Tochtergesellschaft und mit Unterstützung der örtlichen Personalabteilung, den Sachverhalt. Es stellt sich heraus, dass die Hinweise im Wesentlichen zutreffen und dass die Verstöße zeitlich mit einer Neubesetzung in der regionalen Vertriebsorganisation zusammenfallen: Der neue regionale Vertriebsverantwortliche hat offenbar eine Reihe von langjährigen Ablauf- und Dokumentationsschwächen des antiquierten lokalen IT-Systems ausgenutzt. Aufgrund eines nicht konsequent durchgehaltenen Vier-Augen-Prinzips konnte er dies auch längere Zeit allein tun. Eine Controllerin in der Landesorganisation hatte wohl zumindest einmal Bedenken geäußert, hatte sich damit aber nicht durchsetzen können.
- 88** Der Chief Compliance Officer informiert die Geschäftsleitung der Muttergesellschaft und legt bald darauf seinen Bericht vor, den er auf forensische Datenanalysen der Innenrevision und auf zwei Zeugenaussagen stützen kann. Der zu vermutende materielle Schaden für das Unternehmen ist beträchtlich.
- 89** Mittlerweile hat sich der „Whistleblower“ zu erkennen gegeben und mitgeteilt, dass er Entdeckung und Gegenmaßnahmen fürchte. Mit Hilfe der Personalabteilung und des örtlichen Compliance-Beauftragten ist es gelungen, diese Befürchtungen einstweilen zu zerstreuen.
- 90** Die Geschäftsleitung informiert den Aufsichtsrat, dessen Präsidium den Chief Compliance Officer in einer kurzfristig anberaumten Sondersitzung um einen kurzen „Live-Bericht“ bittet. Hier bewährt sich, wie schon gegenüber der Geschäftsleitung, das im Laufe zahlreicher früherer Begegnungen und Projekte gewachsene Vertrauensverhältnis zwischen dem CCO und den Leitungs- bzw. Aufsichtsorganen des Unternehmens.
- 91** Chief Compliance Officer und Landesgeschäftsführer informieren daraufhin den örtlichen Betriebsrat, danach konfrontieren sie den Verdächtigen mit den Vorwürfen, wobei sie ihm mitteilen, dass er sich nicht sofort zu den Vorwürfen äußern müsse, wenn er dies nicht wolle. Er wird vom Dienst freigestellt, von der Unternehmenssicherheit diskret nach draußen geleitet und sein Computerzugang wird, mit Hilfe der örtlichen IT-Kollegen, einstweilen gesperrt. Zwei Tage später meldet sich der Verdächtige und räumt die Vorwürfe im Wesentlichen ein. Dabei stellt sich heraus, dass er während des über mehr als ein Geschäftsjahr andauernden Tatzeitraums einen aktiven Gehilfen und zwei mögliche „Mitwisser“ hatte.
- 92** Angesichts des offenkundig gewordenen kriminellen Verhaltens werden Täter und, nach Anhörung, der Gehilfe fristlos entlassen und die zugrunde liegenden

Umstände werden der örtlichen Staatsanwaltschaft angezeigt. Die beiden „Mitwisser“ werden angehört und erhalten schließlich, nachdem sich ihr Tatbeitrag nur unvollständig rekonstruieren lässt, in Abstimmung zwischen der Personalabteilung vor Ort und in der Unternehmenszentrale, eine schriftliche Abmahnung. Die örtliche Geschäftsleitung hat für den Fall, dass die Angelegenheit in die Öffentlichkeit gelangt, vorsichtshalber eine mit Compliance und Unternehmenskommunikation abgestimmte Presseerklärung zur Hand.

Kurz darauf halten der Geschäftsleiter der Muttergesellschaft, der Chief Compliance Officer und die örtliche Geschäftsführung eine Betriebsversammlung bei der betroffenen Tochtergesellschaft ab, in der die Belegschaft über den Vorfall und die gezogenen Konsequenzen informiert wird. Dabei legen CEO und örtliche Geschäftsführung klare und unmissverständliche Bekenntnisse zur Compliance ab. **93**

Auf der Unternehmens-Intranetseite wird ein von Compliance entworfenes, mit der Unternehmenskommunikation abgestimmtes Memorandum veröffentlicht und die Einrichtung einer Reihe von Prozessabsicherungen angekündigt. Mitarbeiterschulungen sollen in Kürze folgen. **94**

Diese Maßnahmen werden im Anschluss daran auch tatsächlich und zügig eingeführt und, sowohl in der ursprünglich betroffenen Tochtergesellschaft als auch in anderen Unternehmenseinheiten, regelmäßig durch Datenanalysen und stichprobenartige Audits überprüft. Der Fall wird, in anonymisierter Form, in den Schulungskatalog von Compliance aufgenommen. **95**

III. Fazit

Weit mehr als andere „Stakeholder“ im Unternehmen ist Compliance eine Schnittstellenfunktion. Sie ist, auch aufgrund ihrer „Janusköpfigkeit“ als Business-Partner einerseits und Risikomanager andererseits,⁴⁹ ganz besonders auf vertrauensvolle Zusammenarbeit und intensiven Austausch angewiesen. Da sie für manche immer noch relativ neu ist und bisweilen auf Zurückhaltung und Skepsis trifft, hat sie vielfältige „Bring- und Holschulden“: Die Compliance muss aktiv auf die anderen Funktionen zugehen, sich erklären, dann verstehen, was diese tun und schließlich Wege entwickeln und erhalten, auf denen sie mit diesen Funktionen effektiv zusammenarbeiten kann. **96**

Auf Compliance hat niemand gewartet. Sie sollte auch nicht damit rechnen, dass sie überall mit offenen Armen empfangen wird oder dass ihre Aktivitäten im Unternehmen stets willkommen sind oder spontane Unterstützung erfahren. Wenn der CCO sich dies zur robusten mentalen Ausgangsbasis nimmt, dann wird er nicht allzu viele Enttäuschungen erleben. **97**

Im Ernst: Die Idee, dass sich Unternehmen, ihre Organe und Mitarbeiter regelgerecht verhalten sollen und wollen, ist nicht neu. Wenn man dann aber eine ei- **98**

49 Vgl. *Galster/Rau*, in: Bürkle/Hauschka/Schieffer, *Der Compliance Officer*, § 2 Rn. 8 ff.

gene Unternehmensfunktion schafft oder ertüchtigt, die wesentlich dafür verantwortlich sein soll, der Erreichung dieses hehren Ziels nahezukommen und an ihr gemessen zu werden, muss man sich fragen, wie dies gelingen soll.

99 Die Antwort lautet:

- **Erstens:** Compliance geht alle an, Compliance, das sind wir alle. Alle Unternehmensangehörigen müssen daran glauben und aktiv daran arbeiten, sich regelkonform zu verhalten und dies auch zu wollen.
- **Zweitens:** Anfangs- und Endpunkt dieser Botschaft ist die Unternehmensleitung. Compliance wird von ihr in unzweideutiger Weise vertreten, verteidigt und täglich vorgelebt. Das gilt insbesondere auch bei Zwischenfällen, in Krisen oder in wirtschaftlich schwierigen Zeiten.
- **Drittens:** Auch die tägliche Umsetzung der Compliance ist unser aller Aufgabe. Compliance ist nicht die Unternehmenspolizei. Compliance ist auch nicht etwas, das man einer kleinen Fachabteilung „vor die Füße kippt“ und sich dann, mokant lächelnd, aus dem Staub macht. Nur wenn wir alle die täglichen Anstrengungen der hauptamtlich mit der Compliance-Thematik befassten Kollegen verstehen, respektieren, sie nach Kräften unterstützen und Kritik in konstruktiver Weise äußern, kann Compliance nachhaltiger Erfolg haben.

100 Die vorstehenden Ausführungen und das Fallbeispiel haben der Compliance-Fachabteilung einen Spiegel vorgehalten, in dem dann die für die Gesamtunternehmens-Compliance entscheidenden Kompetenzen und Verhaltensweisen wie in einem Brennglas in den Fokus traten: Der gelebte „Tone at the Top“ an der Unternehmensspitze, die begleitende Aufsicht und wohlwollende Unterstützung durch den Aufsichtsrat, die fachliche und inhaltliche Verzahnung mit Legal und HR, eine mögliche zusätzliche „Erdung“ durch den Betriebsrat, die analytischen, risikosteuernden und investigativen Fähigkeiten von Finanzabteilung und Innenrevision, gegebenenfalls der professionelle und im Prozessmanagement erfahrene Flankenschutz durch die externen Wirtschaftsprüfer und, last but not least, das Finden des richtigen Tons mithilfe der Unternehmenskommunikation.

101 Auf diese „Angebote“ seitens der anderen Unternehmens-Stakeholder müssen die Compliance-Fachleute mit den folgenden eigenen Qualitäten und Kompetenzen eingehen:

- **Kompetenz in praktischer Bewährung:** Compliance muss das Unternehmen, sein Geschäftsmodell, seine Märkte und seine Wettbewerber kennen. Der regulatorische Rahmen, innerhalb dessen das Unternehmen wirtschaftet, muss ihr geläufig sein. Neben der Kenntnis des Inhalts anwendbarer Rechtsnormen muss Compliance auch ein realistisches Verständnis für die Risikointensität des Unternehmenshandelns entwickeln und daraus eine vernünftige Priorisierung der in Angriff zu nehmenden Maßnahmen ableiten.
- **Kommunikation:** In ganz ausgeprägtem Maße muss Compliance mit praktisch allen anderen Unternehmensfunktionen kommunizieren. Sie muss ungefiltert die Unternehmensrealität und die sich aus einem globalen Wirtschaften

zwingend ergebenden Zielkonflikte aus Regelkonformität und Unternehmenserfolg aufnehmen und verarbeiten. Wo immer möglich muss Compliance konkreten Rat und Hilfestellung geben, auch damit in den Weiten und Tiefen der Unternehmensorganisation sich die Meinung verbreiten kann, dass Compliance letztlich Bestandteil der unternehmerischen Wertschöpfung ist und eben kein Fremdkörper. Nur realistische Richtlinien und Schulungen, die verständlich sind, die Mitarbeiter „an der operativen Front“ auch erreichen und die in regelmäßigen Abständen dem Praxistest unterzogen und entsprechend nachjustiert werden, haben Aussicht darauf, auch langfristig und mit innerer Akzeptanz Teil der Unternehmenswirklichkeit zu werden. Compliance muss also in jeder Hinsicht die Sprache des Unternehmens sprechen.

- **Vertrauen:** Erforderlich ist zunächst ein Vertrauensvorschuss in Richtung Compliance: Teil des „Tone at the Top“ ist es, Compliance gegenüber der Belegschaft mit einem Vertrauenskredit auszustatten. Entscheidenderweise muss die Compliance-Funktion dann aber – manchmal entgegen verständlicher beruflicher Reflexe – die, im Einzelfall natürlich widerlegliche, Vermutung aufstellen, dass Unternehmen und Mitarbeiter grundsätzlich regeltreu arbeiten und wirtschaften wollen und dass Regelverstöße nur im Ausnahmefall Ausdruck vorsätzlichen Verhaltens sind. Von dem mit einer Vorschusszahlung seitens der Geschäftsleitung ausgestatteten Vertrauenskonto sollten der Chief Compliance Officer und seine Leute mit Augenmaß abheben – und darauf achten, dass sie es auch immer wieder „auffüllen“ – durch stetige Verbesserung, durch immer besseres Kennenlernen des Unternehmens, durch eine immer verständlichere Sprache und „Nutzerfreundlichkeit“ (insbesondere beim Erteilen von Rat und beim Abfassen von Richtlinien) und durch die richtige Mischung aus Vertrauen und Kontrolle.

Gewonnen hat die Idee der Compliance, also ein in allen Teilen des Unternehmens geltender ernsthafter Anspruch, sich durchgängig regelkonform zu verhalten, dann, wenn der „Tone at the Top“ auch als „Tone in the Middle“ und insbesondere als „Tone in the Trenches“ Widerhall findet, wenn also das Ziel, „sauberes Business“ zu betreiben, von allen Unternehmensfunktionen und einer überwältigenden Mehrheit der Mitarbeiterinnen und Mitarbeiter geteilt, als realistisch empfunden und in der täglichen Praxis auch gelebt wird.

102

4. Kapitel

Einführung eines „Code of Conduct“

I. Einleitung

Ein „Code of Conduct“ oder „Code of Ethics“ ist eine Sammlung von Regelungen und Richtlinien, die ein Unternehmen sich selbst auferlegt, um das Verhalten des Managements, der Mitarbeiter und teilweise auch der Geschäftspartner zu beeinflussen.¹

Lange Zeit waren solche Verhaltenskodizes eine Besonderheit internationaler Konzerne. Manche ausländischen Rechtsordnungen verpflichten Unternehmen ausdrücklich, einen Code of Conduct einzuführen, der auch Tochtergesellschaften bindet (vgl. etwa Sec. 406 Sarbanes-Oxley-Act). Mittlerweile führen viele kleinere und mittelständische Unternehmen, die (ausschließlich) in Deutschland ansässig sind, ebenfalls einen „Code of Conduct“ ein.

Die Gründe sind vielfältig: Zum einen verpflichtet auch das deutsche Recht in unterschiedlichem Kontext zu Compliance-Maßnahmen. Betroffen sind nicht nur börsennotierte Unternehmen (§ 80 WpHG), sondern jeder Arbeitgeber (vgl. § 130 OWiG). Teilweise nimmt der Gesetzgeber die Unternehmen nicht nur für das Verhalten der eigenen Mitarbeiter, sondern auch für das Geschäftsgebaren Dritter in die Pflicht (vgl. § 13 MiLoG). Zum anderen eröffnet nur ein effizientes Compliance-System die Chance, nicht (oder nur eingeschränkt) für Regelverstöße anderer Personen zu haften (vgl. § 12 AGG).² Der Unternehmer kann seine Verantwortung (teilweise) auf Dritte übertragen, beispielsweise auf interne oder externe Beauftragte für Datenschutz oder Arbeitssicherheit. Dies setzt freilich weitere Maßnahmen wie die sorgfältige Auswahl, Schulung und Kontrolle der Mitarbeiter voraus.³

Schließlich handeln viele Unternehmer aus dem aufrichtigen Wunsch, ihren Wertvorstellungen und Überzeugungen jenseits des Betriebsgeländes ein Stück weit Geltung zu verschaffen. Ein guter „Code of Conduct“ regelt nicht nur, wie sich das Unternehmen und seine Mitarbeiter im Geschäftsleben verhalten, sondern vermittelt den Adressaten auch die intrinsischen Motive für solche Vorgaben. Dies sind die geltenden Gesetze, aber immer häufiger auch die Werte des Unternehmens.⁴ Viele Verhaltenskodizes erklären und werben für ihre Vorgaben. Wer seine Mitarbeiter von einer gemeinsamen „Mission“ überzeugen kann, wird

1 Grützner/Jakob, Compliance von A–Z, Code of Conduct (CoC).

2 Zu Ziel und Funktionen von Compliance Management siehe → Schulz, Kap. 1 Rn. 13 ff.

3 Zu Umfang und Grenzen der Delegation von Compliance-Maßnahmen siehe → Schulz, Kap. 1 Rn. 56 f.

4 Zum Zusammenhang von Compliance Management und einem Werte- bzw. Integritätsmanagement → Schulz, Kap. 1 Rn. 73 f.

mit seinem „Code of Conduct“ auf größere Zustimmung stoßen, als jemand, dem es nur darum geht, die gesetzlichen Standards sicher zu stellen.

- 5 Teilweise wird dieses „ethische Bekenntnis“ auch zur Imagepflege und in der Kommunikation mit den Stakeholdern eingesetzt. Ein Unternehmen, das im Fokus öffentlicher Kritik oder behördlicher Ermittlungen steht, kann so möglicherweise seine Glaubwürdigkeit verteidigen oder wiederherstellen.
- 6 Häufig hat sich auch die Erkenntnis durchgesetzt, dass eine nachhaltige Unternehmenspolitik nicht auf dem Ansatz „race to the bottom“ beruhen kann.⁵ Dies gilt insbesondere im Wettbewerb um Fachkräfte und Talente. Gerade bei den Arbeitsbedingungen bieten viele Unternehmen mittlerweile auch dort einen möglichst hohen Standard, wo er nicht gesetzlich vorgeschrieben ist. Compliance wird so zu einem Standortvorteil.
- 7 Ein effizientes Compliance-System setzt nicht zwangsläufig einen voluminösen Verhaltenskodex voraus. Gleichwohl ist die Einführung eines „Code of Conduct“ häufig das Mittel der Wahl. Dies hängt auch damit zusammen, dass so ein sichtbarer Nachweis der eigenen Anstrengungen auf diesem Gebiet geschaffen wird.⁶

II. Ausgestaltung

1. Erscheinungsformen

- 8 „Code of Conduct“ ist ein schillernder Begriff. Es gibt weder eine generelle Verpflichtung zur Einführung noch einen „Goldstandard“ bei der Ausgestaltung. Zahlreiche Verhaltenskodizes sind über das Internet frei zugänglich; sie unterscheiden sich in Umfang und Inhalt deutlich. Auffällig ist, dass „Code of Conduct“ immer häufiger im Zusammenhang mit dem Einsatz und der Nutzung künstlicher Intelligenz anzutreffen sind.⁷ Die Aktivitäten des europäischen Gesetzgebers werden manche Unternehmen zum Handeln veranlassen.⁸
- 9 Manche Unternehmen umreißen im „Code of Conduct“ die ethischen Grundprinzipien ihres Handelns. Sie bekennen sich zu gegenseitigem Respekt, zu fairem Verhalten im Geschäftsleben, zu „Loyalität“ und zu einem guten Arbeitsklima. Sie versprechen, das (geistige) Eigentum, die Privatsphäre und Würde anderer Menschen zu achten. Und sie verurteilen Kinderarbeit, Mobbing, Diskriminierung und sexuelle Belästigung.⁹ Ein solcher Verhaltenskodex beschreibt eher das Selbstverständnis eines Unternehmens, als dass er neue Regeln für die Belegschaft formuliert.

5 Vgl. dazu Göpfert, NZA 2011, 1259.

6 Vgl. Mengel, Compliance und Arbeitsrecht, Einleitung Rn. 1; Dieners/Lembeck, in: Dieners, Handbuch Compliance im Gesundheitswesen, Rn. 10.

7 Vgl. Müller, öAT 2024, 26, 28.

8 Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz, (COM(2021)0206 – C9–0146/2021 – 2021/0106(COD) – KI-VO).

9 Vgl. LAG Niedersachsen v. 20.6.2022, 12 Sa 434/21, BeckRS 2022, 26757.

Für die Mitarbeiter haben solche „ethischen Bekenntnisse“ vor allem dann zusätzliche rechtliche Relevanz, wenn sie für ein Tendenzunternehmen arbeiten.¹⁰ Gleichwohl sollte man die Bedeutung eines „Code of Conduct“, der die Belegschaft auf gemeinsame Grundprinzipien einschwört, nicht unterschätzen: Compliance ist mehr als schlichte Regelkonformität. Vielmehr geht es um die Organisation rechtskonformen Verhaltens im Unternehmen.¹¹ Der Erfolg der Compliance-Organisation basiert allerdings nicht nur auf regelbasierten Vorgaben, sondern hängt maßgeblich auch von einer entsprechenden Werteorientierung der Unternehmensangehörigen ab (Regelbefolgung und Integrität als Bestandteile der „Compliance-Kultur“).¹² Die Formulierung von Werten gibt den Unternehmensangehörigen zudem Orientierung, insbesondere für diejenigen Fragen und Fallkonstellationen, die nicht bzw. nicht eindeutig durch Regeln erfasst bzw. geklärt sind.¹³ Ein Arbeitgeber, der seinen Mitarbeitern glaubhaft vermitteln kann, welche Werte das Unternehmen verkörpert und warum sich ein entsprechendes Engagement lohnt, erreicht damit m. E. etwas anderes, aber nicht weniger als mit einem ausgefeilten Regelwerk.

Andere Unternehmen skizzieren (darüber hinaus) die aktuelle Gesetzeslage in sensiblen Bereichen und halten ihre Belegschaft mehr oder weniger eindringlich zur Rechtstreue an. Ein derartiger Verhaltenskodex betont beispielsweise die Strafbarkeit von Geldwäsche, Vorteilsgewährung oder unlauterem Wettbewerb. Die Belegschaft wird ausdrücklich auf die Einhaltung von Arbeits- und Umweltschutzbestimmungen verpflichtet. Häufig stellt ein solcher „Code of Conduct“ auch die besondere Bedeutung bestimmter Pflichten aus dem Arbeitsvertrag (Verschwiegenheit, Umgang mit Firmeneigentum etc.) heraus. Konsequenterweise enthält der Verhaltenskodex schließlich einen Hinweis, dass ein Verstoß gegen diese Vorgaben gravierende Folgen für das Unternehmen und für das Arbeitsverhältnis haben kann: „Neben arbeitsrechtlichen Konsequenzen bis hin zu einer fristlosen Kündigung kann ein Fehlverhalten auch strafrechtliche Folgen haben, die von einer Geldstrafe bis hin zu einer Freiheitsstrafe reichen.“

Der „Code of Conduct“ konkretisiert in diesen Fällen die bereits qua Gesetz oder Vertrag bestehenden Pflichten. Außerdem wird den Mitarbeitern und dem Management verdeutlicht, dass das Unternehmen ein großes Interesse an der Einhaltung und Erfüllung dieser Pflichten hat. Ob ein Fehlverhalten aber tatsächlich zu einer Kündigung des Arbeitsverhältnisses berechtigt, ist eine Frage des Einzelfalls. Verhaltensbedingte Kündigungen setzen regelmäßig eine Abmahnung voraus. Eine Warnung in einer Betriebsvereinbarung oder in einem Verhaltens-

10 Mengel, Compliance und Arbeitsrecht, § 1 Rn. 26; Hohenstatt/Dzida, in: Henssler/Willemsen/Kalb, Arbeitsrecht, § 118 BetrVG Rn. 23.

11 Siehe hierzu die Nachweise bei → Schulz, Kap. 1 Rn. 1.

12 Zur Bedeutung der Compliance-Kultur ausführlich → Schulz, Kap. 1 Rn. 68 ff. mit weiteren Nachweisen.

13 → Schulz, Kap. 1 Rn. 73 f. mit weiteren Nachweisen zum Zusammenhang von Compliance- und Integritätsmanagement.

kodex kann eine vorweggenommene Abmahnung darstellen, die den Arbeitgeber berechtigt, sofort nach dem ersten Verstoß zu kündigen.¹⁴ Dies kommt allerdings nur bei besonders hervorgehobenen wesentlichen Pflichten oder konkreten schweren Pflichtverletzungen in Betracht.¹⁵ Der Arbeitgeber kann nicht eine Vielzahl von Pflichten pauschal unter den Vorbehalt einer sofortigen Kündigung stellen – weder in einem Arbeitsvertrag noch in einem „Code of Conduct“.

- 13 Schließlich gibt es Verhaltenskodizes, die ein umfangreiches und detailliertes Regelwerk zu zahlreichen Aspekten des Arbeitsalltags im Unternehmen enthalten. Der „Code of Conduct“ setzt nicht nur das geltende Recht um, sondern stellt zusätzlich eigene Verhaltensregeln auf. Das Spektrum der Themen, die adressiert werden, kann von ganz grundsätzlichen Wertentscheidungen über arbeitsrechtliche Verhaltensvorgaben (Meldepflichten und „Whistleblowing“)¹⁶ bis hin zu kleinteiligen Regelungen des Betriebsablaufs (Torkontrollen, unbezahlte Freistellungen) reichen. Der „Code of Conduct“ ist dann häufig ein sogenanntes „Employee Handbook“ mit einer umfassenden Betriebsordnung (§ 87 Abs. 1 Nr. 1 BetrVG). Manchmal existieren Vorbilder bei einer ausländischen Muttergesellschaft, die möglichst originalgetreu bei der deutschen Tochtergesellschaft umgesetzt werden.
- 14 Verhaltenskodizes, die nach diesem Muster entworfen sind, können ein „großer Wurf“ sein. Allerdings besteht die Gefahr, dass es zu unerfreulichen Diskrepanzen zwischen Regelungen des „Code of Conduct“ und den Vorgaben deutscher Gesetze kommt.¹⁷ Viele Lebensbereiche, die im Ausland der Regelungshoheit der Parteien überlassen bleiben, sind in Deutschland gesetzlich ausgeformt. So mag eine umfassende Regelung, ob und zu welchen Bedingungen Elternzeit gewährt wird oder wie bei wiederholtem Zuspätkommen eines Mitarbeiters vorzugehen ist, in manchen US-amerikanischen Bundesstaaten sinnvoll sein. In Deutschland unterwirft sich der Arbeitgeber dagegen möglicherweise durch derartige Regelungen ohne Not zusätzlichen Beschränkungen. Besonders nachteilig können sich solche Regelungen auswirken, wenn das Unternehmen sich verpflichtet, vor einer Kündigung ein ausgefeiltes Beschwerdeverfahren („grievance procedure“) zu durchlaufen. Die unternehmensinternen Vorgaben (z.B. eine zeitaufwendige Anhörung) sollten beispielsweise nicht dazu führen, dass der Arbeitgeber zwingende gesetzliche Anforderungen nicht mehr einhalten kann (z.B. die Zwei-Wochen-Frist im Falle einer Kündigung gem. § 626 BGB).
- 15 Für welchen Ansatz sich ein Unternehmen entscheidet, ist nicht nur eine Frage der Unternehmensphilosophie, sondern häufig auch bestimmter Notwendigkeiten und Zwänge. In einer Unternehmensgruppe, in der mehrere Betriebe an unterschiedlichen Standorten übergreifend zusammenarbeiten, ist es regelmäßig erstrebenswert und zum Teil auch notwendig, einen einheitlichen „Code of Con-

14 Vgl. BAG v. 5.4.2001, 2 AZR 580/99, NZA 2001, 893, 898.

15 Mengel, Arbeitsrecht und Compliance, § 5 Rn. 10 ff.

16 Vgl. auch Müller, öAT 2022, 30, 31.

17 Vgl. dazu auch Eufinger, CCZ 2022, 411.

duct“ und insbesondere auch seine einheitliche Anwendung zu etablieren.¹⁸ Anderenfalls drohen Wertungswidersprüche, die das Unternehmen wenig glaubwürdig erscheinen lassen, wenn es einmal einen Verstoß gegen den „Code of Conduct“ sanktionieren will. Ein ambitionierter „Code of Conduct“ erweitert häufig den Pflichtenkreis der Mitarbeiter; eine erfolgreiche Umsetzung setzt dann regelmäßig einen Konsens mit der Belegschaft und dem Betriebsrat voraus. In internationalen Konzernen müssen regelmäßig unterschiedliche Kulturen auf einen möglichst großen gemeinsamen Nenner gebracht werden. Deutsche Unternehmen mit einer ausländischen Muttergesellschaft stehen vor der Herausforderung, ungewohnte Konzepte der Personalführung im eigenen Haus zu implementieren. Dies wirft diverse kulturelle Fragen (kooperativer Führungsstil vs. hierarchische Entscheidungsfindung), aber auch rechtliche Probleme¹⁹ (Übermittlung personenbezogener Daten in Nicht-EU-Staaten, namentlich die USA²⁰) auf.

2. Typische Regelungen

Die Verhaltenskodizes vieler Unternehmen sind im Internet frei verfügbar. Die Spanne ist groß, auch in qualitativer Hinsicht. Es gibt jedenfalls keine „Blaupause“, die auf jedes Unternehmen passt. Ein „Code of Conduct“ könnte sich jedoch an folgender Struktur orientieren und die genannten Punkte ansprechen: **16**

Übergeordnete Werte des Unternehmens

17

- „Mission Statement“,
- Vorstellung der übergeordneten Werte,
- Erläuterung der Bedeutung des Code of Conduct (für den Betriebsablauf, die Mitarbeiter, die Kunden, die Stakeholder etc.),
- gendersensible Sprache.

Integrität beim Geschäftsverkehr

18

- Integrität im Geschäftsverkehr,
- Einhaltung der nationalen und international geltenden Gesetze,
- Verzicht auf jegliche Form von Korruption und Bestechung,
- Regeln für Zuwendungen und Geschenke, Spenden und Sponsoring,
- Einhaltung der Regeln eines fairen Wettbewerbs, insbesondere der geltenden kartell- und wettbewerbsrechtlichen Vorschriften,
 - Einhaltung von Sanktions- und Embargoregelungen,
 - Achtung geistigen Eigentums,
 - Verantwortung für die Reputation des Unternehmens,
 - Vorgaben zum Umgang mit Behörden und Presse.

¹⁸ Vgl. LAG Rheinland-Pfalz v. 11.5.2022, 2 Sa 276/20, BeckRS 2022, 24530.

¹⁹ Vgl. dazu auch *Eufinger*, CCZ 2022, 411.

²⁰ Vgl. dazu *Grau/Granetzny*, NZA 2016, 405 ff. Zum Datenschutz und Compliance ausführlich → *Becker/Böhlke/Fladung*, Kap. 12.

19 Integrität in der eigenen Organisation

- Einhaltung der unternehmensinternen Richtlinien und Regelwerke,
- Kollegialität, Fairness, respektvoller Umgang, Chancengleichheit, Vereinbarkeit von Beruf und Familie,
- Vorgaben für das soziale Miteinander (z. B. unerwünschte Verhaltensweisen auf Firmenfeiern, Alkoholverbote etc.)
- proaktives Eintreten gegen Mobbing, Diskriminierung und Belästigung,
- Bekenntnis zu Inklusion, Gleichbehandlung und Förderung von Menschen mit Behinderung,
- Schutz vertraulicher Daten und Informationen,
- sorgfältiger und bestimmungsgemäßer Umgang mit Betriebsmitteln,
- Transparenz und Dokumentation wesentlicher Geschäftsabläufe,
- vollständige und wahrheitsgemäße Berichterstattung und Buchhaltung,
- Vermeidung von Interessenkonflikten und Beachtung von Insiderregeln,
- (ggf.) Schranken für politische/religiöse Aktivitäten,
- vertrauensvolle Zusammenarbeit mit Arbeitnehmervertretern und anderen Stakeholdern.

20 Produktqualität und Produktsicherheit

- Bekenntnis zu den eigenen Qualitätsansprüchen,
- Priorität der Sicherheit für Mensch und Umwelt im Herstellungsprozess sowie bei Lieferung von Produkten und Erbringung von Leistungen,
- Erfüllung sämtlicher gesetzlicher und vertraglich vereinbarter Qualitäts- und Sicherheitsanforderungen,
- Einholung und Vorhaltung sämtlicher für die Leistung und den Export erforderlicher Registrierungen, Lizenzen und Genehmigungen.

21 Gesundheit und Arbeitssicherheit

- Priorität von Gesundheitsschutz und Arbeitssicherheit,
- Gewährleistung eines sicheren Arbeitsumfelds,
- Bereitstellung geeigneter Schutzmaßnahmen und Schulungen,
- Priorisierung von Gesundheits- und Sicherheitsaspekten bei der Planung von Arbeitsabläufen,
- regelmäßige Durchführung sämtlicher erforderlicher Wartungs- und Instandhaltungsmaßnahmen.

22 Menschenrechte und Sozialstandards

- Garantie menschenwürdiger Arbeitsbedingungen an allen Standorten,
- Unterbindung jeder Form der Kinderarbeit,
- Unterbindung jeder Form der Zwangsarbeit oder unfreiwilligen Arbeit, der Ausbeutung, der Sklaverei und des Menschenhandels,
- faire Behandlung von Mitarbeitern,
- Unterbindung jeder Form grober oder unmenschlicher Behandlung,
- Gewährleistung von Sozial- und Mindeststandards.

Umweltschutz und Nachhaltigkeit

23

- Verpflichtung auf einen aktiven Beitrag zur Sicherstellung und Verbesserung des Umweltschutzes,
- Einhaltung sämtlicher Umweltschutzgesetze, Richtlinien und Standards,
- sicherer Umgang mit Gefahrstoffen, Zubereitungen und Substanzen,
- kontinuierliches Bemühen um umweltfreundliche Lösungen bei der Festlegung von Herstellungsprozessen, eine effiziente Ressourcennutzung sowie eine Verringerung von Abfall und Emissionen.

Hinweise zur Umsetzung

24

- Pflicht zur Lektüre/Teilnahme an (IT-basierten) Schulungen,
- Pflicht zur Nachfrage/Erkundigung bei Unklarheiten,
- Verhalten bei Verstößen Dritter/Ombudsmann,
- allgemeiner Hinweis auf Kontrolle durch Revision,
- allgemeiner Hinweis auf Sanktionen.

Typischerweise wird ein „Code of Conduct“ durch weitere Richtlinien ergänzt. Gegenstand sind beispielsweise Vorgaben zum Verhalten gegenüber Kunden oder Wettbewerbern, zu Kontakten mit der Öffentlichkeit oder zum Umgang mit personenbezogenen Daten. Diese Trennung ist dort sinnvoll, wo das Unternehmen häufig und rasch auf Veränderungen reagieren muss und Beteiligungsrechte des Betriebsrats nicht betroffen sind.

25

III. Einführung eines „Code of Conduct“

Ein Verhaltenskodex ist regelmäßig nur sinnvoll, wenn er für die Adressaten – Geschäftsführung, Mitarbeiter, Geschäftspartner – auch verbindlich ist. Ausnahmen mögen für reine „Mission Statements“ gelten, die eher auf die öffentliche Wahrnehmung als auf die eigene Belegschaft abzielen.

26

Soweit es darum geht, Geschäftspartner rechtlich an bestimmte Vorgaben zu binden (etwa das Verbot von Kinderarbeit oder die Garantie eines Mindestlohns), muss das Unternehmen auf einer ausdrücklichen Vereinbarung bestehen.²¹ Ob dies gelingt, ist häufig eine Frage der Markt- bzw. Verhandlungsmacht. Tatsächlich müssen Dienstleister und Zulieferer großer Unternehmen immer häufiger Erklärungen dahingehend abgeben, dass ihre Geschäftspraktiken im Einklang mit den ethischen und rechtlichen Erwartungen des Auftraggebers stehen. Umgekehrt werden entsprechende Erklärungen seltener verlangt und kaum abgegeben. Die Wirkung solcher Vereinbarungen hängt ganz entscheidend davon ab, ob die Vereinbarung nach Unterzeichnung noch praktische Relevanz entfaltet oder schlicht im Firmenarchiv endet.

27

Soll der Verhaltenskodex in der eigenen Belegschaft eingeführt werden, bieten sich grundsätzlich zwei Möglichkeiten an. Der Arbeitgeber kann sein Regelwerk

28

²¹ Unrühmliches Vorbild sind die zahlreichen Versuche, sich bei Geschäftspartnern gegen die (zu weit ausgelegte) Auftraggeberhaftung nach § 13 MiLoG abzusichern.

entweder auf der einzelvertraglichen Ebene umsetzen oder eine entsprechende Betriebsvereinbarung abschließen. Teilweise müssen auch beide Wege parallel beschritten werden: Eine Betriebsvereinbarung entfaltet keine Wirkung für leitende Angestellte oder Geschäftsführer; in diesen Fällen muss eine individualvertragliche Regelung erfolgen. Umgekehrt genügen einzelvertragliche Lösungen dort nicht, wo betriebsverfassungsrechtliche Mitwirkungsrechte bestehen und der Betriebsrat zwingend zu beteiligen ist. In jedem Fall ist der Arbeitgeber gut beraten, bei der Einführung eines „Code of Conduct“ die Anregungen aus der Belegschaft zu berücksichtigen. Regelkonformes Verhalten hängt maßgeblich von der Akzeptanz dieser Regeln im Adressatenkreis ab. Mit der praktischen Umsetzung des „Code of Conduct“ können auch Arbeitnehmer mit Führungsaufgaben betraut werden, die in ihrem Verantwortungsbereich dafür sorgen, dass die Regelungen bekannt gemacht und eingehalten werden.²² Der „Code of Conduct“ dient dabei auch als Hilfestellung, um eine Orientierung für die Verantwortlichkeiten zu erlangen, die solchen Führungskräften durch Arbeitsvertrag oder Weisung übertragen werden.²³

1. Individualvertragliche Umsetzung

a) Weisungsrecht des Arbeitgebers

- 29 Der Arbeitgeber wird zunächst prüfen, ob er die gewünschten Verhaltensregeln durch schlichte arbeitsrechtliche Weisung in das Anstellungsverhältnis einführen kann. Nach § 106 GewO kann der Arbeitgeber Inhalt, Ort und Zeit der Arbeitsleitung nach billigem Ermessen näher bestimmen, soweit diese Arbeitsbedingungen nicht bereits durch höherrangiges Recht festgelegt sind.
- 30 Dies gilt selbstverständlich für alle Weisungen, die sich auf die vertraglich geschuldete Arbeitsleistung beziehen. Solche tätigkeitsbezogenen Weisungen, die beispielsweise den richtigen Umgang mit Gefahren am Arbeitsplatz oder mit personenbezogenen Daten betreffen, sind zumeist unproblematisch. Ein Mitbestimmungsrecht des Betriebsrats kommt ebenfalls nicht in Betracht, solange es nur um das sogenannte Arbeitsverhalten geht.
- 31 Das Weisungsrecht gilt grundsätzlich aber auch für Vorgaben zur Ordnung und zum Verhalten der Mitarbeiter im Betrieb.²⁴ Sofern es sich nicht um einen Einzelfall handelt, steht dem Betriebsrat insofern ein Mitbestimmungsrecht zu (§ 87 Abs. 1 Nr. 1 BetrVG).
- 32 In jedem Fall beschränkt sich das arbeitsrechtliche Direktionsrecht darauf, die bestehenden vertraglichen Pflichten zu konkretisieren; der Arbeitgeber kann auf

22 LAG Niedersachsen v. 19.4.2021, 15 Sa 557/20, BeckRS 2021, 5296, Rn. 82; *Kempter/Steinat*, NZA 2017, 1505, 1507.

23 *Müller*, öAT 2023, 26, 28.

24 *Preis*, in: *ErfK ArbR*, GewO § 106 Rn. 3.

diesem Wege nicht die bestehenden Absprachen ändern oder neue Verpflichtungen einführen.²⁵

Für ein breites Spektrum compliance-relevanter Vorgaben, die üblicherweise den Kern vieler Verhaltenskodizes ausmachen, müssen aber meist keine neuen Pflichten begründet werden **33**

Zum einen treffen Management und Mitarbeiter weitreichende Loyalitäts-, Treue- und Rücksichtnahmepflichten gegenüber ihrem Arbeitgeber. Sie sind verpflichtet, alle Handlungen zu unterlassen, die den Arbeitgeber, sein Eigentum und seine geschäftlichen Interessen schädigen könnten. Dies bedeutet beispielsweise auch, dass ein Arbeitnehmer das Unternehmen vor möglicherweise drohenden Schäden warnen muss.²⁶ Grundlage dieser Verpflichtung ist die allgemeine Leistungstreuepflicht (§ 242 BGB)²⁷ bzw. das Gebot zur Rücksichtnahme (§ 241 Abs. 2 BGB),²⁸ die bzw. das impliziter Bestandteil jedes Schuldverhältnisses ist. Insoweit bedarf es keiner ausdrücklichen Vereinbarung. **34**

Zum anderen wird jedes Anstellungsverhältnis nachhaltig durch die besonderen persönlichen Bindungen der Vertragspartner geprägt. Daraus resultieren Nebenpflichten, deren praktische Bedeutung teilweise deutlich weiter reicht als in anderen Schuldverhältnissen: **35**

- vertragliche Wettbewerbsverbote,
- Schutz von (geistigem) Eigentum des Arbeitgebers,
- Schutz von Geschäftsgeheimnissen,
- Wahrung der betrieblichen Ordnung.

Auch in diesen Fällen bedarf es keiner ausdrücklichen Vereinbarung; die entsprechenden Pflichten verstehen sich grundsätzlich von selbst. **36**

Schließlich enthalten viele Anstellungsverträge üblicherweise eine Reihe von Vorschriften, die unmittelbar darauf abzielen, ein gesetzeskonformes Verhalten der Mitarbeiter sicherzustellen. Dazu zählen Vorgaben zum Umgang mit Interessenkonflikten und Geschenken, zu (persönlichen) Äußerungen in der Öffentlichkeit, zur Nutzung von E-Mail und Internet oder zum Umgang mit personenbezogenen Daten. Typische Beispiele sind auch Vereinbarungen, mit denen bestimmte Arbeitgeberpflichten (z. B. für Arbeitssicherheit) vertraglich auf einen Arbeitnehmer übertragen werden. Die Regelungsdichte nimmt tendenziell zu, je höher der Vertragsinhaber in der Unternehmenshierarchie angesiedelt ist. Besonders ausgeprägt sind solche Vorschriften in der Finanzbranche; teilweise **37**

²⁵ *Preis*, in: *ErfK ArbR*, *GewO* § 106 Rn. 8.

²⁶ Dies gilt jedenfalls für Wahrnehmungen im Rahmen der arbeitsvertraglichen Aufgaben. Die Arbeitnehmer sind dagegen nicht ohne Weiteres gehalten, Beobachtungen außerhalb ihres Aufgabenbereichs oder gar aus dem außerdienstlichen Bereich zu melden; *Reinfeld*, in: *Moll, Münchener Anwaltshandbuch Arbeitsrecht*, § 33 Rn. 35 ff.

²⁷ BAG v. 5.3.1968, 1 AZR 229/67.

²⁸ *Reinfeld*, in: *Moll, Münchener Anwaltshandbuch Arbeitsrecht*, § 33 Rn. 35 ff.; *Schuster/Dar-sow*, *NZA* 2005, 273, 273.

setzen die Anstellungsverträge zwingende Vorgaben des Kreditwesengesetzes oder der Institutsvergütungsverordnung unmittelbar um (z. B. das Verbot einer privaten Absicherung gegen die Risiken eines Selbstbehalts bei einer D&O-Versicherung oder gegen den Verlust einer aufgeschobenen variablen Vergütung). Auch hier kann der Arbeitgeber vertraglich bereits begründete Pflichten im Rahmen seines Weisungsrechts einseitig weiter konkretisieren und ausgestalten.

- 38** Das arbeitsrechtliche Direktionsrecht besteht nur im Rahmen billigen Ermessens (§ 315 BGB). Der Arbeitgeber muss alle wesentlichen Umstände, insbesondere die berechtigten Interessen der betreffenden Mitarbeiter, angemessen berücksichtigen und sie mit seinen eigenen Belangen abwägen, bevor eine Weisung ergeht. Diese Grenze wird häufig (aber keineswegs immer) dann überschritten, wenn sich eine Regelung auf das außerdienstliche Verhalten der Mitarbeiter erstreckt. Gerade ethisch motivierte Vorgaben mit hohem Sendungsbewusstsein sind häufig mit Eingriffen in grundrechtlich geschützte Positionen der Arbeitnehmer verbunden; hier kommt es auf die Verhältnismäßigkeit im Einzelfall an.²⁹
- 39** Vor diesem Hintergrund wird ein Unternehmen seinen Verhaltenskodex vor allem dann mittels Weisung einführen, wenn es „nur“ darum geht, bereits bestehende Pflichten zu wiederholen bzw. zu konkretisieren, die Grenzen des „billigen Ermessens“ sicher gewahrt werden und Mitbestimmungsrechte des Betriebsrats nicht einschlägig sind. Der Arbeitgeber veröffentlicht den „Code of Conduct“ regelmäßig im Intranet und stellt ihn den Mitarbeitern auch per E-Mail oder als Broschüre zur Verfügung.³⁰ Ratsam sind individuelle Empfangs- und Lesebestätigungen. Die Vorzüge dieser Vorgehensweise liegen auf der Hand: Der Arbeitgeber kann einen „Code of Conduct“ ohne großen Aufwand einführen und auch kurzfristig wieder ändern. Diese Flexibilität kann sich als großer Vorteil erweisen; die internen und externen Anforderungen an den Verhaltenskodex ändern sich erfahrungsgemäß rasch. Zudem ist es in späteren Auseinandersetzungen, in denen es um die Einhaltung oder Nichteinhaltung eines „Code of Conduct“ geht, von Vorteil, wenn der Arbeitgeber nachweisen kann, dass die betreffenden Mitarbeiter den „Code of Conduct“ empfangen und gelesen haben sowie bestenfalls sogar darüber individuell belehrt wurden.³¹

b) Vertragliche Vereinbarung

- 40** Der Arbeitgeber kann einen Verhaltenskodex auch mittels einzelvertraglicher Vereinbarungen im Unternehmen einführen. Diese Option kommt in Betracht, wenn das arbeitsrechtliche Direktionsrecht alleine nicht ausreicht, um den „Code of Conduct“ zu implementieren. Dies ist insbesondere der Fall, wenn das Unternehmen nicht nur die bestehenden Pflichten konkretisieren, sondern auch

²⁹ *Fitting* u. a., *BetrVG*, § 87 Rn. 71.

³⁰ Vgl. auch *Tödtmann/Winstel*, in: Kubis/Tödtmann, *Arbeitshandbuch für Vorstandsmitglieder*, § 13 Rn. 70 ff.

³¹ Vgl. LAG Köln v. 16.11.2020, 2 Sa 112/20, BeckRS 2020, 43238, Rn. 24.

neue Vertragspflichten einführen will (z.B. Ausweitung der Melde- und Berichtspflichten über das normale arbeitsvertragliche Maß hinaus).

Eine solche Vertragsänderung oder -ergänzung setzt die ausdrückliche Zustimmung der betroffenen Mitarbeiter voraus. Eine stillschweigende Annahmeerklärung kann regelmäßig nicht unterstellt werden: Der „Code of Conduct“ und damit die Vertragsänderung wirken sich nicht sofort und unmittelbar auf das Anstellungsverhältnis aus; der Arbeitgeber kann daher nicht nach Treu und Glauben annehmen, seine Mitarbeiter würden dem geänderten Anstellungsvertrag widersprechen, wenn sie mit den Änderungen nicht einverstanden seien.³² Vor der Aufgabe, von wirklich allen Mitarbeitern das ausdrückliche Einverständnis mit dem neuen Verhaltenskodex einzuholen, dürften allerdings auch Unternehmen, die sich durch ein gutes Betriebsklima auszeichnen, größeren Respekt haben. **41**

Die Einführung eines Verhaltenskodex mittels arbeitsrechtlicher Vereinbarung wirft zudem praktische Probleme auf. Kaum ein Unternehmen wird alle compliance-relevanten Vorgaben abschließend im Anstellungsvertrag aufführen; dies dürfte das Dokument überfrachten. Daher wird der Anstellungsvertrag oder die Änderungsvereinbarung regelmäßig auf den „Code of Conduct“ verweisen. **42**

Enthält die Vereinbarung eine dynamische Verweisung auf die „jeweils geltende Fassung“ des Verhaltenskodex, so bedeutet dies keineswegs, dass das Unternehmen seine Regelungen später wieder einseitig und mit verbindlicher Wirkung für alle Mitarbeiter abändern könnte. Arbeitsvertragliche Absprachen unterliegen einer Inhaltskontrolle anhand der §§ 305 ff. BGB. Eine dynamische Verweisung würde das Klauselverbot in § 308 Nr. 4 BGB (Änderungsvorbehalt) verletzen und wäre zudem intransparent (§ 307 Abs. 1 Satz 2 BGB).³³ Nur solche Vorgaben, die sich entweder unter das Weisungsrecht fassen lassen oder lediglich die gesetzlichen Vorgaben wiederholen, können im Wege einer dynamischen Verweisung in den Anstellungsvertrag einbezogen werden. In allen anderen Fällen riskiert das Unternehmen, dass der „Code of Conduct“ nicht wirksam eingeführt wird und im Ernstfall für die Mitarbeiter nicht verbindlich ist. **43**

Enthält die Vereinbarung eine statische Verweisung, so nimmt sie nur auf eine konkrete Fassung des „Code of Conduct“ Bezug. Spätere Änderungen führen nicht automatisch zu einer Anpassung des Anstellungsvertrages; es bedarf insoweit der erneuten Zustimmung der betroffenen Mitarbeiter. Der Arbeitgeber vermeidet die oben angesprochene Überfrachtung der Vertragsdokumente; diesen Vorteil bezahlt er allerdings mit der fehlenden Flexibilität statischer Verweisungen. **44**

³² Mengel, Compliance und Arbeitsrecht, § 1 Rn. 53.

³³ Vgl. dazu auch Mengel, CCZ 2008, 85, 86; anders Schreiber, NZA-RR 2010, 617, der § 308 Nr. 4 BGB bei Compliance-Richtlinien nicht für einschlägig hält, da der Arbeitgeber bei der Einführung oder Veränderung von Compliance-Richtlinien nicht die versprochene Leistung ändere.

- 45** Im Übrigen unterliegen auch die Compliance-Bestimmungen selbst als Standardarbeitsbedingungen einer Inhaltskontrolle anhand der §§ 305 ff. BGB. Die Bestimmungen des „Code of Conduct“ dürfen die Mitarbeiter somit nicht entgegen den Geboten von Treu und Glauben unangemessen benachteiligen (§ 307 Abs. 1 BGB). Dies kann beispielsweise der Fall sein, wenn der Verhaltenskodex eine umfassende Kontrolle am Arbeitsplatz vorsieht (z. B. ständige Videoüberwachung) oder auch Angehörige der Mitarbeiter in die Pflicht nimmt (z. B. Verbot von Beteiligungen oder Auskünfte zu Anlagegeschäften). Besonderes Augenmerk verdient die sprachliche Ausgestaltung des „Code of Conduct“: Wenn die einzelnen Bestimmungen nicht auch für Laien klar und verständlich formuliert sind, scheitern selbst gute Absichten am Transparenzgebot.
- 46** Vor diesem Hintergrund führen Unternehmen einen „Code of Conduct“ m. E. vergleichsweise selten mittels einer arbeitsvertraglichen Vereinbarung ein. Manchmal wird dieser Weg beschritten, um eine gleichlautende Weisung abzusichern. Die Nachteile einer vertraglichen Vereinbarung (z. B. Konsens der gesamten Belegschaft, Flexibilität bei künftigem Änderungsbedarf) überwiegen häufig die möglichen Vorteile.

c) Änderungskündigung

- 47** Eine eher exotische Variante ist die einseitige Einführung eines „Code of Conduct“ mittels einer Änderungskündigung. Diese Option kommt nur in Ausnahmefällen in Betracht. Aus juristischer Sicht bedarf es zumindest im Anwendungsbereich des Kündigungsschutzgesetzes einer sozialen Rechtfertigung (§ 2 KSchG), die alle Bestimmungen des einzuführenden Verhaltenskodex stützt. Staatliche Vorgaben wie im Kreditwesengesetz mögen punktuell eine Änderungskündigung rechtfertigen; es ist m. E. aber sehr fraglich, ob ein ganzer Verhaltenskodex über diese Schiene rechtssicher umgesetzt werden kann. Ein zwangsweise durchgesetzter Wertekanon beruht zudem selten auf einem breiten Konsens in der Belegschaft; dies lässt m. E. Rückschlüsse auf die Glaubwürdigkeit des „ethischen Bekenntnisses“ und auf die mittelfristigen Erfolgsaussichten solcher Anstrengungen zu.

2. Betriebsvereinbarung

- 48** Der Arbeitgeber kann einen „Code of Conduct“ schließlich auch im Wege einer Betriebsvereinbarung im Unternehmen einführen.
- 49** Diese Option einer Betriebsvereinbarung besteht nicht nur, wenn Teile des Verhaltenskodex ohnehin mitbestimmungspflichtig sind, sondern auch dann, wenn der Arbeitgeber alle relevanten Vorschriften durch schlichte Weisung umsetzen könnte. Auch eine freiwillige Regelung ist eine vollwertige Betriebsvereinbarung. Voraussetzung ist die Existenz eines zuständigen und konsensbereiten Betriebsrats. Der Arbeitgeber kann seinen Beitrag zur Konsensbereitschaft leisten; die Zuständigkeit richtet sich ausschließlich nach den gesetzlichen Vorgaben.

Eine Betriebsvereinbarung, die nicht mit dem zuständigen Betriebsrat abgeschlossen wurde, entfaltet keine Wirkung.

In der Betriebsverfassung gilt eine strikte Trennung der Zuständigkeiten von Betriebsräten, Gesamtbetriebsräten und Konzernbetriebsräten. Danach werden die 50
Beteiligungsrechte grundsätzlich von den örtlichen Betriebsräten wahrgenommen. Dies begründet aber weder eine generelle „Primärzuständigkeit“ des örtlichen Betriebsrats noch eine Auffangzuständigkeit des Gesamtbetriebsrats für betriebsratslose Betriebe.³⁴ Jedes Gremium kann nur im Rahmen seiner originären Zuständigkeit handeln und wirksame Vereinbarungen mit dem Arbeitgeber treffen.

Nach dieser zwingenden Aufgabenverteilung ist der Gesamtbetriebsrat gem. 51
§ 50 Abs. 1 BetrVG nur zuständig, wenn

- eine Angelegenheit das gesamte Unternehmen oder zumindest mehrere Betriebe betrifft und
- diese Angelegenheit nicht durch die örtlichen Betriebsräte innerhalb ihrer Betriebe geregelt werden kann.

Es muss ein zwingendes Erfordernis für eine betriebsübergreifende Regelung 52
bestehen; der bloße Wunsch des Arbeitgebers, aus Kosten- oder Praktikabilitäts-erwägungen eine einheitliche Regelung zu treffen, ist regelmäßig nicht ausreichend.³⁵

Daneben kommt eine Beauftragung des Gesamtbetriebsrats durch die einzelnen 53
Betriebsräte in Betracht (§ 50 Abs. 2 BetrVG). Im Falle eines unternehmensweiten Verhaltenskodex würde dies jedoch den Konsens aller Betriebsräte voraussetzen. Ferner kann der Auftrag jederzeit und ohne Vorliegen besonderer Gründe widerrufen werden – auch in einem späten Stadium der Verhandlungen.

Für die Zuständigkeit des Konzernbetriebsrats gegenüber den Gesamtbetriebsräten 54
gelten die gleichen Grundsätze; die Regelung in § 58 BetrVG ist § 50 BetrVG nachgebildet.

Soweit ein Verhaltenskodex darauf abzielt, eine bestimmte „Philosophie“ im 55
Unternehmen umzusetzen und zu gewährleisten, dass alle Mitarbeiter nach einheitlichen Wertmaßstäben arbeiten, besteht regelmäßig ein zwingendes Interesse an einer einheitlichen Regelung. Ein solcher „Code of Conduct“ kann nur einheitlich in allen Betrieben eingeführt werden; die ethischen Maßstäbe können nicht davon abhängen, ob ein Mitarbeiter in Hamburg oder in München arbei-

34 Der Gesamtbetriebsrat kann auch nur im Rahmen seiner originären Zuständigkeit eine Gesamtbetriebsvereinbarung für betriebsratslose Betriebe abschließen (BAG v. 9.12.2009, 7 ABR 46/08, NZA 2010, 662).

35 Vgl. *Fitting* u. a., BetrVG, § 50 Rn. 23 m. w. N. Anders sieht die Situation im Bereich von freiwilligen Betriebsvereinbarungen aus. Hier kann der Arbeitgeber eine Zusage davon abhängig machen, dass eine unternehmensübergreifende Regelung getroffen wird.

tet.³⁶ Die Einführung eines Verhaltenskodex fällt damit grundsätzlich in die Zuständigkeit des Gesamt- oder Konzernbetriebsrats.³⁷

- 56** Gelingt eine Einigung mit dem Betriebsrat über den „Code of Conduct“, so ist dies in verschiedener Hinsicht vorteilhaft. Der Arbeitgeber kann den Verhaltenskodex einführen, ohne die individuelle Zustimmung seiner Mitarbeiter einholen zu müssen. Spätere Änderungen und Ergänzungen muss er nur mit einem einzelnen Ansprechpartner verhandeln. Eine Betriebsvereinbarung wird zudem nicht inhaltlich anhand der §§ 305 ff. BGB überprüft. Sie unterliegt lediglich einer durch § 75 BetrVG bestimmten Rechtskontrolle; insoweit gelten weniger strenge Maßstäbe.³⁸ Hervorzuheben ist aber insbesondere die Signalwirkung, die von einem gemeinsam verabschiedeten „Code of Conduct“ ausgeht. Die Zustimmung des Betriebsrats zu den ethischen Grundsätzen des Arbeitgebers trägt häufig erheblich zur Akzeptanz dieser Regeln in der Belegschaft bei.
- 57** Allerdings stößt auch diese Umsetzungsform an rechtliche Grenzen. Ganz allgemein müssen die Betriebspartner die grundrechtlich gewährleisteten Freiheitsrechte der Mitarbeiter achten; hier sieht die Betriebsverfassung sogar ausdrückliche Schutzpflichten vor (vgl. § 75 Abs. 2 BetrVG). Die private Lebensgestaltung der Mitarbeiter ist der Regelungskompetenz von Betriebsrat und Arbeitgeber grundsätzlich entzogen. Verhaltensregeln zulasten Dritter (z. B. Angehöriger) sind nicht möglich. Vorgaben zu Äußerungen in der Öffentlichkeit oder zu politischem bzw. religiösem Engagement begegnen ebenfalls Vorbehalten; die Einschränkungen, die den Mitarbeitern abverlangt werden, sind kritisch mit den Belangen des Arbeitgebers abzuwägen.
- 58** Problematisch ist auch das Verhältnis zu anderen einschlägigen Regelungen – insbesondere zu den einzelnen Anstellungsverträgen. Hier gilt das Günstigkeitsprinzip. Sofern der Anstellungsvertrag bereits Vorgaben zu compliance-relevanten Sachverhalten enthält, gehen diese Regelungen einer Betriebsvereinbarung vor, wenn sie aus Sicht des Arbeitnehmers günstiger sind.³⁹ Striktere Vorschriften im „Code of Conduct“ etwa zur privaten Nutzung von Firmengeräten oder zur Annahme von Geschenken – gehen dann ins Leere. Anders verhält es sich nur in den (seltenen) Fällen, in denen der Anstellungsvertrag eine Öffnungsklausel zugunsten (ungünstigerer) Betriebsvereinbarungen enthält.
- 59** Ein einmal durch eine Betriebsvereinbarung eingeführter „Code of Conduct“ kann schließlich nicht einseitig mittels Direktionsrecht geändert werden. Ändern

36 BAG v. 22.7.2008, 1 APR 40/07, NZA 2008, 1248; LAG Düsseldorf v. 14.11.2005, 10 TaBV 46/05, NZA-RR 2006, 81, 83 f.

37 BAG v. 22.7.2008, 1 ABR 40/07, NZA 2008, 1248; vgl. auch *Dzida*, NZA 2008, 1265, und *Fitting u. a.*, BetrVG, § 58 Rn. 12.

38 *Fitting u. a.*, BetrVG, 30. Aufl. 2020, § 77 Rn. 231 ff. m. w. N.; *Richardi/Picker*, in: *Richardi, BetrVG*, § 77 Rn. 132.

39 Vgl. dazu auch *Mengel*, *Compliance und Arbeitsrecht*, 1. Aufl. 2009, 36, die zu Recht betont, dass sich eine Betriebsvereinbarung nicht dazu eignet, ein komplettes Compliance-System eines ausländischen Konzerns zu implementieren.

sich die rechtlichen Rahmenbedingungen oder die Anforderungen des Unternehmens, muss der Arbeitgeber die Betriebsvereinbarung vielmehr kündigen und den „Code of Conduct“ neu verhandeln. Hier kann der Nachwirkung gem. § 77 Abs. 6 BetrVG eine maßgebliche Bedeutung zukommen.

IV. Datenschutzrechtliche Implikation

Der Datenschutz hat seit dem Inkrafttreten der Datenschutzgrundverordnung (DSGVO) einen deutlich größeren Stellenwert als in der Vergangenheit.⁴⁰ Dies gilt auch für die Einführung eines „Code of Conduct“, wo dieses Thema bislang kaum eine Rolle spielte.⁴¹ Enthält der „Code of Conduct“ beispielsweise Regelungen zur Meldung von Verstößen gegen Verhaltensregeln oder möchte der Arbeitgeber die Einhaltung der Vorgaben überprüfen, werden regelmäßig personenbezogene Daten erhoben, verarbeitet und genutzt. In der Folge sind die Voraussetzungen der DSGVO zu beachten. Besonderer Aufmerksamkeit gebühren dabei den gesetzlichen Aufklärungs- und Informationspflichten gegenüber den „Betroffenen“ (Art. 13 ff. DSGVO).

Die Erhebung, Verarbeitung und Nutzung – hierzu zählt auch die Übermittlung – personenbezogener Daten im Arbeitsverhältnis richtet sich regelmäßig nach Art. 88 DSGVO i. V. m. § 26 BDSG und bedarf daher stets eines Erlaubnistatbestands. Erlaubnistatbestände können eine gesetzliche Grundlage, die Einwilligung des Arbeitnehmers (§ 26 Abs. 2 BDSG) oder eine Betriebsvereinbarung (§ 26 Abs. 4 Satz 1 BDSG) sein.⁴² Wird der „Code of Conduct“ mittels einer Betriebsvereinbarung eingeführt, bietet es sich an, hier gleichzeitig die erforderliche Datenverarbeitung rechtlich abzusichern.

Die DSGVO spart insoweit nicht an regelungsbedürftigen Inhalten und Vorgaben. Bei manchen Datenschutzregelungen genügt es, wenn sie in einer sog. Rahmenbetriebsvereinbarung abgebildet werden. Diese Inhalte müssen nicht in jeder Einzelbetriebsvereinbarung wiederholt werden.⁴³

Andere Regelungsinhalte müssen dagegen in jeder Einzelbetriebsvereinbarung aufgenommen werden. Dies betrifft solche Regelungen, die auf die jeweilige Betriebsvereinbarung zugeschnitten sind. Hierzu gehören mindestens der Zweck der Verarbeitung i. S. v. § 26 Abs. 5 BDSG i. V. m. Art. 5 DSGVO, die Dauer der Verarbeitung, Löschungsregeln und die Zugriffsrechte.⁴⁴ Entsprechende Bestim-

40 Zur Bedeutung der DSGVO für das Compliance Management siehe ausführlich → *Böhlke/Becker/Fladung*, Kap. 15.

41 Vgl. Schritte zur Etablierung eines „Code of Conduct“ im Bereich des Datenschutzes bei Forschungsprojekten *Molnár-Gábor/Kaldowski/Korbel*, ZD 2021, 313, 317.

42 BAG v. 30.8.1995, 1 ABR 4/95, NZA 1996, 218, 221 (zu § 4 Abs. 1 BDSG), dies gilt auch für die neue DSGVO, vgl. Öffnungsklausel in Art. 82 DSGVO und Erwägungsgrund 155, welcher als „Kollektivvereinbarung“ ausdrücklich auch die Betriebsvereinbarung erwähnt.

43 *Körner*, NZA 2019, 1389, 1392.

44 *Körner*, NZA 2019, 1389, 1392.

mungen sollten – je nach konkreter Ausgestaltung – auch in den „Code of Conduct“ aufgenommen werden.

- 64** Werden personenbezogene Daten erhoben, verarbeitet oder genutzt, ohne dass hierfür ein Erlaubnistatbestand gegeben ist, hat dieser Datenschutzverstoß u. U. weitreichende Folgen. Die forschende Bußgeldpraxis der Aufsichtsbehörden hat für heftige Diskussionen gesorgt und wird noch die Gerichte beschäftigen. Aus einem Datenschutzverstoß kann aber – je nach Einzelfall – für den Arbeitgeber auch ein sog. Sachvortragsverwertungsverbot folgen. Bietet der Arbeitgeber beispielsweise in einem Kündigungsschutzprozess Beweise an, die unter Verstoß gegen die DSGVO erlangt wurden, darf das Gericht in diesem Fall nicht nur die angebotenen Beweise des Arbeitgebers nicht erheben (bloßes Beweisverwertungsverbot), sondern muss u. U. den gesamten arbeitgeberseitigen Vortrag bei seiner Entscheidung unberücksichtigt lassen.⁴⁵

V. Mitbestimmungsrecht des Betriebsrats

- 65** Ein „Code of Conduct“ muss zwingend als Betriebsvereinbarung eingeführt werden, wenn und soweit Mitbestimmungsrechte des Betriebsrats berührt werden.
- 66** Die Beteiligungsrechte des Betriebsrats hängen naturgemäß von den konkreten Regelungen und Vorgaben des jeweiligen Verhaltenskodex ab. In Betracht kommt in erster Linie ein Mitbestimmungsrecht gem. § 87 Abs. 1 Nr. 1 BetrVG. Daneben können sich Beteiligungsrechte aber auch aus anderen Vorschriften ergeben (§§ 80 Abs. 2, 87 Abs. 1 Nr. 6, 94, 95 BetrVG).
- 67** Wichtig ist, dass der Verhaltenskodex nicht entweder nur insgesamt oder aber überhaupt nicht der Mitbestimmung unterliegt; dies ist eine Quintessenz der Honeywell-Entscheidung des Bundesarbeitsgerichts.⁴⁶ Dass ein Arbeitgeber unterschiedliche Verlautbarungen in einem Gesamtwerk (etwa einem „Code of Conduct“) zusammenfasst, hat somit nicht zur Folge, dass dieses Gesamtwerk mitbestimmungsrechtlich nur einheitlich behandelt werden kann. Vielmehr muss die rechtliche Bewertung nach dem Inhalt der einzelnen Regelungen differenzieren: Manche Teile des Verhaltenskodex können mitbestimmungspflichtig sein, während andere Teile nicht der Mitbestimmung unterliegen.⁴⁷
- 68** Die Rechtsprechung hat insbesondere folgende Regelungen als (mitbestimmungspflichtige) Tatbestände des Ordnungsverhaltens bewertet:

45 BAG v. 27.7.2017, 2 AZR 681/16, NZA 2017, 1327; *Fuhlrott*, ArbRAktuell 2020, 103.

46 BAG v. 22.7.2008, 1 ABR 40/07, NZA 2008, 1248.

47 Allgemeine Meinung im Schrifttum, vgl. etwa *Richardi/Maschmann*, in: *Richardi*, BetrVG, § 87 Rn. 198; *Fitting* u. a., BetrVG, § 87 Rn. 71; *Köhler/Häferer*, GWR 2015, 159; im Ergebnis auch LAG Düsseldorf v. 14.11.2005, 10 TaBV 46/05, NZA-RR 2006, 81, 84 ff.

- Eine Verpflichtung, „ethische Bedenken“ oder mögliche Verstöße gegen den „Code of Conduct“ zu melden, ist mitbestimmungspflichtig, weil sie über die allgemeine Pflicht zur Abwendung von Schäden weit hinausgeht.⁴⁸
- Mitwirkungspflichten der Arbeitnehmer an internen Untersuchungen unterliegen der Mitbestimmung, da diese Pflichten über die arbeitsvertraglichen Nebenpflichten der Arbeitnehmer zur Beobachtung und Meldung strafbaren Verhaltens hinausgehen.⁴⁹
- Auch Verfahrensregelungen im Rahmen einer Whistleblower-Klausel können mitbestimmungspflichtig sein, wenn sie den Mitarbeitern aufgeben, bestimmte Kanäle (Vorgesetzter, Hotline etc.) für Meldungen oder Beschwerden zu nutzen.⁵⁰
- Ebenso unterliegen die Regelungen zu standardisierten internen Prozessen zur Meldung von Datenschutzvorfällen der Mitbestimmung, da die Meldung dem Ordnungsverhalten zuzuordnen ist.⁵¹
- Ein Verbot der Annahme von Geschenken löst ebenfalls ein Mitbestimmungsrecht aus, da die wirtschaftlichen Grenzen regelmäßig verhandelbar sind.⁵²
- Verhaltensvorgaben zur Vermeidung „ungebührlicher Vorgesetztenverhältnisse“ in Gestalt von familiären oder engen persönlichen Verbindungen unterliegen ebenfalls der Mitbestimmung. Derartige Regelungen gehen weit über die allgemeine Pflicht des Arbeitnehmers zur Rücksichtnahme und Vermeidung von Interessenkonflikten hinaus.⁵³
- Das Verbot des Zeigens oder Verbreitens von Bildern, Karikaturen oder Witzen sexueller Natur ist mitbestimmungspflichtig, da die Regelungen des AGG diesen Tatbestand nicht vollständig erfassen und insoweit ein der Mitbestimmung zugänglicher Gestaltungsspielraum verbleibt.⁵⁴
- Verhaltensregeln zur Vermeidung von Belästigungen und unangemessenem Verhalten unterliegen der Mitbestimmung, weil die Möglichkeiten die Arbeitnehmer in dieser Hinsicht zu schützen vielfältig und nicht umfassend gesetzlich geregelt sind.⁵⁵
- Mitbestimmungspflichtig sind zudem Vorgaben zur angemessenen Nutzung elektronischer Medien, soweit es um die Art und Weise der privaten Nutzung geht.⁵⁶

48 LAG Düsseldorf v. 14.11.2005, 10 TaBV 46/05, NZA-RR 2006, 81, 84 f.

49 LAG München v. 4.9.2014, 2 TaBV 50/13, abrufbar unter BeckRS 2015, 68238.

50 BAG v. 22.7.2008, 1 ABR 40/07, NZA 2008, 1248, 1255 f.; LAG Düsseldorf v. 14.11.2005, 10 TaBV 46/05, NZA-RR 2006, 81, 84 f.; LAG München v. 4.9.2014, 2 TaBV 50/13, abrufbar unter BeckRS 2015, 68238.

51 LAG Schleswig-Holstein v. 6.8.2019, 2 TaBV 9/19, abrufbar unter BeckRS 2019, 23585.

52 LAG Düsseldorf v. 14.11.2005, 10 TaBV 46/05, NZA-RR 2006, 81, 85 f.

53 BAG v. 22.7.2008, 1 ABR 40/07, NZA 2008, 1248, 1254 f.; LAG München v. 4.9.2014, 2 TaBV 50/13, abrufbar unter BeckRS 2015, 68238.

54 BAG v. 22.7.2008, 1 ABR 40/07, NZA 2008, 1248, 1256.

55 LAG Düsseldorf v. 14.11.2005, 10 TaBV 46/05, NZA-RR 2006, 81, 86.

56 LAG Nürnberg v. 29.1.1987, 5 TaBV 4/86, NZA 1987, 572; LAG München v. 4.9.2014, 2 TaBV 50/13, abrufbar unter BeckRS 2015, 68238.

– Auch ein generelles Verbot der Benutzung privater Mobiltelefone zu privaten Zwecken während der Arbeitszeit ist mitbestimmungspflichtig.⁵⁷

- 69** Wichtig ist, dass ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG nicht notwendig voraussetzt, dass der „Code of Conduct“ verbindliche Verhaltensregeln einführt. Ausreichend ist bereits, wenn die Maßnahme des Arbeitgebers darauf gerichtet ist, das Verhalten der Arbeitnehmer zu steuern oder die Ordnung des Betriebs zu gewährleisten.⁵⁸ Maßgeblicher Orientierungspunkt, um einzuschätzen, ob eine Regelung im „Code of Conduct“ der Mitbestimmung unterliegt, ist die Abgrenzung zwischen dem mitbestimmungsfreien Arbeitsverhalten und dem mitbestimmungspflichtigen Ordnungsverhalten.⁵⁹ Bezieht sich eine Regelung auf das Arbeitsverhalten, wird lediglich die vertraglich geschuldete Arbeitspflicht konkretisiert. Regelungen, die sich auf die Gestaltung des Zusammenwirkens und -lebens der Arbeitnehmer in dem jeweiligen Unternehmen beziehen, betreffen das Ordnungsverhalten; hier steht dem Betriebsrat ein Mitbestimmungsrecht zu. Dies gilt beispielsweise für eine Nutzungsregelung für die vom Unternehmen zur Verfügung gestellten Parkflächen, welche manche Stellplätze aufgrund der dort vorhandenen Ladesäulen nur für Elektroautos vorsieht.⁶⁰ Auch eine Regelung, die die Arbeitnehmer verpflichtet, Verstöße gegen den „Code of Conduct“ an den Arbeitgeber zu melden, betrifft das Ordnungsverhalten und unterliegt einem Mitbestimmungsrecht gem. § 87 Abs. 1 Nr. 1 BetrVG.⁶¹ Übersehen wird teilweise, dass Regelungen bereits dann mitbestimmungspflichtig sind, wenn sie lediglich darauf abzielen, das Verhalten der Arbeitnehmer nur zu steuern, ohne sie zu einem bestimmten Verhalten zu verpflichten.⁶²
- 70** Neben § 87 BetrVG können auch andere Mitbestimmungstatbestände relevant sein. Häufig finden sich Regelungen, nach denen sich Arbeitnehmer über die Inhalte des „Code of Conduct“ schulen lassen müssen. Dies stellt zwar keine Berufsbildung dar, die gem. §§ 96 ff., 98 BetrVG ein Mitbestimmungsrecht auslösen würde. Denkbar ist aber, hierin eine „sonstige Bildungsmaßnahme“ zu sehen ist, die nach § 98 Abs. 6 BetrVG mitbestimmungspflichtig ist. Voraussetzung ist, dass es sich nach Ausgestaltung der Schulungsmaßnahme um eine Veranstaltung mit echtem Bildungscharakter handelt. Eine bloße Informationsveranstaltung, z. B. über die Einführung des „Code of Conduct“, löst keine Mitbestimmungsrechte aus.⁶³
- 71** Für bestimmte Bereiche hat die Rechtsprechung auch ausdrücklich eine Mitbestimmung ausgeschlossen, weil den Betriebspartnern die Regelungskompetenz

57 ArbG München v. 18.11.2015, 9 BVGa 52/15, abrufbar unter BeckRS 2015, 73302.

58 BAG v. 22.7.2008, 1 ABR 40/07, NZA 2008, 1248, 1254.

59 Jarosch/Schreier, ARP 2023, 262, 268.

60 Heinmann/Flöter, ESG 2022, 138, 142.

61 Grainer/Kalle, RdA 2021, 76, 82.

62 BAG v. 22.7.2008, 1 ABR 40/07, NZA 2008,

63 Reinhard, NZA 2016, 1233, 1236.

fehlt. Notorisch ist das „Flirtverbot am Arbeitsplatz“. Regelungen über private Beziehungen im Betrieb sind aber, wie eben aufgezeigt, nicht von vornherein der Mitbestimmung entzogen.⁶⁴ Unzulässig sind auch Meldepflichten zum außerdienstlichen Verhalten und zur privaten Lebensführung von Kollegen. Vorgaben, die sich unmittelbar an Mitarbeiter richten und die private Lebensführung regeln, stellen einen Eingriff in die allgemeine Handlungsfreiheit dar, der aber im Einzelfall verhältnismäßig sein kann (z. B. Alkoholverbot vor Dienstaufnahme).⁶⁵ Der Betriebsrat muss im Rahmen der Mitbestimmung darauf achten, dass die Regelungen des „Code of Conduct“ nicht die Persönlichkeitsrechte der Arbeitnehmer verletzen.

Kein Mitbestimmungsrecht besteht schließlich bei Regelungen, die lediglich die geschuldete Arbeitsleistung konkretisieren oder bei Dokumenten, die ausschließlich die Werte des Arbeitgebers oder die Unternehmenszielen beschreiben. Der Arbeitgeber kann einen entsprechenden „Code of Conduct“ regelmäßig durch eine schlichte Weisung einführen. **72**

Soweit eine Maßnahme der Mitbestimmung unterliegt, kann der Arbeitgeber sie nur mit Zustimmung des Betriebsrats durchführen. Dies gilt auch für die Einführung eines „Code of Conduct“ und zwar selbst dann, wenn eine ausländische Rechtsordnung zwingend die Einführung eines solchen Regelwerks vorschreibt. Die Beteiligungsrechte des Betriebsrats werden nicht dadurch ausgeschlossen oder eingeschränkt, dass ausländische Bestimmungen den in Deutschland tätigen Unternehmen bestimmte Pflichten auferlegen. Dies gilt auch dann, wenn der Arbeitgeber seinen Sitz im Ausland hat. Allerdings handelt es sich bei den Vorgaben ausländischen Rechts, die das eigene Unternehmen binden, um wichtige betriebliche Belange, die der Betriebsrat nicht einfach ignorieren darf (vgl. § 2 Abs. 1 BetrVG). Notfalls muss die Einigungsstelle für einen angemessenen Ausgleich sorgen. **73**

Verletzt der Arbeitgeber ein Mitbestimmungsrecht, steht dem Betriebsrat ein Anspruch auf Unterlassung zu. Dieses Recht kann er auch mittels einer einstweiligen Verfügung durchsetzen. Außerdem kommt ein Antrag nach § 23 Abs. 3 BetrVG in Betracht: Bei „groben Verstößen“ verpflichtet das Gericht den Arbeitgeber nicht nur, die fragliche Maßnahme zu unterlassen, sondern verurteilt ihn auch für jeden Fall der Zuwiderhandlung zu einem Ordnungsgeld. **74**

Die individualrechtlichen Folgen einer Verletzung des Mitbestimmungsrechts fallen möglicherweise noch stärker ins Gewicht. Nach der „Theorie der Wirksamkeitsvoraussetzung“ sind einseitige Maßnahmen des Arbeitgebers, die das Mitbestimmungsrecht des Betriebsrats verletzen, im Verhältnis zu den Arbeitnehmern unwirksam.⁶⁶ Die Vorgaben eines einseitig eingeführten „Code of Con- **75**

64 BAG v. 22.7.2008, 1 ABR 40/07, NZA 2008, 1248, 1255.

65 Problematisch sind auch Vorgaben, die sich auch an Angehörige von Mitarbeitern richten (z. B. Verbot bestimmter Geschäfte und Anlageformen).

66 St. Rspr., BAG v. 3.12.1991, GS 2/90, NZA 1992, 749; *Fitting* u. a., BetrVG, § 87 Rn. 599.

Teil 1 Grundlagen, Erfolgsfaktoren und Handlungsstrategien

duct“ entfalten keine Bindungswirkung, sofern sie der Mitbestimmung unterliegen.⁶⁷ Missachten die Arbeitnehmer diese Vorgaben, so stellt dies keine Pflichtverletzung dar, die der Arbeitgeber sanktionieren könnte. Nimmt man die eigentlichen Ziele eines „Code of Conduct“ zum Maßstab, dürfte dieses Ergebnis alle Bemühungen um ein rechtskonformes und ethisch glaubwürdiges Auftreten am Markt *ad absurdum* führen.

⁶⁷ Köhler/Häferer, GWR 2015, 159, 161.

5. Kapitel

Hinweisgebersysteme – Aufbau und Management

I. Einleitung

Bis in die Mitte der 90er Jahre des letzten Jahrhunderts befand sich die Bekämpfung von Korruption national wie international in einem Dornröschenschlaf. So war in Deutschland zwar die inländische Korruption unter Beteiligung von Amtsträgern strafbar, die Bestechung von Amtsträgern im Ausland war jedoch nicht strafbar und dazu verwendete Beträge konnten sogar steuermindernd abgesetzt werden. Zahlreiche in Deutschland bekannt gewordene Fälle von Bestechung¹ führten aber dazu, dass das Thema „Korruptionsbekämpfung“ immer stärker Gegenstand der öffentlichen Aufmerksamkeit und zum Thema zahlreicher gesellschaftlicher Initiativen wurde. Mit dem OECD-Übereinkommen zur Bekämpfung der Bestechung wurde im Jahr 1997 ein erster multilateraler Mechanismus geschaffen und ein internationaler Standard gesetzt, der die Vertragsstaaten erstmals verpflichtete, auch die Bestechung ausländischer Amtsträger unter Strafe zu stellen und wirksam zu verfolgen.

Vor dem Hintergrund zunehmend im Fokus der Öffentlichkeit stehender Korruptionsskandale und dem daraus folgenden gesellschaftspolitischen Ziel der Korruptionsbekämpfung rückten sowohl in der Wissenschaft als auch in der Unternehmenspraxis zunehmend Möglichkeiten und Mechanismen der Gegensteuerung in den Blick. Die gesellschaftliche Bereitschaft, sich mit Korruption als Kriminalitätserscheinung einfach abzufinden,² nahm immer stärker ab. Vor diesem Hintergrund begann in den westlichen Demokratien ein mehrgleisiger Prozess,³ der die weltweite Bekämpfung von Korruption und anderer Wirtschaftskriminalität zum Ziel hatte.

Auf staatlicher Seite erfolgte eine Stärkung der staatlichen Abschreckung etwa durch die Verschärfung und Erweiterung von Sanktionsnormen⁴ und die ver-

1 So bspw. die sog. „Amigo-Affäre“ in Bayern, Korruption im Zusammenhang mit Panzerlieferung Thyssen an Saudi-Arabien, Waffenhändleraffäre „Maxwell“ im Zusammenhang mit Herrn *Karlheinz Schreiber*.

2 Vgl. hierzu auch die Veröffentlichung der sog. „Panama Papers“, die durch einen „Whistleblower“ ausgewählten Medien zugespielt wurden und zu einer erneuten regen öffentlichen Diskussion geführt haben.

3 Vgl. *Kölbl/Herold*, MschrKrim 2010, 424.

4 Vgl. hierzu bspw. die Verschärfungen durch das „Gesetz zur Bekämpfung der Korruption“ in 2015 mit Einführung des sog. Geschäftsherrenmodells. Neueste Initiative hierzu sind die laufenden Bemühungen der EU-Kommission zur Bildung einer gemeinsamen EU-Antikorruptionsstrategie, zur Verstärkung der Antikorruptionsprävention und der Harmonisierung und Verschärfung des Sanktionenrechts, [becklink 2026965](#).

stärkte Ausschöpfung der bestehenden Sanktionsmöglichkeiten.⁵ Im Bereich der (börsennotierten) Privatwirtschaft wurde verstärkt auf Selbstverpflichtungen im Rahmen der Corporate Compliance und des Deutschen Corporate Governance Kodex in Verbindung mit § 161 AktG gesetzt.⁶

- 4 Der Betrieb eines sog. „Whistleblowing“- oder Hinweisgebersystems greift bei den vorgenannten Elementen zur Vorbeugung und Aufklärung von Gesetzesverstößen auf: Durch die Entgegennahme und Prüfung von Hinweisen erfolgt eine eigene Aufklärung des Verdachts eines Verstoßes sowie dessen Abstellung durch das Unternehmen selbst. Mit der Erstattung einer Strafanzeige wird eine Sanktionierung durch staatliche Stellen ermöglicht.
- 5 Diese Selbstkontrolle im Unternehmen wirkt sich in zweierlei Hinsicht aus: Zum einen ermöglicht ein Hinweisgebersystem die Aufdeckung bereits erfolgter Normverstöße, zum anderen unterstützt das hierdurch erhöhte Entdeckungsrisiko zugleich die Prävention weiterer Zuwiderhandlungen.⁷
- 6 „Whistleblowing-Systeme“ wurden anfänglich vornehmlich im angloamerikanischen Raum etabliert.⁸ Gesetzliche Anstrengungen zur verpflichtenden Einrichtung von Hinweisgebersystemen erfolgten in der EU zunächst für einzelne regulierte Industriezweige, namentlich für die Finanzdienstleistungsbranche durch die EU-Verordnung (EU) Nr. 575/2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen, die durch das CRD IV-Umsetzungsgesetz in 2013 in Deutschland umgesetzt wurde. Außerhalb des Finanzsektors wurde der Handlungsdruck in Sachen Whistleblowing in Deutschland und den weiteren EU-Mitgliedstaaten nicht zuletzt seit den Enthüllungen durch *Edward Snowden*, die Plattform *wikileaks* und auch aufgrund der Entscheidung des Europäischen Gerichtshofs für Menschenrechte⁹ über den Fall der Altenpflegerin *Heinisch* sowie *LuxLeaks* immer drängender. Vorläufiger Schlusspunkt dieser Entwicklung war auf europäischer Ebene die Verabschiedung der Richtlinie des Europäischen Parlaments und des Rates vom 27.10.2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden.¹⁰

5 Vgl. hierzu auch die zunehmende Anzahl der Verhängung erheblicher Sanktionen gegen Unternehmen, z. B. die Verhängung eines Bußgeldes in Höhe von 870 Mio. EUR gegen die Daimler AG sowie in Höhe von 1 Mrd. EUR gegen die Volkswagen AG im Zusammenhang mit dem sog. Dieselskandal.

6 Vgl. *Kölbl/Herold*, MschrKrim 2010, 424, sowie *Benz/Klindt*, BB 2010, 2979. § 161 AktG, der eine jährliche Erklärung zum Deutschen Corporate Governance Kodex erforderlich machte, trat am 26.7.2002 in Kraft.

7 Vgl. hierzu auch *Guttenberger*, in: *Ruhmannseder/Behr/Krakow*, Hinweisgebersysteme, S. 49 f.

8 *Kölbl/Herold*, MschrKrim 2010, 424.

9 EGMR, Urt. v. 21.7.2011, 28272/08, NJW 2011, 3501 (*Heinisch/Deutschland*).

10 Richtlinie (EU) des Europäischen Parlaments und des Rates vom 23.10.2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, ABl. L 305 vom 26.11.2019, S. 17 ff. (im Weiteren abgekürzt als „WBRL“).

1. Begriffsbestimmung

Im angloamerikanischen Sprachraum wurde Whistleblowing begrifflich als „the disclosure by organization members (former or current) of illegal, immoral or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action“¹¹ definiert. Prägend für Whistleblowing ist somit, dass die Aufdeckung von in einem Unternehmen, Verband etc. bestehenden Missständen durch anonyme oder namentlich bekannte Personen erfolgt, die mit dem betroffenen Unternehmen z. B. als Arbeitnehmer, Lieferant, Kunde etc. unmittelbar verbunden sind oder waren und aufgrund dieser Beziehung über ein besonderes Wissen zu illegalen Vorkommnissen innerhalb des Unternehmens verfügen.¹² 7

Häufig wird auch im deutschsprachigen Raum der Begriff des „Whistleblowing“ verwendet und ist der Betrieb eines „Whistleblowing-Systems“ gängiger Sprachgebrauch.¹³ Hierbei geht der Ausdruck „Whistleblowing“ auf das Signal einer Pfeife zurück, die vor einer drohenden Gefahr warnt oder eine Tätigkeit abrupt stoppt.¹⁴ Allerdings ist nicht zu verkennen, dass dieser Begriff gerade im deutschsprachigen Raum lange Zeit auch eine negative Konnotation aufwies, wurde er lange Zeit doch häufig auch mit „verpfeifen“¹⁵ oder „denunzieren“ durch den Meldenden in Verbindung gebracht.¹⁶ Diese Konnotation dürfte infolge des oben beschriebenen allgemeinen Bewusstseinswandels und der mittlerweile EU-weit erfolgten gesetzlichen Verankerung von „Whistleblowing-Systemen“ nunmehr endgültig der Vergangenheit angehören. 8

2. Gründe für die Einführung eines Hinweisgebersystems („Whistleblowing-Systems“)

Unabhängig von der mittlerweile bestehenden gesetzlichen Pflicht zur Einrichtung eines Hinweisgebersystems für Unternehmen auch in Deutschland sprachen und sprechen zahlreiche weitere Gründe für die Einrichtung eines Hinweisgebersystems. Im Ergebnis wird die Einrichtung eines solchen Hinweisgebersystems als elementarer Bestandteil eines effektiven Compliance-Management-Systems angesehen.¹⁷ Dies wird bestätigt durch die zwischenzeitlich ergangene höchst- 9

11 Kölbl/Herold, MschrKrim 2010, 424 (u. a. unter Verweis auf Miceli, Near & Dworkin, Explaining the Whistle-Blowing Process: Suggestions from Power Theory and Justice Theory, 1993, 394).

12 Zu den Merkmalen des Phänomens Whistleblowing auch Rotsch/Wagner, in: Rotsch, Criminal Compliance, § 34 C Rn. 3 ff.

13 Vgl. Mahnhold, NZA 2008, 737; Schmidl, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, Rn. 345.

14 Fritz, in: Maschmann, Corporate Compliance, S. 111.

15 Vgl. Wybitul, ZD 2011, 118.

16 Vgl. zur negativen Konnotation vor dem geschichtlichen Hintergrund auch Bock, Criminal Compliance, S. 734.

17 Moosmayer, in: Rotsch, Criminal Compliance, § 34 C Rn. 98.

richterliche Rechtsprechung. So hat der 5. Strafsenat des BGH in seiner Entscheidung vom 27.4.2022 ausdrücklich bestätigt, dass die Einführung eines Hinweisgebersystems bei der Sanktionierung vorhergehender Verstöße strafmildernd zu berücksichtigen ist:

„Das LG hat sich zutreffend an den Maßstäben des § 17 Abs. 3 OWiG orientiert, namentlich an der Bedeutung der Anlasstat und dem Ausmaß der dem Angekl. K. vorzuwerfenden Pflichtverletzungen sowie an den wirtschaftlichen Verhältnissen der Nebenbeteiligten (vgl. BGH, Urteil vom 18. Mai 2017 – 3 StR 103/17, NJW 2017, 2565). Zudem hat es den anschließenden Selbstreinigungsprozess der Nebenbeteiligten (u. a. Einführung umfassender Compliance-Maßnahmen und eines Hinweisgebersystems) zu Recht honoriert.“¹⁸

- 10 Bereits 2017 hatte der BGH betont, dass es bei der Bemessung von Geldbußen erheblich sei, ob und inwieweit ein Unternehmen ein effizientes Compliance-Management-System zur Vorbeugung gegen Gesetzesverstöße installiert oder nach Bekanntwerden der Rechtsverstöße optimiert habe.¹⁹
- 11 In der Vergangenheit ließ sich feststellen, dass unabhängig von der Einrichtung eines solchen Systems jedes Unternehmen Hinweise oder Beschwerden erhielt. Dabei wurden von den jeweiligen Hinweisgebern²⁰ beliebige Ansprechpartner ausgewählt: vom Vorstand/der Geschäftsführung oder dem Aufsichtsrat des Unternehmens über den Betriebsrat, die Personal-, Rechts- oder Compliance-Abteilung bis hin zu den jeweiligen Vorgesetzten oder aufgrund anderer Umstände bekannten Personen, die für das Unternehmen arbeiten. Darüber hinaus wandten sich Hinweisgeber unter Umständen sofort an die Öffentlichkeit, sei es an die Presse oder über eine entsprechende Kommunikation der Vorwürfe in den sozialen Medien. Da, wie noch nachstehend gezeigt wird, der gesetzliche Hinweisgeberschutz jedenfalls in Deutschland von der Abgabe eines Hinweises über den gesetzlich definierten zulässigen Meldeweg abhängt und die oben genannten potenziellen Ansprechpartner hierzu (häufig) nicht gehören, bleibt für die Zukunft abzuwarten, ob die bisherigen Ansprechpartner weiterhin im gleichen Umfang wie bislang durch Hinweisgeber kontaktiert werden.
- 12 Die Einrichtung eines Hinweisgebersystems kann sowohl den Mitarbeitern des Unternehmens als auch Dritten wie beispielsweise Kunden oder Lieferanten eine Möglichkeit der Hinweisabgabe bieten, die eine besondere Vertraulichkeit und die Bearbeitung durch speziell geschulte Fachleute sicherstellt²¹ und so sowohl für das Unternehmen wie für den Hinweisgeber vorteilhaft ist. So kann die Exis-

18 BGH, Beschl. v. 27.4.2022 – 5 StR 278/21, Rn. 30.

19 BGH, BeckRS 2017, 114578, Rn. 118.

20 Zur besseren Lesbarkeit wird nachfolgend die grammatikalisch männliche Form „Hinweisgeber“ für hinweisgebende Personen jedweden Geschlechts verwendet.

21 Vgl. hierzu auch *Moosmayer*, in: Rotsch, Criminal Compliance, § 34 C Rn. 98 sowie die diesbezüglichen Anforderungen in der WBRL.

tenz eines Hinweisgebersystems im Unternehmen dazu beitragen, dass sich Mitarbeiter nicht vorrangig an die Medien wenden oder Strafanzeige erstatten, sondern zunächst den internen Weg beschreiten, um Gesetzesverstöße bekannt zu machen und so zu versuchen, Missstände zunächst innerbetrieblich beizulegen. Die Priorisierung interner Meldewege ist sowohl ausdrückliches Ziel der WBRL als auch von deren Umsetzung im deutschen HinSchG.

Darüber hinaus ermöglichen Erkenntnisse, die aus eingegangenen Hinweisen resultieren, dass bereits in einem frühen Stadium Gegensteuerungsmaßnahmen gegen unternehmensbezogenes Fehlverhalten Einzelner oder möglicherweise bestehende Prozessschwächen im Unternehmen eingeleitet werden können.²² **13**

Gerade für die Korruptionsbekämpfung ist der Betrieb eines Hinweisgebersystems von besonderer Bedeutung, weil bei Korruptionsdelikten von einem hohen Dunkelfeld auszugehen ist. Korruptionsdelikte sind typischerweise durch eine Täter-Täter-Beziehung gekennzeichnet (sog. „opferloses Heimlichkeitsdelikt“). Der Sachverhalt der Korruption zeichnet sich (unjuristisch gesprochen) dadurch aus, dass eine Person eine andere dafür bezahlt, dass sie etwas bekommt, was ihr nicht zusteht. Beide Beteiligte profitieren von der Tathandlung und werden sich so gemeinsam darum bemühen, dass das Tatgeschehen verdeckt wird.²³ Somit sind sowohl der „gebende“ als auch der „nehmende“ Teil Täter des vorgeworfenen Verhaltens. **14**

Zudem zeigt die Praxis, dass einige gerade in der (jüngeren) Vergangenheit bekannt gewordene Korruptionsskandale, Fälle von Gestaltungsmissbrauch im Steuerrecht oder auch andere erhebliche Missstände ohne die Hinweise von Mitarbeitern, Lieferanten oder Kunden nicht aufgedeckt worden wären.²⁴ Gleichwohl existierten lange Zeit auch Stimmen, die die praktische Relevanz und insbesondere den Erfolg eines Hinweisgebersystems eher gering einschätzten.²⁵ **15**

3. Aktuelle Rechtliche Rahmenbedingungen

a) Internationale Anforderungen

Auf internationaler Ebene existieren zahlreiche Regelungen, aus denen sich unmittelbar oder mittelbar das Erfordernis des Betreibens eines funktionierenden Hinweisgebersystems ergibt (siehe hierzu nachfolgend → Rn. 17–24). Hierzu gehört neben der Einrichtung eines solchen Systems auch eine angemessene Do- **16**

22 Hierzu auch *Guttenberger*, in: Ruhmannseder/Behr/Krakow, Hinweisgebersysteme, S. 49 f.

23 *Altenburg*, Bucerius Law Journal 2008, 3.

24 *Wybitul*, ZD 2011, 118; *Zimmer/Seebacher*, CCZ 2013, 31; als Beispiel der jüngeren Vergangenheit kann hierzu auch der Fall zweier Mitarbeiter eines Apothekers genannt werden, die aufdeckten, dass der Apotheker „gepanschte“ Krebsmedikamente verkaufte, vgl. hierzu beispielsweise <https://www.zeit.de/2018/22/whistleblower-wirtschaftsskandale-schutz-eu-richtlinien> (zuletzt abgerufen am 4.5.2024); durch den EGMR wurde Anfang 2023 bestätigt, dass erst der Hinweis des Whistleblowers die Aufdeckung der „LuxLeaks“-Affäre ermöglichte, EGMR, NZA 2023, 555, Rn. 187, 189.

25 Etwa *Hefendehl*, in: Hefendehl, FS Amelung, S. 621 ff.

kumentation des Vorgehens bei Eingang eines Hinweises sowie der zu treffenden Entscheidungen und Konsequenzen. Dabei waren es besonders Entwicklungen im angelsächsischen Recht, die auf überstaatliche Regelungen in der OECD und der Europäischen Union ausstrahlten und der Einrichtung von Hinweisgebersystemen internationale Dynamik verliehen.

aa) Sarbanes-Oxley Act (SOX) (USA)

- 17** Von entscheidender Bedeutung für die Notwendigkeit des Betriebs eines Hinweisgebersystems ist – in dessen Geltungsbereich – Sec. 301 des SOX.²⁶ Gemäß Sec. 301 SOX ist in einem Unternehmen ein sogenanntes Audit Committee zu bilden, das für die Überwachung der Ordnungsmäßigkeit der Rechnungslegung und Abschlussprüfung verantwortlich ist. Im Rahmen dessen enthält Art. 301 SOX die Verpflichtung, Verfahren einzurichten, die eine vertrauliche, anonyme Meldung von Bedenken durch Angestellte in Bezug auf mögliches Fehlverhalten ermöglichen. Hieraus ergibt sich das Erfordernis der Einrichtung eines Systems zur vertraulichen – ausdrücklich auch anonymen – Anzeige von möglichem Fehlverhalten, das jedoch allein auf die Bereiche der Rechnungslegung und der Abschlussprüfung beschränkt ist. Genauere Vorgaben, wie das Hinweisgebersystem zu betreiben ist, enthalten die Regelungen des SOX nicht.

bb) Dodd-Frank Act (USA)

- 18** Nach Sec. 922 des Dodd-Frank Act haben Hinweisgeber, die der US-amerikanischen Börsenaufsichtsbehörde (SEC) „originäre Informationen“ liefern, Anspruch auf eine Belohnung, sofern die von dem Hinweisgeber abgegebene Information zur Aufdeckung von Verstößen gegen amerikanische Wertpapiergesetze führen. Zu diesen Gesetzen gehören auch die Vorschriften des Sarbanes-Oxley Act (SOX) und des Foreign Corrupt Practices Act (FCPA), der die Strafbarkeit der Bestechung ausländischer Amtsträger regelt. Darüber hinaus sieht Sec. 922 den Schutz von Hinweisgebern, zum Beispiel vor Kündigungen durch den Arbeitgeber, vor.
- 19** Das auf der Grundlage der Sec. 922 umgesetzte Whistleblower-Programm der SEC hat vorrangig zum Ziel, natürliche Personen zu belohnen,²⁷ die frühzeitig handeln, um Verstöße offenzulegen, und bedeutende Hinweise liefern, die es der SEC ermöglichen, erfolgreiche Ermittlungsverfahren zu führen. Um für eine Belohnung durch die SEC in Betracht zu kommen, bestimmt das genannte Programm, dass der Hinweisgeber der SEC freiwillig originäre Informationen liefert, die zu einer erfolgreichen Durchsetzung eines Verfahrens vor einem

²⁶ Zu den Anforderungen des SOX vgl. auch von Zimmermann, WM 2007, 1060 ff.; Marsch-Barner, ZHR 181, 847, 848.

²⁷ Gerade diese Vorschriften führen auch in Deutschland immer wieder zu Diskussionen über die Einführung einer Belohnung/Prämie für Hinweisgeber, so etwa auf der von Transparency International veranstalteten Tagung zu Hinweismanagementsystemen; vgl. hierzu allgemein sowie speziell zu den Regelungen in den USA Granetznj/Krause, CCZ 2020, 29 ff.

Bundesgericht oder eines behördlichen Verfahrens durch die SEC führen, in dem die SEC Geldstrafen von insgesamt mehr als 1 Mio. USD erhält. Soweit diese Voraussetzungen erfüllt sind, wird der Hinweisgeber im Rahmen eines sog. Bounty-Programms in Höhe von mindestens 10% bis zu maximal 30% an den sog. „monetary sanctions“ beteiligt.²⁸ Die konkrete Höhe der Prämie liegt im Ermessen der Behörde.

Nach den Ausführungsbestimmungen der SEC²⁹ ist es nicht erforderlich, dass Arbeitnehmer, die einen Hinweis an die SEC abgeben, diese Informationen zunächst intern an den Arbeitgeber melden. Die Ausführungsbestimmungen verstärken jedoch den Anreiz für den Hinweisgeber, sich zunächst an das interne Hinweismanagement eines Unternehmens zu wenden, wenn dies angemessen ist. So sehen die Regelungen vor, dass ein Hinweisgeber auch dann für eine Belohnung in Frage kommt, wenn er intern seine Informationen an den Arbeitgeber weitergibt und das Unternehmen selbst die SEC über die Verstöße unterrichtet.

Schließlich stellt die freiwillige Beteiligung des Whistleblowers an dem internen Hinweismanagement einen Faktor dar, der den Betrag der Belohnung erhöhen kann, wohingegen die Nicht-Weitergabe der Information an das interne Hinweismanagement zu einer Verringerung des Betrages führen kann.³⁰

cc) UK Bribery Act³¹ (Großbritannien)

Der im Jahr 2011 in Kraft getretene UKBA verlangt von Unternehmen, geeignete Maßnahmen zur Verhinderung von Bestechung zu ergreifen.³² Das betroffene Unternehmen kann sich nach den Regelungen des UKBA nur dann einer Haftung im Falle eines Verstoßes entziehen, wenn es nachweisen kann, dass es angemessene Verfahren („adequate procedures“) im Unternehmen umgesetzt hat, durch die Korruption verhindert werden soll.³³

28 Zum sog. „Bounty-Programm“ der SEC s. auch *Schürle/Fleck*, CCZ 2011, 218 f.; *Marsch-Barner*, ZHR 181, 847, 848. Im Jahr 2018 wurden nach den Vorgaben des Dodd-Frank Act 138 Mio. USD an insgesamt 13 Hinweisgeber ausgezahlt, vgl. SEC 2018 Annual Report to Congress, Whistleblower Programm, S. 9, <https://www.sec.gov/files/sec-2018-annual-report-whistleblower-program.pdf> (zuletzt abgerufen am 11.3.2024); im Jahr 2019 waren es 60 Mio. USD, die an 8 Hinweisgeber ausgezahlt wurden, vgl. SEC 2019 Annual Report to Congress, Whistleblower Programm, S. 9, <https://www.sec.gov/files/sec-2019-annual-report-whistleblower-program.pdf> (zuletzt abgerufen am 11.3.2024). Im Mai 2023 zahlte die SEC 279 Mio. USD an einen einzelnen Whistleblower, <https://www.sec.gov/news/press-release/2023-89> (zuletzt abgerufen am 23.4.2024).

29 Die als „final rules“ zu findenden Ausführungsbestimmungen sind abrufbar unter <https://www.sec.gov/files/rules/final/2022/34-95620.pdf> (zuletzt abgerufen am 23.4.2024).

30 Siehe Ziffern 21F-4(b)(7) und 21F-4(c) sowie 21F-6 (a) (4) der Ausführungsbestimmungen.

31 Im folgenden UKBA.

32 Siehe http://www.legislation.gov.uk/ukpga/2010/23/pdfs/ukpga_20100023_en.pdf (zuletzt abgerufen am 11.3.2024), vgl. dort Sec. 7.

33 Siehe http://www.legislation.gov.uk/ukpga/2010/23/pdfs/ukpga_20100023_en.pdf (zuletzt abgerufen am 11.3.2024), vgl. dort sec. 7 (2).

- 23** Anhaltspunkte dafür, was unter diesen „geeigneten Maßnahmen“ zu verstehen ist, enthält die „Guidance“ des Ministry of Justice.³⁴ Unter dem dortigen „5. Prinzip“ wird ausgeführt, dass die Unternehmensorganisation ein Hinweisgebersystem zu implementieren und Strukturen zur Untersuchung von Hinweisen zu schaffen hat. Einzige Möglichkeit, eine Strafbarkeit des Unternehmens nach Sec. 7 UKBA zu vermeiden, ist der Beweis der Implementierung geeigneter Maßnahmen zur Verhinderung der Korruptionshandlung und damit der Nachweis, dass es sich bei der begangenen Korruptionshandlung nicht um ein „systemisches Ereignis“ im Unternehmen handelt, sondern um einen Ausnahmefall. Sollte dieser Nachweis nicht möglich sein, kann dies zu erheblichen Sanktionen gegen das Unternehmen führen. Diese Sanktionen können in Geldstrafen in unbegrenzter Höhe, der Möglichkeit von Schadenersatzklagen sowie der Sperrung für Regierungsaufträge/öffentliche Ausschreibungen bestehen. So enthält Nr. 2.3 des sog. „Principle 2 Top-level commitment“ die Empfehlung zur Einrichtung von Mechanismen zur „protection and procedures for confidential reporting of bribery (whistle-blowing)“.³⁵ In die gleiche Richtung geht Nr. 1.7 des „Principle 1 Proportionate Procedures“, wonach die Einrichtung von Hinweisgebersystemen zu den geeigneten Vorbeugungsmaßnahmen gegen Korruption gehört.
- 24** Von entscheidender Bedeutung zur Vermeidung einer Strafbarkeit des Unternehmens gemäß Sec. 7 UKBA kann somit der Nachweis sein, dass eingehende Hinweise auf Korruption angemessen verfolgt werden; hierbei sind sowohl das Vorgehen als auch die getroffenen Entscheidungen angemessen zu dokumentieren.

dd) OECD-Übereinkommen vom 17.12.1997

- 25** Staatenübergreifend ergab sich auch im Zusammenhang mit den gewachsenen Anforderungen an die grenzüberschreitende Korruptionsbekämpfung durch das OECD-Übereinkommen über die Bekämpfung der Bestechung ausländischer Amtsträger im internationalen Geschäftsverkehr vom 17.12.1997 eine rechtliche Verpflichtung zur Einrichtung von verstärkten Kontrollmechanismen.³⁶ Diese wurden im Rahmen der OECD u. a. durch die „Leitlinien für empfehlenswerte Verfahrensweisen in den Bereichen interne Kontrollsysteme, Ethik und Compliance“ vom 18.2.2010 zur weiteren Bekämpfung der Bestechung ausländischer Amtsträger im internationalen Geschäftsverkehr konkretisiert: deren Ziffer 11

34 Siehe <https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf> (zuletzt abgerufen am 11.3.2024).

35 Nr. 2.3 des Principle 2 der Guidance to Bribery Act 2010.

36 Vgl. hierzu auch Stellungnahme 1/2006 der Art. 29-Datenschutzgruppe zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität, S. 8.

regelt die Einrichtung von Verfahren, die die Abgabe von vertraulichen Meldungen ermöglichen.³⁷

b) Rechtslage in Deutschland

Seit dem 2.7.2023 existiert mit dem „Gesetz für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden“³⁸ auch in der deutschen Rechtsordnung **eine generelle** unmittelbare Pflicht zur Einrichtung eines Hinweisgebersystems für alle privaten und öffentlichen Unternehmen, die mehr als 249 Personen beschäftigen. Seit dem 17.12.2023 gilt diese Verpflichtung sogar für alle Unternehmen mit mindestens 50 Beschäftigten.³⁹ **26**

Davor enthielten bereits einige Spezialgesetze die Verpflichtung für Unternehmen bzw. Behörden, Meldungen zu ermöglichen. **27**

So wurde schon in 2014 beispielsweise für Kreditinstitute mit § 25a Abs. 1 Satz 6 Nr. 3 KWG eine spezielle gesetzliche Regelung geschaffen, die die Einführung eines Hinweisgebersystems vorsieht.⁴⁰ § 25a Abs. 1 Satz 6 Nr. 3 KWG bestimmt, dass eine ordnungsgemäße Geschäftsorganisation von Instituten einen Prozess umfasst, der es den Mitarbeitern unter Wahrung der Vertraulichkeit ihrer Identität ermöglicht, potenzielle oder tatsächliche Verstöße gegen bestimmte, im einzelnen benannte EU-Verordnungen, das KWG und die dazu erlassenen Rechtsverordnungen sowie sonstige strafbare Handlungen innerhalb des Unternehmens an geeignete Stellen zu melden. **28**

Entsprechende Vorgaben enthalten § 28 Abs. 1 Satz 2 Nr. 9 KAGB für Kapitalverwaltungsgesellschaften sowie § 23 Abs. 6 VAG für Versicherungsgesellschaften. **29**

Des Weiteren regelt § 4d FinDAG eine Verpflichtung für die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), ein System zur Annahme von Meldungen über potenzielle oder tatsächliche Verstöße gegen Gesetze, Rechtsverordnungen, Allgemeinverfügungen und sonstige Vorschriften sowie Verordnungen und Richtlinien der Europäischen Union, bei denen es die Aufgabe der Bundesanstalt ist, deren Einhaltung durch die von ihr beaufsichtigten Unternehmen und Personen sicherzustellen oder Verstöße dagegen zu ahnden, einzurichten. § 4d Abs. 1 Satz 2 FinDAG sieht ausdrücklich vor, dass Meldungen auch anonym abgegeben werden können. Darüber hinaus ist in § 4d Abs. 6 FinDAG geregelt, dass eine Meldung abgebende Mitarbeiter von beaufsichtigten Unternehmen weder nach arbeits- oder strafrechtlichen Vorschriften verantwortlich gemacht **30**

37 Abrufbar unter https://www.oecd.org/berlin/themen/Annex%20II_Internal%20Control_GER.pdf (zuletzt abgerufen am 17.1.2024).

38 Im Folgenden als „Hinweisgeberschutzgesetz“ oder „HinSchG“ bezeichnet.

39 Zu den Vorgaben des HinSchG siehe die nachstehende Darstellung in → Rn. 38 ff.

40 Zu den ersten Erfahrungen mit § 25a KWG, *Renz/Rohde-Liebenau*, BB 2014, 692 ff.

noch zum Ersatz von Schäden herangezogen werden dürfen, es sei denn, die Meldung wurde vorsätzlich oder grob fahrlässig unwahr abgegeben.

- 31 Entsprechende Regelungen finden sich in § 3b BörsG, § 53 GwG.
- 32 Schließlich ergeben sich darüber hinaus auch aus einer Reihe einzelner Regelungen Anhaltspunkte für die Notwendigkeit des Betriebs eines Hinweisgebersystems, die sich als Folge der allgemein angenommenen Pflicht eines Unternehmens zu geeigneten Compliance-Maßnahmen herleiten lassen.

aa) Gesellschaftsrechtliche Vorgaben

- 33 Ein wesentlicher Grund für die Durchführung von Compliance-Maßnahmen folgt aus der Legalitätspflicht der Unternehmensleitung gemäß §§ 91 Abs. 2, 93 AktG bzw. § 43 GmbHG. Die jeweilige Unternehmensleitung ist nach diesen Normen verpflichtet, dafür Sorge zu tragen, dass das von ihr geführte Unternehmen nicht gegen Gesetze verstößt. Die Einrichtung von Hinweisgebersystemen ist hierfür ein mittlerweile höchstrichterlich anerkanntes geeignetes Instrument zur Erfüllung dieser Pflicht (→ Rn. 9 f.).

bb) Ordnungswidrigkeitenrechtliche Vorgaben

- 34 Auch eine Norm aus dem Ordnungswidrigkeitenrecht (§ 130 OWiG), hat entscheidende Auswirkungen auf die Verpflichtung der Unternehmensleitung, Zuwiderhandlungen gegen Gesetze zu verhindern.⁴¹ § 130 Abs. 1 Satz 1 OWiG bestimmt ausdrücklich, dass der Inhaber eines Betriebes oder Unternehmens dann eine Ordnungswidrigkeit begeht, wenn er vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen solche straf- oder bußgeldbewehrte Pflichten des Inhabers zu verhindern. Aus dieser Norm ergibt sich, dass die Unternehmensleitung diejenigen Aufsichtsmaßnahmen durchzuführen hat, die erforderlich sind, um Ordnungswidrigkeiten und Straftaten aus dem Unternehmen heraus zu verhindern. Die Erfüllung dieser Pflicht erfordert jedoch, dass die Unternehmensleitung über diejenigen Risiken informiert ist, denen sich das Unternehmen ausgesetzt sieht; einen wesentlichen Beitrag zur Entdeckung dieser Risiken kann der Betrieb eines Hinweisgebersystems leisten. Die Unterlassung der notwendigen organisatorischen Maßnahmen ist für das Unternehmen nicht nur wegen der drohenden Strafen so gefährlich, sondern vor allem auch wegen der damit möglichen Abschöpfung sämtlicher wirtschaftlichen Vorteile, die das Unternehmen aus dem illegalen Verhalten seiner Mitarbeiter gezogen hat (§ 17 Abs. 4 OWiG).

41 Siehe hierzu → Böttger, Kap. 2 Rn. 29.

cc) Vorgaben des Deutschen Corporate Governance Kodex

Darüber hinaus sieht auch der Deutsche Corporate Governance Kodex⁴² eine Verpflichtung zur Implementierung von Compliance-Maßnahmen vor, da in Grundsatz 5 die Vorgabe enthalten ist, dass der Vorstand für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und auf deren Beachtung durch die Unternehmen hinzuwirken hat (Compliance). Des Weiteren enthält die Empfehlung und Anregung A 2 die Aufforderung an den Vorstand, für ein an der Risikolage des Unternehmens ausgerichtetes Compliance-Management-System zu sorgen und dessen Grundzüge offenzulegen. Auch soll den Beschäftigten auf geeignete Weise die Möglichkeit eingeräumt werden, geschützt Hinweise auf Rechtsverstöße im Unternehmen zu geben; auch Dritten soll nach den Kodex-Regelungen diese Möglichkeit eingeräumt werden. **35**

Über § 161 AktG erlangt der Kodex eine rechtliche Verbindlichkeit, als Vorstand und Aufsichtsrat einer börsennotierten Gesellschaft jährlich erklären müssen, dass sie den Empfehlungen entsprechen, oder aber darlegen müssen, warum die Gesellschaft welche Empfehlungen nicht angewendet hat. **36**

dd) Vorgaben aus der Rechtsprechung

Darüber hinaus hebt auch eine Entscheidung des EGMR vom 21.7.2011⁴³ die Wichtigkeit von Hinweisen von Mitarbeitern auf mögliche Straftaten auch im Hinblick auf das Recht auf freie Meinungsäußerung gemäß Art. 10 EMRK hervor. Von besonderem Interesse ist auch, dass der EGMR nicht nur die Interessen der betroffenen Arbeitnehmerin in seiner Entscheidung berücksichtigt, sondern darüber hinaus auch darauf verweist, dass durch Kündigungen, die wegen Strafanzeigen gegen den eigenen Arbeitgeber ausgesprochen werden, ein Einschüchterungseffekt gegenüber anderen Arbeitnehmern erzielt werde.⁴⁴ Insbesondere wird durch das Urteil auch die Bedeutung des internen Whistleblowings deutlich. Der EGMR betonte in seiner Urteilsfindung nämlich, dass die dortige Klägerin vor Erstattung der Strafanzeige zunächst mehrfach durch interne Mitteilungen an den Arbeitgeber auf die bestehenden Missstände hingewiesen hatte.⁴⁵ Da Hinweisgebersysteme eine wertvolle Hilfestellung zum Abgeben solcher Hinweise und damit auch zur Ausübung des Rechts auf freie Meinungsäußerung darstellen, ergab sich auch aus der genannten Entscheidung des EGMR ein erheblicher Handlungsdruck für Unternehmen, Hinweisgebersysteme zur Förderung und Entgegennahme interner Hinweise einzurichten. **37**

42 Die aktuelle Fassung des DCGK vom 28.4.2022 wurde am 27.6.2022 durch das BMJV im Bundesanzeiger veröffentlicht, <https://www.dcgk.de/de/kodex.html> (zuletzt abgerufen am 24.4.2024).

43 EGMR, 21.7.2001, 28274/08, NJW 2011, 3501.

44 Vgl. hierzu auch *Ulber*, NZA 2011, 963.

45 EGMR, NJW 2011, 3502.

II. Die Vorgaben des deutschen Hinweisgeberschutzgesetzes

- 38 Nach langen, zum Teil sehr kontrovers geführten Diskussionen und zahlreichen Verhandlungen innerhalb des Trilogverfahrens wurde durch den Ministerrat der EU die „Richtlinie des Europäischen Parlaments und des Rates vom 27.10.2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden“ (WBRL) verabschiedet.⁴⁶
- 39 Die nationalen Gesetzgeber hatten nach der Veröffentlichung der Richtlinie im Amtsblatt der Europäischen Union am 16.12.2019 zwei Jahre Zeit, die Richtlinie in nationales Recht umzusetzen. Die Umsetzung erfolgte in den einzelnen Mitgliedstaaten insgesamt sehr verzögert. Nach Ablauf der Umsetzungsfrist am 17.12.2021 richtete die EU-Kommission im Januar 2022 Aufforderungsschreiben an 24 Mitgliedstaaten, die die WBRL noch nicht oder nur unzureichend in nationales Recht umgesetzt hatten.⁴⁷ Auch der deutsche Gesetzgeber hielt die Umsetzungsfrist nicht ein, da sich die damals regierende große Koalition nicht auf ein Umsetzungsgesetz einigen konnte.⁴⁸ Die EU-Kommission leitete daraufhin gegen Deutschland und vier weitere Mitgliedstaaten ein Vertragsverletzungsverfahren vor dem Gerichtshof der Europäischen Union ein.⁴⁹ Nachdem die neue Bundesregierung im November 2021 eine weitreichende Umsetzung der WBRL im Koalitionsvertrag angekündigt hatte,⁵⁰ dauerte es noch bis zum 2.6.2023, bis das deutsche Hinweisgeberschutzgesetz verkündet wurde.⁵¹ Das HinSchG trat zum 2.7.2023 in Kraft.

1. Ziel des Gesetzes

- 40 Gemäß § 1 Abs. 1 HinSchG regelt das Gesetz den Schutz von natürlichen Personen, die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese an die nach dem Gesetz vorgesehenen Meldestellen melden oder offenlegen. Des Weiteren werden Personen geschützt, die Gegenstand einer Meldung oder Offenlegung sind, sowie sonstige Personen, die von einer Meldung oder Offenlegung betroffen sind (§ 1 Abs. 2 HinSchG). Der Schutzzweck geht zurück auf Art. 1 der WBRL, wonach **sichere Wege für das Melden von Verstößen gegen Uni-**

46 Vgl. zur Entstehungsgeschichte der WBRL und zum Entwurf der Europäischen Kommission vom 23.4.2018 *Thüsing/Rombey*, NZG 2018, 1001 ff.; *Gerdemann*, RdA 2019, 16.

47 Eine Übersicht zur Umsetzung der WBRL findet sich auf <https://www.whistleblowingmonitor.eu/> (Stand: 1.3.2024).

48 Zum Gesetzgebungsverfahren in Deutschland ausführlich *Lüneborg*, ZIP 2023, 941 ff.

49 Vgl. https://germany.representation.ec.europa.eu/news/aktuelle-vertragsverletzungsverfahren-klage-gegen-deutschland-wegen-mangelnden-schutzes-von-2023-02-15_de (Stand: 1.3.2024).

50 Koalitionsvertrag zwischen SPD, FDP und Bündnis 90/Die Grünen (abrufbar z.B. unter https://www.fdp.de/sites/default/files/2021-11/Koalitionsvertrag%202021-2025_0.pdf) (Stand: 12.3.2024), S. 111.

51 Zum Gesetzgebungsverfahren in Deutschland ausführlich *Lüneborg*, ZIP 2023, 941 ff.

onsrecht eröffnet werden und **Hinweisgeber vor Vergeltungsmaßnahmen** wie Kündigungen oder anderen Repressalien geschützt werden sollten.

2. Überblick über den Inhalt des Hinweisgeberschutzgesetzes

Neben Regelungen zum sachlichen Anwendungsbereich, den Begriffsbestimmungen und der Abgrenzung zu anderen Vorschriften⁵² enthält das HinSchG im Kern Bestimmungen über die Pflicht zur Einrichtung von (unternehmens-)internen und externen (behördlichen) Meldestellen, zum Verfahren der Entgegennahme und Bearbeitung von internen und externen Meldungen sowie zu den zu ergreifenden Folgemaßnahmen,⁵³ Bestimmungen zur möglichen direkten Offenlegung der Meldung durch den Hinweisgeber⁵⁴ sowie die zugunsten der Hinweisgeber vorgesehenen Schutzmaßnahmen.⁵⁵ **41**

Neben der Verpflichtung für private und öffentliche Unternehmen und Behörden, eine interne Meldestelle nebst funktionierendem Whistleblowing-Management einzuführen, sind die im Hinweisgeberschutzgesetz erstmals vorgesehenen umfangreichen Schutzmaßnahmen zugunsten von Hinweisgebern die entscheidenden Bestimmungen des Gesetzes. **42**

3. Sachlicher Anwendungsbereich

Das Hinweisgeberschutzgesetz dient dem Schutz von Personen, die Verstöße gegen die in § 2 genannten Vorschriften melden oder offenlegen. **43**

Der sachliche Anwendungsbereich des HinSchG ist eröffnet, wenn strafbewehrte Verstöße gemeldet werden (§ 2 Abs. 1 Nr. 1 HinSchG). Damit sind insbesondere Verstöße gegen das StGB und andere Strafvorschriften vollständig erfasst. Des Weiteren fallen auch bußgeldbewehrte Verstöße in den sachlichen Anwendungsbereich, soweit die verletzte Vorschrift dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient (§ 2 Abs. 1 Nr. 2 HinSchG). Hierdurch hat der Gesetzgeber von der in Art. 2 Abs. 2 WBRL eingeräumten Möglichkeit Gebrauch gemacht, den Schutz nach nationalem Recht in Bezug auf Bereiche oder Rechtsakte **auszuweiten**, die nicht unter den durch die Richtlinie benannten Schutzbereich fallen (sog. „**Gold-Plating**“). **44**

In § 2 Abs. 1 Nr. 3 werden in einem umfangreichen Katalog Verstöße gegen Rechtsvorschriften des Bundes und der Länder sowie unmittelbare Rechtsakte der Europäischen Union in den sachlichen Anwendungsbereich aufgenommen.⁵⁶ Dies sind insbesondere Vorschriften betreffend **45**

⁵² Abschnitt 1 des HinSchG.

⁵³ Abschnitt 2 des HinSchG.

⁵⁴ Abschnitt 3 des HinSchG.

⁵⁵ Abschnitt 4 des HinSchG.

⁵⁶ Dies dient der Umsetzung von Art. 2 WBRL.

Teil 1 Grundlagen, Erfolgsfaktoren und Handlungsstrategien

- Geldwäsche und Terrorismusfinanzierung,
- öffentliche Auftragsvergabe,
- Finanzdienstleistungen, Finanzprodukte und Finanzmärkte,
- Produktsicherheit und -konformität,
- Verkehrssicherheit,
- Umweltschutz,
- Strahlenschutz und kerntechnische Sicherheit sowie zur Förderung der Nutzung von Energie aus erneuerbaren Quellen und der Energieeffizienz,
- Lebensmittel- und Futtermittelsicherheit, Tiergesundheit und Tierschutz,
- Qualitäts- und Sicherheitsstandards von Arzneimitteln und Medizinprodukten,
- öffentliche Gesundheit,
- Verbraucherrechte und Verbraucherschutz,
- Schutz der Privatsphäre und personenbezogener Daten sowie Sicherheit von Netz- und Informationssystemen,
- Rechte von Aktionären,
- Buchführung, Rechnungslegung und Abschlussprüfung von Unternehmen,
- Steuerrecht,
- Kartell- und Wettbewerbsrecht,
- finanzielle Interessen der Union im Sinne von Art. 325 AEUV sowie den genaueren Definitionen in einschlägigen Unionsmaßnahmen und
- Binnenmarktvorschriften i. S. v. Art. 26 Abs. 2 AEUV, einschließlich Verstöße gegen Unionsvorschriften über Wettbewerb und staatliche Beihilfen.

4. Persönlicher Anwendungsbereich des Hinweisgeberschutzgesetzes

- 46 Das Gesetz gilt für Hinweisgeber, die im **privaten oder im öffentlichen Sektor** tätig sind und im Zusammenhang mit ihrer **beruflichen Tätigkeit Informationen über Verstöße** erlangt haben, die in den sachlichen Anwendungsbereich des Gesetzes fallen und die über die im HinSchG vorgesehenen Meldestellen melden oder offenlegen (§ 1 Abs. 1 HinSchG). Dies umfasst sowohl Verstöße bei dem Beschäftigungsgeber, bei dem die hinweisgebende Person tätig ist oder war, als auch bei anderen Stellen, mit denen die hinweisgebende Person in beruflichem Kontakt stand (§ 3 Abs. 3 HinSchG).
- 47 Hintergrund dieser Regelung ist, dass davon auszugehen ist, dass die Personen besonderen Rechtsschutz benötigen, wenn sie Informationen melden, von denen sie im Rahmen ihrer beruflichen Tätigkeit Kenntnis erlangt haben, und sich damit dem Risiko von berufsbezogenen Repressalien aussetzen. Der Grund für den Schutz dieser Personengruppe liegt somit in ihrer wirtschaftlichen Abhängigkeit von der Person, auf die sie de facto bezüglich ihrer Beschäftigung angewiesen ist.⁵⁷

57 BT-Drs. 20/3442, S. 56; vgl. auch Erwägungsgrund 36 der WBRL.

Der persönliche Anwendungsbereich ist nach dem Willen des Gesetzgebers weit zu verstehen. Entscheidend ist, ob die hinweisgebende Person die Information im Zusammenhang mit einer beruflichen Tätigkeit erlangt hat. So werden insbesondere die nachfolgend dargestellten Personengruppen vom Schutzbereich erfasst:⁵⁸ **48**

- Arbeitnehmer, darunter fallen auch in Teilzeit beschäftigte Personen,
- Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind (insb. Selbstständige⁵⁹ oder in Heimarbeit Beschäftigte),
- Leiharbeiternehmer,⁶⁰
- Auszubildende sowie bezahlte und unbezahlte Praktikanten,
- Beamte, Richter, Soldaten und andere Personen, die im öffentlichen Sektor arbeiten,⁶¹
- Anteilseigner und Personen, die dem Verwaltungs-, Leitungs- oder Aufsichtsorgan eines Unternehmens angehören,
- Freiwillige sowie
- Personen, die unter der Aufsicht und Leitung von Auftragnehmern, Unterauftragnehmern und Lieferanten arbeiten.

In den Schutzbereich einbezogen sind auch Hinweisgeber, die Informationen über Verstöße melden oder offenlegen, von denen sie im Rahmen eines inzwischen beendeten Arbeitsverhältnisses Kenntnis erlangt haben. Auch gilt das HinSchG für Hinweisgeber, deren Arbeitsverhältnis noch nicht begonnen hat und die während des Einstellungsverfahrens oder anderer vorvertraglicher Verhandlungen Informationen über Verstöße erlangt haben.⁶² **49**

Der persönliche Anwendungsbereich erstreckt sich schließlich auch auf **Mittler und Dritte**, die mit dem Hinweisgeber in Verbindung stehen und die den Hinweisgeber bei einer Meldung unterstützen oder in einem beruflichen Kontext Repressalien erlitten haben (z.B. Kollegen, Familienangehörige, Verwandte oder Freunde des Hinweisgebers) sowie juristische Personen, die im Eigentum des Hinweisgebers stehen oder für die der Hinweisgeber arbeitet (§ 34 Abs. 1 und 2 HinSchG). **50**

5. Voraussetzungen für den Schutz von Hinweisgebern

Der Schutz von Hinweisgebern gilt nicht uneingeschränkt, sondern nur unter bestimmten Voraussetzungen. Hinweisgeber werden nach § 33 Abs. 1 HinSchG geschützt, wenn **51**

⁵⁸ BT-Drs. 20/3442, S. 56 mit Verweis auf Art. 4 der WBRL.

⁵⁹ Colneric/Gerdemann, in: BeckOK HinSchG, § 3 HinSchG Rn. 50.

⁶⁰ Vgl. § 16 Abs. 1 HinSchG.

⁶¹ Erwägungsgrund 38 der WBRL.

⁶² BT-Drs. 20/3442, S. 56.

- sie intern gemäß § 17 oder extern gemäß § 28 HinSchG eine Meldung erstattet oder eine Offenlegung gemäß § 32 HinSchG vorgenommen haben,
- sie dabei **hinreichenden Grund zur Annahme** hatten, dass die **gemeldeten Informationen über Verstöße** zum **Zeitpunkt der Meldung** der **Wahrheit** entsprachen und
- diese Informationen in den **sachlichen Anwendungsbereich des Hinweisgeberschutzgesetzes** fallen.

52 Hinweisgeber genießen den gesetzlichen Schutz unabhängig davon, ob sie eine Meldung über die interne (unternehmenseigene) oder die externe Meldestelle abgeben.

a) Gemeinsame Schutzvoraussetzungen

- 53** Neben der Erfüllung der Voraussetzungen des persönlichen Anwendungsbereichs (siehe hierzu → Rn. 46–50) sind Hinweisgeber nur dann geschützt, wenn sie zum Zeitpunkt der Meldung oder Offenlegung hinreichenden Grund zur Annahme hatten, dass die von ihnen gemeldeten oder offengelegten Informationen der Wahrheit entsprachen (§ 33 Abs. 1 Nr. 2 HinSchG). Das Tatbestandsmerkmal „hinreichender Grund zur Annahme“ ist nicht rein objektiv zu betrachten, sondern setzt voraus, dass der Hinweisgeber **subjektiv** an das Vorliegen eines Verstoßes geglaubt haben muss und dass dieser Glaube zum Zeitpunkt der Informationsweiterleitung vorgelegen haben muss.⁶³ Es ist daher erforderlich, dass der Hinweisgeber im Zeitpunkt einer Meldung oder Offenlegung hinsichtlich des Vorliegens eines Verstoßes **gutgläubig** ist und insbesondere **keine vorsätzlich oder grob fahrlässig falschen Angaben** macht.⁶⁴
- 54** Geschützt werden sollen auch Hinweisgeber, denen bei der Bewertung des Sachverhalts Fehler unterlaufen sind und die in gutem Glauben ungenaue oder unzutreffende Informationen gemeldet haben. Nicht geschützt werden hingegen Personen, die missbräuchlich oder böswillig unrichtige Informationen melden.⁶⁵ Maßgeblich ist eine Ex-ante-Sicht. In objektiver Hinsicht verlangt ein hinreichender Grund zur Annahme eines Verstoßes, dass tatsächliche Anknüpfungspunkte für diesen vorliegen. Nicht erfasst sind damit Spekulationen oder Gerüchte.⁶⁶
- 55** Das Motiv des Hinweisgebers für die Abgabe seiner Meldung ist indes unerheblich,⁶⁷ sodass auch Hinweisgeber geschützt sind, wenn sie in Schädigungsabsicht handeln, solange die übrigen Schutzvoraussetzungen erfüllt sind.
- 56** Geschützt sind Meldungen von Informationen über „**Verstöße**“. Dies sind **Handlungen oder Unterlassungen** im Rahmen einer beruflichen, unternehme-

⁶³ Colneric/Gerdemann, in: BeckOK HinSchG, § 33 HinSchG Rn. 25.

⁶⁴ Colneric/Gerdemann, in: BeckOK HinSchG, § 33 HinSchG Rn. 26 m. w. N.

⁶⁵ BT-Drs. 20/3442, S. 92.

⁶⁶ BT-Drs. 20/3442, S. 92.

⁶⁷ BT-Drs. 20/3442, S. 92.

rischen oder dienstlichen Tätigkeit, **die rechtswidrig**⁶⁸ sind und Rechtsgebiete betreffen, die in den sachlichen Anwendungsbereich (§ 2) fallen; hierzu können auch missbräuchliche Handlungen oder Unterlassungen gehören, die dem Ziel oder dem Zweck der in § 2 genannten Vorschriften oder Rechtsgebieten zuwiderlaufen (§ 3 Abs. 2 HinSchG).

„**Informationen über Verstöße**“ erfassen begründete Verdachtsmomente oder Wissen über tatsächliche oder mögliche Verstöße, die bereits begangen wurden oder sehr wahrscheinlich erfolgen werden. Die Formulierung ist sehr weit zu verstehen und umfasst neben tatsächlichen auch potenzielle Verstöße, sodass darunter auch begründete Verdachtsmomente über einen potenziellen, im Ergebnis sich aber nicht bestätigenden Verstoß fallen. Um Verstöße wirksam zu unterbinden, ist der Schutz auch für solche Personen gerechtfertigt, die zwar keine eindeutigen Beweise beibringen, aber begründete Bedenken oder einen begründeten Verdacht äußern.⁶⁹ **57**

Weitere Voraussetzung ist, dass die gemeldeten Verstöße bei dem Beschäftigungsgeber, bei dem der Hinweisgeber tätig ist oder war, oder bei einer anderen Stelle, mit der der Hinweisgeber beruflich in Kontakt steht oder stand, begangen wurden. **58**

b) Besonderheiten in Abhängigkeit vom Meldeweg

Hinweisgeber haben ein **Wahlrecht**, ob sie sich für ihre Meldung des **internen** **59**
oder externen Meldewegs bedienen (§ 7 HinSchG).

aa) Interne Meldungen gemäß § 17 HinSchG

Das Gesetz sieht **keinen Vorrang** des internen vor dem externen Whistleblowing vor. Zwar regelt § 7 Abs. 1 Satz 2 HinSchG, dass hinweisgebende Personen in den Fällen, in denen intern wirksam gegen den Verstoß vorgegangen werden kann und sie keine Repressalien befürchten, die Meldung an die interne Meldestelle bevorzugen „sollten“. Diese Regelung geht letztlich auf die Vorgabe aus Art. 7 Abs. 2 WBRL zurück, der die Mitgliedstaaten dazu auffordert, sich dafür einzusetzen, dass die Meldung über interne Meldekanäle gegenüber der Meldung über externe Meldekanäle grundsätzlich bevorzugt wird.⁷⁰ Hierdurch wird jedoch das Wahlrecht des Hinweisgebers nicht eingeschränkt. § 7 Abs. 1 Satz 2 HinSchG ist daher lediglich klarstellender Natur und stellt sich als rechtsfolgenlose Vorschrift mit reinem Appell- und Signalcharakter dar.⁷¹ **60**

68 Diese Regelung steht im Widerspruch zur Regelung des § 5 Nr. 2 GeschGehG, die davon ausgeht, dass ein Verrat von Geschäfts- und Betriebsgeheimnissen auch dann gerechtfertigt ist, wenn nicht rechtswidrige, sondern „lediglich“ unethische Verhaltensweisen gemeldet werden; siehe hierzu auch Beschluss des OLG Oldenburg v. 21.5.2019, CB 2020, 220.

69 BT-Drs. 20/3442, S. 65; *Colneric/Gerdemann*, in: BeckOK HinSchG, § 3 HinSchG Rn. 17.

70 Siehe zur politischen Diskussion um das Wahlrecht des Hinweisgebers: *Garden/Hiéramente*, BB 2019, 963, sowie *Wiedmann/Seyfert*, CCZ 2019, 12 ff.

71 Vgl. zum Ganzen: *Colneric/Gerdemann*, in: BeckOK HinSchG, § 7 HinSchG Rn. 8.

- 61 Nach § 7 Abs. 1 Satz 3 HinSchG bleibt es Hinweisgebern unbenommen, sich nach Abgabe einer Meldung über die interne Meldestelle an die externe Meldestelle zu wenden, wenn dem intern gemeldeten Verstoß nicht abgeholfen wurde. Unklar ist, ob die Nichtabhilfe nach einer internen Meldung notwendige Voraussetzung für die anschließende Abgabe einer externen Meldung ist. Viel spricht dafür, dass es sich bei dieser Regelung nur um ein gesetzliches Beispiel handelt, durch das aber das grundsätzliche Wahlrecht des Hinweisgebers nicht eingeschränkt werden sollte.⁷²
- 62 Eine Besonderheit ist bei **Meldungen von Kartellverstößen** zu beachten. Hier regelt § 22 Abs. 1 Satz 2 HinSchG, dass die Regelung des § 7 Abs. 1 Satz 3 mit der Maßgabe anzuwenden ist, dass sich Hinweisgeber **jederzeit und unabhängig vom Ausgang des Verfahrens über die interne Meldung** an die zuständige externe Meldestelle – das Bundeskartellamt – wenden können. Hintergrund dieser Regelung ist, dass eine effektive Durchsetzung des Kartellverbots sichergestellt werden soll. Speziell bei der Meldung von Kartellverstößen ist zu beachten, dass daran immer mehrere Unternehmen beteiligt sind. Nach interner Meldung mag zwar das betroffene Unternehmen seine Beteiligung an dem Kartell stillschweigend einstellen; die Existenz des Kartells im Übrigen wäre jedoch nicht aufgedeckt; seine Aufdeckung vielmehr erschwert. Es droht eine Verdunkelung des Sachverhalts. Zusätzlich ist der Gefahr zu begegnen, dass hinweisgebende Personen als potenzielle Kronzeugen nicht mehr in Betracht kämen.⁷³

bb) Externe Meldungen gemäß § 27 HinSchG

- 63 Darüber hinaus genießen auch die Personen den Schutz des Gesetzes, die sich **direkt an die externen Meldekanäle der zuständigen Behörde** wenden.
- 64 Als Gründe, warum sich Hinweisgeber direkt an die zuständige Behörde wenden könnten, kommt laut den Erwägungsgründen der WBRL z. B. in Betracht, dass keine internen Meldekanäle bestehen oder diese nicht angemessen funktionieren.⁷⁴
- 65 Insbesondere kann es in der Praxis Fälle geben, in denen vernünftigerweise nicht erwartet werden kann, dass die Nutzung interner Kanäle angemessen funktioniert. Dies kann dann der Fall sein, wenn Hinweisgeber hinreichenden Grund zu der Annahme haben, dass sie im Zusammenhang mit der Meldung, auch infolge der Verletzung der Vertraulichkeitspflicht, Repressalien erleiden würden. Dies kann etwa dann der Fall sein, wenn der für die Bearbeitung einer Meldung verantwortliche Mitarbeiter an dem Verstoß beteiligt ist oder die Gefahr besteht,

72 Zum Meinungsstand vgl. *Colneric/Gerdemann*, in: BeckOK HinSchG, § 7 HinSchG Rn. 12 m. w. N.

73 BT-Drs. 20/3442, S. 84.

74 Erwägungsgrund 61 der WBRL.

dass der Verstoß verschleiert oder diesbezügliche Beweismittel unterdrückt bzw. vernichtet werden könnten.⁷⁵

Die Erwägungsgründe der WBRL nennen zudem Sachverhalte, in denen die zuständige Behörde in einer besseren Position wäre, gegen den gemeldeten Verstoß vorzugehen. So beispielsweise, wenn die Wirksamkeit von Untersuchungsmaßnahmen durch die zuständige Behörde im Fall einer internen Meldung gefährdet wäre, so beispielsweise im Fall von Meldungen über Kartellabsprachen oder andere Verstöße gegen Wettbewerbsvorschriften oder wenn **dringender Handlungsbedarf** besteht, etwa zum **Schutz der Gesundheit oder der Sicherheit von Menschen oder zum Schutz der Umwelt**.⁷⁶ **66**

cc) Offenlegung gemäß § 32 HinSchG

Schließlich hat ein Hinweisgeber unter bestimmten Umständen auch dann Anspruch auf Schutz im Rahmen des Gesetzes, wenn er seine Informationen offenlegt. Unter **Offenlegung** ist ein öffentliches Zugänglichmachen der Informationen über Verstöße zu verstehen (§ 3 Abs. 5 HinSchG). Dies kann etwa über Online-Plattformen und soziale Medien, gewählte Amtsträger, zivilgesellschaftliche Organisationen, Gewerkschaften oder Berufsverbände erfolgen. Es reicht auch aus, wenn Informationen „nur“ betriebsöffentlich bekannt gemacht werden.⁷⁷ **67**

Ein Hinweisgeber, der diesen Weg wählt, hat gemäß § 32 Abs. 1 HinSchG Anspruch auf Schutz, wenn er **zunächst eine externe Meldung** erstattet hat, aber zu seiner Meldung innerhalb der in § 28 Abs. 4 HinSchG geregelten Zeiträume (drei Monate oder in umfangreichen Fällen sechs Monate) **keine geeigneten Maßnahmen** ergriffen wurden oder er keine Rückmeldung über das Ergreifen solcher Maßnahmen erhalten hat. **68**

Die Angemessenheit der Folgemaßnahmen richtet sich nach objektiven Kriterien. Sie ist somit abhängig von den fallspezifischen Umständen und der Art der Vorschriften, gegen die verstoßen wurde.⁷⁸ **69**

Darüber hinaus kann ein Hinweisgeber gemäß § 32 Abs. 1 Nr. 1 HinSchG auch direkt eine Offenlegung vornehmen, wenn er hinreichenden Grund zu der Annahme hat, dass **70**

- der Verstoß wegen eines Notfalls, der Gefahr irreversibler Schäden oder vergleichbarer Umstände eine unmittelbare oder offenkundige **Gefährdung des öffentlichen Interesses** darstellen kann, oder
- im Fall einer externen Meldung **Repressalien zu befürchten** sind, oder

⁷⁵ So Erwägungsgrund 62 der WBRL.

⁷⁶ So Erwägungsgrund 62 der WBRL.

⁷⁷ Colneric/Gerdemann, in: BeckOK HinSchG, § 3 HinSchG Rn. 28.

⁷⁸ BT-Drs. 20/3442, S. 90.

- aufgrund der besonderen Umstände des Falls **geringe Aussichten bestehen, dass wirksam gegen den Verstoß vorgegangen** wird, z. B. weil Beweismittel unterdrückt oder vernichtet werden oder wenn zwischen einer Behörde und dem Urheber des Verstoßes Absprachen bestehen könnten oder die Behörde an dem Verstoß beteiligt sein könnte.

6. Pflicht zur Einrichtung eines internen Hinweisgebersystems

- 71** Kernstück des Hinweisgeberschutzgesetzes aus Unternehmenssicht ist die Pflicht für private und öffentliche Unternehmen (Beschäftigungsgeber), eine Stelle für interne Meldungen einzurichten, an die sich Beschäftigte wenden können.

a) Unternehmen des privaten Sektors

- 72** Natürliche Personen, juristische Personen, Personengesellschaften und rechtsfähige Personenvereinigungen des privaten Sektors (gemeinsam: private Beschäftigungsgeber) trifft seit dem 17.12.2023 diese Verpflichtung, sofern sie 50 oder mehr Beschäftigte haben (§ 12 Abs. 1 HinSchG); im Übergangszeitraum zwischen dem Inkrafttreten des Gesetzes am 2.7.2023 und dem 17.12.2023 galt dies zunächst nur für private Beschäftigungsgeber mit mehr als 249 Beschäftigten.⁷⁹ Für „mittelgroße“ private Beschäftigungsgeber mit 50 bis 249 Beschäftigten sieht das Gesetz eine Erleichterung vor: solche Unternehmen können sich Ressourcen für die Entgegennahme von Meldungen und für möglicherweise durchzuführenden Untersuchungen teilen (§ 14 Abs. 2 HinSchG).
- 73** Von praktischer Relevanz ist in diesem Zusammenhang insbesondere die Frage, ob sich miteinander verbundene (Konzern-)Unternehmen eine zentrale interne Meldestelle teilen dürfen (siehe hierzu ausführlich → Rn. 90 ff.).
- 74** Für Unternehmen aus bestimmten Sektoren gilt die Pflicht zur Einrichtung interner Meldestellen unabhängig von der Zahl ihrer Beschäftigten (§ 12 Abs. 3 HinSchG). Hierbei handelt es sich insbesondere um Wertpapierdienstleistungsunternehmen, Börsenträger, Kredit- und Finanzdienstleistungsinstitute und Kapitalverwaltungsgesellschaften. Hintergrund ist, dass diese Unternehmen aufgrund unionsrechtlicher Vorschriften bereits vor Inkrafttreten des HinSchG zur Einrichtung interner Meldestellen verpflichtet waren.⁸⁰
- 75** In diesem Zusammenhang ist ferner zu berücksichtigen, dass bereits bestehende sektorspezifische Regelungen zur Einrichtung von Hinweisgeber- oder Meldesystemen der allgemeinen Pflicht aus dem HinSchG vorgehen. Insoweit stellt § 4 Abs. 1 HinSchG klar, dass die dort genannten Vorschriften Vorrang vor dem HinSchG haben. Hintergrund dessen ist, dass die sektorspezifisch tätigen und etablierten Meldestellen regelmäßig über große Expertise und tiefes Fachwissen

⁷⁹ § 42 Abs. 1 HinSchG.

⁸⁰ BT-Drs. 20/3442, S. 78.

verfügen. Daher sollen Fälle, deren Bearbeitung dieses Fachwissen verlangt, nicht von diesen Stellen zu einer allgemeinen Meldestelle, wie sie mit dem HinSchG eingerichtet wird, verlagert werden.⁸¹ Dies betrifft insbesondere die einschlägigen Vorschriften des Geldwäschegesetzes, des Kreditwesengesetzes, des Wertpapierhandelsgesetzes, des Versicherungsaufsichtsgesetzes oder des Börsengesetzes. Nur soweit diese Vorschriften keine Regelungen zum Hinweisgeberschutz enthalten, gelten subsidiär die Vorschriften des HinSchG.

b) Juristische Personen des öffentlichen Sektors

Die genannte Verpflichtung zur Einrichtung interner Meldestellen besteht auch für alle **juristischen Personen des öffentlichen Sektors, einschließlich solcher Stellen, die im Eigentum oder unter der Kontrolle einer solchen juristischen Person stehen** (§ 12 Abs. 1 HinSchG). Die obersten Bundes- oder Landesbehörden können als Beschäftigungsgeber Organisationseinheiten in Form von einzelnen oder mehreren Behörden, Verwaltungsstellen, Betrieben oder Gerichten bestimmen, die interne Meldestellen einzurichten und zu betreiben haben. Durch diese flexible Regelung kann je nach Verwaltungs- und Organisationsstrukturen eine passgenaue Lösung gefunden werden.⁸² **76**

Für Gemeinden und Gemeindeverbände richtet sich die Pflicht zur Einrichtung interner Meldestellen nach dem jeweiligen Landesrecht, da dem Bund die Kompetenz fehlt, unmittelbar Aufgaben an Gemeinden und Gemeindeverbände zu übertragen.⁸³ In Umsetzung von Art. 8 Abs. 9 Unterabs. 2 der WBRL kann insoweit im jeweiligen Landesrecht auch vorgesehen werden, dass Gemeinden und Gemeindeverbände mit weniger als 10.000 Einwohnern von der Pflicht zur Einrichtung interner Meldestellen ausgenommen werden.⁸⁴ **77**

7. Gesetzliche Anforderungen an ein internes Hinweisgebersystem

In Umsetzung der Vorgaben aus der WBRL enthält das Hinweisgeberschutzgesetz diverse Vorgaben zur Ausgestaltung des unternehmensinternen Hinweisgebersystems. **78**

a) Wahrung der Vertraulichkeit

Um das gesetzgeberische Kernziel eines bestmöglichen Hinweisgeberschutzes sowie des Schutzes der durch eine Meldung Betroffenen zu erreichen, sieht das Gesetz eine strenge Vertraulichkeitsverpflichtung vor. Demnach haben die internen Meldestellen die Vertraulichkeit der Identität des Hinweisgebers und Dritter, die in der Meldung erwähnt werden, zu wahren (§ 8 Abs. 1 HinSchG). Die Identität der geschützten Personen darf ausschließlich den Personen, die für die Ent- **79**

⁸¹ BT-Drs. 20/3442, S. 67.

⁸² BT-Drs. 20/3442, S. 77.

⁸³ „Durchgriffsverbot“ nach Art. 84 Abs. 1 Satz 7 GG.

⁸⁴ BT-Drs. 20/3442, S. 77.

gegennahme von Meldungen und die Ergreifung von Folgemaßnahmen zuständig sind, bekannt werden. Allen anderen Mitarbeitern ist der Zugriff darauf zu verwehren.⁸⁵ Dadurch wird eine Weitergabe eingegangener Meldungen innerhalb der Meldestelle auf das zwingend notwendige Maß beschränkt. Ein Bekanntwerden der Identitäten ist neben den für die Meldung zuständigen Personen auch gegenüber unterstützendem Personal wie Büro- und IT-Kräften zulässig, soweit dies für die Unterstützungstätigkeit notwendig ist.⁸⁶

- 80** Verstöße gegen die Verletzung der Vertraulichkeitsverpflichtungen sind bußgeldbewehrt. Bei vorsätzlicher oder leichtfertiger Verletzung drohen den handelnden Personen Bußgelder von bis zu 50.000 EUR (§ 40 Abs. 3, 6 Satz 1 HinSchG). Bei Verstößen von Leitungspersonen i. S. d. § 30 OWiG kann die Geldbuße sogar bis zu 500.000 EUR betragen.⁸⁷
- 81** Ausnahmen vom Vertraulichkeitsgebot sind gesetzlich in § 9 HinSchG geregelt. Eine Ausnahme gilt zunächst im Fall von Hinweisgebern, die vorsätzlich oder grob fahrlässig unrichtige Informationen über Verstöße melden. Die Identität solcher bösgläubiger Hinweisgeber ist nicht geschützt. Ferner dürfen Informationen über die Identität von Hinweisgebern in Strafverfahren auf Verlangen der Strafverfolgungsbehörden oder aufgrund Anordnungen der zuständigen Verwaltungsbehörden im Verwaltungsverfahren oder aufgrund gerichtlicher Entscheidungen herausgegeben werden. In diesen Fällen ist der Hinweisgeber vorab über die Weitergabe zu informieren, es sei denn, dass die empfangende Behörde oder das Gericht dies wegen drohender Gefährdung des Verfahrens untersagt hat. Des Weiteren dürfen Informationen über die Identität des Hinweisgebers auch dann weitergegeben werden, soweit dies für Folgemaßnahmen erforderlich ist und der Hinweisgeber zuvor in diese Weitergabe eingewilligt hat.
- 82** Etwas weiter sind die Ausnahmen vom Vertraulichkeitsgebot in Bezug auf Personen, die Gegenstand einer Meldung sind, gefasst. Hier ist die Weitergabe außer im Falle der vorgenannten Ausnahmen auch dann zulässig, wenn dies im Rahmen interner Untersuchungen oder zur Ergreifung von Folgemaßnahmen im betroffenen Unternehmen erforderlich ist (§ 9 Abs. 4 HinSchG).

b) Meldewege

- 83** Meldungen müssen in **Textform** (auf dem Postweg, über einen Beschwerdebriefkasten oder über eine Online-Plattform im Inter- oder Intranet⁸⁸) oder (telefonisch oder mittels einer anderen Art der Sprachübermittlung) in **mündlicher Form** ermöglicht werden. Auf Ersuchen des Hinweisgebers muss darüber hinaus eine mündliche Meldung bei **einem physischen Zusammentreffen** innerhalb eines angemessenen Zeitrahmens möglich sein. Mit Einwilligung des Hinweis-

⁸⁵ So auch *Colneric/Gerdemann*, in: BeckOK HinSchG, § 8 HinSchG Rn. 27.

⁸⁶ BT-Drs. 20/3442, S. 74.

⁸⁷ §§ 40 Abs. 6 Satz 2 HinSchG, 30 Abs. 2 Satz 3 OWiG.

⁸⁸ Vgl. Erwägungsgrund 53 der WBRL.

gebers kann die Zusammenkunft aber auch im Wege der Bild- und Tonübertragung, z.B. über gängige Videokonferenzsysteme, erfolgen (§ 16 Abs. 3 HinSchG).⁸⁹

§ 16 Abs. 1 Satz 5 HinSchG regelt, dass Unternehmen nicht verpflichtet sind, Meldekanäle so zu gestalten, dass die Abgabe anonymer Meldungen ermöglicht wird. Allerdings regelt Satz 4, dass anonym eingehende Meldungen bearbeitet werden sollten (siehe hierzu nachfolgend → Rn. 148 ff.).⁹⁰ **84**

Nach § 16 Abs. 1 Satz 3 HinSchG steht es Unternehmen frei, den internen Meldekanal auch für einen weiteren Personenkreis (z. B. Mitarbeiter von Lieferanten oder andere Personen, die im Rahmen ihrer beruflichen Tätigkeit mit dem Unternehmen Informationen erhalten) zu öffnen. Eine Verpflichtung hierzu besteht jedoch nicht. **85**

Schließlich haben die Unternehmen **klare und leicht zugängliche Informationen** über die Verfahren für externe Meldungen an die zuständigen Behörden zur Verfügung zu stellen (§ 13 Abs. 2 HinSchG) (siehe hierzu → Rn. 105 ff.). **86**

c) Interne Meldestelle

Mit Blick auf das Vertraulichkeitsgebot stellt § 16 Abs. 2 HinSchG klar, dass die Meldekanäle so zu gestalten sind, dass nur die für die Entgegennahme und Bearbeitung der Meldungen zuständigen Personen Zugriff auf die eingehenden Meldungen haben (siehe hierzu bereits → Rn. 79 ff.). Dies ist von den Unternehmen bei der Wahl des Meldewegs und der Ausgestaltung des Hinweisgeberverfahrens in besonderem Maße zu berücksichtigen. **87**

Die interne Meldestelle kann nach § 14 Abs. 1 HinSchG in der Weise eingerichtet werden, dass eine oder mehrere beim Unternehmen tätige Personen mit den Aufgaben der internen Meldestelle beauftragt werden. Ebenso ist es möglich, dass externe **Dritte** mit dieser Aufgabe betraut werden können. Dritte können insbesondere externe Berater (in der Praxis häufig Rechtsanwälte), Gewerkschaftsvertreter oder Arbeitnehmervertreter sein.⁹¹ Wird die Aufgabe an einen Dritten übertragen, stellt das Gesetz klar, dass das beauftragende Unternehmen dadurch nicht von der Pflicht befreit wird, geeignete Maßnahmen zu ergreifen, um festgestellte Verstöße abzustellen (§ 14 Abs. 1 Satz 2 HinSchG). **88**

Die Personen, die die Aufgaben der internen Meldestelle wahrnehmen, müssen nach § 15 Abs. 1 HinSchG bei der Ausübung dieser Tätigkeit **unabhängig** sein. Sie dürfen neben dieser Tätigkeit jedoch auch andere Tätigkeiten ausüben, solange diese anderen Tätigkeiten nicht zu Interessenkonflikten führen. Was genau unter dem Merkmal der Unabhängigkeit zu verstehen ist, konkretisiert das Ge- **89**

⁸⁹ Dilling, in: BeckOK HinSchG, § 16 HinSchG Rn. 13.

⁹⁰ Ungeachtet dessen wird die Bearbeitung von anonymen Hinweisen in der Praxis aufgrund der Legalitäts- und Schadensabwendungspflicht regelmäßig geboten sein.

⁹¹ BT-Drs. 20/3442, S. 79.

setz nicht.⁹² Unternehmen müssen der internen Meldestelle die **notwendigen Befugnisse** übertragen, um ihre Aufgaben wahrzunehmen, insbesondere um Meldungen zu prüfen und Folgemaßnahmen zu ergreifen (§ 12 Abs. 4 Satz 1 HinSchG). Ferner müssen Unternehmen dafür Sorge tragen, dass die Meldestellenbeauftragten über die notwendige Fachkunde für diese Tätigkeit verfügen (§ 15 Abs. 2 HinSchG).

d) Exkurs: Interne Meldestellen im Konzern

- 90** In der Praxis stellt sich insbesondere für Konzerne mit oft einer Vielzahl von Tochtergesellschaften die Frage, ob jede einzelne Konzerngesellschaft, die mehr als 50 Personen beschäftigt, ein eigenes Hinweisgebersystem einrichten muss. Dem Wortlaut nach verpflichtet das HinSchG jeden einzelnen Beschäftigungsgeber, also jede juristische Person oder Personengesellschaft (vgl. §§ 3 Abs. 8, 12 Abs. 1 HinSchG).
- 91** Die Europäische Kommission vertrat in zwei viel diskutierten Stellungnahmen im Ergebnis die Auffassung, dass grds. jede in den Anwendungsbereich der WBRL fallende juristische Person einen eigenen, lokalen Meldekanal einrichten müsse. Insbesondere der in vielen Konzernen seit Jahren etablierten Praxis von zentralen Meldekanälen für den gesamten Konzern wurde eine Absage erteilt. Begründet wird dies mit dem klaren Wortlaut von Art. 8 Abs. 1 HinSchG und Erwägungsgrund 54 der WBRL. Ausnahmen seien nur für solche Konzerngesellschaften mit 50 bis 249 Beschäftigten möglich, die nach Art. 8 Abs. 6 WBRL Ressourcen teilen dürften. Weitergehende Ausnahmen oder gar ein Konzernprivileg sehe die WBRL nicht vor. Im Ergebnis stehe es Konzernen zwar frei, neben lokalen Meldekanälen bei den einzelnen verpflichteten Konzerngesellschaften zusätzlich auch zentrale Meldekanäle einzurichten. Ein zentraler Kanal allein sei jedoch nicht ausreichend.⁹³
- 92** Nach intensiver Kritik aus Literatur und Praxis⁹⁴ entschied sich der deutsche Gesetzgeber, der strengen Auffassung der EU-Kommission nicht zu folgen. Nach der Gesetzesbegründung zum HinSchG haben Konzernunternehmen in Deutschland nun die Möglichkeit, anstelle eines eigenen Meldewegs auf einen gemeinsamen Konzernmeldeweg zurückzugreifen, der z.B. bei einer Konzernobergesellschaft angesiedelt wird (sog. „**Konzernlösung**“).⁹⁵ Das bedeutet, dass sie sich mit jeder anderen Konzerngesellschaft (Mutter-, Tochter- oder Schwester-gesellschaft) im In- oder Ausland einen Meldeweg teilen dürfen. Rechtlich ba-

⁹² Auch die WBRL enthält hierzu keine Vorgaben, vgl. Erwägungsgrund 56 der WBRL.

⁹³ S. 3 des Protokolls über das 5. Treffen der Expertengruppe der Europäischen Kommission zur Umsetzung der HinSch-RL v. 14.6.2021; S. 2 des Schreibens der Europäischen Kommission v. 16.7.2021 (JUST/C2/MM/rp/(2021)5129001); zum Ganzen siehe auch *Dilling*, in: BeckOK HinSchG, § 14 HinSchG Rn. 6–26.

⁹⁴ *Lüneborg*, DB 2022, 375; *Passarge*, CB 2021, 453, 457; *Bürkle* CCZ 2022, 335, 339, siehe auch *Dilling*, in: BeckOK HinSchG, § 14 HinSchG Rn. 13 m. w. N.

⁹⁵ BT-Drs. 20/3442, S. 79.

siert dies auf § 14 Abs. 1 HinSchG, der es juristischen Personen erlaubt, **externe Dritte** mit den Aufgaben der internen Meldestelle zu betrauen. Nach der Argumentation der Bundesregierung sind andere juristische Personen – auch wenn sie Teil des Konzerns sind – wegen des gesellschaftsrechtlichen Trennungsprinzips auch als externe Dritte anzusehen.

Nach der aktuellen Fassung des HinSchG ist die Konzernlösung daher zulässig. 93
Es bleibt abzuwarten, ob diese Auslegung der WBRL Bestand haben oder in Zukunft vom EUGH kassiert werden wird.

e) Bearbeitung der eingehenden Meldungen

Das Hinweisgeberschutzgesetz sieht in § 17 vage Regelungen für die weitere Bearbeitung eingehender Meldungen vor. Dabei bleiben viele Aspekte im Detail unregelt. 94

Die interne Meldestelle hat dem Hinweisgeber den Eingang seiner Meldung innerhalb einer **Frist von sieben Tagen** zu bestätigen. Sie hat im weiteren Verlauf mit dem Hinweisgeber Kontakt zu halten und ihn bei Bedarf um weitere Informationen zu ersuchen. Hierdurch soll ein Vertrauensverhältnis zum Hinweisgeber aufgebaut und zugleich vermieden werden, dass der Hinweisgeber sich doch noch an eine externe Meldestelle wendet.⁹⁶ 95

Des Weiteren soll die interne Meldestelle eine Erstprüfung der Meldung vornehmen. Dabei ist zu prüfen, ob die Meldung in den sachlichen Anwendungsbereich des HinSchG fällt und ob die Meldung stichhaltig ist. Dies bedeutet, dass geprüft wird, ob die Meldung plausibel und widerspruchsfrei ist und ob die übermittelten Tatsachen sich so zugetragen haben können.⁹⁷ 96

Kommt die Erstprüfung zum Ergebnis, dass die Meldung in den sachlichen Anwendungsbereich des HinSchG fällt und stichhaltig ist, so hat die interne Meldestelle angemessene Folgemaßnahmen zu ergreifen (§ 18 HinSchG). Folgemaßnahmen können insbesondere sein: 97

- Kontaktaufnahme mit den von der Meldung betroffenen Personen und Durchführung interner Untersuchungen; konkrete Vorgaben, wie eine Untersuchung durchzuführen ist, macht das Gesetz nicht;⁹⁸
- Abgabe des Verfahrens zwecks weiterer Untersuchungen an eine andere Stelle im Unternehmen, die für interne Untersuchungen zuständig ist, oder an eine Behörde;
- Verweis des Hinweisgebers an eine andere zuständige Stelle (z. B. an den Betriebsrat oder die Personalabteilung); dies wird vor allem dann in Betracht kommen, wenn die Meldung nicht in den sachlichen Anwendungsbereich des

⁹⁶ *Handel*, Meldestellenbeauftragte, S. 146.

⁹⁷ *Dilling*, in: BeckOK HinSchG, § 17 HinSchG Rn. 8.

⁹⁸ Insoweit gelten die allgemeinen Grundsätze. Einen groben Überblick hierzu gibt *Dilling*, in: BeckOK HinSchG, § 17 HinSchG Rn. 22–45.

HinSchG fällt oder wenn die interne Meldestelle selbst keine Abhilfemaßnahmen ergreifen kann;

– Abschluss des Verfahrens.

- 98** Die im Gesetz genannten Folgemaßnahmen sind nicht abschließend und werden auch nicht näher geregelt. Die Unternehmen haben daher einen weiten Ermessensspielraum, wie sie das Verfahren nach der Erstprüfung einer Meldung ausgestalten, welche Folgemaßnahmen im Einzelnen ergriffen werden und welche internen Abteilungen hier eingebunden werden. Während des gesamten Verfahrens ist jedoch stets das Vertraulichkeitsgebot zu beachten. Ferner findet das Ermessen in Bezug auf die zu ergreifenden Folgemaßnahmen seine Grenze in der Beachtung der Legalitätspflicht. Sofern dem Unternehmen über die interne Meldestelle Hinweise auf gravierende Gesetzesverstöße bekannt werden, so muss das Unternehmen diesen nachgehen und sie ggf. abstellen.⁹⁹
- 99** Dem Hinweisgeber ist innerhalb von drei Monaten nach der Eingangsbestätigung eine Rückmeldung zu geben (§ 17 Abs. 2 HinSchG). Dabei ist er über die geplanten oder schon ergriffenen Folgemaßnahmen zu unterrichten. Soweit Folgemaßnahmen erst noch festgelegt werden, sollte der Hinweisgeber auch hierüber unterrichtet werden, zudem sollte ihm mitgeteilt werden, welche weiteren Rückmeldungen er erwarten kann.¹⁰⁰
- 100** Hinweisgeber sollen auch über die Gründe für Folgemaßnahmen informiert werden. Hinweisgeber sollen durch diese Information die Entscheidung nachvollziehen können und das Vertrauen in die Funktion des Hinweisgebersystems soll so gestärkt werden.¹⁰¹ Ihre Grenze findet die Pflicht zur Rückmeldung an den Hinweisgeber dann, wenn die Information die interne Untersuchung berühren oder die Rechte der von der Meldung betroffenen Person beeinträchtigen würde.¹⁰² Sofern in solchen Fällen eine knappe Rückmeldung möglich ist, die beispielsweise keine oder nur eine verkürzte Begründung enthält, ist die Meldestelle gehalten, eine solche Rückmeldung zu geben.¹⁰³

f) Dokumentation und Datenschutz

- 101** Das Hinweisgeberschutzgesetz enthält nur wenige Regelungen zum Datenschutz. In § 10 HinSchG ist geregelt, dass die Meldestellen befugt sind, personenbezogene Daten zu verarbeiten, soweit dies zur Erfüllung ihrer zugewiesenen Aufgaben erforderlich ist. Durch diesen datenschutzrechtlichen Erlaubnistatbestand dürfen die in den Meldungen enthaltenen personenbezogenen Daten durch die Meldestellen sowohl entgegengenommen als auch ausgewertet werden. Soweit erforderlich, ist auch die Verarbeitung besonderer Kategorien personenbe-

⁹⁹ So auch *Dilling*, in: BeckOK HinSchG, § 18 HinSchG Rn. 3.

¹⁰⁰ Erwägungsgrund 58 der WBRL.

¹⁰¹ BT-Drs. 20/3442, S. 82.

¹⁰² Erwägungsgrund 57 der WBRL.

¹⁰³ BT-Drs. 20/3442, S. 82.

zogener Daten nach Art. 9 Abs. 1 DSGVO durch die interne Meldestelle zulässig. Darüber hinaus dürfen bei der Durchführung der Folgemaßnahmen neue personenbezogene Daten erhoben und weiterverarbeitet werden. Die Meldestellen haben zudem die geltenden Vorschriften der DSGVO und des BDSG zu beachten.¹⁰⁴

Die für die interne Meldestelle tätigen Personen haben die eingehenden Meldungen in dauerhaft abrufbarer Weise und unter Beachtung des Vertraulichkeitsgebots zu dokumentieren (§ 11 Abs. 1 HinSchG). **102**

Besondere Anforderungen an die Dokumentation gelten bei mündlich abgegebenen Meldungen nach § 11 Abs. 2 bis 4: Demnach darf bei telefonischen Meldungen oder Meldungen mittels anderer Art der Sprachübermittlung eine dauerhaft abrufbare Tonaufzeichnung oder eine genaue Niederschrift in Form eines Wortprotokolls nur mit Einwilligung des Hinweisgebers erfolgen. Sofern diese nicht vorliegt, ist die Meldung durch eine Zusammenfassung in Form eines Inhaltsprotokolls zu dokumentieren. Bei Meldungen, die im Rahmen einer Zusammenkunft abgegeben werden, darf mit Zustimmung des Hinweisgebers eine vollständige und genaue Aufzeichnung der Zusammenkunft durch Tonaufzeichnung oder Wortprotokoll erstellt werden. Wird ein Wortprotokoll erstellt, so ist dem Hinweisgeber Gelegenheit zu geben, das Protokoll zu prüfen, ggf. zu korrigieren und es durch Unterschrift oder in elektronischer Form zu bestätigen. **103**

Die Dokumentation ist drei Jahre nach Abschluss des Verfahrens aufzubewahren. Eine längere Aufbewahrung ist zulässig, um die Anforderungen nach dem HinSchG oder anderen Vorschriften zu erfüllen, solange dies erforderlich und verhältnismäßig ist (§ 11 Abs. 5 HinSchG). Dies ist beispielsweise dann der Fall, wenn eine Meldung im Rahmen eines Rechtsstreits zur Handakte des bearbeitenden Rechtsanwalts gelangt. Die lange Aufbewahrungsfrist soll der Notwendigkeit Rechnung tragen, im Fall von Rechtsstreitigkeiten, die sich aus einer Meldung ergeben können, auf die Dokumentation zurückgreifen zu können.¹⁰⁵ **104**

8. Pflicht zur Einrichtung externer Meldestellen

In Umsetzung der Vorgaben aus Art. 11 Abs. 1 der WBRL regeln §§ 19 ff. HinSchG die Einrichtung und den Betrieb externer Meldestellen. Diese haben die Aufgabe, in ihrem Zuständigkeitsbereich Meldungen von solchen Hinweisgebern entgegenzunehmen und zu bearbeiten, die sich in Ausübung ihres gesetzlichen Wahlrechts (§ 7 Abs. 1 HinSchG) nicht an die interne Meldestelle ihres Unternehmens wenden möchten. **105**

Die zentrale externe Meldestelle des Bundes ist beim Bundesamt für Justiz angesiedelt. Sie ist zuständig für alle Meldungen, die nicht in den Zuständigkeitsbe- **106**

¹⁰⁴ BT-Drs. 20/3442, S. 76; einen Überblick über die datenschutzrechtlichen Anforderungen findet sich bei *Handel*, Meldestellenbeauftragte, S. 66 ff.

¹⁰⁵ BT-Drs. 20/3442, S. 77.

reich der anderen, in §§ 20 bis 23 HinSchG genannten externen Meldestellen fällt.

- 107** § 20 HinSchG ermöglicht es den Ländern, eigene externe Meldestellen für Meldungen einzurichten, die die Landesverwaltung und die Kommunalverwaltungen betreffen.
- 108** Für Meldungen, die den Zuständigkeitsbereich der Finanzaufsicht betreffen, ist die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) externe Meldestelle (§ 21 HinSchG).
- 109** Für Meldungen, die Kartellverstöße oder Submissionsabsprachen betreffen, ist das Bundeskartellamt zuständige externe Meldestelle (§ 22 HinSchG). Wie bereits dargestellt, stellt § 22 Abs. 1 Satz 2 HinSchG klar, dass sich Hinweisgeber jederzeit und unabhängig vom Ausgang des Verfahrens über eine bereits abgegebene interne Meldung an das Bundeskartellamt als externe Meldestelle wenden können (siehe bereits oben → Rn. 62 ff.).
- 110** Die gesetzlichen Anforderungen an die externen Meldestellen decken sich im Wesentlichen mit denen an interne Meldestellen. Die externen Meldestellen haben Meldekanäle einzurichten und zu betreiben, über die Hinweisgeber Meldungen über Verstöße abgeben können, die in den Anwendungsbereich des HinSchG fallen (§ 24 HinSchG). Sie haben (potenziellen) Hinweisgebern u. a. umfassende Informationen und Beratung im Zusammenhang mit dem Schutz vor Repressalien, die Voraussetzungen für den Schutz nach dem HinSchG und dem Ablauf des Meldeverfahrens anzubieten.
- 111** Auch die externen Meldestellen sind im Rahmen dieser Aufgabe unabhängig (§ 25 HinSchG). Die Vorschriften zum Schutz der Identität der Hinweisgeber, zum Datenschutz und zur Dokumentation von Meldungen gelten für die externen Meldestellen gleichermaßen wie für interne Meldestellen (§§ 8 bis 11 HinSchG) (siehe bereits oben → Rn. 72 ff.).
- 112** Auch externe Meldungen können in schriftlicher oder mündlicher (telefonisch oder mittels einer anderen Art der Sprachübermittlung) Form sowie auf Ersuchen des Hinweisgebers bei einem physischen Zusammentreffen innerhalb eines angemessenen Zeitrahmens abgegeben werden (§ 27 Abs. 3 HinSchG). Die Entgegennahme und Bearbeitung anonymer Meldungen ist auch hier nicht generell vorgeschrieben; jedoch bieten die externen Meldestellen des Bundes diese Möglichkeit.¹⁰⁶
- 113** Auch hat die externe Meldestelle dem Hinweisgeber den Eingang der Meldung umgehend, spätestens nach sieben Tagen, zu bestätigen sowie dem Hinweisgeber innerhalb eines angemessenen Zeitraums von maximal drei bzw. sechs Monaten Rückmeldung zu erstatten (§ 28 Abs. 1 und 4 HinSchG). Des Weiteren hat sie

¹⁰⁶ So z. B. die externe Meldestelle des Bundesamts für Justiz (<http://formulare.bfj.bund.de/ffw/action/invoke.do?id=externeMeldestelle>) oder des Bundeskartellamts (<https://www.bkms-system.net/bkwebanon/report>).

dem Hinweisgeber das abschließende Ergebnis der durch die Meldung ausgelösten Untersuchungen mitzuteilen (§ 31 Abs. 5 HinSchG).

Die externe Meldestelle hat nach Abgabe der Eingangsbestätigung ebenfalls zu prüfen, ob die Meldung in den sachlichen Anwendungsbereich des Hinweisgeberschutzgesetzes fällt und stichhaltig ist. Sodann ergreift sie angemessene Folgemaßnahmen. Dies können insbesondere die Einholung von Auskünften von betroffenen Personen und Unternehmen, den Verweis der Hinweisgeber an die zuständigen Stellen, die Abgabe des Verfahrens an die zuständige Behörde zwecks weiterer Untersuchungen oder der Abschluss des Verfahrens sein (§ 29 HinSchG). **114**

9. Schutzmaßnahmen

Das Hinweisgeberschutzgesetz sieht in den §§ 35 ff. weitgehende Schutzmaßnahmen zugunsten von Hinweisgebern vor, wenn die Schutzvoraussetzungen erfüllt sind (siehe hierzu → Rn. 51 ff.). Personen, die Hinweisgeber benachteiligen, drohen strenge Sanktionen (§ 40 HinSchG). **115**

a) Verbot von Repressalien und Schutz von Hinweisgebern

Generell sind Repressalien, die sich gegen Hinweisgeber richten, verboten. Dies gilt auch bereits für die Androhung und den Versuch, solche Repressalien auszuüben (§ 36 Abs. 1 HinSchG). **116**

Der Begriff der „Repressalie“ ist weit zu verstehen und umfasst alle Handlungen und Unterlassungen im Zusammenhang mit der beruflichen Tätigkeit des Hinweisgebers, die Reaktion auf eine Meldung oder Offenlegung sind und durch die einem Hinweisgeber ein ungerechtfertigter Nachteil entsteht oder entstehen kann (§ 3 Abs. 6 HinSchG). Repressalien sind insbesondere:¹⁰⁷ **117**

- Suspendierung, Kündigung oder vergleichbare Maßnahmen;
- Herabstufung oder Versagung einer Beförderung;
- Aufgabenverlagerung, Änderung des Arbeitsortes, Gehaltsminderung, Änderung der Arbeitszeit;
- Versagung der Teilnahme an Weiterbildungsmaßnahmen;
- negative Leistungsbeurteilung oder Ausstellung eines schlechten Arbeitszeugnisses;
- Disziplinarmaßnahmen, Rügen oder sonstige Sanktionen einschließlich finanzieller Sanktionen;
- Nötigung, Einschüchterung, Mobbing oder Ausgrenzung;
- Diskriminierung, benachteiligende oder ungleiche Behandlung;
- Nichtumwandlung eines befristeten Arbeitsvertrags in einen unbefristeten Arbeitsvertrag in Fällen, in denen der Arbeitnehmer zu Recht erwarten durfte, einen unbefristeten Arbeitsvertrag angeboten zu bekommen;

¹⁰⁷ BT-Drs. 20/3442, S. 95 mit Verweis auf die Umsetzung von Art. 19 WBRL.

- Nichtverlängerung oder vorzeitige Beendigung eines befristeten Arbeitsvertrages;
 - Schädigung (einschließlich Rufschädigung), insbesondere in den sozialen Medien, oder Herbeiführung finanzieller Verluste (einschließlich Auftrags- oder Einnahmeverluste);
 - Erfassen des Hinweisgebers auf einer „schwarzen Liste“ auf Basis einer informellen oder formellen sektor- oder branchenspezifischen Vereinbarung mit der Folge, dass der Hinweisgeber sektor- oder branchenweit keine Beschäftigung mehr findet;
 - vorzeitige Kündigung oder Aufhebung des Vertrags über Waren oder Dienstleistungen;
 - Entzug einer Lizenz oder einer Genehmigung;
 - psychiatrische oder ärztliche Überweisungen.
- 118** Sofern ein Hinweisgeber im Zusammenhang mit der beruflichen Tätigkeit eine Repressalie erleidet und (z. B. in einem gerichtlichen Verfahren) geltend macht, dass diese Repressalie Folge der Meldung oder Offenlegung nach dem Hinweisgeberschutzgesetz ist, so wird vermutet, dass diese Benachteiligung eine Repressalie für diese Meldung oder Offenlegung ist (§ 36 Abs. 2 HinSchG).
- 119** Macht ein Hinweisgeber im Prozess eine Repressalie geltend, hat das Unternehmen oder die Person, die den Hinweisgeber benachteiligt hat, nach § 36 Abs. 2 HinSchG zu beweisen, dass die Benachteiligung auf hinreichend gerechtfertigten Gründen basierte oder nicht auf der Meldung oder Offenlegung beruhte. Das Gesetz sieht somit eine **Beweislastumkehr zugunsten des Hinweisgebers** vor. Der Entlastungsbeweis setzt voraus, dass eine im Anschluss an eine Meldung oder Offenlegung vorgenommene Benachteiligung nur dann keine Repressalie darstellt, wenn die subjektiven Beweggründe für die Ausübung einer nachteiligen Maßnahme in keiner Weise mit der Meldung oder Offenlegung bzw. einer anderen unter dem HinSchG geschützten Verhaltensweise in Verbindung standen, die Maßnahme also aus gänzlich anderen Gründen veranlasst wurde.¹⁰⁸
- 120** Zur Ergänzung des Schutzes regelt § 35 Abs. 1 HinSchG, dass Hinweisgeber nicht für die Beschaffung der oder den Zugriff auf Informationen, die gemeldet oder offengelegt wurden, haftbar gemacht werden können, sofern nicht die Beschaffung oder der Zugriff selbst eine eigenständige Straftat darstellt.¹⁰⁹ Des Weiteren verletzt ein Hinweisgeber keine Offenlegungsbeschränkungen und haftet nicht für die Weitergabe von Informationen, wenn er hinreichenden Grund zur Annahme hatte, dass die Weitergabe der Information erforderlich war, um den Verstoß aufzudecken (§ 36 Abs. 2 HinSchG).¹¹⁰

¹⁰⁸ Colneric/Gerdemann, in: BeckOK HinSchG, § 36 HinSchG Rn. 92.

¹⁰⁹ z. B. Hausfriedensbruch nach § 123 StGB oder Ausspähen von Daten nach § 202a StGB.

¹¹⁰ Dies betrifft z. B. die Verletzung von vertraglichen Vertraulichkeitsverpflichtungen oder von Zugriffsbeschränkungen, vgl. BT-Drs. 20/3442, S. 94.

Für den Fall, dass ein Hinweisgeber unrechtmäßig Repressalien erleidet, ist der Verursacher verpflichtet, den daraus entstandenen Schaden zu ersetzen (§ 37 Abs. 1 HinSchG).¹¹¹ **121**

b) Sanktionen bei Verstößen

Verstöße und versuchte Verstöße gegen das Repressalienverbot sowie die Behinderung oder versuchte Behinderung von Meldungen oder der Kommunikation im Rahmen einer Meldung sind Ordnungswidrigkeiten und bußgeldbewehrt (§ 40 Abs. 2 Nr. 3 HinSchG). Die Bußgelder betragen bis zu 50.000 EUR. Bei Verstößen von Leitungspersonen im Unternehmen i. S. d. § 30 OWiG kann die Geldbuße sogar bis zu 500.000 EUR betragen.¹¹² **122**

III. Aufbau/Einführung eines Hinweisgebersystems im Unternehmen

Im Folgenden werden wesentliche Aspekte dargestellt, die bei der Einrichtung eines Hinweisgebersystems im Unternehmen zu berücksichtigen sind. Insbesondere werden Fragestellungen aufgezeigt, die sich in der Praxis im Zusammenhang mit Hinweisgebersystemen regelmäßig ergeben. **123**

1. Entscheidungen hinsichtlich der konkreten Ausgestaltung

a) Organisation

Bei der Entscheidung über die konkrete Ausgestaltung des Hinweisgebersystems ist selbstverständlich, dass die Organisation und Ausgestaltung von den Anforderungen des einzelnen Unternehmens, wie zum Beispiel der Branche, in welcher das Unternehmen tätig ist, oder der Größe des Unternehmens, abhängen wird. **124**

Auch ist es für das effektive Funktionieren des Systems erforderlich, dessen Erreichbarkeit und die Art der Hinweise zu kommunizieren, die über das System abgegeben werden können. Schließlich sollte im Rahmen der Kommunikation des Hinweisgebersystems verdeutlicht werden, dass der Missbrauch des zur Verfügung gestellten Systems durch das Unternehmen nicht toleriert wird und nur der Hinweisgeber geschützt wird, der einen Hinweis in gutem Glauben an dessen Richtigkeit abgibt. Somit sollte auch darauf hingewiesen werden, dass bewusst falsche oder verleumderische Hinweise sowohl straf- als auch arbeitsrechtliche Folgen haben können.¹¹³ **125**

¹¹¹ Der Ersatz von immateriellen Schäden ist grds. nicht vorgesehen, vgl. § 253 Abs. 1 BGB.

¹¹² §§ 40 Abs. 6 Satz 2 HinSchG, 30 Abs. 2 Satz 3 OWiG.

¹¹³ Vgl. auch *Wybitul*, ZD 2011, 122.

b) Ausgestaltungsmöglichkeiten

- 126** Im Rahmen der Entscheidung über den Betrieb eines Hinweisgebersystems durch ein Unternehmen sind weitreichende Möglichkeiten der Ausgestaltung denkbar.
- 127** Letztendlich kann man sich in der Praxis bei der konkreten Ausgestaltung durch folgende Fragen leiten lassen:
- Wer soll Hinweise abgeben können?
 - An wen und auf welchem Weg sollen Hinweise gemeldet werden können?
 - Auf welche Sachverhalte sollen sich die Hinweise beziehen?
 - Auf welche Weise soll die Einführung des Hinweisgebersystems geregelt werden?
 - Sollen anonyme Meldungen entgegengenommen und bearbeitet werden?

aa) Kreis der Hinweisgeber

- 128** Zunächst ist zu entscheiden, ob der Kreis potenzieller Hinweisgeber beschränkt werden sollte. Auf der Hand liegt zunächst, dass nur solche Personen als Hinweisgeber in Betracht kommen, die in einer wie auch immer ausgestalteten Beziehung zu dem Unternehmen stehen. Dies umfasst neben den Mitarbeitern des Unternehmens auch Geschäftspartner, Lieferanten und Kunden. Da die Öffnung des Hinweisgebersystems für Geschäftspartner gesetzlich nicht verpflichtend ist (§ 16 Abs. 1 Satz 3 HinSchG), sollte überlegt werden, ob Externen die Möglichkeit eingeräumt werden soll, Meldungen über das Hinweisgebersystem abzugeben.
- 129** Ist eine Öffnung des Hinweisgebersystems für Externe nicht gewünscht, kann eine Beschränkung des Kreises potenzieller Hinweisgeber dahingehend vorgenommen werden, dass nur in einem aktuellen Beschäftigungsverhältnis stehende oder ehemalige Mitarbeiter des Unternehmens Hinweise über das Hinweisgebersystem abgeben können. Da das HinSchG auch Personen schützt, die im Vorfeld ihrer beruflichen Tätigkeit Informationen über Verstöße erlangt haben, sollten auch diese in den Kreis der potenziellen Hinweisgeber aufgenommen werden.
- 130** Generell sprechen für eine weite Bestimmung des Kreises möglicher Hinweisgeber zahlreiche Argumente: So dürfte davon auszugehen sein, dass Unternehmensexterne oder ehemalige Mitarbeiter des Unternehmens eher bereit sind, (ggf. unter Nennung ihres Namens) Hinweise abzugeben, da sie naturgemäß keine Sanktionen im Arbeitsverhältnis zu fürchten brauchen. Auch erhöht sich durch die Einbeziehung eines weiten Kreises potenzieller Hinweisgeber die Anzahl von Personen, die über von ihnen wahrgenommene Missstände berichten können; dies dürfte gerade im Bereich von Korruptionsdelikten aus den genannten Gründen (siehe hierzu → Rn. 14) hilfreich sein. Die Erfahrung aus der Praxis zeigt, dass nicht selten substantiierte und berechtigte Hinweise von Externen abgegeben werden.

Jedoch sind auch mögliche Risiken in den Blick zu nehmen: Gerade dann, wenn auch die Abgabe anonymer Hinweise in dem Hinweisgebersystem möglich ist, steigt durch eine umfassende Nutzbarkeit des Systems potenziell die Gefahr des Missbrauchs. Im Rahmen einer Vergabe oder eines Vertragsschlusses mit dem Unternehmen nicht berücksichtigte Konkurrenten könnten das Hinweisgebersystem nutzen, Hinweise ins Blaue hinein oder sogar bewusst unwahre, verleumdende Hinweise abzugeben. Gleiches gilt auch für ehemalige Mitarbeiter des Unternehmens oder gar für aus dem privaten Umfeld von Mitarbeitern stammende Hinweisgeber, die einen Mitarbeiter aus privaten Gründen diskreditieren möchten. Gleichwohl haben sich in der Vergangenheit Befürchtungen, die Zulassung anonymer Hinweise würde in erheblicher Zahl zum Missbrauch von Hinweisgebersystemen einladen, nicht bestätigt. Insoweit scheinen die bei einem solchen Missbrauch drohenden strafrechtlichen und zivilrechtlichen Sanktionen ausreichende Abschreckung zu bewirken. **131**

Die Beantwortung der Frage, ob der Zugang zu dem Hinweisgebersystem beschränkt werden sollte, dürfte jeweils im Einzelfall von den Bedürfnissen des Unternehmens, dessen Struktur und Betätigungsfeld abhängig sein.¹¹⁴ **132**

bb) Zentrale Meldestelle vs. lokale Meldestellen

Wie dargestellt, ermöglicht das HinSchG für deutsche Unternehmen die sog. Konzernlösung. Es ist nach aktueller Rechtslage daher grundsätzlich möglich, eine zentrale Meldestelle für alle Konzernunternehmen einzurichten. Nach diesseitiger Auffassung ist die Konzernlösung eine gut vertretbare Auslegung des HinSchG,¹¹⁵ die auch den Anforderungen der Praxis gerecht wird. Nicht auszuschließen ist indes, dass die Konzernlösung von der Europäischen Kommission in einem Vertragsverletzungsverfahren gegen Deutschland gekippt werden könnte. Auch viele andere Mitgliedstaaten der EU erlauben – ähnlich wie Deutschland – die Konzernlösung.¹¹⁶ **133**

Dessen ungeachtet gibt es auch einige EU-Mitgliedstaaten, die strikt der Auffassung der Europäischen Kommission folgen und es sogar für unzulässig erachten, dass Gesellschaften mit 50 bis 249 Beschäftigten, die nach Art. 8 Abs. 6 HinSch-RL (§ 14 Abs. 2 Satz 1 HinSchG) Ressourcen teilen dürfen, einen gemeinsamen Meldekanal mit einer größeren Gesellschaft (z. B. Konzernmutter) teilen.¹¹⁷ Trotz der Erleichterungen durch die Konzernlösung in einigen Ländern kann für internationale Konzerne daher eine Auslagerung der internen Meldestelle von der Konzernmutter an eine kleinere Konzerngesellschaft mit weniger als 249 Beschäftigten (Stichwort: „Whistleblowing-Holding“) erwägenswert **134**

¹¹⁴ Siehe hierzu auch *Nuster*, in: Ruhmannseder/Behr/Krakov, Hinweisgebersysteme, S. 153 f.

¹¹⁵ A. A. wohl *Dilling*, CCZ 2023, 91, 92 ff.

¹¹⁶ So z. B. Österreich, Frankreich, Spanien.

¹¹⁷ So z. B. Ungarn, Rumänien.

sein.¹¹⁸ Im Ergebnis müssen international tätige Unternehmen die diesbezügliche Rechtslage in allen Ländern prüfen, in denen sie über Tochtergesellschaften verfügen, die die relevante Beschäftigtenzahl von 50 oder eine in den jeweiligen Jurisdiktionen festgelegte noch niedrigere Mindestzahl von Beschäftigten überschreiten.

cc) Meldekanäle

- 135** In Bezug auf die möglichen Meldekanäle ist zunächst die grundlegende Entscheidung zu treffen, ob eine unternehmensinterne oder eine unternehmensexterne Möglichkeit der Hinweisabgabe geschaffen werden soll.¹¹⁹
- 136** So gibt es zunächst die Möglichkeit, interne Ansprechpartner z. B. im Rahmen einer telefonischen Hotline zu benennen, die mit der Entgegennahme und weiteren Bearbeitung der Hinweise betraut sind. Darüber hinaus hatte sich vor Inkrafttreten des Hinweisgeberschutzgesetzes neben der Abgabe von Hinweisen mittels Briefes oder Telefax an dafür eingerichteten Stellen auch die Möglichkeit der Abgabe von Hinweisen über bestimmte unter den Mitarbeitern oder über die Internetpräsenz bekannt gemachte E-Mail-Adressen etabliert. Insbesondere bei der Nutzung von E-Mail-Adressen oder Postadressen sind aber heute besonders die strengen Vertraulichkeitsanforderungen des § 8 HinSchG zu beachten. Vor allem bei E-Mail-Adressen ist nicht auszuschließen, dass eingehende Meldungen allzu leicht an Unbefugte weitergeleitet oder von diesen eingesehen werden können, was dann einen bußgeldbewehrten Verstoß gegen das Vertraulichkeitsgebot darstellt. Sofern man solche Meldekanäle heutzutage noch nutzen möchte, ist daher in besonderem Maße sicherzustellen, dass Unbefugte keinen Zugriff auf das E-Mail-Postfach der Meldestelle erhalten.
- 137** Die Aufgabe der Entgegennahme und Bearbeitung von Hinweisen sollte hier von speziell geschulten bzw. ausgebildeten Mitarbeitern übernommen werden, die zunächst die Hinweise entgegennehmen, gegebenenfalls, soweit dies im konkreten Einzelfall möglich ist, Rückfragen an den Hinweisgeber richten sowie die Hinweise im Hinblick auf ihre Plausibilität und die Notwendigkeit weiterer Untersuchungsmaßnahmen bzw. Reaktionen bewerten.
- 138** Eine weitere Möglichkeit der Ausgestaltung besteht in dem Einsatz von Ombudsleuten;¹²⁰ in der Praxis ist festzustellen, dass die eingesetzten Ombudsleute zumeist als Rechtsanwälte zugelassen sind. Hier wird durch das Unternehmen ein bestimmter Ansprechpartner benannt, an welchen sich die Hinweisgeber bei Verdachtsmomenten etwa wegen Korruptionsdelikten oder anderen Regelverstößen wenden können. Auch können sie im Rahmen der Schlüssigkeitsprüfung die

¹¹⁸ *Block/Nickel*, ZCG 2024, 11 ff.

¹¹⁹ Gerade für größere Unternehmen bietet sich auch eine Kombination beider Varianten dahingehend an, dass neben unternehmensinternen Ansprechpartnern etwa in der Compliance-Abteilung ergänzend externe Ombudsleute benannt werden.

¹²⁰ Vgl. hierzu auch *Buchert*, CCZ 2008, 148 ff.

Plausibilität des Hinweises und die Glaubwürdigkeit des Hinweisgebers bewerten, bevor eine Information des Unternehmens erfolgt.¹²¹ Innerhalb des Unternehmens müssen aber auch dann Mitarbeiter benannt werden, die für die Durchsicht der Schlüssigkeitsprüfung, für die Entscheidung über weitere Untersuchungsschritte und die Entscheidung über Folgemaßnahmen und deren Umsetzung unter Wahrung der gebotenen Vertraulichkeit zuständig sind. Es empfiehlt sich, die einzelnen Arbeitsschritte, Zuständigkeiten und Berichtswege sowie die Maßnahmen zur Schulung der Mitarbeiter der Meldestelle und die Unterrichtung der Arbeitnehmer im Rahmen einer unternehmensinternen Richtlinie vorab zu regeln.

Darüber hinaus werden in der Praxis auch verstärkt freiwillig IT-gestützte Systeme eingesetzt.¹²² Bei dieser Form des Hinweisgebersystems können die Hinweisgeber sowohl unter Offenlegung des Namens wie auch anonym zunächst über eine internetbasierte Plattform Hinweise abgeben und dann z. B. über einen elektronischen Postkasten mit dem Unternehmen kommunizieren und auch Rückfragen der Mitarbeiter des Unternehmens zu den mitgeteilten Informationen beantworten.¹²³ Der Einsatz eines solchen Systems ermöglicht es, auch vom anonym bleibenden Hinweisgeber weitere, detailliertere Informationen über den gemeldeten Verstoß zu erhalten. Das ist deswegen besonders wichtig, weil Hinweisgeber typischerweise bei ihrer Erstmeldung eher kryptisch bleiben und erst einmal prüfen wollen, ob das betroffene Unternehmen engagiert und verantwortungsvoll mit ihrem Hinweis umgeht. Ein weiterer Vorteil IT-gestützter Hinweisgebersysteme ist die Möglichkeit, Hinweise rund um die Uhr abzugeben. Dies ist deshalb sinnvoll, da sich Hinweisgeber nicht selten außerhalb der regulären Arbeitszeiten zur Abgabe einer Meldung entschließen. Ferner ermöglichen viele IT-gestützte Hinweisgebersysteme auch die Abgabe von mündlichen Meldungen.¹²⁴ Die mitunter geäußerten Bedenken, dass die Implementierung und Lizenzierung eines digitalen Hinweisgebertools für Unternehmen im Verhältnis zum Nutzen zu kostspielig und teuer sei, ist nach diesseitiger Auffassung unbegründet.¹²⁵ Mittlerweile haben sich viele Anbieter auf dem Markt etabliert, die bereits für eine jährliche Lizenzgebühr im unteren vierstelligen Bereich ein IT-gestütztes Hinweisgebersystem mit allen wesentlichen Funktionen anbieten. Berücksichtigt man zudem, dass sich mit einem solchen System ohne großen Aufwand die gesetzlichen Anforderungen an die vertrauliche Dokumentation der

139

121 Vgl. Fritz, in: Maschmann, Corporate Compliance und Arbeitsrecht, S. 130 f.

122 Die im HinSchG zunächst verpflichtend vorgesehene Nutzung von digitalen Hinweisgebersystemen wurde im Vermittlungsausschuss wieder gestrichen.

123 Vgl. zum Einsatz des Business Keeper Monitoring Systems – BKMS – im Rahmen eines Whistleblowing-Systems, Altenburg, Bucerius Law Journal 2008, 3 ff.

124 Ein digitales Hinweisgebertool hat üblicherweise eine Voice-Memo-Funktion, die in der Regel den Anforderungen an eine mündliche Meldung auch in anderen EU-Mitgliedstaaten genügt.

125 Vgl. Lüneborg, ZIP 2023, 941, 944; Brobeil, Die Auswirkungen der Richtlinie (EU) 2019/1937 auf Arbeitnehmer-Hinweisgeber, S. 268 m. w. N.

eingehenden Meldungen (§ 11 Abs. 1 HinSchG) und die Sicherstellung der Vertraulichkeit (§ 8 Abs. 1 HinSchG) leicht erfüllen lassen, zeigt sich schnell, dass in aller Regel der Nutzen eines digitalen Hinweisgebersystems regelmäßig dessen Kosten überwiegen wird.¹²⁶

- 140** Nach Inkrafttreten des Hinweisgeberschutzgesetzes hat sich in der Praxis vor allem für mittelständische Unternehmen eine Kombinationslösung etabliert. Die Nutzung eines IT-gestützten Hinweisgebersystems wird kombiniert mit der Beauftragung externer Ombudspersonen (zumeist Rechtsanwälte). Diese übernehmen dann die Aufgabe als ausgelagerte Meldestelle des Unternehmens unter Einsatz eines IT-gestützten Hinweisgebersystems. Nach einer Erstprüfung eingehender Meldungen übernehmen diese die Kommunikation mit dem Hinweisgeber und leiten dann die Meldung ggf. mit Handlungsempfehlungen an die zuständige Stelle im Unternehmen weiter, von wo aus notwendige Folgemaßnahmen (z. B. Untersuchungen) durchgeführt werden können.
- 141** In der Praxis bewährt haben sich Hinweisgebersysteme, die dem Hinweisgeber verschiedene Kanäle zur Hinweisabgabe zur Verfügung stellen. So wird es dem Hinweisgeber ermöglicht, den Weg zu wählen, der aus seiner Sicht als der für ihn praktikabelste erscheint:
- 142** Zum einen sollten Hinweisgeber die Möglichkeit haben, sich persönlich oder telefonisch an die für die Prüfung der Hinweise zuständigen Mitarbeiter der internen Meldestelle zu wenden. Dies hat den Vorteil, dass der Hinweisgeber in einem persönlichen Gespräch über den Ablauf des Prozesses der Hinweisabgabe, über die Möglichkeit der anonymen Abgabe des Hinweises sowie den weiteren Verlauf der Prüfung des Hinweises und die sich anschließende Aufklärung des Sachverhalts unterrichtet werden kann.
- 143** Darüber hinaus sollten auch Eingangswege zur Verfügung gestellt werden, die keinen persönlichen Kontakt zwischen Hinweisgeber und Unternehmen voraussetzen; dies ermöglicht auch Hinweisgebern, die keine direkte persönliche, sondern eine schriftliche Kommunikation wünschen, die Abgabe eines Hinweises. Hier bietet sich neben den herkömmlichen Wegen wie Brief, Fax oder E-Mail auch die Etablierung eines digitalen Hinweisgebersystems an.
- 144** Beim Einsatz digitaler Hinweisgebersysteme besteht auch die Möglichkeit, dass Hinweisgeber im Rahmen der Meldungsabgabe (in Textform) um ein persönliches Gespräch oder ein Gespräch per Video-Call mit den zuständigen Ansprechpartnern der internen Meldestelle oder dem Ombudsmann bitten. Diese Lösung ist insbesondere interessant für Unternehmen, die nur einen einzigen Meldekanal einrichten möchten.

¹²⁶ Block/Nickel, ZCG 2024, 11 ff.

dd) Arten der meldbaren Verstöße

Des Weiteren ist eine Entscheidung darüber zu treffen, welche Arten von Verstößen durch einen Hinweisgeber gemeldet werden können und welche dann einer Aufklärung des Sachverhalts zugeführt werden. **145**

Das Unternehmen sollte sich fragen, ob es nur Hinweisen auf Gesetzesverletzungen, also zumeist Straftaten oder Ordnungswidrigkeiten, nachgehen möchte oder aber ob auch der Verstoß gegen interne Richtlinien Gegenstand von Hinweisen sein kann. **146**

In der Praxis kann bei Unternehmen hier ein unterschiedliches Vorgehen beobachtet werden; so gibt es Unternehmen, in denen lediglich Verstöße gegen Gesetze und Vorschriften gemäß § 2 HinSchG gemeldet werden können, während andere Unternehmen schon Verstöße gegen unternehmensinterne Richtlinien ausreichen lassen, um den Anwendungsbereich des Hinweisgebersystems zu eröffnen. Zu berücksichtigen ist dabei, dass sowohl die WBRL als auch das HinSchG in einem für juristische Laien eher undurchsichtigen Katalog an Verstößen und Regelungsbereichen aufzählen, welche Meldungen dem gesetzlichen Hinweisgeberschutz unterliegen (vgl. § 2 HinSchG). Um bei Hinweisgebern Rechtsunsicherheit zu vermeiden und das Hinweisgebersystem auf alle für das Unternehmen relevanten Sachverhalte zu erstrecken, kann die freiwillige Erweiterung des sachlichen Anwendungsbereichs des Hinweisgebersystems auf sämtliche Gesetzesverletzungen und zumindest gewichtige Verstöße gegen interne Verhaltensvorschriften (z. B. den Code of Conduct) gewichtige Vorteile haben.¹²⁷ **147**

ee) Anonyme Meldungen

Eine in der Praxis sehr relevante Frage ist, ob anonyme Meldungen entgegengenommen und bearbeitet werden sollen. **148**

Wie bereits dargestellt, ist in Deutschland die Einrichtung von internen Meldestellen zur Entgegennahme und Bearbeitung anonymer Hinweise gesetzlich nicht verpflichtend. Die interne Meldestelle „sollte“ jedoch anonyme Meldungen bearbeiten (§ 16 Abs. 1 Satz 4 HinSchG). Diese Empfehlung ist ernst zu nehmen. Denn zumindest nach allgemeinen Compliance-Standards und unter Berücksichtigung der geltenden Organisations- und Legalitätspflicht der Geschäftsführung kann die Bearbeitung anonymer Meldungen ohnehin als verpflichtend angesehen werden, wenn diese Informationen enthalten, die eine weitere Untersuchung des Sachverhalts erfordern, um Schaden für das Unternehmen abzuwenden. In der Praxis ist zudem nicht ausgeschlossen, dass selbst bei einem ausgereiften Hinweisgebersystem für Hinweisgeber weiterhin eine Hemmschwelle besteht, sich aus der Deckung zu wagen.¹²⁸ **149**

¹²⁷ So auch *Reuter*, BB 2023, 1539, 1540 f.; *Block/Nickel*, ZCG 2024, 11 ff.

¹²⁸ *Brobeil*, Die Auswirkungen der Richtlinie (EU) 2019/1937 auf Arbeitnehmer-Hinweisgeber, S. 270; *Schmolke*, NZG, 2020, 5, 11.

- 150** Die im Gesetzgebungsverfahren zur Sprache gekommene Annahme, eine fehlende Pflicht zur Entgegennahme und Bearbeitung anonymer Meldungen reduziere das Risiko für Denunziantentum, deckt sich indes nicht mit den Erfahrungen aus der Praxis und empirischen Untersuchungen. Unternehmen, die bereits seit längerer Zeit ein Hinweisgebersystem eingerichtet haben, haben die Erfahrung gemacht, dass denunziatorische Meldungen in der Praxis selten vorkommen. Denunziatorische Meldungen kommen in Unternehmen, die die Abgabe anonymer Meldungen ermöglichen, zudem nicht häufiger vor als in Unternehmen, die dies nicht tun.¹²⁹ Die Sorge vor missbräuchlichen Meldungen sollte daher kein Grund sein, von der Entgegennahme anonymer Meldungen abzusehen. Im Gegenteil: Die Erfahrung zeigt, dass nicht wenige Meldungen, die sich später als relevant und begründet herausstellten, anonym abgegeben wurden.¹³⁰

ff) Regelungen zur Einführung eines Hinweisgebersystems

- 151** Bei der Implementierung des Hinweisgebersystems ist schließlich auch darüber zu entscheiden, auf welchem Weg die Einführung geschehen soll.
- 152** Obwohl nach deutschem Recht keine Verpflichtung für Unternehmen besteht, einen Verhaltenskodex einzuführen, sprechen doch zahlreiche Gründe für die Implementierung. Existiert bereits ein Verhaltenskodex im Unternehmen, sollte dort jedenfalls auf die Existenz des Hinweisgebersystems, den Schutz des redlichen Hinweisgebers aber auch auf die Folgen einer missbräuchlichen Verwendung des Hinweisgebersystems hingewiesen werden.
- 153** Neben der skizzierten Aufnahme der Einführung/der Existenz des Hinweisgebersystems in den Verhaltenskodex sollten die Einzelheiten zum konkreten Betrieb des Systems und zum Meldeverfahren in einer gesonderten unternehmensinternen Richtlinie geregelt werden. Dies ist auch deswegen anzuraten, da Unternehmen nach § 7 Abs. 3 Satz 2 HinSchG gehalten sind, für Beschäftigte klare und leicht zugängliche Informationen über die Nutzung des internen Meldeverfahrens bereit zu stellen.
- 154** Unabhängig von der Aufnahme der Darstellung des Hinweisgebersystems in dem Verhaltenskodex des Unternehmens bzw. in eine Richtlinie zum Hinweismanagement ist zu entscheiden, über welchen Weg die Nutzung und Funktionsweise des Systems in verbindlicher Weise gegenüber den Arbeitnehmern geregelt werden soll. Neben dem Gebrauch des Weisungsrechts des Arbeitgebers, dem Abschluss von Änderungs- bzw. Ergänzungsvereinbarungen oder dem Abschluss von Tarifverträgen bietet sich vor allem der Abschluss einer Betriebsvereinbarung an.¹³¹ Bei der geplanten Einführung digitaler Hinweisgebersysteme

129 Vgl. Whistleblowing Report 2021, S. 61 f., www.fhgr.ch/whistleblowingreport (Stand: 13.3.2024).

130 Block/Nickel, ZCG 2024, 11 ff.

131 Siehe hierzu auch Berger, in: Ruhmannseder/Behr/Krakow, Hinweisgebersysteme, S. 75 f.

ist nach h. M. gemäß § 87 Abs. 1 Nr. 6 BetrVG ein Mitbestimmungsrecht des Betriebsrats gegeben.¹³²

Eine solche Betriebsvereinbarung zum Hinweismanagement hat neben der sicheren Wahrung der Mitbestimmungsrechte des Betriebsrats vor allem den Vorteil einer größeren Akzeptanz der Einführung des Hinweisgebersystems bei den Mitarbeitern. Darüber hinaus können im Rahmen der Betriebsvereinbarung erforderliche datenschutzrechtliche Regelungen getroffen werden.¹³³ **155**

2. Kommunikation

Schließlich ist im Rahmen der Einführung eines Hinweisgebersystems über Art und Umfang der Kommunikation der Einführung zu entscheiden.¹³⁴ **156**

Eine empfangergerechte Kommunikation und die daraus resultierende Akzeptanz eines Hinweisgebersystems stellen den Schlüssel zu dessen Erfolg dar. **157**

Vor dem Hintergrund der vor allem in Deutschland nach wie vor häufig anzutreffenden Bewertung eines Hinweisgebers als Denunziant¹³⁵ ist es von besonderer Bedeutung, in der Kommunikation des Hinweisgebersystems hervorzuheben, dass die Person, die in redlicher Absicht einen Hinweis abgibt, verantwortungsvoll handelt und das Unternehmen schützt. **158**

Hierbei ist insbesondere die Botschaft von Bedeutung, welche wichtige Aufgabe der Hinweisgeber erfüllt: Der Hinweisgeber zeigt zum einen Verantwortung für das Unternehmen, wenn er Verdachtsfälle auf Wirtschaftskriminalität an das Hinweismanagement meldet. Basierend auf der dort erfolgenden professionellen Bearbeitung der Hinweise kann das Unternehmen wirksam vor Schäden geschützt werden. Darüber hinaus schützt der Hinweisgeber auch die Lauterkeit des Unternehmens im Wettbewerb und damit letztlich auch den nachhaltigen wirtschaftlichen Erfolg. **159**

Nicht zuletzt sollte auf die unternehmensinterne Kommunikation auch wegen des gesetzlichen Wahlrechts von Hinweisgebern (§ 7 Abs. 1 HinSchG) großer Wert gelegt werden. Ein eingehend und transparent kommuniziertes Hinweisgebersystem kann das Vertrauen der Beschäftigten in das interne Verfahren deutlich stärken und den vom Gesetzgeber ausdrücklich angeregten Anreiz darstellen, dass Meldungen vorrangig intern und nicht über die externe (behördliche) Meldestelle abgegeben werden. Dies ist letztlich im Interesse des Unternehmens. **160**

¹³² *Handel*, Meldestellenbeauftragte, S. 203; *Wiedmann/Hoppmann*, CCZ, 2023, 11 ff.

¹³³ So zum Beispiel zur Weitergabe der mit dem Hinweis verbundenen personenbezogenen Daten in einem Konzern oder zur Durchführung unternehmensinterner Untersuchungen.

¹³⁴ Zur Bedeutung der Kommunikation im Rahmen eines wirksamen Compliance Managements siehe ausführlich → *Hastenrath*, Kap. 6.

¹³⁵ Siehe hierzu *Nuster*, in: *Ruhmannseder/Behr/Krakow*, Hinweisgebersysteme, S. 141 ff. und unten unter → Rn. 150.

3. Datenschutzrechtliche Regelungen

- 161** Bei der Meldung von Verstößen werden typischerweise personenbezogene Daten verarbeitet; dies betrifft sowohl die personenbezogenen Daten des Hinweisgebers, so dieser die Meldung nicht anonym abgibt, als auch die personenbezogenen Daten der durch den Hinweis betroffenen Person.
- 162** Durch die Einführung der Datenschutzgrundverordnung (DSGVO) und der Neufassung des BDSG haben sich zahlreiche Änderungen im Hinblick auf die datenschutzrechtlichen Anforderungen ergeben.¹³⁶ Aus Sicht der Unternehmen, die beim Betrieb eines Hinweisgebersystems zur Einhaltung der Vorgaben der DSGVO verpflichtet sind, ist indes bedauerlich, dass das HinSchG das Verhältnis zu den Vorschriften der DSGVO kaum regelt, sodass sich in der Praxis relevante Fragen ergeben, die zu beachten sind.
- 163** Eine grundlegende Frage betrifft die Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen eines Hinweisgebersystems. Die Einrichtung und der Betrieb eines Hinweisgebersystems dient der Erfüllung der gesetzlichen Vorgaben der §§ 12 ff. HinSchG. Daher kann die Datenverarbeitung im Rahmen des Hinweisgebersystems auf Art. 6 Abs. 1 lit. c DSGVO gestützt werden, jedenfalls soweit durch das jeweilige Hinweisgebersystem die Anforderungen des HinSchG umgesetzt werden.
- 164** Sofern ein Unternehmen freiwillig den Anwendungsbereich des Hinweisgebersystems erweitert (siehe dazu oben → Rn. 146 ff.) und z. B. auch für Meldungen über Verstöße gegen rein interne Vorschriften öffnet, kann die Datenverarbeitung indes nicht mehr auf Art. 6 Abs. 1 lit. c DSGVO gestützt werden.¹³⁷ In diesen Fällen wird sich die Berechtigung zur Datenverarbeitung aber regelmäßig aus Art. 6 Abs. 1 lit. f DSGVO ergeben. Das hierfür geforderte berechtigte Interesse besteht in dem Bestreben des Unternehmens, sonstige Gesetzesverstöße und Verstöße gegen die Unternehmensethik zu erfahren und aufzuklären; denn auch solche Verstöße können erhebliche Schäden zulasten des Unternehmens nach sich ziehen.¹³⁸
- 165** Auch kommt als weitere Rechtsgrundlage gemäß § 26 Abs. 4 Satz 1 BDSG der Abschluss einer Kollektivvereinbarung (Tarifvertrag oder Betriebsvereinbarung) in Betracht.¹³⁹ Ob dies auch künftig noch gilt, bleibt vor dem Hintergrund eines Vorlagebeschlusses des BAG an den EuGH abzuwarten.¹⁴⁰

¹³⁶ Zur Bedeutung der DSGVO für das Compliance Management siehe ausführlich → *Böhlke/Becker/Fladung*, Kap. 12.

¹³⁷ *Handel*, Meldestellenbeauftragte, S. 70.

¹³⁸ *Heuking/von Coelln*, in: Rübenstahl/Hahn/Voet van Vormizeele, Kartell Compliance, Kap. 27, Rn. 63; *Handel*, Meldestellenbeauftragte, S. 72.

¹³⁹ Vgl. hierzu Orientierungshilfe der DSK, S. 4 ff.; *Baranowski/Glaßl*, CB 2018, 271 ff.; *Schröder*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Rn. 56 f.

¹⁴⁰ BAG, Vorlagebeschl. v. 22.9.2022 – 8 AZR 209/21.

Im Hinblick auf den datenschutzkonformen Betrieb des Hinweisgebersystems ist vor allem auf die Einhaltung der Unterrichts- und Auskunftspflicht gemäß Art. 13, 14 und 15 DSGVO, die korrekte Behandlung bei der Weitergabe der personenbezogenen Daten an Dritte,¹⁴¹ die Berichtigung, Sperrung und Löschung personenbezogener Daten zu achten. Hier ist zu berücksichtigen, dass der grundsätzlich zugunsten des Betroffenen bestehende Löschungsanspruch nach Art. 17 Abs. 1 DSGVO im Zusammenhang mit dem Betrieb eines Hinweisgebersystems eingeschränkt wird. Denn § 11 Abs. 5 HinSchG sieht eine Löschung der Dokumentation erst drei Jahre nach Abschluss des Verfahrens vor, wobei eine längere Aufbewahrung möglich ist, wenn und soweit dies zur Erfüllung von anderen gesetzlichen Anforderungen erforderlich und verhältnismäßig ist. § 11 Abs. 5 HinSchG stellt eine gesetzliche Ausnahme vom Löschungsanspruch nach Art. 17 Abs. 3 lit. b DSGVO dar. Denn die Dokumentation einer Meldung, die personenbezogene Daten enthält, ist eine Verarbeitung, die zur Erfüllung einer gesetzlichen Pflicht erfolgt.¹⁴² Als relevante gesetzliche Verpflichtungen gelten auch Speicherungspflichten der Mitgliedstaaten.¹⁴³

Von erheblicher praktischer Bedeutung ist auch die Frage, ob ein von einer Meldung Betroffener über den Auskunftsanspruch des Art. 15 DSGVO die Identität des Hinweisgebers erfahren kann. Das HinSchG verhält sich jedoch auch zu dieser Frage nicht. Ein Auskunftsanspruch gemäß Art. 15 DSGVO besteht jedoch dann nicht, wenn dieser durch Rechtsvorschriften der Union oder der Mitgliedstaaten zur Verhütung oder Aufdeckung von Straftaten oder zum Zweck des Schutzes der betroffenen Person oder der Rechte und Freiheiten anderer Personen eingeschränkt wird (Art. 23 Abs. 1 lit. d und lit. i DSGVO). Eine solche Beschränkung regelt § 29 Abs. 1 Satz 2 BDSG, wonach das Recht auf Auskunft dann nicht besteht, soweit die Auskunft Informationen offenbaren würde, die wegen der überwiegenden berechtigten Interessen eines Dritten geheim gehalten werden müssen. Im Ergebnis darf daher die Identität des Hinweisgebers auch gegenüber dem Betroffenen nicht offengelegt werden (siehe hierzu auch → Rn. 177 ff.).

Ein weiteres Beispiel für eine im HinSchG nicht adressierte Frage ist die Datenschutz-Folgenabschätzung nach Art. 35 Abs. 1 DSGVO, die bei einer Datenverarbeitung erforderlich ist, die aufgrund der Art und des Umfangs der Verarbeitung von Daten und der Zwecke dieser Verarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ hat. Hieraus folgert die Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder die Notwendigkeit einer Datenschutz-Folgenab-

141 Art. 6 Abs. 1 lit. f DSGVO i. V. m. § 24 Abs. 1 Nr. 1 BDSG zur Verfolgung von Straftaten.

142 *Handel*, Meldestellenbeauftragte, 2023, S. 95; *Dilling*, in: BeckOK HinSchG, § 11 HinSchG Rn. 24.

143 *Nolte/Werkmeister*, in: Gola/Heckmann, DS-GVO/BDSG, Art. 17 DS-GVO Rn. 46.

schätzung bei jeder Einführung eines Hinweisgebersystems.¹⁴⁴ Daher haben Unternehmen, die ein Hinweisgebersystem einrichten und betreiben wollen, im Vorfeld eine Datenschutz-Folgenabschätzung vorzunehmen.

IV. Die praktische Arbeit mit einem Hinweisgebersystem

- 169** Im Rahmen des praktischen Betriebs eines Hinweisgebersystems ergeben sich ergänzend einige wichtige Einzelfragen, auf die nachfolgend näher eingegangen werden soll.

1. Schutz des Hinweisgebers vor Nachteilen

- 170** Wie bereits oben unter → Rn. 115 ff. erläutert, ist der umfassende Schutz des Hinweisgebers ein wesentlicher Bestandteil der internen Regelungen des Unternehmens zum Hinweisgebersystem. So muss es intern strikt verboten sein, Mitarbeiter, die mutmaßliches Fehlverhalten melden, in irgendeiner Weise zu benachteiligen. Dieses Benachteiligungsverbot umfasst jede Maßnahme, die direkt oder indirekt einen negativen Einfluss auf das Arbeitsverhältnis des Mitarbeiters, seine Verdienst- oder Entwicklungsmöglichkeiten haben kann.¹⁴⁵ So wurde beispielsweise die Versetzung eines Hinweisgebers aufgrund der aus der Abgabe des Hinweises resultierenden Störung des Betriebsfriedens für rechtswidrig erklärt.¹⁴⁶
- 171** In der Praxis ist somit strikt darauf zu achten, dass bereits der Anschein vermieden wird, einem Hinweisgeber seien Nachteile aufgrund der Abgabe eines Hinweises entstanden.¹⁴⁷ Vor dem Hintergrund der gesetzlich angeordneten Beweislastumkehr zugunsten von Hinweisgebern bei Benachteiligungen (§ 36 Abs. 2 HinSchG) ist eine sorgfältige und detaillierte Dokumentation bei der Bearbeitung einer Meldung besonders wichtig. Denn dies erleichtert die Möglichkeit eines vom Unternehmen zu führenden Entlastungsbeweises erheblich, wenn – aus anderen Gründen – einmal Maßnahmen gegen einen Hinweisgeber ergriffen werden müssen. In diesem Zusammenhang zeigt sich auch die Bedeutung des Vertraulichkeitsgebots. Die Identität von Hinweisgebern sollte den für die Entscheidung über Personalmaßnahmen zuständigen Personen im Unternehmen

144 Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines, 14.11.2018, S. 12, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/11/OH-Whistleblowing-Hotlines-Stand-14_11_2018.pdf#page=12 (zuletzt abgerufen am 23.4.2024).

145 Moosmayer in: Rotsch, Criminal Compliance, § 34 C, Rn. 104.

146 VG Bremen, Urt. v. 8.9.2014 – 6 K 1003/14.

147 Dies kann sich im Einzelfall durchaus schwierig gestalten, da nicht übersehen werden darf, dass z. B. Kollegen eines Hinweisgebers, der offen als Hinweisgeber auftritt, auch durch den Arbeitgeber nicht dazu veranlasst werden können, z. B. weiterhin mit dem Hinweisgeber die Mittagspause zu verbringen oder ihn zum gemeinsamen Mittagessen mitzunehmen; dies wird bisweilen von Hinweisgebern bereits als Repression für die Abgabe des Hinweises wahrgenommen.

grundsätzlich nicht bekannt werden. Denn bei einer entsprechenden Funktions-trennung wird die Führung des Entlastungsbeweises deutlich erleichtert.

Durch die Abgabe eines Hinweises stellt sich der Hinweisgeber nicht selten ge- **172**
gen die etablierten formellen und informellen Hierarchien in dem Unterneh-
men.¹⁴⁸

Hinzu kommt, dass sich in der Praxis der Umgang mit Hinweisgebern nicht im- **173**
mer einfach gestaltet. So befinden sich als Hinweisgeber auftretende Mitarbeiter
häufig in schwierigen beruflichen oder persönlichen Situationen, mitunter auch
deshalb, weil sie bereits vor Abgabe des Hinweises im Kollegenkreis oder ge-
genüber den Vorgesetzten die von ihnen wahrgenommenen oder auch nur ange-
nommenen Missstände bereits mehrfach mitgeteilt haben und von Kollegen oder
Vorgesetzten keine Unterstützung erfahren haben. So entsteht bei Hinweis-
gebern häufig schnell Misstrauen gegenüber anderen Mitarbeitern des Unter-
nehmens, das sich auch auf die Mitarbeiter im Compliance-Bereich beziehen
kann.

Der Umgang mit Hinweisgebern erfordert daher neben umfassenden rechtlichen **174**
Kenntnissen und einer großen Erfahrung mit Compliance-Themen auch das not-
wendige „Fingerspitzengefühl“ im Umgang mit Menschen.¹⁴⁹ Der angemessene
Umgang mit Hinweisgebern ist auch vor dem Hintergrund des Wahlrechts des
Hinweisgebers zwischen interner und externer Meldestelle von Bedeutung.
Denn viele Hinweisgeber werden nur dann Vertrauen in das interne
Hinweisgebersystem haben, wenn sie bei der Behandlung ihrer Meldung das Ge-
fühl vermittelt bekommen, dass die Meldung ernst genommen und sorgfältig be-
arbeitet wird.

2. Schutz des Betroffenen

Auch der Schutz der von dem Hinweis betroffenen Person bedarf der Beachtung. **175**
So muss zum einen durch die strikte Einhaltung des Vertraulichkeitsgebots und
der datenschutzrechtlichen Vorgaben sichergestellt sein, dass keine unzulässigen
Eingriffe in die Persönlichkeitsrechte des Betroffenen stattfinden und dass die
Identität betroffener Personen nur insoweit weitergegeben wird, als dies für die
Ergreifung von Folgemaßnahmen notwendig ist.

Darüber hinaus haben die unternehmensinternen Vorschriften zum Hinweisma- **176**
nagement festzuhalten, dass ein vorsätzlich falscher Hinweis seinerseits als
Compliance-Verstoß gewertet wird und entsprechend sanktioniert wird.

¹⁴⁸ So auch *Moosmayer*, in: Rotsch, Criminal Compliance, § 34 C, Rn. 104, unter Hinweis auf
Buchert/Jacob-Hofbauer, in: Knierim/Rübenstahl/Tsambikakis, Internal Investigations,
S. 267.

¹⁴⁹ Zum Umgang mit Hinweisgebern und deren Psyche: *Benne*, CCZ 2014, 189 f.

3. Datenschutzkonformer Umgang mit eingegangenen Hinweisen

- 177 Werden personenbezogene Daten im Rahmen der Entgegennahme eines Hinweises ohne Kenntnis der betroffenen Person erhoben, ist diese gemäß Art. 14 DSGVO insbesondere über die Speicherung der Daten, die Art der Daten, den Zweck der Verarbeitung, die Identität des Verantwortlichen sowie gegebenenfalls auch über den Hinweisgeber zu informieren.¹⁵⁰ Durch diese Verpflichtung zur im Grundsatz erforderlichen umgehenden Information des Betroffenen entsteht insoweit in der Praxis ein Problem, weil eine sofortige Benachrichtigung zumindest zu einer wesentlichen Erschwerung der Aufklärung des Sachverhalts führen dürfte.¹⁵¹ Allerdings ermöglicht die Regelung des Art. 14 Abs. 5 lit. b DSGVO dann eine Ausnahme von der Pflicht zur Benachrichtigung, wenn die Verwirklichung der Ziele der Verarbeitung durch eine solche Benachrichtigung zumindest ernsthaft beeinträchtigt würde. Zum Schutz des berechtigten Interesses der beschuldigten Person nach Art. 14 Abs. 5 lit. b DSGVO ist die Information jedoch dann nachzuholen, sobald der Grund für den Aufschub entfallen ist.
- 178 Gemäß Art. 15 DSGVO haben sowohl der Hinweisgeber wie auch die von dem Hinweis betroffene Person Anspruch auf Auskunft der zu ihrer Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen. Dieser Auskunftsanspruch des Betroffenen kollidiert im Hinblick auf die Identität des Hinweisgebers offensichtlich mit den Grundsätzen eines effektiven Hinweisgeberschutzes und – nach Inkrafttreten des HinSchG auch mit dem zwingenden Vertraulichkeitsgebot aus § 8 HinSchG.¹⁵²
- 179 Ein Auskunftsanspruch gemäß Art. 15 DSGVO besteht jedoch dann nicht, wenn dieser durch Rechtsvorschriften der Union oder Mitgliedstaaten zur Verhütung oder Aufdeckung von Straftaten oder zum Zweck des Schutzes der betroffenen Person oder Rechte und Freiheiten anderer Personen eingeschränkt wird (Art. 23 Abs. 1 lit. d und lit. i DSGVO). Eine solche Beschränkung regelt § 29 Abs. 1 Satz 2 BDSG, wonach das Recht auf Auskunft dann nicht besteht, soweit die Auskunft Informationen offenbaren würde, die wegen der überwiegenden berechtigten Interessen eines Dritten geheim gehalten werden müssen.¹⁵³ Daher ist jedenfalls bei Meldungen, die im guten Glauben abgegeben werden, von einem überwiegenden berechtigten Interesse des Hinweisgebers auszugehen. Dies soll auch dann gelten, wenn die Bearbeitung einer Meldung abgeschlossen wurde, und sogar dann, wenn nach einer Untersuchung feststeht, dass kein Verstoß vorlag.¹⁵⁴

150 Vgl. hierzu Orientierungshilfe der DSK, S. 10. Zu den datenschutzrechtlichen Anforderungen im Rahmen des Compliance Managements ausführlich → *Böhlke/Becker/Fladung*, Kap. 12.

151 So auch von *Zimmermann*, RDV 2006, 247.

152 Vgl. zu diesem Spannungsverhältnis auch LAG Baden-Württemberg, Urt. v. 20.12.2018 – 17 Sa 11/18.

153 Vgl. hierzu auch Orientierungshilfe der DSK, S. 11.

154 *Handel*, Meldestellenbeauftragte, S. 86, m. w. N.

Ausgehend von Art. 17 Abs. 1 lit. a DSGVO ist die Verpflichtung zur Löschung von personenbezogenen Daten grundsätzlich daran zu messen, ob und wie lange die Kenntnis der Daten zur Erfüllung des Zwecks der Speicherung erforderlich ist. Allerdings stellt die gesetzliche Löschfrist nach § 11 Abs. 5 HinSchG gemäß Art. 17 Abs. 3 lit. b HinSchG eine Ausnahmeregelung dar, die den Löschanpruch des Betroffenen einschränkt (siehe → Rn. 166). Beim Betrieb des Hinweisgebersystems haben die für die interne Meldestelle zuständigen Personen daher darauf zu achten, dass die in § 11 Abs. 5 HinSchG geregelte Frist zur Löschung der Dokumentation eingehalten wird. Hierfür sollte ein Erinnerungs- oder Wiedervorlagesystem eingerichtet werden, das die Einhaltung der Löschfristen im Einzelfall gewährleistet. **180**

V. Fazit

Die Einführung eines Hinweisgebersystems im Unternehmen ist nicht nur von Gesetzes wegen geboten, sondern auch aus zahlreichen Gründen sinnvoll: **181**

Nur durch die frühzeitige Erkennung von unternehmensinternen Risiken kann die Unternehmensleitung angemessene Gegensteuerungsmaßnahmen ergreifen. Auch hat jedes Unternehmen ein vitales Interesse daran, dass – auch vermeintliche – Missstände zunächst im Unternehmen gemeldet werden und gegebenenfalls Abhilfe geschaffen werden kann und nicht „unkanalisiert“ Informationen an die Medien oder Strafverfolgungsbehörden gegeben werden.¹⁵⁵ Schließlich kann ein Hinweisgebersystem auch im Rahmen der Außendarstellung positiv genutzt werden. Immer häufiger wird auch im Rahmen von Vertragsverhandlungen die Existenz eines funktionierenden Compliance-Management-Systems und damit auch eines Hinweisgebersystems national und international abgefragt. **182**

Bei der Ausgestaltung des Hinweisgebersystems sind vor allem an der Branche, der Größe, der Internationalität des Unternehmens ausgerichtete Entscheidungen zu treffen. Besonders wichtig ist hierbei die Wahl der Eingangswege für Hinweise, die Bestimmung des Kreises potenzieller Hinweisgeber und eine klare Regelung der zu meldenden Themen. **183**

Bei der Ausgestaltung des Hinweisgebersystems sind vor allem an der Branche, der Größe, der Internationalität des Unternehmens ausgerichtete Entscheidungen zu treffen. Besonders wichtig ist hierbei die Wahl der Eingangswege für Hinweise, die Bestimmung des Kreises potenzieller Hinweisgeber und eine klare Regelung der zu meldenden Themen. **184**

Bei der Ausgestaltung des Hinweisgebersystems sind vor allem an der Branche, der Größe, der Internationalität des Unternehmens ausgerichtete Entscheidungen zu treffen. Besonders wichtig ist hierbei die Wahl der Eingangswege für Hinweise, die Bestimmung des Kreises potenzieller Hinweisgeber und eine klare Regelung der zu meldenden Themen.

Von entscheidender Bedeutung für das Funktionieren des Hinweisgebersystems ist jedoch die Akzeptanz gerade bei den Mitarbeitern. Hierfür erforderlich ist vor allem eine glaubwürdige Kommunikation durch die Unternehmensleitung (Tone from the Top), ein transparenter und nachvollziehbarer, datenschutzkonformer Umgang mit eingehenden Hinweisen und nicht zuletzt ein effektiver Schutz sowohl des Hinweisgebers als auch des von einem Hinweis betroffenen Mitarbeiters.

¹⁵⁵ Allgemein zum Thema Meldeverhalten von Whistleblowern, *Herold*, Whistleblower – Entscheidungsfindung, Meldeverhalten und kriminologische Bewertung, S. 196 ff.

6. Kapitel

Kommunikationsmanagement und Schulungen (analog und remote)

I. Einleitung

Kommunikationsmanagement und Schulungen sind zur Umsetzung eines Compliance-Management-Systems in der Praxis ein unverzichtbares Kernelement.¹ Unter Kommunikationsmanagement wird in diesem Zusammenhang jede Maßnahme verstanden, die sich aus der Compliance-Abteilung oder einer unterstützenden Funktion, direkt oder indirekt an die Mitarbeiter wendet. Ziel dabei ist die Sensibilisierung der Organe und Mitarbeiter für Compliance-Themen und deren Umsetzung im Unternehmen. Schulungen sind dabei ein Tool des Kommunikationsmanagements, welches wegen seiner herausragenden Bedeutung gesondert dargestellt und untersucht wird. 1

Das vorliegende Kapitel befasst sich dabei zunächst mit den Grundzügen der Kommunikation (→ Rn. 3 ff.). Hierbei werden nach der allgemeinen Betrachtung der Relevanz der Compliance-Kommunikation im Unternehmen zunächst Modelle aus der Kommunikationswissenschaft kurz dargestellt, um im Anschluss daran deren Praxisrelevanz an einem Beispiel zu verdeutlichen. Aus der langjährigen Erfahrung der Autorin hat sich gezeigt, dass Wissen für die Compliance-Officer hier sehr hilfreich ist, in der Praxis allerdings oftmals fehlt. Abschnitt III. (→ Rn. 20 ff.) zeigt ausgewählte Instrumente der Compliance-Kommunikation, die sich in den letzten Jahren in der Unternehmenspraxis bewährt haben. In Abschnitt IV. (→ Rn. 32 ff.) werden die verschiedenen Modalitäten der Compliance-Schulungen näher betrachtet, wobei sowohl Präsenzvarianten als auch digitale remote Lösungen erläutert werden. Der nächste Abschnitt setzt sich mit den in der Praxis am häufigsten auftretenden Stolpersteinen in der Compliance-Kommunikation auseinander und zeigt Lösungsansätze, u. a. unter Verwendung der in Abschnitt II. (→ Rn. 3 ff.) aufgezeigten Kommunikationsmodelle auf. Der letzte Abschnitt (→ Rn. 106 ff.) zieht ein Fazit aus den vorab betrachteten Gesichtspunkten. 2

1 *Hastenrath*, in: Bay/Hastenrath, Compliance-Management-Systeme, S. 183. Zur Compliance-Kommunikation ausführlich *Hastenrath*, Compliance-Kommunikation. Siehe auch → *Schulz*, Kap. 1 Rn. 78 ff. m. w. N.

II. Grundzüge zur Kommunikation in der Unternehmenspraxis

1. Relevanz der Kommunikation im Unternehmen und bei Compliance

- 3 Die richtige Kommunikation des Compliance Officers,² einem Kernelement eines CMS und einer Kernqualifikation eines Compliance Officers,³ ist unverzichtbar für den Erfolg von Compliance. Dies soll an einem Beispiel einer Kommunikationssituation geschildert werden. Das Beispiel zeigt eine erfolgreiche Kommunikationsstrategie.

4 **Beispiel: Erfolgreiche Kommunikation des Chief Compliance Officers mit der Rechtsabteilung**

Der junge Chief Compliance Officer (folgend: CCO) ist neu in das Unternehmen gekommen. Er ist mittlerweile seit etwas über drei Monaten mit dem Aufbau eines Compliance-Management-Systems im Unternehmen beschäftigt. Teil davon ist auch die Einführung einer Antikorruptionsrichtlinie, wozu er den ausdrücklichen Auftrag des Vorstands hat. Alle Rechtsthemen, wozu bisher auch die Richtlinienhoheit zählte, lagen bisher in der ausschließlichen Zuständigkeit der Rechtsabteilung. Die General Counsel ist eine angesehene Kollegin, die seit mehr als 25 Jahren für das Unternehmen tätig ist. Sie wird diese Position noch bis zu ihrem in zwei Jahren angestrebten Ruhestand innehaben.

Der Chief Compliance Officer fragt bei der General Counsel nach einem Termin zwecks der Vorstellung seiner Person, seiner Aufgabenstellung und ersten gemeinsamen Ideen, wie man eine Antikorruptionsrichtlinie, eine der Aufgaben, die der Vorstand ihm zugewiesen habe, ausgestalten könne. Ein Termin in zwei Wochen im Büro der General Counsel wird vereinbart.

Der Termin beginnt mit dem Eintreffen des CCO, der sich um zehn Minuten verspätet hat, da sein Vorgesetzter, der CEO ihn kurzfristig angerufen hat. Der CCO begrüßt die General Counsel und entschuldigt sich für seine Verspätung. Ihm sei dies wirklich unangenehm, er wisse, wie viele Termine die General Counsel habe. Es sei aber so gewesen, dass sein Chef, der CEO, ihn angerufen habe, als er sich gerade auf den Weg zur General Counsel habe machen wollen. Da er ja noch relativ neu im Unternehmen sei und seinen Chef nicht enttäuschen wollte, wäre er jetzt leider zehn Minuten zu spät ge-

2 Auch *Nothelfer*, CCZ 2013, 23, 28, sieht in der ausgeprägten Kommunikationsfähigkeit des Compliance Officers einen Schlüssel für die erfolgreiche Einführung eines CMS; ebenso *Schulz/Renz*, CB 2013, 294, 297, die Kommunikations- und Schulungsmaßnahmen des Compliance Officers als Schlüsselfunktion bezeichnen; zu digitalen Kommunikationsanforderungen an den Compliance Officer: *Hastenrath*, Compliance Praxis (Österreich), Ausgabe 4/2019, S. 16 ff.; vgl. auch zur Relevanz des Elements: IDW Verlautbarungen, Werkstand: IDW Life 2/2024, Rn. 27

3 *Raum*, Vorsitzender Richter des 1. Strafsenats am BGH, in: *Hastenrath*, Compliance-Kommunikation, S. 37.

kommen. Die General Counsel nickt und bestätigt, dass sie derartige ad-hoc Anrufe ihres Vorgesetzten auch des Öfteren erhalte und sich deshalb verspäte. Sie habe Verständnis für seine Lage und jetzt wäre er ja da. Sie wäre schon sehr gespannt, was es mit der Compliance-Funktion auf sich habe, sie hätte nur am Rande mitbekommen, dass diese Funktion jetzt neu geschaffen werde und u. a. auch einige Rechtsthemen behandeln solle. Da sie aber in den letzten Wochen ein großes Projekt in den USA vor Ort betreut habe, sei sie noch nicht zur tieferen Befassung mit dem Thema gekommen. Der CCO fragt interessiert zu diesem USA-Projekt und sagt, wie herausfordernd solche Projekte sicherlich seien und dass er großen Respekt davor habe, ein solches Projekt, wie die General Counsel, komplett intern, ohne externe Anwälte, zu bewältigen.

Der CCO händigt im nun folgenden Verlauf eine Präsentation an die General Counsel aus. Er habe ihr diese eigentlich schon vorab zukommen lassen wollen, aber leider sei ihm auch hier eine kurzfristige Aufgabe durch seinen Chef dazwischengekommen. Er fragt, ob es deshalb in Ordnung sei, wenn er sie stattdessen durch die Präsentation zu den Grundzügen von Compliance in ihrem gemeinsamen Unternehmen sowie seinen genauen Aufgaben und möglichen Schnittstellen zum Rechtsbereich führen könne. Die General Counsel ist einverstanden.

In der Präsentation zeigt der CCO insbesondere seine Aufgaben für dieses Jahr auf. Dazu gehört das Erstellen einer Antikorruptionsrichtlinie. Er bittet die General Counsel hier um ihren besonderen Input sowie ihre Vorstellung zur Ausgestaltung dieser Schnittstelle, da er weiß, dass die Richtlinienhoheit bisher erfolgreich durch die Rechtsabteilung ausgeübt wurde. Wenn das so in Ordnung sei, würde er als CCO gerne einen ersten Grobentwurf zu der Antikorruptionsrichtlinie machen und diesen dann mit der General Counsel besprechen, um insbesondere von ihrer langjährigen Erfahrung im Verfassen von Richtlinien in ihrem Unternehmen zu profitieren und ihre gemeinsame Schnittstelle sauber zu definieren.

Das Telefon der General Counsel klingelt in diesem Moment. Diese nimmt ab, nickt kurz und legt auf. Sie kehrt an den Besprechungstisch zurück und sagt, dass sie sich jetzt leider nur noch zehn Minuten Zeit für ihn nehmen könne, da ihr Chef sie ad hoc in zwanzig Minuten in sein Büro gebeten habe. Sie habe aber bereits einen guten Einblick in die Materie gewonnen und ist einverstanden, dass der CCO einen ersten Entwurf einer Richtlinie schreibt und sie diesen besprechen. Da der CCO auf seinen Zeitdruck zur Fertigstellung der Richtlinie hinweist, verspricht ihm die General Counsel, einen Termin, so schnell wie ihre eigenen Termine es zulassen, einzuplanen. Beide verabschieden sich.

Wie das Fallbeispiel bereits nach dieser kurzen Darstellung zeigt, kann der Grundstein für eine fruchtbare Zusammenarbeit durch ein gutes Kommunikati- **5**

onsmanagement gelegt werden. Und dies ist bereits auf Grundlage eines einzigen Gesprächs möglich.

- 6 Damit zeigt sich, wie relevant ein gutes Kommunikationsmanagement ist und dass hierfür einerseits genug Zeitreserven eingeplant werden müssen, andererseits für Compliance-Mitarbeiter und CCO Kenntnisse und Fortbildungen in diesem Bereich unabdingbar sind.

2. Kommunikationsmodelle

- 7 Wie sich oben (→ Rn. 4) gezeigt hat, kann bereits eine einzige, richtig vorbereitete und geführte Kommunikation zu positiven Ergebnissen für den Erfolg der Compliance-Arbeit führen. Daher ist es notwendig für die Compliance-Verantwortlichen, gewisse Modelle anlässlich und über die Kommunikation zu kennen, um derartige Erfolge erzielen zu können. Der nachfolgende Abschnitt stellt zwei Modelle vor, die für die Compliance-Arbeit besonders relevant sind.

a) Modell zu Konfliktarten als Grundlage für die Kommunikation

- 8 Besonders relevant für die Compliance-Arbeit ist das Modell zu Konfliktarten nach *Benien*,⁴ wonach sich jede Kommunikation, auch die Compliance-Kommunikation, im Konfliktfall spezifisch einordnen lässt. *Benien* beschreibt vier Konfliktarten, nämlich den inneren Konflikt, den Bedürfniskonflikt, den Sachkonflikt und den Beziehungskonflikt. Dies wird in folgender Grafik verdeutlicht:



Abbildung 1: Konfliktarten nach *Benien*

4 Siehe dazu das Gesamtwerk *Benien*, in: Benien, Schwierige Gespräche führen. Modelle für Beratungs-, Kritik- und Konfliktgespräche im Berufsalltag, S. 1 f.

Für die Compliance-Arbeit relevant sind insbesondere der **Sach-** und der **Beziehungs-** 9
konflikt, sodass sich die folgende Betrachtung darauf beschränkt.

Sachkonflikte lassen sich in drei Unterkategorien aufteilen und sind beispielsweise: 10

1. Rechtskonflikte

Hier streiten die verschiedenen Parteien darum, wer Recht hat z. B. nach der aktuellen Gesetzeslage oder Rechtsprechung. Daher gibt es auch eine autorisierte Entscheidungsinstanz in Form der Gerichte, die hier eine finale Entscheidung erzielen kann. Wenn die Parteien unbedingt jeweils Recht haben wollen, kann sich hieraus schnell ein Beziehungskonflikt entwickeln.⁵

2. Bewertungskonflikte

Hier geht es um verschiedene Sichtweisen, Eigenschaften oder Verhaltensweisen, ohne dass eine Partei objektiv und sicher wissen kann, was richtig oder falsch ist. Beispiele hierfür sind Bewertungen der Wichtigkeit oder der Rangfolge von anfallenden Arbeiten, unterschiedliche Interpretation von Effizienz, Sinnhaftigkeit, Nützlichkeit usw.

3. Verteilungskonflikte

Verteilungskonflikte sind ökonomische Konflikte beim Kampf um knappe oder begehrte Güter. Beispiele sind mehrere Bewerbungen um eine Position, ein bestimmtes Büro, ein spezieller Parkplatz auf dem Firmengelände oder Konflikte um Marktanteile.

Diese sind zu unterscheiden von den sogenannten **Beziehungskonflikten**, 11
 die sich ebenfalls in drei Unterkategorien unterteilen lassen:

1. Grenzkonflikte

Grenzkonflikte kommen bei der Verletzung im persönlichen Umgang und deren Grenzen vor. Beispiele hierfür können indiskrete Fragen des Chefs zu privaten Themen des Mitarbeiters sein oder Uneinigkeit über die Regeln für den gemeinsamen Umgang. Diese Grenzkonflikte werden häufig als Sachkonflikte getarnt.

2. Persönlicher Angriff

Hierunter fallen Angriffe auf das Selbstwertgefühl und die Identität des Kollegen oder Mitarbeiters, wobei es zu einer Abwertung des Anderen als Person insgesamt kommt. Beispiele dafür sind etwa Vorwürfe, dass man jemandem nicht geholfen hat, unsachliches und inhaltlich ungerechtfertigtes, wiederholtes Schlechtmachen von Leistungen des Gegenübers, Aberkennen der Leistungen und Werte bzw. Wertvorstellungen einer Person. Dies löst fast immer Verärgerung aus, die zu Impulsen führt, das gestörte Selbstbild wieder herzustellen, sich also durch Gegenangriffe zu wehren.

⁵ Dazu sogleich ausführlich unter dem Punkt Beziehungskonflikte (→ Rn. 11).

3. Vertrauenskrise

Hierbei wird die Beziehung zwischen den Parteien durch den Verdacht belastet, dass der Andere nicht aufrichtig und ehrlich agiert und dies vorsätzlich zulasten des Anderen tut. Beispiele hierfür sind das wiederholte Missachten von Vereinbarungen, das bewusste Hintergehen der Gegenpartei zu deren Schaden und dem eigenen Nutzen oder die Abgabe von falschen Versprechungen, die nicht eingehalten werden.

- 12** Im Kommunikationsmanagement muss man sich diese beiden Ebenen von Sach- und Beziehungskonflikt bewusst machen. Betrachten wir das obige Beispiel, zeigt sich, dass eine gemeinsame Arbeitsebene mit gegenseitigem Respekt gefunden wurde. In diesem Beispiel haben keine Angriffe auf der Beziehungsebene stattgefunden. Vielmehr hat der Chief Compliance Officer die Herausforderungen auf der Beziehungsebene vorbildlich gelöst. Er betont in allen Situationen seine eigene „Drucksituation“ und entschuldigt sich für die Unannehmlichkeiten, die dies der General Counsel bereiten könnte. Zudem schätzt er ihre Erfahrung und ihre bisherigen Leistungen. Auch dieses Verhalten spiegelt sich im Verhalten der General Counsel. Sie zeigt einerseits Verständnis für die Dilemmata des Chief Compliance Officers, andererseits kommt sie auf ihn zu und erklärt, unter welchen Zwängen sie selbst steht.
- 13** Die Kenntnis zwischen Sach- und Beziehungsebene ist daher in vielen Situationen im Compliance-Bereich maßgeblich für dessen Erfolg, denn die mangelnde Kenntnis, dass Beziehungsprobleme nicht auf der Sachebene lösbar sind, verhindert dagegen regelmäßig den Erfolg.

b) Praxisrelevantes Beispiel

- 14** Ein weiteres, relevantes Modell für die Compliance-Kommunikation ist der sogenannte „**4-Schritte-Dialog**“. Dies ist eine spezielle Technik, festgefahrene und emotional aufgeladene Gespräche wieder in eine konstruktive Richtung zu lenken. Diese Dialogform ist insbesondere für bilaterale Gespräche geeignet. Einsetzbar im Compliance-Bereich ist diese immer, wenn die Person mit der Compliance-Funktion und die eine andere Funktion wahrnehmende Person als Gegenüber, etwa aus dem Bereich Einkauf oder Vertrieb, konträre Ziele haben und diese Ziele im bisherigen Gesprächsverlauf mit zunehmender Vehemenz verteidigt haben.
- 15** Der 4-Schritte-Dialog setzt sich wie folgt zusammen:
- **Schritt 1** beinhaltet, eine Beobachtung zu formulieren, ohne zu werten. Dies ist in Praxis nicht einfach und muss vor einem wichtigen Gespräch oftmals geübt werden, da der Gesprächsführende sonst sofort in eine Bewertung verfällt, statt seine objektive Beobachtung zu äußern.

- **Schritt 2** gibt die Stimmung und Gefühle wieder, die die sich äuernde Person in der konkreten Situation hat.
- **Schritt 3** formuliert das Bedürfnis, welches der Vortragende hat. Achtung! Dieses unterscheidet sich gegenüber einer Bitte/einem Wunsch (wie in Schritt 4 formuliert), da hier das dahinterliegende Interesse vorgetragen wird, welches sich nicht nur auf diese Gesprächssituation bezieht. Eine derartige Öffnung muss ebenfalls vorab in leichteren Situationen geübt werden, ansonsten mangelt es häufig an der Fähigkeit, sich diesbezüglich zu offenbaren, was jedoch für den Erfolg des 4-Schritte-Dialogs elementar ist.
- **Schritt 4** formuliert eine konkrete Bitte/einen konkreten Wunsch. Ein Wunsch ist in der Regel leichter zu akzeptieren als eine Forderung.

Als Beispiel für das Formulieren jeweiliger Einleitungssätze können folgende Muster gut verwendet werden, ohne zu „weich“ zu wirken, sodass diese auch im Business-Kontext einsetzbar sind:

Phase 1:

„Ich habe gerade/jetzt/im Verlauf des Gesprächs beobachtet ...“

„Mir ist aufgefallen, dass ...“

„Ich habe bemerkt, dass ...“

„Folgenden Punkt habe ich im Verlauf unseres Gesprächs beobachtet: ...“

Phase 2:

„Das wirkt auf mich irritierend/merkwürdig/unpassend.“

„Das verärgert/ärger mich.“

„Das ist für mich unbefriedigend.“

Phase 3:

„Ich habe das Bedürfnis/die Vorstellung, dass wir zu einem Ergebnis kommen/dass wir in diesem Gespräch jetzt wieder zum eigentlichen Kernpunkt zurückkommen/dass Sie mich und meine Funktion respektieren ...“

Phase 4:

„Mein Wunsch/mein Ziel ist es, dass wir heute ...“

„Ich würde heute gerne zu folgendem Ergebnis kommen, dass ...“

Als Beispiel für den 4-Schritte-Dialog in konkreten Compliance-Kommunikationssituationen dienen folgende Beispiele:

Beispiel 1:

Phase 1:

„Folgenden Punkt habe ich im Verlauf unseres Gesprächs beobachtet: Sie sind mit der Stimme zunehmend laut geworden und haben mich mehrfach mit der Aussage, dass unsere Firma diese Compliance-Maßnahme nicht brauche, in meinen Ausführungen unterbrochen.“

16

17

Phase 2:

„Das verärgert mich.“

Phase 3:

„Ich habe die Vorstellung, dass wir eine Lösung für die angedachte Maßnahme finden, da ich sehr hohen Druck von der Geschäftsleitung habe, diese in den nächsten vier Wochen umzusetzen. Sollte mir dies nicht gelingen, werde ich bei meinem Vorgesetzten in große Erklärungsnot kommen.“

Phase 4:

„Mein Wunsch ist es daher, dass wir eine für uns beide gangbare Lösung finden, die Compliance-Maßnahme so umzusetzen, dass Sie nicht unnötig in Ihren operativen Tätigkeiten beschränkt werden und wir dabei keinem hohen Risiko eines Rechtsverstößes ausgesetzt sind.“

18 Beispiel 2:

Phase 1:

„Ich habe bemerkt, dass Sie die Fäuste unter dem Tisch ballen und den Kopf mehrfach ablehnend geschüttelt haben.“

Phase 2:

„Das irritiert mich.“

Phase 3:

„Ich habe das Bedürfnis, dass wir zu einem Ergebnis kommen, denn es ist Teil meines Tätigkeitsbereichs, möglicherweise nicht mehr adäquate Verhaltensweisen der Mitarbeiter in sicherere Alternativen zu verändern. Das ist nicht gegen Sie oder die Mitarbeiter Ihrer Abteilung gerichtet. Wenn ein Verstoß passiert, kann ich als Chief Compliance Officer nicht nur meinen Job verlieren, sondern auch persönlich zivil- und strafrechtlich verfolgt werden.“

Phase 4:

„Ich würde heute gerne zu folgendem Ergebnis kommen: Wir suchen gemeinsam nach Möglichkeiten, wie Sie und Ihre Mitarbeiter in Zukunft agieren können, ohne einen Rechtsverstoß zu riskieren bzw. einen solchen nach Möglichkeit weitestgehend zu minimieren.“

- 19** Viele kritische Compliance-Gespräche können so vor einer Eskalation bewahrt werden. Dies wird umso wichtiger, als dass die Compliance-Aufgaben in den folgenden Jahren voraussichtlich immer komplexer und globaler werden, während die wirtschaftliche Lage durch den Angriffskrieg Russlands und den dadurch verursachten globalen Verwerfungen für deutsche Unternehmen schwieriger werden wird. Dies wird zu wachsenden Spannungen zwischen zunehmendem operativem Druck bei gleichzeitig verstärkten Compliance-Vor-

gaben diverser Gesetz- und Standardgeber führen. Wenn die Parteien sich aber gegenseitig ihre hinter ihren vertretenen Positionen liegenden Interessen und Bedürfnisse mitteilen, entsteht ein ganz anderes Verständnis des Gegenübers. So können Lösungen gefunden werden, die für beide Seiten akzeptabel sind. Nur solche Lösungen haben langfristig Erfolg und werden von der Gegenseite mitgetragen. Lösungen, die einer Seite qua Weisungsbefugnis oder qua der Entscheidungsgewalt des Gegenübers mit Druck aufgezwungen und gegebenenfalls nicht verstanden werden, führen regelmäßig zu Gegendruck.⁶ Dieser kann sich im möglichen Umgehen oder Untergraben der Lösung manifestieren. Der 4-Schritte-Dialog sollte deshalb als Möglichkeit der guten Compliance-Kommunikation in passenden Situationen in Betracht gezogen werden.

III. Ausgewählte Instrumente der Compliance-Kommunikation

1. Tone from the Top

Unabdingbare Grundlage für jedes funktionierende Compliance-Management-System ist ein „**Tone from the Top**“ oder, oftmals synonym verwendet, ein „Tone at the Top“ der Geschäftsleitung.⁷ Ein Tone at the Top ist ein ernstgemeintes Bekenntnis („Commitment“) der Unternehmensspitze, sämtliche relevanten Vorgänge, Prozesse, Verträge, Geschäftspartner, Expansionspläne und Ähnliches mehr auf ihre Rechtskonformität durch die Compliance-Abteilung und angrenzende Funktionen prüfen zu lassen und im Zweifelsfall, also bei hoher Wahrscheinlichkeit eines Rechtsverstoßes oder Reputationsrisikos, davon Abstand zu nehmen, auch wenn sich dies unter Umständen kurzfristig negativ auf die Umsätze auswirkt oder man sich von langjährigen Geschäftspartnern trennen muss.⁸ Ein Ausdruck davon kann auch die Kündigung von wichtigen Funktionsträgern und Umsatzverantwortlichen sein, etwa wenn diese in rechtswidrige Geschäfte verwickelt sind. In den letzten Jahren hat sich der Fokus hin zu einer „Action-at-the-Top“ bzw. eines „Conduct-at-the-Top“ als Best Practice verlagert, die sogar noch mehr vom Top-Management verlangt, nämlich ein konkretes Verhalten für ein regeltreues Verhalten der Belegschaft.⁹ 20

In der Praxis entscheidend sind Anhaltspunkte für Umsetzungsformen des Tone-from-the-Top, wie das Budget und die Ressourcenausstattung der Compliance-Abteilung, die Einbindung in relevante Geschäfte und strategische Entscheidungen, der Schutz der Compliance-Mitarbeiter oder die Incentivierung von compliance-gerechtem Verhalten.¹⁰ 21

⁶ Dieses Druckverhalten zeigt sich auch in den steigenden Zahlen der Begehung von Veruntreuung, Betrug und Unterschlagung durch Unternehmensmitarbeiter, vgl. *Klinger*, in: *Klinger*, Das Interne Kontrollsystem im Unternehmen, S. 8.

⁷ Siehe hierzu → *Schulz*, Kap. 1 Rn. 69 m. w. N.

⁸ Ausführlich → *Schulz*, Kap. 1 Rn. 24 ff. m. w. N.

⁹ Siehe → *Schulz*, Kap. 1 Rn. 68 ff.

¹⁰ Eine ausführliche Darstellung hierzu in *Hastenrath*, in: *Hastenrath*, Compliance-Kommunikation, Kap. 6 Rn. 17 ff.

- 22 Für einen fehlenden Tone from the Top können das Fehlen der vorgenannten Punkte sowie vor allem versteckte Äußerungen der Geschäftsführung gegen Compliance sprechen.¹¹

2. Persönlicher Kontakt mit dem Compliance Officer

- 23 Viele Compliance-Situationen sind durchaus kritisch. Das heißt, wenn ein Mitarbeiter eine solche Situation dem Compliance Officer offenbart, muss dafür vorab ein grundsätzliches Vertrauensverhältnis bestehen. Dies insbesondere dann, wenn es keinen Schutz für interne Hinweisgeber in einer Richtlinie oder Ähnlichem gibt. Ein solches Vertrauen kann nur über den persönlichen, zwischenmenschlichen Kontakt mit dem Compliance Officer aufgebaut werden. Der Ersatz durch reine Online-Videomeetings kann dies nicht leisten und ist daher kritisch zu betrachten.
- 24 Es ist daher für den Compliance Officer ratsam, jede Chance zu einem persönlichen Kontakt mit den Mitarbeitern zu suchen. Neben gemeinsamen Kantinenbesuchen können dies etwa eine offene Sprechzeit des Compliance Officers, regelmäßige Rundgänge im eigenen Haus sowie Besuche bei den Tochtergesellschaften, die entsprechend ausführliche Bearbeitung von Anfragen mit persönlicher Erklärung oder die Teilnahme am Betriebssport sein. Auf internationalem Level sind dafür Dienstreisen unverzichtbar, die im Budget für Compliance daher hinreichend berücksichtigt werden müssen.

3. Zusammenarbeit des Compliance Officers mit Schlüsselfunktionen im Unternehmen

- 25 Ob ein Compliance-Management-System Erfolg hat, hängt in hohem Maße von der Unterstützung der Compliance-Abteilung durch andere Abteilungen ab, die mit dem Thema eine oder mehrere Schnittstellen haben.¹² Deshalb ist es gerade in der Etablierungsphase von Compliance notwendig, mit allen Leitern und gegebenenfalls mit zusätzlichem Personal der Abteilungen zu sprechen und gemeinsame Strategien und Synergien zu erarbeiten, sowie Doppelbearbeitungen zu vermeiden. Neben Gesprächen können diese Schnittstellenfunktionen auch in einem beratenden Compliance-Gremium gebündelt werden. Damit wird das Fachwissen sehr zeitsparend zusammengezogen und andererseits besteht für den Compliance Officer die Chance, mögliche Vorbehalte gegen seine Funktion abzubauen oder mindestens zu minimieren.

11 Eine ausführliche Darstellung hierzu in *Hastenrath*, in: *Hastenrath*, Compliance-Kommunikation, Kap. 6 Rn. 25 ff.

12 Zu dem erforderlichen „Schnittstellenmanagement“ siehe auch → *Schulz*, Kap. 1 Rn. 85; → *Rau*, Kap. 3; sowie → *Renz/Frankenberger*, Kap. 20.

4. Schriftliche Informationen an die Mitarbeiter

Sowohl beim Aufbau als auch beim Ausbau und der Anpassung bestehender Compliance-Management-Systeme ist eine der wichtigsten Maßnahmen, die adressierten Mitarbeiter ausreichend zu informieren. Dazu zählt zunächst eine frühzeitige Information zu anstehenden Compliance-Maßnahmen. Dann sind die konkreten Maßnahmen zu planen, um auch die zeitliche Verfügbarkeit der Mitarbeiter zu sichern. Im Nachgang zu Schulungen oder der Verteilung neuer Richtlinien sind weitere Erklärungen und Erläuterungen dazu zu verfassen. Neben der Ansprache per E-Mail, welche in Zeiten der E-Mail-Fluten leicht untergeht, sind persönliche Hinweise für die räumlich erreichbaren Mitarbeiter, ein Hinweis im Compliance-Bereich des Intranets sowie Aushänge an schwarzen Brettern und die Ankündigung der Compliance-Maßnahmen durch Dritte in deren Management-Veranstaltungen oder Abteilungs-Meetings ratsam. 26

5. Compliance im firmeneigenen Intranet

Der Aufbau und das Betreiben eines eigenen Intranetauftritts im Rahmen des Intranets des Unternehmens sind für die Compliance-Abteilung ratsam. In der Praxis ist es häufig so, dass eine zentrale Compliance-Abteilung etabliert ist. Teilweise sind in großen Tochtergesellschaften oder nach Regionen geordnet noch zusätzliche Vollzeitkräfte mit fachlicher Führungsverantwortung nachgeschaltet. Die weitere Compliance-Arbeit wird jedoch auf lokaler Ebene durch Compliance-Mitarbeiter ausgeführt, die in ihrer Hauptfunktion mit anderen Aufgaben betraut sind. Diese kennen sich in den einzelnen Compliance-Fachthemen häufig nicht ausreichend aus und vernachlässigen das Thema ggf. gänzlich, wenn sie nicht ausreichend von den zentralen Compliance-Funktionen mit Informationen versorgt werden und diese ebenfalls Anforderungen zu eigenen Tätigkeiten der lokalen Compliance-Mitarbeiter stellen. 27

Da eine permanente, persönliche Information der dezentralen Funktionen sowohl aus Kapazitätsgesichtspunkten als auch aus finanziellen Gründen kaum möglich ist, haben viele zentrale Compliance-Funktionen einen eigenen Intranetauftritt aufgebaut, auf den im Idealfall alle Mitarbeiter zeitunabhängig Zugriff haben. 28

Eine sinnvolle Aufteilung des Intranetauftritts in Unterthemen kann wie folgt aussehen: 29

- Im Bereich „Compliance Basics“ werden Grundelemente des firmeneigenen Compliance-Systems erklärt.
- Im Bereich „Interne Grundlagen“ werden zusätzliche Dokumente wie die Unternehmensgrundsätze und Führungsleitlinien hinterlegt, die zwar keine originären Compliance-Dokumente sind, aber oftmals wichtige Voraussetzungen für die Einhaltung der Compliance-Vorgaben schaffen.
- Im Bereich „Der Unternehmens-Kodex“ werden dieser sowie zusätzliche Beispiele aufgeführt.

- Im Bereich „Übersichten, Richtlinien u. a. m.“ werden die wichtigsten Grundlagendokumente von und für Compliance hinterlegt und mögliche Hinweise zu Schulungsterminen veröffentlicht.
 - Im Bereich „Relevante Vorgaben und Gesetze international“ können nationale Besonderheiten dargestellt werden. So können Gemeinsamkeiten und Unterschiede und gegebenenfalls Anpassungsbedarfe für einzelne Länder leichter ermittelt werden.
 - Im Bereich „Compliance-Organisation und Schnittstellen zu anderen Bereichen“ werden Aufgaben und Zuständigkeiten der Compliance-Abteilung in Abgrenzung zu angrenzenden Funktionen dargestellt.
 - Im Bereich „Hinweise“ können, soweit es in die Firmenkultur passt, Hinweise von Mitarbeitern anonym oder nicht anonym aufgenommen werden.
- 30** Die Erarbeitung eines derartigen Intranetauftritts erfordert neben einem hohen Zeitaufwand bei der Etablierung auch einen ständigen Pflegeaufwand, um neue Beispiele, Gesetzesänderungen, Schulungsankündigungen oder Personalwechsel aktuell anzuzeigen.¹³
- 31** Soweit das Unternehmen statt oder neben einem Intranet auch die Möglichkeit der Etablierung einer App für die Mobilfunkgeräte der Mitarbeiter hat, kann auch dies für Compliance-Informationen genutzt werden. Dann müssen die Inhalte ggf. verkürzt werden, um für das Format besser nutzbar zu sein.

IV. Schulungen

1. Persönliche Schulungen durch die Compliance-Funktion

- 32** Persönliche Schulungen durch den Chief Compliance Officer oder seine Mitarbeiter sind die unverzichtbare Grundlage, den Mitarbeitern die Compliance-Fragstellungen aufzuzeigen und notwendiges Vertrauen zum Chief Compliance Officer und seinen Mitarbeitern aufzubauen.¹⁴ In den Schulungen, die je nach Adressatengruppe individuell angefertigt und aufgebaut sein müssen, können die Mitarbeiter wichtige Rückfragen stellen.¹⁵ Dies ist wichtig, um das Verständnis der Mitarbeiter für die Themen tatsächlich zu gewinnen. Daneben können zusätzliche Mitarbeiterfragen die Compliance-Abteilung auf relevante Prozesse und Sachverhalte hinweisen, die die Compliance-Abteilung bisher noch nicht angeschaut hat, in denen aber unter Umständen Risiken stecken, die bearbeitet werden müssen.

13 Ausführlich zum Aufbau eines Compliance-Intranet-Auftritts *Hastenrath*, in: Bay/Hastenrath, Compliance-Management-Systeme, S. 190 ff.

14 Vgl. zur Bedeutung von Präsenzs Schulungen: *Zimmermann*, in: Momsen/Grützner, Wirtschaftsstrafrecht: Handbuch für die Unternehmens- und Anwaltspraxis, S. 951; vgl. zu E-Learning und Präsenzs Schulungen: *van Vormizeele*, CCZ 2009, 41, 43; zur essenziellen Notwendigkeit von Schulungen: *Mengel*, in: Mengel, Compliance und Arbeitsrecht, S. 9; weiterführend zum Umgang mit Social Media in der Compliance: *Oberlin*, CB 2019, 67 ff.

15 Zu mangelhaften Trainings, deren Gründen und Auswirkungen siehe *Röhrich*, in: Röhrich, Methoden der Korruptionsbekämpfung, S. 30 ff.

Was auf den ersten Blick einfach klingt, ist in der Praxis mit verschiedenen Herausforderungen verbunden. Neben der Koordination internationaler Termine und Tagungsräume ist die Erstellung besagter, zielgruppengerechter Schulungsunterlagen eine Kunst. Es hat sich gezeigt, dass die Darstellung von Risiken und den damit verbundenen Normen im Gesetz nicht ausreicht. Vielmehr müssen Fälle und Beispiele eingearbeitet sein, die die jeweilige Zielgruppe möglichst aus ihrem direkten Arbeitsalltag kennen bzw. damit Berührungspunkte haben. Soweit die internen Compliance-Mitarbeiter einige Fachthemen nicht selbst abdecken, sollte externe Unterstützung beigezogen werden. Dies zum einen, um relevante Mitarbeiterfragen auch beantworten zu können, zum anderen aus Gesichtspunkten eines möglichen Enthaltungsbeitrags für die Geschäftsführung.¹⁶ **33**

2. Schulungen mit klassischem E-Learning

Neben den Präsenztrainings greifen viele Compliance Officer zu einer unterstützenden, digitalen Schulung in Form eines sogenannten „E-Learnings“. ¹⁷ Dieses ist eine Schulung mit einer schriftlichen Präsentation sowie interaktiven Elementen, die der Mitarbeiter in einem gewissen Zeitraum selbstständig an seinem PC-Arbeitsplatz ausführen kann.¹⁸ **34**

Zu E-Learnings gibt es eine Reihe von Fehleinschätzungen, die hier kurz angerissen werden sollen.¹⁹ Zunächst wird die Geschäftsführung nicht automatisch enthaftet, nur weil die Mitarbeiter nachweislich ein E-Learning zu einem Thema durchgeführt haben, in dem später ein Verstoß aufgetreten ist. Die Schulung kann ein Indiz für die Compliance-Bemühungen des Unternehmens darstellen. Soweit ein Verstoß eintritt, werden diese aber nach aller Voraussicht von der Rechtsprechung als nicht hinreichend betrachtet werden.²⁰ **35**

Zudem ist ein E-Learning keine per se kostengünstige Trainingsmethode, da z. B. eine Nutzungspauschale des Anbieters von 8 EUR pro Mitarbeiter erhoben wird oder Übersetzungen je Sprache 8.000 EUR kosten können.²¹ Im Ergebnis ist damit ein Betrag von 50.000 EUR pro E-Learning keine Seltenheit. Dankenswerterweise wandelt sich der Markt hier jedoch zurzeit, sodass auch sehr gute und kostengünstigere Produkte am Markt erhältlich sind.²² Seit 2020 sind zudem **36**

¹⁶ Siehe ausführlich und vertiefend zum musterhaften Aufbau einer internen Kartellrechtsschulung *Hastenrath*, in: *Hastenrath*, Compliance-Kommunikation, Kap. 6 Rn. 50 ff.

¹⁷ Zu E-Learnings siehe auch *Wendel*, in: *Wieland/Steinmeyer/Grüniger*, Handbuch Compliance Management, S. 653, 657 f.

¹⁸ Ausführlich zum Aufbau eines Compliance-E-Learnings siehe *Hastenrath*, in: *Bay/Hastenrath*, Compliance-Management-Systeme, 2. Aufl. 2016, S. 175 ff.

¹⁹ Ausführlich dazu auch *Hastenrath*, CCZ 2014, 132 ff.

²⁰ Vgl. hierzu die Anforderungen an ein ausreichendes Compliance-Management-System nach der Rechtsprechung des LG München I, 10.12.2013 – 5 HKO 1387/10 (Neubürger-Entscheidung; unter Aktenzeichen so im Internet verfügbar).

²¹ Persönliche Erfahrungen der Autorin.

²² Siehe zum Beispiel die Compliance-Produkte von Haufe unter: <https://www.haufe-akademie.de/hierarchy/compliance> (zuletzt abgerufen am 28.6.2024).

viele Start-ups mit sehr günstigen Lösungen am Markt, was durch die Covid-19-Pandemie und die zunehmende Homeoffice-Tätigkeit ausgelöst wurde.

- 37 Ein E-Learning ist jedoch nicht für alle Schulungen einsetzbar. Durch den vorgegebenen, knappen Zeitrahmen zur Bearbeitung von durchschnittlich 45 bis 60 Minuten sowie der fehlenden Rückfragemöglichkeiten können am besten Grundlagenfragen und -themen behandelt werden, etwa wie der Code of Conduct oder Grundzüge der Korruptionsprävention. Speziellere und vertiefte Betrachtung sollten den Präsenzs Schulungen vorbehalten werden. Hier kann ein E-Learning höchstens als Ergänzung oder Auffrischung nach einer solchen Präsenzs Schulung verwendet werden.
- 38 Schließlich ist eine zunehmende E-Learning-Müdigkeit der Mitarbeiter zu beobachten, da diese teilweise zehn oder mehr E-Learnings verschiedener Fachbereiche absolvieren müssen. Der Einsatz von E-Learnings ist daher auch aus dieser Perspektive genau zu überdenken.

3. Digitale Schulungen: Schulungen mit Webinaren, Podcasts, Livestreams oder vertonten Präsentationen

- 39 Ein Konzept des Kommunikationsmanagements im Rahmen der Digitalisierung von Compliance sind Schulungen ohne persönliche Präsenz vor Ort mit Referenten, die über ein technisches Programm zugeschaltet sind, vorab eine Präsentation vertonen oder via Livestream per Video zugeschaltet sind. In vielen Unternehmen werden schon jetzt aufwendige Dienstreisen zugunsten von Meetings per Videokonferenz oder Ähnlichem ersetzt. Dieser Trend wird zunehmend auch den Schulungsbereich betreffen, insbesondere wenn sich die Energiekosten weiter erhöhen oder globale Reisetätigkeiten vor Gefahren wie etwa Pandemien („Covid 19“) künftig in Frage gestellt werden könnten.
- 40 Der große Vorteil dieser digitalen Schulungsformen ist die moderne Darbietungsform z.B. auch in Form spielerischer Elemente (Stichwort: „Gamification“²³), der Wiederverwendbarkeit z.B. aufgezeichneter Schulungen mit dem Compliance Officer sowie die nahezu weltweit mögliche Zusammenarbeit, ohne den physischen Arbeitsplatz verlassen zu müssen.
- 41 Näher betrachtet wird nachfolgend das Webinar. Vorteil hiervon ist die Mischung aus Präsentation, z.B. als Power-Point-Präsentation, des Live-Vortrags des Referenten über technische Hilfsmittel sowie die Fragemöglichkeit der Teilnehmer, je nach Programm über eine Chatfunktion oder per Audiospur.²⁴
- 42 Webinare sind in der Compliance-Kommunikation noch eine junge Disziplin. Ein erfolgreiches Webinar muss anders konzipiert werden als andere Schulungs-

23 Siehe zu Gamification auch *Petrushevska*, CCZ 2023, 241, 246.

24 Aktuell verbreitet in der Compliance sind hier die Anwendungen Zoom, Microsoft Teams, Google Hangouts oder Adobe Connect, ohne das hierfür eine abschließende Klärung zu Datenschutz und Datensicherheit getroffen werden konnte.

formate, weshalb einige Punkte zu beachten sind. Ein Schwerpunkt dieses Kapitels soll daher auf die musterhaften Kernelemente zur Ausgestaltung eines Webinars gelegt werden. Der gewählte Aufbau, Inhalt und die Darstellung je Musterfolie werden jeweils zusätzlich erklärt, was einen Transfer in das eigene Unternehmen erleichtert.

Inhaltsverzeichnis Webinar Compliance im Vertrieb	
1.	Haftungsrisiken für Vertriebsmitarbeiter
2.	Risikofelder im Vertrieb (mit Behörden, Kunden, Wettbewerbern u.a., auch in Hochrisikoländern)
a)	Kartellrechtliche Risiken im Umgang mit Wettbewerbern
b)	...
3.	Lösungsmöglichkeiten zum Umgang mit diesen Risikofeldern
a)	Lösungsansatz zu kartellrechtlichen Risiken
b)	...
4.	Ergebniszusammenfassung „to go“
5.	Quellen/Literaturhinweise/Veranstaltungstipps

Abbildung 2: Musterfolie 1 Webinar

Mit dem Inhaltsverzeichnis beginnt der erste Kontakt zwischen Teilnehmern und Referent. Es kann sein, dass es vorher technische Probleme gab, noch nicht alle Teilnehmer „eingeloggt“ sind oder der Referent anfangs nervös ist. Daher sollte diese Folie genutzt werden, um sich gemeinsam auf das kommende Training einzustimmen. Auch wenn sich Teilnehmer erst jetzt zuschalten, können sie aufgrund der klaren Struktur der Folie schnell ins Thema einsteigen, selbst wenn sie einige Minuten verpasst haben sollten. Die klare Struktur mit kurzer Darstellung der Hauptthemen und Unterpunkte ist auch deshalb empfehlenswert, um einerseits den Gesamthalt kurz zu umreißen, andererseits können die Teilnehmer sich schon einmal auf die Themen einstellen und darüber nachdenken. Dies ist für die kommenden Fragen an die Teilnehmer auch notwendig. Sollte es zu diesem Zeitpunkt noch technische Schwierigkeiten geben, kann sich der Referent per Audio oder in einem separaten Textfeld neben der Erläuterung des Inhalts an den IT-Support wenden, ohne den roten Faden gegenüber den Teilnehmern zu verlieren. Es empfiehlt sich ohnehin, dass ein IT-Support für die gesamte Zeit des Trainings zugeschaltet ist oder jedenfalls auf Abruf unmittelbar reagiert. Es können technische Schwierigkeiten auftreten, auch bei den Teilnehmern, z. B. Ton- oder Bildstörungen, um die der Referent sich nicht selbst kümmern kann und dafür den besagten IT-Support benötigt.

43

Warm-up: Vorstellung

- Kurzvorstellung des Referenten



- Ihr prägnantestes Beispiel zum heutigen Thema?



Abbildung 3: Musterfolie 2 Webinar

- 44** Referenten und Teilnehmer konnten sich nicht wie im Rahmen von persönlichen Trainings beim Betreten des Seminarraums o.Ä. direkt durch Handschlag und einem kurzen „Small Talk“ aufeinander einstimmen. So unwichtig diese Kleinigkeit auf den ersten Blick erscheinen mag, umso ungewohnter ist es jedoch, wenn sie wegfällt. Um diese zu ersetzen, wurde Musterfolie 2 konzipiert. In dieser stellt sich der Referent kurz vor und begrüßt die Teilnehmer noch einmal, bzw. eine gute Möglichkeit zum Einstieg ist auch die Frage, wo sich die Teilnehmer räumlich befinden und in welcher Zeitzone, soweit das Training international ausgerichtet ist. Dies lockert die Stimmung auf und stellt möglicherweise Gemeinsamkeiten heraus. Der Vorstellung folgen sollte dann eine direkte, inhaltliche Frage an die Teilnehmer, die diese per Chat beantworten. Hier wird ebenfalls eine erste Basis für die gemeinsame Arbeit im folgenden Training gelegt. Zusätzlich kann der Referent hier noch wichtige Erkenntnisse gewinnen, wie er gegebenenfalls seine Schwerpunkte im Training setzt, um den Interessen der Teilnehmer am besten gerecht zu werden.

Warm-up: Ihre Erwartungen

- Von diesem Webinar (nach vorab ausgefülltem Fragebogen):
 - Persönliche Haftung und unternehmerische Haftung?
 - Sorgfaltspflicht des Arbeitgebers?
 - Wenn Kundenkontakte in persönliche Freundschaften übergehen - was darf der Vertriebsmitarbeiter dann noch ohne Bedenken tun?
 - Umgang mit "zugespielten" Angeboten, Preislisten o.ä. Dokumenten von Wettbewerbern
 - Wird differenziert, ob es sich um einen internen oder externen Vertriebsmitarbeiter handelt?

Abbildung 4: Musterfolie 3 Webinar

Die Erfahrung hat gezeigt, dass eine vorherige Abfrage der Erwartungen an ein Webinar vorteilhaft ist. Zum einen setzen sich die Teilnehmer so bereits vor dem eigentlichen Webinar mit ihren Erwartungen und Problemstellungen auseinander. Zum anderen besteht auch hier die Chance für den Referenten, weitere Folien für den Adressatenkreis aufzunehmen, um deren Fragen zu beantworten. Soweit die Fragen zu weit vom eigentlichen Thema entfernt liegen, sollte der Referent die Erwartung zwar aufnehmen, dann aber im Webinar darauf hinweisen, dass dies kein Thema des Webinars ist und deshalb, auch im Interesse der anderen Teilnehmer, nicht oder nur in ein bis zwei Sätzen angesprochen werden kann. **45**

Auch sollten hier Fragen zu Erwartungen, die vielleicht noch präzisiert werden können, wie in der Musterfolie in etwa der Punkt zu den Sorgfaltspflichten des Arbeitgebers, direkt vom Vortragenden an die Teilnehmer gestellt werden. Das sichert zum einen das richtige Verständnis des Referenten und bezieht auch die Teilnehmer aktiv mit ein. Denn für den Referenten ist es in einem Webinar teilweise nicht erkennbar, ob seine Teilnehmer noch vor Ort sind und mitdenken und seinen Vortrag verfolgen oder möglicherweise nur den PC angestellt haben, sich aber ansonsten anderen Themen widmen. Dies kann für den Vortragenden unbefriedigend sein, sodass seine Ankündigung gleich zu Anfang des Webinars, dass die Teilnehmer durch das ganze Training hindurch immer wieder aktiv mit Fragen und Input einbezogen werden, dem vorbeugen kann. **46**

1. Haftungsrisiken für Vertriebsmitarbeiter

Der Fall Keith Packer



Abbildung 5: Musterfolie 4 Webinar

- 47 Wie auch in allen anderen Schulungsformen spielen passende und überzeugende Beispiele eine große Rolle. Diese werden am besten zu Beginn eines Kapitels oder Sinnabschnitts als Einleitung gewählt. Dies bindet die Aufmerksamkeit der Teilnehmer, insbesondere, wenn sie sich persönlich in einem gewählten Beispiel wiederfinden. Bei der Wahl der Beispiele sollte vom Referenten zusätzlich darauf geachtet werden, dass es nicht um eine bloße „Angstmache“ geht, also keine Beispiele, in denen die gesetzliche Haftung mit persönlichen Strafen als besonderes Damoklesschwert dargestellt werden. Dies führt oftmals zu einer „Abstumpfung“, insbesondere wenn die Teilnehmer seit Jahren ggf. kritische Tätigkeiten praktizieren oder praktiziert haben, es aber noch nie zu rechtlichen Konsequenzen kam. Die Beispiele sollten besser eine persönliche Betroffenheit und einen gewissen Überraschungseffekt enthalten, sodass die Mitarbeiter einerseits sehen, dass die rechtlichen Auswirkungen auch sie selbst treffen können und das oftmals für Verhaltensweisen, die für den Rechtslaien noch als rechtlich unkritisch oder zulässig angesehen werden.

1. Haftungsrisiken für Vertriebsmitarbeiter

- Viele Länder stellen auch die Bestechlichkeit und Bestechung im geschäftlichen Verkehr zwischen privaten Personen/Unternehmen unter Strafe (z.B. im deutschen, chinesischen, russischen und spanischen Strafgesetzbuch, im italienischen Dekret 231 oder in verschiedenen US-amerikanischen bundesstaatlichen Gesetzen)
- Strafen gegen den Vertriebsmitarbeiter reichen von persönlichen Geldstrafen bis hin zu Haftstrafen (z.B. Kartellrechtsverstöße nach US-Recht)
- Auch nach „fremden“ Jurisdiktionen können deutsche Vertriebler haften; zivilrechtliche Sanktionen kommen hinzu

Abbildung 6: Musterfolie 5 Webinar

Neben Beispielen und Interaktion darf auch die klassische Wissensvermittlung nicht fehlen. In Musterfolie 5 in etwa werden Grundzüge zu Auswirkungen von Bestechung und Bestechlichkeit in verschiedenen Jurisdiktionen dargestellt. Von Compliance-Verantwortlichen wird oftmals überschätzt, inwieweit sich die Mitarbeiter in für diese relevanten Rechtsthemen auskennen. Oftmals ist das Wissen bestenfalls fragmentarisch, (stark) veraltet oder unzulässig vereinfacht. Zwar sollen die Mitarbeiter keine Rechtsexperten werden, dennoch müssen sie die Grundrichtung und Grundaussagen der wichtigsten Normen kennen, mit denen sie im Arbeitsalltag in Berührung kommen. Dabei müssen diese Normen nicht unbedingt alle im originalen Gesetzeswortlaut in der Präsentation mit abgedruckt werden. Es können auch vereinfachte Inhalte im Zusammenhang mit erläuternden Beispielen gewählt werden. Gesamte Texte oder Gesetze haben, wenn überhaupt, Platz in einer Annex, die die Teilnehmer zur Nacharbeit und Eigenlektüre verwenden können. **48**

Ob ausgeschriebene Sätze oder Stichpunkte verwendet werden, ist dem jeweiligen Stil des Referenten überlassen. Da es sich bei dem Webinar jedoch um einen Vortrag handelt, in dem frei gesprochen wird, können sich Stichpunkte anbieten, da diese nicht zum „Vorlesen“ der Folien wie mit ganzen Sätzen verleiten. Insgesamt muss die Sprache so gewählt sein, dass diese vom Zielpublikum verstanden wird. Dies kann im internationalen Kontext ein Problem darstellen. Es empfiehlt sich daher immer, die Texte, wenn sie in eine andere Sprache übersetzt werden, von einem Muttersprachler oder professionellen Übersetzer anfertigen oder jedenfalls gegenlesen zu lassen. So lassen sich unliebsame Übersetzungsfehler und damit die Gefahr einer Entstellung des Sinnes des Textes vermeiden. **49**

2. Risikofelder im Vertrieb (mit Behörden, Kunden, Wettbewerbern u.a., auch in Hochrisikoländern)

a) Kartellrechtliche Risiken im Umgang mit Wettbewerbern

Abstimmung



Frage:
Ist folgendes Verhalten problematisch: Sie unterhalten sich mit dem Vertriebskollegen eines Wettbewerbers darüber, dass Ihr Unternehmen sein Angebot wegen einem Produktionsengpass erst mit zwei Wochen Verspätung einreichen kann.

Abbildung 7: Musterfolie 6 Webinar

- 50** Webinare haben den Vorteil einer hohen Interaktionsmöglichkeit. Eine solche Möglichkeit, die regelmäßig in Webinaren verwendet werden kann und sollte, ist die der Abstimmung. Eine Abstimmung muss vorab mit dem Technikteam besprochen und an der gewünschten Stelle integriert werden. Der Abstimmungsmodul kann sich auf zwei Optionen wie „Ja“ und „Nein“ beschränken, kann aber auch mehrere und differenzierte Antwortmöglichkeiten vorgeben. Neben der für Juristen typischen Aussage „Es kommt darauf an“ können auch „Ja“- oder „Nein“-Antworten mit weiteren Bedingungen verknüpft werden. Bei „Ja“ könnte es zum Beispiel als eine Antwortoption heißen „Ja, wenn der Mitarbeiter Vorsatz hatte“.
- 51** Die Teilnehmer und der Referent erhalten durch eine Abstimmung ein Bild, wie die Mehrheit oder die Minderheit eine Situation einschätzen. Liegen die Einschätzungen der Teilnehmer mehrheitlich neben der richtigen Lösung oder spiegeln sie im Gegenteil mehrheitlich die richtige Lösung wider, obwohl es vielleicht eine sehr schwere Frage war, kann der Referent im „Chat“ nachfragen, wie die Teilnehmer auf diese Lösung gekommen sind. So erfolgt in etwa beim Chat über eine falsche Lösung unmittelbar ein Lerneffekt, da der Referent den Teilnehmern erklären kann, wo diese gegebenenfalls noch ein Detail nicht beachtet oder rechtlich nicht richtig eingeordnet haben.

2. Risikofelder im Vertrieb (mit Behörden, Kunden, Wettbewerbern u.a., auch in Hochrisikoländern)

a) Kartellrechtliche Risiken im Umgang mit Wettbewerbern



Redflags sind u.a.:

- Unternehmenskultur: Austausch mit Wettbewerbern
- Verbandstreffen mit Wettbewerbern ohne vorherige Sensibilisierung
- Markt ist in Krise
- Neue Marktplayer etablieren sich (mögl. Kartelle werden wirkungslos, oft hier Kronzeugenantrag gestellt)
- Bisher keine Schulungen durch das Unternehmen für die Risikogruppen erfolgt
- Dezentrale Vertragsschlüsse ohne zwingende Einbindung der Rechtsabteilung/„Sideletter“

Abbildung 8: Musterfolie 7 Webinar

Besonders beliebt bei den Praktikern sind Checklisten und andere Hilfen, die im hektischen Arbeitsalltag erste schnelle Antworten und Abhilfe liefern. Das sollte in ein Webinar an einer oder mehreren Stellen aufgenommen werden. Es bieten sich zum Beispiel Checklisten zu sog. „Red Flags“ an, also Situationen oder Verhaltensweisen, die möglicherweise ein Indiz für ein rechtswidriges Verhalten darstellen oder eine erhöhte Wahrscheinlichkeit dafür darstellen, dass ein solches Verhalten in einer bestimmten Lage verstärkt vorkommen könnte. In Musterfolie 7 sind daher typische „Red Flags“ im Bereich des Kartellrechts aufgeführt. Insbesondere im Bereich des Kartellrechts gibt es klassische Situationen, die zu kartellrechtswidrigem Verhalten verleiten könnten.²⁵ Dazu zählt beispielsweise eine veränderte Marktsituation, weil ein neuer Wettbewerber in das Marktgeschehen eintritt. Dies hat in der Vergangenheit oftmals dazu geführt, dass bestehende Kartelle der bisherigen Wettbewerber aufgegeben wurden, da diese nun nicht mehr funktionierten, und einer der Wettbewerber einen Kronzeugenantrag beim Bundeskartellamt gestellt hat, um so selbst bußgeldfrei auszugehen, während die Wettbewerber mit empfindlichen Bußen belegt wurden. Als eine weitere „Red Flag“ ist das dezentrale Abschließen und Verwalten von Verträgen zu nennen. Hier werden oftmals unlautere Praktiken beobachtet, insbesondere wenn es sich um große Projekte handelt und die operativen Abteilungen eigene Verträge schließen können. Der Basisvertrag wird zwar meistens von der Rechtsabteilung aufgesetzt oder jedenfalls geprüft, etwaige Nachträge jedoch schließen die operativen Abteilungen häufig selbstständig. In diesen Nachträgen, die rechtlich nicht geprüft wurden oder, schlimmer noch, in die Vereinbarungen aufgenommen werden, die die Rechtsabteilung abgelehnt hätte, finden sich teilweise wettbewerbswidrige Absprachen.

²⁵ Siehe hierzu ausführlich → *Seeliger/Mross/Seydel*, Kap. 27.

- 53** Im Zusammenhang mit den Checklisten können die Teilnehmer im Webinar wieder nach ihren eigenen Erfahrungen gefragt werden. Auch kommen im Zusammenhang mit „Red Flags“ oftmals Fragen der Teilnehmer auf, ob diese oder jede Verhaltensweise auch als kritisch einzustufen sei, die der Referent beantworten kann.

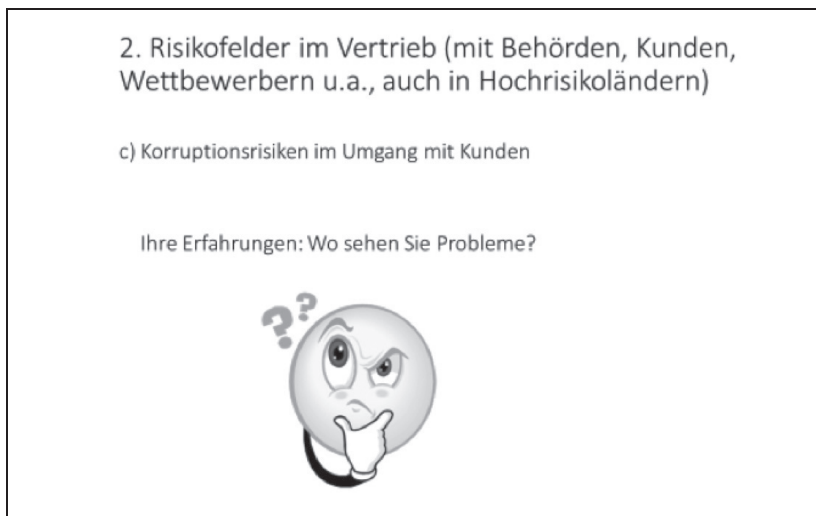


Abbildung 9: Musterfolie 8 Webinar

- 54** Ferner können in einem Webinar aktive Arbeitsaufträge an die Teilnehmer gegeben werden. Es bieten sich insbesondere zwei Formen an: Zum einen kann den Teilnehmern z. B. fünf Minuten Zeit gegeben werden, um sich Antworten auf die Frage des Referenten zu überlegen. Diese können dann per Chat allen anderen Teilnehmern und dem Referenten mitgeteilt und besprochen werden. Daneben gibt es die Möglichkeit, direkt im Webinar Stichpunkte auf einer Art „Online Flipchart“ zu sammeln. Die Teilnehmer geben also ihre Antworten per Chat an den Referenten weiter und dieser sammelt diese dann gemeinsam in einem Dokument, welches er direkt online beschreiben kann. Soweit diese technische Möglichkeit nicht besteht, ist es auch möglich, dass der Referent bzw. der technische Support den Teilnehmern Audiorechte einräumt, sodass diese wie in einer Präsenzsitzung ihre Antworten in den Raum rufen können. Dann kann der Referent an ein tatsächliches Flipchart treten und diese Antworten aufschreiben, was über die Webcam für die Teilnehmer sichtbar sein muss. Bei dieser Variante ist allerdings im Vorhinein zu prüfen, ob die Lichtverhältnisse, die Kameraauflösung und der sichtbare Radius von dem Referent mit Flipchart für die Teilnehmer gut erkennbar sind.

Nicht empfehlenswert ist es dagegen, die Schreibfunktion für alle Teilnehmer zu aktivieren (was einige Programme zulassen), da es dabei einerseits zu gegenseitigen Behinderungen kommen kann, wenn alle Teilnehmer gleichzeitig schreiben und das Programm dies nicht umsetzen kann; andererseits kann es so zu „Mehrfachnennungen“ kommen. **55**

Das Aktivieren der Audiofunktion für alle Teilnehmer birgt ähnliche Probleme. Hier kommen teilweise nur „Wortfetzen“ an oder die Sätze der Teilnehmer vermischen sich. Bei mehr als zehn Teilnehmern sollte die Audiofunktion daher allenfalls punktuell an vereinzelt Stellen eingesetzt werden. **56**

Es gibt verschiedene Lerntypen unter den Menschen und damit auch unter den Mitarbeitern. Ein Lerntyp beschreibt visuell orientierte Menschen. Diese können sich grafisch aufbereitete Inhalte erheblich besser merken als reine Texte. Daher sollten immer wieder auch solche optischen Elemente in Form von Bildern, Grafiken oder Tabellen im Webinar dargestellt werden. Der Grad der Komplexität sollte dabei nicht zu hoch sein. Wenn ein Teilnehmer mehr als zwei Minuten benötigt, um alle Elemente einer Grafik erstmalig zu lesen, ist dies für ein Webinar zu viel, da die meisten Referenten den Teilnehmern nicht zwei oder mehr Minuten Zeit geben, eine Grafik zu begreifen, sondern meistens direkt in die Erklärung zu der Grafik springen. Dies überfordert die Teilnehmer dann aber schnell, da sie sich mit den Inhalten der Grafik nicht so zügig vertraut machen konnten. **57**

3. Lösungsmöglichkeiten zum Umgang mit diesen Risikofeldern

a) Lösungsansatz zu kartellrechtlichen Risiken

Kurz und knapp für den Vertrieb: 5 Grundregeln



1. Preis- und Konditionenabsprachen:

Treffen Sie mit Wettbewerbern keine Absprachen über Einkaufs-/Verkaufspreise, Geschäftsbedingungen, Kalkulations- und Kostenpositionen, die Sie gegenüber Kunden oder Lieferanten anwenden oder vorhaben anzuwenden. Tauschen Sie auch niemals entsprechende Informationen mit Wettbewerbern aus.

2. Marktaufteilung und Kundenschutz:

Aufteilungen von Märkten, Produkten oder Versorgungsquellen zwischen Wettbewerbern sind kartellrechtlich verboten. Darüber hinaus ist auch eine Marktaufteilung nach Kunden oder Lieferanten unzulässig. Auch „Nichtangriffsakte“ oder Vereinbarungen zum Schutz von „Heimatsmärkten“ werden von den Kartellbehörden als schwere Kartellrechtsverstöße gewertet.

Abbildung 10: Musterfolie 9 Webinar

Ein wichtiger Bestandteil eines guten Webinars sind kurze und klare Lösungsansätze, die die Teilnehmer unmittelbar in ihrem Alltag einsetzen können. Ein gu- **58**

ter derartiger Lösungsansatz sind fünf bis zehn Grundregeln, die zum Beispiel ein Vertriebsmitarbeiter als Datei auf seinem Smartphone jederzeit zur Verfügung hat und diese damit auch außerhalb der Firma bei konkreten Aufträgen und Angeboten bei Kunden einsehen kann. Jede Grundregel sollte dabei verständlich und möglichst präzise formuliert sein. Der Mitarbeiter muss also möglichst auf den ersten Blick erkennen, welche seiner Handlungen akzeptabel sind und welche sich möglicherweise im Bereich eines Rechtsverstößes bewegen. Werden die Regeln zu lang, in etwa pro Regel eine halbe Seite und mehr, erhöht sich die Gefahr, dass diese zu kompliziert und zu aufwendig für einen „schnellen Blick darauf“ werden und deshalb von den operativen Mitarbeitern ignoriert oder nur unvollständig beachtet werden.

3. Lösungsmöglichkeiten zum Umgang mit diesen Risikofeldern

b) Lösungsansatz zu Korruptionsrisiken im Umgang mit Behörden/Amtsträgern

- **Faustregeln:**
- **Im Ausland: Frage nach Beteiligungen dieser vorab**
- **Ggfs. behördliche Genehmigung einholen (Vgl. § 331 Abs. 3 StGB)**
- **Repräsentanzfunktionen und Geschäftsabschlüsse strikt trennen**
- **Keine Bargeldkassen; falls unentbehrlich: durchgehendes 4-Augen-System**

Abbildung 11: Musterfolie 10 Webinar

- 59** Ebenfalls sehr geschätzt in der Praxis sind sog. „Faustregeln“. Diese geben, ähnlich den Checklisten, in konkreten und potenziell kritischen Situation erste Handlungsoptionen zur Orientierung. Deshalb sollten auch diese in ein Webinar Einzug finden.
- 60** Allerdings sei an dieser Stelle davor gewarnt, die Annahme der Teilnehmer zu bestätigen, dass Checklisten oder Faustregeln für die Bearbeitung aller Fälle ausreichen würden. Es muss vom Referenten immer ausdrücklich darauf hingewiesen werden, dass diese nur eine erste „Marschrichtung“ vorgeben und ganz grundlegende Fragestellungen beantworten können, aber auch nicht mehr. Keinesfalls darf nach der Abarbeitung einer Checkliste oder Faustregel davon ausgegangen werden, dass damit alles Erforderliche aus Compliance-Sicht getan sei. Checklisten und Faustregeln sind ein erster Schritt in die richtige Richtung. Diesem ersten Schritt müssen aber immer gezielte, fallspezifische, weitere Prü-

fungen folgen. Je nach Branche, Land oder Risikogeneigntheit eines Sachverhalts müssen weitere und gegebenenfalls andere, speziellere Kriterien zu einer Compliance-Prüfung herangezogen werden. Hierbei kann es sich empfehlen, lokale Spezialisten beizuziehen.

3. Lösungsmöglichkeiten zum Umgang mit diesen Risikofeldern

d) Lösungsansatz zu Umgang mit Beratern und Intermediären

Intermediäre

- Interne Prüfung: Wo werden Intermediäre eingebunden?
- Checkliste/Voraussetzungen für eine Einbindung
 - Name des Intermediäres
 - Name des Endkunden
 - Auftragsvolumen Ihr Unternehmen-Intermediär
 - Auftragsvolumen Intermediär - Endkunde (wenn bekannt)
 - Wirtschaftliche Gründe für die Einschaltung des Intermediäres
 - Firmensitz des Intermediäres
 - ...



Abbildung 12: Musterfolie 11 Webinar

Wie bereits zur vorangegangenen Musterfolie erwähnt, spielen Checklisten als erster Schritt für die Einordnung und Prüfung einer Situation im Compliance-Bereich eine wichtige Rolle. Auch im Bereich der Intermediäre, also zwischen das eigene Unternehmen und den eigentlichen Kunden eingeschaltete Unternehmen oder Personen, macht der Einsatz von Checklisten Sinn. Intermediäre sind ein „Einfallstor“ für Korruption und müssen daher von der Compliance-Abteilung kritisch untersucht werden. Da die Intermediäre häufig im Kundenland und damit weit von einer zentralen Compliance-Abteilung entfernt sitzen, sollten in diesem Bereich standardisierte Listen eingesetzt werden, die primär vom Vertrieb selbst oder in Zusammenarbeit mit dem Intermediär ausgefüllt werden können. Sind alle Grunddaten vollständig und in verständlicher Sprache an die Compliance-Abteilung zur Prüfung weitergeleitet worden, muss diese auch hier die jeweiligen Besonderheiten des Einzelfalls beachten und darf sich nicht blind auf eine ausgefüllte Checkliste verlassen. Die Volksweisheit „Papier ist geduldig“ trifft auch gerade in diesem Bereich in besonderem Maße zu. Eine kritische Gegenprüfung zum Wahrheitsgehalt der ausgefüllten Checkliste ist daher ein unumgängliches Muss für die Compliance-Verantwortlichen.

4. Ergebniszusammenfassung „to go“

- Haftungsrisiken für Vertriebsmitarbeiter sowie Unternehmen ergeben sich aus diversen Vorschriften insb. aus Antikorruptions- und Wettbewerbsschutzgesetzen
- Mögliche Korruptionstatbestände können in „verschiedenen Gewändern“ verwirklicht werden
- Beziehungspflege und Korruption gehen fließend ineinander über und werden je nach Landeskultur sehr unterschiedlich aufgefasst
- Im Kartellrecht sollte eine Grundsensibilisierung z.B. mit einfachen Kernaussagen erfolgen

Abbildung 13: Musterfolie 12 Webinar

- 62** An dieser Stelle erwähnt, da häufig vergessen, sei schließlich auch ein sauberer Abschluss des Webinars. Nachdem die Teilnehmer mit einer Fülle von teilweise für sie neuen Inhalten konfrontiert wurden, sollte das Gehörte möglichst durch eine kompakte Zusammenfassung noch einmal verdeutlicht werden. Wiederholungen erhöhen den Grad des Behaltens von neuen Lerninhalten erheblich. Zusätzlich können derartige Zusammenfassungen von den Teilnehmern intern auch verwendet werden, um das Erlernte und für das jeweilige Unternehmen relevante Wissen anderen Funktionen und gegebenenfalls der Geschäftsführung in Kürze aufzuzeigen.
- 63** Insgesamt sollte die moderne Schulungsform wegen ihrer vielen Vorteile und Optionen zur Interaktivität mit den Teilnehmern sowie der Standortunabhängigkeit viel häufiger in Unternehmen eingesetzt und genutzt werden. Da die Anforderungen an den Referenten jedoch von denen einer Präsenzschulung in einigen Punkten abweichen, sollte dieser selbst vorab ein Training als E-Trainer²⁶ absolvieren oder sich mindestens in einigen Testdurchläufen mit den Möglichkeiten, Grenzen und gegebenenfalls auftretenden, technischen Schwierigkeiten vertraut machen. Ggf. kann hier die eigene IT-Abteilung Hilfestellung geben oder eine hauseigene Akademie, soweit eine solche vorhanden ist.

²⁶ Eine solche E-Trainer-Ausbildung wird zum Beispiel angeboten unter <https://www.leading-interactive.de/e-trainer/inhalte/> (zuletzt abgerufen am 26.2.2024.).

4. Unterstützung dezentraler Compliance-Funktionen: das Schulungshandbuch

Die meisten Compliance-Abteilungen bestehen aus einer zentralen Compliance-Funktion in der Holding oder einer der Hauptgesellschaften sowie zusätzlichen, dezentralen Compliance-Mitarbeitern in weiteren nationalen und internationalen Gesellschaften oder jedenfalls Regionen. Letztgenannte Mitarbeiter befassen sich überwiegend nicht Vollzeit mit der Compliance-Aufgabe, sondern nur zu 5 bis 20 %, manchmal bis zu 50 % ihrer Stelle.²⁷ Zudem sind diese Mitarbeiter fast nie Juristen, sondern setzen sich aus Mitarbeitern mit verschiedenen Ausbildungen und Studiengängen zusammen. Es verwundert daher wenig, dass diese Mitarbeiter bei Compliance-Fragen schnell an die Grenze ihrer Kenntnisse, Fähigkeiten und zeitlichen Ressourcen kommen. Da sie aber eine wichtige Rolle als erste und direkte Ansprechpartner vor Ort spielen, benötigen sie ein solides Grundwissen zu den relevanten Compliance-Themen für ihr Unternehmen. Daneben müssen sie auch in der Lage sein, die Mitarbeiter vor Ort selbstständig zu schulen.²⁸ Dies ist einer zentralen Compliance-Funktion einerseits aus Zeitmangel, andererseits wegen kultureller und sprachlicher Klippen oftmals nicht oder nicht ausreichend möglich. 64

Um den dezentralen Compliance-Mitarbeitern mit deren eingeschränkten Zeitressourcen und teilweise unzureichender Ausbildung in Compliance-Themen eine Hilfestellung zu geben, bietet es sich an, dass die zentrale Compliance-Funktion ein einheitliches Trainingshandbuch für alle Compliance-Mitarbeiter erstellt.²⁹ Dies bietet sich insbesondere deshalb an, weil die zentralen Compliance-Mitarbeiter häufig sehr gut in dieser Materie ausgebildet sind, zum anderen eine Vollzeitposition für Compliance bekleiden und schließlich am ehesten über ein notwendiges Budget³⁰ verfügen. 65

Ein derartiges Schulungshandbuch sollte wie folgt aufgebaut werden: 66

²⁷ Hastenrath, in: Hastenrath, Compliance-Kommunikation Kap. 6 Rn. 77.

²⁸ Zur Aufgabenstellung der Compliance-Verantwortlichen im Schulungs- und Kommunikationsbereich siehe Schulz/Galster, in: Bürkle/Hauschka, Der Compliance Officer – Ein Handbuch in eigener Sache, 2015, 95 ff.

²⁹ Zu allgemeinen und weiteren Schulungsaufgaben der Compliance-Funktion siehe auch Kleinfeld/Müller-Störr, in: Wieland/Steinmeyer/Grüniger, Handbuch Compliance Management, 1. Aufl. 2010, 406 ff.

³⁰ Zu Budgetproblemen der Compliance-Funktion siehe Bay/Seeburg, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, S. 210.

Inhaltsverzeichnis	
1.	Ausgangslage
2.	Aufbau und Hauptaufgaben der Compliance-Organisation nach der Compliance-Organisationsrichtlinie
3.	Interne Vorgaben für Compliance
3.1	Richtlinien des Group Compliance-Offices (Holding)
3.2	Richtlinien der Regionen
4.	Pflichtbestandteile für Schulungen der dezentralen Compliance-Officer (LCO)
4.1	Ausgangslage
4.2	Wichtigste Compliance-Entwicklungen
4.3	Verhaltenskodex
4.4	Antikorruptionsrichtlinie
4.5	Kartellrechtsrichtlinie
5.	Zusammenfassung „In a nutshell“

Abbildung 14: Musterfolie Schulungshandbuch

- 67 Nach einer Erläuterung der spezifischen Ausgangslage des eigenen Konzerns oder Unternehmens hat es sich bewährt, den Aufbau, die Aufgaben, Rechte und Pflichten der Compliance-Organisation zu beschreiben. Dazu zählen die zentralen Mitarbeiter in einer eigenen Compliance-Abteilung ebenso wie Mitarbeiter, die nur mit einem Teil ihrer Arbeitskraft Compliance-Aufgaben wahrnehmen und in Tochter- oder Enkelgesellschaften angesiedelt sind. Auch Schnittstellenfunktionen sollten an dieser Stelle beleuchtet werden, um Lücken in der Aufgabenbearbeitung oder Doppelzuständigkeiten zu vermeiden. Im Anschluss daran können die für das Gesamtunternehmen geltenden Richtlinien und anderen Vorgaben komprimiert dargestellt und erläutert werden. Denn je größer das Unternehmen, desto weniger bekannt sind diese Vorgaben z.B. im Ausland oder in neu gekauften Unternehmen oder Unternehmensbeteiligungen. Der ausführlichste und wichtigste Teil folgt unter Punkt 4. Hierunter befindet eine Schulungsunterlage mit allen Themen, die dezentrale Compliance-Mitarbeiter beherrschen und selbstständig schulen können müssen. Als besonderer Service kann dieser Teil separat so an die dezentralen Funktionen verschickt werden, dass sie diesen direkt einsetzen können und nur noch den Namen ihrer Einheit sowie ggf. landesrechtliche Besonderheiten ergänzen müssen. Bevor die dezentralen Funktionen nach dem Handbuch schulen, sollte dies einmal durch die erstellende Compliance-Abteilung persönlich oder in einem Webinar erläutert werden. Dadurch erhalten die dezentralen Funktionen wichtiges Hintergrundwissen und sehen

auch noch einmal Ziele und Verständnis von Compliance aus der zentralen Compliance-Abteilung. Abgerundet wird ein derartiges Handbuch durch eine Zusammenfassung, hier in Punkt 5 dargestellt, die die relevantesten Erkenntnisse und Anforderungen auf zwei bis drei Seiten darstellt.³¹

V. Die „Top 5 Stolpersteine“ in der Compliance-Kommunikation und Lösungsvorschläge

Nachdem in den vorherigen Abschnitten Techniken und Beispiele zur Verbesserung des Kommunikationsmanagements sowie der persönlichen und technischen Schulungsmöglichkeiten erläutert wurden, soll dieser Abschnitt die kommunikativen Fähigkeiten des Compliance Officers weiter schärfen, indem in der Praxis verbreitete Fehler („Stolpersteine“) in der Compliance-Kommunikation und deren Management aufgezeigt werden. Nach jedem Stolperstein oder Kommunikationsfehler folgt ein möglicher Lösungsvorschlag dieses Problems. **68**

Eine besondere Beachtung der Kommunikation ist von großer Bedeutung, da der zunehmende Einsatz von Online-Kommunikation oftmals zu Missverständnissen führt, die jedoch mangels einem persönlichen Kontakt nicht aufgeklärt werden. **69**

1. Fehlende, verspätete oder missverständliche Information

a) Problemstellung

Informationen zu geplanten Compliance-Maßnahmen sind für die betroffenen Mitarbeiter unerlässlich, damit diese sich auf die neuen Vorgaben und Anforderungen einstellen können. Erfolgt diese Information nicht, sind die Mitarbeiter davon überrascht. Bestenfalls wird die Maßnahme dann verspätet umgesetzt, im schlechtesten Fall wird sie nicht oder mangels Verständnis fehlerhaft umgesetzt. **70**

Dennoch trifft man in der Unternehmenspraxis immer wieder den Fall an, dass zum Beispiel eine Richtlinie zu Compliance-Themen einfach zentral in Kraft gesetzt wird und dann ins Intranet gestellt wird und hier selbstständig von den Mitarbeitern zum einen überhaupt gefunden werden, zum Zweiten dann gelesen, verstanden und umgesetzt werden soll. Dies funktioniert nicht, wie Skandale wie etwa der „Korruptionsskandal von Siemens“³² gezeigt haben. Hier lagen mehr als ausreichend interne Vorgaben und Richtlinien vor, die jedoch nicht hinreichend kommuniziert und umgesetzt und gelebt wurden. **71**

31 Eine ausführliche Darstellung des Aufbaus und Inhalts sowie dezidierte Erläuterungen dazu können bei *Hastenrath*, in: *Hastenrath*, Compliance-Kommunikation, Kap. 6 Rn. 77 ff. nachgelesen werden.

32 Eine gute Kurzübersicht zu dem Siemensskandal kann unter <http://www.br.de/nachrichten/spezial/zeitstrahl-siemens-skandale100.html> eingesehen werden (zuletzt abgerufen am 28.6.2024).

b) Lösungsvorschlag

- 72 Der erste Schritt zu einer Lösung beginnt bereits bei der Konzeption der Maßnahme, zum Beispiel der Antikorruptionsrichtlinie. Statt hier theoretisches Buchwissen oder ausschließlich externe rechtliche Expertise einzukaufen und in einer Richtlinie umzusetzen, müssen die Besonderheiten des Unternehmens, der Branche sowie ggf. von Tochtergesellschaften in einzelnen Jurisdiktionen ermittelt werden. Dies kann nicht „im stillen Kämmerlein“ des Compliance Officers in der Zentrale erfolgen, sondern beinhaltet die Einbeziehung und entsprechende Kommunikation mit unterschiedlichen Funktionen im Unternehmen.³³ Neben der Unternehmensspitze ist hier an den Vertrieb, den Einkauf, das Marketing sowie die einzelnen Landesgesellschaften zu denken.³⁴ Nur so wird die Richtlinie für das Unternehmen passend und berücksichtigt notwendige Besonderheiten. Sorgfalt sollte in diesem Zusammenhang mit der Kommunikation mit Unternehmensmitarbeitern über „Social Media“ an den Tag gelegt werden, da hier zahlreiche Unwägbarkeiten und Gefahren lauern.³⁵
- 73 In einem folgenden Schritt sollte der Richtlinienentwurf an eine kleine Zahl von Testpersonen verteilt werden, die später zum Adressatenkreis der Richtlinie gehören. Diese Testpersonen haben die Aufgabe, den Entwurf auf Verständlichkeit, Umsetzbarkeit und zutreffende Beschreibung ggf. kritischer Arbeitsabläufe und Situationen zu überprüfen. Dabei werden oftmals unerlässliche Verbesserungen gemacht und unentdeckte Schwachstellen behoben.
- 74 Bevor die Richtlinie dann in Kraft tritt bzw. mit ihrem Inkrafttreten, sind einerseits Gesprächstermine zwischen den Adressaten und der Compliance-Abteilung anzubieten, andererseits muss die Compliance-Abteilung die wichtigsten Adressaten zeitnah schulen. So wird sichergestellt, dass die Richtlinie verstanden wird. Nur wenn diese verstanden wird, können die darin enthaltenen Vorgaben auch von den operativen Mitarbeitern umgesetzt werden.
- 75 Soweit es Anpassungen der Richtlinie im Verlauf der Zeit gibt, sind Wiederholungsschulungen in regelmäßigen Abständen anzubieten. Auch sind Wiederholungen für das Behalten unerlässlich, denn nur einmal gehörte Informationen geraten schnell wieder in Vergessenheit.

33 Kommunikation wird oft als wichtiger Erfolgsfaktor in Projekten unterschätzt, so *Besl*, in: Bay, Handbuch Internal Investigations, S. 173 (im Zusammenhang mit internen Untersuchungen). Zur Notwendigkeit des „Schnittstellen-Managements“ der Compliance-Abteilung mit anderen Unternehmensfunktionen siehe ausführlich → *Rau*, Kap. 3 Rn. 4 ff.

34 Zum sog. „Schnittstellenmanagement“ zwischen der Compliance-Funktion und anderen Unternehmensfunktionen siehe auch → *Schulz*, Kap. 1 Rn. 85; → *Rau*, Kap. 3 sowie → *Renz/Frankenberger*, Kap. 20.

35 So *Lexa/Hammer*, CCZ 2014, 45 ff.; zu den Herausforderungen ebenfalls: *Lanzinner/Wirth*, CCZ 2021, 151 f.

2. Mangelnde Authentizität („Nicht gelebte Hochglanzaussagen“)**a) Problemstellung**

Die Compliance-Abteilung erlässt inhaltlich gute Richtlinien, prüft Prozesse im Rahmen von Risikoanalysen und macht notwendige Verbesserungsvorschläge, schult relevante Themen und richtet auch systemische Anpassungsbedarfe an die Unternehmensleitung. Die Unternehmensleitung zeichnet Richtlinien frei und hat auch eine Compliance-Abteilung eingerichtet, die Informationen zu Compliance in Schulungen und Ähnlichem an die Mitarbeiter geben kann. Wenn und wo es jedoch zu Verbesserungsvorschlägen und systematischen Anpassungsbedarfen aus Sicht der Compliance-Abteilung kommt, werden diese nur sehr zögerlich umgesetzt. Das heißt beispielsweise, eine Risikoanalyse ergibt, dass die Zusammenarbeit mit speziellen Beratern ein hohes Risiko zur Korruption birgt, dass selbst mit schärferen Compliance-Prüfungsvorgaben für diese Berater nicht ausgeschlossen oder auf ein akzeptables Maß minimierbar ist. Der Rat der Compliance-Abteilung ist daher, die Zusammenarbeit mit diesen Beratern komplett einzustellen und stattdessen fest angestelltes Personal vor Ort einzusetzen. Die Unternehmensleitung sieht zwar den entsprechenden Bericht und das darin beschriebene Risiko, stellt die Zusammenarbeit mit den Beratern aber nicht ein. Entweder wird der Prozess verschleppt, indem verschiedene Gutachten zur Lage der Berater über Monate hinweg extern beauftragt werden oder es wird durch die Unternehmensspitze gefordert, dass die Compliance-Abteilung das Risiko anderweitig beheben soll, was jedoch nicht möglich ist. **76**

Ein weiteres Beispiel für mangelnde Authentizität kann sich darin äußern, dass zwar von Unternehmensleitung und „oberer Führungsmannschaft“ die Bedeutung von Compliance betont wird, Compliance-Mitarbeiter aber bei wichtigen Entscheidungen nicht oder zu spät einbezogen werden. Möchte das Unternehmen also beispielsweise in ein hoch korruptes Land expandieren und hat schon das Unternehmen vor Ort gegründet und Mitarbeiter eingestellt, ohne die Compliance-Abteilung zu involvieren, lässt dies an der Ernsthaftigkeit der Beteuerungen von höchster Stelle zu compliance-gerechtem Verhalten zweifeln. **77**

b) Lösungsvorschlag

Dieses Problem kann nur von der Unternehmensleitung (oder einem etwaigen Aufsichtsgremium) gelöst werden.³⁶ Wenn es bei Mitgliedern der Geschäftsführung an der Überzeugung fehlt, dass gesetzmäßiges Handeln ein „Muss“ in jeder relevanten unternehmerischen Entscheidung ist, ist dies irreparabel. Die entsprechende Person kann dann nur ausgetauscht werden, da sonst kein funktionierendes Compliance-Management-System etabliert werden kann. Unterbleibt dies, weil das Organmitglied eine zu hohe Machtposition hat oder einen hohen Umsatz generiert, wird das Unternehmen früher oder später für seine Rechtsverstö- **78**

³⁶ Zur Rolle der Unternehmensleitung bzgl. der Gestaltung der Compliance-Kultur siehe → Schulz, Kap. 1 Rn. 69 ff. m. w. N.

ße zur Rechenschaft gezogen werden. Die dabei anfallenden Geldbußen, Freiheitsstrafen und der entstehende Reputationsverlust sind kaum vorhersehbar. Selbst wenn viele derartige Verstöße in der Vergangenheit unentdeckt und ungeahndet blieben, so hat sich die Verfolgungsbereitschaft und -intensität von staatlichen Behörden in den letzten 10 bis 15 Jahren immens erhöht. Hinzu kommt, dass im digitalen Zeitalter diese Behörden mit modernster Technik ausgestattet sind und Daten, die einmal im Unternehmen in einen PC eingegeben wurden, im Zweifel auch nach Jahren trotz Löschung der Unternehmensmitarbeiter noch aufgefunden werden können. Zudem hat sich auch die grenzüberschreitende Verfolgung von Behörden durch gegenseitige Unterstützung stark erhöht. Schließlich haben im Jahr 2024 nahezu alle Länder weltweit Gesetze gegen Korruption oder Kartell- und Wettbewerbsverstöße erlassen, wohingegen vor 20 Jahren noch viele, weiße Flecken auf der globalen Landkarte bestanden.

- 79 Sollte die Unternehmensleitung nicht aus Vorsatz, sondern aus Unwissenheit Compliance nicht die notwendige Unterstützung zuteilwerden lassen, ist es Aufgabe des Compliance-Verantwortlichen, die Geschäftsleitung diesbezüglich aufzuklären. Dabei hat der Compliance Officer die Geschäftsleitung insbesondere auf ihre Vorbildfunktion³⁷ hinzuweisen. Denn wenn schon die Geschäftsleitung keine Geschenke oder opulenten Einladungen annimmt, so spricht sich dies im Handumdrehen im Unternehmen herum und auch die meisten Mitarbeiter werden sich entsprechend verhalten. Spricht sich im Gegensatz dazu im Unternehmen herum, dass die Geschäftsleitung es „mit Compliance nicht so genau nimmt“, wird auch dieses Verhalten von den Mitarbeitern zu großen Teilen übernommen. Hier hat der Mitarbeiter dann immer die subjektive Rechtfertigung, dass „die oben es ja genauso machen“. Das Ernstnehmen des Themas „Compliance“ kann und muss daher von höchster Stelle stets selbst kommuniziert (Tone at the Top) und praktiziert (Action at the Top) werden.

3. Fehler im Kommunikationsmanagement: Budget- und Ressourcenmangel

a) Problemstellung

- 80 Einer der schwersten und häufigsten Fehler in Unternehmen ist das mangelhafte Management der Compliance-Kommunikation, teils aus Unkenntnis der Materie, teils aus Ignoranz.
- 81 Einige Beispiele sollen dies verdeutlichen: Der Chief Compliance Officer eines Unternehmens hat eine internationale Compliance-Organisation unter sich. Statt mit dieser nun eine passende Kommunikationsstrategie gegenüber den Mitarbeitern zu entwickeln, versucht er aus der Holding heraus seine Kommunikationsmaßnahmen „durchzudrücken“. Da er die größte Macht in der Compliance-Organisation hat, glaubt er qua seiner Stellung, so schnell und am

37 Zur Bedeutung der Vorbildfunktion der Unternehmensleitung siehe → *Schulz*, Kap. 1 Rn. 69 ff. m. w. N.

kostensparendsten Compliance-Themen im Konzern zu verbreiten. Dabei über-
sieht er, dass Mitarbeiter, hier die der Compliance-Organisation, auf Druck stets
mit Gegendruck agieren. Vielleicht nicht sofort und offensichtlich, jedoch un-
zweifelhaft zunächst in subtiler Form und immer austestend, ob die Macht des
Chief Compliance Officers noch besteht. Ist dies nicht der Fall, werden sie des-
sen Vorgaben zunehmend offen attackieren und nicht umsetzen und dabei auch
versuchen, ihre lokalen Geschäftsführungen von der Richtigkeit ihres Handelns
zu überzeugen.

Ein anderes Beispiel ist der (Irr-)Glaube der Geschäftsführung, dass die Kom- **82**
munikation kostenfrei oder mit minimalem Aufwand möglich sei.³⁸ Dies ist aus
Sicht der Autorin umso erstaunlicher, als dass es in diesem Bereich viele, hoch-
karätige Managementtrainings gibt, die auf die Relevanz und den notwendigen
Aufwand für eine geeignete Kommunikation im Unternehmen hinweisen.³⁹
Auch hier sollen Beispiele zur Verdeutlichung herangezogen werden.

aa) Unzureichende Übersetzung eines Code of Conduct (CoC)

Das global tätige Unternehmen möchte einen Code of Conduct (CoC)⁴⁰ erstellen **83**
und weltweit verteilen. Diese Aufgabe wird in der Compliance-Abteilung bear-
beitet. Nachdem der Compliance Officer eine genaue Erhebung gemacht hat,
welche sieben Sprachen im Unternehmen hauptsächlich gesprochen werden und
das Englisch in vielen Ländern Südeuropas, Lateinamerikas und Asiens bei den
Mitarbeitern des Unternehmens, die nicht im höheren Management sind, nicht
oder nur sehr rudimentär verstanden und gesprochen wird, empfiehlt er der Ge-
schäftsleitung, den CoC in die sieben ermittelten Sprachen übersetzen zu lassen.
Jede Übersetzung kostet ca. 400 bis 500 EUR, die die interne Übersetzungsabtei-
lung intern in Rechnung stellen würde. Die Geschäftsleitung entscheidet, dass
man aus Kostengründen, also hier zur Ersparnis von maximal 2.500 EUR (!) nur
eine englische und eine deutsche Variante anbietet. Sie erwarte, dass alle Mitar-
beiter hinreichend Englisch sprächen, was nachweislich nicht der Fall ist, wie
die Erhebung und Befragung einiger Mitarbeiter im Vorfeld ergeben hatte. Da-
rauf weist der CCO auch noch einmal hin, insbesondere äußert er die Befürchtung,
dass die Regelungen des CoC so nicht richtig verstanden und umgesetzt
werden könnten. Dies ändert an der Entscheidung der Geschäftsleitung aller-
dings nichts. In der Folgezeit wird der CoC in den zwei genannten Sprachen ver-

38 In diesem Zusammenhang wird derzeit auch der Umfang und der erforderliche Aufwand, in-
klusive der dazugehörigen Kommunikation, der Geschäftsführung der Konzernobergesell-
schaft und Tochtergesellschaften im Rahmen einer Haftung nach § 130 OWiG diskutiert,
siehe dazu ausführlich *Caracas*, CCZ 2015, 167 ff.

39 Siehe hierzu beispielsweise die Seminare zu Schlüsselkompetenzen einer erfolgreichen
Kommunikation unter: Compliance-Kommunikation von Haufe unter: <https://www.haufe-akademie.de/4376> oder ein Angebot des Manager Instituts unter: <https://www.manager-institut.de/training/seminar/compliance-kommunikation.html> (beide Fundstellen zuletzt abgeru-
fen am 18.3.2024).

40 Zur Entwicklung und Bedeutung eines Code of Conduct siehe *Benkert*, Kap. 4 m. w. N.

öffentlich. Der CCO ist weiterhin für das Projekt verantwortlich und erhält u. a. aus Asien die Anfrage, ob eine Übersetzung ins Chinesische vor Ort möglich sei, da die Mehrheit der Mitarbeiter die englische Fassung nicht verstehe. Eben solche Anfragen erhält er im Laufe der nächsten Monate aus Südamerika, Portugal, Russland und Belgien. In Belgien sei die Übersetzung aus gesetzlichen Gründen ins Französische notwendig, eine englische Fassung reiche nicht aus. Der CCO ist mit diesen Anfragen, Rücksprachen mit den jeweiligen Compliance-Mitarbeitern vor Ort und in den größten Einheiten, der Sichtung und Prüfung der angefertigten Sprachversionen sowie mit zwei Entscheidungsvorlagen an die Geschäftsleitung über eine Arbeitswoche beschäftigt. Im Ergebnis stimmt die Geschäftsleitung insoweit zu, dass die anderen Sprachversionen als „Höflichkeitsübersetzung“ angefertigt werden können, im Zweifelsfall zur Beurteilung von Verstößen o. Ä. aber nur die englische und deutsche Fassung Geltung finden. Im Ergebnis haben die Übersetzungen in die weiteren Sprachen somit weit über 10.000 EUR gekostet.

- 84** Diesem Problem kann künftig ggf. durch den Einsatz von Künstlicher Intelligenz (KI) begegnet werden, die eine Übersetzung in sehr guter Qualität kostenfrei zur Verfügung stellt. Allerdings ist hier zu hinterfragen, ob die Daten geeignet sind, auf diese Weise übersetzt zu werden, da diese dann nicht mehr in der Datenhoheit des Unternehmens liegen, sondern gemäß der Nutzungsbedingungen vieler KI-generierter Übersetzungsprogramme von diesen genutzt werden können, ohne dass das Unternehmen darauf noch einen Einfluss nehmen kann.

bb) Unzureichendes Schulungsbudget

- 85** Als weiteres Beispiel soll die Durchführung von Präsenztrainings im Kartellrecht dienen.⁴¹ Das Thema wurde vom CCO aufgegriffen, da er im Rahmen einer Risikoanalyse festgestellt hat, dass hier erhebliche Gefahren für das Unternehmen liegen. Der CCO ermittelt daraufhin die konzernweit zu schulenden Kollegen anhand von deren Tätigkeiten. Im Ergebnis sollen mit verschiedenen Konzernunternehmen in verschiedenen Ländern fünf Schulungen mit je 15 Mitarbeitern für je zwei bis drei Stunden stattfinden. Einerseits sollen nur Kollegen zusammen geschult werden, die in der gleichen Unternehmenssparte arbeiten und in der nötigen Offenheit untereinander im Rahmen der Schulung Probleme offenlegen, zum anderen ist eine konstruktive Arbeitsatmosphäre bei Gruppen über 15 bis 20 Mann nicht gewährleistet, da sich in großen Gruppen die Kollegen gerne hintereinander verstecken. Der CCO legt dieses Schulungskonzept so der Geschäftsführung zur Freigabe vor. Die Geschäftsleitung hält den Aufwand für zu hoch und genehmigt stattdessen einen Slot zum Kartellrecht von 45 Minuten auf der nächsten, zweitägigen Managementkonferenz mit 150 Teilnehmern am zweiten Tag um 15 Uhr. Auf der Tagung wird die Kartellrechtsschulung wie genehmigt durchgeführt. Zu diesem Zeitpunkt sind allerdings schon

41 Zu Schulungen im Kartellrecht ausführlich → *Seeliger/Mross/Seydel*, Kap. 27.

viele Teilnehmer abgereist, da die Tagung um 16 Uhr endet. Fragen werden kaum gestellt.

b) Lösungsvorschlag

Wirksame Kommunikation kostet Geld. Das muss die Unternehmensleitung erkennen. In Zeiten zunehmender Aufgabenverdichtung und Informationsüberflutung reicht eine „Postwurfsendung“ mit einer neuen Richtlinie oder eine einmalige Schulung von 45 Minuten in einem Thema noch viel weniger aus als früher. Nicht umsonst investieren Unternehmen in die Kundenkommunikation, nämlich vornehmlich in die Werbung, nicht selten Millionenbeträge. Aufwendige „TV-Spots“ werden produziert und zur besten Sendezeit platziert, Werbeplakate mit teuren Agenturen erarbeitet und an exponierten Stellen plakatiert oder es werden kostspielige Gewinnspiele oder Aktionen durchgeführt, um die Kunden auf das eigene Produkt aufmerksam zu machen oder daran zu binden. Warum sollte demgegenüber in der internen Kommunikation mit den Mitarbeitern alles anders funktionieren? Die Zeiten, in denen Mitarbeiter nach der Lehre oder dem Studium eine Lebensanstellung im Unternehmen gefunden hatten und sich bedingungslos mit ihrem Unternehmen identifiziert haben, sind auch Dank der Unternehmensstrategien, Mitarbeiter als beliebig austauschbares und trotz hohen Gewinnen jederzeit abbaubares „Humankapital“ zu betrachten, vorbei. Die Mitarbeiter wollen rechtzeitig, ansprechend und möglichst umfassend über die sie betreffenden Ereignisse im Unternehmen informiert werden. Dies wird gerade von jüngeren Arbeitnehmern als selbstverständlich vorausgesetzt und erwartet. Erfolgt dies nicht und hält die unzureichende Kommunikation über einen längeren Zeitraum an, etwa bei Unternehmensumstrukturierungen anlässlich einer Krise, gehen zuerst die Leistungsträger. Diejenigen, die aus Zwängen nicht gehen können oder wollen sowie diejenigen Mitarbeiter, die Schwierigkeiten haben, eine neue Anstellung zu finden, bleiben dem Unternehmen dagegen erhalten. Allerdings sinkt deren Arbeitsleistung und Einsatzbereitschaft oftmals erheblich, Fehlzeiten nehmen zu. Zwar passiert dies nicht in dem extremen Maße wie im beschriebenen Umstrukturierungsbeispiel bei nicht oder nicht gut kommunizierten Compliance-Maßnahmen, aber in kleinerem Maße sehr wohl. Das Ergebnis ist, dass die angestrebte Verhinderung von Rechtsverstößen nicht erreicht wird, mit allen negativen Konsequenzen, die damit verbunden sind.

Daher müssen Unternehmen und insbesondere die Geschäftsleitung schon aus ureigenen „Enthaftungsinteressen“ ein ausreichendes Kommunikationsmanagement für Compliance aufbauen und die notwendigen Ressourcen bereitstellen.

4. Probleme mit der Technik

a) Problemstellung

Unternehmen sind heute häufig stark abhängig von der Technik. Ohne PC und IT-Support funktioniert in vielen Unternehmen nichts mehr. Die IT-Budgets von großen Konzernen liegen im mehrstelligen Millionenbereich.

- 89** Auch für das Management der Compliance-Kommunikation hat das erhebliche Folgen. Es wird einerseits erwartet, dass die Mitarbeiter alle IT-Lösungen bedienen können. Andererseits wird beim Einkauf von diesen für den Compliance-Bereich von diesen Produkten erwartet, dass sie weltweit im Konzern einsetzbar sind und problemlos in die bestehende IT-Landschaft des Hauses integriert werden können. Zwei Annahmen, die leider in vielen Fällen in Unternehmen nicht zutreffen.
- 90** Zunächst seien die Mitarbeiter betrachtet, denen oftmals ohne jegliches Training zugemutet wird, digitale Programme zu bedienen. Oder es wird vorausgesetzt, dass jeder Mitarbeiter über einen PC-Arbeitsplatz verfügt, um zum Beispiel ein E-Learning für Compliance zu absolvieren. Dies ist von der Unternehmensrealität häufig weit entfernt. Nicht nur ältere Mitarbeiter, auch Mitarbeiter der Produktion und angrenzender Bereiche sind im Umgang mit dem PC, abgesehen von absoluten Basiskenntnissen, oftmals überfordert. Hinzu kommt, dass viele Programme auch für geübte Mitarbeiter von IT-Standardanwendungen, Probleme beinhalten, die nicht ohne Vorkenntnisse bzw. eine ausreichende Einarbeitung in das Programm oder IT-Support gelöst werden können. Dies funktioniert meistens auch nicht durch eine Anleitung als Dokument, sondern bedarf eines persönlichen Trainings, in welchem die einzelnen Anwendungsschritte gezeigt und mögliche Fragen beantwortet werden können.
- 91** Hinzu kommt, dass die „IT-Landschaft“ gerade in Konzernen und großen Unternehmen oftmals höchst komplex und nicht selten instabil und fehleranfällig geworden ist. In vielen Fällen kann daher ein neues „Compliance-IT-Produkt“ nicht ohne Zeitverzögerung und internem wie externem Kostenaufwand eingerichtet werden. Es kann und ist in der Praxis mehrfach vorgekommen, dass Compliance-IT-Produkte wie ein E-Learning in einzelnen Ländern, in denen Tochterunternehmen des Unternehmens angesiedelt waren, überhaupt nicht funktionierten oder dass die interne Integration eines E-Learnings ein zusätzliches halbes Jahr in Anspruch genommen hat und ein fünfstelliges, nicht einkalkuliertes Budget zur Implementierung notwendig wurde.⁴²
- 92** Aktuell zeigen sich auch Probleme in den zahlreichen, unterschiedlichen IT-Tools zur Videotelefonie, die oftmals untereinander inkompatibel sind und sich gegenseitig stören. Gerade im internationalen Konzern kommt es aber häufig vor, dass mehr als ein Programm im Einsatz ist, und Probleme hier daher besonders störend sind.

b) Lösungsvorschlag

- 93** Probleme mit der Technik lassen sich von der Compliance-Funktion nur bedingt lösen, da diese unternehmensübergreifend sind und die Compliance-Abteilung auf vieles in diesem Bereich keinen oder nur einen sehr begrenzten Einfluss hat. Dennoch gibt es einige Ansatzpunkte, die das Compliance-Kommunikationsma-

42 Persönliche Erfahrungen oder Erfahrungen aus dem Netzwerk der Autorin.

nagement der Compliance-Abteilung gegenüber den Mitarbeitern jedenfalls verbessern.

Zunächst ist bei allen Einsätzen von technischer Unterstützung für Compliance-Maßnahmen, seien es E-Learnings, Webinare, Business-Partner-Prüfungen mit einer Software, (Risiko-)Abfragen mit einer Software, Lieferantenprüfungen o. Ä., ein entsprechendes IT-Budget einzuplanen. Oftmals gibt es im Unternehmen auch ein Gesamtbudget für die Frage, wie viele Ausgaben unternehmensweit für neue Technik eingesetzt werden soll. Kommt man hier als Compliance Officer zu spät oder hat das Projekt aus Sicht der IT oder/und Unternehmensleitung den Nachrang gegenüber anderen IT-Projekten, so kann dies dazu führen, dass ein Compliance-IT-Projekt in einem Jahr nicht umgesetzt werden kann. Diese mögliche Restriktion muss vorab in die Überlegungen der Compliance-Abteilungen aufgenommen werden. Nichts ist ärgerlicher, als eine technische Compliance-Kommunikationsmaßnahme auf einer internen Tagung bereits angekündigt zu haben, um diese dann nicht „auf den Boden zu bekommen“. Dies nimmt der gesamten Compliance-Tätigkeit Glaubwürdigkeit und kann auch dazu führen, dass die Compliance-Mitarbeiter ihre Zielvereinbarungen für das Jahr nicht erreichen können. **94**

Ist die Budgetfrage geklärt, muss der Einkauf oder die eigene, interne Entwicklung von IT-Produkten nicht nur von der Compliance-Abteilung vorgenommen werden, sondern es muss zwingend frühzeitig die IT-Abteilung mit einbezogen werden. Nur diese hat einen genauen Überblick über die interne IT-Landschaft und kann mit ihrer Fachkompetenz ein passendes Anforderungsprofil an neue IT-Produkte formulieren. Leider wird dies in der Praxis häufig versäumt, sodass nach den Beteuerungen der externen Anbieter ein Produkt bereits eingekauft ist, ohne die IT nach entsprechenden Parametern befragt zu haben. Die Konsequenz sind unnötige Zeit- und Kostenaufwände und erheblicher Ärger. **95**

Schließlich ist es die Aufgabe der Compliance-Abteilung zu evaluieren, welche Mitarbeiter, die mit technischem Einsatz geschult werden sollen oder die Informationen mit Unterstützung von IT-Anwendungen an die Compliance-Abteilung liefern sollen, diesen Anforderungen überhaupt gewachsen sind. Sind Mitarbeiter dem nicht gewachsen, müssen diese zunächst in die Technik eingeführt werden. Dazu sind Kosten- und Zeitaufwände notwendig und unvermeidbar. Insbesondere die Bedienung neuer IT-Lösungen bedarf eines oftmals 4–5fach höheren Aufwands im Vergleich zu einer bekannten und schon mehrfach gehaltenen Powerpoint-Präsentation.⁴³ **96**

Nicht minder wichtig ist es für die Compliance-Abteilung sicherzustellen, dass alle Mitarbeiter, die IT-Lösungen im Compliance-Kontext nutzen sollen, auch ausreichenden Zugang zu einem PC-Arbeitsplatz haben. Ob dies durch die Einrichtung von allgemeinen PC-Terminals in der Produktion oder anderen Abtei- **97**

43 Erfahrungswerte der Verfasserin im Umgang mit den IT-Lösungen „Zoom“, „WBS Learn-space 3D“ und „Microsoft Teams“.

lungen ohne individuelle PC-Arbeitsplätze erfolgt oder die Mitarbeiter sich mit privaten Geräten einwählen können, spielt letztlich keine Rolle. Wichtig ist nur, dass dieser Punkt frühzeitig erkannt und von der Compliance-Abteilung mit eingeplant und gelöst wird. So können ungeplante Verzögerungen und Störungen präventiv vermieden werden.

5. Fehler im Kommunikationsmanagement von Compliance aufgrund von Kulturunterschieden

a) Problemstellung

- 98** Compliance-Maßnahmen sind nie national beschränkt, sondern erstrecken sich regelmäßig auf das gesamte Unternehmen. Je größer und internationaler dieses ist, desto unterschiedlichere Jurisdiktionen und damit Kulturkreise sind betroffen.
- 99** Oftmals läuft das Aufsetzen und Durchführen z.B. von Präsenztrainings wie folgt ab: Ein Compliance-Mitarbeiter aus der deutschen Muttergesellschaft setzt ein Antikorruptionstraining auf, welches an deutschem Recht und dem deutschen Kulturraum ausgerichtet ist, ggfs. mit Exkursen zu einzelnen, besonders wichtigen Jurisdiktionen wie den USA. Dieses Training wird dann zumeist ins Englische übersetzt und dann weltweit eingesetzt. Es wird dabei davon ausgegangen, dass dieses Training, das in Deutschland auch gut funktionieren mag, gleichen Erfolg in anderen Ländern haben wird. Das ist jedoch oftmals nicht der Fall. Ganz im Gegenteil. Es werden derartige „Kardinalfehler“ gemacht, dass die Schulung in manchen Ländern in keiner Weise akzeptiert wird und damit deren Inhalte auch nicht umgesetzt werden. Die folgenden Beispiele können das am treffendsten verdeutlichen:
- 100** In einem muslimischen Land wird ein Compliance Officer für die Schulung eingesetzt. In der Schulung gibt es zwar keine offene Ablehnung, aber auch keine aktive Teilnahme. Einige Zeit nach der Schulung wird überprüft, inwieweit die Teilnehmer die Inhalte der Schulung in ihrem Unternehmen umgesetzt haben. Das Ergebnis ist sehr schlecht, es ist so gut wie nichts umgesetzt worden.
- 101** In den USA werden die Mitarbeiter, nicht jedoch die Vorgesetzten geschult. Die Schulung erfolgt durch einen Compliance-Mitarbeiter, nicht durch den Chief Compliance Officer. Als in der Folgezeit die deutschen Compliance-Mitarbeiter auf die Umsetzung einiger Compliance-Maßnahmen drängen, welche die amerikanischen Kollegen auch zugesagt hatten, jedoch nichts passiert war, fragen sich die deutschen Mitarbeiter, woran diese Verzögerung liegen könnte. Sie sind ratlos.
- 102** Der deutsche Compliance Officer fliegt zu einem wichtigen Compliance-Projekt nach Italien. In seinen drei Tagen vor Ort muss er ein sehr anspruchsvolles und umfangreiches Maßnahmenpaket hinsichtlich des Dekrets 231/2001, des italienischen Antikorruptions- und „Antimafiagesetzes“, in entscheidenden Punkten umsetzen. Sein Flugzeug landet um 7 Uhr in Mailand, um 8.45 Uhr ist er am Ort

der Tochtergesellschaft und wird vom Empfangspersonal in den Konferenzraum geführt. Für 9 Uhr ist der Beginn der ganztägigen Besprechung angesetzt, für die der Compliance Officer die Erarbeitung zahlreicher Unterlagen mit den italienischen Kollegen vereinbart hatte. Bis 13 Uhr treffen die entsprechenden Kollegen jedoch nicht im Besprechungsraum ein und melden sich auch nicht auf die Kontaktversuche per E-Mail und Telefon durch den deutschen Compliance Officer. Um 13.10 Uhr erscheint schließlich der erste italienische Kollege und weist darauf hin, dass es kurzfristig wichtige Managementmeetings gäbe, weshalb er und seine Kollegen die Unterlagen für den deutschen Kollegen absprachewidrig nicht fertigstellen könnten und von den geplanten drei Tagen auch nur ein Tag für Besprechungen zum Dekret 231/2001 zur Verfügung stünde. Der deutsche Compliance Officer ist entsetzt.

b) Lösungsvorschlag

Die Lösung ist denkbar einfach. Zunächst ist der Compliance Officer im interkulturellen Kontext zu schulen.⁴⁴ Das heißt, er sollte Trainings zum Umgang mit einzelnen Ländern und deren Kulturkreisen absolvieren. Solche interkulturellen Trainings sollten je Land mindestens einen vollen Tag dauern und am besten durch Trainer aus dem jeweiligen Land oder Trainern, die selbst lange in diesem Land gelebt haben, durchgeführt werden.⁴⁵ Besonders geeignet sind auch speziell auf das jeweilige Unternehmen zugeschnittene Inhouse-Seminare. **103**

Ebenfalls kann es sich anbieten, an Projekten im Land teilzunehmen, nachdem das erste interkulturelle Training abgeschlossen wurde. Hier sollte zunächst eine gewisse Zurückhaltung des Compliance-Verantwortlichen an den Tag gelegt werden, sodass er zunächst das kulturelle Verhalten im Land auf sich wirken lässt und im Anschluss daran versucht, dieses in seinem Verhalten und seinen Compliance-Maßnahmen zu berücksichtigen. **104**

Soweit Compliance-Maßnahmen aufgesetzt werden, müssen diese so oft wie möglich mit einem oder mehreren Mitarbeitern jedes Ziellands vorab durchgesprochen und ggf. auf landestypische Besonderheiten angepasst werden. Diese Abstimmungen mögen zunächst zeitaufwendig erscheinen. Mittel- und langfristig rechnen sich diese jedoch immer, da nur so sichergestellt werden kann, dass die Mitarbeiter die Inhalte der Compliance-Maßnahmen verstehen, kulturell akzeptieren und schließlich auch umsetzen. **105**

44 Vgl. dazu auch Kark, in: Bürkle/Hauschka/Schieffer, Der Compliance Officer, Anhang – Checklisten, Checkliste 5: Kernkompetenzen des Compliance Officers, die interkulturelles Verständnis als eine Kernkompetenz eines Compliance Officers ansieht.

45 Interkulturelle Trainings werden in etwa angeboten unter: <https://www.kitzmann.biz/seminare/seminaruebersicht/fuehrung/interkulturelle-kompetenz/?gclid=CMB74cnd-McCFRITGwodUIMA1Q> oder unter: <http://www.eidam-und-partner.de/de/interkulturelles-training> (beide Fundstellen zuletzt abgerufen am 18.3.2024).

VI. Fazit zur Compliance-Kommunikation

- 106** Die Ausführungen in diesem Kapitel haben gezeigt, dass das Kommunikationsmanagement im Bereich Compliance vielschichtig und anspruchsvoll ist. Keinesfalls darf es nur als das „nicht durchdachte Ende“ einer inhaltlich erarbeiteten Compliance-Maßnahme betrachtet werden, die jetzt „nur noch mal eben und irgendwie“ an die Adressaten verteilt werden muss. Eine derartige Denk- und Handlungsweise gefährdet den gesamten Erfolg der jeweiligen Compliance-Maßnahme, wie die ausführlichen Beispiele gezeigt haben. Nur wenn die Adressaten in für sie verständlicher und kulturell passender Weise adressiert werden, können die Compliance-Maßnahmen erfolgreich umgesetzt werden. Wird hier im Gegensatz dazu mit Druck und Zwang in der Kommunikation gearbeitet, ist davon allenfalls ein widerwilliger, kurzfristiger Erfolg zu erwarten. Mittel- und langfristig funktioniert ein solches Vorgehen nicht.
- 107** Durch den Einsatz weniger, einfacher Kommunikationsmodelle wie dem von *Benien* zu den Konfliktarten oder dem 4-Schritte-Dialog, kann die Compliance-Kommunikation erheblich verbessert werden. Da es hier neben dem Erlernen von Wissen für den Compliance Officer insbesondere um den Erwerb von praktischem Können geht, sollte dieser die vorgeschlagenen Modelle in einem oder mehreren Trainings zunächst in der Umsetzung anwenden und üben. Ansonsten wird er unter Umständen in kritischen Kommunikationssituationen nicht die notwendige Sicherheit und Geschwindigkeit haben, derer es für den erfolgreichen Einsatz dieser Modelle bedarf.
- 108** In der Praxis haben sich in den letzten 20 Jahren eine Reihe von Instrumenten der Compliance-Kommunikation wie etwa Informationsschreiben, persönliche Beratungen, ein Compliance-Intranetauftritt oder Ähnliches bewährt. Erfolg haben diese insbesondere dann, wenn sie inhaltlich und zeitlich im Rahmen eines Projektplans passend aufeinander abgestimmt sind. Dies erfordert einige Erfahrung oder externe Unterstützung des Compliance Officers, da es hier eine Reihe von Punkten zu beachten gilt, die nicht sofort auf der Hand liegen und entsprechende Erfahrung in diesem Bereich erfordern.
- 109** Nach wie vor nicht ersetzbar im Kommunikationsmanagement von Compliance sind Schulungen. Hier kommen zunächst immer persönliche Präsenzs Schulungen durch den Compliance Officer, ggf. mit externer Unterstützung oder Unterstützung durch Compliance-Mitarbeiter aus einzelnen Regionen oder Ländern, in Betracht. Soweit diese Schulungen gut durchdacht sind, d.h. adressatengerecht und mit unternehmensindividuellen Beispielen versehen sind, werden diese die erforderliche Sensibilisierung der Mitarbeiter erzielen. Tritt auch der Compliance Officer mit einer Einstellung als Unterstützer und Problemlöser der Operativen, soweit dies rechtlich und ethisch zulässig ist, auf, wird so eine Vertrauensbasis geschaffen, die die Grundlage für die Lösung von Compliance-Risiken im Unternehmen darstellt.

Neben den nach wie vor unverzichtbaren persönlichen Schulungen, denen zeitliche und ressourcentechnische Grenzen gesetzt sind, hat sich auch der Einsatz von technischer Schulungsmethodik (digitale Compliance) bewährt und durchgesetzt. Zunächst ist hier an das klassische E-Learning zu denken, bei welchem die Mitarbeiter am PC zu einem von ihnen frei wählbaren Zeitpunkt eine Compliance-Schulung absolvieren können. Beachtet der Compliance Officer die Grenzen solcher E-Learnings, hier zu nennen sind vor allem die Eignung der E-Learnings hauptsächlich für Basisthemen und als Wiederholung oder Vertiefung nach Präsenzs Schulungen, kann ein E-Learning ein wertvolles Trainings- und Kommunikationsmittel darstellen. In diesem Beitrag vertieft betrachtet wurde auch die Schulung mit Webinaren. Webinare kombinieren die technische Möglichkeit von E-Learnings, den Teilnehmern Inhalte am PC zu präsentieren mit dem Element der Präsenzs Schulung, live und persönlich vor den Mitarbeitern zu sprechen und auf Fragen direkt eingehen zu können. Da für das Durchführen von Webinaren andere Fähigkeiten und Techniken des Compliance Officers als bei Präsenzs Schulungen gefordert sind, sollte dieser sich als E-Trainer ausbilden lassen oder jedenfalls einige Webinare als „Trockenübung“ vor einigen wenigen Kollegen, vielleicht aus der Compliance- oder Rechtsabteilung durchführen, um final ein gutes und überzeugendes Webinar vor dem eigentlichen Zielpublikum abhalten zu können. Aktuell werden Webinare in der Compliance in etwa über die IT-Lösungen Zoom, Microsoft Teams, Adobe Connect oder WBS Learn Space 3D durchgeführt.

Schließlich wurden einige der größten Fehler im Kommunikationsmanagement von Compliance beleuchtet sowie Lösungsmöglichkeiten aufgezeigt, diese Fehler von vornherein zu vermeiden. Diese Fehler lassen sich in drei grobe Gruppen aufteilen. Zunächst gehören eine fehlende, verspätete oder missverständliche Information sowie ein Budget- und Ressourcenmangel inhaltlich in denselben Bereich. Hier tritt entweder mangelndes Wissen und Können in der Umsetzung von Kommunikation oder mangelndes Wissen und Können gepaart mit mangelndem Budget und mangelnden Ressourcen auf. Es soll noch einmal betont werden, wie stark das Einsparen von Mitteln an dieser Stelle den Erfolg jeder Compliance-Maßnahme gefährdet. Es muss daher immer ausreichend Zeit und Budget für die Kommunikation an dieser Stelle eingeplant werden.

Die nächste Gruppe ist die der mangelnden Authentizität der höchsten Führungsebene, ohne die kein CMS im Unternehmen funktioniert. Oftmals wird dies von der Geschäftsleitung nicht oder nicht hinreichend berücksichtigt. Insbesondere die gelebte Vorbildfunktion ist oftmals mangelhaft.

Ein nicht zu unterschätzender Stolperstein ist auch eine nicht funktionierende technische Umsetzung der Compliance-Kommunikation. Wenn sich in einem E-Learning einzelne Elemente nicht anklicken lassen, Webinare während der Übertragung wiederholt abstürzen oder Mitarbeiter nicht über die technischen Geräte und Kenntnisse in deren Bedienung verfügen, sind diese Maßnahmen von Beginn an zum Scheitern verurteilt. Es bedarf daher einer sorgfältigen Pla-

nung und Prüfung durch den Compliance-Verantwortlichen unter frühzeitigem und dauerhaftem Einbezug der IT-Experten im Haus, die ggf. auch den compliance-gerechten Umgang mit KI-Tools trainieren.

- 114** Schließlich müssen kulturelle Unterschiede in den verschiedenen Ländern, in denen ein Konzern (Tochter-)Gesellschaften betreibt, beachtet werden. Eine in Deutschland erfolgreiche Schulung kann aus kulturellen Gründen beispielsweise in Russland ein Misserfolg werden und umgekehrt. Hier bedarf es zunächst des grundsätzlichen Erkennens dieser Unterschiede gefolgt von einer Umsetzung, die diese berücksichtigt. Am einfachsten ist hier die Einbeziehung bei der Entwicklung von Kommunikationsmaßnahmen der jeweiligen Mitarbeiter des zutreffenden Landes. Dadurch werden kulturelle Fehlritte vermieden und durch die aktive Einbeziehung die Akzeptanz für die jeweilige Maßnahme erhöht.

7. Kapitel

Auswirkungen des ISO-Standards 37301 auf die Prüfung von Compliance-Management-Systemen nach IDW PS 980 und Vergleich mit ISO 31022*

I. Einleitung

Die ISO-Norm 37301:2021 „Compliance management systems – Requirements with guidance for use“¹ legt Anforderungen fest und enthält Leitlinien sowie empfohlene Praktiken zur Ausgestaltung, Einführung und Durchführung von Compliance-Management-Systemen (CMS). Die Anforderungen und Leitlinien sollen laut Standard in Bezug auf Größe, Struktur, Art und Komplexität an alle Organisationen anpassbar sein. In den letzten Jahren haben viele Unternehmen ihr CMS bereits nach dem Standard des Instituts der Deutschen Wirtschaftsprüfer (IDW) zur ordnungsmäßigen Durchführung von Prüfungen eines CMS (IDW PS 980) auf Angemessenheit und Wirksamkeit prüfen lassen. Das nachfolgende Kapitel² beleuchtet, welche Gemeinsamkeiten und Unterschiede zwischen den Standards bestehen, welche Auswirkung der ISO-Standard auf eine nach IDW PS 980 durchgeführte CMS-Prüfung hat, bzw. ob eine Prüfung nach IDW PS 980 die Einhaltung der ISO-Norm 37301:2021 bestätigen kann. Auch die ISO-Norm 37301:2021 selbst ist nun, anders als noch ihre Vorgängerin, zertifizierbar (ISO-Zertifizierung).

Der IDW PS 980³ hat seit der Veröffentlichung im Jahr 2011 und seiner Aktualisierung im Jahr 2022 (IDW PS 980 n.F.)⁴ eine weite Verbreitung bei der Beurteilung von CMS gefunden. Eine zunehmende Anzahl von Unternehmen richtet sich bei der Ausgestaltung ihres CMS an den Vorgaben dieses Standards aus. Es stellt sich die Frage, welche Gemeinsamkeiten und Unterschiede zwischen den

* Die Autoren danken Herrn Dr. *Konstantin von Busekist*, der in der Voraufage an der Bearbeitung dieses Beitrags mitgewirkt hat.

1 ISO 37301:2021, Compliance-Managementsysteme – Anforderungen mit Leitlinien zur Anwendung, 1. Anwendungsbereich, S. 10, www.iso.org/obp/ui/#iso:std:iso:19600:ed-1:v1:en (zuletzt abgerufen am 14.8.2024).

2 Dieses Kapitel basiert auf dem Aufsatz von *Withus/Kunz*, Auswirkungen des neuen ISO 19600:2014 zu Compliance-Management-Systemen auf die Prüfung nach IDW PS 980, BB 2015, 685 ff. und stellt eine Fortschreibung und Aktualisierung desselben dar.

3 IDW Prüfungsstandard: Grundsätze Ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980), WPg Supplement 2/2011.

4 IDW PS 980 n.F. (09/2022), <https://www.idw.de/idw/idw-aktuell/idw-ps-980-n-f-09-2022-zur-pruefung-von-compliance-management-systemen-verab-schiedet.html> (zuletzt abgerufen am 14.8.2024).

beiden Standards bestehen und welche Auswirkung der ISO 37301:2021⁵ auf die Beurteilung der Angemessenheit von CMS haben kann bzw. wie sich die Beziehung zwischen ISO-Standard und IDW-Prüfungsstandard darstellt. Zu beurteilen ist, ob ein nach der ISO-Norm ausgestaltetes CMS, Gegenstand einer Prüfung nach IDW PS 980 sein kann, bzw. ob eine solche Prüfung die Einhaltung der Anforderungen der ISO-Norm 37301:2021 bescheinigen kann. Hierzu sollen zunächst die Zielsetzung und die Zielgruppen sowie der Betrachtungsgegenstand der beiden Standards analysiert werden. Anschließend werden die Anforderungen dargestellt, die der IDW-Standard an Rahmenwerke stellt, die der Ausgestaltung von CMS zugrunde gelegt werden. Darauf aufbauend wird untersucht, ob und inwieweit die Aussagen der beiden Standards zur Ausgestaltung von CMS Verbindlichkeit besitzen und ob diese Anforderungen kompatibel oder eventuell widersprüchlich sind.

II. Zielsetzung und Zielgruppe

1. Ausgangslage

- 3 Die Begriffe „Compliance“ und „Compliance-Management-System“ wurden seit Beginn der 2010er-Jahre nahezu inflationär verwendet, eine inhaltliche Konkretisierung fehlte jedoch. Dass Compliance als Pflicht zur Einhaltung von Gesetzen eine Binsenweisheit ist, hatte *Schneider* schon 2003 festgestellt;⁶ und nicht erst seit dem Urteil des LG München⁷ im Jahr 2013 dürfte es herrschende Meinung sein, dass es hierfür gezielter organisatorischer Maßnahmen im Rahmen eines einheitlichen CMS bedarf.⁸ Auch das Gesetz zur Stärkung der Finanzmarktintegrität (FISG)⁹ vom 3.6.2021 enthält Anreize zur Einrichtung eines CMS und verpflichtet durch den neu geschaffenen § 91 Abs. 3 AktG börsennotierte Unternehmen jedenfalls zur Einrichtung eines angemessenen und wirksamen internen Kontroll- und Risikomanagementsystem.¹⁰ Ähnlich wie im Hinblick auf das Compliance Management verzichtet der Gesetzgeber jedoch bislang darauf, konkrete Anforderungen an ein solches internes Kontroll- und Risikomanagementsystem zu definieren. Entsprechendes gilt mit Blick auf die Regelungen des Entwurfs der EU-Richtlinie zur Bekämpfung der Korruption vom 3.3.2023, die in ihrem Art. 18 Abs. 2 lit. b eine Sanktionsmilderung für Unternehmen vorschreibt, die „vor oder nach der Begehung der Straftat wirksame

5 ISO 37301:2021, Compliance management systems – Requirements with guidance for use, <https://www.iso.org/standard/75080.html#:~:text=What%20is%20ISO%2037301%3F,compliance%20management%20system%20within%20organizations> (zuletzt abgerufen am 14.8.2024).

6 *Schneider*, ZIP 2003, 645, 646.

7 LG München, 10.12.2013, 5 HKO 1387/10, BB 2014, 850 LS m. BB-Komm. *Grützner*. Siehe hierzu auch → *Schulz*, Kap. 1 Rn. 39.

8 So im Ergebnis auch *Merkt*, DB 2014, 2271, 2273. Zur Compliance-Organisationspflicht und den damit verbundenen Maßnahmen siehe auch → *Schulz*, Kap. 1 Rn. 27 ff.

9 BGBl. 2021 I, S. 1534 mit Wirkung zum 1.7.2021 in Kraft getreten.

10 *Spindler*, in: MünchKomm-AktG, § 91 Rn. 105.

Programme für interne Kontrollen, Ethiksensibilisierungsprogramme und Compliance-Programme durchgeführt“ hat.¹¹ Die gesetzgeberische Regelungslücke, welche konkrete Anforderungen an erforderliche Maßnahmen und Grundsätze eines CMS offenlässt und mithin zwar das „Ob“ aber nicht das „Wie“ regelt, führt zu einer fortwährenden Unsicherheit der jeweiligen Verantwortlichen in den Unternehmen. In der Praxis führte dies bislang dazu, dass Unternehmen externe Expertise bei der Konzeptionierung und Einrichtung sowie der Beurteilung des Reifegrads des eingerichteten CMS einholen mussten. Hierzu eignen sich im besonderen Maße Compliance-Standards, die unmittelbar zwar ohne rechtliche Bindungswirkung sind, aber von der Rechtsprechung als „Expertenwissen“ angesehen werden und deren Beachtung regelmäßig ein Indiz begründet, dass die Sorgfaltspflichten des jeweiligen Verkehrskreises eingehalten worden sind.¹²

2. Zielsetzung des IDW PS 980

Diese Ausgangslage veranlasste u. a. das IDW, einen Arbeitskreis zu gründen, um einen Standard zur Prüfung von CMS zu entwickeln. Der Standard wendet sich ausdrücklich an Wirtschaftsprüfer und regelt die beruflichen Grundsätze, wie eine solche externe Beurteilung eines CMS durch Wirtschaftsprüfer ordnungsgemäß durchzuführen ist. Betriebswirtschaftliche Prüfungen zeichnen sich dadurch aus, dass im Rahmen der Prüfung die vorhandene Wirklichkeit daran abgeglichen wird, ob sie den Anforderungen eines „Sollobjekts“ gerecht wird. Ist das „Soll“ nicht definiert, kann über das „Ist“ kein zusammenfassendes Prüfungsurteil abgegeben werden. Für den IDW-Arbeitskreis stellte diese Bestimmung des ‚Sollobjekts‘ einer solchen Prüfung eine der größten Herausforderungen dar. Ein Bezug auf ein verlässliches Regelungs- oder Rahmenwerk, das allgemeingültig die Anforderungen an ein CMS beschrieb, war nicht möglich, da ein solches nicht vorhanden war. **4**

3. Zielsetzung des ISO 37301:2021

Der ISO 37301:2021 ist – wie der IDW PS 980 – auf die Prüfung bzw. Zertifizierung von CMS gerichtet und legt dafür „Anforderungen fest und bietet Leitlinien für den Aufbau, die Entwicklung, die Umsetzung, die Bewertung, die Aufrechterhaltung und die Verbesserung eines wirksamen Compliance-Management-Systems innerhalb einer Organisation“.¹³ Die Zielgruppe umfasst somit neben den Prüfern bzw. Zertifizierern eines CMS, insbesondere auch die für die Sicherstellung der Compliance verantwortlichen Personen von Organisationen, bei Unternehmen regelmäßig die Geschäftsleitung sowie im Rahmen von Delegationen **5**

11 Abrufbar unter: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52023P.C0234> (zuletzt abgerufen am 14.8.2024).

12 Rack, CB 2021, 433, 435 f.; siehe ferner → Schulz, Kap. 1 Rn. 51.

13 ISO 37301:2021, Compliance-Managementsysteme – Anforderungen mit Leitlinien zur Anwendung, 1. Anwendungsbereich, S. 10, www.iso.org/obp/ui/#iso:std:iso:19600:ed-1:v1:en (zuletzt abgerufen am 14.8.2024).

z.B. Compliance Officer. Dazu geht der Standard detailliert auf eine Vielzahl von Aspekten ein, die bei der Ausgestaltung eines CMS zu beachten sind, und definiert vorab grundlegende Begrifflichkeiten.

4. Vergleich

- 6 Beide Standards betrachten folglich das CMS, allerdings aus unterschiedlichen Blickwinkeln und letztlich zu unterschiedlichen Zeitpunkten. Während sich ISO 37301 primär mit der Ausgestaltung und Einrichtung sowie der laufenden Durchführung von CMS aus der Sicht des CMS-Verantwortlichen beschäftigt, hat der IDW PS 980 wesentlich stärker die Art und Weise sowie Maßstäbe der Prüfung von Angemessenheit und Wirksamkeit des CMS zum Gegenstand. Anforderungen an das CMS ergeben sich aus dem IDW PS 980 damit als Reflex aus den Prüfungsmaßstäben.

III. Unterschiedliche Regelungstiefe zur Ausgestaltung des CMS

1. CMS-bezogene Regelungsinhalte des IDW PS 980

- 7 Wie oben ausgeführt, erforderte das Fehlen eines allgemeingültigen Regelungs- oder Rahmenwerks für ein CMS, dass sich das IDW in seinem Prüfungsstandard auch grundlegend zu den Anforderungen an ein CMS äußerte. Gleichwohl war und ist es nicht die Aufgabe eines Prüfungsstandards, die Grundsätze eines CMS selbst zu bestimmen – nicht zuletzt, weil es zumindest fraglich ist, wie konkret sich solche Grundsätze allgemeingültig – für Unternehmen aller Branchen und Größenordnungen sowie alle relevanten Regelungsgebiete – sinnvoll definieren lassen. Der IDW PS 980 beschränkt sich daher darauf festzulegen, wie der CMS-Prüfer beurteilen kann, ob das betrachtete CMS vom Unternehmen nach Grundsätzen ausgestaltet wurde, die in Bezug auf die relevanten einzuhaltenden Regeln für das konkrete Unternehmen ein angemessenes „Soll“ darstellen. Diese Beschränkung erforderte zunächst die grundlegende Definition von Compliance als Einhaltung von Regeln und eines CMS als Gesamtheit der Regelungen und Maßnahmen im Unternehmen zur Vermeidung bzw. zeitnahen Aufdeckung von Compliance-Verstößen. Dabei wurde das CMS für die Prüfung in verschiedene Betrachtungsebenen, die sieben sog. Grundelemente, eingeteilt: Compliance-Kultur, Compliance-Ziele, Compliance-Risiken, Compliance-Programm, Compliance-Organisation, Compliance-Kommunikation und Compliance-Überwachung.
- 8 Diese Grundelemente, die sich erkennbar an den Rahmenwerken des Committee of Sponsoring Organizations of the Treadway Commission (COSO) zu Internen Kontroll- und Risikomanagementsystemen¹⁴ anlehnten, wurden vom IDW nur generisch beschrieben. Sie stellen quasi die Aspekte dar, unter denen das zu prüfende CMS betrachtet wird. Hierdurch wird sichergestellt, dass eine umfassende

¹⁴ Vgl. *Withus*, Betriebswirtschaftliche Grundsätze für Compliance-Management-Systeme, S. 76. Zu den Kernelementen wirksamer Compliance-Management-Systeme siehe auch → *Schulz*, Kap. 1 Rn. 52 ff.

Beurteilung stattfindet, die gleichzeitig nicht starr anhand von Checklisten erfolgt, sondern die spezifischen Anforderungen des jeweiligen CMS beachtet. Der IDW-Arbeitskreis war bei der Erstellung des Standards der Ansicht, dass Anforderungen an CMS die Unterschiede bei den relevanten Regelungen und in unterschiedlich strukturierten Unternehmen berücksichtigen müssen.

Die im Standard enthaltenen Hinweise auf die Ausgestaltung einzelner CMS-Grundelemente – und das Fehlen von CMS-spezifischen Rahmenkonzepten – führten dazu, dass der IDW PS 980 in der Praxis zunehmend als Grundlage für die Einrichtung eines CMS herangezogen wird. Gleichwohl bleibt die inhaltliche Beschreibung der Grundelemente relativ allgemein. Hierdurch ist sichergestellt, dass die Prüfungsgrundsätze weitgehend unabhängig vom im Einzelfall dem CMS zugrunde gelegten Rahmenkonzept oder den relevanten Regeln anwendbar sind. **9**

Der aus dem Jahr 2011 stammende IDW PS 980 wurde durch den Hauptfachausschuss des IDW umfassend überarbeitet und im September 2022 als IDW PS 980 n. F. (09.2022) veröffentlicht.¹⁵ Anlass der Überarbeitung stellten die inzwischen zahlreichen Fortentwicklungen bei der Einrichtung und der Prüfung von CMS dar. Der IDW PS 980 n. F. berücksichtigt insbesondere die neuere Rechtsprechung und die Entwicklungen durch neue CMS-Rahmenkonzepte wie z. B. die ISO 37301:2021. Inhaltlich änderte sich in der Überarbeitung vor allem die vorgesehene Art der Compliance-Prüfung. Der IDW PS 980 n. F. beschränkt sich auf die Beschreibung des unternehmenseigenen CMS. Vom Unternehmen wird eine eigene kritische Hinterfragung des internen CMS erwartet. Der Prüfer verifiziert nur noch dessen Dokumentation. Zudem findet keine Komplettprüfung, sondern lediglich eine Prüfung in Teilbereichen statt.¹⁶ Schließlich sind ebenfalls die Elemente eines CMS nach IDW PS 980 überarbeitet worden, wobei hiervon nicht die Zahl und der wesentliche Inhalt berührt worden ist.¹⁷ Im Ergebnis konzentriert sich der IDW PS 980 n. F. nun noch stärker auf das CMS-Konzept als solches. **10**

2. Regelungsinhalte des ISO 37301

Auch das CMS-Rahmenkonzept des ISO erfuhr durch die Neuauflage des ISO 19600:2014 in Form des ISO 37301:2021 eine Überarbeitung. Der lediglich empfehlende Charakter des ehemaligen ISO 19600:2014 und die damit verbundene fehlende unmittelbare Zertifizierbarkeit wurden in der Vergangenheit zum Teil kritisiert und bildete einen Anlass für die ISO, einen neuen Standard mit verbindlichen Vorgaben zu entwickeln. Dieser Standard liegt nunmehr unter der Bezeichnung DIN ISO 37301:2021 vor¹⁸ und ersetzte im April 2021 den ISO **11**

15 Vgl. <https://www.idw.de/idw/idw-aktuell/idw-ps-980-n-f-09-2022-zur-pruefung-von-compliance-management-systemen-verab-schiedet.html> (zuletzt abgerufen am 14.8.2024).

16 *Schefold*, ZRFC 2022, 170, 171.

17 Vgl. hierzu *Schefold*, ZRFC 2022, 170, 172 ff.

18 ISO/DIS 37301 Compliance Management Systems – Requirements with guidance for use, <https://www.iso.org/obp/ui/#iso:std:iso:37301:dis:ed-1:v1:en> (zuletzt abgerufen am 14.8.2024).

19600:2014.¹⁹ Wesentlicher Unterschied zu ISO 19600:2014 ist, dass die bisher als Empfehlungen formulierten Aspekte („should“) nunmehr als verbindliche Anforderungen an das CMS umformuliert wurden („shall“).²⁰ Der ISO 37301:2021 ist damit ein zertifizierbarer Level-A-Standard. In seiner Struktur und inhaltlich folgt der ISO 37301:2021 jedoch, von kleineren Anpassungen, Ergänzungen und Verschiebungen abgesehen, im Wesentlichen weiterhin dem ISO 19600:2014.²¹

- 12 Selbstverständlich muss jedes Unternehmen auch bei einer Ausgestaltung seines CMS nach den Anforderungen und Leitlinien des ISO 37301 die konkreten Bedingungen und Anforderungen des eigenen Unternehmens beachten. Zwar hat das Unternehmen jeweils bei der Beurteilung der Eignung und Angemessenheit einen Ermessensspielraum, ggf. müssen aber Ermessenseinschränkungen aus relevanten Regeln heraus beachtet werden.²² Unterbleibt insoweit die Beachtung der nunmehr verbindlichen Anforderungen des ISO 37301, obwohl deren Beachtung für das konkrete Unternehmen erforderlich wäre, so ist das jeweilige CMS nicht angemessen. Zugleich kann eine fehlende Angemessenheit aber auch aus einer Nichtbeachtung der Leitlinien und der Nichtberücksichtigung der Praxis hinweise des Anhangs folgen, gleichwohl jene nicht als verbindliche Anforderungen formuliert sind.
- 13 Die nunmehr enthaltenen Anforderungen des ISO 37301 sind kurz und bündig formuliert, sind aber weiterhin von einer hohen Abstraktheit gekennzeichnet. Die Fokussierung des ISO auf die Festlegung von Definitionen, Identifizierung von Systemkomponenten und beschreibender Darstellung von grundlegenden Konzepten bleibt weiterhin bestehen. Vielmehr ist die Abstraktheit allgemeingültigen Rahmenkonzepten immanent und schmälert nicht deren Nutzung und Anerkennung. Rahmenkonzepte sollen möglichst allgemeingültig sein, „umso generischer die Darstellungen sind, umso größer ist der Kreis möglicher Anwender“.²³ So ist z. B. auch das COSO-Rahmenkonzept zu Risikomanagementsystemen²⁴ lediglich beschreibend und stellt keine konkreten Anforderungen auf. Ein höherer Verbindlichkeitsgrad eines Rahmenkonzepts würde tatsächlich keinen Mehrwert darstellen, auch wenn dies aufgrund eines geringeren Entscheidungs-

19 Siehe <https://www.iso.org/standard/75080.html> (zuletzt abgerufen am 14.8.2024); Veröffentlichung der deutschen Übersetzung durch das Deutsche Institut für Normung in Form des Arbeitsausschusses NA 175-00-01 AA „Governance und Compliance-Management“ im November 2021; siehe <https://www.beuth.de/de/norm/din-iso-37301/344577424> (zuletzt abgerufen am 14.8.2024).

20 ISO 19600:2014 Compliance Management Systems – Guidelines, www.iso.org/obp/ui/#iso:std:iso:19600:ed-1:v1:en, I. Scope (zuletzt abgerufen am 14.8.2024).

21 So auch *Borowa*, in: Bay/Hastenrath, Compliance-Management-Systeme, § 4 Rn. 38.

22 Vgl. z. B. die Darstellung zu den detaillierten Anforderungen an ein CMS, die bei Anwendung der US Sentencing Guidelines zu beachten sind in *Withus*, Betriebswirtschaftliche Grundsätze für Compliance-Management-Systeme, S. 67 ff.

23 *Withus*, Betriebswirtschaftliche Grundsätze für Compliance-Management-Systeme, S. 71.

24 Vgl. COSO Enterprise Risk Management – Integrated Framework, 2004, 11.

bedarfs zunächst so erscheinen mag. Ein zu hoher Konkretisierungsgrad eines CMS-Rahmenkonzepts kann im Gegensatz sogar kontraproduktiv sein. Die fehlende Beachtung der Anforderungen des konkreten Unternehmens kann das CMS ineffizient oder gar ineffektiv werden lassen. Zudem lassen abweichende gesetzliche Anforderungen in unterschiedlichen Jurisdiktionen keinen einheitlich hohen Verbindlichkeits- bzw. Konkretisierungsgrad hinsichtlich der erforderlichen Maßnahmen im Rahmen eines CMS zu. Auch wenn „Empfehlungen, die mit Vorschriften des nationalen Rechts kollidieren würden, nicht umzusetzen sind“,²⁵ stellt sich dann immer die Frage, ob das CMS auch ohne diese konkret vorgeschriebene Maßnahme überhaupt noch wirksam sein kann, bzw. welche Alternative dann eventuell umzusetzen wäre.

Auch in Bezug auf die ISO-Norm stellt die geringe Konkretisierung der Anforderungen somit keinen Mangel dar. Sie ist vielmehr Voraussetzung für die notwendige Flexibilität des Rahmenkonzepts. Hierdurch kann es als Ausgangsbasis für eine große Anzahl von CMS dienen, unabhängig von den konkret relevanten Regeln sowie Größe, Struktur und Rahmenbedingungen der jeweiligen Unternehmen. Die Umsetzung von ISO 37301:2021 in der Praxis erfordert eine hohe fachliche Qualifikation des Anwenders.

Tabelle 1: Wesentliche Unterschiede zwischen ISO 37301 und IDW PS 980 n. F.

	ISO 37301	IDW PS 980 n. F.
Primäre Zielgruppe	CMS-Verantwortliche	Wirtschaftsprüfer
Zielsetzung	Anforderungen, Leitlinien und empfohlene Praktiken zur Ausgestaltung, Einrichtung, Durchführung eines CMS	Grundsätze für ordnungsgemäße Prüfung eines CMS
Betrachtungsgegenstand	Einzelne Maßnahmen und Grundsätze des CMS	Beschreibung des eingerichteten CMS, angemessene und wirksame Umsetzung eines Rahmenwerkes unter Beachtung von relevanten Regeln
Regelungstiefe in Bezug auf CMS	Rahmenwerk, verbindliche Anforderungen, häufig Wahlrechte, Ermessensentscheidung der Verantwortlichen auf Basis der relevanten Gesetze/Regeln notwendig	Standard zur ordnungsgemäßen Prüfungsdurchführung, verbindliche Darstellung der zu betrachtenden Grundelemente eines CMS, Keine verbindlichen Aussagen zur Ausgestaltung des CMS, sondern Verweis auf Rahmenwerke

²⁵ Makowicz/Wüstemann, BB 2015, 1195, 1198.

IV. ISO 37301 als geeignetes, angemessenes Rahmenkonzept für ein CMS

1. Anforderungen des IDW PS 980 an ein Rahmenkonzept

- 16 Im Verhältnis zum IDW-Standard ergibt sich nunmehr ausdrücklich aus Anlage 1 zum IDW PS 980 n. F., dass der ISO 37301 ein geeignetes Rahmenkonzept für ein CMS darstellt, d. h. ein hiernach ausgestaltetes CMS einer Prüfung nach IDW PS 980 zugänglich ist. Die Hintergründe dieser Einordnung sollen nachfolgend herausgearbeitet werden.
- 17 Wie oben dargestellt, beschränkt sich der Prüfungsstandard IDW PS 980 auf grundsätzliche Aussagen zur Ausgestaltung eines CMS in Form der Darstellung der sieben Grundelemente eines CMS. Diese stellen quasi die Betrachtungsaspekte dar, unter denen der Prüfer die Ermessenentscheidungen der CMS-Verantwortlichen zu beurteilen und z. B. gegen relevante Gesetze und Regeln abzugleichen hat. Der Standard fordert aber, dass die Einrichtung des CMS auf Grundsätzen beruhen muss. D. h., Ermessensentscheidungen bei der Einrichtung des CMS dürfen nicht willkürlich erfolgen, sondern müssen in einem konzeptionellen Zusammenhang stehen. Ergänzend wird vom IDW PS 980 definiert, dass hierzu „die in Anlage 1 genannten allgemein anerkannten Rahmenkonzepte, andere angemessene Rahmenkonzepte oder individuell entwickelte angemessene CMS-Grundsätze in Betracht“²⁶ kommen. Dabei müssen die Grundsätze alle sieben Grundelemente eines CMS abdecken und in konkrete Richtlinien und Maßnahmen transformieren.
- 18 IDW PS 980 versteht unter allgemein anerkannten Rahmenkonzepten solche, „die von einer autorisierten oder anerkannten standardsetzenden Organisation im Rahmen eines transparenten Verfahrens entwickelt und verabschiedet oder durch gesetzliche oder andere rechtliche Anforderungen festgelegt werden“.²⁷ Der Prozess zur Verabschiedung von ISO-Normen verfügt faktisch über eine sehr eingeschränkte Transparenz. Die Entwürfe werden nur den Mitgliedern zugänglich gemacht. Zwar steht die Mitgliedschaft theoretisch jedermann offen, praktisch ist der Teilnehmerkreis aber sehr eingeschränkt. Eine Diskussion und Möglichkeit zur Stellungnahme durch alle interessierten, fachlich einschlägigen Kreise findet nicht statt. Es kann auch hinterfragt werden, ob ISO in Bezug auf die Festlegung von Anforderungen an Managementsysteme tatsächlich eine ähnliche allgemeine Anerkennung hat, wie dies in Bezug auf technische Normen wohl zweifelsfrei der Fall ist.

26 Vgl. IDW Prüfungsstandard: Grundsätze Ordnungsmäßiger Prüfung von Compliance Managementsystemen (IDW PS 980), WPg Supplement 2/2011, Tz. 8, 9.

27 IDW Prüfungsstandard: Grundsätze Ordnungsmäßiger Prüfung von Compliance Managementsystemen (IDW PS 980), WPg Supplement 2/2011, Tz. 9.

Im Gegensatz zu allgemein anerkannten Rahmenkonzepten werden „andere angemessene Rahmenkonzepte“ im IDW PS 980 nicht näher definiert. Allerdings werden nicht beliebige Rahmenkonzepte zugelassen, sondern nur „angemessene“. Während bei allgemein anerkannten Rahmenkonzepten die Eignung zur Ausgestaltung eines CMS unterstellt wird, müssen andere Rahmenkonzepte ausdrücklich angemessen sein. Im Ergebnis hat die Klassifizierung eines Rahmenkonzepts als „allgemein anerkannt“ oder „anderes angemessenes“ indes keine grundsätzliche Auswirkung auf die Eignung zur Ausgestaltung eines CMS. Die Unterscheidung führt aber dazu, dass bei nicht „allgemein anerkannten“ Rahmenkonzepten der Prüfer zunächst die Angemessenheit des anderen Rahmenkonzepts beurteilen muss. Hierzu wird im Wesentlichen ein Vergleich mit allgemein anerkannten Rahmenkonzepten erfolgen – einschließlich der Beurteilung, ob alle vom IDW PS 980 genannten Grundelemente eines CMS abgedeckt sind.²⁸ Diese Beurteilung soll nachfolgend für die Inhalte des ISO 37301 nachvollzogen werden. 19

2. Vergleich ISO 37301 Anforderungen mit IDW PS 980-Grundelementen

Um die Gründe für die Angemessenheit des ISO 37301 in Bezug auf eine Prüfung nach den Grundsätzen des IDW PS 980 nachvollziehen zu können, muss abgeglichen werden, inwieweit diese ISO-Anforderungen umfassend alle Grundelemente eines CMS abdecken. Hierzu können die wesentlichen Anforderungen des ISO 37301 synoptisch den Grundelementen zugeordnet werden. 20

²⁸ IDW Prüfungsstandard: Grundsätze Ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980), WPg Supplement 2/2011, A30.

Teil 1 Grundlagen, Erfolgsfaktoren und Handlungsstrategien

21 **Tabelle 2:** Exemplarische Zuordnung der ISO 37301 Anforderungen zu IDW PS 980-Grundelementen

ISO 37301 Anforderungen		IDW PS 980 Grundelemente
4.5.2	Maintenance of compliance obligations	Compliance-Überwachung und Verbesserung
9	Performance evaluation	
10	Improvement	
4.4	Compliance management system and principle of good	Compliance-Kultur
5.1	Leadership and commitment	
7.3.2.1	Behaviour – General	
7.3.2.2	Top management's role in encouraging compliance	Compliance-Ziele
4.2	Understanding the needs and expectations of interested parties	
4.3	Determining the scope of the compliance management system	
4.5.1	Identification of compliance objectives	
6.2	Compliance objectives and planning to achieve them	
5.3.2	Assigning responsibilities in the organization Compliance-Organisation	Compliance-Organisation
5.3.3	Governing body and top management role and responsibilities	
5.3.4	Compliance function	
5.3.5	Management responsibilities	
5.3.6	Employee responsibilities	
7.1	Resources	
7.2.1	Competence	
7.5	Documented information	
4.1	Understanding the organization and its context	
4.6	Identification, analysis and evaluation of compliance risks	Compliance-Risiken
5.2	Compliance policy	Compliance-Programm
6.1	Actions to address compliance risks	
8	Operation	
5.3.5	Management responsibilities	Compliance-Kommunikation
5.3.6	Employee responsibilities	
7.2.2	Training	
7.3.1	Awareness – General	
7.3.2.3	Compliance culture	
7.4	Communication	

Die Gegenüberstellung zeigt, dass die Anforderungen des ISO 37301 auf alle sieben Grundelemente eines CMS eingehen. Da die Grundelemente selbst nicht scharf getrennt nebeneinander stehen, sondern lediglich eine strukturierte Betrachtung eines CMS ermöglichen sollen, lassen sich einzelne Inhalte der ISO 37301 Anforderungen durchaus auch mehreren Grundelementen zuordnen. Umgekehrt können die Inhalte der generischen Beschreibung der Grundelemente in IDW PS 980 in den Guidelines wiedergefunden werden. **22**

Die vom ISO-Standard 37301 festgelegten Definitionen der Begrifflichkeiten im Standard stehen ebenfalls im Einklang mit den Abgrenzungen und Definitionen des IDW PS 980. Insgesamt kann somit nachvollzogen werden, weshalb der ISO 37301 ein angemessenes Rahmenkonzept zur Ausgestaltung eines CMS darstellt und ein hiernach ausgestaltetes CMS einer Prüfung nach IDW PS 980 zugänglich ist, wie Anlage 1 zum IDW PS980 nunmehr ausdrücklich bestätigt. Dies muss entsprechend auch für den ehemaligen ISO 19600 angenommen werden, da dieser strukturell und inhaltlich weitgehend dem ISO 37301 entspricht. **23**

V. Zwischenergebnis

Die Inhalte des ISO 37301 stellen eine umfangreiche Sammlung von grundsätzlich allgemein gehaltenen Anforderungen und Leitlinien sowie Best Practices zur Ausgestaltung von CMS dar. Die vom Standard vorgenommene Gliederung der Inhalte anhand eines prozessualen Ablaufs erschwert zwar einen Abgleich mit anderen Standards, wie z. B. den COSO-Rahmenwerken oder auch dem über die Grenzen Deutschlands als Prüfungsstandard anerkannten IDW PS 980. Gleichwohl ist auch eine solche Gliederung der Betrachtung sachgerecht, es gibt hier keine zwingend logische Betrachtungsweise. Ein Vergleich mit den Grundelementen des IDW PS 980 ergibt, dass die Anforderungen und Leitlinien des ISO 37301 alle relevanten Aspekte eines CMS abdecken. Die enthaltenen Anforderungen sind einerseits hinreichend genau, andererseits erlauben sie eine sachgerechte, angemessene Ausgestaltung unter Beachtung der relevanten Regeln und Rahmenbedingungen des Unternehmens. **24**

ISO 37301:2021 ist im Sinne von IDW PS 980 ein angemessenes Rahmenwerk für die Grundsätze und Maßnahmen eines angemessenen CMS. **25**

VI. Die Legalitätskontrolle als Bindeglied zwischen Risiko- und Compliance-Management?

Das klassische Risikomanagement, als die Messung und Steuerung betriebswirtschaftlicher Risiken²⁹ und die Compliance in Form eines CMS sind neben dem Internen Kontrollsystem (IKS) in der Theorie verschiedene Corporate-Governance-Systeme, die in der Praxis sich jedoch häufig faktisch überlappen. Es ist eine Tendenz der zunehmenden Verschränkung beider Systeme zu beobachten, **26**

²⁹ Nietsch, ZHR 180 (2016), 733, 757.

wenngleich vor einer vorschnellen 1:1-Übertragung gewarnt werden muss.³⁰ Während IDW PS 980 und ISO 37301 das CMS betrachten, konzentrieren sich ISO 31000:2018 und IDW PS 981 auf das Risikomanagement. In der Praxis stellt sich angesichts dessen häufig die Frage, ob nicht mittels eines einheitlichen Ansatzes, der sog. „One Governance“, die Anforderungen beider Governance-Systeme zugleich umgesetzt werden können.

- 27 Der Umgang mit Rechtsrisiken bzw. Compliance-Risiken im Rahmen der Legalitätskontrolle trägt dabei eine herausgehobene Stellung. Von Ausnahmen abgesehen³¹ fehlt eine gesetzgeberische Ausformulierung der konkreten Anforderungen und praktisch sind Unternehmen häufig auf Standards angewiesen. ISO 31022:2020 „Risk management – Guidelines for the management of legal risk“ formuliert Leitlinien zum Umgang mit spezifisch rechtlichen Risiken. Er konkretisiert damit den ISO 31000:2018 „Risk management – Guidelines“, welcher Leitlinien für den Umgang mit jeglicher Art von Risiken definiert.
- 28 Rechtsrisiken beschreiben weit verstanden „alle Kosten und Einbußen oder Gewinnminderungen, die aufgrund einer für das Unternehmen nachteiligen Gesetzeslage, Rechtsprechung oder einer erschwerten bzw. vereitelten Rechtsdurchsetzung entstehen“.³²
- 29 Compliance-Risiken hingegen beschreiben in ihrer Grundform Risiken, die aus der Verletzung von Gesetzen entstehen können. Die DIN ISO 37301 definiert das Compliance-Risiko³³ als Wahrscheinlichkeit des Auftretens und die Folgen von Non-Compliance,³⁴ wobei die Non-Compliance die Nichterfüllung aller Anforderungen, die eine Organisation zwingend zu erfüllen hat oder der sie sich freiwillig unterwirft, darstellt.³⁵
- 30 Die umfassende, Governance-System-übergreifende Betrachtung von Rechtsrisiken ist insbesondere für die Praxis bedeutsam, da der Umgang mit rechtlichen Risiken methodisch weitgehend ein Schattendasein fristet.³⁶ So ist schon die eigentliche Abgrenzung zwischen Rechts- und Compliance-Risiken unklar.³⁷ Dennoch und gerade im Bereich der Legalitätskontrolle scheint sich eine Verknüpfung beider Systeme aufzudrängen. Einerseits handelt es sich bei vielen Risiken zugleich um Risiken finanzieller, operativer und rechtlicher Natur und andererseits erlaubt die Nutzung eines übereinstimmenden Methodenansatzes eine

30 *Nietsch*, ZHR 180 (2016), 733, 757.

31 Zu besonderen Vorgaben im Bereich der Finanzdienstleistungen → *Renz/Frankenberger*, Kap. 20; zu den Compliance-Vorgaben durch das Lieferkettensorgfaltspflichtengesetz (LkSG) siehe → *Heske*, Kap. 18 sowie → *Schulz*, Kap. 1 Rn. 4.

32 *Nietsch*, ZHR 180 (2016), 733, 759.

33 Vgl. DIN ISO 37301, Ziff. 3.24.

34 Vgl. DIN ISO 37301, Ziff. 3.27/3.25.

35 Zum Compliance-Risikomanagement siehe auch → *Schulz*, Kap. 1 Rn. 60 ff. sowie → *Romeike*, Kap. 9.

36 *Nietsch*, ZHR 180 (2016), 733, 758.

37 *Nietsch*, ZHR 180 (2016), 733, 759.

schnellere und effizientere Prozessgestaltung. Ein Ansatz der vor dem Hintergrund der ISO 31022 im Folgenden näher untersucht werden soll.

1. Zielsetzung des ISO 31022

ISO 31022 zielt auf den sachgerechten Umgang mit Rechtsrisiken durch die Bereitstellung von entsprechenden Leitlinien und Prozessen ab. ISO 31022 bietet Verantwortlichen in den Unternehmen eine Hilfestellung für die Ausrichtung eines Risikomanagementsystems auf die spezifische Risikokategorie der Rechtsrisiken. Der Standard stellt wie die ISO 31000 allgemeine Leitlinien zur freiwilligen Anwendung bereit und kann (bzw. muss) je nach Unternehmenskontext entsprechend angepasst werden.³⁸ Er ist nicht zertifizierbar. **31**

2. Regelungsinhalte des ISO 31022

Inhaltlich konkretisiert ISO 31022 die Anforderungen des ISO 31000 im Kontext rechtlicher Risiken. Die Grundprinzipien des Hauptdokuments werden aufgegriffen, im Kontext des Managements rechtlicher Risiken neu definiert und darüber hinaus ein neues Grundprinzip „Equity“ eingeführt. Auf Grundlage dessen stellt der ISO 31022 einen „Legal risk management process“³⁹ vor und erörtert die Bedingungen für eine sinnvolle Implementation des Prozesses in das Rahmenwerk des allgemeinen Risk Managements. **32**

Der dargelegte „Legal risk management process“ enthält im Wesentlichen zwei Einzelschritte. Zunächst sind rechtliche Risiken in einem „Assessment“ zu beurteilen (Risikobeurteilung), um diese anschließend bewältigen zu können (Risikobewältigung).⁴⁰ **33**

Die Beurteilung rechtlicher Risiken setzt einen Dreiklang aus Identifikation, Analyse und Bewertung voraus, wobei im Rahmen der Analyse die Wahrscheinlichkeit und die möglichen Konsequenzen etwaiger Rechtsverstöße zu beachten sind. **34**

Im Hinblick auf das „Treatment of legal risk“ sind auf Grundlage der zuvor erfolgten Bewertung, unter Einbeziehung der allgemeinen Grundsätze, entsprechende Strategien zur Bewältigung dieser Rechtsrisiken zu entwickeln. Eingeraht wird dieser Prozess des Umgangs mit Rechtsrisiken durch allgemeine Maßnahmen, wie Kommunikation und Konsultation, Überwachung und Überprüfung und eine abschließende Berichterstattung bzw. Dokumentation. **35**

Die sinnvolle Implementation dieses Prozesses in das jeweilige Risk Management des Unternehmens setzt das Entwickeln einer Richtlinie zum Umgang mit Rechtsrisiken (einschließlich dem Bestimmen von Verantwortlichkeiten), das **36**

³⁸ Herdmann/Henschel, ZRFC 2018, 111, 115.

³⁹ Vgl. ISO 31022, Ziff. 4.

⁴⁰ Vgl. ISO 31022, Ziff. 5.3, 5.4.

Entwickeln von Verfahren zur Integration des Prozesses in bereits bestehende Prozesse und die Bereitstellung entsprechender Ressourcen voraus.

3. Vergleich zum Compliance-Risiko/Vergleich zur ISO 37301

- 37 Der in der ISO 31022 enthaltene Prozess zum Umgang mit Rechtsrisiken ist durch die Prozessschritte der Risikoidentifikation und der anschließenden Bewertung samt Folgenanalyse geprägt. Der methodische Ablauf der Risikomesung kann zunächst durchaus auch an den Umgang mit Compliance-Risiken im Rahmen eines CMS erinnern und scheint einen Gleichlauf anzudeuten.⁴¹
- 38 Wesentliche Unterschiede zeigen sich jedoch bereits in der Art des Analyseprozesses und seiner Zielsetzung.⁴² Während die ISO 37301 im Rahmen des CMS vor allem auf das Identifizieren des relevanten Pflichtenprogramms und einem möglichst umfassenden Auffinden bislang unbekannter Regelverstöße setzt, handelt es sich bei der Analyse von Rechtsrisiken um einen breiteren Ansatz, der insbesondere zugleich auf die Betrachtung von Finanzrisiken setzt.
- 39 Darüber hinaus unterscheiden sich die Möglichkeiten und Maßnahmen der folgenden Risikobewältigungstechniken wesentlich. Im Hinblick auf die Compliance-Risiken schränkt die Legalitätspflicht grds. die Möglichkeit der Reaktion auf ein Compliance-Risiko ein. Eine Ermessensentscheidung im Hinblick auf die Befolgung etwa von mit Strafen oder Geldbußen bewehrten Rechtsnormen und damit den Umgang mit Compliance-Risiken gewährt diese gerade nicht. Hingegen erlaubt die Bewertung von breiter verstandenen bloßen Rechtsrisiken einen deutlich weiteren Handlungsspielraum und Reaktionsmaßnahmen können abhängig von der jeweiligen Qualität des Risikos sein. Dieser Grundunterschied muss sich zugleich auf die Risikoanalyse und Risikobewertung im Hinblick auf eine andere Zielsetzung niederschlagen.

4. Zwischenergebnis

- 40 Compliance-Risiken sind ein Teilbereich des Rechtsrisikos.⁴³
- 41 ISO 31022 bietet eine sinnvolle Ergänzung zur Ausgestaltung des unternehmensinternen Risikomanagementsystem um die spezifische Betrachtung von Rechtsrisiken. Dennoch ersetzen Prozesse zum Umgang mit Rechtsrisiken nach ISO 31022 nicht die Entwicklung spezifischer Maßnahmen zum Umgang mit Compliance-Risiken auf Grundlage der ISO 37301 vor dem Hintergrund eines CMS. Die wesentlich unterschiedliche Zielsetzung der Analyse und der Risikobewältigungsmaßnahmen erfordert einen compliance-spezifischen Ansatz.
- 42 Die ISO 31022 kann im Hinblick auf die Ausgestaltung von Prozessen dennoch eine Orientierungsfunktion bieten und zeigt eine Möglichkeit der Ausgestaltung

⁴¹ *Nietsch*, ZHR 180 (2016), 733, 764.

⁴² *Nietsch*, ZHR 180 (2016), 733, 765.

⁴³ *Nietsch*, ZHR 180 (2016), 733, 766.

von Risikoanalysen auch im Bereich der Anforderungen an ein CMS im Rahmen der ISO 37301 auf.

VII. Argumente für eine Ausrichtung des CMS nach ISO 37301

1. Basis für Ermessensentscheidung und Compliance-Richtlinie

„Normen“ haben schnell die Vermutung für sich, dass ihre Anwendung zwingend geboten ist oder zumindest eine Art „Best Practice“ darstellt. Dies mag für die technischen Normen von ISO bzw. des Deutschen Instituts für Normung sicherlich häufig der Fall sein, da diese die Vermutung in sich tragen, dass sie den Stand der allgemein anerkannten Regeln der Technik wiedergeben.⁴⁴ Eine solche Vermutung hat die Rechtsprechung für die Management-Normen von DIN und ISO bislang nicht ausgesprochen. Es ist auch sehr zu bezweifeln, ob diesen Normen eine ähnliche Bedeutung wie den technischen Normen zukommen kann. Hierfür mangelt es schon an einer einheitlichen Definition des Begriffs „Management“. Gegen eine solche Vermutung spricht auch die – gerade im Vergleich zu technischen Normen – geringe Konkretisierung des Standards. ISO 37301 erzeugt zwar in der aktualisierten Version grds. eine höhere Verbindlichkeit für Unternehmen, die ihr CMS entsprechend strukturieren oder bei einem bestehenden CMS zusätzliche oder ergänzende Maßnahmen einrichten wollen, aber die enthaltenen Anforderungen sind durchgängig generisch und darauf ausgerichtet einen möglichst großen Anwenderbereich zu erfassen.

ISO 37301 steht, zumindest unter dem Aspekt als Rahmenkonzept, derzeit eigenständig neben anderen – breit anerkannten – Rahmenwerken, wie z. B. dem United States Federal Sentencing Guidelines Manual. Ob sich mittelfristig eine breite Akzeptanz der ISO 37301 entwickelt und das explizit hierauf aufbauende CMS sich als „Best Practice“ positionieren, wird die Zeit beantworten. Die eigenständige Zertifizierbarkeit mag jedoch die Attraktivität durchaus von anderen Standards abheben.

Zugleich bleibt weiterhin die Frage nach der gerichtlichen Art und Weise der Berücksichtigung einer Zertifizierung nach ISO 37301 offen. Eine solche ist grds. nicht vorhersagbar und immer einer Einzelfallentscheidung des jeweiligen Gerichts.⁴⁵

Unternehmen haben daher weiterhin eine Wahl, ob sie ISO 37301 als Grundlage für die Ausgestaltung ihres CMS heranziehen. Es stellt sich deswegen die Frage, ob die Nutzung von ISO 37301:2021 empfehlenswert sein kann.

ISO 37301 wendet sich grundsätzlich an alle Organisationen und versteht hierunter sowohl Unternehmen aller Rechtsformen, wie auch gemeinnützige Organisationen oder öffentliche Körperschaften. Die im Standard festgelegten Anforderungen und dargestellten Leitlinien erreichen ihren breiten Anwendungsbereich

⁴⁴ BGH, Urt. v. 24.5.2013 – V ZR 182/12, openJur 2013, 29766.

⁴⁵ Hastenrath, in: Bay/Hastenrath, Compliance-Management-Systeme, § 9 Rn. 62 f.

durch einen hohen Grad der Abstraktheit. Durch den generischen Ansatz kann die ISO 37301 auch die Grundlage für zu entwickelnde spezielle Rahmenkonzepte darstellen. Solche speziellen Rahmenkonzepte bestehen bereits z. B. für die Immobilienwirtschaft⁴⁶ oder die Vertriebsorganisation in Versicherungsunternehmen.⁴⁷ Durch ihre engere Ausrichtung auf bestimmte, tendenziell eher gleichartige Unternehmen können diese weitaus konkreter werden und für einzelne Wirtschaftsbereiche eine „Best Practice“ widerspiegeln. Durch die Ausgestaltung der bisherigen Richtlinien als verbindliche Anforderungen konnte zudem eine Kohärenz mit der ISO-Norm 37001:2016 zu Anti-Korruptions-Managementsystemen, welche bereits seit 2016 auf die Struktur in Form von verbindlichen Anforderungen setzte, erreicht werden.⁴⁸ Ob ein solcher Ansatz – zum einen allgemein gültig auch für sehr unterschiedlich strukturierte Unternehmen, zum anderen aber sehr spezifisch und detailliert in den Anforderungen – den Herausforderungen zur Gestaltung eines wirksamen CMS gerecht werden kann, bleibt abzuwarten. Es kann durchaus bezweifelt werden, dass es sinnvoll ist, bei der Ausgestaltung eines CMS die Besonderheiten zu ignorieren, die sich aus Größenordnungen, Hierarchiestrukturen, regionalen oder kulturellen Gegebenheiten und einer Vielzahl anderer Faktoren ableiten können.

- 48** Wenn Rahmenkonzepte lediglich generische Anforderungen definieren und dadurch einen „bloßen“ Rahmen für deren Ausgestaltung festlegen, ist in Bezug auf ISO 37301 ebenso die Frage berechtigt, welchen Mehrwert dieses Rahmenkonzept gegenüber anderen allgemeinen Rahmenkonzepten, wie z. B. den COSO-Rahmenwerken hat. Im COSO-Rahmenwerk zu IKS wurden bei der Überarbeitung 2013 zwar zusätzliche Hinweise zur Zielsetzung von Compliance aufgenommen; COSO betrachtet aber grundsätzlich das gesamte Risikomanagement. ISO 37301 ist dagegen konkret auf Sicherstellung der Compliance ausgerichtet, die dargelegten Anforderungen und Leitlinien sind dadurch zielgerichteter und für den adressierten Anwender einfacher verständlich. Dabei liefert ISO 37301 für alle Grundelemente eines CMS eine umfangreichere Darstellung von Systemkomponenten, CMS-spezifischen Definitionen und bei der Ausgestaltung von CMS zu beachtenden Fragestellungen und Beurteilungen. Dies kann in der Praxis bei der Ausgestaltung von CMS die Einrichtung von konkreten, angemessenen Maßnahmen sowie deren praktische Umsetzung erleichtern. Die weltweite Verbreitung des Standards kann Grundlage dafür sein, dass seine Anwen-

46 Vgl. Initiative Corporate Governance der deutschen Immobilienwirtschaft e. V. (Hrsg.), Pflichtenheft zum Compliance-Management in der Immobilienwirtschaft, 2018, http://www.icg-institut.de/wp-content/uploads/2019/01/Pflichtenheft_2018_low.pdf (zuletzt abgerufen am 14.8.2024).

47 Vgl. Verhaltenskodex des Gesamtverbands der Deutschen Versicherungswirtschaft für den Vertrieb von Versicherungsprodukten, GDV 2018; <https://www.gdv.de/resource/blob/10302/551f3e81d903f48d890800037fd22251/verhaltenskodex-fuer-den-vertrieb-vom-25-09-2018-data.pdf> (zuletzt abgerufen am 14.8.2024).

48 Siehe <https://www.iso.org/obp/ui/#iso:std:iso:37001:ed-1:v1:en> (zuletzt abgerufen am 14.8.2024); vgl. auch Neiger, *comply* 2021, 433, 435.

dung als CMS-Rahmenkonzept für international agierende Unternehmen die Einführung eines weltweiten CMS erleichtert. Dies ist z. B. schon durch die Vereinheitlichung von Definitionen der Fall.

Welche konkreten Grundsätze und Maßnahmen dabei aus den Leitlinien des ISO 37301 abgeleitet werden und unter Beachtung der relevanten zu beachtenden Regeln angemessen sind, muss von den CMS-Verantwortlichen in eigener Verantwortung entschieden werden. Auf der Basis des ISO 37301 können Unternehmen – analog zu einer Bilanzierungsrichtlinie – ihre Entscheidungen für die Ausnutzung von ISO-Wahlrechten schriftlich festhalten. Diese „Compliance-Richtlinie“ kann an die Konzerneinheiten ausgereicht und von diesen individuell – unter Beachtung der gesetzlichen Anforderungen in der jeweiligen Jurisdiktion – an die besonderen lokalen Besonderheiten angepasst werden. In internationalen Konzernen würde dadurch nicht nur die Einrichtung von CMS erleichtert. Die Darstellung der wesentlichen Elemente einer solchen Compliance-Richtlinie in einer CMS-Beschreibung würde auch den Unternehmensorganen die Überwachung des konzernweiten CMS erleichtern und Benchmarkvergleiche innerhalb des Konzerns ermöglichen. **49**

2. Beurteilung der angemessenen Einrichtung eines wirksamen CMS

Ob die Umsetzung des CMS – unter Beachtung des ISO 37301 – in Bezug auf die einzuhaltenden Regeln angemessen erfolgte und wirksam durchgeführt wurde, ist zunächst von den Aufsichtsverpflichteten des Unternehmens zu überwachen. Hierbei kann eine Prüfung nach den Grundsätzen des IDW PS 980 unterstützen. Die Angemessenheit ist dabei vorrangig in Bezug auf die jeweils relevanten Regeln (insbes. gesetzlichen Vorschriften) zu beurteilen. Wie oben bereits dargestellt, ist dabei auf Basis dieser relevanten Regeln für jede einzelne Anforderung der Norm die Frage zu beantworten, ob diese ein tatsächliches Wahlrecht darstellt oder faktisch eine Notwendigkeit ist, um ein angemessenes CMS einzurichten. **50**

Zwar entscheidet nicht das Rahmenkonzept über die Angemessenheit des CMS, sondern die unternehmensspezifische Ausgestaltung des CMS unter Beachtung der relevanten Regeln. Aber auch, wenn der externe Prüfer vorrangig diese relevanten Regeln im Blick haben muss, muss er prüfen und kann bei Bedarf bescheinigen, dass die Grundsätze des jeweiligen Rahmenwerks beachtet wurden. Eine CMS-Prüfung nach IDW PS 980 kann somit auch die Ausgestaltung des CMS nach ISO 37301:2021 beurteilen und im Ergebnis bescheinigen. Ebenso kann dies natürlich auch eine Zertifizierung nach ISO 37301:2021 selbst leisten. **51**

Wurde das CMS bereits in Vorjahren nach IDW PS 980 geprüft, ist regelmäßig zu erwarten, dass sich durch die Entscheidung des Unternehmens für sein CMS zukünftig die ISO 37301 als Rahmenkonzept zu nutzen, keine signifikanten Änderungen ergeben werden. Insoweit sind Befürchtungen substanzlos, wonach durch den ISO-Standard neue Anforderungen aufgestellt oder gar die Beurtei- **52**

lung der Wirksamkeit des CMS beeinflusst und damit Haftungsrisiken erhöht würden.

- 53** Jedoch sollten zum einen Unternehmen, deren CMS sich im Aufbau befindet, mit den Vorgaben und Leitlinien des ISO-Standards differenziert auseinanderzusetzen und die Wahlrechte (ggf. gesellschaftsspezifisch) ausüben.
- 54** Zum anderen ist selbst bei Unternehmen, deren CMS einen hohen Reifegrad besitzt, regelmäßig die fortgesetzte Angemessenheit und Wirksamkeit des eingerichteten CMS zu überprüfen. Auch eine bereits durchgeführte externe Prüfung des CMS nach IDW PS 980 entbindet die Verantwortlichen nicht von dieser fortlaufenden Überwachungspflicht, da sich relevante Rahmenbedingungen, wie z. B. gesetzliche Anforderungen, jederzeit ändern können. Sowohl ISO 37301 wie auch der IDW PS 980 weisen auf diese Überwachungspflicht hin.⁴⁹ Eine gesetzliche Verpflichtung, dabei explizit die Ausführungen des ISO 37301 zu beachten, ist nicht zu begründen. ISO 37301:2021 kann aber wertvolle Vorgaben und Leitlinien im Falle von notwendigen Anpassungen geben.

VIII. Zusammenfassung

- 55** 1. ISO 37301 und IDW PS 980 haben unterschiedliche, sich ergänzende Blickwinkel auf die Thematik Compliance-Management-System und richten sich in ihrer Gestaltung an unterschiedliche Zielgruppen. Inhaltlich gibt es indes einen hohen Überschneidungsgrad.
2. ISO 37301 legt im Gegensatz zu seiner Vorversion (ISO 19600) nunmehr Anforderungen an die Ausgestaltung eines CMS fest. Darüber hinaus enthält ISO 37301 Leitlinien und gibt CMS-Verantwortlichen im Anhang praktische Hinweise dazu, welche Aspekte, Prinzipien und Zusammenhänge bei der Ausgestaltung von CMS zu berücksichtigen sind. Die Leitlinien im ISO 37301 können Unternehmen darüber hinaus für die Überwachung, die kontinuierliche Verbesserung oder Anpassung des CMS an geänderte Rahmenbedingungen wertvolle Guidance geben. Die Beurteilung, ob diese Guidance angemessen und wirksam umgesetzt wurde, unterliegt der Beurteilung der Compliance-Verantwortlichen.
3. IDW PS 980 stellt für Wirtschaftsprüfer die Grundsätze auf, die bei der Prüfung der implementierten Grundsätze und Maßnahmen auf Angemessenheit und Wirksamkeit zu beachten sind.
4. Die beiden Standards stehen dabei durch die neue Ausgestaltung des ISO 37301 als zertifizierbarer Typ-A-Standard selbstständig nebeneinander. Beide Standards enthalten Anforderungen – jene des IDW PS 980 konkreter und jene des ISO 37301 generischer – deren Einhaltung durch externe Prüfer zertifizierbar ist. Bei einer Prüfung nach IDW PS 980 kann neben der Angemes-

⁴⁹ *Withus*, Betriebswirtschaftliche Grundsätze für Compliance-Management-Systeme, S. 208 ff. Zur Notwendigkeit regelmäßiger Aktualisierung der Compliance-Maßnahmen siehe auch → *Schulz*, Kap. 1 Rn. 89.

senheit und Wirksamkeit in Bezug auf die Maßnahmen zur Beachtung der relevanten Regeln und gesetzlichen Vorschriften auch die Beachtung der Anforderungen und Leitlinien des ISO 37301:2021 bestätigt werden. Ob dieses komplementäre Verhältnis aufgrund der Selbstständigkeit der ISO 37301 weiterhin Bestand haben kann, bleibt abzuwarten. Jedenfalls stehen Unternehmen nunmehr vor der Wahl, ob sie ihr jeweiliges CMS nach IDW PS 980 oder ISO 37301 prüfen lassen wollen. Letzterer kann gerade für international agierende Unternehmensgruppen einen bedeutsamen Vorteil darstellen, um eine Vergleichbarkeit der CMS-Ausgestaltung in den Konzerngesellschaften in verschiedenen Ländern zu erreichen. Die Information über eine erfolgreich durchgeführte Prüfung des CMS kann gleichzeitig als Nachweis hinsichtlich der Beachtung der Compliance-Anforderungen anderer Geschäftspartner genutzt werden.

8. Kapitel

Management interner Untersuchungen

I. Einleitung

Unter einer internen Untersuchung versteht man die unternehmensinterne Aufklärung von Fehlverhalten durch Mitarbeiter im oder aus dem Unternehmen heraus. Sie ist in Abgrenzung zu externen Ermittlungen von Ermittlungs- oder Aufsichtsbehörden zu sehen. Bei dem aufzuklärenden Fehlverhalten von Mitarbeitern – den hier sogenannten Compliance-Verstößen in Abgrenzung zu Rechtsverstößen durch außenstehende Dritte – kann es sich um Verstöße gegen reines „Binnenrecht“ des Unternehmens, z.B. Reise- oder Spesenrichtlinien, handeln. Oft werden jedoch Korruptions- und Untreuedelikte, Steuerstraftaten, Kartellverstöße oder Verletzungen von Insiderrecht zur Aufklärung stehen.¹

Interne Untersuchungen sind als „Internal Investigations“ aus dem anglo-amerikanischen Rechtsraum bekannt, mittlerweile aber auch hierzulande als wesentlicher Bestandteil jedes effektiven Compliance-Programms etabliert. Sie dienen nicht nur dazu, mögliches Fehlverhalten aufzuklären, abzustellen und arbeits- oder zivilrechtlich zu sanktionieren. Vielmehr tragen sie auch zur Prävention künftigen Fehlverhaltens bei. Denn zum einen dokumentiert das Unternehmen gegenüber seinen Mitarbeitern, dass Hinweisen auf Fehlverhalten nachgegangen und dieses nicht einfach hingenommen wird. Zum anderen helfen interne Untersuchungen, Schwächen bestehender Kontroll- und Compliance-Systeme zu identifizieren und diese anzupassen und zu verbessern.

Mit dem „Gesetz zur Stärkung der Integrität in der Wirtschaft“,² dessen Kernstück das „Gesetz zur Sanktionierung von verbandsbezogenen Straftaten“ („Verbandssanktionengesetz“ – VerSanG) war, sollte erstmalig im deutschen Strafrecht eine explizit strafrechtliche Sanktionierung von „Verbänden, deren Zweck auf einen wirtschaftlichen Geschäftsbetrieb gerichtet ist“, geregelt und gesetzliche Vorgaben für interne Untersuchungen geschaffen werden. Als wesentlichen Gesetzeszweck definierte der Regierungsentwurf, die auch als Beschuldigte verfolgbaren Wirtschaftsunternehmen zu internen Untersuchungen anzuhalten und einen eigenen Beitrag zur Aufklärung von Straftaten zu leisten. Aufgrund zu großer Differenzen, insbesondere zum Umgang mit Berichten aus internen Untersuchungen, scheiterte die Einführung des Verbandssanktionengesetzes im Jahr 2021 letztlich jedoch.

1 Siehe zur Criminal Compliance sowie zum Entwurf des Verbandssanktionengesetzes → Böttger, Kap. 2 Rn. 16 ff., 143 ff.

2 Gesetzentwurf der Bundesregierung zum Entwurf eines Gesetzes zur Stärkung der Integrität vom 16.6.2020, https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/RegE/RegE_Staerkung_Integritaet_Wirtschaft.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 12.6.2024), im Weiteren RegE VerSanG v. 16.6.2020.

- 4 Gesetzgeberische Erwähnung finden interne Untersuchungen nun in dem am 2.7.2023 in Kraft getretenen Gesetz für einen besseren Schutz hinweisgebender Personen (**Hinweisgeberschutzgesetz – HinSchG**).³ So kann die nach § 12 HinSchG bei Unternehmen einzurichtende, interne Meldestelle bei Vorliegen konkreter Hinweise auf Fehlverhalten von Mitarbeitern nach § 18 HinSchG u. a. entweder selbst eine dort sogenannte „**interne Untersuchung**“ durchführen oder das Verfahren zwecks weiterer Untersuchungen an eine bei dem Unternehmen für „**interne Ermittlungen**“ zuständige Arbeitseinheit abgeben.⁴
- 5 Interne Untersuchungen, insbesondere grenzüberschreitende, weisen eine Vielzahl komplexer rechtlicher Fragestellungen aus verschiedenen Rechtsbereichen auf. Deren Beachtung ist eine wesentliche Bedingung für ihren Erfolg. Dieser Beitrag widmet sich indes in erster Linie dem Management, d. h. der Organisation von Aufgaben und Abläufen interner Untersuchungen. Dabei können rechtliche Aspekte jedoch nicht vollständig ausgeklammert werden, zeichnet sich gutes Management doch durch die richtige Balance zwischen rechtlicher Verpflichtung und praktischer Zweckmäßigkeit aus.
- 6 Nachfolgend soll die Lösung praktischer Fragen einer internen Untersuchung anhand ihres zeitlichen Ablaufs aufgezeigt werden. Sie beginnt mit der Entscheidung über die Durchführung einer internen Untersuchung (→ Rn. 7 ff.), führt über die Vornahme eventuell notwendiger Eilmaßnahmen (→ Rn. 24 ff.) und einer notwendigen gründlichen Planung (→ Rn. 34 ff.) bis zur Durchführung der Untersuchungsmaßnahmen und einem Festhalten der Ergebnisse im Untersuchungsbericht (→ Rn. 108 ff.). Die „Nachphase“, in der das Unternehmen die notwendigen arbeits- oder zivilrechtlichen Konsequenzen zieht und Arbeitsprozesse oder Kontroll- und Compliance-Systeme aufgrund der Erkenntnisse aus der internen Untersuchung anpasst, wird dem Gegenstand dieser Abhandlung entsprechend nicht weiter vertieft.⁵

II. Entscheidung über die Durchführung interner Untersuchungen

- 7 Die Frage nach der Durchführung einer internen Untersuchung stellt sich den im Unternehmen dafür zuständigen Stellen (nachfolgend → Rn. 8 ff.) regelmäßig dann, wenn es Anhaltspunkte für Compliance-Verstöße gibt. Diese können sich etwa aus Meldungen im Rahmen von Hinweisgebersystemen, Hinweisen auf Auffälligkeiten durch die Abschlussprüfer oder aufgrund ermittlungs- oder aufsichtsbehördlicher Auskunftersuchen ergeben. Bei Vorliegen eines konkreten Anfangsverdachts sind Maßnahmen zur weiteren Aufklärung verpflichtend (nachfolgend → Rn. 11 ff.). Zu entscheiden ist dann, ob die notwendige Aufklä-

3 RegE VerSanG v. 16.6.2020, 1 f.; siehe hierzu auch → Böttger, Kap. 2 Rn. 16 ff., 143 ff.; kritisch Raum, CCZ 2020, 245, 249.

4 Hinweisgeberschutzgesetz vom 31.5.2023 (BGBl. 2023 I Nr. 140).

5 Siehe hierzu auch → Block/Sonnenberg, Kap. 5.

rung durch eine interne Untersuchung erfolgen soll oder externen Ermittlungs- oder Aufsichtsbehörden überlassen bleiben kann (nachfolgend → Rn. 14 ff.).

1. Entscheidungsbefugte Stellen

Die Entscheidung über die Durchführung von internen Untersuchungen liegt regelmäßig bei der Geschäftsleitung als Teil ihrer allgemeinen Compliance-Verantwortung.⁶ Innerhalb der Geschäftsleitung kann sie einem Mitglied als primär Verantwortlichem zugewiesen sein (horizontale Delegation).⁷ 8

Die Geschäftsleitung kann – was ab einer gewissen Unternehmensgröße praktisch der Regelfall ist – die Primärverantwortung für die Aufklärung von Compliance-Verstößen auch auf nachgeordnete Unternehmensstellen übertragen (vertikale Delegation), etwa an eine eigenständige Compliance-Abteilung bzw. den Chief Compliance Officer, die interne Revision oder die Rechtsabteilung.⁸ Hier sind unterschiedlichste Zuständigkeitsaufteilungen zwischen Geschäftsleitung und nachgeordneten Stellen einerseits und zwischen letzteren andererseits denkbar, etwa nach der Art der jeweils in Rede stehenden Compliance-Verstöße oder dem durch sie möglicherweise verursachten finanziellen Schaden. 9

Auch sofern Mitglieder der Geschäftsleitung selbst in Compliance-Verstößen involviert sein können oder Schadensersatzansprüche des Unternehmens gegen sie im Raum stehen, obliegt die Einleitung und Durchführung einer internen Untersuchung als Geschäftsführungsmaßnahme vorrangig der Geschäftsführung.⁹ Im Normalfall wird diese vom Aufsichtsgremium (Aufsichtsrat der Aktiengesellschaft, Beirat der GmbH) lediglich begleitet. Dieses ist verpflichtet, das Bestehen von Ansprüchen der Gesellschaft gegen amtierende oder ehemalige Vorstandsmitglieder eigenverantwortlich zu prüfen, und erforderlichenfalls auch zu verfolgen und durchzusetzen.¹⁰ Erst dann, wenn hinreichende Anhaltspunkte dafür vorliegen, dass die von der Geschäftsleitung eingeleitete Untersuchung nicht (mehr) zu der notwendigen Sachverhaltsaufklärung führt, muss das Aufsichtsgremium seine Kontrolltätigkeit intensivieren und gegebenenfalls eine eigenständige interne Untersuchung durchführen.¹¹ 10

2. Pflicht zur Aufklärung konkreter Verdachtsfälle

Die Geschäftsleitung bzw. die mit der Compliance-Verantwortung betrauten nachgeordneten Stellen sind verpflichtet, bei konkreten Hinweisen auf Compli- 11

6 Vgl. dazu *Moosmayer*, Compliance, Rn. 320 sowie 338 ff. und 344 ff.

7 *Schulz/Galster*, in: Bürkle/Hauschka/Schieffler, Der Compliance Officer, § 3 Rn. 21 ff.

8 Zu den Grenzen der horizontalen Delegation siehe auch → *Böttger*, Kap. 2 Rn. 120.

9 Ausführlich zu unterschiedlichen Organisationsmodellen für die Compliance-Funktion *Moosmayer*, Compliance, Rn. 105 ff.; *Schulz/Galster*, in: Bürkle/Hauschka/Schieffler, Der Compliance Officer, § 3 Rn. 2 ff.; zur vertikalen Delegation auch → *Böttger*, Kap. 2 Rn. 121.

10 BGH, Urt. v. 21.4.1997 – II ZR 175/95 (= NJW 1997, 1926); zur Compliance-Pflicht der Unternehmensleitung → *Schulz*, Kap. 1 Rn. 27 ff.

11 *Wagner*, CCZ 2009, 8, 12; *Moosmayer/Hartwig*, Interne Untersuchungen, S. 159 Rn. 7.

ance-Verstöße Maßnahmen zu deren Aufklärung einzuleiten und erkannte Rechtsverstöße abzustellen und – wobei hier ein bestimmter Ermessensspielraum besteht – auch zu ahnden („Aufklären, Abstellen, Ahnden“).¹² Die Verletzung der Aufklärungspflicht kann ihrerseits zu einer Haftbarkeit der Geschäftsleitung führen. Entsprechendes gilt für das Aufsichtsgremium in der Konstellation eines Verdachts auf Compliance-Verstöße unter Beteiligung der Geschäftsleitung.

- 12 Um die Notwendigkeit zu weiteren Aufklärungsmaßnahmen beurteilen zu können, muss die entscheidungsbefugte Stelle zunächst die Plausibilität und Belastbarkeit des Hinweises im Hinblick auf in Betracht kommende Compliance-Verstöße überprüfen (lassen). Gegebenenfalls muss der Hinweisgeber weiter befragt werden. (Nur) wenn ein hinreichend konkreter Anfangsverdacht auf Compliance-Verstöße besteht, sind weitere Maßnahmen zur Aufklärung einzuleiten.
- 13 Damit ist nicht gesagt, dass die weitere Aufklärung *notwendigerweise* durch eine interne Untersuchung erfolgen muss; sie könnte je nach in Rede stehenden Compliance-Verstößen grundsätzlich auch den Ermittlungs- oder Aufsichtsbehörden überlassen bleiben (dazu sogleich). Auch die bereits angesprochene Entwurfsfassung des Verbandssanktionengesetzes sah keine Verpflichtung zur internen Untersuchung eines strafrechtlichen Verdachtssachverhalts vor, maß ihrer ordnungsgemäßen Durchführung jedoch entscheidende Bedeutung für eine Milderung der späteren, strafrechtlichen Sanktion des Unternehmens bei.¹³ Des Weiteren ist mit der Entscheidung für eine interne Untersuchung nichts über deren Umfang und Gestalt gesagt. Der unterschiedlichen Bedeutung möglicher Compliance-Verstöße oder den etwaigen Nachteilen der Untersuchung für das Unternehmen kann – und muss – auf Basis einer Verhältnismäßigkeitsprüfung bei der Ausgestaltung der internen Untersuchung Rechnung getragen werden.¹⁴

3. Interne Untersuchung oder externe Ermittlung?

- 14 Im Falle des Verdachts möglicher straf- oder aufsichtsrechtlich relevanter Compliance-Verstöße steht die entscheidungsbefugte Stelle vor der Frage, ob sie diese intern untersuchen oder die Aufklärung den externen Ermittlungs- oder Aufsichtsbehörden überlassen soll.

12 Wagner, CCZ 2009, 8, 12; Moosmayer/Hartwig, Interne Untersuchungen, S. 159 Rn. 7.

13 LG München I, 10.12.2013 – 5 HK O 1387/10, NZG 2014, 345 – Siemens/Neubürger; vgl. hierzu Fleischer, NZG 2014, 321.

14 §§ 16–18 RegE VerSanG v. 16.6.2020. Zum Verbandssanktionengesetz siehe auch → Böttger, Kap. 2 Rn. 16 ff., 143 ff.; zur Haftung der Geschäftsführung bei verfehlter Milderungsmöglichkeit Giese/Dachner, ZIP 2020, 498, 503.

a) Bereits laufendes behördliches Verfahren

Soweit in diesem Entscheidungsstadium bereits ein behördliches (Ermittlungs-)Verfahren zum Untersuchungsgegenstand eingeleitet ist, bestimmen sich die Rechte und Pflichten des betroffenen Unternehmens nach dem jeweils anwendbaren Prozessrecht. **15**

Nach deutschem Strafprozessrecht ist eine parallele interne Untersuchung nicht ausgeschlossen.¹⁵ Allerdings muss sich die entscheidungsbefugte Stelle die Frage stellen, ob angesichts der ohnehin stattfindenden Aufklärung des möglichen Compliance-Verstoßes durch die Ermittlungsbehörden, der notwendigen Abstimmung einer internen Untersuchung mit den staatlichen Behörden sowie der behördlicherseits regelmäßig erwarteten Herausgabe der Untersuchungsergebnisse¹⁶ eine solche interne Untersuchung tatsächlich parallel durchgeführt werden soll. **16**

Trotz der genannten Aspekte ist die parallele Durchführung einer internen Untersuchung bereits nach aktueller Rechtslage in der Regel zu empfehlen oder durch das von der Geschäftsleitung zu wahrende Unternehmensinteresse sogar geboten. Dieses lässt sich ohne Weiteres für die Fälle bejahen, in denen die Ermittlungsbehörden die Durchführung einer internen Untersuchung unter Inanspruchnahme von Vergünstigungen bei der Sanktionierung verlangen. Dessen ungeachtet werden die eigenen Untersuchungen des Unternehmens regelmäßig dazu beitragen, dass die Behörden ihre Ermittlungen beschränken und so damit einhergehende, mitunter erhebliche Beeinträchtigungen der Geschäftsabläufe reduziert werden. Zu berücksichtigen ist zudem insbesondere der Umstand, dass der Zeitraum, in dem die Unternehmensleitung zu arbeits-, haftungs- und gegebenenfalls auch bilanzrechtlichen Fragen aufgrund von Compliance-Verstößen eine Antwort finden muss, meist deutlich kürzer bemessen ist, als die Dauer eines oft mehrere Jahre andauernden Ermittlungsverfahrens. **17**

Der in die Abwägung einzustellende Aspekt der Vergünstigung bei der Sanktionierung wurde im Regierungsentwurf des Verbandssanktionengesetzes kodifiziert: Parallel geführte, interne Untersuchungen sollten – soweit sie wesentlich zu einer Aufklärung der Verbandstraftat beitragen – nicht nur ausdrücklich erlaubt sein, sondern würden bei gesetzeskonformer Durchführung automatisch mit Strafmilderungen belohnt. Die mit der Beauftragung externer Rechtsanwälte einhergehenden Ziel- und Interessenkonflikte bei der Evaluation und Kommunikation interner Untersuchungen löste der Gesetzesentwurf mit dem Gebot einer klaren Trennung¹⁷ von Untersuchungsführern einerseits und Verteidigern von beschuldigten Personen und Unternehmen andererseits. Dies sollte nicht nur er-

15 Siehe zum Verhältnismäßigkeitsprinzip → Rn. 36 f.

16 Siehe aber in der Tendenz durchaus kritisch: LG Mannheim, NSTZ 2012, 713, 716, das feststellt, dass „Unternehmen als Anzeigenerstatter – auch von mit ‚internal investigations‘ betrauten Rechtsanwälte unterstützte – zuweilen nur sehr sukzessive bzw. mit offenbar wohl durchdachter Strategie die ihnen zur Verfügung stehenden Beweismittel vorlegen“.

17 Siehe dazu *Wettner/Mann*, DStR 2014, 655, 657 ff.

folgen, um die Glaubwürdigkeit der Ergebnisse interner Untersuchungen gegenüber Ermittlungsbehörden zu stärken,¹⁸ sondern künftig auch mit einer unterschiedlichen Handhabung des Beschlagnahmeschutzes von Untersuchungsergebnissen korrespondieren, je nachdem, ob diese von Untersuchungsführern oder im Verteidigungsverhältnis agierenden Personen gewonnen wurden. Nach der entfallenen Umsetzung des Regierungsentwurfs stehen insoweit gesetzliche Regelungen zwar weiter aus, die interpretatorische Einwertung von Rechtskreisen und Beschlagnahmeprivilegien der verschiedenen Beteiligten wird jedoch durch den Blick auf Entwurfsinhalt und Gesetzgebungsmaterialien schärfer gestellt.

- 19 Und schließlich ist zu bedenken, dass sich die staatlichen Ermittlungsbehörden – trotz der gesetzlich in § 160 Abs. 2 StPO festgeschriebenen Verpflichtung zur Objektivität – bereits seit längerer Zeit nicht von der Tendenz eines eher auf den Belastungsbeweis fokussierten Ermittlungsansatzes freimachen, um medienwirksam Unternehmensgeldbußen und Gewinnabschöpfungen zugunsten der Staatskasse in immer größeren Volumina herbeizuführen.¹⁹ Vor diesem Hintergrund nutzt eine eigene, interne Aufklärung des Sachverhalts zur Sicherstellung des Auffindens und der Berücksichtigung aller – auch entlastenden – Beweise häufig nicht nur einer weitergehenden und objektiveren Untersuchung der „prozessualen Wahrheit“, sondern auch unmittelbar den wirtschaftlichen Interessen des betroffenen Unternehmens. Nicht selten fördert auch der intensivere Zugriff einer internen Untersuchung auf das unternehmensinterne Know-how Ergebnisse und Zusammenhänge zutage, die von den Ermittlungsergebnissen der Strafverfolgungsbehörden in entscheidenden Details deutlich abweichen können.

b) (Noch) kein behördliches Verfahren

- 20 Ist zum Untersuchungsgegenstand (noch) kein Ermittlungsverfahren anhängig, stellt sich die Frage, ob das Unternehmen durch eine Anzeige des möglichen Compliance-Verstoßes ein solches – als Alternative zu eigenen Untersuchungen – initiieren sollte.
- 21 Nach deutschem Recht besteht grundsätzlich keine Pflicht des Unternehmens oder seiner Mitarbeiter zur Anzeige vermuteter oder tatsächlicher Straftaten.²⁰ Das Unternehmen kann diese eigenständig durch interne Untersuchungen auf-

18 § 17 Abs. 1 Satz 1 Nr. 2 RegE VerSanG v. 16.6.2020.

19 Vgl. Nr. 13 der FAQ zum RegE VerSanG v. 16.6.2020, https://www.bmj.de/SharedDocs/Downloads/DE/Themen/Nav_Themen/FAQ_Integritaet_Wirtschaft.html (zuletzt abgerufen am 12.6.2024).

20 So exemplarisch der damalige Leitende Oberstaatsanwalt der Staatsanwaltschaft München I, *Manfred Nötzel*, in einem Interview mit *Issig* in der Welt am Sonntag vom 14.8.2011 aus Anlass des „Erfolgs“ des in diesem Jahr erstmalig „direkt für den Staatshaushalt abgeschöpften“ Unternehmensbußgeld-Volumens von einer Milliarde Euro, <http://www.welt.de/print/wams/muenchen/article13543574/Wenn-er-kommt-ist-Zahntag.html> (zuletzt abgerufen am 12.6.2024).

klären. Auch ist dann, wenn noch kein externes Ermittlungsverfahren zum Untersuchungsgegenstand eingeleitet ist, nicht gefordert, dass das Unternehmen geplante interne Untersuchungsmaßnahmen mit den staatlichen Ermittlungsbehörden abstimmt oder diese offenlegt.²¹ Insoweit ist jedoch neu zu bedenken, dass diese Abwägungsmöglichkeiten den Unternehmen durch das Hinweisgeberschutzgesetz teilweise entzogen und – im Falle von gegebenen Hinweisen – auf die insoweit einzurichtende **Interne Meldestelle** übertragen wurden (vgl. § 18 HinSchG).²²

Dessen ungeachtet kann es für das Unternehmen in bestimmten Konstellationen sinnvoll sein, im oder aus dem Unternehmen heraus begangene (mögliche) Straftaten anzuzeigen, etwa um von Kronzeugenregelungen zu profitieren (dazu noch → Rn. 30) oder um so ein staatliches Ermittlungsverfahren zu initiieren. Letzteres ist etwa der Fall, wenn sich das Unternehmen im staatlichen Verfahren die Ermittlung und Sicherung von Informationen oder Vermögenswerten verspricht, an die es sonst – etwa mangels eigener Zwangsbefugnisse – kaum gelangen würde. Auf derartige Informationen kann dann im Wege der Akteneinsicht Zugriff genommen werden.²³

Aus den bereits oben genannten Gründen werden aus Unternehmenssicht externe Ermittlungen die interne Untersuchung in der Regel nicht ersetzen können, sondern allenfalls zu deren Komplementierung dienen. Ob dies sinnvoll ist, muss im Einzelfall entschieden werden. Zu beachten ist dabei stets, dass die Anzeige von Straftaten sowie deren eigene interne Untersuchung auch Risiken birgt, namentlich die Gefahr von Geldbußen für das Unternehmen oder dessen aufsichtspflichtige Personen (§§ 30, 130 OWiG)²⁴ oder den Zugriff der Ermittlungsbehörden auf die Untersuchungsergebnisse. Sind die Ermittlungsbehörden erst einmal informiert, kann das Unternehmen deren weiteres Vorgehen nicht kontrollieren.

III. Vornahme von Eilmaßnahmen

Noch vor bzw. zu Beginn der eigentlichen Planung der internen Untersuchung ist an Maßnahmen zu denken, die faktisch oder aus rechtlichen Gründen, etwa weil kurze Fristen einzuhalten sind, regelmäßig besonders eilbedürftig sind und gegebenenfalls unverzüglich vorgenommen werden müssen. Auch im Laufe der

21 Das deutsche Strafgesetzbuch sieht in § 138 StGB lediglich eine Anzeigepflicht für geplante Straftaten vor, die im Kontext von Compliance-Untersuchungen regelmäßig nicht relevant werden (z. B. Mord, Totschlag). Daneben bestehen branchenspezifische Anzeigepflichten für Geldwäschedelikte nach dem Geldwäschegesetz (GwG), die aber weniger auf das eigene Unternehmen, als auf Auffälligkeiten bei Kunden und Geschäftspartnern abzielen.

22 Weder „Ob“ noch „Wie“ der Compliance-Untersuchung müssen offengelegt werden. Vgl. auch *Grützner*, in: *Momsen/Grützner, Wirtschaftsstrafrecht*, 2013, Kap. 4 Rn. 73.

23 Zum Hinweisgeberschutz siehe auch → *Block/Sonnenberg*, Kap. 5.

24 Siehe dazu *Wettner/Mann*, DStR 2014, 655, 660 f.

Untersuchung kann sich je nach Erkenntnisstand die Notwendigkeit solcher Maßnahmen ergeben.

1. Einrichtung einer zentralen Koordinierungsstelle

- 25** Ist im Unternehmen bereits eine Compliance-Organisation vorhanden und ein Compliance-Management-System (CMS) etabliert, wird bereits vorgegeben sein, wer unternehmensintern für die Planung und Steuerung einer internen Untersuchung zuständig ist. Andernfalls muss zunächst eine zentrale Stelle installiert werden, die sämtliche Aufgaben im Rahmen der Untersuchung sowie die Kommunikation nach innen und außen koordiniert.²⁵ Dies ist auch in Sachverhalts-Konstellationen geboten, in denen die Mitwirkung von Mitarbeitern der zuständigen Einheit am zu untersuchenden Compliance-Verstoß im Raum steht. Dies ist häufig der Fall, wenn der Verdacht besteht, dass Compliance-Mitarbeiter trotz positiver Kenntnis von rechtswidrigen Vorgängen notwendige Maßnahmen unterlassen haben.
- 26** In Ermangelung einer eigenständigen oder konfliktfreien Compliance-Abteilung sollte in einer Koordinierungsstelle die Rechtsabteilung des Unternehmens zumindest vertreten sein, die die Notwendigkeit von Eilmaßnahmen und deren rechtmäßige Vornahme noch vor der Hinzuziehung externer Anwälte rechtlich beurteilen kann. Die Koordinierungsstelle muss zügig die unternehmensinternen Regelungen, namentlich Richtlinien, Arbeitsanweisungen oder Betriebsvereinbarungen, im Zusammenhang mit den zu untersuchenden Sachverhalten und vorzunehmenden (Sofort-)Maßnahmen zusammenstellen.²⁶ Bei internen Untersuchungen mit Breiten- und Außenwirkung fällt der Koordinierungsstelle auch die zügige Entwicklung einer PR-Strategie zu, gegebenenfalls unter Einschaltung von spezialisierten PR-Beratern.

2. Maßnahmen der Daten- und Beweissicherung

- 27** Zuallererst ist zu überlegen, welche relevanten Daten und potenziellen Beweismittel im Unternehmen vorhanden sind, die gegen Veränderung oder Unterdrückung gesichert werden müssen. Dabei ist insbesondere an Folgendes zu denken: Im Unternehmen vorhandene Standardprozesse zur turnusmäßigen Vernichtung von Dokumenten und Daten müssen auf ihre Relevanz für den (noch im Einzelnen zu definierenden – siehe dazu → Rn. 44 ff.) Untersuchungsgegenstand geprüft und gegebenenfalls ausgesetzt werden. In Abstimmung mit der IT-Abteilung des Unternehmens sollten Sicherungskopien der E-Mail-Accounts und Festplatten von betroffenen Mitarbeitern und Arbeitseinheiten (Abteilungen, Projektgruppen etc.) erstellt werden.

²⁵ Siehe dazu → Böttger, Kap. 2 Rn. 139 ff.

²⁶ Scheunemann/Hellfritsch, in: Bay, Hdb. Internal Investigations, Kap. 6 Rn. 13.

3. Arbeitsrechtliche Maßnahmen

Im Zusammenhang mit der Daten- und Beweissicherung ist auch zu überlegen, ob Arbeitnehmern der Zugang zu ihrem Arbeitsplatz bzw. ihren Arbeitsmitteln (insbesondere Computer, Laptop, Mobiltelefon) zu versagen ist oder sie sogar freigestellt werden sollten. Fristlose Kündigungen von Mitarbeitern aus wichtigem Grund sind zu Beginn der Untersuchung, wenn auf Basis eines Anfangsverdachts erst noch weiter ermittelt werden muss, in der Regel (noch) nicht angezeigt. Andernfalls und für den weiteren Verlauf der Untersuchung ist zu beachten, dass hierfür nach deutschem Recht eine Zwei-Wochen-Frist ab dem Zeitpunkt gilt, in dem der Kündigungsberechtigte von den für die Kündigung maßgebenden Tatsachen Kenntnis erlangt hat (§ 626 Abs. 2 BGB). Zu berücksichtigen ist auch, ob es für die Maßnahmen der Daten- und Beweissicherung wie (sonstiger) arbeitsrechtlicher Maßnahmen der Beteiligung des etwaigen Betriebsrats bzw. Sprecherausschusses oder des Datenschutzbeauftragten bedarf. **28**

4. Beachtung von Informations- und Berichtspflichten

Schließlich sind etwaige Informations- und Berichtspflichten des Unternehmens gegenüber Dritten zu beachten.²⁷ **29**

Gibt es im deutschen Recht auch keine Pflicht zur (Selbst-)Anzeige bei Ermittlungs- oder Aufsichtsbehörden, so kann diese zur Reduzierung des Haftbarkeitsrisikos des Unternehmens notwendig werden. Dies gilt insbesondere zur Bußgeldvermeidung oder -reduzierung bei Kartellverstößen im Rahmen der geltenden Kronzeugenregelungen oder gegenüber der US-amerikanischen SEC und dem DOJ.²⁸ Auch im deutschen Recht kann die freiwillige Offenlegung von Straftaten im Rahmen der gegen das Unternehmen möglichen ordnungsrechtlichen Mittel (Geldbuße und Verfall) mildernd berücksichtigt werden. **30**

Des Weiteren müssen die Unternehmensverantwortlichen sowie die mit der Untersuchungsverantwortung betrauten Personen im eigenen Interesse der Vermeidung von Strafbarkeitsrisiken immer auch steuerrechtliche Tatbestände und gegebenenfalls notwendige Korrekturmeldungen im Blick haben (dazu noch → Rn. 42). In diesem Zusammenhang sind auch die zeitlichen Zwänge zu beachten, wenn die untersuchten – auch in der Vergangenheit liegenden – Sachverhalte für die Aufstellung des aktuellen Jahresabschlusses eines Unternehmens nach IFRS/IAS oder HGB Relevanz entfalten, weil im Falle der Bestätigung eines bestehenden Verdachts Rückstellungen gebildet werden müssen. **31**

Daneben müssen börsennotierte Unternehmen immer auch prüfen, ob und wann sie nach den kapitalmarktrechtlichen Bestimmungen, insbesondere nach den **32**

27 Siehe zur unbedingten Beachtung der geltenden, auch unternehmensinternen, Regelungen → Rn. 36.

28 Zu den aus ausländischen Rechtsordnungen stammenden Verpflichtungen zu Untersuchungsmaßnahmen vgl. im Überblick: *Taschke/Schoop*, in: Rotsch, Criminal Compliance, § 34 B Rn. 96 ff.

Grundsätzen über die sogenannte Ad-hoc-Publizität (Art. 17 Abs. 1 UAbs. 1 Marktmissbrauchs-VO²⁹ bzw. § 26 WpHG), zu einer Veröffentlichung der (geplanten) Untersuchung oder deren Gegenständen verpflichtet sind. Dies ist der Fall, wenn die genannten Umstände, die direkt oder indirekt einen oder mehrere Emittenten oder ein oder mehrere Finanzinstrumente betreffen, noch nicht öffentlich bekannt sind, im Falle ihres Bekanntwerdens aber den Kurs dieser Finanzinstrumente oder den Kurs damit verbundener derivativer Finanzinstrumente erheblich beeinflussen können (Art. 7 Marktmissbrauchs-VO). Eine dann notwendige Ad-hoc-Meldung hat unverzüglich zu erfolgen.

- 33** Darüber hinaus ist unbedingt an mögliche Anzeigepflichten gegenüber Versicherern zu denken. Diese ergeben sich regelmäßig aus den Bedingungen der bestehenden Policen. Auch aufgrund laufender Verhandlungen über die Verlängerung oder den Neuabschluss einer Versicherung kann die Anzeige geboten sein.

IV. Planung der internen Untersuchung

- 34** Hat man sich über etwaige Sofortmaßnahmen ein Bild gemacht und diese gegebenenfalls durchgeführt, ist in die (weitere) Planung der internen Untersuchung einzusteigen. Nachfolgend werden nach einer Erörterung der Grundlagen der Planung (nachfolgend → Rn. 35 ff.) zunächst die einzelnen Bereiche und Aspekte dargestellt, die bei der Planung zu berücksichtigen sind (nachfolgend Rn. 44 bis 89). Ziel und Arbeitsergebnis dieser Planungsphase ist ein umfassender Untersuchungsplan, der das Untersuchungsprogramm möglichst detailliert festlegt (nachfolgend → Rn. 90 ff.).

1. Grundlagen der Planung

- 35** Bei der Planung der Untersuchung und einzelnen Maßnahmen ist zum einem strikt auf deren Recht- und Verhältnismäßigkeit zu achten. Zum anderen sollte man sich bereits bei der Planung gegebenenfalls unerwünschte Risiken und Folgen der Untersuchung vergegenwärtigen, um diesen bestmöglich begegnen zu können.

a) Beachtung von Recht- und Verhältnismäßigkeit

- 36** Dass die interne Untersuchung zur Aufdeckung von Rechtsverstößen selbst geltendes Recht und interne Regelungen, etwa die Verhaltens- oder Datenschutzrichtlinien, strikt zu beachten hat, versteht sich von selbst. Andernfalls drohen Haftbarkeitsrisiken der mit der Entscheidung, Planung und Durchführung der Untersuchung befassten Personen, ist die Verwertbarkeit der gefunden Untersuchungsergebnisse in nachfolgenden Prozessen oder für arbeitsrechtliche Maßnahmen gefährdet und steht die Reputation des Unternehmens nach außen wie

²⁹ Verordnung (EU) Nr. 596/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über Marktmissbrauch.

innen auf dem Spiel.³⁰ Unumgänglich ist daher stets die enge Einbindung interner Syndizi oder spezialisierter externer Rechtsanwälte.³¹

Der zu beachtende Grundsatz der Verhältnismäßigkeit setzt der Untersuchung zunächst im Rahmen einer Kosten-Nutzen-Relation Grenzen. Es ist nicht eine Aufklärung „um jeden Preis“ gefordert. Welchen personellen und finanziellen Aufwand die Untersuchung rechtfertigt, ist in Ansehung des Untersuchungsgegenstandes und der verfolgten Ziele zu bewerten. Darüber hinaus ist im Hinblick auf die betroffenen Mitarbeiter die Verhältnismäßigkeit der Mittel zu wahren. Insbesondere für tief in deren Persönlichkeitssphäre eingreifende Untersuchungsmaßnahmen wie der Einsatz von Privatdetektiven oder Telefon- und Videoüberwachungen verbleibt damit – ungeachtet ihrer rechtlichen (Un-)Zulässigkeit – regelmäßig nur ein geringer Einsatzspielraum.³² Eine zusätzliche Ermittlung durch mit entsprechenden Ermittlungs- und Zwangsbefugnissen ausgestattete staatliche Stellen, die durch entsprechende Anzeigen initiiert werden kann (dazu → Rn. 20 ff.), sollte stets zumindest mitbedacht werden.³³ 37

b) Beachtung von Risiken und Folgen der internen Untersuchung

Ungeachtet aller Vorteile einer (eigenen) Aufklärung möglicher Compliance-Verstöße und ihrer Selbstreinigungs- und Publizitätswirkung zur Spiegelung der Unternehmens-Compliance kann eine interne Untersuchung auch zu – ungewollten – Folgen für das Unternehmen und seinen Organen und Mitarbeitern führen. Werden diese Folge-Szenarien auch regelmäßig nicht dazu Anlass geben können, die Aufklärung eines möglichen Compliance-Verstoßes zu unterlassen („Ob“), so sollten sie bei der Gestaltung der internen Untersuchung („Wie“) beachtet und durchdacht werden. 38

Die Aufdeckung strafrechtlicher Compliance-Verstöße kann **die strafrechtliche Verantwortung** der betroffenen Mitarbeiter oder Organe oder Sanktionen durch Aufsichts- oder Ermittlungsbehörden, etwa Unternehmensgeldbußen, nach sich ziehen. Im Rahmen der internen Untersuchung produzierte Dokumente können der Beschlagnahme durch die Strafverfolgungsbehörden unterliegen. 39

Die Untersuchungsergebnisse können auch dem **Zugriff (privater) Dritter** ausgesetzt sein. Hier ist im anglo-amerikanischen Rechtsraum an die Offenlegung in sogenannten Pre-Trial-Discovery-Verfahren zu denken. In Deutschland erscheint dieses Risiko zwar geringer. Aber auch hier können geschädigte Verbraucher, Geschäftspartner oder Wettbewerber durch mögliche Einsichtnahmen in strafrechtliche Ermittlungsakten Kenntnis von dort befindlichen – zuvor be- 40

30 Zum Ganzen auch *Poppe*, in: Inderst/Bannenberg/Poppe, Compliance, 6. Kap. Rn. 31 ff.; zu strafrechtlichen Risiken innerhalb von Compliance-Prozessen und insbesondere internen Untersuchungen, → *Böttger*, Kap. 2 Rn. 196 ff.

31 *Moosmayer*, Compliance, Rn. 321.

32 Vgl. *Moosmayer*, Compliance, Rn. 325.

33 Vgl. *Moosmayer*, Compliance, Rn. 325.

schlagnahmen – Unterlagen erlangen. Jenseits rechtlich begründeter Zugriffe ist bei aller Vertraulichkeit schließlich auch ein „Durchstechen“ von Unterlagen und Informationen aus dem Umfeld staatlicher Ermittlungsbehörden nicht auszuschließen.

- 41 Ein weiterer wichtiger Aspekt ist die **Wahrscheinlichkeit der Entdeckung weiterer Compliance-Verstöße** durch die anstehende Untersuchung. Sind solche zu erwarten, ist eine Vorabprüfung ihres Umfangs und der daraus möglicherweise folgenden Konsequenzen – auch unter Berücksichtigung von Verjährungsvorschriften und internationalen Bezügen (etwa in die USA) – vorzunehmen, um überraschende Effekte für das Unternehmen entsprechend abzumildern.
- 42 Neben der Aufdeckung weiterer, bisher unbekannter kritischer Sachverhalte ist stets auch an **steuerrechtliche Tatbestände** zu denken. Ergibt die interne Untersuchung, dass das Unternehmen bestimmte steuerrelevante Geschäftsvorgänge in der Vergangenheit nicht oder unzutreffend gegenüber den Finanzbehörden erklärt hat, können die durch die Untersuchung zutage geförderten Erkenntnisse gegebenenfalls die umgehende Korrektur angegebener Steuererklärungen gemäß § 153 AO erforderlich machen; andernfalls kann das Risiko einer (weiteren) Steuerhinterziehung oder der Beihilfe dazu durch die mit der Untersuchungsverantwortung betrauten Personen bestehen. Die strafrechtlichen Risiken einer versäumten Korrekturmeldung nach Maßgabe des § 153 AO sind insbesondere sehr schwer in den Fällen zu überblicken, in denen sich ein zeitlich vorgelagerter, steuerrechtlicher Verstoß aufgrund von Sorglosigkeiten einzelner Verantwortlicher ergeben hat, welche in der Ex-post-Betrachtung die Grenze zur „billigenden Inkaufnahme“ eines steuerrechtlichen Verstoßes überschritten haben.³⁴
- 43 Schließlich muss bedacht werden, dass das Unternehmen über die Untersuchungsergebnisse gegebenenfalls im Rahmen seiner **Unternehmensberichterstattung** berichten muss. Gegebenenfalls kann die Berichtigung vergangener Jahresabschlüsse erforderlich werden.

2. Festlegung des Untersuchungsgegenstands

- 44 Eine Umgrenzung des zu untersuchenden Sachverhaltes kann – ausgehend vom vorliegenden Anfangsverdacht – im Hinblick auf den zu untersuchenden **Zeitraum, personell** im Hinblick auf einen präzisierten Kreis von Mitarbeitern, **strukturell** hinsichtlich des Vorgehens bestimmter Abteilungen oder Geschäftsbereiche, aber auch **sachlich** durch die Fokussierung auf ganz bestimmte Arten von Geschäften oder Geschäftspartnern erfolgen.

³⁴ Eine Orientierung in diesem Spannungsfeld vermittelt BGH, Beschl. v. 17.3.2009 – 1 StR 479/08, BGHSt 53, 210: „Nach Ansicht des Senats gebieten Wortlaut, Sinn und Zweck der Vorschrift des § 153 Abs. 1 Satz 1 Nr. 1 AO, eine steuerrechtliche Anzeige- und Berichtungspflicht aus dieser Vorschrift auch dann anzunehmen, wenn der Steuerpflichtige die Unrichtigkeit seiner Angaben bei Abgabe der Steuererklärung nicht gekannt, aber billigend in Kauf genommen hat, und er später zu der sicheren Erkenntnis gelangt ist, dass die Angaben unrichtig sind.“

Maßgebliches Kriterium für diese Festlegung ist vor allem, welche Bedeutung der in Rede stehende mögliche Compliance-Verstoß hat und welche weiteren Ziele – neben Aufklärung und Abstellen dieses Verstoßes – verfolgt werden, etwa die Verteidigung des Unternehmens gegen straf-, aufsichts- oder zivilrechtliche Vorwürfe oder die Verfolgung eigener Ansprüche. Um eine effiziente Aufklärung in der gegebenen – meist kurzen – Zeit zu gewährleisten, sollte der Untersuchungsgegenstand nicht zu weit gefasst werden; andernfalls droht die Untersuchung zu oberflächlich zu bleiben und ihre Ergebnisse nicht hinreichend belastbar zu sein. **45**

Der Untersuchungsgegenstand wird regelmäßig in einem formellen Untersuchungsauftrag der entscheidungsbefugten Stelle festgehalten werden. Dieser Untersuchungsauftrag bildet die innerbetriebliche Grundlage für die Durchführung der Untersuchungsmaßnahmen und legitimiert das Untersuchungsteam im Unternehmen.³⁵ Ergeben sich im Laufe der Untersuchung Hinweise zu weiteren Compliance-Verstößen oder Beteiligten, muss das Untersuchungsteam dies an die zuständige Stelle – etwa die zentrale Koordinierungsstelle – melden. Gegebenenfalls muss der Untersuchungsauftrag durch die entscheidungsbefugte Stelle angepasst bzw. erweitert werden.³⁶ **46**

3. Bestimmung des Untersuchungsteams und der Verantwortlichkeiten

Abhängig von Umfang und Komplexität des Untersuchungsgegenstands, den mit der internen Untersuchung verfolgten Zielen, den heranzuziehenden Informationsquellen sowie den internen Organisationsstrukturen ist das Untersuchungsteam aufzustellen. **47**

a) Auswahl von Mitarbeitern und externen Beratern

Hier ist nach internen Ressourcen und externen Beratern einerseits sowie den notwendigen Professionen und Qualifikationen andererseits zu unterscheiden. **48**

Bei überschaubaren oder Sachverhalten ohne besondere Öffentlichkeitswirkung spricht in der Regel nichts gegen die Durchführung einer – im Wortsinne – rein internen Untersuchung durch die zuständige Abteilung des Unternehmens, etwa durch die Innenrevision. Unter Kostengesichtspunkten kann dies sogar angezeigt sein. Voraussetzung ist allerdings, dass eine Mitwirkung dieser Abteilungen oder Mitarbeiter an dem zu untersuchenden Sachverhalt sicher ausgeschlossen werden kann. **49**

Oft empfiehlt es sich aber, spezialisierte Anwälte oder Wirtschaftsprüfer heranzuziehen.³⁷ Sind bereits ermittlungs- oder aufsichtsbehördliche Untersuchungen **50**

³⁵ Moosmayer, Compliance, Rn. 315.

³⁶ Vgl. Scheunemann/Hellfritzsch, in: Bay, Hdb. Internal Investigations, Kap. 6 Rn. 27.

³⁷ Bei Abwägung aller Vor- und Nachteile kann die Einschaltung externer Berater für die interne Untersuchung im Unternehmensinteresse sogar geboten sein; eine a priori bestehende Pflicht zur Beauftragung externer Berater dürfte allerdings nicht anzunehmen sein.

zum Untersuchungsgegenstand eingeleitet, werden die Behörden regelmäßig die Führung der internen Untersuchung durch externe Berater erwarten, insbesondere wenn die Bereitschaft besteht, für ihre eigenen Ermittlungen auch die Ergebnisse der internen Untersuchungen nutzbar zu machen. Externe Berater bürgen durch ihre grundsätzliche Weisungsfreiheit für eine größere Unabhängigkeit der Untersuchung,³⁸ was den Beweiswert ihrer Ergebnisse erheblich steigern kann (siehe auch → Rn. 18 f.).

- 51 Neben besonderer fachlicher Expertise und Erfahrung spielt aber auch der Geheimnisschutz durch Rechtsanwälte und Wirtschaftsprüfer als Berufsgeheimnisträger eine nicht unerhebliche Rolle bei deren Mandatierung. Mitarbeiter der eigenen Rechtsabteilung oder der Innenrevision genießen – auch wenn es sich um Syndizi handelt – diesen Schutz grundsätzlich nicht.
- 52 Ein bei der Auswahl der internen Ermittler – wie auch generell bei der Besetzung und Kompetenzausstattung von Compliance-Abteilungen – oft vernachlässigter Aspekt ist schließlich die Unternehmenshierarchie. Betroffene Mitarbeiter und Geschäftsleitungsmitglieder lassen sich von in der Unternehmenshierarchie (gefühl) unter ihnen stehenden Mitarbeitern ungern „etwas sagen“. Auch aus diesem Grund kann der Einsatz externer Berater sinnvoll sein.

b) Festlegung von Verantwortlichkeiten und Berichtswegen

- 53 Wichtig ist die genaue Festlegung der Verantwortlichkeiten aller Beteiligten und der einzuhaltenden Berichtswege.
- 54 Dies gilt zunächst im Verhältnis zwischen Mitarbeitern des Unternehmens und externen Beratern. Auch wenn die Untersuchung von externen Beratern geführt wird, sind diese je nach Fall auf die Kenntnisse des Unternehmens und der Branche angewiesen. Bei der Auftragserteilung ist darauf zu achten, dass diese inhaltlich und zeitlich präzise gefasst ist und die Verantwortlichkeiten klar definiert werden. Grundsätzlich sollte vertraglich vereinbart werden, an wen die externen Berater zu berichten haben, etwa an den Aufsichtsrat des Unternehmens.
- 55 Die vertragliche Festlegung vermeidet auch mögliche Auseinandersetzungen, die auftreten können, wenn sich externe Dienstleister und Berater unter Hinweis auf ihre eigenen „Codes of Conduct“ vorbehalten, Erkenntnisse oder Berichte über vermeintliche Straftaten „in jedem Fall und vollumfänglich“ an die entsprechenden Behörden weiterzugeben. In diesen Fällen geht es oft nicht um das „Ob“ einer Weitergabe, sondern um Art und Umfang der weiterzugebenden Materialien. Hier sollte etwa vereinbart werden, dass eine Weitergabe von Arbeitspapieren oder Dokumenten im Entwurfsstadium unbedingt unterbleibt.

38 Zu diesen und weiteren Gründen für die Mandatierung externer Berater siehe *Böhmer*, in: Bay, Hdb. Internal Investigations, Kap. 2 Rn. 1 ff.; *Giese/Dachner*, ZIP 2020, 498, 503 f.

Um thematisch abgrenzbare Arbeitspakete effizient abzuarbeiten, bietet sich die Einrichtung von Projektausschüssen an.³⁹ Je nach definierter Aufgabe sind diese mit Mitarbeitern und/oder externen Beratern besetzt. Unabdingbar ist eine regelmäßige Berichterstattung des Untersuchungsteams sowie der etwaigen Projektausschüsse an die zentrale Koordinierungsstelle (bzw. an die im Rahmen eines bestehenden CMS vorgesehene Stelle). Deren Aufgabe besteht im Laufe der Untersuchung in der Bewertung der zusammengetragenen Informationen im Hinblick auf gegebenenfalls notwendige Eilmaßnahmen und die Überprüfung der Entscheidungsreife gemessen am Untersuchungsauftrag. Gegebenenfalls sind die ermittelten Sachverhalte dem Untersuchungsteam wieder „zurückzugeben“ und unter Hinweis auf konkrete Informationsdefizite weitere Untersuchungshandlungen anzufordern. **56**

4. Bestimmung und Vorbereitung der Informationsquellen

Anhand des Untersuchungsgegenstands müssen die zur Verfügung stehenden Informationsquellen und -mittel identifiziert werden, die im Rahmen der internen Untersuchung abzuarbeiten sind. **57**

a) Relevante Informationsquellen

Neben frei zugänglichen Informationsquellen (etwa Handelsregister oder Auskunfteien) spielen unternehmensinterne Informationsquellen die zentrale Rolle. **58**

aa) Dokumente

Regelmäßig werden im Rahmen einer internen Untersuchung die Geschäftsunterlagen des Unternehmens benötigt. Hierzu gehören Inventare, Jahres- und Konzernabschlüsse, Ein- und Ausgangsrechnungen, Buchungsbelege, Kontenauszüge, geschäftliche Korrespondenz usw. **59**

Derartige dienstliche Dokumente darf das Unternehmen – und die in seinem Auftrag tätigen Ermittler – grundsätzlich immer einsehen und auswerten, auch wenn sie naturgemäß von einem Mitarbeiter erstellt oder an seinem Arbeitsplatz verwahrt werden. Private Dokumente hingegen dürfen grundsätzlich nur in eng umgrenzten Ausnahmefällen untersucht werden, insbesondere im Falle des erheblichen Verdachts der Begehung einer Straftat durch den betroffenen Mitarbeiter. **60**

bb) Elektronische Daten und E-Mails

Die meisten zur Aufklärung erforderlichen Informationen werden jedoch nicht in Geschäftsunterlagen enthalten sein, sondern allein bestimmten Mitarbeitern bekannt sein und sich auf deren Dienstcomputern oder Mobiltelefonen bzw. in deren E-Mail-Accounts finden. **61**

³⁹ Scheunemann/Hellritzsch, in: Bay, Hdb. Internal Investigations, Kap. 6 Rn. 59 ff.

- 62 Unter Einschaltung der IT-Abteilung des Unternehmens sind die möglichen Informationsquellen und der Zugriff auf sie (einschließlich auf Back-ups und Servern) in technischer Hinsicht zu klären. In den (späteren) Interviews der Mitarbeiter sollten diese zudem nach weiteren relevanten Dokumenten und Daten befragt werden.
- 63 Gerade der Zugriff auf elektronische Daten und insbesondere die E-Mail-Kommunikation – auch die nach dem Vorstehenden grundsätzlich untersuchungsfähige – unterliegt strengen arbeits- und datenschutzrechtlichen Beschränkungen. Eine vorherige rechtliche Bewertung der zulässigen Informations- und Auswertungsmöglichkeiten ist unerlässlich.

cc) (Ehemalige) Mitarbeiter

- 64 Unverzichtbare Informationsquelle im Rahmen jeder internen Untersuchung sind auch Befragungen (Interviews) von Mitarbeitern. Diese sind als Arbeitnehmer gegenüber ihrem Arbeitgeber und den von diesem eingeschalteten Ermittlern über Angelegenheiten im Zusammenhang mit ihrer unmittelbaren betrieblichen Tätigkeit und ihrem Aufgabenbereich auskunftspflichtig. Bezüglich Wahrnehmungen des Mitarbeiters, die nicht direkt mit seinem Aufgabenbereich zu tun haben, findet eine Abwägung zwischen den Interessen des Mitarbeiters, etwa sich nicht selbst oder seine Kollegen zu belasten, und den Interessen des Arbeitgebers an der verlangten Auskunft statt.
- 65 Besondere Beachtung erfordern hierbei die Regelungen des HinSchG, das beispielsweise in § 8 ein Vertraulichkeitsgebot für hinweisgebende Mitarbeiter formuliert und gestaltet. Insoweit ist vor der Befragung von oder der Informationserhebung bei (ehemaligen) Mitarbeitern jeweils zu prüfen, ob es sich um einen Hinweisgeber im Sinne von § 1 HinSchG handelt und welche Konsequenzen sich insoweit für geplante Beweis- und Informationserhebungen hieraus ergeben können.
- 66 Auch die Auskunft ehemaliger Mitarbeiter, etwa bei der Aufklärung zeitlich länger zurückliegender Sachverhalte, kann relevant werden. Deren (nachvertragliche) Auskunftspflicht ist jedoch wesentlich schwächer ausgeprägt. Nicht zuletzt aus Gründen der Vertraulichkeit – als nur *ehemalige* Mitarbeiter sind diese Auskunftspersonen letztlich Dritte – wird ihre Befragung wohl überlegt und zeitlich präzise geplant werden müssen.
- 67 Ungeachtet der rechtlichen Verpflichtung zur Auskunftserteilung wird das Ziel, möglichst viel Information zu erhalten, letztlich nur durch Kooperation mit den Mitarbeitern erreicht werden. In diesem Zusammenhang kann es sinnvoll sein, Mitarbeiteramnestien in Aussicht zu stellen.⁴⁰ Danach kann das Unternehmen Mitarbeiter, die bei der Aufklärung des Compliance-Verstoßes kooperieren und Aussagen machen, von arbeits- oder zivilrechtlichen Sanktionen verschonen.

40 Krull, in: Bay, Hdb. Internal Investigations, Kap. 3 Rn. 40 ff.

b) Notwendige Abstimmung der geplanten Untersuchungsmaßnahmen

Bei der Planung der Untersuchungsmaßnahmen ist an die notwendigen internen und externen Abstimmungen zu denken. **68**

aa) Beteiligung von Betriebsrat oder Sprecherausschuss

Die Durchführung interner Untersuchungen kann sowohl Informations- als auch Beteiligungsrechte des Betriebsrats oder des Sprecherausschusses berühren. Möglicherweise – und in der Praxis sinnvoll – existieren Betriebsvereinbarungen, die die Einbindung des Betriebsrats regeln. Diese sind unbedingt zu beachten. Ungeachtet dieser rechtlichen Gebotenheit kann die frühzeitige Kooperation mit dem Betriebsrat durchaus auch deshalb empfehlenswert sein, da dieser Einfluss auf die Mitarbeiter ausüben und daher einen wesentlichen Faktor für die Kooperationsbereitschaft der Mitarbeiter darstellen kann. **69**

bb) Abstimmung mit Ermittlungs- und Aufsichtsbehörden

Soweit interne Untersuchungsmaßnahmen parallel zu straf- oder aufsichtsrechtlichen Ermittlungen durchgeführt werden sollen, wird regelmäßig eine umfangreiche Abstimmung und Kooperation mit den Ermittlungsbehörden geboten sein, um sich nicht dem Vorwurf der Behinderung staatlicher Ermittlungen oder gar der Unterdrückung von Beweisen auszusetzen. **70**

Gerade die Befragung von (ehemaligen) Mitarbeitern im Rahmen der sogenannten Interviews sollte Gegenstand entsprechender Abstimmungen sein: Häufig kann eine (zu) frühzeitige Konfrontation von Mitarbeitern, die Schlüsselzeugen für strafrechtliche Ermittlungen darstellen, mit bestimmten Informationen und Dokumenten den Beweiswert ihrer Aussagen (deutlich) reduzieren. Diese Zeugen können dadurch aus Sicht der Ermittlungsbehörden für deren spätere Befragungen „verbrannt“ werden. Gleiches gilt für eine frühzeitige Durchführung von Interviews mit (potenziellen) Beschuldigten – hier stößt eine frühzeitige Konfrontation mit eindeutigen Erkenntnissen und Informationen selten auf die Zustimmung der Ermittlungsbehörden. **71**

Die Ermittlungsbehörden können zwar eine Befragung der Mitarbeiter nicht verbieten. Jedoch kann ein Erhalt der Gerichtsverwertbarkeit der Angaben der in geplanten Interviews zu befragenden Personen zumindest die Einhaltung der vorgegebenen Standards bei der Interview-Durchführung gebieten. Wird dies garantiert und erfolgt auch eine Abstimmung über die ermittlungsstrategische Priorisierung bestimmter Befragungen mit den Behörden, kann mit diesen häufig eine wesentlich konstruktivere und vertrauensvollere Zusammenarbeit erreicht werden. In diesem günstigen Fall wird auch die Durchführung der eigenen internen Untersuchungen häufig enorm erleichtert, weil dann nicht nur logistische Vereinbarungen mit den Behörden, zum Beispiel über einen schnellen Zugang zu asservierten Unternehmensunterlagen und Daten, sondern auch über „Schutzzonen“ für Zwangsmaßnahmen (z. B. Absehen von Durchsuchungsmaß- **72**

nahmen zur Beschlussnahme von Untersuchungszwischenergebnissen bei den externen Berufsträgern, die mit der Durchführung der internen Untersuchung betraut sind) getroffen werden können. Die Ergebnisse entsprechender Abstimmungsgespräche sind hierbei sinnvollerweise in Bestätigungsschreiben an die Ermittlungsbehörden oder gemeinsam gefertigten Besprechungsprotokollen zu „quittieren“.

c) Einrichtung eines Datenraums oder eines „Projektportals“

- 73 Die zu untersuchenden Daten müssen vollständig und gerichtsfest erfasst und es muss sichergestellt werden, dass die notwendigen Informationen dort zum richtigen Zeitpunkt zu Verfügung stehen, wo sie benötigt werden. Zweckmäßigerweise wird ein elektronischer Datenraum einzurichten sein, in den alle zu untersuchenden Dokumente und Daten eingestellt werden. Auch der über einen solchen Datenraum dokumentierbare Zugriff einzelner Personen auf die darin eingestellten Dokumente vermag in der gerichtsfesten Beweisführung eine Rolle zu spielen.
- 74 Die für das Gelingen einer internen Untersuchung wesentlichen Qualitätskriterien der **Nachvollziehbarkeit** und **Gerichtsverwertbarkeit** der gefundenen Untersuchungsergebnisse sind schon beim Anfall eines Untersuchungsumfangs, der mehrere Wochen Zeit in Anspruch nimmt, sinnvollerweise durch ein sogenanntes „Projektportal“ sicherzustellen, in dem der gesamte Hergang von Untersuchung und Ergebnisgewinnung dokumentiert wird.⁴¹
- 75 Derartige Projektportale beinhalten nicht nur die Funktion der schon angesprochenen virtuellen Datenräume, in denen das gesamte gewonnene Wissen, Dokumente, Daten und Informationen abgelegt, organisiert und dokumentiert werden. Sie dienen auch allen Projektbeteiligten als gemeinsame Werk- und Datenbank, aus der heraus auch die weitere Projektplanung bewerkstelligt werden kann. Über eine integrierte Projektdatenbank lassen sich auch Stand, Verlauf und Fortschritt der einzelnen Untersuchungsprojekte sowie der Fertigstellungsgrad der einzelnen Untersuchungsziele und -berichte in zeitlicher und personeller Hinsicht dokumentieren und nachvollziehen.
- 76 In Anbetracht der Komplexität von internen Untersuchungen, die sich auch erst in deren Verlauf etwa durch überraschend auftretende Probleme oder neue Erkenntnisse ergeben kann, wird die anfängliche Investition in ein effizientes Projektportal im Verbund mit einem integrierten Dokumenten-Management-System oftmals zu empfehlen sein. Häufig erbringt eine derartige Dokumentationslösung erhebliche Zeit- und Ressourcen-Einsparungen im weiteren Untersuchungsverlauf.

41 Vertiefend hierzu *Idler/Knierim/Waerber*, in: *Knierim/Rübenstahl/Tsambikakis*, *Internal Investigations*, Kap. 4 Rn. 127, 130.

5. Sicherung der Vertraulichkeit

Bei Festlegung von Art und Umfang der zu erstellenden Dokumentation und der Kommunikation ist zu berücksichtigen, an wen die Dokumentation gelangen soll oder kann und welche Konsequenzen sich daraus ergeben. Unbedachte, dem Zugriff Dritter ausgesetzte Kommunikation oder Dokumentation kann den Erfolg der Untersuchung gefährden bzw. zu überraschenden unerwünschten Konsequenzen für das Unternehmen oder seine Mitarbeiter führen. 77

a) Zugriffsmöglichkeiten Dritter

Im rein nationalen Kontext ist insbesondere an den Zugriff von Ermittlungsbehörden und Versicherern zu denken. Bei Bezügen des Unternehmens oder des Untersuchungsgegenstandes zum anglo-amerikanischen Rechtsraum kann darüber hinaus das Risiko bestehen, dass im Rahmen (bevorstehender) Gerichtsverfahren dem oder den Prozessgegnern Dokumente und Unterlagen umfänglich zur Verfügung gestellt werden müssen. 78

aa) Beschlagnahme durch Ermittlungsbehörden

Wenn nicht ohnehin gewollt ist, die Untersuchungsunterlagen an Ermittlungsbehörden herauszugeben, sollten sich die Untersuchungsführer bereits zu Beginn einer internen Untersuchung vergegenwärtigen, dass Ermittlungsbehörden auch gegen den Willen des Unternehmens Informationen herausverlangen und Unterlagen beschlagnahmen können.⁴² 79

Von besonderer Bedeutung ist dabei die Frage, ob und unter welchen Umständen die speziell im Rahmen der internen Untersuchung und ggf. durch die mit der Untersuchung beauftragten Anwälte angefertigten **Untersuchungsunterlagen** beschlagnahmt werden können, namentlich Interviewprotokolle, Untersuchungsberichte oder anwaltliche Gutachten zu Haftungs- oder Strafbarkeitsfragen.⁴³ Denn zum einen können die Ermittlungsbehörden diese zur Strafverfolgung einzelner Mitarbeiter oder zur Verhängung von Verbandsgeldbußen gegen das Unternehmen selbst nutzen. Zum anderen können in die Ermittlungsakten gelangte Untersuchungsunterlagen in die Hände von Privaten gelangen und diesen zur Begründung von Ansprüchen gegen das Unternehmen dienen.⁴⁴ 80

Zu unterscheiden war bisher zwischen Untersuchungsunterlagen, die sich im Gewahrsam externer Rechtsanwälte (d.h. im Bürogebäude eben dieser externen Anwälte oder in einem von diesen erstellten Extranet) befinden und Untersuchungsunterlagen, die sich im Unternehmen (beispielsweise in den Räumen der Rechtsabteilung) befinden. In der Rechtsprechung zeigte sich bis zu den sog. 81

⁴² Wettner/Mann, DSStR 2014, 655, 657 ff.

⁴³ Wettner/Mann, DSStR 2014, 655, 658 f.; LG Hamburg (HSH Nordbank), 15.10.2010, NJW 2011, 942 ff.; LG Mannheim, 3.7.2012, NSStZ 2012, 713 ff.

⁴⁴ Zu Akteneinsichtsrechten siehe Wettner/Mann, DSStR 2014, 655, 660 f.

Jones Day-Entscheidungen des BVerfG⁴⁵ eine erfreuliche praxisorientierte Tendenz zum Schutz solcher Untersuchungsunterlagen vor Beschlagnahme. Zunächst bestätigte eine Entscheidung des LG Mannheim den gesetzessystematischen Auslegungsansatz, nach dem unter Berücksichtigung des neugefassten § 160a StPO Unterlagen aus dem Mandatsverhältnis zwischen Nichtbeschuldigten (auch Unternehmen) und Rechtsanwälten, in gleicher Weise wie Verteidigungsunterlagen dem Beschlagnahmeschutz des § 97 Abs. 1 Nr. 3 StPO unterliegen.⁴⁶ Jedenfalls aber sollten Unterlagen, soweit sie *auch* zur Verteidigung des Unternehmens gegen Verbandsgeldbußen im anwaltlichen Mandatsverhältnis erstellt wurden (**Verteidigungsunterlagen**), nach einer Entscheidung des LG Braunschweig aus dem Jahr 2015 auch in den Räumen des Unternehmens vor Beschlagnahmen geschützt werden, selbst wenn zum Zeitpunkt ihrer Erstellung ein Ermittlungsverfahren gegen das Unternehmen noch nicht eingeleitet war.⁴⁷ Diese Rechtsprechung hat sich jedoch nicht etabliert, sondern ist nach der angesprochenen Entscheidung des BVerfG vielmehr als beendet anzusehen. Nach der äußerst restriktiven und rein formellen Auslegung des § 97 Abs. 1 Nr. 3 StPO durch das BVerfG in den Jones Day-Entscheidungen soll das Beschlagnahmeverbot nur noch Unterlagen aus der Beziehung des im konkreten Strafverfahren Beschuldigten mit den Zeugnisverweigerungsberechtigten schützen und diese auch lediglich dann, soweit sie ab einem Zeitpunkt entstanden sind, zu dem gegen diesen Beschuldigten ein konkreter Verdacht von Strafverfolgungsbehörden zum jeweiligen Verfahrensgegenstand bestand.⁴⁸

- 82 Die in dieser Rechtsprechung bereits kategorisch herangezogenen Grundsätze zur Bestimmung der Reichweite des Beschlagnahmeschutzes aus § 97 StPO sollten in Artikel 5 des Regierungsentwurfs des „Gesetzes zur Stärkung der Integrität der Wirtschaft“ mittels einer Änderung der §§ 97 und 160a StPO umgesetzt werden. Etwaige Rechtsunsicherheiten die vor – und ausweislich der Gesetzesbegründung auch nach – der Entscheidung des BVerfG vom 27.6.2018 bestanden,⁴⁹ sollen durch die Klarstellungen in den beiden Vorschriften ausgeräumt werden. Damit sollte Artikel 5 des Entwurfs für die im Rahmen interner Untersuchungen erstellten Unterlagen normieren, was sich bereits als allgemeingültige Interpretation der §§ 97 und 160a StPO in der aktuellen Fassung ergibt: Erkenntnisse und Unterlagen aus internen Untersuchungshandlungen vor der Einleitung eines konkreten Ermittlungsverfahrens sind in keinem Fall beschlagnahmefest. Erkenntnisse und Unterlagen aus nach Beginn eines Ermittlungsverfahrens vorgenommenen, internen Untersuchungen sind jeweils – aber nur dann beschlagnahmefrei, wenn die Untersuchungen durch das beschuldigte Unterneh-

45 BVerfG, Beschl. v. 27.6.2018 – 2 BvR 1405/17, 2 BvR 1780/17.

46 LG Mannheim, 3.7.2012, 24 – Qs 1/12; 24 Qs 2/12.

47 LG Braunschweig, 21.7.2015 – 6 Qs 116/15; in diesem Sinne bereits LG Frankfurt/M., 27.4.2004, StraFo 3004, 239.

48 BVerfG, Beschl. v. 27.6.2018 – 2 BvR 1405/17, 2 BvR 1780/17, Rn. 93–95.

49 RegE des „Gesetzes zur Stärkung der Integrität in der Wirtschaft“ v. 16.6.2020, 137. Zu den vorgeschlagenen Neuregelungen siehe auch → *Böttger*, Kap. 2 Rn. 16 ff., 143 ff.

men selbst oder dessen Verteidiger vorgenommen werden, und zwar unabhängig davon, ob sie im Gewahrsam des Unternehmens oder dessen Verteidigern aufgefunden werden. Erfolgt die interne Untersuchung nicht durch einen Verteidiger, sind die daraus entstandenen Unterlagen und Erkenntnisse stets als beschlagnahmefähig anzusehen. Gerade diese Trennung von Unternehmensverteidigung und interner Untersuchung war jedoch ein wesentlicher Kritikpunkt an dem Verbandssanktionengesetz, weshalb dieses scheiterte (siehe → Rn. 3).

bb) Herausgabe von Unterlagen an Versicherer

Bei der Art und Weise der Kommunikation und Dokumentation ist auch zu beachten, dass Versicherer des Unternehmens (etwa im Rahmen bestehender D&O-Versicherungen) ein umfangreiches gesetzliches bzw. vertragliches Auskunfts- und Belegrecht zur Aufklärung des Versicherungsfalls haben.⁵⁰ Ein Versicherer kann grundsätzlich jegliche Informationen und Unterlagen verlangen, die er zur Aufklärung des Versicherungsfalls und des Umfangs seiner Deckungspflicht für erforderlich hält.⁵¹ 83

Das Risiko des Unternehmens besteht dabei darin, dem Versicherer Informationen und Unterlagen herausgeben zu müssen, aufgrund derer der Versicherer einen Ausschluss des Versicherungsschutzes einzuwenden versucht. Bei Compliance-Verstößen wird regelmäßig der typische Vorsatzausschluss in Rede stehen, wonach die Versicherungsdeckung für Schäden aufgrund vorsätzlicher oder wissentlicher Pflichtverletzung der Organe oder Mitarbeiter ausgeschlossen ist. Gerade die Information über nachteilige Tatsachen, die zum Verlust des Versicherungsschutzes führen können, ist der Sinn und Zweck des umfangreichen Auskunftsrechts.⁵² 84

b) Begrenzung der E-Mail- und sonstigen schriftlichen Kommunikation

Die vorgenannten Zugriffsmöglichkeiten im Rahmen der internen Untersuchung zu berücksichtigen, bedeutet selbstverständlich nicht, den Ermittlungsbehörden oder Versicherern offenzulegende Informationen vorzuenthalten oder diese zu unterdrücken. Derartiges kann – und muss – gegebenenfalls strafrechtliche Konsequenzen haben bzw. den Versicherungsschutz kosten. Es bedeutet aber, dass sich die an einer internen Untersuchung beteiligten Mitarbeiter und externen Berater bewusst sein müssen, dass auch unbedachte, vorläufige oder generell auf 85

⁵⁰ Nach § 31 Versicherungsvertragsgesetz (VVG) bzw. vergleichbaren Versicherungsbedingungen.

⁵¹ BGH, 22.10.2014 – IV ZR 303/13, BeckRS 2014, 20926: „Zur Reichweite der Auskunftspflicht gilt, dass es grundsätzlich Sache des VR ist, welche Angaben er zur Ermittlung des Sachverhalts für erforderlich hält [...]. Danach erstreckt sich die Auskunftspflicht auf jeden Umstand, der zur Aufklärung des Tatbestandes dienlich sein kann [...]“.

⁵² BGH, VersR 2000, 222: „Der Zweck der Auskunftspflicht besteht im Wesentlichen darin, den VN zu zwingen, an der Aufklärung des Sachverhalts auch insoweit mitzuwirken, als es um Tatsachen geht, die zum Verlust des Versicherungsschutzes führen können“.

(subjektiver) Interpretation beruhende Einschätzungen, die sich letztlich als unbegründet erweisen können, von Dritten zum Nachteil des Unternehmens genutzt werden könnten.

- 86** Insbesondere die E-Mail-Kommunikation birgt im Hinblick auf den Vertraulichkeitsschutz erhebliche Risiken. Dies sollte generell wie insbesondere im Zusammenhang mit internen Untersuchungen allen Beteiligten bewusst gemacht werden. Für die gesamte schriftliche interne Kommunikation sowie die Kommunikation der Unternehmensvertreter mit den externen Beratern gilt: Sie sollte sich generell auf ein Minimum und inhaltlich auf reine Tatsachen beschränken. (Vorläufige) Wertungen und Interpretationen von Geschehensabläufen sollten möglichst unterbleiben.

c) Kennzeichnung und Aufbewahrung geschützter Kommunikation

- 87** In Anbetracht der Rechtsprechung zu Beschlagnahmeverboten von „der Verteidigung dienenden Unterlagen“, ist es in einem ersten Schritt notwendig, sich über eine einheitliche Markierung von „Unterlagen der Verteidigung“, sei es im Betreff einschlägiger E-Mail-Korrespondenz oder durch entsprechende Beschriftung von Aktenordnern, in denen physische Verteidigungsdokumente gesammelt werden, zu verständigen und diese zu praktizieren. Der Begriff der „Verteidigungsunterlage“ beschreibt dabei freilich eher eine *in der* oder *für die* (spätere) Verteidigung gegen Sanktionsmaßnahmen *erarbeitete* Unterlage im engeren Sinne. Er darf insoweit gerade nicht als begrifflicher Ersatz eines Aktenvernichters verstanden werden, in dem alle unangenehmen Beweisdokumente gesammelt und einem Zugriff der Ermittlungsbehörden durch die Aufschrift „Verteidigungsunterlage“ entzogen werden.
- 88** Wie bereits verdeutlicht empfiehlt sich als sicherster Aufbewahrungsort die Kanzlei der externen Rechtsanwälte, da entsprechende Unterlagen nur in deren Gewahrsam unstreitig qua Gesetzeswortlaut des § 97 Abs. 2 Satz 1 StPO Schutz vor Beschlagnahme genießen.⁵³ Belässt man Verteidigungsunterlagen in der Sphäre des Unternehmens, so empfiehlt sich, diese zumindest in einem Raum bzw. abschließbaren Behältnissen zu konzentrieren, um auf diesem Weg innerhalb des Unternehmens eine „Gewahrsamsinsel“ zu schaffen. Deren einziger Zugangsberechtigter mit Schlüsselgewalt sollte ein Justiziar des Unternehmens, vorzugsweise ein Rechtsanwalt, sein. Gegebenenfalls ist zu überlegen, dem (strafrechtlichen) externen Berater ein entsprechendes Büro mit alleiniger Schlüsselgewalt zuzuteilen und dieses entsprechend zu kennzeichnen. Die Einhaltung dieser Regeln dürfte im Rahmen von Durchsuchungsmaßnahmen auftretende Unklarheiten und die Gefahren daran geknüpfter, streitiger Rechtsmittelverfahren vermeiden.
- 89** Kommt es infolge eines Zugriffs von Ermittlungsbehörden dennoch zur Beschlagnahme oder Sicherstellung von Unterlagen, die möglicherweise privile-

⁵³ LG Mannheim, 3.7.2012, 24 – Qs 1/12, NStZ 2012, 713 ff.

gierte anwaltliche Beratungskorrespondenz verkörpern, so ist deren Asservierung zu widersprechen und die Versiegelung dieser Unterlagen zu verlangen. Auf diesem Wege bleibt zumindest sichergestellt, dass die in Rede stehenden Beratungsunterlagen erst im Beisein der Betroffenen bzw. ihrer anwaltlichen Vertreter entsiegelt werden und die Fragen ihrer Privilegierung erneut diskutiert werden können.

6. Erstellen eines Untersuchungsplans

Der Untersuchungsplan legt Reihenfolge und zeitlichen Ablauf der konkreten Untersuchungsmaßnahmen sowie die Dokumentation und Kommunikation der Untersuchungsergebnisse fest. **90**

Es empfiehlt sich, eine Liste der benötigten Dokumente und Daten zu erstellen, für deren Abarbeitung ein Mitarbeiter des Unternehmens, vorzugsweise ein Angehöriger der Rechtsabteilung oder ein Mitglied der zentralen Koordinierungsstelle, verantwortlich ist bzw. die externen Anwälte dabei unterstützt. Die Dokumenten- und Datenbeschaffung und -sichtung sowie die Interviews von (ehemaligen) Mitarbeitern müssen zeitlich aufeinander abgestimmt werden. Regelmäßig wird mit Ersterer zu beginnen sein und darauf aufsetzend bzw. in Ergänzung werden die Interviews durchzuführen sein. **91**

Der Untersuchungsplan ist „work in progress“ und im Laufe der Untersuchung fortzuschreiben oder anzupassen. Oftmals wird er zu Beginn jedenfalls in Teilen eher generisch sein und im Laufe der Untersuchung und zunehmender Sachverhaltskenntnis immer detaillierter werden. Bei der Abfassung des Untersuchungsplans ist zu beachten, dass auch dieser beschlagnahmt werden kann oder an Versicherer herauszugeben ist. **92**

V. Durchführung der internen Untersuchung

1. Allgemeine Untersuchungsgrundsätze

Wie bei der Planung sind auch bei der Durchführung der Untersuchungsmaßnahmen deren **Recht- und Verhältnismäßigkeit** sowie die **Vertraulichkeit** unbedingt zu beachten. Darüber hinaus sollte das Untersuchungsteam die folgenden weiteren Grundsätze beachten, die generell für das Funktionieren einer internen Untersuchung als probates Aufklärungsmittel wie für den Erfolg der konkreten Untersuchung von Bedeutung sind: **93**

- So sollte es selbstverständlich sein, dass **Hinweisgeber (sog. Whistleblower) von dem Unternehmen geschützt** und keinerlei Repressalien geduldet werden.⁵⁴ Sofern der Hinweisgeber die Geheimhaltung seiner Identität gegenüber weiteren Unternehmenseinheiten wünscht, sollte dies respektiert werden. Durch das 2023 in Kraft getretene HinSchG wurde der umfassende Schutz von Whistleblowern nunmehr gesetzlich verankert. Sowohl der Schutz der

⁵⁴ Moosmayer, in: Rotsch, Criminal Compliance, § 34 B Rn. 104 ff.

Identität des Whistleblowers, als auch der Schutz des Whistleblowers vor persönlichen und beruflichen Repressalien wird durch die Vorschriften des HinSchG gewährleistet. Informationen über die Identität des Whistleblowers dürfen nach § 9 Abs. 2 HinSchG grundsätzlich nur nach vorheriger schriftlicher Unterrichtung des Betroffenen unter Angabe der Gründe an Gerichte und Strafverfolgungs- sowie Verwaltungsbehörden weitergegeben werden.

- Auf der anderen Seite muss auch ein **fairer Umgang mit den Mitarbeitern** gewährleistet sein, die eines Compliance-Verstoßes verdächtig sind. Solange ein Verstoß nicht nachgewiesen ist, gilt die Unschuldsvermutung. Ziel der Untersuchung ist die Ermittlung belastender wie entlastender Tatsachen.
- Des Weiteren muss die **Unabhängigkeit der Untersuchung** sichergestellt sein. Das Untersuchungsteam hat sich daher auch im Laufe der Untersuchung stets zu vergewissern, dass keine Sachverhalte vorliegen, die die Unabhängigkeit der Mitglieder des Untersuchungsteams beeinflussen könnten (Interessenkonflikt). Sollte ein solcher (möglicher) Interessenkonflikt auftreten, muss die Koordinierungsstelle umgehend informiert werden, um nicht den Wert der gesamten internen Untersuchung zu gefährden.
- Ebenso muss das Untersuchungsteam im Verlauf der Untersuchung die bereits genannten **Eilmaßnahmen im Blick** haben (siehe → Rn. 24 ff.), um eventuelle weitere Schäden für das Unternehmen abzuwenden. Auch hierfür ist die Rückkopplung mit der Koordinierungsstelle notwendig.
- Im Hinblick auf die Verwertbarkeit der Untersuchungsergebnisse hat das Untersuchungsteam darauf zu achten, dass die Durchführung der Untersuchung hinsichtlich ihres **Umfangs und der gefundenen Ergebnisse nachvollziehbar** ist. Belege sind regelmäßig in Kopie beizufügen; eventuell vor Gericht zu verwendende Beweismittel (z.B. handschriftliche Notizen) müssen unverseht bleiben.

2. Dokumentation der Untersuchung

- 94** Welche technischen Maßnahmen über eine verlässliche Steuerung der internen Untersuchung hinaus auch deren nachvollziehbare und gerichtsverwertbare Dokumentation gewährleisten können, wurde bereits unter → Rn. 73 ff. dargestellt. Gleichwohl ist in den Fällen, in denen Budget, Untersuchungsumfang oder logistische Gründe keinen Rückgriff auf eine softwarebasierte Automation – etwa in Gestalt eines Projektportals – zulassen, umso mehr darauf zu achten, dass die Grundlagen einer inhaltlichen und chronologischen Nachvollziehbarkeit bei der Dokumentation der internen Untersuchung gesichert sind. Diese Sicherung muss neben der Benennung entsprechender Projektverantwortlicher für die Dokumentation durch eine fortlaufende, chronologisch nachvollziehbare und schriftliche Protokollierung und Registrierung
- der **Fortschritte** bei der Abarbeitung des Untersuchungsplans bzw. dessen Änderungen und Erweiterungen,

- der erhobenen, eingegangenen und ausgewerteten **Dokumente, Zwischenberichte und Protokolle**,
- der angetroffenen **Untersuchungshindernisse**,
- der **durchgeführten Tätigkeiten** der einzelnen Mitglieder des Untersuchungsteams

erfolgen.

Diese nur kursorische Aufzählung dokumentationswürdiger Untersuchungsergebnisse ist, soweit man von einer automatisierten und software-/datenbankbasierten Untersuchungssteuerung absieht, für das jeweilige Untersuchungsdesign und den gewählten Modus der Berichterstattung anzupassen und zu vertiefen. 95

3. Erhebung und Auswertung von Dokumenten

Die interne Ermittlungstätigkeit im Hinblick auf zu untersuchende Dokumente sollte sich nicht nur auf die Beschaffung und Aufarbeitung der im Untersuchungsplan benannten Dokumentation beschränken. In den Fällen durchgeführter Durchsuchungs- und Beschlagnahmemaßnahmen aufgrund parallellaufender, externer strafrechtlicher Ermittlungen ist jeweils sicherzustellen, dass ein Überblick über die einzelnen, bei den Ermittlungsbehörden lagernden Asservate gewonnen werden kann. Relevante Unterlagen für die Aufklärung des Sachverhalts sind dabei zu identifizieren und ebenfalls in die Untersuchung einzubeziehen. Nur so kann gewährleistet werden, dass die Ergebnisse der internen Untersuchung nicht durch die Ergebnisse der externen, behördlichen Ermittlungen konterkariert und somit wertlos werden. 96

Nach der Identifizierung relevanter Dokumente und Schriftstücke sind diese zunächst zu sichern, bevor sie in einem nächsten Schritt ausgewertet werden können.⁵⁵ Nach Herstellung von Duplikaten eines Dokuments und einer entsprechend sicheren (und vor unbefugtem Zugriff geschützten) Archivierung des Originals ist es im Rahmen einer ersten Auswertung oft zielführend, die Bedeutsamkeit eines Dokuments in verschiedenen Verdachts- oder Beweiswertstufen zu kategorisieren und bereits augenscheinliche Querverbindungen (etwa zu bestimmten Personen oder Ereignissen) zu vermerken. 97

Durch diese Vorarbeit werden erste Konkretisierungen des Untersuchungssachverhalts anhand „ganz wesentlicher Beweismittel“ erleichtert und die Vorbereitung von Mitarbeiter-Befragungen vereinfacht, aber auch auf einem gleichbleibenden Standard gewährleistet. 98

Beim Umgang des Untersuchungsteams mit dem erhobenen Dokumentenmaterial, aber auch mit allen anderen Informationen und Daten im Untersuchungsverlauf, ist stets darauf zu achten, das „Need to know“-Prinzip einzuhalten und 99

⁵⁵ Dies ist wiederum bedeutsam in den Fällen, in denen wichtige Dokumente den Ermittlungsbehörden zu einem späteren Zeitpunkt zu Beweis Zwecken vorgelegt werden sollen – zur gesamten Problematik *Bittmann*, in: Rotsch, Criminal Compliance, § 34 B Rn. 136.

den Adressatenkreis der jeweils erhobenen Dokumente auf ein Minimum zu beschränken. Dies dient einerseits dem durch diesen Grundsatz verfolgten Zweck einer so geringstmöglichen Stigmatisierung der Betroffenen. Andererseits wird aber auch sichergestellt, dass sich in den erhobenen Dokumenten oder Daten enthaltene brisante Informationen nicht „verselbstständigen“ und zu einer möglichen Verfälschung des Untersuchungsergebnisses führen.

4. Erhebung und Auswertung von elektronischen Daten

- 100** Die zentrale Erkenntnisquelle interner Erhebungen bilden zumeist die elektronischen Daten und insbesondere die E-Mail-Korrespondenz der vom Untersuchungsgegenstand betroffenen Mitarbeiter. Nach Klärung der schon angesprochenen, rechtlichen Vorfragen, nämlich:

- Bestehen dokumentierte, tatsächliche Anhaltspunkte, die den Anfangsverdacht einer Straftat des Mitarbeiters begründen (§ 32 Abs. 1 Satz 2 BDSG)?
- Handelt es sich um rein dienstliche oder aufgrund von Genehmigung teilprivat genutzte persönliche E-Mail-Accounts?

ist zunächst eine für die Verwertung in späteren justiziellen Verfahren maßgebliche Datensicherung zu gewährleisten, die etwa durch digitale „Versiegelung“ des Datenbestands mittels eines standardisierten „Snapshots“ bewerkstelligt werden kann.⁵⁶

- 101** Bei der Auswertung der elektronischen Daten und E-Mails steht sodann die Vorbereitung und Anwendung einer schlüssigen Suchwortliste im Vordergrund.⁵⁷ Nur so kann eine effiziente Filterung der wesentlichen Vorgänge aus dem „Kosmos der Unternehmensdaten“ erfolgen, die gleichzeitig aber auch nicht dazu führen darf, dass zum Beispiel wesentliche Inhalte einer E-Mail-Kommunikation infolge einer mangelhaften Suchwortliste übergangen werden.
- 102** Werden im Untersuchungsverlauf erhebliche Verstöße innerhalb des Unternehmens sowie gleichzeitig Lücken in der elektronischen Dokumentation festgestellt, wird häufig auch die Frage einer Identifizierung und Wiederherstellung von gelöschten Daten in bestimmten EDV-Bereichen zu erwägen sein.

5. Befragung von Mitarbeitern

- 103** Auch der Befragung von (ehemaligen) Mitarbeitern kommt insbesondere eine maßgebliche Bedeutung bei der internen Untersuchung von Sachverhalts-Konstellationen zu, die auf Basis der vorhandenen Dokumente nicht eindeutig aufzuklären sind, sondern nur vage Anhaltspunkte für ein Fehlverhalten erkennen lassen. Derartige Beweisanzeichen können durch Befragungen von Mitarbeitern erhärtet oder auch entkräftet werden. Gerade im Bereich der Durchführung von

⁵⁶ Weitere Hinweise zu den technischen Standards bei *Strecker/Reutter*, in: Knierim/Rübenstahl/Tsambikakis, Internal Investigations, Kap. 6 Rn. 26 ff.

⁵⁷ Vgl. *Grützner*, in: Momsen/Grützner, Wirtschaftsstrafrecht, 2013, 368 ff.

Interviews ist auf eine besonders strikte Einhaltung der handwerklichen Standards zu achten, zumal die entsprechende Beweisperson nach einer fehlerbehafteten Befragung „kontaminiert“ ist und nicht mehr gerichtsverwertbar zum Beweis von Untersuchungsergebnissen herangezogen werden kann.

Wie bereits geschildert ist aus arbeitsrechtlicher Sicht zunächst davon auszugehen, dass der zu befragende Mitarbeiter als Arbeitnehmer den Vertretern des Unternehmens gegenüber grundsätzlich zur Auskunft verpflichtet ist. Verweigert der Mitarbeiter die Teilnahme an einem Interview oder die Beantwortung zulässiger Fragen, sind die entsprechenden arbeitsrechtlichen Konsequenzen abzuwägen und ggfs. zu vollziehen. Auch die in Interviews spontan hervorgebrachten Forderungen von Mitarbeitern nach dem Beistand eines Rechtsanwalts oder durch einen Vertreter des Betriebsrats entbehren regelmäßig eines rechtlichen Anspruchs, worauf in sachlicher Form hinzuweisen ist. Wird trotz entsprechenden Hinweisen eine solche unberechtigte Forderung aufrechterhalten, ist im Ergebnis ebenfalls von einer Verweigerung auszugehen, deren gesamte Umstände wiederum zu protokollieren und dann zu bewerten sind. **104**

Eine rechtlich stark veränderte Ausgangslage ist jedoch gegeben, wenn die Aufklärung eines **strafrechtlich relevanten** Vorwurfs den Gegenstand der Untersuchung bildet und/oder bereits ein paralleles **behördliches Ermittlungsverfahren** zur Aufklärung des Untersuchungsgegenstands bekannt gegeben worden ist. In dieser Konstellation einer strafrechtlich relevanten Untersuchung gilt es, weitere, ganz wesentliche Regeln zu beachten, die durch den Regierungsentwurf des VerSanG präzisiert und normiert wurden: **105**

- **Sicherstellung und Garantie „fairer“ Interviews** auf Basis der niedergelegten Grundsätze samt der zugehörigen Erläuterungen der These 3 der Bundesrechtsanwaltskammer zum Unternehmensanwalt im Strafrecht,⁵⁸ (ergänzt durch die in § 17 Abs. 1 Nr. 1 RegE VerSanG formulierten, exemplarischen Anforderungen):
- die **Belehrung der Betroffenen** über ihr Recht auf Begleitung durch einen Rechtsbeistand, der gegebenenfalls durch das Unternehmen bezahlt werden sollte,
- die Einräumung des Rechts für die **Betroffenen/Befragten**, einen **anwaltlichen Beistand oder ein Mitglied des Betriebsrats zu Befragungen hinzuzuziehen**, sowie der Hinweis auf dieses Recht vor der Befragung (vgl. § 17 Abs. 1 Nr. 5 lit. b RegE VerSanG),
- der **Hinweis** an die Befragten, dass ihre **Auskünfte in einem Strafverfahren gegen sie** verwendet werden können, (vgl. § 17 Abs. 1 Nr. 5 lit. a RegE VerSanG),
- die Einräumung des Rechts für die **Betroffenen/Befragten**, die **Auskunft auf Fragen zu verweigern**, deren Beantwortung sie selbst oder einen Angehörigen im Sinne von § 52 Abs. 1 StPO der Gefahr aussetzen würden, wegen einer

⁵⁸ BRAK Stellungnahme Nr. 35/2010.

Straftat oder Ordnungswidrigkeit verfolgt zu werden, sowie der Hinweis auf dieses Recht vor der Befragung (vgl. § 17 Abs. 1 Nr. 5 lit. c RegE VerSanG),

- **keinerlei Beeinflussungen**, Täuschungen oder Einwirkung mit unlauteren Maßnahmen auf den Betroffenen während der Befragung, insbesondere keine Drohung mit arbeitsrechtlichen Konsequenzen,
- **Anfertigung einer Niederschrift** und Genehmigung derselben durch den Betroffenen auf dessen Verlangen; sowie seine entsprechende Belehrung über dieses Recht,
- Belehrung über Möglichkeiten und Grenzen in Aussicht gestellter **Amnestiemaßnahmen**,
- Belehrung über Möglichkeit der **Weitergabe ausgehändigter Dokumente** an Ermittlungsbehörden.

106 Soweit sich die internen Ermittler bei der Befragung von den Kriterien der Thesen der Bundesrechtsanwaltskammer zum Unternehmensanwalt im Strafrecht leiten lassen,⁵⁹ ist jedenfalls davon auszugehen, dass sich die erhobenen Erkenntnisse auf der sicheren Seite einer Gerichtsverwertbarkeit befinden. Allein die – berechnete – Diskussion darüber, welche strafprozessualen Standards in den Interviews einer internen Untersuchung verbindlich sind,⁶⁰ befreit den privaten Ermittler in der Praxis insoweit nicht gänzlich von der Einhaltung strafprozessualer Mindeststandards, auch wenn diese nur analog erfolgen muss, denn: ein – auch aus dem Gesamtablauf eines Interviews durchaus ableitbarer – Verstoß gegen die Selbstbelastungsfreiheit verletzt stets den Menschenwürdegehalt des allgemeinen Persönlichkeitsrechts und führt unmittelbar zu einem Beweisverwertungsverbot gemäß § 136a StPO.⁶¹

107 Während die dargestellten Vorgaben in ihrem Wirkungsumfang zu überprüfen und ihre Einhaltung sicher zu stellen ist, muss andererseits auch die strategische Wirksamkeit und Effizienz der Befragung vorbereitet und gewährleistet werden. Hier gilt der Grundsatz, dass zunächst ein Überblick über die vorzuhaltenden Dokumente und Informationen hergestellt werden sollte, die dann in die entsprechende Vorbereitung von Interviews durch Formulierung von Vorhalten und Fragenkatalogen einfließen sollte. Grundsätzlich wird man „tatferne“ Zeugen vor „tatnahen“ möglichen Mittätern oder Teilnehmern befragen und mit der Befragung von Zeugen beginnen, die in der Hierarchie des Unternehmens eher niedriger angesiedelt sind.

6. Auswertung und Aufarbeitung der Untersuchungsergebnisse

108 Die inhaltliche Aufarbeitung der – gemäß dem fortgeschriebenen Untersuchungsplan erhobenen – Untersuchungsergebnisse erfolgt idealerweise zunächst fortschreitend durch Anfertigung und Rückgriff auf Zwischenberichte über we-

⁵⁹ BRAK Stellungnahme Nr. 35/2010.

⁶⁰ *Szesny*, BB 45/2011, VI/VII.

⁶¹ *Eisenberg*, Beweisrecht der StPO, Rn. 396.

sentliche Erhebungen von Informationen. Erreicht die Untersuchung das Stadium der „Berichtsreife“, ist eine zusammenfassende Aufarbeitung des untersuchten Sachverhalts auf der Grundlage aller Zwischenberichte vorzunehmen, wodurch alle Ergebnisse in die Schlussberichterstattung zusammengeführt werden. Sowohl Zwischen- als auch Schlussberichterstattung unterliegen grundlegenden Qualitätsanforderungen, die nicht nur den Inhalt, sondern auch die Struktur von dessen Aufbereitung betreffen. Beachtliche Kriterien sind insbesondere:

- **Inhaltliche Zuverlässigkeit der Berichterstattung** setzt neben Fehlerfreiheit und Vollständigkeit vor allem auch voraus, dass frei von Wertungen und ausgewogen berichtet wird.
- **Struktur und Relevanz der berichteten Informationen** sollten in erster Linie eine effiziente und verständliche Beantwortung der vereinbarten Fragestellungen des Untersuchungsauftrags herbeiführen; unwichtige Informationen sollten zwar auch evaluiert und bewertet werden, sind dann jedoch aus der Berichterstattung herauszuhalten. Wesentliche Vorgaben und Beschränkungen inhaltlicher Art sind an die Frage geknüpft, ob es sich um einen freiwilligen Bericht oder einen Pflichtbericht gemäß gesetzlicher Vorgaben handelt.
- Ein **Rückgriff auf Erkenntnisquellen standardisierter Art und Güte** sollte in der Berichterstattung jeweils vorausgesetzt sein, Abweichungen hiervon sind anmerkungsbedürftig und entsprechend zu kennzeichnen. Vorausgesetzt wird etwa der Rückgriff auf explizit benannte Beweismittel und Beweisdokumente, Vermerke, Statusberichte, Sitzungs- und Interview-Protokolle. Soweit zusammenfassende Erkenntnisse aus Mitarbeiter-Befragungen präsentiert werden, ist beispielsweise darauf zu achten, dass die berichtete Information nicht nur von einer befragten Person stammt, sondern durch weitere Befragte bestätigt wurde – anderenfalls ist dies durch eine Anmerkung im Bericht zu kennzeichnen.
- Die **Erfüllung der Anforderungen an einen Untersuchungsbericht**⁶² setzt unter Beachtung der vorgenannten Kriterien die Beschreibung (1) der Auftragsdurchführung, (2) der erlangten und ausgewerteten Informationsquellen und Beweismittel, (3) der Methodik ihrer Auswertung; (4) eine Darstellung der Beweisergebnisse, (5) deren Würdigung im Hinblick auf bestimmte Vorgänge und/oder das Verhalten bestimmter Unternehmensmitarbeiter sowie (6) erster Handlungs- und Entscheidungsempfehlungen voraus.

Im Übrigen sind für die Ausgestaltung des Abschlussberichts neben dem Untersuchungsauftrag und dessen Umsetzung nach Maßgabe des Untersuchungsplans noch weitere Regeln und Grenzen maßgeblich, die sich aus dem Adressatenkreis des Berichts ergeben. In diesem Zusammenhang ist zu bedenken, ob lediglich an

109

⁶² Idler/Knierim/Waerber, in: Knierim/Rübenstahl/Tsambikakis, Internal Investigations, Kap. 4 Rn. 172 ff.

den Auftraggeber Bericht erstattet wird oder auch eine Berichterstattung an die Behörden erfolgen soll oder gar muss.⁶³

- 110** Ist absehbar, dass der Abschlussbericht (auch) an eine Behörde übergeben wird, empfiehlt sich dringend, *nur eine* Berichtsfassung zu erstellen und die Berichtsinhalte nicht etwa für unterschiedliche Adressaten abzuschichten.⁶⁴ Letzteres wird von Behörden im Falle der Entdeckung unterschiedlicher Versionen als Aufkündigung einer etwa zugesagten Kooperation oder gar als Verdunklungshandlung bewertet.
- 111** Problematisch ist jeweils die Behandlung von Informationen, die das Untersuchungsteam vertraulich oder rechtswidrig erlangt hat. Erstere Informationen sollten grundsätzlich ohne Quellenangabe als „Erkenntnis“ des Untersuchungsteams in zusammengefasster Form wiedergegeben werden. Von der Verwendung der letztgenannten Informationen, die durch illegale Beweiserhebungen erlangt wurden, ist im Grundsatz abzuraten, da sie das Risiko beinhaltet, dass der gesamte Bericht das Qualitätskriterium der „Gerichtsverwertbarkeit“ verfehlt.

VI. Fazit

- 112** Sobald Anzeichen für einen Compliance-Verstoß im Unternehmen zutage treten, die eine interne Untersuchung nahelegen oder zumindest als probates Mittel erscheinen lassen, ist eine frühzeitige Beratung zur Entscheidung über die Frage(n), ob eine Untersuchung – und ggfs. mit welchem Umfang, Ziel und Auftrag – durchgeführt werden sollte, angezeigt.
- 113** Dies ergibt sich unter anderem daraus, dass die später durch Dritte nachzuvollziehende Entscheidung, ob eine interne Untersuchung entweder nicht, oder aber mit einem bestimmten Ziel und Auftrag durchgeführt wird, durch ein Hinzutreten staatlicher Behörden unumkehrbare Pflichten und Konsequenzen auslösen kann, die zunächst nicht vollständig erkennbar sind. Auch die Verabredungen, die mit den Betroffenen einer internen Untersuchung getroffen werden, können solche irreversiblen Konsequenzen haben.
- 114** Das gesamte Management einer internen Untersuchung muss berücksichtigen, dass in deren gesamten Verlauf nicht nur „dingliche Sicherungen“ von Daten und Beweismitteln vorzunehmen sind, sondern stets auch ein sensibler Umgang mit Informations- und Berichtswegen und der Zusammensetzung des Untersuchungsteams zu beachten ist. Dabei spielen wiederum rechtliche Aspekte des Geheimnisschutzes und der Unternehmenshierarchie eine ganz maßgebliche Rolle. Diese sowie arbeits- und datenschutzrechtliche Gesichtspunkte wirken sich in besonderer Weise auf die Erhebung personaler Informationsquellen – etwa bei der Befragung (ehemaliger) Mitarbeiter oder Auswertung deren individueller Korrespondenz – aus.

⁶³ Grützner, in: Momsen/Grützner, Wirtschaftsstrafrecht, 2013, 422.

⁶⁴ Idler/Knierim/Waerber, in: Knierim/Rübenstahl/Tsambikakis, Internal Investigations, Kap. 4 Rn. 169 f.

Einerseits ist im Hinblick auf die möglicherweise später geforderte Herausgabe von Unterlagen und Informationen an Ermittlungsbehörden oder (D&O-)Versicherer an eine bewusste Zurückhaltung bei der schriftlichen Dokumentation und Kommunikation sowie – angesichts möglicher Beschlagnahmen – an die Kennzeichnung und Gewahrsamskontrolle geschützter Unterlagen zu denken. Andererseits sind Untersuchungsteams mit Blick auf die Verwertbarkeit der Untersuchungsergebnisse stets gehalten, ihre Untersuchungsführung und Ergebnisfindung nachvollziehbar und transparent zu halten. Letzteres setzt eine möglichst vollständige, wertungsfreie und ausgewogene Dokumentation – nicht nur der Fortschritte, sondern auch der Hindernisse – im internen Untersuchungsablauf bis zu einem entsprechenden Abschlussbericht voraus. **115**

Das „gute“ Management interner Untersuchungen muss vielfältigen rechtlichen und praktischen Anforderungen gerecht werden. Eine intensive Planung, welche die denkbaren „Überraschungen“ antizipiert, und eine fachkundige Durchführung sind unerlässlich. **116**

Teil 2

Übergreifende Themen und Herausforderungen

Abschnitt 2.1

Risiko und Governance

9. Kapitel

Risiko- und Chancenmanagement – Erfolgsfaktoren für eine wirksame Umsetzung

I. Corporate Governance und das Management von Chancen und Risiken

1. Grundlagen und Einführung

Die Zukunft ist kein Spiegel der Vergangenheit. Daher sollte man sich bei der Analyse neuer Risikoszenarien nicht auf einen Blick in den Rückspiegel verlassen. Aus der Risikoforschung ist seit langem bekannt, dass Menschen systematisch die mitunter „schmerzhaften“ Wirkungen von Extremereignissen unterschätzen.¹ Die Gründe hierfür sind einfach und schlicht: Wir denken in schlüssigen Geschichten, verknüpfen Fakten zu einem stimmigen Bild, nehmen die Vergangenheit als Modell für die Zukunft. So schaffen wir uns eine Welt, in der wir uns zurechtfinden. Aber die Wirklichkeit ist anders: chaotisch, komplex, überraschend und häufig unberechenbar. Oftmals ist für diese Fälle die Vergangenheit ein sehr schlechter Berater und führt zu einer eingeschränkten und vernebelten Sicht. Auch ein Autofahrer steuert sein Gefährt nicht über einen Blick in den Rückspiegel. Der Erkenntnisgewinn ist gering, denn potenzielle zukünftige Szenarien werden so ausgeblendet.

Eine seriöse Risikobewertung sowie die Analyse sinnvoller präventiver oder reaktiver Maßnahmen bedingt einen evidenzbasierten und wissenschaftlichen Diskurs sowie eine interdisziplinäre Risikoanalyse, basierend auf Fakten sowie fundierten Methoden jenseits „gefühlter Wahrheiten“ oder ideologischer Weltbilder. Wenn dann scheinbar unvorhersehbar ein ungewünschtes Szenario eintritt, wird schnell der „Schwarze Schwan“² aus dem Hut gezaubert. „Das kann-

1 Vgl. hierzu vertiefend *Kahneman*, Thinking, Fast and Slow.

2 Bevor Australien entdeckt wurde, waren die Menschen in der Alten Welt überzeugt, alle Schwäne seien weiß. Diese Überzeugung war unanfechtbar, da sie durch die empirische Evidenz anscheinend völlig bestätigt wurde. Als der erste schwarze Schwan gesichtet wurde, wurde das bisherige Gedankengebäude schwer erschüttert. Die Schwarze-Schwan-Illustration veranschaulicht eine schwerwiegende Beschränkung bei unserem Lernen durch Beobachtung oder Erfahrung und die Zerbrechlichkeit unseres (historischen) Wissens. Da die meisten Beobachter

ten wir nicht wissen!“ heißt es dann. Der „Schwarze Schwan“ ist ein Symbol für Ereignisse, die als völlig unwahrscheinlich gelten und gänzlich überraschend eintreten. Doch bei genauerem Hinsehen stellt sich heraus, dass der scheinbar „schwarze Schwan“ nur ein schmutziger weißer Schwan war. Man hat schlicht und einfach Frühwarnindikatoren ausgeblendet, diese nicht verstanden oder nicht ernstgenommen – da sie beispielsweise nicht in das eigene Weltbild passen. Der „schwarze Schwan“ wird zu einer Entschuldigung für die eigene Inkompetenz, Risikoblinkheit und Risikoignoranz. So wird eine „[...] vermeintliche Unvorhersehbarkeit von Ereignissen nur allzu oft als Ausrede für fehlendes Risikomanagement hergehalten [...]. Auf diese Weise wird aus menschlichem Versagen höhere Gewalt, aus Leichtsinn Pech, aus Verantwortungslosigkeit Schicksal“,³ so *Nikolaus von Bomhard*, Ex-Vorstandsvorsitzender des globalen Rückversicherers Munich Re.

- 3 Der im Jahr 2010 verstorbene französische Mathematiker *Benoît B. Mandelbrot* kritisierte immer wieder den unprofessionellen Umgang mit Risiken und Unsicherheit in Unternehmen. Basierend auf seinen Analysen sind die meisten Risikomanagementsysteme blind für Extremereignisse. *Mandelbrot* wies darauf hin, dass Risiken falsch gemessen werden und schmerzhaftes „Worst case“-Szenarien ausgeblendet würden: „Jahrhunderte hindurch haben Schiffbauer ihre Rümpfe und Segel mit Sorgfalt entworfen. Sie wissen, dass die See in den meisten Fällen gemäßigt ist. Doch sie wissen auch, dass Taifune aufkommen und Hurrikane toben. Sie konstruieren nicht nur für die 95 % der Seefahrtstage, an denen das Wetter gutmütig ist, sondern auch für die übrigen 5 %, an denen Stürme toben und ihre Geschicklichkeit auf die Probe gestellt wird. Die Finanziere und Anleger der Welt sind derzeit wie Seeleute, die keine Wetterwarnungen beachten.“⁴
- 4 So liefert uns die durch das Coronavirus SARS-CoV-2 verursachte COVID-19-Pandemie ein sowohl eindrückliches als auch schmerzhaftes Beispiel für Risikoblinkheit und fehlende Risikokompetenz bei Verantwortlichen im Staat sowie bei vielen Unternehmenslenkern. Eine Pandemie war ein Ereignis, das mit Gewissheit irgendwann eintreffen wird. Die einzige Unbekannte war der genaue Zeitpunkt – aber eben gerade nicht das Ereignis. Und Risikomanagement sollte genau solche Stressszenarien antizipieren und Maßnahmen definieren, damit Unternehmen in der stürmischen See nicht untergehen. Viele Akteure haben

über den eigenen Tellerrand nicht hinausschauen, war für sie klar, dass alle Schwäne weiß sind. Es lag schlichtweg außerhalb der eigenen Vorstellungskraft, dass schwarze (Trauer-)Schwäne in allen Bundesstaaten Australiens vorkommen, sowohl auf dem Festland wie auch in Tasmanien. Der Trauerschwan ist sogar das offizielle Wappentier Westaustraliens und wird in der Staatsflagge dargestellt. Vgl. hierzu *Romeike/Stallinger*, Risiko Manager, 06/2014, 1, 7–13.

3 *Bomhard*, Schwarzer Schwan und Vogel Strauss, FAZ v. 1.4.2016.

4 Vgl. vertiefend *Mandelbrot*, Fraktale und Finanzen – Märkte zwischen Risiko, Rendite und Ruin, sowie *Romeike*, Beautiful, Colourful Risk: Benoît B. Mandelbrot – Remembering the Father of Fractals, in: Union Investment Institutional (Hrsg.), The Measurement of Risk, S. 197–207.

schlicht und einfach die Wetterwarnungen ignoriert und es versäumt, Rettungsboote zu bauen. Denn Rettungsboote werden nicht erst im Sturm gebaut.

Infektionsrisiken und Pandemien bereiten Wissenschaftlern sowie weitsichtigen und seriös arbeitenden Risikomanagern seit vielen Jahren schlaflose Nächte (wie übrigens auch das Szenario eines „Black Outs“ sowie der Eskalation geopolitischer Konflikte). Der exzellente Statistiker, Risikoforscher und Professor für internationale Gesundheit, *Hans Rosling*, hat bereits vor vielen Jahren auf die fünf globalen Risiken hingewiesen, die uns beunruhigen sollten. Als Top-1-Risiko beschreibt er in seinem Buch „Factfulness“ das Risiko einer globalen Pandemie.⁵ Nicht selten muss die vermeintliche Unvorhersehbarkeit von Ereignissen als Ausrede für fehlendes Risikomanagement herhalten.

Wirksames Risikomanagement konzentriert sich auf „Überraschungen“ in der Zukunft und versucht daher „aus der Zukunft zu lernen“.

Doch manchmal lohnt ein Blick zurück in die Vergangenheit, um den Blick für das Zukünftige zu schärfen.⁶ Risikomanager und Unternehmenslenker können über die Erfolgsfaktoren eines wirksamen Risikomanagements einiges aus der Geschichte lernen – denn Risikomanagement ist nicht erst eine Erfindung unserer Zeit.

2. Die Odyssee und der Umgang mit Risiken

Bereits der Zusammenbruch von Troja mit Hilfe des Trojanischen Pferdes – beschrieben in den ältesten und einflussreichsten Dichtungen der abendländischen Literatur, der Odyssee – lehrt uns viel über funktionierendes und auch fehlerhaftes Risiko- und Chancenmanagement. Cassandra war durch ihre hellseherischen Fähigkeiten die perfekte Risikomanagerin; allerdings fehlte bei den Bürgern Trojas eine gelebte Risikokultur. Sie glaubten schlicht und einfach den Risikoanalysen von Cassandra nicht.⁷ Auch in der heutigen Praxis ist es wichtig, dass ein Risikomanagement (und viele weitere präventive Systeme, wie Compliance Management oder Qualitätsmanagement) auf einer gelebten Risiko- und Fehlerkultur basiert. Wenn diese nicht existiert, ist Risikomanagement nicht wirksam.

5 Vgl. *Rosling*, *Factfulness*: Ten Reasons We're Wrong About the World – and Why Things Are Better Than You Think.

6 Vgl. hierzu vertiefend *Romeike*, *Risikomanagement*, S. 13 ff., sowie *Romeike*, *Grundlagen des Risikomanagements in der Versicherungsbetriebslehre*, in: *Romeike/Müller-Reichart*, *Risikomanagement in Versicherungsunternehmen*, S. 53 ff.

7 Der Gott Apollon, der Cassandra liebte, schenkte ihr die Gabe der Weissagung. Da jedoch Cassandra die Liebe Apollons nicht erwiderte, machte er die Gabe wirkungslos und verdamnte sie dazu, dass niemand ihren (richtigen) Prophezeiungen Glauben schenken solle. Und so passierte es dann auch: Cassandra sagte die Zerstörung Trojas voraus und keiner interessierte sich dafür. Die siegestrunkenen Trojaner schenken ihr kein Gehör und zogen das hölzerne Pferd in ihre Stadt. Daher spricht man auch heute noch von einem „Kassandraruf“, wenn eine Warnung ungehört verhallt.

Und wenn Risikomanagement nicht wirksam ist, kann anschließend nur noch ein reaktives und situatives Krisenmanagement die Schmerzen lindern.

- 9 Nach dem Sieg über Troja begab Odysseus sich mit seinen zwölf Schiffen auf die Heimreise. Der schlaue Sagenheld und chancen- und risikoorientiert denkende Seefahrer erkannte auf seiner Reise proaktiv und präventiv (er hatte eine gute Sensorik für Frühwarnindikatoren), dass Wasser und Nahrung an Bord langsam knapp wurden. So beschlossen Odysseus und seine Gefährten, auf der (gefährlichen) Insel der Kyklopen (oder auch Zyklopen in deutscher Sprache) zu landen. Die Kyklopen waren einäugige Riesen, die auf der Insel als Schafhirten lebten. Angekommen auf der Insel legte sich Odysseus mit dem größten der Zyklopen, Polyphem, an. Die Konsequenz war der Eintritt eines Risikos, d. h. einer nicht überraschenden Ziel- oder Planabweichung: Er wird postwendend mit seinen Männern in eine Höhle gesperrt. Dort nun beginnt Polyphem, die ersten Männer aus Odysseus' Mannschaft genüsslich zu verspeisen. Doch Odysseus verzagt nicht, sondern stellt sich dem Riesen mit dem Namen „Outis“ vor (ein im Deutschen nicht wiederzugebendes Wortspiel, da „Outis“ zugleich „Odysseuschen“ und „Niemand“ bedeutet).
- 10 Schließlich kann er ihn (im Sinne einer aktiven Risikosteuerung) in ein Gespräch verwickeln und betrunken machen. Mit einem glühenden Holzpfeil stechen sie dem schnarchenden Polyphem danach das einzige Auge aus. Dieser ruft sofort die anderen Kyklopen mit den Worten „Niemand hat mich geblendet!“ zu Hilfe. Doch alle halten ihn für verrückt und kümmern sich nicht weiter um ihn. Am nächsten Morgen rollte der geblendete Riese Polyphem den Stein zur Seite und blieb vor dem Höhleneingang sitzen, um Odysseus und seine Männer bei einem Fluchtversuch zu erwischen. Als nun seine Widder ins Freie traten, tastete er nur deren Rücken ab, während Odysseus und seine Männer sich an deren Bauchfell festklammerten (wieder ein Beispiel für eine präventive Risikosteuerung). Diese weitsichtige Chancen- und Risikobewertung und präventive Risikosteuerung rettete ihnen das Leben. So zog Odysseus weiter zur Insel der Sirenen. Auch hier beweist er, dass er ein erfolgreicher und präventiv agierender Chancen- und Risikomanager ist.
- 11 Als er seine Fahrt vorbei an den liebeizenden, aber zugleich gefährlichen Sirenen plante, befolgte er den Rat der Zauberin Kirke. Die schlug ihm und seinen Männern eine Art „Verhaltenskodex“ (heute würden Unternehmen von einem „Code of Conduct“ sprechen) vor, um mit seinem Schiff die gefürchteten Sirenen zu passieren.
- 12 Die Chancen auf ein weiteres Leben während und die Risiken des Getötetwerden minimierend, verstopften sich die Männer die Ohren mit Wachs. Somit konnten diese die betörenden Gesänge der Sirenen nicht hören. Odysseus selbst ließ sich an den Mast des Schiffes binden, damit er den Lockungen der Sirenen nicht erliegen konnte.

Im Grunde handelt es sich bei dem von *Homer* beschriebenen Abenteuer des Odysseus um die Schablone für ein praxisnahes, präventives und effektives Risikomanagement. Im Klartext heißt das: Was uns Odysseus' Abenteuer im speziellen Fall lehrt, ist ein Chancen- und Risikomanagement par excellence. Die beste Route wählen. Chancen und Risiken in Abstimmung mit Kirke, als eine Art Analystin fungierend, im Vorfeld abwägen, um die richtigen Schlüsse zu ziehen und vorausschauend zu agieren. Unternehmen und auch politische Akteure könnten aus dieser scheinbar simplen Geschichte rund um den Kapitän sowie Risikomanager Odysseus für das Hier und Jetzt lernen. **13**

3. Risikomanagement als zentraler Erfolgsfaktor

Die Fähigkeit, Chancen und Gefahren (Risiken) adäquat abzuwägen, ist ein zentraler Erfolgsfaktor des unternehmerischen Erfolgs, aber auch des staatlichen Handelns. Der Erfolg eines Unternehmens hängt wesentlich von der Qualität der Entscheidungen der Unternehmensführung ab.⁸ Gleiches gilt für das politische Handeln, etwa bei der Umsetzung der drei zentralen Funktionen eines Staates für seine Bürger: Sicherheit, Wohlfahrt und Legitimität/Rechtsstaatlichkeit. **14**

In diesem Kontext zählt Risikomanagement zu den originären Leitungsaufgaben eines jeden Geschäftsleiters und ist fester Bestandteil einer guten „Corporate Governance“, d. h. den Grundsätzen einer „guten“ Unternehmensführung, weil jede unternehmerische Tätigkeit direkt mit Unsicherheit und damit den hieraus entstehenden Chancen und Risiken zusammenhängt.⁹ Bei jeder unternehmerischen Entscheidung geht es schlussendlich um das Abwägen von Chancen und Risiken. In diesem Kontext spielen vor allem der Risikoappetit sowie die Risikoakzeptanz des Entscheiders im Wechselspiel mit der vorhandenen Risikotragfähigkeit des Unternehmens eine wesentliche Rolle. **15**

4. Überblick über aktuelle regulatorische Entwicklungen

Die Anforderung an das Risikomanagement deutscher Unternehmen wurde im Jahr 2021 durch zwei Gesetze, nämlich das StaRUG (Unternehmensstabilisierungs- und -restrukturierungsgesetz)¹⁰ und das FISG (Finanzmarktintegritätsstärkungsgesetz),¹¹ präzisiert und erweitert. Bisher bezogen sich die gesetzlichen Anforderungen, die auch die Abschlussprüfer betrachtet haben, primär auf die Risikofrüherkennung und nicht auf weitere Aspekte eines umfassenden Risikomanagements, wie die Risikobewältigung. Mit dem am 1.1.2021 in Kraft getretenen StaRUG wird daher beispielsweise die Geschäftsleitung von Aktiengesell- **16**

8 Vgl. hierzu vertiefend *Romeike/Hager*, Erfolgsfaktor Risikomanagement 4.0: Methoden, Beispiele, Checklisten – Praxishandbuch für Industrie und Handel, sowie *Gleißner*, Risiko Manager 1/2019, 28–35.

9 Zum Zusammenhang zwischen Risiko- und Compliance-Management siehe → *Schulz*, Kap. 1 Rn. 60 ff.

10 BGBl. I 2020, S. 3256.

11 BGBl. I 2021, S. 1534.

schaften und GmbHs verpflichtet, bei Bedarf „geeignete Maßnahmen“ der Bestandssicherung durchzuführen. Empirische Studien zeigen nämlich, dass ein Großteil der deutschen Unternehmen die gesetzlichen Anforderungen aus den §§ 91 und 93 AktG nicht erfüllt, obwohl die Abschlussprüfer keine „schwerwiegenden Mängel“ aufzeigen: So werden beispielsweise mögliche „bestandsgefährdende Entwicklungen“ im Sinne § 91 AktG infolge von Kombinationseffekten von Einzelrisiken mangels Risikoaggregation oft nicht erkannt. Die Defizite im Risikomanagement resultieren insbesondere auch daher, dass die Abschlussprüfer die Methoden des Risikomanagements (anders als Prozesse und Organisationen) kaum analysieren.¹² Die Defizite resultieren auch daher, dass manche Aufsichtsräte durch den Vorstand nur unzureichend über die Risikolage und die Qualität des Risikomanagements informiert werden.

- 17 Am 1.7.2021 ist zudem das FISG (2021) in Kraft getreten. Ausgelöst durch den „Fall Wirecard“¹³ soll durch das Gesetz insbesondere eine Stärkung der internen Kontroll- und Risikomanagementsysteme börsennotierter deutscher Aktiengesellschaften erreicht werden. Des Weiteren ergeben sich aus dem Gesetz zur Stärkung der Finanzmarktintegrität (FISG) neue Anforderungen bezüglich der Unabhängigkeit der Abschlussprüfer.

5. Krisenfrüherkennung gemäß Unternehmensstabilisierungs- und -restrukturierungsgesetz (StaRUG)

- 18 Das StaRUG betrifft neben Aktiengesellschaften auch andere juristische Personen, insbesondere GmbH.¹⁴ Mit neuen gesetzlichen Regelungen zum sogenannten Restrukturierungsplan sollen mehr Möglichkeiten für Unternehmen in einer Krise geschaffen werden, diese Krise ohne eine Insolvenz zu bewältigen. Das StaRUG ist aber nicht nur relevant für Unternehmen in der Krise, sondern für alle Unternehmen, weil es auch Anforderungen an die Krisenfrüherkennung und damit das Risikomanagement formuliert.
- 19 So ist in § 1 (Krisenfrüherkennung und Krisenmanagement bei haftungsbeschränkten Unternehmensträgern) des StaRUG definiert:

„Die Mitglieder des zur Geschäftsführung berufenen Organs einer juristischen Person (Geschäftsleiter) wachen fortlaufend über Entwicklungen, welche den Fortbestand der juristischen Person gefährden können. Erkennen sie solche Entwicklungen, ergreifen sie geeignete Gegenmaßnahmen und erstatten den zur Überwachung der Geschäftsleitung berufenen Organen (Überwachungsorganen) unverzüglich Bericht.“

12 Vgl. vertiefend *Köhlbrandt/Gleißner/Günther*, Corporate Finance, Heft Nr. 07-08/2021, 248–258 sowie *Link/Scheffler/Flath/Oehlmann/Dommers*, Controller Magazin, Heft 2/2021, 54–61.

13 Vgl. *Velte/Eulerich*, ZIR, 56. Jg., Heft 2/2021, S. 64–69.

14 Vgl. *Gleißner/Romeike*, Der Aufsichtsrat 01/2022, 2–4.

Der erste Satz entspricht den Anforderungen des § 91 Abs. 2 AktG, demzufolge Systeme zur Früherkennung von „bestandsgefährdenden Entwicklungen“ einzurichten sind. Schon aus den Erläuterungen zum KonTraG¹⁵ ist bekannt, dass die Krisenfrüherkennung ein Risikofrüherkennungssystem erfordert (siehe beispielsweise hierzu IDW PS 340 n. F.).¹⁶ Dieses soll durch Risikoanalysen aufzeigen, welcher „Grad der Bestandsgefährdung“ sich aus den aggregierten Risiken und dem Risikodeckungspotenzial (RDP) ergibt. Da sich „bestandsgefährdende Entwicklungen“ meist aus Kombinationseffekten mehrerer Einzelrisiken ergeben, ist eine Risikoaggregation erforderlich.

Bestandsgefährdungen ergeben sich in der Praxis aus einer Gefahr der Illiquidität. Der Begriff der drohenden Zahlungsunfähigkeit wurde im StaRUG modifiziert. Von einer drohenden Zahlungsunfähigkeit wird (spätestens) ausgegangen, wenn die Durchfinanzierung des Unternehmens nicht mit überwiegender Wahrscheinlichkeit in den nächsten 24 Monaten gewährleistet ist. Zur Beurteilung der drohenden Zahlungsunfähigkeit ist damit eine integrierte Unternehmensplanung mit zugehöriger Liquiditätsprognose erforderlich.¹⁷

In diesem Zusammenhang sei darauf hingewiesen, dass das StaRUG über bisherige gesetzliche Anforderungen aus dem KonTraG hinausgeht.¹⁸ Die Geschäftsleiter werden nun mit § 1 StaRUG verpflichtet, „geeignete Gegenmaßnahmen“ zu ergreifen, wenn eine schwere, also bestandsgefährdende, Krise droht. Es wird also eine Planung von Gegenmaßnahmen und eine „unternehmerische Entscheidung“ zu Krisenbewältigungsmaßnahmen gefordert.

Gleichzeitig mit der Initiierung von Gegenmaßnahmen ist gemäß § 1 StaRUG das Überwachungsgremium, also bei einer Aktiengesellschaft der Aufsichtsrat, zu informieren. Diese Information sollte neben einer Einschätzung der Gefährdungslage auch die von der Geschäftsleitung vorgesehenen „geeigneten Gegenmaßnahmen“ enthalten und deren Wirksamkeit erläutern (§ 14 StaRUG).¹⁹ Aufgrund der Bedeutung sind Entscheidungen über „geeignete Gegenmaßnahmen“, bis hin zur Entscheidung über einen Restrukturierungsplan, als „unternehmerische Entscheidung“ (§ 93 AktG) anzusehen. Erforderlich ist hierfür eine Entscheidungsvorlage, die insbesondere über bestehende Handlungsoptionen und die mit der Entscheidung verbundenen Veränderungen des Risikoumfangs – speziell des Insolvenzrisikos – informiert. In der Regel wird die „unternehmerische Entscheidung“ über diese Maßnahmen aufgrund ihrer großen Bedeutung unter dem Vorbehalt der Zustimmung durch den Aufsichtsrat gesetzt („unternehmerische Entscheidungen unter Vorbehalt“). Ab welchem Grad der Gefährdung des Unternehmens Gegenmaßnahmen zu initiieren sind und der Aufsichtsrat zu in-

15 Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ist ein umfangreiches Artikelgesetz, das am 1.5.1998 in Kraft getreten ist.

16 Vgl. hierzu vertiefend *Gleißner/Romeike*, Der Aufsichtsrat, Heft 04/2020, 55–57.

17 Vgl. *Gleißner/Romeike*, Der Aufsichtsrat 01/2022, 2–4.

18 Zur Vertiefung vgl. *Gleißner/Nickert/Romeike*, Board 01/2024, 22–24.

19 Vgl. *Nickert/Nickert*, GmbHR, Heft 8 (April 2021), 401–413.

formieren ist, ist im Gesetz nicht explizit festgelegt. Der Schwellenwert sollte daher vom Aufsichtsrat festgelegt werden.

- 24** Eine wichtige Implikation aus § 1 StaRUG ist, dass das Gesetz nun alle haftungsbegrenzten Gesellschaften, und damit speziell auch Tochtergesellschaften von Konzernen und in der Rechtsform einer GmbH, anspricht. Die Geschäftsführer solcher Tochtergesellschaften sind nun eigenständig verantwortlich, durch eine Risikoanalyse und Risikoaggregation mögliche „bestandsgefährdende Entwicklungen“ aufzuzeigen. Erreicht werden soll so eine bessere Verankerung des Risikomanagements in den Tochtergesellschaften, da nun die Geschäftsleiter ein Eigeninteresse daran haben, sich mit den für ihre Gesellschaften relevanten Risiken zu befassen.
- 25** Durch §§ 32 und 43 StaRUG und § 57 StaRUG wurden zudem Pflichten und Haftung der Organmitglieder erweitert. Im Krisenfall ist nun explizit auf die Wahrung der Interessen der „Gesamtheit der Gläubiger“ zu achten. Daraus ergibt sich eine Erweiterung der Innenhaftung von Geschäftsleitern, die nun potenziell auch für einen durch ihr Fehlverhalten den Gläubigern entstandenen Schaden unmittelbar haften.

6. FISG fordert Internes Kontrollsystem und Risikomanagementsystem

- 26** Mit dem am 20.5.2021 vom Deutschen Bundestag verabschiedeten Finanzmarktintegritätsstärkungsgesetz (FISG) ergeben sich neue Anforderungen an die Abschlussprüfung, beispielsweise im Hinblick auf die Prüferrotation, und den Aufsichtsrat.²⁰ § 100 Abs. 2 AktG fordert zudem nun zwei Finanzexperten im Aufsichtsrat bzw. dessen Prüfungsausschuss bei Unternehmen von öffentlichem Interesse, insbesondere also den großen kapitalmarktorientierten Unternehmen/Aktiengesellschaften.
- 27** Für das Risikomanagement wesentlich ist die Verpflichtung zur Einrichtung eines angemessenen und wirksamen internen Kontrollsystems und eines entsprechenden Risikomanagementsystems; dazu findet man nun im neuen Absatz 3 des § 91 AktG:

„Der Vorstand einer börsennotierten Gesellschaft hat darüber hinaus ein im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames internes Kontrollsystem und Risikomanagementsystem einzurichten.“

- 28** Das Risikomanagement erfährt damit eine hervorgehobene Positionierung unter den Managementsystemen, weil nach der Diskussion über die Gesetzesvorlagen beispielsweise andere wesentliche Managementsysteme – wie das Compliance-Management oder das Controlling – im Gesetz nicht genannt werden.²¹

²⁰ Vgl. *Velte*, WPg, 74. Jg., Heft 6/2021, 387–398.

²¹ Vgl. *Gleißner/Romeike*, Der Aufsichtsrat 01/2022, 2–4.

Aus ökonomischer Perspektive ist ein „umfassendes Risikomanagement“ zunächst ein System, das alle Managementsysteme und Aktivitäten einbezieht, die sich mit Risiken befassen. Man kann dabei das Risikomanagement (im weiteren Sinn) grundsätzlich so ausrichten, dass alle anderen Managementsysteme diesem zugeordnet werden, sofern sie sich mit Chancen und Gefahren (Risiken) befassen. Alternativ ist es möglich, das zentrale Risikomanagement als ein dem Vorstand (und Aufsichtsrat) verantwortliches zentrales Managementsystem zu positionieren, das die Risikoinformationen von allen anderen Managementsystemen erhält (also beispielsweise aus Controlling, Informationssicherheit-Management oder Compliance-Management). **29**

Bei den börsennotierten Aktiengesellschaften sollte nun sichergestellt werden, dass ein „umfassendes“ Risikomanagementsystem implementiert ist, das sich – unabhängig von möglichen bestandsgefährdenden Entwicklungen – mit allen wesentlichen Chancen und Gefahren (Risiken) befasst, speziell auch mit geeigneten Methoden für Risikosteuerung und Risikobewältigung. Ein solches Risikomanagementsystem hat entsprechend § 93 AktG insbesondere die Aufgabe, bei der Vorbereitung „unternehmerischer Entscheidungen“ durch Risikoanalysen mitzuwirken („entscheidungsorientiertes Risikomanagement“).²² **30**

Gemäß § 107 AktG ist nun auch eine direkte Kommunikation zwischen dem Aufsichtsrat (Prüfungsausschuss) einerseits und dem Risikomanagement (sowie interner Revision und internem Kontrollsystem) andererseits vorgesehen. Zielsetzung ist es sicherzustellen, dass der Aufsichtsrat ein eigenständiges – auch vom Vorstand möglichst wenig beeinflusstes – Bild von der Risikolage und der Wirksamkeit und Qualität des Risikomanagementsystems erhält.²³ **31**

II. Abgrenzung des Risiko- und Chancenbegriffs

Aufgrund des vielfachen, teils inflationären und zugleich verwirrenden Einsatzes der Begriffe und ihrer Deutungen sowie der höchst unterschiedlichen Definition je nach Sprach- und Kulturraum ist eine saubere Definition des Risikobegriffs wichtig. **32**

Tatsache ist, dass Chancen und Risiken elementare Bestandteile des Unternehmens darstellen. Die Zahl verschiedenartiger Risikodefinitionen ist umfangreich und konzentriert sich umgangssprachlich zumeist auf die negative Komponente der Nichterreichung eines erwarteten Zielzustandes. „Seit dem 16. Jahrhundert hat sich das Wort Risiko für alle Arten von Gefährdungen eingebürgert. Der Bedeutungsumfang des Risikobegriffs ist sehr weit geworden: Man **33**

²² Vgl. hierzu vertiefend *Gleißner/Romeike*, Der Aufsichtsrat, Heft 04/2020, 55–57.

²³ Konkrete Anforderungen an ein solches Risikofrüherkennungssystem und Risikomanagementsystem sind in Standards definiert, wie dem DIIR RS Nr. 2 (Deutsches Institut für interne Revision) oder dem IDW Prüfungsstandard 340 n. F. (2020) sowie in der Fachliteratur, vgl. beispielsweise *Romeike/Hager*, Erfolgsfaktor Risikomanagement 4.0: Methoden, Beispiele, Checklisten – Praxishandbuch für Industrie und Handel, und *Gleißner*, Grundlagen des Risikomanagements – Handbuch für ein Management unter Unsicherheit.

spricht von wirtschaftlichen Risiken wie von gesundheitlichen, von Misserfolgsrisiken wie vom Unfallrisiko.“²⁴

- 34 Etymologisch kann der Begriff Risiko zum einen auf rhiza (griechisch = Wurzel, Klippe) zurückverfolgt werden; siehe auch: risc (arabisch = Schicksal). Auf der anderen Seite steht der Begriff Risiko für das lateinische Wort „ris(i)co“, die Klippe, die es zu umschiffen gilt. Jedoch ist der Ursprung des Begriffs bis heute nicht eindeutig geklärt. Während der „Duden“ das Wort über das vulgärlateinische, nicht belegte „risicare“ (resecare, Gefahr laufen, wagen) auf das altgriechische Wort für Wurzel (*ρίζα, rhíza*), zurückführt, nennt das Etymologische Wörterbuch der deutschen Sprache als etymologischen Hintergrund nur das lateinische bzw. vulgärlateinische „resicum“, „riscum“, „riscus“ (Felsklippe), die zur Gefahr für Schiffe werden kann.²⁵
- 35 Der deutsche Begriff des Risikos wird umgangssprachlich verstanden als ein möglicher negativer Ausgang bei einer Unternehmung – mit möglichen Nachteilen, Verlusten oder Schäden. Von Risiken spricht man nur, wenn die Folgen ungewiss sind. Eine genauere Definition von Risiken sieht diese als aus der Unvorhersehbarkeit der Zukunft resultierende, durch „zufällige“ Störungen verursachte Möglichkeiten, von geplanten Zielwerten abzuweichen.
- 36 Im chinesischen Schriftzeichen für Risiko „Wei-ji“ (vgl. Abbildung 1) beispielsweise sind die beiden Zeichenbestandteile für Chance und Gefahr enthalten, womit auch die positive Abweichung von einem erwarteten Zielzustand unter den Risikobegriff fällt.²⁶



Abbildung 1: Das chinesische Schriftzeichen für Risiko²⁷

- 37 In einer modernen Definition sind Risiken die aus der Unvorhersehbarkeit der Zukunft resultierenden, durch „zufällige“ Störungen verursachten Möglichkeiten, von geplanten Zielwerten abzuweichen. Risiken können daher auch als

24 Vgl. Karten, ZVersWiss 3/1988, 347.

25 Kluge, Etymologisches Wörterbuch der deutschen Sprache, 25. Aufl. 2010.

26 Vgl. Bayerische Rück, Gesellschaft und Unsicherheit, 1987, S. 7.

27 Quelle: Eigene Abbildung.

„Streuung“ um einen Erwartungs- oder Zielwert betrachtet werden (vgl. Abbildung 2).²⁸

Risiken sind immer nur in direktem Zusammenhang mit der Planung bzw. den definierten Zielen eines Unternehmens, Projekts etc. zu interpretieren. Mögliche Abweichungen von den geplanten Zielen stellen Risiken dar – und zwar sowohl negative („Gefahren“) wie auch positive Abweichungen („Chancen“). 38

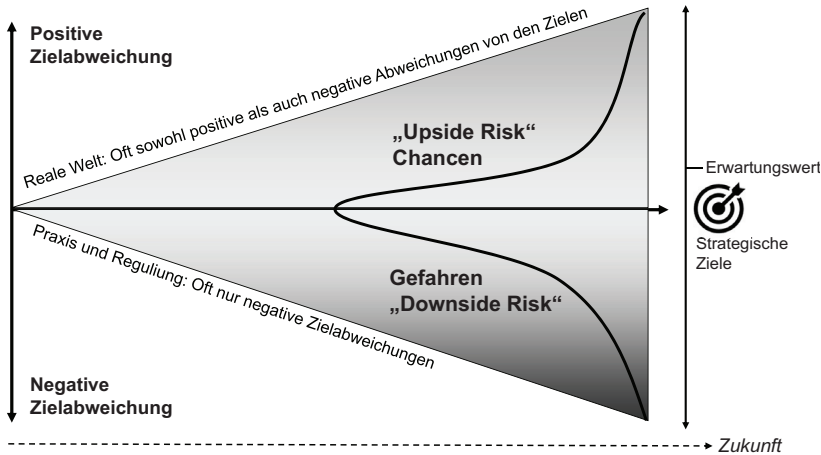


Abbildung 2: Risiko als mögliche Planabweichung²⁹

Analog bezeichnet auch der entscheidungstheoretische Risikobegriff durch das Konstrukt der Standardabweichung (Maß für die Streuung der Wahrscheinlichkeitsdichte um ihren Schwerpunkt) die positiven wie auch negativen Zielabweichungen von einem Erwartungswert. Dieser entscheidungsorientierte Risikobegriff berücksichtigt zudem, dass alle menschlichen Tätigkeiten auf Entscheidungen beruhen, die oft unter unvollkommener Information (= Ungewissheit oder Unsicherheit im engeren Sinne³⁰) über die Auswirkungen in der Zukunft getroffen werden, womit Informationsdefizite das Risiko vergrößern und zu ungünstigen Abweichungen zwischen Plan und Realisierung führen können. 39

Risiken sind klar von Entscheidungen unter Sicherheit abzugrenzen. Bei Entscheidungen unter Sicherheit fehlt das Charakteristikum der „Zufälligkeit“, da ein Ereignis sicher eintritt. Die Eintrittswahrscheinlichkeit dieses Ereignisses p beträgt somit 100 %. Risikomanagement konzentriert sich daher auf Entscheidungen unter Risiko sowie Entscheidungen unter Unsicherheit. Als Unsicherheit 40

28 Vgl. Gleißner/Romeike, Risikomanagement – Umsetzung, Werkzeuge, Risikobewertung, S. 27.

29 Quelle: Romeike, Risikomanagement, S. 9.

30 Vgl. Laux, Entscheidungstheorie, 1995, S. 24 ff.

bezeichnet man einen bewusst wahrgenommenen Mangel an Sicherheit oder an Reliabilität und Validität. Bei Entscheidungen unter Unsicherheit sind die möglichen Szenarien mit ihren Auswirkungen nicht oder nicht vollständig bekannt; auch können für die Szenarien keine festen Eintrittswahrscheinlichkeiten angegeben werden.

- 41 Internationale Standards, beispielsweise die ISO 31000:2018 (Risk management Guidelines), definieren den Begriff Risiko (risk) wie folgt:

„risk = effect of uncertainty on objectives. An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats. Objectives can have different aspects and categories, and can be applied at different levels. Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.“

- 42 Das US-amerikanische Committee of Sponsoring Organizations of the Treadway Commission (COSO)³¹ definiert den Begriff Risiko (risk) wie folgt:

„There is risk in not knowing how an entity's strategy and business objectives may be affected by potential events. The risk of an event occurring (or not), creates uncertainty. In business, uncertainty exists whenever an entity sets out to achieve future strategies and business objectives. In this context, risk is defined as: The possibility that events will occur and affect the achievement of strategy and business objectives.“

III. Nutzen eines wirksamen Chancen- und Risikomanagements

- 43 Es ist eine primäre Aufgabe des Risikomanagements, „Überraschungen“ auf der „Reise zum Ziel“ (vgl. Abbildung 5) sowie die Schwankungsbreite von Gewinn und Cashflow zu reduzieren und so Verluste und mögliche „bestandsgefährdende Entwicklungen“ (Krisen) zu vermeiden. Dies führt zu folgenden Vorteilen für ein Unternehmen:³²
- Die Reduzierung der Schwankungen erhöht die Planbarkeit und Steuerbarkeit eines Unternehmens, was einen positiven Nebeneffekt auf das erwartete Ertragsniveau hat.

31 COSO wurde im Jahr 1985 als Plattform für die „National Commission on Fraudulent Financial Reporting“ (Treadway Commission) gegründet und wird durch die fünf bedeutendsten US-Organisationen für Kontrolle im Finanz- und Rechnungswesen unterstützt: Institute of Internal Auditors (IIA), American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), Institute of Management Accountants (IMA) und American Accounting Association (AAA).

32 Vgl. *Gleißner/Romeike*, Risikomanagement – Umsetzung, Werkzeuge, Risikobewertung, S. 28, sowie *Romeike/Hager*, Erfolgsfaktor Risikomanagement 4.0: Methoden, Beispiele, Checklisten – Praxishandbuch für Industrie und Handel, S. 85 ff.

- Eine prognostizierbare Entwicklung der Zahlungsströme reduziert die Wahrscheinlichkeit, unerwartet auf teure externe Finanzierungsquellen zurückgreifen zu müssen, und sichert den Spielraum für Investitionen.
- Eine Verminderung der risikobedingten Schwankungsbreite der zukünftigen Zahlungsströme senkt die Kapitalkosten und wirkt sich positiv auf den Unternehmenswert aus.
- Eine stabile Gewinnentwicklung mit einer hohen Wahrscheinlichkeit für eine ausreichende Kapitaldienstfähigkeit ist im Interesse der Fremdkapitalgeber, was sich in einem guten und stabilen Rating, einem vergleichsweise hohen Finanzierungsrahmen und günstigen Kreditkonditionen widerspiegelt.
- Eine stabile Gewinnentwicklung reduziert die Wahrscheinlichkeit einer Insolvenz und damit den Erwartungswert der Konkurskosten.
- Eine stabile Gewinnentwicklung sowie eine niedrigere Insolvenzwahrscheinlichkeit sind im Interesse von Arbeitnehmern, Kunden und Lieferanten, was es erleichtert, qualifizierte Mitarbeiter zu gewinnen und langfristige Beziehungen zu Kunden und Lieferanten aufzubauen.
- Bei einem progressiven Steuertarif haben zudem Unternehmen mit schwankenden Gewinnen Nachteile gegenüber Unternehmen mit kontinuierlicher Gewinnentwicklung.
- Eine prognostizierbare Entwicklung des Cashflows reduziert die Wahrscheinlichkeit, unerwartet auf teure externe Finanzierungsquellen zurückgreifen zu müssen oder ökonomisch sinnvolle Investitionen nicht durchführen zu können.
- Risikomanagement bietet insgesamt vor allem eine Erhöhung der Planungssicherheit durch eine Reduktion potenzieller Überraschungen und eine nachhaltige Steigerung des Unternehmenswerts (wertorientierte Steuerung).
- Reduzierung des persönlichen Haftungsrisikos für Organmitglieder (siehe Business Judgement Rule).³³

Auf den messbaren Nutzen eines Risikomanagementsystems sowie basierend auf dem grundlegenden Verständnis von Nachhaltigkeit und den Erkenntnissen der Bewertungstheorie haben *Gleißner, Günther und Walkshäusl* im Jahr 2022 ein Messkonzept für die hier relevante „finanzielle Nachhaltigkeit“ entwickelt, das die enge Beziehung zwischen Nachhaltigkeit und Risikomanagement zeigt.³⁴ **44**

Die Autoren konnten zeigen, dass finanzielle Nachhaltigkeit, die man als komplexes Risikomaß zur Beurteilung der Zukunftsfähigkeit interpretieren kann, mit vier Kennzahlen erfasst werden kann.³⁵ Die Messung, Steuerung und Verbesserung von finanzieller Nachhaltigkeit ist von so grundlegender Bedeutung im **45**

33 Vgl. vertiefend *Hartmann/Romeike*, Business Judgement Rule, FIRM Jahrbuch 2015, S. 157–160. Zur Business Judgement Rule siehe vertiefend → *Schulz*, Kap. 1 Rn. 53, → *Jacobs*, Kap. 13 Rn. 11 sowie → *Bensinger*, Kap. 14 Rn. 90 ff.

34 Vgl. *Gleißner/Günther/Walkshäusl*, Journal of Business Economics, Vol. 92, 2022, 467–516.

35 Vgl. hierzu vertiefend *Gleißner/Romeike*, FIRM Yearbook 2023, S. 125–127.

Nachhaltigkeitsmanagement, weil die Existenz des Unternehmens natürlich Voraussetzung für alles andere ist.

- 46** Für die Beurteilung finanzieller Nachhaltigkeit dienen vier finanzielle Kennzahlen, deren Ausprägungen wiederum ganz erheblich den Unternehmenswert bestimmen. Hohe finanzielle Nachhaltigkeit charakterisiert Qualitätsunternehmen und ist gegeben, wenn
1. ein Unternehmen langfristig real wächst,
 2. die risikoabhängige Insolvenzwahrscheinlichkeit (p) niedrig ist,
 3. das Ertragsrisiko, beispielsweise ausgedrückt durch den Variationskoeffizient V der Gewinne, gering und für die Eigentümer „akzeptabel“ ist und
 4. die Kapitalrendite des Unternehmens höher ist als die risikoabhängigen Kapitalkosten, das heißt die risikogerechten Anforderungen an die Rendite.
- 47** Finanzielle nachhaltige Unternehmen weisen also eine positive reale Wachstumsrate auf, sie haben ein niedriges Ertragsrisiko (Variationskoeffizient der Gewinne), eine niedrige Insolvenzwahrscheinlichkeit und nachhaltig eine Kapitalrendite oberhalb der risikoabhängigen Kapitalkosten. In einer empirischen Studie für die Euro STOXX 600-Unternehmen in den letzten 30 Jahren können die Autoren zeigen, dass Unternehmen mit hoher finanzieller Nachhaltigkeit nicht nur weniger Risiko und eine höhere Überlebensfähigkeit aufweisen. Ganz auf der Linie des im strategischen Management bekannten Rendite-Risiko-Paradoxons haben solche Unternehmen an der Börse sogar deutlich höhere Renditen, nämlich eine Überrendite von rund 5 % pro Jahr.
- 48** Die empirischen Ergebnisse für den europäischen Aktienmarkt belegen konkret, dass Unternehmen mit hoher finanzieller Nachhaltigkeit risikoärmer sind und zugleich langfristig signifikant risikoadjustierte Überrenditen aufweisen.³⁶ Die Überrenditen bewegen sich in Abhängigkeit der Portfoliogewichtung und der verwendeten Modelle zur Risikoadjustierung zwischen 3,7 % und 6,5 % pro Jahr. Diese Resultate deuten darauf hin, dass die Marktteilnehmer bislang die Bedeutung finanzieller Nachhaltigkeit unterschätzen und die entsprechenden Informationen nicht umgehend in den Aktienkursen einpreisen.
- 49** Eine quantitative Risikoanalyse und Risikoaggregation sind also nicht nur Verfahren, die geboten sind, um gesetzliche Mindestanforderungen an das Risikomanagement zu erfüllen (siehe § 1 StaRUG sowie § 91 AktG), sondern auch Basis für die Beurteilung und Verbesserung der finanziellen Nachhaltigkeit.

IV. Unterscheidung von Ursachen – Risiken – Wirkungen

- 50** Für die Beschreibung von Risiken – definiert als potenzielle Ziel- bzw. Planabweichungen – ist es wichtig, dass zwischen Ursachen, dem potenziellen Ereignis (Event) und den Wirkungen unterschieden wird.

³⁶ Vgl. *Gleißner/Günther/Walkshäusl*, Journal of Business Economics, Vol. 92, 467–516.

Die „Bow-Tie-Analyse“ ist eine grafische Darstellungsform und Methode, die eine logische Beziehung zwischen den Ursachen (causes) und Wirkungen (effects) eines Ereignisses, beispielsweise eines Risikos, darstellt. Die Ursachen, Ereignisse/Risiken und Wirkungen werden übersichtlich in einem „Bow-Tie-Diagramm“ dargestellt und bilden damit eine Grundlage für eine transparente und leicht verständliche Risikokommunikation und die Definition von präventiven und reaktiven Maßnahmen zur Risikosteuerung. **51**

Bereits in den frühen neunziger Jahren übernahm die Royal Dutch Shell Group die Bow-Tie-Analyse als Methode und Unternehmensstandard für die Analyse und das Management von Risiken. Später übernahmen weitere Unternehmen aus der Öl- und Gasindustrie sowie aus der Luftfahrtindustrie, dem Schienenverkehr, der Schifffahrt, im Chemie- und Gesundheitswesen sowie Banken und Versicherungen die Bow-Tie-Analyse als Standard zur Strukturierung und Analyse von Risiken.³⁷ Wenn (quantitative) Daten zu Ursachen und Wirkungen verfügbar sind, kann die Bow-Tie-Analyse auch zur Risikobewertung genutzt werden. **52**

Da ein Risiko in der Regel eine Vielzahl von Ursachen, aber auch Wirkungen aufweist, hat das Diagramm die Form einer Fliege (oder einer Krawattenschleife; im Englischen „bow tie“, siehe Abbildung 3). Teilweise wird das Bow-Tie-Diagramm auch als „Schmetterlingsdiagramm“ bezeichnet. **53**

Die Bow-Tie-Analyse hat sich auf der Basis vier weiterer Methoden entwickelt. Diese sind:³⁸ **54**

- die Fehlerbaumanalyse (Fault Tree Analysis, FTA);
- die Ereignisbaumanalyse (Event Tree Analysis, ETA);
- die Ursache-Wirkungs-Diagramme (Cause and Effect Diagram, Fishbone Diagram)
- sowie die Barrier Analysis.

37 Vgl. hierzu *Romeike*, Risikomanagement, S. 74 ff., sowie *Romeike*, GRC aktuell 01/2019, 39–44.

38 Vgl. *de Ruijter/Guldenmund*, Safety Science 88/2016, 211–218, sowie *Romeike/Spitzner*, Einsatz von Simulationmethoden im Logistik-Risikomanagement, in: Huth/Romeike (Hrsg.), Risikomanagement in der Logistik, S. 127–158.

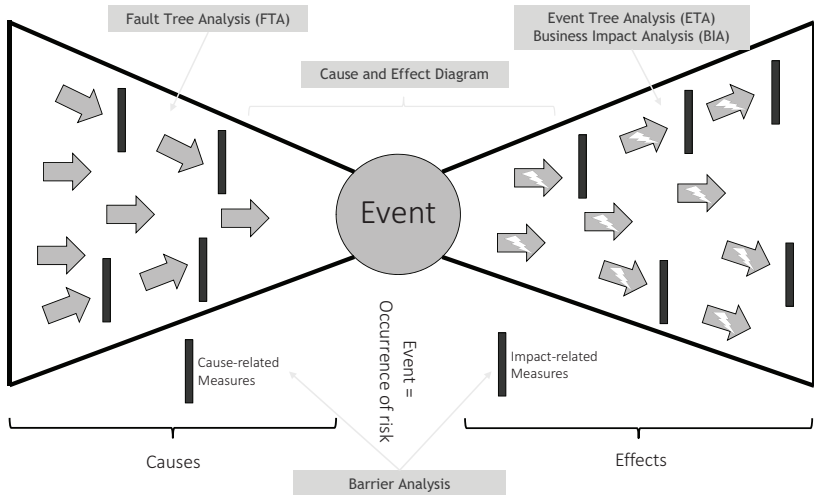


Abbildung 3: Unterscheidung von Ursachen, Risiken und Wirkungen in einem Bow-Tie-Diagramm³⁹

- 55 Es existieren verschiedene Variationen der Bow-Tie-Analyse, die davon abhängen, zu welchem Zweck die Analyse genutzt werden soll (Risikoidentifikation, Risikobewertung, Risikokommunikation) und aus welchen konkreten Elementen das Diagramm besteht bzw. welche Methoden angewandt werden.
- 56 Eine fundierte und detaillierte Analyse der Ursachen ist vor dem Hintergrund wichtig, dass Maßnahmen zunächst an den Ursachen ansetzen sollten („Vorbeugen ist besser als heilen“), um den Risikoeintritt durch präventive Maßnahmen (etwa im Bereich von organisatorischen Maßnahmen bzw. einer gelebten Risikokultur) zu verhindern. Dies wird selbstverständlich nicht bei allen potenziellen Risiken möglich bzw. betriebswirtschaftlich sinnvoll sein.
- 57 Die Kritikalität eines Risikos kann erst über die Wirkungsmechanismen beurteilt werden. So ist es denkbar, dass eine kleine Ursache (eine scheinbar harmlose „Softwaremanipulation“) zu einer extremen Wirkung führt (Schadensersatzforderungen, strafrechtliche Konsequenzen, Reputationsverlust, Insolvenzrisiko steigt, Ratingeinstufung sinkt, Fremdkapitalkosten steigen etc.). Die Kritikalität eines Szenarios lässt sich beispielsweise nach einer Bewertung der Wirkung bei Risikoeintritt auf das Betriebsergebnis oder die Risikotragfähigkeit beurteilen. Wenn die Risikotragfähigkeit bei einem potenziellen Risikoszenario nicht ausreicht, um die Verluste zu tragen, kann von einem existenzbedrohenden Risiko gesprochen werden.

³⁹ Quelle: Romeike, Risikomanagement, S. 75.

In Abbildung 4 ist die Unterscheidung zwischen Ursachen, Risiken und Wirkungen beispielhaft wiedergegeben. Alle skizzierten Risiken weisen eine hohe Kritikalität auf. Allerdings können die Risiken 1 und 3 mit Maßnahmen präventiv oder zumindest reaktiv beeinflusst werden. 58

Nr.	Cause	Risk	Effect	Criticality	Ability to Act
				1 1 2 1 3 1 4 1 5	1 1 2 1 3 1 4 1 5
1	Sturm deckt das Dach der Produktion teilweise ab (keine sturmsichere Konstruktion)	Betriebsunterbrechung in Produkthalle C.	- Reparaturkosten - Produktionsstillstand während Reparatur - Schadensersatz von Kunden Z	★	★
2	Cyberangriff auf zentrales ERP-System	Stillstand des Bestellsystems (Verfügbarkeit) und Wiederherstellung des ERP-Systems, Datenverlust	- Keine fristgerechte Lieferung mehr möglich - Schadensersatz von Kunden W - Reputationsverlust / Verlust Großauftrag - Zusätzliche Personalkosten durch personellen Mehraufwand		★
3	Entwicklungsfehler Dieseleinspritzpumpe durch verunreinigtes Teflon	Ausfall Dieseleinspritzpumpe und Kundenrückruf	- Austausch aller Dieseleinspritzpumpen (> 1,7 Mio. Stück) - Rückrufkosten - Kosten für Austausch der Pumpen - Kosten für neue Produktion - Reputationsschaden - Schadensersatzforderung von Kunden Y	★	★
4					
5					
Weitere ...					

★
 ↓
 5 = highly critical

 ★
 ↓
 5 = risk acceptance

Abbildung 4: Beispiel für Unterscheidung von Ursachen, Risiken und Wirkungen⁴⁰

V. Verknüpfung von Risikomanagement und Strategie

Abbildung 5 verdeutlicht, dass eine flankierende Risikostrategie bzw. ein Risikomanagement Unternehmen dabei unterstützt, möglichst auf der Idealroute das definierte Ziel zu erreichen. Damit wird deutlich, dass Risikomanagement immer entscheidungsorientiert – unter Berücksichtigung der Unternehmensstrategie – ausgerichtet sein muss.⁴¹ Die Praxis zeigt, dass Unternehmen durch Risikoeintritte oft die Idealroute verlassen müssen, da sie zuvor keine präventiven Maßnahmen definiert haben (siehe beispielsweise die Auswirkungen auf die Wertschöpfungsketten in der Folge der SARS-CoV-2-/COVID-19-Pandemie). Die flankierende Risikostrategie sowie ein adäquates Risikomanagement stellen Werkzeuge zur Verfügung, damit Unternehmen möglichst auf der Idealroute zum definierten Ziel gelangen. 59

⁴⁰ Quelle: Eigene Abbildung.

⁴¹ Vgl. vertiefend *Gleißner/Romeike*, Der Aufsichtsrat 4/2020, 55–57 sowie *Romeike/Hager*, Erfolgsfaktor Risikomanagement 4.0: Methoden, Beispiele, Checklisten – Praxishandbuch für Industrie und Handel, S. 81 ff.

Teil 2 Übergreifende Themen und Herausforderungen – Risiko und Governance

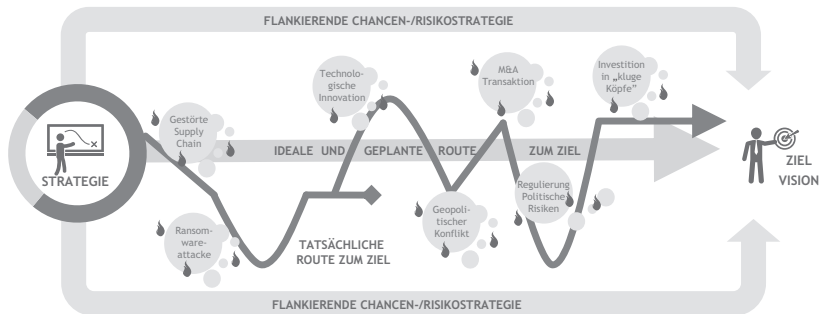


Abbildung 5: Mehrwert eines Risikomanagements⁴²

- 60** So wird beispielsweise in Versicherungsunternehmen die Verknüpfung von Risikomanagement und Strategie auch seitens des Gesetzgebers in § 26 Versicherungsaufsichtsgesetz (VAG) unter der Überschrift „Risikomanagement“ gefordert:
- 61** „(1) [...] Das Risikomanagementsystem muss die Strategien, Prozesse und internen Meldeverfahren umfassen, die erforderlich sind, um Risiken, denen das Unternehmen tatsächlich oder möglicherweise ausgesetzt ist, zu identifizieren, zu bewerten, zu überwachen und zu steuern sowie aussagefähig über diese Risiken zu berichten. [...]“
- (2) Zu den zu entwickelnden Strategien zählt insbesondere eine auf die Steuerung des Unternehmens abgestimmte Risikostrategie, die Art, Umfang und Komplexität des betriebenen Geschäfts und der mit ihm verbundenen Risiken berücksichtigt.“⁴³
- 62** Die Notwendigkeit einer definierten Risikostrategie für ein wirksames Risikomanagement lässt sich direkt auch auf Unternehmen aller anderen Branchen übertragen.
- 63** Die relevanten Fragestellungen, die in einer Risikostrategie beantwortet werden sollten, sind in Abbildung 6 in einer kompakten Form wiedergegeben.⁴⁴

42 Quelle: Eigene Abbildung in Anlehnung an Romeike, Risikomanagement, S. 35.

43 Vgl. hierzu vertiefend Korte/Romeike, MaRisk VA erfolgreich umsetzen: Praxisleitfaden für das Risikomanagement in Versicherungen, S. 51 ff.; analoge Regelungen gelten in der Bankenregulierung.

44 Der detaillierte Prozess zur Definition einer Risikostrategie ist beschrieben in: Romeike, Grundlagen des Risikomanagements in der Versicherungsbetriebslehre, in: Romeike/Müller-Reichert, Risikomanagement in Versicherungsunternehmen, S. 71 ff.

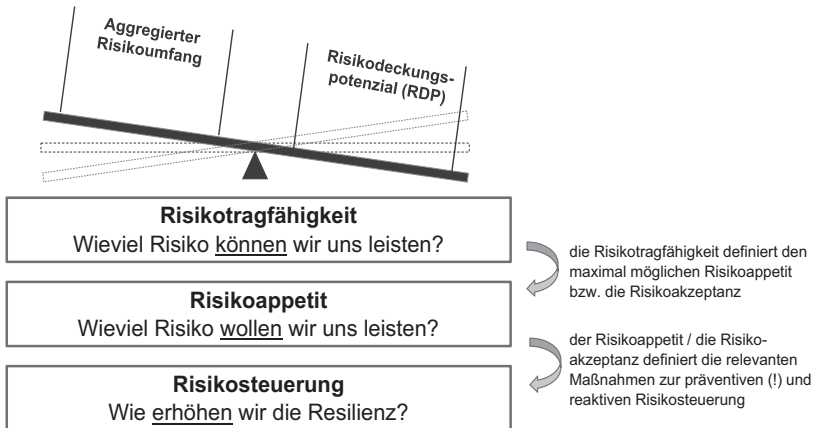


Abbildung 6: Fragestellungen im Kontext Risikostrategie⁴⁵

VI. Der Risikomanagement-Prozess als Regelkreis

Ein Risikomanagementsystem besteht aus verschiedenen Elementen. Exemplarisch werden nachfolgend die Komponenten basierend auf dem internationalen Standard COSO ERM (2017) beschrieben, veröffentlicht vom „Committee of Sponsoring Organizations of the Treadway Commission“, einer freiwilligen privatwirtschaftlichen Organisation in den Vereinigten Staaten von Amerika.⁴⁶ 64

Ein wesentliches Element eines Risikomanagementsystems ist der Regelkreis des Risikomanagement-Prozesses, auf den in den folgenden Kapiteln im Detail eingegangen wird. 65

Der Standard COSO ERM (2017) basiert auf fünf Komponenten: 66

- **Risiko-Governance und -Kultur (Risk Governance and Culture):** Risiko-Governance und -Kultur bilden zusammengekommen die Grundlage für alle anderen Komponenten des unternehmensweiten Risikomanagements. Risk Governance definiert die Risikostrategie, unterstützt die Relevanz und legt die Verantwortlichkeiten für das Risikomanagement im Unternehmen fest. Risikokultur bezieht sich auf ethische Werte, gewünschte Verhaltensweisen

⁴⁵ Quelle: Eigene Abbildung.

⁴⁶ COSO wurde im Jahr 1985 als Plattform für die „National Commission on Fraudulent Financial Reporting“ (Treadway Commission) gegründet und wird durch die fünf bedeutendsten US-Organisationen für Kontrolle im Finanz- und Rechnungswesen unterstützt: Institute of Internal Auditors (IIA), American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), Institute of Management Accountants (IMA) und American Accounting Association (AAA).

und das Verständnis von Risikomanagement in der Organisation. Die „gelebte“ Risikokultur sollte sich hierbei auch im Entscheidungsprozess widerspiegeln.

- **Risiko, Strategie und Zielsetzung (Risk, Strategy, and Objective-Setting):** Das Risikomanagement im Unternehmen ist durch den Prozess der Festlegung von Strategie und Geschäftszielen in die strategische Planung integriert. Nur mit einem klar definierten Fokus auf die definierte Strategie und die definierten strategischen Ziele ist es möglich, die internen und externen Risikofaktoren sowie deren Wirkungen auf das Unternehmen zu analysieren. Ein Unternehmen muss den Risikoappetit bzw. die Risikoakzeptanz im Kontext der Unternehmensstrategie definieren. Die Unternehmensziele ermöglichen die Umsetzung der Strategie und definieren die Prioritäten des Unternehmens.
- **Risikomanagement-Prozess (Risk in Execution):** Ein Unternehmen identifiziert und bewertet Risiken (Risikoanalyse), die auf die definierte Strategie sowie die festgelegten Ziele des Unternehmens einen negativen und/oder positiven Einfluss haben könnten. Das Unternehmen priorisiert die Risiken nach ihrer Relevanz und Kritikalität und unter Berücksichtigung des definierten Risikoappetits bzw. der Risikoakzeptanz. Das Unternehmen definiert anschließend mögliche Maßnahmen zur Risikosteuerung (sofern möglich) oder akzeptiert das Risiko. Auf diese Weise entwickelt das Unternehmen eine Portfoliobetrachtung der Risiken (und ggf. Chancen), die es bei der Verfolgung seiner Strategie und seiner Geschäftsziele eingegangen ist.
- **Risikoinformationen, Kommunikation und Berichterstattung (Risk Information, Communication, and Reporting):** Kommunikation ist der kontinuierliche, iterative Prozess der Informationsbeschaffung und -weitergabe in der gesamten Organisation. Das Management verwendet relevante und wichtige Informationen aus internen und externen Quellen, um das Risikomanagement im Unternehmen zu unterstützen. Das Unternehmen verwendet (auch softwarebasierte) Informationssysteme zur Erfassung, Verarbeitung und Verwaltung von Daten und Informationen.
- **Überwachung der Leistungsfähigkeit des Risikomanagements im Unternehmen (Monitoring Enterprise Risk Management Performance):** Durch die Überwachung der Performance des unternehmensweiten Risikomanagements kann ein Unternehmen analysieren, wie wirksam das Risikomanagements tatsächlich ist und ob es einen Mehrwert für die Unternehmenssteuerung und bei der Erhöhung des Unternehmenswerts stiftet.

- 67 Ein Risikomanagement-Prozess funktioniert ähnlich dem menschlichen Organismus oder anderer Netzwerkstrukturen in der Natur. In einem menschlichen Organismus arbeiten Gehirn, Herz und Nervensystem zusammen.⁴⁷ Übertragen auf den Prozess des Risikomanagements bedeutet dies, dass verschiedene Sensoren und Sinne (etwa Auge, Ohr oder Nerven) die Risiken aufnehmen (Risikoana-

47 Vgl. Romeike/Hager, Erfolgsfaktor Risikomanagement 4.0: Methoden, Beispiele, Checklisten – Praxishandbuch für Industrie und Handel, S. 94 ff.

lyse) und sie an eine zentrale Stelle weiterleiten (Gehirn bzw. Risikomanager). Und insgesamt entscheidet die strategische Ausrichtung des Systems (Unternehmens) über das Risikoverständnis. In diesem Zusammenhang ist es wichtig, das Risikomanagement immer im Kontext der Geschäftsstrategie zu betrachten.

Die strategische Dimension des Risikomanagements bildet die Basis sowie integrative Klammer und das Fundament des gesamten Risikomanagement-Prozesses (vgl. Abbildung 7). Dies beinhaltet vor allem die Formulierung von Risikomanagement-Zielen in Form einer Risikostrategie (vgl. Abbildung 6). Diese muss eine direkte Verbindung zur definierten Unternehmensstrategie herstellen, d. h. die relevanten Risiken sollten aus den strategischen Unternehmenszielen abgeleitet werden („Welche Risiken können beispielsweise die Erfolgspotenziale des Unternehmens gefährden?“). **68**

Risiken effizient zu steuern, zu kontrollieren sowie Chancen zu erkennen und zu nutzen, gehört zur unternehmerischen Kerntätigkeit jedes Unternehmens. Trotzdem ist die Bereitschaft der Unternehmen, Risiken einzugehen, sehr unterschiedlich und abhängig von den Eigentumsverhältnissen, der Liquidität (Risikodeckungspotenzial bzw. Risikotragfähigkeit) und auch der persönlichen Risikoneigung (Risikoappetit) der Unternehmensleitung bzw. der Eigentümer. **69**

Das operative Risikomanagement beinhaltet den Prozess der systematischen und laufenden Risikoanalyse der Geschäftsabläufe. Ziel der Risikoidentifikation ist das frühzeitige Erkennen von potenziellen Ziel- und Planabweichungen, das heißt die möglichst vollständige Erfassung aller Risikoquellen, Schadensursachen und Störpotenzialen (siehe Ursachen im Bow-Tie-Diagramm, vgl. Abbildung 3). Für einen effizienten Risikomanagement-Prozess kommt es darauf an, dass dieser als kontinuierlicher Prozess – im Sinne eines Regelkreises – in die Unternehmensprozesse integriert wird. Außerdem werden neben den Ursachen auch die Wirkungen potenzieller Ereignisse (Events) analysiert (siehe Wirkungen im Bow-Tie-Diagramm, vgl. Abbildung 3). **70**

Die Informationsbeschaffung ist die schwierigste Phase im gesamten Prozess und eine Schlüsselfunktion des Risikomanagements, da dieser Prozessschritt die Informationsbasis für alle nachfolgenden Phasen liefert – schließlich können nur Risiken bewertet und gesteuert werden, die auch erkannt wurden. **71**

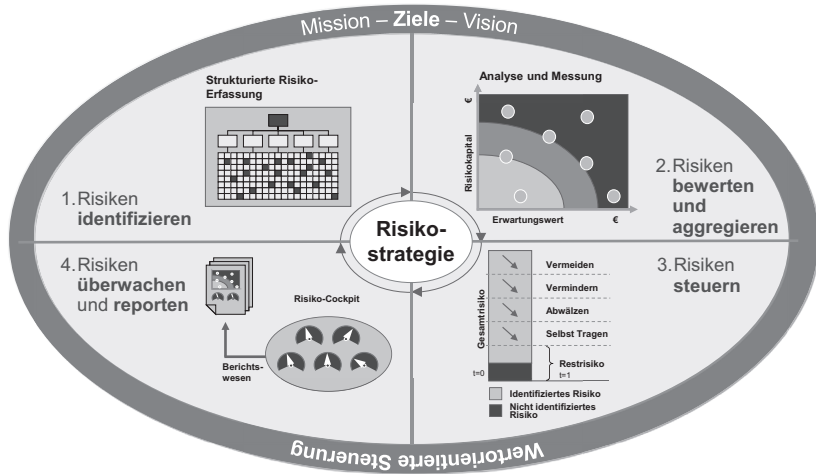


Abbildung 7: Der Risikomanagement-Prozess als Regelkreis⁴⁸

- 72** In der Prozessphase der Risikoidentifikation erfolgt
- eine möglichst konsistente Erfassung sämtlicher Risiken, Risikotreiber (Ursachen), Wirkungen und Risikobezugsgrößen;
 - eine Dokumentation der Risikoursachen und Risikowirkungen;
 - eine Definition der Wesentlichkeitsgrenzen zur Risikoanalyse.
- 73** In der Prozessphase der Bewertung erfolgt
- eine (vor allem quantitative) Bewertung der in der Prozessphase der Identifikation dokumentierten Risiken mit Hilfe geeigneter Methoden;
 - die Festlegung des Bewertungszeithorizonts in Übereinstimmung mit dem unternehmensindividuellen Planungshorizont;
 - die Bewertung mit Hilfe geeigneter Verteilungsfunktionen (bspw. Häufigkeiten und Schadensszenarien);
 - eine Aggregation aller Risiken – unter Berücksichtigung evtl. Abhängigkeiten.
- 74** In der Prozessphase der Risikosteuerung
- erfolgt die Definition von geeigneten präventiven und reaktiven Maßnahmen zur Risikosteuerung (beispielsweise Risikovermeidung, Risikoverminderung, Risikotransfer oder Risikotragung) durch die „Risk Owner“, in der Regel also die operativen Geschäftsbereiche.

⁴⁸ Quelle: Romeike/Hager, Erfolgsfaktor Risikomanagement 3.0: Lessons learned, Methoden, Checklisten und Implementierung, S. 102, sowie Romeike, Risikomanagement, S. 38.

In der Prozessphase von Risikoüberwachung und -reporting 75

- erfolgt die kontinuierliche Überwachung der identifizierten und bewerteten Risiken durch die unabhängige Risikocontrolling-, Risikomanagementfunktion bzw. durch die Risk Owner.

Der Werkzeugkasten des Risikomanagers bietet eine große Vielfalt an Methoden und Analysemethoden zur Identifikation und Bewertung von Risiken. Die Auswahl der Werkzeuge und Methoden wird primär von den verfügbaren Daten der einzelnen Risiken sowie der verfügbaren Zeit für die Analyse determiniert. 76

VII. Methoden zur Risikoidentifikation und -bewertung

Für die Identifikation und Bewertung von Risiken eignen sich unterschiedliche Methoden, die nachfolgend überblicksartig beschrieben werden:⁴⁹ 77

- **Risiken aus der Strategie sowie den strategischen Zielen ableiten:** Im Kontext der strategischen Unternehmensplanung muss sich ein Unternehmen über seine maßgeblichen Erfolgspotenziale (Kernkompetenzen, interne Stärken und für den Kunden wahrnehmbare Wettbewerbsvorteile) Klarheit verschaffen. Die wichtigen „strategischen Risiken“ lassen sich identifizieren, indem die für das Unternehmen wichtigsten Erfolgspotenziale systematisch dahingehend untersucht werden, welchen Bedrohungen diese ausgesetzt sind. Hierfür eignet sich beispielsweise eine SWOT-Analyse oder eine deterministische bzw. stochastische Szenarioanalyse oder auch die Flip-Flop-Technik.
- **Risiken abgeleitet aus der operativen Planung und Budgetierung (Controlling):** Im Rahmen der Unternehmensplanung oder Budgetierung werden bestimmte Annahmen getroffen (beispielsweise bezüglich Konjunktur, Wechselkursen und Umsatzentwicklungen in der Folge von Vertriebsaktivitäten). Alle unsicheren Planannahmen sind direkt mit einem Risiko bzw. einer Chance verbunden, weil hier potenzielle Planabweichungen (negativ oder positiv) auftreten können. Hierfür eignet sich die stochastische Szenarioanalyse in Form einer Bandbreitenplanung.⁵⁰
- **Risk-Assessment-Workshops zu leistungswirtschaftlichen Risiken:** Bestimmte Risikoarten lassen sich am besten im Rahmen eines Workshops – unterstützt durch Kreativitätsmethoden – erfassen. Hierzu gehören insbesondere die Risiken aus den Leistungserstellungsprozessen (operative Risiken), rechtliche (Compliance-Risiken) und politische/regulatorische Risiken sowie Risiken aus Unterstützungsprozessen (beispielsweise Informationstechnologie). Bei operativen Risiken der Wertschöpfungsketten bietet es sich beispielsweise an, diese Arbeitsprozesse zunächst (einschließlich der wesentlichen Schnitt-

⁴⁹ Einen umfassenden Überblick über diverse Methoden zur Identifikation und Bewertung von Risiken bieten: *Romeike*, Risikomanagement, sowie *Romeike/Hager*, Erfolgsfaktor Risikomanagement 4.0: Methoden, Beispiele, Checklisten – Praxishandbuch für Industrie und Handel.

⁵⁰ Vgl. vertiefend *Romeike/Stallinger*, RC&A 06/2012, 12–21.

stellen) zu beschreiben und anschließend Schritt für Schritt zu überprüfen, durch welche Risiken eine Abweichung des tatsächlichen vom geplanten Prozessablauf eintreten kann.

- 78 Die Qualität der Ergebnisse aus dem Prozessschritt der Risikoidentifikation und Risikobewertung liefert die Grundlage für die Aggregation der Risiken sowie der Steuerung der Risiken. Wenn bei der Risikoidentifikation und -bewertung – zum Beispiel aufgrund einer schwachen methodischen Fundierung, zu oberflächlicher Analyse oder anderen Gründen – Fehler gemacht werden, wirken sich diese Fehler unweigerlich auf die Priorisierung von Risiken sowie die Entwicklung und Anwendung von Maßnahmen zur Risikosteuerung aus. Risiken, deren Bedeutung unterschätzt wird oder die gar „übersehen“ werden (das heißt, die bei der Identifizierung nicht erkannt werden), können zu gravierenden „Kettenreaktionen“ und Folgeschäden führen.⁵¹
- 79 Aus diesem Grund ist es von besonderer Bedeutung, dass Risikomanager den „Werkzeugkoffer“ für Risikoidentifikation, -analyse und -bewertung kennen und zielgerichtet einsetzen können.

Kollektionsmethoden	Suchmethoden	
	Analytische Methoden	Kreativitätsmethoden
• Checkliste • Schadenfall-Datenbank • (Control-) Self-Assessment • Risiko-Identifikations-Matrix (RIM), Risikofeldermatrix • Strukturierte oder semi-strukturierte Interviews • ...	• Bow-Tie-Analyse • Empirische Datenanalyse • Fehlerbaumanalyse (Fault tree analysis, FTA) • Fehlermöglichkeits- und Einflussanalyse (FMEA) • Hazard and operability studies (HAZOP) • Hazard Analysis and Critical Control Points (HACCP) • Business impact analysis (BIA) • Root cause analysis (Fehler-Ursachen-Analyse) • Ereignis-Baumanalyse (Event tree analysis, ETA) • Cause and consequence analysis • Markov analysis (Stochastische Prozesse) • Social Network Analysis • Scoring-Methodik • Spieltheorie (Game Theory) • Bayesian statistics and Bayes Nets • Structured "What-if" Technique (SWIFT) ...	• SWOT-Analyse • Morphologische Verfahren • Brainstorming & Brainstorming 2.0 • Brainwriting • Brainwriting Pool • Mind Mapping • Storytelling • K.J-Methode • Flip-Flop-Technik (Kopfstandtechnik) • Bisoziation • World-Café • Delphi-Methode • Business Wargaming • Deterministische Szenarioanalyse • Stochastische Szenarioanalyse • System Dynamics • Crowdsourcing, Social Forecasting etc. • Risk Analytics, Predictive Analytics • ...
Vorwiegend geeignet zur Identifikation bekannter Risiken		Vorwiegend geeignet zur Identifikation zukünftiger und bisher unbekannter Risikopotentiale (proaktives Risikomanagement)

Abbildung 8: Werkzeuge und Methoden zur Risikoidentifikation und Risikobewertung⁵²

- 80 Die Methoden zur Risikoidentifikation, Risikoanalyse und Risikobewertung lassen sich in Kollektionsmethoden sowie Suchmethoden unterteilen (vgl. Abbildung 8).

51 Vgl. hierzu *Romeike*, Risikomanagement, S. 55 ff. Das Buch liefert eine detaillierte Übersicht über Methoden zur Identifikation, Bewertung und Steuerung von Risiken.

52 Quelle: *Romeike*, Risikomanagement, S. 56, sowie *Romeike*, GRC aktuell 01/2018, 41–45.

Kollektionsmethoden sind vornehmlich für Risiken geeignet, die offensichtlich oder bereits bekannt sind (beispielsweise aufgrund einer bereits in der Vergangenheit durchgeführten Risikoidentifikation). In der Praxis erfolgt die Identifikation von Risiken recht häufig (insbesondere bei einem niedrigen Reifegrad des Risikomanagements) unter Verwendung von Checklisten. **81**

Suchmethoden dagegen lassen sich vor allem für bisher unbekannte Risiken einsetzen. Die Suchmethoden können in analytische Methoden und Kreativitätsmethoden klassifiziert werden.⁵³ **82**

Alle analytischen Suchverfahren sind darauf fokussiert, zukünftige und bisher unbekannte Risikopotenziale zu identifizieren. Einige analytische Suchverfahren wurden ursprünglich für die Risikoanalyse im Qualitätsmanagement entwickelt. Da die Prozessstruktur und Methodik des Risikomanagements einige Parallelen zum Qualitätsmanagement (bei dem im Kern Qualitätsrisiken identifiziert, bewertet und gesteuert werden) aufweist, liegt es nahe, etablierte Methoden auch auf den Risikoidentifikationsprozess für andere Risikoarten zu übertragen. **83**

Kreativitätsmethoden hingegen basieren auf kreativen Prozessen, die durch divergentes und kreatives Denken charakterisiert sind, um relativ flüssig und flexibel zu neuartigen Einfällen und originellen Lösungen zu gelangen. Kreativitätstechniken lassen – im Gegensatz zum rationalen und strukturierten Denken – das Denken chaotisch werden und ermöglichen so vor allem die Identifikation bisher unbekannter Risikopotenziale. **84**

Auf den Einsatzzweck, den Input bzw. Datenbedarf, den Output, den zeitlichen Aufwand für den Methodeneinsatz sowie die Stärken und Grenzen der einzelnen Methoden wird in diesem Beitrag nicht explizit eingegangen. Hier sei auf die weiterführende Literatur verwiesen.⁵⁴ **85**

Um den Risikogehalt eines einzelnen Risikos zu quantifizieren, das heißt, um Risiken in Zahlenwerten abzubilden, eignen sich Risikomaße. Darunter versteht man Kennzahlen, die dem Risikogehalt einer Position oder Variablen einen numerischen Wert zuordnen und damit eine Vergleichbarkeit von Handlungsalternativen hinsichtlich ihres Risikogehalts ermöglichen. Im mathematischen Sinne ist ein Risikomaß eine Abbildung der Zufallsvariable auf reelle Zahlen. Dazu zählen Lage- und Streuungsparameter sowie Zusammenhangsmaße.⁵⁵ **86**

⁵³ Vgl. hierzu *Romeike*, Risikomanagement, S. 55 ff.

⁵⁴ Vgl. vertiefend vor allem *Romeike*, Risikomanagement, sowie die Artikel-Serie zu Risikomaßen: *Gleißner*, Risikomaße und Bewertung, Teil 1: Grundlagen – Entscheidungen unter Unsicherheit und Erwartungsnutzentheorie; *Gleißner*, Risikomaße und Bewertung, Teil 2: Downside-Risikomaße – Risikomaße, Safety-First-Ansätze und Portfoliooptimierung; *Gleißner*, Risikomaße und Bewertung, Teil 3: Kapitalmarktmodelle – Alternative Risikomaße und Unvollkommenheit des Kapitalmarkts und die dort zitierte Spezialliteratur.

⁵⁵ Vgl. *Nguyen/Romeike*, Versicherungswirtschaftslehre – Grundlagen für Studium und Praxis, S. 6 f.

VIII. Aggregation von Risiken

- 87 Eine wesentliche Zielsetzung des Risikomanagements – mit Hilfe der Methoden der Risikoaggregation – ist die Bestimmung der Gesamtrisikoposition des Unternehmens sowie eine Ermittlung der relativen Bedeutung der Einzelrisiken unter Berücksichtigung von Wechselwirkungen bzw. Abhängigkeiten (beispielsweise abgebildet mit Hilfe von Korrelationen, logischen Kausalbeziehungen oder Copulae⁵⁶) zwischen diesen Einzelrisiken.⁵⁷

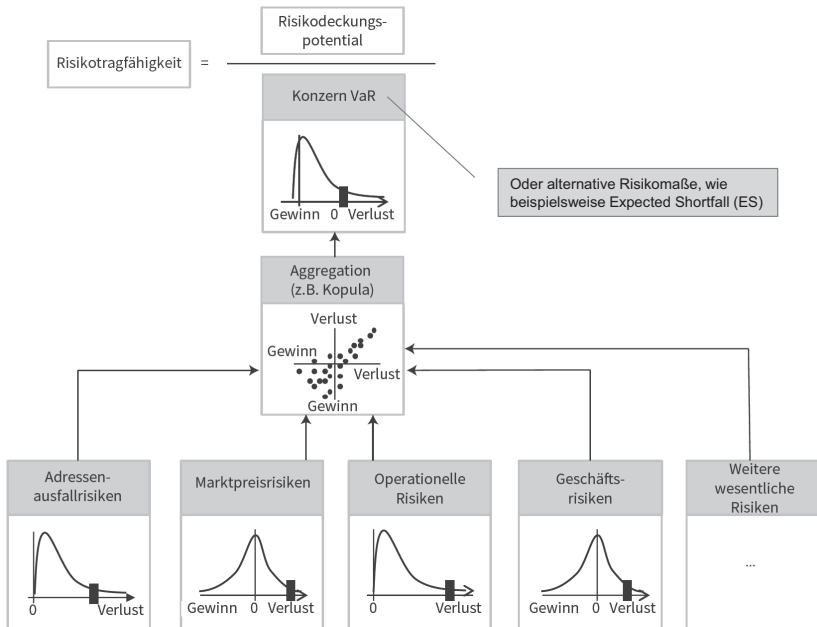


Abbildung 9: Risikodeckungspotenzial und Risikotragfähigkeit⁵⁸

- 88 Die Risikoaggregation kann erst durchgeführt werden, wenn die Wirkungen der Risiken unter Berücksichtigung ihrer jeweiligen Eintrittswahrscheinlichkeit bzw. Häufigkeit, ihrer Schadensverteilung (quantitative Auswirkung) sowie ihrer Wechselwirkungen untereinander durch ein geeignetes Verfahren ermittelt

56 Vgl. vertiefend *Mai/Scherer*, *Simulating Copulas* (Stochastic Models, Sampling Algorithms and Applications).

57 Vgl. *Gleißner/Romeike*, *Risikomanagement – Umsetzung, Werkzeuge, Risikobewertung*, S. 31 ff.; *Romeike/Hager*, *Erfolgsfaktor Risikomanagement 3.0: Lessons learned, Methoden, Checklisten und Implementierung* sowie *Nguyen/Romeike*, *Versicherungswirtschaftslehre – Grundlagen für Studium und Praxis*.

58 Quelle: Eigene Abbildung in Anlehnung an *Andrae/Hellmich/Schmaltz*, *Bankaufsichtliches Risikomanagement – Grundlagen und Anwendung, Regulatorischer Anforderungen*, S. 430.

werden. Das grundsätzliche methodische Vorgehen der Risikoaggregation ist in Abbildung 9 skizziert. Abbildung 9 verdeutlicht auch den Unterschied zwischen Risikotragfähigkeit (als Quotient) und Risikodeckungspotenzial (beispielsweise ermittelt über die freie Liquidität).

Eine Aggregation aller relevanten Risiken ist erforderlich, weil sie auch in der Realität zusammen auf die Liquidität bzw. das Eigenkapital wirken. Es ist damit offensichtlich, dass alle Risiken gemeinsam die Risikotragfähigkeit eines Unternehmens belasten (siehe Abbildung 9 sowie Abbildung 10). 89

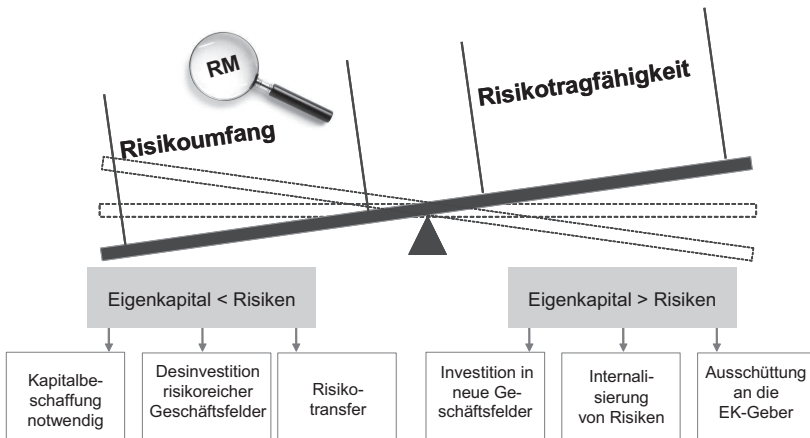


Abbildung 10: Die Gesetzmäßigkeit der Risikotragfähigkeit⁵⁹

IX. Maßnahmen zur Risikosteuerung

Sollte der vorhandene Risikoumfang eines Unternehmens gemessen an der Risikotragfähigkeit zu hoch sein (siehe Abbildung 10), werden zusätzliche Maßnahmen der Risikobewältigung erforderlich. Die Kenntnis der relativen Bedeutung der Einzelrisiken (Sensitivitätsanalyse) ist für ein Unternehmen in der Praxis wichtig, um die Maßnahmen der Risikofinanzierung und -steuerung zu priorisieren. 90

⁵⁹ Quelle: Romeike/Hager, Erfolgsfaktor Risikomanagement 3.0: Lessons learned, Methoden, Checklisten und Implementierung, S. 136, sowie Romeike, Risikomanagement, S. 43.

Teil 2 Übergreifende Themen und Herausforderungen – Risiko und Governance

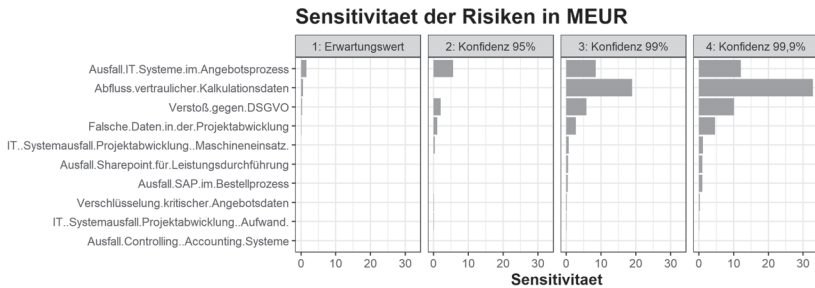


Abbildung 11: Sensitivitätsanalyse⁶⁰

- 91** In Abbildung 11 sind die Ergebnisse einer Sensitivitätsanalyse exemplarisch dargestellt. Mit Hilfe einer Sensitivitätsanalyse werden mögliche Auswirkungen relevanter Risiken auf das Unternehmen ermittelt (Top-X Reihenfolge der Risiken hinsichtlich Wirkung auf eine Zielgröße (EBIT, Projektbudget, Anzahl beförderter Passagiere etc.)). Methodisch basiert die Sensitivitätsanalyse entweder auf der Berechnung der Korrelationen oder einer Sortierung der Risiken nach deren Sensitivität in Bezug auf die definierte Zielgröße. In Abbildung 11 erfolgt die Sensitivitätsberechnung basierend auf dem EBIT-Effekt in MEUR. Anschließend werden die Sensitivitäten in Form eines Tornado-Chart grafisch ausgegeben. Ein Konfidenz/Sicherheitsniveau von 95 % spiegelt hierbei einen 20-Jahres-Zeithorizont wider. Ein 99%-Konfidenzniveau entspricht einem 100-Jahres-Ereignis. Beim 99,9%-Sicherheitsniveau werden sog. Stressszenarien in den Fokus gesetzt.
- 92** Die Prozessphase der Risikosteuerung zielt darauf ab (siehe Abbildung 12), die Risikolage des Unternehmens positiv zu verändern bzw. ein ausgewogenes Verhältnis zwischen Ertrag (Chance) und Verlustgefahr (Risiko) zu erreichen, um den Unternehmenswert zu steigern oder die Resilienz (im Sinne einer Widerstandsfähigkeit) des Unternehmens zu erhöhen.

⁶⁰ Quelle: Eigene Abbildung.

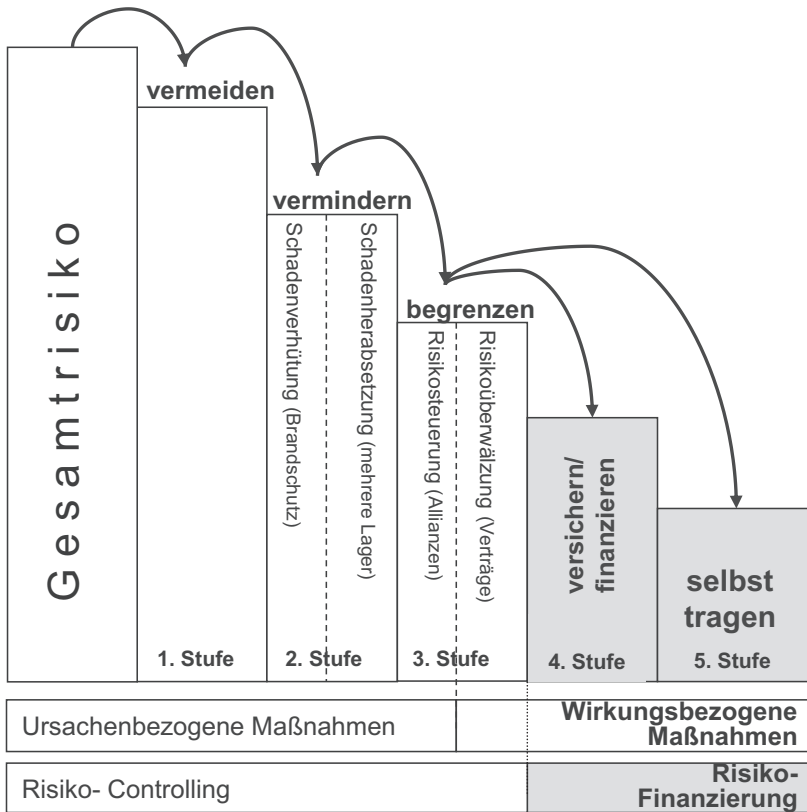


Abbildung 12: Risikosteuerung in der Praxis⁶¹

Die Risikosteuerung und -kontrolle umfasst alle Mechanismen und Maßnahmen zur Beeinflussung der Risikosituation, entweder durch eine Verringerung der Eintrittswahrscheinlichkeit bzw. -häufigkeit und/oder des Schadensausmaßszenarios. Dabei sollte die Risikosteuerung und -kontrolle mit den in der Risikostrategie definierten Zielen sowie den allgemeinen Unternehmenszielen übereinstimmen. Ziele dieser Prozessphase sind die Vermeidung von nicht akzeptablen Risiken sowie die Reduktion und der Transfer von nicht vermeidbaren Risiken auf ein akzeptables Maß. Eine optimale Risikosteuerung und -bewältigung ist

⁶¹ Quelle: *Romeike/Hager*, Erfolgsfaktor Risikomanagement 4.0: Methoden, Beispiele, Checklisten – Praxishandbuch für Industrie und Handel, S. 138 sowie *Romeike*, Risikomanagement, S. 45.

dabei diejenige, die durch eine Optimierung der Risikopositionen des Unternehmens den Unternehmenswert steigert.

X. Unterschiedliche Reifegrade im Risikomanagement

- 94 In Abbildung 13 ist eine Reifegradtreppe (Risk Maturity Model) wiedergegeben, die die wesentlichen Schritte von einem initialen Risikomanagementsystem hin zu einem „Leading“-System skizziert.

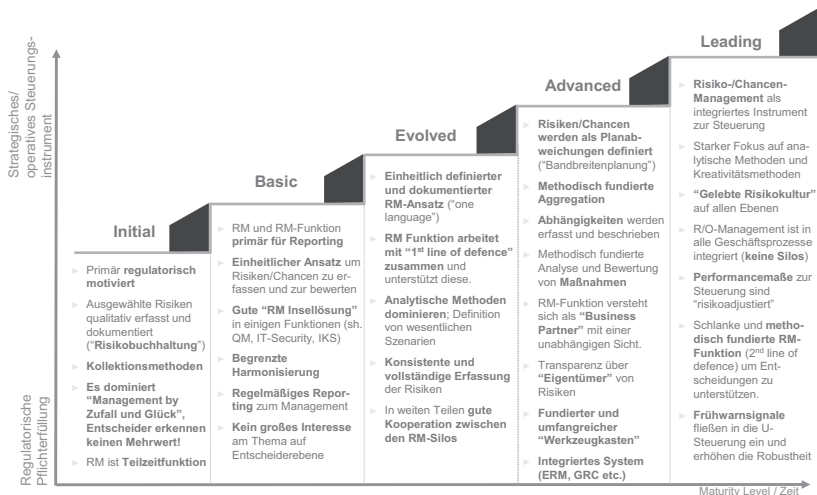


Abbildung 13: Reifegradtreppe im Risikomanagement⁶²

- 95 Der Reifegrad „Initial“ beschreibt ein Risikomanagementsystem, das primär umgesetzt wird, um grundlegende regulatorische bzw. gesetzliche Anforderungen zu erfüllen. Durch die Einführung des StaRUG (im Jahr 2021) sowie die Neufassung des gesetzlich verpflichtenden Prüfungsstandards IDW PS 340 (im Jahr 2020⁶³) muss in diesem Kontext darauf hingewiesen werden, dass ein Risikomanagementsystem basierend auf dem Reifegrad „Initial“ keinesfalls mehr die gesetzlichen Anforderungen erfüllt. So bedingt ein wirksames Risikomanagementsystem (im Sinne IDW PS 340 sowie des DIIR RS Nr. 2 und des StaRUG) eine Risikoquantifizierung und Risikoaggregation.⁶⁴

62 Vgl. Romeike, Risikomanagement, S. 57, sowie Romeike, GRC aktuell 01/2018, 41–45.

63 Vgl. IDW, Neufassung des IDW Prüfungsstandards: Die Prüfung des Risikofrüherkennungssystems (IDW PS 340 n. F.), Stand: 27.5.2020.

64 In Textziffer 11 fordert der IDW PS 340: „Bestandsgefährdende Entwicklungen können auch aus dem Zusammenwirken mehrerer Risiken resultieren, die bei isolierter Betrachtung an sich nicht bestandsgefährdend sind. Bei der Beurteilung, ob eine bestandsgefährdende Entwicklung vorliegt, ist daher eine Aggregation der Risiken vorzunehmen.“

Zwischen dem Reifegrad des Risikomanagements und dem Einsatz unterschiedlicher Werkzeuge und Methoden besteht ein direkter und zwingender Zusammenhang. Auf der Stufe eines initialen Risikomanagements sowie auf der Stufe „Basic“ dominieren in der Praxis häufig Kollektionsmethoden, d. h. relativ einfache Methoden zur Identifikation und Bewertung von Risiken (etwa basierend auf Checklisten oder standardisierten Risikolandkarten). Auf der Reifegrad-Stufe „Evolved“ erfolgt immerhin bereits eine gute Kooperation zwischen den existierenden „Silos“ im Unternehmen, die sich mit Risiken beschäftigen. Beispielsweise zwischen Risikomanagement, dem Compliance Management, dem Controlling oder dem Qualitätsmanagement. Neben Kollektionsmethoden kommen auch analytische Methoden zum Einsatz. Bei „Advanced“ erfolgt zum einen eine Verknüpfung von Planung und Risikomanagement in Form einer „Bandbreitenplanung“ sowie zum anderen die Integration von Compliance Management und Risikomanagement zu einem integrierten ERM-System (Enterprise-Risk-Management-System) bzw. GRC-System (Governance, Risk & Compliance-System). Dies bedingt auch den Einsatz eines fundierten und umfassenden Werkzeugkastens, etwa von quantitativen Methoden zur methodisch fundierten Aggregation von Risiken (siehe hierzu die Ausführungen zu den gesetzlichen Anforderungen resultierend aus dem StaRUG sowie dem IDW PS 340). In der höchsten Ausbaustufe („Leading“) wird Risiko-/Chancenmanagement als strategisches und wertorientiertes Instrument der Unternehmenssteuerung verstanden.⁶⁵ Compliance Management, IKS und Controlling sind hier selbstverständlich integriert in ein einheitliches Methodensetting und System. Außerdem ist Risiko- und Chancenmanagement (bzw. Risk-/Opportunity-Management) voll integriert in die Geschäftsprozesse. Basierend hierauf wird Risiko-/Chancenmanagement in der gesamten Organisation gelebt (Risikokultur) und ist einer der Kernprozesse des Unternehmens.

XI. Fazit und Ausblick

„Management ist die Kunst, mit anderen Leuten zusammen Dinge zu erledigen!“, so wird die US-amerikanischen Autorin *Mary Parker Follett* zitiert, die Unternehmen als soziale Systeme betrachtete. **97**

Auch für ein wirksames Risikomanagement gilt, dass der wesentliche Erfolgsfaktor ist, dass Menschen den Umgang mit Risiken (und Chancen) tagtäglich leben. So zeigen Statistiken in der Luftfahrt und der Seefahrt, dass der Risikofaktor Mensch bei katastrophalen Unfällen eine überragende Rolle spielt – Schätzungen zufolge sind mindestens 90% aller Unfälle auf das Fehlverhalten Einzelner zurückzuführen.⁶⁶ **98**

⁶⁵ Vgl. vertiefend *Gleißner/Romeike*, Der Aufsichtsrat 4/2020, 55–57.

⁶⁶ Vgl. *Romeike/Hager*, Erfolgsfaktor Risikomanagement 4.0: Methoden, Beispiele, Checklisten – Praxishandbuch für Industrie und Handel.

- 99 Das obige Zitat könnte man für das Risikomanagement ein wenig modifizieren:
- Risikomanagement ist die Kunst, mit anderen Leuten Risiken und Chancen professionell zu antizipieren und sicher durch die stürmische See zu kommen!
- 100 Die „Kunst“ des Risikomanagements beherrschte nicht nur Odysseus nahezu perfekt, sondern beispielsweise auch der Polarforscher Sir *Ernest Henry Shackleton*. Heutige Führungskräfte und auch Risikomanager könnten von seinen Erfahrungen eine Menge lernen.⁶⁷
- 101 Der Polarforscher Sir *Ernest Henry Shackleton*, geboren am 15.2.1874 im County Clare in Irland, zählt zweifellos zu den besten Risikomanagern und war einer der herausragendsten Führungspersönlichkeiten überhaupt. Am 5.12.1914 bricht er mit 27 Männern an Bord des Schiffes *Endurance* (deutsch: Standhaftigkeit, Ausdauer) von Südgeorgien aus auf. *Shackleton* hatte sich zum Ziel gesetzt, als erster Mensch mit Schiff, Hundeschlitten und zu Fuß die Antarktis zu durchqueren.
- 102 Es wird berichtet, dass *Shackleton* seine Mannschaft mit der wohl erfolgreichsten Stellenanzeige aller Zeiten fand: „Männer für gefährliche Reise gesucht. Geringer Lohn, bittere Kälte, monatelange völlige Dunkelheit, ständige Gefahr. Sichere Heimkehr zweifelhaft. Ehre und Ruhm im Erfolgsfalle.“ Über 5.000 Kandidaten bewarben sich. Schließlich baute *Shackleton* seine Mannschaft um einen Kern erfahrener und krisenerprobter Fachleute auf. Außerdem wählte *Shackleton* einen zuverlässigen Stellvertreter, der seine Führungsgrundsätze teilte und vor allem loyal war. Aber er wollte keinen Ja-Sager. Die Idealbesetzung fand er schließlich in *Frank Wild*, der außerdem noch als Bindeglied zwischen der Mannschaft und dem Boss fungierte. Man berichtet über *Wild*, dass er das Talent hatte, die Männer dazu zu animieren, genau das zu tun, was erforderlich war, auch ohne etwas zu sagen. Bei der Auswahl aller anderen Mitglieder seiner Expedition waren *Shackleton* ebenfalls Eigenschaften wie Loyalität, Heiterkeit, Anständigkeit, mentale und physische Stärke, Optimismus, Forscherdrang, Erfahrung und Fachkenntnis die wichtigsten Voraussetzungen, die er erwartete.
- 103 Welche Rolle spielen bei einem Einstellungsgespräch in der heutigen Zeit Eigenschaften wie Loyalität, Heiterkeit, Anständigkeit, mentale und physische Stärke, Optimismus oder Forscherdrang?
- 104 Soziale Kompetenz, Wertvorstellungen sowie die Lebens- und Arbeitseinstellung der Kandidaten waren *Shackleton* ebenfalls sehr wichtig. Auch prüfte er die Bewerber in der Praxis und ließ sie Proviantstöße schleppen, Kartoffeln schälen und die Küche schrubben. *Shackleton* bemühte sich dabei immer, niemanden mit falschen Versprechungen in die Irre zu führen, sondern sorgte dafür, dass jeder genau wusste, was von ihm erwartet wurde. Neben seinen intensiven Bemü-

67 Vgl. vertiefend *Erben/Romeike*, Allein auf stürmischer See – Risikomanagement für Einsteiger, S. 123 ff.

hungen um eine stimmige Zusammensetzung des Teams rüstete er die Mannschaft mit modernsten Werkzeugen aus: Schlitten, Skier, Äxte, Seile, Werkzeuge und elektrische Beleuchtung waren damals „State of the Art“. *Shackleton* war der Meinung, dass veraltete, unzuverlässige Werkzeuge nur unnötig belasten.

Auch hier kann eine Brücke zum Risikomanagement gebaut werden. Viele Unternehmen verharren im Risikomanagement auf einem niedrigen Reifegrad, weil sie eben gerade nicht mit „State of the art“-Werkzeugen arbeiten. Dies führt wiederum dazu, dass in der Organisation die Methoden und Werkzeuge nicht akzeptiert werden und man nur widerwillig mitmacht, damit der Risikomanager „endlich Ruhe gibt“. So quält man sich beispielsweise durch meterlange Checklisten und fragt sich nach dem Sinn der Übung. Und vor lauter Abhaken von Szenarien aus der Vergangenheit vergisst man den Blick auf die wirklich relevanten Szenarien, die uns in der Zukunft erwarten könnten. **105**

Die Strukturierung des Tages wurde exakt geplant. Die Männer erarbeiteten genaueste Anweisungen für Arbeit und Freizeit. Er kannte keine traditionellen Hierarchien. Vielmehr wurde von jedem erwartet, einen Beitrag zu sämtlichen Arbeiten an Bord des Schiffes zu leisten. So halfen die Matrosen etwa bei wissenschaftlichen Messungen und Proben. Umgekehrt gingen die Wissenschaftler den Seeleuten bei deren täglicher Arbeit zur Hand. **106**

Eine der wichtigsten Maximen *Shackletons* war: Sich ein neues Ziel setzen, wenn das alte nicht erreicht werden kann, dieses mit allem Einsatz verfolgen – aber noch vor das Ziel den Menschen selbst an die oberste Stelle setzen. Und so sollte es passieren: Auf ihrer Reise nach Süden stieß die *Endurance* bereits am 7.12.1914 – ungewöhnlich weit im Norden – auf das erste Packeis. Trotz des immer dichter werdenden Eises segelte das Schiff weiter Richtung Weddellmeer. Ende Januar 1915 saß die *Endurance* dann endgültig im Packeis fest. Wochenlang versuchte die Mannschaft, das Packeis zu durchbrechen, scheiterte aber immer wieder. Das Schiff war „wie eine Mandel in einer Tafel Schokolade“ stecken geblieben. Am 24. Februar verwandelte *Shackleton* das Schiff schließlich in ein Winterquartier. Und damit begann das vorbildliche Risiko- und Krisenmanagement. Denn alles wurde noch viel schlimmer. Nachdem das Packeis das Schiff gefährlich nach Norden getrieben hatte, wurde es schließlich vom Eis zermalmt und versank. Die Männer mussten beißende Kälte ertragen und verbrachten fast vier Monate in der eisigen Dunkelheit der langen Polarnacht. Das neue Ziel von *Shackleton* hieß nun: Rettung der Mannschaft. Mit den drei übriggebliebenen Rettungsbooten landeten die Schiffbrüchigen auf der unbewohnten Insel Elephant Island. *Shackleton* hatte den Plan, mit dem seetüchtigsten der drei Rettungsboote und fünf Männern das 700 Seemeilen nördlich gelegene Südgeorgien anzusteuern, um von der dortigen Walfangstation Hilfe zu holen. Und sie schafften es: Am 10.5.1916 landete das Schiff auf der unbewohnten Seite der Insel. Nach weiteren 36 Stunden Fußmarsch und einer Gletscher- und Gebirgsüberquerung erreichten die Männer die Walfangstation und konnten auch die zurückgebliebene Mannschaft retten. **107**

- 108** Der Aufbau dieser solidarischen und loyalen Mannschaft war die Voraussetzung für *Shackletons* (Unternehmens-)Philosophie bzw. Risikokultur. Und obwohl die Gruppe äußerst heterogen in Bezug auf Beruf, Temperament und soziale Herkunft war, bildete sie ein herausragendes Team.
- 109** Für heutige Risikomanagement-Systeme können wir hieraus eine ganze Menge lernen. Grundsätzlich existieren vier Erfolgsfaktoren, damit ein Risikomanagement wirksam ist und einen Mehrwert stiftet.
1. Risikomanagement muss gelebt werden („Risiko- und Fehlerkultur“). Hierbei geht es vor allem um die Frage, wie wir im Unternehmen mit Fehlern und Risiken umgehen. Vielfach gelten Fehler und Risiken als etwas Schlechtes, das wir tunlichst vermeiden müssen. Dabei sind Fehler und Risiken immer dann am nützlichsten, wenn alle davon lernen. Entscheidend ist daher eine gelebte „nicht strafende Fehlerkultur“ (non punitive). In der Praxis dominiert nicht selten eine PuMist-Kultur (Punish Mistakes).⁶⁸
 2. Risikomanagement benötigt einen Prozess in Form eines kontinuierlichen Regelkreises. „Kontinuierlich“ bedeutet, dass sich eine Organisation permanent mit sog. bestandsbedrohenden Risikoszenarien zu beschäftigen hat und nicht nur in einer festgelegten Frequenz, beispielsweise „einmal im Jahr“.
 3. Risikomanagement muss in eine Organisation eingebettet werden und sollte keinesfalls als isolierter „Silo“ betrachtet werden.
 4. Risikomanagement basiert auf adäquaten und auf die Fragestellung angepassten Methoden. Für die Analyse von Währungsrisiken werden anderen Methoden angewendet, als wenn Risiken aus der Supply Chain oder Risiken aus Compliance-Verstößen analysiert werden.
- 110** Hierbei ist es wichtig, dass Unternehmen als (komplexes und soziales) System betrachtet werden. Und Unternehmen selbst sind wieder Teil eines noch größeren Gesamtsystems (mit einer Menge systemischer Risiken etc.). Und Systemgrößen dürfen keinesfalls als starr betrachtet werden, sondern als sich ständig verändernde Größen. Ein System ist ein Gebilde mit inneren Gesetzmäßigkeiten, die beachtet werden müssen. Lebendige Systeme haben eigene Bedürfnisse und eigene Ziele. Diese Komplexität, Vielgestaltigkeit und Innergesetzmäßigkeit ist insgesamt mit einer hohen Unsicherheit behaftet und macht daher eine Vorhersagbarkeit (des Verhaltens von Teilsystemen oder des Gesamtsystems) nur bedingt möglich. Feststellbar sind eher Makro-Eigenschaften der (Teil-)Systeme, die über größere Bereiche (zeitlich, räumlich oder strukturell) festzustellen sind, beispielsweise deren Wahrscheinlichkeiten.
- 111** Die Systemtheorie bietet uns hier einen Ansatz, um ein System interdisziplinär zu analysieren. So können beispielsweise biologische Zellen, der Mensch insgesamt, eine Organisation, ein Staat, aber auch Computernetzwerke als Systeme betrachtet und systemtheoretisch beschrieben werden. Die Systemtheorie „blickt

⁶⁸ Zur Bedeutung der Compliance-Kultur für den Erfolg des Compliance-Risiko-Managements → *Schulz*, Kap. 1 Rn. 68 ff.

über den Tellerrand“ einer Einzeldisziplin und hat immer schon das Ziel verfolgt, der Zersplitterung des Wissens in den wissenschaftlichen Disziplinen entgegenzuwirken. Dieser ganzheitliche Ansatz der Systemtheorie sollte beim Aufbau eines wirksamen Risikomanagementsystems immer berücksichtigt werden.

10. Kapitel

Auditverfahren: Compliance als Dauerpflcht¹

I. Einleitung

Alle Auditverfahrensvorschriften schreiben mit fast gleichem Wortlaut vor, das Management als oberste Leitung habe die dauerhafte oder fortdauernde Wirksamkeit des Compliance-Management-Systems (CMS) sicherzustellen. Verkannt wird diese Dauerpflcht, wenn Zertifikate nach Audits schon gegen die bloße Vorlage eines sog. „Rechtskatasters“ erteilt werden. Ein CMS wirkt nur dauerhaft, wenn einschlägige Rechtspflichten nicht nur einmalig ermittelt und im Audit vorgezeigt werden, sondern aktualisiert, delegiert, erfüllt, kontrolliert und dokumentiert werden, und zwar dauerhaft. Ansonsten wird der Zweck des CMS nicht erreicht, Vorstand und Geschäftsführung vor dem Vorwurf des Organisationsverschuldens zu schützen sowie Beweise für den unvorhersehbaren Zeitpunkt von Rechtsverstoß und Schadenseintritt zu sichern. Für Organisationsverschulden haften Organe ihrer Gesellschaft. Ein Zertifikat ohne Prüfung der dauerhaften Wirksamkeit des CMS ist falsch und begründet die sog. „Expertenhaftung“ von Auditoren und Umweltgutachtern gegenüber der zertifizierten Gesellschaft und gegenüber Dritten, die auf die Richtigkeit des Zertifikats vertraut haben. 1

II. Die Dauerpflcht zur Sicherstellung der dauerhaften Wirksamkeit des CMS nach DIN und EMAS

Der Satz, dass die oberste Leitung das jeweilige Managementsystem bewerten muss, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen, kommt in jedem der folgenden aufgelisteten Managementsysteme vor: 2

1. DIN ISO 45001 – Managementsysteme für Sicherheit und Gesundheit bei der Arbeit – Anforderungen mit Anleitung zur Anwendung
„9.3 Managementbewertung
Die oberste Leitung muss das Managementsystem für Sicherheit und Gesundheit bei der Arbeit (SGA-Managementsystem) der Organisation in geplanten Abständen bewerten, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen.“

1 Dem Kapitel liegt der Beitrag *Rack*, Auditverfahren: Compliance als Dauerpflcht, CB Heft 1–2 2024, 23 ff. zugrunde, der für die Veröffentlichung im vorliegenden Buch aktualisiert und erweitert wurde.

2. DIN ISO 37301 – Compliance-Managementsysteme – Anforderungen mit Leitlinien zur Anwendung
„8.2 Festlegung der Steuerungen und Verfahren
Die Organisation muss Steuerungen für das Management ihrer Compliance-Verpflichtungen und die damit verbundenen Compliance-Risiken einführen. Diese Steuerungen müssen aufrechterhalten, regelmäßig bewertet und geprüft werden, um ihre dauerhafte Wirksamkeit sicherzustellen.“
3. DIN EN ISO 9001:2015 Qualitätsmanagementsysteme – Anforderungen
„9.3 Managementbewertung
9.3.1 Allgemeines
Die oberste Leitung muss das Qualitätsmanagementsystem der Organisation in geplanten Abständen bewerten, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit sowie dessen Angleichung an die strategische Ausrichtung der Organisation sicherzustellen.“
4. DIN EN ISO 14001 – Umweltmanagementsysteme – Anforderungen mit Anleitung zur Anwendung
„9.3 Managementbewertung
Die oberste Leitung muss das Umweltmanagementsystem der Organisation in geplanten Abständen bewerten, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen.“
5. DIN EN ISO 50001 – Energiemanagementsysteme
„9.3 Managementbewertung
5.1.1 Die oberste Leitung muss das EnMS der Organisation in geplanten Abständen bewerten, um dessen fortdauernde Eignung, Angemessenheit, Wirksamkeit und Übereinstimmung mit der strategischen Ausrichtung der Organisation sicherzustellen.“
6. DIN EN ISO/IEC 27001 Informationssicherheitsmanagementsysteme
„9.3 Managementbewertung
Die oberste Leitung muss das Informationssicherheitsmanagementsystem der Organisation in geplanten Abständen bewerten, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen.“
7. Verordnung (EG) Nr. 1221/2009 über die freiwillige Teilnahme von Organisationen an einem Gemeinschaftssystem für Umweltmanagement und Umweltbetriebsprüfung (EMAS III)
„Anhang I Teil B
B.4 Einhaltung von Rechtsvorschriften
Nach EMAS registrierte Organisationen oder Organisationen, die sich nach EMAS registrieren möchten, müssen nachweisen, dass sie alle nachstehend genannten Bedingungen erfüllt haben:
1) Sie haben alle geltenden rechtlichen Verpflichtungen im Umweltbereich ermittelt und kennen deren Auswirkungen auf ihre Organisation;

- 2) sie sorgen für die Einhaltung der Umweltvorschriften, einschließlich Genehmigungen und zulässiger Grenzwerte in Genehmigungen, und legen die entsprechenden Nachweise vor;
- 3) sie verfügen über Verfahren, die es ihnen ermöglichen, die Einhaltung der Umweltvorschriften dauerhaft sicherzustellen.“

III. Die Beweislast für Vorstände und Geschäftsführer

Vorstände und Geschäftsführer tragen nach § 93 AktG die Beweislast dafür, dass sie ihre Organisationspflichten erfüllt haben. Diese Beweislastumkehr gilt auch für GmbH-Geschäftsführer und zwingt sie dazu, sich dauerhaft legal zu verhalten und dafür zu sorgen, dass ihre Angestellten ebenfalls dauerhaft alle an sie delegierten Rechtspflichten einhalten. Mit einem CMS betreiben Geschäftsleiter ständige Beweissicherung. Diese Beweissicherungsfunktion wird nicht erfüllt, wenn nur am Tag des Audits ein Rechtskataster vorgelegt wird, das gerade nicht nachweist, dass die darin aufgelisteten Rechtspflichten auch dauerhaft eingehalten werden. Es fehlt der Nachweis der Delegation, der Aktualisierung, der Erfüllung, ihrer Kontrolle und Dokumentation. **3**

IV. Die Unvorhersehbarkeit von Rechtsverstößen als Grund für Compliance als Dauerpflicht

Die fortdauernde Kontrolle ist für einen erfolgreichen Entlastungsbeweis unverzichtbar, weil der Beweis am Tag des Rechtsverstoßes mit Schadensereignis zu führen ist. Der Eintritt von Rechtsverstoß und Schadensereignis sind ungewiss. Der Entlastungsbeweis ist deshalb an einem noch unbekannten Tag X zu führen. Wäre der Rechtsverstoß im Unternehmen vorhersehbar, könnte er abgewendet werden. Um am ungewissen Zeitpunkt des Rechtsverstoßes mit Schadenseintritt nicht ohne entlastenden Kontrollnachweis zu sein, sind Vorstände und Geschäftsführer verpflichtet, vor allem auch im eigenen Interesse, ihre Pflicht zur Legalitätskontrolle zu erfüllen. Stichproben reichen zur Entlastung nicht aus. Eine Kontrolllücke nimmt dem Entlastungsbeweis die angestrebte Wirkung, den Vorwurf des Organisationsverschuldens zu widerlegen. **4**

V. Zertifikate sind bloße Momentaufnahmen ohne Nachweis dauerhafter Wirksamkeit eines CMS

Zu den erfolglosen Entlastungsversuchen gehört der Hinweis, das Unternehmen sei zertifiziert. Das Zertifikat liefere dem Unternehmen den Entlastungsbeweis vom Vorwurf des Organisationsverschuldens. Ein Zertifikat enthält aber nur abstrakt die Übereinstimmung mit einer Organisationsnorm wie der DIN ISO 14001 über Umweltmanagementsysteme oder nach EMAS oder nach der DIN ISO 9001 zum Qualitätsmanagementsystem. **5**

Ein Zertifikat enthält jedoch keinerlei Aussage über die konkrete Organisation des jeweiligen Unternehmens. Ob gerade die für einen Produktfehler in Betracht **6**

kommenen Ursachen erfasst worden sind, lässt sich dem Zertifikat nicht entnehmen.² Ein Zertifikat ersetzt kein Managementsystem, dessen Zweck darin besteht, den Beweis für die Entlastung vom Vorwurf des Organisationsverschuldens zu führen. Ein Zertifikat ersetzt vor allem nicht den Entlastungsbeweis, wie er nach der ständigen Rechtsprechung zum Organisationsverschulden und zur herrschenden Meinung im Gesellschaftsrecht gefordert wird. Zertifiziert ist nicht exkulpiert. Die Gründe dafür, dass ein Zertifikat keine haftungsrechtliche Entlastungswirkung gegen den Vorwurf des Organisationsverschuldens haben kann, ist ausführlich zu behandeln, insbesondere auch deshalb, weil sich dieser Irrtum hartnäckig hält, obwohl die Rechtsprechung und die herrschende Meinung im Organisationsrecht eindeutig Zertifikate als Entlastungsbeweise ablehnen.

- 7 Auch eine validierte Umwelterklärung nach der EG-Öko-Audit-Verordnung begründet keine widerlegliche Vermutung, dass das Unternehmen dauerhaft alle Umweltvorschriften einhält.³ Die deutschen Haftpflichtversicherer haben davon abgesehen, den Betrieben, die am Auditsystem teilnehmen, Rabatte einzuräumen, da das Umweltaudit weder eine absolute und objektive Aussage über die Umweltsituation treffe, noch die Eintrittswahrscheinlichkeit eines Unfalls messbar gesenkt wird.⁴

VI. Das Stichprobenargument in Rechtsprechung und Literatur

- 8 Das erste Argument gegen die Entlastungswirkung von Zertifikaten ist das Stichprobenargument. Audits mit dem Ergebnis eines Zertifikats stellen Stichproben und bloße Momentaufnahmen dar. Stichproben reichen jedoch zur Entlastung vom Vorwurf der Verletzung von Aufsichtspflichten nicht aus.
- 9 Seit dem Kutscher-Urteil von 1911⁵ gilt dies als Maßstab für den Umfang der Kontrollpflicht und als Anforderung für einen erfolgreichen Entlastungsbeweis. Von einem Pferdeomnibus-Kutscher wurde ein Passant überfahren und tödlich verletzt. Der Kutscher war mehrfach mit Verkehrswidrigkeiten aufgefallen und galt deshalb als unzuverlässig. Der Vorstand hat sich auf seine Unkenntnis über die Unzuverlässigkeit dieses Einzelnen von fünftausend Kutschern berufen, für die der Vorstand verantwortlich war. Die Berliner Verkehrsbetriebe haben sich mit ihrer Betriebsorganisation ohne Erfolg zu entlasten versucht. Eine größere Zahl von Kontrolleuren würde unausgesetzt den gesamten Wagenverkehr in Berlin überwachen. Diesen Entlastungsversuch hat das Reichsgericht abgelehnt. Die Aufsichtsorganisation habe im konkreten Schadensfall versagt. Vor allem

2 *Spindler*, Unternehmensorganisationspflichten: Zivilrechtliche und öffentlich-rechtliche Regelungskonzepte, S. 814.

3 *Falke*, ZUR 1995, 4, 5; *Spindler*, Unternehmensorganisationspflichten: Zivilrechtliche und öffentlich-rechtliche Regelungskonzepte, S. 813.

4 *Pohl*, BB 1998, 381, 385; *Spindler*, Unternehmensorganisationspflichten: Zivilrechtliche und öffentlich-rechtliche Regelungskonzepte, S. 813.

5 RG vom 14.12.1911 (VI 75/11), in: RGZ 78 S. 107 – Kutscher-Urteil.

habe sie – so wörtlich das Reichsgericht – nur Stichproben geliefert. Die Kontrolle hätte im Zeitpunkt des Schadensereignisses nachgewiesen werden müssen.

Diese Entscheidung von 1911 ist die Leitentscheidung für eine Serie von Urteilen, in denen die Beklagten sich vom Vorwurf des Organisationsverschuldens mit dem Argument zu entlasten versucht haben, es bestehe nachweislich eine umfassende Aufsichtsorganisation mit ausführlichem Regelwerk. Der Entlastungsversuch scheiterte regelmäßig daran, dass die Anwendungen der Aufsichtsorganisation im Zeitpunkt des Schadensereignisses und vor allem im speziellen Einzelfall des schädigenden Kutschers nicht nachgewiesen werden konnten und deshalb die Haftung mit der verletzten Pflicht zur Aufsichtsorganisation begründet wurde. Der Entlastungsbeweis nach § 831 BGB blieb erfolglos. Das Unternehmen konnte konkret weder vortragen noch beweisen, ob gerade der Kutscher, der den Passanten überfahren hat, auf seine konkrete Zuverlässigkeit im Verkehr zeitnah zum Unfall kontrolliert wurde. **10**

Ausschlaggebend für die fehlende Entlastungswirkung bei Zertifizierungen ist, dass diese nach DIN ISO 9001 oder 14001 oder 27001 oder 37301 sowie anderen Zertifizierungssystemen stets nur punktuelle Momentaufnahmen einer Organisation darstellen, die keinerlei Gewähr dafür bieten, dass sich Missstände nicht auch nach dem Zeitpunkt der Zertifizierung einschleichen. Die Rechtsprechung fordert von der Organisation eine dauerhafte und kontinuierliche Überwachung der Mitarbeiter. **11**

Zertifizierungen stellen nur zeitlich begrenzte Kontrollen einer Organisation dar und bieten keine Gewähr für die spätere Befolgung des Standards.⁶ **12**

Im Kutscher-Fall hat das Reichsgericht entschieden, dass über den vollen Zeitraum eines Dienstvertrages die Zuverlässigkeit eines Angestellten überwacht werden muss.⁷ Zwischen dem Zeitpunkt seiner Einstellung und einem späteren Schadensereignis kann sich die Zuverlässigkeit eines Angestellten so ändern, dass er zu einem späteren Zeitpunkt nicht mehr eingestellt würde. Die Praxis von Personalabteilungen berücksichtigt heute dieses Risiko und es wird im Jahresrhythmus beurteilt. **13**

Den Zertifikaten kann in der Regel keine Entlastungsfunktion für die Frage des Organisationsverschuldens zukommen, da kein Auditoren-Team in der für die Zertifizierung üblichen kurzen Zeitspanne in der Lage sein dürfte, alle möglichen Fehlerquellen einer Organisation zu überprüfen.⁸ Der Nachweis einer lückenlosen Qualitätsregelung reicht im Bereich der Produkthaftung nicht für den Entlastungsbeweis nach § 831 BGB oder nach § 823 Abs. 1 BGB aus, da **14**

6 *Spindler*, Unternehmensorganisationspflichten: Zivilrechtliche und öffentlich-rechtliche Regelungskonzepte, S. 813, 814 m. w. N.

7 RG v. 14.12.1911 – VI 75/11, RGZ 78 S. 107 – Kutscher- Urteil.

8 *Spindler*, Unternehmensorganisationspflichten: Zivilrechtliche und öffentlich-rechtliche Regelungskonzepte, S. 812.

dieser hinsichtlich sämtlicher Hilfspersonen erforderlich ist, durch deren individuelle Fehlleistung der Produktfehler entstanden sein kann.⁹

- 15 Gerade im Schubstreben-Fall hat der BGH entschieden, dass auch in der Urlaubszeit die Fertigungskontrolle mit einem Ersatzmann für den Kontrollexperten besetzt sein muss und dass durch die organisatorische Maßnahme eines Vertreterplans jede Kontrolllücke zu vermeiden ist.¹⁰ Kein Tag darf ohne Kontrolle bleiben.
- 16 Schon im Kleinbahn-Urteil von 1938 forderte das Reichsgericht die dauerhafte Überprüfung von Dienstanordnungen auf ihre fortdauernde Eignung zur Schadensrisikoabwehr und die praktische Vollzugstauglichkeit im Unternehmen.¹¹
- 17 Der erfolgreiche Entlastungsbeweis setzt nach Rechtsprechung und herrschender Literaturmeinung eine permanente, lückenlose und fortlaufende Überwachung und deren Nachweis voraus. Die Kontrollen an den wenigen Tagen eines Audits im Unternehmen haben keine Entlastungswirkung, wenn nicht darüber hinaus während der gesamten Zeitspanne zwischen den Audits fortlaufende Kontrollen stattfinden und nachgewiesen werden können. Sind die Kontrollen auf Stichproben beschränkt, steigt das Risiko, dass am ungewissen Tage X eines Schadensereignisses Organisationslücken bestehen und ein Organisationsverschulden begründen können.
- 18 In einem Managementsystem muss deshalb jederzeit vom Management abgefragt werden können, welcher Mitarbeiter welche konkreten Pflichten in welchem Betriebsteil und in welchem Zeitraum wie erfüllt hat und ob und mit welchem Ergebnis die Erfüllung der Pflichten kontrolliert wurde.

VII. Der erfolglose Entlastungsversuch durch den Hinweis auf Regeln ohne Anwendung

- 19 Der Hinweis auf ein Zertifikat macht diesen Entlastungsbeweis auch aus einem anderen Grund erfolglos. Zertifikate enthalten keine Aussagen darüber, wie im jeweiligen Unternehmen konkret organisiert wird und ob im Einzelfall die speziellen Schadensrisiken des Unternehmens mit Aussicht auf Erfolg abgewendet werden.
- 20 Festgestellt wird in den Zertifikaten die abstrakte Übereinstimmung mit den Organisationsnormen wie z.B. DIN ISO 14001, EMAS, den Produktsicherheitsrichtlinien oder DIN ISO 9001. Keine Aussagen enthalten die Zertifikate darüber, wie im jeweiligen Unternehmen konkret organisiert wird und ob im Einzelfall die jeweils speziellen Risiken des Unternehmens durch ge-

⁹ *Spindler*, Unternehmensorganisationspflichten: Zivilrechtliche und öffentlich-rechtliche Regelungskonzepte, S. 812 mit Hinweis auf die Schubstreben-Entscheidung.

¹⁰ Schubstreben-Fall: BGH v. 17.10.1967 – VI ZR 70/66, NJW 1968, 247 ff.

¹¹ RG vom 12.1.1938 – VI 172/37, RGJW 1938, S. 1651130 – Kleinbahn-Urteil.

eignete organisatorische Maßnahmen mit Erfolgsaussichten abgewendet werden.

Zu Recht betont *Spindler*, das bloße Implementieren und Vorhalten von Regeln zur Risikoabwehr reiche nicht zur Abwehr vom Organisationsverschulden aus. Vielmehr müssten die Regeln auch angewendet werden.¹² Ihre Anwendung muss im konkreten Schadensfall bewiesen werden. Ein Verantwortlicher im Unternehmen kann beim hohen Abstraktionsgrad der Normen gerade nicht aus dem Regelwerk ablesen, was er konkret zu tun oder zu unterlassen hat. *Spindler* verweist auf die DIN ISO 9001, die sogar schon in ihrer Einleitung davon ausgeht, dass die Organisation jeweils dem konkreten Unternehmen anzupassen ist und nur generelle Leitlinien vorgegeben werden. Das gleiche gilt für die DIN ISO 14001 zum Umweltmanagementsystem, wie für die EG-Öko-Audit-Verordnung, die sich ebenfalls auf abstrakte Forderungen beschränkt. Auch in der Einleitung der DIN ISO 14001 wird darauf hingewiesen, „dass Audits allein nicht ausreichen“, um einer Organisation die Gewissheit zu geben, dass über Umweltleistung nicht nur im Augenblick, sondern ständig ihren rechtlichen Verpflichtungen und politischen Anforderungen gerecht wird. Um wirksam zu sein, müssen diese Prüfungen im Rahmen eines in der Organisation integrierten, strukturierten Managementsystems durchgeführt werden. Die abstrakten Regeln lassen sich auf vielfältige Weise in den Unternehmen konkretisieren.¹³ **21**

Abstrakte Regeln ohne konkrete Anwendung entlasten allerdings nicht. Dies gilt nicht nur für die zitierten Organisationsnormen, sondern für sämtliche abstrakt-generellen Regelungen, wie Gesetze, Verordnungen und alle Regelwerke. Sie gelten für eine Vielzahl von Normadressaten. Sie regeln jedoch nicht den konkreten Einzelfall. Sie sind nicht an einen konkreten Einzeladressaten gerichtet. **22**

Wenn ein Unternehmen im Audit ein sogenanntes „Rechtskataster“, nämlich eine Liste von Gesetzen, Verordnungen, sonstigen Regelwerken vorzeigt und der Auditor die Existenz dieses Regelwerks im Unternehmen bestätigt, ist keine Aussage darüber getroffen, ob im Unternehmen diese abstrakt-generellen Rechtsnormen in den konkreten Risikofällen auch angewendet werden. Die bloße Kenntnis von Gesetzen im Unternehmen sagt nichts darüber aus, ob die speziellen Risiken im Unternehmen mit Hilfe dieser Rechtsnormen abgewendet werden. Das Zertifikat nach einem Audit beweist damit nicht, ob im konkreten Einzelfall das spezielle Risiko erfasst, durch eine geeignete organisatorische Maßnahme abgewendet wurde und schließlich den verantwortlichen Geschäftsleitern kein Organisationsfehler und kein konkretes Organisationsverschulden vorgeworfen werden kann. Die bloße Existenz einer aktuell gehaltenen Gesetzessammlung oder eines Rechtskatasters entlastet deshalb nicht vom Vorwurf **23**

12 *Spindler*, Unternehmensorganisationspflichten: Zivilrechtliche und öffentlich-rechtliche Regelungskonzepte, S. 814.

13 *Spindler*, Unternehmensorganisationspflichten: Zivilrechtliche und öffentlich-rechtliche Regelungskonzepte, S. 806.

des Organisationsverschuldens, weil nicht sichergestellt ist, ob sie im konkreten Einzelfall auch angewandt werden.

- 24 Die ausführlich von *Spindler* in seinem Standardwerk zu Unternehmensorganisationspflichten dargestellte herrschende Meinung zur Frage der Entlastungswirkung von Zertifikaten wird durch die einschlägige Rechtsprechung bestätigt. In allen Fällen der Haftung wegen Organisationsverschuldens konnten die beklagten Unternehmen gerade nicht nachweisen, dass sie im konkreten Schadensfall die Anwendung der abstrakten Rechtsnormen zur Abwehr des konkreten Risikos geprüft und angewandt haben.
- 25 Die Verantwortlichen prüfen Rechtspflichten zur Abwehr konkreter Risiken in aller Regel nicht vor dem Schaden, sondern erst nachdem er eingetreten ist und zwar um zu klären, wer für den Schaden haftet. In keinem Haftungsfall wegen Organisationsverschuldens konnten die Beklagten vortragen und nachweisen, dass sie das Risiko noch vor Eintritt des Schadens erfasst, die konkrete Rechtspflicht zur Abwehr des Risikos geprüft haben und zu dem Ergebnis gekommen sind, ihr Verhalten sei legal.
- 26 Ein Entlastungsbeweis muss immer für den Einzelfall und nicht für den Regelfall geführt werden. Versäumt wird in aller Regel die Erfüllung der Legalitätspflicht und die Erfüllung der Legalitätskontrollpflicht. Sie müssen im Unternehmen organisiert werden. Bezeichnend ist für alle bekannten Fälle des illegalen Verhaltens im Unternehmen, dass die Beklagten nicht vortragen konnten, sie hätten ihr Verhalten rechtlich vor dem Eintritt des Schadens und vor Bekanntwerden des Rechtsverstoßes auf die Rechtmäßigkeit ihres Verhaltens geprüft.¹⁴
- 27 Der Entlastungsbeweis nach dem Eintritt eines konkreten Schadens muss immer für den konkreten Einzelfall, einen ganz speziellen Sachverhalt und einen individuell verantwortlichen Unternehmensmitarbeiter geführt werden. In allen Haftungsfällen wegen Organisationsverschuldens lässt sich jedoch beobachten, dass der Entlastungsbeweis durch den Hinweis zu führen versucht wird, wie in vergleichbaren ähnlichen Fällen die Organisation und die Beachtung von Regeln praktiziert wird. Nicht dagegen wird dargelegt und bewiesen, wie im konkreten Fall das Schadensrisiko abzuwenden versucht, und vor allem an welche verantwortlichen Unternehmensmitarbeiter die Rechtspflicht delegiert und ob der Verantwortliche kontrolliert wurde. Ohne diese konkreten Beweise können sich Vorstände und Geschäftsführer nicht erfolgreich entlasten. Der Hinweis auf die generelle Praxis der Unternehmensorganisation und die vorhandenen Regeln ersetzt nicht den konkreten Beweis im einzelnen konkreten Schadensfall. Der Hinweis, wie ein Unternehmen sich generell oder in der Regel oder grundsätzlich in vergleichbaren ähnlichen Fällen verhält, bleibt immer ein erfolgloser Entlastungsversuch. Dieser geschilderte Missstand beim Entlastungsbeweis lässt sich

14 BGHSt 53, 6 (NBW); BGHZ 180, 9; BGHZ 152, 280; offen bleibt die Frage, warum illegales Verhalten vor allem in Großunternehmen immer nach und nicht vor dem Vorwurf des Fehlverhaltens geprüft und nicht abgewendet wird.

durch die Entscheidungspraxis in den Fällen belegen, in denen zwar allgemein gehaltene Regeln nachgewiesen wurden, nicht aber deren Anwendung im konkreten Schadensfall. Die Vermutung des Organisationsverschuldens konnte durch den Entlastungsbeweis nicht widerlegt werden. Im Ergebnis war jedes Mal der Entlastungsversuch aus den gleichen Gründen erfolglos.

Im Kutscher-Fall von 1911 hat der beklagte Verkehrsbetrieb vorgetragen, der gesamte Wagenverkehr werde laufend überwacht. Diesen Entlastungsversuch hat das Reichsgericht nicht anerkannt. Die Aufsichtsorganisation habe versagt. Nicht vorgetragen und bewiesen wurde, ob gerade derselbe Kutscher, der den Passanten überfahren hatte, auf seine konkrete Zuverlässigkeit im Verkehr zeitnah zum Unfall kontrolliert wurde. Dabei hilft es nicht, wenn der Mitarbeiter nur im Zeitpunkt seiner Einstellung auf seine Zuverlässigkeit beurteilt wurde. Vielmehr verlangte schon das Reichsgericht, eine fortdauernde Überwachung während der gesamten Dienstzeit zwischen dem Zeitpunkt der Einstellung und dem Schadensereignis. **28**

VIII. Die Haftung von Vorständen und Geschäftsführern für fehlende und fehlerhafte CMS nach der Rechtsprechung

Seit der Verurteilung des Finanzvorstands der S. AG zu 15 Mio. EUR Schadensersatz durch das LG München wegen eines fehlenden CMS¹⁵ häufen sich die Haftungsfälle. Wegen des gestiegenen Haftungsrisikos müssen Vorstände und Geschäftsführer ein gesteigertes Interesse an einem dauerhaft wirksamen CMS haben.¹⁶ Falsche Zertifikate ohne Prüfung der dauerhaften Wirkung des CMS müssen die verantwortlichen Geschäftsleiter im eigenen Interesse vermeiden. Gefälligkeitszertifikate schaden den für die Organisationspflicht Verantwortlichen und begründen ihr eigenes Haftungsrisiko gegenüber ihrer Gesellschaft. **29**

IX. Die Haftung von Auditoren und Umweltgutachtern gegenüber dem zertifizierten Unternehmen nach der Expertenhaftung

Werden Schäden durch Fehler am Zertifikat verursacht, haftet der Auditor und Umweltgutachter für den Schaden nach § 634 Nr. 4 BGB, der dem Unternehmen durch den Fehler entsteht. Umfasst werden Schäden, die dem Werk, hier dem Bericht, Zertifikat und der Gültigkeitserklärung unmittelbar anhaften, weil es infolge eines Fehlers unbrauchbar oder wertlos ist. Fehlerhaft sind Zertifikate insoweit, als sie missverständliche Prüfungsergebnisse wiedergeben, nicht vollständig sind und weitere Erläuterungen und Gutachten veranlassen. Nach **30**

15 LG München, 10.12.2013 – 5 HKO 1387/10 – Neubürger-Urteil, CB 2014, 167 m. Kommentar *Kränzlin/Weller* und BB 2014, 850 Ls m. Kommentar *Grützner*.

16 LAG Düsseldorf, 27.11.2015 – 14 Sa 800/15 – Schienenkartell-Urteil, WuW 2016, 251, Rn. 113; ArbG Frankfurt a. M., 11.9.2013 – 9 Ca 1551/13, zuletzt: OLG Nürnberg, Urt. v. 30.3.2022 – 12 U 1520/19 – Haftung des Geschäftsführers für Pflichtverletzungen im Rahmen der internen Unternehmensorganisation – Vier-Augen-Prinzip.

der BGH-Rechtsprechung zur Expertenhaftung haften Berufsgruppen für Mangelschäden durch falsche Prüfergebnisse, die ähnlich wie die Auditoren und Umweltgutachter der Expertenhaftung unterliegen.

- 31 Schadensersatz wegen Schlechtleistung bei Prüfungsverträgen kann einmal durch falsche uneingeschränkte Zertifikate oder durch eingeschränkte Zertifikate verursacht werden. Wird ein positives Zertifikat erteilt, obwohl es nicht hätte erteilt werden dürfen, weil auf erkennbare Missstände nicht hingewiesen wurde, kann ein Schadensersatzanspruch begründet werden. Wirtschaftsprüfern obliegt nach § 321 HGB eine Redepflicht. Sie haben auf erkannte Missstände hinzuweisen. Analog wird eine Redepflicht auch dem Umweltgutachter und Auditor auferlegt, wenn es darum geht, auf erkannte Missstände hinzuweisen.¹⁷ Schäden können auch dadurch entstehen, dass Umweltgutachter unberechtigte Abweichungen erklären und unnötige Aufwendungen dadurch verursachen – eine Fallkonstellation, die eher selten sein dürfte.
- 32 Zu den vertraglichen Pflichten gehört auch die Einhaltung des Pflichtenstandards bei Auditoren. Bei Umweltgutachtern, die nach EMAS zertifizieren, ergeben sich die Pflichtenstandards aus den Leitlinien des Umweltgutachterausschusses. Zu überprüfen hat der Umweltgutachter danach die Einhaltung der einschlägigen Umweltvorschriften am Standort, die technische Eignung der Umweltprüfung, die Umweltbetriebsprüfung, die theoretische Wirksamkeit, die praktische Umsetzung des Umweltmanagements und die Vollständigkeit der Umwelterklärung.¹⁸
- 33 Vor allem hat der Auditor die dauerhafte Wirksamkeit des CMS nach den in den Nr. 1.1 bis 1.6 dargestellten Vorgaben der diversen Managementsysteme zu prüfen und zu bestätigen.
- 34 Darüber hinaus hat der Auditor Berufspflichten zu erfüllen zur Unabhängigkeit, Unbefangenheit, Gewissenhaftigkeit, Eigenverantwortlichkeit, Verschwiegenheit und Unparteilichkeit. Der Pflichtenstandard des Umweltauditors nach der DIN ISO 14001 ergibt sich aus dem konkret aufgelisteten Maßnahmenkatalog von Anforderungen an das Umwelt-Management-System.
- 35 Neben den vertraglichen Hauptpflichten haben die Auditoren und Gutachter Schutz- und Nebenleistungspflichten einzuhalten. Aufgrund ihrer besonderen Qualifikation verfügen Experten über eine überdurchschnittliche Menge an Informationen. Durch ihre Prüfungspraxis verfügen Auditoren über ein höheres Expertenwissen als der Umweltbeauftragte eines Unternehmens, der nur sein Unternehmen kennt, und für den die Zertifizierung eine einmalige Erfahrung

17 Grünh, Der Umweltgutachter, Berufsrecht und Haftungsrecht im Vergleich zum Wirtschaftsprüfer, 5. 49.

18 Grünh, Der Umweltgutachter, Berufsrecht und Haftungsrecht im Vergleich zum Wirtschaftsprüfer, 5. 175.

darstellt, während der Umweltgutachter und Auditor eine Vielzahl von Unternehmen zertifiziert.¹⁹ Aufgrund dieses Wissens- und Erfahrungsvorsprungs wird eine erhöhte Aufklärungspflicht vom Umweltgutachter aufgrund seiner Rolle als Experte verlangt. Dazu zählen auch Hinweise, wie die Betriebsorganisation aufgebaut werden kann und welche Missstände zu beseitigen sind, um die Anforderungen an ein Umwelt-Management-System zu erfüllen.²⁰

X. Die Expertenhaftung von Auditoren und Umweltgutachtern gegenüber Dritten

Unter dem Begriff des Experten versteht man Personen, die aufgrund ihrer beruflichen Ausbildung über eine gesteigerte Sachkunde in speziellen Bereichen des täglichen Lebens verfügen. Dazu zählen Wirtschaftsprüfer, Steuerberater, Rechtsanwälte, Sachverständige, insbesondere die öffentlich bestellten und vereidigten, die entgeltliche Leistungen erbringen, indem sie ihren Vertragspartnern Auskünfte, Gutachten und Beratungen zukommen lassen. Dem Auftraggeber kann gegenüber dem Experten ein vertraglicher Anspruch auf Schadensersatz zustehen. **36**

Fehlt ein Vertragsverhältnis zwischen Geschädigtem und Experten, kämen zunächst nur deliktsrechtliche Ansprüche nach § 823 Abs. 1 BGB in Betracht. Sie ersetzen jedoch keine Vermögensschäden. Außerdem verlangt eine deliktsrechtliche Haftung im Regelfall den Nachweis eines vorsätzlichen Verhaltens des Experten, der schwer zu erbringen ist. **37**

Der Vermögensschutz vor Expertenfehlern ist im Deliktsrecht nicht wirksam. Deshalb hat die Rechtsprechung den Vertrag mit Schutzwirkung zugunsten Dritter entwickelt. Es handelt sich um eine Anspruchsgrundlage aufgrund richterlicher Rechtsfortbildung, für die offenbar ein Bedürfnis nach einer leichter zu begründenden Haftung durch Vertragsrecht bestand. Dritte wurden als schutzbedürftig angesehen, weil sie z. B. auf ein Gutachten eines Experten vertraut haben, das ihnen bestimmungsgemäß zugeleitet worden ist. Dieses Vertrauen galt insbesondere als schutzbedürftig, weil den Auskünften von Experten und deren Erklärungen grundsätzlich Vertrauen entgegengebracht wird. Experten gelten als objektiv, neutral, kompetent und gewissenhaft und sind deshalb geeignet, Vertrauen zu erwecken. Ebenso wie zwischen zwei Vertragspartnern vertraut ein Dritter auch ohne Vertrag auf die Erklärungen eines Experten. Mit diesen Erwägungen wird die Haftung von Experten gegenüber Dritten auch ohne Vertragsbeziehung begründet.²¹ **38**

¹⁹ Rack, CB 2016, 284, 328.

²⁰ Grünh, Der Umweltgutachter, Berufsrecht und Haftungsrecht im Vergleich zum Wirtschaftsprüfer, 5. 176.

²¹ Näher mit weiteren Nachweisen: Rack, CB 2016, 284, 328.

XI. Aufsicht und Sanktionen von Behörden gegen Umweltgutachter und Auditoren für falsche Zertifikate nach dem Auditverfahren

- 39 Neben den dargestellten zivilrechtlichen Schadensersatzansprüchen von zertifizierten Unternehmen und Drittfirmen, die auf falsche Zertifikate vertraut haben, können fehlerhafte Zertifikate zusätzlich aufsichtsrechtliche Konsequenzen für Auditoren und Umweltgutachter haben. Auch nach ihrer Zulassung werden Umweltgutachter und Auditoren der behördlichen Aufsicht unterzogen, müssen Anordnungen erfüllen und können schlimmstenfalls ihre Zulassung durch Rücknahme und Widerruf nach § 17 UAG verlieren.
- 40 Umweltgutachter sind gemäß Umweltauditgesetzes (UAG) natürliche oder juristische Personen, denen durch das Umweltauditgesetz das Recht zuerkannt ist, Organisationen, wozu Industrie-, Dienstleistungsunternehmen oder sonstige Einrichtungen zählen, die Erfüllung der Anforderungen nach dem europäischen Öko-Audit System (EMAS) zu bestätigen.

XII. Der Gesetzeszweck des UAG

- 41 Der Zweck des UAG ist die Sicherstellung der wirksamen Durchführung der Verordnung (EG) Nr. 1221/2009 des Europäischen Parlaments und des Rates vom 25.11.2009 über die freiwillige Teilnahme von Organisationen an einem Gemeinschaftssystem für Umweltmanagement und Umweltbetriebsprüfung auch in Bezug auf die Umweltdimension der nachhaltigen Entwicklung und der Grundlagen einer nachhaltigen Unternehmensführung.
- 42 Erreicht werden soll der Gesetzeszweck des UAG durch **Zulassungsbedingungen, Aufsicht** und ein **Register** über die geprüften Organisationen nach §§ 32 bis 35 UAG.

XIII. Die Zulassung

- 43 Die Bedingungen der Zulassung sind geregelt nach Abschnitt 1 gemäß §§ 4 bis 14 UAG. Nach § 4 UAG müssen die Anforderungen an Umweltgutachter erfüllt werden, nach § 5 UAG muss seine Zuverlässigkeit, nach § 6 UAG seine Unabhängigkeit und nach § 7 UAG seine Fachkunde gewährleistet sein. Die Anforderungen sind detailliert geregelt. Umweltgutachter und Umweltorganisationen durchlaufen ein spezielles Zulassungsverfahren, das von der Deutschen Akkreditierungs- und Zulassungsgesellschaft für Umweltgutachter mbH (DAU) durchgeführt wird.
- 44 Gemäß § 9 Abs. 4 UAG umfasst die Zulassung als Umweltgutachter auch die Befugnis, Zertifizierungsbescheinigungen nach DIN EN ISO 14001 (Umweltmanagementsysteme) und DIN EN ISO 50001 (Energiemanagementsysteme) zu erteilen.

XIV. Die Aufsicht

Die **Aufsicht** ist geregelt in Abschnitt 2, gemäß §§ 15 bis 17 UAG, die erstens aus der **Überprüfung** der Umweltgutachter und der Umweltgutachterorganisation gemäß § 15 UAG besteht, zweitens aus den **Anordnungen und der Unter-sagung**, ganz oder teilweise vorläufig, bis zur Erfüllung der angeordneten Pflichten gemäß § 16 UAG und drittens als schärfste Aufsichtsmaßnahme durch **Rücknahme und Widerruf** der Zulassung gemäß § 17 UAG. **45**

Nach § 15 Abs. 1 UAG sind die Umweltgutachter und die Umweltgutachterorganisationen in regelmäßigen Abständen von mindestens 24 Monaten daraufhin zu überprüfen, ob die Zulassungsvoraussetzungen, Zuverlässigkeit, Unabhängigkeit und Fachkunde noch vorliegen. Überprüft wird die Qualität der vorgenommenen Begutachtungen in den Unternehmen, die die Durchführung einer Überprüfung durch die Zulassungsstelle dulden müssen. **46**

Die Funktion der Zulassungsstelle²² erfüllt die Deutsche Akkreditierungs- und Zulassungsgesellschaft für Umweltgutachter mbH (DAU) nach § 15 Abs. 1 UAG und der UAG Beleihungsverordnung von 18.12.1995 (BGBl. I, S. 2013). **47**

Die Zulassungsstelle kann die Zulassungsvoraussetzungen im Rahmen einer Geschäftsstellenprüfung im Umweltgutachterbüro durchführen. Darüber hinaus können aus besonderem Anlass nach § 15 Abs. 4 UAG Aufsichtsmaßnahmen von der Zulassungsstelle im Rahmen einer Anlassprüfung ergriffen werden, wenn die Zulassungsstelle Anhaltspunkte dafür hat, dass der Umweltgutachter seinen Aufgaben nicht ordnungsgemäß nachgeht. **48**

Nach § 16 Abs. 1 UAG kann die Zulassungsstelle die erforderlichen Maßnahmen gegenüber Umweltgutachtern und deren Organisationen verfügen. Sie kann insbesondere die Fortführung der Gutachtertätigkeit ganz oder teilweise vorläufig untersagen, wenn der Umweltgutachter nach § 16 Abs. 2 Nr. 1 UAG pflichtwidrig eine Umwelterklärung mit unzutreffenden Angaben und Beurteilungen, insbesondere hinsichtlich der Einhaltung der an einem Standort einer Organisation geltenden Umweltvorschriften validiert hat. **49**

XV. Die Konkretisierung des UAG durch Richtlinien des Umweltgutachterausschusses

Nach § 21 UAG etabliert das Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit den Umweltgutachterausschuss, der Richtlinien zur Auslegung und Anwendung der §§ 4 bis 18 UAG erlässt. **50**

Zur Konkretisierung der Anlassaufsicht nach § 15 Abs. 4 UAG gibt die Richtlinie auf Seite 10 vor, dass die Zulassungsstelle Anhaltspunkten nachgeht, wenn ein Umweltgutachter eine Umwelterklärung trotz Vorliegens eines Gesetzesver- **51**

²² Siehe Bekanntmachung von Richtlinien des Umweltgutachterausschusses nach dem Umweltauditgesetz vom 30.7.2012, Seite 3.

stoßes der begutachteten Organisation validiert hat. Bei einem erheblichen Gesetzesverstoß oder einem anderen schwerwiegenden Verstoß gegen die Pflichten eines Umweltgutachters schreitet die Zulassungsstelle unverzüglich ein.

- 52** Die UAG-Aufsichtsrichtlinie vom 10.5.2012 (UAG-AufsR) enthält eine nicht abschließende Auflistung von 16 Aufsichtsmaßnahmen in dem Katalog des Anhangs zur Aufsichtsrichtlinie auf Seite 16 und 17. Die teilweise oder vollständige Untersagung der gutachterlichen Tätigkeit ist unter Ziff. 6 anzuordnen, wenn eine Umwelterklärung mit unzutreffenden Angaben validiert wird, insbesondere hinsichtlich der Einhaltung der an einem Standort einer Organisation geltenden Umweltvorschriften. Wird die fortdauernde Einhaltung aller einschlägigen Rechtsvorschriften nicht geprüft, nicht korrigiert und nicht dokumentiert, und wird diese Lücke entdeckt, droht dem Umweltgutachter der Entzug seiner Zulassung zur gutachterlichen Tätigkeit.

XVI. Mehr Risiken durch Anordnungen, Untersagungen und Widerruf der Zulassung für Umweltgutachter und Auditoren durch Hinweise auf Rechtsverstöße nach dem Hinweisgeberschutzgesetz

- 53** Bei der vorgestellten Rechtslage für den Fall eines falschen Zertifikats im Auditverfahren müssen Auditoren und Umweltgutachter ihr Risiko erkennen, dass ihnen im Rahmen der Aufsicht nach dem UAG ihre gutachterliche Tätigkeit ganz oder teilweise untersagt werden kann und sie im schlimmsten Fall sogar ihre Zulassung widerrufen wird und sie ihre berufliche Existenz gefährden. Dieses Risiko besteht bei Gefälligkeitszertifikaten, durch die die fortdauernde Wirkung des Compliance Managements bestätigt wird, dass alle einschlägigen Rechtspflichten fortlaufend und dauerhaft ermittelt, delegiert, aktualisiert, erfüllt, kontrolliert und dokumentiert sind, obwohl dies nicht der Fall ist.
- 54** Kommt es trotz des Zertifikats durch den Umweltgutachter nach einem Audit zum Rechtsverstoß mit Schadensfolgen, wird aufgedeckt, dass das validierte Management-System fehlerhaft ist und vom Gutachter nicht hätte validiert werden dürfen.
- 55** Fehlerhafte Validierungen können im Rahmen der Regelaufsicht, der Witness-Aufsicht und der Anlassaufsicht entdeckt werden.
- 56** Erhöht hat sich das Risiko der Entdeckung von Rechtsverstößen durch das Hinweisgeberschutzgesetz. Neu ist nämlich der Schutz von Hinweisgebern, die einen Rechtsverstoß melden, weil sie durch das Gesetz vor Schikanen und Nachteilen durch den Arbeitgeber geschützt werden. Wer einen Hinweis auf einen Rechtsverstoß meldet und vorher den sachlichen Anwendungsbereich nach § 2 HinSchG mit dem Ergebnis geprüft hat, dass seine Meldung zum sachlichen Anwendungsbereich zählt, kann sicher sein, dass er vor Benachteiligungen und Schikanen durch das Hinweisgeberschutzgesetz geschützt wird.

Angestellte sind zur Meldung an ihre Geschäftsleiter arbeitsrechtlich verpflichtet und Vorstände und Geschäftsführer sind zur Informationsbeschaffung verpflichtet.²³ Die Sorge vor Nachteilen durch Meldungen über Pflichtverletzungen im Unternehmen hält Angestellte erfahrungsgemäß zurück, Verstöße zu melden. Diese Sorge nimmt nun das Hinweisgeberschutzgesetz, indem es die Hinweisgeber vor Nachteilen schützt. Compliance wird damit zur Aufgabe der gesamten Belegschaft und hilft dabei, Rechtsverstöße aufzudecken, die im Unternehmen zwar bekannt sind, aber verschwiegen werden. Rechtsverstöße, die bisher unentdeckt blieben, weil aus Sorge vor Nachteilen niemand im Unternehmen Hinweise gemeldet hat, können durch den Schutz durch das neue HinSchG offengelegt werden, ohne dass Hinweisgeber Nachteile zu fürchten haben. **57**

XVII. Mehr Risiken für Umweltgutachter und Auditoren durch den erweiterten Kreis der Hinweisgeber außerhalb der Unternehmensbelegschaft

Das Risiko der Entdeckung von Rechtsverstößen steigt außerdem durch Hinweisgeberschutzgesetz auch noch dadurch, dass der persönliche Anwendungsbereich nach § 1 Abs. 1 HinSchG um Hinweisgeber außerhalb der Belegschaft erweitert wurde. **58**

Geschützt vor Nachteilen werden Personen, **59**

„die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese an die nach diesem Gesetz vorgesehenen Meldestellen melden oder offenlegen (hinweisgebende Personen)“.

Damit erstreckt sich der Anwendungsbereich auch auf hinweisgebende Personen, deren Arbeitsverhältnis zwischenzeitlich beendet oder noch nicht begonnen wurde. Wenn Personen in vorvertraglichen Verhandlungen Informationen über Verstöße erlangen und diese melden, werden sie ebenfalls vor Nachteilen geschützt. Ein Zusammenhang mit der beruflichen Tätigkeit ist anzunehmen, wenn laufende oder auch frühere berufliche Tätigkeiten betroffen sind und sich daraus bei einer Meldung Repressalien ergeben könnten. Nicht geschützt wird die Meldung von Informationen über privates Fehlverhalten (Begründung des Gesetzentwurfs HinSchG, Seite 63). Geschützt werden nach § 1 Abs. 2 HinSchG auch Personen, die von der Meldung betroffen und potenzielle Zeugen sein können. Personen außerhalb der Belegschaft stellen für Umweltgutachter und Auditoren das größte Risiko dar, weil sie weniger Nachteile zu fürchten haben als die Belegschaftsmitglieder und als Externe des Unternehmens dem Einfluss der Unternehmensleitung entzogen sind. **60**

Umweltgutachter und Auditoren müssen deshalb nach der Erweiterung des Kreises der geschützten Hinweisgeber damit rechnen, dass Rechtsverstöße, die im **61**

²³ Rack, CB 2013, 58.

Auditverfahren bewusst aus Gefälligkeit oder aus Nachlässigkeit oder aus dem Mut zur Lücke übersehen oder toleriert wurden, unter dem geltenden Hinweisgeberschutzgesetz leichter durch neuerdings geschützte interne oder externe Hinweisgeber aufgedeckt werden und damit im Ergebnis die Fehlerhaftigkeit des Zertifikats leichter festgestellt werden kann. Auditoren und Umweltgutachter sind dadurch mehr als früher den Sanktionen des UAG ausgesetzt, wodurch sie ihre Zulassung verlieren können. Auditoren und Umweltgutachter, die durch Gefälligkeitszertifikate den nächsten Auditauftrag durch das zertifizierte Unternehmen sich sichern wollen, übersehen dabei das Risiko, ihre Zulassung und damit alle weiteren Aufträge für Audits auch bei anderen Unternehmen und damit ihre berufliche Existenz zu verlieren. Diese Abwägung lässt nur einen Schluss zu, im Auditverfahren sämtliche Rechtspflichten des Unternehmens lückenlos zu prüfen, Rechtsverstöße offenzulegen und nur Zertifikate zu erteilen, auf deren Richtigkeit sowohl die Geschäftsleitung des auditierten Unternehmens als auch alle Dritten vertrauen können. Die Geschäftsführer und Vorstände können nur dann sicher sein, dass das Audit als ihr Instrument zur Informationsbeschaffung und zur Selbstkontrolle auch funktioniert und alle Informationen darüber liefert, ob alle Rechtspflichten des Unternehmens und damit die Legalitätspflichten der Unternehmensleitung erfüllt werden, wenn der Umweltgutachter lückenlos die dauerhafte Einhaltung aller einschlägigen Unternehmenspflichten prüft und bestätigt.

- 62 Das Risiko von Auditoren, dass durch das Hinweisgeberschutzgesetz von unternehmensinternen oder auch externen Hinweisgebern Rechtsverstöße gemeldet werden, die von Auditoren im Auditverfahren übersehen, unterschlagen oder nicht geprüft wurden, ob aus Gefälligkeit oder Nachlässigkeit, und das Zertifikat falsch ist, besteht nicht nur bei EMAS sondern bei allen aufgelisteten Managementsystemen, die auditiert werden können.

XVIII. Fazit

- 63 Alle am Auditverfahren Beteiligte, insbesondere Umweltgutachter und Geschäftsleiter sind vor der Selbsttäuschung über die dauerhafte Wirksamkeit eines CMS zu warnen. Wenn schon finanzieller und zeitlicher Aufwand für Auditverfahren betrieben wird, sollten Haftungsrisiken vermieden statt durch falsche Zertifikate begründet werden. Die beteiligten Umweltgutachter und Auditoren riskieren Ruf, Reputation, sogar ihre Zulassung und schlechte Presse zum eigenen und zum Schaden des falsch zertifizierten Unternehmens. Schließlich sind die Risiken der Entdeckung von Rechtsverstößen trotz Validierung im Auditverfahren erheblich durch interne und besonders durch unternehmensexterne Hinweisgeber gestiegen, die das Hinweisgeberschutzgesetz vor Nachteilen durch die Unternehmensleitung schützt.

11. Kapitel

Governance, Risk und Compliance im Mittelstand – Zusammenhänge und Abhängigkeiten

In diesem Kapitel soll auf die Verknüpfung der verschiedenen Elemente der Überwachung von Unternehmen aus der Sicht des Beraters und Prüfers mittelständischer Unternehmen eingegangen werden. Anders als börsennotierte, international agierende Großkonzerne mit eigenständigen Abteilungen für Compliance, Risikomanagement, Rechnungswesen, Controlling und Interne Revision, sind diese Unternehmen besonders daran interessiert, die notwendigen Elemente der Überwachung möglichst „schlank“ und integriert auszugestalten. 1

I. Einleitung – Die Notwendigkeit der Einrichtung von Instrumenten zur Überwachung von Unternehmen

In mehr oder weniger regelmäßigen Abständen bringen Skandale wie der sog. „Dieselgate“,¹ die Vorwürfe der Korruption im Zusammenhang mit der Vergabe der Fußball-WM 2006² und zuletzt der Wirecard-Skandal³ die Problematik der Überwachung von Unternehmen in das Bewusstsein auch der breiten Öffentlichkeit. Häufig stellt sich dann die Frage, warum die vorhandenen Instrumente zur Unternehmensüberwachung nicht ausreichend waren oder versagt haben. 2

Im Vordergrund steht hier die Überlegung, unter welchen Voraussetzungen Mitarbeiter und Führungskräfte überhaupt dolos bzw. geschäftsschädigend handeln. Nach dem Wirtschaftskriminologen *Donald R. Cressey* liegen die Gründe für Betrug (Fraud) in einer Kombination aus Druck, innerer Rechtfertigung und Gelegenheit, die auch als „Fraud Triangle“ bezeichnet werden: 3

„Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property.“⁴

Druck kann in der beruflichen Tätigkeit aufgrund eines Gefühls, überarbeitet, unterbezahlt oder übergangen worden zu sein, entstehen. Auch private Schulden, 4

1 Siehe unter anderem: <https://www.zdf.de/nachrichten/thema/dieselskandal-abgasskandal-104.html> (zuletzt abgerufen am 12.8.2024).

2 Siehe <http://www.zeit.de/sport/2012-07/blatter-wm-2006-korruption> (zuletzt abgerufen am 12.8.2024).

3 Siehe <https://www.sueddeutsche.de/wirtschaft/wirecard-zusammenfassung-aufstieg-und-fall-1.5750529> (zuletzt abgerufen am 12.8.2024).

4 *Cressey*, *Other People's Money*, S. 30.

generelle Gier oder Spiel-, Alkohol- sowie Drogensucht können ursächlich für den Druck sein.

- 5 Zur inneren Rechtfertigung führt möglicherweise ein Mangel an Ethik. Typische Denkweisen sind dabei: „Ich nehme mir auch nur das, was sich der Vorstand auch unrechtmäßig nimmt“, oder: „Ich leihe es mir nur aus ...“.
- 6 „Gelegenheit macht Diebe“, sagt bereits ein altes Sprichwort, das die Diskussion in den Raum stellt, wie viel Vertrauen ein Unternehmen verträgt und wie viel Kontrolle es braucht. Letztendlich geht es hier ja auch um die Relation von Risiko einerseits und Kosten der Kontrolle andererseits.
- 7 Den Kontrollkosten gegenüber stehen allerdings jene Kosten, die durch Non-Compliance anfallen können. Nicht alle Kostenfaktoren aufgrund von Non-Compliance können ohne Weiteres gut eingeschätzt werden. Schäden durch Korruption oder die Folgekosten in Form von Strafzahlungen und Kosten für die Schadensbegrenzung durch externe Anwälte lassen sich vergleichsweise gut abschätzen, ebenso die Kosten für Kommunikations- und Marketingmaßnahmen. Andere Faktoren wie Umsatzausfälle oder sinkende Marktanteile lassen sich deutlich schwerer beziffern, genau wie die Folgen aus dem gesunkenen Ansehen bei Mitarbeitern, der Öffentlichkeit etc.
- 8 So sind bei VW für die Folgen des Dieselskandals laut einem Bericht der ARD bereits Rechtskosten von über 30 Mio. EUR entstanden.⁵ Ob diese ausreichen, ist derzeit noch offen. Inzwischen werden die Gesamtkosten inklusive Strafzahlungen und Rückzahlungen sogar auf 100 Mrd. EUR oder höher geschätzt.⁶
- 9 Für die Schäden durch Wirtschaftskriminalität nennt die alle zwei Jahre durchgeführte Studie der „Association of Certified Fraud Examiners (ACFE)“ im Jahr 2022 eine durchschnittliche (median) Schadenshöhe von 117.000 USD, in der Immobilienbranche sogar von 435.000 USD.⁷ Aber nicht nur dieser direkte Schaden stellt ein Problem dar. Auch ein Reputationsverlust infolge eines Gesetzesverstößes kann schwerwiegende Auswirkungen auf die Zukunft des betroffenen Unternehmens haben. So ermittelt beispielsweise Biesalski & Company eine Veränderung des Reputationsindex für Volkswagen von 59 (2018) gegenüber 79 (2012).⁸ Die gleiche Studie beziffert auch das der Anteil des Umsatzes von VW, der auf den guten Ruf zurückzuführen ist, im gleichen Zeitraum von 29%

5 Siehe <https://www.absatzwirtschaft.de/reputationsindex-2018-volkswagen-buesst-am-meisten-glaubwuerdigkeit-ein-miele-haribo-und-daimler-halten-positives-image-aufrecht-221752/> (abgerufen am 19.3.2024).

6 <https://www.zeit.de/wirtschaft/2015-10/volkswagen-diesel-affaere-kosten-klagewelle/seite-2> (zuletzt abgerufen am 12.8.2024).

7 Siehe <https://acfe-public.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf> (zuletzt abgerufen am 12.8.2024).

8 <https://www.biesalski-company.com/wp-content/uploads/2021/07/Corporate-Reputation-Score-2018-1.pdf> (zuletzt abgerufen am 12.8.2024). Zur Bedeutung von Reputationsverlusten infolge von Non-Compliance siehe auch → *Schulz*, Kap. 1 Rn. 11, 23 ff. m. w. N.

auf 22 % zurückgegangen ist.⁹ Während der ersten Monate des Dieselskandals stürzte der Kurs der Volkswagen Vorzugsaktien von 169,75 EUR am 9.9.2015 auf 92,36 EUR am 2.10.2015. Ein Minus von fast 46 %.

Dabei ist die Diskussion über die Intensität und Wirksamkeit der Überwachung von Unternehmen und des Managements der Unternehmen bereits über zwei Jahrhunderte alt. Schon *Adam Smith* verwies im Jahr 1776 in seinem Werk „The Wealth of Nations“ auf das Problem:

„The directors of such companies, however, being the managers rather of other people's money than of their own, it cannot well be expected that they should watch over it with the same anxious vigilance with which the partners in a private copartnery frequently watch over their own. [...] Negligence and profusion, therefore, must always prevail, more or less, in the management of the affairs of such a company.“¹⁰

In der betriebswirtschaftlichen Theorie findet sich diese Diskussion unter dem Stichwort der Agency-Theorie wieder, die sich mit der Analyse von ökonomischen Beziehungen befasst, bei der eine Partei (Agent) im Auftrag einer anderen Partei (Principal) – also im vorliegenden Fall Management und Unternehmer – handelt und wie sich in dieser Beziehung Informationsasymmetrien auswirken, die sich daraus ergeben, dass der Agent, also derjenige, der eigentlich im Auftrag seines Auftraggebers handelt, über bessere Informationen verfügt, als sein Auftraggeber selbst.¹¹

Durch geeignete Instrumente der Unternehmensüberwachung sollen einerseits Informationsasymmetrien abgebaut werden. Andererseits sollen die Instrumente verhindern, dass sich die Asymmetrien nachteilig für die Eigentümer der Unternehmen auswirken. Nachstehend werden insbesondere die Elemente der Unternehmensüberwachung betrachtet, die sicherstellen sollen, dass essenzielle das Unternehmen gefährdende Entwicklungen abgewendet oder möglichst früh entdeckt und bekämpft werden können.

Um dem Bedarf nach einer Überwachung des Unternehmens oder genauer des Managements Rechnung zu tragen, hat der Gesetzgeber entsprechende Regelungen erlassen. Darüber hinaus haben die Rechtsprechung und die betriebliche Praxis Standards geschaffen. Im Folgenden wird an entsprechender Stelle auf diese verwiesen.

9 <https://www.biesalski-company.com/wp-content/uploads/2021/07/Corporate-Reputation-Score-2018-1.pdf> (zuletzt abgerufen am 12.8.2024).

10 *Smith, A.*, The Wealth of Nations, <https://www.econlib.org/library/Smith/smWN.html> (zuletzt abgerufen am 12.8.2024).

11 Vgl. auch: *Bergmoser/Theusinger/Gushurst*, BB 2008, 1, 11.

II. Das System der Unternehmensüberwachung

1. Überblick über das Gesamtsystem

- 14 In Theorie und Praxis finden sich zahlreiche Begriffe, die mehr oder weniger große Teilaspekte der Unternehmensüberwachung adressieren. Die bedeutendsten davon sind (Jahres-)Abschlussprüfung, Corporate Governance, Risk Management, Compliance und das interne Kontrollsystem (IKS). Nachstehend sollen zunächst die internen wie externen Komponenten des Systems der Unternehmensüberwachung in einem Gesamtüberblick dargestellt werden.

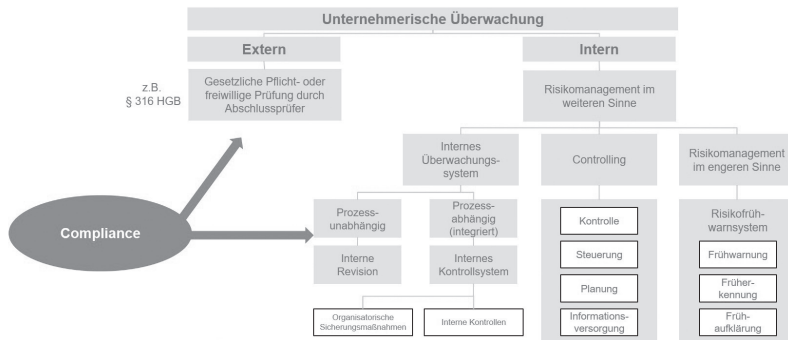


Abbildung 1: Das System der Unternehmensüberwachung¹²

- 15 Anhand der obigen Abbildung wird ersichtlich, dass der Begriff der Compliance einerseits unter Bezug auf die externe unternehmerische Überwachung gesehen werden kann. So wird im Rahmen der Jahresabschlussprüfung durch den Abschlussprüfer geprüft, ob die Vorschriften der Rechnungslegung durch das Unternehmen eingehalten wurden, während durch das interne System der unternehmerischen Überwachung sichergestellt werden soll, dass es nicht zu Verstößen gegen Normen und Regeln kommt. Andererseits umfasst die unternehmerische Überwachung auch zahlreiche unternehmensinterne Komponenten wie bspw. das interne Kontrollsystem, das Controlling oder auch das Risikomanagement.

2. Externe Komponenten der Unternehmensüberwachung

- 16 Die externen Komponenten der Unternehmensüberwachung ergeben sich aus expliziten gesetzlichen Vorschriften bzw. auch als freiwillige Prüfung, z. B. aufgrund gesellschaftsrechtlicher Vereinbarungen oder aufgrund branchenspezifischer Anforderungen (z. B. von Banken). Unter die verpflichtenden Prüfungen fällt zunächst vor allem die im Handelsgesetzbuch geregelte Prüfung des Jahresabschlusses durch die Wirtschaftsprüfer.¹³

¹² In Anlehnung an Küting/Busch, DB 2009, 1361 ff.

¹³ Siehe §§ 316 ff. HGB.

Es muss aber darauf hingewiesen werden, dass sich daneben auch aus anderen gesetzlichen Vorschriften Anforderungen an weitere Aspekte der Unternehmensüberwachung ergeben. Im Unterschied zur Jahresabschlussprüfung stellen diese jedoch jeweils nur grundsätzliche Anforderungen dar, beziehungsweise richten sich nicht immer an alle Unternehmen. So ergeben sich zum Beispiel ganz wesentliche Anforderungen an Banken und andere Finanzdienstleister oder kapitalmarktorientierte Unternehmen. Als Beispiel seien hier insbesondere die Mindestanforderungen an das Risikomanagement (MaRisk) der Bundesanstalt für Finanzdienstleistungsaufsicht zu nennen, die den betroffenen Kreditinstituten und Finanzdienstleistungsunternehmen explizite Vorgaben für die Einrichtung und den Betrieb eines angemessenen Risikomanagements geben, jedoch für Unternehmen außerhalb dieses Sektors keine derartige Bedeutung haben und allenfalls als Richtlinie dienen können.¹⁴

Als weiteres Element der (hoheitlichen) Überwachung für den Teilaspekt der Rechnungslegung ist an dieser Stelle noch das sog. „Enforcement“ zu nennen.

Unter Enforcement wird die Überprüfung der Einhaltung der Vorschriften zur Rechnungslegung und Offenlegung verstanden.¹⁵ Das Enforcementverfahren wurde in der Folge des Wirecard-Skandals neu gestaltet. Nunmehr ist allein die BaFin für die Einleitung eines Verfahrens zuständig. Dabei wird zwischen einer anlassbezogenen (§ 107 Abs. Satz 1 WpHG) und einer Stichprobenprüfung (§ 107 Abs. 1 Satz 3 WpHG) unterschieden.¹⁶ Die kritisierte Überwachung durch die privatrechtlich organisierte DPR ist nunmehr entfallen.

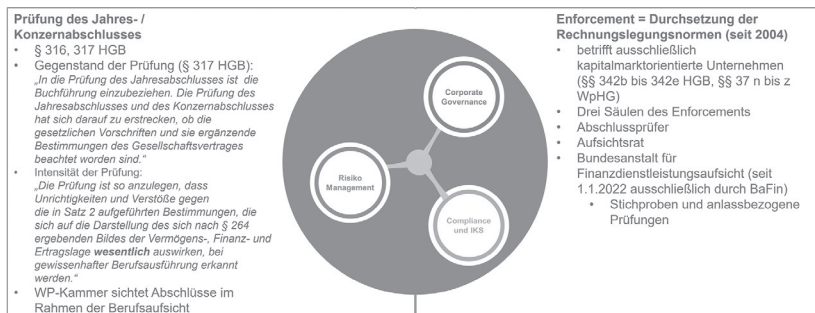


Abbildung 2: Externe Komponenten der Unternehmensüberwachung

¹⁴ Siehe hierzu → *Renz/Frankenberger*, Kap. 20 Rn. 23 ff.

¹⁵ Siehe hierzu auch: *Scheffler* in: Böcking/Gros/Oser/Scheffler/Thormann, Beck'sches Handbuch der Rechnungslegung, Werkstand 70. EL Juli 2023, Rn. 91 ff.

¹⁶ Zur Neugestaltung des Enforcementverfahrens siehe *Koch/Brand*, BKR 2023, 489 ff.

3. Interne Komponenten der Unternehmensüberwachung

- 20 Die Aspekte der internen unternehmerischen Überwachung lassen sich auch unter dem Begriff des Risikomanagements im weiteren Sinne zusammenfassen.¹⁷
- 21 Als ersten wesentlichen Teilaspekt wird das interne Überwachungssystem, das je nach seiner Stellung zu den Prozessen als internes Kontrollsystem („IKS“, in die Prozesse integriert) bzw. als interne Revision (prozessunabhängig) ausgestaltet sein kann, genannt. Das interne Kontrollsystem hat hierbei die Aufgabe, durch seine Integration in die Prozesse Compliance- Aspekte wahrzunehmen, indem sichergestellt wird, dass Verstöße gegen gesetzliche oder andere Vorschriften sozusagen online/im laufenden Betrieb entdeckt werden.¹⁸ Die interne Revision hat hingegen die Aufgabe, mithilfe nachgelagerter Prüfungshandlungen festzustellen, ob Verstöße vorlagen bzw. ob das interne Kontrollsystem so ausgeprägt ist, dass Verstöße aufgedeckt werden. Beide Komponenten gehen aber über die reine Aufgabe der Compliance-Überwachung hinaus, da auch Wirtschaftlichkeitsaspekte eine Rolle spielen.
- 22 Auch wenn sich in der Literatur zahlreiche Definitionen für „Controlling“ finden lassen, werden weitgehend übereinstimmend als Aufgaben des Controllings die Koordinierung der Unternehmensführungs-Teilsysteme, die Funktionssicherung des betrieblichen Informationssystems sowie die Funktionssicherung des Planungs- und Kontrollsystems verstanden.¹⁹
- 23 Ein weiteres Element der internen Überwachung ist das Risikomanagement im engeren Sinne, das dazu dient, alle für das Unternehmen relevanten Risiken abzudecken.²⁰ Diese Risiken (auch Compliance-Risiken) sollen anschließend qualitativ und quantitativ bewertet, durch geeignete Maßnahmen begrenzt, auf andere übergewälzt oder akzeptiert werden. Dabei erfolgt das Abwehren und Begrenzen der Risiken nicht nur durch das Risikomanagement, sondern vor allem auch durch die Elemente des internen Kontrollsystems oder auch durch das Compliance Management.²¹

17 Vgl. *Küting/Busch*, DB 2009, 1361 ff.; siehe dazu auch die Abbildung weiter oben → Rn. 14 f.

18 Zur Bedeutung des IKS bei Finanzdienstleistungsinstituten siehe → *Renz/Frankenberger*, Kap. 20 Rn. 69 ff.

19 *Pampel/Krolak*, in: *Hauschka/Moosmayer/Lösler*, Corporate Compliance, § 15 Rn. 12

20 Siehe zum Risikomanagement ausführlich → *Romeike*, Kap. 9.

21 Vgl. *Küting/Busch*, DB 2009, 1361 ff.

III. Die Verknüpfung der einzelnen Elemente der Unternehmensüberwachung

1. Der GRC-Ansatz

In den letzten Jahren wurde das GRC-Konzept als integrierendes Modell für alle drei Bereiche der Unternehmensverfassung (Corporate Governance), Risikomanagement und Compliance entwickelt und entsprechend propagiert. 24

Die Abkürzung „GRC“ hat Eingang gefunden in die Bezeichnung für Software, Marketingpräsentationen und die Bezeichnung ganzer Abteilungen multinationaler Konzerne.²² Auch wenn die Konzepte von Unternehmensverfassung, Risikomanagement und Compliance an sich nicht neu sind, ist doch der holistische Ansatz des GRC-Konzeptes durchaus neu.²³ 25

GRC kann definiert werden als „integrierter, holistischer Ansatz für ein die gesamte Organisation umfassende Governance, Risiko- und Compliance Management-System, das sicherstellt, dass die Organisation ethisch korrekt und in Übereinstimmung mit ihrer Risikoeinstellung, den internen Richtlinien und externen Regularien durch die Abstimmung der Strategie, der Prozesse, Technologie und Menschen handelt, mit dem Ziel, die Effizienz und Effektivität zu steigern“.²⁴ 26

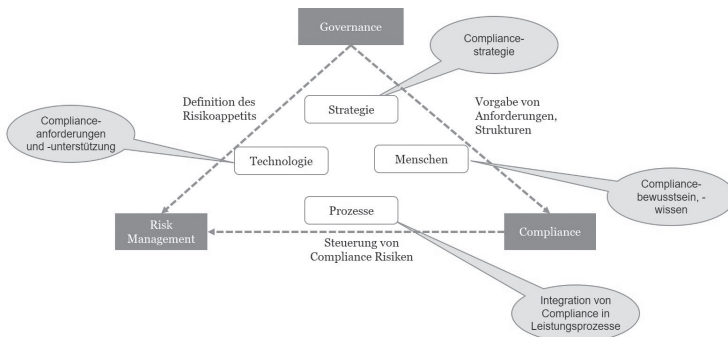


Abbildung 3: Der integrierte GRC-Ansatz²⁵

Dabei können sich vor allem auf Basis der unterschiedlichen Geschäftsmodelle und der unterschiedlichen regulatorischen Anforderungen teilweise sehr unterschiedliche Ausprägungen des Systems ergeben. 27

²² Racz/Weippl/Seufert, in: De Decker/Schaumüller-Bichl, Communications and Multimedia Security, S. 106 ff.

²³ Racz/Weippl/Seufert, in: De Decker/Schaumüller-Bichl, Communications and Multimedia Security, S. 106 ff.

²⁴ Racz/Weippl/Seufert, in: De Decker/Schaumüller-Bichl, Communications and Multimedia Security, S. 106 ff.

²⁵ In Anlehnung an Racz/Weippl/Seufert, A frame of Reference for Research of Integrated Governance, Risk & Compliance (GRC)

²⁶ Siehe hierzu auch → Renz/Frankenberger, Kap. 20 Rn. 3 ff.

- 28** Entwickelt insbesondere für große börsennotierte Unternehmen hat das Konzept bislang überwiegend Einzug bei großen international agierenden Unternehmen gehalten. Demgegenüber waren mittelständisch geprägte Unternehmen eher zurückhaltend bei der Umsetzung. Hauptgrund dafür ist sicher die schwere Vereinbarkeit des doch sehr umfassend erscheinenden GRC-Ansatzes mit den meist eigentümergeprägten Führungsstrukturen und dem Kostenbewusstsein des klassischen Mittelständlers.
- 29** Mit einem pragmatischen Verständnis des Ansatzes soll in späteren Ausführungen versucht werden, die wesentlichen Ziele dieses gesamthaften Ansatzes auf die Verhältnisse typisch mittelständischer Unternehmen anzupassen.

2. Das interne Kontrollsystem und die anderen Elemente der Überwachung des Unternehmens

- 30** In Deutschland finden sich Definitionen zum Thema Internes Kontrollsystem insbesondere im Prüfungsstandard 261 n. F. des Instituts der Wirtschaftsprüfer.²⁷ Dort heißt es zur Definition des internen Kontrollsystems: „Unter einem internen Kontrollsystem werden die von dem Management im Unternehmen eingeführten Grundsätze, Verfahren und Maßnahmen (Regelungen) verstanden, die gerichtet sind auf die organisatorische Umsetzung der Entscheidungen des Managements:
- zur Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit (hierzu gehört auch der Schutz des Vermögens, einschließlich der Verhinderung und Aufdeckung von Vermögensschädigungen),
 - zur Ordnungsmäßigkeit und Verlässlichkeit der internen und externen Rechnungslegung sowie
 - zur Einhaltung der für das Unternehmen maßgeblichen rechtlichen Vorschriften.“²⁸
- 31** Wie bereits aus dieser Definition deutlich wird, umfasst das interne Kontrollsystem also nicht nur rechnungslegungsbezogene Kontrollen, sondern eben auch darüber hinaus Maßnahmen, durch die sichergestellt werden soll, dass die Wirtschaftlichkeit eines Unternehmens gegeben ist.
- 32** Die einzelnen Maßnahmen lassen sich dabei weiter wie folgt differenzieren: Zum einen kann zwischen fehlervermeidenden (präventiven) und fehleraufdeckenden (detektiven) Maßnahmen unterschieden werden. Zum anderen kann nach der Eingliederung in die betrieblichen Prozesse nach den prozessintegrierten und prozessunabhängigen Maßnahmen unterschieden werden.

²⁷ Institut der Wirtschaftsprüfer, IDW Prüfungsstandard 261 „Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken“ (IDW PS 261 n. F.) (Stand: 15.9.2017).

²⁸ Institut der Wirtschaftsprüfer, IDW Prüfungsstandard 261 „Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken“ (IDW PS 261 n. F.) (Stand: 15.9.2017).

Prozessintegrierte Überwachungsmaßnahmen	Prozessintegrierte Überwachungsmaßnahmen
Die einzelnen Maßnahmen sind in die Geschäftsprozesse als konkrete Schritte integriert • Organisatorische Sicherungsmaßnahmen sollen Fehler verhindern, sind in die Aufbau- und Ablauforganisation so eingegliedert, dass sie ein bestimmtes Sicherheitsniveau gewährleisten • Kontrollen dienen zum einen dem Auffinden von Fehlern, zum anderen sollen sie sicherstellen, dass Fehler verhindert werden.	Diese Maßnahmen sind entsprechend unabhängig von den konkreten Leistungsprozessen. • Die interne Revision untersteht in der Regel der Unternehmensleitung und untersucht einerseits anlassbezogen oder anlassunabhängig die Einhaltung von gesetzlichen und internen Regelungen aber auch die Wirtschaftlichkeit. • Sonstige Maßnahmen können durch die Unternehmensleitung selbst oder in ihrem Auftrag erfolgen.

Abbildung 4: Überwachungsmaßnahmen in Bezug auf die Integration in die Geschäftsprozesse

Damit wird bereits aus der Definition des internen Kontrollsystems dessen Verknüpfung mit Aspekten der Compliance wie auch des auf die Wirtschaftlichkeit des Unternehmens gerichteten Controllings deutlich. **33**

Teilaspekte des internen Kontrollsystems zielen gerade auch auf die Aufdeckung von Verstößen gegen Vorschriften aus dem Bereich der Rechnungslegung oder gegen steuerliche Vorschriften. Darüber hinaus zielt das interne Kontrollsystem auch auf die Verhinderung von Vermögensverlusten durch dolose Handlungen ab. **34**

Das Aufdecken von Risiken aus Fehlern und Verstößen schließlich ist die Basis für ein angemessenes Risikomanagement. **35**

Umgekehrt leiten sich aus dem Compliance- und Risikomanagement die Anforderungen an entsprechende Maßnahmen der Überwachung im Rahmen des internen Kontrollsystems ab. **36**

3. Compliance- und Risikomanagement

Auch hinsichtlich der Systeme des Compliance- und Risikomanagements lassen sich auf mehr als einer Ebene Verknüpfungen und Wechselwirkungen feststellen. So stellen Risiken aus Compliance-Verstößen einen Teilaspekt der durch das Risikomanagement betrachteten Risiken dar.²⁹ Daneben stellt ein angemessenes Risikomanagement eine der gesetzlichen Verpflichtungen dar, die Unternehmen einzuhalten haben, und deren Umsetzung somit im Rahmen des Compliance Managements sichergestellt werden soll. Diese Verpflichtung ergibt sich aus § 91 Abs. 2 AktG, wodurch der Vorstand einer Aktiengesellschaft dazu verpflichtet ist, „... geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand des Unternehmens gefährdende Entwicklungen früh erkannt werden“. Dabei gilt diese Verpflichtung aber nicht nur für Aktiengesellschaften, sondern mittelbar auch für die GmbH, worauf der Gesetzgeber bereits in der Gesetzesbegründung des Gesetzes **37**

²⁹ Zum Zusammenhang zwischen Compliance und Risikomanagement siehe auch → Schulz, Kap. 1.

zur Kontrolle und Transparenz im Unternehmensbereich (KontraG) verweist, durch das der § 91 Abs. 2 AktG eingeführt wurde.³⁰

- 38** In Folge des Wirecard-Skandals wurde für börsennotierte AG § 91 AktG um einen dritten Absatz erweitert, der explizit für diese die Verpflichtung zur Einrichtung eines „im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames internes Kontrollsystem und Risikomanagementsystem“ vorsieht.³¹

4. Risikomanagement und Controlling

- 39** Der Zusammenhang von Risikomanagement und Controlling lässt sich unter anderem aus zwei Perspektiven sehen. Wesentlicher Bestandteil des Risikomanagements ist das Risikocontrolling. Unter dem Risikocontrolling versteht man dabei das aktive Steuern von Maßnahmen zur Risikobegrenzung. Darunter fallen sowohl das Reporting von Risiken, als auch der Status des Risikoeintritts und der damit verbundenen Aufwendungen zur Handhabung von Risiken in Form der Risikoüberwälzung, Risikominimierung oder -begrenzung.
- 40** Das Controlling in seiner Teilfunktion als Informationsversorgung liefert letztendlich auch Angaben zur Bewertung, Steuerung und Handhabung von Risiken. So kann je nach der erwarteten Eintrittswahrscheinlichkeit die Reaktion auf diese Risiken auch unterschiedlich ausfallen, wie die nachstehende Grafik beispielhaft zeigt.

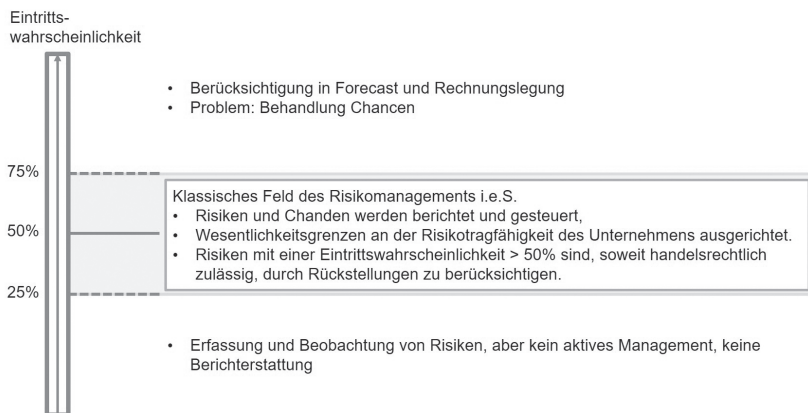


Abbildung 5: Einbeziehung von Risiken in das Risikomanagement unter dem Aspekt der Eintrittswahrscheinlichkeit

30 Bundesregierung – Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich, Drucksache 13/9712 des Bundestags, <http://dipbt.bundestag.de/doc/btd/13/097/1309712.pdf>, S. 15 (zuletzt abgerufen am 12.8.2024).

31 Siehe dazu auch *Koch*, Aktiengesetz, 18. Aufl. 2024, § 91 Rn. 15–37.

Hier wird deutlich, dass auch die Rechnungslegung in diese Zusammenhänge einbezogen wird, beispielsweise dann, wenn Risiken bereits in Form von Rückstellungen oder auch in der Berichterstattung in Anhang und Lagebericht zu berücksichtigen sind.³² **41**

5. Interne Revision, Compliance und Risikomanagement

Die interne Revision als prozessunabhängige Form der Unternehmensüberwachung³³ erfüllt wesentliche Aufgaben in Verbindung mit dem Compliance und dem Risikomanagement.³⁴ **42**

So kann durch konkrete (stichprobenhafte) Prüfungen im Rahmen der internen Revision untersucht werden, ob es zu Verstößen gegen Gesetze oder andere Vorschriften im Unternehmen gekommen ist. Damit stellt die interne Revision gemäß der bereits erwähnten Studie „Report to the Nations on Occupational Fraud and Abuse“ die zweitwichtigste Quelle für die Aufdeckung von Wirtschaftsstraftaten dar.³⁵ Neben der direkten Aufdeckung von Verstößen geht es dabei auch darum, zu prüfen, inwieweit das vorhandene interne Kontrollsystem angemessen und wirksam hinsichtlich der Verhinderung von Gesetzesverstößen ist. **43**

Grundlage der Arbeit der internen Revision ist in der Regel eine Risikobewertung der verschiedenen Prozesse und Bereiche im Unternehmen. So werden häufig die erfassten und bewerteten Risiken z. B. im Rahmen einer entsprechenden Risikolandkarte (auch als „Audit Universe“ bezeichnet) als Basis für die Erarbeitung der mehrjährigen Prüfungsplanung im Rahmen der internen Revision verwendet. **44**

Auf der anderen Seite gehen die Ergebnisse der Prüfungen der internen Revision in die Erfassung der Risiken im Rahmen des Risikomanagements ein. **45**

6. Fazit

Es kann also festgestellt werden, dass zwischen den einzelnen internen Elementen der Unternehmensüberwachung intensive Zusammenhänge bestehen. Daher ist es auch sinnvoll, bei der Einführung der entsprechenden Strukturen in Unternehmen diese Zusammenhänge und Abhängigkeiten zu betrachten. **46**

32 Vgl. auch Schubert, in: Beck'scher Bilanz-Kommentar HGB, § 249 Rn. 1–6, 13. Aufl. 2022, Grottel, in: Beck'scher Bilanz-Kommentar HGB, § 315 Rn. 160–165, 13. Aufl. 2022.

33 Vgl. dazu auch → Rn. 14 f.

34 Zum Schnittstellenmanagement siehe auch → Rau, Kap. 3.

35 Siehe <https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf> (zuletzt abgerufen am 12.8.2024).

IV. Grundkonzept für die Ausgestaltung eines integrierten Systems der Überwachung für mittelständisch geprägte Unternehmen

- 47 Nachstehend soll aufgezeigt werden, wie die oben aufgezeigten Zusammenhänge und Abhängigkeiten im Rahmen der Ausgestaltung eines integrierten Systems der Überwachung für mittelständisch geprägte Unternehmen beachtet aber auch genutzt werden können.

1. Bestimmung der Zielgruppe der Unternehmen

- 48 Voranstellend soll definiert werden, welche Unternehmen hier betrachtet werden sollen. Hintergrund dafür ist, dass es nicht sinnvoll erscheint, ein Konzept abzubilden, das für alle Unternehmen passt. Die hier betrachteten Unternehmen zeichnen sich durch eine mittelständische Prägung aus. Dabei soll weniger auf bestimmte Größenordnungen als vielmehr auf charakteristische Strukturen abgestellt werden.
- 49 Prägend für die hier betrachteten Unternehmen ist die geringe Ausprägung von Stabsstellen und Fachabteilungen. Im kaufmännischen Bereich sind alle wesentlichen Funktionen aus den Bereichen Personal, Rechnungswesen und Steuern, Controlling, Recht sowie Auftragsabwicklung zusammengefasst. Für spezielle Fragestellungen wird häufig auf externe Dienstleister – wie den Abschlussprüfer oder Steuerberater – zurückgegriffen. Eine interne Revision als eigenständige Funktion kann vorhanden sein, übernimmt aber häufig auch noch andere Aufgaben.
- 50 Typisch für diese Unternehmen ist auch, dass der Fokus häufig auf der Optimierung der Prozesse mit dem Ziel der Kosteneffizienz und Kundenfokussierung liegt. Kaufmännische Prozesse sind häufig kostenoptimiert. Die Prozesse der Abschlusserstellung sind nicht bis in den letzten Schritt auf ein möglichst schnelles Reporting ausgerichtet. Im Controlling sind die Prozesse zur Vor- und Nachkalkulation gut ausgeprägt. Andere Bereiche des Controllings sind eher schwach entwickelt.

2. Zielstellung für die Einführung eines integrierten Systems der Überwachung

- 51 Mit der Einführung eines integrierten Systems sollen vor allem zwei Ziele verfolgt werden: Zum einen sollen die bereits vorhandenen Strukturen unter dem Aspekt der Überwachung des Unternehmens optimiert werden. Zum anderen sollen Strukturen und Prozesse eingerichtet werden, die die Balance von Kosten und Erfolg der Unternehmensüberwachung so gut wie möglich finden.

3. Vorgehensweise

- 52 Um ein abgestimmtes und integriertes System der Überwachung einzuführen, hat sich ein Vorgehen in vier Schritten bewährt. An dieser Stelle soll aber keine

detaillierte Handlungsanweisung gegeben werden, sondern vielmehr dargestellt werden, welche Themen zu bearbeiten sind.

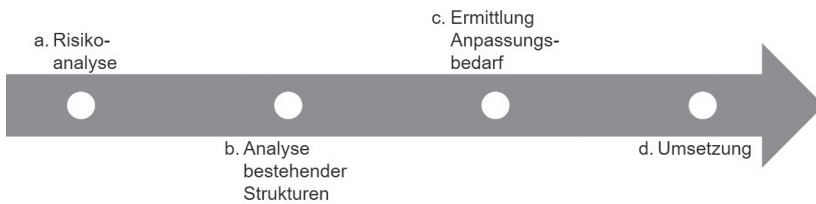


Abbildung 6: Vorgehensmodelle zur Implementierung von GRC-Strukturen

a) Risikoanalyse

In der ersten Phase, der Risikoanalyse (auch „Risikoinventur“), werden die für das Unternehmen relevanten Risiken ermittelt.³⁶ Die Ermittlung erfolgt dabei idealerweise auf Basis bereits vorhandener Risikoeinschätzungen und -analysen. Dabei werden die unternehmensinternen Risiken zum Beispiel anhand der Leistungs- und unterstützenden Prozesse oder anhand der Aufbauorganisation definiert. Bei Konzernstrukturen kann es erforderlich sein, bestehende Unterschiede in den verschiedenen Geschäftsbereichen zu differenzieren. Neben den für die Ausgestaltung des Compliance Managements erforderlichen rechtlichen Risiken sind auch die Risiken in wirtschaftlicher Hinsicht zu beachten.

Sich aus externen Faktoren ergebende Risiken werden in der Regel differenziert nach geografischen Kriterien (z. B. differenziert auf der Basis des „Corruption Perception Index“ von der Organisation „Transparency International“³⁷) und auf Basis branchenspezifischer Risikoeinschätzungen, die sich zum Beispiel auch auf der Basis der Informationen von Verbänden oder Branchenanalysen ableiten lassen.³⁸ In der Literatur lassen sich weitere Informationen zum Thema Risikoanalyse finden.³⁹

Im Ergebnis der Risikoanalyse lässt sich die Gesamtheit der Risikosituation zum Beispiel in Form einer entsprechenden „Landkarte“ (oder auch „Heat Map“) darstellen:

36 Siehe auch → *Schulz*, Kap. 1 Rn. 49, sowie zum Risikomanagement allgemein → *Romeike*, Kap. 9.

37 Siehe <https://www.transparency.de/cpi/> (zuletzt abgerufen am 12.8.2024).

38 Siehe zum Beispiel für die Immobilienwirtschaft in Deutschland die Risikoübersicht der Initiative Corporate Governance der deutschen Immobilienwirtschaft e. V. unter <https://icg-institut.de/wp-content/uploads/2020/07/Risikoubersicht-final.pdf> (zuletzt abgerufen am 12.8.2024).

39 Siehe unter anderem: *Moosmayer*, Compliance-Risikoanalyse, 1. Aufl. 2015, 6 Rn. 24 ff., sowie → *Schulz*, Kap. 1 Rn. 47 ff., und → *Romeike*, Kap. 9.

	Acme Konzern	Corporate Functions	Zentraleinkauf	Corporate Finance	Treasury	Accounting	Region EMEA	Acme Deutschland	Einkauf	Key Account Management	HR	...
Rechtsgebiet												
Kartellrecht												
Einkaufskartell												
Preisabsprachen												
Arbeitsschutz und Sicherheit												
Intellectual Property Rights												
Verstoß Lizenzvereinbarungen												
Untergang Lizenzen												
Datenschutz												
Korruption												

Abbildung 7: Risk Map nach Risikogebieten und Organisations-Struktur

b) Analyse bestehender Strukturen

- 56
- In der zweiten Phase werden die bestehenden Strukturen und Prozesse in den oben beschriebenen internen Komponenten des Systems der Unternehmensüberwachung auf ihren Beitrag zur Überwachung der im ersten Schritt ermittelten Risiken hin analysiert. Mit einzubeziehen sind die vorhandenen personellen und technischen sowie finanziellen Ressourcen. Dabei ist es hilfreich, auch bereits bestehende Verknüpfungen, zum Beispiel zwischen Risikomanagement und Controlling, zu benennen.

c) Ermittlung des Anpassungsbedarfs

- 57
- In einem dritten Schritt wird aus der Analyse der bestehenden Strukturen abgeleitet, welche Anpassungen in den Strukturen und Prozessen der vorhandenen internen Komponenten vorzunehmen sind, um ein den Risiken angepasstes System der Unternehmensüberwachung zu erhalten. Dabei sollten unternehmensindividuell Prioritäten definiert werden, die dann die Basis für die Planung der Umsetzung der Optimierung der bestehenden Strukturen bilden. Denn gerade in der beschriebenen Zielgruppe von Unternehmen sind Unternehmer wie Management bemüht, unnötige Kosten speziell in den Nicht-Leistungsprozessen zu minimieren. Auf Basis der gesetzten Prioritäten können daher einzelne Anpassungsmaßnahmen aufwandsseitig geplant und bewusst zeitlich gestaffelt vorgenommen werden.

d) Umsetzung

Die Umsetzung der Maßnahmen erfolgt dann durch eine Anpassung von Prozessen und Strukturen und – soweit erforderlich – durch die Einführung neuer Instrumente und Systeme. **58**

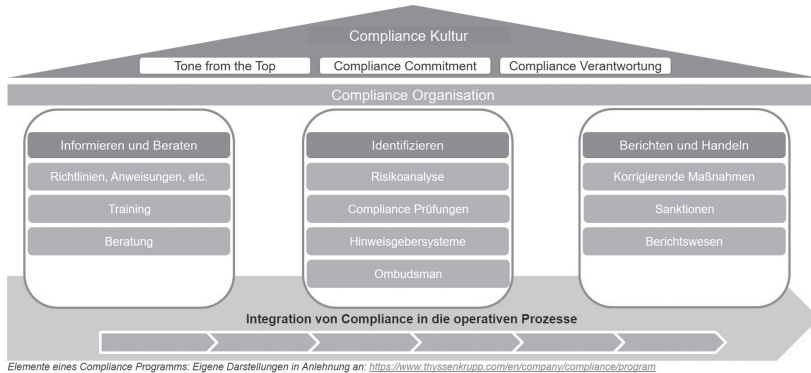


Abbildung 8: Einführung von Elementen des Compliance Managements⁴⁰

„Klassische“ Elemente des Compliance Managements wie entsprechende Richtlinien (Code of Conduct etc.) und Hinweisgebersysteme sind in den meisten Fällen neu einzuführen. Durch Nutzung entsprechender branchenspezifischer Richtlinien und Vorlagen lässt sich der Aufwand für Richtlinien aber deutlich begrenzen.⁴¹ **59**

Auf Basis dieser definierten Richtlinien können dann entsprechende Trainings entwickelt werden. Diese müssen die Mitarbeiter nach der Einstellung zum Beispiel in Form eines webbasierten Trainings durchlaufen.⁴² **60**

Funktionen wie die eines Ombudsmanns oder Hinweisgebersysteme⁴³ können Beispiel auch an entsprechende Dienstleister vergeben werden. Damit werden nicht nur die Kosten stärker variabel gehalten. Vielmehr kann ein Externer als Ansprechpartner bei Compliance-Verstößen es auch internen Mitarbeitern leichter machen, entsprechende Hinweise zu geben, gerade wenn die Hinweise Kollegen oder Vorgesetzte betreffen. **61**

⁴⁰ Elemente eines Compliance-Programms: eigene Darstellung in Anlehnung an <https://www.thyssenkrupp.com/en/company/compliance/program> (zuletzt abgerufen am 12.8.2024).

⁴¹ Zum Beispiel: <http://www.markenverband.de/kompetenzen/corporate-social-responsibility/code-of-conduct> (zuletzt abgerufen am 19.3.2024).

⁴² Zu Schulungen ausführlich → *Hastenrath*, Kap. 6.

⁴³ Siehe hierzu auch → *Sonnenberg/Block*, Kap. 5, sowie *Moosmayer*, Compliance, 4. Aufl. 2021, Rn. 26.

- 62 Die Prüfung auf Einhaltung der Compliance-Vorschriften kann als Bestandteil der Arbeit der internen Revision durch eigene Kräfte oder aber auch durch externe Dienstleister erfolgen.
- 63 Neben diesen Elementen kann es aber auch erforderlich sein, die bestehenden operativen Prozesse durch weitere Compliance-Elemente zu ergänzen. Als Beispiel hierfür sei die Integration des sog. „Business Partner Screenings“ in die Einkaufs- und Vertriebsprozesse genannt.
- 64 Beim „Business Partner Screening“⁴⁴ werden sowohl Kunden als auch Lieferanten im Rahmen der Einkaufs- und Vertriebsprozesse hinsichtlich möglicher Risiken aus den Bereichen Geldwäsche und Korruption überprüft und bewertet. Dazu werden öffentlich zugängliche Informationen und entsprechende Datenbanken genutzt. Einige Anbieter bieten hierfür eine entsprechende Integration in die IT-gestützten Prozesse an.
- 65 Bei Vorliegen entsprechender Verdachtsmomente wird dann auf Basis bestimmter Regeln und durch Management Judgement entschieden, ob mit dem Geschäftspartner weiterhin Geschäftsbeziehungen aufrechterhalten werden, ggf. auch unter einem Monitoring der weiteren Entwicklung.

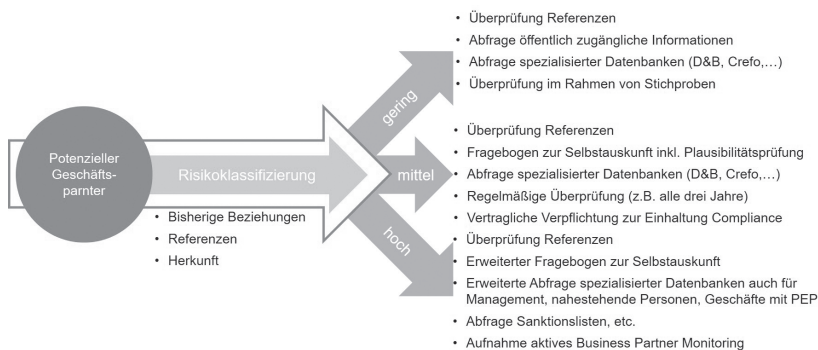


Abbildung 9: Ergänzung des internen Kontrollsystems

- 66 Ein weiteres Beispiel ist die Ergänzung der vorhandenen Prozesse um zusätzliche Maßnahmen zur Abwehr z. B. von Risiken aus dolosen Handlungen. So ergänzte ein Unternehmen der Immobilienwirtschaft sein bisheriges „Vier-Augen-Prinzip“ bei der Genehmigung von Bau- und Instandhaltungsmaßnahmen in den Niederlassungen durch eine rein zufallsgesteuerte Weiterleitung einzelner Bestellungen einer Niederlassung an eine weitere Niederlassung, die künftig die fachliche Angemessenheit der Bestellung prüft.

44 Siehe hierzu u. a. Potinecke/Schaffner/Posch, in: Hamann/Sigle/Grub, Gesellschaftsrecht, Finanzierung, Unternehmensnachfolge, § 17 Governance, Risk, Compliance (GRC) Rn. 194–199. Zur Frage der Compliance in der Lieferkette siehe → Schleper/Förstl, Kap. 17.

Daneben kann auch eine halbjährliche Analyse der Vergabe von Aufträgen im Zusammenhang mit einer Analyse von Nachforderungen, der Qualität der Lieferanten dabei helfen, selbst relativ „gut“ gesteuerte Korruptionsansätze zu verhindern. **67**

4. Fazit

Mittelständisch geprägte Unternehmen weisen häufig einen geringeren Grad der Standardisierung und Dokumentation von Prozessen, Strukturen und Systemen auf. Um dennoch eine angemessene Überwachung der Unternehmen zu erreichen, ohne ein Ausufern der Kosten der Überwachung zu riskieren, bietet es sich an, auf den vorhandenen Strukturen, Prozessen und Instrumenten aufzusetzen und diese auf Basis einer Risikoanalyse zu optimieren. **68**

Eine Einrichtung von Systemen der Überwachung, wie sie internationale Konzerne entweder aus regulatorischen Zwängen oder wegen ihrer Komplexität erfordern, würde mittelständische Unternehmen aus Kosten- und Ressourcenperspektive zumeist überfordern. Daher sollte der Fokus auf der Optimierung und punktuellen Erweiterung der vorhandenen Komponenten liegen, die bereits vorhandene Zusammenhänge und Abhängigkeiten berücksichtigen. **69**

Abschnitt 2.2

Datenschutz und IT-Security

12. Kapitel

Datenschutz im Compliance Management

I. Einleitung

Mit der stetig voranschreitenden Digitalisierung¹ und der neben den klassischen personenbezogenen Daten auch aus mit dem Internet verbundenen Geräten generierten Daten und deren Zuordnung zu Personen (Internet of Things, kurz „IoT“), gewinnt nicht nur in Konzernen das Daten(schutz)management eine immer größere Bedeutung. Gerade die Technikgestaltung, Produktentwicklung und Datenverarbeitung im Personalmanagement erfordern eine frühzeitige Auseinandersetzung mit datenschutzrechtlichen Fragestellungen. Das Inkrafttreten der Datenschutzgrundverordnung (**DSGVO**) im Mai 2018 hat zu einer Dynamik bei der Anwendung, Umsetzung und Beachtung von datenschutzrechtlichen Vorschriften geführt, welche im dynamischen Umfeld der Digitalisierung durch den AI Act² sowie den Data Act³ zu komplexen Wechselwirkungen führen und bei der datenschutzrechtlichen Bewertung hinsichtlich Zulässigkeit und Folgenabschätzung erheblichen Einfluss haben werden. Nicht immer traf der Datenschutz auf Zustimmung und so kam es teilweise auch zu medial wirksam dargestellten Kapriolen, die teilweise Kopfschütteln verursachten.⁴ Dennoch bleibt aber festzustellen, dass die DSGVO neben einzelnen Schwierigkeiten zu erheblicher Rechtssicherheit geführt hat und viele Befürchtungen sich seit Mai 2018 nicht bestätigt haben. Vielmehr erweist sich die DSGVO als moderne Regelung zum Datenschutz, die im Zuge der praktischen Umsetzung zu immer mehr Rechtssicherheit führt und zudem sogar von anderen Staaten bei der Ausgestaltung ihrer Datenschutzgesetze herangezogen wird.⁵ Zudem erfährt der Datenschutz auch dadurch einen Bedeutungsgewinn, dass immer mehr Menschen ein Verständnis dafür entwickelt haben, was Datenschutz bedeutet und sie machen ihre diesbezüglichen Rechte verstärkt geltend. Auch die zunehmende Bedeutung

1 Siehe auch → *Jacobs*, Kap. 13 Rn. 1 ff.

2 KI-Verordnung: <https://digital-strategy.ec.europa.eu/de/policies/regulatory-framework-ai> (zuletzt abgerufen am 19.3.2024).

3 Das Datengesetz: <https://digital-strategy.ec.europa.eu/de/policies/data-act> (zuletzt abgerufen am 19.3.2024).

4 U. a. <https://www.bunte.de/family/kinder-schule/kinderbetreuung/dsgvo-wahnsinn-datenschutz-extrem-bei-dieser-kita-haben-auf-fotos-jetzt-alle-gesichter-schwarze.html> (zuletzt abgerufen am 25.12.2023).

5 Siehe u. a. <https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do> (zuletzt abgerufen am 19.3.2024).

von Compliance in Unternehmen hat dazu geführt, dass Datenschutzgesetze und deren Beachtung verstärkt intern überwacht werden (müssen).

- 2 Worum geht es eigentlich beim Datenschutz? Datenschutz ist der Schutz des Einzelnen vor der Beeinträchtigung seines Persönlichkeitsrechts im Allgemeinen und seiner Privatsphäre im Besonderen, einschließlich des Rechts auf informationelle Selbstbestimmung durch die Erhebung und Verarbeitung bestimmter Daten, die Aufschluss über das Verhalten einer Person geben, d. h. „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen“ (Art. 4 Abs. 1 DSGVO)⁶ und der Schutz vor Missbrauch dieser Daten dort, wo sie denn einmal erhoben wurden. Der Datenschutz soll also die möglichst ungehinderte und ungestörte Bewegungsfreiheit im datenerhebungsfähigen Bereich für jeden Einzelnen gewährleisten, soweit keine schutzwürdigen Interessen eines Dritten entgegenstehen. Der Begriff „Datenschutz“ verleitet noch immer zu Fehlinterpretationen, denn es geht in erster Linie nicht darum, Daten im technischen Sinne zu schützen (z. B. Geschäftsgeheimnisse oder Finanzdaten) – dies ist primäre Aufgabe der IT-Sicherheit⁷ oder dies wird durch andere Gesetze geschützt.⁸ Die IT-Sicherheit gewährleistet – soweit personenbezogene Daten von der Datenverarbeitung betroffen sind – regelmäßig die technische Umsetzung sowie die Effektivität der technischen und organisatorischen Maßnahmen zum Schutz der Daten. Das ob, zu welchem Zweck und in welcher Form personenbezogene Daten verarbeitet werden, ist dagegen Kernaufgabe des Datenschutzes. Dabei können die Kernaufgaben des Datenschutzes unmittelbar aus Art. 5 DSGVO abgeleitet werden: Denn hiernach hat die Verarbeitung von personenbezogenen Daten nach Treu und Glauben, transparent und rechtmäßig zu erfolgen, wobei der Grundsatz der Datenminimierung zu wahren ist und die erhobenen Daten richtig sein müssen. Ferner sind die Daten nach Zweckerreichung wieder zu löschen und sie müssen mit geeigneten Maßnahmen verarbeitet werden, um ihre Integrität und Vertraulichkeit zu wahren.
- 3 Hilfreich zum Verständnis des Datenschutzes ist ein Blick in die historische Entwicklung des Persönlichkeitsrechts, der nicht erst bei der Entstehung des Datenschutzrechts im heute engeren Sinne ansetzt. Denn der Begriff des Datenschutzes erfuhr seine heute übliche Bedeutung in Deutschland erst in den 1970er

6 Gemäß Art. 4 Nr. 1 DSGVO sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

7 Siehe auch → *Jacobs*, Kap. 13.

8 Siehe Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG); dieses Gesetz dient dem Schutz von Geschäftsgeheimnissen vor unerlaubter Erlangung, Nutzung und Offenlegung.

Jahren⁹ und wurde zuvor teilweise auch für Datensicherheit verwendet.¹⁰ Schaut man jedoch zurück in die historische Entwicklung des Persönlichkeitsrechts, dann reiht sich der Datenschutz ein in den Schutz der Privatsphäre und die Einflussnahme darauf, was über eine Person uneingeschränkt veröffentlicht oder in Erfahrung gebracht werden darf. Damit steht der Datenschutz als Teilbereich der Privatsphäre stets im Spannungsfeld mit der Meinungsfreiheit und dem Schutz der Allgemeinheit vor Gefahren (u. a. Informationsbedürfnis der Allgemeinheit sowie Terrorabwehr und damit zusammenhängende Datenabgleiche vs. Schutzinteressen des Einzelnen). In ganz besonderem Maße ist in diesem Zusammenhang auf die Verarbeitung von Daten zur Abwehr und Eindämmung von Pandemien, wie COVID-19, zu verweisen; hier wurden nicht nur die persönlichen Freiheiten jedes Einzelnen im Allgemeinen sondern insbesondere auch der Datenschutz einer harten Bewährungsprobe unterzogen.¹¹ Zieht man diesen weiten Bogen und betrachtet das Recht auf Datenschutz als Bestandteil des Persönlichkeitsrechts und der Privatsphäre, dann ist die Rechtsentwicklung hierzu weit älter: Bereits 1890 erschien erstmals ein Artikel im Harvard Law Review zum Thema Privatsphäre.¹² Darin wird zum ersten Mal der Begriff „Privacy“ definiert, welcher im englischsprachigen Raum oft synonym zum Begriff „Data Protection“ oder „Data Privacy“ verwendet wird. Privatsphäre wird dort im Ergebnis als Recht definiert, in Ruhe gelassen zu werden („right to be let alone“). Die Autoren des Artikels schreiben vor dem Hintergrund der sich gerade als Massenphänomen im Journalismus verbreitenden Fotografie, dass die Rechtsentwicklung die Privatsphäre hervorgebracht habe, welche Anerkennung in der Rechtsprechung erfordere. Politische, soziale und wirtschaftliche Veränderungen erfordern die Anerkennung von neuen Rechten und das (Gewohnheits-)Recht in seiner ewigen Jugend entwickelt sich, um den gesellschaftlichen Anforderungen gerecht zu werden.¹³ Diese Worte gelten auch heute noch, gerade vor dem Hintergrund der mit der COVID-19-Pandemie einhergehenden Auseinandersetzung über Zweck und Umfang der Verarbeitung auch sensibler personenbezogener Daten im Anwendungsbereich der DSGVO.

Obwohl der o. a. Vergleich manch einem Leser als weit hergeholt erscheinen mag, 4
gilt die Definition des Begriffs der Privatsphäre im US-Rechtsraum noch heute als Grundlage für die Anerkennung des Rechts auf Privatsphäre im datenschutzrechtlichen Sinne. Zwar erfolgte die damalige Auseinandersetzung mit der Privatsphäre vor dem Hintergrund der Entwicklung der Fotografie. In Deutschland

9 Seidel, Datenbanken und Persönlichkeitsrecht, unter besonderer Berücksichtigung der amerikanischen Computer Privacy.

10 Siehe Datenschutzgesetz des Landes Hessen vom 7.10.1970, <http://starweb.hessen.de/cache/GVBL/1970/00041.pdf#page=1> (zuletzt abgerufen am 19.3.2024).

11 Im Einzelnen dazu: Schmitz, ZD-Aktuell 2020, 04404; Geminn/Johannes/Miedzianowski, ZD-Aktuell 2020, 07073; <https://www.datenschutz-bayern.de/corona/> (zuletzt abgerufen am 19.3.2024).

12 Warren/Brandeis, 4 Harvard Law Review, 1890, 193 ff.

13 Warren/Brandeis, 4 Harvard Law Review, 1890, 196 f.

mündete diese Entwicklung im Jahre 1907 in die Regelung durch das Kunsturhebergesetz, welches ganz wesentlich davon getragen wurde, die Privatsphäre von Personen des öffentlichen Lebens vor zu aufdringlichen Fotografen schützen zu wollen.¹⁴ Jedoch ist gerade in Zeiten der rasant voranschreitenden Digitalisierung die Verbindung von ursprünglich nicht unmittelbar vom Datenschutz erfassten Lebensbereichen unter Berücksichtigung des Rechts auf Privatsphäre gesamtgesellschaftlich zu betrachten.¹⁵ Gerade auch mit dem Internet der Dinge (IoT) und der daraus resultierenden digitalen Verknüpfung aller Lebensbereiche ist der Datenschutz neu und gesamtgesellschaftlich vor diesem Hintergrund zu bewerten.

- 5 Damit bleibt der Datenschutz eine herausfordernde und stets aktuelle Aufgabe. Die Möglichkeit der umfassenden Datenerfassung bei einer Vielzahl menschlicher Tätigkeiten (Lokalisierung über das Mobiltelefon oder den Pkw, Gesundheitsdatenerfassung über Smartwatches, Telemetriedatenerfassung im Pkw zur Erlangung eines günstigeren Kfz-Versicherungstarifs, Kaufverhalten in Online-Shops etc.) lässt die Aufgabenfülle des Datenschutzbeauftragten schier endlos erscheinen. Diese Aufgaben zu strukturieren, zu organisieren und zu administrieren, ist herausfordernd aber auch spannend. Während die datenschutzrechtliche Compliance in Unternehmen vor Inkrafttreten der DSGVO im Mai 2018 oft nur wenig priorisiert wurde und kurzfristige DSGVO-Projekte nur punktuell die Datenschutz-Compliance sicherstellen konnte, sind Unternehmen gut beraten, den Schutz der Privatsphäre von Personen und mithin des Datenschutzes ernst zu nehmen und diesen als dauerhafte Aufgabe in Unternehmensabläufen zu verfestigen. Und das aus folgenden Gründen:
1. Bürger, als Verbraucher und Kunden haben inzwischen ein wesentlich besseres Verständnis bezüglich der Rechte an ihre Person betreffende Daten entwickelt. Unternehmen, die bei den Bürgern im Ruf stehen, es mit dem Datenschutz nicht so genau zu nehmen, werden von diesen, d.h. Kunden und Mitarbeitern, negativ wahrgenommen und gemieden.¹⁶
 2. Die DSGVO erfordert eine höhere Sorgfalt beim Umgang mit personenbezogenen Daten (Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO). Bei einer unzureichenden datenschutzrechtlichen Compliance werden immer höhere Bußgelder erhoben, die Unternehmen erheblichen Schaden zufügen können.¹⁷

14 Zur Entstehung des Kunsturhebergesetzes siehe insofern *Prinz*, Medienrecht: Die zivilrechtlichen Ansprüche, 1. Aufl. 1999, Rn. 786.

15 Datenhungrige Autos – ADAC deckt auf: Diese Daten senden moderne Autos ständig an den Hersteller, http://www.focus.de/auto/ratgeber/sicherheit/datenhungrige-autos-adac-deckt-auf-diese-daten-senden-moderne-autos-staendig-an-den-hersteller_id_5580278.html (zuletzt abgerufen am 19.3.2024).

16 Siehe *Conroy/Milano/Narula/Singhal*, Building customer trust, <https://www2.deloitte.com/us/en/insights/topics/risk-management/consumer-data-privacy-strategies.html> (zuletzt abgerufen am 19.3.2024).

17 Siehe Art. 83 Abs. 1 DSGVO: „Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.“; insofern siehe

Vor diesem Hintergrund tun Unternehmen gut daran, den Datenschutz sorgfältig in die Compliance-Struktur zu integrieren. Es wird in Unternehmen mit erheblichem Verbraucher-Kontakt oder umfassendem Umgang mit personenbezogenen Daten von gesteigerter Bedeutung sein, den Datenschutz allumfassend im Unternehmen zu implementieren und ein funktionierendes Datenschutzmanagementsystem („DMS“) zu etablieren. **6**

II. Der konzeptionelle Schutz personenbezogener Daten

1. Gesetzliche Grundlagen

Die Verwendung personenbezogener Daten und der Schutz personenbezogener Daten sowie damit zusammenhängende Pflichten und Rechte aber auch etwaige Bußgelder oder gar Strafen bei Verstößen sind in Deutschland umfassend gesetzlich geregelt. Allerdings sind die gesetzlichen Grundlagen nicht zuletzt durch die DSGVO für den Anwender in der Praxis eine nur schwer zu erarbeitende Materie. Nachfolgend werden die für die Praxis wesentlichen gesetzlichen Grundlagen kurz und bündig dargestellt. **7**

a) Datenschutzgrundverordnung

In der Praxis hat die DSGVO das BDSG abgelöst und nunmehr die größte Bedeutung bekommen. Die DSGVO regelt den Umgang mit personenbezogenen Daten für privatwirtschaftliche Unternehmen. **8**

Das bisher bestehende System aus Richtlinien und nationalen Gesetzen wurde durch die DSGVO verdrängt, da sie als Verordnung Geltungs- und Anwendungsvorrang hat. Die DSGVO gilt ohne Umsetzungsakt unmittelbar in allen EU-Mitgliedstaaten. Im Gegensatz zu einer Richtlinie ist es den Mitgliedstaaten daher nicht möglich, den von der Verordnung festgeschriebenen Datenschutz durch nationale Regelungen abzuschwächen oder zu verstärken. Die DSGVO ist am 14.4.2016 durch das EU-Parlament beschlossen worden und damit endete die seit 2012 andauernde Gesetzgebungsphase für die DSGVO. **9**

Da die DSGVO die Bußgeldrahmen ganz erheblich anhebt, ist die Einhaltung datenschutzrechtlicher Vorschriften und Verpflichtungen seit 2018 essenziell. Nunmehr sind Bußgelder bis zu 20 Mio. EUR oder 4% des weltweiten Jahresumsatzes, je nachdem was höher ist, möglich. Damit hat das Thema Datenschutz in der Unternehmenspraxis einen herausgehobenen Stellenwert bekommen. Ferner ist der geografische Anwendungsbereich des europäischen Datenschutzes **10**

auch die neue Bußgeldpraxis: Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, siehe https://www.datenschutzkonferenz-online.de/media/st/20230118_DSK_Stellungnahme_Datenschutzverstoesse_von_Unternehmen.pdf (zuletzt abgerufen am 19.3.2024), vom 5.1.2023; Leitlinien 04/2022 zur Berechnung von Bußgeldern nach der DSGVO, siehe https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf; <https://www.enforcementtracker.com/> (zuletzt abgerufen am 19.3.2024); Rost/Wigger, CB 2023, 333 ff.

rechts erheblich ausgeweitet worden – so findet die DSGVO immer dann Anwendung, wenn personenbezogene Daten von Bürgern der EU-Mitgliedstaaten erhoben, verarbeitet und genutzt werden – und zwar unabhängig davon, wo dies geschieht.

- 11 Weitere wichtige Neuerungen mit Praxisrelevanz sind die Benachrichtigung der Aufsichtsbehörde bei der Übermittlung von personenbezogenen Daten an Behörden und andere staatliche Stellen von Drittstaaten sowie die sog. Datenportabilität. Demnach müssen nun – wie man es etwa von Telefonnummern kennt – Daten vom bisherigen zu einem neuen Anbieter auf Wunsch des Betroffenen portiert werden. Die neu eingeführten Vorgaben zu „data protection by design and by default“ (Datenschutz durch Technikgestaltung und Voreinstellung) und das „data protection impact assessment“ (Datenschutzfolgenabschätzung) haben ebenfalls erhebliche Praxisrelevanz.
- 12 Auch wenn von Kritikern der DSGVO stets behauptet wurde, das hohe Datenschutzniveau in Deutschland würde durch die europäischen Reformbestrebungen herabgesetzt, war die Herstellung von Compliance mit den neuen Vorgaben für die Unternehmen mit einem teilweise sehr großem Aufwand verbunden.

b) Bundesdatenschutzgesetz

- 13 Das BDSG trat 1977 in Kraft und unterlag seitdem einer ständigen Weiterentwicklung und Anpassung an die jeweils aktuellen Gegebenheiten und europäischen Vorgaben. Es wurde 1990, also rund sieben Jahre nach dem sog. Volkszählungsurteil des Bundesverfassungsgerichts, neu gefasst. Eine dritte Fassung trat 2001 zur Umsetzung der Vorgaben aus der EG-Datenschutzrichtlinie 95/46/EG in Kraft. Eine Reihe von Datenschutzskandalen führte 2009 zu einer weiteren Überarbeitung. Am 25.5.2018 schließlich hat die DSGVO das alte BDSG im Wesentlichen abgelöst.
- 14 Mit Inkrafttreten der DSGVO am 25.5.2018 trat auch das neue BDSG 2018 in Kraft. Das neue BDSG 2018 stellt eine Konkretisierung der DSGVO dar, denn die DSGVO enthält einige Öffnungsklauseln für nationale Regelungen. Art. 88 DSGVO eröffnet den Mitgliedstaaten die Möglichkeit, den Beschäftigtendatenschutz national zu regeln. Von dieser Möglichkeit hat der deutsche Gesetzgeber Gebrauch gemacht. Das BDSG 2018 enthält unter anderem die wesentlichen Bestimmungen für den Beschäftigtendatenschutz aber auch viele weitere Konkretisierungen der DSGVO. Insofern hat sich die Komplexität des Datenschutzrechts leider nicht reduziert – für eine abschließende Beantwortung datenschutzrechtlicher Fragestellungen muss auch das BDSG 2018 herangezogen werden, da hier zum Teil relevante Konkretisierungen enthalten sind.

c) Landesdatenschutzgesetz

- 15 Die einzelnen Datenschutzgesetze der Bundesländer regeln den Umgang mit personenbezogenen Daten für öffentliche Stellen der Länder. Die Gesetze sind

für die privatwirtschaftliche Praxis daher regelmäßig von nachrangiger Relevanz. Abgrenzungsfragen können sich aber bei wirtschaftlichen Unternehmen der Gemeinden oder Gemeindeverbände, Eigenbetrieben oder juristischen Personen des öffentlichen Rechts, die am Wettbewerb teilnehmen, ergeben. Die Landesdatenschutzgesetze unterscheiden sich aber inhaltlich kaum und spiegeln im Wesentlichen die Vorschriften des BDSG wider. Im Regelfall dürfte also eine nach BDSG zulässige Datenverarbeitung auch nach den jeweiligen Landesdatenschutzgesetzen zulässig sein.

Eine gewisse Praxisrelevanz haben die Landesdatenschutzgesetze aber auch für die Privatwirtschaft, da sie zumeist auch die für die diese zuständige Aufsichtsbehörde festlegen. **16**

d) Europäische Richtlinien und Verordnungen

Das Datenschutzrecht ist maßgeblich von europarechtlichen Vorgaben geprägt. Neben der DSGVO sind die sog. Richtlinie für elektronische Kommunikation 2002/58/EG („ePrivacy Richtlinie“) und die in der Praxis als „Cookie-Richtlinie“ bezeichnete E-Privacy-Richtlinie 2009/136/EG hervorzuheben. **17**

Die durch die DSGVO abgelöste Datenschutzrichtlinie 95/46/EG war bis zum Inkrafttreten der DSGVO die wichtigste europarechtliche Regelung zum Datenschutz. Wie jede Richtlinie bedurfte sie der Umsetzung in nationales Recht – und zwar ohne größere nationalstaatliche Abweichungen, d. h. im Wege der sog. Vollharmonisierung. In Deutschland wurde sie im Wesentlichen durch eine Anpassung des bestehenden BDSG in nationales Recht umgesetzt. **18**

Die sog. Cookie-Richtlinie regelt sehr kleinteilig und detailliert die Verwendung von sog. Cookies, also Dateien, die Informationen über den Nutzer von Webseiten enthalten und z. B. Rückschlüsse auf seine Gewohnheiten zulassen können. Das sog. Profiling und Targeting, also die vermeintliche bedarfs- und nutzergerichtete Werbung sollte nach Ansicht des europäischen Gesetzgebers nur unter erschwerten Bedingungen zulässig sein, da man ansonsten den Schutz der Privatsphäre gefährdet sah. Praxisrelevanz hatte insbesondere das Erfordernis einer Einwilligung für die Verwendung von Cookies für Werbezwecke im weiteren Sinne. **19**

Die Datenverordnung oder englisch „Data Act“ zielt darauf ab, den Austausch und die Nutzung von Daten innerhalb des Europäischen Wirtschaftsraums zu erleichtern und zu fördern. Die Verordnung (EU) 2023/2854 trat am 11.1.2024 in Kraft und ist ab dem 12.9.2025 anwendbar. **20**

Das Gesetz über digitale Dienste oder englisch „Digital Services Act“ beinhaltet Haftungs- und Sicherheitsvorschriften für digitale Plattformen, Dienste und Produkte. Das Gesetz über digitale Dienste ist seit dem 17.2.2024 vollständig anwendbar – die Kernvorschriften waren bereits seit dem 16.11.2022 anwendbar. **21**

Der sog. AI Act, die Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz, befindet sich derzeit noch im parlamentarischen Prozess und soll den Umgang mit künstlicher Intelligenz (KI) umfassend regeln. Es wird **22**

derzeit nicht mit einem Inkrafttreten des AI Act vor 2025 gerechnet, und anwendbar wären die Regelungen zwölf Monate nach Inkrafttreten.

e) Weitere Gesetze mit datenschutzrechtlichen Vorgaben

- 23** Große Praxisrelevanz können die spezialgesetzlichen Regelungen in diversen Nebengesetzen haben. Wichtige Gesetze in diesem Zusammenhang sind das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG), dessen Anwendungsbereiche und datenschutzrechtlichen Regelungen nachfolgend kurz dargestellt werden. Zudem enthält das Gesetz gegen unlauteren Wettbewerb (UWG) eine in der Praxis überaus relevante Vorschrift zur Verwendung von Daten zu Werbezwecken.
- 24** Das TDDDG enthält in Teil 2 besondere bereichsspezifische Vorgaben und Verpflichtungen betreffend den Umgang mit personenbezogenen Daten. Hervorzuheben sind die detaillierten Vorgaben für eine rechtmäßige Erhebung und Nutzung von sog. Verkehrsdaten und Standortdaten. Zudem sind Diensteanbieter zur Wahrung des Fernmeldegeheimnisses verpflichtet, dessen Verletzung strafrechtlich sanktioniert werden kann und daher von besonderer Praxisrelevanz ist.

25 **Vorsicht bei der Auswertung von E-Mails und anderen Telekommunikationsdaten**

Bevor E-Mails ausgewertet und gesichtet werden, sollte geprüft werden, ob die private Nutzung des betrieblichen E-Mail-Systems gestattet oder ausdrücklich verboten ist. Nach recht umstrittener und teilweise von Arbeitsgerichten abgelehnter, aber immer noch verbreiteter Auffassung unter anderem von Aufsichtsbehörden und insbesondere bei der hier gebotenen vorsichtigen Betrachtung, sind nämlich Unternehmen, die ihren Mitarbeitern die (auch nur gelegentliche) **private Nutzung** des dienstlichen E-Mail-Accounts **gestatten**, zur Wahrung des Fernmeldegeheimnisses verpflichtet, da sie Telekommunikationsdienste für Dritte, nämlich ihre Mitarbeiter, anbieten. Die Verletzung des Fernmeldegeheimnisses kann mit einer Freiheitsstrafe von bis zu fünf Jahren bestraft werden, vgl. § 206 StGB. Vor einer Auswertung von E-Mails etwa im Rahmen einer internen Untersuchung sollte daher die Rechtmäßigkeit sorgfältig und unter Beachtung der aktuellen Rechtsprechung geprüft werden. Eine rechtskonforme Sichtung von E-Mails und anderen Telekommunikationsdaten, die vom Fernmeldegeheimnis geschützt sind, erfordert momentan wohl regelmäßig die Einwilligung des bzw. der Betroffenen und ist daher ein mühsamer und langwieriger Prozess. In der Praxis hat man häufig aber gerade keine Zeit und es ist Eile geboten, die Daten auszuwerten, da etwa eine Kronzeugenregelung in Anspruch genommen werden soll. Hier werden häufig finanzielle gegen strafrechtliche Folgen abgewogen. Dieser Problematik kann man aber leicht entgehen, indem man die private Nutzung des betrieblichen E-Mail-Systems vollständig untersagt oder

die Nutzung von der Unterzeichnung einer umfassenden und informierten Einwilligungserklärung abhängig macht (vertiefend hierzu unten unter → Rn. 111 und 172 ff.). Sofern die private Nutzung des betrieblichen E-Mail-Accounts aber ausdrücklich untersagt ist, müssen bei der Sichtung und Auswertung von E-Mails der Mitarbeiter die datenschutzrechtlichen Vorschriften beachtet werden. Die datenschutzrechtlichen Vorschriften, hinzuweisen ist hier insbesondere auf Art. 5 und Art. 6 DSGVO, verlangen eine umfassende Interessenabwägung der berechtigten Interessen des Unternehmens mit den schutzwürdigen Interessen der Betroffenen – die Sichtung und Auswertung muss verhältnismäßig sein. Regelmäßig zulässig dürfte etwa eine Auswertung der E-Mails der zuständigen Mitarbeiter des Vertriebs sein, wenn ein begründeter Verdacht auf Bestechung oder Submissionsbetrug im Raum steht (vertiefend hierzu unten → Rn. 222 ff. und 232 ff.).

Das UWG enthält mit § 7 UWG eine überaus praxisrelevante Vorschrift zur Verwendung von personenbezogenen Daten zu Werbezwecken. Im Zusammenspiel mit den Vorgaben der DSGVO wird – leider sehr verwirrend und schwer verständlich – geregelt, unter welchen Voraussetzungen Kundendaten zu Werbezwecken verarbeitet werden dürfen. Grundsätzlich ist demnach für die Verarbeitung von personenbezogenen Daten für Werbezwecke eine umfassende Einwilligung notwendig. Die Vorgaben an eine rechtskonforme sog. informierte Einwilligungserklärung werden durch die wettbewerbsrechtliche Rechtsprechung ständig weiterentwickelt und den aktuellen Erfordernissen angepasst.¹⁸ **26**

2. Zentrale Grundsätze

Ein Kerngedanke des Datenschutzrechts ist seit der fortschreitenden Digitalisierung und der damit einhergehenden Gefahren der Schutz des Einzelnen vor dem Missbrauch seiner Daten. Ausgangspunkt ist das Grundrecht auf informationelle Selbstbestimmung, das das Bundesverfassungsgericht in einem vielbeachteten Urteil zu einer für 1983 geplanten Volkszählung herausgearbeitet hat.¹⁹ **27**

Die nachfolgend erläuterten zentralen Grundsätze bestimmen das Datenschutzrecht maßgeblich und sind für das Verständnis der gesetzlichen Vorgaben und Pflichten sowie die Umsetzung von Datenschutz-Compliance essenziell. **28**

a) Verbot mit Erlaubnisvorbehalt

Das Datenschutzrecht folgt dem Prinzip „Verbot mit Erlaubnisvorbehalt“. Diese Rechtsregel besagt, dass zunächst grundsätzlich alles verboten ist, es sei denn, es ist ausdrücklich erlaubt. Das Verarbeiten personenbezogener Daten ist also grundsätzlich verboten. Das Verarbeiten, und dazu gehört bereits das Erheben, **29**

¹⁸ Weiterführend und mit zahlreichen Praxisbeispielen hierzu: https://www.lda.bayern.de/de/thema_werbung.html (zuletzt abgerufen am 19.3.2024).

¹⁹ BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83, BVerfGE 65, 1.

personenbezogener Daten ist nur zulässig, sofern dies aufgrund einer Rechtsvorschrift erlaubt oder angeordnet ist oder der Betroffene eingewilligt hat – so Art. 5 und 6 DSGVO.

- 30** Dieser zentrale Grundsatz ist für das Verständnis des Datenschutzrechts und seine Auslegung wichtig – in der Praxis zeigt sich aber, dass die meisten Datenverarbeitungsszenarien bei entsprechender Ausgestaltung zulässig sind. Es sind aber Feinarbeit und *Awareness* der beteiligten Parteien notwendig.

31 Erlaubter Umgang mit Daten

Eine der häufigsten Fragen in der Praxis lautet: Darf ich personenbezogene Daten erheben, verarbeiten oder nutzen – und unter welchen Voraussetzungen? Die wichtigsten Erlaubnistatbestände der DSGVO und ihre Voraussetzungen sind:

- Einwilligung des Betroffenen, Art. 6 Abs. 1 lit. a, Art. 7 DSGVO
Die DSGVO hat auch Erleichterungen mit sich gebracht, so ist die bisherige strenge Schriftform, d.h., eine eigenhändige Unterschrift des Betroffenen, nicht mehr erforderlich. Die Einwilligung ist also auch auf elektronischem Weg möglich. Allerdings ist hier Vorsicht geboten, denn die verantwortliche Stelle trägt weiterhin die Beweislast, muss also jederzeit nachweisen können, dass der Betroffene eingewilligt hat. Der Betroffene muss zudem freiwillig einwilligen, d.h. ohne Zwang oder aleatorische Reize. Zudem muss der Betroffene umfassend informiert werden.
- Begründung, Durchführung oder Beendigung von Schuldverhältnissen, Art. 6 Abs. 1 lit. b DSGVO

Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung muss für die Begründung, Durchführung oder Beendigung eines Schuldverhältnisses erforderlich sein. Zudem müssen die schutzwürdigen Interessen des Betroffenen angemessen berücksichtigt werden. Diese gesetzliche Erlaubnis ist von überausgroßer praktischer Relevanz und gestattet wohl den Großteil der Datenverarbeitungsvorgänge in einem Unternehmen. (Fast) alle anderen Datenverarbeitungsvorgänge sind aufgrund nachfolgender gesetzlicher Erlaubnis zulässig.

- Wahrung berechtigter Interessen der verantwortlichen Stelle, Art. 6 Abs. 1 lit. f DSGVO

Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung muss zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich sein. Die berechtigten Interessen sind nicht abschließend aufgeführt und reichen beispielsweise von Gründen der Kostenersparnis und Effizienz bis zur Abwehr von Spionage. Wichtig ist aber, dass keine schutzwürdigen Interessen der Betroffenen überwiegen – es findet daher eine Interessenabwägung statt. Häufig können die schutzwürdigen Interessen etwa durch flankierende Maßnahmen wie Pseudonymisierung oder Anonymisierung hinreichend gewahrt werden,

sodass die berechtigten Interessen der verantwortlichen Stelle überwiegen.

- Erheben, Verarbeiten und Nutzen von Beschäftigtendaten, § 26 BDSG, Art. 6 ff. DSGVO

Art. 88 DSGVO enthält eine Öffnungsklausel für nationale Regelungen im Bereich des Beschäftigtendatenschutzes. Das BDSG enthält Regelungen zum Umgang mit solchen Beschäftigtendaten. Die Regelungen entsprechen im Wesentlichen den alten Vorgaben des § 32 BDSG. Hierzu ist jedoch die neuere Rechtsprechung des EuGH mit Wirkung für die Regelungen des § 26 Abs. 1 BDSG zu berücksichtigen, wonach diese als zu unspezifisch und damit europarechtswidrig zu bewerten sind.²⁰ Zugleich beabsichtigt der Gesetzgeber eine Reform des BDSG und der darin enthaltenen Regelungen zum Beschäftigtendatenschutz (vgl. näher → Rn. 156).²¹ Beschäftigtendaten dürfen aufgrund der gesetzlichen Erlaubnis zum Zwecke des Beschäftigtenverhältnisses erhoben, verarbeitet und genutzt werden, wenn dies für die Begründung, Durchführung oder Beendigung erforderlich ist. Demnach ist etwa das Erheben von Bewerberdaten zulässig, aber auch die Auswertung des Buchhaltungs- oder Kommunikationssystems (ggf. unter Beachtung des Fernmeldegeheimnisses) zur Aufdeckung eines Kartellverstoßes (hierzu unten unter → Rn. 182 ff. ausführlich).

- Aufdeckung von Straftaten von Beschäftigten, § 26 BDSG 2018
Zudem gestattet § 26 Abs. 1 Satz 2 BDSG die Erhebung, Verarbeitung und Nutzung personenbezogener Daten der Beschäftigten zur Aufdeckung von Straftaten eines Beschäftigten, die dieser in Ausübung seiner Beschäftigung begangen hat. Zu den hier einschlägigen Delikten gehören Betrug, Diebstahl, Unterschlagung und Bestechung, aber auch der Submissionsbetrug oder der Geheimnisverrat. Wichtig ist aber, dass tatsächliche Anhaltspunkte diesen Verdacht begründen und diese vor Beginn der Maßnahmen dokumentiert werden. Zudem ist die Verhältnismäßigkeit zu wahren (hierzu ausführlich unten unter → Rn. 232 ff.).
- Betriebsvereinbarung, § 26 Abs. 4 BDSG 2018
Das BDSG 2018 gestattet nunmehr ausdrücklich die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Beschäftigten aufgrund einer Kollektivvereinbarung. Unternehmen können also die Zulässigkeit ihrer Datenverarbeitungsmaßnahmen in einer Betriebsvereinbarung regeln – in vielen größeren Unternehmen gelebte Praxis (hierzu ausführlich unten unter → Rn. 166 ff.).

²⁰ Vgl. weitere Ausführungen im Abschnitt VI. zum Beschäftigtendatenschutz → Rn. 154 ff.

²¹ Vgl. Gesetzentwurf der Bundesregierung „Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes“, verabschiedet am 7.2.2024.

b) Prinzip der Verhältnismäßigkeit

- 32 Das Verhältnismäßigkeitsprinzip ist ein zentraler Grundsatz des Datenschutzrechts. Jede Erhebung, Verarbeitung und Nutzung personenbezogener Daten stellt einen Eingriff in das Persönlichkeitsrecht des Betroffenen dar und ist nur dann rechtmäßig, wenn die kollidierenden Interessen in einem angemessenen Verhältnis zueinander stehen.
- 33 Jede Erhebung, Verarbeitung und Nutzung personenbezogener Daten muss daher zunächst einen legitimen Zweck verfolgen und zudem angemessen sein. Das Verhältnismäßigkeitsprinzip erfordert regelmäßig, dass die gegenläufigen Interessen, d.h. die berechtigten Interessen der verantwortlichen Stelle und die schutzwürdigen Interessen des Betroffenen, sorgfältig abgewogen werden.
- 34 Ausfluss des Verhältnismäßigkeitsprinzips sind auch die gesetzlichen Vorgaben zur Datensparsamkeit, Transparenz und Zweckbindung, die nachfolgend erläutert werden.

c) Datensparsamkeit

- 35 Die Vorgaben zur Datensparsamkeit wurden durch die DSGVO deutlich verschärft. Unternehmen sind grundsätzlich verpflichtet, so wenig personenbezogene Daten wie möglich zu verarbeiten – also möglichst sparsam mit personenbezogenen Daten umzugehen. Prominentes Beispiel hierfür ist das sog. Privacy by Design, Art. 25 DSGVO, wonach Verantwortliche Datenschutz durch entsprechende Gestaltung der Technik und durch datenschutzfreundliche Voreinstellungen sicherstellen sollen. Zudem sollten Unternehmen die Daten pseudonymisieren oder anonymisieren soweit dies nach dem Verwendungszweck und mit einem verhältnismäßigen Aufwand möglich ist. Die Datensparsamkeit kann im Unternehmen durch Umsetzung des „Need to know“-Prinzips leicht umgesetzt werden.

36 Praxisbeispiele:

- Für die Teilnahme an einem Gewinnspiel vor einem Supermarkt etwa ist die Bekanntgabe der Telefonnummer oder der E-Mail-Adresse sowie Angaben zu Hobbies oder Haustieren nicht erforderlich. Bei einem Online-Gewinnspiel hingegen kann die Angabe einer E-Mail-Adresse zur Gewinnbenachrichtigung erforderlich sein.
- Klarnamen der Kunden von Banken oder Versicherungen oder Patienten von Arztlaboratorien sollten durch Pseudonyme wie etwa Kundennummern ersetzt werden, da eine Kenntnis des konkreten Kunden bzw. Patienten für viele Arbeitsschritte nicht erforderlich sein dürfte.
- Mitarbeiter von Call-Centern benötigen regelmäßig keinen vollen Zugriff auf sämtliche Kundendaten, sodass auch hier der Grundsatz der Datensparsamkeit durch eine Beschränkung der Leserechte gewahrt werden kann.

d) Transparenz

Das Datenschutzrecht verlangte stets nach Offenheit und Transparenz. Die DSGVO setzt hier aber neue Maßstäbe und widmet mit den Art. 12 ff. DSGVO dem Transparenzgrundsatz einen ganzen Abschnitt. **37**

Unternehmen müssen etwa die Betroffenen umfassend über die Verwendung ihrer Daten informieren. So müssen sie bei Erhebung der Daten über ihre Identität, die Zweckbestimmung und die Kategorien etwaiger Empfänger informieren. Zudem haben die Betroffenen ein umfassendes Auskunftsrecht und können von einer verantwortlichen Stelle etwa Auskunft über die Empfänger ihrer Daten verlangen. Umgekehrt müssen Unternehmen die Betroffenen regelmäßig benachrichtigen, wenn sie erstmals personenbezogene Daten von ihnen speichern. **38**

Auch Einwilligungen müssen den Betroffenen umfassend informieren. Dies ist in der Praxis häufig eine Gratwanderung, da eine umfassend informierende Einwilligungserklärung gleichzeitig die Vorschriften zu den allgemeinen Geschäftsbedingungen beachten muss. Die Vorschriften zu den AGB verlangen, dass die Betroffenen nicht mit Informationen überfrachtet und verwirrt werden dürfen – die Einwilligungserklärung mithin also noch transparent und verständlich ist. **39**

e) Zweckbindung

Der Grundsatz der Zweckbindung besagt, dass personenbezogene Daten regelmäßig nur für die Zwecke verarbeitet und genutzt werden dürfen, für die sie ursprünglich auch erhoben wurden. Dieser Grundsatz und seine Ausnahmen finden sich an vielen Stellen der DSGVO. Grundsätzlich dürften bei einer strengen Befolgung der Zweckbindung etwa Kundendaten, die im Rahmen eines Kaufvertrags erhoben wurden, nur für die Abwicklung dieses Vertrags genutzt werden und müssten anschließend gelöscht oder gesperrt werden. Das DSGVO gestattet gleichsam als Ausnahme vom Zweckbindungsgrundsatz, dass Unternehmen die Kundendaten unter bestimmten Voraussetzungen auch für Werbezwecke nutzen dürfen. **40**

3. Grundbegriffe

Das Datenschutzrecht ist geprägt von fachspezifischen Begriffen und gesetzlichen Definitionen, die dem Unkundigen den Zugang zu dieser Rechtsmaterie erschweren. Nachfolgend werden daher die wichtigsten Begriffe des Datenschutzrechts kurz und verständlich erläutert. **41**

Lohnender Blick in die DSGVO

Wenn man im Alltag einen Begriff nicht kennt, lohnt sich ein Blick ins Gesetz bzw. die DSGVO. In Art. 4 DSGVO sind die meisten Fachbegriffe erklärt (sog. Legaldefinition). **42**

a) Personenbezogene Daten

- 43** Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen, vgl. Art. 4 (1) DSGVO. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Demnach können zu den personenbezogenen Daten also beispielsweise der Name oder die Telefonnummer einer Person gehören, da dies Einzelangaben über persönliche Verhältnisse einer natürlichen Person sind. Ist eine natürliche Person hingegen nicht bestimmt oder bestimmbar, etwa weil an der postalischen Adresse eine Vielzahl natürliche Personen wohnen oder die Telefonnummer einem Unternehmen, also einer juristischen Person, zugeteilt ist, handelt es sich nicht um personenbezogene Daten im Sinne der DSGVO. Geschützt wären aber hingegen wiederum Name und Adresse eines eingetragenen Einzelkaufmanns, da dieser eine natürliche Person ist. Die Frage, ob ein personenbezogenes Datum vorliegt, ist also immer eine Frage des Einzelfalls und Bedarf einer sorgfältigen Prüfung.
- 44** Keine personenbezogenen Daten sind ferner anonymisierte oder aggregierte Daten, da sich die Einzelangaben in diesem Fall gerade nicht mehr einer bestimmten oder bestimmbar Person zuordnen lassen. Pseudonymisierte Daten hingegen sind noch personenbezogene Daten, da sich das Pseudonym aufdecken lässt und die natürliche Person also nach wie vor bestimmbar ist. Umstritten ist im Fall pseudonymisierter Daten allerdings, ob es sich für den Verwender auch dann um personenbezogene Daten handelt, wenn er selbst nicht im Besitz des Schlüssels zur Aufdeckung des Pseudonyms ist und möglicherweise sogar nur durch strafrechtlich relevantes Handeln an den Schlüssel gelangen kann. Bei der gebotenen vorsichtigen Betrachtung sollte grundsätzlich auch in diesem Fall davon ausgegangen werden, dass es sich um personenbezogene Daten handelt, da die natürlichen Personen hinter dem Pseudonym bestimmbar sind.

45 Personenbezogene Daten in einem Unternehmen

Nahezu sämtliche Daten, die von einem Unternehmen erhoben, verarbeitet und genutzt werden, sind personenbezogene Daten. Offenkundig ist dies etwa bei Customer Relationship-Systemen und in der Personalverwaltung. Aber auch Informationen in Finanzdatenbanken, die auf den ersten Blick als reine Finanzdaten ohne jeglichen Personenbezug erscheinen, können sich nach sorgfältiger Prüfung als personenbezogene Daten herausstellen, etwa weil alle Buchungen mit einem Kennzeichen des zuständigen Sachbearbeiters versehen sind (z. B. einer SAP User ID).

Besonders geschützt sind die besonderen Kategorien personenbezogener Daten. Hierzu zählen Angaben über rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben. Diese Informationen dürfen nur unter den besonderen Voraussetzungen des Art. 9 DSGVO erhoben, verarbeitet und genutzt werden. **46**

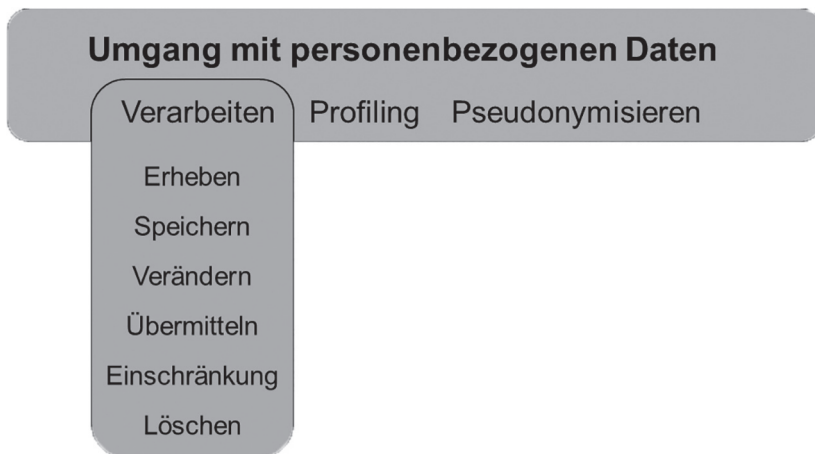
b) Verantwortliche Stelle

Die verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder diese durch andere im Auftrag verarbeiten lässt, Art. 4(7) DSGVO. **47**

Ein Unternehmen, das beispielsweise durch ein fremdes Call-Center oder ein Marktforschungsinstitut personenbezogene Daten erheben lässt, ist in Bezug auf diese Daten die verantwortliche Stelle und folglich für diese Daten und den ordnungsgemäßen Umgang mit ihnen verantwortlich. **48**

c) Umgang mit personenbezogenen Daten

Beim Umgang mit personenbezogenen Daten führt die DSGVO zu einer Vereinfachung. Wurde früher noch zwischen Erheben, Verarbeiten, Nutzen, etc. unterschieden, gibt es nunmehr nur noch den zentralen Oberbegriff der Verarbeitung, vgl. Art. 4 Abs. 2 DSGVO. Zudem gibt es weiterhin die Pseudonymisierung und neu das sog. Profiling. **49**



Verarbeitung ist jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die **50**

Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

aa) Erheben

- 51 Erheben** ist das Beschaffen von Daten über den Betroffenen und ist grundsätzlich verboten, soweit es nicht erlaubt ist oder der Betroffene eingewilligt hat (Verbot mit Erlaubnisvorbehalt). Es gilt der sog. Direkterhebungsgrundsatz, d. h. die Daten sind grundsätzlich beim Betroffenen selbst und nicht bei Dritten zu erheben.
- 52** Bei der Erhebung der Daten ist der Betroffene über die Identität der verantwortlichen Stelle, den Verwendungszweck und etwaige Empfänger zu unterrichten, vgl. etwa Art. 5 Abs. 1 lit. b DSGVO.

bb) Speichern

- 53 Speichern** ist das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck der weiteren Verarbeitung oder Nutzung. Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene grundsätzlich von der Speicherung, der Art der Daten, der Zweckbestimmung und der Identität der verantwortlichen Stelle zu benachrichtigen. Allerdings gibt es zahlreiche Ausnahmen von diesem Grundsatz, etwa wenn die Speicherung durch ein Gesetz ausdrücklich vorgesehen ist, vgl. Art. 14 Abs. 5 lit. c DSGVO.

cc) Verändern

- 54 Verändern** ist das inhaltliche Umgestalten gespeicherter personenbezogener Daten.

dd) Übermitteln

- 55 Übermitteln** ist das Bekanntgeben gespeicherter oder durch einen Datenverarbeiter gewonnener personenbezogener Daten an einen Dritten. Hierbei ist unerheblich, ob die Daten an den Dritten tatsächlich weitergegeben oder dem Dritten lediglich zur Einsicht oder zum Abruf bereitgehalten und von diesem eingesehen oder abgerufen werden. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle – also auch andere Unternehmen einschließlich der Mutter in einem Konzern oder Unternehmensverbund. Es gibt kein sog. Konzernprivileg, wonach personenbezogene Daten frei in einem Konzern ausgetauscht werden dürfen. Wie jede andere Übermittlung ist auch die Übermittlung in einem Konzern grundsätzlich verboten. Keine Übermittlung ist hingegen die Weitergabe von personenbezogenen Daten an einen Auftragsverarbeiter (siehe auch unten → Rn. 65 ff., da dieser nicht als Dritter gilt – mithin also gerade keine Weitergabe personenbezogener Daten an einen Dritten stattfindet. Neu ist nunmehr, dass die

Auftragsverarbeitung nicht zwingend in der Europäischen Union stattfinden muss. Das ist eindeutig eine Erleichterung im Vergleich zur früheren Rechtslage, wonach etwa die Weitergabe an einen Auftragsverarbeiter in Indien stets als Datenübermittlung zu werten war und folglich eine andere gesetzliche Hürde nehmen musste.

Der Empfänger der Daten, muss zudem in einem Land ansässig sein, das über ein angemessenes Datenschutzniveau verfügt. Das sind die Mitgliedstaaten der EU und die Vertragsstaaten des EWR sowie weitere Länder, für die die Europäische Kommission ein adäquates Datenschutzniveau konstatiert hat – das sind unter anderem die Schweiz und Kanada. Sofern der Staat, in dem der Empfänger der Daten ansässig ist, über kein angemessenes Datenschutzniveau verfügt, muss eine Übermittlung grundsätzlich unterbleiben, es sei denn, es wird auf andere Weise ein adäquates Datenschutzniveau hergestellt, eine gesetzliche Ausnahme greift oder der Betroffene hat eingewilligt. Werden etwa sog. EU-Standardverträge zur Datenübermittlung abgeschlossen, die den Empfänger zur Wahrung des EU-Datenschutzniveaus verpflichten, dürfen die Daten übermittelt werden. Auch verbindliche Unternehmensregeln (sog. Binding Corporate Rules, siehe Art. 47 DSGVO) können innerhalb eines Konzerns für ein angemessenes Datenschutzniveau sorgen. **56**

Schließlich können sich Datenempfänger in den USA dem neuen EU-US Data Privacy Framework unterwerfen und sich selbst verpflichten, die europäischen Datenschutzvorschriften zu befolgen (vormals das sog. Privacy Shield, das vom Europäischen Gerichtshof in der als Schrems II-Entscheidung bekannten Urteil vom 16.7.2020 für unzureichend befunden wurden).²² Der Data Privacy Framework ist eine informelle Absprache zwischen der Europäischen Union und den Vereinigten Staaten von Amerika und besteht aus Zusicherungen der US-amerikanischen Bundesregierung und einem Beschluss der EU-Kommission vom 10.7.2023. Die Garantien für die Übermittlung von Daten auf der Grundlage des Data Privacy Frameworks entsprechen nach Ansicht der EU-Kommission den Datenschutzstandards in der EU – und folglich gewährleisten teilnehmende Empfänger in den USA ein adäquates Datenschutzniveau. Die US-amerikanischen Unternehmen, die am Data Privacy Framework teilnehmen möchten, müssen sich lediglich in eine entsprechende Liste eintragen und sich selbst dazu verpflichten, die diesbezüglichen Verpflichtungen einzuhalten. Es gibt keinen Zertifizierungsprozess oder ein Genehmigungsverfahren – das Data Privacy Framework beruht nur auf Selbstverpflichtung. **57**

Gesetzliche Ausnahmen vom Erfordernis eines angemessenen Datenschutzniveaus gibt es etwa im Fall, dass die Daten für ein Gerichtsverfahren benötigt oder **58**

²² Offizielle vertiefende Informationen sowie eine Liste der teilnehmenden Unternehmen findet man auf der offiziellen Webseite: <https://www.dataprivacyframework.gov/> (zuletzt abgerufen am 19.3.2024).

die Daten für die Abwicklung eines Vertrags mit dem Betroffenen in das unsichere Drittland übermittelt werden.

- 59 Beispiel:** Ein Reisebüro darf die personenbezogenen Daten des Reisenden an die deutsche Fluggesellschaft sowie den Busunternehmer und das Hotel in Ägypten weitergeben, sofern und soweit die Übermittlung der Daten zur Abwicklung des Vertrags mit dem Betroffenen erforderlich ist.

- 60** Die Anforderungen an eine zulässige Übermittlung von Beschäftigtendaten ist unter → Rn. 188 ff. ausführlich erläutert.

61 Zwei-Stufen-Test

Ob eine Übermittlung rechtmäßig ist, kann schnell mithilfe des sog. Zwei-Stufen-Tests festgestellt werden. Auf der ersten Stufe wird geprüft, ob eine Übermittlung im Rechtssinne vorliegt und sie rechtlich zulässig ist, d.h. eine Vorschrift der DSGVO oder eine andere Rechtsvorschrift die Übermittlung gestatten oder der Betroffene eingewilligt hat.

Auf der zweiten Stufe wird geprüft, ob der Empfänger über ein angemessenes Datenschutzniveau verfügt. Die zweite Stufe entfällt daher regelmäßig bei Empfängern in der EU oder einem sicheren Drittstaat. Sitzt der Empfänger aber in einem unsicheren Drittstaat, muss entweder ein angemessenes Datenschutzniveau hergestellt werden oder die Übermittlung aufgrund einer gesetzlichen Ausnahme oder einer Einwilligung zulässig sein.

- 62 Einschränkung der Verarbeitung** (vormals **Sperren**) ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken. Nach Art. 18 DSGVO haben Betroffene das Recht, von dem Verantwortlichen bei Vorliegen bestimmter Voraussetzungen, wenn beispielsweise die Richtigkeit der Daten bestritten wird, die Einschränkung der Verarbeitung zu verlangen.

- 63 Löschen** ist das Unkenntlichmachen gespeicherter personenbezogener Daten. Grundsätzlich sind personenbezogene Daten zu löschen, soweit ihre Speicherung nicht mehr erforderlich ist, vgl. Art. 5 Abs. 1 lit. e DSGVO. Wurde beispielsweise nach Abschluss eines Kaufvertrags die Ware an den Kunden geliefert, sind die personenbezogenen Daten des Kunden grundsätzlich zu löschen, soweit die Daten nicht auch für weitere Zwecke, etwa zu Werbezwecken, erhoben und gespeichert wurden. Einer unverzüglichen Löschung können aber auch Aufbewahrungspflichten der verantwortlichen Stelle, etwa aus handels- oder steuerrechtlichen Vorschriften, entgegenstehen. Im Fall entgegenstehender Aufbewahrungspflichten sind die personenbezogenen zu sperren, d.h. so zu kennzeichnen, dass sie von weiterer Verarbeitung und Nutzung ausgenommen sind.

Erst nach Ablauf der Aufbewahrungsfristen sind die Daten dann endgültig zu löschen. Neu ist nun auch das Recht auf Vergessenwerden, d. h. Betroffenen haben einen umfangreichen Anspruch auf Löschung der sie betreffenden personenbezogenen Daten, vgl. Art. 17 DSGVO.

Privacy by Design – Unternehmen sollen sich vor jeder Einführung eines neuen IT-Systems, d. h. vor jeder Erhebung personenbezogener Daten, überlegen, welche Daten tatsächlich benötigt werden und auch wann und wie die Daten zu löschen sind. Für jede Anwendung und Datenbank in einem Unternehmen sollte es daher ein Löschkonzept geben. Im Rahmen eines unabhängigen Datenschutz-Audits oder einer aufsichtsrechtlichen Kontrolle durch die zuständige Datenschutzbehörde wird regelmäßig das Vorhandensein von effektiven Löschkonzepten geprüft.

64

d) Auftragsverarbeitung

Im Wege der Auftragsverarbeitung können Dienstleister (Auftragsverarbeiter) in einem gewissen Umfang personenbezogene Daten von Drittunternehmen (Verantwortliche) verarbeiten. Der damit einhergehende Datenaustausch bedarf selber keiner Rechtfertigung, d. h. er ist gestattet, sofern die beteiligten Unternehmen einen Vertrag über die Auftragsverarbeitung abgeschlossen haben. Die Weitergabe der Daten an den Auftragsverarbeiter ist unter diesen Umständen rechtlich keine Übermittlung, da der Empfänger nicht *Dritter* im Sinne der DSGVO ist – es bedarf für die Weitergabe damit auch keiner rechtlichen Erlaubnis und man spricht daher von einer Privilegierung der Auftragsdatenverarbeitung. Das war nach dem alten BDSG noch anders und insofern bringt die DSGVO hier eine Erleichterung mit sich – eine „privilegierte“ Auftragsverarbeitung kann auch in einem sog. Drittland stattfinden und muss nicht innerhalb der Europäischen Union erfolgen. Zu beachten ist natürlich, dass ein adäquates Datenschutzniveau etwa durch Standardvertragsklauseln sichergestellt sein muss, wenn sich der Auftragsverarbeiter in einem Drittland mit nicht adäquatem Datenschutzniveau wie beispielsweise Indien befindet.

65

Die Anforderungen an den Vertrag und seinen Inhalt sind gesetzlich vorgegeben, vgl. Art. 28 Abs. 3 DSGVO. Demnach müssen unter anderem vertraglich festgelegt werden, welche Daten verarbeitet werden sollen und dass die Daten nach Abschluss der Tätigkeiten zurückgegeben oder gelöscht werden. Zudem muss sich der Auftraggeber vor Weitergabe von personenbezogenen Daten versichern, dass der Auftragnehmer die vertraglich festgelegten technischen und organisatorischen Maßnahmen zur Sicherheit der Daten einhalten kann.

66

Der Auftragsverarbeiter verarbeitet die Daten streng weisungsgebunden und allein für Zwecke des Auftraggebers. Er ist bildlich gesprochen das Werkzeug der verantwortlichen Stelle. Abzugrenzen ist die Auftragsverarbeitung aber von der

67

sog. Funktionsübertragung, bei der der Auftragnehmer so viel Ermessen hinsichtlich der Datenverarbeitung hat und die Daten gerade nicht mehr weisungsgebunden verarbeitet, dass er als Dritter anzusehen ist. In diesem Fall ist die Weitergabe der Daten an den Auftragnehmer folglich eine Übermittlung mit der Folge, dass diese erlaubt sein muss. Die Abgrenzung zwischen einer ohne Weiteres zulässigen Auftragsverarbeitung und einer nur unter bestimmten Voraussetzungen zulässigen Funktionsübertragung ist in der Praxis nicht immer trennscharf möglich. Es ist umstritten, wann ein Auftraggeber gerade noch genug Kontrolle und Weisungsbefugnis hat, dass man von einer Auftragsverarbeitung sprechen kann und ab wann die Schwelle zu einer Funktionsübertragung überschritten wird. Werden ganze Abteilungen im Wege eines Outsourcing an einen Auftragnehmer übergeben, dürfte regelmäßig eine Funktionsübertragung vorliegen. Wird hingegen lediglich die Wartung und Pflege einer Datenbank an einen IT-Dienstleister übertragen, dürfte regelmäßig noch eine (privilegierte) Auftragsdatenverarbeitung vorliegen.

III. Betrieblicher Datenschutz

1. Pragmatischer Ansatz: Wo fange ich an?

- 68 Die erste Frage, die sich immer aufdrängt ist, ob überhaupt ein betrieblicher Datenschutzbeauftragter (**DSB**) zu bestellen ist.²³ Für öffentliche Stellen besteht die Pflicht hierzu bei automatisierter Verarbeitung personenbezogener Daten stets. Die Anforderungen an den Einsatz automatisierter Verfahren zur Verarbeitung personenbezogener Daten sind dabei gering: Es genügt z.B. der Einsatz von E-Mail-Programmen mit Adressbuch, eine elektronische Liste mit Ansprechpartnern bei Lieferanten oder Kundenlisten. Allein wenn ein kleines Unternehmen (nicht-öffentliche Stelle) diese Frage beantworten möchte, tut es schon gut daran, die Bestellung eines DSB in Erwägung zu ziehen, denn: Die Ausnahmen, wann ein DSB nicht bestellt werden muss, sind begrenzt. Grundsätzlich gilt aber, dass nur dann **kein** DSB bestellt werden muss, wenn das Unternehmen weniger als 20 Mitarbeiter mit mehr oder weniger dauerhafter Tätigkeit am PC, Kundenterminals oder sonstigen Datenverarbeitungsgeräten, wie z.B. Bestell- und Zahlungsterminals in Gastronomiebetrieben oder Auftragsterminals (automatisierte Datenverarbeitung), beschäftigt. Dagegen ist unabhängig von der Mitarbeiterzahl auch dann ein DSB zu bestellen, wenn Verarbeitungen vorgenommen werden, die (a.) einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO²⁴ unterliegen, oder wenn (b.) personenbezogene Daten ge-

23 Siehe § 5 Abs. 1 BDSG (öffentliche Stellen) sowie § 38 Abs. 1 BDSG (nichtöffentliche Stellen), jeweils in Verbindung mit Art. 37 Abs. 1 DSGVO.

24 Siehe Art. 35 Abs. 1 Satz 1 DSGVO: Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.

geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden.²⁵ Ergänzend dazu ist ein DSB dann zu bestellen, wenn die Kerntätigkeit des Unternehmens in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen oder in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DSGVO²⁶ oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO besteht. Darüber hinaus gilt, dass auch Unternehmen, die keine Pflicht zur Bestellung eines DSB haben, verpflichtet sind, die datenschutzrechtlichen Bestimmungen der DSGVO zu beachten und umzusetzen. Damit dürften fast sämtliche Betriebe, Arztpraxen, Kanzleien usw., d. h. bei sämtlichen Tätigkeiten mit EDV-Einsatz zu geschäftlichen Zwecken auch die Beachtung der Datenschutzanforderungen eine gewisse Aufmerksamkeit erfordern. Mithin sollte auch ohne Pflicht zur Bestellung eines DSB stets in Betracht gezogen werden die Funktion auf freiwilliger Basis einem Mitarbeiter zu übertragen, um die Anforderungen des Datenschutzes nicht gänzlich außer Betracht zu lassen; in Einzelfällen kann auch eine freiwillige Bestellung eines DSB angeraten sein.²⁷

Die datenschutzrechtlich formelle Bestellung des DSB sollte auch unter Berücksichtigung von Art. 5 Abs. 2 DSGVO schriftlich erfolgen. Bestellt werden kann dabei jede Person, die die berufliche Qualifikation hat, erforderliche Fachkunde und die Fähigkeit zur Erfüllung Aufgaben des DSB besitzt,²⁸ wobei der (qualitative) Umfang der Verarbeitung personenbezogener Daten das Maß der Fachkunde bestimmt. Zudem sollten weiterhin die mit der Datenverarbeitung beschäftigten Personen auf das Datengeheimnis verpflichtet werden, auch wenn die gesetzliche Pflicht direkt nun nicht mehr besteht, dennoch aber aufgrund der Bestimmungen der DSGVO weiterhin geboten erscheint.²⁹ Für diese formellen An-

69

25 Siehe § 38 Abs. 1 Satz 2 BDSG i. V. m. Art. 37 DSGVO.

26 Besondere Denkkategorien sind gemäß Art. 9 Abs. 1 DSGVO Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

27 V. d. Bussche/Voigt, Konzerndatenschutz, Teil 2, Kap. 1 Rn. 4

28 Siehe Art. 37 Abs. 5 DSGVO, Art. 39 DSGVO sowie § 4f Abs. 2 u. 3 BDSG (alt): https://www.datenschutz.rlp.de/fileadmin/lfdi/Konferenzdokumente/Datenschutz/Duesseldorfer_Kreis/Beschluesse/20101125_betdrsb.html (zuletzt abgerufen am 19.3.2024).

29 Nach dem Wegfall von § 5 Satz 2 BDSG-alt sollte vor dem Hintergrund von Art. 5 Abs. 2 und Art. 32 Abs. 4 DSGVO die Verpflichtung auf das Datengeheimnis weiterhin dokumentiert werden.

forderungen finden sich Muster im Internet, welche grundsätzlich herangezogen werden können.³⁰

- 70** Die Aufgaben des DSB sind in der DSGVO geregelt.³¹ Der DSB hat als Kernaufgaben auf die datenschutzkonforme Verarbeitung personenbezogener Daten hinzuwirken. Hierzu gehören die Unterrichtung und Beratung der Geschäftsführung und der Beschäftigten, die Datenverarbeitungen durchführen (für eigene Zwecke oder im Auftrag), hinsichtlich ihrer Pflichten nach der DSGVO sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten. Hinzu kommt die Überwachung der Einhaltung der DSGVO, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen, Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Art. 35 DSGVO. Schließlich gehört auch die Zusammenarbeit mit der Aufsichtsbehörde sowie die Funktion der Kontaktperson für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation zu Datenschutz-Folgeabschätzungen, und gegebenenfalls Beratung zu allen sonstigen Fragen dazu. Dabei ist insgesamt festzustellen, dass die Dokumentation von datenschutzrelevanten Verfahren sowie die Information von Behörden, Betroffenen und evtl. der Öffentlichkeit zunehmend an Bedeutung gewinnt.
- 71** Die Anforderungen an die datenschutzrechtliche Beratung sind vielfältig. Sie erfolgt gegenüber dem Management eines Unternehmens, gegenüber Fachabteilungen, der IT und mit zunehmender Verarbeitung von personenbezogenen Daten in verschiedensten Bereichen einer Organisation in immer komplexerer Form. Die Beratung hat dabei die IST-Situation, die Anforderungen des anzuwendenden Rechts sowie das datenschutzrechtliche Bewusstsein innerhalb der Organisation zu berücksichtigen. Je nach vorgefundener IST-Situation muss das zukünftige Soll-Niveau des Datenschutzes innerhalb eines Unternehmens definiert oder ein bereits hohes Datenschutzniveau aufrechterhalten oder weiterentwickelt werden. All diese Anforderungen sollten in strukturierten Prozessschritten entwickelt und umgesetzt werden. Gerade die Entwicklung neuer Produkte, der Einsatz neuer Software oder die Änderung von internen Prozessen erfordert die frühzeitige Einbindung des DSB, damit dieser die Entwicklung und Anpassung zielführend in einem Stadium begleitet, in dem erforderliche datenschutzrechtliche Aspekte einfließen und im Zuge der Realisierung umgesetzt werden können.

30 Siehe die Muster zur Verpflichtung auf die Vertraulichkeit: <https://www.gdd.de/service/publikationen-und-aktionen/>; https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_19.pdf (beide Quellen zuletzt abgerufen am 19.3.2024).

31 Siehe Art. 39 DSGVO.

Am Anfang einer jeden datenschutzrechtlichen Tätigkeit sollte eine Bestandsaufnahme stehen. Hierfür sind Kenntnisse der datenschutzrechtlichen Gesetze erforderlich, aber wesentlich ist ein Gespür dafür, durch Gespräche mit Kollegen und Vorgesetzten, festzustellen, welche datenschutzrechtliche Kultur im Unternehmen herrscht. Durch Gespräche mit sog. „Stakeholdern“ im Unternehmen kann sich der DSB einen Überblick über die bisherige Praxis verschaffen. Je nach Organisationsstruktur und Größe eines Unternehmens sollte daher (1.) die eigene Stellung innerhalb der Organisation/des Unternehmens konkretisiert sowie (2.) die datenschutzrechtlich relevanten Entscheidungsträger zur bisherigen datenschutzrechtlichen Praxis befragt werden. Die eigene Stellung innerhalb eines Unternehmens kann unterschiedlich ausgeprägt sein:

- direkt an die Geschäftsführung berichtend (Dies könnte wegen der unmittelbaren Berichterstattungspflicht an die höchste Managementebene sinnvoll sein)
- innerhalb der Compliance-Organisation;
- als Teil der Rechtsabteilung (In der Vergangenheit durchaus häufig anzutreffen, mit der aus der DSGVO erwachsenen Tragweite des Datenschutzes und den umfassenden administrativen Anforderungen sowie technischen Fachkenntnissen für diese Aufgabe möglicherweise nicht mehr empfehlenswert);
- unterhalb der IT-Leitung (Dies ist wegen der Schnittstelle zur IT-Sicherheit sowie der zum Datenschutz abweichenden Zielsetzung der IT/IT-Sicherheit eines Unternehmens nicht besonders praxistauglich und wird daher an dieser Stelle nicht empfohlen).

In Einzelfällen kann es auch sinnvoll sein, mit Übernahme der Funktion des DSB ein Audit von einem neutralen Dritten durchführen zu lassen, um den Status des Datenschutzes innerhalb des Unternehmens darzustellen und die Verantwortung des neuen DSB für Risiken aus der Vergangenheit zu begrenzen. 73

Je nach fachlicher und disziplinarischer Eingliederung innerhalb der Organisationsstruktur ist es für den DSB von entscheidender Bedeutung, sich gegenüber Entscheidungsträgern Gehör zu verschaffen. Nicht umsonst ist schon deshalb gesetzlich geregelt, dass der DSB „unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters“ berichtet.³² Diese direkte Berichtslinie muss keinen Einfluss auf die disziplinarische Eingliederung des DSB haben, bestimmt aber, dass sich dieser stets unmittelbar hinsichtlich datenschutzrechtlicher Fragestellungen an ein Leitungsorgan wenden können muss und dieser zumindest fachlich zu unterstellen ist.³³ 74

Die datenschutzrechtlich relevanten Entscheidungsträger, die den Erfolg der datenschutzrechtlichen Arbeit mitbestimmen, sind: 75

³² Siehe Art. 38 Abs. 3 Satz 3 DSGVO

³³ Vgl. *Jaspers/Reif*, in: *Schwartmann/Jaspers/Thüsing/Kugelmann*, DS-GVO/BDSG, 1. Aufl. 2018, Art. 38 Rn. 21.

Teil 2 Übergreifende Themen und Herausforderungen – Datenschutz und IT-Security

- der Compliance Officer;
 - der IT-Security-Verantwortliche;
 - der IT-Leiter;
 - der Personalleiter;
 - der Revisionsleiter (Internal Audit),
 - der Business-Development-Leiter (neue Produkte mit Datenschutzrelevanz, z.B. Internet der Dinge oder Betrieb eines Online-Shops und Webseiten-Kommunikation mit Kunden);
 - der Marketing-Leiter (CRM, Target Marketing o. Ä.);
 - die Geschäftsführung.
- 76 Erst nachdem die Stellung des DSB und des Datenschutzes selbst innerhalb der Organisation geklärt sind, macht es Sinn, die datenschutzrechtliche Praxis daran auszurichten.
- 77 Hierzu ist es u. a. auch von Bedeutung zu wissen, inwieweit die Organisation bereits über datenschutzrelevante Kodizes, wie z.B. Binding Corporate Rules, (Konzern-)Richtlinien oder sonst über eine ausgeprägte Dokumentation der datenschutzrechtlich relevanten Verfahren und/oder Prozesse verfügt. Die Umsetzung des Datenschutzes kann wie folgt dargestellt werden:



Abbildung 1: Hierarchie der datenschutzrechtlich relevanten Regelungen in einem Unternehmen

2. Beratungspraxis

Die Beratungspraxis des DSB ist geprägt von der eigenen Stellung im Unternehmen und der bisherigen Wahrnehmung des Datenschutzes innerhalb der Organisation. Hier hängt es vom sogenannten datenschutzrechtlichen Reifegrad³⁴ eines Unternehmens ab, wo man mit seinem Beratungsschwerpunkt ansetzt. Oftmals ist es einem DSB z. B. unmöglich, proaktiv auf sämtliche relevante Bereiche zuzugehen, um das Erfordernis datenschutzrechtlicher Beratung abzufragen. Noch schwieriger ist die datenschutzrechtliche Beratung in Unternehmen ohne Betriebsrat. Denn während der Betriebsrat die datenschutzrechtlichen Interessen der Arbeitnehmer wahrnehmen wird und damit auch das allgemeine datenschutzrechtliche Bewusstsein in einem Unternehmen fördern kann, ist ein betrieblicher DSB in Unternehmen ohne Betriebsrat nicht nur Berater zu datenschutzrechtlichen Fragestellungen, sondern auch Wahrer unternehmerischer und unternehmenskultureller Interessen, die im Hinblick auf Einzelfragen Berücksichtigung finden sollten. Dabei ist der grundsätzliche Anspruch eines Unternehmens im Auge zu behalten: Soll lediglich formal dem Datenschutzrecht entsprochen werden oder aber gilt es, auch übergeordnete Interessen des Unternehmens zu berücksichtigen? – Bei der datenschutzrechtlichen Beratung sind damit nicht nur die rechtlichen Bestimmungen, sondern auch die Unternehmensethik, üblicherweise in einem „Code of Ethics“ oder „Verhaltenskodex“ o. Ä. geregelt) und im Verhältnis zu den Betroffenenrechten (Mitarbeiter/Kunden/Lieferanten) insbesondere der Grundsatz der Verhältnismäßigkeit³⁵ zu beachten.

Bei jeder datenschutzrechtlichen Beratung ist zu differenzieren, ob es sich um proaktive oder reaktive Beratung handelt. D. h., soll eine datenschutzrechtlich relevante Maßnahme innerhalb der Organisation implementiert werden oder gab es einen Vorfall, der datenschutzrechtliches Tätigwerden erfordert? Proaktiv ist eine datenschutzrechtliche Beratung dann, wenn die Einführung neuer datenschutzrechtlicher Prozesse oder die Ausgestaltung von Verfahren oder die Dokumentation dieser im Zuge unternehmerischer Tätigkeiten für die Zukunft erforderlich wird. Reaktiv ist dagegen die datenschutzrechtliche Beratung, wenn im Zuge der unternehmerischen Tätigkeit ein Vorfall die datenschutzrechtliche Bewertung eines konkreten Sachverhalts erfordert. Während bei der proaktiven datenschutzrechtlichen Beratung häufig die Ausgestaltung rechtssicherer Prozesse im Vordergrund stehen dürfte, kommt es bei der reaktiven datenschutzrechtlichen Beratung häufig impliziter zur Bewährungsprobe für zuvor umgesetzte datenschutzrechtliche Prozesse und Verfahren.

34 Damit ist gemeint, inwieweit der Datenschutz bereits in einem Unternehmen implementiert ist, z. B. durch Richtlinien, ein Datenschutzmanagementkonzept, Bewusstsein in der Leitungsebene sowie in der Mitarbeiterschaft usw.

35 Vgl. *Schmidl*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 28 Rn. 36 ff.

80 Beispiele proaktiver datenschutzrechtlicher Beratung sind (u. a.):

- Bei der Einführung neuer Verfahren zur automatisierten Verarbeitung personenbezogener Daten:
 - die Datenschutz-Folgenabschätzung:³⁶ Diese ist bei der Verarbeitung besonderer Kategorien von personenbezogenen Daten³⁷ oder im Bereich der Leistungskontrolle und des Kundenprofilings z.B. zu Werbezwecken durchzuführen;
 - die Erstellung der Verzeichnisse der Verarbeitungstätigkeiten:³⁸ Dieses beschreibt die einzelnen eingesetzten Verfahren (Verfahrensdokumentation). Dabei ist eine gute und strukturierte Dokumentation hilfreich, die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO zu erfüllen. Wo derartige Dokumentationen fehlen oder diese nicht regelmäßig aktualisiert werden (was idealerweise im Rahmen eines „Privacy by Design“ Ansatzes innerhalb der IT verortet sein sollte), dürfte eine umfassende Kontrolle der Verarbeitung personenbezogener Daten schwierig werden;
 - die Umsetzung der technischen und organisatorischen Maßnahmen:³⁹ Hier ist zu prüfen, ob die IT-Sicherheit die Anforderungen des Datenschutzes für das jeweilige Verfahren beachtet und umgesetzt hat;
 - die ordnungsgemäße Beauftragung von Dienstleistern für die Verarbeitung personenbezogener Daten:⁴⁰ Hierzu sind regelmäßig Standardmuster für die Auftragsverarbeitung⁴¹ im Einsatz, die mit Auftragsverarbeitern (Dienstleistern) eingesetzt und entsprechend angepasst werden;
 - internationaler Datentransfer;⁴²
 - Datentransfer außerhalb der EU in ein Land mit/ohne angemessenem Datenschutzniveau und ggf. Erfordernis des Einsatzes von Standardvertragsklauseln;⁴³

36 Siehe Art. 35 DSGVO, vorherige Konsultation der Aufsichtsbehörde, Art. 36 DSGVO.

37 D.h. personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (Art. 9 Abs. 1 DSGVO).

38 Siehe Art. 30 DSGVO.

39 Siehe Art. 24 DSGVO, „Privacy by Design & Default“ gem. Art. 25 DSGVO sowie Sicherheit der Verarbeitung, Art. 32 DSGVO.

40 Siehe Art. 27–29 DSGVO.

41 Siehe <https://www.bitkom.org/sites/default/files/file/import/170515-Auftragsverarbeitung-Anlage-Mustervertrag-online.pdf>; <https://www.gdd.de/service/publikationen-und-aktionen/>; https://www.lda.bayern.de/media/muster_adv.pdf (alle Quellen zuletzt abgerufen am 19.3.2024).

42 Z. B. Berücksichtigung anderer nationaler Gesetzgebungen, Art. 26, 27 DSGVO.

43 Siehe Art. 26 DSGVO, Art. 28 Abs. 8 DSGVO oder Restriktionen bzgl. der Übermittlung von personenbezogenen Daten in Drittstaaten unter Einsatz z. B. der Standardvertragsklauseln – Muster der Standardvertragsklauseln sind abrufbar unter: https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_de (zuletzt abgerufen am 19.3.2024).

- Binding Corporate Rules für die konzernweite Datenverarbeitung:⁴⁴ Mit Einführung von Binding Corporate Rules kann der Datentransfer in einem Konzern durch Regelung einheitlicher Prozesse und Regeln grenzüberschreitend vereinheitlicht und erleichtert werden;
- Berücksichtigung der Mitwirkungsrechte des Betriebsrats:⁴⁵ Bei bestimmten Datenverarbeitungsverfahren insbesondere betreffend Regelungen bzgl. der Mitarbeiter besteht regelmäßig ein Mitspracherecht des Betriebsrats.
- Bei Datenschutzinformationen und Einwilligungen:
 - Datenschutzhinweise auf Webseiten;⁴⁶
 - Einverständnis und Einwilligung der Betroffenen u.a. für Marketingzwecke.⁴⁷
- Bei organisationsinternen Maßnahmen und Regelungen:
 - Übermittlung personenbezogener Daten im Konzern;
 - Regelungen zum konzerninternen Datentransfer;
 - Betriebsvereinbarungen (z. B. zur Internet- und E-Mail-Nutzung).

Reaktive datenschutzrechtliche Beratung umfasst u. a.:

81

- Ausübung von Betroffenenrechten (Betroffene, deren personenbezogene Daten von der verantwortlichen Stelle erhoben und/oder verarbeitet werden können, um verschiedene Rechte gegenüber der verantwortlichen Stelle geltend zu machen)⁴⁸ hinsichtlich:
 - Auskunftsrecht über gespeicherte personenbezogene Daten,⁴⁹
 - Berichtigungs-, Löschungs- und Sperrungsansprüche,⁵⁰
 - Recht auf Datenübertragbarkeit;⁵¹
 - Informationspflichten bei Datenpannen:⁵² Je nach Einzelfall sind die Betroffenen, die Aufsichtsbehörde und/oder die Öffentlichkeit zu informieren;
 - (anlasslose) aufsichtliche Kontrolle;⁵³
 - E-Discovery-Anforderungen z.B. der internen Revision versus datenschutzrechtlicher Rechte der Betroffenen;

44 Siehe Art. 47 DSGVO, im BDSG bisher nicht geregelt, aber von der Artikel-29-Datenschutzgruppe in diversen Arbeitspapieren geregelt.

45 Siehe §§ 79, 87 Nr. 6, 90 BetrVG.

46 Siehe § 13 Abs. 1 TMG.

47 Siehe § 13 Abs. 2 TMG, § 7 Abs. 2 Nr. 2 und 3 UWG, § 94 TKG; Art. 6–8 DSGVO, insb. Art. 6 Abs. 1 lit. a sowie Art. 20 Abs. 2 lit. a, Art. 22 Abs. 2 lit. c DSGVO.

48 Siehe Art. 12–20 DSGVO.

49 Siehe Art. 15 DSGVO.

50 Siehe Art. 16–19 DSGVO, inkl. „Recht auf Vergessenwerden“, Art. 17 DSGVO.

51 Siehe Art. 20 DSGVO.

52 Siehe Art. 34 DSGVO.

53 Siehe Art. 57 Abs. 1 und hier insb. lit. a DSGVO.

- rechtssichere Datenanalyse im Zuge der Prüfung der Wirksamkeit interner Kontrollsysteme oder Ermittlung bei möglichem unrechtmäßigem Handeln durch Mitarbeiter (Beweiserhebung und Beweisverwertbarkeit);
- Datenschutz Audits (intern).

a) Der betriebliche Datenschutzbeauftragte

- 82** Die Bestellung und der Tätigkeitsbereich eines DSB sind inzwischen EU-weit in der DSGVO geregelt und werden zudem durch das BDSG ergänzt.⁵⁴ Der zunehmende Automatisierungsgrad sowie die Erfassung von immer mehr Unternehmens- und Lebensbereichen durch die Datenerfassung (Bsp.: Internet der Dinge; Videoüberwachung in öffentlichen Räumen) lassen immer weniger Raum für Bereiche ohne Datenerfassung und Mitarbeiter haben oft keinen geschulten Blick dafür, welche Möglichkeit aus der Kombination und algorithmischen Auswertung von unscheinbaren, vordergründig anonymen Nutzerdaten im Hintergrund durch das intelligente Zusammenführen solcher Daten im Bereich der Profilbildung oder sonstigen Datenanalyseverfahren mit Personenbezug erwachsen.
- 83** Auch sonst unterstützt die (freiwillige) Bestellung eines DSB unternehmerische Prozesse, weil Unternehmen mit dediziertem DSB datenschutzrelevante Aufgaben durch die eindeutige Aufgabenzuweisung fokussiert angehen können. Ohnehin kann unter Berücksichtigung der aktuellen technologischen und wirtschaftlichen Entwicklung stets zu einer Bestellung eines DSB geraten werden, denn die Datenverarbeitung in sämtlichen Wirtschaftsbereichen hat inzwischen einen Umfang erreicht, der es kaum möglich erscheinen lässt, dass ein Management oder die weiteren verantwortlichen Bereiche die datenschutzrechtliche Tragweite von Maßnahmen richtig erfassen können, sobald personenbezogene Daten erhoben werden oder aber Meta- oder Telemetriedaten zur Nutzung bestimmter Produkte erfasst werden sollen (z. B. bei Smart-TVs, vernetzten Elektrogeräten inkl. moderner Waschmaschinen oder sog. Smart-Home-Lösungen sowie den stetig wachsenden Bereich von künstlicher Intelligenz, wie z. B. der Einsatz von sog. Large Language Modellen und konkret ChatGPT).
- 84** Vor dem Hintergrund eines zunehmenden Compliance-Bewusstseins in Unternehmen sind immer weniger Umstände denkbar, in denen ein verantwortlich handelndes Management einen DSB nicht anhört oder aber gebotene und vorgeschlagene Maßnahmen nicht umsetzt.
- 85** Die Stellung des DSB innerhalb der Organisationsstruktur eines Unternehmens ist vom Gesetzgeber hoch angesiedelt worden. Mit der – zumindest fachlich – direkten Berichtspflicht an die höchste Managementebene des Unternehmens

⁵⁴ Siehe Art. 39 DSGVO sowie § 38 BDSG.

(Verantwortliche Stelle oder Auftragsverarbeiter),⁵⁵ hat der DSB jederzeit die Möglichkeit, sich bei der Geschäftsführung Gehör zu verschaffen. Dies ist auch sinnvoll, sollte allerdings stets mit Bedacht ausgeübt werden. Denn bei der Vielzahl der (operativen) datenschutzrechtlichen Aufgaben sollte die Einbindung der Unternehmensführung in operative datenschutzrechtliche Fragestellungen nicht überstrapaziert werden. Je nach Größe eines Unternehmens sollte die Geschäftsführung nur zur Klärung strategischer oder bedeutender operativer Fragestellungen direkt einbezogen werden. Der Schwerpunkt der datenschutzberatenden Tätigkeit wird stets im operativen Bereich liegen und daher idealerweise mit den Fachabteilungen geklärt werden können. In erster Linie sind daher die datenschutzrechtliche Unternehmenskultur sowie strategische Ziele mit der Geschäftsführung abzustimmen.

Grundsätzlich ist der DSB den operativen Geschäftsbereichen zuzuordnen. Die Beratung durch den DSB hat zwar unmittelbaren Einfluss auf die technische Ausgestaltung von Verfahren zur Verarbeitung personenbezogener Daten, allerdings ist die Gestaltung der erforderlichen (Geschäfts-)Prozesse Aufgabe der anfordernden operativen Bereiche, d. h., das „Was“ und „Wozu“ wird durch die operativen Bereiche und den DSB bestimmt. Die Umsetzung im IT-Bereich, d. h., das technische „Wie“ wird durch die IT selbst bzw. die IT-Sicherheit gemäß den operativen und datenschutzrechtlichen Vorgaben definiert und anhand des jeweils anzuwendenden aktuellen Standes der Technik ermittelt. Bindeglied zwischen dem Datenschutz und der IT-Sicherheit sind hier die technischen und organisatorischen Maßnahmen, die abhängig vom Umfang und der Intensität der Verarbeitung personenbezogener Daten bestimmen, welche grundlegenden Aspekte bei der Umsetzung von operativen Anforderungen durch die IT beachtet werden müssen. Aber gerade in diesem Bereich der Bestimmung der datenschutzrechtlichen Bedeutung bei operativen Maßnahmen und deren Einfluss auf die Ausgestaltung von Datenverarbeitungsprozessen ist dem DSB eine starke Stellung einzuräumen, denn die Beachtung gerade der technischen und organisatorischen Maßnahmen führt häufig zu erheblichen Mehraufwänden und erweiterten Dokumentationspflichten, die auch den Zeitrahmen für die Realisierung neuer Datenverfahrungsverfahren erheblich beeinflussen können. Dabei ist seit Geltung der DSGVO insbesondere den Anforderungen des „Datenschutz durch Technikgestaltung“ („Privacy by Design“)⁵⁶ und „Datenschutz durch datenschutzfreundliche Voreinstellungen“ („Privacy by Default“)⁵⁷ Rechnung zu tragen. Die Beachtung und Umsetzung dieser Anforderungen an Datenverarbei-

86

⁵⁵ Siehe Art. 38 Abs. 3 Satz 3 DSGVO.

⁵⁶ Siehe Art. 25 Abs. 1 DSGVO.

⁵⁷ Siehe Art. 25 Abs. 2 DSGVO.

tungsverfahren ist nicht banal: Gerade bei Individuallösungen muss bei der Umsetzung/Gestaltung von Softwarelösungen der Datenschutz als sog. nicht-funktionale Anforderungen berücksichtigt werden. Gerade in agilen Projekten bedeutet dies aber, dass der Datenschutzbeauftragte bei jeder Weichenstellung bzgl. der Verarbeitung personenbezogener Daten beratend hinzuzuziehen ist, um die Gestaltung des Verfahrens daran ausrichten zu können.⁵⁸ Deshalb sollte sich ein DSB stets seiner Rolle und Verantwortung im Unternehmen bewusst sein, aber auch eine über die rein gesetzliche Stellung hinausgehende Funktion innehaben, die es ihm ermöglicht, datenschutzrechtlich gebotene Maßnahmen effektiv umzusetzen oder zu veranlassen.

b) Prozess der Datenschutzberatung

- 87** Der DSB hat auf die Einhaltung der datenschutzrechtlichen Vorschriften hinzuwirken,⁵⁹ indem er die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, überwacht,⁶⁰ was ggf. auch durch eine Datenschutz-Folgenabschätzung⁶¹ sicherzustellen ist, sowie diese zu dokumentieren.⁶² Zudem besteht die Pflicht zur Schulung von Mitarbeitern, die bei der Verarbeitung personenbezogener Daten tätig sind⁶³ und die Zusammenarbeit mit der Aufsichtsbehörde.⁶⁴ Diese Pflichten des DSB können als die proaktiven Pflichten wie folgt zusammengefasst werden:

- Schulung;
- Datenschutz-Folgenabschätzung und Beratung bei der Einführung von Datenverungsverfahren (Beratung);
- Dokumentation;
- Überwachung des Betriebs von Datenverungsverfahren (Kontrolle);
- Zusammenarbeit mit Aufsichtsbehörden (Dieses stellt eigentlich keine eigentliche Aufgabe des DSB dar, sondern dient nur zur Klarstellung, dass der DSB die Schnittstelle zwischen Aufsichtsbehörde und der verantwortlichen Stelle/Auftragsverarbeiter ist).

58 Siehe diesbzgl. Checklisten zur Ausgestaltung: <https://www.ihk.de/bayreuth/hauptnavigation/service/recht/datenschutz/privacy-by-design-und-privacy-by-default-4399912/>; <https://www.datenschutzberater365.de/wp-content/uploads/2017/02/Checkliste-Privacy-by-Default.pdf>; Privacy by Design umsetzen: Datenschutz als Standardeinstellung – computerwoche.de (zuletzt abgerufen am 10.3.2024).

59 Siehe Art. 39 Abs. 1 lit. a DSGVO.

60 Siehe Art. 39 Abs. 1 lit. b DSGVO.

61 Siehe Art. 39 Abs. 1 lit. c i. V. m. Art. 35 DSGVO.

62 Siehe Art. 30 und auch Art. 25 DSGVO.

63 Siehe Art. 39 Abs. 1 lit. a DSGVO.

64 Siehe Art. 39 Abs. 1 lit. d und e DSGVO.

Damit kann auch zur Darstellung des Reifegrades des Datenschutzes im Unternehmen folgendes Modell zur Veranschaulichung dienen: **88**

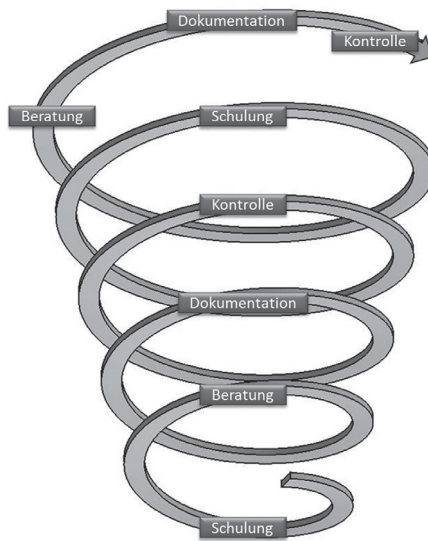


Abbildung 2: Zyklischer Prozess der Pflichten des Datenschutzbeauftragten

Ein weiterer bestimmender Faktor für die konkreten Anforderungen an eine effektive Datenschutzberatung ist der Reifegrad der Datenschutzorganisation. Bestehen schon weitreichende prozessuale Regelungen, wie z.B. Richtlinien⁶⁵ oder ein Datenschutzmanagementsystem im Unternehmen, gestaltet sich die Beratung oftmals leichter, weil (a) formale Prozesse bereits etabliert sind und (b) ein datenschutzrechtliches Bewusstsein in den relevanten Organisationsbereichen besteht. Die datenschutzrechtliche Beratung sollte sich dabei stets an dem gesetzlich vorgeschriebenen Leitbild orientieren, das wie folgt ausgestaltet ist: **89**

⁶⁵ Hilfreich hierfür das BSI-IT-Grundschutzkompendium: https://www.bsi.bund.de/DE/The men/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html, hier: Prozess-Baustein CON.2 „Datenschutz“ (zuletzt abgerufen am 19.3.2024).

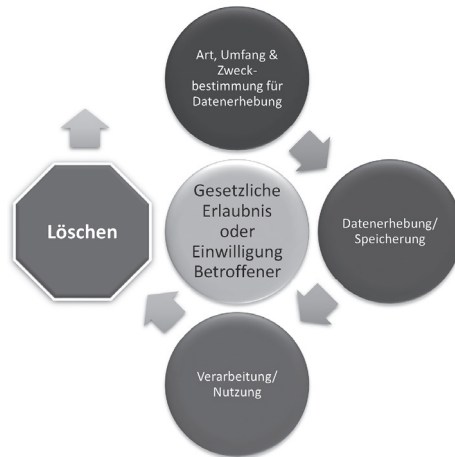


Abbildung 3: Nutzungszyklus personenbezogener Daten

- 90** Entscheidend für eine effektive Datenschutzberatung und Implementierung von Organisationsprozessen zum Datenschutz ist das Verständnis für datenschutzrechtliche Relevanz in den betroffenen Organisationseinheiten (z. B. durch Schulung) sowie die zielführende Beratung und Dokumentation bei der Umsetzung von datenschutzrelevanten Verfahren. Wichtig ist dabei auch, bei der einzelfallbezogenen Beratung frühzeitig Muster zu erkennen, die es ermöglichen, Prozesse oder Standards zu etablieren und in einheitliche Regelungen zu fassen, weil dies hilft, den Tätigkeitsaufwand für wiederkehrende Tätigkeiten zu verringern. Nur so wird es dem DSB langfristig möglich sein, seine Aufgaben effektiv zu erfüllen und zugleich die Möglichkeit zu erhalten, strategisch den Datenschutz weiterzuentwickeln. Auch sollte die Einzelfallberatung und die Rückmeldung von Betroffenen oder Mitarbeitern genutzt werden, die technischen und organisatorischen Maßnahmen und die etablierten Richtlinien zum Datenschutz zu hinterfragen und zu überprüfen sowie ggf. an aktuelle Entwicklungen und neue gesetzliche Vorgaben anzupassen. Die Rückkopplung zwischen strategischem und operativem Datenschutz ist dabei von entscheidender Bedeutung.
- 91** Die in Abschnitt III.2. (→ Rn. 78 ff.) beschriebene proaktive und reaktive Beratung hat folgende Relevanz für die datenschutzrechtliche Beratung: Die reaktive Beratung führt dazu, dass der DSB stets nur Sachverhalte oder Ereignisse („Incident-Management“) abarbeitet. Damit hat der DSB keine Möglichkeit, gestaltend den Datenschutz mitzubestimmen, sondern ist im Wesentlichen auf die Schadensbegrenzung beschränkt. Für eine effektive Compliance im Datenschutz ist es aber entscheidend, dass der DSB Prozesse proaktiv mitgestaltet („Process-Implementation & Management“), anstatt datenschutzrelevante Sachverhalte nur reaktiv abzuarbeiten. Nur so ist es möglich, eine datenschutzrechtskonforme

Verarbeitung personenbezogener Daten dauerhaft rechtssicher gewährleisten zu können bzw. einen hohen Datenschutz-Reifegrad im Unternehmen zu erreichen.

c) Praxisrelevante Beispiele

Anhand einiger Fallbeispiele soll nunmehr dargestellt werden, welchen Reifegrad ein DSB in einem Unternehmen in den dafür relevanten Bereichen vorfinden kann. Dabei ist aber auch zu berücksichtigen, dass die gegenwärtige Entwicklung enorme Herausforderungen beinhaltet. Durch die zunehmende Datenverarbeitung (Big Data, Internet der Dinge usw.) werden bisher etablierte „Datensilos“ aufgebrochen. Daten werden vernetzt und komplexe Analysen ermöglichen Einsichten in persönliche oder personenbezogene Bereiche, die vor kurzer Zeit noch gar nicht denkbar waren. 92

Beispiel 1: Durch Zufall erfährt der DSB von einem Kollegen, dass demnächst für den Online-Shop des Unternehmens Werbung wesentlich kundenspezifischer ausgestaltet werden soll. Durch Einsatz von Cookies⁶⁶ (Textdateien, die bestimmte Nutzungsverhaltensdaten von besuchten Webseiten speichern) und IP-Adressen sollen Kunden auch nach dem Verlassen der Webseiten des Online-Shops auf anderen Webseiten mit zuvor besuchten Produkten aus dem Online-Shop beworben werden. Aufgrund dieser Hinweise erkundigt sich der DSB bei der zuständigen Fachabteilung bzgl. dieses Werbeverfahrens. Der verantwortliche Projektleiter erklärt, dass die Informationen stimmen, er sich aber keine Sorgen machen müsse, weil personenbezogene Daten, wie z. B. Namen, Adressdaten usw., nicht Gegenstand dieses Verfahrens seien, wodurch die Einbeziehung des DSB entbehrlich sei. 93

Hier fehlt es der verantwortlichen Fachabteilung an der Sensibilität bzgl. personenbezogener Daten. Zwar ist inzwischen geklärt, wann auch sog. dynamische IP-Adressen als personenbezogene Daten gelten⁶⁷; die Bewertung hat jedoch gerade deshalb für jeden Einzelfall individuell zu erfolgen. Zudem dürften auch Personen mit statischen IP-Adressen den Online-Shop besuchen. Ferner ist ohne weitere Klärung, was im Zusammenhang mit der IP-Adresse in den Cookie-Dateien gespeichert wird, Personenbezug anzunehmen und damit auch die Anpas- 94

66 Umfassend zu Cookies *Rauer/Ettig*, ZD 2015, 255 ff.; siehe hierzu auch: <https://www.bunddesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020067.html> und „Das Setzen von Cookies erfordert die aktive Einwilligung des Internetnutzers“ siehe <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190125de.pdf> (zuletzt abgerufen am 19.3.2024).

67 Siehe EuGH, Urt. v. 19.10.2016 – C-582/14, <https://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=DE> – Dynamische IP-Adressen haben relativen Personenbezug, d. h. eine dynamische IP-Adresse kann für den Anbieter von Online-Mediendiensten ein personenbezogenes Datum darstellen, an deren Speicherung ein berechtigtes Interesse besteht (zuletzt abgerufen am 19.3.2024).

sung von Datenschutzinformationen für die Webseite erforderlich werden. Um ein Einwilligungserfordernis bewerten zu können, wären weitere Sachverhaltsaufklärungen durchzuführen.

95

Beispiel 2: Der Automobilhersteller X-AG stellt Premium Pkw her. Darin enthalten ist u. a. eine fortschrittliche Notruffunktion („eCall-System“),⁶⁸ die es im Falle eines Unfalls ermöglicht, Rettungsmaßnahmen automatisiert einzuleiten. Über diese Notrufschnittstelle kann man auch Zusatzdienste, wie z. B. Verkehrsmeldungen in Echtzeit für das Navigationssystem abrufen, um stets die verkehrsgünstigste Route bestimmen zu können. Um diese Zusatzfunktion für die ersten 24 Monate ohne Zusatzkosten nutzen zu können, muss der Fahrzeugkäufer der Datenübermittlung zum eigenen Fahrverhalten an den Fahrzeughersteller zustimmen, weil hierdurch die Genauigkeit der Verkehrsdaten verbessert und die Entwicklung neuer Fahrzeuge anhand von Fahrverhaltensdaten der Käufer optimiert werden kann. Der serviceorientierte Verkäufer stellt dem privaten Käufer das Fahrzeug zur Abholung bereit und teilt diesem mit, dass er bereits alles im System eingerichtet habe, damit der Käufer Fahrspaß ab der ersten Minute hat. Der Käufer freut sich insbesondere über das angesprochene technisch bisher unerreichte Notrufsystem und das Navigationssystem mit Verkehrsführung unter Berücksichtigung von Echtzeitdaten. Nach Erläuterung der Funktionen fährt der Käufer voller Freude davon.

96

In diesem Fallbeispiel ist zumindest problematisch, dass der serviceorientierte Mitarbeiter die erforderlichen Einstellungen bereits vorgenommen hat. Für die Erhebung und Übermittlung dieser Daten besteht kein gesetzlicher Erlaubnistatbestand. Gemäß Art. 6 Abs. 1 lit. a DSGVO hätte der Käufer daher in die Übermittlung seiner Fahrdaten einwilligen müssen, denn diese Daten ermöglichen die Geo-Lokalisierung des Käufers durch die Übermittlung der Daten über eine Mobilfunkverbindung mit individualisierter IMEI-Nummer. Diese Daten können z. B. auch (theoretisch) herangezogen werden, um Fehlverhalten des Käufers (Fahrers) zu ermitteln; Personenbezug gemäß Art. 4 Ziff. 1 DSGVO läge zweifellos vor. Eine gesetzliche Pflicht zur Übermittlung der weitreichenden Fahrdaten besteht (gegenwärtig) nicht. Zudem wäre hier noch zu erörtern, ob nicht die Einwilligungserklärung nebst transparenter Erläuterung der Datenverarbeitung nicht auch schriftlich hätte erfolgen müssen, denn eine so weitreichende Datenverarbeitung lediglich über das Multimedia-System des Fahrzeugs darzustellen und bestätigen zu lassen, dürfte dem Käufer kaum die Möglichkeit bieten, die näheren Einzelheiten der Datenübermittlung in angemessener Form wahrzunehmen. Hier hätte wahrscheinlich die Einwilligung schriftlich oder sonst dokumentiert erfolgen müssen, um dem Kunden die Möglichkeit einer freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich

68 Zu den technischen Möglichkeiten und rechtlichen Implikationen: *Balzer/Nugel*, NJW 2016, 193 ff.; *Lüdemann*, ZD 2015, 247 ff.

abgegebene Willensbekundung in Form einer Erklärung zu ermöglichen.⁶⁹ Es ist zweifelhaft, ob eine Einwilligung bei Nutzung eines Multi-Media-Systems (kleiner Bildschirm) wirksam sein kann, da die Einwilligungserklärung inklusive der dazugehörigen Informationen kaum adäquat lesbar sein dürften. Eine konkludente Einwilligung bestehend aus der kostenlosen Nutzung des Echtzeit-Navigationssystems gegen Einwilligung in die Datenübermittlung an den Automobilhersteller dürfte dagegen nicht anzunehmen sein, weil dies u. a. dem Grundsatz der Transparenz widerspräche.⁷⁰

Die vorgenannten Beispiele zeigen, dass die Themen eines DSB komplexer werden. Längst geht es nicht mehr darum, dass Mitarbeiter eines Unternehmens überhaupt nicht verstehen, worum es beim Datenschutz geht. Auch dürften heute kaum noch Unternehmensführungen anzutreffen sein, die das Thema Datenschutz ignorieren oder für irrelevant erachten. Die vielfältigen Möglichkeiten der Datenerhebung, Datenanalyse und Datenverarbeitung erfordern eine neue Qualität des Datenschutzes. Es geht nicht mehr allein um das Führen von Verfahrensverzeichnis für standardisierte Datenverarbeitungsverfahren oder singuläre Schulungen über den Datenschutz im Allgemeinen. Die aktuellen Entwicklungen im Bereich der Big-Data-Analytics, CRM und Internet der Dinge erfordern das Erfassen komplexer Vorgänge, die Bewertung der jeweiligen Datenschutzrelevanz auf Grundlage genauer Verfahrensanalysen und Voranalysen (ggf. mit Datenschutz-Folgeabschätzung) sowie die rechtssichere Ausgestaltung von interaktiven Datenverarbeitungsverfahren, die insbesondere die Interaktion verschiedener Datenverarbeitungssysteme unter Einbeziehung verschiedenster Daten/Datenbanken und Datenkategorien beinhaltet. **97**

Auch im Hinblick auf die Einbindung von künstlicher Intelligenz in Unternehmenslösungen ist stets zu prüfen, inwieweit personenbezogene Daten aus welchen Quellen (öffentlich zugängliche Trainingsdaten o. Ä.) eingesetzt werden, um die KI hinsichtlich ihrer Entwicklungshöhe gezielt zu trainieren und fortzuentwickeln. Ferner dürfte auch der Data Act (EU Datengesetz) datenschutzrechtlichen Einfluss haben, denn es muss stets abgewogen werden, wie detailliert Maschinen- oder Produktdaten, die beim Betrieb dieser gespeichert werden, ein so genaues Profil des Nutzers zeichnen, dass hierdurch ein Personenbezug möglich wird. **98**

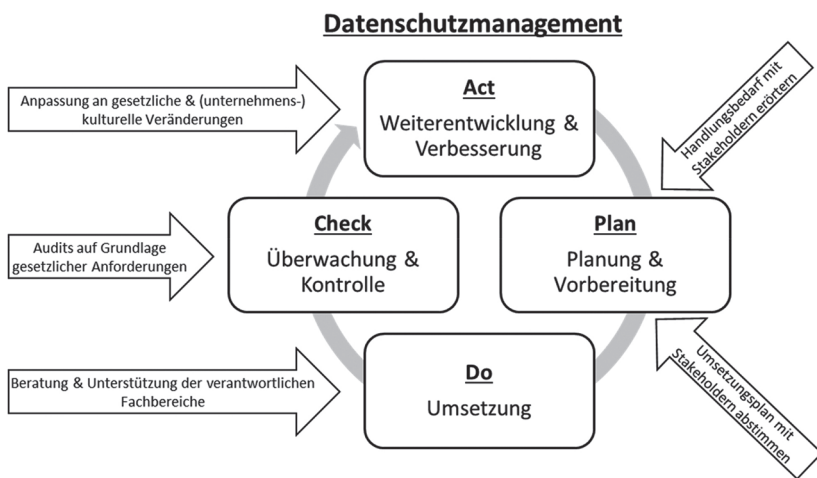
3. Implementierung

Die Implementierung eines effektiven Datenschutzmanagementsystems erfolgt in Stufen. Zunächst sind Prozesse zur Datenschutzberatung zu implementieren (siehe → Rn. 78 ff.). Erst hiernach sollten die datenschutzrechtlich relevanten Regelungen in einem Unternehmen überarbeitet, ergänzt oder sukzessive implementiert werden. Für die Einführung bestimmter Unternehmensregeln ist eine **99**

69 *Schwartmann/Klein*, in: *Schwartmann/Jaspers/Thüsing/Kugelman*, DS-GVO/BDSG, 1. Aufl. 2018, Art. 6 Rn. 12 ff. und Rn. 21.

70 *Schwartmann/Klein*, in: *Schwartmann/Jaspers/Thüsing/Kugelman*, DS-GVO/BDSG, 1. Aufl. 2018, Art. 6 Rn. 22 ff.

Grundstruktur erforderlich, damit die eingeführten Regelungen tragfähig im Unternehmen umgesetzt und beachtet werden können sowie nicht als Fremdkörper innerhalb der Unternehmensorganisation wirkungslos bleiben. Auch für die Entwicklung des Datenschutzmanagementsystems innerhalb eines Unternehmens ist ein Phasenmodell von Vorteil.



- 100** Mit diesem Modell kann das Datenschutzmanagementsystem schrittweise entwickelt und angepasst werden. Sämtliche Maßnahmen des DSB sollten stets aufeinander abgestimmt sein, denn es ist wenig hilfreich, Maßnahmen einzusteuern, die keine Verbindung zu anderen relevanten Bereichen haben oder aber eine Rückkopplung auf bestehende Maßnahmen nicht zulassen.
- 101** Dabei ist das Datenschutzniveau innerhalb des Unternehmens zu berücksichtigen: Ohne Sensibilisierungsmaßnahmen (Schulungen), die wirklich greifen, werden Mitarbeiter datenschutzrechtlich relevante Verfahren oder das Erfordernis der Hinzuziehung des DSB weder erkennen, noch proaktiv mit dem DSB abstimmen.⁷¹ Die Dokumentation von datenschutzrechtlich relevanten Verfahren ist dagegen arbeitsintensiv und gerade bei sich dynamisch entwickelnden Verfahren ein laufender Prozess. Damit dürfte eine dauerhafte Einbindung des DSB bei einem effektiv implementierten Datenschutzmanagementsystem in datenschutzrelevante Projekte unentbehrlich sein, um fortgesetzt in Entwicklungszyklen involviert zu sein und sein Fachwissen einbringen zu können.
- 102** Zu einem Datenschutzmanagementsystem gehören auch die Entwicklung und Implementierung von Richtlinien für die operativen Fachbereiche sowie ein technisches Datenschutzumsetzungskonzept für den IT-Bereich. Die Abstim-

⁷¹ Siehe auch Neundorff, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 29 Rn. 56 f.

mung dieser Richtlinien sowie die regelmäßige Überprüfung anhand operativer, technischer, gesetzlicher und datenschutzkultureller Weiterentwicklungen sind dabei fortwährend zu beachten. Der Anpassungsbedarf wird durch (Selbst-)Audits und direkte Kontrollmaßnahmen des DSB ermittelt.

Oftmals stellt sich in Unternehmen die Frage, in welchem Umfang oder mit welcher Intensität der Datenschutz umgesetzt werden soll. Die Unternehmensleitung erkennt häufig den Mehrwert eines effektiven Datenschutzmanagements und gestattet nur so wenige Eingriffe wie zwingend nötig in operative Prozesse. Natürlich kann damit nur das Mindestmaß an Datenschutz umgesetzt werden. Gerade in Unternehmen mit Privatkundengeschäft (Endkunden/Verbraucher) kann das Vertrauen der Kunden in einen professionellen und gut organisierten Umgang mit ihren personenbezogenen Daten ganz erheblich zum Erfolg des Unternehmens beitragen.⁷² Daher ist die Frage nach der richtigen Datenschutzstrategie sehr wichtig – aber auch einzelfallbezogen. Folgende strategische Herangehensweisen können unterschieden werden:

103

- Umsetzung der gesetzlichen Mindestanforderungen: Nur die datenschutzrechtlich zwingenden Anforderungen werden umgesetzt. Jede Einbindung des DSB wird dahingehend bewertet, inwieweit zusätzliche Maßnahmen Auswirkungen auf das Projekt haben könnten und wird stets auf das zwingende Mindestmaß begrenzt, um die operative Gestaltung und Implementierung durch den Datenschutz möglichst unbeeinflusst zu lassen. Die jeweils gegenwärtige datenschutzrechtliche Compliance wird damit erreicht, mehr aber auch nicht.
- Umsetzung eines nachhaltigen Datenschutzes: Immer mehr Unternehmen erkennen, dass eine strukturierte Implementierung des Datenschutzes Einfluss auf die Nachhaltigkeit beim Datenschutzmanagement haben kann und sich damit langfristig Kosten sparen lassen, indem Strukturen geschaffen werden, die eine integrierte Umsetzung von Datenschutzmaßnahmen ermöglichen. Unterstützt werden diese Maßnahmen nicht nur durch die Implementierung von Richtlinien zum Datenschutz, sondern auch durch z. B. Binding Corporate Rules (**BCR**) für internationale Konzerne oder aber äquivalente Regelungen für Unternehmen, die die Implementierung von BCR nicht benötigen oder denen die administrativen Aufwände als nicht passend für die Unternehmensstruktur erscheinen. Unternehmen, die ein effektives Datenschutzmanagementsystem implementieren, wollen auf die Entwicklung im Datenschutzbereich vorbereitet sein. Behörden- und Betroffenenanfragen sollen effektiv und zeitnah beantwortet werden können. Dies fördert das Vertrauen der Betroffenen in das professionelle Datenschutzmanagement eines Unternehmens. Zudem sollen Informationspflichten, Kontrollen durch Aufsichtsbehörden und insbesondere auch unternehmensinterne Untersuchungen rechtssicher und effizient durchgeführt werden, um beweisrelevante Befunde auch

⁷² Siehe *Conroy/Milano/Narula/Singhal*, Building customer trust, abrufbar unter: https://www2.deloitte.com/content/dam/insights/us/articles/consumer-data-privacy-strategies/DUP_970-Building-consumer-trust_MASTER.pdf (zuletzt abgerufen am 19.3.2024).

rechtssicher verwerten zu können. Mit einer solchen Strategie ist ein Unternehmen auf die Entwicklung des Datenschutzes vorbereitet und kann reaktive Datenschutzmaßnahmen effizient und rechtssicher ausführen.

- Umsetzung eines marketingorientierten Datenschutzes: Die Umsetzung eines marketingorientierten Datenschutzes erfordert die Implementierung eines effektiven Datenschutzmanagementsystems. Hinzu kommt ein regelmäßiger Austausch mit den datenschutzrelevanten Fachbereichen. Die Organisation des Datenschutzes muss neben den Anforderungen eines nachhaltigen Datenschutzes auch noch die Bereiche der Unternehmenskommunikation und das Marketing einbeziehen. Mit Einbeziehung auch dieser Bereiche können die umgesetzten Datenschutzmaßnahmen und Prozesse aktiv dazu genutzt werden, um das Kundenvertrauen zum Unternehmen zu steigern und die Professionalität und Offenheit (Transparenz!) des Unternehmens im Umgang mit personenbezogenen Daten darzustellen. Diese offene Kommunikation eines „transparenten“ Datenschutzes kann dann Kundenloyalität fördern und somit einen Mehrwert für das Unternehmen bieten.

- 104** Die o.g. Implementierungsstrategien zeigen, wie Unternehmen das Datenschutzmanagement individuell auf ihre Bedürfnisse und strategischen Ziele ausrichten können.

4. Zusammenarbeit mit Behörden

- 105** Für den DSB ist die Zusammenarbeit mit der Datenschutzaufsicht verpflichtend geregelt⁷³ und eine proaktive und offene Zusammenarbeit mit dieser kann zudem sehr hilfreich sein, denn der DSB kann u. a. auch die Beratung der Aufsichtsbehörde in Anspruch nehmen. Diese Hilfe kann gerade in Zweifelsfällen und bei der Datenschutz-Folgenabschätzung (s. Art. 36 DSGVO) nicht nur geboten, sondern auch sehr nützlich sein, um die Planung und Einführung von neuen Verfahren frühzeitig rechtssicher zu gestalten. Bei Beschwerden von Betroffenen gegenüber der zuständigen Behörde kann ein derart vorab mit der Aufsichtsbehörde abgestimmtes Verfahren oftmals unbeanstandet bestehen bleiben und einer solchen Betroffenen-Beschwerde mit einer Erklärung zur Rechtmäßigkeit des Verfahrens abgeholfen werden. Beschwerden Betroffener gegenüber der Aufsichtsbehörde können diese ebenfalls leichter klären, wenn der DSB bereits zuvor mit der Datenschutzaufsicht zusammengearbeitet hat, weil hierdurch leichter abgeschätzt werden kann, ob ein datenschutzrechtliches Problem bei der verantwortlichen Stelle wahrscheinlich ist oder ob die Sorge des Betroffenen anhand von Auskünften zum Verfahren oder der Datenverarbeitung zielführend erläutert werden können.
- 106** Eine weitere Möglichkeit der Zusammenarbeit mit der Datenschutzaufsicht, die nicht unterschätzt werden sollte, bieten sich gemäß Art. 33 und Art. 34 DSGVO an, welche häufig sogar eine Pflicht zur Information oder zur Zusammenarbeit mit der Aufsichtsbehörde begründet. Obwohl hiernach schon bestimmte perso-

73 Siehe Art. 39 Abs. 1 lit. d und e DSGVO.

nenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, kann eine unverzügliche Einschaltung der Datenschutzaufsicht dazu beitragen, die richtigen Maßnahmen einzuleiten und Beschwerden Betroffener, die an die Datenschutzaufsicht gerichtet werden, können effektiver beantwortet werden. In solchen Fällen ist es ratsam, alle zur Verfügung stehenden Maßnahmen zu ergreifen, um das Vertrauen Betroffener – die häufig Kunden der verantwortlichen Stelle sind⁷⁴ – in das Unternehmen aufrechtzuerhalten. Es muss dabei auch berücksichtigt werden, dass in einem hochkomplexen Wirtschaftsumfeld die absolute Sicherheit von Daten insbesondere auch durch die zunehmende Professionalisierung von Cyberkriminellen nicht immer sichergestellt werden kann. Umso mehr ist es daher erforderlich, auch auf Datenangriffe und Datendiebstähle professionell zu reagieren. Die enge Abstimmung und effektive Zusammenarbeit mit der Datenschutzaufsicht unterstützen sowohl die Bearbeitung aktueller als auch die Abwehr zukünftiger Cyberattacken und können so Kundenvertrauen bewahren helfen.

IV. Instrumente der datenschutzrechtlichen Compliance

1. Tone from the Top

Das Thema Datenschutz hat mit Inkrafttreten der DSGVO eine sehr große Bedeutung in den Unternehmen gewonnen, da die Bußgelder im Fall der *Non-Compliance* zum Teil drastisch verschärft wurden. Wichtig ist daher, dass sich Unternehmen datenschutzkonform verhalten. Dies gelingt nur, wenn alle Bereiche eines Unternehmens mitwirken – nicht nur der Beauftragte für den Datenschutz. Gerade in den Bereichen Vertrieb, Marketing und Entwicklung bestehen leider häufig Defizite in Bezug auf *Datenschutz-Compliance*. Eine gute Unternehmensführung wirbt daher für die Einhaltung der datenschutzrechtlichen Vorschriften von höchster Ebene – siehe hierzu auch unten „Interne Kommunikation und Awareness“ unter → Rn. 121. Es ist momentan üblich und weit verbreitet, dass Unternehmen sich in ihrem Unternehmensgrundsatz oder Code of Conduct zur Einhaltung des Datenschutzes verpflichten und alle Mitarbeiter dazu auffordern. Sofern Unternehmen über Whistleblowing-Systeme verfügen, sollten Datenschutzverletzungen zu den meldefähigen Tatbeständen gehören – allerdings sollte dann auch sichergestellt werden, dass etwaige Beschwerden in angemessener Zeit abgearbeitet werden können, da ab Kenntniserlangung möglicherweise Meldefristen laufen.

107

2. Interne Richtlinien

Richtlinien können helfen, Verhaltensregeln in einem Unternehmen zu definieren. Jedoch sollten Richtlinien nur dort implementiert werden, wo ein ausreichendes Maß an Prozessen und Standardisierung erreicht ist, damit eine Richt-

108

⁷⁴ Siehe <http://www.spiegel.de/netzwelt/gadgets/vtech-spielzeug-daten-von-eltern-und-kinder-erbeutet-a-1065182.html>; <http://www.welt.de/wirtschaft/webwelt/article13314277/Sony-entschuldigt-sich-fuer-Playstation-Datenleck.html> (beide Quellen zuletzt abgerufen am 19.3.2024).

linie auch gelebt werden kann. Zudem sollten Richtlinien eingreifen, wenn eine Vielzahl von Ereignissen oder Sachverhalten unter gleichartige Verhaltensmuster fallen und vereinheitlicht bearbeitet werden sollen. Für allgemeine Verhaltensregeln oder Nutzungsbestimmungen sollte eine Richtlinie schon dann festgelegt werden, wenn hierdurch ein einheitlicher rechtlicher Rahmen für alle Mitarbeiter geschaffen werden kann. Für speziellere Sachverhalte sind Prozesse zu definieren, wenn Sachverhalte häufiger oder regelmäßig auftreten, diese auch zukünftig zu erwarten sind und eine klare Festlegung von Prozessen dazu beitragen kann, diese Sachverhalte zukünftig standardisiert und professionell abarbeiten zu können. Haben diese Sachverhalte für eine Vielzahl von Mitarbeitern Relevanz (Adressatenkreis), dann sind bereichsspezifische Richtlinien festzulegen. Sobald eine Schwelle überschritten ist, ab der die zu regelnden Sachverhalte die Mehrheit der Mitarbeiter betreffen sollten Richtlinien grundsätzlich für sämtliche Mitarbeiter gelten. Richtlinien müssen dabei klar formuliert werden und die Ziele, den persönlichen und sachlichen Geltungsbereich sowie die rechtlichen oder sonstigen regelungsbedürftigen Grundlagen genau beschreiben.

a) Datenschutzrichtlinie

- 109** Die Datenschutzrichtlinie regelt den betrieblichen Umgang mit personenbezogenen Daten für sämtliche mit der Datenverarbeitung beschäftigten Personen im Unternehmen. Man könnte nun einwenden, dass die Verarbeitung personenbezogener Daten schon im Gesetz hinlänglich bestimmt ist, aber es werden nicht sämtliche Mitarbeiter das Verständnis für die Auslegung der DSGVO, des BDSG sowie weiterer bereichsspezifischer gesetzlicher Regelungen mitbringen. Daher ist es sinnvoll, eine Richtlinie zu etablieren, die in allgemeiner Form beschreibt, wie der einzelne Mitarbeiter mit personenbezogenen Daten umzugehen hat. In einer solchen Richtlinie sollte praxisnah beschrieben werden, was alles personenbezogene Daten sein können, in welchem Umfang personenbezogene Daten genutzt werden dürfen, welche Bereiche zusammenwirken müssen oder wie und wann der DSB zu kontaktieren oder einzubeziehen ist. Zudem sollten die Grundsätze zur Verarbeitung personenbezogener Daten darin geregelt werden und zwar in einer verständlichen und nachvollziehbaren Form.

b) IT-Nutzungsrichtlinie

- 110** Die IT-Nutzungsrichtlinie regelt die Nutzung von datenverarbeitenden Endgeräten. Darin ist zu regeln, welche Endgeräte (z. B. PCs, Laptops, Smartphones) in welcher Form (stationär, mobil) für welche Zwecke (dienstlich/privat) vom jeweiligen Mitarbeiter genutzt werden dürfen. Für diese Richtlinie sind u. a. folgende Punkte zu berücksichtigen:

- Dürfen private Geräte dienstlich genutzt werden?⁷⁵ Hierbei wäre dann zu regeln, wie der Arbeitgeber Zugriff auf dienstliche Daten erhält und was ge-

⁷⁵ Siehe hierzu *Neundorff*, in: Hauschka/Moosmayer/Lösler, *Corporate Compliance*, § 29 Rn. 151 ff.

schieht, wenn der Mitarbeiter das Unternehmen verlässt. Dieser sensible Bereich wäre umfassend organisatorisch zu regeln und in der Richtlinie detailliert zu beschreiben. Ohne eindeutige Regelung mit welchen Befugnissen der Arbeitgeber Zugriff auf dienstliche Daten des privaten Endgeräts erhält und wie diese – u. a. Betriebsgeheimnisse – zum Ende der Mitarbeit ausschließlich beim Arbeitgeber verbleiben, ist zu berücksichtigen.

- Ist Mitarbeitern die private Nutzung dienstlicher Endgeräte gestattet? Dieses Thema wird immer wieder kontrovers diskutiert,⁷⁶ denn wenn die private Nutzung dienstlicher Endgeräte gestattet ist, sollte geregelt sein, in welchem Umfang die private Nutzung gestattet ist und wie der Arbeitgeber auf dienstliche Informationen (z. B. E-Mails, s.u. → Rn. 111) zugreifen darf.
- Ferner sind die Protokollierung und Stichprobenkontrollen der Nutzung von Endgeräten zu regeln, denn der Arbeitgeber wird stets ein Interesse daran haben zu wissen, wie mit seinen Geschäftsdaten umgegangen wird, wie der Arbeitgeber die Kontrolle hierüber behalten kann und erforderlichenfalls Missbrauch sanktionieren kann. Die Protokollierung dürfte auch bei der Möglichkeit von Telearbeit oder Homeoffice relevant sein.

c) E-Mail-Policy

E-Mails sind als das wesentliche Kommunikationsmittel in Unternehmen unentbehrlich. Die Regelung zur Nutzung des dienstlichen E-Mail-Systems ist in vielerlei Hinsicht sinnvoll. Grundsätzlich ist zu regeln, ob das dienstliche E-Mail-Postfach zu privaten Zwecken genutzt werden darf. Diese Entscheidung hat weitreichende Auswirkungen auf Zugriffsmöglichkeiten auf die E-Mails von Mitarbeitern. Bei einer Duldung oder aktiven Gestattung der privaten Nutzung des dienstlichen E-Mail-Postfachs muss der Arbeitgeber klären, wie er geschäftliche E-Mails als Geschäftsbriefe (§ 35a Abs. 1 GmbHG) im gesetzlich erforderlichen Umfang (z. B. § 147 Abs. 1 Nr. 2 AO) aufbewahrt und private E-Mails hiervon ausnimmt, denn Letztere darf der Arbeitgeber weder archivieren noch einsehen. Auch der Zugriff auf das dienstliche E-Mail-Postfach z. B. bei internen Untersuchungen wird bei Gestattung privater Nutzung erheblich erschwert. Die Rechtsprechung⁷⁷ und die Literatur⁷⁸ sind hierzu bisher noch zu keinem klaren

111

⁷⁶ Vgl. <https://www.bitkom.org/sites/main/files/file/import/130304-LF-BYOD.pdf> (zuletzt abgerufen am 19.3.2024); *Franck*, RDV 2013, 185 ff.; *Brink*, ZD 2015, 295 ff.

⁷⁷ Die Anbietereigenschaft des Arbeitgebers gemäß § 2 Abs. 2 Nr. 1 und § 3 Abs. 2 TTDSG (seit 13.5.2024 inhaltsgleich im TDDDg aufgenommen) und Zugriffsrecht des Arbeitgebers auf dienstliche E-Mails trotz privater Nutzungsmöglichkeit des dienstlichen E-Mail-Postfachs gemäß §§ 32, 28 BDSG bejahend: LAG Berlin-Brandenburg, Urt. v. 16.2.2011 – 4 Sa 2132/10; LAG Niedersachsen, Urt. v. 31.5.2010 – 12 Sa 875/09; VGH Baden-Württemberg, Urt. v. 30.7.2014, 1 S 1352/13. – Gemäß EGMR – Rs. Barbulescu gegen Rumänien (61496/08) – verletzt die Kündigung nicht das Menschenrecht auf Achtung des Privat- und Familienlebens gemäß Art. 8 Abs. 1 der Europäischen Menschenrechtskonvention (EMRK); siehe insofern auch LG Erfurt vom 28.4.2021 – 1 HK O 43/20.

⁷⁸ Überblick: *Behling*, CB 2013, 265 ff.; BVerfG, Beschl. v. 16.6.2009 – 2 BvR 902/06.

Ergebnis gekommen, weshalb eine klare betriebliche Regelung zu mehr Rechtssicherheit beitragen kann.

d) Social-Media und Messaging-Dienste

- 112** Immer häufiger werden auch Messaging-Dienste zu dienstlichen Zwecken eingesetzt. Oftmals erfolgt dies aufgrund der großen Beliebtheit/Verbreitung sowie des häufig nicht klar abgegrenzten Bereichs zwischen privater und dienstlicher Nutzung insbesondere auf Mobilfunkgeräten (Smartphone). Grundsätzlich gelten für Messaging-Dienste (Skype, WhatsApp, usw.) die gleichen Anforderungen, wie für E-Mail-Dienste. Allerdings dürfte die an sich erforderliche Archivierung von geschäftlicher Kommunikation über diese Dienste eher selten Beachtung finden (§ 35a GmbHG). Daher sollten auch bezüglich dieser Dienste Regelungen zum Einsatz im geschäftlichen Umfeld bestehen, um zu verhindern, dass erhebliche Geschäftskommunikation in diesem schwer überschaubaren Bereich erfolgt oder gar sensible Daten hierüber ausgetauscht werden.
- 113** Gleiches gilt auch für Postings in sozialen Medien. Denn gerade hier ist es insbesondere im IT-Umfeld üblich geworden, Profile mit Projekten, an denen Mitarbeiter mitgewirkt haben, anzureichern, wodurch sehr viele Informationen über das Unternehmen in möglicherweise ungefilterter aber auch kritischer Form publiziert werden können, was sich schädigend auf das Unternehmen und andere beteiligte Mitarbeiter auswirken kann. Daher sind Unternehmen auch hier gut beraten, ihren Mitarbeitern klare Dos & Don'ts mitzuteilen, damit keine unbedarften Postings zum Schaden der betroffenen Mitarbeiter selbst, von Kollegen oder dem Unternehmen online gestellt werden.

**e) IT-Datenschutzmanagement-Richtlinie
(Datenschutzmanagementkonzept)**

- 114** Die IT-Datenschutzmanagement-Richtlinie richtet sich in erster Linie an IT-Mitarbeiter. Diese Richtlinie regelt den Umgang mit personenbezogenen Daten im IT-Umfeld. Hier sind u. a. Grundsätze zur Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO zu spezifizieren. Weitere wichtige Punkte einer solchen Richtlinie sind z. B.:
- Regelung der Datenschutzverantwortlichkeiten innerhalb der IT;
 - Prüfung rechtlicher Rahmenbedingungen und Datenschutz-Folgenabschätzung;
 - Verfahren zur Sicherstellung der Rechte der Betroffenen (hier insb.: Bearbeitung von Auskunfts- und Löschersuchen von Betroffenen oder auch das Recht auf Datenübertragbarkeit⁷⁹);
 - Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten;
 - Datenschutzrechtliche Freigabeprozesse;
 - Meldung und Regelung von Abrufverfahren;

⁷⁹ Siehe Art. 20 DSGVO.

- Regelung der Auftragsverarbeitung (bei rechtlicher Selbstständigkeit z.B. der Konzern-IT auch die Auftragsverarbeitung für die Konzerngesellschaften);
- Regelung zur Verknüpfung und Verwendung von personenbezogenen Daten;
- Dokumentation der datenschutzrechtlichen Zulässigkeit;
- Aufrechterhaltung des Datenschutzes im laufenden Betrieb;
- Datenschutzaspekte bei der Protokollierung;
- Datenschutzgerechte Löschung/Vernichtung;
- Umsetzung der „Datenschutz durch Technikgestaltung“ („Privacy by Design“) und „Datenschutz durch datenschutzfreundliche Voreinstellungen“ („Privacy by Default“);
- Insbesondere im Zuge des Einsatzes von KI-Lösungen sind auch Regelungen zu automatisierten Entscheidungen vorzusehen (Art. 22 DSGVO);
- Mitwirkung bei der Zusammenarbeit mit Aufsichtsbehörden.

Eine solche Regelung ist hilfreich, wenn das Handeln der IT-Fachabteilung in Bezug zu den operativen Einheiten spezifiziert werden soll. Insbesondere zur Umsetzung gesetzlich erforderlicher Maßnahmen kann eine solche Richtlinie als interner Leitfaden dienlich sein und helfen, die datenschutzrechtlichen (Verfahrens-)Prozesse im Unternehmen zu strukturieren und zu den IT-spezifischen (technikbezogenen) Regelungen abzugrenzen. 115

f) Archivierungs- und Lösungsrichtlinie

Die Archivierungs- und Lösungsrichtlinie immer stärker an Bedeutung gewinnen. Schon allein um Kosten zu sparen und die Performanz von Datenverarbeitungssystemen nicht zu beeinträchtigen, ist es hilfreich, Altdaten regelmäßig zu löschen. Der für Unternehmen häufigste Fall der Datenlöschung ist in Art. 17 DSGVO geregelt, wonach personenbezogene Daten zu löschen sind, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, wenn der Betroffene seine Einwilligung widerruft oder der Verarbeitung seiner Daten widerspricht, die Daten unrechtmäßig verarbeitet wurden, die Löschung zur Erfüllung einer rechtlichen Verpflichtung erfolgt oder wenn Daten von Kindern verarbeitet wurden. Durch Zeitablauf dürften Daten regelmäßig dann zu löschen sein, wenn Rechtsansprüche Betroffener verjährt sind, eine gesetzliche Archivierungspflicht nicht mehr besteht (Bis dahin sind personenbezogene Daten ggf. zu sperren)⁸⁰ oder ein öffentliches Informationsinteresse hieran nicht mehr besteht (z. B. Presseartikel und wenn im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke nicht mehr gegeben sind). Im Hinblick auf die Vielzahl geltender Aufbewahrungsfristen (z. B. § 147 AO) gestaltet sich ein schlüssiges Archivierungs- und Lösungskonzept insbesondere in internationalen Konzernen als Herausforderung. Dennoch sollte ein solches Konzept nicht wegen seiner Komplexität vernachlässigt werden, denn mit dem „Recht auf Vergessenwerden“ nach Art. 17 EU-DSGVO dürfte diese Anforderung eine weit höhere Bedeutung erlangen als bisher. 116

80 Siehe § 35 Abs. 3 Nr. 1 BDSG; Art. 18 DSGVO.

3. Verzeichnis von Verarbeitungstätigkeiten

- 117 Unternehmen müssen den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben unterstützen und ihm insbesondere Hilfsmittel, Einrichtungen, Geräte und Mittel zur Verfügung stellen. Zudem muss dem Beauftragten für Datenschutz eine umfassende Übersicht über sämtliche Datenverarbeitungsprozesse im Unternehmen zur Verfügung gestellt werden (sog. Verzeichnis der Verarbeitungstätigkeiten, vgl. Art. 30 DSGVO, und er ist über alle Neuerungen und Vorhaben zu informieren.

118 **Erfassen der Datenverarbeitungsvorgänge im Unternehmen**

Datenschutz-Compliance erfordert eine enge Zusammenarbeit von Geschäftsleitung, dem Compliance Officer und dem DSB sowie insbesondere den operativen Geschäftsbereichen. Im Alltag eines Unternehmens wird diese Zusammenarbeit nicht immer gelebt. Die Unternehmensleitung sollte daher sämtliche mit der Bearbeitung von personenbezogenen Daten befassten Abteilungen des Unternehmens zur Mitwirkung an der Verfahrensübersicht und ihrer fortlaufenden Aktualisierung sowie insbesondere an einer frühzeitigen Einbeziehung des DSB bei IT-gestützten Projekten anhalten und je nach Situation ggf. verpflichten. Aber auch der DSB sollte einen ständigen Austausch mit den relevanten Mitarbeitern etablieren. Bewährt haben sich monatliche oder quartalsweise Jour Fixe sowie jährliche Gesprächsrunden mit den relevanten Abteilungen im Rahmen etwa eines Datenschutz-Audits (hierzu ausführlich unten unter → Rn. 135 ff.). Eines aufwendigen Prozesses mit Formblättern und dergleichen mehr bedarf es rechtlich zwar nicht, hat sich in der Praxis aber häufig als alternativlos herausgestellt – hier gilt es Balance zu wahren und die Kollegen *in operativen Geschäftsbereichen* nicht zu überfordern. Wichtig für eine funktionierende *Datenschutz-Compliance* sind zudem ein reger Austausch mit den Kollegen, schnelle Reaktion und lösungsorientiertes Mitwirken.

- 119 Das Verzeichnis von Verarbeitungsvorgängen ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen, vgl. Art. 30 DSGVO.
- 120 Das Verzeichnis nach Art. 30 DSGVO muss unter anderem folgende Angaben enthalten:
- Name und Anschrift der datenverarbeitenden Stelle sowie Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
 - Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung,
 - Beschreibung der betroffenen Personengruppen (z.B. Kunden und Mitarbeiter),

- Beschreibung der Daten und Datenkategorien (z.B. Kundendaten, Adressdaten),
- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
- Regelfristen für die Löschung der Daten und
- geplante Datenübermittlungen in Drittstaaten (z.B. in die USA oder nach Indien).

4. Interne Kommunikation und Awareness

Die direkte Kommunikation mit den Mitarbeitern sollte vom DSB so häufig wie möglich genutzt werden. Sie bietet ein effektives Mittel, sämtliche Mitarbeiter zu erreichen sowie regelmäßig das Thema Datenschutz bei diesen ins Bewusstsein zu rufen. Als Foren können hier Abteilungsmeetings, sog. „Town-Hall-Meetings“ oder andere Zusammenkünfte oder Treffen in Unternehmen genutzt werden, um Datenschutz als Teil der Agenda zum Bestandteil der Kommunikation an die Mitarbeiter zu etablieren.⁸¹ Mit den heutigen elektronischen Massenkommunikationsmitteln kann zudem die Mitarbeiterschaft eines gesamten Konzerns erreicht werden. Jedoch sollte beim Einsatz von Kommunikationsmitteln stets darauf geachtet werden, fachbereichsspezifische Ausdrucksformen zu vermeiden. Gerade in internationalen Konzernen ist es wichtig, dass auch kulturelle Unterschiede bei der Kommunikation berücksichtigt werden. Besteht ein Bereich Unternehmenskommunikation o.Ä., sollte die Unterstützung dieses Bereichs erwogen werden, um mit der Kommunikation effektiv eine Vielzahl von Mitarbeitern zu erreichen. Entscheidend für die Kommunikation im Datenschutz ist, dass diese einprägsam und bewusstseinsbildend ist, um das Thema Datenschutz als Allgemeingut im Handeln der Mitarbeiter zu etablieren.

121

a) Der Datenschutz-Newsletter

Der Datenschutz-Newsletter bietet eine einfache und effektive Möglichkeit, sich regelmäßig bei den Mitarbeitern ins Gedächtnis zu rufen und über aktuelle Themen aus dem Unternehmen, zum Datenschutz und zu allgemeinen Entwicklungen im Bereich Datenschutz Stellung zu beziehen. Auch hier sollte vermieden werden, rechtlich oder fachlich zu komplexe Themen darzustellen. Vielmehr sollte anhand praktischer Beispiele gezeigt werden, welche Themen bewegen oder was aktuell geschieht. Wichtig ist, dass eine Vielzahl von Mitarbeitern den Newsletter liest und der Datenschutz damit bei den Mitarbeitern präsent bleibt. Dies kann durch ansprechende Layouts oder sog. Eyecatcher im Text erreicht werden. Ideal ist es, wenn man über die Themen des Newsletters unter den Mitarbeitern spricht.

122

⁸¹ Zur Bedeutung von Kommunikationsmaßnahmen bei Compliance Management siehe ausführlich → *Hastenrath*, Kap. 6.

b) Intranet

- 123** Das Intranet bietet sich an, um dauerhaft Informationen über den Datenschutz des Unternehmens darzustellen. Die Informationen können die Organisation, Ansprechpartner, Zuständigkeitsbereiche, Richtlinien, Muster zur Auftragsverarbeitung, Formulare Checklisten sowie andere Arbeitshilfen oder auch die bisherigen Aktivitäten wie Jahresberichte, Vorträge, Schulungsunterlagen oder das Newsletter-Archiv beinhalten. Dabei sollte die Struktur die Wichtigkeit der jeweiligen Information berücksichtigen. Mitarbeiter werden in diesem Bereich des Intranets in erster Linie Ansprechpartner, Antworten zu allgemeinen oder aktuellen Fragen und Arbeitshilfen suchen.

c) Der „Datenschutz-Tag“ und Fachtagungen

- 124** Zusätzlich kann auch ein „Datenschutz-Tag“ erheblich zur Wahrnehmung des Themas Datenschutz beitragen. Ein solcher Tag sollte sorgfältig vorbereitet und abgestimmt werden, denn hier geht es darum, die Mitarbeiter des Unternehmens auf unterhaltsame Weise über das Thema Datenschutz zu informieren. Dies kann durch Podiumsdiskussionen mit interessanten Gesprächspartnern oder möglichen Kritikern des Datenschutzes erfolgen. Zudem kann auch zusammen mit dem Revisionsleiter oder Compliance Officer die Wichtigkeit des Datenschutzes zur Wahrung des Verhältnismäßigkeitsprinzips (Sicherheit und Aufklärung von Fehlverhalten vs. freie Entfaltung am Arbeitsplatz und dem Recht auf informationelle Selbstbestimmung) erörtert werden. Es gibt gerade gegenwärtig sehr viele Themen, die anschaulich dargestellt werden können: Internet der Dinge, das sog. Recht auf Vergessenwerden, Datenprofile im Internet, Datenmissbrauch, Beschäftigten-Gesundheitsdatenverarbeitung zur Risikominimierung und Verhinderung der Ausbreitung von Pandemien, usw. Die Darstellung dieser Themen kann in Diskussionen, technischen Beispielen oder Schaudiagrammen erfolgen.
- 125** Inhaltlich begleitet und ergänzt werden können solche Datenschutz-Tage auch durch Fachtagungen und Workshops zusammen mit externen Experten oder interdisziplinär durch Mitarbeiter aus anderen Bereichen, Betrieben oder Landesorganisationen. Damit kann man die alltägliche Vorgehensweise durch Erfahrungen anderer Bereiche erweitern und evtl. auch neue Möglichkeiten aufzeigen, um die Arbeit effektiver und zielführender zu gestalten.

5. Schulungen

- 126** Schulungen von Mitarbeitern, die mit der Verarbeitung personenbezogener Daten beschäftigt sind, bilden die Grundlage oder auch das Fundament, auf dem der DSB seine Tätigkeit ausüben kann. Ohne Schulungen können die jeweiligen Mitarbeiter oftmals gar nicht erkennen, welche Sensibilität ihre Tätigkeit im Bereich Datenschutz erfordert. Daher ist der regelmäßigen Schulung von sensiblen Bereichen eines Unternehmens stets eine hohe Aufmerksamkeit zu widmen.⁸² Zu schu-

⁸² Zur Relevanz von Schulungen und vielfältigen Schulungsmöglichkeiten ausführlich → *Hastenrath*, Kap. 6.

lende Kernbereiche sind die Personalabteilung, die Kundenbetreuung, die Revision, der Vertrieb, die Beschaffung, die IT, der Betriebsrat und immer mehr auch der Marketingbereich. Hier gilt es sowohl das Fachwissen (Was ist zu tun, wie muss ich mich verhalten?), aber insbesondere auch den Wertekodex des Datenschutzes zu vermitteln (Warum soll ich das machen? – Wen interessiert das?). Denn nur, wenn Mitarbeiter den Sinn hinter einer Tätigkeit verstehen, werden sie die gebotenen Aufgaben auch mit dem erforderlichen Engagement umsetzen.

a) Persönliche Schulungen

Die persönliche Schulung von Kernbereichen, d.h. solchen Bereichen, die ständig und in ausgeprägter Form mit personenbezogenen Daten zu tun haben, ist unerlässlich. Für das sehr komplexe Thema Datenschutz ist eine lebendige Darstellung hilfreich. Statische Schulungen oder Schulungen, in denen versucht wird, gesetzlich lückenlos zu präsentieren, werden den Zuhörer schon sehr bald ablenken. Wenn solche Schulungen u.a. Präsentationen nutzen, in denen Gesetzestexte hineinkopiert werden oder Textdateien schlicht in Präsentationsfolien umgewandelt wurden, besteht die Gefahr, dass die Zuhörer nicht folgen können. Nachfolgend zunächst ein Beispiel einer eher schwer zu vermittelnden, wenn auch juristisch kaum zu beanstandenden Präsentation:

127

Pflicht zur Bestellung eines Datenschutzbeauftragten nach Art. 37 DSGVO/ § 38 BDSG

Nach Art. 37 DSGVO benennen der Verantwortliche und der Auftragsverarbeiter auf jeden Fall einen Datenschutzbeauftragten, wenn

- die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln,
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.

Erweitert durch § 38 BDSG:

- Ergänzend benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.
- Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

Diese Präsentation enthält sämtliche wichtigen Informationen zum Erfordernis der Bestellung eines DSB. Allerdings wird es den Zuhörern schwerfallen, während des mündlichen Vortrags die Präsentation zu lesen und der Präsentierende wird versucht sein, die umfassende Darstellung abzulesen. Anders sieht es im folgenden Beispiel aus:

128

Pflicht zur Bestellung eines Datenschutzbeauftragten

- Verarbeitung erfolgt von Behörde oder öffentlicher Stelle (Ausnahme: Gerichte im Rahmen Rechtssprechungstätigkeit) – (DSGVO)
- Kerntätigkeit besteht hins. Art, Umfang und/oder Zwecke in Verarbeitung von pbD (DSGVO)
- Kerntätigkeit besteht in umfangreicher Verarbeitung besonderer Kategorien von Daten oder pbD über strafrechtliche Verurteilungen und Straftaten (DSGVO)
- Ergänzend (BDSG), soweit Unternehmen in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen
- Ergänzend (BDSG), unabhängig von der Anzahl damit beschäftigten Personen:
 - wenn Unternehmen Daten verarbeiten, die einer Datenschutz-Folgenabschätzung unterliegen
 - wenn Unternehmen pbD geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeiten.

- 129** Im zweiten Beispiel werden lediglich die fundamentalen Eckwerte zur Bestellung eines DSB nach Art. 37 DSGVO und § 38 BDSG benannt, ohne die Gesetzesnormen selbst zu referenzieren. Obwohl diese Darstellung nicht alle Details des Gesetzeswortlauts wiedergibt, wird es jedoch insbesondere dem nichtjuristischen Zuhörer ermöglicht, den wesentlichen Inhalt des Vortrags schnell zu erfassen, dem Vortragenden die Aufmerksamkeit zu schenken, die Kernaussagen zu verstehen und es ermöglicht dem Vortragenden, den Vortrag frei zu gestalten ohne den Text nur abzulesen. Für den Vortragenden sollte hierbei stets klar sein: Es kommt nicht auf die Lückenlosigkeit des Vortrags an, sondern dass die Zuhörer die Kernbotschaft verstanden haben. Auch sollte stets verdeutlicht werden, worum es beim Datenschutz geht: Der Schutz der Daten ist Mittel, der Schutz der Person vor Missbrauch und Ausbeutung im digitalen Umfeld ist Zweck!
- 130** In der Praxis hat sich zudem die Workshop-Schulung als wesentlich effektiver gezeigt, als die Präsentations-Schulung. Der Unterschied besteht darin, dass nicht frontal anhand von Präsentationen das für wichtig erachtete Fachwissen durch den Vortragenden vermittelt wird sondern in einer offenen Diskussion der Arbeitsalltag, die Arbeitsabläufe und Inhalte mit den Beschäftigten erörtert werden, um anhand dieser die datenschutzrechtlichen Berührungspunkte darzustellen und die Umsetzung von erforderlichen und adäquaten Maßnahmen zur Verbesserung des Datenschutzes zu erörtern. Damit nehmen die geschulten Mitarbeiter praktisch dargestellte Maßnahmen für ihren Arbeitsalltag mit und werden aktiver Teil der Schulung.

b) E-Learning/Webinars

- 131** In Unternehmen mit mehreren oder vielen nationalen oder internationalen Standorten sind Präsenzschulungen kaum kosteneffizient durchzuführen. Hier bietet es sich an, die Schulungen zu automatisieren, indem man mit auf bestimmte Bereiche oder auch die Allgemeinheit der Mitarbeiter abgestimmten Schulun-

gen eine möglichst große Zahl von Mitarbeitern erreicht. Diese Schulungen sollten so abgestimmt sein, dass sie:

- die Zielgruppe erreichen;
- den Zweck der Schulung (Initial- oder Folgeschulung) transportieren;
- die Problemfelder in aktueller und verständlicher Form darstellen;
- den Schulenden interaktive Elemente anbietet (durch entsprechend aufbereitetes Schulungsmaterial oder bei Schulungen durch Telefonkonferenzen, in dem Fragerunden ermöglicht werden);
- die Teilnahme dokumentieren.

Nur so kann gewährleistet werden, dass die datenschutzrechtlichen Themen der Zielgruppe adressiert, die erforderlichen Maßnahmen vermittelt und die datenschutzrechtlichen Risiken im Rahmen des Schulungserfordernisses vermindert werden. **132**

E-Learnings oder Webinars können ebenso dazu beitragen, die Beschäftigten die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach den Datenschutzvorschriften zu beraten, zu sensibilisieren und zu schulen.⁸³ Gerade im Hinblick auf die stetige und gegenwärtig sehr dynamische Entwicklung im Datenschutz sollten diese Möglichkeiten genutzt werden, um die Flut an Neuerungen effektiv vermitteln zu können. **133**

c) Unterstützung dezentraler Compliance-Funktionen

Die umfassenden Aufgaben des DSB sind seit Einführung der Datenschutzgrundverordnung noch erheblich umfangreicher geworden (man bedenke nur die erweiterten Dokumentationspflichten und Prozesse, um die „Privacy by Design & Default“-Anforderungen gemäß Art. 25 DSGVO erfüllen zu können). Von daher wird es von immer größerer Wichtigkeit, dezentrale Unternehmenseinheiten zu unterstützen und die Zusammenarbeit zu koordinieren. Schulungsunterlagen oder Muster können ausgetauscht werden oder zentrale Netzwerkressourcen (Netzlaufwerke, Sharepoint usw.) können dem Austausch und der gegenseitigen Verfügbarmachung von Mustern, Formularen, Schulungsunterlagen oder aktuellen Diskussionen dienen. Ein derartiger Know-how-Austausch dürfte bei zunehmender Komplexität der datenschutzrechtlichen Anforderungen und auch der IT-Infrastruktur sehr hilfreich sein. Zudem kann eine zentrale Koordination und Verfügbarmachung von Verzeichnissen von Verarbeitungstätigkeiten und datenschutzrechtlichen Dokumentationen auch dazu beitragen, dass diese nicht mehrfach – z.B. in einem dezentral organisierten international tätigen Unternehmen – erstellt werden müssen. **134**

⁸³ Siehe Art. 39 Abs. 1 lit. a und b DSGVO.

V. Effektive Datenschutzüberwachung

- 135** Neben der rechtlichen Beratung und der Projektbegleitung mit Erstellung oder Beratung zur Erstellung der erforderlichen Dokumentation gehört auch die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden (Art. 30 DSGVO und Art. 25 im Hinblick auf „Privacy by Design & Default“-Dokumentationspflichten). Eine solche Überwachung kann mit diversen Mitteln erfolgen. Denn neben der Kontrolle gehört auch die Kommunikation der Feststellungen dazu. Die Geschäftsführung ist sich oft z. B. nicht darüber bewusst, welche Risiken und Probleme in datenschutzrechtlicher Hinsicht bestehen. Daher ist es u. a. erforderlich, die Feststellungen auch richtig zu adressieren. Die Überwachung und Kontrolle der Datenverarbeitung dagegen können in diversen Schritten mit unterschiedlicher Intensität erfolgen.

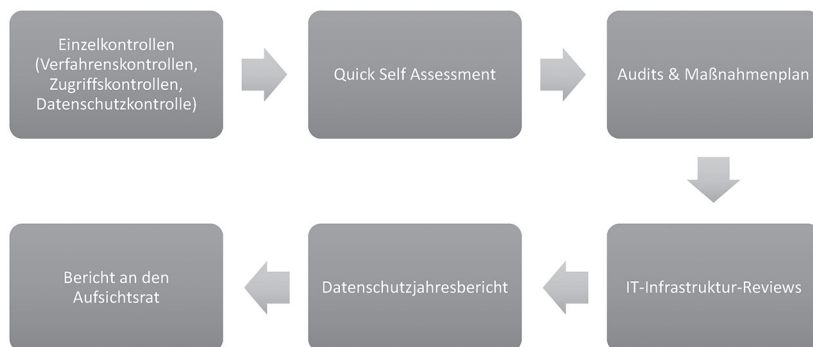


Abbildung 4: Maßnahmen der datenschutzrechtlichen Kontrolle

1. Audits und Maßnahmenpläne/Quick Self-Assessment

- 136** Die Datenschutzkontrolle kann als Einzelfallkontrolle (Überprüfung der Verarbeitung, Zugriffskontrollen, Datenschutzkontrolle nach Art. 39 Abs. 1 lit. b DSGVO), als Quick Self-Assessment oder als (Groß-)Audit erfolgen. Sämtliche dieser Prüfungen können in einer Jahresplanung festgelegt oder aber vorfall- oder verdachtsbezogen durchgeführt werden.
- 137** Die Einzelfallkontrolle bietet sich bei allgemein gängigen, etablierten und strukturierten Datenverarbeitungsverfahren an. Denn die Einzelfallkontrolle erfolgt punktuell und betrachtet nur einen Ausschnitt eines Datenverarbeitungsverfahrens. Hierzu können Kurzinterviews mit verantwortlichen Personen oder die Auswertung sämtlicher Daten, die zur Sicherstellung des ordnungsgemäßen Betriebes vorliegen (z. B. Logdateien), herangezogen und ausgewertet werden. Die Einzelfallkontrolle dient der Stichprobenprüfung für Datenverarbeitungsverfahren, die vom datenschutzrechtlichen Reifegrad her als grundsätzlich sicher

eingestuft werden können oder aber als Folge- bzw. Zwischenprüfung nach erfolgten Audits durchgeführt werden. Ferner erfolgen Einzelfallkontrollen zusammen mit IT-Security oder der internen Revision bei Verdachts- oder Vorfall-Audits, um schnell im Hinblick auf Compliance-relevante Vorfälle eingreifen zu können. Bei diesen Einzelfallkontrollen sollten auch das jeweilige Verzeichnis der Verarbeitungstätigkeit auf Vollständigkeit und Aktualität überprüft werden.

Quick Self-Assessments dienen dem DSB dazu, mit verhältnismäßig geringem Aufwand die datenschutzrechtliche Überwachung von Datenverarbeitungsverfahren zu gewährleisten, die entweder nicht im Fokus eines Audits stehen (Relevanz des Datenverarbeitungsverfahrens oder kurzer Zeitraum seit dem letzten Audit) oder weil ein Audit aufgrund anderweitiger Prioritäten nicht erfolgen kann. Ein solches Quick Self-Assessment wird von verantwortlichen Personen des jeweiligen Datenverarbeitungsverfahrens durchgeführt und es gibt insbesondere Aufschluss über (a) Selbstwahrnehmung des/der Verantwortlichen für das jeweilige Datenverarbeitungsverfahren, (b) einen Überblick über das Datenverarbeitungsverfahren und (c) eine gegenwärtige Risikobetrachtung⁸⁴ im Hinblick auf das jeweilige Datenverarbeitungsverfahren. Damit das Quick Self-Assessment auch selbstkritisch von den Verantwortlichen durchgeführt wird, ist sicherzustellen, dass die das Quick Self-Assessment durchführenden Verantwortlichen darauf hingewiesen werden, dass eine zu positive Darstellung auch dazu führen kann, dass mögliche Risiken von den verantwortlichen Mitarbeitern zu verantworten sein können, denn nur eine kritische und offene Selbstwahrnehmung ermöglicht die Einleitung erforderlicher Maßnahmen zur Risikominimierung.

Audits (Groß-Audits, Regel-Audits) erfolgen im Rahmen von jährlichen Planungen. Sie haben dabei die Relevanz der zu prüfenden Datenverarbeitungsverfahren sowie die Intervalle zwischen zwei Audits zu berücksichtigen. Je nach Umfang des zu prüfenden Datenverarbeitungsverfahrens müssen Abstimmungen mit den Verantwortlichen des Datenverarbeitungsverfahrens erfolgen. Audits bei Auftragsverarbeitern haben auch vertragliche Bestimmungen über die Ankündigungsfrist, den Umfang und die Häufigkeit solcher Audits zu beachten. Die Vorbereitung, Durchführung und die Erstellung eines Abschluss- und Maßnahmenplans können sich dabei über mehrere Wochen oder gar Monate hinziehen. Hat der DSB nicht selbst die Ressourcen zur Durchführung von Audits, sind diese mit der internen Revision abzustimmen und in die jährliche Prüfungsplanung aufzunehmen. Das Ergebnis der Prüfungen ist transparent darzustellen. Aus den einzelnen Feststellungen sollten Maßnahmen abgeleitet werden, die es den Verantwortlichen ermöglichen, in einem angemessenen Umfang festgestellte Defizite oder Risiken zu beseitigen. Hierauf sich anschließende Folge-Audits können sich dann wiederum auf punktuelle Prüfungen oder Quick Self-Assessments beschränken.

138

139

84 *Schmidl*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 28 Rn. 5 ff.

2. IT-Infrastruktur-Reviews und Koordinierung mit IT-Security

- 140** Ein IT-Infrastruktur-Review oder auch ein ITIL-Service-Review (ITIL = IT Infrastructure Library, welche eine Sammlung von vordefinierten und standardisierten Prozessen, Funktionen und Rollen, wie sie typischerweise in jeder IT-Infrastruktur von mittleren und großen Unternehmen vorkommen,⁸⁵ darstellt) stellt eine Herausforderung für alle Beteiligten dar, denn ein solches Review erfordert eine langfristige Planung und ist mit den relevanten Bereichen abzustimmen (insb. IT und interne Revision). Ein solches Review kann nur als „Joint Review“ zusammen mit der IT-Security, der internen Revision sowie erforderlichenfalls externen Dienstleistern gemeinsam in einem überschaubaren Zeitrahmen durchgeführt werden.⁸⁶ Die aus einem solchen Review gewonnenen Erkenntnisse sollten dann ebenfalls mit einem Maßnahmenplan versehen werden, sodass Risikobeseitigungen aber auch Prozessoptimierungen effizient umgesetzt werden können. Bei einem solchen Review dürften regelmäßig auch die Maßnahmenpläne umfangreicher sein, sodass schon bei der Planung eines solchen Reviews der zeitliche Umfang und Kostenaufwand für die Maßnahmenrealisierung mitberücksichtigt werden sollten.
- 141** Mit einem IT-Infrastruktur-Review oder ITIL-Service-Review sollen die IT-Ressourcen und Datenverarbeitungsverfahren hinsichtlich eines sicheren und strukturierten IT-Betriebs insbesondere im Hinblick auf die Integrität und Verfügbarkeit der IT auf Grundlage des Sicherheitskonzepts geprüft werden. Das Sicherheitskonzept muss mit der IT-Strategie und der IT-Organisation übereinstimmen und eine Bewertung der spezifischen Sicherheitsrisiken des Unternehmens ermöglichen.⁸⁷ Die aus dem Sicherheitskonzept abgeleiteten Verfahren, Anweisungen oder Sicherungsmaßnahmen umfassen physische und logische Sicherungsmaßnahmen, die in datenschutzrechtlicher Hinsicht den Härte- oder Reifegrad der Ausgestaltung der technischen und organisatorischen Maßnahmen⁸⁸ darstellen und durch ein solches Review verifiziert und ggf. auch einem Belastungs- oder Stresstest ausgesetzt werden sollten.

3. Incident- und Regel-Reporting aus den Betrieben

- 142** In Unternehmen mit diversen in- und/oder ausländischen Beteiligungen sollte frühzeitig über eine effiziente (zentrale) Datenschutzorganisation⁸⁹ nachgedacht werden. Gerade vor dem Hintergrund von zentralen Datenverarbeitungsverfahren

⁸⁵ Siehe https://de.wikipedia.org/wiki/IT_Infrastructure_Library (zuletzt abgerufen am 19.3.2024).

⁸⁶ Zur Notwendigkeit eines sog. Schnittstellenmanagements bei Compliance-Maßnahmen siehe ausführlich → *Rau*, Kap. 3.

⁸⁷ Zur wachsenden Bedeutung der IT-Security im Rahmen des Compliance Managements siehe → *Bensinger*, Kap. 14.

⁸⁸ Siehe Art. 32 DSGVO geregelt.

⁸⁹ Vgl. v. d. *Bussche/Voigt*, Konzerndatenschutz, Teil 2, Kap. 1 Rn. 30 ff.; siehe auch Art. 37 Abs. 2 DSGVO.

ren (Buchhaltung, Warenwirtschaftssystem, ERP, CRM usw.) ist es hilfreich, wenn die datenschutzrechtlich relevanten Maßnahmen dort geprüft werden, wo sie zentral oder erstmalig eingeführt werden. Zugleich ist es erforderlich, eine aktive Rückkopplung aus den Beteiligungen oder Landesorganisationen zu erhalten, um mögliche Risiken, Defizite oder sonstige Maßnahmen erfordernde Sachverhalte zu erfahren. Hierfür eignen sich Incident- und Regel-Reports, die standardisiert an den z.B. Konzern-DSB⁹⁰ zu übermitteln sind. Diese Reports können kurzfristig dabei helfen, bei schwierigen Sachverhalten zu unterstützen oder aber zentrale Gegenmaßnahmen abzustimmen sowie bei Regel-Reports, einen Statusbericht über den allgemeinen Zustand des Datenschutzes in der jeweiligen Organisation zu erhalten.

4. Der Datenschutzjahresbericht

Der Datenschutzjahresbericht⁹¹ ist streng genommen kein Überwachungsinstrument. Allerdings dient dieser dazu, die Geschäftsführung eines Unternehmens über die Wahrnehmungen und Erkenntnisse des DSB aus Audits und Einzelfallprüfungen zu informieren und dieser somit Aufschluss über den Ist-Zustand des Datenschutzes im Unternehmen zu geben. Hierdurch wird die Geschäftsführung erst in die Lage versetzt, ggf. Maßnahmen einzusteuern oder Budgets freizugeben, denn die Risikodarstellung im Jahresdatenschutzbericht liefert häufig erst die Begründung für die Mittelfreigabe. **143**

Der Datenschutzjahresbericht sollte für einen festgelegten Zeitraum die durchgeführten Maßnahmen des DSB, die Feststellungen und Risiken sowie die erforderlichen Maßnahmen zur Risikominimierung darstellen. Er kann vor Übergabe an die Geschäftsführung mit der IT-Security, dem Compliance Officer oder auch der internen Revision abgestimmt oder sogar um eigene Kapitel ergänzt werden, um ein umfassendes Bild über den Zustand des Datenschutzes vermitteln zu können. Allerdings gilt auch für den Jahresdatenschutzbericht, dass der DSB bei Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei ist.⁹² **144**

5. Bericht an Aufsichtsrat/Compliance-Bericht/Audit Committee

Angelehnt an den Jahresdatenschutzbericht kann es auch hilfreich sein, einen jährlichen Bericht an den Aufsichtsrat zu erstellen. Ein solcher kann auf dem Jahresdatenschutzbericht an die Geschäftsführung basieren, sollte jedoch berücksichtigen, dass eine vergleichbare Detailtiefe hier nicht geboten ist, denn der Aufsichtsrat soll strategische Weichen für das Unternehmen stellen. Daher **145**

⁹⁰ Siehe v. d. Bussche/Voigt, Konzerndatenschutz, Teil 2, Kap. 2 Rn. 41 ff.; siehe auch Art. 37 Abs. 2 DSGVO.

⁹¹ Simitis, in: Simitis, BDSG, § 4g Rn. 94; v. d. Bussche/Voigt, Konzerndatenschutz, Teil 2, Kap. 1 Rn. 78.

⁹² Siehe Art. 38 Abs. 3 Satz 1 DSGVO.

wären operative Risiken oder gar die Darstellung einzelner Datenverarbeitungsmaßnahmen wenig hilfreich. Vielmehr sollte hierin darüber berichtet werden, ob sich der Datenschutz im Unternehmen auf einem guten Weg befindet oder wo strategische Maßnahmen zur besseren Ausrichtung des Datenschutzes geboten sind.

- 146** Eine weitere Möglichkeit zum Bericht über den Zustand des Datenschutzes stellt der Compliance-Bericht dar. In diesem kann der Datenschutz als eigenes Kapitel dargestellt werden. Regelmäßig wird die Darstellung von empfohlenen Maßnahmen hier jedoch wenig hilfreich sein, weil der Compliance-Bericht an einen zu breiten Adressatenkreis gerichtet ist. Deshalb wäre in einem solchen Bericht der Fokus eher auf durchgeführte Maßnahmen und festgestellte Risiken zu lenken.

6. Zusammenarbeit mit dem Compliance Officer, IT-Security und Revision

- 147** Bei der Datenschutzüberwachung ist der DSB regelmäßig auch auf die Zusammenarbeit mit anderen Fachbereichen angewiesen. Dies erfolgt durch gegenseitige Unterstützung bei der täglichen Zusammenarbeit und durch die Abstimmung von Maßnahmen zur Sicherstellung eines effektiven Datenschutzes. Relevant für die Zusammenarbeit im Unternehmen können die folgenden Bereiche sein.

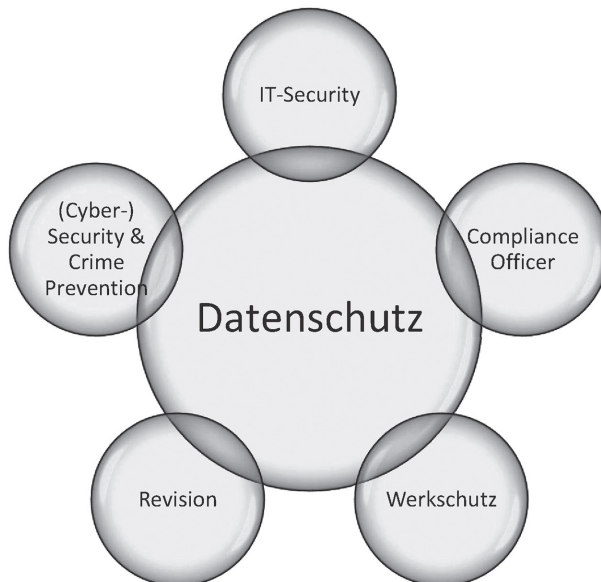


Abbildung 5: Zusammenarbeit des Datenschutzbeauftragten mit anderen Bereichen

Die IT-Security ist für den DSB der regelmäßige Ansprechpartner bei Fragen zur Umsetzung des technischen Datenschutzes insbesondere im Hinblick auf die technischen und organisatorischen Maßnahmen, die nunmehr aus Art. 24, Art. 25 und Art. 32 DSGVO abgeleitet werden können. Man könnte auch sagen, dass der DSB die datenschutzrechtlichen Anforderungen der operativen Fachbereiche mitdefiniert (das „Was“, „Wieviel“ und „Wozu“) und sodann die IT-Security auf IT-Seite die technische Umsetzung (das „Wie“) mitdefiniert. Hierbei ist eine enge Abstimmung unumgänglich. **148**

Auch bei der täglichen Zusammenarbeit ist ein fortwährender Austausch erforderlich, damit datenschutzrechtlich relevante Maßnahmen effektiv umgesetzt und berücksichtigt werden können. Die IT-Security kann den DSB bei seiner Arbeit insbesondere hinsichtlich der Umsetzung folgender technischer und organisatorischer Maßnahmen⁹³ unterstützen: Verschlüsselung, Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme. Zudem unterstützt die IT-Security bei der Umsetzung von Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen. Im Rahmen der zusätzlichen Anforderungen aus dem DORA und der NIS-2 Verordnung ergeben sich zusätzliche Anforderungen an die IT-Sicherheit, die zudem ein enges Zusammenspiel zwischen dem Datenschutzbeauftragten sowie dem IT-Sicherheitsbeauftragten erfordern.⁹⁴ **149**

Der Bereich (Cyber-)Security und Crime Prävention – soweit vorhanden, ansonsten die interne Revision – kann den DSB insbesondere bei der Zugriffs-, Weitergabe- und Eingabekontrolle (Datenintegrität) unterstützen.⁹⁵ Denn diese Abteilung kann insbesondere bei einem Verdacht des illegalen Datenzugriffs, der Datenmanipulation oder der unberechtigten Weitergabe prüfen, ob und in welcher Form unberechtigt personenbezogene Daten genutzt, sich verschafft oder an Dritte übermittelt wurden. Zudem kann dieser Bereich dabei unterstützen, Schwachstellen in den o. g. Bereichen der technischen und organisatorischen Maßnahmen aufzuzeigen bzw. solche vom DSB bewerten lassen. **150**

Der Werkschutz wiederum kann den DSB im Bereich der Zutritts- und Weitergabekontrolle (Verschlüsselung und Vertraulichkeit) von personenbezogenen Daten unterstützen. Dieser kann z. B. effektive Maßnahmen mit dem DSB abstimmen, um den unberechtigten Zutritt zu datenschutzrechtlich sensiblen Bereichen durch Einführung eines Berechtigungssystems abzusichern. Zudem sind Kontrollen bzgl. der Nutzung privater Speichermedien oder Geräte denkbar, um **151**

93 Hilfreich hierzu auch: https://www.lda.bayern.de/media/checkliste/baylda_checkliste_tom.pdf (zuletzt abgerufen am 19.3.2024).

94 Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act) sowie Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union (NIS2-Richtlinie), <https://digital-strategy.ec.europa.eu/de/policies/nis2-directive> (zuletzt abgerufen am 19.7.2024).

95 Zu Cyber Crime und IT-Security siehe ausführlich → *Bensinger*, Kap. 14.

zu verhindern, dass Besucher oder Mitarbeiter des Unternehmens personenbezogene Daten unberechtigt mitnehmen.

- 152** Die interne Revision ist im Zusammenhang mit einer effektiven Datenschutzkontrolle unverzichtbar. Ihr obliegt es, im Zuge der Durchführung von Audits bei Feststellungen mit datenschutzrechtlicher Relevanz den DSB hinzuzuziehen, um geeignete Maßnahmen festlegen zu können. Gerade bei den immer wichtiger werdenden sog. E-Discovery-Maßnahmen, wie z. B. E-Mail-Screenings⁹⁶ oder der Kontrolle des Internetzugangs und der Internetnutzung durch Mitarbeiter,⁹⁷ ist im Vorfeld die Rechtmäßigkeit der Maßnahme genau zu prüfen, um anschließend rechtlichen Problemen bis hin zu möglichen Beweisverwertungsverböten⁹⁸ begegnen zu können. Sollte der DSB Datenschutz-Audits nicht selbst oder durch Hilfspersonen durchführen können, sollte der DSB erforderliche Datenschutz-Audits durch die interne Revision durchführen lassen. Hierzu wären der Prüfungsplan sowie der Prüfungsinhalt (Checklisten) mit der internen Revision jeweils abzustimmen.
- 153** Schließlich ist auch die Zusammenarbeit mit dem Compliance Officer von Bedeutung für den DSB.⁹⁹ Mit dem Compliance Officer sollte der DSB abstimmen, inwieweit ein einheitliches Compliance-Reporting-System auch datenschutzrechtliche Aspekte umfassen soll. Hierdurch können standardisierte Reports an die verschiedenen Bereiche übermittelt werden und einheitliche Prozesse ermöglichen es den jeweiligen Bereichen, mit einem einheitlich strukturierten Report umfassend Auskunft geben zu können, ohne jeden einzelnen compliance-relevanten Bereich getrennt mit Reports versorgen zu müssen, was ohnehin die administrative Komplexität nur zusätzlich erhöhen würde. Zudem können in Compliance-Schulungen auch allgemeine datenschutzrechtliche Aspekte angesprochen werden. Damit kann die Frequenz der bewusstseinsbildenden Maßnahmen bei den Mitarbeitern zusätzlich erhöht werden, ohne dass der DSB diese Maßnahmen stets selbst durchführen muss. Ferner ist der DSB auch zur effektiven Umsetzung der Compliance heranzuziehen, denn das Spannungsfeld (Datenvermeidung und Datensparsamkeit vs. Transparenz) zwischen dem Beschäftigtendatenschutz (§ 26 BDSG i.V.m. Art. 88 DSGVO) und die effektive Ausgestaltung von Maßnahmen zur Gewährleistung einer effektiven Compliance werden eine enge Zusammenarbeit zwischen diesen beiden Funktionen stets erfordern.

⁹⁶ Siehe v. Brühl/Sepperer, ZD 2015, 415 ff.

⁹⁷ Schmidl, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 28 Rn. 355 f.

⁹⁸ Beschluss des LAG Berlin-Brandenburg vom 15.5.2014 – 18 TaBV 828/12 u. 18 TaBV 830/12, zum Beweisverbot von unter datenschutzrechtswidrig erlangten Beweisen durch den Betriebsrat; siehe auch: ZD 2015, 591 ff.

⁹⁹ Siehe auch: v. d. Bussche/Voigt, Konzerndatenschutz, Teil 5, Kap. 1 Rn. 1 ff.; Renz/Frankenberg, ZD 2015, 158 ff.

VI. Beschäftigtendatenschutz

1. Bedeutung des Beschäftigtendatenschutzes für Compliance

Compliance ist vor allem Managementaufgabe – wie sich aus diesem Handbuch allenthalben zu Recht entnehmen lässt. Dies betrifft jedoch neben den üblichen Rechtsbereichen vorrangig auch den Datenschutz¹⁰⁰ und damit auch den Beschäftigtendatenschutz. Während sich der allgemeine Datenschutz mit Daten in Drittbeziehungen (z. B. Kundendaten, Lieferantendaten etc.) befasst, betrifft der Beschäftigtendatenschutz die Verarbeitung von Daten der Mitarbeiter im eigenen Unternehmen und Betrieb. 154

Aus der Sicht eines Compliance-Verantwortlichen eröffnet sich beim Beschäftigtendatenschutz ein Schnittstellenbereich zwischen Compliance, Arbeitsrecht und Datenschutz. Das Verhältnis von Arbeitgeber und Arbeitnehmer ist durch zahlreiche beiderseitige Rechte und Pflichten geprägt, die unmittelbar die Compliance-Arbeit beeinflussen. Zudem bilden Regelungswerke wie Betriebsvereinbarungen – in Zusammenarbeit mit dem Betriebsrat – die Basis für Verhaltensvorgaben an Mitarbeiter. Gleichzeitig sind die Möglichkeiten der Informationsbeschaffung und der Verwendung von Mitarbeiterdaten durch die datenschutzrechtlichen Grenzen geprägt. Sowohl das Arbeitsrecht als auch der Datenschutz sind wesentliche Bestandteile einer regelkonformen Compliance-Organisation, während sie zugleich jeweils eigene Risikofelder **determinieren**. Das gilt erst recht für den Beschäftigtendatenschutz. 155

Die zentrale Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten im Betrieb war bisher auch vor allem in § 26 Abs. 1 BDSG geregelt, der die Datenverarbeitung zum Zwecke der Begründung, Durchführung und Beendigung des Arbeitsverhältnisses zum Gegenstand hat. Die Begrifflichkeit des Beschäftigtendatenschutzes – welcher nach wie vor seine Gültigkeit besitzt – wird dabei synonym für die Begriffe Arbeitnehmer-, Mitarbeiter- und Personaldatenschutz verwendet und hat sich spätestens mit der Anpassung des BDSG an die DSGVO¹⁰¹ als solche weitgehend durchgesetzt. Der Begriff des Beschäftigten, welcher im Rahmen von § 26 BDSG Anwendung findet, wird in § 26 Abs. 8 BDSG legaldefiniert. Er ist weit gefasst, deckt sich nicht mit dem sozialversicherungsrechtlichen Begriff des Beschäftigten und umfasst aus diesem Grund nicht nur Arbeitnehmer, sondern u. a. auch zur Berufsbildung beschäftigte Personen, arbeitnehmerähnliche Personen und Bewerber sowie Personen, deren Beschäftigungsverhältnis beendet ist (Rentner und Pensionäre). Offen ist die Stellung von Organen, z. B. Fremd-Geschäftsführer, Vorstandsmitglied u. Ä. Diese sind laut Gesetzeswortlaut nicht erfasst. Das widerspricht aber teilweise europäischem Recht, wonach z. B. Fremd-Geschäftsführer praktisch in einem Unter- 156

100 Man spricht insoweit von einem Datenschutzmanagementsystem (DMS).

101 Vgl. die Gesetze zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU).

ordnungsverhältnis zur Gesellschaft stehen und daher als Arbeitnehmer zu qualifizieren sind.¹⁰²

- 157** Mit dem EuGH-Urteil¹⁰³ vom 30.3.2023 wird die zentrale Rechtsgrundlage des § 26 Abs. 1 BDSG im Beschäftigungsverhältnis im Kern erschüttert. Der EuGH hat sich erstmalig zum deutschen Beschäftigendenschutz und der nationalen Umsetzung des Art. 88 DSGVO geäußert. Das Urteil des EuGH führt zu erheblichen Unsicherheiten bei den Rechtsanwendern. In dem Urteil wurden Vorfragen zu der Frage beantwortet, ob § 23 Abs. 1 Satz 1 Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG) anwendbar ist, wenn Lehrerinnen und Lehrer des hessischen Schuldienstes zum Halten von Unterricht per Videokonferenz verpflichtet werden. Diese Vorschrift verstößt nach Ansicht des EuGH gegen die DSGVO, da sie eine bloße Generalklausel und keine „spezifischere Vorschrift“ i. S. v. Art. 88 Abs. 1 DSGVO darstellt. Die Vorschrift regelt nur, dass personenbezogene Daten von Beschäftigten für gewisse Zwecke verarbeitet werden dürfen, wenn dies zur Vertragsdurchführung „erforderlich“ ist. Im Ergebnis besteht damit kein Unterschied zur Regelung in der DSGVO selbst (vgl. Art. 6 Abs. 1 lit. b DSGVO). Aufgrund der nahezu wortgleichen Formulierung in § 26 Abs. 1 Satz 1 BDSG lässt sich die Bewertung in unmittelbarer Analogie auf diesen übertragen.¹⁰⁴ Bei der Verarbeitung von Beschäftigtendaten müssen Arbeitgeber sich nun auf die europaweit einheitlichen Rechtsgrundlagen stützen, wenn sie die Rechtsunsicherheit vermeiden wollen.
- 158** Unternehmen sollten sich jedenfalls der Tatsache bewusst sein, dass § 26 Abs. 1 Satz 1 BDSG keine Datenverarbeitungen legitimieren kann, die nicht bereits nach Art. 6 Abs. 1 Satz 1 DSGVO zulässig sind. An dieser Vorschrift ist nach der Rechtsprechung des EuGH jede Verarbeitung personenbezogener Daten zu messen, auch Datenverarbeitungen im Beschäftigungskontext (s. → Rn. 68 ff. des Urteils des EuGH vom 30.3.2023 – C-34/21). Hilfsweise müssen nun u. a. Art. 6 Abs. 1 lit. b, f DSGVO herangezogen werden. Dies erfordert jedoch unbedingt eine Prüfung und damit einhergehende Interessenabwägung in jedem Einzelfall. Für die Praxis bedeutet dies letztlich, dass bei der Anwendung von § 26 BDSG insgesamt immer die Lesbarkeit i. V. m. den Art. 6 Abs. 1 Satz 1 lit. a–f DSGVO bzw. Art. 6 Abs. 4 DSGVO zu empfehlen ist. Weiterhin ist hiermit zwecks Konkretisierung aufgrund Interessenabwägung und der sich aus der DSGVO ergebenden Nachweispflicht (vgl. Art. 5 DSGVO) ein höherer Dokumentationsaufwand verbunden.

¹⁰² *Taegeer/Gabel*, DSGVO BDSG, 3. Aufl. 2019, § 26 Rn. 104.

¹⁰³ EUGH, Urt. v. 30.3.2023 – C 34/21.

¹⁰⁴ Eine abschließende Feststellung fehlt hier durch die nationalen Gerichte wie z. B. dem vorlegenden VG Wiesbaden noch, ist aber gemäß der Bewertung der Datenschutzaufsichtsbehörden als wahrscheinlich anzunehmen; vgl. etwa die Ausführungen des LfDI Baden-Württemberg „FAQ zum EuGH-Urteil vom 30. März 2023 – C-34/21“ unter <https://www.baden-wuerttemberg.datenschutz.de/faq-rechtsgrundlagen-bei-beschaeftigtendaten/> (zuletzt abgerufen am 19.3.2024).

Nicht zuletzt aufgrund der europarechtlichen Bedenken gegenüber den nationalen Regelungen des BDSG hat die Bundesregierung den „Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes“ am 7.2.2024 verabschiedet. Die Reformbedürftigkeit des BDSG ist bereits lange vor dem Entstehen der DSGVO bekannt. Der Gesetzentwurf zielt im Wesentlichen darauf ab, Ergebnisse aus der Evaluierung des BDSG umzusetzen. So soll die Datenschutzkonferenz (DSK) institutionalisiert und eine bessere Durchsetzung und Kohärenz des Datenschutzes erreicht werden. Weitere Anpassungen bleiben ebenso abzuwarten wie der Umstand, dass bereits Reformbemühungen in der Vergangenheit ohne Erfolg blieben. **159**

Der Beschäftigtendatenschutz als besonderer Regelungsbereich des Datenschutzes ist unmittelbar Teilbereich der gelebten Compliance im Unternehmen. Letztlich geht es um die Einhaltung der Vorgaben der DSGVO¹⁰⁵ zu dem Zweck, im Unternehmen den entsprechenden Umgang mit Beschäftigtendaten nicht nur zu leben, sondern auch entsprechend zu überwachen und zu dokumentieren. In der Praxis erläutert häufig eine interne Richtlinie die Vorgaben – insbesondere für den Kernbereich der Verarbeitung von personenbezogenen Daten im Beschäftigungsverhältnis: die Personalabteilung. Originäre Aufgabe ist es, den Schutz der Beschäftigtendaten als Aufgabe der verantwortlichen Stelle wahrzunehmen und die Risiken beim Umgang mit Beschäftigtendaten sowie mit Gesundheitsdaten (sensible Daten) zu minimieren. **160**

Dies alles soll im täglichen Kerngeschäft nicht untergehen und muss somit intern als Richtlinie bzw. Verhaltensleitlinie herausgestellt werden. Compliance als Instrument der Nachhaltigkeit kann dabei nicht nur helfen, die datenschutzrechtlichen Vorgaben einzuhalten, sondern auch den Umgang mit den oben genannten Daten zu steuern. **161**

Weitere Kontrollinstrumente im Rahmen der datenschutzrechtlichen Compliance sind die Dokumentation für die eigenen Prozessabläufe und Behördenkontrollen im täglichen Umgang mit Beschäftigtendaten sowie der rechtlich einwandfreie Umgang mit Daten bei der Aufdeckung von Straftaten im Rahmen des Beschäftigungsverhältnisses. **162**

Nicht zuletzt sind die enorm gestiegenen Bußgelder,¹⁰⁶ Schadenersatzforderungen und Strafen ein weiterer Grund für den Compliance-Verantwortlichen, das Datenschutzmanagement in das bestehende CMS zu integrieren.¹⁰⁷ Dabei wird man schnell erkennen, dass die Anforderungen an ein DMS aus der DSGVO und dem BDSG zu einem Großteil deckungsgleich mit den Anforderungen an **163**

¹⁰⁵ Vgl. auch die Regelungen in Art. 5, Art. 24 und in der Öffnungsklausel des Art. 88 DSGVO.

¹⁰⁶ Nach Art. 83 Abs. 1 DSGVO müssen diese wirksam, verhältnismäßig und abschreckend sein.

¹⁰⁷ Dies lohnt sich vor allem deswegen, weil sich insbesondere präventive Maßnahmen haftungsmildernd nach Art. 83 DSGVO auswirken i. V. m. Art. 40 ff. DSGVO auswirken.

ein wirksames CMS sind.¹⁰⁸ Bei diesem Vorhaben kann folgende **Checkliste** helfen:

164

Checkliste zur Integration von einem DMS in ein bestehendes CMS:¹⁰⁹

1. Kultur der Datenvermeidung und Datensparsamkeit schaffen (Tone from the Top)¹¹⁰
2. Datenschutzbeauftragten und Personaler in Compliance-Organisation einbinden
3. Datenfluss analysieren (entspricht besonderer Risikoanalyse)¹¹¹
4. Daten- und IT-Sicherheit gewährleisten¹¹²
5. Datenschutz in Compliance-Richtlinien aufnehmen¹¹³
6. Datenschutzschulung zum Umgang mit (sog. sensiblen) Beschäftigten
7. Datenschutzbeiräte benennen¹¹⁴
8. Mitarbeiter-Monitoring verhältnismäßig gestalten
9. Dokumentation der Beschäftigtendatenvorgänge sicherstellen¹¹⁵

¹⁰⁸ *Fladung*, CB 2015, 364.

¹⁰⁹ Nach *Fladung*, CB 2015, 364.

¹¹⁰ Nach Möglichkeit sollten sinnvolle Instrumente wie Pseudonymisierung und Anonymisierung zum Standardrepertoire gehören. Zur Bedeutung des Tone from the Top für die Wirksamkeit von Compliance-Maßnahmen siehe → *Schulz*, Kap. 1 Rn. 69.

¹¹¹ Allein dies hilft schon das Risiko der vielfach gefürchteten sog. Datenpanne nach Art. 33 DSGVO zu verringern.

¹¹² Mit Art. 32 DSGVO und dem IT-Sicherheitsgesetz vom 25.7.2015, welches sich jüngst wiederum in einer verschärfenden Reform befindet, wurden die Anforderungen nochmals höher gesetzt.

¹¹³ Nichtssagende Standardsätze, die die Beachtung der DSGVO versichern, finden sich in der Praxis immer noch häufig. Hier sollten künftig zum einen die Vorgaben aus der DSGVO und dem BDSG präzisiert werden und zum anderen klare Maßgaben zur vernünftigen Abwägung zur Wahrung des Persönlichkeitsrechts der einzelnen Mitarbeiter an die Hand gegeben werden.

¹¹⁴ Diese können bei der Vermittlung der Bedeutung an Mitarbeiter unterstützend tätig werden; vgl. auch *Thüsing* in seinem CB-Editorial in CB 10/2015.

¹¹⁵ Ob in einer zentralen mit gesonderten Zugriffsrechten versehenen Compliance-Datenbank oder über ein bereits vorhandenes Informationsmanagementsystem – personenbezogene Daten unterliegen dem besonderen Schutz der DSGVO bzw. des BDSG. So wurde vom BGH bereits lange vor dem Inkrafttreten der DSGVO in seiner Entscheidung vom 28.7.2015 – VI ZR 340/14, Rn. 40, unter Heranziehung der Ausführungen von *Wybitul/Fladung*, BB 2012, 509, 511, ein „Recht auf Vergessenwerden“ unter dem Gesichtspunkt der Störerhaftung bestätigt (vgl. dazu mittlerweile auch Art. 17 DSGVO).

2. Rechtsgrundlagen für den Umgang mit Mitarbeiterdaten

Rechtsgrundlagen für den Umgang mit Mitarbeiterdaten sind aktuell nun vor allem neben der ursprünglich zentralen gesetzlichen Norm des § 26 BDSG, vor allem die Art. 6 ff. DSGVO und die Kollektivvereinbarungen.¹¹⁶ Insbesondere Art. 6 Abs. 1 lit. c DSGVO stellt auf rechtliche Verpflichtungen ab, denen der Verantwortliche unterliegt. Mit Art. 6 Abs. 1 (7) DSGVO hat der europäische Gesetzgeber eine Auffangnorm geschaffen, die auf das überwiegende Interesse abstellt, die im Rahmen von Compliance-Maßnahmen mit Beschäftigtendatenschutzbezug einer ausführlichen Abwägung durch den Verantwortlichen erforderlich macht, aber auch gerade auch ermöglicht.¹¹⁷ Die Einwilligung hat ihre Bedeutung in der Praxis nach allgemeiner Ansicht verloren, da diese nur noch in wenigen Fällen notwendig ist und verlässlichere gesetzliche Rechtsgrundlagen geschaffen wurden.

165

a) Kollektivvereinbarungen zur Nutzung von Mitarbeiterdaten

Kollektivvereinbarungen – wie beispielsweise Tarifverträge und Betriebsvereinbarungen – sind ausdrücklich genannte Rechtsgrundlagen i. S. d. Art. 88 Abs. 1 bzw. § 26 Abs. 4 BDSG¹¹⁸ und stellen in der Betriebspraxis zuverlässige Rechtsgrundlagen dar.¹¹⁹ Die Herausforderung besteht darin, die Anforderungen des Art. 88 Abs. 2 DSGVO zu erfüllen, der geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person u. Ä. erfordert. Tarifverträge regeln in den seltensten Fällen Fallkonstellationen, die auf den individuellen Bedarf des Betriebs zugeschnitten sind und bieten daher der Compliance-Abteilung kaum Handlungsspielraum für die Gestaltung der datenschutzrechtlichen Compliance. Ganz anders verhält es sich mit **Betriebsvereinbarungen**, die den gewohnten Handlungsrahmen eröffnen, wie ihn die Compliance-Abteilung z. B. bei der Implementierung des Compliance-Systems bereits nutzt.¹²⁰ Der Vorteil der Betriebsvereinbarung gegenüber der Einwilligung ist ihre Beständigkeit aufgrund ihrer Laufzeit und die Möglichkeit, zumindest alle nicht leitenden Mitarbeiter

166

116 Vgl. zur detaillierten Darstellung der Erlaubnisnormen die Ausführungen unter → Rn. 29.

117 Für den Umgang mit Gesundheitsdaten ist Art. 9 DSGVO relevant.

118 Infolge des EuGH-Urteils vom 30.3.2023 – C34/21 – ist nicht auszuschließen, dass der Verweis in § 26 Abs. 4 Satz 2 BDSG auf Art. 88 Abs. 2 DSGVO ebenfalls als unspezifische Regelung anzusehen ist, sodass § 26 Abs. 4 BDSG ebenso als europarechtswidrig einzustufen ist. Dies schließt jedoch Kollektivvereinbarungen und insbesondere Betriebsvereinbarungen als Regelungsinstrument damit nicht aus. Die Norm des Art. 88 Abs. 1 DSGVO ermöglicht Kollektivvereinbarungen unmittelbar, wenn die Bedingungen aus Art. 88 Abs. 1 und Abs. 2 DSGVO erfüllt sind. Das Recht Betriebsvereinbarungen zu schaffen, wird den Betriebsparteien vom Gesetzgeber bereits auf Basis des § 77 BetrVG gewährt.

119 Vgl. dazu auch die „Hinweise zur Regelung der Nutzung von Beschäftigtendaten“ unter → Rn. 216.

120 Vgl. dazu Ausführungen zu den Herausforderungen für das Personalmanagement, → Benkert, Kap. 4 Rn. 60 ff.

auf einmal zu erreichen (kollektive Wirkung). Dafür ist jedoch auch das Bestehen eines Betriebsrats erforderlich, der die beabsichtigten Regeln mitträgt, dafür aber de facto möglicherweise für sog. „Kompensationsgeschäfte“ nutzt.

- 167** Seit der Honeywell-Entscheidung des Bundesarbeitsgerichts¹²¹ ist bekannt, dass der Betriebsrat nach § 87 Abs. 1 Nr. 1 BetrVG mitzubestimmen hat, wenn der Arbeitgeber in einem Verhaltenskodex das Verhalten der Arbeitnehmer und die betriebliche Ordnung regeln will.¹²²
- 168** Eine Betriebsvereinbarung als Rechtsgrundlage zur Verarbeitung von Beschäftigtendaten findet dort ihre Grenzen, wo ein schwerwiegender Eingriff in das Selbstbestimmungsrecht des einzelnen Mitarbeiters geregelt werden soll. Maßnahmen, die den einzelnen Mitarbeiter im geschützten innersten Kern seiner Persönlichkeitssphäre betreffen, können durch eine Betriebsvereinbarung nicht legitimiert werden.¹²³ Eine Betriebsvereinbarung kann daher die Grenzen des geltenden Gesetzesrechts nicht unterschreiten, sondern lediglich die Anwendung in der Praxis ausgestalten.¹²⁴ Dies muss der Compliance-Verantwortliche gerade vor dem Hintergrund der regelkonformen Ausgestaltung des Compliance-Systems im Auge behalten. Dies betrifft auch den Umfang der Legitimierung des Datenumgangs. So wenig wie eine Generaleinwilligung in alle denkbaren datenschutzrelevanten Sachverhalte durch den Mitarbeiter erfolgen kann, so wenig kann eine Betriebsvereinbarung mittels Generalklausel den unbeschränkten Umgang mit Beschäftigtendaten regeln.
- 169** Das Verhältnis der Rechtsgrundlagen zueinander hat sich mit dem Inkrafttreten zudem grundlegend geändert. Sollte man früher noch Betriebsvereinbarung und Einwilligung nicht parallel für den gleichen Sachverhalt verwenden, ist dies heute möglich. Rechtmäßig ist eine Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO, wenn „mindestens“ einer der dort aufgeführten Erlaubnistatbestände erfüllt ist. Eine Datenverarbeitung lässt sich also auch auf mehrere Rechtsgrundlagen stützen. D.h., dass der Verantwortliche zusätzlich eine Einwilligung einholen darf, auch wenn bereits ein gesetzlicher Rechtsgrund einschlägig ist.¹²⁵

121 BAG, Beschl. v. 22.7.2008 – 1 ABR 40/07, BB 2008, 2520 mit BB-Komm. *Sittard*.

122 Das Mitbestimmungsrecht an einzelnen Regelungen begründet jedoch nicht notwendig ein Mitbestimmungsrecht am Gesamtwerk. Gleichwohl ist es empfehlenswert, das Gesamtwerk mit dem Betriebsrat zu besprechen, um die Akzeptanz der Regelungen in der Belegschaft zu steigern. Der Betriebsrat ist insoweit auch nicht unwesentlicher Teil der Compliance-Kommunikation. Vgl. zur Zusammenarbeit mit dem Betriebsrat auch die Ausführungen unter → Rn. 206 ff.

123 Z. B. Zwang zu einer Genomanalyse.

124 Dies ergibt bereits aus § 1 Abs. 3 BDSG, wonach das BDSG nur gegenüber Rechtsvorschriften des Bundes subsidiär ist.

125 Vgl. etwa die Ausführungen des Landesbeauftragten für Datenschutz Baden-Württemberg vom 19.10.2018, Einstieg ins Datenschutzrecht für behördliche Datenschutzbeauftragte, S. 26.

Daraus ergibt sich die Möglichkeit mit etwas Aufwand¹²⁶ eine erheblich größere Rechtssicherheit beim Umgang mit Beschäftigtendaten im Rahmen der Compliance-Arbeit zu gewinnen.

Neu zu gestaltende und bereits bestehende Betriebsvereinbarungen sind wegen des Anwendungsvorrangs der Verordnung an deren Standard anzupassen.¹²⁷ Folgende **Checkliste** soll die Umsetzung i. R. d. Betriebsvereinbarungen erleichtern: **170**

Checkliste zur Anpassung von Betriebsvereinbarungen nach der DSGVO: **171**

1. Schaffung eines datenschutzrechtlichen Ausnahmetatbestands deutlich machen
2. Schaffung eines Erlaubnistatbestandes hervorheben
3. Zulässigen Rückgriff auf andere Rechtsgrundlagen vereinbaren
4. Datenverarbeitung genau und transparent beschreiben
5. Rechte der betroffenen Personen und deren Geltendmachung beschreiben
6. Pflichten des für die Verarbeitung Verantwortlichen benennen
7. Umfangreiche Zweckbeschreibung vornehmen
8. Mögliche Zweckänderungen voraussehen
9. Datensicherheit und technische und organisatorische Maßnahmen beschreiben
10. geeignete Maßnahmen beschreiben ...
 - a) zur Wahrung der menschlichen Würde
 - b) zu den berechtigten Interessen
 - b) zur Sicherung der Grundrechte der betroffenen Personen

b) Rechtfertigende Einwilligung des Mitarbeiters

Gemäß der gesetzgeberischen Vorstellung ist eine wirksame Einwilligung das Instrument auf die das Erheben, Verarbeiten oder Nutzen personenbezogener Daten alternativ gestützt werden kann. Die Einwilligung als Unterfall der Zustimmung muss jedoch ein paar grundlegende Voraussetzungen für ihre Wirksamkeit erfüllen: **172**

Die Einwilligung muss zeitlich vor dem Erheben, Verarbeiten oder Nutzen eingeholt werden. Sie muss zudem freiwillig erfolgen, d.h. auf dem freien Willen des Betroffenen beruhen. Zusätzlich muss ein Hinweis auf den Zweck erfolgen und sie muss entsprechend deutlich hervorgehoben werden. Handelt es sich um besondere Arten von personenbezogenen Daten, so muss sich die Einwilligung auch auf solche besonderen Daten erstrecken. **173**

¹²⁶ So ist etwa darauf zu achten, dass der Betroffene über die verschiedenen Rechtsgrundlagen informiert wird.

¹²⁷ Vgl. die Ausführungen zur DSGVO unter → Rn. 8 ff.

- 174** Im Arbeitsverhältnis besteht eine besonders hohe Prüfpflicht hinsichtlich der Freiwilligkeit der Einwilligung.¹²⁸ Kritische Vertreter verneinen sogar die Möglichkeit der Einwilligung im Arbeitsverhältnis, da das Über-Unter-Ordnungsverhältnis zwischen Arbeitgeber und Arbeitnehmer einen freien Willen des Mitarbeiters generell ausschließen würde.¹²⁹ Die herrschende Auffassung geht jedoch unter strenger Prüfung davon aus, dass die Einwilligung auch im Arbeitsverhältnis zulässig ist. Dem trägt auch Art. 7 Abs. 4 DSGVO Rechnung, welcher unter Heranziehung eines Koppelungsverbots ebenfalls von der Zulässigkeit ausgeht.
- 175** Gleichwohl birgt die Einwilligung aufgrund ihrer jederzeitigen Widerruflichkeit Verlässlichkeitsrisiken, die der Compliance-Verantwortliche im Rahmen einer ständigen Überwachung im Fokus behalten muss.¹³⁰ Darüber hinaus sprechen die Dokumentationspflicht und die Notwendigkeit, im Streitfall die gewährte Einwilligung nachweisen zu können, dafür, diese schriftlich zu fixieren, auch wenn es dafür keine gesetzliche Pflicht gibt. Die Beweislast für erfolgte Einwilligung trägt insoweit der für die Verarbeitung Verantwortliche.
- 176** Die Wirksamkeitsvoraussetzungen der Einwilligung sind im Rahmen der Compliance-Arbeit demnach entsprechend abzufragen, zu prüfen und zu dokumentieren. Beispielsweise¹³¹ sind zu prüfen: Hat ein Personaler die entsprechenden schriftlichen Dokumente für die Einwilligung vorliegen? Wurde dem Mitarbeiter das Dokument im Vorfeld vorgelegt? Beruhte die Entscheidung auf dem freien Willen des Betroffenen?
- 177** Compliance prüft im Rahmen des sog. Datenschutz-Audits ab, inwieweit und bis zu welchem Grad die gesetzlichen Vorgaben und die Umsetzung der internen Richtlinien umgesetzt wurden. Dies kann im Einzelfall künftig als Anlass genommen werden, die jeweiligen Prozesse entsprechend anzupassen.

c) Arbeitsvertragliche Regelungsmöglichkeiten

- 178** Der Klassiker in Sachen Anhang zum Arbeitsvertrag findet für nicht-öffentliche Stellen kein ausdrückliches gesetzliches Pendant mehr im Gesetz.¹³² Gleichwohl sind Personen, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Die Dokumentationspflicht hinsichtlich des Datengeheimnisses leitet sich nun aus

128 EG 33 der DSGVO spricht von „echter Wahlfreiheit“.

129 Statt vieler: *Trittin/Fischer*, NZA 2009, 343.

130 Als verlässliche Alternative steht dem Arbeitgeber der Art. 6 Abs. 1 lit. f DSGVO zur Verfügung, wonach ein überwiegendes berechtigtes Interesse vorliegen muss. Über diese Rechtsgrundlage und die damit verbundene Verarbeitung muss der Arbeitnehmer jedoch ebenfalls ausreichend informiert werden.

131 Vergleiche weitere Beispielsfälle unter → Rn. 92 ff.

132 Eine solche Pflicht war auch für nicht-öffentliche Stellen ursprünglich in § 5 Satz 2 BDSG a. F. festgeschrieben. Die neue Regelung des § 53 BDSG zum Datengeheimnis ist hingegen für nicht-öffentliche Stellen nicht unmittelbar anwendbar.

Art. 5 Abs. 2 und Art. 32 Abs. 4 DSGVO ab.¹³³ Bisherige Verpflichtungen auf das Datengeheimnis müssen daher an die neuen Regelungen der DSGVO angepasst werden. Eine Fortwirkung des Datengeheimnisses – wie bisher in § 5 Satz 3 BDSG-alt geregelt – ist auch hier dringend angeraten. HR-Compliance überprüft im Rahmen des HR-Reviews, ob bei Einstellung entsprechende Dokumente vorgelegt werden und ob die Verpflichtung auf das Datengeheimnis bei Tätigkeitsaufnahme (Einstellung) in den Prozess integriert wird. Darüber hinaus muss dieser Prozess schriftlich dokumentiert werden. Der Mitarbeiter unterzeichnet die entsprechende Verpflichtung. Zudem wird ein Belegexemplar hierfür zur Personalakte abgelegt. Ein einfacher Vorgang, der jedoch im Rahmen von Audits auf Vollständigkeit hin abzurufen ist. Besteht hier eine Lücke im HR-Prozess, kann dies weitreichende Konsequenzen haben. Diese sind nicht immer unmittelbar zu spüren, können allerdings im Einzelfall zum Wettbewerbsnachteil werden. Sinn und Zweck dieser Regelung ist es, das Unternehmen und sein Know-how sowie alle Betriebsinterna zu schützen.¹³⁴

Letztlich geht es jedoch um weit mehr. Es ist die Verpflichtung jedes Einzelnen auf die Beachtung des gesetzlichen Verbots unbefugter Datenerhebung und -verwendung. Hiermit kommt zum Ausdruck, dass nicht nur der Verantwortliche zuständig ist, sondern auch jeder Beschäftigte. Die Verpflichtung auf das Datengeheimnis stellt für jeden Beschäftigten seine persönliche Verantwortung hinsichtlich der datenschutzrechtlichen Vorschriften beim Umgang mit personenbezogenen Daten dar.¹³⁵ Das Datengeheimnis ist aus Sicht der Compliance weit auszulegen. Hiermit fallen auch Praktikanten, freie Mitarbeiter, Leiharbeiter, ehrenamtliche Helfer und regelmäßig eingesetzte Dienstleister – wie beispielsweise das Reinigungspersonal – unter diese Verpflichtung. Wichtig im gesamten Prozessablauf ist, dass die Verpflichtung auf das Datengeheimnis bereits bei der Aufnahme der Tätigkeit erfolgt. Damit ist die Verpflichtung möglichst am ersten Arbeitstag vorzunehmen und in einem gesonderten Dokument festzuhalten und abzuzeichnen.¹³⁶

All diese Prozesse überprüft die HR-Compliance auf Vollständigkeit und Richtigkeit im Rahmen einer regelmäßigen und internen Kontrolle der Abteilun-

179**180**

133 Auch eine analoge Anwendung des § 53 BDSG ist denkbar, da eine vergleichbare Interessenlage zu den öffentlichen Stellen besteht und ein redaktionelles Versehen vor dem Hintergrund der aus der DSGVO bestehenden Dokumentationspflicht nicht auszuschließen ist.

134 Insoweit kann dieser Prozess auch die Maßnahmen nach dem GeschGehG bzw. aus der Know-how-Schutz-Richtlinie (EU) 2016/943 flankieren und ergänzen.

135 Vgl. das „Kurzpapier Nr. 19 Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO“ der Datenschutzkonferenz unter https://www.lda.bayern.de/media/dsk_kpnr_19_verpflichtungBeschaeftigte.pdf (Stand: 29.5.2018), S. 1.

136 Vgl. das „Kurzpapier Nr. 19 Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO“ der Datenschutzkonferenz unter https://www.lda.bayern.de/media/dsk_kpnr_19_verpflichtungBeschaeftigte.pdf (Stand: 29.5.2018), S. 2.

gen.¹³⁷ Neben den erwähnten Kontrollen ist den Mitarbeitern die Bedeutung dieser Vorschrift zu erläutern. Denn zur Verpflichtung gehört ebenso eine Belehrung in regelmäßigen Zeitintervallen.¹³⁸ Zusätzlich sollte im Rahmen interner Schulungsmaßnahmen die Bedeutung und Tragweite auch dieser Vorschrift erläutert werden, um sicherzustellen, dass nicht nur eine Verpflichtung auf dem Papier besteht. Nur gelebte Compliance kann insofern die Einhaltung von Vorschriften sicherstellen.

- 181** Nicht zu empfehlen ist hingegen die Regelung von Einwilligungen im Rahmen von Arbeitsverträgen. Spätestens mit Umsetzung der DSGVO sind alle Umstände zu vermeiden, die darauf schließen lassen könnten, dass die Einwilligung als Gegenleistung für die Einstellung oder eine sonstige Begünstigung vom Mitarbeiter verlangt wurde.¹³⁹

d) Gesetzliche Erlaubnistatbestände

- 182** Auch nach dem Inkrafttreten der DSGVO ist aus Perspektive der Compliance insbesondere § 26 Abs. 1 Satz 2 BDSG¹⁴⁰ als spezifischere Vorschrift gemäß Art. 88 DSGVO¹⁴¹ relevant, und zwar im Rahmen der Aufdeckung von Straftaten der Mitarbeiter. Dies bedeutet i. S. d. Wortlautes von § 26 BDSG, dass personenbezogene Daten eines Beschäftigten „zur Aufdeckung von Straftaten“ nur dann verarbeitet werden dürfen, wenn zu dokumentierende tatsächliche Anhaltspunkte hierbei einen Verdacht begründen können.
- 183** Bei Maßnahmen zur Aufdeckung konkreter, bereits begangener Straftaten kommt die speziellere Regelung des § 26 Abs. 1 Satz 2 BDSG zur Anwendung.¹⁴² Kontrollen der Leistung oder des Verhaltens der Mitarbeiter fallen grundsätzlich unter die allgemeinen Erlaubnisnormen der DSGVO oder werden

137 Vgl. auch HR-Review.

138 Vgl. das „Kurzpapier Nr. 19 Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO“ der Datenschutzkonferenz unter https://www.lda.bayern.de/media/dsk_kpnr_19_verpflichtungBeschaeftigte.pdf (Stand: 29.5.2018), S. 3.

139 So Art. 7 Abs. 4 DSGVO.

140 Auch vor dem Hintergrund des EuGH-Urteils vom 30.3.2023 – C-34/21 – (vgl. → Rn. 158 ff.) ist davon auszugehen, dass § 26 Abs. 1 Satz 2 BDSG eine spezifischere Regelung im Verhältnis zur DSGVO enthält, sodass dieser den Vorgaben aus Art. 88 Abs. 2 DSGVO grundsätzlich genügen dürfte. Auch enthält § 26 Abs. 1 Satz 2 BDSG eine konkrete Zweckbestimmung, sodass die Anwendbarkeit zumindest für Art. 6 Abs. 1 Satz 1 lit. c und/oder lit. e DSGVO über Art. 6 Abs. 3 DSGVO erhalten bleibt. Hier dürfte auch Art. 6 Abs. 3 Satz 4 DSGVO erfüllt sein, da die Wahrung des Betriebsfriedens durch die Aufdeckung von Straftaten ein übergeordnetes Interesse des Staates im Rahmen eines funktionierenden Wirtschaftslebens darstellt.

141 Als allgemeine Auffangvorschrift kommt insbesondere Art. 6 Abs. 1 lit. f DSGVO in Betracht, der die Erforderlichkeit zur Wahrung der berechtigten Interessen des Unternehmens in den Mittelpunkt stellt.

142 *Taeger/Gabel*, DSGVO BDSG, 3. Aufl. 2019, § 26 Rn. 68.

entsprechend durch Kollektivvereinbarungen geregelt.¹⁴³ Im Übrigen bietet Art. 6 Abs. 1 lit. f DSGVO hierzu einen Auffangtatbestand.

Unter Datenschutzexperten besteht die einhellige Auffassung, dass beide **184** Rechtsgrundlagen auch nach dem Inkrafttreten der DSGVO und der entsprechenden Anpassung des BDSG weiterhin reformbedürftig sind.¹⁴⁴ Der Gesetzgeber entschied sich dafür, die bisherigen Regelungen weitestgehend unverändert fortzuführen und der bestehenden Rechtsprechung zu § 32 BDSG-alt eine möglichst weite Fortgeltung zuzubilligen.¹⁴⁵ Damit bieten in Teilen die Regelungen des § 26 BDSG und vor allem des Art. 6 DSGVO aus Compliance-Sicht zunächst ausreichend Rechtssicherheit, um unter Wahrung der allgemeinen Datenschutzgrundsätze die wichtigsten Compliance-Maßnahmen gegenüber Mitarbeitern im Betrieb ergreifen zu können.¹⁴⁶

So können präventive Compliance-Maßnahmen wie ein Hinweisgeber-System **185** (z. B. unter Verwendung einer digitalen Hinweisgeberplattform) auf § 26 Abs. 1 Satz 2 BDSG oder auf Art. 6 Abs. 1 lit. f DSGVO beruhen.¹⁴⁷ Im Rahmen der Angemessenheitsprüfung sind die dem Unternehmen obliegenden Pflichten, welche der Gesetzgeber und die Rechtsprechung an das Unternehmen stellen, zu berücksichtigen. So sieht § 130 OWiG eine Pflicht der Unternehmensleitung zur Verhinderung von unternehmensbezogenen Straftaten u. Ä. vor. Gleichzeitig sind Mitarbeiter im Rahmen ihrer arbeitsrechtlichen Treuepflicht zur Einhaltung von Compliance-Standards verpflichtet. Ähnliche Argumentationen lassen sich auch für die Kontrolle von E-Mails der Mitarbeiter finden, auch wenn die Regelung durch Betriebsvereinbarung jeweils eindeutig vorzugswürdig ist.¹⁴⁸

Das für das Hinweisgeber-System einschlägige HinSchG¹⁴⁹ berührt mit dem dort **186** geregelten Vertraulichkeitsgebot einen Kernbereich des Datenschutzes, da die Identität des Hinweisgebers allein den Personen bekannt werden darf, die für die Entgegennahme von Meldungen oder für das Ergreifen von Folgemaßnahmen zuständig sind, sowie den sie unterstützenden Personen. Es darf insbesondere

143 *Taegeer/Gabel*, DSGVO BDSG, 3. Aufl. 2019, § 26 Rn. 41.

144 Der Gesetzgeber hätte mit der Anpassung des BDSG die Chance gehabt, die bereits seit 2009 bestehenden und bekannten Unsicherheiten im Umgang mit diesen Bestimmungen zu beseitigen. Zudem kritisierten die Aufsichtsbehörden der Länder in einer gemeinsamen Entschließung bereits rechtzeitig vor der Anpassung des BDSG-alt an die DSGVO, dass die getroffenen Regelungen voraussichtlich nicht europarechtskonform seien.

145 Vgl. die Gesetzesbegründung in BT-Drs. 18/11325, S. 96 f. Der Gesetzgeber hat sich aber vorbehalten, konkretere Vorschriften zum Beschäftigtendatenschutz zu erlassen.

146 Vgl. dazu auch den Beispielsfall unter → Rn. 232 ff.

147 Vgl. die „Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz“ der Datenschutzkonferenz unter https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf (Stand: 14.11.2018).

148 Vgl. dazu auch die Hinweise zur Regelung der Nutzung von Internet und E-Mail unter → Rn. 222 ff.

149 Vgl. zum HinSchG die allgemeinen Ausführungen → *Block/Sonnenberg*, Kap. 5.

kein allgemeiner Zugriff auf die übermittelten Nachrichten möglich sein.¹⁵⁰ Erlaubnisnorm für die Verarbeitung von personenbezogenen Daten durch die interne Meldestelle ist zunächst § 10 HinSchG. Aufgrund der in der Praxis häufig vorkommenden Unsicherheit, ob die von der hinweisgebenden Person übermittelten Informationen tatsächlich zur Erfüllung der Aufgaben durch die Meldestelle erforderlich sind, empfiehlt es sich, neben der Implementierung einer entsprechenden Hinweisgeber-Richtlinie eine Betriebsvereinbarung zu schaffen, die eine entsprechende Erlaubnisnorm enthält. Dies gilt insbesondere bei Einführung und Nutzung einer digitalen Hinweisgeberplattform, die zahlreiche Funktionen vorsehen kann, die über das gesetzliche Erfordernis hinausgeht.

187 Checkliste zu den datenschutzrechtlichen Anforderungen an ein Hinweisgeber-System:

1. Risikoanalyse in Form einer Datenschutz-Folgenabschätzung (DSFA)
2. Frühzeitige Einbindung des Datenschutzbeauftragten
3. Betroffeneninformation für Hinweisgeber (Transparenz)¹⁵¹
4. Zugriffskonzept zur Sicherstellung des Vertraulichkeitsgebots
5. Datensicherheit: geeignete technische und organisatorische Maßnahmen
6. Aufbewahrungs- bzw. Löschfristen müssen festgelegt werden
7. Der Prozess über den internen Meldekanal muss im Verzeichnis der Verarbeitungstätigkeiten (VVT) aufgenommen werden
8. Gemeinsame Verantwortlichkeit bei interner Meldestelle im Konzernverbund¹⁵²
9. Auftragsverarbeitungsvertrag (AVV) bei Beauftragung externer Dienstleister

¹⁵⁰ Abgesehen von den Ausnahmeregelungen nach § 9 HinSchG.

¹⁵¹ Verfahren zur Meldung von Missständen haben sicherzustellen, dass Hinweise regelmäßig vertraulich bzw. anonym erfolgen. Daher kann die Informationspflicht nach Art. 14 DSGVO gegenüber dem Beschuldigten nur beschränkt erfüllt werden. Werden personenbezogene Daten für die Meldung von Missständen ohne Kenntnis des Beschuldigten erhoben, ist dieser grundsätzlich insbesondere über die Speicherung, die Art der Daten, die Zweckbestimmung und die Identität des Verantwortlichen zu informieren. Wenn das Risiko erheblich ist, dass eine solche Unterrichtung die Fähigkeit des Unternehmens zur wirksamen Untersuchung des Vorwurfs oder zur Sammlung der erforderlichen Beweise gefährden würde, kann die Information der beschuldigten Person so lange aufgeschoben werden, wie diese Gefahr besteht. Spätestens in Gerichtsverfahren hat die betroffene Person ein Auskunftsrecht, um ihre Rechtsverteidigung zu ermöglichen (vgl. LAG Baden-Württemberg, Urt. v. 20.12.2018 – 17 Sa 11/18; vgl. dazu die Ausführungen unter den → Rn. 239 ff.).

¹⁵² Gesellschaften eines Konzerns werden datenschutzrechtlich von der DSGVO als Dritte behandelt, d. h. personenbezogene Daten dürfen nur auf Basis einer eigenen Rechtsgrundlage übermittelt werden. Der Datenschutz muss zwischen den Konzernunternehmen durch einen gesonderten Vertrag sichergestellt werden. Bei einer gemeinsamen Meldestelle ist dies regelmäßig eine Vereinbarung zur gemeinsamen Verantwortlichkeit gemäß Art. 26 DSGVO.

e) Internationaler Datenverkehr mit Beschäftigtendaten

Der internationale Datenverkehr ist auch hinsichtlich der Übertragung von Beschäftigtendaten kaum wegzudenken. In multinationalen Unternehmen sitzen personaldatenverarbeitende Stellen nur in seltenen Fällen im selben Land wie die Mitarbeiter selbst. So funktionieren bspw. globale Personalmanagement-Systeme nur durch Übertragung der Beschäftigtendaten.

188

In der Gesamtschau bleibt festzuhalten, dass eine Übermittlung von personenbezogenen Daten in ein Drittland, für das kein Angemessenheitsbeschluss nach Art. 45 Abs. 3 DSGVO vorliegt, immer einer Rechtsgrundlage bedarf, Art. 46 ff. DSGVO. Dies können sein:

189

- die Einwilligung durch die Betroffenen: praktisch kaum umsetzbar; General-einwilligungen sind ausgeschlossen.
- Binding Corporate Rules: Die sog. BCR sind nach dem europäischen Gesetzgeber erste Wahl und unter engen Voraussetzungen durch die DSGVO umsetzbar; in der Regel langwierige Abstimmung mit der Behörde notwendig.
- EU-Standardvertragsklauseln: Auch hier wird die Datenschutzbehörde prüfen müssen, ob die vom EuGH aufgestellten Grundsätze gewahrt sind.¹⁵³
- EU-US Data Privacy Framework: Aktueller Maßstab für die Übermittlung in die USA ist derzeit das sog. EU-US Data Privacy Framework („DPF“). Der Nachfolger des ursprünglichen EU-US Privacy Shield bzw. des Safe-Harbor-Abkommens soll den Schutz europäischer Daten bei zertifizierten US-amerikanischen Unternehmen sicherstellen. Die EU-Kommission hat mit Beschluss vom 10.7.2023¹⁵⁴ entschieden, dass unter dem Selbstzertifizierungsmechanismus des DPF ein angemessenes Datenschutzniveau für Datenübermittlungen in die USA besteht. Hiermit besteht erneut die Vorgabe für US-Unternehmen, einen Selbstzertifizierungsmechanismus durchzuführen. Nur für US-Organisationen, die über das Department of Commerce (DoC) in eine sog. „Data Privacy Framework List“ (DPF-List) eingetragen sind, besteht ein angemessenes Datenschutzniveau. Zusätzlich gelten für die Übermittlung von Beschäftigtendaten besonders enge Abstimmungsvoraussetzungen zwischen Übermittler und Empfänger; bei sensiblen Daten werden besondere Organisationsstrukturen gefordert. Auch hier gelten die Anforderungen nach Art. 5 Abs. 2 DSGVO. Weiterhin ist eine entsprechende die Übermittlung umspannende vertragliche Regelung notwendig. Diese sollte zur Rückgabe bzw. Löschung der Daten verpflichten, sofern das Unternehmen in den USA von der DPF-List genommen und ihm damit die Zertifizierung entzogen wird. Empfehlenswert ist damit insbesondere eine jährlich fällige Erneuerung der Zertifizierung. So-

153 Nach Ansicht des EU-Generalanwalts im Vorabentscheidungsersuchen C-311/18 obliege es den EU-Datenschutzbehörden, im Einzelfall zu überprüfen, ob es in den Zielländern Mängel im Datenschutz gibt.

154 Vgl. Durchführungsbeschluss (EU) 2023/1795 der Kommission v. 10.7.2023 über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA.

lange die Zertifizierung besteht, bedarf es keiner weiteren Standarddatenschutzklauseln, keines Transfer Impact Assessments (TIA) und keiner weiteren Datenschutzgarantien. Allerdings muss eine Rechtsgrundlage für den Datentransfer losgelöst vom Drittlandsbezug bestehen.¹⁵⁵ Die Entscheidung der EU-Kommission bedeutet damit erneut nicht, dass für die USA allgemein ein angemessenes Datenschutzniveau festgestellt wurde. Die Entscheidung der EU-Kommission zum neuen Framework gilt unter der Maßgabe von Art. 45 Abs. 9 DSGVO fort. Es bleibt weiterhin auch hier abzuwarten, ob das neue Framework ähnlich wie das Privacy Shield gegenüber einer künftigen und neuerlichen EuGH-Entscheidung Bestand hat.¹⁵⁶ Vor diesem Hintergrund kann es dennoch ratsam sein, ggf. über das Instrument der Standarddatenschutzklauseln oder der Binding Corporate Rules einen sichere Datenübermittlung zu gewährleisten.

- 190** Compliance muss im Rahmen von internen Prüfungen in Zusammenarbeit mit dem jeweiligen DSB nachhalten und prüfen, wo Anpassungsbedarf besteht und wie hoch die jeweiligen Risiken einzuschätzen sind. Die Sachverhalte, Änderungen zu Verträgen, Kooperationen etc. müssen im Sinne von Compliance dokumentiert, nachgehalten und aktualisiert werden, um das entsprechende Schutzniveau gewährleisten zu können, welches nach aktuellem Stand verlangt wird.
- 191** Bis zur abschließenden Klärung der Zulässigkeit der Übermittlung von Beschäftigtendaten sind folgende Vorsichtsmaßnahmen zu ergreifen:
- Datenübertragung in die USA so weit wie möglich minimieren;
 - nach Möglichkeit Technik mit europäischen Servern verwenden;
 - laut Art. 29-Datenschutzgruppe: Standardvertragsklauseln oder BCR verwenden;
 - ergänzend Business-Partner-Compliance: Zertifikate vorweisen lassen.
- 192** Ein Untätigbleiben von Seiten des internen DSB ist hier ein Anlass für den Compliance Officer, tätig zu werden und in Rücksprache mit den jeweiligen Fachabteilungen zu treten. Dies belegt umso mehr, dass der DSB und der Compliance Officer ein gemeinsames Interesse daran haben müssen, auf ein einheitliches Datenschutzniveau hinzuwirken.

3. Risiken beim Umgang mit Beschäftigtendaten

- 193** Es wird zu jeder Zeit, d. h. in jeder Phase des Kontakts zum (künftigen) Mitarbeiter ein gesetzeskonformer Umgang mit seinen personenbezogenen Daten gefordert. Das Unternehmen ist damit sowohl bei der Gewinnung und Speicherung von Bewerberdaten, während des Anstellungsverhältnisses und auch im Anschluss daran an die entsprechenden Vorgaben aus Gesetz und Rechtsprechung

¹⁵⁵ Vgl. die FAQ zum Angemessenheitsbeschluss der EU-Kommission zum EU-US Data Privacy Framework (EU-US DPF) der GDD vom 26.7.2023.

¹⁵⁶ Das EU-US-Privacy-Shield sieht sich trotz Nachbesserungen ganz ähnlicher Kritik ausgesetzt wie das Safe-Harbor-Abkommen, das mit EuGH-Urteil vom 6.10.2015 gekippt wurde.

gebunden. Zu jeder Phase bedeutet im üblichen „Unternehmenswording“: Beim Boarding, On Board und Off Boarding gibt es spezielle unternehmerische Risiken, die nicht nur den Umgang mit Unternehmensdaten, sondern auch mit personenbezogenen Daten betreffen können.

a) Phase 1: Begründung des Arbeitsverhältnisses/„Boarding-Phase“

Gewinnung von Bewerberdaten und Informationen: Über § 26 Abs. 8 BDSG ist auch noch mal klargestellt, dass Bewerber „Beschäftigte“ im Sinne dieser Vorschrift sind. Bei der Gewinnung von Bewerberdaten kann der Arbeitgeber alle ihm öffentlich zugänglichen Daten nutzen.¹⁵⁷ **194**

Risikobereich: Risikobelastet sind die Bereiche, die als sog. Grauzone dem Arbeitgeber so nicht zugänglich sind und beispielsweise im Raum des Web 2.0 gewonnen werden. Dies betrifft vor allem Informationen, von denen der Bewerber im Zweifel nicht möchte, dass sie bekannt werden. Bei Daten aus Social Media ist daher zu differenzieren. Wenn private Beziehungen im Vordergrund stehen (z. B. Facebook, Instagram) ist die Verarbeitung nicht zulässig, während die aus berufsbezogenen Netzwerken (z. B. XING und LinkedIn) erhobenen Daten genutzt werden dürfen.¹⁵⁸ **195**

Gesetzliche Vorgaben: Die gesetzlichen Vorgaben sind hier vor allem der DSGVO, dem BDSG, dem Wettbewerbsrecht, dem AGG und den Grundsätzen zum Fragerecht des Arbeitgebers im Bewerbungsprozess zu entnehmen. **196**

Praxistipp

Das bisher geltende Prinzip der Direkterhebung bei der betroffenen Person (§ 4 Abs. 2 BDSG a. F.) hat der europäische Gesetzgeber nicht normiert. Der Betroffene muss nach Art. 14 DSGVO jedoch über die Verarbeitung der Daten informiert werden. Dies ist ein wesentliches Mittel zur Sicherstellung der Transparenz beim Umgang mit personenbezogenen Daten. Dies entspricht auch einem compliance-konformen Umgang mit Daten im Bewerberprozess. **197**

b) Phase 2: Durchführung des Arbeitsverhältnisses/„On Board-Phase“

Umgang mit personenbezogenen Daten im Beschäftigtenverhältnis: Dem Arbeitgeber muss es möglich sein, die für die Durchführung des Arbeitsverhältnisses erforderlichen Daten zu erheben und zu verarbeiten (also Name, Alter, Beruf, sonstige Qualifikationen und Einsatzfähigkeit). Dazu gehören auch Beschäftigtendaten, die zwar zurzeit noch nicht von Bedeutung sind, die es aber **198**

¹⁵⁷ *Taege/Gabel*, DSGVO BDSG, 3. Aufl. 2019, § 26 Rn. 32. Ohne einen Zweck und eine ausreichende Transparenz ist aber auch dann die Verarbeitung von Daten nicht zulässig. Im Übrigen gilt die Erforderlichkeitsprüfung.

¹⁵⁸ Insoweit ist aber eine Kontaktaufnahme unter Vorspiegelung falscher Tatsachen untersagt. Vgl. *Taege/Gabel*, DSGVO BDSG, 3. Aufl. 2019, § 26 Rn. 32.

werden könnten. Nicht verwendet werden dürfen Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse¹⁵⁹ oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben.

- 199 Risikobereich:** Die Grenzen der zulässigen Verarbeitung von Beschäftigtendaten sind vor allem bei der internen Ermittlung von Sachverhalten¹⁶⁰ mit Personenbezug und mit Bezug zu den Gesundheitsdaten der Mitarbeiter zu beachten. Letztere kommen immer auch dann ins Spiel, wenn die Einsatzfähigkeit der Mitarbeiter fraglich ist. Die DSGVO sieht insoweit eine Erleichterung vor, als dass diesbezügliche Eignungstests ausdrücklich erlaubt sind, soweit diese für die Personalplanung und Beschäftigung erforderlich sind.
- 200 Gesetzliche Vorgaben:** Grundlage des Umgangs mit Beschäftigtendaten im Arbeitsverhältnis stellt § 26 BDSG dar. Untergesetzliche Bestimmungen zur Ermittlung der Einsatzfähigkeit der Mitarbeiter (z.B. Vorgaben der Berufsgenossenschaften zum G25-Eignungstest o.Ä.) können lediglich Rechtfertigungshilfe, nicht aber Rechtsgrundlage sein.

201 Praxistipp

Aufgrund der Reformbedürftigkeit des Beschäftigtendatenschutzes – insbesondere der Regelungen des § 26 BDSG – sind sämtliche datenschutzrechtlichen und Compliance-relevanten Vorgänge umfassend und auch für Dritte nachvollziehbar zu dokumentieren. Die Datenschutzaufsichtsbehörden der Länder legen Wert darauf, dass die Grundsätze des Datenschutzes eingehalten werden und vor allem die erforderlichen Abwägungen der Interessen nachvollzogen werden können.

c) Phase 3: Beendigung des Arbeitsverhältnisses/„Off Boarding-Phase“

- 202 Ausscheidungsprozess des Mitarbeiters:** Dem Arbeitgeber muss es gerade vor dem Hintergrund der Anforderungen des KSchG möglich sein, die kündigungsrelevanten Sachverhalte nicht zuletzt auch vor Gericht vortragen zu können. Die im Zusammenhang mit dem Beschäftigungsverhältnis stehenden Beschäftigtendaten muss der Arbeitgeber daher speichern dürfen. Dies gilt auch für sämtliche Daten, die im Rahmen eines Interessenausgleichs und Sozialplans erforderlich sind.
- 203 Risikobereich:** Die Grenze stellt wie üblich auch hier die Erforderlichkeit dar. Aufbewahrungsfristen ergeben sich aus zahlreichen anderen Gesetzen. Bedeutsam ist hier zumeist auch das AGG, das einen sog. Entschädigungsanspruch des ehemaligen Mitarbeiters bis zu zwei Monate nach Ausscheiden vorsieht. Auch

¹⁵⁹ Ausnahme: Konfession für die Abführung von Kirchensteuern aufgrund gesetzlicher Regelungen.

¹⁶⁰ Vgl. dazu den Beispielsfall „zur Kontrolle bei Verdacht gegen Mitarbeiter“ unter → Rn. 232 ff.

dagegen muss sich das Unternehmen wehren können, sodass hier ein Interesse an der Aufbewahrung der Beschäftigtendaten besteht. Gleichzeitig muss hier das Risiko der zeitlich darüberhinausgehenden Speicherung von Beschäftigtendaten eingedämmt werden. Dies erfordert ein umfassendes Löschmanagement. Dieses wurde noch durch Ansprüche auf Beseitigung von Suchergebnissen in Suchmaschinen erweitert (sog. Recht auf Vergessenwerden; Art. 17 DSGVO).

Gesetzliche Vorgaben: Neben der Löschpflicht aus Art. 17 DSGVO bestehen zahlreiche auch steuerrechtliche Aufbewahrungspflichten. Das AGG und das KSchG bilden dazu einen weiteren Rahmen.

204

Praxistipp

Schon während der Aussteuerungsphase des Mitarbeiters sollte ein Augenmerk auf den künftigen Umgang mit den Daten des ausscheidenden Mitarbeiters gelegt werden. Die Rechtsprechung flankiert diese Überlegungen durch zahlreiche Ansprüche auf Löschung und Beseitigung bis hin zur Eliminierung der Daten aus den sozialen Netzwerken.

205

4. Zusammenarbeit mit dem Betriebsrat

Beim Umgang mit Beschäftigtendaten spielt der Betriebsrat eine maßgebliche Rolle. So ist er natürlich zunächst den Interessen der Mitarbeiter verpflichtet und damit nicht zuletzt auch dem Schutz der Persönlichkeitsrechte als Ausfluss des Datenschutzes.

206

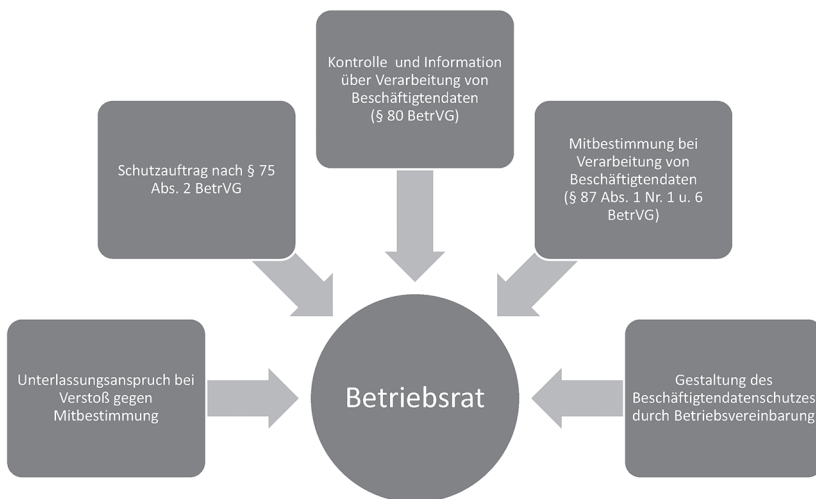


Abbildung 6: Der Betriebsrat im Datenschutzsystem

- 207** Des Weiteren ermöglicht eine vertrauensvolle Zusammenarbeit mit dem Betriebsrat auch die Schaffung von Regelwerken, die es erst ermöglichen, ein datenschutzrechtlich intaktes Compliance-System zu betreiben. Um eine solche Zusammenarbeit unter Hinzuziehung der Personalabteilung zu erreichen, muss man zunächst verstehen, welche Stellung der Betriebsrat datenschutzrechtlich im Betrieb einnimmt. Es ist zunächst zu beachten, dass mit Einführung des § 79a BetrVG der Arbeitgeber der für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften ist, soweit der Betriebsrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet.¹⁶¹ Damit trägt der Arbeitgeber die Haftung für die Datenverarbeitung des Betriebsrats. Bei der Verarbeitung personenbezogener Daten hat der Betriebsrat zwar die Vorschriften über den Datenschutz einzuhalten und die Betriebsparteien sollen sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften unterstützen, jedoch ist der Datenschutzbeauftragte gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet über Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen. Damit ist eine Kontrolle des DSB durch den Betriebsrat wesentlich erschwert, wenn nicht sogar in der Praxis nahezu unmöglich gemacht. Dieses Dilemma der Haftung ohne Kontrollmöglichkeit lässt sich nach einhelliger Meinung lediglich durch eine klarstellende Betriebsvereinbarung beseitigen, in der die wechselseitigen Unterstützungsaufgaben insbesondere hinsichtlich der datenschutzrechtlichen Pflichten des Betriebsrats ausreichend konkretisiert werden. Aufgrund des Umstands, dass der Betriebsrat zudem eine eigene Datenschutzorganisation (Datensicherungspflicht, Verpflichtung auf Datengeheimnis, Löschmanagement etc.) vorzuhalten hat, lassen sich diese beiden Aufgabengebiete miteinander kombinieren. Die Datenschutzorganisation ist einem entsprechenden Datenschutzkonzept zu dokumentieren.¹⁶²
- 208** Eine vertrauensvolle Zusammenarbeit mit dem Betriebsrat bietet zudem die Chance, dass Compliance- und Datenschutzregeln auf eine viel größere Akzeptanz in der Belegschaft treffen. Der Betriebsrat trägt seine Auffassung vom Compliance-System als Kommunikator zu den von ihm vertretenen Mitarbeitern. Eine stichhaltige Argumentation und ein rechtzeitiges Einbeziehen in ein-

161 Die Aufsichtsbehörden der Bundesländer haben sich dafür entsprechend ausgesprochen. Allen voran vertritt dies der Landesbeauftragte für Datenschutz und Informationssicherheit Baden-Württemberg in seinem Tätigkeitsbericht für das Jahr 2018 explizit; vgl. den „Tätigkeitsbericht Datenschutz 2018“ unter <https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/02/LfDI-34.-Datenschutz-Tätigkeitsbericht-Internet.pdf> (zuletzt abgerufen am 19.3.2024). Diese Ansicht lässt sich u. a. aus der Definition des Verantwortlichen nach Art. 4 Abs. 7 DSGVO ableiten, der regelt, dass jede „natürliche oder juristische Person [...], die allein oder mit andern über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“ verantwortlich ist.

162 Laut Beschluss des LAG Baden-Württemberg vom 20.5.2022 – 12 TaBV4/21 – darf der Arbeitgeber ohne bestehendes Datenschutzkonzept des Betriebsrats diesem auch keine Daten übermitteln.

zelne Compliance-Maßnahmen und Planungen sind daher unabdingbar. Die Grenze eines wohlwollenden Miteinanders zwischen Arbeitgeber und Betriebsrat ist natürlich dann überschritten, wenn ein Betriebsratsmitglied begünstigt wird.

5. Personalleiter und Betriebsrat als Teil des Datenschutz- und Compliance-Teams

Der Personalbereich als Kernbereich eines Unternehmens mit seinen Verknüpfungen zu allen internen Prozessen, kann kaum losgelöst von den anderen Unternehmensbereichen agieren. **209**

In der Gesamtorganisation steht der Personalbereich mit seinem Personalleiter schon durch das BetrVG in unmittelbarer rechtlicher Verknüpfung. Dieses Gesetz verknüpft die Teilbereiche Personal und Betriebsrat nicht zuletzt aufgrund von Mitbestimmungsrechten und Informationspflichten. Darüber hinaus sind diese eben genannten Teilbereiche als Bereiche von Arbeitgeberseite und Arbeitnehmerseite datenverarbeitende und prozesslastige Themenfelder. In vielen Fällen wird es in der Praxis zu inhaltlichen Überschneidungen oder gar Problemstellungen kommen, die nur in der Gesamtschau zu lösen sind. Dies bedeutet, dass der Personalbereich und der Betriebsrat als Teil des Datenschutz- und Compliance-Teams fungieren müssen. **210**

Dennoch kann gesagt werden, dass selbstverständlich jeder Fachbereich eine eigene Perspektive und Interessen vertritt. Dies erschwert natürlich die Zusammenarbeit in ganz praktischer Hinsicht. Jedoch hat jeder hier genannte Fachbereich seine eigene Berechtigung hierfür: **211**

1. Personalwesen: Organisation und Koordination der Mitarbeiter im Unternehmen
2. Betriebsrat: Interessenvertretung der Mitarbeiter – für AT evtl. Sprecherausschuss
3. Datenschutz: Organisation und Koordination von Datenschutz im Unternehmen (Umgang mit personenbezogenen Daten) – Hinwirken auf Datenschutzkonformität
4. Compliance: Organisation, Koordination und Kontrolle (Audit) von Prozessen im Unternehmen (hier gibt es je nach Perspektive und Aufbau der Compliance-Abteilung unterschiedliche Aufgaben. Vorliegend ist die wohl übliche Aufgabenteilung beschrieben).

Diese Auflistung macht deutlich, in welchem Lager die einzelnen Abteilungen stehen können. Die folgende Darstellung ist eine mögliche Perspektive und Abgrenzung der einzelnen Bereiche zueinander. **212**

Sehr eindeutig sind der Betriebsrat sowie der Bereich Datenschutz aufseiten der Mitarbeiter einzuordnen. Der DSB betreibt letztlich Persönlichkeitsrechtsschutz, der Betriebsrat schützt die Rechte der Arbeitnehmer im Allgemeinen und setzt sich logischerweise auch für den Arbeitnehmerdatenschutz ein. Der **213**

DSB ist auf Grundlage von Art. 33 DSGVO (sog. Datenschutzverletzung) verpflichtet, die zuständige Aufsichtsbehörde und die Betroffenen zu informieren (vgl. dazu auch → Rn. 106f.). Dies ist der Fall, wenn die Daten unrechtmäßig zur Kenntnis gelangt sind und schwerwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt sind. Allein diese Regelung macht deutlich, dass der DSB im Zweifelsfall auch nicht zugunsten des Unternehmens handeln kann. Er fungiert hier teilweise als verlängerter Arm der staatlichen Aufsichtsbehörde. Der Staat stellt hiermit weitere sog. Schutzbeauftragte ab: die Aufsichtsbehörden i. S. v. Art. 51 DSGVO i. V. m. § 40 BDSG und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), § 8 BDSG. Die jeweiligen Landesbehörden prüfen in ihrem Rahmen, ob die Ausführung der datenschutzrechtlichen Anforderungen eingehalten wird. Der BfDI überwacht bei Bundesbehörden, anderen öffentlichen Stellen des Bundes sowie bei Telekommunikations- und Postdienstunternehmen die Einhaltung des Datenschutzes und setzt dies durch (Art. 57 DSGVO, § 14 BDSG). Er kontrolliert zudem die Einhaltung des Datenschutzes bei der Durchführung von Sicherheitsüberprüfungen nach dem Sicherheitsüberprüfungsgesetz (SÜG) des Bundes, auch soweit sie private Unternehmen betreffen.

- 214** Im Falle der Compliance-Abteilung ist dies etwas anders zu beurteilen. Hier ist grundsätzlich alles in privater Hand. Selbstverständlich kann eine derartige Meldepflicht i. S. d. oben erwähnten BDSG auch für den Compliance-Bereich gelten, sofern für den Einzelfall hierzu eine Verpflichtung besteht; beispielsweise im Falle der Strafverfolgung nach dem StGB, da andernfalls ein Unterlassen seitens der Compliance-Abteilung bestünde. Dennoch kann gesagt werden, dass der Compliance Officer im Lager des Unternehmens steht und grundsätzlich alle präventiven Maßnahmen ergreifen wird, damit es nicht zu einer sog. „red flag“ kommt. Er wägt Risiken ab und berät die Geschäftsleitung in Fragen der Haftung. Den Compliance Officer trifft vielmehr eine Dokumentations- und Beweispflicht im Auftrag der Geschäftsleitung.
- 215** Dies gilt ebenso im Personalbereich. Er ist als „Organ“ der Geschäftsleitung und des gesamten Unternehmens zu sehen und führt letztlich die berechtigten Interessen¹⁶³ aus.

6. Hinweise, Muster und Beispielfall

a) Hinweise zur Regelung der Nutzung von Beschäftigtendaten

- 216** Die betriebsinterne Nutzung von Beschäftigtendaten sollte genauestens in einer eigenen Betriebsvereinbarung zum Datenschutz im Unternehmen geregelt sein.

¹⁶³ Dies können u. a. sein: personalpolitische Ziele, wie Gleichbehandlungsgrundsätze oder internationale Ausrichtung des Unternehmens, Förderung von Elternzeit für werdende Väter etc. sowie Kündigungsmaßnahmen im Rahmen von betriebswirtschaftlichen Entscheidungsprozessen.

Dabei versteht es sich von selbst, dass darin weder allein der Gesetzestext wiederholt noch reine Schutzbehauptungen zur Einhaltung des BDSG enthalten sein sollten. Betriebsvereinbarungen geben dem Betrieb die Möglichkeit, die gesetzgeberischen Freiräume zu nutzen und eigene Rechtsgrundlagen zu schaffen. Diese sollten dabei soweit wie möglich an den Grundsätzen des Datenschutzes orientiert sein.

Gemäß § 77 Abs. 4 Satz 1 BetrVG gelten Betriebsvereinbarungen unmittelbar und zwingend. Damit können Betriebsvereinbarungen den bestehenden Arbeitsvertrag modifizieren. Nach ständiger Rechtsprechung des BAG gilt sogar Folgendes: Wenn mit einer Betriebsvereinbarung nicht gegen grundlegende datenschutzrechtliche Prinzipien verstoßen wird, kann diese nach Art. 88 Abs. 1 DSGVO i.V.m. § 26 Abs. 4 Satz 1 BDSG das Verarbeiten von personenbezogenen Daten rechtfertigen. **217**

Bei einer Betriebsvereinbarung sollten stets folgende Fragestellungen im Zusammenhang mit der DSGVO und dem BDSG geprüft werden: **218**

- Welche Inhalte regelt die BV?
- Für wen gilt die BV? Welchen Geltungsbereich hat die BV?
- Steht die BV im Widerspruch zum Datenschutz (BDSG bzw. DSGVO) und zu datenschutzrechtlichen Grundprinzipien?
- Greifen die enthaltenen Regelungen in unverhältnismäßiger Weise in das Persönlichkeitsrecht des Betroffenen (hier: Arbeitnehmer) ein?
- Sind die Vorgaben des Art. 88 Abs. 2 DSGVO gewahrt (Menschenwürde, berechnigte Interessen, Grundrechte)?
- Soll die BV eine eigene Rechtsgrundlage bilden?
- In welchem Verhältnis steht die BV zu anderen Rechtsgrundlagen?
- Welche Verarbeitungszwecke sollen erfasst sein?
- Soll eine Datenübermittlung innerhalb der Unternehmensgruppe ermöglicht werden?
- Soll die Möglichkeit der Überwachung erlaubt werden?
- Welche Wirkung hat die BV für Regelungen aus der Vergangenheit?

Im Ergebnis hilft eine gut ausgestaltete Betriebsvereinbarung auch dem Personal, alle Schritte im Arbeitsverhältnis rechtlich einwandfrei einzuordnen und entsprechend vertraglich zu gestalten. Compliance kann hieran anknüpfen und entsprechend den Personalbereich auf die Einhaltung der gesetzlichen Vorgaben (und auch Umsetzung) überprüfen. Darüber hinaus ist Compliance für seine eigene Tätigkeit verpflichtet, die Vorschriften der DSGVO und des BDSG einzuhalten und nur insbesondere nach dem Grundsatz der Datensparsamkeit zu agieren. Für die Praxis heißt das: Daten nur zweckgebunden zu erheben und möglichst wenig Daten zu erheben. **219**

Dies stellt für die Praxis oftmals ein Problem dar. Die Compliance-Abteilung ist meist im Zusammenhang mit internen Prüfungen dazu angehalten, entsprechendes Beweismaterial zu sichern und zu dokumentieren. In vielen Fällen kann dies **220**

umgangen werden, indem die jeweilige Abteilung zu einem bestimmten Testlauf verpflichtet wird und die Auswertungen dann verschlüsselt als Beleg an die Compliance-Abteilung weitergibt.

- 221** In vielen Audit-Bereichen geht es nicht darum, dass eine bestimmte Person etwas getan hat, sondern darum, ob bestimmte Prozesse und Prozessabläufe eingehalten werden. Damit ist das Verarbeiten von personenbezogenen Daten hinfällig. Die jeweiligen Prüfungen sollten – egal ob intern oder extern ausgeführt – möglichst prozess- und inhaltsorientiert ausgerichtet sein. Nur so ist es auch Compliance möglich, datenschutzfreundlich zu prüfen und die strengen Vorgaben einzuhalten. Für den Fall, dass ein Gesetz eine Berichtspflicht normiert, ist dies, wie oben erwähnt, kein Problem.

b) Hinweise zur Regelung der Nutzung von Internet und E-Mail

- 222** Die Datenschutzaufsichtsbehörden haben eine Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz veröffentlicht.¹⁶⁴ Diese Orientierungshilfe zeigt den datenschutzrechtlichen Rahmen und Regelungsmöglichkeiten der Nutzung des betrieblichen Internet- und E-Mail-Dienstes durch die Beschäftigten auf. Zusätzlich enthält diese Orientierungshilfe ein Muster für eine Betriebsvereinbarung (Richtlinie) für die private Nutzung von Internet und/oder des betrieblichen E-Mail-Postfachs.
- 223** Sofern der Arbeitgeber Hardware bzw. Software zur Verfügung stellt, dürfen Dienste grundsätzlich nur für die betriebliche Tätigkeit genutzt werden. Eine private Nutzung ist damit nicht erlaubt, es sei denn, der Arbeitgeber hat eine Privatnutzung ausdrücklich – entweder im Arbeitsvertrag oder in einer Betriebsvereinbarung – geregelt. Darüber hinaus besteht auch die Möglichkeit, in Kenntnis und Duldung der privaten Nutzung über einen längeren Zeitraum dies konkludent zu genehmigen (sog. „betriebliche Übung“). Den gesetzlichen Rahmen geben die DSGVO, das BDSG, das Arbeitsrecht und das TTDSG vor.¹⁶⁵
- 224** Im Idealfall gibt es eine Betriebsvereinbarung sowie interne Richtlinien, welche die genauen Grenzen abstecken und allen Beteiligten klar machen, was möglich

¹⁶⁴ Vgl. die „Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ unter https://www.datenschutzkonferenz-online.de/media/oh/201601_oh_email_und_internetdienste.pdf (zuletzt abgerufen am 19.3.2024), die auch nach dem Inkrafttreten der DSGVO Bestand hat.

¹⁶⁵ Vgl. die „Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ unter https://www.datenschutzkonferenz-online.de/media/oh/201601_oh_email_und_internetdienste.pdf; https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OH_ZurDatenschutzgerechtenNutzungVonEMailUndAnderenInternetdienstenAmArbeitsplatz.html (beide Quellen zuletzt abgerufen am 19.3.2024), die auch nach dem Inkrafttreten der DSGVO Bestand hat.

ist. In den meisten Fällen wird es in den Unternehmen eine entsprechende Betriebsvereinbarung geben, welche die Nutzung ausdrücklich regelt. Wie auch immer dies geregelt sein mag, es ist von großer Bedeutung, die Nutzungsbedingungen klar an die Belegschaft zu kommunizieren und transparent zu machen (vgl. dazu auch → Rn. 37). Neben all den Nutzungsmöglichkeiten will sich das Unternehmen weiterhin technisch sauber aufstellen. Aus diesem Grund ist zu empfehlen, Mitarbeiter zusätzlich darauf hinzuweisen, dass bei privater Nutzung des dienstlichen E-Mail-Postfachs, private Mails im Hinblick auf Viren- oder Spamfilter, wie dienstliche gehandhabt werden.

Wie bereits erwähnt, sollte das Thema Internet- und E-Mail-Nutzung standardmäßig in einer Betriebsvereinbarung geregelt werden. Um jedoch E-Mails im Bedarfsfall auch filtern zu können, wie es u. a. im Zusammenhang mit Compliance-Verfahren notwendig sein kann, sollten einige Aspekte berücksichtigt werden.

225

Checkliste zu den besonderen Regelungsaspekten im Rahmen von Compliance-Verfahren:

226

- Nutzungsform und Nutzungsbedingungen
- Bei erlaubter privater Nutzung werden die privaten E-Mails dienstlichen E-Mails gleichgestellt, sodass Virenanalysen, Spamfilter und sonstige automatisierte Kontrollen weiterhin ermöglicht werden können (Zustimmung des Betroffenen)
- Vorgehensweisen und Abläufe bei notwendigem Zugriff auf das Postfach bei Abwesenheit des Beschäftigten oder der Geschäftsleitung (bspw. länger andauernder Krankheitsfall – Person ist nicht mehr ansprechbar)
- Ablaufplan für interne Untersuchungen im Rahmen von Compliance-Ermittlungen

Im Ergebnis ist nur ein Verbot im Hinblick auf die Privatnutzung wirklich sicher. Neben dieser sehr restriktiven Vorgehensweise besteht die Möglichkeit, den Mitarbeitern die Nutzung von Web-Mail-Diensten freizugeben oder darüber hinausgehend einzelne Rechner als „Surf-Stationen“ oder W-LAN für private Devices freizugeben. Dies ist letztlich eine Abwägungsfrage.

227

Für Compliance ist standardmäßig die Perspektive der Aufsichtsbehörden als Maßstab heranzuziehen, um eine entsprechende Empfehlung an die Geschäftsleitung geben zu können. Auch hierzu gibt die Orientierungshilfe der Datenschutzkonferenz ein paar wichtige Empfehlungen.

228

229 Empfehlungen der Aufsichtsbehörden¹⁶⁶ zur Internet- und E-Mail-Nutzung:

- Es sollten schriftliche Regelungen zur Internet- und E-Mail-Nutzung getroffen werden. Hier sollten folgende Punkte geregelt sein: Fragen des Zugriffs, Protokollierung, Auswertung, Durchführung von Kontrollen. Auf mögliche Überwachungsmaßnahmen und damit in Verbindung stehende Sanktionen sind die Beschäftigten hinzuweisen.
- Für den Fall, dass der Arbeitgeber seinen Beschäftigten die Möglichkeit der privaten Nutzung des betrieblichen E-Mail-Accounts ermöglicht, sollte klar sein, dass damit das Fernmeldegeheimnis gilt. Dies kann in der Praxis zu einigen Problemen führen. Insbesondere dann, wenn der Arbeitgeber für den Geschäftsablauf auf das betriebliche Postfach des Beschäftigten Zugriff nehmen möchte. Wie bereits erwähnt, sollte den Beschäftigten besser die Nutzung von Web-Mail-Diensten angeboten werden. Damit ist auch das Problem der Nutzung des betrieblichen Accounts für private Zwecke besser gelöst. Das betriebliche Postfach wird hiermit nicht mit privaten Nachrichten vermengt.
- Bei privater Nutzung des betrieblichen E-Mail-Accounts: E-Mails mit erkennbar privatem Inhalt dürfen nur in dem Umfang zur Kenntnis genommen werden, wie dies von der Einwilligung gedeckt ist, um eine Abgrenzung von den betrieblichen Mails zu erreichen. Dasselbe gilt für die Kommunikation mit sog. „Geheimnisträgern“ (Betriebsrat, Jugend- und Ausbildungsvertretung, Schwerbehindertenvertretung, Gleichstellungsbeauftragte u. a.). Dies bedeutet, wenn sich im Rahmen der Sichtung aus dem Absender ergibt, dass es sich um eine geschützte und dem Privatbereich zuzurechnende E-Mail handelt, ist die Arbeitgeberseite nicht berechtigt, den Inhalt der E-Mail zur Kenntnis zu nehmen, zu verarbeiten oder zu nutzen.
- Bei Ausscheiden von Mitarbeitern aus dem Unternehmen sollte darauf geachtet werden, dass die persönliche betriebliche E-Mail-Adresse so schnell wie möglich deaktiviert wird. Dies kann im Rahmen von internen Prozessen definiert und festgelegt werden. Hierbei ist selbstverständlich erforderlich, dass die Personalabteilung in Abstimmung mit der IT-Abteilung diesen Prozess aufsetzt und entsprechend kommuniziert. Compliance behält sich hierbei vor, diesen Prozessablauf zu überprüfen, um die Einhaltung der Vorschriften der DSGVO und des BDSG intern zu gewährleisten.

¹⁶⁶ Vgl. die „Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ unter https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OH_ZurDatenschutzgerechtenNutzungVonEMailUndAnderenInternetdienstenAmArbeitsplatz.html (Stand: Januar 2016), S. 1, 10.

Ein noch viel komplexeres Feld eröffnet sich, wenn vertrauliche Dateien auf private Geräte gelangen, die außerhalb der Kontrolle der Firmen-IT liegen. Denn hierbei können vertrauliche Dokumente und Daten nicht mehr ferngesteuert gelöscht werden. Darüber hinaus kann es passieren, dass mittels eines ungesicherten Privatgeräts der User sich in ein ungeschütztes Netzwerk einloggt. **230**

Es ist Unternehmen daher aus Compliance-Sicht unbedingt anzuraten, eine interne Regelung im Umgang mit dem „Privatbereich“ zu treffen. Somit kann zumindest auf ein datenschutzkonformes Verhalten hingewirkt werden. **231**

c) Beispielsfall zur Kontrolle bei Verdacht gegen Mitarbeiter

Unrechtmäßiges Verhalten von Mitarbeitern ruft regelmäßig auch die Compliance-Abteilung auf den Plan, da schwere Compliance-Verstöße nicht zuletzt auch mit fristgemäßen und außerordentlichen Kündigungen geahndet werden sollen. In enger Abstimmung mit der Personalabteilung ist dann die Ermittlung des Sachverhalts voranzutreiben (sog. internal investigation). Besteht bei Kunden regelmäßig noch die Möglichkeit, durch Kontrollen Diebstähle u. Ä. zu vermeiden, so sind solche offenen Maßnahmen aufgrund der besonderen Kenntnis der Mitarbeiter in der Praxis meistens untauglich. Anhand eines in jüngster Vergangenheit entschiedenen Urteils des BAG zur Schrankkontrolle¹⁶⁷ wird im Folgenden das arbeits- und datenschutzrechtliche korrekte Vorgehen bei Vorliegen eines Tatverdachtes gegen einen Mitarbeiter erläutert. Vor allem die zeitlichen Komponenten aus den Arbeitsrechtsvorschriften geben hier den Takt vor. Gleichzeitig wird schnell ersichtlich, dass auch das (Beschäftigten-)Datenschutzrecht den Compliance-Maßnahmen deutliche Grenzen setzt. Es ist daher Aufgabe des Compliance Officers, in enger Abstimmung mit dem Personalleiter und dem DSB auf der einen Seite, die Fristen und auf der anderen Seite, die Grenzen der zulässigen Ermittlung des Sachverhalts zu managen. **232**

Fallbeispiel: Der Leiter eines Großhandelsmarkts verdächtigt einen Mitarbeiter der Getränkeabteilung, diverse Damenunterwäsche aus dem Sortiment des Markts gestohlen zu haben. Aus diesem Grund informiert der Marktleiter den Betriebsrat umgehend von seinem Diebstahlsverdacht und holt dessen Zustimmung zur Durchsuchung des privaten und verschlossenen Schanks des Mitarbeiters ein. Im Beisein eines Betriebsratsmitglieds wird der Schrank geöffnet und durchsucht, ohne den Mitarbeiter von dieser Maßnahme zu informieren. Tatsächlich befinden sich darin vier gestohlene Wäscheartikel. **233**

Was zunächst als eindeutiger Fall zu beginnen scheint, kann sich schnell als arbeits- und datenschutzrechtlich unhaltbar und damit für die Compliance-Abteilung als Worst-Case-Szenario entwickeln. Aus arbeitsrechtlicher Sicht berech- **234**

¹⁶⁷ BAG, Urt. v. 20.6.2013 – 2 AZR 546/12, BB 2014, 890 mit BB-Komm. *Ihle*.

tigt ein nachweisbarer Diebstahl zu einer außerordentlichen Kündigung, da nach ständiger Rechtsprechung des BAG Straftaten zulasten des Arbeitgebers – insbesondere Diebstahl und Betrug – einen wichtigen Kündigungsgrund darstellen.¹⁶⁸ Nichts weniger als die erfolgreiche Durchführung der fristlosen Kündigung als angemessene Compliance-Maßnahme wird daher regelmäßig von der Geschäftsleitung erwartet werden.

- 235 Um hier bereits nicht formell schon zu scheitern, ist die kurze Zwei-Wochen-Frist des § 626 Abs. 2 BGB zu beachten.¹⁶⁹ Sie beginnt mit der Kenntnis des Arbeitgebers vom Sachverhalt, der zur Kündigung berechtigen würde. Innerhalb dieser Zeit sind regelmäßig der Mitarbeiter und der Betriebsrat zu hören. Viel Zeit bleibt der Arbeitgeberseite daher nicht. Gleichzeitig kann der Arbeitgeber, der Anhaltspunkte für ein strafbares Verhalten des Mitarbeiters hat, grundsätzlich den Fortgang eines laufenden Straf- oder Ermittlungsverfahrens abwarten. Es steht ihm jedoch frei, eigene Ermittlungen anzustellen und die Strafverfolgungsbehörden nicht oder nicht unmittelbar einzuschalten. Auch private Ermittlungen hemmen – zügig vorangetrieben – den Lauf der Zwei-Wochen-Frist.¹⁷⁰
- 236 Daneben beschränkt der Beschäftigtendatenschutz die Möglichkeiten des Arbeitgebers zudem nicht unerheblich. Das BAG hat in seiner Entscheidung vom 20.6.2013 klargestellt, dass das BDSG auf tatsächliche Ermittlungsmaßnahmen wie das Öffnen und Durchsuchen eines Schrankes anwendbar ist. Der Arbeitgeber muss daher dem Erlaubnisvorbehalt entsprechend zumindest die Erfüllung der Tatbestandsvoraussetzungen einer Erlaubnisnorm wie z. B. des § 26 Abs. 1 Satz 2 BDSG nachweisen können. Im Ergebnis laufen die Erlaubnisnormen für den Umgang mit Beschäftigtendaten jedoch alle auf die Prüfung der Rechtmäßigkeit des Eingriffs nach Art. 2 Abs. 1 GG hinaus. Die Überwachung und Durchsuchung des Mitarbeiters stellt einen Eingriff in dessen Persönlichkeitsrecht dar. Der Arbeitgeber hat demnach gerade keinen eigenen Entscheidungsspielraum, welche Überwachungs- und Kontrollmaßnahme er anwendet.¹⁷¹ Diese Prüfung hat sich am Verhältnismäßigkeitsprinzip zu orientieren. Die Maßnahme muss der Mitarbeiter daher nur dulden, wenn sie geeignet, erforderlich und angemessen ist.
- 237 Insbesondere die Erforderlichkeit wird in der Praxis nicht selten eher behauptet, denn genau geprüft, obwohl deren Fehlen für den Richter am augenfälligsten ist. Ist eine Maßnahme ebenso erfolgversprechend, aber greift sie weniger tief in das Persönlichkeitsrecht des Mitarbeiters ein, so ist sie vorrangig anzuwenden. Diese **Kontrollüberlegung** sollten Compliance Officer ihren internen Ermittlern standardmäßig vorgeben. Im Fallbeispiel führt sie dem BAG entsprechend dazu, dass die Schrankkontrolle ohne Hinzuziehung des Mitarbeiters datenschutz-

168 Zu (strafbarem) Fehlverhalten als Regelungsgegenstand eines Code of Conduct siehe → Benkert, Kap. 4 Rn. 11 ff.

169 Vgl. BAG, Urt. v. 16.7.2015 – 2 AZR 85/15, BB 2016, 505 mit BB-Komm. von Helwig.

170 BAG, Urt. v. 16.7.2015 – 2 AZR 85/15, BB 2016, 505 mit BB-Komm. von Helwig.

171 Ihle, BB 2014, 890, 896.

rechtlich unzulässig ist, da nicht ersichtlich ist, weshalb diese Kontrolle weniger erfolgversprechend wäre, wenn der Mitarbeiter beim Öffnen anwesend ist. Die nicht heimliche Kontrolle des Mitarbeiters ist daher als milderes Mittel häufig vorzuziehen. Der Fall wird andernfalls auch vor Gericht nicht dadurch zu retten sein, dass Zeugen aufgefahren werden können. Laut BAG resultiert aus der rechtswidrigen Beweiserhebung auch ein Beweisverwertungsverbot, da die Verwertung einen erneuten Eingriff in das Persönlichkeitsrecht des Mitarbeiters bedeutet.¹⁷²

Im Ergebnis müssen Maßnahmen zur Verhinderung oder Aufdeckung von Regelverstößen selbst regelkonform sein. Compliance-Prozesse sind daher auf die Einhaltung datenschutzrechtlicher Vorgaben zu überprüfen und anzupassen.¹⁷³ Die Risikominimierung durch Hinzuziehung des Betriebsrats bzw. des DSB bei der Kontrollmaßnahme selbst funktioniert nur teilweise. Die generelle Hinzuziehung bedeutet zunächst sogar eine nicht gewollte Intensivierung des Eingriffs in das Persönlichkeitsrecht, da eine weitere Person die Daten des Mitarbeiters zur Kenntnis nimmt. Sehen betriebsinterne Datenschutzregelungen hingegen eine stufenweise Information und Beiziehung vor, die ersichtlich auf einen möglichst geringen Eingriff abzielen, fallen diese Bedenken deutlich geringer aus.

238

d) Beispielsfall zum Auskunftsrecht eines Mitarbeiters bei Untersuchungen von Compliance-Verstößen

Die Ermittlung von Compliance-Verstößen ist regelmäßig von der Erlangung entsprechender einschlägiger Kenntnisse abhängig. Wirksame Compliance Management-Systeme setzen hierfür regelmäßig auf Hinweisgeber-Systeme (sog. Whistleblowing-Systeme).¹⁷⁴ Die Wirksamkeit eines solchen Systems lebt von der Bereitschaft der Mitarbeiter dieses zu nutzen. Aus diesem Grund wird regelmäßig – auch zum Schutz des hinweisgebenden Mitarbeiters und zur Vermeidung datenschutzrechtlicher Friktionen – die Anonymität zugesichert. Gleichzeitig sieht der Grundsatz der Transparenz ein entgegenlaufendes **Recht auf Auskunft** des betroffenen, will heißen „verpiffenen“ Mitarbeiters nach Art. 15 Abs. 3 Satz 1 DSGVO vor. Mit diesen widerstrebenden Interessen hatte sich das Landesarbeitsgericht Baden-Württemberg¹⁷⁵ auseinanderzusetzen.

239

172 Für diesen erneuten Eingriff fehlt es regelmäßig an einem überwiegenden Interesse des Arbeitgebers.

173 *Wybitul/Astor*, CB 2014, 260, 264.

174 Eine Pflicht zur Errichtung interner Meldekanäle ergibt sich künftig auch nach der Umsetzung der Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23.10.2019 in nationales Recht.

175 LAG Baden-Württemberg, Urt. v. 20.12.2018 – 17 Sa 11/18.

- 240** **Fallbeispiel:** In dem zu entscheidenden Kündigungsschutzverfahren hatte ein gekündigter Mitarbeiter einen Auskunftsanspruch nach Art. 15 DSGVO geltend gemacht sowie beantragt, dass die beklagte Arbeitgeberin ihm eine Kopie seiner personenbezogenen Leistungs- und Verhaltensdaten zur Verfügung stellt. Zudem forderte er das Unternehmen auf, ihm Einsicht in das Whistleblowingsystems – konkret in die sog. Einsicht in eine Business Practices Office-Akte (BPO-Akte) – zu ermöglichen, dass die Beklagte zum Zwecke der Untersuchung von etwaigen Compliance-Verstößen und möglichen sonstigen Regelverletzungen betreibt.
- 241** Das LAG verurteilt die beklagte Arbeitgeberin unter anderem dazu, die Einsichtnahme in die BPO-Akte zu gewähren und dem Kläger Auskunft über die von der Arbeitgeberin verarbeiteten und nicht in der Personalakte gespeicherten, personenbezogenen Leistungs- und Verhaltensdaten zu erteilen. Hinsichtlich des Antrags auf Auskunftserteilung urteilte das Gericht, dem Kläger die geforderten Auskünfte umfassend zu erteilen. Das Mindestmaß müsse folgende Informationen umfassen:
- Zwecke der Datenverarbeitung,
 - Empfänger gegenüber denen personenbezogene Daten des Klägers/Anspruchstellers offengelegt werden,
 - Speicherdauer oder Kriterien zur Festlegung der Dauer,
 - Herkunft der personenbezogenen Daten, soweit diese nicht bei dem Kläger selbst erhoben wurden,
 - automatisierte Entscheidungsfindung (inkl. Profiling) sowie aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer Verarbeitung.
- 242** Das LAG Baden-Württemberg forderte die Beklagte allerdings auch auf, dem Kläger Auskunft über jeden einzelnen Empfänger zu geben und ging damit sogar über die von den Aufsichtsbehörden geforderten Informationen hinaus.
- 243** Das Gericht qualifiziert zudem die BPO-Akten als Personalakte.¹⁷⁶ Das gesetzlich nicht eingeschränkte Akteneinsichtsrecht kann demnach gerade nicht mit der Begründung verweigert werden, Mitarbeiter, die eine interne Untersuchung durch ihren Hinweis ausgelöst haben, müssten geschützt werden. Trotz zugesicherter Anonymität dürfe der Arbeitgeber nicht gegen das Verbot des Führens von Geheimakten im Rahmen der Personalakte verstoßen.
- 244** In der Konsequenz hätte der Arbeitgeber zur Erfüllung seiner Pflichten die Informationen, die Rückschlüsse auf die Person des Hinweisgebers erlauben, gar nicht erst zur Akte nehmen. Alternativ hätte er auch Teile der Akte schwärzen oder durch sonstige Vorkehrungen unkenntlich machen können. Die Anonymität

¹⁷⁶ Irrelevant soll sein, ob der Arbeitgeber die Unterlagensammlung als Personalakte i. S. d. § 83 BetrVG bezeichnet oder nicht.

von Hinweisgebenden¹⁷⁷ kann insbesondere sichergestellt werden, indem interne Untersuchungen über externe Berater als Ombudspersonen durchgeführt werden. Eine Beschränkung des Anspruchs auf Auskunft und Erhalt einer Kopie ist in diesen Fällen wegen entgegenstehender berechtigter Interessen Dritter gesetzlich möglich.¹⁷⁸ Dies erfordert aber eine konkrete Abwägung im Einzelfall, aus der sich ein überwiegendes Interesse des Dritten an der Geheimhaltung ergibt. Ein automatisches Überwiegen des Geheimhaltungsinteresses lehnt das Gericht ab. Das Urteil zieht damit nicht zwangsläufig einen geringeren Schutz von Hinweisgebern nach sich. Vielmehr zeigt es, dass der Beschäftigtendatenschutz einen festen Platz in der täglichen Compliance-Praxis eingenommen hat.

VII. Fazit

Im modernen Compliance Management nimmt der Schutz personenbezogener Daten bereits jetzt eine zentrale Rolle ein. Das gilt sowohl in konzeptioneller als auch in rechtstatsächlicher Hinsicht, was die betrieblichen Abläufe angeht. Compliance lässt sich ohne datenschutzrechtliche Kenntnis nicht mehr seriös betreiben. Ohne den rechtmäßigen Umgang mit personenbezogenen Daten ist ein Compliance-System nicht mit Leben zu erfüllen. Dies betrifft sowohl Kunden- als auch Beschäftigtendaten. Beschäftigtendatenschutz betrifft dabei den Kernbereich der täglichen Compliance-Arbeit. Er beschreibt nicht nur eigene Risikofelder, sondern setzt bedeutsame Maßstäbe für das regelkonforme Betreiben von Compliance im Unternehmen.

245

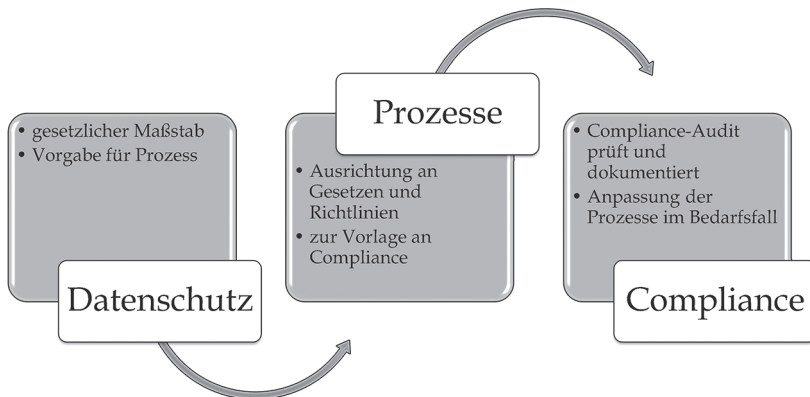


Abbildung 7: Ausrichtung der Compliance-Prozesse am Datenschutz

¹⁷⁷ Die Zusicherung von Anonymität zum Zwecke der Aufklärung innerbetrieblichen Fehlverhaltens hat das Gericht grundsätzlich als berechtigtes Interesse anerkannt und sogar die höhere Effektivität von anonymen Meldeverfahren gerade innerhalb hierarchischer Strukturen betont.

¹⁷⁸ Vgl. Art. 15 Abs. 4 DSGVO, § 34 Abs. 1 i.V.m. § 29 Abs. 1 Satz 2 BDSG.

- 246** Ein Compliance-System funktioniert zudem nur dann, wenn es gelebt wird. Ein Compliance-System lebt damit von den Mitarbeitern, die sich mit diesem System identifizieren. Ein wesentlicher Baustein ist dabei die Vorgabe nachvollziehbarer Regelungen durch eine Richtlinie (Betriebsvereinbarung). Diese ist wiederum vom Betriebsrat maßgeblich mitbeeinflusst, der die Interessen der Beschäftigten wahrnimmt. Letztlich sind es die Daten der Mitarbeiter, die im Rahmen des Compliance-Systems erhoben, verarbeitet und genutzt werden. Um dieses Zusammenspiel so regelkonform wie möglich zu gestalten, sind Personaler und DSB in die Compliance-Organisation weitgehend und rechtzeitig einzubinden.
- 247** Mit Blick auf die seit 2018 anzuwendende Datenschutzgrundverordnung sind die mit dem Datenschutz verbundenen Herausforderungen noch weiter gestiegen. Umso wichtiger sind Schulungs- und andere Maßnahmen, damit Datenschutzanforderungen langfristig nicht zu Fallstricken des Compliance Managements werden. Die internen Compliance-Prozesse sind demgemäß an den Grundsätzen des Datenschutzes auszurichten.

13. Kapitel

IT-Compliance – Software-Lizenzmanagement, Blockchain und Nutzung von Daten

I. Rechtliche Herausforderungen der fortschreitenden Digitalisierung und Vernetzung

Obwohl es schon aufgrund der Unterschiedlichkeit der verfolgten Ziele, kein einheitliches Gesetz gibt, das sämtliche Aspekte der IT-Compliance regelt, wird unter diesem Begriff die Einhaltung der speziell die Informationstechnik eines Unternehmens betreffenden Regelwerke, Richtlinien und Gesetze verstanden. 1

Hierunter fallen beispielsweise ein Lizenzmanagements, d.h. eines Verfahrens, mit dessen Hilfe sichergestellt wird, dass ausreichend Lizenzen für die Anzahl aktiver Nutzer vorhanden sind und dass sonstige Nutzungsbeschränkungen aus den Lizenzverträgen beachtet werden. 2

Daneben ist auch die Nutzung von Daten sowohl für die Arbeit im Risikomanagement als auch für die Business- und Prozessoptimierung eine Quelle völlig neuer Möglichkeiten.¹ 3

II. Software-Lizenzmanagement

Die Auswahl und die Beschaffung von Unternehmenssoftware erfolgt oftmals bedarfsorientiert und daher häufig unstrukturiert im Sinne einer Gesamtstrategie für den Bereich IT. Dementsprechend ist es schwierig, kontinuierlich einen Überblick einerseits über die aktuell im eigenen Unternehmen eingesetzte Software und andererseits über die erworbenen Lizenzen zu behalten. Unternehmen sollten jedoch sicherstellen, dass Art und Anzahl der Lizenzen für Software mit deren Einsatzzweck übereinstimmen. Rechtlich stellt die Nutzung von Software oftmals eine grundsätzlich dem Rechteinhaber vorbehaltene Vervielfältigung der Software oder wesentlicher Teile davon dar. Notwendig ist daher die Einholung ausreichender Nutzungsrechte durch entsprechende Lizenzverträge. Unternehmen sollten daher sowohl prüfen, welche Lizenzen für den beabsichtigten Einsatzzweck notwendig sind, aber auch wie sich ein veränderter Einsatzzweck, neue Hardware oder eine geänderte IT-Infrastruktur auf die erworbenen Nutzungsrechte auswirken. Hierfür sollte ein Lizenzmanagement aufgebaut werden.² 4

1 Gaess, IT-Governance, 8. Data-Governance, S. 74.

2 Rath/Kuß, in: Umnuß, Corporate Compliance Checklisten, 4. Aufl. 2020, Kap. 8 Rn. 16, die ergänzend darauf hinweisen, dass regelmäßig mit einem Softwareupdate oder weiteren Lizenzen neue Lizenzbedingungen verbunden werden, insbesondere auch durch den Einsatz von Endnutzer-Lizenzbedingungen (EULA).

- 5 Der Einsatz eines effektiven Lizenzmanagements ermöglicht daher nicht nur eine Verringerung der Kosten,³ sondern auch die Vermeidung rechtlicher Probleme.⁴ Durch einen Überblick über den aktuellen Lizenzbestand kann neue Software bedarfsgerecht eingekauft und damit eine Überlizenzierung (wodurch unnötige Kosten entstehen) oder Unterlizenzierung (wodurch das Risiko rechtlicher Sanktionen entsteht) vermieden werden.⁵

1. Rechtliche Grundlagen der Nutzung von Computerprogrammen

- 6 §§ 69c, 69d UrhG bilden die Grundlage für die Ausgestaltung von Softwareüberlassungs- und Softwarenutzungsverträgen. Nach § 69c UrhG ist derjenige, der ein Computerprogramm geschaffen oder die Rechte daran erworben hat, ausschließlich dazu berechtigt, das unter anderem Programm dauerhaft oder auch nur vorübergehend zu vervielfältigen (Nr. 1), es zu übersetzen und zu bearbeiten (Nr. 2), jede Form der Verbreitung einschließlich der Vermietung (Nr. 3) oder anderen Nutzern öffentlich zugänglich zu machen (Nr. 4) oder dies Dritten zu gestatten.
- 7 Ausgenommen von diesen zustimmungsbedürftigen Handlungen sind nach § 69d Abs. 1 UrhG die in § 69c Nr. 1 und 2 UrhG genannten Handlungen, wenn diese für eine bestimmungsgemäße Benutzung des Computerprogramms notwendig sind, vorausgesetzt, dass keine abweichenden vertraglichen Bestimmungen vorliegen. Darüber hinaus sind nach § 69d Abs. 2 und 3 UrhG die Erstellung einer Sicherungskopie und der Funktionstest eines Programms, sowie gem. § 69e UrhG die Dekompilierung keine zustimmungsbedürftigen Handlungen des Rechtsinhabers. Bei Softwarevertriebsverträgen⁶ wurden bisher regelmäßig Vervielfältigungsstücke überlassen mit der Einräumung von Nutzungsrechten nach Maßgabe der Lizenzbestimmungen. In diesem Fall kann bei der dauerhaften Überlassung das Verbreitungsrecht gem. § 69c Nr. 3 UrhG erschöpft sein.⁷

3 Studien haben ergeben, dass mit einem funktionierenden Lizenzmanagement eine Kostenreduktion von ca. 15% realisiert werden kann, siehe Lizenzmanagement in deutschen Unternehmen – Ergebnisse einer Umfrage von KPMG, abrufbar unter <https://www.yumpu.com/de/document/view/20636554/kpmg-studie-lizenzmanagement-in-deutschen-pbroker> (zuletzt abgerufen am 20.3.2024).

4 Das OLG Karlsruhe hat die persönliche Haftung des Geschäftsführers bejaht, weil der Geschäftsführer es versäumt habe, „im Rahmen des Zumutbaren und Erforderlichen Maßnahmen zu treffen, die eine Gefährdung der Urheberrechte Dritter ausschließen oder doch ernsthaft mindern.“, OLG Karlsruhe, Urt. v. 23.4.2008 – 6 U 180/06.

5 Rath/Kuß, in: Umnuß, Corporate Compliance Checklisten, 4. Aufl. 2020, Kap. 8 Rn. 17 weisen ergänzend darauf hin, Unternehmen neben einem Lizenzmanagement konkrete Richtlinien darüber erlassen müssen, wie Software im Unternehmen eingesetzt werden darf, und technische Maßnahmen ergreifen, um Urheberrechtsverletzungen auszuschließen oder zu mindern. Zudem müssen Unternehmen im Jahresabschluss ihre immateriellen Güter, einschließlich etwaiger Lizenzen erfassen und bewerten.

6 Polley/Seeliger, CR 2001, 1 ff.

7 Wiebe, in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 3, Rn. 75.

Über diese gesetzlich geregelten Nutzungsrechte können eigenständige Nutzungsarten vereinbart werden; müssen jedoch nach der Verkehrsauffassung hinreichend klar abgrenzbar sowie wirtschaftlich-technisch als einheitlich und selbstständig anzusehen sein.⁸ Eine Beschränkung auf bestimmte Personenkreise innerhalb eines Vertriebswegs ist ebenso wenig mit dinglicher Wirkung möglich wie auf bestimmte Formen des Gebrauchs beim Nutzer.⁹

Rechtlich umstritten ist darüber hinaus die so genannte „indirekte Nutzung“ von Software, also Lizenzmodelle welche berücksichtigen, dass die zunehmende Digitalisierung und Automatisierung von Geschäftsprozessen sowie das Internet der Dinge dazu führen, dass immer weniger menschliche Nutzer notwendig sind, um Geschäftsvorgänge über Software abzuwickeln und dass die entstehende Lücke durch andere Software geschlossen wird, die automatisiert mit anderen Computerprogrammen interagiert. Mehr Automatisierung führt zu weniger menschlichen Nutzern und folglich zu geringeren Lizenzeinnahmen.¹⁰

Umstritten ist nun, ob die indirekte Nutzung von Software nur zulässig ist, wenn der Rechteinhaber zustimmt, oder nicht, also welche Handlungen die bestimmungsgemäße Benutzung eines Computerprogramms gemäß § 69d Abs. 1 UrhG erfasst.¹¹

2. Besondere Arten von Software, insbesondere Open-Source-Software

Damit die Unternehmensleitung im Hinblick auf das Software-Lizenzmanagement eine unternehmerische Entscheidung auf Grundlage angemessener Informationen treffen kann („Business Judgement Rule“), ist zu ermitteln, welche Art von Software in welcher Version genutzt wird. Zu berücksichtigen sind hierbei auch die Besonderheiten von Public Domain-Software,¹² Freeware,¹³ Shareware¹⁴ und insbesondere von „Open-Source“-Software.

8 BGH, GRUR 1992, 310, 311 – Taschenbuch-Lizenz; BGH, GRUR 2001, 153, 154 – OEM; BGH, GRUR 2003, 416, 418 – CPU-Klausel. Unterhalb der dadurch gezogenen Grenze können Nutzungsbeschränkungen zwar grundsätzlich mit schuldrechtlicher Wirkung vereinbart werden, aber nicht mit dinglicher Wirkung gegenüber Dritten.

9 Siehe hierzu *Grützmacher*, in: Wandtke/Bullinger, Praxiskommentar UrhR, § 69c UrhG Rn. 30 ff.

10 *Rath/Kuß*, in: Umnuß, Corporate Compliance Checklisten, 4. Aufl. 2020, Kap. 8 Rn. 17.

11 Vgl. *Metzger/Hoppen*, CR 2017, 625; *Barnitzke*, K&R 2018, 455; *Schneider*, ITRB 2017, 286; *Redeker*, ITRB 2017, 44; *Kroke*, CR 2019, 73.

12 Unter Public-Domain-Software wird allgemein unentgeltliche und frei nutz-, vervielfältig-, bearbeit- und verbreitbare Software verstanden, OLG Stuttgart, CR 1994, 743, 744 m. w. N.; LG Stuttgart, CR 1994, 162, 163.

13 Anders als bei Public-Domain-Software ist es bei Freeware nicht erlaubt, Veränderungen vorzunehmen und die Software in dieser veränderten Form zu vertreiben, *Marly*, Praxishandbuch Softwarerecht, Rn. 867.

14 Shareware wird dauerhaft nur gegen Registrierung überlassen, wobei der Benutzer aufgefordert wird, eine Registrierungs-, letztlich also eine Lizenzgebühr an den Rechteinhaber zu entrichten, OLG Hamburg, CR 1994, 616, 617.

- 12 Open-Source-Software ist Software, welche oftmals unentgeltlich vertrieben wird, deren Nutzung jedoch an die Einhaltung bestimmter Bedingungen geknüpft ist,¹⁵ bei Lizenzen mit sogenanntem Copyleft-Effekt¹⁶ insb. die der Offenlegung des Quellcodes.¹⁷ Die am weitesten verbreiteten Lizenzbedingungen im Bereich Open-Source-Software sind die GNU General Public License Version 2 aus dem Jahr 1991 (GPLv2)¹⁸ und die Version 3 aus dem Jahr 2007 (GPLv3).¹⁹ Daneben existieren weitere Open-Source-Software-Lizenzbedingungen mit und ohne den Copyleft-Effekt.²⁰ Strittig ist, ob zwischen Urheber und Lizenznehmer ein zweiseitiger (kausaler) Lizenzvertrag zustande kommt²¹ oder lediglich einseitig die Nutzungsrechte von den Urhebern dinglich eingeräumt werden.²² Darüber hinaus ist in Rechtsprechung und Literatur umstritten, inwieweit dingliche Beschränkungen und Aufspaltungen der Nutzungsrechte zulässig sind und Auswirkungen auf die Erschöpfung der Rechte haben.²³ Diese Fragen sind beim Lizenzmanagement zu berücksichtigen.

3. Software-Lizenzmanagement im Rahmen verantwortungsbewusster Unternehmensführung

- 13 Die unternehmensinterne Erfassung und Bewertung von Software-Lizenzen ist nicht nur relevant bei dem Verkauf von Unternehmensteilen, der Umstrukturierung und Ausgliederung, dem Outsourcing von IT-Funktionen oder Geschäftsprozessen sowie ähnlichen Maßnahmen.²⁴ Vielmehr ist ein angemessenes Software-Lizenzmanagement Bestandteil einer verantwortungsbewussten Unternehmensführung. Im Rahmen des Jahresabschlusses einer Gesellschaft bedarf es einer Erfassung und Bewertung immaterieller Vermögenswerte (§ 248 Abs. 2 HGB). Insbesondere große und mittelgroße Kapitalgesellschaften müssen in diesem Zusammenhang sicherstellen, dass eine ordnungsgemäße Bewertung im Einklang mit den gesetzlichen Vorschriften erfolgt (§ 266 Abs. 2 HGB). Darüber hinaus verlangt § 93 Abs. 1 Satz 2 AktG ein Handeln des Vorstands zum „Wohl der Gesellschaft“, worunter der Gesetzgeber die langfristige Stärkung des Ertrags und der Wettbewerbsfähigkeit versteht. Der Vorstand muss daher Struktura-

15 Nimmer, CRi 2006, 129.

16 Der Copyleft-Effekt schreibt fest, dass Bearbeitungen des Werks nur dann erlaubt sind, wenn alle Änderungen mit den gleichen oder zumindest ähnlichen Bedingungen weitergegeben werden.

17 Vgl. etwa LG Hamburg, CR 2013, 498, 499 m. Anm. Mantz, CR 2013, 640, 641.

18 Wiedergegeben bei Jaeger/Metzger, Open Source Software, Anhang A.

19 Funk/Zeifang, CR 2007, 617; Grütmacher, ITRB 2009, 184, 186 ff.; Jaeger/Metzger, GRUR 2008, 130.

20 Koch, CR 2000, 273 f.

21 So die h. M.: Deike, CR 2003, 9, 13, 15 ff.; Metzger/Jaeger, GRUR Int. 1999, 839, 843; Koch, CR 2000, 333, 338; Kreutzer, MMR 2004, 695, 696 f.; Sester, CR 2000, 797, 804.

22 Heussen, MMR 2004, 445, 447 f.

23 Grütmacher, in: Wandtke/Bullinger, Praxiskommentar UrhR, § 69c UrhG Rn. 79.

24 Schrey/Krupna, CCZ 2012, 141.

ren stets so einrichten und für die Etablierung solcher Prozesse sorgen, dass die finanziellen, sachlichen und personellen Ressourcen der Gesellschaft möglichst optimal dem Wohle der Gesellschaft dienend eingesetzt werden.²⁵

4. Rechtsfolgen einer Unterlizenzierung

Bei Verwendung einer nicht oder nicht ausreichend lizenzierten Software steht dem Rechtsinhaber nach § 97 Abs. 1 Satz 1 UrhG ein Anspruch auf Beseitigung der Beeinträchtigung, nach § 97 Abs. 1 Satz 2 UrhG ein Anspruch auf Unterlassung und bei Kenntnis der nicht oder nicht ausreichend bestehenden Lizenzierung gemäß § 97 Abs. 2 UrhG ein Anspruch auf Schadensersatz zu. Darüber hinaus kommen gemäß § 98 UrhG Ansprüche auf Vernichtung, Rückruf und Überlassung sowie gemäß § 101a UrhG auf Vorlage und Besichtigung in Betracht. Gegenüber den Inhabern eines Unternehmens besteht nach § 99 UrhG eine eigenständige verschuldensunabhängige Haftung für Unterlassungs- und Beseitigungsansprüche, wenn von einem Arbeitnehmer oder Beauftragten im Unternehmen ein Urheberrecht verletzt wurde. Neben den zivilrechtlichen Ansprüchen kommt bei einem vorsätzlichen Handeln des Arbeitnehmers auch eine Strafbarkeit nach § 106 UrhG in Betracht. **14**

Auch ein Mitglied der Geschäftsleitung kann auf Unterlassung und Schadensersatz nach § 97 UrhG in Anspruch genommen werden, sobald es Kenntnis von der Verwendung nicht lizenzierter Software hatte.²⁶ Bei einer Verletzung von Lizenzrechten kommen darüber hinaus Schadensersatzansprüche der Gesellschaft gegen die Unternehmensleitung gemäß § 43 Abs. 2 GmbHG und § 93 Abs. 2 AktG in Betracht. **15**

III. Software-Lizenzmanagement im Rahmen von Cloud-Diensten

Cloud Computing-Dienste und die hiermit verbundene Ablösung bisheriger Lizenzmodelle, werfen bei einem Vergleich mit der werkträgerbasierten Software-Nutzung eine Reihe rechtlicher Fragen auf.²⁷ **16**

1. Nutzungshandlungen beim Cloud Computing

Ob Software in einer „Cloud“ genutzt werden darf, hängt zunächst davon ab, ob dadurch Ausschließlichkeitsrechte des Rechtsinhabers berührt werden. Ist dies der Fall, so ist anhand der Lizenzbedingungen des Herstellers zu klären, ob die dafür benötigten Nutzungsrechte bereits erworben wurden oder vom Anwender zu erwerben sind. **17**

²⁵ Schrey/Krupna, CCZ 2012, 141.

²⁶ Schrey/Krupna, CCZ 2012, 141, 143 m. w. N.

²⁷ Vergleichbare Fragen stellen sich beim sog. Application Service Providing, siehe hierzu näher Grützmacher, ITRB 2001, 59, 62; OLG München, GRUR-RR 2009, 91; Jaeger, CR 2002, 309, 311.

- 18 Hinsichtlich der technischen Ausgestaltung sind mindestens drei Formen des Cloud Computing zu unterscheiden: Beim sog. „Software-as-a-Service“ (SaaS) wird dem Kunden die Nutzung von auf der Infrastruktur des Anbieters installierter Software ermöglicht, ohne dass die Software auf dem Rechner des Nutzers installiert werden muss. „Platform-as-a-Service“ (PaaS) umschreibt das Angebot einer kosteneffizienten cloud-basierten Entwicklungsumgebung an Nutzer. Bei der Ausgestaltung als „Infrastructure-as-a-Service“ (IaaS) werden Kunden jeweils Rechenleistung und Speicherplatz auf virtuellen Servern zur Verfügung gestellt, nicht jedoch die für Anwendungen erforderliche Applikationssoftware.²⁸

a) Recht der öffentlichen Zugänglichmachung der Software

- 19 Entgegen der wohl h.M.²⁹ ist im Rahmen des Cloud Computing, sowohl bei SaaS, wie auch IaaS und PaaS, nur dann das Recht zur öffentlichen Zugänglichmachung betroffen, wenn die Benutzeroberfläche selber schutzfähig ist, oder bei Verwendung client-seitig laufender Programmteile.³⁰ Öffentlich zugänglich gemacht werden durch Cloud-Dienste im Zweifel (noch) lediglich die Grafikdaten.³¹ Selbst soweit technisch doch (schon) eine Zugänglichmachung der Programmdateien stattfindet, liegt nur auf dem Rechner des Anbieters ein Vervielfältigungsstück vor.³² Der insofern vom OLG München vorgebrachte Vergleich, auch andere Werke (Theaterstücke oder Musikwerke) würden etwa durch öffentliche Darbietung (z. B. ohne Textbuch oder Partitur) in unkörperlicher Form zugänglich gemacht,³³ ist verfehlt, da in diesen Fällen das ganze Werk wahrnehmbar gemacht wird, beim Cloud Computing das Computerprogramm aber regelmäßig nicht.³⁴
- 20 Cloud-Dienste erfordern daher die Einräumung eines Nutzungsrechtes sui generis an den Provider. Eine eigene Nutzungsart liegt vor, wenn es sich nach der Verkehrsauffassung um eine als solche hinreichend klar abgrenzbare, wirtschaftlich-technisch als einheitlich und selbstständig erscheinende Nutzungsart handelt.³⁵ Ebenso wie für die Überlassung von Software im Wege des Application Service Providing und der zugrunde liegenden Single-Tenant-Architektur

28 Siehe hierzu *Nägele/Jacobs*, ZUM 2010, 281, 282.

29 OLG München, GRUR-RR 2009, 91; *Marly*, Praxishandbuch Softwarerecht, Rn. 1087; *Jae-ger*, CR 2002, 309, 311.

30 *Grützmacher*, in: Wandtke/Bullinger, Praxiskommentar UrhR, § 69c UrhG Rn. 66; *Nägele/Jacobs*, ZUM 2010, 281, 287, 290; vgl. zum ASP *Grützmacher*, ITRB 2001, 59, 62.

31 Vgl. *Lehmann/Giedke*, CR 2013, 681, 682.

32 *Grützmacher*, in: Wandtke/Bullinger, Praxiskommentar UrhR, § 69c UrhG Rn. 66.

33 OLG München, GRUR-RR 2009, 91.

34 *Grützmacher*, in: Wandtke/Bullinger, Praxiskommentar UrhR, § 69c UrhG Rn. 66; ähnlich auch *Koch*, ITRB 2011, 42, 43 f. zu CALs.

35 BGH, GRUR 1992, 310, 311 – Taschenbuchlizenz unter Verweis auf BGH, GRUR 1990, 669, 671 – Bibelreproduktion und BGH, GRUR 1979, 637, 638 – White Christmas.

ist bei Cloud-Diensten und deren Multi-Tenant-Architektur davon auszugehen, dass diese Voraussetzungen erfüllt sind, da ein und dasselbe Programm zeitgleich mehreren Nutzern zugänglich gemacht und damit einer erhöhten wirtschaftlichen Auswertung zugeführt wird.³⁶

b) Recht zur Vervielfältigung der Software

21 Sofern im Rahmen einer Cloud-Dienstleistung die Software nur auf dem Server des Cloud-Computing-Dienstleisters läuft und ein Nutzer lediglich mittels eines Browsers auf die Software zugreift, so wird, entsprechend den vorherigen Ausführungen, auf dem Rechner des Nutzers grundsätzlich nur die Benutzeroberfläche vervielfältigt³⁷ und nicht die Anwendersoftware. Für den Fall des nicht applet-basierten Cloud Computings bedarf es daher auch keines Rückgriffs auf § 44a UrhG bzw. § 69d Abs. 1 UrhG.³⁸

22 Auf dem Rechner des Cloud Computing-Dienstleisters hingegen liegt mit Blick auf die Lizenzierung aufgrund der eigenständigen technischen und bei mehreren Nutzern wirtschaftlichen Bedeutung eine eigenständige Nutzungsart vor und ohne entsprechende Rechtseinräumung keine bestimmungsgemäße Nutzung. Beim SaaS und dem damit zusammenhängenden Angebot von Software durch den Dienstleister benötigt dieser dementsprechend ein auf diese Nutzungsart bezogenes Nutzungsrecht.³⁹ Demgegenüber erfolgt die Vervielfältigung einer Applikation beim IaaS oder PaaS primär nur durch den Nutzer,⁴⁰ welcher die Erstellung von Vervielfältigungsstücken auf dem Server des Cloud-Computing-Dienstleisters vornimmt und/oder veranlasst.⁴¹

2. Lizenzmanagement im Zusammenhang mit Cloud Computing-Diensten

23 Verlagert der Kunde eines Cloud-Dienstes eigene Software und/oder Anwendungen in eine Cloud, so muss er nicht nur prüfen, ob er über die dazu benötigten Nutzungsrechte verfügt; er muss vielmehr auch im Rahmen einer Bestandsaufnahme über die erforderlichen Kennzahlen verfügen, aus denen sich die Häufig-

36 *Leupold*, in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 4, Rn. 120 m. w. N.

37 Die Benutzeroberfläche als solche genießt aber nur in Ausnahmefällen Urheberrechtsschutz, jedoch nicht als Computerprogramm.

38 *Grützmaker*, in: Wandtke/Bullinger, Praxiskommentar UrhR, § 69d UrhG Rn. 13; *Nägele/Jacobs*, ZUM 2010, 281, 289 f.; so aber *Pohle/Ammann*, CR 2009, 273, 276; *Splitzgerber/Rockstroh*, BB 2011, 2179.

39 *Grützmaker*, in: Wandtke/Bullinger, Praxiskommentar UrhR, § 69d UrhG Rn. 13; so auch *Nägele/Jacobs*, ZUM 2010, 281, 290; *Pohle/Ammann*, CR 2009, 273, 276, empfehlen eine solche Regelung auch aus Anwendersicht.

40 Vgl. *Grützmaker*, CR 2011, 697, 704 f.; *Nägele/Jacobs*, ZUM 2010, 281, 290.

41 *Nägele/Jacobs*, ZUM 2010, 281, 286; *Bisges*, MMR 2012, 574, 578; weitergehend *Niemann*, CR 2009, 661, 662 f.; a. A. *Schuster/Reichl*, CR 2010, 38, 40.

keit und Intensität der Nutzung einer Software ergibt⁴² und diesen Ausgaben die langfristigen Kosten für Pflegeleistungen und Lizenzgebühren gegenüberstellen.

- 24 Das Aufkommen von Cloud-Diensten hatte zunächst die Hoffnung geweckt, dass das Software-Lizenzmanagement obsolet werden würde, da der Cloud-Anbieter das genaue Ausmaß der Nutzung durch jeden Anwender überwachen und steuern könne.⁴³ Aufgrund der (gegenwärtigen) parallelen Nutzung von lokalen Softwareinstallationen („On-Premise“) und Software, die auf Abruf zur Verfügung gestellt wird („On-Demand“) durch viele Unternehmen, ist das Software-Lizenzmanagement allerdings im Gegenteil deutlich komplexer geworden, von der Messung der Nutzung bis zum Abgleich mit den Verträgen.⁴⁴ Es gilt daher, sowohl die On-Premise- wie auch die On-Demand-Dienste und deren Abrechnungsmodelle in die Lizenzbilanz und Kostenstruktur zu integrieren.
- 25 Bewährte und teilweise von der Rechtsprechung als zulässig anerkannte Lizenzmodelle,⁴⁵ wie etwa die Koppelung der Nutzungsrechte an eine bestimmte Hardware, Einzel-User („Named-User-Modell“) oder User-Gruppen („Concurrent-User“-Modell). Der große Vorteil von Cloud-Diensten, Ressourcen und/oder Applikationen nach Bedarf zur Verfügung zu stellen, macht vielmehr dynamische und flexible Lizenzmodelle notwendig, in deren Rahmen der Anwender bedarfsabhängig die Nutzung bestimmter Software und/oder IT-Dienstleistungen mietet (sog. „User Subscription License“).⁴⁶ Hierdurch wird der Anwender oftmals berechtigt, für den jeweiligen Zeitraum die Software auf verschiedenen Endgeräten (u. a. PCs, Smartphones, Tablets) anzuwenden, wobei die erzeugten Daten zentral in der Cloud gespeichert werden.

IV. Rechtsrahmen von Softwarelizenz-Audits

- 26 Softwarelizenz-Audit bezeichnet die durch den Rechtsinhaber angestoßene Überprüfung, ob die von dem Nutzer dieses Programms erworbenen Nutzungs-

42 So berichtet von *Leupold*, in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 4, Rn. 122. Im Idealfall wird mittels eines Lizenzpoolings sichergestellt, dass immer nur diejenigen Mitarbeiter Zugriff auf eine Softwareanwendung erhalten, die diese auch tatsächlich nutzen, *Kassing*, Softwarepooling im Konzern – Möglichkeiten und Grenzen, 2007.

43 So berichtet von *Leupold*, in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 4, Rn. 123.

44 *Drews*, Softwarelizenzen richtig verwalten, <https://www.computerwoche.de/a/softwarelizenzen-richtig-verwalten,2500448> (zuletzt abgerufen am 20.3.2024). Nach *Doubrava*, in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 4, Rn. 110, kommt dem Lizenzmanagement daher mindestens ebenso große Bedeutung zu, wie den bisher vorrangig diskutierten Themen Datenschutz und Datensicherheit.

45 Vgl. zu CPU-Klauseln BGH, MMR 2003, 393.

46 Siehe hierzu *Leupold/James*, in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 4, Rn. 129 f. m. w. N.

rechte (Softwarelizenzen) dessen tatsächliche Nutzung decken.⁴⁷ Hintergrund solcher Audits ist die (bisherige) Schwierigkeit der Rechtsinhaber die tatsächliche Nutzung zu überprüfen und sein Interesse an der Wahrung der aus dem urheberrechtlichen Schutz des Computerprogramms (§ 69a UrhG) resultierenden Befugnis, eine von ihm nicht autorisierte Nutzung zu untersagen. Demgegenüber hat der Lizenznehmer ein Interesse, nicht mit finanziellen Nachforderungen für eine tatsächliche oder vermeintliche Unterlizenzierung konfrontiert zu werden, Ressourcen für die Untersuchung zur Verfügung zu stellen und das Risiko einzugehen, Betriebs- und Geschäftsgeheimnisse zu verletzen bzw. personenbezogene Daten Dritter unberechtigt zugänglich zu machen.⁴⁸ Die möglichen Arten eines Audits reichen von einer bloßen Selbstauskunft des Lizenznehmers bis hin zur Besichtigung seiner Räumlichkeiten und dem Zugriff auf seine IT-Systeme durch den Lizenzgeber.

1. Rechtliche Grundlagen für einen Softwarelizenz-Audit

Um seinen Auskunftsanspruch durchsetzen zu können, benötigt der Lizenzgeber **27** entweder eine gesetzliche oder eine vertragliche Anspruchsgrundlage. Mögliche gesetzliche Auskunftsrechte finden sich in § 101 UrhG und § 242 BGB. Diese werden durch die Vorlage- und Besichtigungsrechte in § 101a UrhG und § 809 BGB ergänzt.

Nach § 101 Abs. 1 UrhG kann der Lizenzgeber vom Lizenznehmer Auskunft **28** über den Lizenzbestand und die Softwarenutzung verlangen,⁴⁹ wenn eine Rechtsverletzung in einem gewerblichen Ausmaß vorliegt.⁵⁰ Der Anspruchsteller muss hierbei zumindest „in der Lage sein, einen Sachverhalt vorzutragen, der das Auskunftsbegehren rechtfertigt“, eine Ausforschung des Anspruchsgegners lässt § 101 Abs. 1 UrhG indes nicht zu.⁵¹ Ein Softwarelizenz-Audit hat allerdings gerade eine anlassunabhängige Ermittlung möglicherweise existierender anspruchsbegründender Tatsachen zum Ziel, also die Frage, ob ein Anspruch überhaupt in Betracht kommt.⁵² Das Auskunftersuchen muss nach § 101 Abs. 4 UrhG ferner verhältnismäßig, also geeignet, erforderlich und angemessen sein, um die Überschreitung des Lizenzbestands aufzudecken. Die Verhältnismäßigkeit ist einzelfallabhängig anhand der Eindeutigkeit sowie der Art und Schwere

47 Definition nach *Kotthoff/Wieczorek*, MMR 2014, 3.

48 *Kotthoff/Wieczorek*, MMR 2014, 3.

49 Die Auskunft umfasst jedoch nicht die Besichtigung von Räumlichkeiten, Computern und Servern, die Vorlage von Unterlagen, Bucheinsicht oder darüberhinausgehende Maßnahmen, *Hoeren*, CR 2008, 409 f.

50 Das ist dann der Fall, wenn eine Verletzungshandlung im geschäftlichen Verkehr vorgenommen wird, um einen unmittelbaren oder mittelbaren wirtschaftlichen oder kommerziellen Vorteil zu erlangen, Erwägungsgrund 14 der RL 2004/48/EG; *Dreier*, in: *Dreier/Schulze*, UrhG, § 101 Rn. 6 f.

51 BT-Drs. 11/4792, S. 31.

52 *Kotthoff/Wieczorek*, MMR 2014, 3, 4.

der Rechtsverletzung zu bestimmen und mit den berechtigten Geheimhaltungsinteressen des Anspruchsgegners abzuwägen.⁵³

- 29** Gem. § 101a UrhG kann der Lizenzgeber die Vorlage von Urkunden und die Besichtigung von Sachen verlangen. Darunter fällt grundsätzlich auch ein Zugriff auf die Software.⁵⁴ Zur Geltendmachung des Anspruchs muss der Lizenzgeber dabei die Lizenzdokumente und die Software genau bezeichnen⁵⁵ sowie die hinreichende Wahrscheinlichkeit einer Rechtsverletzung nachweisen (§ 101a Abs. 1 Satz 1 UrhG).⁵⁶ Zudem müssen bei einem Auditverlangen nach § 101a UrhG die Interessen des Lizenzgebers diejenigen des Lizenznehmers überwiegen und verhältnismäßig sein.⁵⁷
- 30** Daneben gewährt § 242 BGB einen allgemeinen, auf Treu und Glauben gestützten Auskunftsanspruch,⁵⁸ welcher eine Sonderverbindung zwischen Lizenzgeber und -nehmer sowie den begründeten Verdacht einer Pflichtverletzung voraussetzt und durch den Anspruch auf Besichtigung nach § 809 BGB ergänzt wird.

2. Vertragliche Ausgestaltung eines Softwarelizenz-Audits

- 31** Ob und inwieweit Softwarelizenz-Audits auf rein gesetzlicher Grundlage in der Praxis möglich und zulässig sind, wird in der Literatur überwiegend kritisch beurteilt.⁵⁹ Zur Vermeidung dieser Unsicherheit werden durch die Hersteller und/oder Anbieter von Software regelmäßig vertragliche Auditierungsrechte gefordert. Derartige vertragliche Auditierungsrechte sehen in der Regel vor, dass dem Lizenzgeber ein anlassloses Recht gewährt wird, die Einhaltung der vertraglich vereinbarten Nutzungsbedingungen überprüfen zu können. Bei der Formulierung einer vertraglichen Auditklausel zur Prüfung der Softwarelizenzen sind insbesondere die vom Prüfer einsehbaren Informationen und Anonymisierungen/Pseudonymisierungen, die Prüfungsfrequenz, die Person des Prüfers, die Prüf-

53 *Czychowski*, in: Fromm/Nordemann, Urheberrecht, § 101 Rn. 82. Umstritten ist, ob die Einschaltung einer zur Verschwiegenheit verpflichteten, neutralen Vertrauensperson geboten ist, der gegenüber die Auskunft anstelle des Anspruchstellers erteilt wird (sog. Wirtschaftsprüfervorbehalt), wie auch wer die Beweislast für die Unverhältnismäßigkeit trägt, siehe hierzu *Kotthoff/Wieczorek*, MMR 2014, 3, 4.

54 BGH, MMR 2013, 526, 527.

55 BT-Drs. 16/5048, S. 49.

56 Siehe hierzu *Kotthoff/Wieczorek*, MMR 2014, 3, 4 m. w. N., die ergänzend darauf hinweisen, dass im Rahmen eines Softwarelizenz-Audits es nicht ausreicht, auf allgemeine Erfahrungswerte hinzuweisen, nach denen Audits für ein bestimmtes Produkt typischerweise Lizenzierungslücken aufzeigen.

57 Dies wird in der Literatur überwiegend streng und deshalb im Ergebnis skeptisch beurteilt, *Kotthoff/Wieczorek*, MMR 2014, 3, 5; *Ohst*, in: Wandtke/Bullinger, Praxiskommentar UrhR, § 101a Rn. 10.

58 Wie sich die §§ 242, 809 BGB zu den §§ 101, 101a UrhG verhalten, ist nicht eindeutig geklärt, zutreffend gehen *Kotthoff/Wieczorek*, MMR 2014, 3, 5, davon aus, dass Einiges dafür spricht, dass die §§ 242, 809 BGB durch die §§ 101, 101a UrhG verdrängt werden.

59 Siehe *Hoeren*, CR 2008, 409 f.; *Huppertz/Schneider*, ZD 2013, 427 ff. m. w. N.; *Intveen*, ITRB 2012, 208, 210 ff.; *Moos*, CR 2006, 797, 798; *Strittmatter/Harnos*, CR 2013, 621 ff.

methode, die verwendeten Applikationen und Messverfahren, eine Vorankündigungspflicht, Verfahrensregeln, Nachkaufkonditionen und Vereinbarungen zur Vertraulichkeit zu regeln.⁶⁰

Sofern es sich bei einem Lizenzvertrag um einen Standardvertrag handelt, ist dieser der AGB-Kontrolle nach den §§ 305 ff. BGB unterworfen.⁶¹ Die Unwirksamkeit einer Auditklausel in AGB kann sich daraus ergeben, dass die Klausel intransparent ist (§ 307 Abs. 1 Satz 2 BGB) oder den Lizenznehmer unangemessen benachteiligt (§ 307 Abs. 1 Satz 1, Abs. 2 Nr. 1 BGB), d. h. insbesondere als Abweichen von dem gesetzlichen Regelfall nach § 101a UrhG zulasten des Lizenznehmers nach § 307 Abs. 2 Nr. 1 BGB unzulässig ist oder der Lizenzgeber durch eine einseitige Vertragsgestaltung missbräuchlich eigene Interessen auf Kosten des Lizenznehmers durchsetzt.⁶² Sofern der Lizenznehmer im Rahmen der Verhandlungen eine echte Wahlfreiheit genießt und eine freie Entscheidung bezüglich der Einbeziehung und Ausgestaltung der Klausel treffen kann, stellen derartige Klauseln keine AGB dar, sondern sind vielmehr individualvertragliche Regelungen, auf die die AGB-Kontrolle der §§ 305 ff. BGB keine Anwendung findet.⁶³

V. Rechte an und Zugang zu nicht-personenbezogenen Daten⁶⁴

Die Datenverordnung (Data Act) wurde am 22.12.2023 im Amtsblatt der Europäischen Union verkündet⁶⁵ und trat am zwanzigsten Tag nach dieser Veröffentlichung in Kraft. Der Data Act gilt nach Ablauf von 20 Monaten ab dem Datum ihres Inkrafttretens.⁶⁶

60 Siehe hierzu *Kotthoff/Wieczorek*, MMR 2014, 3, 9.

61 Die AGB-Kontrolle ist gem. § 305 Abs. 1 Satz 1 BGB eröffnet, wenn eine vom Verwender gestellte Klausel für eine Vielzahl von Verträgen vorformuliert wurde. Die §§ 308, 309 BGB gelten zwischen Unternehmern gem. § 310 Abs. 2 Satz 1 BGB zwar nicht direkt, jedoch entfalten die Normen i. R. v. § 307 BGB als Indizien und Wertungsmöglichkeiten mittelbare Wirkung.

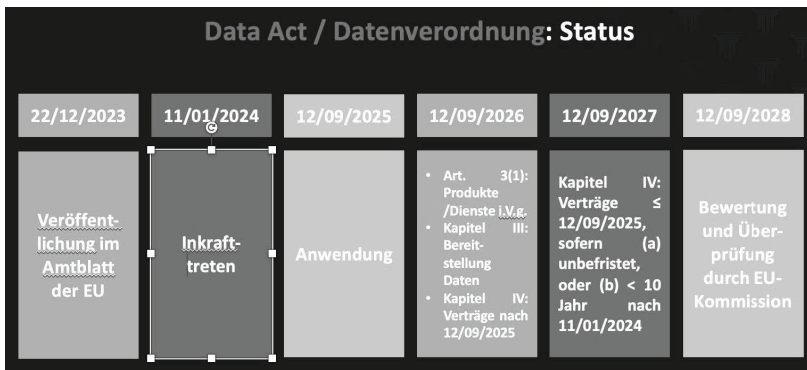
62 Vgl. BGHZ 143, 103, 113; BGH, NJW 2005, 1774, 1775.

63 *Grüneberg*, in: *Grüneberg*, BGB, § 305 Rn. 10 m. w. N.

64 Zum Schutz personenbezogener Daten siehe → *Becker/Böhlke/Fladung*, Kap. 12.

65 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202302854#d1e4429-1-1 (zuletzt abgerufen am 20.3.2024).

66 Art. 3 Abs. 1 (Anforderungen für den vereinfachten Zugang zu Daten für neue Produkte) gilt jedoch für vernetzte Produkte und damit zusammenhängende Dienste, die in Verkehr gebracht werden, nach Ablauf von 32 Monaten ab dem Datum des Inkrafttretens der Verordnung. Darüber hinaus gilt Kapitel III des Data Act nur in Bezug auf Datenbereitstellungspflichten nach dem Unionsrecht oder nach im Einklang mit Unionsrecht erlassenen nationalen Rechtsvorschriften, die nach dem 12.9.2025 in Kraft treten; Kapitel IV gilt für Verträge, die nach dem 12.9.2025 geschlossen wurden, und Kapitel IV gilt ab dem 12.9.2027 für Verträge, die am oder vor dem 12.9.2025 geschlossen wurden, sofern a) sie unbefristet sind oder b) ihre Geltungsdauer frühestens zehn Jahre nach dem 11.1.2024 endet, siehe Art. 50 Data Act.



- 34 Um „die EU zu einem Vorreiter in unserer datengesteuerten Gesellschaft zu machen“,⁶⁷ will der Data Act Vorschriften für einen fairen Datenzugang und eine faire Datennutzung schaffen.
- 35 Daneben basiert der Data Act auf der Grundannahme, dass Hersteller von vernetzten Produkten bzw. Dritte, denen solche Gerätedaten zufließen, *De-facto*-Kontrolle über diese Daten ausüben, sodass sie weder für den Nutzer noch für datengetriebene Geschäftsmodelle von Drittanbietern verfügbar sind.⁶⁸ Der Data Act geht im Hinblick auf Produktdaten oder verbundene Dienstdaten daher davon aus, dass diese „digitalisierte Nutzerhandlungen und -vorgänge darstellen“ und daher „dementsprechend für den Nutzer zugänglich sein sollten“.⁶⁹
- 36 Diesen „Datenschutz“⁷⁰ soll der Data Act durch die in Form einer horizontalen Verordnung⁷¹ vorgesehenen zwingenden Datenzugangs-, Nutzungs- und Weitergaberechte des Nutzers zugänglich machen. Ziel ist, dadurch datengetriebene Geschäftsmodelle auf nachgelagerten Märkten zu etablieren und Innovation zu fördern.⁷²

67 „Die heutige Annahme wird ein Katalysator für ein Europa sein, das für das digitale Zeitalter gerüstet ist. Das neue Gesetz wird ein enormes wirtschaftliches Potenzial freisetzen und erheblich zu einem europäischen Binnenmarkt für Daten beitragen. Der Datenhandel und die übergreifende Nutzung von Daten werden gefördert, und es werden neue Marktchancen zum Nutzen unserer Bürgerinnen und Bürger und Unternehmen in ganz Europa eröffnet.“, Pressemitteilung des Rats der Europäischen Union, abrufbar unter <https://www.consilium.europa.eu/de/press/press-releases/2023/11/27/data-act-council-adopts-new-law-on-fair-access-to-and-use-of-data/> (zuletzt abgerufen am 20.3.2024).

68 Antoine, CR 2024, 1.

69 Erw.-Grd. 15 Data Act.

70 Schweitzer/Metzger, GRUR-Int. 2023, 337.

71 Erw.-Grd. 6, 42 DA. Antoine, CR 2024, 1, 2 weist darauf hin, dass dementsprechend Raum für sektorspezifische Regelungen verbleibt.

72 Erw.-Grd. 20. Assion/Willecke, MMR 2023, 805, 806 weisen allerdings zutreffend darauf hin, dass der Data Act eine Reihe von sehr unterschiedlichen Regelungszielen verfolgt, welche so

Nutzern wird insoweit ein originäres Nutzungsrecht zugewiesen, während die Nutzung der Daten durch den Dateninhaber und Dritte (die Datenempfänger) von einer vertraglichen Genehmigung durch den Nutzer abhängt.⁷³ **37**

1. Regelungsinhalt und Struktur des Data Act

Insgesamt verfolgt der Data Act einen Regulierungsansatz, der nicht auf der klassischen Marktversagenslogik fußt, sondern „durch pro-aktive Regulierung den Versuch eines Market Shaping wagt“.⁷⁴ **38**

Nach Art. 1(2) Data Act erstreckt sich der Regelungsbereich „auf personenbezogene und nicht-personenbezogene Daten, einschließlich der folgenden Arten von Daten“, und grenzt die Regelungsgegenstände, Rechte und Pflichten entsprechend den Kapiteln des Data Act wie folgt ab: **39**

- Kapitel II gilt für die Weitergabe von Daten, mit Ausnahme von Inhalten, die die Leistung, Nutzung und Umgebung von vernetzten Produkten und verbundenen Diensten betreffen;
- Kapitel III gilt für alle Daten des Privatsektors, die rechtlichen Verpflichtungen mit Blick auf die Datenweitergabe unterliegen;⁷⁵
- Kapitel IV gilt für alle Daten des Privatsektors, die auf der Grundlage von Verträgen zwischen Unternehmen abgerufen und genutzt werden;⁷⁶
- Kapitel V gilt für die Bereitstellung aller Daten des Privatsektors mit Schwerpunkt auf nicht-personenbezogenen Daten an öffentliche Stellen wegen „außergewöhnlicher Notwendigkeit“;
- Kapitel VI gilt für alle von Anbietern von Datenverarbeitungsdiensten verarbeiteten Daten und Dienste und regelt umfangreich die Pflichten bei einem Wechsel von Datenverarbeitungsdiensten; und
- Kapitel VII gilt für alle nicht-personenbezogenen Daten, die in der Union von Anbietern von Datenverarbeitungsdiensten gehalten werden, und staatlichen Zugang und die Übermittlung solcher Daten.⁷⁷

ungleich sind, „dass es problemlos möglich gewesen wäre, sie in mehreren separaten Rechtsverordnungen zu regeln“.

73 *Assion/Willecke*, MMR 2023, 805, 807 weisen darüber hinaus zutreffend darauf hin, dass das Recht der Nutzer nicht mit den Schutzrechten der „Betroffenen“ im Rahmen der DSGVO verwechselt werden darf und der Schutz von personenbezogenen Daten nach der DSGVO deutlich weiter reiche als der Schutz von Produkt- und Dienstedaten nach dem Data Act.

74 *Antoine*, CR 2024, 1, 2; *Metzger/Schweitzer*, ZEuP 2023, 42, 49 ff.

75 Kapitel III erfasst also deutlich mehr Daten als Kapitel II, *Assion/Willecke*, MMR 2023, 805, 806.

76 Kapitel IV etabliert darüber hinaus eine inhaltliche Kontrolle von Vertragsklauseln in Bezug auf den Datenzugang und die Datennutzung oder die Haftung und Rechtsbehelfe bei Verletzung oder Beendigung datenbezogener Pflichten, die ein Unternehmen einem anderen Unternehmen einseitig auferlegt, Art. 13 Abs. 1.

77 Zutreffend *Assion/Willecke*, MMR 2023, 805, 806: „Die vorstehende Liste zeigt, dass die Regelungsgegenstände des Data Act sehr weit auseinander gehen. Der einzige gemeinsame Nenner der Regelungen des „Data Act“ ist letztlich (nur), dass alle seine Regelungen sich ir-

- 40 Die nachfolgende Darstellung fokussiert sich auf die Regelungen zur Datenweitergabe nach Kapitel II und III, zu missbräuchlichen Vertragsklauseln in Bezug auf den Datenzugang und die Datennutzung nach Kapitel IV und zum Wechsel zwischen Datenverarbeitungsdiensten nach Kapitel VI der Datenverordnung.

2. Datenweitergabe unter dem Data Act

- 41 Der Anwendungsbereich der Regelungen zum Datenzugang und zur Datenweitergabe des Data Act richtet sich maßgeblich an drei zentralen Rollen aus und deren Nutzung von „verbundenen Produkten“⁷⁸ oder „verbundenen Diensten“⁷⁹ aus.
- 42 „Nutzer“ ist eine natürliche oder juristische Person, die ein vernetztes Produkt besitzt oder der vertraglich zeitweilige Rechte für die Nutzung des vernetzten Produkts übertragen wurden oder die verbundenen Dienste in Anspruch nimmt (Art. 2(12) Data Act). Demgegenüber ist ein „Dateninhaber“ eine natürliche oder juristische Person, die nach dem Data Act, nach geltendem Unionsrecht oder nach nationalen Rechtsvorschriften berechtigt oder verpflichtet ist, Daten zu nutzen und bereitzustellen Art. 2(13) Data Act).
- 43 Sofern mehrere Personen gleichzeitig Nutzer eines vernetzten Produkts oder eines damit verbundenen Dienstes sind, hat jede dieser Personen die Rechte als „Nutzer“ unter dem Data Act.⁸⁰
- 44 Zusätzlich räumt der Data Act auch Drittparteien, den Datenempfängern, Datenzugangsrechte ein. Ein „Datenempfänger“ ist eine natürliche oder juristische Person, die zu Zwecken innerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handelt, ohne Nutzer eines vernetzten Produktes oder verbundenen Dienstes zu sein, und der vom Dateninhaber Daten bereitgestellt werden, einschließlich eines Dritten, dem der Dateninhaber auf

gendwie auf Daten beziehen. Es sind aber keineswegs überall dieselben Datenarten gemeint.“

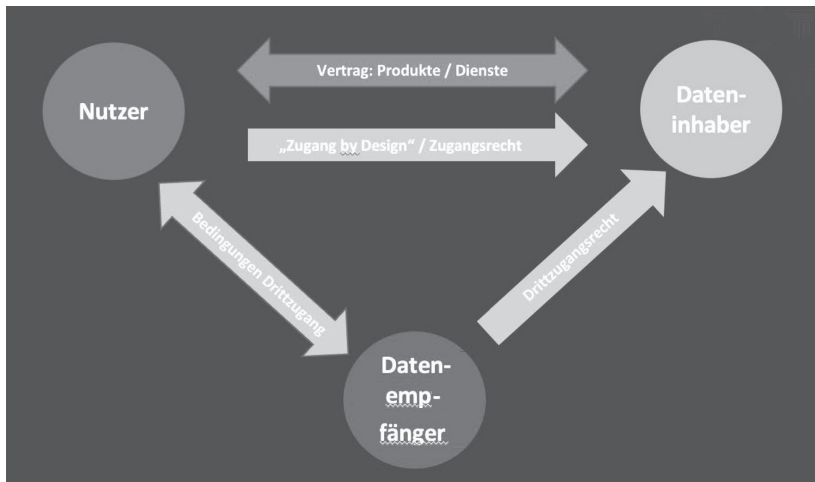
78 Ein „vernetztes Produkt“ ist ein „Gegenstand, der Daten über seine Nutzung oder Umgebung erlangt, generiert oder erhebt und der Produktdaten über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang übermitteln kann und dessen Hauptfunktion nicht die Speicherung, Verarbeitung oder Übertragung von Daten im Namen einer anderen Partei – außer dem Nutzer – ist, Art. 2 (5) Data Act. Der letzte Halbsatz zielt auf den Betrieb von Servern oder Cloud-Infrastrukturen ab, die von ihren Eigentümern ausschließlich im Auftrag Dritter betrieben werden, siehe Erw-Grd. 16 Data Act.

79 Ein „verbundener Dienst“ ist ein „digitaler Dienst, bei dem es sich nicht um einen elektronischen Kommunikationsdienst handelt – einschließlich Software –, der zum Zeitpunkt des Kaufs, der Miete oder des Leasings so mit dem Produkt verbunden ist, dass das vernetzte Produkt ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte oder der anschließend vom Hersteller oder einem Dritten mit dem Produkt verbunden wird, um die Funktionen des vernetzten Produkts zu ergänzen, zu aktualisieren oder anzupassen, Art. 2 (6) Data Act. Assion/Willecke, MMR 2023, 805, 807 weisen darauf hin, dass „die unpräzise gestaltete Rechtslage viel Raum für Interpretation lässt“.

80 Erw.-Grd. 18 Data Act.

Verlangen des Nutzers oder im Einklang mit einer rechtlichen Verpflichtung aus anderem Unionsrecht oder aus nationalen Rechtsvorschriften Daten bereitstellt (Art. 2(14) Data Act).

Die Zugangs- und Weitergaberechte nach Kapitel II und III des Data Act finden in sachlicher Hinsicht Anwendung auf durch vernetzte Produkte und verbundene Dienste generierte Daten; in räumlicher Hinsicht erstreckt sich der Anwendungsbereich nach Art. 1(3) Data Act auf vernetzte Produkte, die in der EU auf den Markt gebracht werden, unabhängig von der Niederlassung des Herstellers/Anbieters, und kommt überdies zur Anwendung, wenn der Nutzer oder Datenempfänger in der EU ansässig ist.⁸¹ **45**



a) Allgemeine Pflichten

Nach Art. 3(1) Data Act müssen vernetzte Produkte so konzipiert und hergestellt und verbundene Dienste so konzipiert und erbracht werden, dass die Produktdaten und verbundenen Dienstdaten – einschließlich der für die Auslegung und Nutzung dieser Daten erforderlichen relevanten Metadaten – standardmäßig für den Nutzer einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, direkt zugänglich sind („Data Access by Design“). **46**

Darüber hinaus sieht Art. 3(2) Data Act Transparenzpflichten des Verkäufers, Vermieters oder Leasinggebers vor Abschluss eines Vertrages vor, indem mindestens die folgenden Informationen „in klarer und verständlicher Art und Weise“ bereitgestellt werden müssen: **47**

⁸¹ Antoine, CR 2024, 1, 2.

- die Art, das Format und der geschätzte Umfang der Produktdaten, die das vernetzte Produkt generieren kann;
- die Angabe, ob das vernetzte Produkt in der Lage ist, Daten kontinuierlich und in Echtzeit zu generieren;
- die Angabe, ob das vernetzte Produkt in der Lage ist, Daten auf einem Gerät oder einem entfernten Server zu speichern, gegebenenfalls einschließlich der vorgesehenen Speicherdauer; und
- die Angabe, wie der Nutzer auf die Daten zugreifen, sie abrufen oder gegebenenfalls löschen kann, einschließlich der technischen Mittel hierfür sowie die betreffenden Nutzungsbedingungen und die betreffende Dienstqualität.

b) Erfasste Datenkategorien

- 48** Produkt- und verbundene Dienstdaten umfassen nur solche Daten, die bei der Nutzung eines vernetzten Produkts oder während der Erbringung eines verbundenen Dienstes generiert werden.
- 49** Nicht als Produkt- und verbundene Dienstdaten gelten demgegenüber aus Daten gefolgerte oder abgeleitete Informationen, die das Ergebnis zusätzlicher Investitionen in die Zuweisung von Werten oder Erkenntnissen aus den Daten sind (insbesondere mittels komplexer proprietärer Algorithmen, einschließlich solcher, die Teil proprietärer Software sind).⁸²
- 50** Daneben sind nicht erfasst Daten, die bei der Nutzung von sonstigen Diensten (inkl. unabhängiger Software) oder beim Abspielen von Inhalten (inkl. der Inhalte selbst) generiert werden.⁸³

c) Datenzugriffsrechte für Nutzer

- 51** Sofern Nutzer nicht direkt von dem vernetzten Produkt oder verbundenen Dienst auf die Daten zugreifen können („Data Access by Design“), müssen Dateninhaber gemäß Art. 4(1) Data Act die „ohne Weiteres verfügbaren Daten einschließlich der zur Auslegung und Nutzung der Daten erforderlichen Metadaten“ bereitstellen.
- 52** Die Bereitstellung hat dabei „unverzüglich, einfach, sicher, unentgeltlich, in einem umfassenden, gängigen und maschinenlesbaren Format und – falls relevant und technisch durchführbar – in der gleichen Qualität wie für den Dateninhaber kontinuierlich und in Echtzeit“ zu erfolgen.
- 53** Der Nutzer ist dann berechtigt, diese Daten grundsätzlich zu jedem rechtmäßigen Zweck zu nutzen; dies umfasst insbesondere auch die Weitergabe der erhaltenen Daten an Dritte, zu kommerziellen und nicht-kommerziellen Zwecken.⁸⁴

⁸² Erw.-Grd. 15 Data Act.

⁸³ Antoine, CR 2024, 1, 3.

⁸⁴ Antoine, CR 2024, 1, 5; siehe Art. 4(10) und Art. 5(3)(c) Data Act sowie Erw.-Grd. 26 und 33.

Der Datenzugriff von Nutzern kann jedoch durch einen Dateninhaber vertraglich beschränkt werden, wenn dies die im Unionsrecht oder im nationalen Recht festgelegten Sicherheitsanforderungen des vernetzten Produkts beeinträchtigen und damit zu schwerwiegenden nachteiligen Auswirkungen auf die Gesundheit oder die Sicherheit von natürlichen Personen führen könnte (Art. 4(2)(1) Data Act). **54**

Außerdem sollen Geschäftsgeheimnisse nur offengelegt werden, „wenn vom Dateninhaber und vom Nutzer vor der Offenlegung alle Maßnahmen getroffen worden sind, die erforderlich sind, um die Vertraulichkeit der Geschäftsgeheimnisse, insbesondere gegenüber Dritten, zu wahren“ (Art. 4(6) Data Act). Der Schutz von Geschäftsgeheimnissen unter dem Data Act wird allerdings nur als „eine Art ultima ratio“ angesehen, falls keine andere Möglichkeit zum Schutz der Geschäftsgeheimnisse besteht.⁸⁵ **55**

Sollte sich ein Dateninhaber auf ein Verweigerungsrecht berufen, hat er dies der zuständigen Aufsichtsbehörde anzuzeigen (Art. 4(2) und 4(8) Data Act). Daneben kann ein betroffener Nutzer Beschwerde bei dieser Aufsichtsbehörde einlegen oder eine Streitbeilegungsstelle unter dem Data Act anrufen (Art. 4(3) und 4(9) Data Act). **56**

d) Recht der Nutzer auf Datenweitergabe an Dritte

Nutzer können nicht nur die Weitergabe der Produkt- und Dienstedaten und der zur Auslegung dieser Daten notwendigen Metadaten an sich selbst verlangen, sondern auch an Dritte (Art. 5(1) Data Act).⁸⁶ Der Nutzer ist in der Auswahl des Dritten grundsätzlich frei⁸⁷; Ausnahme sind Gatekeeper i.S.d. Art. 3 Digital Markets Act (Art. 5(3) Data Act). **57**

Die Pflicht zur Datenherausgabe an Dritte ist grundsätzlich an ähnliche Voraussetzungen geknüpft wie die Pflicht zur Herausgabe an den Nutzer:⁸⁸ Die Daten sind „unverzüglich, für den Nutzer unentgeltlich, in derselben Qualität, die dem Dateninhaber zur Verfügung steht, einfach, sicher, für den Nutzer unentgeltlich, in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, kontinuierlich und in Echtzeit“ bereitzustellen. **58**

Nach Art. 6(1) Data Act schließen auch Nutzer und Dritter eine Vereinbarung über Bedingungen und Zwecke, für die die Daten zugänglich gemacht werden und nach der sich die Nutzungsbefugnis des Dritten bestimmt. **59**

⁸⁵ Assion/Willecke, MMR 2023, 805, 808.

⁸⁶ Gemeint sind damit in erster Linie Unternehmen, die mit den Dateninhabern auf abgeleiteten Märkten konkurrieren, die sich auf die vernetzten Produkte beziehen, Erw.-Grd. 15 und 25 Data Act.

⁸⁷ Antoine, CR 2024, 1, 7 weist darauf hin, dass sich der Dritte nicht einmal in der EU befinden muss.

⁸⁸ Assion/Willecke, MMR 2023, 805, 808.

- 60 In B2B-Verhältnissen müssen sich Dateninhaber und Dritter überdies entsprechend Art. 8 und Art. 9 Data Act über die Bedingungen für die Datenbereitstellung inklusive einer angemessenen Vergütung⁸⁹ einigen. Nach Art. 8(1) Data Act ist der Dateninhaber dabei verpflichtet, Datenzugang zu fairen, angemessenen und nichtdiskriminierenden Bedingungen bereitzustellen (FRAND-Konditionen – „fair, reasonable and non-discriminatory“).⁹⁰

3. Verhältnis zum Datenschutzrecht

- 61 Umstritten ist das Verhältnis des Data Act zum Datenschutzrecht, insbesondere zur DSGVO.⁹¹ Zwar enthält der Data Act die grundsätzliche Aussage, dass dieser „unbeschadet des Unionsrechts und des nationalen Rechts über den Schutz personenbezogener Daten“, also insbesondere der DSGVO gelte (Art. 1(5) Data Act).
- 62 Im Detail ist allerdings unklar, was im Hinblick auf Datenherausgabeansprüche unter dem Data Act gilt, sofern die Daten auch personenbezogene Daten enthalten und der Anspruchsberechtigte unter dem Data Act nicht zugleich auch der Betroffene unter der DSGVO ist.⁹² Ein Dateninhaber, der zur Weitergabe nicht-personenbezogener Daten unter dem Data Act verpflichtet wäre, müsste daneben auch sicherstellen, dass, sofern der Ersuchende unter dem Data Act nicht zugleich Betroffener unter der DSGVO ist, auch eine entsprechende Rechtsgrundlage für die Weitergabe personenbezogener Daten gegeben ist.⁹³

4. Nutzung durch und Weitergabe von Daten durch den Dateninhaber

- 63 Eine wesentliche Neuerung des Data Act betrifft die Nutzung und Weitergabe nicht-personenbezogener Daten durch den Dateninhaber. Da durch den Data Act gerade keine ausschließliche Rechtsposition an den betreffenden Daten geschaffen werden soll,⁹⁴ überrascht es allerdings, dass „Nutzer und Dateninhaber keine

89 Art. 9 Data Act.

90 Zum Verhältnis zu Art. 13 Data Act, siehe unten → Rn. 68 ff.

91 *Hartl/Jentzen*, ZdiW 2023, 65, 66 f.; *Hartmann/McGuire/Schulte-Nölke*, RDi 2023, 49, 52 f.; *Richter*, MMR 2023, 163; *Steinrötter*, GRUR 2023, 216.

92 Erw.-Grd. 7 stellt hierzu klar: „Handelt es sich bei dem Nutzer nicht um die betroffene Person, so bietet die vorliegende Verordnung keine Rechtsgrundlage für die Gewährung des Zugangs zu personenbezogenen Daten oder für deren Bereitstellung an Dritte und sollte nicht so verstanden werden, dass sie dem Dateninhaber ein neues Recht auf die Nutzung personenbezogener Daten, die bei der Nutzung eines vernetzten Produkts oder verbundenen Dienstes generiert wurden, verleiht.“ Hierdurch wird allerdings nicht klargestellt, ob nicht schon Art. 6(1)(c) DSGVO eine existierende Rechtsgrundlage darstellt. Nach *Assion/Willecke*, MMR 2023, 805, 808 ist die Rechtslage „vor allem eins: Unklar“.

93 *Hartmann/McGuire/Schulte-Nölke*, RDi 2023, 49, 56 weisen zutreffend darauf hin, dass die immer noch diskutierte Frage, ob Daten einen Personenbezug aufweisen, sich somit auch auf den Data Act auswirkt.

94 Erw.-Grd. 6 Data Act.

äquivalente Position einnehmen, sondern der Data Act einem strikt nutzerzentrierten Modell folgt“.⁹⁵

Nach Art. 4(13) Data Act dürfen Dateninhaber „ohne Weiteres verfügbare“⁹⁶ nicht-personenbezogene Daten nur auf Grundlage eines Vertrages mit dem jeweiligen Nutzer oder den jeweiligen Nutzern verarbeiten. Außerdem darf ein Dateninhaber solche Daten auch nicht verwenden, „um daraus Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden des Nutzers oder in die Nutzung durch den Nutzer auf jegliche andere Art, die die gewerbliche Position dieses Nutzers auf Märkten, auf denen dieser tätig ist, untergraben könnte, zu erlangen“.⁶⁴

Daneben etabliert Art. 4(14) Data Act, dass Dateninhaber „nicht-personenbezogene Produktdaten“ Dritten zu keinen anderen kommerziellen oder nichtkommerziellen Zwecken als zur Erfüllung ihres Vertrags mit dem Nutzer bereitstellen. Diese Einschränkung wird ergänzt durch Art. 8(4) Data Act, wonach Daten einem Datenempfänger vom Dateninhaber nur dann bereitgestellt werden dürfen, wenn ein Nutzer dies verlangt hat.⁶⁵

Anders als in Art. 7 Abs. 4 DSGVO enthalten die Datennutzungsregelungen des Data Act allerdings gerade kein Kopplungsverbot, d. h. es existiert kein Verbot, die Nutzung vernetzter Produkte oder verbundener Dienste von der Zustimmung der Nutzung der nicht-personenbezogenen Daten durch den Dateninhaber abhängig zu machen.⁹⁷ Daher wird der Erwerb des Produkts bzw. die Inanspruchnahme des Dienstes vielfach schlicht an eine entsprechende Vereinbarung zur Datennutzung i. S. d. Art. 4(13) Data Act gekoppelt sein.⁹⁸⁶⁶

Zutreffend wird darauf hingewiesen, dass eine solche Kopplung allerdings schwierige AGB-rechtliche Fragen aufwerfen wird. Während im B2C-Bereich die nationalen Regeln der §§ 307 ff. BGB zur Anwendung kommen, ist für das B2B-Verhältnis Art. 13 Data Act maßgeblich.⁹⁹⁶⁷

⁹⁵ *Antoine*, CR 2024, 1, 2.

⁹⁶ Siehe Art. 2(17) und Erwägungsgrund 20 Data Act.

⁹⁷ Dennoch bringen die Datennutzungsregelungen des Data Act unter anderem auch erhebliche praktische Schwierigkeiten bei der Nutzung von Bestandsdaten oder Bestandsverträgen mit sich.

⁹⁸ *Bomhard/Merkle*, RDi 2022, 168, 174; *Specht-Riemenschneider*, ZRP 2022, 137, 139; *Podszun/Pfeifer*, GRUR 2022, 953, 956.

⁹⁹ *Antoine*, CR 2024, 1, 5, die ergänzend darauf hinweist, dass der Nutzer dadurch aber gerade nicht daran gehindert wird, seinerseits die Zugangs-, Nutzungs- und Weitergaberechte des Data Act geltend zu machen, da letzteres nach Art. 7(2) bzw. Art. 12(2) Data Act nicht möglich sei, und dass es im Falle von mehreren Nutzern darüber hinaus für einen Dateninhaber schwierig sei festzustellen, ob es weitere Nutzer gibt, mit denen er eine Vereinbarung i. S. d. Art. 4(13) Data Act schließen müsste, um die ihm zufließenden generierten Daten nutzen zu dürfen.

5. Missbräuchliche Vertragsklauseln

- 68 Ergänzend zu den vorgenannten Regelungen zu Datenweitergabe/Datenzugang und zur Datennutzung bestimmt Art. 13 Data Act, dass einseitig auferlegte Vertragsklauseln¹⁰⁰ „in Bezug auf den Datenzugang und die Datennutzung“ oder „die Haftung und Rechtsbehelfe bei Verletzung oder Beendigung datenbezogener Pflichten“ für ein Unternehmen nicht bindend sind, wenn sie missbräuchlich sind.¹⁰¹
- 69 Neben der Generalklausel des Art. 13(3) Data Act, wonach Vertragsklauseln missbräuchlich sind, wenn ihre Anwendung „eine grobe Abweichung von der guten Geschäftspraxis bei Datenzugang und Datennutzung darstellt“ oder „gegen das Gebot von Treu und Glauben verstößt“, enthält Art. 13(4) Data Act Beispiele für missbräuchliche Klauseln und Art. 13(5) Data Act Beispiele für Klauseln, bei denen die Missbräuchlichkeit vermutet wird.
- 70 Missbräuchliche Klauseln ohne Wertungsmöglichkeit nach Art. 13(4) Data Act sind insbesondere Klauseln, welche die Haftung für Vorsatz oder grobe Fahrlässigkeit ausschließen oder beschränken, Rechtsbehelfe bei Nichterfüllung ausschließen oder die Haftung beschränken oder einseitig das Recht gewähren, zu entscheiden, ob gelieferte Daten vertragsgemäß sind.
- 71 Klauseln mit vermuteter Missbräuchlichkeit nach Art. 13(5) Data Act sind insbesondere solche Klauseln, die eine „unangemessene Beschränkung“ der Rechtsmittel bei Nichterfüllung von Vertragspflichten oder der Haftung bei einer Verletzung dieser Pflichten bezwecken oder bewirken, den Zugang und die Nutzung von Daten einer Partei entgegen deren berechtigten Interessen gestatten oder die zugrunde liegende Vereinbarung innerhalb einer angemessenen Frist zu kündigen oder abzuändern.
- 72 Die Missbrauchskontrolle gilt allerdings nicht für Vertragsklauseln, in denen der Hauptgegenstand des Vertrags festgelegt wird, oder Klauseln welche die Angemessenheit des Preises für die als Gegenleistung weitergegebenen Daten bestimmen.¹⁰²

6. Sanktionen

- 73 Im Unterschied zur DSGVO enthält der Data Act kein detailliertes Sanktionsregime. Vielmehr gibt Art. 40(1) Data Act lediglich vor, dass die Mitgliedstaaten

100 Nach Art. 13(6) Data Act gelten Vertragsklauseln als einseitig auferlegt, wenn sie von einer Vertragspartei eingebracht werden und die andere Vertragspartei ihren Inhalt trotz des Versuchs, hierüber zu verhandeln, nicht beeinflussen kann.

101 So auch *Antoine*, CR 2024, 1, 7: „Deshalb sollte Art. 8 (1) DA dahingehend ausgelegt werden, dass der – für Datenzugang ohnehin schwer zu fassende – FRAND-Maßstab lediglich in den Fällen, in denen sich Dateninhaber und Datenempfänger *nicht* über Bedingungen einigen können, heranzuziehen ist.“

102 Art. 13(8) Data Act.

Vorschriften über Sanktionen erlassen, die „wirksam, verhältnismäßig und abschreckend“ sein müssen.

VI. Wechsel von Datenverarbeitungsdiensten

In Ergänzung zu den vorgenannten Regelungen zur Datenweitergabe und Datennutzung, sieht der Data Act in den Art. 23 ff. umfangreiche Regelungen zum Wechseln von Datenverarbeitungsdiensten¹⁰³ und den hierbei anzuwendenden Konditionen vor. **74**

Hierbei sind nach Art. 23 Data Act solche Hindernisse für einen wirksamen Wechsel zu beseitigen, welche Kunden von Datenverarbeitungsdiensten daran hindern, einen Vertrag über einen Datenverarbeitungsdienst nach der maximalen Kündigungsfrist und dem Wechselprozess nach Art. 25 Data Act zu kündigen, neue Verträge mit einem anderen Anbieter von Datenverarbeitungsdiensten für die gleiche Dienstleistung abzuschließen, exportierbare Daten des Kunden und digitale Vermögenswerte zu übertragen oder Funktionsäquivalenz¹⁰⁴ zu erreichen. **75**

Hierdurch ergeben sich für die Anbieter solcher Datenverarbeitungsdienste unter anderem Herausforderungen bei der internen Umsatzanerkennung sowie bei der Frage, ob Mindestvertragslaufzeiten und Vorfälligkeitsentschädigungen weiterhin zulässig sind. **76**

Die Hindernisse für einen Wechsel sind dabei sowohl bei einem Wechsel zu einem anderen Datenverarbeitungsdienst als auch zu einem sog. On-Premise-Dienst („IKT-Infrastruktur in eigenen Räumlichkeiten“) zu beseitigen. **77**

Die Rechte des Kunden und die Pflichten des Anbieters von Datenverarbeitungsdiensten in Bezug auf den Wechsel zwischen Anbietern solcher Dienste sind „eindeutig in einem schriftlichen Vertrag“ festzulegen,¹⁰⁵ welcher mindestens die folgenden Inhalte enthalten soll:¹⁰⁶ Klauseln, die es dem Kunden ermöglichen, auf Verlangen und nach Ablauf einer Übergangsfrist und der im Data Act vorgesehenen maximalen Kündigungsfrist¹⁰⁷ zu einem anderen Datenverarbeitungsdienst zu wechseln, die Pflicht des bisherigen Anbieters, die Ausstiegsstrategie des Kunden zu unterstützen, und eine abschließende Auflistung aller Kategorien von Daten und digitalen Vermögenswerten, die übertragen werden können. **78**

¹⁰³ Siehe Art. 2(8) Data Act.

¹⁰⁴ Siehe Art. 24 Data Act.

¹⁰⁵ Art. 25(1) Data Act.

¹⁰⁶ Siehe Art. 25(2) Data Act für eine vollständige Liste.

¹⁰⁷ Die nach Art. 25(2)(d) Data Act „zwei Monate nicht überschreiten darf“. Daneben hat der Kunde nach Art. 25(3) Data Act das im Vertrag zu vereinbarende Recht, den Anbieter des Datenverarbeitungsdienstes nach Ablauf der maximalen Kündigungsfrist darüber zu unterrichten, ob er einen Wechsel zu einem neuen Anbieter eines Datenverarbeitungsdienstes, zu einer On-Premise-Lösung oder die Löschung seiner exportierbaren Daten und digitalen Vermögenswerte wünscht.

- 79** Sollte der vorgenannte maximale Übergangszeitraum technisch nicht realisierbar sein, so hat der Anbieter des Datenverarbeitungsdienstes dies innerhalb von 14 Arbeitstagen mitzuteilen und einen alternativen Zeitraum anzugeben, der sieben Monate nicht überschreiten darf.¹⁰⁸ Des Weiteren hat der Vertrag zwischen dem Kunden und dem Anbieter eines Datenverarbeitungsdienstes Klauseln zu enthalten, wonach der Kunde berechtigt ist, den Übergangszeitraum einmal um einen Zeitraum zu verlängern, „den er für seine eigenen Zwecke für angemessener hält“.¹⁰⁹
- 80** Daneben hat der Anbieter von Datenverarbeitungspflichten umfangreiche Informationspflichten (Art. 26 Data Act).

VII. Blockchain und Smart Contracts

- 81** Unter einer Blockchain (Blockkette) wird eine verteilte Datenbank (Distributed Ledger) verstanden, die eine erweiterbare Liste von Datensätzen enthält und deren Integrität (Sicherung gegen nachträgliche Manipulation) durch Speicherung der (kryptografischen) Prüfsumme des vorangehenden Datensatzes im jeweils nachfolgenden gesichert ist.¹¹⁰ Ausgangspunkt einer Blockchain ist ein Software-Client, der zunächst eine individuelle ID generiert, die mit einem Private Key anhand der zugehörigen Public Keys von anderen Clients identifiziert werden kann.¹¹¹
- 82** Die wesentlichen Elemente einer Blockchain und jeder darauf aufsetzenden Anwendung sind deren dezentraler Aufbau und die Verifikation von Willenserklärungen ohne zentrale Instanz. Dies führt dazu, dass beispielsweise Transaktionen ohne Intermediäre durchgeführt werden können, welche üblicherweise die Rolle der Verifikationsstelle einnehmen. Die Verifikation erfolgt innerhalb einer Blockchain vielmehr durch die einzelnen Mitglieder des Netzwerks: Hat eine bestimmte Anzahl der Mitglieder bzw. Clients einen Vorgang bestätigt, wird die Blockchain um diesen verifizierten Vorgang fortgeschrieben.¹¹²
- 83** In Zusammenhang mit einer Blockchain werden häufig auch sog. „Smart Contracts“ verwendet, also Computerprotokolle, welche die Logik von Verträgen abbilden oder überprüfen oder die Verhandlung oder Abwicklung eines Vertrages technisch unterstützen.
- 84** Der Data Act definiert einen „intelligenten Vertrag“ als „ein Computerprogramm, das für die automatisierte Ausführung einer Vereinbarung oder eines Teils davon verwendet wird, wobei eine Abfolge elektronischer Datensätze ver-

108 Art. 25(4) Data Act.

109 Art. 25(5) Data Act.

110 Klein, DSRITB 2015, 429, 433.

111 Engelhardt/Klein, MMR 2014, 355, 355 f.; Spindler/Bille, WM 2014, 1357, 1358.

112 Klein, DSRITB 2015, 429, 433.

wendet wird und die Integrität dieser Datensätze sowie die Richtigkeit ihrer chronologischen Reihenfolge gewährleistet werden“.¹¹³

Smart Contracts werden dabei auch als geeignete technische Schutzmaßnahme angesehen, um den unbefugten Zugang zu Daten zu verhindern und die Einhaltung der Bedingungen, unter denen Dateninhaber Datenempfängern Daten bereitstellen, sicherzustellen.¹¹⁴ Nutzer, Dritte und Datenempfänger dürfen solche technischen Schutzmaßnahmen nur ändern oder aufheben, wenn der Dateninhaber dem zugestimmt hat.¹¹⁵ **85**

Dies betrifft zum einen schon den Vertragsschluss und die Einordnung von M2M-Kommunikation in Form von Smart Contracts als rechtsverbindliche Willenserklärungen wie auch die Bestimmung des anwendbaren Rechts und datenschutzrechtliche Fragestellungen. **86**

Auch vor dem Hintergrund des großen Potenzials der Blockchain und von Smart Contracts sollten Unternehmen im Rahmen einer Risikoeinschätzung diesen Rechtsfragen ausreichend Beachtung und eine umfassende rechtliche Würdigung schenken. **87**

VIII. Implementierung eines IT-Compliance-Systems

Grundlage jeder unternehmerischen Entscheidung sollte also die Schaffung einer ausreichenden Tatsachengrundlage sein. Eine Unternehmensleitung muss daher nicht nur alle zur Verfügung stehenden Erkenntnisquellen ausschöpfen, sondern unter Abwägung zwischen Kosten und Nutzen einer ausgiebigen Tatsachenermittlung auch permanent in der Lage sein, unternehmerische Entscheidungen zu treffen. **88**

Um zu ermitteln, welche Inhalte Teil einer IT-Compliance sein sollen, bedarf es einer individuellen, d. h. auf das Unternehmen (insbesondere hinsichtlich seiner Anforderungen an IT-Sicherheit, seiner Tätigkeitsbranche, seiner Größe, der anfallenden Datenmenge) zugeschnittenen Risikoanalyse. Hierbei sollten die jeweiligen Besonderheiten Teil der rechtlichen Folgenabschätzung und Risikoabwägung sein, insbesondere aus urheber-, daten- und datenschutzrechtlicher Sicht. **89**

Um ein ordnungsgemäßes Lizenzmanagement zu gewährleisten, muss zunächst der vorhandene Softwarenutzungsbedarf ermittelt werden, wobei, entsprechend den obigen Ausführungen, zwischen On-Premise- und On-Demand-Software unterschieden werden muss. **90**

113 Art. 2(39) Data Act.

114 Art. 11(1) Data Act.

115 Beim Einsatz solcher technischen Schutzmaßnahmen sind allerdings die Anforderungen in Art. 36 Data Act zu beachten, insbesondere hinsichtlich Robustheit und Zugangskontrolle, Datenarchivierung und Datenkontinuität und der Durchführung einer Konformitätsbewertung.

- 91** Im Anschluss sind der Inhalt und die Nutzungsrechte aus den vorhandenen Lizenz- und Wartungsverträgen festzustellen. Die anschließende Erstellung einer Datenbank sollte weitgehend automatisiert erfolgen und diese sich einfach aktualisieren lassen sowie Schnittstellen zu Drittsystemen bieten. Daneben sollte ein aktuelles Lizenzmanagement-System in der Lage sein, komplexe und verteilte Firmenstrukturen zu erfassen.
- 92** Im Hinblick auf die Nutzung von und Rechte an Daten sind, neben den Vorschriften des Datenschutzrechts¹¹⁶ und der Datensicherheit,¹¹⁷ eine angemessene Data Governance und Data Compliance zu beachten.
- 93** Data Governance definiert, wer innerhalb einer Organisation die Autorität und Kontrolle über definierte Datenbestände hat und wie diese Datenbestände verwendet werden dürfen. Dies betrifft insbesondere die Fähigkeit einer Organisation, eine hohe Datenqualität während des gesamten Lebenszyklus von Daten zu gewährleisten und Datenkontrollen zu implementieren, die die Geschäftsziele unterstützen. Das System umfasst die Personen, Prozesse und Technologien, die erforderlich sind, um die Daten sowie deren Wege in einem Unternehmen zu schützen und effizient zu verwalten.¹¹⁸
- 94** Demgegenüber geht es bei Daten-Compliance darum, sicherzustellen, dass die unternehmensinternen Datenpraktiken mit rechtlichen Anforderungen und Industriestandards für die Erfassung, Handhabung und Verwendung von Daten im Einklang stehen. Daten-Compliance kann als ein Teil sowie Ergebnis eines umfassenden Data-Governance-Programms gesehen werden.

¹¹⁶ Siehe → *Becker/Böhlke/Fladung*, Kap. 12.

¹¹⁷ Siehe → *Bensing*, Kap. 14.

¹¹⁸ *Gaess*, IT-Governance, 8. Data-Governance, S. 74, 75.

14. Kapitel

Cybersecurity, IT-Sicherheit und Krisenmanagement

I. Analyse

1. Ziele der IT-Sicherheit

Sowohl die diversen gesetzlichen Vorgaben zur IT-Sicherheit, als auch das davon unabhängige Bestreben von Unternehmen, IT-Sicherheit so weit wie möglich zu gewähren, verfolgen verschiedene Ziele. Diese Ziele zu verstehen ist wichtig für das Verständnis und die Auslegung der jeweiligen Vorgaben. 1

Vor dem im Juli 2015 in Kraft getretenen IT-Sicherheitsgesetz¹ waren Unternehmen in Deutschland zur IT-Sicherheit im Wesentlichen nur in zwei Kategorien verpflichtet: Alle Unternehmen (und im Übrigen auch andere, insb. Öffentliche Institutionen) mussten schon bisher im Bereich des Datenschutzes durch das BDSG-alt und die Landesdatenschutzgesetze die Sicherheit von IT-Systemen gewährleisten. Diese Verpflichtung, die seit 2018 durch die Datenschutz-Grundverordnung (DSGVO)² ersetzt bzw. ergänzt wurde (siehe hierzu → Rn. 45 ff. gilt unabhängig von dem Sektor, in dem das Unternehmen tätig ist, und auch unabhängig von den konkreten Tätigkeiten, denn Ziel der Vorschriften ist es, so weit wie möglich zu gewährleisten, dass personenbezogene Daten,³ die von dem Unternehmen verarbeitet und gespeichert werden, gesichert und vor dem Zugriff Dritter geschützt sind.⁴ Ob andere Teile des IT-Systems gesichert sind, ist in diesem Zusammenhang irrelevant, und entsprechend unterlagen Unternehmen bis 2015 diesbezüglich keinen allgemeinen gesetzlichen Verpflichtungen. Einzige Ausnahme bildeten schon vor dem IT-Sicherheitsgesetz einige wenige Sektoren oder Arten von Unternehmen wie etwa Kreditunternehmen nach dem KWG oder Energieunternehmen nach dem EnWG. Abgesehen davon, dass es sich bei diesen Regelungen um recht allgemeine, unspezifische Vorschriften handelte, dienen diese Vorschriften dem institutionellen Schutz von (zum Beispiel) Banken und Kreditunternehmen, die zum einen wichtige und sensible Geschäfte für ihre Kunden tätigen und einen besonders hohen Grad an Integrität und Verlässlichkeit bieten müssen, zum anderen wichtige Funktionen in der Gesellschaft übernehmen, nämlich in unserem Beispiel die Gewährleistung des Zahlungsver- 2

1 BGBl. I, S. 1324.

2 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L119/1 v. 4.5.2016.

3 Zur Definition personenbezogener Daten nach Datenschutzrecht siehe → *Becker/Böhlke/Fladung*, Kap. 12 Rn. 43 ff.

4 Zum Datenschutz beim Compliance Management ausführlich → *Becker/Böhlke/Fladung*, Kap. 12 Rn. 1 ff.

kehrs, deren Wegfall oder Beeinträchtigung verheerende Folgen hätte und es deshalb zu verhindern gilt.

- 3 Demgegenüber gibt es Compliance-Verpflichtungen des Vorstands einer Aktiengesellschaft oder der Geschäftsführung einer GmbH, die sich auch auf die Gewährleistung der IT-Sicherheit richten. Diese Verpflichtungen sollen wiederum das Unternehmen selbst und seine Aktionäre bzw. Gesellschafter vor Schäden durch Angriffe auf die IT-Infrastruktur eines Unternehmens, aber auch zum Beispiel deren Ausfall schützen.
- 4 Hauptanwendungsbereich der Verpflichtungen zur IT-Sicherheit sind damit An-, Zu- oder Eingriffe durch Unbefugte in die IT-Infrastruktur. Diese Eingriffe können von innen durch hierzu nicht befugte Mitarbeiter erfolgen, oder von außen durch externe Dritte. Letzteres ist insbesondere durch die zunehmende Vernetzung von Unternehmen und ihrer IT-Systeme eine wachsende Gefahr. Solche Eingriffe haben viele Ausformungen und Namen – „Cybercrime“ und „Hackerangriff“ sind nur einige davon. Demgegenüber wird der Ausfall der IT-Infrastruktur insgesamt oder in Teilen weniger diskutiert. In der Tat sind z. B. personenbezogene Daten hiervon in der Regel nur dann betroffen, wenn der Ausfall den Wegfall von Sicherheitsschranken zur Folge hat. Für das Funktionieren der Gesellschaft wichtige Infrastrukturen sind aber durch einen Ausfall der IT-Struktur kompromittiert, und dem Unternehmen selbst entstehen hierdurch in der Regel hohe Schäden.

2. Cybercrime im Wandel

- 5 Die Berichte über die wachsende Zahl von Angriffen, immer neue Sicherheitslücken und die zunehmende Kompromittierung von unternehmensrelevanten Daten machen deutlich, welchen Bedrohungen Unternehmen auch in Deutschland ausgesetzt sind. Nach wie vor bleiben Angriffe mit Ransomware die größte Bedrohung für die Cybersicherheit in Deutschland.⁵ Allein in Deutschland wurden im Jahr 2022 136.865 bekannte Fälle von „Cybercrime“ verzeichnet;⁶ 2023 waren es durchschnittlich täglich rund 21.000.⁷ Hinzu kommt eine signifikante Dunkelziffer von nicht erkannten und nicht gemeldeten Angriffen.⁸ Immer häufiger sind dies Akte organisierter Kriminalität, und nicht nur die Taten einzelner Hacker. Die organisierte Kriminalität agiert hierbei nicht nur als Täter, z. B. in

5 Cybercrime – Bundeslagebild 2023, S. 46, 85, https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html (zuletzt abgerufen am 14.5.2024).

6 Cybercrime – Bundeslagebild 2022 des BKA, S. 5. Dies spiegelt jedoch nicht realitätsgetreu die tatsächliche Entwicklung im Deliktsbereich Cybercrime wider. In der Inlands-PKS werden Fälle, bei denen zwar Schäden in Deutschland verursacht werden, aber der Aufenthaltsort des Täters im Ausland liegt oder unbekannt ist (sogenannte Auslandstaten), nicht berücksichtigt (Bundeslagebild 2022, S. 6).

7 Cybercrime- Bundeslagebild 2023, S. 13, https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html (zuletzt abgerufen am 14.5.2024).

8 Cybercrime – Bundeslagebild 2022 BKA, S. 4, 30

Form von digitaler Schutzgelderpressung (z.B. bei sog. „Ransomware“) und dem Diebstahl von Konto- und Kreditkarteninformationen, sondern auch als Lieferant von Produkten, mit denen ihre „Kunden“ Angriffe auf die Unternehmens-IT durchführen können.⁹ Diese Spielart wird auch „Crime as a Service“ genannt und hat dieser Art von Verbrechen eine äußerst bedrohliche Dimension gebracht, da hierdurch das Interesse an einem Angriff oder Zugriff auf ein IT-System nicht mehr verbunden sein muss mit den technischen Kenntnissen und Fertigkeiten, um diesen auch auszuführen. Mithilfe solcher Produkte, beispielsweise sogenannter „Exploit-Kits“,¹⁰ stehen den Angreifern Werkzeuge zur Verfügung, mit denen sie in Unternehmensnetze eindringen, die Netzstruktur analysieren und kritische Unternehmensinformationen abgreifen können oder durch sog. „Denial-of-Service-Angriffe“ die Nutzung der unternehmenseigenen IT, digitale Produktionsanlagen oder auch an Kunden gerichtete Webportale stören können.¹¹

a) Ideelle Hintergründe

Waren früher vor allem „Targeted Attacks“, also zielgerichtete Angriffe gegen Unternehmen oder bestimmte Bereiche von Unternehmen üblich, greifen heute Hackergruppen mit klassischen Hackerfähigkeiten und unter Ausnutzung von Social Media Unternehmen auch in sogenannten „Combined Attacks“ an. Dabei wird ein „Denial-of-Service-Angriff“ beispielsweise mit einem „Shitstorm“ gegen das Unternehmen und einer „Facebook-Attacke“ gegen die Geschäftsleitung verbunden. Oftmals werden mit den Angriffen keine wirtschaftlichen Ziele verfolgt. Vielmehr soll z.B. auf – in den Augen der Angreifer (sog. „Cyberaktivisten“) – vom Unternehmen zu verantwortende Missstände aufmerksam gemacht und so der Ruf des Unternehmens geschädigt werden.¹²

Nach wie vor zählt wohl der im Dezember 2016 bekannt gegebene Angriff auf „Yahoo!“ als einer der größten Hackerangriffe der letzten Jahre. Das Unternehmen enthüllte, dass es im Laufe der Jahre (vor allem 2013 und 2014) mehreren großen Hackerangriffen zum Opfer gefallen war, durch die persönliche Daten

9 Vgl. z.B. https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2024/Presse2024/240410_PM_Abschaltung_illegaler_Onlineservice.html oder <https://www.security-insider.de/was-ist-cybercrime-as-a-227da54abd15f73a0f3072b4e798b1ed/> (beide zuletzt abgerufen am 3.5.2024).

10 Ein Exploit-Kit ist ein sogenannter Werkzeugkasten, der automatisch Sicherheitslücken in Browsern, Betriebssystemen, Applikationen oder anderen Softwareprogrammen erkennt und ausnutzt. Die Nutzung eines Exploit-Kits ist auch ohne detaillierte Programmierkenntnis möglich. In der Regel beinhalten diese Kits auch Möglichkeiten für den Fernzugriff (Remote Access).

11 Vgl. *Bensinger/Kozok*, CB 2015, 376; https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220509_PM_CybercrimeBLB.html (zuletzt abgerufen am 3.5.2024).

12 Vgl. *Bensinger/Kozok*, CB 2015, 376.

wie Namen, E-Mail-Adressen, Telefonnummern und Geburtsdaten von drei Milliarden Nutzern erbeutet wurden.¹³

- 8 Aber auch die Hackerangriffe auf Microsoft¹⁴ (bekannt geworden 2023) und die Hackerwelle vom Februar 2023¹⁵ haben beträchtliche Schäden hinterlassen; als Motivation wurden allgemeine Schädigungs- und Verunsicherungsabsichten vermutet.
- 9 Bei dem im September 2023 bekanntgegebenen Hackerangriff (wohl ein Ransomware-Angriff) auf die Hotelkette Motel One hatte die Hackergruppe ALPHV offenbar einen knapp sechs Terabyte großen Datensatz erbeutet und Millionen Namen und Reisedaten von Hotelgästen der Firma landeten im Netz.¹⁶ Noch gravierender war der im November 2018 bekannt gegebene Angriff auf die später von der Hotelkette Marriott erworbene Hotelkette Starwood, bei der sich Hacker die Namen, Adressen, Kontaktinformationen und Passnummern von mehr als 300 Millionen Hotelgästen verschafften und in die Starwood-Reservierungsdatenbank mit ca. 500 Millionen Konten eindringen. Das Hacking dauerte wahrscheinlich bereits seit 2014 an.¹⁷
- 10 Deutschland gehört mittlerweile zu den Staaten, in denen Unternehmen und Institutionen besonders beliebte Ziele von Cyberattacken, insbesondere Ransomware-Attacken, sind.¹⁸ So wurde etwa zuletzt eine Hamburger Hochschule von der Hackergruppe „Vice Society“ (hinter der der russische Staat vermutet wird) bedroht,¹⁹ 2022 wurde der Automobilzulieferer Continental gehackt²⁰ und Ende September 2019 wurde ein Hacker-Angriff auf das Berliner Kammergericht mit dem Trojaner „Emotet“ festgestellt, bei dem der Angreifer höchstwahrscheinlich in der Lage war, den gesamten Datenbestand des Kammergerichts zu exfiltrieren und zu manipulieren.²¹

13 Vgl. <https://www.sueddeutsche.de/wirtschaft/yahoo-hackerangriff-bei-yahoo-traf-alle-drei-milliarden-konten-1.3693671> (zuletzt abgerufen am 15.5.2024).

14 Vgl. <https://www.tagesschau.de/investigativ/swr/microsoft-outlook-e-mails-sicherheitsluecke-hacker-100.html> (zuletzt abgerufen am 3.5.2024).

15 Vgl. <https://www.tagesschau.de/inland/gesellschaft/cyberattacke-deutschland-101.html> (zuletzt abgerufen am 3.5.2024).

16 Vgl. <https://www.spiegel.de/netzwelt/motel-one-datenleck-betrifft-millions-von-kunden-a-e44aee50-743b-43b4-b7b9-6ebe8dbdbd10> (zuletzt abgerufen am 3.5.2024).

17 Vgl. <https://www.psw-group.de/blog/hackerangriffe-2018/6673> (zuletzt abgerufen am 15.4.2020).

18 Vgl. https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_no_de.html (zuletzt abgerufen am 3.5.2024).

19 Vgl. <https://www.tagesschau.de/investigativ/rbb/hackernangriff-haw-vice-101.html> (zuletzt abgerufen am 3.5.2024).

20 Vgl. <https://www.tagesschau.de/wirtschaft/hackerangriff-continental-101.html> (zuletzt abgerufen am 3.5.2024).

21 Vgl. <https://www.sueddeutsche.de/wirtschaft/berlin-kammergericht-hacker-angriff-emotet-1.4775305> (zuletzt abgerufen am 15.5.2024).

Immer häufiger sind Unternehmen und staatliche Institutionen politisch motivierten sog. „State Sponsored Attacks“ ausgesetzt, sei es als Teil der kritischen Infrastrukturen oder wegen Produkten/Aktionen, die in der öffentlichen Diskussion stehen.²² **11**

Exemplarisch seien hier der immer noch spektakuläre Angriff auf die Sony Corporation (und insbesondere ihren Entertainment-Zweig) im Jahr 2014 sowie der Computerwurm „Stuxnet“ genannt, der erstmals im Juni 2010 entdeckt wurde. Hinter dem „Sony-Hacking“ stand wohl nach weit verbreiteter Überzeugung der Staat Nordkorea,²³ und auch die Komplexität und Entwicklung von „Stuxnet“ speziell zum Angriff auf Industrieanlagen lassen nach Expertenmeinung eine dahinterstehende staatliche Organisation vermuten.²⁴ Wenngleich der Angriff auf die SPD (2023) oder der auf das Datennetz der Bundesverwaltung (Informationsverbund Berlin-Bonn, IVBB), Russland zugeschrieben werden,²⁵ scheint andererseits der Ukraine-Krieg keinen Anstieg von (erfolgreichen) russischen Hacker-Angriffen mit sich zu bringen.²⁶ **12**

Neuerdings nutzen nordkoreanische Hacker (z. B. „Kimsuky“) offenbar den Google-Webbrowser für Angriffe.²⁷ Auch der Erpressungstrojaner „Wannacry“, der im Mai 2017 in Großbritannien zahlreiche Kliniken und das Gesundheitssystem des NHS lahmgelegt hatte, von dem aber auch die Deutsche Bahn, der Automobilhersteller Renault, der Telekommunikationsanbieter Telefónica und das russische Innenministerium betroffen waren,²⁸ wird Nordkorea zugeschrieben.²⁹ **13**

Der im Juli 2019 bekannte gewordene und wahrscheinlich schon mehrere Jahre andauernde Hacker-Angriff auf mehrere DAX-Konzerne, darunter Siemens, BASF, Henkel und Lanxess vonseiten der Hackergruppe „Winnti“ wird von IT- **14**

22 Vgl. *Bensinger/Kozok*, CB 2015, 376; KPG-Studie „Cyber Security in Österreich 2022“, https://bmi.gv.at/magazin/2022_07_08/08_Cyber-Sicherheit.aspx#:~:text=Die%20Cyber%2DSecurity%2DStudie%202022,Opfer%20entstand%20ein%20finanzieller%20Schaden (zuletzt abgerufen am 3.5.2024).

23 Vgl. <http://www.zeit.de/digital/2014-12/sony-hack-fbi-beschuldigung-nordkorea>; <http://www.heise.de/security/meldung/US-Geheimdienste-Fehler-beim-Sony-Hack-belegen-Schuld-Nordkorea-2513504.html> (beide zuletzt abgerufen am 15.5.2024).

24 Vgl. <https://www.faz.net/aktuell/feuilleton/debatten/digitales-denken/trojaner-stuxnet-der-digitale-erstschock-ist-erfolgt-1578889.html> (zuletzt abgerufen am 15.5.2024).

25 Vgl. <https://www.sueddeutsche.de/politik/cyberattacken-russland-bundesregierung-1.4157697> (zuletzt abgerufen am 23.4.2020); <https://www.zeit.de/politik/2024-05/auswaertiges-amt-bestellt-nach-cyberangriff-russischen-diplomaten-ein> (zuletzt abgerufen am 3.5.2024).

26 Vgl. https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_norde.html (zuletzt abgerufen am 3.5.2024).

27 Vgl. <https://www.tagesschau.de/investigativ/ndr-wdr/nordkorea-cyberspionage-suedkorea-verfassungsschutz-101.html> (zuletzt abgerufen am 3.5.2024).

28 Vgl. <https://www.zeit.de/digital/datenschutz/2017-12/wannacry-cyberattacke-nordkorea-us-regierung> (zuletzt abgerufen am 13.5.2020).

29 Vgl. <http://www.zeit.de/digital/2014-12/sony-hack-fbi-beschuldigung-nordkorea>; <http://www.heise.de/security/meldung/US-Geheimdienste-Fehler-beim-Sony-Hack-belegen-Schuld-Nordkorea-2513504.html> (zuletzt abgerufen am 15.5.2024).

Sicherheitsexperten und deutschen Sicherheitsbehörden dem chinesischen Staat zugeschrieben.³⁰

b) Materielle Hintergründe

- 15** Meist werden die Fähigkeiten der Hacker jedoch mit dem Ziel eingesetzt, Vermögenswerte oder geldwerte Daten/Informationen oder wettbewerbliche Vorteile zu erlangen. Insbesondere hat die organisierte Kriminalität die Industriespionage als Geschäftsmodell entdeckt. Neben den Entwicklungsabteilungen mit ihren Patenten, deren Vorstufen und anderem Know-how, sind auch die Vertragsabteilungen, Kunden- und Mitarbeiterdaten und die Finanzbuchhaltung mit den entsprechenden Kontoinformationen für Angreifer interessant. Eine weitere Spielart ist das Ausspähen von Unternehmensdaten im Rahmen von privaten und öffentlichen Ausschreibungen, um durch die Abgabe entsprechend angepasster Angebote zum einen Konkurrenten auszuschalten und zum anderen den Ausschreibenden zu benachteiligen. Auch „Denial-of-Service-Angriffe“ werden nicht nur aus ideologischen Gründen ausgeführt, sondern durchaus auch zur Schädigung von Konkurrenten.

3. Entwicklungen bei Schutzmaßnahmen

- 16** Früher lag der Schwerpunkt der technischen und organisatorischen Maßnahmen, die Unternehmen zur Verbesserung der IT-Sicherheit gemeinhin getroffen hatten, eher auf dem reaktiven Schutz der IT-Systeme mit dem vorrangigen Ziel, Angriffe von außen abzuwehren und aufzuklären, welche Systeme betroffen sind – etwa durch Firewall-, Virenschutz- und „Intrusion Detection“-Systeme. Seit dem Zeitalter der „Industrie 3.0“ und erst recht in der Ära der „Industrie 4.0“ mit Cloud-Angeboten, „Bring Your Own Device“, mobilem Arbeiten in dezentralen Strukturen und der gewachsenen Abhängigkeit von IT-Systemen in Produktion und Entwicklung ist jedoch ein ganzheitlicher Ansatz erforderlich. Neben der notwendigen durchgängigen Verschlüsselung aller unternehmensrelevanten Informationen und dem weiterhin notwendigen Schutz vor „Malware“ sind Analyse- und Auswertetools und ein zielgerichtetes Auditing heutzutage unabdingbar. Diese Entwicklung lässt sich am besten mit dem Begriff „Cyberintelligenz“ beschreiben: Es geht nicht nur darum, die betroffenen Systeme zu identifizieren, sondern im Rahmen der Angriffserkennung auch herauszufinden, wer der Angreifer ist, welche Methoden er angewandt hat und welche Tools er eingesetzt hat, um die unternehmenseigenen Systeme zu kompromittieren.³¹ Die hierzu notwendige Hard- und Software, wie z.B. eine „Next Generation Firewall“, IDS- oder SIEM-Systeme und moderne Auditingtools ergänzen die vorhandenen IT-Sicherheitssysteme und unterstützen nicht nur die Angriffserkennung, son-

³⁰ Vgl. <https://web.br.de/interaktiv/winnti/und> <https://www.spiegel.de/netzwelt/web/hacker-gruppe-winnti-griff-auch-basf-siemens-roche-und-henkel-an-a-1278705.html> (beides zuletzt abgerufen am 15.5.2024).

³¹ Für eine Illustration der verschiedenen Angriffswege vgl. Ahrend, CB 2019, 105, 106.

dern erleichtern auch die erforderlichen Maßnahmen im Rahmen des „Business Continuity Managements“.³²

II. Vorbeugende Maßnahmen

Eine Reihe von gesetzlichen Regelungen formulieren – mehr oder weniger konkret – Anforderungen, die Unternehmen im Bereich der IT-Sicherheit erfüllen *müssen*. Hervorzuheben sind die DSGVO, das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das durch das im Mai 2021 in Kraft getretene IT-Sicherheitsgesetz 2.0³³ an die neuen EU-rechtlichen Standards angepasst wurde. Daneben gibt es noch Vorschriften für spezielle Sektoren, wie etwa Kredit- und Finanzdienstleistungsinstitute (§§ 25a, 25b KWG, §§ 28, 28a, 29 KAGB), Energieversorger (§ 11 EnWG) oder Telematiksysteme im Gesundheitswesen (§ 306 ff. SGB V³⁴). § 333 SGB-V stärkt die Aufsicht des BSI über die Gesellschaft für Telematik (gematik) im Hinblick auf mögliche Sicherheitsmängel und ermächtigt die gematik, Betreibern von Diensten und Anwendungen zur Beseitigung festgestellter Sicherheitsmängel unmittelbare Anweisungen zu erteilen.³⁵ Das E-Health-Gesetz enthält konkrete Maßnahmen für den Aufbau der sicheren Telematikinfrastruktur und die Einführung medizinischer digitaler Anwendungen. Seitdem wird die Digitalisierung des Gesundheitswesens durch verschiedene gesetzliche Maßnahmen, zum Beispiel mit dem Terminservice- und Versorgungsgesetz (TSVG), dem Gesetz für mehr Sicherheit in der Arzneimittelversorgung (GSAV), dem Digitale-Versorgung-Gesetz (DVG), dem Patientendaten-Schutz-Gesetz (PDSG) sowie zuletzt mit dem am 9.6.2021 in Kraft getretenen Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPfMG) vorangetrieben.³⁶ Auf EU-Ebene haben die 2016 in Kraft getretene EU-Richtlinie zur Verbesserung der Netz- und Informationssicherheit³⁷ (NIS-Richtlinie) sowie die 2023 in Kraft getretene NIS-2-Richtlinie³⁸ einen einheitlichen Rechtsrahmen für IT-Sicherheit aufgestellt. Der Anwendungsbereich

32 Vgl. BSI, Empfehlungen für die Wirtschaft, jeweils auch für Teilbereiche der Wirtschaft, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_006.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 3.5.2024); *Bensinger/Kozok*, CB 2015, 376 f.

33 http://www.bgb1.de/xaver/bgb1/start.xav?startbk=Bundesanzeiger_BGB1&jumpTo=bgb1121s1122.pdf

34 Zu § 333 SGB V vgl. *Michels*, in: Becker/Kingreen, SGB V, § 333 Rn. 2 ff.

35 *Michels*, in Becker/Kingreen, SGB V, § 333 Rn. 8

36 Vgl. <https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/e/e-health-gesetz.html> (zuletzt abgerufen am 15.5.2024).

37 Richtlinie (EU) 2016/1148 vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194/1 v. 19.7.2016.

38 Richtlinie (EU) 2022/2555 vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie); umzusetzen bis 18.10.2024, Art. 41 NIS-2-Richtlinie.

der NIS-2-Richtlinie wurde hierbei auf neue Sektoren und Einrichtungen ausgeweitet, um die Resilienz und Reaktionsfähigkeit öffentlicher und privater Einrichtungen, der zuständigen Behörden und der EU insgesamt weiter zu verbessern.³⁹ Keine Verpflichtungen für Unternehmen, sondern für die Geschäftsleitung einer Aktiengesellschaft bzw. einer GmbH enthalten die allgemeinen Compliance-Vorschriften der §§ 91, 93, 116 AktG sowie § 43 GmbHG. Diese Vorschriften enthalten keine spezifischen Pflichten zur IT-Sicherheit, werden aber auch hierfür herangezogen.

1. Adressaten

- 18** Abgesehen von den Vorschriften der DSGVO, die alle Unternehmen und Institutionen verpflichtet, wenn und soweit diese personenbezogene Daten verarbeiten,⁴⁰ richten sich alle anderen gesetzlichen Verpflichtungen zu vorbeugenden IT-Sicherheitsmaßnahmen nur an einen ganz bestimmten, zum Teil eng abgegrenzten Adressatenkreis:

a) KRITIS-Betreiber

- 19** Adressat der öffentlich-rechtlichen Pflichten der §§ 8a und 8b BSIG sind „Betreiber kritischer Infrastrukturen“ (auch KRITIS-Betreiber genannt), d. h. Unternehmen aus den Bereichen Energie, Informationstechnik, Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, deren Einrichtungen und Anlagen von hoher Bedeutung für das Funktionieren des Gemeinwesens sind. Mit Umsetzung der NIS-2-Richtlinie⁴¹ werden noch die Sektoren Weltraum und öffentliche Verwaltung (als Sektoren mit hoher Kritikalität) hinzukommen. Anders als Nicht-KRITIS-Unternehmen dürfen also KRITIS-Unternehmen nicht selbst entscheiden, ob und welche IT-Sicherheitsmaßnahmen sie für sinnvoll und angemessen erachten und ergreifen wollen. Als Begründung für diese Sonderverpflichtung gilt, dass durch einen Ausfall oder eine Beeinträchtigung der von KRITIS-Unternehmen betriebenen kritischen Infrastruktur erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden (§ 2 Abs. 10 BSIG). Nach der Gesetzesbegründung sind etwa 2.000 in Deutschland ansässige Unternehmen als KRITIS-Betreiber einzustufen.⁴² Die im Mai 2016 in Kraft getretene Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) regelte zunächst nur für die Sektoren Energie, Informationstechnik, Telekommunikation sowie Wasser und Ernährung, wann ein Unternehmen eine kritische Infrastruktur betreibt und in den Anwendungsbereich des IT-Sicherheitsgesetzes bzw. des BSIG

39 Vgl. <https://digital-strategy.ec.europa.eu/de/policies/nis2-directive>, (zuletzt abgerufen am 28.4.2024).

40 Zum Datenschutz beim Compliance Management ausführlich → *Becker/Böhlke/Fladung*, Kap. 12.

41 Die NIS-2-Richtlinie ist bis 18.10.2024 umzusetzen, Art.41 NIS-2-Richtlinie.

42 Gesetzesbegründung zum IT-Sicherheitsgesetz, BT-Drs. 18/4096, S. 21.

fällt. So enthält die Verordnung konkrete Bestimmungen zu den entsprechenden Dienstleistungen, Bereichen sowie den Anlagenkategorien und diesbezüglichen Schwellenwerten. Die Verordnung wurde maßgeblich vom BSI und UP KRITIS⁴³ erarbeitet, was den betroffenen Unternehmen die Möglichkeit gab, bei der Entwicklung der Verordnung mitzuwirken. Durch die 1. Änderungsverordnung vom 21.7.2017 wurde die noch ausstehende Bestimmung kritischer Infrastrukturen in den Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr vorgenommen.⁴⁴ Mit der 3. Änderungsverordnung vom 1.3.2023 wurden die Anlagenkategorien in den Anhängen 1 und 4 um LNG-Anlagen und Seekabelanlandestationen ergänzt, und die 4. Änderungsverordnung vom 1.1.2024 ergänzt Anlagenkategorien und Schwellenwerte im Sektor Siedlungsabfallentsorgung.⁴⁵

Eine fast deckungsgleiche Zielgruppe wird von der am 8.8.2016 in Kraft getretenen NIS-Richtlinie verpflichtet: Auch diese Richtlinie richtet sich an Betreiber von kritischen Infrastrukturen,⁴⁶ allerdings aus etwas anderen Sektoren: Energie, Transport, Bank- und Finanzwesen, Gesundheitswesen, Wasserversorgung und digitale Infrastruktur. Insbesondere Telekommunikationsanbieter sind hier also nicht erfasst. Jedenfalls B2B-Anbieter von Informations- und Kommunikationstechnik werden aber von der NIS-2-Richtlinie erfasst werden, die ab dem 18.10.2024 die NIS-Richtlinie ersetzen wird. Die zusätzlichen Zielgruppen (auch Weltraum und öffentliche Verwaltung) sind mit der 4. Änderungsverordnung aber in Deutschland bereits umgesetzt (vgl. → Rn. 19). Wichtig ist, dass die NIS-2-Richtlinie nicht mehr zwischen KRITIS-Betreibern und Anbietern digitaler Dienste unterscheidet, da diese Unterscheidung nicht die tatsächliche Bedeutung der Sektoren oder Dienste für die gesellschaftlichen und wirtschaftlichen Tätigkeiten im Binnenmarkt widerspiegelt.⁴⁷

Am 16.1.2023 ist die EU-Richtlinie über die Resilienz kritischer Einrichtungen⁴⁸ (CER-Richtlinie) in Kraft getreten, welche Mindeststandards für die staatliche Überwachung und für KRITIS-Betreiber festlegt. Die Richtlinie ist vor dem Hintergrund der bestehenden dynamischen Bedrohungslage (einschließlich terroristischer Bedrohungen und wachsender gegenseitiger Abhängigkeiten zwi-

43 Öffentlich-private Kooperation zwischen Betreibern kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen, vgl. https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/UP-KRITIS/up-kritis_node.html (zuletzt abgerufen am 15.5.2024).

44 Erste Verordnung zur Änderung der BSI-Kritisverordnung, BGBl. I 2017, S. 1903 ff.

45 Vgl. hierzu auch *Deusch/Eggendorfer*, in: Taeger/Pohle ComputerR-HdB, 50.1 IT-Sicherheit Rn. 411 ff.

46 Ähnlich wie das IT-Sicherheitsgesetz adressiert die NIS-Richtlinie außerdem auch Anbieter digitaler Dienstleistungen, siehe → Rn. 25.

47 ErwG der NIS-2-Richtlinie, vgl. hierzu unten → Rn. 85.

48 Richtlinie (EU) 2022/2557 vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates, ABl. L 333/164 v. 27.12.2022.

schen Infrastrukturen und Sektoren) und einem bestehenden physischen Risiko im Zusammenhang mit Naturkatastrophen und dem Klimawandel entstanden (vgl. ErwG 3 der CER-RL).⁴⁹ Die nationale Umsetzung erfolgt mit dem KRITIS-Dachgesetz, das zum 18.10.2024 in Kraft treten soll.⁵⁰

- 22** Mittelbar sind neben den KRITIS-Betreibern aber noch weitere Unternehmen betroffen, etwa solche, die (IT-)Dienstleistungen für KRITIS-Betreiber erbringen und denen die neuen Standards vertraglich auferlegt werden.
- 23** Außerdem wurde mit dem IT-Sicherheitsgesetz 2.0 die Gruppe der „Unternehmen im besonderen öffentlichen Interesse“ (UBI) eingeführt (§ 2 Nr. 14 BSIG). UBI sind keine KRITIS-Betreiber, werden aber in vielerlei Hinsicht als solche behandelt (siehe → Rn. 32). Hierunter fallen etwa Unternehmen der Rüstungsindustrie, Hersteller von IT-Produkten für die Verarbeitung staatlicher Verschlusssachen, Unternehmen, die einer Regulierung durch die Verordnung zum Schutz von Gefahrstoffen unterliegen, sowie Unternehmen von erheblicher volkswirtschaftlicher Bedeutung – und damit weitere Teile der Wirtschaft. Absehbar werden allerdings die UBI mit Umsetzung der NIS-2-Richtlinie keine eigene Gruppe mehr bilden, sondern (gemeinsam mit den Anbietern digitaler Dienste, vgl. → Rn. 26) in den „wichtigen Einrichtungen“ und „besonders wichtigen Einrichtungen“ nach dem BSIG aufgehen.⁵¹

b) Anbieter von Telemediendiensten

- 24** Auch für Anbieter von Telemediendiensten gelten wegen der von ihnen verwalteten Kundendaten spezialgesetzliche Anforderungen, obwohl diese an sich keine kritischen Infrastrukturen betreiben. Die Anforderungen, die bislang im TMG (insb. § 13 TMG) geregelt waren, finden sich nun im Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG; insb. § 19 TTDSG). Geblieben ist der weite Adressatenkreis: Wie das TMG, gilt auch das TTDSG für Anbieter von „geschäftsmäßig angebotenen Telemedien“. Hierzu gehören etwa Websites, Blogs, Shops, aber auch Online-Games und Apps, sofern sie Online-Inhalte darstellen.⁵² Da insbesondere fast jeder Websitebetreiber zu den Telemediendiensteanbietern zählt, sind die Anforderungen von einer Vielzahl von Unternehmen zu beachten.

49 Eisenmenger, NVwZ 2023, 1203, 1203.

50 Derzeit liegt der 2. Referentenentwurf vom 21.12.2023 vor, <https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KRITIS-DachG.html> (zuletzt abgerufen am 3.5.2024).

51 Vgl. Referentenentwurf für ein Umsetzungsgesetz der NIS-2-Richtlinie (NISUmsuCG_Ref E), S. 35 f. (§ 28 BSIG) sowie S. 189 (zu § 3 Abs. 1 Satz 2 Nummer 24 BSIG) https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwurf/CI1/NIS-2-RefE.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 12.5.2024).

52 Hilgert, Das IT-Sicherheitsgesetz: Neue Anforderungen für alle geschäftsmäßigen Online-dienste, CR-online.de Blog, <https://www.cr-online.de/blog/2015/08/17/das-it-sicherheitsgesetz-neue-anforderungen-fuer-alle-geschaeftsmaessigen-onlinedienste/> (zuletzt abgerufen am 15.5.2024).

Demgegenüber sind Adressaten der NIS-Richtlinie (vgl. → Rn. 20 und Rn. 84 ff.) nur „Anbieter digitaler Dienstleistungen“. Im Vergleich zum Anbieter von Telemediendiensten dürfte es sich hier nur um solche Dienstleister handeln, die konkret Dienstleistungen für Kunden anbieten, also etwa Betreiber von E-Commerce-Plattformen, Cloud-Dienste-Anbieter oder Suchmaschinenbetreiber. Allerdings hebt die NIS-2-Richtlinie die Differenzierung von Anbietern digitaler Dienstleistungen auf: Stattdessen werden „Betreiber kritischer Einrichtungen“ (also in Anhang I zur NIS-2-Richtlinie genannte Sektoren) und „Betreiber wichtiger Einrichtungen“ (also in Anhang II zur NIS-2-Richtlinie genannte Sektoren) unterschieden. Anbieter digitaler Dienste werden (nur noch) im Anhang II der NIS-2-Richtlinie genannt, und zwar als Anbieter von Online-Marktplätzen, von Online-Suchmaschinen und von sozialen Netzwerken. Insbesondere Cloud-Computing-Dienste zählen nicht mehr zu Anbietern digitaler Dienste, sondern zur Digitalen Infrastruktur (und damit unter Anhang I zur NIS-2-Richtlinie). Die technischen und methodischen Anforderungen an das Risikomanagement sowie die Anforderungen an die Berichtspflichten von ehemals unter den Begriff „Anbieter digitaler Dienste“ fallenden Online-Marktplätzen, Online-Suchmaschinen und Cloud-Computing-Diensten sowie zusätzlicher Diensteanbieter im Bereich Internetkommunikationsinfrastrukturen werden durch Durchführungsakte der Kommission festgelegt (Art. 21 Abs. 5, Art. 23 Abs. 11 NIS-2-Richtlinie).⁵³

§ 8c BSIG adressiert nunmehr ebenfalls „Anbieter digitaler Dienste“. Allerdings werden diese absehbar mit Umsetzung der NIS-2-Richtlinie keine eigene Gruppe mehr bilden, sondern in den „wichtigen Einrichtungen“ und „besonders wichtigen Einrichtungen“ aufgehen.⁵⁴

c) Anbieter von Telekommunikationsdiensten

Aufgrund der hohen Bedeutung zuverlässiger und sicherer Kommunikation für Wirtschaft und Gesellschaft gelten auch für die Anbieter von Telekommunikationsdiensten besondere Verpflichtungen.⁵⁵ Zum einen folgen diese schon aus §§ 8a und 8b BSIG, da Telekommunikationsanbieter KRITIS-Unternehmen sind; zum anderen sind solche Verpflichtungen im TKG geregelt (siehe → Rn. 61 f.). Die Bundesnetzagentur soll für die Aufrechterhaltung von Integrität und Sicherheit der öffentlichen Kommunikationsnetze sorgen. Um dies zu gewährleisten, ist die Mitwirkung der Diensteanbieter erforderlich, woraus sich insbesondere eine Meldepflicht für Sicherheitsverletzungen ergibt (siehe → Rn. 139).

53 *Beucher/Ehlen/Utzerath*, in: Kipker, Cybersecurity, Kap. 14 Rn. 13.

54 Vgl. Referentenentwurf für ein Umsetzungsgesetz der NIS-2-Richtlinie (NISUmsuCG_Ref E), S. 35 f. (§ 28 BSIG) sowie S. 189 (zu § 3 Abs. 1 Satz 2 Nr. 24 BSIG) https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwurfe/C11/NIS-2-RefE.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 12.5.2024).

55 So schon ErwG 44 der RL 2009/140/EG.

d) Bank- und Finanzwesen

- 28 Für Kreditinstitute sieht das Kreditwesengesetz (KWG) Regelungen zur Sicherheit der Geschäftsorganisation vor, zu denen über die von der BaFin aufgestellten „Mindestanforderungen an das Risikomanagement“ (MaRisk) auch Pflichten zur Sicherheit der IT-Infrastruktur gehören.⁵⁶ Ähnlich sind E-Geldinstitute und Zahlungsinstitute durch § 22 ZAG und Kapitalverwaltungsgesellschaften nach den §§ 28, 28a, 29 KAGB zu bestimmten Risikosicherungsmaßnahmen auch im IT-Bereich verpflichtet.

e) Energiewirtschaft

- 29 Für Betreiber von Energieversorgungsnetzen oder Energieanlagen nach dem EnWG (Energieanlagen jedoch nur, wenn sie als Kritische Infrastruktur nach dem BSI-Gesetz einzustufen sind) sieht § 11 Abs. 1a EnWG, der durch das IT-Sicherheitsgesetz konkretisiert und um die Absätze 1b und 1c ergänzt wurde, ein Pflichtenprogramm zur Gewährleistung der IT-Sicherheit vor.⁵⁷ Dieses ist seither durch die von der Bundesnetzagentur erstellten IT-Sicherheitskataloge zu § 11 Abs. 1a EnWG⁵⁸ und § 11 Abs. 1b EnWG⁵⁹ detailliert ausgearbeitet worden. Netzbetreiber müssen in der Konstellation „Betriebsführung durch Dritte“ (also in Fällen, in denen die vom IT-Sicherheitskatalog erfassten Telekommunikations- und elektronischen Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind, über einen Betriebsführungsvertrag von einem Dritten betrieben werden) grds. selbst zertifizieren und hierüber einen Nachweis erbringen.⁶⁰ Umgekehrt besteht nach Auffassung der BNetzA keine Umsetzungspflicht für die Sicherheitsanforderungen des IT-Sicherheitskatalogs und bedarf es keiner Zertifizierung, wenn ein Netzbetreiber keine vom IT-Sicherheitskatalog erfassten Systeme in seinem Netz betreibt und diese auch nicht von einem externen Dienstleister betreiben lässt bzw. es sich nur um Systeme ohne Gefährdungspotenzial handelt.⁶¹

56 Zur MaRisk-Compliance ausführlich → *Renz/Frankenberger*, Kap. 20 Rn. 23 ff.

57 Vgl. ausführlich *Weise/Brühl*, CR 2015, 290 ff., und *Giebichenstein/Schirp*, CB 2015, 66, 68.

58 IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz von August 2015, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 15.4.2024).

59 IT-Sicherheitskatalog gemäß § 11 Absatz 1b Energiewirtschaftsgesetz von Dezember 2018, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_2018.pdf?__blob=publicationFile&v=4 (zuletzt abgerufen am 15.5.2024).

60 Mitteilung der BNetzA vom 29.3.2022 https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/BetriebsfuehrungdurchDritte.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 3.5.2024); *Bartsch*, EnWZ 2023, 72 f.

61 *Bartsch*, EnWZ 2023, 69, 72; FAQ der BNetzA, https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/IT_Sicherheit/Netzbetreiber/artikel.html (zuletzt abgerufen am 3.5.2024).

f) Geschäftsführung von Aktiengesellschaften und GmbHs

Die §§ 76, 91, 93 AktG sowie § 43 GmbHG richten sich an einen ganz anderen Adressatenkreis: Hiernach sind nicht (bestimmte) Unternehmen zur Vorhaltung von Risikomanagementsystemen verpflichtet, sondern die Mitglieder des Vorstands von Aktiengesellschaften und GmbH-Geschäftsführer persönlich – und zwar grundsätzlich unabhängig davon, ob das Unternehmen eine kritische Infrastruktur betreibt oder sonst selbst zu bestimmten IT-Sicherheitsmaßnahmen verpflichtet ist. **30**

2. Inhalt der gesetzlichen Verpflichtungen

Die Gefahren der Cyberkriminalität gehen weit über den Verlust oder die unrechtmäßige Verarbeitung von personenbezogenen Daten hinaus. Da es Pflichten zur Vermeidung von Industriespionage oder zur Sicherung der Operationsfähigkeit wichtiger Unternehmen und Strukturen zuvor nicht bzw. nur vereinzelt und unkonkret gab, stellte 2015 das IT-Sicherheitsgesetz auch im internationalen Vergleich eine wichtige und bemerkenswerte Änderung der Rechtslage dar. Rechtstechnisch handelte es sich bei dem IT-Sicherheitsgesetz um ein Artikelgesetz, das ein ganzes Paket an Änderungen bestehender Gesetze im Bereich IT-Sicherheit bewirkte. Weitere Änderungen kamen 2017 hinzu, als die NIS-Richtlinie ins deutsche Recht umgesetzt wurde. Als EU-Richtlinie entfaltet die 2016 in Kraft getretene und bis zum 10.5.2018 von den Mitgliedstaaten umzusetzende NIS-Richtlinie⁶² keine unmittelbare Rechtswirkung. Mit dem Gesetz zur Umsetzung der NIS-Richtlinie vom 29.6.2017⁶³ wurde die Regelung ins deutsche Recht umgesetzt, soweit dies angesichts des IT-Sicherheitsgesetzes noch nötig war. Insbesondere wurden die Aufsichts- und Durchsetzungsbefugnisse des BSI gegenüber KRITIS-Betreibern erweitert (→ Rn. 39 ff.) und Regelungen für Anbieter Digitaler Dienste neu geschaffen (→ Rn. 25 f. und 36). **31**

Als Reaktion auf weitreichende Cyberangriffe, insbesondere auf den Bundestag und das Auswärtige Amt 2017/18, trat im Mai 2021 das IT-Sicherheitsgesetz 2.0 in Kraft, welches das BSIG, das TKG und das TMG geändert hat. Das IT-Sicherheitsgesetz 2.0 erweitert die bereits bestehenden Befugnisse des BSI, das nun auch für die Entwicklung und Veröffentlichung eines Standes der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte zuständig ist, als nationale Behörde für die Cybersicherheitszertifizierung gem. EU Cybersecurity Act⁶⁴ agiert und befugt wird, bestimmte informationstechnische Systeme auf **32**

62 Richtlinie (EU) 2016/1148 vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194/1 v. 19.7.2016, Art. 25 Abs. 1.

63 BGBl. I, S. 1885.

64 Vgl. <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32019R0881> (zuletzt abgerufen am 13.5.2024). Kernelemente der Verordnung sind ein permanentes Mandat für die europäische Cybersicherheitsagentur ENISA („European Union Agency for Cybersecurity“) sowie die Einführung eines einheitlichen europäischen Zertifizierungsrahmens für IKT-Pro-

Schadprogramme und Sicherheitslücken zu überprüfen.⁶⁵ Darüber hinaus übernimmt das BSI die Beratung, Information und Warnung von staatlichen und privaten Stellen in Fragen der Informationssicherheit, spricht Empfehlungen für Identifizierungs- und Authentifizierungsverfahren aus und stellt Krisenreaktionspläne auf. Für diejenigen Komponenten, die explizit für den Betrieb einer Kritischen Infrastrukturanlage ausschlaggebend sind, werden über ein sog. „BSI-Sicherheitskennzeichen“ Mindeststandards definiert.⁶⁶ Mit der Erweiterung der Pflichten der (ebenfalls erweiterten) KRITIS-Unternehmen wurde auch der Anwendungsbereich der Regelungen ausgedehnt.⁶⁷ So werden die verpflichtenden Mindeststandards und Meldepflichten für KRITIS-Betreiber auf „Infrastrukturen im besonderen öffentlichen Interesse“ (UBI, vgl. → Rn. 23) und damit weitere Teile der Wirtschaft ausgeweitet.

- 33** Schließlich wurden die Bußgelder erhöht: Die bußgeldauslösenden Tatbestände sind auf vier Stufen angeordnet, nach denen je nach Pflichtverletzung Bußgelder zwischen bis zu 100.000 EUR (z. B. bei Nichterreichen der Kontaktstelle) und bis zu 20 Mio. EUR (z. B. bei Zuwiderhandlung gegen Anordnungen des BSI) drohen. Eine Abhängigkeit des Bußgelds vom Umsatz des verstoßenden Unternehmens ist nicht mehr vorgesehen.
- 34** Die Verabschiedung der NIS-2-Richtlinie im Jahr 2022 brachte abermals inhaltliche Änderungen der Pflichten der verpflichteten Unternehmen und Institutionen, die aber noch nicht gelten, sondern größtenteils noch bis Oktober 2024 im BSIG umgesetzt werden müssen; ein entsprechender Referentenentwurf für ein Umsetzungsgesetz liegt bereits vor.⁶⁸ Insbesondere muss der eher allgemein gehaltene § 8a BSIG eine Erweiterung und Konkretisierung erfahren, um den Maßnahmen-Anforderungen des Art. 18 NIS-2-RL gerecht zu werden. Auch die in §§ 8b, 8c BSIG vorgeschriebenen Meldepflichten hinsichtlich Cybersicherheitsvorfällen müssen mit Blick auf Art. 20 NIS-2-Richtlinie weiter verschärft werden. Neu ist vor allem die Pflicht zum Bericht auch der „near misses“ (Art. 23 Abs. 10 NIS-2-Richtlinie).⁶⁹

dukte, -Dienstleistungen und -Prozesse. Diese sollen gemäß definierter Sicherheitslevel in „niedrig“, „mittel“ und „hoch“ nach unterschiedlichen Vorgaben zertifiziert werden.

65 Rath/Ekardt/Schiela, MMR 2023, 176, 179.

66 Vgl. hierzu auch Rath/Ekardt/Schiela, MMR 2023, 176, 179.

67 Rath/Ekardt/Schiela, MMR 2023, 176, 179; Deusch/Eggendorfer, in: Taeger/Pohle ComputerR-HdB, 50.1 IT-Sicherheit Rn. 411 ff.

68 Referentenentwurf für ein Umsetzungsgesetz der NIS-2-Richtlinie (NISUmsuCG_RefE) vom 7.5.2024 https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwurfe/CII/NIS-2-RefE.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 12.5.2024).

69 Rath/Ekardt/Schiela, MMR 2023, 176, 178.

a) BSIG*aa) Pflichten der KRITIS-Betreiber*

Insbesondere das BSIG wurde durch die IT-Sicherheitsgesetze und die NIS-Richtlinie weitreichend geändert. Im Vordergrund stehen die Anforderungen an die KRITIS-Betreiber, die sich dahingehend zusammenfassen lassen, dass KRITIS-Betreiber ein Information Security Management betreiben und kritische Cyber-Assets identifizieren und managen müssen. Daneben müssen Maßnahmen zur Angriffsprävention und -erkennung getroffen und ein „Business Continuity Management“ eingerichtet werden. Hierbei haben die KRITIS-Betreiber branchenspezifische Besonderheiten zu beachten und umzusetzen.⁷⁰ **35**

Der Gesetzgeber hat sich dabei für eine dynamische und eigenverantwortliche Lösung entschieden (§ 8a Abs. 1 BSIG): Die Unternehmen müssen selbst entscheiden, welche Maßnahmen für sie erforderlich und nach Abwägung der Umstände angemessen sind. Jedoch haben sie sich stets am Stand der Technik zu orientieren. „Stand der Technik“ ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt.⁷¹ Konkretisiert wurden die Pflichten im Hinblick auf eingesetzte Systeme zur Angriffserkennung: Diese müssen nun ausdrücklich geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten, und müssen dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen (§ 8a Abs. 1a BSIG). Für Anbieter Digitaler Dienste gelten nach § 8c BSIG (noch) besondere Anforderungen: Abs. 1 verlangt geeignete und verhältnismäßige technische und organisatorische Maßnahmen, um Risiken für die Sicherheit der Netz- und Informationssysteme, die sie zur Bereitstellung der digitalen Dienste innerhalb der EU nutzen, zu bewältigen und den Auswirkungen von Sicherheitsvorfällen auf innerhalb der EU erbrachten digitalen Diensten vorzubeugen (bzw. die Auswirkungen so gering wie möglich zu halten). Dabei ist der Sicherheit der Systeme und Anlagen, der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen, dem Betriebskontinuitätsmanagement, der Überwachung, Überprüfung und Erprobung sowie der Einhaltung internationaler Normen besonders Rechnung zu tragen.⁷² **36**

Anerkannte Standards, Regelwerke oder Interpretationsmaßstäbe wie die Mindestanforderungen an das Risikomanagement (MaRisk) der BaFin können die **37**

⁷⁰ BT-Drs. 18/4096, S. 26 f.

⁷¹ Gesetzesbegründung, BT-Drs. 18/4096, S. 26.

⁷² *Schneider/Forgó/Helfrich*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil XII. Kap. 4. Überblick zu Risikomanagement unter BSIG, BSI-KritisV, NIS-RL i.V.m. DS-GVO Rn. 7.

Pflichten der KRITIS-Betreiber konkretisieren. So nennt die Gesetzesbegründung z. B. die (zertifizierbaren) branchenunabhängigen ISO-Normen als Maßstab.⁷³ Demgegenüber betrachtet das BSI seine eigenen Empfehlungen wie z. B. die Grundsatzkataloge lediglich als Orientierungshilfe, und (weder im positiven noch im negativen Sinne) nicht als Vorgabe. Deshalb kommt den Branchenorganisationen eine besondere Bedeutung zu: Gemäß § 8a Abs. 2 BSIG können branchenspezifische Sicherheitsstandards (B3S) vorgeschlagen werden, die das Bundesamt für Sicherheit für geeignet erklären muss.⁷⁴ In den Branchen Trinkwasserversorgung/Abwasserbeseitigung, Lebensmittelhandel und IT sowie in den Anlagenkategorien Rechenzentrum, Serverfarmen und CDN sowie Ernährungswirtschaft, Fernwärme, Versicherungen, (medizinische) Labore, Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr und Elektrizität⁷⁵ wurde die Eignung der Sicherheitsstandards durch das BSI bereits erfolgreich festgestellt. Hält sich ein Unternehmen dann an die spezifischen Standards seiner Branche, so dürften die Anforderungen jedenfalls insoweit als erfüllt anzusehen sein.⁷⁶ Die Feststellung der Eignung eines B3S erfolgt in der Regel für zwei Jahre. Spätestens nach zwei Jahren sollte daher überprüft werden, inwiefern die im B3S getroffenen Annahmen und Beschreibungen sowie die umzusetzenden Maßnahmen noch der aktuellen Bedrohungslage und dem aktuellen „Stand der Technik“ entsprechen. Bei aller Kritik am Fehlen konkreter Maßstäbe bietet dieses Regime jedenfalls ausreichend Flexibilität, um auch neue, alternative Ansätze für IT-Sicherheitsstandards zu etablieren, wie z. B. kooperative Ansätze. Hilfreich ist außerdem, dass das BSI schon von Gesetzes wegen auf Ersuchen der KRITIS-Betreiber diese bei der Sicherung ihrer IT beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen kann.

- 38 Grundsätzlich brauchen KRITIS-Betreiber auch nur angemessene Maßnahmen zu implementieren, bei denen also der erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Infrastruktur steht. Was genau das heißt, ist schon im Rahmen der Business-Judgment-Rule des § 93 AktG unklar (siehe → Rn. 90 ff.); hier dürfte die Latte aber wegen der Bedeutung der kritischen Infrastrukturen noch höher anzulegen sein.
- 39 Die KRITIS-Betreiber haben mindestens alle zwei Jahre beim BSI nachzuweisen, dass sie die oben genannten Anforderungen erfüllen und entsprechende Vor-

73 Gesetzesbegründung, BT-Drs. 18/4096, S. 27; hierzu ausführlich *Giebichenstein/Schirp*, CB 2015, 66, 69 ff.

74 Vgl. https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/Branchenspezifische-Sicherheitsstandards-B3S/branchenspezifische-sicherheitsstandards-b3s_node.html (zuletzt abgerufen am 28.4.2024). Es handelt sich bei der Entscheidung des BSI um eine Allgemeinverfügung i. S. d. § 35 Satz 2 VwVfG (*Guckelberger*, DVBl 2019, 525, 531).

75 Vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=8 (zuletzt abgerufen am 28.4.2024).

76 So im Ergebnis schon *Reinhard/Pohl/Capellaro*, IT-Sicherheit und Recht, S. 37 ff.; *von Holleben/Menz*, CR 2010, 63, 65 f.

kehrungen getroffen haben. Die Nachweise können durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Das BSI kann dazu Verfahrensanforderungen nach Anhörung von Vertretern der betroffenen Betreiber und Wirtschaftsverbände festlegen, was es mit den Grundsätzliche Anforderungen im Nachweisverfahren (GAI_N) vom 12.5.2023 getan hat.⁷⁷ Die in diesem Dokument aufgeführten Anforderungen sind verpflichtend für die ordnungsgemäße Umsetzung der §§ 8a ff. BSIG. Für eine geeignete Nachweiserbringung hat der Betreiber ihre Erfüllung sicherzustellen. Soweit sie Regelungsbereiche betreffen, zu denen das BSI weitere Vorgaben veröffentlicht hat, ergänzen sich die bestehenden Regelungen; im Falle einer inhaltlichen Überschneidung gilt die speziellere Regel (üblicherweise die sektorspezifische Vorschrift, z. B. für die Anlagenkategorie 2.1.1 Rechenzentrum⁷⁸). Bei Feststellung einer inhaltlichen Überschneidung oder einer möglichen Unanwendbarkeit einer Regelung ist das BSI unverzüglich zu informieren und um Entscheidung zu bitten; eine spätere Berufung auf die Unsicherheit ist nach Auffassung des BSI nicht möglich.⁷⁹ Ergänzend gibt es (unverbindliche) Orientierungshilfen des BSI zu Nachweisen gemäß § 8a Abs. 3 BSIG.⁸⁰

Neu seit 2021 müssen KRITIS-Betreiber den geplanten erstmaligen Einsatz **40** einer kritischen Komponente dem Bundesministerium des Innern anzeigen (§ 9b BSIG).

bb) Befugnisse des BSI

§ 8a Abs. 4 Satz 1 BSIG verleiht dem BSI eine Eingriffsbefugnis zur Überprüfung der Anforderungen des § 8a Abs. 1 BSIG unabhängig von der Anzeige konkreter Mängel. Diese Eingriffsbefugnis wird flankiert von § 8a Abs. 4 Satz 2 BSIG: Hiernach müssen KRITIS-Betreiber dem BSI und den in dessen Auftrag handelnden Personen das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten gestatten, auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorlegen, Auskünfte erteilen und sonstige erforderliche Unterstützung gewähren. Bei konkreten Anhaltspunkten für berechnete Zweifel an der Einhaltung des § 8a Abs. 1 BSIG darf das BSI nach § 8a Abs. 4 Satz 3 BSIG Gebühren und Auslagen für die Überprüfung des KRITIS-Betreibers erheben. **41**

⁷⁷ Vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/anforderungen_gain.pdf?__blob=publicationFile&v=5 (zuletzt abgerufen am 12.5.2024).

⁷⁸ Vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Themen-Downloads/IT-TK/anforderungen-anlage-rz.pdf?__blob=publicationFile&v=5 (zuletzt abgerufen am 28.4.2024).

⁷⁹ Grundsätzliche Anforderungen im Nachweisverfahren (GAI_N) vom 12.5.2023, Abschnitt 1.

⁸⁰ Vgl. https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-Nachweise/OH_Nachweise/orientierungshilfe_node.html (zuletzt abgerufen am 28.4.2024).

- 42 § 7 BSIG enthält eine Ermächtigung für das BSI zu Warnungen und Empfehlungen. Nach Abs. 1 Satz 1 Nr. 1 kann das BSI Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten und Warnungen an die Öffentlichkeit oder die betroffenen Kreise veröffentlichen, zum Beispiel in Bezug auf Sicherheitslücken in informationstechnischen Produkten und Diensten, auf Schadprogramme sowie bei einem Verlust oder unerlaubten Zugriff auf Daten. Außerdem kann das BSI Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen (§ 7 Abs. 1 Satz 1 Nr. 2 BSIG). Erlässt das BSI Warnungen oder Empfehlungen bzgl. bestimmter informationstechnischer Produkte oder Dienste, so dürfte insoweit von einer Änderung des „Standes der Technik“ auszugehen sein, sodass Unternehmen solche Warnungen und Empfehlungen berücksichtigen müssen.⁸¹
- 43 Wenn hinreichende Anhaltspunkte dafür vorliegen, dass von diesen Produkten oder Diensten Sicherheitslücken bzw. Gefahren für die Sicherheit in der Informationstechnik ausgehen, darf das BSI die Öffentlichkeit sogar unter Nennung der Bezeichnung und des Herstellers des betroffenen Produkts/Dienstes warnen. Vor Produktwarnungen müssen die Hersteller rechtzeitig informiert werden, sofern hierdurch der Zweck der Maßnahme nicht gefährdet wird (§ 7 Abs. 1 Satz 3 BSIG).

b) KRITIS-Dachgesetz

- 44 Seit dem 21.12.2023 liegt der zweite Referentenentwurf für das KRITIS-Dachgesetz (KRITIS-DachG) vor.⁸² Kern der Anforderungen nach dem KRITIS-DachG wird die Pflicht zur Etablierung von Resilienzmaßnahmen nach § 10 KRITIS-DachG-RefE sein, wonach Betreiber kritischer Anlagen verpflichtet sind, geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz zu treffen.⁸³ Dazu können z. B. Maßnahmen zur Anpassung an den Klimawandel, Zugangskontrollen, Notstromversorgung oder die Ermittlung alternativer Lieferketten zählen (vgl. § 10 Abs. 3 KRITIS-DachG-RefE). Diese Pflicht besteht nach Ablauf von zehn Monaten nach der Registrierung, welche gem. § 6 KRITIS-DachG-RefE spätestens drei Monate nach dem Zeitpunkt zu erfolgen hat, zu dem der Betreiber erstmals oder erneut als Betreiber kritischer Anlagen gilt. Für die Einrichtung der Resilienzmaßnahmen helfen zum einen die Ergebnisse der staatlichen Risikoanalyse und -bewertung (§ 8 KRITIS-DachG-RefE), zum anderen die der eigenen Risikoanalyse und -bewertung nach § 9 KRITIS-DachG-RefE, die alle

81 Anders aber *Guckelberger*, DVBl 2019, 525, 533.

82 Referentenentwurf vom 21.12.2023, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwurfe/KM4/KRITIS-DachG-2.pdf;jsessionid=B717C873DE9C79D411064EACB83BE046.live861?__blob=publicationFile&v=4 (zuletzt abgerufen am 29.2.2024)

83 *Kipker/Dittrich*, ZRP 2023, 230, 231.

vier Jahre durchzuführen ist (wobei jeweils der Stand der Technik einzuhalten ist) (vgl. § 10 Abs. 2 KRITIS-DachG-RefE).⁸⁴

c) DSGVO

Den zweiten wichtigen Regelungsrahmen bietet die DSGVO mit Art. 32 **45** DSGVO. Zwar bezweckt der Datenschutz primär den Schutz der Person, nicht der Daten. Dennoch besteht eine inhärente Verknüpfung zur IT-Sicherheit, denn ein unberechtigter Zugriff auf die IT-Systeme kann zu einem Verlust oder unberechtigten Zugriff auf personenbezogene Daten führen.⁸⁵ Deshalb verpflichtet in der Regel alle Datenschutzgesetze, und insbesondere auch die DSGVO, IT-Systeme jedenfalls insoweit gegen unbefugten Zugriff oder Versagen zu schützen, als mit ihnen personenbezogene Daten verarbeitet werden. Nach Art. 32 Abs. 1 DSGVO sind sowohl der Verantwortliche als auch der Auftragsverarbeiter verpflichtet, geeignete technische und organisatorische Maßnahmen⁸⁶ zum Schutz personenbezogener Daten und zur Vorbeugung gegen ihre unrechtmäßige Verarbeitung zu treffen.⁸⁷ Der Verantwortliche kann zwar ihn treffende Pflichten durch einen Auftragsverarbeiter erfüllen lassen, zum Beispiel, wenn personenbezogene Daten gar nicht beim Verantwortlichen selbst verarbeitet werden. Dies ändert jedoch nichts daran, dass der Verantwortliche selbst Pflichtenadrsat bleibt.⁸⁸

Die entsprechenden Maßnahmen müssen ein Schutzniveau gewährleisten, das **46** den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist.⁸⁹ Art. 32 Abs. 1 DSGVO verpflichtet den Verantwortlichen und den Auftragsverarbeiter mithin nicht zu einem absoluten Schutz(niveau) der Daten.⁹⁰ Das Schutzniveau muss vielmehr, je nach Verarbeitungskontext und dem Risiko für die Rechte und Freiheiten der betroffenen Personen im Einzelfall angemessen sein. Für die Analyse des konkret notwendigen Schutzniveaus gibt die DSGVO eine Reihe von zu berücksichtigenden Fakto-

⁸⁴ Kipker/Dittrich, ZRP 2023, 230, 232.

⁸⁵ Schmitz/v. Dall'Armi, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil XII, Kap. 1. Anforderungen an die IT-Sicherheit und deren rechtliche Grundlage Rn. 5. Zum Datenschutz im Compliance Management ausführlich → Becker/Böhlke/Fladung, Kap. 12.

⁸⁶ Für eine Übersicht über in Frage kommende Maßnahmen zum Schutz der Datensicherheit und des Datenschutzes vgl. Schmitz/v. Dall'Armi, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil XII., Kap. 1. Anforderungen an die IT-Sicherheit und deren rechtliche Grundlage Rn. 37. Für eingehendere Ausführungen vgl. Schmieder, in: Forgó/Helfrich/Schneider Betr. Datenschutz, Teil XII., Kap. 2. Technische und organisatorische Maßnahmen Rn. 44 ff.

⁸⁷ Conrad, in: Auer-Reinsdorf/Conrad, HdB IT- und Datenschutzrecht, § 33 Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung Rn. 180.

⁸⁸ Piltz, in: Gola/Heckmann, DS-GVO/BDSG, Art. 32 Rn. 8.

⁸⁹ ErwG 83 zu DSGVO.

⁹⁰ Martini, in: Paal/Pauly, DS-GVO BDSG, Art. 32 Rn. 46. Siehe auch → Becker/Böhlke/Fladung, Kap. 12 Rn. 30 ff.

ren vor.⁹¹ Im Ergebnis ist also eine Verhältnismäßigkeitsprüfung anhand dieser Prüfungsfaktoren vorzunehmen.⁹² Daraus ergibt sich auch, dass die Maßnahmen das angemessene Schutzniveau nicht nur einmalig herstellen, sondern auch in der Zukunft beibehalten müssen.⁹³ Die Erfüllung der Umsetzungspflicht wird damit von einer Verhältnismäßigkeitsprüfung abhängig gemacht.⁹⁴ Im Ergebnis ist eine Schutzbedarfsfeststellung bzw. Risikoanalyse⁹⁵ durch das Unternehmen vorzunehmen, deren Ziel und Zweck es ist zu klären, welches Schutzniveau Informationen (bzw. die zugehörigen Dokumente oder Daten) benötigen, und welche angemessenen Sicherheitsmaßnahmen für die einzelnen Objekte erforderlich sind.⁹⁶ Im Rahmen der Schutzbedarfsfeststellung sollten folgende Schritte eingehalten werden: Strukturanalyse, Einrichtung von Schutzbedarfskategorien (Schutzklassen),⁹⁷ Feststellung (Klassifikation) des Schutzbedarfs von Gruppen von Verarbeitungstätigkeiten sowie Ableitung (Klassifikation) des Schutzbedarfs der weiteren, damit zusammenhängenden IT-Systeme und Kommunikationsverbindungen.⁹⁸ Im Rahmen der Risikoanalyse wird v. a. anhand der Eintrittswahrscheinlichkeit und des Schadensausmaßes das Gefährdungspotenzial ermittelt.

- 47 Im Rahmen der Verhältnismäßigkeitsprüfung sind gemäß Art. 32 Abs. 1 DSGVO folgende Prüfungsfaktoren zu beachten: der Stand der Technik, die Implementierungskosten und Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen. Insbesondere fließt hier auch eine Einschätzung des Risikos ein, dass ein unautorisierter Zugriff überhaupt erfolgt. Mit dem „Stand der Technik“ sind nicht die absolut besten und leistungsfähigsten Technologien zum Zeitpunkt der Verhältnismäßigkeitsprüfung gemeint, sondern vielmehr bekannte, bewährte und effektive Maßnahmen, die derzeit auf dem Markt verfügbar und etabliert sind.⁹⁹ Es muss somit die aktuelle Marktsituation und das Verhalten von Wettbewerbern analysiert werden.

91 Martini, in: Paal/Pauly, DS-GVO BDSG, Art. 32 Rn. 48.

92 Schmieder, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil XII, Kap. 2. Technische und organisatorische Maßnahmen, Rn. 24.

93 Piltz, in: Gola/Heckmann, DS-GVO/BDSG, Art. 32 Rn. 11 f.

94 Piltz, in: Gola/Heckmann, DS-GVO/BDSG, Art. 32 Rn. 9.

95 Wie eine solche Risikoanalyse aussehen könnte, veranschaulichen Schmitz/v. Dall'Armi, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil XII, Kap. 1. Anforderungen an die IT-Sicherheit und deren rechtliche Grundlage, Rn. 35.

96 Conrad, in: Auer-Reinsdorff/Conrad, HdB IT- und Datenschutzrecht, § 33 Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, Rn. 193.

97 Für Einzelheiten vgl. Conrad, in: Auer-Reinsdorff/Conrad, HdB IT- und Datenschutzrecht, § 33 Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, Rn. 195 ff.

98 Conrad, in: Auer-Reinsdorff/Conrad, HdB IT- und Datenschutzrecht, § 33 Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, Rn. 194.

99 Piltz, in: Gola/Heckmann, DS-GVO/BDSG, Art. 32 Rn. 18; Schmitz/v. Dall'Armi, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil XII, Kap. 1. Anforderungen an die IT-Sicherheit und deren rechtliche Grundlage, Rn. 47.

Zudem sind auch Informationen und Empfehlungen staatlicher Stellen zu berücksichtigen, wie etwa die IT-Grundschutz-Kataloge des BSI, die weitere Empfehlungen zur Gewährleistung der IT-Sicherheit enthalten und im EU-Raum die ISO 27000-Normenreihe mit dem Zertifizierungsstandard ISO 27002.¹⁰⁰

Der zweite Prüfungsfaktor – die Implementierungskosten – erlaubt es dem Verantwortlichen, ökonomische Aspekte in die Ermittlung des notwendigen Schutzniveaus einzubeziehen.¹⁰¹ Der Verantwortliche hat im Rahmen einer Wirtschaftlichkeitsbetrachtung zu prüfen, ob Kosten und Risiken in einem angemessenen Verhältnis zueinander stehen.¹⁰² Hohe Implementierungskosten allein können es jedoch nicht rechtfertigen gar keine oder schlechterdings unzureichende Sicherheitsmaßnahmen zu treffen, sondern nur die Art und den Umfang der erforderlichen Maßnahmen beeinflussen.¹⁰³ Im Ergebnis bewirkt der Prüfungsfaktor der Implementierungskosten, dass nicht alles implementiert werden muss, was dem gegenwärtigen Stand der Technik entspricht, wenn dadurch die Kosten unverhältnismäßig hoch werden.¹⁰⁴ Grundsätzlich gilt: Je risikoreicher die Datenverarbeitung und je größer der daraus resultierende Schaden für die betroffene Person, desto höhere notwendige Implementierungskosten müssen in Kauf genommen werden.¹⁰⁵ Streitig ist hier insbesondere, ob mit den Implementierungskosten auch Folgekosten (und nicht nur einmalige Kosten der Einführung von Maßnahmen) erfasst werden können. Hierfür spricht viel; insbesondere sollen die Implementierungskosten wohl alle Kosten erfassen, die für die Umsetzung der Maßnahmen erforderlich sind. Dazu gehören aber auch laufende und Folgekosten.¹⁰⁶

100 *Martini*, in: Paal/Pauly, DS-GVO BDSG, Art. 32 Rn. 57 f. Es gibt zahlreiche weitere Kataloge, wie etwa die des TeleTrusT, Handreichung zum „Stand der Technik“ technischer und organisatorischer Maßnahmen, 2018, https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/TeleTrusT-Handreichung_Stand_der_Technik_-_Ausgabe_2018.pdf (zuletzt abgerufen am 15.5.2024).

101 *Laue*, in: Spindler/Schuster, Recht der elektronischen Medien, DS-GVO Art. 32 Rn. 7.

102 *Jandt*, in: Kühling/Buchner, DS-GVO/BDSG, Art. 32 Rn. 11; *Schultze-Melling*, in: Taeger/Gabel, DSGVO – BDSG – TTDSG, Art. 32 Rn. 14.

103 *Laue*, in: Spindler/Schuster, Recht der elektronischen Medien, DS-GVO Art. 32 Rn. 7; *Mantz*, in: Sydow, Europäische Datenschutzgrundverordnung, DSGVO Art. 32 Rn. 1, 10; *Paulus*, in: BeckOK DatenschutzR, 31. Ed. 1.11.2019, DS-GVO Art. 32 Rn. 9; a. A. *Martini*, in: Paal/Pauly, DS-GVO BDSG, Art. 32 Rn. 60, wenn die Gefahren für den Betroffenen gering sind und Datensicherheitsmaßnahmen zugleich hohe Implementierungskosten nach sich zögen.

104 *Schultze-Melling*, in: Taeger/Gabel, DSGVO – BDSG – TTDSG, Art. 32 Rn. 14.

105 *Jandt*, in: Kühling/Buchner, DS-GVO/BDSG, Art. 32 Rn. 11; *Schultze-Melling*, in: Taeger/Gabel, DSGVO – BDSG – TTDSG, Art. 32 Rn. 14.

106 So auch *Laue*, in: Spindler/Schuster, Recht der elektronischen Medien, DS-GVO Art. 32 Rn. 8; *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, DSGVO Art. 32 Rn. 26; *Martini*, in: Paal/Pauly, DS-GVO BDSG, Art. 32 Rn. 60a; jetzt auch *Mantz*, in: Sydow, Europäische Datenschutzgrundverordnung, DSGVO Art. 32 Rn. 1, 10. Anders aber *Schmitz/v. Dall'Armi*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil XII, Kap. 1. Anforderungen an die IT-Sicherheit und deren rechtliche Grundlage, Rn. 50.

- 49 Bei der Risikobestimmung sind auch besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO zu identifizieren, die besonderen Beschränkungen oder Anforderungen unterliegen.¹⁰⁷
- 50 Allerdings sind diese Prüfungsfaktoren nur zu „berücksichtigen“, d. h., sie müssen in der Verhältnismäßigkeitsprüfung zwar beachtet, aber nicht notwendigerweise insgesamt geschützt werden. Dies ist insbesondere für den Prüfungsfaktor „Stand der Technik“ relevant. Dieser ist bei der erforderlichen Abwägungsentscheidung vor Umsetzung der Maßnahmen zu berücksichtigen und quasi als Leitlinie zu beachten.¹⁰⁸
- 51 In Übereinstimmung mit dem Gedanken der Technikneutralität und Entwicklungsoffenheit werden keine konkreten Maßnahmen verlangt. Art. 32 Abs. 1 Hs. 2 DSGVO zählt jedoch einige Maßnahmen und insbesondere Datensicherheitsziele auf, die von den verpflichteten Stellen zu erreichen sind: (a) Pseudonymisierung und Verschlüsselung personenbezogener Daten; (b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; (c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen und (d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu etablieren. Die Aufzählung in Art. 32 Abs. 1 Hs. 2 DSGVO erfolgt entgegen des Wortlauts nur beispielhaft und orientiert sich ebenfalls am Verhältnismäßigkeitsprinzip.¹⁰⁹
- 52 Gesetzliche Definitionen der verwendeten Begrifflichkeiten im Rahmen von Maßnahme (b) existieren in der DSGVO nicht. Für die Anwendung in der Praxis kann auf die bereits bekannten Definitionen der Begriffe durch das BSI zurückgegriffen werden.¹¹⁰ Danach ist unter Vertraulichkeit der Schutz vor unbefugter Preisgabe von Informationen zu verstehen. Die DSGVO definiert insbesondere den neuen Begriff der Belastbarkeit nicht weiter. Darunter ist wohl die Fähigkeit der Systeme zu verstehen, auch unter hoher Inanspruchnahmefrequenz ordnungsgemäß zu funktionieren.¹¹¹ Die verwendete IT-Infrastruktur, d. h. Räumlichkeiten, Hard- und Software, Netze und Dienste, muss möglichst wenig risikofähig sein. Durch dieses Schutzziel der „Belastbarkeit“ wird ein neuer

107 Conrad, in: Auer-Reinsdorff/Conrad, HdB IT- und Datenschutzrecht, § 33 Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, Rn. 185. Siehe auch → Becker/Böhlke/Fladung, Kap. 12 Rn. 46.

108 Piltz, in: Gola/Heckmann, DS-GVO/BDSG, Art. 32 Rn. 14.

109 Piltz, in: Gola/Heckmann, DS-GVO/BDSG, Art. 32 Rn. 23 f.

110 Vgl. IT-Grundschutz-Kompendium, Glossar (Edition 2023), S. 35 ff. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1 (zuletzt abgerufen am 15.5.2024).

111 Piltz, in: Gola/Heckmann, DS-GVO/BDSG, Art. 32 Rn. 31.

Fokus auf die Effizienz der technischen und organisatorischen Maßnahmen gelegt, der stärker ist als im BDSG-alt.¹¹²

Art. 32 Abs. 1 lit. d DSGVO verpflichtet zur regelmäßigen dokumentierten Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen zur Sicherstellung der Datensicherheit. Der Verantwortliche muss den Nachweis erbringen, dass die umgesetzten Maßnahmen bezogen auf das prognostizierte Risiko geeignet sind, ein angemessenes Schutzniveau zu gewährleisten und somit den Anforderungen des Art. 32 gerecht werden.¹¹³ **53**

Die Norm konkretisiert nicht, wie genau derartige Untersuchungen auszugestaltet sind. Daher kommen sowohl technische Maßnahmen wie etwa Penetrationstests¹¹⁴ als auch organisatorische Maßnahmen in Frage, wie etwa externe oder interne Prüfberichte,¹¹⁵ Befragungen von Nutzern oder Betroffenen oder die Einsichtnahme in den Ablauf und die Ergebnisse von Verarbeitungsprozessen.¹¹⁶ Außerdem ist zu denken an die Auswertung von Sicherheitsmeldungen des Verarbeitungssystems, auffälligen Protokolleinträgen, Hinweisen der Hersteller auf Updates oder Patches sowie Warnungen aus der Fachpresse oder durch das BSI.¹¹⁷ Im Rahmen der Bewertung und Evaluierung sind die Testergebnisse auszuwerten. Sollte der Verantwortliche zu dem Ergebnis kommen, dass die Wirksamkeit der Maßnahmen nicht (mehr) ausreichend ist, besteht die Pflicht zur Anpassung der technischen und organisatorischen Maßnahmen.¹¹⁸ **54**

Die genauen Zeitabstände für eine Überprüfung werden nicht näher konkretisiert und sind daher vom Verantwortlichen selbst risikoorientiert zu bestimmen.¹¹⁹ Je größer das Risiko für einen internen oder externen Systemangriff und je höher das angemessene Schutzniveau, desto häufiger sind die Kontrollen durchzuführen. **55**

112 *Conrad*, in: Auer-Reinsdorff/Conrad, HdB IT- und Datenschutzrecht, § 33 Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, Rn. 203.

113 *Piltz*, in: Gola/Heckmann, DS-GVO/BDSG, Art. 32 Rn. 36, 37; *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, DSGVO Art. 32 Rn. 53 f.

114 Dabei werden Systemangriffe simuliert, um die Empfindlichkeit des Systems zu prüfen, vgl. *Hladjk*, in: Ehmann/Selmayr, DS-GVO, 3. Aufl. 2024, Art. 32 Rn. 10; *Jandt*, in: Kühling/Buchner DS-GVO/BDSG, Art. 32 Rn. 29.

115 *Schmitz/v. Dall'Armi*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil XII, Kap. 1. Anforderungen an die IT-Sicherheit und deren rechtliche Grundlage, Rn. 40 f.

116 *Laue*, in: Spindler/Schuster, Recht der elektronischen Medien, DS-GVO Art. 32 Rn. 18; weitere Methoden bei *Martini*, in: Paal/Pauly, DS-GVO BDSG, Art. 32 Rn. 44–44a.

117 *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, DSGVO Art. 32 Rn. 56.

118 *Jandt*, in: Kühling/Buchner, DS-GVO/BDSG, Art. 32 Rn. 29; *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, DSGVO Art. 32 Rn. 56; *Martini*, in: Paal/Pauly, DS-GVO BDSG, Art. 32 Rn. 44a; *Behling*, ZIP 2017, 697, 702.

119 *Laue*, in: Spindler/Schuster, Recht der elektronischen Medien, DS-GVO Art. 32 Rn. 19; *Jandt*, in: Kühling/Buchner, DS-GVO/BDSG, Art. 32 Rn. 30; *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, DSGVO Art. 32 Rn. 55.

ren.¹²⁰ Das Angriffsrisiko steigt in der Regel mit dem Umfang der behandelten Daten, der Komplexität der Verarbeitungsprozesse und der Zahl der (Unter-) Auftragnehmer.¹²¹ Zudem sind anlassbezogene Kontrollen anzuraten, etwa wenn sich die technischen oder organisatorischen Rahmenbedingungen ändern (z.B. bei einem Software-Update) oder wenn neue Bedrohungen oder Meldungen von Sicherheitsvorfällen bekannt werden.¹²²

- 56** Die vorgenommene Planung und Durchführung der Tests sowie die Testergebnisse sollten dokumentiert werden, um die regelmäßige Überprüfung im Zweifelsfall entsprechend Art. 5 Abs. 2 DSGVO nachweisen zu können.¹²³
- 57** Nach Art. 83 Abs. 4 lit. a DSGVO kann ein Verstoß gegen die Vorgaben des Art. 32 DSGVO mit einem Bußgeld von bis zu 10.000.000 EUR oder von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet werden. Nach Art. 83 Abs. 2 lit. d DSGVO ist jedoch bei der Entscheidung über die Verhängung eines Bußgeldes zu berücksichtigen, welche technischen und organisatorischen Maßnahmen getroffen wurden. Das bedeutet, dass wirksame und geeignete Maßnahmen sich bei dem Ob und der Höhe des Bußgeldes bei einem Verstoß gegen die Vorgaben der DSGVO mildernd auswirken.¹²⁴ In diesem Zusammenhang erlangt die Dokumentations- und Nachweispflicht besondere Bedeutung, denn nur solche Compliance-Maßnahmen, deren Vornahme nachgewiesen werden kann, können auch geltend gemacht werden.¹²⁵ Die Dokumentations- und Nachweispflicht ergibt sich aus der allgemeinen Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) für die Datensicherheit, die sich explizit aus Art. 5 Abs. 1 lit. f ergibt. Relevant für Unternehmen ist, dass Art. 32 Abs. 3 DSGVO es dem Verantwortlichen und dem Auftragsverarbeiter ermöglicht, die Anforderungen an die geeigneten technischen und organisatorischen Maßnahmen durch Einhaltung genehmigter Verhaltensregeln (Art. 40 Abs. 2 lit. H DSGVO), oder eines genehmigten Zertifizierungsverfahrens (Art. 42 DSGVO) nachzuweisen.¹²⁶

120 Jandt, in: Kühling/Buchner, DS-GVO/BDSG, Art. 32 Rn. 30; Hansen, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, DSGVO Art. 32 Rn. 55; Laue, in: Spindler/Schuster, Recht der elektronischen Medien, DS-GVO Art. 32 Rn. 19; Mantz, in: Sydow, Europäische Datenschutzgrundverordnung, DSGVO Art. 32 Rn. 21.

121 Martini, in: Paal/Pauly, DS-GVO BDSG, Art. 32 Rn. 45a.

122 Jandt, in: Kühling/Buchner, DS-GVO/BDSG, Art. 32 Rn. 30; Hansen, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, DSGVO Art. 32 Rn. 55.

123 Hansen, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, DSGVO Art. 32 Rn. 56; Laue, in: Spindler/Schuster, Recht der elektronischen Medien, DS-GVO Art. 32 Rn. 19.

124 Piltz, in: Gola/Heckmann, DS-GVO/BDSG, Art. 32 Rn. 57.

125 Conrad, in: Auer-Reinsdorff/Conrad, HdB IT- und Datenschutzrecht, § 33 Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, Rn. 210.

126 Hladjk, in: Ehmann/Selmayr, DS-GVO, 3. Aufl. 2024, Art. 32 Rn. 15.

d) BDSG

Die Regelung der erforderlichen Sicherheitsmaßnahmen in Art. 32 DSGVO ist an die Stelle von § 9 BDSG-alt getreten,¹²⁷ der mitsamt der Anlage hierzu ersatzlos entfallen ist.¹²⁸ **58**

Im neuen BDSG hat § 64 BDSG einen ähnlichen Regelungsgehalt zu § 9 BDSG-alt,¹²⁹ allerdings nur für die Datenverarbeitung durch Polizei und Justiz zum Zweck der Gefahrenabwehr bzw. Strafverfolgung (vgl. § 45 Satz 1 BDSG).¹³⁰ Der allgemeine datenschutzrechtliche Teil des BDSG enthält keine Vorschrift mehr zu technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung.¹³¹ § 64 BDSG konkretisiert den Grundsatz der Sicherheit der Verarbeitung aus § 47 Nr. 6 BDSG.¹³² Die in § 64 Abs. 2 BDSG genannten Zwecke, die durch die ausgewählten technischen und organisatorischen Maßnahmen erzielt werden müssen, spiegeln die Inhalte des Art. 32 Abs. 1 lit. a–c DSGVO wieder. Abs. 3 konkretisiert die zu erreichenden Zwecke für den Fall einer automatisierten Verarbeitung. Der Katalog entspricht weitestgehend § 9 BDSG-alt und dem Anhang hierzu.¹³³ **59**

e) TTDSG und TKG*aa) TTDSG*

Mit dem seit Dezember 2021 in Kraft getretenen TTDSG sind die datenschutzrechtlichen Vorschriften des TMG entfallen. Dies gilt insbesondere für Art. 13 Abs. 7 TMG-alt, an dessen Stelle nun § 19 Abs. 7 TTDSG getreten ist, dem neben Art. 32 DSGVO insofern eine eigenständige Bedeutung zukommt,¹³⁴ als die technisch-organisatorische Vorkehrungen eben nicht nur personenbezogene Daten schützen müssen, sondern die für Telemedienangebote genutzten Einrichtungen insgesamt – und dies, obwohl sie an sich keine kritischen Infrastrukturen betreiben (siehe hierzu → Rn. 24). **60**

bb) TKG

Nach § 165 Abs. 1 TKG (bisher: § 109 TKG-alt) haben Erbringer von Telekommunikationsdiensten oder daran Mitwirkende angemessene technische Vorkehrungen und sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten zu treffen. Hinzu kommen Verpflichtungen nach **61**

127 *Conrad*, in: Auer-Reinsdorff/Conrad, HdB IT- und Datenschutzrecht, § 33 Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, Rn. 182.

128 *Jandt*, in: Kühling/Buchner, DS-GVO/BDSG, Art. 32 Rn. 41.

129 *Marnau*, in: Gola/Heckmann, BDSG, § 64 Rn. 3.

130 *Braun*, in: Gola/Heckmann, BDSG, § 45 Rn. 1–2.

131 *Jandt*, in: Kühling/Buchner, DS-GVO/BDSG, Art. 32 Rn. 41.

132 *Bock*, in: BeckOK DatenschutzR, 31. Ed. 1.2.2020, BDSG, § 64 Rn. 1.

133 *Gräber/Nolden*, in: Paal/Pauly, DS-GVO BDSG, § 64 Rn. 5–6.

134 So wohl auch *Jandt*, in: Kühling/Buchner, DS-GVO BDSG, Art. 32 DSGVO, Rn. 42–44.

§ 165 Abs. 2 ff. und §§ 166 ff. TKG zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von TK-Netzen und Diensten führen können. Insbesondere sind die Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Maßnahmen zu treffen, um den ordnungsgemäßen Betrieb der Netze zu gewährleisten und Risiken für deren Sicherheit zu beherrschen.

- 62 Nach § 166 TKG ist von den Diensteanbietern ein Sicherheitsbeauftragter zu bestimmen, ein in der Europäischen Union ansässiger Ansprechpartner zu benennen und ein Sicherheitskonzept zu erstellen. Dieses Sicherheitskonzept ist der Bundesnetzagentur unverzüglich nach Aufnahme des Netzbetriebes vorzulegen. Die Bundesnetzagentur kann auch eine Überprüfung des Sicherheitskonzepts und seiner Implementierung anordnen, sowie Abhilfemaßnahmen fordern, wenn sich dabei Mängel herausstellen. Nach § 167 TKG stellt die Bundesnetzagentur gemeinsam mit dem BSI Sicherheitskataloge¹³⁵ auf, die verbindliche Mindeststandards darstellen. § 8a BSIG ist gem. § 8c Abs. 2 Satz 1 Nr. 1 BSIG nicht gleichzeitig anwendbar; die datenschutzrechtlichen Pflichten gelten aber daneben auch für Telekommunikationsdiensteanbieter, schon in Ausfüllung des § 165 Abs. 1 Satz 1 Nr. 2 TKG.

cc) Verhältnis zur DSGVO

- 63 Als EU-Verordnung hat die DSGVO grundsätzlich in ihrem Anwendungsbereich Vorrang vor den nationalen Bestimmungen des Datenschutzes.¹³⁶ Art. 95 DSGVO erklärt jedoch nationale Ausführungsvorschriften zur ePrivacy-Richtlinie zur *lex specialis* gegenüber den gleichgerichteten Vorschriften der DSGVO.¹³⁷ Demnach werden nur solche nationalen Regelungen im Anwendungsbereich der DSGVO von dieser verdrängt, die entweder nicht auf der ePrivacy-Richtlinie beruhen oder die ePrivacy-Richtlinie überschießend umsetzen. Eine weitere Ausnahme besteht für Regelungen, die über eine Öffnungsklausel der DSGVO Anwendung finden (für öffentliche Stellen kommt insbesondere Art. 6 Abs. 2 DSGVO in Betracht).¹³⁸ Da § 19 Abs. 4 TTDSG nach wohl herrschender Meinung keine Umsetzung der ePrivacy-Richtlinie darstellt,¹³⁹ dürfte

135 Bundesnetzagentur, Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG) Version 2.0, Stand 29.4.2020, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen.pdf?__blob=publicationFile&v=6 (zuletzt abgerufen am 15.5.2024).

136 Eckhardt, in: Spindler/Schuster, Recht der elektronischen Medien, TKG § 91 Rn. 6.

137 Karg, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, DSGVO Art. 95 Rn. 16; Holländer, in: BeckOK DatenschutzR, 31. Ed. 1.11.2019, DS-GVO Art. 95 Rn. 5.

138 Golland, in: Taeger/Gabel, DSGVO – BDSG – TTDSG, Art. 95 Rn. 17.

139 Jandt, in: Kühling/Buchner, DS-GVO BDSG, Art. 32 DSGVO, Rn. 42–44; Golland, in: Taeger/Gabel, DSGVO – BDSG – TTDSG, Art. 95 Rn. 26; Gierschmann, in: Gierschmann/Baumgartner, TTDSG § 1 Rn. 21.

es hier an einer Öffnungsklausel fehlen und die Regelung insoweit von Art. 32 DSGVO verdrängt werden, als sie personenbezogene Daten betrifft.¹⁴⁰ Im Hinblick auf die Konkurrenz von TKG zur DSGVO gilt Folgendes: Jedenfalls für Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes setzen die §§ 162 ff. TKG (auch) die ePrivacy-Richtlinie (insb. deren Art. 4) um und verdrängen insoweit Art. 32 DSGVO.¹⁴¹ Ob das aber auch für den über die ePrivacy-Richtlinie hinausgehenden Bereich, also Betreiber von nicht öffentlich zugänglichen Telekommunikationsdiensten, gilt, ist zumindest fraglich¹⁴² – der praktische Anwendungsbereich ist aber wohl gering.

f) KWG, ZAG, MaRisk etc.

Kreditinstitute müssen nach § 25a KWG über eine ordnungsgemäße Geschäftsorganisation verfügen, wozu auch die Einrichtung eines angemessenen und wirksamen Risikomanagements gehört. Die Verantwortung hierfür liegt bei der Geschäftsleitung. Es wird jedoch vom Gesetz selbst kein konkretes Risikomanagement vorgegeben, sondern lediglich bestimmte qualitative Mindeststandards festgelegt. Ausgangspunkt der Überlegungen zum Risikomanagement ist der Schutz des Kundenvermögens, die Sicherstellung der Ordnungsmäßigkeit der Erbringung der Bank- und Finanzdienstleistungen, die Vermeidung von erheblichen Nachteilen für die Gesamtwirtschaft sowie der Schutz der Kunden bei Erbringung von Wertpapierdienstleistungen und Wertpapiernebenleistung. Für Zahlungsdienstleistungen hat die EU-Richtlinie (EU) 2015/2366 vom 25.11.2015¹⁴³ (gemeinhin als PSD II bezeichnet) weitgehende und komplexe Anforderungen eingeführt. Diese wurden 2017 ins deutsche Recht umgesetzt (§ 55 Abs. 1 ZAG),¹⁴⁴ was seit dem 15.3.2021 auch aufsichtsbehördlich verbindlich ist (auch in Bezug auf die sog. Starke Kundenauthentifizierung, auch Zwei-Faktor- oder Multi-Faktor-Authentifizierung genannt). Ziel der Starken Kundenauthentifizierung ist eine Anhebung des Sicherheitsniveaus bei den drei genannten Transaktionen; Kern ist die Doppelung der zu verwendenden Authenti-

64

140 Golland, in: Taeger/Gabel, DSGVO – BDSG – TTDSG, Art. 95 Rn. 26; Gierschmann, in: Gierschmann/Baumgartner, TTDSG § 1 Rn. 21 m. w. N. Anderer Ansicht wohl Karg, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, DSGVO Art. 95 Rn. 16; Holländer, in: BeckOK DatenschutzR, 31. Ed. 1.11.2019, DS-GVO Art. 95 Rn. 22.

141 Golland, in: Taeger/Gabel, DSGVO – BDSG – TTDSG, Art. 95 Rn. 25; Karg, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, DSGVO Art. 95 Rn. 16; Holländer, in: BeckOK DatenschutzR, 31. Ed. 1.11.2019, DS-GVO Art. 95 Rn. 22.

142 Eckhardt, in: Geppert/Schütz, TKG § 165 Rn. 8-14. Anders wohl Golland, in: Taeger/Gabel, DSGVO – BDSG – TTDSG, Art. 95 Rn. 19.

143 Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG.

144 Vgl. https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Verordnungen/2017-07-21-G-z-Umsetzung-d-Zweiten-Zahlungsdiensterichtlinie.html (zuletzt abgerufen am 17.4.2020).

fizierungselemente, die gem. § 1 Abs. 24 ZAG auf mindestens zwei der drei Kriterien Wissen, Besitz, Inhärenz (biometrische Merkmale) basieren müssen. Die z. T. äußerst komplexen technischen Details sind in der zum 14.9.2019 in Kraft getretenen Delegierten-VO (EU) 2018/389 (sog. RTS-Standards) erläutert (vgl. auch unten → Rn. 74).¹⁴⁵

aa) MaRisk (Mindestanforderungen an das Risikomanagement)

- 65 § 25a KWG ist eine allgemeine Norm, die zwar festlegt, dass das Risikomanagement insbesondere die Festlegung eines angemessenen Notfallmanagements, insbesondere für IT-Systeme, erfasst, die Verpflichtungen im Zusammenhang mit Informationstechnologien aber nicht spezifisch nennt.¹⁴⁶ Wichtig sind in diesem Zusammenhang deshalb die von der BaFin aufgestellten MaRisk.¹⁴⁷ Hierbei handelt es sich eher um interne, aber veröffentlichte Interpretationsgrundsätze, wann die BaFin die Anforderungen des § 25a KWG als erfüllt ansieht. Faktisch kommt ihnen damit aber Regelungscharakter zu, und entsprechend werden sie von der BaFin regelmäßig überarbeitet.¹⁴⁸ Einzelne Bankenverbände geben wiederum Interpretationsleitlinien für die MaRisk heraus, die diese noch weiter spezifizieren – so zum Beispiel der Interpretationsleitfaden MaRisk des Deutschen Sparkassen- und Giroverbandes (DSGV).¹⁴⁹ Gemäß § 25b KWG darf eine Auslagerung die ordnungsgemäße Geschäftsorganisation, insbesondere das angemessene und wirksame Risikomanagement, nicht beeinträchtigen und nicht zu einer Übertragung der Verantwortung der Geschäftsleitung an das Auslagerungsunternehmen führen.¹⁵⁰
- 66 Inhaltlich fordern die MaRisk¹⁵¹ eine angemessene technisch-organisatorische Ausstattung des Finanzinstitutes. Konkret ist das Institut entsprechend Art, Umfang, Komplexität und Risikogehalt seiner Geschäftsaktivitäten dazu verpflichtet, Regelungen zur Aufbau- und Ablauforganisation zu treffen sowie angemess-

145 Vgl. Köndgen, in: BeckOGK, BGB § 675j Rn. 31–35.

146 Vgl. Braun/Wolfgarten, in: Boos/Fischer/Schulte-Mattler, KWG, 4. Aufl. 2012, § 25a Rn. 1.

147 Zur MaRisk-Compliance ausführlich → Renz/Frankenberger, Kap. 20 Rn. 23 ff.

148 Insgesamt hierzu aufschlussreich Kokert/Held, IT-Sicherheit: Erwartungen der Bankenaufsicht (Stand 31.10.2013), https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2013/fa_bj_2013_11_it_sicherheit.html (zuletzt abgerufen am 15.5.2024). Zur Compliance-Funktion in einem Kreditinstitut siehe → Renz/Frankenberger, Kap. 20.

149 Vgl. https://www.stiftung-wissenschaft.de/xpage/s-wissenschaft.nsf/xsp/.ibmmodes/domi no/OpenAttachment/xpage/s-wissenschaft.nsf/A13356AE1981245AC12585BC00214385/Anhang/20200402%20ILF%20BaFin_Merkblatt_1.0_Internet.pdf (zuletzt abgerufen am 12.5.2024).

150 So auch Schneider/Forgó/Helfrich, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil XII. Kap. 4. Überblick zu Risikomanagement unter BSiG, BSI-KritisV, NIS-RL i. V. m. DS-GVO Rn. 17.

151 Rundschreiben 05/2023 (BA) – Mindestanforderungen an das Risikomanagement – MaRisk https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2023/rs_05_2023_MaRisk_BA.html (zuletzt abgerufen am 7.11.2023). Vgl. insgesamt hierzu Krimphove, BKR 2023, 500.

sene Risikosteuerungs- und Risikocontrollingprozesse einzurichten, die eine Identifizierung, Beurteilung, Steuerung sowie Überwachung und Kommunikation der wesentlichen Risiken und damit verbundener Risikokonzentrationen (einschließlich der Auswirkungen von ESG-Risiken) gewährleisten (AT 4.3.2 Tz. 1 MaRisk).¹⁵² Durch geeignete Maßnahmen ist sicherzustellen, dass die identifizierten Risiken und damit verbundenen Risikokonzentrationen wirksam begrenzt werden (AT 4.3.2. Tz. 1 MaRisk). Diese Maßnahmen können sowohl aus quantitativen Instrumenten (z. B.: Limit- oder Ampelsysteme) als auch qualitativen Instrumenten (z. B.: regelmäßige Risikoanalysen) bestehen. Bestandteile einer ordnungsgemäßen Geschäftsorganisation sind nach den MaRisk insbesondere, dass die etablierten Regelungen zur Aufbau- und Ablauforganisation schriftlich dokumentiert sind und die betroffenen Mitarbeiter die Regelungen kennen (AT 5 Tz. 1 und 2 MaRisk), die Beachtung des Prinzips der Funktionstrennung (AT 4.3.1 Tz. 1 MaRisk), die sofortige und vollständige Erfassung aller Geschäftsvorfälle und die laufende Überwachung der Einhaltung der Regelungen.¹⁵³ Das Prinzip der Funktionstrennung verlangt die Verteilung von Funktionen und Tätigkeiten auf verschiedene Personen, Stellen und Bereiche unter Beachtung des Vier-Augen-Prinzips.¹⁵⁴

Bestandteil des Risikomanagements ist auch die in AT 1 Tz. 1 Satz 3 Nr. 3 lit. c MaRisk ausdrücklich geforderte Einrichtung einer Risikocontrolling-Funktion. Die Anforderungen hieran werden konkretisiert in AT 4.4.2 MaRisk. Die Risikocontrolling-Funktion ist für die unabhängige Überwachung und Kommunikation der Risiken zuständig und demzufolge aufbauorganisatorisch von den Bereichen zu trennen, die für die Initiierung bzw. den Abschluss von Geschäften zuständig sind (AT 4.4.1 Tz. 1 MaRisk).¹⁵⁵ Der Compliance-Funktion kommen drei Kernaufgaben zu. Sie muss die wesentlichen rechtlichen Regelungen und Vorgaben identifizieren, deren Nichteinhaltung das Vermögen des Instituts gefährden kann (AT 4.4.2 Tz. 2 MaRisk), auf die Implementierung wirksamer Verfahren zur Einhaltung dieser Regeln und auf entsprechende Kontrollen hinwirken (AT 4.4.2 Tz. 1 Satz 2 MaRisk) und die Geschäftsleitung zukunftsbezogen hinsichtlich der Einhaltung dieser Regeln beraten und unterstützen (AT 4.4.2 Tz. 1 Satz 3 MaRisk).¹⁵⁶ Bei wichtigen risikopolitischen Entscheidungen der Geschäftsleitung ist die Leitung der Risikocontrolling-Funktion zu beteiligen (AT 4.4.1 Tz. 4 MaRisk).

Weitere essenzielle Bestandteile des Risikomanagements sind die sog. Stress-
tests und die Pflicht zur Einrichtung einer Internen Revision (AT 4.4.3 Ma-

67**68**

152 *Braun*, in: Fischer/Schulte-Mattler, KWG, § 25a Rn. 372–374. Siehe auch → *Renz/Frankenberger*, Kap. 20 Rn. 26 ff.

153 *Braun*, in: Fischer/Schulte-Mattler, KWG, § 25a Rn. 377.

154 *Langen/Donner*, in: Schwennicke/Auerbach, KWG, § 25a Rn. 70.

155 *Braun*, in: Fischer/Schulte-Mattler, KWG, § 25a Rn. 238.

156 *Langen/Donner*, in: Schwennicke/Auerbach, KWG, § 25a Rn. 90.

Risk).¹⁵⁷ Stresstest ist ein Oberbegriff für die unterschiedlichen Methoden, mit denen die Institute ihr individuelles Gefährdungspotenzial auch bezüglich außergewöhnlicher Risiken überprüfen.¹⁵⁸ Es sind regelmäßig sowie anlassbezogen angemessene Stresstests für die wesentlichen Risiken durchzuführen, die Art, Umfang, Komplexität und den Risikogehalt der Geschäftsaktivitäten widerspiegeln. Hierfür sind die für die jeweiligen Risiken wesentlichen Risikofaktoren zu identifizieren (AT 4.3.3 Tz. 1 MaRisk).

- 69** Die Geschäftsleitung muss sich in angemessenen Abständen über die Risikosituation berichten lassen (Risikobericht, AT 4.3.2 Tz. 3 MaRisk). Neben dieser regelmäßigen Berichterstattung ist eine Ad-hoc-Berichterstattung bei Eintritt besonderer Ereignisse, Zustände oder Vorkommnisse (z. B. Überschreitung von Grenzwerten, Änderung wesentlicher Marktbedingungen etc.) notwendig. In den Risikoberichten sind insbesondere auch die Ergebnisse der Stresstests, die den Stresstests zugrunde liegenden wesentlichen Annahmen und deren potenzielle Auswirkungen auf die Risikosituation und das Risikodeckungspotenzial darzustellen (BT 3.1 Tz. 2 MaRisk). Weitere Einzelheiten zur Risikoberichterstattung sind in BTR 1–BTR 4 der MaRisk 2012 geregelt. Die Geschäftsleitung hat das Aufsichtsorgan vierteljährlich über die Geschäftslage und die Risikosituation einschließlich vorhandener Risikokonzentrationen in angemessener Weise schriftlich zu informieren (AT 4.3.2 Tz. 3 MaRisk). Die Risikosteuerungs- und -controllingprozesse sowie die zur Risikoquantifizierung eingesetzten Methoden und Verfahren sind regelmäßig sowie bei sich ändernden Bedingungen auf ihre Angemessenheit zu überprüfen und ggf. anzupassen (AT 4.3.2 Tz. 5 MaRisk).¹⁵⁹
- 70** Ziffer AT 4.3.4 der MaRisk verpflichtet „bedeutende Institute“ sowohl auf Gruppenebene als auch auf Ebene der ihr zugehörigen Institute, entscheidungserhebliche Daten zu ermitteln, diese aufzuarbeiten und bereitzustellen.
- 71** Zudem fordern die MaRisk ein angemessenes Notfallkonzept für IT-Systeme (AT 7.3 MaRisk). Die im Notfallkonzept festgelegten Maßnahmen müssen dazu geeignet sein, das Ausmaß möglicher Schäden zu reduzieren. Dabei sind Wirksamkeit und Angemessenheit des Notfallkonzepts regelmäßig zu überprüfen. Das Notfallkonzept muss außerdem auch Geschäftsfortführungs- und Wiederanlaufpläne mit umfassen. Nach AT 7.2 MaRisk müssen die IT-Systeme und IT-Prozesse die Integrität, Verfügbarkeit und Authentizität sowie Vertraulichkeit der Daten sicherstellen. Bei Ausgestaltung der IT-Systeme und IT-Prozesse ist auf die gängigen Standards abzustellen, z. B. ISO/IEC 27001, ISO/IEC 27002, IT-Grundschutzkatalog des BSI, CoBiT oder die Bankaufsichtlichen Anforderungen an die IT (BAIT) der BaFin: Eine wesentliche Neuerung der Novelle der

¹⁵⁷ Für Einzelheiten zur Internen Revision vgl. *Braun*, in: Fischer/Schulte-Mattler, KWG, § 25a Rn. 562 ff.

¹⁵⁸ *Langen/Donner*, in: Schwennicke/Auerbach, KWG, § 25a Rn. 80.

¹⁵⁹ *Braun*, in: Fischer/Schulte-Mattler, KWG, § 25a Rn. 233 und 236.

BAIT vom 16.8.2021¹⁶⁰ betrifft das neu geschaffene Kapitel 10 „IT-Notfalldatenmanagement“, welches den erweiterten AT 7.3. der novellierten MaRisk („Notfallmanagement“) konkretisiert. Ein zentraler Ansatz ist dabei die Erstellung von IT-Notfallplänen in Form von Wideranlauf-, Notbetriebs- und Wiederherstellungsplänen. Die Institute haben die Notfallpläne durch jährliche IT-Notfalltests auf Grundlage eines IT-Testkonzepts zu überprüfen.¹⁶¹ Innerhalb der Sparkassen-Finanzgruppe hat sich außerdem der SIZ Informations-Sicherheitsstandard „Sicherer IT-Betrieb“ etabliert.¹⁶² Die Eignung der IT-Systeme ist vor ihrem erstmaligen Einsatz und nach wesentlichen Änderungen zu testen und abzunehmen und auch anschließend regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen. Zu berücksichtigen ist hier auch AT 8.2 MaRisk, wonach vor wesentlichen Änderungen in den IT-Systemen deren Auswirkungen auf die eingerichteten Kontrollverfahren und die Kontrollintensität zu analysieren sind.

Nach AT 9 Tz. 1 MaRisk gelten die Anforderungen der MaRisk auch dann, wenn ein Institut ein anderes Unternehmen mit der Wahrnehmung oder Teilwahrnehmung seiner Geschäftstätigkeit betraut. Die Auslagerung von Geschäftsaufgaben führt nicht zur Übertragung der Verantwortung der Geschäftsleitung auf ein anderes Unternehmen (AT 9 Tz. 4 MaRisk). Das bedeutet, dass ein Institut Kontrollfunktionen wie etwa die des Risikocontrollings, der Compliance und die der Internen Revision grundsätzlich nicht vollständig outsourcen kann. Diese Funktionen kann ein übergeordnetes Institut allenfalls vollständig auf sein Tochterinstitut innerhalb einer Institutsgruppe auslagern, sofern dieses Tochterinstitut hinsichtlich seiner Größe, Komplexität und dem Risikogehalt der Geschäftsaktivitäten für den nationalen Finanzsektor als auch hinsichtlich seiner Bedeutung innerhalb der Gruppe als nicht wesentlich einzustufen ist (AT 9 Tz. 5 MaRisk). Eine vollständige Auslagerung der Compliance-Funktion oder der Internen Revision ist ferner bei kleinen Instituten möglich, sofern deren Einrichtung vor dem Hintergrund der Institutsgröße sowie der Art, des Umfangs, der Komplexität und des Risikogehalts der betriebenen Geschäftsaktivitäten nicht angemessen erscheint (AT 9 Tz. 5 Satz 4 MaRisk). Die Auslagerung einzelner Tätigkeiten und Prozesse ist demgegenüber möglich. Bei wesentlichen Auslagerungen ist die Kontinuität und Qualität der ausgelagerten Aktivitäten und Prozesse besonders zu gewährleisten (AT 9 Tz. 6–11 MaRisk). Dies geschieht im Wesentlichen durch die Einrichtung und den Unterhalt eines zentralen Auslagerungsmanagements (AT 9 Tz. 12 MaRisk).

Mangels Normcharakters der MaRisk können diese keine Sanktionen bei Verstößen vorschreiben. Allerdings liegt in einem Verstoß gegen die MaRisk gleichzei-

160 Abrufbar unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2021/fa_bj_2108_BAIT.html (zuletzt abgerufen am 12.5.2024).

161 *Beucher/Ehlen/Utzerath*, in: Kipker, Cybersecurity, Kap. 14 Rn. 190, 192.

162 Mittlerweile ebenfalls ISO 27001 zertifiziert; <https://www.siz.de/de/themenfelder/informationssicherheit/sicherer-it-betrieb-iso-27001.html> (zuletzt abgerufen am 15.4.2024).

tig ein Verstoß gegen die Rechts- bzw. Gesetzesnormen, die die MaRisk (BA) interpretieren (i. d. R. §§ 1, 25a KWG). Zudem ist eine wiederholte, nachhaltige und schuldhaft Missachtung von in den MaRisk niedergelegten Verhaltensanweisungen als Indiz für eine nicht ordnungsgemäße Geschäftsorganisation und Geschäftsführung und unter Umständen auch für die Unzuverlässigkeit der Mitglieder ihres Leitungsorgans bzw. des Verwaltungs- oder Aufsichtsorgans oder für deren fehlende Sachkunde, i. S. d. § 32 Abs. 1 Satz 3 Nr. 8 KWG, zu werten. Dementsprechend kann ein andauernder oder wiederholter Verstoß gegen Inhalte der MaRisk (BA) die Sanktionen des KWG (Versagen oder Aufheben der Erlaubnis; Abberufung der Geschäftsleitung) zur Folge haben.¹⁶³

bb) ZAG¹⁶⁴

- 74 Zusätzlich zu der Einrichtung einer entsprechenden Geschäftsorganisation haben die Finanzinstitute auch die Sicherheit von Internetzahlungen zu gewährleisten. Hierzu hatte die BaFin im Mai 2015 mit dem inzwischen aufgehobenen Rundschreiben 4/2015 bestimmte Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI) aufgestellt. Der Abschnitt „Starke Kundenauthentifizierung“ ist nunmehr in § 55 ZAG geregelt.¹⁶⁵ Die Delegierten-Verordnung (EU) 2018/389¹⁶⁶ (DelVO) konkretisiert (u. a.) die §§ 48 ff. ZAG, indem sie eine Reihe der von der Europäischen Bankaufsichtsbehörde (European Banking Authority, EBA) erarbeiteten RTS für verbindlich erklärt.¹⁶⁷ Die EBA hat Anfang 2018 Leitlinien zu Sicherheitsmaßnahmen bezüglich der operationellen und sicherheitsrelevanten Risiken von Zahlungsdiensten gemäß der PSD II herausgegeben.¹⁶⁸ Zur Erstellung bzw. Anpassung von Leitlinien durch die BaFin an das seit 2018 bzw. 2019 geltende Zahlungsdiensterecht, die DelVO und die neuen EBA-Leitlinien gibt es mittlerweile das Rundschreiben 11/2021 (BA) zu den „Zahlungsdienstaufsichtlichen Anforderungen an die IT“ (ZAIT) vom 16.8.2021.¹⁶⁹

163 Krimphove, BKR 2018, 1, 5.

164 Vgl. Kociok, in: Auer-Reinsdorff/Conrad, HdB IT- und Datenschutzrecht, zu den Missbrauchsszenarien beim Online-Banking § 27 Rn. 13 ff., zu den Missbrauchsszenarien bei Kreditkartenzahlungen im Internet § 27 Rn. 45 ff.

165 Jungmann, in: MünchKomm-BGB, 8. Aufl. 2020, § 675m Rn. 22.

166 Delegierten-Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation.

167 Vgl. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv:OJ.L_.2018.069.01.00.23.01.DEU (zuletzt abgerufen am 12.5.2024).

168 Vgl. https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2081899/6724cc1a-6e5b-427a-8503-3f7e23552acc/Guidelines%20on%20the%20security%20measures%20under%20PSD2%20%28EBA-GL-2017-17%29_DE.pdf?retry=1 (EBA-GL-2017-17)_DE.pdf (zuletzt abgerufen am 12.5.2024); Steinhoff, in: Casper/Terlau, ZAG, § 53 Rn. 12 ff.

169 Abrufbar unter https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1121_BA_ZAIT.pdf?jsessionid=267FF5FBD9729E2E3B605DFDB9C31C6B.internet992?__blob=publicationFile&v=2 (zuletzt abgerufen am 12.5.2024).

Dort finden sich nunmehr Regelungen zum Management von IT-Ressourcen, Informationsrisikomanagement, Informationssicherheitsmanagement und die Konkretisierung von Anforderungen nach § 53 Abs. 1 ZAG.¹⁷⁰

Inhaltlich ist insbesondere die Verpflichtung zur „Starken Kundenauthentifizierung“ (vgl. → Rn. 64 sowie Rn. 79) jetzt in § 55 Abs. 1, § 1 Abs. 24 ZAG geregelt. Verstöße gegen § 55 ZAG werden von § 64 ZAG nicht sanktioniert. Sie stellen aber Organisationspflichtverletzungen dar (§ 27 Abs. 1 Satz 1 ZAG), gegen die die BaFin einschreiten kann. Zivilrechtlich kommt es außerdem zu einer Haftungsverschärfung im Schadensfall (§ 675 v Abs. 4 BGB).¹⁷¹ **75**

Weiterhin setzt jetzt § 53 ZAG den Art. 95 PSD II um, der eine Pflicht zum Aufbau und zur Umsetzung einer Governance-Struktur aufstellt. Zahlungsdienstleister müssen angemessene Risikominderungsmaßnahmen und Kontrollmechanismen für die Beherrschung von operativen und sicherheitsrelevanten Risiken umsetzen. Angelehnt ist die Regelung damit im Ergebnis an die schon für die Banken bestehenden Regelungen des § 25a KWG und den dort festgelegten Anforderungen für eine ordnungsgemäße Geschäftsorganisation.¹⁷² Dadurch werden die Anforderungen für Zahlungsdienstleister an ihre Geschäftsorganisation nunmehr angehoben auf das Niveau von Banken, womit der Abstand zu den regulatorischen Anforderungen an Banken weiter verringert wird.¹⁷³ **76**

§ 53 Abs. 2 ZAG verpflichtet Zahlungsdienstleister, die Bewertung der operativen und sicherheitsrelevanten Risiken einmal jährlich an die BaFin zu übermitteln. Der Bericht muss eine Darstellung der ergriffenen Risikominderungsmaßnahmen und Kontrollmechanismen enthalten.¹⁷⁴ **77**

Inhaltlich werden die Pflichten des § 53 ZAG (insb. nach Aufhebung der MaSI) durch die ZAIT und EBA-Leitlinien ergänzt bzw. ausgefüllt (siehe → Rn. 74). Danach sollen die Institute formelle Sicherheitsrichtlinien aufstellen, umsetzen und regelmäßig überprüfen, um die Risiken zu kontrollieren und zu mindern. Hierzu gehört auch die Implementierung eines „gestaffelten Sicherheitskonzepts“. Ein solches Konzept beinhaltet insbesondere das „Prinzip des geringsten Zugriffsrechts“, die Befreiung der Server, die die sensiblen Funktionen hosten, von überflüssigen Daten und Funktionen, die Verwendung von Sicherheitszertifikaten, generelle Datenverringerung und die Rückverfolgbarkeit von Transaktionen und Einzugsermächtigungen. **78**

Im Hinblick auf die Authentifizierung der Kunden verlangt § 55 ZAG eine sog. starke Kundenauthentifizierung, also ein Verfahren, das auf mindestens zwei der folgenden Elemente basiert: (a) Wissen (z. B. Passwort, Code), (b) Besitz (z. B. **79**

170 Vgl. *Steinhoff*, in: Casper/Terlau, ZAG, § 53 Rn. 3 f.; BaFin, Rundschreiben 11/2021 (BA) vom 16.8.2021, ZAIT.

171 *Zahrte*, BKR 2019, 484, 486.

172 *Steinhoff*, in: Casper/Terlau, ZAG, § 53 Rn. 1.

173 *Steinhoff*, in: Casper/Terlau, ZAG, § 53 Rn. 2.

174 *Steinhoff*, in: Casper/Terlau, ZAG, § 53 Rn. 82.

Token, Smartcard, Mobiltelefon) und (c) Eigenschaft des Nutzers (z. B. biometrische Daten wie Fingerabdruck oder Stimme). Drei Anwendungsfälle werden in § 55 ZAG hierfür geregelt: 1. der Online-Zugriff auf das Zahlungskonto durch den Kunden oder Zahlungsdienstnutzer; 2. Auslösung eines elektronischen Zahlungsvorgangs, und zwar auch an einem Point of Sale (POS), und 3. bei kritischen Handlungen über einen Fernzugang, also solchen, bei denen Betrugs- oder Missbrauchsverdacht besteht.¹⁷⁵

cc) § 27 Abs. 1 ZAG

- 80** Inhaltlich ähnlich dem § 25a KWG legt § 27 Abs. 1 ZAG für E-Geldinstitute und Zahlungsinstitute fest, dass diese über eine ordnungsgemäße Geschäftsorganisation verfügen müssen. Die MaRisk werden hier entsprechend angewandt.

dd) DORA

- 81** Am 17.1.2025 wird die europaweit erste einheitliche Regulierung der Themen Cybersicherheit, IKT-Risiken und digitale operationale Resilienz im Finanzsektor in Kraft treten: die EU-Verordnung 2022/2554 über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act, DORA).¹⁷⁶ DORA sieht einen umfassenden IT-Risikomanagement-Rahmen, Tests der IT-Systeme, ein Drittparteienrisikomanagement zur Absicherung bei der Einbindung von Vertragspartnern sowie Vorgaben an das Business Continuity Management vor.¹⁷⁷ Ergänzt wird damit das durch die BAIT und MaRisk konkretisierte KWG und das BSiG mit seinen Anforderungen an Kritische Infrastrukturen im Finanzsektor.¹⁷⁸ Die BAIT-Novelle 2021 hatte bereits viele Elemente des DORA aufgegriffen, als sie neue Anforderungen im Bereich des Informationssicherheitsmanagements auf Basis der „EBA Guidelines on ICT and Security Risk Management“ von 2019 eingeführt hat.¹⁷⁹ Da die BaFin einzelne Instrumente zur Erhöhung der IKT-Sicherheit des deutschen Finanzsektors bereits geschaffen hat (harmonisierte Anforderungen an das IKT-Risikomanagement für die einzelnen Finanzsektoren (BAIT, ZAIT, VAIT, KAIT), vereinheitlichte Auslagerungsanzeigen, Überwachungsrahmen für IT-Mehrmandantendienstleister und vereinheitlichte Strukturen für das Meldewesen von IKT-bezogenen Vorfällen), ist der deutsche Finanzsektor und die Aufsicht laut BaFin grundsätzlich in einer guten

¹⁷⁵ Insgesamt zu § 55 ZAG vgl. *Brechfeld*, in: Luz/Neus/u. a., ZAG, § 55.

¹⁷⁶ Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011, ABl. L 333/1, 27.12.2022.

¹⁷⁷ *Dittrich/Heinelt*, RD 2023, 164, 164.

¹⁷⁸ *Dittrich/Heinelt*, RD 2023, 164, 165.

¹⁷⁹ *Dittrich/Heinelt*, RD 2023, 164, 165.

Startposition für die Anwendung von DORA ab 2025.¹⁸⁰ Am 17.1.2024 veröffentlichten die drei ESAs (EBA, EIOPA und ESMA) die ersten finalen Entwürfe der technischen Regulierungs- (RTS) und Implementierungsstandards (ITS) zu DORA.¹⁸¹ Im Hinblick auf IT-sicherheitsrechtliche Vorschriften wird das Verhältnis und die Konkurrenz zwischen DORA, PSD II und NIS-2-Richtlinie bzw. den diese implementierenden BSIG-Vorschriften zu bewerten sein.¹⁸²

ee) Konkurrenz zum BSIG

Viele Kreditinstitute und Zahlungsdienstleister werden auch kritische Infrastrukturen i. S. d. § 8a BSIG betreiben und damit den dort neu kodifizierten Pflichten unterliegen. Das wirft die Frage nach einer Konkurrenz der unter Umständen unterschiedlichen Regelungen auf. Hierzu bestimmt § 8d Abs. 2 Nr. 5 BSIG, dass jedenfalls die Pflichten nach § 8a BSIG (also die Verpflichtung zu angemessenen technisch-organisatorischen Maßnahmen) dann für KRITIS-Betreiber nicht gelten, wenn sie aufgrund von (anderen) Rechtsvorschriften vergleichbare oder strengere Anforderungen erfüllen müssen. Zwar enthalten die §§ 25a KWG und 27 Abs. 1 ZAG keine spezifischen Regeln zur IT-Sicherheit, und handelt es sich bei den MaRisk und den ZAIT nicht um „Rechtsvorschriften“. Jedoch finden sich nun in §§ 53, 54 ZAG Verpflichtungen zu angemessenen technisch-organisatorischen Maßnahmen, die insoweit § 8a BSIG vorgehen. **82**

g) EnWG

§ 11 Abs. 1a EnWG wurde ebenfalls durch das IT-Sicherheitsgesetz überarbeitet und um die Absätze 1b und 1c ergänzt. Nach § 8d Abs. 2 Nr. 2 BSIG sind die Vorschriften des BSIG nicht auf Betreiber von Energieversorgungsnetzen oder Energieanlagen i. S. d. EnWG anwendbar. Stattdessen gelten hier die Sicherheitskataloge nach § 11 Abs. 1a und 1b EnWG,¹⁸³ die direkt von der Bundesnetzagentur gemeinsam mit dem BSI aufgestellt werden. Zur Verpflichtung der Netzbetreiber zum Betrieb eines sicheren Energieversorgungsnetzes gehört nach Einführung des § 11 Abs. 1a EnWG im Jahr 2011 auch der angemessene Schutz der Telekommunikations- und elektronischen Datenverarbeitungssysteme, die der Netzsteuerung dienen. Sofern der Netzbetreiber die Anforderungen des nach § 11 Abs. 1a EnWG erstellten Sicherheitskataloges erfüllt, wird ein angemessener Schutz angenommen. Dasselbe gilt nach § 11 Abs. 1b EnWG für die Betreiber von solchen Energieanlagen, die eine Kritische Infrastruktur nach dem BSIG darstellen, und die die Anforderungen des nach § 11 Abs. 1b EnWG erstellten Sicherheitskatalogs der Bundesnetzagentur erfüllen. Sofern jedoch auf Tele- **83**

180 BaFin – DORA, https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html (zuletzt aufgerufen 26.2.2024).

181 BaFin – DORA, https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html (zuletzt aufgerufen 26.2.2024).

182 *Beucher/Ehlen/Utzerath*, in: Kipker, Cybersecurity, Kap. 14 Rn. 202.

183 Vgl. Fundstellen in Fn. 58 und 59 sowie zum Katalog von 2015 ausführlich *Weise/Brühl*, CR 2015, 290 ff. und *Giebichenstein/Schirp*, CB 2015, 66, 68.

kommunikations- oder Datenverarbeitungssysteme von Anlagen nach § 7 Abs. 1 AtomG Vorgaben des AtomG anwendbar sind, haben diese Vorrang, wie § 11 Abs. 1b Satz 3 EnWG klarstellt. Nachrangig ist jedoch dennoch der entsprechende Sicherheitskatalog anwendbar, der für diese Anlagen ebenfalls ausdrücklich Regelungen vorsieht.

h) NIS-Richtlinien

- 84** Die Richtlinie zur Verbesserung der Netz- und Informationssicherheit (NIS-Richtlinie) in der Europäischen Union¹⁸⁴ führt Mindestvorgaben für die Cybersicherheit in Europa ein. Sie ist am 8.8.2016 in Kraft getreten und in Deutschland durch das Gesetz zur Umsetzung der NIS-Richtlinie umgesetzt worden. Angesichts des zuvor bereits in Kraft getretenen IT-Sicherheitsgesetzes war der Umsetzungsbedarf in Deutschland allerdings gering.
- 85** Ziel der Richtlinie ist insbesondere die Etablierung eines Mindestsicherheitsniveaus für digitale Technologien, Netze und Dienste in allen Mitgliedstaaten. Ein solches einheitliches Sicherheitsniveau ist schon aufgrund der Entwicklung des Binnenmarkts der EU, der vor Netz- und Informationssystemen nicht Halt macht, erforderlich. Die Mitgliedstaaten sollen daher zukünftig sowohl die strategische als auch operationelle Kooperation verstärken. Wie das IT-Sicherheitsgesetz auch, verfolgt die NIS-Richtlinie maßgeblich den Zweck, das Sammeln, „Poolen“ und den Austausch von Informationen und Wissen im Zusammenhang mit IT-Sicherheit zu verstärken. Auf europäischer Ebene ist die ENISA hierfür die zentrale Behörde und „Drehkreuz“ und es leuchtet unmittelbar ein, dass eine Ausweitung des Pools auf die gesamte EU für die verfolgten Zwecke nur förderlich sein kann.
- 86** Als Reaktion auf den durch die COVID-19-Krise verstärkten digitalen Wandel der Gesellschaft und die dadurch erfolgte Erweiterung der Bedrohungslandschaft kam es am 16.1.2023 zum Inkrafttreten der EU-Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie),¹⁸⁵ um den neuen Herausforderungen gerecht zu werden.¹⁸⁶ Neu ist insbesondere die Erweiterung der Sektoren und die Unterscheidung zwischen wesentlichen und wichtigen Einrichtungen (vgl. Art. 3 NIS-2-Richtlinie) anhand des Grades der Kritikalität der Einrichtungen in Bezug auf ihren Sektor, die Art der von ihnen erbrachten Dienste sowie ihrer Größe anstatt der bisherigen Unter-

184 Richtlinie (EU) 2016/1148 vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194/1 v. 19.7.2016.

185 Richtlinie (EU) 2022/2555 vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. L 333/80, 27.12.2022.

186 Europäische Kommission, NIS2-Richtlinie, <https://digital-strategy.ec.europa.eu/de/node/10361/printable/pdf> (zuletzt abgerufen am 22.2.2024).

scheidung zwischen Betreibern Kritischer Infrastrukturen und Anbietern digitaler Dienste.¹⁸⁷ Zur Umsetzung der NIS-2-Richtlinie ins deutsche Recht wurde zuletzt im Mai 2024 vom Bundesministerium des Innern und für Heimat ein Referentenentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) vorgelegt.¹⁸⁸

i) §§ 76, 91, 93 AktG

Eine ganz andere Zielrichtung verfolgen die Pflichten des Vorstands bzw. der GmbH-Geschäftsführung nach den §§ 91, 93 AktG (i.V.m. § 76 AktG und § 43 GmbHG). Diese Pflichten stellen nicht wie die vorgenannten Pflichten öffentlich-rechtliche Verpflichtungen dar, sondern solche gegenüber der Gesellschaft selbst, deren Verletzung zu Schadensersatzverpflichtungen führt. Aus den Legalitätspflichten und der Pflicht zur Legalitätskontrolle der Geschäftsleitung folgen konkrete Organisations- und Überwachungspflichten für die Unternehmensführung, deren wesentliches Element die Einrichtung eines auf Schadensprävention und Risikokontrolle angelegten effizienten Compliance-Systems ist, um Rechtsverstöße zu verhindern.¹⁸⁹ Dabei sind Art, Größe und Organisation des Unternehmens, sowie die geografische Präsenz und das Aufkommen etwaiger Verdachtsfälle in der Vergangenheit mit zu berücksichtigen.¹⁹⁰ Die gesetzlichen Regelungen stellen zwar keine konkreten IT-bezogenen Pflichten auf, Äsndern beinhalten allgemeine Regeln zur Implementierung von Risikomanagementsystemen. Wegen der hohen Bedeutung der IT-Infrastruktur für Unternehmen einerseits und dessen hoher Sicherheitsanfälligkeit andererseits gehören hierzu auch IT-Risikomanagementsysteme.¹⁹¹ Teil der Schadensprävention für das Unternehmen ist es auch, dass der Vorstand so weit wie möglich dafür Sorge trägt, dass Dritte keine Rechtsverletzung gegenüber dem Unternehmen und dessen Kunden vornehmen können.¹⁹²

So haftet die Geschäftsleitung etwa gegenüber der Gesellschaft gemäß den § 43 GmbHG, § 93 AktG, wenn das Unternehmen aufgrund der Verletzung von gesetzlichen Verpflichtungen einen Schaden erleidet und der Geschäftsführer da-

87

88

187 Wegmann, BB 2023, 835, 838; Beucher/Ehlen/Utzerath, in: Kipker, Cybersecurity, Kap. 14 Rn. 12.

188 2. Referentenentwurf, Bearbeitungsstand: 3.7.2023, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-RefE.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 12.5.2024); vgl. zum 1. Referentenentwurf Kipker/Dittrich, MMR 2023, 481 ff.

189 Schulz, BB 2019, 579 ff.; Spindler, CR 2017, 715, 721; Behling, ZIP 2017, 697, 698. Siehe zur Compliance-Organisationspflicht → Schulz, Kap. 1 Rn. 27 ff.

190 LG München I, NZG 2014, 345, 346 f. (Siemens/Neubürger), das zwar keine IT- oder Sicherheits-Compliance-Pflichten betrifft, dessen Maßstäbe aber hierauf durchaus übertragbar sind (so auch Löschhorn/Fuhrmann, NZG 2019, 161, 163).

191 Rath/Kuß, in: Umnuß, Corporate Compliance-Checklisten, Kap. 10 IT-Compliance: Anforderungen an die Informationstechnologie und den Datenschutz Rn. 7; Spindler, CR 2017, 715, 723.

192 Löschhorn/Fuhrmann, NZG 2019, 161, 163, 166.

bei seine Pflichten verletzt hat.¹⁹³ Damit zählen auch Geldbußen von Aufsichtsbehörden gegen das Unternehmen grundsätzlich zum ersatzfähigen Schaden im Rahmen der Vorstandshaftung.¹⁹⁴ Dies hat insbesondere durch den massiv ausgeweiteten Bußgeldrahmen der DSGVO gegenüber dem BDSG besondere Bedeutung gewonnen.¹⁹⁵ Dies bedeutet jedoch zugleich, dass der Vorstand bzw. die Geschäftsführung sich bei einem wirksamen und fortlaufend aktualisierten Compliance-Management-System im Falle von Verstößen, insbesondere durch untergeordnete Mitarbeiter, vom Vorwurf des Organisationsverschuldens bzw. der Verletzung der Aufsichtspflicht, entlasten kann.¹⁹⁶

- 89** Sowohl die NIS-2-Richtlinie (Art. 20) als auch der DORA (speziell für den Finanzsektor, Art. 4) enthalten neuerdings spezifische Regeln über die Pflichten der Geschäftsleitung. In Umsetzung von Art. 20 NIS-2-Richtlinie schlägt das NIS2UmsuCG deshalb einen neuen § 38 BSIG-E vor, der dezidierte Pflichten für die Geschäftsleitung besonders wichtiger und wichtiger Einrichtungen regelt. Zur Geschäftsleitung i. S.d § 2 Abs. 1 Nr. 11 BSIG-E zählen diejenigen natürlichen Personen, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer Einrichtung berufen sind. Dies umfasst u. a. den Vorstand einer AG, Geschäftsführer der GmbH, Vorstände oder besondere Vertreter eines Vereins sowie die Leitungspersonen in öffentlichen Einrichtungen, etwa die Behördenleitung. Die Pflichten nach § 38 BSIG-E umfassen Billigungs-, Überwachungs- und Schulungspflichten der Geschäftsleitung. Zudem soll ein Verzicht der Einrichtung auf Ersatzansprüche aufgrund einer Verletzung der Pflichten unwirksam sein.

aa) Ausgestaltung des IT-Risikomanagementsystems

- 90** Nach der in § 93 Abs. 1 Satz 2 AktG kodifizierten sog. „Business Judgement Rule“,¹⁹⁷ die auch auf IT-relevante Fragen Anwendung findet,¹⁹⁸ steht die konkrete Ausgestaltung eines einzurichtenden IT-Risikomanagementsystems grundsätzlich im unternehmerischen Ermessen der Geschäftsführung.¹⁹⁹ Eine unternehmerische Entscheidung, die den Anforderungen der Business Judgement Rule gerecht wird, liegt vor, wenn der Vorstand eine an den Risiken ausgerichtete, zukunftsorientierte Entscheidung trifft. Dabei darf grundsätzlich eine Kosten-/Nutzen-Abwägung vorgenommen werden.²⁰⁰ Dafür muss sich die Un-

¹⁹³ Löschhorn/Fuhrmann, NZG 2019, 161, 169.

¹⁹⁴ Daghles, DB 2018, 2289, 2291.

¹⁹⁵ Löschhorn/Fuhrmann, NZG 2019, 161, 162; Spindler, CR 2017, 715, 721; vgl. auch Behling, ZIP 2017, 697, 697 f.

¹⁹⁶ Löschhorn/Fuhrmann, NZG 2019, 161, 168. Zu den Anforderungen und Vorteilen eines wirksamen Compliance-Management-Systems → Schulz, Kap. 1.

¹⁹⁷ Entsprechendes gilt für § 43 GmbHG (vgl. Spindler, CR 2017, 715, 717) und über § 34 VAG auch für den Vorstand von Versicherungsvereinen auf Gegenseitigkeit.

¹⁹⁸ Spindler, CR 2017, 715, 717.

¹⁹⁹ So auch von Holleben/Menz, CR 2010, 63, 67; Rodewald/Unger, BB 2006, 113, 115.

²⁰⁰ Daghles, DB 2018, 2289, 2290.

ternehmensführung zunächst eine hinreichende Informationsbasis verschaffen. Sie muss sich unter Ausschöpfung aller ihr zur Verfügung stehenden Erkenntnisquellen über den Ist-Zustand und die Risiken informieren und auf dieser Grundlage eine individuelle Risikoanalyse²⁰¹ sowie eine Prognose erstellen lassen.²⁰² Der Umfang der benötigten Informationsbasis und Risikoanalyse zur Bestimmung der erforderlichen Maßnahmen richtet sich nach der Größe des Unternehmens, der anfallenden Datenmenge und der Bedeutung der IT für das Unternehmen. Die gegenüber früher wesentlich erweiterten Möglichkeiten zur Aggregation und Strukturierung von großen Datenmengen (Stichwort Big Data) erhöhen die Anforderungen an die Informationssammlung.²⁰³ Je nach Komplexität und Größe des Unternehmens kann die Hinzuziehung von externem Rechtsbeistand sowie von externen (IT-)Experten nötig sein.²⁰⁴ Es liegt keine Pflichtverletzung eines Vorstandsmitglieds vor, wenn das Vorstandsmitglied bei einer unternehmerischen Entscheidung vernünftigerweise davon ausgehen durfte, auf der Grundlage angemessener Informationen zum Wohle der Gesellschaft zu handeln. Diese Safe Harbor Regelung findet auch im Bereich von IT-Managemententscheidungen Anwendung. Allerdings sind Vorstand/Geschäftsführung verpflichtet, im Rahmen ihrer Entscheidungen stets Recht und Gesetz einzuhalten. Auch nach der Business Judgement Rule kann eine Kosten-Nutzen-Analyse nicht rechtfertigen, bewusst Rechtsverletzungen in Kauf zu nehmen.²⁰⁵ Bei KRITIS-Betreibern bzw. anderen, durch spezialgesetzliche Vorschriften zu besonderen Sicherheitsmaßstäben verpflichteten Unternehmen (wie etwa Kredit- und Finanzdienstleistungsunternehmen) ist das Ermessen daher durch die gesetzlichen Vorgaben konkretisiert und eingeschränkt.²⁰⁶ Jenseits dieser Grenze muss es aber zulässig sein, betriebswirtschaftliche Aspekte bei der Abwägung zu berücksichtigen.²⁰⁷

Wo konkrete Pflichten fehlen, können z. B. das IT-Grundschutz Compendium²⁰⁸ sowie betriebswirtschaftliche Management- oder Organisationsmodelle (insb. Normungen des Managementsystems, wie die ISO 27001 ff. für den IT-Bereich) zur Konkretisierung des Pflichtenprogramms herangezogen werden.²⁰⁹ Allerdings führt die Einhaltung dieser Vorgaben nicht automatisch dazu, dass die durch § 93 Abs. 1 AktG bzw. § 43 GmbHG geforderte Sorgfalt nachgewiesen

91

201 *Schmitz/v. Dall'Armi* veranschaulichen, wie eine solche Risikoanalyse aussehen könnte (in Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil XII, Kap. 1. Anforderungen an die IT-Sicherheit und deren rechtliche Grundlage, Rn. 35).

202 *Spindler*, in: MünchKomm-AktG, § 91 Rn. 20; *Krieger/Sailer*, in: Schmidt/Lutter, AktG, § 91 Rn. 8; *Müller-Michaels*, in: Hölters, AktG, § 91 Rn. 6.

203 *Spindler*, CR 2017, 715, 717.

204 *Spindler*, CR 2017, 715, 719.

205 *Schulz*, BB 2019, 579, 581; *Daghles*, DB 2018, 2289, 2290; *Spindler*, CR 2017, 715, 717 f.

206 Vgl. dazu *Daghles*, DB 2018, 2289, 2292 f.

207 *Nietsch/Hastenrath*, CB 2015, 221, 223.

208 *Spindler*, CR 2017, 715, 723.

209 *Spindler*, CR 2017, 715, 716.

werden kann. Die Organisation der IT-Sicherheit ist vielmehr höchst individuell, sodass stets eine Prüfung des Einzelfalls erforderlich ist.²¹⁰ Außerdem handelt es sich nicht um rechtliche Vorgaben. Der Vorstand bzw. die Geschäftsführung ist daher nicht verpflichtet, ein bestimmtes betriebswirtschaftliches Managementsystem bzw. -modell oder Normung zu nutzen, solange eine vertretbare, sachlich begründete Wahl getroffen wird. Allerdings muss der Vorstand/die Geschäftsführung sich nichtsdestotrotz mit den einschlägigen Normungen vertraut machen und erläutern weshalb einer Normung gefolgt bzw. nicht gefolgt wird. Anderenfalls laufen sie Gefahr, mangels hinreichender Informationsbasis der Business Judgement Rule nicht gerecht zu werden.²¹¹

- 92** Der Vorstand bzw. die Geschäftsführung müssen über Berichtspflichten ihre fortlaufende Information sicherstellen.²¹² Dafür ist zu empfehlen, Kontroll- und Berichtsstrukturen zu schaffen, um das Reporting an die fachliche Leitung und den Vorstand zu erleichtern.²¹³ So informiert, hat der Vorstand dann die angemessenen organisatorischen und technischen Maßnahmen zu ergreifen und kontinuierlich an den Stand der Technik anzupassen, um eine Verwirklichung der identifizierten Risiken zu verhindern.²¹⁴ Dies umfasst regelmäßige Überprüfungen, bspw. in Form von Audits,²¹⁵ sowie die Erstellung eines Notfallkonzepts (für Kredit- und Zahlungsdienstleister schon nach der MaRisk bzw. § 53 ZAG erforderlich, → Rn. 71). Die Geschäftsleitung von KRITIS-Betreibern muss hier nun auch Informationen berücksichtigen, die das BSI über Sicherheitsvorfälle bei anderen Unternehmen nach § 8b Abs. 2 Nr. 4 BSIG mitgeteilt hat. Je nach Risikoprofil und Angebot kann auch der Abschluss einer Cyberversicherung zu den angemessenen Maßnahmen zählen.²¹⁶ Diese gleicht im Schadensfall nicht nur den finanziellen Schaden aus, sondern kann auch für u.U. notwendigen Rechtsschutz aufkommen und Experten und Dienstleister, insbesondere einen Krisenmanager, vermitteln, um die geschäftliche Tätigkeit zügig wieder aufnehmen zu können.²¹⁷ Bei Hinweisen auf rechtswidrige Handlungen muss eine umfassende Untersuchung der Rechtsverstöße stattfinden (Internal Investigation).²¹⁸ Wichtig ist außerdem: Auch nach Einrichtung eines solchen Risikomanagementsystems muss die Geschäftsleitung das System kontinuierlich an den jeweils aktuellen Stand der Technik anpassen und überwachen, bei-

210 *Spindler*, CR 2017, 715, 723.

211 *Spindler*, CR 2017, 715, 716.

212 LG München I, BB 2007, 2170; *Schulz*, BB 2019, 579, 583; *Krieger/Sailer*, in: Schmidt/Lutter, AktG, § 91 Rn. 8, 13.

213 *Daghles*, DB 2018, 2289, 2294.

214 *Von Holleben/Menz*, CR 2010, 63, 67.

215 *Daghles*, DB 2018, 2289, 2291.

216 *Vogel*, CB 2018, 197, 199; *Schneider/Forgó/Helfrich*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil XII. Kap. 4. Überblick zu Risikomanagement unter BSIG, BSI-KritisV, NIS-RL i.V.m. DS-GVO Rn. 23.

217 *Vogel*, CB 2018, 197, 199.

218 *Löschhorn/Fuhrmann*, NZG 2019, 161, 163.

spielsweise durch das Berichtswesen, Dokumentation oder den Erlass interner Richtlinien.²¹⁹ So schreiben es auch die bankaufsichtsrechtlichen Anforderungen an die IT (BAIT) der BaFin vor: Die von der Geschäftsleitung beschlossene Informationssicherheitsleitlinie muss regelmäßig überprüft und an geänderte Bedingungen angepasst werden. Dabei müssen Veränderungen der Aufbau- und Ablauforganisation sowie der IT-Systeme einer Institution (Geschäftsprozesse, Fachaufgaben, organisatorische Gliederung) und Veränderungen der äußeren Rahmenbedingungen (z. B. gesetzliche Regelungen, regulatorische Anforderungen), der Bedrohungsszenarien oder der Sicherheitstechnologien berücksichtigt werden (vgl. auch → Rn. 71).²²⁰

Die mit der NIS-2-Richtlinie neu aufgestellten Pflichten der Geschäftsführung besonders wichtiger und wichtiger Einrichtungen (vgl. → Rn. 89) beschreiben zum Teil spezifische Pflichten, dürften aber im Übrigen wenig zur Konkretisierung der die Geschäftsführung als Organ und als Einzelperson treffenden Pflichten beitragen. **93**

bb) Anforderungen nach DSGVO

Bei Datenschutzverstößen ist grundsätzlich zu unterscheiden zwischen Verstößen, die aus dem Unternehmen heraus begangen werden (sog. interne Datenschutzverstöße) und Verstößen, die von außen gegen das Unternehmen verübt werden (z. B. Hackerangriffe). Beide Fälle sind echte Compliance-Verstöße.²²¹ **94**

Zur Vorbeugung von internen Datenschutzverstößen sind vor allem eine wirksame Kontrolle von Mitarbeitern auf eine Sicherheitsarchitektur, die den „internen Datenklau“ unmöglich macht, und eine zügige und umfassende Aufklärung wichtig.²²² Die zentrale Norm, die den Pflichtenkatalog festschreibt, ist Art. 32 DSGVO (vgl. → Rn. 45 ff.). **95**

Auch von außen gegen das Unternehmen verübte Datenschutzverletzungen können als Compliance-Verstöße gewertet werden, wenn das Unternehmen nicht über eine dem Stand der Technik entsprechende Sicherheitsarchitektur verfügt. Denn der Pflichtenkatalog von Art. 32 DSGVO verlangt gerade eine solche sicherzustellen und ahndet Verstöße mit Bußgeldern nach Art. 83 Abs. 4 DSGVO.²²³ **96**

219 LG München I, BB 2007, 2170; *Schulz*, BB 2019, 579, 583; *Müller-Michaels*, in: Hölters, AktG, § 91 Rn.9. Für eine Checkliste zur Umsetzung eines angemessenen Cybersecurity Management Systems vgl. *Daghles*, DB 2018, 2289, 2294.

220 Rundschreiben BaFin 10/2017 (BA) BAIT S. 9 unter II. Anforderungen 4. Informationssicherheitsmanagement.

221 *Löschhorn/Fuhrmann*, NZG 2019, 161, 162.

222 *Löschhorn/Fuhrmann*, NZG 2019, 161, 163.

223 *Löschhorn/Fuhrmann*, NZG 2019, 161, 162 f.

cc) Verantwortungsverteilung innerhalb der Geschäftsleitung

- 97 Die IT-Sicherheit ist Aufgabe der Geschäftsleitung als Gesamtorgan. Daher trägt jedes Organmitglied unabhängig von der konkreten Ressortzuständigkeit eine Kontroll- und Überwachungsverantwortung. Jedes Organmitglied hat daher zur eigenen Haftungsvermeidung dafür Sorge zu tragen, dass das Unternehmen so organisiert und beaufsichtigt wird, dass keine Gesetzesverletzungen stattfinden.²²⁴ Eine vertikale Delegation kommt nur für Aufgaben in Betracht, die nicht in den Kernbereich der Leitungsverantwortung der Geschäftsleitung fallen.²²⁵ Übertragbar sind somit nur vorbereitende Aufgaben und Hilfstätigkeiten. Im Rahmen der Auswahlpflicht ist bei vertikaler Delegation vor allem auf Qualifikation und persönliche Eignung der beauftragten Personen zu achten. Zudem verlangt die Überwachungspflicht laufende als auch anlassbezogene Kontrollen. Damit einher gehen umfassende Dokumentationspflichten sowie ggf. Instruktionspflichten hinsichtlich Rechtspflichten und Risiken.²²⁶ Die konkreten Anforderungen bei der Überwachung sind eine Frage des Einzelfalles und hängen etwa ab von der Art und Größe des Unternehmens, der Bedeutung der IT-Systeme im Unternehmen und möglichen Risiken bei Fehlverhalten, sowie den persönlichen Merkmalen des zuständigen Geschäftsleitungsmitglieds (etwa Erfahrung und Fachkenntnis).²²⁷ In Krisensituationen bestehen intensivere Überwachungspflichten.²²⁸ Insbesondere ist auch im Hinblick auf solche IT-Sicherheitspflichten, die aus der DSGVO folgen, keine Delegation der Letztverantwortung (und Haftungsrisiken) auf den Datenschutzbeauftragten des Unternehmens möglich. Dem Datenschutzbeauftragten kommt lediglich eine Beratungsfunktion zu, die datenschutzrechtlichen Handlungspflichten und Haftungsrisiken verbleiben bei dem Unternehmen selbst. Daher kann auch nur die Geschäftsleitung letztverantwortlich entscheiden.²²⁹
- 98 Das bedeutet im Ergebnis, dass (1) die Kontroll- und Überwachungsverantwortung in jedem Fall beim Gesamtvorstand bleibt und nicht nur bei dem ressortzuständigen Organmitglied liegt. Daher muss sich jeder Geschäftsführer ressortunabhängig „auf der Basis der konkreten Besprechungsinhalte und mit gezielten Nachfragen ein eigenes Bild über den Geschäftsbereich“ machen.²³⁰ Außerdem (2) müssen auch Organmitglieder, die mit Spezialthemen – wie hier der IT-Si-

224 BGH, NJW 2019, 1067, Rn. 15; LG München I, NZG 2014, 345, 347 f.; *Conrad/Streitz*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, Rn. 75 f.; *Daghles*, DB 2018, 2289, 2291; *Behling*, ZIP 2017, 697, 699.

225 LG München I, NZG 2014, 345, 348; *Löschhorn/Fuhrmann*, NZG 2019, 161, 163; *Daghles*, DB 2018, 2289, 2291. Zu Delegationsfragen bei Compliance-Maßnahmen siehe auch → *Schulz*, Kap. 1 Rn. 56 f.

226 *Daghles*, DB 2018, 2289, 2291.

227 *Löschhorn/Fuhrmann*, NZG 2019, 161, 166.

228 *Conrad/Streitz*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, Rn. 75 f.; *Spindler*, CR 2017, 715, 721.

229 So auch *Behling*, ZIP 2017, 697, 699.

230 BGH, NJW 2019, 1067, Rn. 34.

cherheit – nicht vertraut sind, das gemäß Ressortverteilung zuständige Organmitglied fortlaufend überwachen und kontrollieren.²³¹

Aufgrund der Anwendbarkeit des sogenannten Prinzips des innerbetrieblichen Organisationsverschuldens kann sich der Vorstand bzw. die Geschäftsführung bei einem wirksamen und fortlaufend aktualisierten Compliance-Management-System im Falle von Verstößen durch untergeordnete Mitarbeiter (vertikale Delegation) gegen die Vorgaben dieses Systems vom Vorwurf des Organisationsverschuldens entlasten, wenn den Aufsichts- und Kontrollpflichten entsprochen wurde und die vertikale Delegation den Anforderungen an eine wirksame Compliance-Organisation entsprach.²³²

dd) Dokumentationspflicht

Insgesamt ist für die Geschäftsführung eine gründliche Dokumentation von essenzieller Bedeutung. Die Dokumentation selbst ist schon unmittelbar Teil der gesetzlichen Anforderungen an ein entsprechendes Risikomanagementsystem.²³³ Zum anderen ist die Dokumentation unverzichtbar, um im Ernstfall nachweisen zu können, dass die erforderlichen Schritte durchgeführt wurden – auch wenn sich Entscheidungen vielleicht im Nachhinein als falsch herausgestellt haben. Denn das in Anspruch genommene Organ muss sich im Hinblick auf sein Verschulden bei der Pflichtverletzung entlasten.²³⁴ Dabei können Nachweise über die Einhaltung der im Verkehr erforderlichen Sorgfalt bei der Installation und der Überwachung der Effizienz des Compliance-Systems helfen.²³⁵ Insbesondere der Nachweis der Einhaltung des BSI-Grundschatzes wirkt sich positiv aus, da dies jedenfalls in den meisten Fällen im Sinne des anzulegenden objektiven Sorgfaltsmaßstabs aufzeigt, dass der Stand der Technik hinsichtlich der ergriffenen Abwehrmaßnahmen gegen einen Cyberangriff eingehalten worden ist.²³⁶

3. Unternehmensinterne Vorkehrungen

a) Interne Vorgaben

Zur effektiven Gewährleistung einer IT-Sicherheit empfiehlt es sich für ein Unternehmen, mit internen Richtlinien, Protokollen und ähnlichen Vorgaben Mitar-

231 *Schmidt-Versteyl*, NJW 2019, 1637, 1640; *Daghles*, DB 2018, 2289, 2291.

232 *Schulz*, BB 2019, 579, 580, 582; *Conrad/Streitz*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, Rn. 75 f.; *Löschhorn/Fuhrmann*, NZG 2019, 161, 168.

233 LG München I, NZG 2008, 319, 320 m. w. N.

234 *Löschhorn/Fuhrmann*, NZG 2019, 161, 169 f.

235 LG München I, NZG 2014, 345, 348 für das AktG: Im Anwendungsbereich von § 92 Abs. 2 AktG und § 43 Abs. 2 GmbHG wirkt auch leichte Fahrlässigkeit haftungsbegründend, da diese Normen keine Einschränkung von § 276 BGB vorsehen.

236 *Schmidt-Versteyl*, NJW 2019, 1637, 1642.

beiter zu bestimmten Handlungsweisen zu verpflichten.²³⁷ Das wird in gewissem Umfang schon deshalb erforderlich sein, um sicherzustellen, dass ein IT-Sicherheitskonzept auch tatsächlich umgesetzt wird, schafft aber auch einen internen Rechtsrahmen, in dem Fehlverhalten der Mitarbeiter sanktioniert werden kann.

- 102** Auch empfiehlt es sich, schon vorbeugend eine gemeinsame Arbeitsgruppe bzw. einen Krisenstab aus Geschäftsführung, Kommunikations- oder Presseabteilung, Rechtsabteilung (mit Compliance und Datenschutz) und vor allem der IT-Abteilung einzurichten und auf Krisensituationen vorzubereiten, mögliche Szenarien durchzuspielen, Handlungsabläufe durchzuprobieren und Protokolle zu entwickeln. Ist das Ereignis einmal da, überschlagen sich die Ereignisse und es bleibt wenig Zeit zur Vorbereitung von Entscheidungen. Dann ist es nicht nur wichtig, ein solches Gremium schon benannt zu haben, sondern auch, dass dieses Gremium in der Zusammenarbeit bereits geübt und auf die sich stellenden Fragen und Situationen vorbereitet ist.

b) Aktuelle technisch-organisatorische Schutzmaßnahmen

- 103** Allein die Etablierung von Compliance-Mechanismen genügt jedoch nicht, um Angriffe auf das System abzuwehren,²³⁸ vielmehr ist dafür ein solide aufgestelltes IT-System notwendig.²³⁹ Unabhängig davon, ob Unternehmen eine eigene Sicherheitsabteilung eingerichtet oder einen externen Dienstleister mit dem Schutz ihrer Systeme betraut haben, schon jetzt dürften die vom BSI vorgeschlagenen Sicherheitsmaßnahmen zum Basisschutz²⁴⁰ oder äquivalente Maßnahmen

237 Auch hier gibt es Vorlagen des BSI, abrufbar z.B. unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium_Einzel_PDFs_2021/02_ORP_Organisation_und_Personal/ORP_3_Sensibilisierung_und_Schulung_Editon_2021.pdf?__blob=publicationFile&v=2 (ORP.3) oder https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium_Einzel_PDFs_2021/02_ORP_Organisation_und_Personal/ORP_2_Personal_Editon_2021.pdf?__blob=publicationFile&v=2 (ORP.3) (beides zuletzt abgerufen am 15.5.2024).

238 Für eine Illustration der verschiedenen Angriffswege vgl. Ahrend, CB 2019, 105, 106.

239 Ahrend, CB 2019, 105, 105.

240 IT-Grundschutz-Kompodium (1.2.2023) des BSI. Im Fokus des IT-Grundschutz-Kompodiums stehen die sog. IT-Grundschutz-Bausteine, die jeweils ein Thema zu allen relevanten Sicherheitsaspekten beleuchten. Vertiefende Informationen sind in den sog. Umsetzungshinweisen zu finden: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium/Umsetzungshinweise_Kompodium_CD_2019.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 15.5.2024). Für kleinere und mittlere Unternehmen ist der BSI Leitfaden zur Basis-Absicherung nach IT-Grundschutz 2017 relevant, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 15.5.2023). Außerdem hilfreich sind die BSI-Standards: BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS) (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.pdf?__blob=publicationFile&v=2); BSI-Standard 200-22: IT-Grundschutz-Methodik (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2); BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grund-

das Minimum der umzusetzenden Schutzmaßnahmen darstellen. Für die Geschäftsführung ist die Implementierung von und Zertifizierung nach ISO 27001-Standards in der Regel eine geeignete Möglichkeit, die Erfüllung ihrer Pflichten nachzuweisen. Da dies aber einigermaßen aufwändig ist, können für kleinere und mittelständische Unternehmen die VDS-Richtlinie 3472²⁴¹ und ISIS 12 zur IT-Sicherheit eher geeignet sein, die dem Stand der Technik entsprechenden IT-Sicherheitsmaßnahmen zu identifizieren und umzusetzen.²⁴² Schon durch einige sehr einfache Prinzipien, wie etwa Inventarisierung, Update/Patch Management, Sichere Konfiguration, Berechtigungsvergabe nach Minimalprinzip und Backups, können Unternehmen ihre IT-Sicherheit erheblich stärken.²⁴³ Weitere Maßnahmen sind in der Regel erforderlich, richten sich aber nach dem entsprechenden Schutzbedarf, der im Rahmen einer Risikoanalyse festgestellt wurde. Dazu gehören Auditing- und Überwachungstools zur Überwachung der Mitarbeiter, zur Verhinderung von „Insider Threats“ oder zur Kontrolle der Datenströme zur Vermeidung von „Data Leakage“, oder proaktive Tools zur Anomalieerkennung und „Intrusion Prevention“, die bei einem festgestellten Angriff die Systeme schützen. „Identity Protection“ sowie „Identity Theft Protection“ – und zwar nicht nur für leitende Mitarbeiter, sondern auf jeder Stufe – dürften mittlerweile auch zu den wichtigsten Standards gehören, schon um ein unbefugtes „Eindringen“ oder unbefugten Zugriff auf die IT des Unternehmens zu verhindern. Bei der Auswahl dieser Systeme sind auch die Besonderheiten des konkreten Geschäftsmodells zu berücksichtigen, da alle Maßnahmen der IT-Sicherheit auch einer Wirtschaftlichkeitsbetrachtung unterliegen. Ein Online-Shop braucht eine hohe Verfügbarkeit, eine Werkzeugmaschinenfabrik integrale Steuersysteme, die Personalabteilung oder Finanzbuchhaltung eine hohe Vertraulichkeit. Dies lässt sich nur durch eine professionelle Risikoanalyse feststellen.²⁴⁴

Neben den bisher bekannten Risiken kommt den sozialen Medien nicht nur in der Veränderung unseres Kommunikationsverhaltens eine zunehmend bedeutende Rolle zu. Facebook und Twitter, Bewertungsportale und andere Formen öffentlicher Meinungsäußerung prägen und verändern maßgeblich das Image einer Firma. Auch „Trolling“ oder ein sogenannter „Shitstorm“ bringt Medienpräsenz – allerdings negative und ungewollte. Hierfür gibt es Auswerte- und Analyse-

104

schutz (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2); BSI-Standard 200-4: Business Continuity Management System (BCMS) (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf?__blob=publicationFile&v=8) (jeweils zuletzt abgerufen am 15.5.2024).

241 Rath/Kuß, in: Umnuß, Corporate Compliance-Checklisten, Kap. 10 IT-Compliance: Anforderungen an die Informationstechnologie und den Datenschutz, Rn. 10.

242 Für einen Überblick über Regelwerke, die ein ISMS (Informations-Sicherheits-Management-System) definieren und bei der Implementierung unterstützen, siehe Schmitz/v. Dall’Armi, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil XII, Kap. 1. Anforderungen an die IT-Sicherheit und deren rechtliche Grundlage, Rn. 26–28.

243 Ahrend, CB 2019, 105, 108 f.

244 Vgl. Bensinger/Kozok, CB 2015, 376, 378.

Tools, welche die Firmen bei der (Früh-)Erkennung von „Social Media“-Angriffen unterstützen und den zuständigen Stellen eine angemessene Reaktion ermöglichen.

- 105** Hilfestellung für konkret erforderliche und verfügbare technische Sicherheitssysteme können (IT-)Berater leisten, die in der Regel den besten Marktüberblick haben. Wichtig bei der Aufstellung solcher Konzepte ist (a) die konsequente Umsetzung, (b) die regelmäßige Aktualisierung und (c) der Abgleich mit dem jeweils geltenden Stand rechtlicher Verpflichtungen.

III. Der Krisenfall

- 106** Haben Schutzmaßnahmen versagt und kommt es zum Krisenfall, so sind sowohl rechtlich wie technisch/organisatorisch andere Maßnahmen gefragt. Vor allem müssen schnell Entscheidungen getroffen und erforderliche Schritte eingeleitet werden. Jetzt zählt es sich aus, wenn diese Maßnahmen, oder ein Teil davon, bereits unter Beteiligung aller einschlägigen Fachbereiche vorbereitet, angelegt und möglichst auch probeweise durchgespielt wurden.

1. Hacker-Angriffe erkennen

- 107** Bei der Erkennung von Hacker-Angriffen beschränken sich viele Betroffene noch auf die Prüfung, wie der oder die Täter in das System eingedrungen sind, welche Systeme betroffen sind und welchen Schaden der Angriff angerichtet hat. Die immer besser werdenden Angriffswerkzeuge machen es jedoch notwendig, sich intensiv mit der Frage nach dem Angriffsverfahren zu beschäftigen und zum Beispiel auch zu analysieren, welche Werkzeuge der Angreifer benutzt hat, ob ein „Trojaner“ installiert wurde, der einen Zugriff von außen erlaubt, ob Malwareprogramme im Netz sind, die erst später aktiv werden, auf welche IT-Systeme der Angreifer zugreifen konnte und welche Ziele er verfolgt.²⁴⁵

2. Rechtliche Konsequenzen und Handlungsoptionen

- 108** Wurde ein Angriff auf das IT-System oder eine andere digitale Attacke gegen das Unternehmen entdeckt, so können daraus ganz konkrete gesetzliche Pflichten des Unternehmens z. B. zur Meldung des Angriffs folgen.

a) Melde- und Informationspflichten

aa) DSGVO

- 109** Sind von dem Angriff personenbezogene Daten betroffen, z. B. von Kunden, Patienten, Mitarbeitern etc., ist zu prüfen, ob Meldepflichten nach der DSGVO bestehen. Das ist schon deshalb wichtig, weil Verstöße hier mit hohen Strafen geahndet werden können, und die Meldungen i. d. R. äußerst öffentlichkeitswirksam sind und deshalb im Rahmen der i. d. R. parallel laufenden Kommunikati-

²⁴⁵ Vgl. *Bensinger/Kozok*, CB 2015, 376, 379.

onsmaßnahmen berücksichtigt werden müssen. Die DSGVO unterscheidet in Art. 33, 34 DSGVO zwischen Meldungen an die Aufsichtsbehörde und Meldungen an die betroffenen Personen.

(1) Meldung an die Aufsichtsbehörde (Art. 33 DSGVO)

Nach Art. 33 Abs. 1 DSGVO trifft den Verantwortlichen eine fristgebundene Meldepflicht gegenüber der Aufsichtsbehörde, wenn er von einer Datenschutzverletzung erfährt. Dabei genügt eine objektive Schutzverletzung, auf ein Verschulden des Verantwortlichen kommt es nicht an. Außerdem muss der Verantwortliche nicht nur eigene, sondern auch Verletzungen des Auftragsverarbeiters oder Dritter (Art. 4 Nr. 10 DSGVO) melden.²⁴⁶

110

(a) *Entstehung der Pflicht:* Grundsätzlich muss dann gemeldet werden, wenn eine Verletzung des Schutzes personenbezogener Daten eingetreten ist, und dies dem Verpflichteten bekannt ist. Eine Meldepflicht besteht also noch nicht, wenn eine Verletzung nur droht oder nur vermutet wird, oder zwar objektiv eingetreten ist, aber dem Verpflichteten nicht bekannt war. Außerdem entfällt die Meldepflicht ausnahmsweise dann, wenn die Datenschutzverletzung nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (Art. 33 Abs. 1 Satz 1 Hs. 2 DSGVO). Ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht, wenn ihnen Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung einer Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile drohen (vgl. ErwG 85 DSGVO). Wichtig ist hier, dass die DSGVO Risiken nur dann sieht, wenn erhebliche Schäden drohen. Je höher der anzunehmende Schaden, desto geringere Anforderungen sind an die Wahrscheinlichkeit des Schadenseintritts zu stellen (vgl. ErwG 85 Satz 1 DSGVO).

111

Demnach bedarf es einer Prognose zu den Folgen des Datenschutzverstoßes; diese erstellt (zunächst) der Verantwortliche selbst. Sie ist im Nachhinein von der Aufsichtsbehörde überprüfbar.²⁴⁷ Stellt sich die Prognose nachträglich als falsch heraus, realisiert sich also entgegen der Prognose das Risiko, ist nicht die Unrichtigkeit der Prognose selbst Grund für eine Sanktionierung. Entscheidend ist vielmehr, ob die Annahmen des Verantwortlichen über die Tatsachenlage und die rechtlichen Überlegungen sowie zur weiteren Fortentwicklung nachvollziehbar und plausibel waren oder nicht. Geprüft wird, ob der Verantwortliche alle maßgeblichen Umstände nach seinen Fähigkeiten ermittelt, vollständig einbezogen sowie zutreffend und nachvollziehbar (vgl. Abs. 5: Dokumentationspflicht) bewertet hat.²⁴⁸

112

²⁴⁶ Brink, in: BeckOK DatenschutzR, 45. Ed. 1.2.2022, DS-GVO Art. 33 Rn. 27 und 28.

²⁴⁷ Brink, in: BeckOK DatenschutzR, 45. Ed. 1.2.2022, DS-GVO Art. 33 Rn. 37.

²⁴⁸ Brink, in: BeckOK DatenschutzR, 45. Ed. 1.2.2022, DS-GVO Art. 33 Rn. 38.

- 113** (b) *Zeitpunkt der Meldepflicht*: Der Verantwortliche muss die Verletzung „unverzüglich“ und soweit es ihm möglich ist binnen 72 Stunden nach Bekanntwerden der Verletzung melden (Art. 33 Abs. 1 Satz 1 DSGVO). Das ist wohl so zu verstehen, dass eine Meldung innerhalb von 72 Stunden immer unverzüglich und damit rechtzeitig ist. Die Vorgabe der 72-Stunden-Regelfrist darf der Verantwortliche nur überschreiten, wenn ihm eine Meldung vorher unmöglich war. Dies hat der Verantwortliche gem. Satz 2 gegenüber der AB darzulegen (ErwG 85 der DSGVO). Auch eine nicht rechtzeitige Meldung kann aufsichtsbehördliche Maßnahmen nach sich ziehen (Verwarnung nach Art. 58 Abs. 2 lit. b DSGVO, Bußgeld nach Art. 83 Abs. 4 lit. a DSGVO).
- 114** (c) *Inhalt der Meldung*: Die Meldung nach Art. 33 DSGVO bedarf keiner bestimmten Form. Angesichts der Bedeutung der Meldepflicht ist jedoch anzuraten, die gebotene Mitteilung (auch) schriftlich an die Aufsichtsbehörde zu richten.²⁴⁹ Der Mindestumfang der Meldung wird in Art. 33 Abs. 3 DSGVO spezifiziert. Lit. a verlangt die Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten (vgl. die Legaldefinition in Art. 4 Nr. 12 DSGVO: Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung), sowie Angaben zu Kategorien und (ungefähren) Zahl der betroffenen Personen und zu Kategorien und (ungefähren) Zahl der betroffenen personenbezogenen Datensätze. Nach lit. b sind Namen und Kontaktdaten des Datenschutzbeauftragten in der Meldung zu nennen. Lit. c verlangt eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten. Nach lit. d muss der Verantwortliche beschreiben, welche Maßnahmen er bereits ergriffen hat oder noch vorschlägt, um die eingetretene Verletzung zu beseitigen oder in ihren Auswirkungen abzumildern, damit die Aufsichtsbehörde beurteilen kann, ob zur Schadensabwehr oder -minimierung weitere Maßnahmen geboten sind.
- 115** Liegen die Information nicht alle zu dem Zeitpunkt vor, zu dem gemeldet werden muss, so sind zunächst die Informationen vorzulegen, über die der Verantwortliche bereits verfügt, und die übrigen dann sukzessive nachzureichen, sobald sie dem Verantwortlichen vorliegen; Schnelligkeit ist hier wichtiger als Richtigkeit und Vollständigkeit (vgl. auch ErwG 85 Satz 2 der DSGVO). Dies resultiert in einer Vorabmeldepflicht im Sinne einer „Erstbenachrichtigung“ auch bei noch nicht vollständigem Lagebild²⁵⁰ – immer vorausgesetzt, dass gleichwohl bereits eine Schutzverletzung eingetreten ist.
- 116** Außerdem trifft den Verantwortlichen nach Abs. 5 eine Dokumentationspflicht hinsichtlich Umfang und Auswirkungen der Datenschutzverletzung sowie zu den ergriffenen Abhilfemaßnahmen. Diese ist insbesondere von Bedeutung, wenn der Verantwortliche von einer Meldung nach Abs. 1 abgesehen hat, weil er kein hinreichendes Risiko gesehen hat. Dann kann die Aufsichtsbehörde diese wertende Entscheidung des Verantwortlichen mithilfe der Dokumentation nach-

249 Brink, in: BeckOK DatenschutzR, 45. Ed. 1.2.2022, DS-GVO Art. 33 Rn. 31.

250 Brink, in: BeckOK DatenschutzR, 45. Ed. 1.2.2022, DS-GVO Art. 33 Rn. 59–61.

vollziehen und ggf. bewerten. Der Verantwortliche hat nicht die Pflicht, die Dokumentation der Aufsichtsbehörde unaufgefordert zuzuleiten. Er muss sie lediglich bereithalten, um sie der Aufsichtsbehörde auf Anfrage unverzüglich übermitteln oder vorlegen zu können.²⁵¹

(d) *Meldepflicht des Auftragsverarbeiters:* Bei Auftragsdatenverarbeitungen ist es häufig der Auftragsverarbeiter, der (zuerst) von einer Datensicherheitsverletzung erfährt. Ihn trifft dann zwar keine eigene Meldepflicht gegenüber der Aufsichtsbehörde, er muss die Verletzung aber unverzüglich dem Verantwortlichen melden (Art. 33 Abs. 2 DSGVO). Da bei Nicht-EU-Auftragsverarbeitern nicht gewährleistet ist, dass sie unmittelbar aus Art. 33 Abs. 2 DSGVO verpflichtet sind, sollte diese Pflicht sowie die Pflicht zur weiteren Unterstützung des Verantwortlichen bei der Schadenbegrenzung, Verfolgung von Rechten, „Stopfen“ des Datenlochs etc. dem Auftragsverarbeiter vertraglich auferlegt werden (vgl. auch Art. 28 Abs. 3 lit. f DSGVO). Zu beachten ist auch, dass für die Meldung des Auftragsverarbeiters die 72-Stunden-Frist nicht gilt; er muss also wirklich unverzüglich melden, auch wenn das früher als 72 Stunden ist. Schließlich muss seine Meldung den Verantwortlichen in die Lage versetzen, rechtzeitig an die Aufsichtsbehörde melden zu können. **117**

(2) Meldung an die Betroffenen (Art. 34 DSGVO)

(a) *Entstehung der Pflicht:* Neben der Meldepflicht des Art. 33 DSGVO kann auch eine Benachrichtigungspflicht gegenüber den Betroffenen nach Art. 34 DSGVO bestehen, falls die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat. Auf ein Verschulden des Verantwortlichen kommt es nicht an,²⁵² sondern auf das Ergebnis einer anzustellenden Risikoprognose. Die Risikoprognose nimmt hier aber eine andere Funktion ein als bei Art. 33 DSGVO: Erst wenn sie ein Risiko statuiert, und zwar ein hohes Risiko, entsteht überhaupt erst die Meldepflicht gegenüber den Betroffenen.²⁵³ Prinzipiell ist das von einer Datenschutzverletzung ausgehende Risiko dann hoch, wenn anzunehmen ist („voraussichtlich“), dass bei ungehindertem Geschehensablauf mit hoher Wahrscheinlichkeit ein Schaden für die Rechte und Freiheiten des/der Betroffenen eintritt. Neben der Eintrittswahrscheinlichkeit sind auch die Art der Verletzung, die Natur, Sensibilität und der Umfang der betroffenen personenbezogenen Daten, der zur Identifizierung der Individuen notwendige Aufwand, die Schwere der Folgen für den Betroffenen sowie spezielle Eigenschaften der Betroffenen zu berücksichtigen.²⁵⁴ So ist das Risiko auch dann hoch, wenn zwar der **118**

251 *Brink*, in: BeckOK DatenschutzR, 45. Ed. 1.2.2022, DS-GVO Art. 33 Rn. 65–68.

252 *Brink*, in: BeckOK DatenschutzR, 45. Ed. 1.2.2022, DS-GVO Art. 34 Rn. 23.

253 So auch *Brink*, in: BeckOK DatenschutzR, 45. Ed. 1.2.2022, DS-GVO Art. 34 Rn. 19.

254 Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten nach der Datenschutz-Grundverordnung (DS-GVO), S. 24 f., https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf (zuletzt abgerufen am 15.5.2024).

Eintritt eines Schadens als wenig wahrscheinlich prognostiziert wird, dieser Schaden dann aber besonders groß wäre (ErwG 75 Satz 1 der DSGVO) oder besondere Kategorien personenbezogener Daten i. S. v. Art. 9 Abs. 1 DSGVO, personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten (vgl. Art. 10 DSGVO) oder Profiling-Daten sowie aus der systematischen Überwachung öffentlich zugänglicher Bereiche (vgl. Art. 35 Abs. 3 DSGVO) Gegenstand der Datenschutzverletzung waren.²⁵⁵ Die Benachrichtigungspflicht entfällt, wenn der Verantwortliche durch vorherige oder nachträgliche Maßnahmen (Art. 34 Abs. 3 lit. a bzw. lit. b DSGVO) eine Risikominimierung erreicht. Ob mit den vorhergehenden Schutzmaßnahmen nur solche gemeint sind, die der Verantwortliche vor Eintritt des Ereignisses eingerichtet hat, ist unklar, denn eigentlich werden diese schon in der Risikoanalyse berücksichtigt, die dann gar kein hohes Risiko indizieren dürfte. Nach § 29 Abs. 1 Satz 3 BDSG entfällt die Pflicht zur Benachrichtigung außerdem dann, wenn und soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach geheim gehalten werden müssen, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten. Allerdings ist ein solches Geheimhaltungsinteresse dann gegen die Interessen der von dem Sicherheitsvorfall betroffenen Person abzuwägen; überwiegen ihre Interessen, insbesondere weil z.B. durch die Meldung drohende Schäden abgewendet werden können, so muss sie trotzdem benachrichtigt werden (§ 29 Abs. 1 Satz 4 BDSG).

- 119** Wie bei Art. 33 DSGVO kann der Verantwortliche natürlich eine (im Nachhinein) falsche Risikoprognose treffen, oder die Aufsichtsbehörde auf Grundlage derselben Tatsachen zu einer anderen Prognose gelangen. Deshalb kann die Aufsichtsbehörde vom Verantwortlichen verlangen, die Benachrichtigung nachzuholen. Sie kann zur Rechtssicherheit des Verantwortlichen auch feststellen, dass eine Benachrichtigung nicht erforderlich ist, weil ein Ausnahmegrund nach Art. 34 Abs. 3 DSGVO vorliegt (Abs. 4). Ein Verantwortlicher, der sich über die Verpflichtung zur Benachrichtigung nach Abs. 1 im konkreten Fall unsicher ist, kann sich an die Aufsichtsbehörde mit dem Antrag wenden, einen solchen Beschluss nach Abs. 4 zu erlassen.²⁵⁶
- 120** (b) *Zeitpunkt der Meldepflicht:* Der Verantwortliche muss unverzüglich benachrichtigen, d.h. ohne schuldhaftes Zögern. Die 72-Stunden-Frist nach Art. 33 DSGVO gilt hier nicht; „unverzüglich“ kann im Einzelfall also auch schon vor 72 Stunden bedeuten. Wegen der unterschiedlichen Maßstäbe des Art. 33 und des Art. 34 DSGVO müssen die Meldepflichten nicht zum selben Zeitpunkt entstehen; so kann sich das hohe Risiko einer Rechtsverletzung, das zur Meldepflicht an die Betroffenen führt, auch erst zu einem späteren Zeitpunkt manifestieren, wenn z.B. mehr Informationen über das Ausmaß des Vorfalls bekannt werden. Ein längeres Abwarten vor der Benachrichtigung ist auch dann als gerechtfertigt anzusehen, um geeignete Maßnahmen gegen fortlaufende oder ver-

²⁵⁵ Brink, in: BeckOK DatenschutzR, 45. Ed. 1.2.2022, DS-GVO Art. 34 Rn. 25, 26.

²⁵⁶ Brink, in: BeckOK DatenschutzR, 45. Ed. 1.2.2022, DS-GVO Art. 34 Rn. 46.

gleichbare Verletzungen zu treffen, wenn dies mit der Aufsichtsbehörde abgesprochen ist oder von anderen zuständigen Behörden, wie bspw. Strafverfolgungsbehörden angewiesen wurde (ErwG 86 der DSGVO). Problematisch ist in diesem Zusammenhang insbesondere, ob entsprechende Weisungen anderer als EU-Behörden hier maßgeblich sein können, z. B. bei EU-Grenzen überschreitenden Sicherheitsvorfällen; insbesondere multinationale Konzerne können sich hier mit einander widersprechenden Pflichten konfrontiert sehen. Erwägungsgrund 86 stellt nicht darauf ab, dass solche Weisungen von EU-Behörden kommen müssen, entscheidend ist allein, ob sie für den Verantwortlichen oder den Sicherheitsvorfall „zuständig“ sind. Im Einzelfall sollte dies mit der Aufsichtsbehörde abgesprochen werden.

(c) *Form und Inhalt der Meldepflicht:* Der Verantwortliche muss dem Betroffenen die Art der Datenschutzverletzung mitteilen und die Informationen nach Art. 33 Abs. 3 lit. b, c und d DSGVO (also Kontaktdaten des Datenschutzbeauftragten, Beschreibung der wahrscheinlichen Folgen der Schutzverletzung für den Betroffenen und die vom Verantwortlichen getroffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung etc.) zukommen lassen. Die Meldung muss in „klarer und einfacher Sprache“ abgefasst sein und hat in präziser, transparenter und leicht zugänglicher Form zu erfolgen. Sie darf also nicht fachsprachlich formuliert sein, sondern muss für jedermann gut verständlich sein. Adressaten der Benachrichtigung sind alle Personen, die von der Datenschutzverletzung betroffen sind.

121

Die Betroffenen sind grundsätzlich individuell zu benachrichtigen, es sei denn, der Benachrichtigungsaufwand wäre unangemessen hoch (Art. 33 Abs. 3 lit. c DSGVO). Anders als noch bei der Meldepflicht nach BDSG-alt kann (muss aber nicht) der Verantwortliche in diesem Fall eine öffentliche Bekanntmachung oder eine ähnlich wirksame Maßnahme vornehmen. Unter öffentlicher Bekanntmachung ist die Verbreitung über amtliche Verkündungsblätter oder Tageszeitungen zu verstehen (vgl. § 186 Abs. 2 ZPO). Als ähnlich wirksame Maßnahme kommt eine Veröffentlichung im Internet in Betracht, soweit zu erwarten ist, dass die betroffenen Personen diese dort auffinden werden.²⁵⁷

122

Da der Auftragsverarbeiter schon aus Art. 33 Abs. 2 DSGVO (und ggf. Vertrag) verpflichtet ist, den Sicherheitsvorfall an den Verantwortlichen zu melden, ist eine erneute Meldepflicht im Rahmen des Art. 34 DSGVO entbehrlich. Die Risikoanalyse und das Ergreifen von Melde- und anderen Maßnahmen ist Aufgabe und Privileg des Verantwortlichen. So sollte dem Auftragsverarbeiter in der Auftragsverarbeitungsvereinbarung zwar Hilfestellung und Mitwirkung auch zur Risikoanalyse und Meldung nach Art. 34 DSGVO auferlegt werden (vgl. Art. 28 Abs. 3 lit. f DSGVO; z. B. durch Mitteilung der Adressen von Betroffenen), dem Auftragsverarbeiter sollte es aber untersagt werden, selbst irgendwelche Meldungen vorzunehmen.

123

²⁵⁷ Brink, in: BeckOK DatenschutzR, 45. Ed. 1.2.2022, DS-GVO Art. 34 Rn. 41, 43.

(3) Sanktionen

- 124** Wenn der Verantwortliche die nach Art. 33 bzw. 34 DSGVO gebotenen Meldungen unterlässt, kann die Aufsichtsbehörde den Verstoß mit einer Geldbuße von bis zu 10 Mio. EUR oder im Falle von Unternehmen sogar in Höhe von bis zu 2 % des weltweiten (Konzern-)Jahresumsatzes ahnden (Art. 83 Abs. 4 lit. a DSGVO). Als Verstoß des Verantwortlichen ist auch eine unvollständige Meldung nach Art. 33 Abs. 3 DSGVO, eine unterlassene Teilmeldung nach Abs. 4 und eine fehlende oder unvollständige Dokumentation nach Abs. 5²⁵⁸ oder eine unverständliche bzw. unvollständige Meldung im Rahmen des Art. 34 DSGVO zu werten.²⁵⁹ Zudem wird auch der Auftragsverarbeiter bei unterlassener Meldung an den Verantwortlichen nach Art. 33 Abs. 2 DSGVO bußgeldpflichtig.²⁶⁰

bb) BDSG

- 125** Meldepflichten nach dem BDSG sind mittlerweile reduziert auf Sicherheitsvorfälle bei öffentlichen Stellen, die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständig sind (§ 65 BDSG). Diese müssen eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst innerhalb von 72 Stunden, nachdem sie ihnen bekannt geworden ist, der oder dem Bundesbeauftragten für Datenschutz und Informationsfreiheit melden. Eine Ausnahme hiervon besteht, wenn die Verletzung voraussichtlich keine Gefahr für die Rechtsgüter natürlicher Personen ausgelöst hat.

cc) BSIG

- 126** Auch das BSIG schreibt eine Meldepflicht für erhebliche Störungen vor (§ 8b Abs. 4 BSIG). Betreiber Kritischer Infrastrukturen haben Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können (Satz 1 Nr. 2) oder geführt haben (Satz 1 Nr. 1) zu melden. In der Meldung müssen Angaben zu der Störung, zu möglichen grenzübergreifenden Auswirkungen und zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur erbrachten kritischen Dienstleistung sowie zu den Auswirkungen der Störung auf diese Dienstleistung gemacht werden. Dafür bleiben Meldungen vergleichsweise diskret: KRITIS-Betreiber sind verpflichtet, erhebliche Störungen (nur) dem BSI zu melden. Das BSI soll hierdurch in die Lage versetzt werden, ggf. andere Unternehmen und relevante Behörden vor Sicherheitslücken oder Angriffen auf die IT-Sicherheit warnen zu können. Das entspricht der Um-

258 Brink, in: BeckOK DatenschutzR, 45. Ed. 1.2.2022, DS-GVO Art. 33 Rn. 19.

259 Brink, in: BeckOK DatenschutzR, 45. Ed. 1.2.2022, DS-GVO Art. 34 Rn. 17.

260 Brink, in: BeckOK DatenschutzR, 45. Ed. 1.2.2022, DS-GVO Art. 33 Rn. 19.

setzung der Meldepflicht in Art. 14 der NIS-Richtlinie, wonach Meldungen nur an die nationale zuständige Behörde oder das nationale CSIRT (Computer Security Incident Response Team) erfolgen. Das BSI kooperiert allerdings dann im Rahmen der Art. 10 ff. NIS-Richtlinie mit der europäischen Behörde ENISA und den anderen nationalen Behörden und CSIRTs.

In der NIS-2-Richtlinie ist die Meldepflicht in Art. 23 geregelt. Anpassungsbedarf ergibt sich neben dem Adressatenkreis auch im Hinblick auf die nach Art. 23 Abs. 1 Satz 2 NIS-2-Richtlinie vorgesehene fakultative („gegebenenfalls“) Unterrichtung von Empfängern der Dienstleistungen über einen Sicherheitsvorfall (vgl. § 35 NIS2UmsuCG).²⁶¹ Die Zusammenarbeit auf nationaler und auf Unions- und internationaler Ebene ist nun in den Art. 13 ff. NIS-2-Richtlinie geregelt. 127

Eine Warnung des BSI kann auch anonymisiert erfolgen; nur dann, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der kritischen Infrastruktur geführt hat, wird das BSI auch den Betreiber namentlich nennen (§ 8b Abs. 4 letzter Satz BSIG). Hier gibt es außerdem Überlegungen, die Meldepflichten durch ein kooperatives Monitoringsystem auf eine übergeordnete Einrichtung zu übertragen und so für das betroffene Unternehmen Anonymität zu wahren.²⁶² Nach § 8c Abs. 3 Satz 1 BSIG trifft den Anbieter digitaler Dienste dieselbe Meldepflicht wie Betreiber Kritischer Infrastrukturen in § 8b Abs. 4 BSIG, das bedeutet für jeden Sicherheitsfall, der erhebliche Auswirkungen auf die Bereitstellung eines von ihm innerhalb der Europäischen Union erbrachten digitalen Dienstes hat.²⁶³ Wenn Anhaltspunkte dafür vorliegen, dass ein Anbieter diesen Anforderungen nicht gerecht wird, kann das BSI von dem Anbieter die Übermittlung der zur Beurteilung der Sicherheit seiner Netz- und Informationssysteme erforderlichen Informationen, einschließlich Nachweisen über ergriffene Sicherheitsmaßnahmen und die Beseitigung der Mängel, verlangen. 128

Außerdem müssen KRITIS-Betreiber gemäß § 8b Abs. 3 BSIG eine Kontaktstelle für die von ihnen betriebenen Kritischen Infrastrukturen benennen. Damit werden sie Teil der Warn- und Meldestruktur des BSI. 129

Es besteht keine Konkurrenz von Art. 33 oder 34 DSGVO zur Meldepflicht nach § 8b Abs. 1 BSIG, da diese eine andere Zielrichtung verfolgt – den Schutz kritischer Infrastrukturen. Daher stehen diese Meldepflicht und diejenige nach Art. 33 bzw. 34 nebeneinander.²⁶⁴ Hingegen sind KRITIS-Betreiber von den Meldepflichten des BSIG ausgenommen, wenn sie aufgrund spezialgesetzlicher 130

261 2. Referentenentwurf, Bearbeitungsstand: 3.7.2023, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwurfe/CI1/NIS-2-RefE.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 12.5.2024).

262 Vgl. Roos, MonIKA: IT-Sicherheit durch kooperative Ansätze, S. 5, 7, 16.

263 Eckhardt, in: Auer-Reinsdorf/Conrad, HdB IT- und Datenschutzrecht, § 33 Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, Rn. 284.

264 Brink, in: BeckOK DatenschutzR, 45. Ed. 1.2.2022, DS-GVO Art. 33 Rn. 18.

Vorschriften vergleichbare oder gar striktere Anforderungen erfüllen müssen (§ 8d Abs. 3 Nr. 5 BSIG). Interessanterweise gilt dies auch dann, wenn diese Anforderungen keine Meldepflichten beinhalten.²⁶⁵ So handelt es sich bei § 54 ZAG um eine solche spezialgesetzliche Rechtsvorschrift (vgl. → Rn. 82), welche die Anwendung von § 8a BSIG ausschließt.

- 131** Nach § 5b BSIG kann das BSI auf Ersuchen des betroffenen KRITIS-Betreibers die erforderlichen Maßnahmen zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des IT-Systems treffen, wenn die Beeinträchtigung der Sicherheit eines IT-Systems einen herausgehobenen Fall darstellt (Abs. 1 Satz 1). Von einem solchen ist nach Abs. 2 insbesondere bei einem Angriff von besonderer technischer Qualität oder in Fällen auszugehen, in denen die zügige Wiederherstellung der IT-Sicherheit von besonderem öffentlichen Interesse ist. Dies ist der Fall, wenn der Ausfall oder die Beeinträchtigung spürbare Auswirkungen auf das Gemeinwohl, zum Beispiel im Sinne der Versorgung der Allgemeinheit mit kritischen Dienstleistungen, haben kann. Gem. Abs. 5 kann das BSI mit Einwilligung des Ersuchenden auf dessen Kosten qualifizierte Dritte zur Hilfe heranziehen. Nach Abs. 6 kann es vom Hersteller des IT-Systems die Mitwirkung an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit des IT-Systems verlangen, soweit dies erforderlich ist. Beruht die Sicherheitslücke auf der verwendeten Hard- oder Software, kann der Produkthersteller schnell und nachhaltig Abhilfe schaffen. Allerdings darf der Hersteller aus Gründen der Verhältnismäßigkeit nach Ablauf des Supportzeitraums nicht zur kostenlosen Mitwirkung herangezogen werden.

dd) ZAG

- 132** § 54 Abs. 1 Satz 1 ZAG verpflichtet Zahlungsdienstleister, die BaFin unverzüglich über schwerwiegende Betriebs- oder Sicherheitsvorfälle zu unterrichten und ersetzt die bisherige Regelung in Nr. 3.2 der MaSi.²⁶⁶ Die BaFin wiederum muss dann die EBA sowie die EZB unverzüglich über den Vorfall informieren (§ 54 Abs. 1 Satz 2 ZAG).
- 133** Unter einem Betriebs- oder Sicherheitsvorfall wird ein Ereignis verstanden, das vom Zahlungsdienstleister nicht geplant war und sich negativ auf die Integrität, die Verfügbarkeit, die Vertraulichkeit, die Authentizität und/oder die Kontinuität von zahlungsbezogenen Diensten auswirkt oder aller Wahrscheinlichkeit nach eine solche negative Auswirkung haben wird.²⁶⁷ Schwerwiegend ist ein Betriebs- oder Sicherheitsvorfall schon dann, wenn quantitativ eine hohe Zahl an offenen Transaktionen oder Kunden betroffen ist, die Ausfallzeit besonders lange dauert, der wirtschaftliche Schaden besonders hoch ist, Auswirkungen auf weitere Zah-

²⁶⁵ Die Gesetzesbegründung (BT-Drs. 18/4096, S. 29) verweist diesbezüglich nur auf die Telematikinfrastruktur im Gesundheitswesen, für die in § 291b SGB V Anforderungen an die IT-Sicherheit, aber keine Meldepflichten festgelegt sind.

²⁶⁶ *Steinhoff*, in: Casper/Terlau, ZAG, § 54 Rn. 20.

²⁶⁷ *Steinhoff*, in: Casper/Terlau, ZAG, § 54 Rn. 11.

lungsdienstleister oder Infrastrukturen vorliegen, ein qualitativ als relevant einzustufender Reputationsschaden droht oder qualitativ eine hohe interne Eskalationsstufe erreicht wird, die über das Standard-Reporting deutlich hinausgeht.²⁶⁸ Dagegen müssen z. B. ein einzelner Phishing-Angriff oder einzelne Brute-Force-Angriffe durch Scriptkiddies nicht gemeldet werden, wenn aufgrund des situativen Einzelfalls eine wie auch immer geartete Serie auszuschließen ist.²⁶⁹ Auch die EBA-Leitlinien zur Meldepflicht schwerwiegender Sicherheitsvorfälle,²⁷⁰ die die BaFin in ihrem letzten Rundschreiben berücksichtigt hat, geben Auskunft darüber, welche Vorfälle konkret meldepflichtig sind.

Die BaFin hat eine Melde- und Veröffentlichungsplattform (MVP-Portal) etabliert, die genutzt werden muss, um der Meldepflicht nachzukommen.²⁷¹ Es gibt drei Arten von Meldungen, die Zahlungsdienstleister kumulativ abgeben müssen, sodass die Abschlussmeldung Informationen zu allen Feldern enthält.²⁷² Zunächst muss der Zahlungsdienstleister eine Erstmeldung innerhalb von vier Stunden der erstmaligen Klassifizierung eines Betriebs- oder Sicherheitsvorfalls als schwerwiegend (oder Reklassifizierung eines zunächst nicht als schwerwiegend klassifizierten Vorfalls²⁷³) über die von der BaFin zur Verfügung gestellten Meldewege senden. Anschließend müssen Zwischenmeldungen eingereicht werden, wenn der Regelbetrieb wiederhergestellt ist oder nach einer Frist von drei Geschäftstagen die normale Geschäftstätigkeit nicht wieder aufgenommen worden ist oder sich wesentliche Änderungen der Informationen seit den vorhergehenden Meldungen ergeben haben. Schließlich muss eine Abschlussmeldung eingereicht werden, und zwar innerhalb von maximal 20 Tagen, bevor der normale Geschäftsablauf wieder aufgenommen wird. Diese Meldung muss dann alle vollständigen Informationen enthalten, also die tatsächlichen Zahlen zu den

134

268 BaFin, Rundschreiben 03/2022 (BA) zur Meldung schwerwiegender Zahlungssicherheitsvorfälle gemäß § 54 Abs. 1 ZAG v. 9.3.2022, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2022/rs_03_2022_schwerwiegender_Zahlungssicherheitsvorfaelle.html (abgerufen am 12.5.2024), Ziffer 1.2; *Steinhoff*, in: Casper/Terlau, ZAG, § 54 Rn. 14, 15.

269 BaFin BA 51, PSD2-Infoveranstaltung, Sicherheit im Zahlungsverkehr einschließlich Meldewesen v. 5.12.2017, S. 40, https://www.bafin.de/SharedDocs/Downloads/DE/Veranstaltung/dl_171205_NeufassungZAG_3_Sicherheit_Zahlungsverkehr.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 15.5.2024).

270 Revised Guidelines on major incident reporting under PSD2 – EBA/GL/2021/03 vom 10.6.2021, https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20major%20incident%20reporting%20under%20PSD2%20EBA-GL-2021-03/1014562/Final%20revised%20Guidelines%20on%20major%20incident%20reporting%20under%20PSD2.pdf (zuletzt abgerufen am 7.12.2023).

271 Vgl. BaFin Rundschreiben 03/2022 (BA) zur Meldung schwerwiegender Zahlungssicherheitsvorfälle gemäß § 54 Abs. 1 ZAG vom 9.3.2022, Punkt 2.1, S. 10; https://www.bafin.de/DE/DieBaFin/Service/MVPportal/PSD2/psd2_artikel.html;jsessionid=D7E6587CEF42F255B3EBC35711B87DF6.1_cid361 (zuletzt abgerufen am 15.5.2024).

272 *Steinhoff*, in: Casper/Terlau, ZAG, § 54 Rn. 23.

273 So auch *Steinhoff*, in: Casper/Terlau, ZAG, § 54 Rn. 24.

Auswirkungen, die eigentliche Ursache und eine Zusammenfassung der Maßnahmen, die zur Beseitigung des Vorfalls getroffen wurden oder geplant sind, um zu verhindern, dass er in der Zukunft erneut auftritt.²⁷⁴

- 135** § 54 Abs. 4 ZAG verpflichtet Zahlungsdienstleister, ihre Nutzer über Vorfälle in Kenntnis zu setzen, die sich auf deren finanzielle Interessen auswirken können. Außerdem müssen diese Nutzer über alle Maßnahmen informiert werden, die getroffen werden können, um negative Auswirkungen des Vorfalls zu begrenzen. Schließlich müssen Zahlungsdienstleister nach § 54 Abs. 5 ZAG mindestens einmal jährlich Betrugsstatistiken an die BaFin liefern.
- 136** Nach § 64 Abs. 3 Nr. 15, Abs. 4 ZAG ist die vorsätzlich oder fahrlässig nicht abgegebene oder nicht richtige, nicht vollständige oder nicht rechtzeitige Meldung mit bis zu 100.000 EUR bußgeldbewehrt.
- 137** Die Meldepflichten nach ZAG lassen andere Meldepflichten, also insb. nach der DSGVO, an andere zuständige Behörden unberührt (§ 54 Abs. 6 ZAG). Art. 33 DSGVO ist damit in jedem Fall zusätzlich anwendbar, wenn ein Vorfall dazu führt, dass unbefugte Dritte Zugriff auf personenbezogene Daten bekommen (insb. von Zahlungsdienstnutzern). Unklar ist aber das Verhältnis zur Benachrichtigungspflicht an die Betroffenen nach Art. 34 DSGVO. Da auch § 54 ZAG auf europarechtlichen Regelungen beruht und insoweit *lex specialis* gegenüber Art. 34 DSGVO ist, wird man aber vertreten können, dass sich eine Benachrichtigung von Zahlungsdienstnutzern nur nach dem ZAG richtet.

ee) Meldepflichten für Energiewirtschaftsunternehmen

- 138** Für Betreiber von Energieversorgungsnetzen und Energieanlagen werden die Meldepflichten nach dem BSIG durch die Meldepflicht nach § 11 Abs. 1c EnWG verdrängt. Hiernach müssen Störungen dem BSI gemeldet werden, das diese dann an die Bundesnetzagentur weitergeben und gemeinsam mit dieser das weitere Störungs-Management begleiten wird. Im Bereich des AtomG gelten außerdem die §§ 6 ff. AtSMV (Atomrechtliche Sicherheitsbeauftragten- und Meldeverordnung).

ff) TMG

- 139** Die Meldepflicht bei Sicherheitsvorfällen nach § 15a TMG-alt ist seit 2021 entfallen. Für Telemedienanbieter, die gleichzeitig als Anbieter digitaler Dienste gem. § 8c BSIG qualifizieren, gelten die in § 8c Abs. 3 BSIG geregelten Pflichten zur Meldung an das BSI. Gemeldet werden müssen Sicherheitsvorfälle, die erhebliche Auswirkungen auf einen in der EU erbrachten digitalen Dienst haben. Ein Sicherheitsvorfall ist hierbei jedes Ereignis, das tatsächlich nachteilige Aus-

²⁷⁴ Vgl. BaFin Rundschreiben 03/2022 (BA) zur Meldung schwerwiegender Zahlungssicherheitsvorfälle gemäß § 54 Abs. 1 ZAG vom 9.3.2022, Punkt 2: Meldeverfahren, S. 11 ff.; *Steinhoff*, in: Casper/Terlau, ZAG, § 54 Rn. 24-28.

wirkungen auf die Sicherheit von Netz- und Informationssystemen hat (Art. 4 Nr. 7 NIS-Richtlinie bzw. Art. 6 Nr. 6 NIS-2-Richtlinie).²⁷⁵

Erhebliche Auswirkungen hat der Sicherheitsvorfall nach Art. 3 der Durchführungsverordnung (EU) 2018/151 der EU-Kommission, wenn der Dienst für mehr als 5 Millionen Nutzer mindestens eine Stunden lang nicht verfügbar war, der Sicherheitsvorfall zu einem Verlust der Integrität, Authentizität oder Vertraulichkeit von Daten oder der Dienste geführt hat und hiervon mehr als 100.000 Nutzer in der EU betroffen sind, durch den Sicherheitsvorfall eine öffentliche Gefahr oder ein Risiko für die öffentliche Sicherheit entstanden ist oder Menschen ums Leben gekommen sind, oder der Sicherheitsvorfall für Nutzer zu einem Sachschaden von mehr als einer Million Euro geführt hat. Entsprechend entfällt die Meldepflicht, wenn der Anbieter keinen ausreichenden Zugang zu den Informationen hat, die erforderlich sind, um diese Auswirkung eines Sicherheitsvorfalls zu bewerten (§ 8c Abs. 3 Satz 3 BSIG). **140**

Für die inhaltlichen Anforderungen an eine Meldung gilt § 8b Abs. 4 BSIG entsprechend,²⁷⁶ es sei denn, Durchführungsakte der EU-Kommission nach Art. 16 Abs. 9 NIS-Richtlinie bestimmen etwas anderes (§ 8c Abs. 3 Satz 4 BSIG). Weitere Anhaltspunkte zum Inhalt der Meldung können der Vorlage des BSI für Meldungen entnommen werden.²⁷⁷ **141**

gg) TKG

Anbieter von Telekommunikationsdiensten haben eine Meldepflicht nach § 168 TKG; § 8b Abs. 4 BSIG gilt für Telekommunikationsanbieter nicht.²⁷⁸ Ähnlich wie bei § 8c Abs. 3 BSIG sind Sicherheitsvorfälle mit beträchtlichen Auswirkungen zu melden, wobei sich hier die Beträchtlichkeit nach den in § 168 Abs. 2 TKG genannten Kriterien richtet (die denen der Durchführungsverordnung zu § 8c BSIG stark ähneln). Die inhaltlichen Anforderungen ergeben sich aus § 168 Abs. 3 TKG und den Mitteilungen der Bundesnetzagentur (BNetzA). **142**

Schon das Bestehen einer besonderen und erheblichen Gefahr eines Sicherheitsvorfalls ist meldepflichtig; in dem Fall sind die potenziell betroffenen Nutzer über alle möglichen Schutz- oder Abhilfemaßnahmen, die von den Nutzern ergriffen werden können, zu informieren sowie gegebenenfalls auch über die Gefahr selbst (§ 168 Abs. 6 TKG). § 8e des BSI-Gesetzes gilt entsprechend. **143**

Falls tatsächlich eine Störung entsteht, kann die BNetzA nach § 168 Abs. 4 Satz 2 TKG einen detaillierten Bericht anfordern. Die Mitteilung muss sowohl an die **144**

²⁷⁵ *Beucher/Ehlen/Utzerath*, in: Kipker, Cybersecurity, Kap. 14 Rn. 234.

²⁷⁶ So auch *Beucher/Ehlen/Utzerath*, in: Kipker, Cybersecurity, Kap. 14 Rn. 237, die den Verweis auf § 8b Abs. 3 BSIG für ein Redaktionsversehen halten.

²⁷⁷ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Themen-Downloads/Digitale-Dienste/formular_meldung_8c3_BSIG_nurtext.html (zuletzt abgerufen am 13.5.2024).

²⁷⁸ So auch *Beucher/Ehlen/Utzerath*, in: Kipker, Cybersecurity, Kap. 14 Rn. 156.

BNetzA als auch an das BSI²⁷⁹ erfolgen.²⁸⁰ Sind von dem Sicherheitsvorfall personenbezogene Daten betroffen, richtet sich die Meldepflicht nach § 169 TKG. Diese Meldung muss dann an die BNetzA und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gemacht werden. Zusätzlich muss der Betroffene informiert werden, wenn anzunehmen ist, dass durch die Verletzung des Schutzes personenbezogener Daten Endnutzer oder andere Personen schwerwiegend in ihren Rechten oder schutzwürdigen Interessen beeinträchtigt werden. Neu hinzugekommen ist mit dem IT-Sicherheitsgesetz die Pflicht, Nutzern solche Störungen zu melden, die auf den Systemen der Nutzer bestehen und dem Anbieter bekannt werden, und die Nutzer auf angemessene technische Mittel zur Erkennung und Beseitigung der Störungen hinzuweisen (§ 169 Abs. 4 TKG). § 169 TKG geht damit noch über die Regelungen zur Meldung von Verletzungen des Schutzes personenbezogener Daten nach Art. 34 DSGVO hinaus.²⁸¹ § 169 TKG bleibt als Umsetzung von Art. 4 Abs. 3 und 4 der Richtlinie 2002/58/EG nach Maßgabe von Art. 95 DSGVO neben der DSGVO anwendbar.²⁸² Für nicht öffentlich zugängliche Kommunikationsdienste kommt § 169 TKG nicht zur Anwendung, sodass insoweit die DSGVO und § 8b BSIG gelten.²⁸³

hh) Sonstige Informationspflichten

- 145** Neben den vorgenannten Meldepflichten kann ein IT-Sicherheitsvorfall auch andere Informationspflichten auslösen, die in dieser Situation zu prüfen und ggf. zu erfüllen sind: Hierzu gehören etwa Ad-hoc-Meldungen bei börsennotierten Unternehmen, versicherungsvertraglich vereinbarte Meldungen an Cyber- und andere Versicherungen sowie interne Informationspflichten an Aufsichtsräte, Betriebsräte oder interne Datenschutzbeauftragte. Bei Datenleaks empfiehlt es sich außerdem zu prüfen, ob hierdurch vertragliche oder gesetzliche Vertraulichkeitsverpflichtungen verletzt wurden, was ggf. Informations- oder auch andere Pflichten auslöst. Insgesamt gilt auch hier, dass ein Abgleich mit der Kommunikationsstrategie unbedingt erforderlich ist.

b) Werkzeuge zur Abwehr von Cyberangriffen

- 146** Selbstverständlich ist eine der vordringlichsten Pflichten des betroffenen Unternehmens im Falle eines IT-Sicherheitsvorfalls, die entstandene Sicherheitslücke zu beseitigen. Stellt der Vorfall (auch) eine Datenschutzverletzung nach Art. 33, 34 DSGVO dar, ergibt sich dies schon aus Art. 32 Abs. 1c DSGVO (und zwar

279 Die Mitteilungspflicht an das BSI wurde durch Art. 5 Nr. 2 des NIS-Umsetzungsgesetzes am 23.6.2017 in das Gesetz eingefügt.

280 *Conrad*, in: Auer-Reinsdorff/Conrad, HdB IT- und Datenschutzrecht, § 33 Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, Rn. 301.

281 *Conrad*, in: Auer-Reinsdorff/Conrad, HdB IT- und Datenschutzrecht, § 33 Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, Rn. 303.

282 *Conrad*, in: Auer-Reinsdorff/Conrad, HdB IT- und Datenschutzrecht, § 33 Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, Rn. 304.

283 *Eckhardt*, in: Spindler/Schuster, Recht der elektronischen Medien, TKG § 109a Rn. 45.

nach Art. 83 Abs. 4 DSGVO bußgeldbewehrt).²⁸⁴ Hierzu ist aber in der Regel zunächst erforderlich, genau zu verstehen, was eigentlich in welchem Ausmaß passiert ist – wozu in erster Linie IT-forensische Analysen erforderlich sein werden. Diese liefern hoffentlich die erforderlichen Informationen zur Abwehr einer Cyberattacke, zur Identifizierung und Lokalisierung des Täters²⁸⁵ und zur Sicherung von Nachweisen für die straf- oder zivilrechtliche Verfolgung.²⁸⁶ Die IT-forensischen Analysen sollten juristisch begleitet werden, schon um sicherzustellen, dass gesicherte Nachweise auch ausreichen, um prozessrechtlich als Beweise zu dienen und nicht etwa Beweisverwertungsverbieten unterliegen. Andere Informationen können besser oder nur mit juristischen Hilfsmitteln (wie z. B. Auskunftsansprüchen gegen Telekommunikationsnetzbetreiber auf Nennung des Inhabers einer IP-Adresse) erlangt werden. Allerdings gibt es für angegriffene Unternehmen keine generellen Ansprüche, sondern nur vereinzelt spezialgesetzliche wie beispielsweise § 101a UrhG. Solche engen Voraussetzungen führen dazu, dass für die Mehrheit von „Cyberattacken“ das Zivil(prozess)recht keine oder nur unzureichende Hilfsmittel gewährt und stattdessen die Polizei oder Staatsanwaltschaft in Anspruch genommen werden muss. Diese sind rechtlich auch deutlich besser ausgestattet,²⁸⁷ etwa durch die Bestandsdatenauskunft (§ 100j StPO, § 113 TKG, Art. 6 Abs. 1 lit. e DSGVO), die Verkehrs- oder Nutzungsdatenauskunft (§ 100g StPO, Art. 6 Abs. 1 lit. e DSGVO), Beschlagnahme (§§ 94 ff. StPO), die verfassungsrechtlich sensible Telekommunikationsüberwachung (§§ 100a, b StPO) oder Durchsicht von Daten nach § 110 StPO, dessen Abs. 3 auch für Daten auf externen Medien (wie z. B. der Cloud) gilt.²⁸⁸ Für die grenzüberschreitende Strafverfolgung von „Cyber-Crimes“ gibt es zwar eine Reihe von Kooperationen²⁸⁹ und Ansätzen,²⁹⁰ gleichwohl bleiben hier viele rechtliche und faktische Hürden, die von Tätern bewusst ausgenutzt werden.

Insbesondere bei rufschädigenden Internet-Attacken können einstweilige Unterlassungsverfügungen, einschließlich der Inanspruchnahme von Blogbetreibern oder Host Providern, ein probates Mittel zur Abwehr darstellen. Diese sollten aber nie einen Selbstzweck erfüllen, sondern Werkzeug einer abgestimmten

147

284 Löschhorn/Fuhrmann, NZG 2019, 161, 162 f.

285 Vgl. Brodowski/Freiling, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, S. 55 f.

286 Vgl. Brodowski/Freiling, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, S. 122 ff.

287 Vgl. Übersicht bei Brodowski/Freiling, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, S. 129 ff.

288 Ausführlich Brodowski/Eisenmenger, ZD 2014, 119 ff.

289 Z. B. das European Cybercrime Centre der EUROPOL, www.europol.europa.eu/ec3 (zuletzt abgerufen am 29.1.2020) oder das Cyber Fusion Centre der INTERPOL, <https://www.interpol.int/Crimes/Cybercrime/Investigative-support-for-cybercrime> (zuletzt abgerufen am 15.5.2024).

290 Vgl. Brodowski/Freiling, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, S. 162 ff.

Kommunikationsstrategie sein (siehe → Rn. 148 f.). Sonst besteht die Gefahr, mit solchen Aktionen noch negativere Presse auszulösen.

3. Interne und externe Kommunikation

- 148** Häufig wird in Krisensituationen die Bedeutung einer professionellen Kommunikationsstrategie unterschätzt. Viele „Cyberattacken“ bezwecken genau die Denunziation des betroffenen Unternehmens in der Öffentlichkeit, und/oder die Störung der Interaktion mit Kunden. Neben der Sorge um die technische Stabilität ist es deshalb von höchster Dringlichkeit, immer gleichzeitig auch die Kommunikation nach außen zu kontrollieren und hierdurch eine Diskreditierung des Unternehmens mit fatalen Folgen für eine zukünftige Geschäftstätigkeit zu verhindern. Selbst wenn eine „Cyberattacke“ aus rechtlichen oder anderen Gründen nicht mehr vor der Presse und der übrigen Außenwelt „geheim gehalten“ werden kann, gibt es noch eine große Bandbreite an Möglichkeiten, wie sich das Unternehmen in seinem Umgang mit der Krise präsentieren kann: Diese Möglichkeiten sollten gezielt abgestimmt und professionell ausgeschöpft werden.
- 149** Hierbei ist die Bildung einer gemeinsamen Arbeitsgruppe bzw. eines Krisenstabs aus Geschäftsführung, Kommunikations- oder Presseabteilung, Rechtsabteilung (mit Compliance und Datenschutz) und vor allem der IT-Abteilung von essenzieller Bedeutung. In Krisensituationen überschlagen sich die Ereignisse, Entscheidungen müssen ohne zeitliche Spielräume getroffen werden. Silo-Denken und Delegation von Fragen an Fachdezernate haben hier keinen Platz. Vielmehr müssen die Entscheidungsträger gemeinsam am Tisch sitzen, um schnell Handlungsschritte unter Berücksichtigung aller wichtigen Aspekte erarbeiten zu können. Beispielsweise muss der Pressesprecher wissen, ob eine Meldung eines „Datenleaks“ zwingend vorgeschrieben ist, und dies gegebenenfalls kommunikativ vorbereiten und begleiten. Idealerweise arbeiten die Heads of Department nicht erst in der Krisensituation so eng zusammen, sondern haben schon zuvor verschiedene Szenarien durchgespielt und Reaktionsstrategien entwickelt.

4. Mittel- und längerfristige Maßnahmen

- 150** Ist ein Unternehmen einmal Opfer einer „Cyberattacke“ geworden, so müssen die erkannten Schwachstellen oder Lücken des bestehenden IT-Sicherheitsmanagements spätestens jetzt geschlossen werden. Auch haben die Mitarbeiter gelernt, dass die Risiken ernst genommen werden müssen. Dieses Bewusstsein sollte in Awareness-Schulungen für Mitarbeiter, für das Management und für die Krisenarbeitsgruppe geschärft werden. Mit den Behörden und Sicherheitsberatern sollte auch weiterhin ein kontinuierlicher Informationsaustausch gepflegt werden.

IV. Ausblick

Die zunehmende Digitalisierung und Vernetzung aller Unternehmen und Institutionen eröffnet auch immer mehr Risiken für Angriffe. Deshalb gilt es, durch effektive, aber umsetzbare Maßnahmen jederzeit einen möglichst hohen Schutzstandard zu erreichen und beizubehalten. Jedenfalls im Bereich der KRITIS- Unternehmen leisten das IT-Sicherheitsgesetz sowie europaweit die NIS-Richtlinie und jetzt auch die NIS-2-Richtlinie hier einen wertvollen Beitrag. Insbesondere die Informationsbündelung beim BSI bzw. anderen kontrollierenden Stellen (z.B. der Bundesnetzagentur) trägt außerdem dazu bei, dass das Wissen um die Techniken und Vorgehensweisen von Cyberkriminellen sowie geeignete Vorbeuge- und Abwehrmaßnahmen sich deutlich besser als bisher verbreiten können. Gleichzeitig zeigen die oft noch unbestimmten rechtlichen Vorgaben insbesondere zu vorbeugenden Schutzmaßnahmen, dass von Unternehmen und ihrer Geschäftsführung eine kontinuierliche Überwachung und Aktualisierung des Risikomanagements gefordert wird. Ebenso wie bei der Abwehr von tatsächlichen Angriffen ist eine effektive Compliance deshalb nur dann möglich, wenn die Geschäftsführung eng mit ihren IT-Spezialisten und Juristen zusammenarbeitet. **151**

Abschnitt 2.3 ESG und Governance

15. Kapitel Corporate Social Responsibility und Corporate Compliance – Entwicklungslinien gesellschaftlicher und juristischer Verantwortung von Unternehmen

I. Einleitung

1. „Shareholder Value“ und „Stakeholder Value“ – eine „Mission Impossible“ für Unternehmen?

In den 1980er Jahren gewann das „Shareholder Value“-Management immer größere Bedeutung. Die bis dahin vorherrschende Form einer gesellschaftlich verantwortungsbewussten Unternehmensführung, die *Frank Abrams* (Standard Oil, CEO) 1951 mit der Aufgabe des Managements zur Herstellung eines „fairen und funktionierenden Ausgleich[s] zwischen den Ansprüchen verschiedener, direkt betroffener Interessensgruppen, wie Aktionären, Beschäftigten, Kunden und der gesamten Öffentlichkeit“,¹ charakterisiert hatte, wurde mehr und mehr von einer kapitalmarktorientierten Unternehmensführung – der das Verständnis vom effizienten Kapitalmarkt innewohnt – abgelöst.² Infolgedessen hatten sich Aktienbeteiligungen nun „auch auf kürzere Sicht so zu rentieren [...], dass der Ertrag in einem angemessenen Verhältnis zum Risiko steht. Wenn dieser Ertrag nicht erwirtschaftet wird, sucht sich der Aktionär eine alternative Anlagemöglichkeit [...]“. Oberstes Ziel für die Unternehmensführung ist es demnach, eine Wertsteigerung für den Aktionär zu erbringen und so sein Vermögen zu mehren. Diesem Ziel sind alle anderen, auch das Überlebensziel der Unternehmung als selbstständige Organisation, klar untergeordnet“, wie es *Peter Wuffli* (McKinsey & Company) 1988 in der Neuen Zürcher Zeitung ausführte.³

Die Globalisierung der Weltwirtschaft – d. h. der Ausweitungsprozess von Märkten über Ländergrenzen hinweg bis hin zu weltweiten Märkten⁴ – schreitet seit den 1950er Jahren stetig voran.⁵ Neben der Reduktion der Distanzüberwindungskosten relativ zu den Produktionskosten, werden hierfür auch der Abbau von Handelshemmnissen sowie die weltweite Deregulierung weiterer Teile der

1 Vgl. *Kuhn/Weibler*, Bad Leadership, S. 41; *Reich*, Superkapitalismus, S. 66.

2 Vgl. *Kuhn/Weibler*, Bad Leadership, S. 41 f.

3 Vgl. Neue Zürcher Zeitung v. 16.11.1988, Nr. 268, S. 41; *Kuhn/Weibler*, Bad Leadership, S. 42.

4 Vgl. *Baßeler/Heinrich/Utecht*, Grundlagen und Probleme der Volkswirtschaft, S. 588 f.

5 <https://www.bpb.de/kurz-knapp/zahlen-und-fakten/globalisierung/52543/entwicklung-des-grenzueberschreitenden-warenhandels/> (zuletzt abgerufen 4.2.2024).

Wirtschaft als ursächlich für diese Entwicklung angesehen.⁶ Gerade für Unternehmen bot die voranschreitende Globalisierung der Weltwirtschaft eine sehr lukrative Möglichkeit an, um den eigenen „Shareholder Value“ zu steigern. Mit Blick auf die Zunahme der globalen Vernetzung der Märkte sowie der weltweiten Arbeitsteilung zeigt sich aber auch, dass die Globalisierung der Weltwirtschaft nicht nur eine positive, sondern auch eine negative Seite für die Weltgesellschaft aufweisen kann. Neben den bereits in der Vergangenheit aufgedeckten Verstöße von Unternehmen gegen Menschenrechte und Umweltschutz zeigen die aktuellen Beeinträchtigungen der globalen Vernetzung der Märkte – u. a. hervorgerufen durch die Covid-Pandemie⁷ oder durch wirtschaftliche und/oder militärische Auseinandersetzungen zwischen konfligierenden Staaten⁸ – die Risiken und Folgen der Globalisierung der Weltwirtschaft auf.

- 3 Im Rahmen eines Gastbeitrages im Harvard Business Manager befasste sich *Joe Kaeser* (Siemens AG, CEO) 2019 mit der gesellschaftlichen Verantwortung von Unternehmen (Corporate Social Responsibility, CSR).⁹ Darin vertrat er die Auffassung, dass Gewinne nicht das einzige Ziel von Unternehmen sein sollten, denn „ihren tieferen Sinn finden Unternehmen [erst] dann, wenn sie Wert schaffen nicht nur für Shareholder und Stakeholder, sondern für eine integrierte Interessengemeinschaft: ‚The business of business is to serve society‘“, so *Kaeser*.¹⁰
- 4 In Zusammenhang mit CSR gibt es aber auch kritische Stimmen, denn: Der „Business Case for Corporate Social Responsibility“ läuft letztlich auf die These hinaus, „dass eine kapitalmarktorientierte Unternehmensführung dann am erfolgreichsten ist, wenn sie eine gesellschaftlich verantwortungsbewusste Unternehmensführung hat“. ¹¹ Oder in anderen Worten ausgedrückt: „Der Shareholder Value ist hoch, wenn der Stakeholder Value hoch ist – und umgekehrt.“¹² Durch die Kombination von „Shareholder Value“-Management mit dem „Stakeholder Value“-Management – d. h. zweier eigentlich entgegengesetzter Verständnisse der Unternehmensführung – wird CSR daher nicht selten als Quadratur des Kreises angesehen – manche Stimmen sprechen in diesem Zusammenhang gar von

6 Vgl. *Baßeler/Heinrich/Utecht*, Grundlagen und Probleme der Volkswirtschaft, S. 590.

7 Vgl. *Flach/Steininger*, Globalisierung nach Covid-19: Die Folgen der Pandemie für die deutsche Wirtschaft, <https://www.ifo.de/publikationen/2020/aufsatz-zeitschrift/globalisierung-nach-covid-19> (zuletzt abgerufen am 29.2.2024).

8 Vgl. *Ankenbrand/Hein/Junge/Löhr*, Die Lieferketten stehen vor der nächsten Zerreißprobe, FAZ-Online 6.4.2022, <https://www.faz.net/aktuell/wirtschaft/wie-der-ukraine-krieg-lieferketten-und-globalisierung-bedroht-17940015.html> (zuletzt abgerufen am 29.2.2024).

9 Vgl. *Kaeser*, Harvard Business Manager 10/2019, 44 ff.

10 Vgl. *Kaeser*, Harvard Business Manager 10/2019, 44 ff.

11 Vgl. *Kuhn/Weibler*, Bad Leadership, S. 43; darstellend dazu u. a.: *Carroll/Shabana*, International Journal of Management Reviews 12 (1), S. 85–105; *Kuhn/Weibler*, Zeitschrift für Betriebswirtschaft 81 (Special Issue 1), S. 93–118.

12 Vgl. *Kuhn/Weibler*, Bad Leadership, S. 44.

einem „Mythos“.¹³ Im Ergebnis zeigt dieser kleine Einblick in die wissenschaftlichen Diskussionen klar auf, vor welch großen Herausforderungen die Leitung eines Unternehmens in der Praxis steht: Maximierung sowohl des Shareholder Values als auch des Stakeholder Values!

2. CSR und Unternehmensführung – Auswirkungen auf die Unternehmen?

Nachdem die gesellschaftliche Verantwortung von Unternehmen über viele Jahre hinweg häufig nur als strategisches und gesellschaftliches Engagement eines Unternehmens angesehen worden war, hat sich in der Zwischenzeit ein Wandel von der traditionellen Philanthropie hin zu modernen Corporate Social Responsibility-Konzeptionen in Unternehmen vollzogen. Um in der Gesellschaft nicht nur als „guter Bürger“ (Corporate Citizen) glaubhaft wahr- und ernstgenommen zu werden (Stichwort: Reputation!), sondern mit dieser neuen strategischen Ausrichtung auch im weltweiten Wettbewerb dauerhaft erfolgreich bestehen zu können, haben sich häufig tiefgreifende Eingriffe in die Kernkompetenzen – insbesondere in das Kerngeschäft – eines Unternehmens als zwingend notwendig und erforderlich erwiesen.¹⁴

Dieser Wandel kam nicht von ungefähr: Den Unternehmen ist klar geworden, dass es heutzutage nicht mehr ausreichend ist, ein unternehmerisches Ziel, das jenseits der Gewinnmaximierung liegt, zu formulieren und sich nur vordergründig zu diesem zu bekennen. Diese Ziele müssen nun ebenso ernsthaft und nachhaltig verfolgt und in die Tat umgesetzt werden.¹⁵ Zwar gibt es auch einige Unternehmen, die nach wie vor „gar nicht mehr Geld in ihre Mitarbeiter, in langlebigere Produkte [und/oder] in den Umweltschutz investieren wollen. Mit dem vordergründigen Bekenntnis zum Purpose wollen sie vielmehr echte Veränderungen hin zu einer gemeinwohl-orientierteren Wirtschaftsweise verhindern“.¹⁶ Die – teilweise schmerzhaft – Abrechnung erfolgt allerdings dann, wenn die Shareholder und Stakeholder dieser Unternehmen bzw. deren Unternehmensleitungen im Hinblick

13 Vgl. Kuhn/Weibler, *Bad Leadership*, S. 44; dazu vertiefend: Raith, *Mythos CSR*; Groening/Kanuri, *Journal of Business Research* 66 (10), S. 1852–1860.

14 Vgl. Osburg, in: Schneider/Schmidpeter (Hrsg.), *Corporate Social Responsibility*, S. 737 f.; Porter/Kramer, *Harvard Business Review*, 2006 (Dezember), S. 78–94.

15 Vgl. dazu u. a. die Absichtserklärung des Business Roundtable, einer Interessensgruppierung US-amerikanischer Unternehmen zur Nachhaltigkeit: FAZ Online v. 20.8.2019, <https://www.faz.net/aktuell/finanzen/finanzmarkt/usa-business-roundtable-distanziert-sich-vom-shareholder-value-16342395.html> (zuletzt abgerufen am 29.2.2024); Süddeutsche Zeitung Online v. 20.8.2019, <https://www.sueddeutsche.de/wirtschaft/shareholder-value-profit-ist-nicht-alles-1.4569768> (zuletzt abgerufen am 29.2.2024); Business Roundtable Online, *Embracing Sustainability Challenge*, <https://www.businessroundtable.org/policy-perspectives/energy-environment/sustainability> (zuletzt abgerufen am 29.2.2024).

16 Vgl. Sommer, *brand eins Magazin* 4/2020, <https://www.brandeins.de/magazine/brand-eins-wirtschaftsmagazin/2020/investieren/viele-die-vom-purpose-reden-wollen-echte-veraenderungen-verhindern> (zuletzt abgerufen am 29.2.2024); vertiefende Darstellung: Kreiß/Siebenbrock, *Blenden Wuchern Lamentieren*.

auf ihre öffentlichen Bekenntnisse hin in die Pflicht nehmen sowie im gleichen Maße öffentlich wirksam Transparenz und Rechenschaft (ab-)verlangen.

- 7 Aus diesem Grund verwundert es nicht, dass das CSR- und Reputationsmanagement nicht mehr nur in den PR- und Kommunikationsabteilungen eines Unternehmens verortet ist und von dort aus (teilweise „unter dem Radar“) betrieben wird. Insbesondere bei Unternehmen, die international oder global agieren, ist zu beobachten, dass das CSR- und Reputationsmanagement sogar bei der Unternehmensleitung angekommen ist und dort auch ernstgenommen wird. Die neu gewonnene Aufmerksamkeit zeigt Wirkung: Der Aspekt der gesellschaftlichen Verantwortung eines Unternehmens erlangt im Rahmen von unternehmerischen Entscheidungen und Handlungen mehr und mehr an Bedeutung.¹⁷

3. CSR und Unternehmensführung – Wechselwirkungen mit dem Compliance Management

- 8 Im Zuge dessen gewinnen auch rechtliche Fragestellungen zunehmend an Bedeutung: Die Unternehmensführung unterliegt schließlich nicht nur einem gesellschaftlichen Legitimitätsprinzip (sog. „licence to operate“),¹⁸ sondern auch einer rechtlich verankerten Legalitäts- und Legalitätskontrollpflicht.¹⁹ Werden diese Pflichten verletzt, indem z.B. gesetzliche Bestimmungen vom Unternehmen, dem Leitungspersonal oder den Mitarbeitern nicht eingehalten werden und/oder das Compliance-Management-System mangelhaft ist, drohen u.U. empfindliche Konsequenzen strafrechtlicher und/oder zivilrechtlicher Art. Es gilt daher zu klären, ob und welche rechtlichen Implikationen CSR auf die Führung eines Unternehmens – insbesondere im Hinblick auf dessen Compliance-Management-System – haben. Da viele Unternehmen weltweit agieren, gewinnen nicht selten sowohl globale CSR-Standards als auch CSR-Normen anderer Nationen sowie sonstige CSR-Themen für ein Unternehmen an Bedeutung.
- 9 Zusammenfassend stellen sich daher insbesondere folgende Fragen:
- Was versteht man unter CSR?
 - In welchem Verhältnis stehen CSR und Corporate Governance?
 - In welchem Verhältnis stehen CSR und Corporate Compliance?
 - Wird CSR überhaupt reguliert? Und wenn ja: Wie wird es reguliert?
 - Inwieweit hat Corporate Compliance CSR-Normen und CSR-Themen zu beachten?
 - Welche Auswirkungen hat CSR auf das Compliance-Risikomanagement?

17 Vgl. dazu vertiefend auch: *Laasch/Suddaby/Freeman/Jamali*, The Research Handbook of Responsible Management; insbesondere: *Carroll/Laasch*, in: *Laasch/Jamali/Freeman/Suddaby* (Hrsg.), The Research Handbook of Responsible Management, S. 84–90. Zum Reputationsmanagement als Bestandteil eines effektiven Compliance Management siehe → *Schulz*, Kap. 1 Rn. 23 ff.

18 Vgl. *Suchanek*, in: *Schneider/Schmidpeter* (Hrsg.), Corporate Social Responsibility, S. 62.

19 Vgl. ausführlich → *Schulz*, Kap. 1 Rn. 2, 36 f.

- Inwieweit hat Corporate Compliance das Reputationsmanagement zu berücksichtigen?²⁰

Im Rahmen dieses Beitrages werden daher unter II. zuerst die Grundlagen zu Corporate Social Responsibility, Corporate Governance und Corporate Compliance einführend dargestellt. Unter III. wird dann die Regulierung von Corporate Social Responsibility beleuchtet. Im Mittelpunkt stehen zum einen die Ansätze und Ebenen von Regulierungsmaßnahmen, zum anderen aber auch deren Umsetzung, die anhand von einschlägigen Regulierungsbeispielen aufgezeigt wird. Anschließend wird unter IV. auf das Zusammentreffen von Corporate Social Responsibility und Corporate Compliance im Unternehmen eingegangen. Neben den Risiken, die für ein Unternehmen durch Corporate Social Responsibility bestehen, wird zudem die Verortung und Integration von Corporate Social Responsibility in die Corporate Compliance näher betrachtet. Der Beitrag schließt unter V. mit einer Zusammenfassung.

II. Grundlagen

1. Corporate Social Responsibility

a) Bedeutungswandel des Begriffsverständnisses

Der Begriff der gesellschaftlichen Verantwortung von Unternehmen hat eine lange Historie. Diese lässt sich – nach den bis dato bekannten Aufzeichnungen – über den Ehrbaren Kaufmann (12. Jahrhundert) bis hin zum 2. Buch Mose (vermutlich 400 v. Chr.) zurückverfolgen.²¹

Im Wandel der Zeit hat sich die Bedeutung dieses Begriffs allerdings stark verändert. Mittlerweile etablierte sich hierfür zwar einheitlich die internationale Bezeichnung „Corporate Social Responsibility (CSR)“. Jedoch fehlt es nach wie vor sowohl an einer gefestigten und abgrenzbaren Konzeption als auch einheitlichen Definition von CSR.²² Votaw bringt es treffend auf den Punkt: „The term [CSR] is a brilliant one; it means something but not always the same thing to everybody. To some it conveys the idea of legal responsibility or liability; to others it means socially responsible behavior in an ethical sense; to still others, the meaning transmitted is that of ‘responsible for’, is a casual mode; many simply equate it with a charitable contribution.“²³

b) Konzeptionen und Modelle

Mit dem „**Four-Part Model of Corporate Social Responsibility**“ hat Carroll 1991 ein CSR-Modell in die CSR-Diskussion eingebracht, das bis zum heutigen

20 Zu diesem Zusammenhang siehe auch → Schulz, Kap. 1 Rn. 23 ff.

21 Votaw, in: Votaw/Sethi (Hrsg.), The Corporate Dilemma, S. 11 f.

22 Schneider, in: Schneider/Schmidpeter (Hrsg.), Corporate Social Responsibility, S. 21 f. und 29, Abb. 1.

23 Votaw, in: Votaw/Sethi (Hrsg.), The Corporate Dilemma, S. 11 f.

Tage an akzeptiert, etabliert sowie stetig weiterentwickelt worden ist. Es handelt sich hierbei um ein Pyramidenkonzept, das aus vier Verantwortlichkeitsebenen besteht, die sich folgendermaßen von unten nach oben aufeinander aufbauen: Economic Responsibility (→ „Required by Society“), Legal Responsibility (→ „Required by Society“), Ethical Responsibility (→ „Expected by Society“) und Philanthropic Responsibility (→ „Desired by Society“). Nach Vorstellung von *Carroll* setzt das Vorliegen einer wahrhaftigen Corporate Social Responsibility voraus, dass ein Unternehmen alle vier genannten Verantwortungsebenen konsekutiv erfüllt.²⁴

- 14 Die **CSR-Reifegradpyramide** von *Schneider* von 2012 stellt dagegen ein aktuelles CSR-Modell mit einer nach oben offenen Skala dar, das u. a. Anleihe an *Carrolls* CSR-Pyramide nahm und diese zeitgemäß weiterentwickelte: Das Fundament der sog. „CSR-Reifegradpyramide“ bildet CSR 0.0, das die passive gesellschaftliche Verantwortung eines Unternehmens (Economic & Legal Responsibility) umfasst. Auf erster Stufe – CSR 1.0 – stehen die philanthropische CSR (Social Sponsoring), das unsystematische Corporate Citizenship sowie lose CSR-Maßnahmen ohne System außerhalb des Kerngeschäfts des Unternehmens. Darauf aufbauend legt die zweite Stufe – CSR 2.0 – mit der unternehmerischen und gesellschaftlichen Wertschöpfung durch ein strategisches, systematisches und integriertes CSR-Management den Fokus auf das Kerngeschäft des Unternehmens. Auf der dritten Stufe – CSR 3.0 – befasst sich dieses Modell schließlich mit dem Unternehmen als proaktivem politischen Gestalter.²⁵
- 15 *Stehr* und *Struve* haben 2017 die CSR-Reifegradpyramide von *Schneider* modifiziert und deren nach oben offene Skala um einen **CSR 4.0-Gedanken** erweitert (vgl. Abb. 1): Darin wird das strategische Corporate Citizenship nicht CSR 1.0, sondern als integraler Bestandteil von CSR 4.0 gesehen. Dieses Verständnis beruht auf dem Gedankengang, dass sich insbesondere internationale Unternehmen bewusst sein müssen, dass sie in einer wechselseitigen Abhängigkeit mit der lokalen Gesellschaft im In- und Ausland stehen – gemäß dem Motto: „Think Global – Act Local“. CSR 4.0 legt den Fokus zudem auf die gelebte Individualethik eines jeden einzelnen Mitarbeiters. Im Sinne eines „Ehrbaren Kaufmanns“ des 21. Jahrhunderts soll deren Verhalten, Einstellung, Gedanken und Überzeugungen dazu beitragen, dass im Unternehmen Veränderungsprozesse angestoßen und Wettbewerbsvorteile generiert werden. Die Führungskräfte tragen zur Implementierung der vom Unternehmen erwünschten Werte bei den Mitarbeitern bei. Auf diese Art und Weise wird die individuelle gesellschaftliche Verantwortung (Personal Social Responsibility, PSR) der Mitarbeiter eines Unternehmens

24 *Carroll*, Business Horizons 1991 (July-August), S. 40 ff., 42, Fig. 3; *Crane/Matten/Glozer/Spence*, Business Ethics, S. 50 f., S. 51, Fig. 2.2; vgl. dazu vertiefend u. a. auch: *Carroll/Brown/Buchholtz*, Business & Society; *Carroll/Shabana*, International Journal of Management Reviews 12 (1), S. 85–105; *Schwartz/Carroll*, Business Ethics Quarterly 13 (4), S. 503–530.

25 *Schneider*, in: *Schneider/Schmidpeter* (Hrsg.), Corporate Social Responsibility, S. 32 ff. und 33, Abb. 2.

bewusst in den Kontext von Individual-, Instituts- und Unternehmensethik gestellt. Ziel ist, dass sich die Mitarbeiter mit ihrem Unternehmen und dessen Unternehmenswerten identifizieren.²⁶ Auf diese Art und Weise können klassische Compliance- und CSR-Management-Systeme zu einem integralen Bestandteil einer jeden Abteilung werden, denn die Mitarbeiter besitzen dann als Wissens- und Werteträger eines Unternehmens bereits vermittelte Werte, die sie im Kontext CSR und Compliance einbringen und anwenden können.²⁷

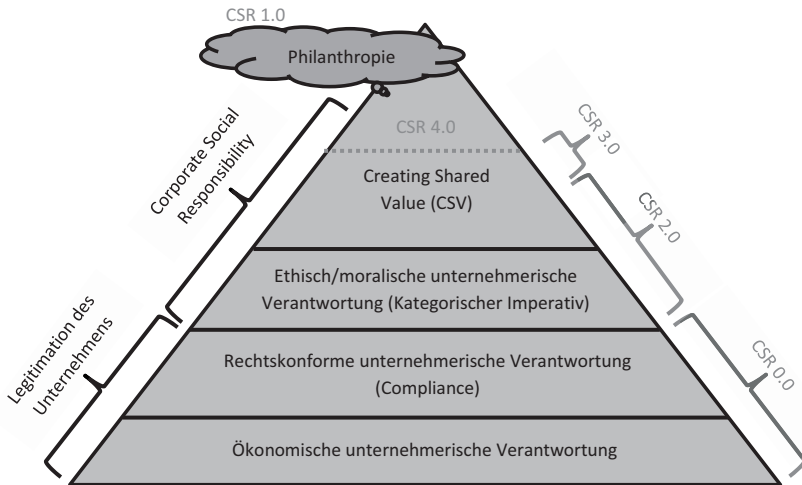


Abbildung 1: Integration des CSR 4.0-Gedankens in die CSR-Pyramide (Stehr/Struve [2017], S. 359, Abb. 7)

c) Definitionen

Nachdem die **Europäische Union** die CSR zu ihrem Anliegen gemacht hatte,²⁸ veröffentlichte die Europäische Kommission 2001 hierzu ihr Grünbuch „Europäische Rahmenbedingungen für die soziale Verantwortung von Unternehmen“.²⁹ Die darin enthaltene CSR-Definition verstand CSR „als ein Konzept, das den Unternehmen als Grundlage dient, auf freiwilliger Basis soziale Belange

16

26 Vgl. dazu u. a. auch das „Total Social Impact“-Konzept: Boston Consulting Group Online v. 25.10.2017, <https://www.bcg.com/publications/2017/total-societal-impact-new-lens-strategy.aspx> (zuletzt abgerufen am 29.2.2024); Karl-Heinz Land Online, <https://karlheinland.com/erde-5-0-total-societal-impact-statt-shareholder-value/> (zuletzt abgerufen am 29.2.2024).

27 Stehr/Struve, in: Schulz (Hrsg.), Compliance Management im Unternehmen, 1. Aufl., 2017, S. 357 ff.

28 KOM (2001) 366 endgültig, S. 3, Rn. 6.

29 KOM (2001) 366 endgültig.

und Umweltbelange in ihre Unternehmenstätigkeit und in die Wechselbeziehungen mit den Stakeholdern zu integrieren“.³⁰ Die Erkenntnisse und Folgen aus bzw. durch die Wirtschafts- und Finanzkrise veranlasste die Europäische Kommission jedoch dazu, die Strategie zur Förderung von CSR in der EU zu überdenken und zu erneuern.³¹ Im Zuge dessen wurde „Eine neue Strategie (2011–14) für die soziale Verantwortung der Unternehmen (CSR)“ erarbeitet und 2011 vorgestellt.³² Das Fundament dazu bildet ein modernes Verständnis von CSR, das von der allein auf Freiwilligkeit basierenden CSR-Konzeption abrückte und so zu einem Paradigmenwechsel im CSR-Verständnis der Europäischen Union führte.³³ Nach der neuen EU-Definition von CSR versteht man unter CSR nun die „Verantwortung von Unternehmen für ihre Auswirkungen auf die Gesellschaft“.³⁴

- 17 Nachdem die Internationale Organisation für Normung ihren **Leitfaden zur gesellschaftlichen Verantwortung von Organisationen (ISO 26000)** im Jahre 2010 veröffentlicht hatte, entwickelte sich die darin enthaltene Definition von „Social Responsibility“ zu einer globalen CSR-Definitionsbasis.³⁵ Dies ist zum einen darauf zurückzuführen, dass dieser freiwillige internationale Standard nicht nur für Unternehmen, sondern für alle Arten von Organisationen in allen Ländern der Welt anwendbar ist; zum anderen, dass er allen Organisationen einen praktischen Orientierungsrahmen – bestehend aus der Definition und Beschreibung grundlegender Prinzipien, Kernthemen und Handlungsfeldern – anbietet, der für die Wahrnehmung und Gestaltung gesellschaftlicher Verantwortung notwendig und erforderlich ist.³⁶ Gemäß der deutschen Übersetzung versteht man unter Social Responsibility die „Verantwortung einer Organisation für die Auswirkungen ihrer Entscheidungen und Aktivitäten auf die Gesellschaft und die Umwelt durch transparentes und ethisches Verhalten, das zur nachhaltigen Entwicklung, Gesundheit und Gemeinwohl eingeschlossen, beiträgt, die Erwartungen der Anspruchsgruppen berücksichtigt, anwendbares Recht einhält und im Einklang mit internationalen Verhaltensstandards steht und in der gesamten Organisation integriert ist und in ihren Beziehungen gelebt wird. Anmerkung 1: Aktivitäten umfassen Produkte, Dienstleistungen und Prozesse. Anmerkung 2: Mit Beziehungen sind solche gemeint, die im Zusammenhang mit den Aktivitäten der Organisation innerhalb ihres Einflussbereichs (2.19) entstehen“.³⁷

30 KOM (2001) 366 endgültig, S. 7, Rn. 20.

31 KOM (2011) 681 endgültig, S. 7.

32 KOM (2011) 681 endgültig.

33 KOM (2011) 681 endgültig, S. 7; *Spießhofer*, Unternehmerische Verantwortung, S. 277.

34 KOM (2011) 681 endgültig, S. 7.

35 *Schneider*, in: *Schneider/Schmidpeter* (Hrsg.), *Corporate Social Responsibility*, S. 27.

36 *Schmiedeknecht/Wieland*, in: *Schneider/Schmidpeter* (Hrsg.), *Corporate Social Responsibility*, S. 299.

37 DIN ISO 26000, Ausgabedatum 2011-01, S. 17.

2. Corporate Governance

a) Begriffsverständnis

„Corporate Governance“ kann dem Kern seiner Bedeutung nach am ehesten mit dem Begriff „Unternehmensverfassung“ ins Deutsche übersetzt werden. Im Grundsatz versteht man unter Corporate Governance „den rechtlichen und faktischen Ordnungsrahmen für die [gute und verantwortungsvolle] Leitung und Überwachung eines Unternehmens“.³⁸ 18

Die Corporate Governance soll „zur Schaffung eines Umfelds von Vertrauen, Transparenz und Rechenschaftspflicht beitragen, wie es nötig ist, um langfristige Investitionen, Finanzstabilität sowie Geschäftsintegrität zu fördern und so ein stärkeres Wachstum und eine inklusivere Gesellschaft möglich zu machen“.³⁹ 19

b) Corporate Governance und Corporate Social Responsibility

Wie bereits die Erläuterungen zur Begrifflichkeit und zum Zweck der Corporate Governance erahnen lassen, haben Corporate Social Responsibility und Corporate Governance über die Corporate Responsibility gemeinsame Wurzeln (vgl. dazu Abb. 2):⁴⁰ 20

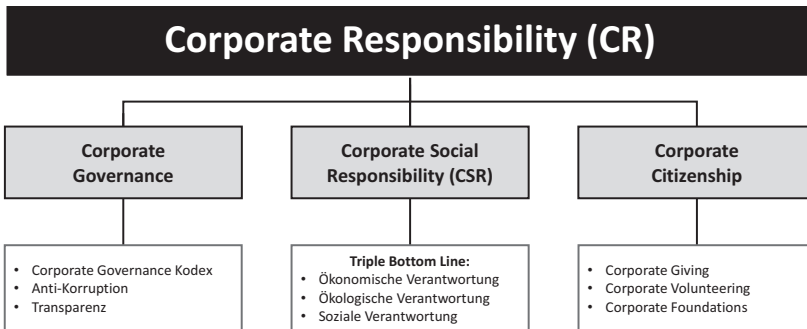


Abbildung 2: Corporate Responsibility und deren Abgrenzung (in Anlehnung an: Bay [2010], ISO 26000 in der Praxis, S. 4, Abb. 1)

38 Vgl. Deutscher Corporate Governance Kodex in der Fassung vom 28.4.2022, S. 2 f., https://www.dcgk.de/files/dcgk/usercontent/de/download/kodex/220627_Deutscher_Corporate_Governance_Kodex_2022.pdf (zuletzt abgerufen am 29.2.2024); Schewe, Unternehmensverfassung, S. 8 ff.

39 Vgl. G20/OECD-Grundsätze der Corporate Governance, OECD-Library Online v. 23.12.2015, S. 7, https://www.oecd-ilibrary.org/governance/g20-oecd-grundsätze-der-corporate-governance_9789264250130-de (zuletzt abgerufen am 29.2.2024).

40 Vgl. u. a. auch Brammer/Pavelin, in: Wrieth/Siegel/Keasey/Filatotchev (Hrsg.), The Oxford Handbook of Corporate Governance, S. 719 ff.; Sahut/Peris-Ortiz/Teulon, Journal of Management and Governance 23, S. 901 ff.

- 21 Nach *Buchholtz et al.* stellen u.a. die folgenden vier Themenkomplexe die Hauptdiskussionsfelder zwischen Corporate Social Responsibility und Corporate Governance dar:⁴¹
- „Defining the purpose of contemporary firms (Does the firm exist only for shareholders?),
 - Evaluating the nature of the professional (senior) manager (Are managers really opportunistic and self-serving?),
 - Questioning the relevance of a range of features of boards of directors for CSR (Does board composition and structure matter for CSR?), and
 - Evaluating the processes whereby individuals obtain board positions (Are selection and appointment processes sufficiently open and how effectively can the voice of shareholders be heard?).“
- 22 Es zeigt sich, dass die Corporate Governance aus insgesamt zwei Perspektiven betrachtet werden sollte:
- Zum einen aus der Innenansicht, die sich mit den Rollen, Kompetenzen, Funktionsweisen und dem Zusammenwirken der Organe eines Unternehmens befasst. Zentrale Bedeutung erlangt dabei u.a. der Bereich der Regelung und Überwachung des Prinzipal-Agent-Verhältnisses, das gerade in Personenvereinigungen – wie z.B. der Aktiengesellschaft – durch die Trennung von Eigentum am Unternehmen (Aktionäre/Gesellschafter) und Leitung des Unternehmens (Vorstand/Geschäftsführer) entsteht. In diesem Zusammenhang steht die Vermeidung von Interessenskonflikten sowie die Gestaltung von Kontroll- und Anreizsystemen im Mittelpunkt der Betrachtung.⁴²
 - Zum anderen aber auch aus der Außenansicht, die sich mit dem Verhältnis zwischen Unternehmensführung und den wesentlichen Stakeholdern – insbesondere der Shareholder – eines Unternehmens beschäftigt. Im Mittelpunkt steht an dieser Stelle u.a. die Bedeutung der gesellschaftlichen Verantwortung eines Unternehmens im Rahmen von strategischen Unternehmensentscheidungen und dem Risikomanagement.⁴³
- 23 Aktuell ist zu beobachten, dass dem Thema CSR auch im Rahmen der Ausgestaltung und Umsetzung von Corporate Governance Maßnahmen in Unternehmen immer größere Bedeutung beigemessen wird. Das zeigt sich z.B. beim „Code of Conduct“ eines Unternehmens.⁴⁴ Hierbei handelt es sich um einen Ko-

41 Vgl. *Brammer/Pavelin*, in: *Wright/Siegel/Keasey/Filatov* (Hrsg.), *The Oxford Handbook of Corporate Governance*, S. 720; *Buchholtz/Brown/Shabana*, in: *Crane/McWilliams/Matten/Moon* (Hrsg.), *The Oxford Handbook of Corporate Social Responsibility*, S. 327 ff.

42 Vgl. *Joost*, *Die Prinzipal-Agenten-Theorien in der Betriebswirtschaft*, S. 11 ff.; *Saenger*, *Gesellschaftsrecht*, Rn. 525.

43 Vgl. *Sahut/Peris-Ortiz/Teulon*, *Journal of Management and Governance* 23, S. 11 ff.; *Brammer/Pavelin*, in: *Wright/Siegel/Keasey/Filatov* (Hrsg.), *The Oxford Handbook of Corporate Governance*, S. 719 ff.; *Saenger*, *Gesellschaftsrecht*, Rn. 525.

44 Vgl. zum Code of Conduct ausführlich → *Benkert*, Kap. 4.

dex, der die Führungskräfte, Mitarbeiter und ggf. Geschäftspartner eines Unternehmens zu einem bestimmten Verhalten verpflichten soll.⁴⁵ Diese Entwicklung ist u. a. auf staatliche Regulierungsmaßnahmen zurückzuführen, wie z. B. dem deutschen Lieferkettensorgfaltspflichtengesetz.⁴⁶ Im Ergebnis hat diese Entwicklung letztlich auch Auswirkungen auf die Ausgestaltung und Umsetzung von unternehmensinternen Kontroll- und Sicherungssystemen – insbesondere dem Compliance-Management-System (CMS) eines Unternehmens.

c) Gesellschaftsrecht und Deutscher Corporate Governance Kodex

Die gesetzliche Regulierung von privatrechtlichen Körperschaften (Grundform: Verein; weitere Formen: u. a. Aktiengesellschaft [AG] und Gesellschaft mit beschränkter Haftung [GmbH]) erfolgt über das Gesellschaftsrecht.⁴⁷ Wie folgende Wesenszüge zeigen, erlangt die Corporate Governance gerade bei privatrechtlichen Körperschaften eine besonders hohe Relevanz:⁴⁸

- Körperschaften wurden für einen häufigen Wechsel ihrer Mitglieder bzw. Gesellschafter konzipiert. Aus diesem Grund weisen sie nur einen geringen Grad an mitgliedschaftlicher Bindung auf. Dies führt zu einer weitreichenden Selbstständigkeit der Körperschaft von ihren Mitgliedern. Diesem Leitbild folgend erlangt ein Gesellschafter – insbesondere in kapitalmarktorientierten Körperschaften wie der Aktiengesellschaft (AG) – primär nur in seiner Eigenschaft als Kapitalgeber – weniger als Person – an Bedeutung.
- Körperschaften beruhen auf einem Gesellschaftsvertrag in Form einer Satzung, die (a) von den gesetzlichen Vorschriften nur abweichen darf, wenn dies ausdrücklich zugelassen ist (sog. „Satzungsstrenge“), (b) von den Gesellschaftern beschlossen wird sowie (c) einer notariellen Beurkundung bedarf. Körperschaften sind i. d. R. in ein Register einzutragen.
- Körperschaften verfügen über eine eigene Rechtspersönlichkeit. Als juristische Person sind sie nicht nur Träger von Rechten und Pflichten, sondern auch Träger des Gesellschaftsvermögens. Wie für Kapitalgesellschaften charakteristisch, ist die Haftung einer Aktiengesellschaft auf das Vermögen der Gesellschaft beschränkt (sog. „Haftungsexklusivität“).
- Körperschaften haben Organe. Bei einer Aktiengesellschaft sind dies die Hauptversammlung, der Aufsichtsrat und der Vorstand. Im Grundsatz wird die Gesellschaft durch den Vorstand (Management) geführt, nicht durch die Aktionäre (Eigentümer). Der Aufsichtsrat wird von der Hauptversammlung eingesetzt, um den Vorstand zu kontrollieren. Damit liegt bei Körperschaften i. d. R. eine Dritt- oder Fremdorganschaft vor.

45 Zur Gestaltung eines Code of Conduct siehe → *Benkert*, Kap. 4.

46 Vgl. BT-Drs. 19/28649, S. 46. Zum LkSG → *Heske*, Kap. 18.

47 Vgl. *Saenger*, Gesellschaftsrecht, Rn. 3 ff., 11 ff.

48 Vgl. *Saenger*, Gesellschaftsrecht, Rn. 11 ff.; *Grigoleit*, Aktiengesetz, § 1 AktG Rn. 1 ff.

- 25 Neben den gesetzlichen Normierungen des Gesellschaftsrechts erlangt der Deutsche Corporate Governance Kodex (DCGK) – ein Verhaltenskodex, der von einer staatlich eingesetzten Regierungskommission formuliert wird, jedoch keinen eigenen Gesetzescharakter innehat – an Bedeutung, insbesondere für Gesellschaften, die an deutschen Börsen notiert sind, denn:⁴⁹
- 26 Nach § 161 Abs. 1 Satz 1 AktG (sog. „Entsprechungsklausel“) haben Vorstand und Aufsichtsrat börsennotierter Gesellschaften jährlich zu erklären, dass den aktuellen Empfehlungen der Regierungskommission Deutscher Corporate Governance Kodex entsprochen wurde und wird oder welche Empfehlungen nicht angewendet wurden oder werden und warum nicht (sog. „comply or explain“). Gemäß § 161 Abs. 2 AktG ist diese Erklärung zudem auch auf der Internetseite der jeweiligen Gesellschaft dauerhaft öffentlich zugänglich zu machen.
- 27 Mit Hilfe dieser rechtlichen Konstruktion wird nicht nur versucht, eine Art „Best Practice“ der Unternehmensführung zu formulieren und diese in die Corporate Governance deutscher Unternehmen zu implementieren, sondern auch das duale deutsche Corporate-Governance-System per se „transparent und nachvollziehbar zu machen“.⁵⁰ Der DCGK baut auf den folgenden drei Elementen auf: (1) Verbindliche gesetzliche Vorschriften zur Unternehmensführung, (2) nicht-verbindliche Empfehlungen und (3) nicht-verbindliche Anregungen. Die Empfehlungen und Anregungen wurden aus international und national anerkannten Standards guter und verantwortungsvoller Unternehmensführung gebildet.⁵¹ Auf diese Art und Weise trägt DCGK dazu bei, die Ausdifferenzierung der deutschen Regulierung von Corporate-Governance-Systemen in den Bereichen (a) Leitung und Überwachung, (b) Besetzung des Vorstands, (c) Zusammensetzung des Aufsichtsrats, (d) Arbeitsweise des Aufsichtsrats, (e) Interessenskonflikte, (f) Transparenz und externe Berichterstattung sowie (g) Vergütung von Vorstand und Aufsichtsrat nachhaltig weiter voranzutreiben.⁵²

49 Saenger, Gesellschaftsrecht, Rn. 523, 572; vgl. Deutscher Corporate Governance Kodex in der Fassung vom 28.4.2022, S. 3, https://www.dcgk.de/files/dcgk/usercontent/de/download/kodex/220627_Deutscher_Corporate_Governance_Kodex_2022.pdf (zuletzt abgerufen am 29.2.2024): Empfehlungen und Anregungen des Kodex mögen nicht-kapitalmarktorientierten Gesellschaften zur Orientierung dienen, aus dem Aufsichtsrecht ergeben sich für die Corporate Governance börsennotierter Kreditinstitute und Versicherungsunternehmen zudem weitere Besonderheiten.

50 Vgl. Regierungskommission Deutscher Corporate Governance Kodex, <https://www.dcgk.de/de/kodex.html> (zuletzt abgerufen am 4.2.2024).

51 Vgl. Regierungskommission Deutscher Corporate Governance Kodex, <https://www.dcgk.de/de/kodex.html> (zuletzt abgerufen am 4.2.2024); Saenger, Gesellschaftsrecht, Rn. 523, 572.

52 Vgl. Deutscher Corporate Governance Kodex in der Fassung vom 28.4.2022, S. 1 und Regelungsabschnitte, https://www.dcgk.de/files/dcgk/usercontent/de/download/kodex/220627_Deutscher_Corporate_Governance_Kodex_2022.pdf (zuletzt abgerufen am 29.2.2024).

Dabei ist bemerkenswert, dass nach der Präambel des DCGK nicht nur die Legalität von Vorstand (Leitungsorgan) und Aufsichtsrat (Aufsichtsorgan) als relevant erachtet werden, sondern auch ein ethisch fundiertes und eigenverantwortliches Verhalten nach dem Leitbild des Ehrbaren Kaufmanns.⁵³ Eine Bezugnahme auf CSR enthält Grundsatz 13 des DCGK, der für eine gute Unternehmensführung offene Diskussionen zwischen Vorstand und Aufsichtsrat sowie in Vorstand und Aufsichtsrat voraussetzt. Dabei haben sich „die Gesellschaft und ihre Organe [...] in ihrem Handeln [stets] der Rolle des Unternehmens in der Gesellschaft und ihrer gesellschaftlichen Verantwortung bewusst zu sein“.⁵⁴ Für den verantwortungsvollen Umgang mit den Risiken der Geschäftstätigkeit bedarf es nach Grundsatz 4 des DCGK eines angemessenen und wirksamen internen Kontroll- und Risikomanagementsystems. Dem Grundsatz 5 des DCGK folgend hat der Vorstand darüber hinaus für die Einhaltung der gesetzlichen Bestimmungen und internen Richtlinien zu sorgen und auf deren Beachtung im Unternehmen (Compliance) hinzuwirken. Gemäß Grundsatz 22 des DCGK hat eine Gesellschaft ihren Anteilseignern und Dritten gegenüber bestimmte Transparenz- und Berichterstattungspflichten zu erfüllen, welchen sie u. a. durch eine CSR-Berichterstattung nachkommen kann.⁵⁵

3. Corporate Compliance

a) Begriffsverständnis

Unter dem Begriff „Compliance“ versteht man die Einhaltung und Übereinstimmung mit Regelwerken, d. h. „i. d. R. mit staatlichen Gesetzen und der unternehmensinternen Regelwelt“.⁵⁶

Unter Corporate Compliance versteht man „eine präventiv wirkende und das Risiko der Haftung des Unternehmens bzw. der Unternehmensleitung minimierenden Unternehmensorganisation“.⁵⁷ Die Primärziele der Corporate Compliance sind (a) Verringerung von Haftungsrisiken und (b) Vermeidung von Schadenser-

53 Vgl. Deutscher Corporate Governance Kodex in der Fassung vom 28.4.2022, S. 2, https://www.dcgk.de/files/dcgk/usercontent/de/download/kodex/220627_Deutscher_Corporate_Governance_Kodex_2022.pdf (zuletzt abgerufen am 29.2.2024).

54 Vgl. Deutscher Corporate Governance Kodex in der Fassung vom 28.4.2022, S. 2, https://www.dcgk.de/files/dcgk/usercontent/de/download/kodex/220627_Deutscher_Corporate_Governance_Kodex_2022.pdf (zuletzt abgerufen am 29.2.2024).

55 Vgl. Deutscher Corporate Governance Kodex in der Fassung vom 28.4.2022, S. 16, https://www.dcgk.de/files/dcgk/usercontent/de/download/kodex/220627_Deutscher_Corporate_Governance_Kodex_2022.pdf (zuletzt abgerufen am 29.2.2024).

56 *Knierim*, in: Wabnitz/Janovsky/Schmitt (Hrsg.), Handbuch Wirtschafts- und Steuerstrafrecht, Kap. 5 Rn. 5; dazu auch einführend: → *Schulz*, Kap. 1 Rn. 1.

57 Vgl. *Knierim*, in: Wabnitz/Janovsky/Schmitt (Hrsg.), Handbuch Wirtschafts- und Steuerstrafrecht, Kap. 5 Rn. 7. Siehe zu Begriffsverständnis und -entwicklung auch → *Schulz*, Kap. 1 Rn. 1 ff.

satzpflichten, Bußgeldern und Reputationsschäden für das Unternehmen durch unternehmerische Handlungen.⁵⁸

- 31 Zwar haben viele Unternehmen bereits ein Compliance-Management-System (CMS) in ihre Unternehmensorganisation implementiert.⁵⁹ Gleichwohl kann selbst ein effektives Compliance-Management-System nicht garantieren, dass jeglicher Compliance-Verstoß verhindert wird, denn „[...] auch ein Optimum an Compliance [kann] nicht verhindern [...], dass einzelne Leitungspersonen Straftaten begehen“.⁶⁰ Hinzu kommt, dass auf Unternehmen täglich neue Herausforderungen warten, die u.U. die Corporate Compliance-Organisation in ihrem Aufbau, aber auch in ihrer täglichen Arbeit maßgeblich verändern und erhebliche Anpassung erfordern.⁶¹ Neue Herausforderungen folgen vermehrt auch aus dem Trend der zunehmenden „Verrechtlichung von CSR“.⁶² Das betrifft aktuell im erheblichen Maße z.B. Corporate Compliance-Organisation von Unternehmen, die unter das Lieferkettensorgfaltspflichtengesetz (LkSG) fallen.⁶³ Im Ergebnis wird bereits an dieser Stelle deutlich, dass aufgrund der Individualität und des individuellen Risikoprofils eines jeden Unternehmens eine sog. „One-Size-Fits-All“-Lösung einer Corporate Compliance-Organisation für alle Unternehmen grundsätzlich ausscheidet.⁶⁴

b) Corporate Compliance und Corporate Governance

- 32 Die Corporate Governance befasst sich u.a. mit den Regelungen, die die Kontroll- und Risikomanagementsysteme eines Unternehmens betreffen. Da die Corporate Compliance eines dieser Kontroll- und Risikosysteme darstellt, konstituiert die Corporate Governance folglich konkrete Regelungen zur Rolle sowie den Rechten und Pflichten der Corporate Compliance in einem Unternehmen. Zur Aufgabe der Corporate Compliance zählt es nun insbesondere, die

58 *Saenger*, Gesellschaftsrecht, Rn. 573; zu den Funktionen von Compliance und Compliance Management ausführlich → *Schulz*, Kap. 1 Rn. 13 ff.

59 Vgl. dazu exemplarisch die drei Anforderungen der Wirksamkeit, Dauerhaftigkeit und Unabhängigkeit an die Organisation und den Aufbau einer Compliance-Funktion von Wertpapierdienstleistungsunternehmen nach § 80 Abs. 1 WpHG i.V.m. Art. 22 DV; weiterführend dazu: *Schäfer*, in: *Krimphove/Kruse* (Hrsg.), *MaComp*, BT 1, Rn. 602 f., 606 ff., 769 ff., 866 ff.

60 Vgl. dazu aus dem Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz eines „Gesetzes zur Stärkung der Integrität in der Wirtschaft“ (Bearbeitungsstand: 22.4.2020), S. 95, https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/RefE_Staerkung_Integritaet_Wirtschaft.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 29.2.2024).

61 Vgl. dazu exemplarisch: *Birnbaum*, in: *Krimphove/Kruse* (Hrsg.), *MaComp*, Einleitung, Rn.1 f., Rn. 27 ff. Siehe zur notwendigen Aktualisierung des Compliance Managements ferner → *Schulz*, Kap. 1 Rn. 89, 103.

62 Vgl. *Teicke*, CCZ 2018, 274 f. sowie → *Schulz*, Kap. 1 Rn. 3 ff.; ebenso: *Kleinfeld*, ZRFC 2023, 295 ff.

63 Vgl. *Wurzberger/Nagel*, ZRFC 2023, 325 ff.; *Wurzberger/Nagel*, ZRFC 2023, 366 ff.

64 Vgl. dazu u. a. → *Schulz*, Kap. 1 Rn. 49, 60 ff.

Vorgaben aus der Corporate Governance aufzunehmen und entsprechend umzusetzen und auszugestalten.

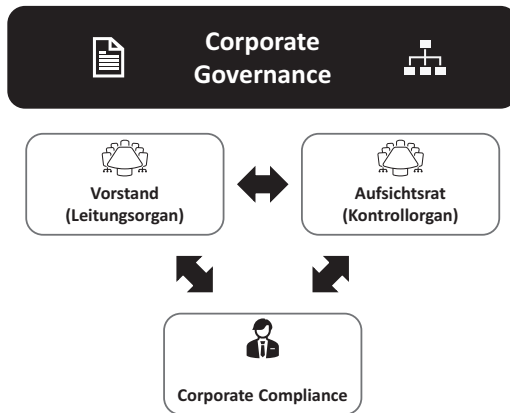


Abbildung 3: Corporate Governance gibt Regelungen über die Zusammenarbeit von Vorstand, Aufsichtsrat und Corporate Compliance in einem Unternehmen vor (eigene Darstellung)

Um zu gewährleisten, dass die für das Unternehmen agierenden Personen geltendes Recht bzw. bestimmte Regeln oder Gebote, die im Interesse des Unternehmens liegen, möglichst optimal einhalten, kann die Unternehmensleitung bestimmte Compliance-Maßnahmen (wie z.B. die Erarbeitung und Umsetzung von Verhaltensstandards) an die Compliance-Organisation delegieren.⁶⁵ Der Zusammenhang zwischen Corporate Compliance und Corporate Governance wird ferner dadurch deutlich, dass auch der Aufsichtsratsvorsitzende einer Aktiengesellschaft in bestimmten Fällen u. a. berechtigt ist, Informationen über Compliance-Themen direkt beim Chief Compliance Officer zu erfragen.⁶⁶ Neben den gesetzlichen und aufsichtsrechtlichen Vorgaben finden sich i. d. R. noch weitere individuelle unternehmensinterne Regelungen in der Corporate Governance, die in der Zusammenschau das Verhältnis zwischen Leitungsorgan, Aufsichtsorgan und Compliance-Organisation in einem Unternehmen konstituieren und versuchen zu konkretisieren (vgl. Abb. 3).

c) Corporate Compliance als Organisationspflicht

Wie das Beispiel der Aktiengesellschaft zeigt, lässt sich die Corporate Compliance als Organisationspflicht nicht nur aus Gesetzen (wie z. B. §§ 91 Abs. 3, 93

⁶⁵ Saenger, Gesellschaftsrecht, Rn. 573. Zu Delegationsfragen siehe → Schulz, Kap. 1 Rn. 56 f.

⁶⁶ Schäfer, in: Krimphove/Kruse (Hrsg.), MaComp, BT 1, Rn. 35a ff.

Abs. 1 AktG, §§ 30, 130, 9 OWiG, §§ 13, 14 StGB), sondern auch aus Rechtsprechungsgrundsätzen (vgl. insbesondere das Urteil zu „Siemens/Neubürger“⁶⁷ sowie das Urteil zur „Pflicht des Geschäftsführers zur Schaffung von Compliance-Strukturen“⁶⁸) ableiten.⁶⁹

d) Aktuelle gesetzliche Entwicklungen in Deutschland und der Europäischen Union

- 35** In der 19. Wahlperiode wurde auf Initiative der damaligen Bundesregierung der Entwurf eines „Gesetz[es] zur Stärkung der Integrität in der Wirtschaft“ in das Gesetzgebungsverfahren des Bundestages eingebracht. Bis zum Ablauf der Wahlperiode konnte für diesen Gesetzentwurf jedoch keine politische Mehrheit gewonnen werden, wodurch die Gesetzesinitiative für ein „Verbandssanktionengesetz“ im Ergebnis scheiterte.⁷⁰ Die Bundesregierung der 20. Wahlperiode griff das Thema „Unternehmenssanktionen“ erneut in ihren Koalitionsvertrag auf. Im Abschnitt „Unternehmensrecht“ findet sich dort zu lesen: „Wir schützen ehrliche Unternehmen vor rechtsuntreuen Mitbewerberinnen und Mitbewerbern. Wir überarbeiten die Vorschriften der Unternehmenssanktionen einschließlich der Sanktionshöhe, um die Rechtssicherheit von Unternehmen im Hinblick auf Compliance-Pflichten zu verbessern und für interne Untersuchungen einen präzisen Rechtsrahmen zu schaffen.“⁷¹ Bis dato hat die aktuelle Bundesregierung jedenfalls weder eine entsprechende Initiative für ein „Verbandssanktionengesetz“ ins Gesetzgebungsverfahren des Bundestages eingebracht noch entsprechende Andeutungen gemacht, dies bis zum Ende der Legislaturperiode noch tun zu wollen. Grundsätzlich bleibt neben der Einführung eines Verbandssanktionengesetzes auch eine entsprechende Anpassung des Ordnungswidrigkeitenrechts weiterhin denkbar.
- 36** Neben dem Entwurf eines Verbandssanktionengesetzes brachte die Bundesregierung u. a. aber auch den Entwurf eines „Gesetz[es] über die unternehmerischen Sorgfaltspflichten in der Lieferkette“ (sog. „Lieferkettensorgfaltspflichtengesetz“, LkSG) in den Bundestag ein. Nachdem für diese Initiative eine politische Mehrheit im Gesetzgebungsverfahren gefunden und das Gesetz verabschiedet werden konnte, trat es am 1.1.2023 in Deutschland in Kraft.⁷² § 3

67 Vgl. Landgerichts München I, Urt. v. 10.12.2013 – 5 HK O 1387/10 sowie hierzu siehe auch → *Schulz*, Kap. 1 Rn. 39.

68 Vgl. OLG Nürnberg, Urt. v. 30.3.2022 – 12 U 1520/19 sowie → *Schulz*, Kap. 1 Rn. 40.

69 *Knierim*, in: Wabnitz/Janovsky/Schmitt (Hrsg.), Handbuch Wirtschafts- und Steuerstrafrecht, Kap. 5 Rn. 47; *Hauschka/Moosmayer/Lösler*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 1 Rn. 28 ff., Rn. 30 ff., Rn. 33 ff. Zur Compliance-Organisationspflicht siehe auch → *Schulz*, Kap. 1 Rn. 27 ff.

70 Vgl. Vorgang zum Gesetzgebungsverfahren: <https://dip.bundestag.de/vorgang/gesetz-zur-st%C3%A4rkung-der-integrit%C3%A4t-in-der-wirtschaft/265689> (zuletzt abgerufen am 29.2.2024).

71 Vgl. Koalitionsvertrag, S. 111.

72 Zum LkSG ausführlich → *Heske*, Kap. 18.

Abs. 1 LkSG verpflichtet die adressierten Unternehmen nunmehr dazu, bestimmte menschenrechtliche und umweltbezogene Sorgfaltspflichten in angemessener Weise in ihren Lieferketten (sowie im eigenen Geschäftsbereich) mit dem Ziel zu beachten, menschenrechtliche oder umweltbezogene Risiken vorzubeugen oder sie zu minimieren oder die Verletzung menschenrechtsbezogener oder umweltbezogener Pflichten zu beenden. Die Sorgfaltspflichten enthalten neben der Einrichtung eines Risikomanagements auch die Festlegung einer betriebsinternen Zuständigkeit, die Durchführung regelmäßiger Risikoanalysen, die Abgabe einer Grundsatzerklärung, die Verankerung von Präventionsmaßnahmen im eigenen Geschäftsbereich und gegenüber unmittelbaren Zulieferern, das Ergreifen von Abhilfemaßnahmen, die Einrichtung eines Beschwerdeverfahrens, die Umsetzung von Sorgfaltspflichten in Bezug auf Risiken bei mittelbaren Zulieferern sowie eine fortlaufende unternehmensinterne Dokumentation als auch eine unternehmensexterne Berichterstattung. Verstöße gegen das LkSG können betroffene Unternehmen teuer zu stehen kommen: Nach § 22 Abs. 3 LkSG kann eine juristische Person oder Personenvereinigung mit einem durchschnittlichen Jahresumsatz von mehr als 400 Mio. EUR mit einer Geldbuße bis zu 2 % des durchschnittlichen Jahresumsatzes sanktioniert werden. Compliance-Maßnahmen, die bereits vor einem sanktionierten Verstoß getroffen worden sind, können sich mindernd auf die Bemessung der Geldbuße auswirken. Zum jetzigen Zeitpunkt wird insbesondere von Seiten der Unternehmen das LkSG sehr kritisch betrachtet. Es wird u. a. vertreten, dass die Politik „ihre Verantwortung nicht an die Wirtschaft auslagern [kann]“. ⁷³ Hinzu kommt, dass inzwischen immer deutlicher wird, dass dieses Gesetz lediglich eingeschränkt wirksam wird. Das sieht man u. a. daran, wenn das LkSG auf die Lebenswirklichkeit in globalen Lieferketten trifft. ⁷⁴

Mit Blick auf die aktuellen gesetzlichen Entwicklungen auf Ebene der Europäischen Union gilt es zum einen die „Corporate Sustainability Reporting Directive“ (CSRD) hervorzuheben, die mit den „European Sustainability Reporting Standards“ (ESRS) zugleich klar definierte europäische Berichtsstandards mit sich bringt. Die CSRD stellt eine EU-Richtlinie zur Unternehmensnachhaltigkeitsberichterstattung dar, die am 5.1.2023 in Kraft trat und nun in einem Zeitraum von 18 Monaten von den Mitgliedstaaten umgesetzt werden muss. ⁷⁵ Da Verstöße gegen die CSRD-Berichterstattungspflichten zu Sanktionen führen können, erlangt diese EU-Richtlinie auch Bedeutung für die Compliance von Unternehmen. Zum anderen gilt es noch die „Corporate Sustainability Due Diligence Directive“ (CSDDD), die sog. „Europäische Lieferkettenrichtlinie“, zu er-

⁷³ Vgl. Lebensmittelzeitung Online v. 8.2.2024, <https://www.lebensmittelzeitung.net/politik/nachrichten/interview-mit-raoul-rossmann-und-christoph-werner-die-politik-kann-ihre-verantwortung-nicht-an-die-wirtschaft-auslagern-175996> (zuletzt abgerufen am 29.2.2024).

⁷⁴ Vgl. Rudkowski/Manzanza Lumingo, RdA 2023, 291.

⁷⁵ Vgl. u. a. <https://www.csr-in-deutschland.de/DE/CSR-Allgemein/CSR-Politik/CSR-in-der-EU/Corporate-Sustainability-Reporting-Directive/corporate-sustainability-reporting-directive-art.html> (zuletzt abgerufen am 29.2.2024).

wählen. Hierbei handelt es sich um eine europäische Richtlinie zum Schutz von Menschenrechten und Umwelt in Liefer- und Wertschöpfungsketten, die Unternehmen noch weitreichender als das deutsche Lieferkettensorgfaltspflichtengesetz in die Pflicht nehmen wird. Für Verstöße von Unternehmen sind in der CSDDD ebenfalls Sanktionen vorgesehen worden.⁷⁶

III. Corporate Social Responsibility und Regulierungsebenen

1. Einführung in die CSR-Regulierung

- 38** Über die letzten Jahrzehnte hinweg wurde eine Vielzahl an CSR-Konzeptionen erarbeitet, die privat- und/oder öffentlich-rechtlich normiert worden sind. Unternehmen stehen sodann häufig vor der Frage, ob und wie diese CSR-Normen nun Geltung für sie erlangt haben.

a) Regulierungsebenen

- 39** Mit Einordnung der Organisationen, die diese CSR-Normierungen erlassen und in Kraft gesetzt haben, in das Gefüge der geltenden Völkerrechtsordnung, lassen sich aus der Perspektive Deutschlands folgende Regulierungsebenen herausarbeiten:⁷⁷
- **Nationale Regulierungsebene** (beispielsweise Normierungen auf Bundesebene)
 - **Supranationale Regulierungsebene** (insbesondere Normierungen der Europäischen Union)
 - **Internationale Regulierungsebene** (beispielsweise Normierungen von UN)
 - **Globale Regulierungsebene** (beispielsweise Normierungen der UN oder OECD)
- 40** Daneben gibt es noch diverse privatrechtliche Vereinigungen und/oder intermediäre Institutionen, die Leitfäden oder Standards – teilweise sektorspezifisch – zu CSR veröffentlicht haben.⁷⁸

b) Regulierungsansätze

- 41** Nachdem die einzelnen Regulierungsebenen aufgezeigt worden sind, stellt sich nun die Frage, welche Regulierungsansätze den Regulatoren zur Verfügung ste-

⁷⁶ Vgl. Richtlinie (EU) 2024/1760: <https://eur-lex.europa.eu/eli/dir/2024/1760/oj> (zuletzt abgerufen am 26.9.2024); weitere Informationen zur CSDDD, u. a.: <https://www.bmu.de/themen/nachhaltigkeit/wirtschaft/lieferketten/europaeische-lieferkettenrichtlinie-csddd> (zuletzt abgerufen am 26.9.2024).

⁷⁷ Vgl. Dörr, in: Grabitz/Hilf/Nettesheim (Hrsg.), EUV/AEUV, Art. 47 EUV Rn. 11 ff.; Spießhofer, Unternehmerische Verantwortung, S. 61 ff., 181 ff., 219 ff., 273 ff., 285 ff.

⁷⁸ Vgl. Spießhofer, Unternehmerische Verantwortung, S. 219 ff., 311 ff., 583 f.

hen, um die erlassenen CSR-Normierungen – hier: gegenüber Unternehmen – wirksam in Kraft setzen zu können.⁷⁹

- **Staatliche/hoheitliche Regulierung**, d.h. nationale oder supranationale Normierung.
- **Regulierte Selbstregulierung (sog. „Koregulierung“)**, d.h. Normierung durch Staat (Rechtsakt) mit Beteiligung privater Parteien (wie z.B. Wirtschaftsteilnehmer, Nichtregierungsorganisationen, Verbände).
- **Selbstregulierung**, d.h. Normierung durch private Parteien (wie z.B. Wirtschaftsteilnehmer, Nichtregierungsorganisationen, Verbände) ohne staatliche Beteiligung.

Zur Vollständigkeit ist an dieser Stelle noch zu erwähnen, dass daneben auch die Möglichkeit besteht, bestimmte CSR-Aspekte bewusst unreguliert – d.h. ohne privat- bzw. öffentlich-rechtliche Regulierung – zu belassen und damit allein der Steuerung durch die Kräfte des Marktes zu überlassen. Die Vertragspartner können auf diese Art und Weise freiwillig auf privatrechtlicher Ebene bilateral individuelle CSR-Vereinbarungen treffen.⁸⁰ **42**

c) Rechtsqualität

Um herausfinden zu können, welche normative Dimension CSR-Normierungen auf den jeweiligen Regulierungsebenen im Zusammenhang mit den jeweiligen Regulierungsansätzen haben, ist die rechtliche Qualität der jeweiligen Regulierungsmaßnahmen zu analysieren. Grundsätzlich wird zwischen zwei Normenkategorien unterschieden: **43**

- **„Hard Law“**, d.h. „staatliches, supranationales und internationales Recht mit rechtsverbindlichen Durchsetzungsmechanismen“, ⁸¹ also „hoheitlich gesetztes und aus diesem Grunde verbindliches Recht“, ⁸² wie z.B. die KonfliktmineralienVO der EU.⁸³
- **„Soft Law“**: d.h. „weiche Normen öffentlicher und privater Provenienz [...], die verhaltenssteuernde Soll-Vorgaben für unternehmerische Verantwortung statuieren, sofern sie gegenüber Unternehmen [...] Bindungswirkung entfalten können“, ⁸⁴ also „Regelungen, Leitlinien, Standards, oder Empfehlungen,

79 Vgl. dazu exemplarisch die institutionelle Vereinbarung des Europäischen Parlaments, des Rates und der Kommission zur „Besseren Rechtsetzung“, veröffentlicht im Amtsblatt der EU – C 321/1, S. 3.

80 Vgl. *Simons*, ZGR 2018, 316, 320: sog. „Vertrags-CSR“.

81 Vgl. *Spießhofer*, Unternehmerische Verantwortung, S. 574.

82 Vgl. *Schütz/Beckmann/Röbken*, Compliance-Kontrolle in Organisationen, S. 16.

83 Verordnung (EU) 2017/821 des Europäischen Parlaments und des Rates vom 17. Mai 2017 zur Festlegung von Pflichten zur Erfüllung der Sorgfaltspflichten in der Lieferkette für Unionseinführer von Zinn, Tantal, Wolfram, deren Erzen und Gold aus Konflikt- und Hochrisikogebieten, veröffentlicht im Amtsblatt der EU L 130/1.

84 Vgl. *Spießhofer*, Unternehmerische Verantwortung, S. 574.

die nicht durch Gesetzgebungsverfahren entstanden sind, sondern durch private Akteure oder unter deren Mitwirkung“,⁸⁵ wie z.B. Leitsätze der OECD und Standards der ISO.⁸⁶

- 44 Der Begriff „Soft Law“ stellt dabei eine Art Zwischenkategorie dar, d.h. eine Kategorie zwischen „Recht“ und „Nicht-Recht“. Bis dato bestehen hierzu noch erhebliche Forschungs- und Theoriedefizite hinsichtlich der genauen juristischen Charakterisierung der unter diesem Terminus versammelten Konzepte.⁸⁷ Im Grunde wurde mit „Soft Law“ – wenn man der Realität Rechnung trägt – „eine Kategorie ‘anerkannter Normativität’ kreiert, die sich [...] im juristischen ‘Niemandland’ befindet“.⁸⁸
- 45 Auch in der Praxis stellt sich die Einordnung von CSR-Normen häufig als große Herausforderung dar, denn deren Bindungswirkung kann – je nach Verwendungskontext – zwischen verbindlich, unverbindlich bzw. freiwillig variieren. Somit zeigt sich, dass nicht nur das „Ob“ und „Wieviel“ an Bindung, sondern auch deren Qualität im Einzelfall für die konkrete Kategorisierung von CSR-Normen bedeutsam ist.⁸⁹

d) Reputationsmanagement

- 46 Unabhängig von der Rechtswirksamkeit einer CSR-Norm ist zu bedenken, dass letztlich aus jedem Verstoß gegen eine (CSR-)Norm oder aus jeder Missachtung eines relevanten CSR-Themas ein Reputationsschaden erwachsen kann.⁹⁰ Aus diesem Grund ist Unternehmen zu empfehlen, die Erwartungen ihrer Stakeholder zu analysieren und ein wirksames Reputationsmanagement zu betreiben.

2. Beispiele für CSR-Regulierung

a) Globale Regulierungsebene

aa) OECD-Leitsätze für multinationale Unternehmen

- 47 Die OECD-Leitsätze für multinationale Unternehmen stellen „Soft Law“ in Form von „Empfehlungen der Regierungen [an multinationale Unternehmen dar], die in oder von den Teilnehmerstaaten aus operieren. Sie enthalten [keine rechtsverbindlichen] Grundsätze und Maßstäbe [, sondern Empfehlungen] für verantwortungsvolles unternehmerisches Handeln in einem globalen Kontext,

85 Vgl. *Schütz/Beckmann/Röbken*, Compliance-Kontrolle in Organisationen, S. 16 f.

86 Vgl. *Bay*, in: Kleinfeld/Martens (Hrsg.), CSR und Compliance, S. 121; *Spießhofer*, Unternehmerische Verantwortung, S. 585 f.

87 Vgl. *Knauff*, Der Regelungsverbund: Recht und Soft Law im Mehrebenensystem, S. 387 ff.; *Spießhofer*, Unternehmerische Verantwortung, S. 579, 583 f. m. w. N.

88 Vgl. *Spießhofer*, Unternehmerische Verantwortung, S. 585.

89 Vgl. *Spießhofer*, Unternehmerische Verantwortung, S. 580, 583 f.

90 Zur Bedeutung von Reputationsrisiken und Reputationsmanagement siehe → *Schulz*, Kap. 1 Rn. 23 ff. m. w. N.

das dem geltenden Recht und international anerkannten Normen entspricht“.⁹¹ Die teilnehmenden Nationalstaaten verpflichten sich, die Leitsätze zu fördern und an Unternehmen zu vermitteln. Zur Erfüllung dieser Aufgabe haben die Nationalstaaten i. d. R. „Nationale Kontaktstellen“ eingerichtet, die u. a. als Beschwerde- sowie Schlichtungsstelle fungieren, um zur Lösung von Problemen bei Verstößen gegen die OECD-Leitsätze beizutragen.⁹²

Da die Umsetzung der OECD-Leitsätze auf Freiwilligkeit der Unternehmen basiert und die öffentliche Wahrnehmung der Leitsätze gering ist, handelt es sich hierbei aller Voraussicht nach um die Hauptgründe, die verantwortlich dafür sind, dass die OECD-Leitsätze für multinationale Unternehmen von den Unternehmen bis dato nur lückenhaft umgesetzt worden sind und ihnen bis dato nur eine geringe operative Bedeutung zugemessen wird.⁹³ **48**

bb) GRI-Berichtsstandards

Die Global Reporting Initiative (GRI), eine unabhängige internationale Organisation, hat ein Rahmenwerk entwickelt, mit dessen Hilfe ein modular aufgebautes und international vergleichbares Nachhaltigkeitsreporting erstellt werden kann. Es handelt sich dabei um „Soft Law“ in Form von Richtlinien für die CSR-Berichterstattung, die mittlerweile von einer Vielzahl an Unternehmen freiwillig angewendet werden.⁹⁴ **49**

Nach Einführung diverser gesetzlicher Verpflichtungen zur nicht-finanziellen Berichterstattung bestimmter Unternehmen konnte der GRI-Berichtsstandard neben Großunternehmen vermehrt auch mittlere Unternehmen für sich gewinnen. Davor fanden Nachhaltigkeits- bzw. CSR-Reportings in der Regel nur bei Großunternehmen Anklang, die diese u. a. als probates Mittel zur Reputationssicherung nutzten.⁹⁵ **50**

Zwar bezieht sich der GRI-Standard nicht nur auf CSR-, sondern auch auf Compliance-Themen, wie z. B. die Ablegung der Rechenschaft „über die Einhaltung von Gesetzen, Normen und externen Richtlinien, in erster Linie aber über ihre internen Maßnahmen zur Sicherstellung verantwortungsvollen Handelns“.⁹⁶ Am Ende dienen alle Maßnahmen letztlich dem Ziel der Herstellung eines interna- **51**

91 Vgl. OECD-Leitsätze für multinationale Unternehmen, S. 3, <https://mneguidelines.oecd.org/48808708.pdf> (zuletzt abgerufen am 29.2.2024); weiterführend: OECD Online, <https://mneguidelines.oecd.org/> (zuletzt abgerufen am 29.2.2024).

92 Vgl. *Schank/Hayduk*, in: Kleinfeld/Martens (Hrsg.), *CSR und Compliance*, S. 79 ff., 83 f., 86 f.; *Spießhofer*, *Unternehmerische Verantwortung*, S. 181 ff., 197 f.

93 Vgl. *Schank/Hayduk*, in: Kleinfeld/Martens (Hrsg.), *CSR und Compliance*, S. 86 f.

94 Vgl. Global Reporting Initiative Online, <https://www.globalreporting.org/> (zuletzt abgerufen am 29.2.2024); *Henrich*, in: Kleinfeld/Martens (Hrsg.), *CSR und Compliance*, S. 91 ff.; *Spießhofer*, *Unternehmerische Verantwortung*, S. 398 ff.

95 Vgl. *Henrich*, in: Kleinfeld/Martens (Hrsg.), *CSR und Compliance*, S. 91 ff.; zum CSR-Reporting siehe auch → *Beisheim*, Kap. 16.

96 Vgl. *Henrich*, in: Kleinfeld/Martens (Hrsg.), *CSR und Compliance*, S. 96.

tional vergleichbaren Nachhaltigkeitsreportings. Der GRI-Standard verfolgt dabei einen integrierten Ansatz von Compliance und Nachhaltigkeitsmanagement, in dem Compliance nur als ein Gesichtspunkt der gesellschaftlichen Verantwortung eines Unternehmens angesehen wird, der sich letztlich der CSR unterzuordnen hat.⁹⁷

cc) UN Global Compact

- 52** Der UN Global Compact stellt die „weltweit größte und wichtigste Initiative für verantwortungsvolle Unternehmensführung [dar]“. ⁹⁸ Er beruht auf zehn universellen Prinzipien.⁹⁹
- 53** Grundsätzlich können alle Unternehmen – unabhängig von Branche und Sektor – am UN Global Compact teilnehmen. Ausgeschlossen sind jedoch Unternehmen, die z. B. UN-Sanktionen unterliegen oder Einnahmen aus Geschäften aus umstrittenen Waffen erzielen.¹⁰⁰ Die Teilnahme erfordert zudem ein Bekenntnis des Unternehmens zu den Prinzipien des UN Global Compact, das an den UN-Generalsekretär zu richten ist. Im Ergebnis resultiert daraus allerdings keine formale Mitgliedschaft, sondern nur eine Teilnahme am UN Global Compact. Kommt es zu Regelverletzungen, können diese Integritätsmaßnahmen nach sich ziehen, wie z. B. den Widerruf des Teilnahmestatus eines Unternehmens bei systematischem oder gravierendem Fehlverhalten.¹⁰¹
- 54** Neben CSR-Themen befasst sich der UN Global Compact auch mit Compliance. Nach dessen Verständnis ist „Compliance [...] zunächst nichts anderes als die an sich selbstverständliche Einhaltung des geltenden Rechts und selbst gesetzter Regeln. Aber Compliance ist und will noch mehr: In der heutigen modernen, schnelllebigen Zeit soll es die Grundsätze des Ehrbaren Kaufmanns untermauern und sich aktiv dazu bekennen. Diese sind Integrität, Seriosität, Glaubwürdigkeit, Stabilität, Verlässlichkeit, Fairness, Sicherheit und Nachhaltigkeit. Hinter einer Compliance-Kultur steckt also auch die Idee von der Übereinstimmung unternehmerischen Verhaltens mit gesellschaftlichen Richtlinien und Wertvorstellungen“. ¹⁰²

⁹⁷ Vgl. *Henrich*, in: Kleinfeld/Martens (Hrsg.), *CSR und Compliance*, S. 96; *Spießhofer*, *Unternehmerische Verantwortung*, S. 399 f.

⁹⁸ Vgl. UN Global Compact Online, <https://www.globalcompact.de/> (zuletzt abgerufen am 29.2.2024).

⁹⁹ Vgl. UN Global Compact Online, <https://www.globalcompact.de/> (zuletzt abgerufen am 29.2.2024).

¹⁰⁰ Vgl. UN Global Compact Online, <https://www.globalcompact.de/teilnehmen/beitritt-business> (zuletzt abgerufen am 29.2.2024); *Höble*, in: Kleinfeld/Martens (Hrsg.), *CSR und Compliance*, S. 105 ff.; *Spießhofer*, *Unternehmerische Verantwortung*, S. 66 ff.

¹⁰¹ Vgl. UN Global Compact Online, <https://www.globalcompact.de/teilnehmen> (zuletzt abgerufen am 29.2.2024); *Höble*, in: Kleinfeld/Martens (Hrsg.), *CSR und Compliance*, S. 105 ff.; *Spießhofer*, *Unternehmerische Verantwortung*, S. 66 ff.

¹⁰² Vgl. Global Compact Netzwerk Deutschland Online v. 14.12.2016, *Compliance – Praxisleitfaden für den Mittelstand*, S. 8, https://www.globalcompact.de/migrated_files/wAssets/

Im Vergleich zu den OECD-Leitlinien für multinationale Unternehmen und dem GRI-Berichtsstandard zeigt sich beim UN Global Compact erstmals, dass ein Verstoß gegen diesen Standard nicht nur Reputationsschäden, sondern auch Integritätsmaßnahmen nach sich ziehen können. Es liegt auch hier wieder lediglich „Soft Law“ vor, allerdings kann aus einem Verstoß eine konkrete Sanktion – nämlich der Widerruf des Teilnahmestatus – resultieren. **55**

dd) ISO 26000

Die ISO 26000 verkörpert einen Leitfaden zur gesellschaftlichen Verantwortung von Organisationen. Er soll „weltweit für Unternehmen und Organisationen jeder Art als Leitfaden für die freiwillige Übernahme von gesellschaftlicher Verantwortung dienen“. ¹⁰³ Er fußt u. a. auf den folgenden sieben Prinzipien: (1) Rechenschaftspflicht, (2) Transparenz, (3) ethisches Verhalten, (4) Achtung der Interessen der Stakeholder, (5) Achtung der Rechtsstaatlichkeit, (6) Achtung internationaler Verhaltensstandards und (7) Achtung der Menschenrechte. ¹⁰⁴ **56**

Auch bei diesem Standard handelt es sich um „Soft Law“, das auf die Freiwilligkeit bei der Umsetzung durch die Unternehmen setzt. Dies entspricht dem Selbstverständnis dieser Normierung: „[ISO 26000] provides guidance rather than requirements, so it cannot be certified to unlike some other well-known ISO standards. Instead, it helps clarify what social responsibility is, helps businesses and organizations translate principles into effective actions and shares best practices relating to social responsibility, globally. It is aimed at all types of organizations regardless of their activity, size or location.“ ¹⁰⁵ **57**

Zwar drohen bei Verstößen gegen die ISO 26000 keine unmittelbaren Sanktionen. Allerdings hat dieser Standard durch die deutsche Umsetzung in die DIN ISO 26000 („Leitfaden zur gesellschaftlichen Verantwortung von Unternehmen“) ¹⁰⁶ an Gewicht gewonnen. Ferner weist er eine hohe Konsistenz mit existierenden internationalen Normen, Konventionen und Verträgen auf. ¹⁰⁷ Des Weiteren gewinnt er durch seine internationale Präsenz und Akzeptanz Einfluss auf die Glaubwürdigkeit und Reputation eines Unternehmens – im positiven wie im negativen Sinne. Zur Vermeidung von nicht nur unerheblichen Reputationsschäden, kann auch in Bezug auf ISO 26000 empfohlen werden, sich an die dort sta- **58**

docs/Korruptionspraevention/Publikationen/Compliance_Praxisleitfaden-fuer-den-Mittelstand.pdf (zuletzt abgerufen am 29.2.2024).

103 Vgl. Bay, in: Kleinfeld/Martens (Hrsg.), CSR und Compliance, S. 121; vertiefend zur ISO 26000: *Spießhofer*, Unternehmerische Verantwortung, S. 222 ff.; *Schmiedeknecht/Wieland*, in: Schneider/Schmidpeter (Hrsg.), Corporate Social Responsibility, S. 299 ff.

104 Vgl. Bay, in: Kleinfeld/Martens (Hrsg.), CSR und Compliance, S. 122 f.

105 Vgl. ISO Online, <https://www.iso.org/iso-26000-social-responsibility.html> (zuletzt abgerufen am 29.2.2024).

106 Vgl. Bundesministerium für Arbeit und Soziales, https://www.bmas.de/SharedDocs/Downloads/DE/Publikationen/a395-csr-din-26000.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 29.2.2024).

107 Vgl. Bay, in: Kleinfeld/Martens (Hrsg.), CSR und Compliance, S. 122.

tuierten Mindestanforderungen zu halten, falls man sich als Unternehmen dazu entschieden hat, sich diesem freiwilligen Standard zu unterwerfen.¹⁰⁸

b) Internationale Regulierungsebene

- 59** In den Jurisdiktionen anderer Nationalstaaten haben u. a. folgende Gesetze in letzter Zeit zur nachhaltigen Förderung und Beachtung von Corporate Social Responsibility beigetragen:
- **Frankreich:** „Loi de Vigilance 2017“ (Gesetz gegen Menschenrechtsverletzungen in der Lieferkette).¹⁰⁹
 - **UK:** „Bribery Act 2010“ (Anti-Korruptionsgesetz)¹¹⁰ und „Modern Slavery Act 2015“ (Gesetz gegen Zwangsarbeit, Sklaverei und Menschenhandel in der Lieferkette).¹¹¹
 - **USA:** „Foreign Corrupt Practices Act 1977“ (Anti-Korruptionsgesetz)¹¹² und „Dodd-Frank Wall Street Reform and Consumer Protection Act 2010“ (Gesetz zur Verbesserung der Verantwortung und Transparenz im Finanzsystem).¹¹³
- 60** Ein Anwendungsbezug kann sich aus diesen Normen für diejenigen deutschen Unternehmen ergeben, die grenzüberschreitend mit Bezug zu den o. a. Rechtsordnungen agieren: Als Anknüpfungspunkt kann z. B. eine internationale Lieferkette in Betracht kommen.¹¹⁴ Jedes Unternehmen hat dann im Einzelfall zu klären, ob die betreffenden Normen nicht doch eine unmittelbare oder mittelbare Bindungswirkung entfalten könnten. Das gilt insbesondere für internationale Normen, die eine extraterritoriale Geltung für sich in Anspruch nehmen. Häufig kommt es dabei zu Jurisdiktionskonflikten.¹¹⁵

108 Vgl. *Schmiedeknecht/Wieland*, in: Schneider/Schmidpeter (Hrsg.), *Corporate Social Responsibility*, S. 307; Bay, in: Kleinfeld/Martens (Hrsg.), *CSR und Compliance*, S. 122 und 137.

109 Vgl. Légifrance Online, <https://www.legifrance.gouv.fr/eli/loi/2017/3/27/2017-399/jo/texte> (zuletzt abgerufen am 29.2.2024).

110 Vgl. UK Legislation Online, <http://www.legislation.gov.uk/ukpga/2010/23/contents> (zuletzt abgerufen am 29.2.2024).

111 Vgl. UK Legislation Online, <http://www.legislation.gov.uk/ukpga/2015/30/contents> (zuletzt abgerufen am 29.2.2024).

112 Vgl. The United States Department of Justice Online, <https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act> (zuletzt abgerufen am 29.2.2024).

113 Vgl. US Law Online, <https://uslaw.link/citation/us-law/public/111/203> (zuletzt abgerufen am 29.2.2024).

114 Vgl. → *Schulz*, Kap. 1 Rn. 2 ff. sowie zur Compliance in Supply Chain → *Schleper/Förstl*, Kap. 17.

115 Vgl. *Spießhofer*, *Unternehmerische Verantwortung*, S. 296 ff., 301 ff.; vertiefend zur Extraterritorialität: *Schwarz*, in: Wieland/Steinmeyer/Grüniger (Hrsg.), *Handbuch Compliance Management*, Rn. 1 ff.; exemplarische Auswahl an nationalen und internationalen Standards und Gesetzen zur verantwortlichen Lieferkettengestaltung: <https://www.csr-praxistage.de/wissen/lieferketten/standards-gesetze/> (zuletzt abgerufen am 29.2.2024).

c) Supranationale bzw. europäische Regulierungsebene

Die Europäische Union legte im Rahmen ihrer „neue[n] EU Strategie (2011–14) für die soziale Verantwortung der Unternehmen (CSR)“¹¹⁶ einen Aktionsplan vor, der „Verpflichtungen für die Kommission selbst sowie Anregungen für Unternehmen, Mitgliedstaaten und andere Stakeholder Gruppen [umfasste]“.¹¹⁷ Eine erste Regulierungsmaßnahme stellte die CSR-Richtlinie 2014/95/EU zur nicht-finanziellen Berichterstattung dar, die mit dem „Gesetz zur Stärkung der nicht-finanziellen Berichterstattung der Unternehmen in ihren Lage- und Konzernlageberichten“ (CSR-Richtlinien-Umsetzungsgesetz, CSR-RUG) in deutsches Recht umgesetzt worden ist. Die neue „Corporate Sustainability Reporting Directive (CSRD)“ (Richtlinie 2022/2464) der EU wird im Grunde die CSR-Richtlinie aus 2014 in Zukunft ablösen. Ein weiteres Beispiel aus der Feder der EU stellt die Verordnung (EU) 2017/821 (KonfliktmineralienVO) dar, die auf die Erfüllung bestimmter Sorgfaltspflichten abstellt, sobald sich bestimmte Mineralien in einer Lieferkette befinden.¹¹⁸

Neben hoheitlichen/staatlichen Regulierungsmaßnahmen setzt die Europäische Union ausdrücklich auch auf Selbst- und Koregulierungsprozesse, denn „derartige Prozesse können, wenn sie entsprechend konzipiert sind, die Unterstützung durch die Stakeholder sichern und ein effizientes Mittel zur Gewährleistung von verantwortlichem unternehmerischen Handeln darstellen. Selbst- und Koregulierung werden von der EU als Bestandteil der Agenda für bessere Rechtsetzung anerkannt“.¹¹⁹ Im Ergebnis setzt die Europäische Union auf verschiedene Regulierungsmaßnahmen, die einen sog. „Smart Mix“ – bestehend aus „Hard Law“, „Soft Law“ sowie sonstigen weichen Steuerungsinstrumenten – darstellen, um ihre Strategie und Idee von CSR umsetzen zu können.¹²⁰

d) Nationale bzw. deutsche Regulierungsebene

Auch Deutschland setzt – ebenso wie die EU – auf einen „Smart Mix“ zur CSR-Regulierung (vgl. Abb. 4). Neben Gesetzen, wie z. B. dem CSR-RUG oder dem LkSG, enthalten u. a. auch diverse Rechtsverordnungen staatliche Regulierungsmaßnahmen, um CSR-Normen als „Hard Law“ in die Rechtsordnung zu implementieren.

116 KOM (2011) 681 endgültig.

117 KOM (2011) 681 endgültig, S. 10.

118 Zum CSR-Reporting siehe ausführlich → *Beisheim*, Kap. 16.

119 KOM (2011) 681 endgültig, S. 12; KOM (2005) 97.

120 Vgl. *Spießhofer*, Unternehmerische Verantwortung, S. 283.

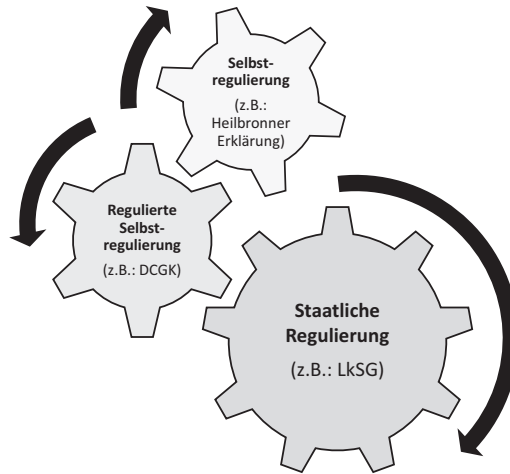


Abbildung 4: Smarter Regulierungsmix in Deutschland (eigene Darstellung)

- 64** Als Beispiel für eine regulierte Selbstregulierung (sog. „Koregulierung“)¹²¹ kann der DCGK herangezogen werden. Mit dem DCGK schafft eine private Kommission einen privaten Kodex, der vom deutschen Gesetzgeber normativ überformt wird. Das wird u. a. anhand der Regelungen des § 161 AktG deutlich, wonach der Vorstand und der Aufsichtsrat bestimmter Aktiengesellschaften nach Abs. 1 einer sog. „comply or explain“-Erklärungsverpflichtung und nach Abs. 2 einer Veröffentlichungspflicht dieser Erklärung unterliegen. Die Publizitätsverpflichtungen gehen aber noch weiter, wie z. B. § 285 Nr. 16 HGB (Veröffentlichung der Erklärung im Bilanzanhang) oder § 325 Abs. 1 Satz 1 Nr. 2 HGB (Veröffentlichung der Erklärung im Handelsregister) zeigen.¹²² Letztlich ist auch der DCGK dem „Soft Law“ zuzuordnen,¹²³ da aus einem Verstoß gegen den DCGK keine unmittelbare Sanktion gegen das Unternehmen verhängt werden kann.¹²⁴
- 65** Als Beispiel für eine freiwillige Selbstregulierung im CSR-Bereich kann die sog. „Heilbronner Erklärung zur gesellschaftlichen Verantwortung des Mittelstands in der Wirtschaft“ von 2012 benannt werden, bei der es sich um eine freiwillige Selbstverpflichtungserklärung für Unternehmen aus der Region Heil-

121 Vgl. *Schütz/Beckmann/Röbken*, Compliance-Kontrolle in Organisationen, S. 16 f.

122 Vgl. *Tieben*, Das Drei-Säulen-System des Bankenmarktes als regulierungsrechtliche Steuerungsressource, S. 134 f. m. w. N.; *Knierim*, in: Wabnitz/Janovsky/Schmitt (Hrsg.), Handbuch Wirtschafts- und Steuerstrafrecht, Kap. 5 Rn. 84.

123 Vgl. *Schütz/Beckmann/Röbken*, Compliance-Kontrolle in Organisationen, S. 17.

124 Vgl. *Simons*, ZGR 2018, 316, 317 f. und 321; *Eidam*, Unternehmen und Strafe, Kap. 5 Rn. 143 f. und Rn. 149.

bronn-Franken handelt.¹²⁵ Auch bei dieser Initiative handelt es sich um „Soft Law“, da grundsätzlich nur eine privatrechtliche Verbindlichkeit zwischen dem Herausgeber der Selbstverpflichtungserklärung und dem sich selbstverpflichtenden Unternehmen erzeugt wird.¹²⁶ Verstößt ein Unternehmen (bewusst) gegen eine freiwillige Selbstverpflichtung (z. B. hinsichtlich einer erlangten CSR-Zertifizierung, mit der sich das Unternehmen oder seine Produkte in der Werbung schmückt), kann dies u. U. wettbewerbsrechtliche Folgen haben.¹²⁷

Darüber hinaus steht es Unternehmen grundsätzlich frei, „inter partes“ – d. h. im Rahmen der Vertragsfreiheit – wirksame CSR-Verträge abzuschließen.¹²⁸ Als Beispiel können hier CSR-Vereinbarungen in Lieferkettenverträgen genannt werden. **66**

3. CSR-Normenflut als Herausforderung für Unternehmen

Wie die unter Rn. 47 ff. genannten Beispiele deutlich gemacht haben, hat das Thema CSR auf nationaler, supranationaler, internationaler sowie globaler Ebene immer größere Bedeutung gewonnen. Ein Grund für diese Entwicklung wird darin gesehen, dass mit Hilfe von CSR-Normen versucht wird, den schwindenden Einfluss von Nationalstaaten auf die Handlungen transnationaler Unternehmen zu kompensieren und entstandene Regelungsfreiräume (sog. „Governance Gaps“) zu minimieren.¹²⁹ Soweit die auf globaler, internationaler oder supranationaler Ebene erlassenen relevanten CSR-Normen noch einer nationalen regulatorischen Berücksichtigung bedürfen, wird diese i. d. R. durch die Nationalstaaten vollzogen. Ebenso wie bei der Umsetzung nationaler CSR-Normen, greifen Nationalstaaten – wie bereits aufgezeigt – häufig auf die Anwendung eines smarten Regulierungsmixes, bestehend aus den Ansätzen der hoheitlichen/staatlichen Regulierung, der regulierten Selbstregulierung (sog. „Koregulierung“) sowie der Selbstregulierung, zurück.¹³⁰ Wie der CSR-Bereich zeigt, wird globales Handeln durch ein Netzwerk gesteuert, das sich aus privaten und öffentlichen Regelungsinstrumenten zusammensetzt. Demnach könnte „transnationales Recht“ u. a. auch als ein Recht verstanden werden, „das sich durch ein maßgeschneidertes Zusammenspiel öffentlicher und privater einschließlich hybrider Mechanismen auszeichnet, die zur Regulierung grenzüberschreitender Sachverhalte und zur Streitschlichtung herangezogen werden“.¹³¹ Klammert man natio- **67**

125 Vgl. Pressemitteilung der German Graduate School vom 9.4.2014, <https://idw-online.de/de/news581896> (zuletzt abgerufen am 29.2.2024).

126 Vgl. *Schütz/Beckmann/Röbken*, Compliance-Kontrolle in Organisationen, S. 17.

127 Vgl. *Birk*, GRUR 2011, 196–203.

128 Vgl. *Simons*, ZGR 2018, 316, 320 f.

129 Vgl. *Schütz/Beckmann/Röbken*, Compliance-Kontrolle in Organisationen, S. 17; weiterführend dazu u. a.: *Spießhofer*, Unternehmerische Verantwortung, S. 571 ff.

130 Vgl. KOM (2011) 681 endgültig, S. 12; *Spießhofer*, Unternehmerische Verantwortung, S. 595; vertiefend zum Prozess der Transnationalisierung des Rechts: *Spießhofer*, Unternehmerische Verantwortung, S. 596 f.

131 Vgl. *Spießhofer*, Unternehmerische Verantwortung, S. 597 m. w. N.

nale Aspekte aus, kann dieses Verständnis zur Analyse grenzüberschreitender Entstehung von CSR beitragen.¹³²

- 68** Wie **Abb. 5** zu entnehmen ist, haben sowohl die Regulierungsebene als auch der jeweilige Regulierungsansatz Einfluss auf die jeweilige Bindungsqualität, die eine CSR-Norm gegenüber einem Unternehmen entfaltet. Der relativen rechtlichen Bindungswirkung von CSR-Normen nach kann dann eine Kategorisierung in „Hard Law“, „Soft Law“ oder „No Law“ erfolgen.¹³³ Ferner zeigt Abb. 5 weiter auf, dass in diesem Zusammenhang auch die Rechtswirksamkeit relevanter CSR-Normen zu klären ist: Handelt es sich um eine formelle oder materielle CSR-Norm? Insbesondere: Handelt es sich bei der relevanten materiellen CSR-Norm um eine Norm, die bei einer Missachtung oder einem Verstoß eine Sanktion für das Unternehmen nach sich ziehen könnte (sog. „juristische Verantwortung“)? Unabhängig von der Rechtswirksamkeit einer CSR-Norm sind zwingend die relevanten Stakeholder eines Unternehmens zu ermitteln, um analysieren zu können, ob einem Unternehmen bei der Missachtung bzw. dem Verstoß gegen eine bestimmte CSR-Norm/Thematik ein Reputationsschaden drohen könnte (sog. „gesellschaftliche Verantwortung“).

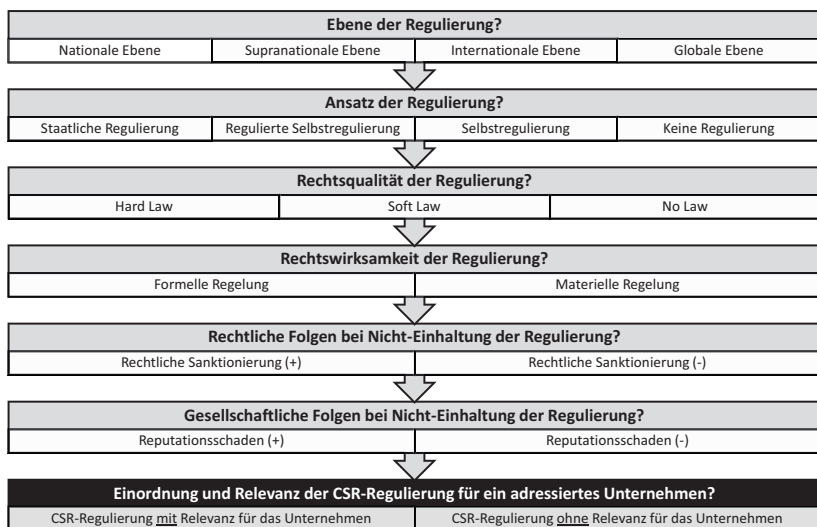


Abbildung 5: Übersicht zur Normierung von CSR sowie deren Einordnung und Relevanz für ein adressiertes Unternehmen (eigene Darstellung)

¹³² Vgl. *Spießhofer*, Unternehmerische Verantwortung, S. 597.

¹³³ Vgl. *Schütz/Beckmann/Röbken*, Compliance-Kontrolle in Organisationen, S. 16 f.; *Spießhofer*, Unternehmerische Verantwortung, S. 574 ff., 579 ff.

Die Unternehmen stehen nun vor der Herausforderung, eine wahre Flut an stetig zunehmenden CSR-Normen¹³⁴ – in regelmäßigen Zeitabständen wiederholend – systematisch zu erfassen. Im Anschluss daran sind die für das Unternehmen relevanten CSR-Normen herauszufiltern und auf ihre relative Rechtsqualität hin zu überprüfen, um Verstöße gegen jene CSR-Normen/Themen zu vermeiden, die Haftungsrisiken, Schadensersatzpflichten, Strafzahlungen, Bußgelder und/oder Reputationsschäden für das Unternehmen auslösen könnten. **69**

IV. Corporate Social Responsibility und Corporate Compliance

1. Einführung

In den letzten Jahren wurde viel über Compliance-Verstöße (die teilweise auch CSR-Themen betrafen) bei namhaften Unternehmen und Verbänden berichtet, u. a.: **70**

- 2006: Siemens AG (Korruptionsaffäre);¹³⁵
- 2012: KiK Textilien und Non-Food GmbH (Feuer in pakistanischer Textilfabrik);¹³⁶
- 2015: Deutscher Fußball-Bund e. V. („Sommermärchen-Skandal“);¹³⁷
- 2015: RWE (Klimaklage eines peruanischen Bergbauern);¹³⁸
- 2015: Volkswagen AG („Abgasskandal“);¹³⁹
- 2020: Siemens AG (Steinkohlebergwerk Carmichael in Australien).¹⁴⁰

134 Vgl. *Schütz/Beckmann/Röbken*, Compliance-Kontrolle in Organisationen, S. 17.

135 Vgl. u. a. Stern Online v. 29.7.2008, <https://www.stern.de/wirtschaft/news/chronologie-der-siemens-skandal-3758286.html> (zuletzt abgerufen am 29.2.2024).

136 Vgl. u. a. Business & Human Rights Resource Centre Online, Blog, letzter Eintrag v. 19.2.2019, <https://www.business-humanrights.org/de/neuste-meldungen/pakistan-opfer-des-feuers-in-der-ali-enterprises-fabrik-drohen-kik-mit-klage-in-deutschland-falls-keine-langfristigen-entsch%C3%A4digungen-vereinbart-werden/> (zuletzt abgerufen am 29.2.2024).

137 Vgl. u. a. LTO Online v. 11.6.2020, <https://www.lto.de/recht/nachrichten/n/wm-2006-sommermaerchen-prozess-kosten-zwanziger-verschleppung-schadensersatz/> (zuletzt abgerufen am 29.2.2024); Spiegel Online v. 10.6.2020, <https://www.spiegel.de/sport/fussball/wm-2006-prozess-darum-sollen-die-dfb-funktionaere-trotz-verjaehrung-zahlen-a-fea1f6b4-7923-456c-9819-951aeab4d672> (zuletzt abgerufen am 29.2.2024); Spiegel Online v. 1.9.2016, <https://www.spiegel.de/sport/fussball/chronologie-des-skandals-um-die-wm-vergabe-2006-a-1110419.html> (zuletzt abgerufen am 29.2.2024).

138 Vgl. u. a. LTO Online v. 29.1.2020, <https://www.lto.de/recht/nachrichten/n/olg-hamm-5-u-15-17-klage-klimafolgen-rwe-beweisaufnahme-ortstermin-peru/> (zuletzt abgerufen am 29.2.2024); Germanwatch Online, Blog, letzter Eintrag v. 8.6.2020, <https://www.germanwatch.org/de/der-fall-rwe> (zuletzt abgerufen am 29.2.2024).

139 Vgl. u. a. Stiftung Warentest Online v. 25.5.2020 (Stand: 8.6.2020), <https://www.test.de/Abgasskandal-4918330-0/> (zuletzt abgerufen am 29.2.2024); NDR Online v. 7.8.2018, https://www.ndr.de/nachrichten/niedersachsen/braunschweig_harz_goettingen/Die-VW-Abgas-Affae-re-eine-Chronologie,volkswagen892.html (zuletzt abgerufen am 29.2.2024).

140 Vgl. u. a. Zeit Online v. 13.1.2020, <https://www.zeit.de/wirtschaft/2020-01/umweltschuetzer-australien-empoe-rung-siemens-kohlebergwerk> (zuletzt abgerufen am 29.2.2024).

- 71 Wie diese prominenten Fälle von Non-Compliance exemplarisch aufgezeigt haben, waren die Konsequenzen für die betroffenen Unternehmen sowohl im In- als auch und im Ausland meist höchst nachteilig. Bemerkenswert ist hierbei der Zusammenhang zwischen Non-Compliance und CSR: Die ökonomischen Vorteile, die ein Unternehmen aus der Globalisierung zog, konnten beim Auftreten eines prominenten Falles von Non-Compliance innerhalb kurzer Zeit mehr als nur aufgebraucht – gar existenzgefährdend für das Unternehmen – sein. Da die relevanten Stakeholder heute regelmäßig über das Internet oder Social Media global vernetzt sind und nahezu ohne Zeitverzögerung kommunizieren können, sind Unternehmen zudem dem Risiko eines globalen Reputationsschadens ausgesetzt. Im Ergebnis drohen einem Unternehmen bei einem Fall von Non-Compliance nicht nur finanzielle, sondern zusätzlich auch nicht-finanzielle Konsequenzen, wie z. B.:¹⁴¹
- negative mediale Berichterstattung (TV, Presse, Radio, Internet, Social Media etc.);
 - Reputationsschaden (Börsenkurs, Markenwert, Mitarbeiterfluktuation etc.);
 - zivilrechtliche Verfahren (Gutachterkosten, Anwaltskosten etc.);
 - zivilrechtliche Schadensersatzpflichten (Schadensersatz, Schmerzensgeld etc.);
 - unternehmensinterne Ermittlungen (Internal Investigations, Anwaltskosten etc.);
 - staatsanwaltschaftliche Ermittlungen (Hausdurchsuchungen, Anwaltskosten etc.);
 - ordnungswidrigkeitenrechtliche Sanktionen (Bußgeld, Gewinnabschöpfung etc.);
 - unternehmensstrafrechtliche Sanktionen (Strafzahlungen, Compliance-Monitor etc.);
 - unternehmensinterne Aufarbeitung (Umstrukturisierungskosten, Beraterkosten etc.).
- 72 Um es an einem konkreten Beispiel zu illustrieren: Die Aufarbeitung des sog. „Abgasskandals“ hatte den Volkswagen-Konzern nicht nur hohe Vergleichs-, Straf- und Bußgeldzahlungen gekostet (wie z. B. Kosten i. H.v. mehr als 20 Mrd. EUR in den USA sowie Kosten i. H.v. 1 Mrd. EUR in Deutschland),¹⁴² dazu kamen auch noch Honorare für Beratungs- und Anwaltsunternehmen in Rekordhöhe.¹⁴³ Im Juni 2019 beliefen sich die Gesamtkosten des Wirtschaftsskandals be-

141 Zu den Nachteilen von Non-Compliance siehe auch → *Schulz*, Kap. 1 Rn. 11 m. w. N.

142 Vgl. u. a. Süddeutsche Zeitung Online v. 13.6.2018, <https://www.sueddeutsche.de/wirtschaft/auto-vw-muss-in-der-diesellaftaere-eine-milliarde-bussgeld-zahlen-dpa.urn-newsml-dpa-com-20090101-180613-99-708935> (zuletzt abgerufen am 29.2.2024).

143 Vgl. u. a. Handelsblatt Online v. 14.6.2019, <https://www.handelsblatt.com/unternehmen/industrie/autohersteller-berater-im-dieselskandal-kosten-den-vw-konzern-mehr-als-1-7-milliarden-euro/24457804.html?ticket=ST-6115684-paEYJULgbSqsnNeB1u9-ap5> (zuletzt abgerufen am 29.2.2024).

reits auf rund 30 Mrd. EUR.¹⁴⁴ Die Aufarbeitung hatte jedoch noch weitere Kosten in Milliardenhöhe für den Volkswagen-Konzern verursacht, wie z.B. die erlangten zivilrechtlichen Schadensersatzansprüche von Kunden, die Dieselfahrzeuge erworben hatten, in den Folgejahren deutlich machten.¹⁴⁵

Die Leitungsorgane von Unternehmen und Verbänden haben rechtsformübergreifend die Pflicht, das Unternehmen so zu organisieren und zu beaufsichtigen, dass sowohl das Unternehmen als auch dessen Mitarbeiter gegen keine Gesetze verstoßen (sog. „Legalitäts- und Legalitätskontrollpflicht“)¹⁴⁶ um Kosten – wie sie z.B. der Volkswagen-Konzern bereits zu tragen hatte – zu vermeiden. Ob und welche Relevanz CSR-Normen für institutionalisierte Vorkehrungsmaßnahmen der Compliance-Organisationspflicht haben, wird im folgenden Abschnitt dieses Beitrages thematisiert. **73**

2. Allgemeine Relevanz von CSR-Normen für die Corporate Compliance

Die Aufgabe der Corporate Compliance besteht darin, Compliance-Verstöße – d.h. Regelverletzungen – möglichst zu verhindern. Damit erlangen grundsätzlich alle CSR-Normen, die unter das „Hard Law“ oder ggf. auch unter das „Soft Law“ subsumiert werden können, Relevanz für die Corporate Compliance eines Unternehmens. **74**

Da (Reputations-)Schäden nicht nur aus Verstößen gegen „Hard Law“ und „Soft Law“ resultieren können, ist zudem zu prüfen, ob ggf. bestimmte CSR-Themen, die das Unternehmen sowie dessen unternehmerische Handeln betreffen, ebenfalls Relevanz für die Corporate Compliance eines Unternehmens erlangen könnten (vgl. dazu Abb. 6), wie z.B. das Angebot CSR-kritischer Produkte/Dienstleistungen. **75**

144 Vgl. u.a. Handelsblatt Online v. 14.6.2019, <https://www.handelsblatt.com/unternehmen/industrie/autohersteller-berater-im-dieselskandal-kosten-den-vw-konzern-mehr-als-1-7-milliarden-euro/24457804.html?ticket=ST-6115684-paEYJULgbSqqsnNeB1u9-ap5> (zuletzt abgerufen am 29.2.2024).

145 Vgl. Bundesgerichtshof, Pressemitteilung 063/2020 v. 25.5.2020, <https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020063.html> (zuletzt abgerufen am 29.2.2024); BGH, 25.5.2020 – VI ZR 252/19.

146 Siehe hierzu → *Schulz*, Kap. 1 Rn. 36 f. m. w. N.; *Knierim*, in: Wabnitz/Janovsky/Schmitt (Hrsg.), Handbuch Wirtschafts- und Steuerstrafrecht, Kap. 5 Rn. 31 ff.; *Eidam*, Unternehmen und Strafe, Kap. 5 Rn. 25.

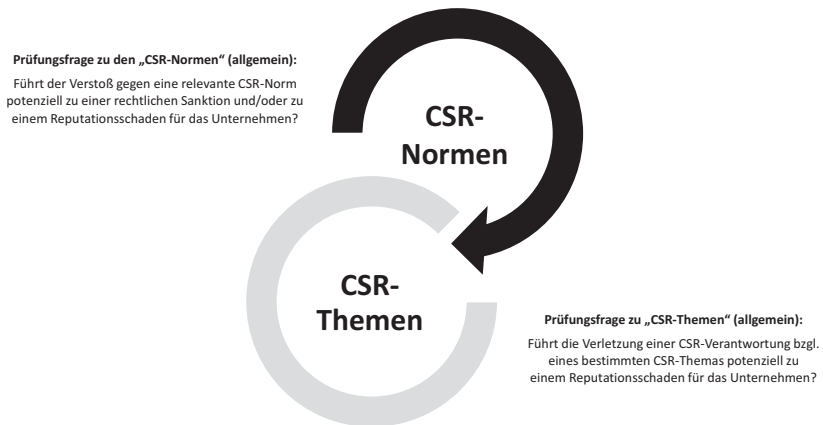


Abbildung 6: Prüfung von CSR-Normen und CSR-Themen auf relevante Compliance-Risiken für ein adressiertes Unternehmen (eigene Darstellung)

3. Konkrete Relevanz von CSR-Normen sowie sonstiger CSR-Themen für die Corporate Compliance

- 76 Die konkrete Relevanz von CSR-Normen sowie sonstiger CSR-Themen für die Corporate Compliance eines Unternehmens ist im Rahmen des Compliance-Risikomanagements zu prüfen. Hierbei handelt es sich um den zentralen Eckpfeiler eines robusten und effektiven Compliance-Management-Systems.¹⁴⁷ Compliance-Risiken werden dem operationellen Risiko eines Unternehmens zugeordnet, wie man z. B. aus der Legaldefinition des Art. 4 Abs. 1 Nr. 52 CRR klar entnehmen kann: „Operationelles Risiko ist das Risiko von Verlusten, die durch die Unangemessenheit oder das Versagen von internen Verfahren, Menschen und Systemen oder durch externe Ereignisse verursacht werden, einschließlich Rechtsrisiken.“¹⁴⁸

147 Vgl. dazu u. a. *Kark*, Compliance-Risikomanagement, Rn. 13; siehe auch → *Schulz*, Kap. 1 Rn. 60 ff.; → *Romeike*, Kap. 9.

148 Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 646/2012, Amtsblatt der Europäischen Union L 176/1 vom 27.6.2013.

a) CSR-Normen und CSR-Themen im Compliance-Risikomanagementprozess

Ein Compliance-Risikomanagementprozess umfasst i.d.R. folgende Schritte 77
(vgl. Abb. 7):

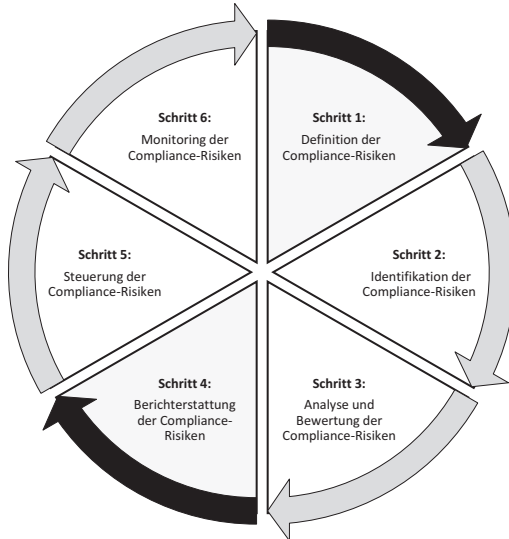


Abbildung 7: Vorschlag für einen Compliance-Risikomanagementprozess in sechs Schritten (in Anlehnung an Kark, Compliance-Risikomanagement, Rn. 644 ff., Abb. 11)

aa) Schritt 1: Definition der Compliance-Risiken

Im ersten Schritt dieses Prozesses sind die Compliance-Risiken des Unternehmens zu definieren.¹⁴⁹ Der Fokus der vorliegenden Prüfung wird auf das Thema Corporate Social Responsibility gelegt. Die Erforderlichkeit einer solchen Prüfung kann z.B. darin begründet sein, dass neue CSR-Normen in Kraft getreten sind, alte CSR-Normen verschärft wurden oder gar ein neues CSR-Thema für das Unternehmen relevant geworden ist. 78

bb) Schritt 2: Identifikation der Compliance-Risiken

Im zweiten Schritt dieses Prozesses sind die konkreten Compliance-Risiken des Unternehmens im Hinblick auf den Themenkomplex Corporate Social Responsibility zu identifizieren. Hierzu wird u. a. auf folgende Informationsquellen zurückgegriffen: Mitarbeiter des Unternehmens (insbesondere aus den CSR-Fach- 79

149 Vgl. Kark, Compliance-Risikomanagement, Rn. 644 ff., 649.

bereichen), Führungskräfte und Mitglieder der Geschäftsleitung, Interne Revision, Rechtsabteilung, Unternehmensanwälte, Wirtschaftsprüfer, Internes Kontrollsystem, Whistleblower und Wettbewerbsanalysen. Auf diese Art und Weise der Informationsgewinnung sollten i. d. R. alle – auch bislang verborgene – CSR-Normen und CSR-Themen, die für das betreffende Unternehmen Relevanz zeigen, identifiziert werden.¹⁵⁰

cc) Schritt 3: Analyse und Bewertung der Compliance-Risiken

- 80 Im dritten Schritt dieses Prozesses erfolgt die Analyse und Bewertung der identifizierten Compliance-Risiken. Dabei erfolgt zuerst eine inhaltliche Analyse. Demzufolge sind nun auch die unternehmensspezifischen CSR-Compliance-Risiken zu sichten, zu strukturieren und weiteren Untersuchungen zu unterziehen, „die den konkreten Bedürfnissen und Anforderungen des Unternehmens [hier: im Kontext Corporate Social Responsibility] Rechnung [tragen]“.¹⁵¹

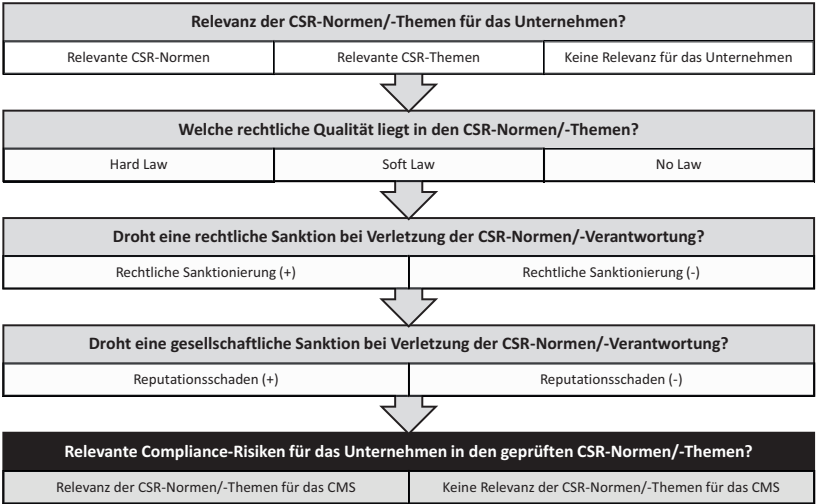


Abbildung 8: Idee zur Analyse und Bewertung von CSR-Normen und CSR-Themen hinsichtlich potenzieller Compliance-Risiken (eigene Darstellung)

- 81 Nach der Analyse erfolgt die Bewertung der identifizierten CSR-Compliance-Risiken (vgl. beispielhaft Abb. 8). Dabei kommt es zuerst auf die Bemessung

150 Vgl. Kark, Compliance-Risikomanagement, Rn. 651 ff., 667 ff.; Philippi, in: Bay/Hastenrath (Hrsg.), Compliance-Management-Systeme, § 3 Rn. 46 ff.

151 Vgl. Kark, Compliance-Risikomanagement, Rn. 742 ff., 746.

der erwarteten Schadenshöhe an.¹⁵² Mit Blick auf die bereits identifizierten CSR-Compliance-Risiken kann insbesondere hier überprüft werden, ob eine konkrete CSR-Norm bzw. ein konkretes CSR-Thema tatsächlich der Corporate Compliance zuzuordnen ist, denn es muss letztlich eine Schadensbemessung in Form einer konkreten Sanktion (wie z. B. Strafe, Geldbuße und/oder Gewinnabschöpfung) oder eines Reputationsschadens denkbar bzw. möglich sein.

Die Bewertung identifizierter CSR-Compliance-Risiken wird mit Prüfung der Eintrittswahrscheinlichkeit – u. a. anhand interner und externer Faktoren – abgeschlossen.¹⁵³ Die Integration in eine Compliance-Risikomatrix (einschließlich der Reputationsrisiken), ein Risikoportfolio und/oder in die Compliance-Risikolandkarte des Unternehmens ist davon mit umfasst.¹⁵⁴

dd) Schritt 4: Berichterstattung der Compliance-Risiken

Im vierten Schritt dieses Prozesses wird das Ergebnis über die analysierten und bewerteten CSR-Compliance-Risiken in einem Bericht verschriftlicht. Die Leitung der Corporate Compliance händigt diesen – nach Freigabe – dann u. a. an den Vorstand bzw. Geschäftsleiter des Unternehmens aus. Der Bericht stellt eine Grundlage dar, auf der die Unternehmensleitung eine informierte Entscheidung über die zukünftige Steuerung der unternehmensspezifischen CSR-Compliance-Risiken treffen kann.¹⁵⁵

ee) Schritt 5: Steuerung der Compliance-Risiken

Im fünften Schritt dieses Prozesses erfolgt die Steuerung der CSR-Compliance-Risiken. Ob und welche präventiven Maßnahmen in einem Unternehmen ergriffen werden, hängt vor allem von der Compliance-Strategie der Unternehmensleitung ab. In diesem Zusammenhang finden u. a. Aspekte wie z. B. die Compliance-Risikokapazität, die Compliance-Risikotoleranz, die Compliance-Risikogrenzen sowie die Ertragschancen des Unternehmens Beachtung. Im Rahmen der Compliance-Risikosteuerung kommen dann i. d. R. konkrete Maßnahmen zur Compliance-Risikovermeidung, Compliance-Risikoverminderung, Compliance-Risikobegrenzung sowie Compliance-Risikoweitergabe zur Anwendung. Die Entscheidung, ob und wie die unternehmensspezifischen CSR-Compliance-Risiken im Unternehmen zukünftig gesteuert werden, liegt letztlich im Ermessen der Geschäftsleitung (sog. „Business Judgement Rule“).¹⁵⁶

152 Vgl. Kark, Compliance-Risikomanagement, Rn. 747 ff., 751 ff.; Philippi, in: Bay/Hastenrath (Hrsg.), Compliance-Management-Systeme, § 3 Rn. 67 ff.

153 Vgl. Kark, Compliance-Risikomanagement, Rn. 767 ff.; Philippi, in: Bay/Hastenrath (Hrsg.), Compliance-Management-Systeme, § 3 Rn. 70 ff.

154 Vgl. Kark, Compliance-Risikomanagement, Rn. 782 ff., Abb. 17; Philippi, in: Bay/Hastenrath (Hrsg.), Compliance-Management-Systeme, § 3 Rn. 79 f.

155 Vgl. Kark, Compliance-Risikomanagement, Rn. 810 ff.; Philippi, in: Bay/Hastenrath (Hrsg.), Compliance-Management-Systeme, § 3 Rn. 116 ff.

156 Vgl. Kark, Compliance-Risikomanagement, Rn. 816 ff., 846; Philippi, in: Bay/Hastenrath (Hrsg.), Compliance-Management-Systeme, § 3 Rn. 87 ff.

ff) Schritt 6: Monitoring der Compliance-Risiken

- 85** Neben der Nachverfolgung, ob die definierten Steuerungsmaßnahmen umgesetzt worden sind, gehört zu diesem Prozessschritt u. a. auch die unterjährige Befassung mit der Compliance-Risikosituation. Im Hinblick auf den Schwerpunkt CSR ist daher zu prüfen, ob während des Jahres womöglich neue CSR-Risiken für das Unternehmen hinzugekommen sind.¹⁵⁷ Ausgehend von den Erkenntnissen aus dem Risikomonitoring können zudem gleich Verbesserungsmaßnahmen angestoßen werden.

b) Verknüpfung von CSR- und Compliance-Risiken

- 86** Im Interesse eines wirksamen Compliance-Management-Systems erscheint der rein regel- bzw. normenbasierter Ansatz allein weder ausreichend noch zeitgemäß zu sein.¹⁵⁸ Wie die normativen Erwartungen der Stakeholder von Unternehmen in der aktuellen CSR-Debatte zeigen, ist die Erweiterung der Compliance-Risikoanalyse um relevante CSR-Normen und CSR-Themen als zwingend erforderlich anzusehen, um Unternehmen auch wirksam vor Reputationsschäden im Zusammenhang mit CSR schützen zu können.

V. Zusammenfassung

- 87** Über die letzten Jahre hinweg haben die nationalen, supranationalen, internationalen und globalen Regulierungsmaßnahmen in Summe das Ausmaß einer wahren Flut an CSR-Normen angenommen, denen insbesondere international agierende Unternehmen ausgesetzt sind. Globale Wirtschaftskrisen haben diese Entwicklung noch einmal erheblich verschärft. Die Kommission der Europäischen Union argumentiert hierzu u. a.: „Die Wirtschaftskrise und ihre sozialen Folgen haben das Vertrauen in die Wirtschaft bis zu einem gewissen Grad erschüttert. Dadurch wurde die Öffentlichkeit für die Leistungen der Unternehmen auf sozialem und ethischem Gebiet sensibilisiert. Die [Europäische] Kommission erneuert ihre Anstrengungen zur CSR-Förderung jetzt um auf mittlere und lang[e] Sicht günstige Bedingungen für nachhaltiges Wachstum, verantwortungsvolles unternehmerisches Verhalten und die Entstehung dauerhafter Arbeitsplätze zu schaffen.“¹⁵⁹ Mit Blick auf die deutschen und europäischen Normierungen bzw. Normierungsvorhaben sowie deren aktuelle Auswirkungen auf die Wirtschaft, erhöhen die Unternehmer zugleich den Druck auf die Politik. Sie wollen es nicht länger hinnehmen, dass die Politik ihre Verantwortung immer weiter auf die Wirtschaft auslagert.¹⁶⁰

¹⁵⁷ Vgl. Kark, Compliance-Risikomanagement, Rn. 864 ff.; Philippi, in: Bay/Hastenrath (Hrsg.), Compliance-Management-Systeme, § 3 Rn. 98 ff.

¹⁵⁸ Vgl. → Schulz, Kap. 1 Rn. 71 ff. m. w. N.

¹⁵⁹ Vgl. KOM (2011) 681 endgültig, S. 5.

¹⁶⁰ Vgl. Lebensmittelzeitung Online v. 8.2.2024, <https://www.lebensmittelzeitung.net/politik/nachrichten/interview-mit-raoul-rossmann-und-christoph-werner-die-politik->

Gleichwohl stehen die Unternehmen weiter vor der großen Herausforderung, die für sie relevanten CSR-Normen und CSR-Themen herauszufiltern und mit ihrer Unternehmensstrategie in Einklang zu bringen. Gerade das jeweilige Kerngeschäft eines Unternehmens muss hierbei genauestens unter die Lupe genommen werden. Der Trend setzt sich weiter fort, dass der „Stakeholder Value“-Ansatz stetig an Bedeutung gewinnt. Daneben sind u.a. Fragen zur Rechtsqualität, Rechtssicherheit und Legitimation von CSR-Normen zu beantworten.¹⁶¹ In diesem Kontext sind die organisatorischen Vorkehrungen zur Vermeidung von Haftungsrisiken, Schadensersatzverpflichtungen, Straf- und Bußgeldern sowie Reputationsschäden zu überprüfen und zu aktualisieren. Hierbei handelt es sich um eine zentrale Aufgabe der Corporate Compliance eines Unternehmens. Durch die CSR-Normen und CSR-Themen gewinnt die Corporate Compliance unternehmensintern an Gewicht und Bedeutung. Im Ergebnis bedeutete dies nun, dass Compliance sich nicht mehr nur mit der juristischen Verantwortung, sondern vermehrt auch mit der gesellschaftlichen Verantwortung eines Unternehmens zu beschäftigen hat. Diese Entwicklung führt am Ende des Tages zu dem zwingenden Schluss, dass ein wirksames Compliance-Management-System heutzutage der Ergänzung des wertorientierten Integrity-Ansatzes bedarf.¹⁶²

kann-ihre-verantwortung-nicht-an-die-wirtschaft-auslagern-175996 (zuletzt abgerufen am 11.2.2024).

161 Vgl. dazu u. a. *Simons*, ZGR 2018, 316 ff.

162 Vgl. dazu u. a.: *Wieland*, in: *Wieland/Steinmeyer/Grüniger* (Hrsg.), *Handbuch Compliance Management*, S. 15–39; *Grüniger*, in: *Wieland/Steinmeyer/Grüniger* (Hrsg.), *Handbuch Compliance Management*, S. 41–71; siehe auch → *Schulz*, Kap. 1 Rn. 71 ff.

16. Kapitel

„ESG-Compliance“:

Herausforderungen des Nachhaltigkeitsreportings

I. Einleitung: Nachhaltigkeit, Corporate Governance und die Rolle von Compliance

Seit vielen Jahren schon ist mit einer gewissen Regelmäßigkeit in Veröffentlichungen jeder Art zu lesen, Nachhaltigkeit, oftmals synonym gebraucht mit Corporate Social Responsibility (CSR) oder den ESG-Kriterien und Rahmenbedingungen für die Berücksichtigung von Umwelt-, Nachhaltigkeits- und Sozialfragen (ESG – Environmental, Social, Governance) innerhalb von Unternehmensführungen, sei in aller Munde.¹ Die Diskussion über diese Themen sei aktueller denn je, Unternehmen hätten sich ihrer mehr denn je anzunehmen. 1

Nachhaltigkeit steht insoweit – in einem engen Kontext mit der Unternehmensethik – für einen Leitgedanken, der mit Blick auf die gesellschaftliche Verantwortung der Unternehmen einen unternehmensspezifisch zu konkretisierenden Handlungsrahmen gewährt. Im Grundsatz geht es darum, auf welche Art und Weise ein Unternehmen seine Gewinne erwirtschaftet. Tatsächlich verhält es sich faktisch so, dass der Begriff der Nachhaltigkeit bereits über eine längere Historie verfügt und seine Bedeutung im Einklang mit der insoweit deutlich wahrnehmbaren gesellschaftlichen Entwicklung – ungeachtet der inhärenten Interpretationsspielräume² – kontinuierlich zunimmt. Kaum jemand, der beruflich oder privat motiviert politische, wirtschaftliche oder gesellschaftliche Themen verfolgt, kommt umhin, sich mit ihm zu befassen – allein die Intensität dürfte variieren. Regelmäßig steht die Auseinandersetzung im engen Kontext mit Fehlentwicklungen in bestimmten Bereichen: Bezogen auf die Wirtschaft geht es so etwa um die Bankenkrise und Korruptionsskandale, um Fehlanreize bei der Management-Vergütung und um Unternehmensgewinne in Zeiten von Stellenabbau. 2

Die Ethik, konkret die sogenannte Wirtschaftsethik, wird in diesem Rahmen vielfach als Orientierungsrahmen mit herangezogen. Die Tugenden des „ehrbaren Kaufmanns“, kaufmännisch-unternehmerische Werte und eine Orientierung der Wirtschaftsunternehmen an verschiedensten „Stakeholder-Interessen“ sollen als wesentliche Bestandteile die „Good Corporate Governance“ in zunehmenden 3

1 Meier, Wirtschaftswoche v. 1.7.2013; Miegel, Frankfurter Allgemeine Feuilleton, 23.10.2013; Hardtke/Kleinfeld, in: Hardtke, Kleinfeld (Hrsg.), Gesellschaftliche Verantwortung von Unternehmen, Vorwort, S. 5 ff.; Ruter, CSR und Aufsichtsrat, in: Schneider/Schmidpeter, Corporate Social Responsibility, S. 1078.

2 Beisheim, Nachhaltigkeit: Eine Tour d’Horizon unter Berücksichtigung neuerer Rechtsentwicklungen, in: Habersack/Huber/Spindler, FS Stilz, 2014, S. 45, 48 ff. Zum CSR-Begriff ferner → Stehr/Knopp, Kap. 15 Rn. 11 ff. m. w. N.

dem Maße prägen. Wann aber gilt heutzutage das Buddenbrook'sche Mahnwort, die Maxime des Firmengründers Johann Buddenbrook: „Mein Sohn, sey mit Lust bey den Geschäften am Tage, aber mache nur solche, daß wir bey Nacht ruhig schlafen können“?³ Welche Werte sind dem wirtschaftsbezogenen Handeln beizumessen und welche Stakeholder sind aus der Unternehmensperspektive im Blick zu behalten? Welcher Rahmen ist bezogen auf Nachhaltigkeitsanforderungen und die gesellschaftliche Unternehmensverantwortung zu beachten und in welcher Form sollte über die diesbezügliche Positionierung berichtet werden? Fragen über Fragen stellen sich und jedenfalls bislang waren die Antworten wenig greifbar, weil über zahlreiche Soft-Law-Ansätze bzw. Selbst- oder Co-Regulierungen wie Reportingstandards und Verhaltenskodizes hinaus verbindliche Vorgaben kaum bzw. nur in wenigen Teilbereichen existierten.⁴ Dies änderte sich indes im Jahr 2017, als ESG-bezogen erstmals gesetzliche Berichtspflichten mit Blick auf die sogenannten nichtfinanziellen Informationen für spezifische Teile der Wirtschaft eingeführt wurden.

- 4 Am 5.1.2023 trat dann weitergehend die „Richtlinie (EU) 2022/2464 des Europäischen Parlaments und des Rates vom 14.12.2022 zur Änderung der Verordnung (EU) Nr. 537/2014 und der Richtlinien 2004/109/EG, 2006/43/EG und 2013/34/EU hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen“ (Corporate Sustainability Reporting Directive – CSRD)⁵ in Kraft. Sie führt zu gravierenden Änderungen insbesondere der Bilanzrichtlinie⁶ und zu einer umfassenden Fortentwicklung der nichtfinanziellen Berichtspflichten hin zu einer anspruchsvollen „Nachhaltigkeitsberichterstattung“ für breite Teile der Wirtschaft. Konkret geht es um eine eklatante Erweiterung des Anwendungsbereichs bzw. des Adressatenkreises der Berichtspflichten wie auch der Berichtsgegenstände und ihres Detaillierungsgrades sowie deren Verortung im Lagebericht mitsamt einer entsprechenden Prüfpflicht.
- 5 Dieser Buchbeitrag ist im Kern ausgerichtet auf Grundsatzfragen der unternehmerischen Verantwortung und der guten Unternehmensführung.⁷ Immer deutlicher wird die übergreifende Rolle von Compliance als wesentliches Element einer guten Corporate Governance und als integraler Bestandteil einer nachhaltigen, auf langfristige Wertschöpfung, Vertrauen und Reputationserhalt angeleg-

3 Mann, Buddenbrooks. Verfall einer Familie, 46. Aufl. 1999, S. 174.

4 Beisheim, in: Habersack/Huber/Spindler, FS Stilz, 2014, S. 45, 51; Schwarze, EuR 2011, 3, 4.

5 Richtlinie (EU) 2022/2464 des Europäischen Parlaments und des Rates vom 14.12.2022 zur Änderung der Verordnung (EU) Nr. 537/2014 und der Richtlinien 2004/109/EG, 2006/43/EG und 2013/34/EU hinsichtlich der „Nachhaltigkeitsberichterstattung von Unternehmen“ (Corporate Sustainability Reporting Directive – CSRD).

6 Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Jahresabschluss, den konsolidierten Abschluss und damit verbundene Berichte von Unternehmen bestimmter Rechtsformen und zur Änderung der Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinien 78/660/EWG und 83/349/EWG des Rates (Bilanz-Richtlinie).

7 Siehe hierzu auch → Schulz, Kap. 1 Rn. 9 f. m. w. N.

ten Unternehmensführung. Diese ist zudem gekennzeichnet von Transparenz und einer Nachvollziehbarkeit der Entscheidungen, einem angemessenen Umgang mit Risiken und der Wahrung der Interessen der Stakeholder – nicht mehr nur der Shareholder.⁸

Die ursprünglich rein regelbasierte Compliance schließt längst mehr und mehr ethische Aspekte mit ein („Compliance 2.0“).⁹ Dieses bereits wertebezogen erweiterte Verständnis¹⁰ kann eine gute Basis für hieran anknüpfende Aktivitäten auch im Bereich der ESG-Compliance sein („Compliance 3.0“). Die künftig notwendige Sicherstellung und Überwachung der Einhaltung der neuen Regelwerke eröffnet der Compliance-Funktion die Möglichkeit neuer Wertschöpfungsbeiträge.

Mit dem Inkrafttreten der „Richtlinie 2014/95/EU des EU-Parlaments und des Rates vom 22.10.2014 im Hinblick auf die Angabe nichtfinanzieller und die Diversität betreffender Informationen“ (verkürzt: „CSR-Richtlinie“ oder auch nur „Richtlinie“) am 5.12.2014 fand im Bereich der Nachhaltigkeitsberichterstattung ein Paradigmenwechsel statt.¹¹ Erstmals ging es um eine für wesentliche Teile der Wirtschaft grundlegende Entwicklung weg von der bisherigen Freiwilligkeit des Reportings und damit letztlich auch der zugrunde liegenden Aktivitäten, hin zu entsprechenden Verpflichtungen. Mit der Richtlinie 2014/95/EU wurde die für das Bilanzrecht zuvor zentrale Richtlinie 2013/34/EU um neue Vorgaben zur nichtfinanziellen Berichterstattung und im Hinblick auf Diversitätskonzepte für die Besetzung von Leitungsorganen ergänzt. Die Richtlinie war bis zum 6.12.2016 von den Mitgliedstaaten in nationales Recht zu überführen, um ihre erstmalige Anwendung im Geschäftsjahr 2017 sicherzustellen. Der deutsche Gesetzgeber kam dieser Anforderung mit dem „CSR-Richtlinie-Umsetzungsgesetz“ (CSR-RUG) etwas verspätet nach, das am 19.4.2017 in Kraft trat und eine nahezu Eins-zu-eins-Umsetzung der CSR-Richtlinie im Wesentlichen durch Änderungen des HGB und AktG enthielt.¹² Diese Entwicklung setzt sich mit dem Inkrafttreten der CSRD am 5.1.2023 und der Veröffentlichung der ersten Europäischen Standards für die Nachhaltigkeitsberichterstattung (European Sustainability Reporting Standards, ESRS) am 22.12.2023 fort. An diesem Tag wurde der delegierte Rechtsakt zum sog. Set 1 der ESRS¹³ im EU-Amtsblatt veröffent-

8 Mühlbert, AG 2009, 766, 768; *Fleischer*, in: Spindler/Stilz, AktG, 4. Aufl. 2019, § 76 Rn. 34.

9 Grundlegend *Grüninger*, Werteorientiertes Compliance Management-System, in: Wieland/Steinmeyer/Grüninger, Handbuch Compliance Management, 2. Aufl. 2014, S. 41 ff.; *Wieland*, Integritäts- und Compliance Management als Corporate Governance, ebenda, S. 15 ff.

10 Vgl. hierzu → *Schulz*, Kap. 1 Rn. 1 ff. m. w. N.

11 Richtlinie 2014/95/EU des Europäischen Parlaments und des Rates vom 22.10.2014 zur Änderung der Richtlinie 2013/34/EU im Hinblick auf die Angabe nichtfinanzieller und die Diversität betreffender Informationen durch bestimmte große Gruppen und Unternehmen; ABl. L 330 v. 15.11.2014, 1; ABl. L 369 v. 24.12.2014, 79 (sprachliche Berichtigung); *Spießhofer*, NZG 2014, 1281, 1282.

12 BGBl. I 2017, S. 802–814; BT-Drs. 18/9982, S. 30.

13 Delegierte Verordnung (EU) 2023/2772.

licht. Die durch die CSRD geänderte Bilanzrichtlinie verpflichtet bestimmte EU-Unternehmen sowie EU-Tochterunternehmen oder -Niederlassungen von Drittstaatenunternehmen, die ESRS anzuwenden. Sämtliche ESRS, es folgen u. a. noch sektorspezifische ESRS, werden – nach fachlicher Ausarbeitung durch die EFRAG – nach Art. 29b, 29c und 40b BilanzRL als delegierte Rechtsakte durch die Europäische Kommission erlassen. Nachdem in Deutschland von der CSR-Richtlinie bzw. dem CSR-RUG zunächst lediglich ca. 550 sog. „große Unternehmen von öffentlichem Interesse“ erfasst wurden, weitet sich zukünftig der Adressatenkreis der Nachhaltigkeitsberichtspflichtigen eklatant aus. Allein in Deutschland werden mehr als 15.000 Unternehmen berichtspflichtig, europaweit handelt es sich um annähernd 50.000 Unternehmen.

II. Status quo und bald Historie: Die CSR-Richtlinie und das CSR-Richtlinie-Umsetzungsgesetz von 2017

1. Zielsetzungen der CSR-Richtlinie und des CSR-Richtlinie-Umsetzungsgesetzes

- 8 Mit der CSR-Richtlinie sowie mit dem CSR-RUG wurden zwei zentrale, miteinander zusammenhängende Ziele verfolgt: die Information der Adressaten der Berichterstattung über nichtfinanzielle Themen und die mittelbare Steuerung des Verhaltens der berichtspflichtigen Unternehmen.
- 9 Angelegt war die regulatorische Tendenz zur Gewährleistung der Wahrnehmung der gesellschaftlichen Verantwortung der Unternehmen bereits seit einigen Jahren. So war bereits die „Binnenmarktakte – Zwölf Hebel zur Förderung von Wachstum und Vertrauen“ der EU-Kommission vom 13.4.2011 darauf ausgerichtet, EU-weit mit Blick auf Unternehmen aller Branchen eine Verbesserung der Transparenz in der Sozial- und Umweltberichterstattung und ein vergleichbar hohes Niveau zu erreichen.¹⁴ Insbesondere die Mitteilung der Kommission vom 25.10.2011 „Eine neue EU-Strategie (2011–14) für die soziale Verantwortung der Unternehmen (CSR)“ schuf indes die Basis für weitere spezifische Maßnahmen zur Beförderung eines verstärkten unternehmerischen Nachhaltigkeitsengagements auf EU- und nationalstaatlicher Grundlage.¹⁵ Die Mitteilung zielte so etwa auch darauf ab, einen Vorschlag für eine Rechtsvorschrift über die Transparenz der sozialen und ökologischen Informationen von Unternehmen aller Branchen zu entwickeln. Die CSR-Richtlinie setzte dann in Verbindung mit dem deutschen CSR-RUG ein wesentliches Element der neuen EU-Strategie um.
- 10 Ausweislich der in den Erwägungsgründen zur CSR-Richtlinie zitierten „Entschließung des EU-Parlaments vom 6.2.2013 zur sozialen Verantwortung der Unternehmen“ ging es insgesamt um ein „rechenschaftspflichtiges, transparentes und verantwortungsvolles Geschäftsgebaren, um soziale Verantwortung“

¹⁴ KOM(2011) 206 endg.

¹⁵ KOM(2011) 681 endg.

und ganz allgemein um eine Förderung der Interessen der Gesellschaft.¹⁶ Der Offenlegung von Informationen zur Nachhaltigkeit durch Unternehmen komme eine große Bedeutung zu, um diesbezügliche Gefahren aufzuzeigen und das Vertrauen von Investoren und Verbrauchern zu gewährleisten. Die konsistente und vergleichbare Angabe nichtfinanzieller Informationen durch die Unternehmen sollte helfen, das Geschäftsergebnis von Unternehmen und ihre Auswirkungen auf die Gesellschaft zu messen, zu überwachen und zu handhaben. Langfristige Rentabilität als Zielsetzung wurde mit sozialer Gerechtigkeit und Umweltschutz verbunden, die Angabe nichtfinanzieller Informationen als ein wesentliches Element der Bewältigung des Übergangs hin zu einer nachhaltigen globalen Wirtschaft begriffen.

Das CSR-RUG hob dementsprechend die zunehmende Bedeutung der Unternehmenskommunikation mit Blick auf nichtfinanzielle Informationen für die Wirtschaft hervor. Insbesondere große Unternehmen, Investoren, aber auch Verbraucherinnen und Verbraucher bewerteten die Unternehmen, mit denen sie Geschäfte machen, längst nicht mehr nur nach ihren Finanzdaten. Zur Anbahnung eines geschäftlichen Kontakts oder in ihrer laufenden Geschäftsbeziehung erwarteten sie ein Mehr an unternehmensspezifischen Informationen. Im Kern gehe es um Vertrauensbildung. Aus Sicht jedes Unternehmens selbst seien nichtfinanzielle Aspekte, nicht zuletzt auch aufgrund der fortschreitenden Globalisierung und der diesbezüglich hohen medialen Sensibilität, deshalb von immer größerer Bedeutung als Entscheidungsfaktoren etwa im Rahmen des Risikomanagements.¹⁷ Ihr Handeln sollte gleichsam über die Berichterstattung zu nichtfinanziellen Belangen beeinflusst werden; den diesbezüglichen Aspekten sollte – einerseits unter Beibehalt eines gewissen Maßes an Handlungsflexibilität, andererseits unter Gewährleistung einer weitgehenden Vergleichbarkeit im Reporting – zukünftig ein deutlich stärkeres Gewicht in der Unternehmensführung beigemessen werden. **11**

2. Neuausrichtung des Nachhaltigkeitsreportings

Aktivitäten auf dem Gebiet der CSR-Berichterstattung über nichtfinanzielle und die Diversität betreffende Informationen waren schon damals nicht grundsätzlich neu und fanden sich vor unterschiedlichen Hintergründen in durchaus weiteren Teilen der deutschen Wirtschaft, insbesondere in größeren Unternehmen. Einerseits bestanden – nur begrenzte – Anforderungen im deutschen Bilanzrecht, andererseits gab es vielgestaltige freiwillige Reportingansätze im Rahmen von Selbstregulierungen nach Maßgabe internationaler und nationaler Berichtsstandards. **12**

16 Entschließung des Europäischen Parlaments vom 6.2.2013 zur sozialen Verantwortung der Unternehmen: Förderung der Interessen der Gesellschaft und ein Weg zu einem nachhaltigen und integrativen Wiederaufschwung (2012/2097(INI)).

17 BT-Drs. 18/9982, S. 1.

a) Bereits vor dem CSR-RUG vorhandene nichtfinanzielle Berichtspflichten im deutschen Bilanzrecht

- 13 Schon langjährig bestehen für große Kapitalgesellschaften im Sinne des § 267 Abs. 3 HGB und über einen Verweis auf § 264d HGB auch für kapitalmarkt-orientierte Unternehmen Verpflichtungen nach § 289 Abs. 3 HGB, im Lagebericht Informationen zu nichtfinanziellen Leistungsindikatoren vorzusehen, soweit diese für das Verständnis des Geschäftsverlaufs oder der Lage der Gesellschaft von Bedeutung sind. Nach § 315 Abs. 3 HGB (§ 315 Abs. 1 HGB a.F.) gilt eine entsprechende Informationspflicht für den Konzernlagebericht. Große Kapitalgesellschaften überschreiten mindestens zwei der drei Merkmale nach § 267 Abs. 2 HGB a. F. (20 Mio. EUR Bilanzsumme, 40 Mio. EUR Umsatzerlöse in den zwölf Monaten vor dem Abschlussstichtag, im Jahresdurchschnitt 250 Arbeitnehmer).¹⁸ Exemplarisch verweisen die Normen auf Informationen über Umwelt- und Arbeitnehmerbelange. In der Praxis beziehen sich die in diesem Kontext erteilten Informationen im Schwerpunkt bislang auf den Personal- und Sozialbereich. In zunehmendem Maße, wenngleich insgesamt von untergeordneter Bedeutung, finden sich in den Lageberichten aber auch Angaben zu umweltbezogenen Aspekten und ferner zu reputationsbezogenen Themen.
- 14 Anzumerken ist, dass der Begriff der nichtfinanziellen Leistungsindikatoren in den Grundsätzen der Rechnungslegung bis Ende 2012 keine weitergehende Konkretisierung erfahren hatte. Dies änderte sich erst mit der Verabschiedung des Deutschen Rechnungslegungs Standards Nr. 20 (DRS 20 – Konzernlagebericht) durch das Deutsche Rechnungslegungs Standards Committee (DRSC) und dessen Bekanntmachung nach § 342 Abs. 2 HGB.¹⁹ Nach DRS 20.105/106 sind die bedeutsamsten nichtfinanziellen Leistungsindikatoren – auf Konzernebene – in die Analyse des Geschäftsverlaufs und der Lage des Konzerns einzubeziehen, soweit sie für das Verständnis des Geschäftsverlaufs und der Lage von Bedeutung sind und sofern sie zur internen Steuerung herangezogen werden. DRS 20.107 benennt in Ausformung der bisherigen HGB-Vorgaben beispielhaft folgende nichtfinanzielle Leistungsindikatoren, also diesbezügliche Faktoren zur Beurteilung von Aspekten der qualitativen oder quantitativen Leistung eines Unternehmens:
- Kundenbelange (Indikatoren zum Kundenstamm, Kundenzufriedenheit etc.),
 - Umweltbelange (Emissionswerte, Energieverbrauch etc.),
 - Arbeitnehmerbelange (Indikatoren zur Mitarbeiterfluktuation, Mitarbeiterzufriedenheit, Betriebszugehörigkeit, Fortbildungsmaßnahmen etc.),
 - Indikatoren zur Forschung und Entwicklung und
 - gesellschaftliche Reputation (Indikatoren zum sozialen und kulturellen Engagement, Wahrnehmung gesellschaftlicher Verantwortung etc.).

18 § 267 HGB in den Schwellenwerten geändert mit Wirkung ab dem 17.4.2024 durch das Zweite Gesetz zur Änderung des DWD-Gesetzes sowie zur Änderung handelsrechtlicher Vorschriften (BT-Drs. 20/10032, 20/10828).

19 Verabschiedung am 2.11.2012, Bekanntmachung der deutschsprachigen Fassung gem. § 342 Abs. 2 HGB durch das Bundesministerium der Justiz am 4.12.2012.

Ganz im Sinne eines sukzessive stärkeren Einbezugs ökologischer und sozialer Aspekte der Geschäftstätigkeit in die Finanzberichterstattung verfolgte auch das DRSC mit der in verschiedener Hinsicht vorgenommenen Angleichung der Regelungen zur nichtfinanziellen Berichterstattung an das klassische finanzielle Reporting die Richtung, der Wertigkeit der nichtfinanziellen Berichterstattung Rechnung zu tragen. In der Praxis indes verfindet dieser Ansatz auch ausweislich von Studien kaum.²⁰ **15**

Letztlich verpflichtete § 289a HGB a.F. bzw. aktuell (noch)²¹ § 289f HGB börsennotierte Aktiengesellschaften und Kommanditgesellschaften auf Aktien sowie andere in der Norm näher bezeichnete emittierende Aktiengesellschaften zur Abgabe einer Erklärung zur Unternehmensführung im Lagebericht oder, unter dortiger Inbezugnahme, auf der Unternehmens-Homepage. In die Erklärung zur Unternehmensführung waren bereits nach § 289a Abs. 2 Nr. 2 HGB a. F. bzw. aktuell (noch) § 289f Abs. 2 Nr. 2 HGB – sehr weich formuliert – „relevante Angaben zu Unternehmensführungspraktiken, die über die gesetzlichen Anforderungen hinaus angewandt werden“ aufzunehmen. Auch in diesem Kontext kam schon damit etwa eine Berichterstattung zu Arbeits- und Sozialbelangen sowie ferner zu ethischen Gesichtspunkten in Betracht. **16**

b) Sog. Soft-Law-Ansätze als Rahmenwerke für das CSR-Reporting

Die Berichterstattung zahlreicher Unternehmen zu Themen der gesellschaftlichen Verantwortung erfolgte zuvor aus unterschiedlichen Motiven heraus auf freiwilliger Grundlage. Tendenziell engagieren sich bislang eher größere Gesellschaften, doch auch KMU berichten, sei es vor dem Hintergrund spezifischer Situationen im Unternehmen, in Branchen oder generell im Markt. Diese Berichte werden regelmäßig auf der Grundlage internationaler oder nationaler Rahmenwerke erstellt. Als solche kommen ihrer Bedeutung bzw. Verbreitung nach insbesondere der „UN Global Compact“,²² die „OECD Leitsätze für multinationale Unternehmen“²³ und die „GRI Standards“²⁴ in Betracht; sie werden neben weiteren Standards im Rahmen der Erwägungsgründe zur CSR-Richtlinie als aner- **17**

20 *Lanfermann*, CSR in Berichterstattung und Bilanzrecht, in: Walden/Depping, CSR und Recht, S. 115 m. w. N.

21 Insbesondere die §§ 289b ff. HGB werden zukünftig durch das Gesetz zur Umsetzung der Richtlinie (EU) 2022/2464 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 zur Änderung der Verordnung (EU) Nr. 537/2014 und der Richtlinien 2004/109/EG, 2006/43/EG und 2013/34/EU hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen („CSRD UmsetzungsG“, Referentenentwurf Bearbeitungsstand: 22.3.2024) umfassend umgestaltet.

22 Siehe www.globalcompact.de.

23 Siehe <https://www.oecd.org/publications/oecd-leitsatze-fur-multinationale-unternehmen-zu-verantwortungsvollem-unternehmerischem-handeln-abd4d37b-de.htm> (Stand 4.9.2023).

24 Siehe <https://www.globalreporting.org/how-to-use-the-gri-standards/gri-standards-german-translations/> (Stand 16.1.2023).

kannte Rahmenwerke aufgeführt.²⁵ In der Begründung zum CSR-RUG findet sich aber exemplarisch auch etwa der „Deutsche Nachhaltigkeitskodex“, der zudem ebenfalls seitens der EU-Kommission explizit geschätzt wird.²⁶

c) Paradigmenwechsel

- 18** Vordergründig betrachtet ging es bei der seitens der EU-Kommission angestoßenen Neuausrichtung der Nachhaltigkeitsberichterstattung um eine Abkehr vom bisherigen Freiwilligkeitsgrundsatz. Bestimmte Teile der deutschen Wirtschaft sollten zukünftig entsprechenden Verpflichtungen unterliegen. Das insoweit veränderte Verständnis von der Bedeutung und der Funktion der Corporate Social Responsibility bildete sich bereits grundhaft in der Entwicklung der CSR-Definitionen auf EU-Ebene ab. Verstand man Anfang des neuen Jahrtausends unter CSR noch „ein Konzept, das den Unternehmen als Grundlage dient, auf freiwilliger Basis soziale Belange und Umweltbelange in ihre Unternehmenstätigkeit und in die Wechselbeziehungen mit den Stakeholdern zu integrieren“, ²⁷ umschreibt die Europäische Kommission CSR seit 2011 in einem sehr viel breiter angelegten Ansatz als „Verantwortung von Unternehmen für ihre Auswirkungen auf die Gesellschaft“. ²⁸ Es geht damit nicht mehr nur um Fragen der Werthaltigkeit des Unternehmens, wie sie bislang im Mittelpunkt des bilanziell ausgerichteten Reportings zu nichtfinanziellen Leistungsindikatoren nach den Vorschriften des HGB standen, sondern weitergehend, so auch nach Maßgabe der Erwägungsgründe zur CSR-Richtlinie, um ein gegenüber der Gesellschaft insgesamt verantwortungsvolles, transparentes und interessengerechtes Geschäftsgebaren.
- 19** Eine Wertung dieser Veränderung als Paradigmenwechsel liegt nahe, ²⁹ verhaltenssteuernde Elemente der neuen Vorgaben waren deutlich wahrnehmbar und wurden ebenfalls in der Begründung zum CSR-RUG hervorgehoben. ³⁰ Eine Verhaltenslenkung erfolgte insoweit, als seither gegenüber sämtlichen Stakeholdern des Unternehmens – über deutlich präzisere Angaben – Transparenz über die verschiedenen im jeweiligen Kontext relevanten nichtfinanziellen Risikofaktoren und deren Management herzustellen ist. Dieser weite Ansatz erfasst indes nicht nur Risiken im Kontext normativer Vorgaben jeder Art, sondern auch die Einhaltung außerrechtlicher „Standards“ – eben soweit ein relevanter „Impact“ des Unternehmens auf die Gesellschaft gegeben ist. ³¹ Gegebenenfalls sind dem-

25 Richtlinie 2014/95/EU, Erwägungsgrund 9.

26 Siehe www.deutscher-nachhaltigkeitskodex.de; BT-Drs. 18/9982, S. 46, 52; IP/13/330 vom 16.4.2013; vgl. zur Verwendung von Rahmenwerken zur Berichterstattung → Rn. 49 ff.

27 KOM(2001) 366 endg.; GRÜNBUCH Europäische Rahmenbedingungen für die soziale Verantwortung der Unternehmen, Rn. 8, 20.

28 KOM(2011) 681 endg.; Mitteilung „Eine neue EU-Strategie (2011–14) für die soziale Verantwortung der Unternehmen; Ziff. 3. Ein modernes Verständnis ...; – Ziff. 3.1. Eine neue Definition.“

29 *Eufinger*, EuZW 2015, 424, 424; *Spießhofer*, NZG 2014, 1281, 1282.

30 BT-Drs. 18/9982, S. 26.

31 So auch *Spießhofer*, NZG 2014, 1281, 1282.

nach rechtlich zulässige, aber aus anderen Gründen etwa ethisch zu hinterfragende Sachverhalte im Rahmen der Geschäftstätigkeit aufzuzeigen – möglicherweise auch nur in einem weiteren Zusammenhang hiermit. Neben Normen konstituieren eben auch Werte die Gesellschaft; eine risikoorientierte Betrachtung im gegebenen Rahmen wird also insgesamt auf Gemeinwohlbezüge ausgerichtet sein bzw. diese zu berücksichtigen haben.

Bezogen auf das Diversitätskonzept hat sich letztlich ein modifizierter Adressatenkreis zukünftig auf eine intensivere Art und Weise mit deutlich mehr relevanten Aspekten auseinanderzusetzen. **20**

3. Adressaten der CSR-Berichtspflichten nach dem CSR-RUG

Die Berichtspflichten finden der Richtlinie zufolge Anwendung auf große Unternehmen von öffentlichem Interesse, die unter das Recht eines EU-Mitgliedstaats fallen und im Geschäftsjahr durchschnittlich mehr als 500 Mitarbeiter beschäftigen. Unternehmen oder Gruppen von öffentlichem Interesse sind nach Art. 2 Nr. 1 der EU-Bilanzrichtlinie (RL 2013/34/EU) kapitalmarktorientierte Unternehmen, Kreditinstitute und Versicherungsunternehmen. Den Mitgliedstaaten der EU stand weitergehend (wie auch bezogen auf verschiedene andere Aspekte) ein sogenanntes Mitgliedstaatenwahlrecht zu, von dem der deutsche Gesetzgeber jedoch keinen Gebrauch gemacht hat. **21**

§ 289b Abs. 1 HGB übernahm für die nichtfinanzielle Erklärung und die Berichtsvarianten mit Blick auf den Adressatenkreis den Anwendungsbereich der Richtlinie 1:1. Die Norm richtet sich seither damit zunächst an Kapitalgesellschaften – AG, KGaA, GmbH –, wenn diese „groß“ im Sinne des § 267 Abs. 3 Satz 1, Abs. 4 bis 5 HGB sind, kapitalmarktorientiert im Sinne des § 264d HGB sind und im Jahresdurchschnitt mehr als 500 Arbeitnehmer beschäftigen. Diese Kriterien sind darüber hinaus auch entsprechend auf nach anderen, besonderen Vorschriften berichtspflichtige Gesellschaften unterschiedlicher Rechtsformen wie Genossenschaften oder haftungsbeschränkte Personenhandelsgesellschaften anzuwenden (ausführlich siehe → Rn. 27 ff.).³² **22**

Im Rahmen von § 267 Abs. 3 Satz 1 HGB haben große Gesellschaften zwei der drei in der Norm enthaltene Kriterien zu erfüllen; im gegebenen Kontext bedarf es damit einer Bilanzsumme von über 20 Mio. EUR oder Umsatzerlösen von über 40 Mio. EUR³³ und der – im hier gegebenen Kontext wie aufgezeigt modifizierten und zwingend erforderlichen – Mindestbeschäftigtenanzahl. Sowohl mangels Verweis in § 289b Abs. 1 Satz 1 Nr. 1 HGB auf § 267 Abs. 3 Satz 2 HGB als auch explizit laut der Gesetzesbegründung zum CSR-RUG müssen die Größenkriterien nach § 267 Abs. 3 Satz 1 HGB tatsächlich erfüllt sein, insbesondere die Fiktion des § 267 Abs. 3 Satz 2 HGB dahingehend, dass eine kapital- **23**

³² BT-Drs. 18/9982, S. 44, 60 f.; *Stawinoga/Velte*, DB, 2016, 841, 842.

³³ Inflationsbedingte Umsetzung neuer Schwellenwerte (Bilanzsumme: 25 Mio. EUR, Umsatz 50 Mio. EUR) erfolgte mit Wirkung zum 17.4.2024, s. → Fn. 18.

marktorientierte Kapitalgesellschaft im Sinne des § 264d HGB stets als „groß“ gilt, ist insoweit nicht anwendbar.³⁴

- 24** Entsprechendes gilt nach § 315b Abs. 1 Satz 1 HGB für die Unternehmen des Adressatenkreises, die Mutterunternehmen einer großen Gruppe sind. Sofern Tochterunternehmen in einen Konzernabschluss einbezogen werden und das Mutterunternehmen eine „konsolidierte nichtfinanzielle Erklärung“, d.h. eine nichtfinanzielle Erklärung im Konzernlagebericht oder einen gesonderten nichtfinanziellen Konzernbericht abgibt, sind die Tochterunternehmen von der Pflicht zur eigenständigen Berichterstattung (nicht aber von den Berichtspflichten betreffend die Diversität in der Erklärung zur Unternehmensführung) nach § 289b Abs. 2 HGB bzw. § 315b Abs. 2 HGB befreit. Eine konzernweite Erklärung soll in diesem Fall genügen und den Berichtsaufwand reduzieren. Die Tochterunternehmen haben ihrerseits dann lediglich den Sachverhalt im Rahmen ihres Lageberichts zu erläutern sowie das berichtende Mutterunternehmen und den Ort der Veröffentlichung in deutscher oder englischer Sprache anzugeben. Die durchschnittliche Mitarbeiteranzahl wird bei einem Reporting nur auf Konzernebene auf einer konsolidierten Basis berechnet.
- 25** Große Kreditinstitute und Versicherungsunternehmen werden unabhängig von einer Kapitalmarktorientierung unter den im Übrigen gleichen Voraussetzungen wie bei § 289b Abs. 1 HGB über die modifizierten Spezialvorschriften der §§ 340a Abs. 1a Satz 1, 341a Abs. 1a Satz 1 HGB bzw. als Konzerne über §§ 340i Abs. 5 Satz 1, 341j Abs. 4 Satz 1 HGB erfasst. Die Vorgaben gelten in beiden Branchen unabhängig von der konkret gewählten Rechtsform, da der Gesetzgeber einen Wettbewerb über die Rechtsformen verhindern möchte und alle Unternehmen den gleichen bilanzrechtlichen Vorgaben unterliegen sollen.³⁵
- 26** Für Europäische Gesellschaften (SE) sind die CSR-Reportingvorgaben nach Art. 61 der Verordnung (EG) Nr. 2157/2001 des Rates vom 8.10.2001 über das Statut der Europäischen Gesellschaft entsprechend anwendbar.
- 27** Über den Verweis des § 264a Abs. 1 HGB werden in der deutschen Gesetzessystematik zudem bestimmte kapitalgesellschaftsähnliche Personengesellschaften in den Anwendungsbereich der Vorgaben einbezogen. Namentlich gilt dies für offene Handelsgesellschaften und Kommanditgesellschaften, bei denen ausschließlich Kapitalgesellschaften oder aber neben Kapitalgesellschaften etwa Genossenschaften oder Stiftungen (und eben nicht auch natürliche Personen) persönlich haftende Gesellschafter sind, insbesondere also für die GmbH & Co. KG. Die Abschlusspublizität wird als notwendiger Ausgleich für die Haftungsbeschränkung betrachtet.

³⁴ BT-Drs. 18/9982, S. 44.

³⁵ Für Kreditinstitute: Richtlinie 86/635/EWG vom 8.12.1986 (ABl. L 372 v. 31.12.1986, 1); für Versicherungsunternehmen: Richtlinie 91/674/EWG vom 19.12.1991 (ABl. L 374 v. 31.12.1991, 7); vgl. auch BT-Drs. 18/9982, S. 61 f.

Gleichermaßen werden Genossenschaften – inklusive Europäischer Genossenschaften (SCE) gemäß Art. 68 VO (EG) 1435/2003 – nach näherer Maßgabe der §§ 336 ff. HGB originär von den Berichtspflichten erfasst (vgl. § 336 Abs. 2 Satz 1 Nr. 2 HGB). Die Rechtsform der Genossenschaft kann in ähnlicher Weise für eine Unternehmenstätigkeit genutzt werden wie Kapitalgesellschaften. Der Gesetzgeber sieht insoweit explizit ein Bedürfnis nach Gleichstellung, weil die Rechtsformwahl nicht durch unterschiedliche Vorgaben des Handelsbilanzrechts beeinflusst werden soll.³⁶ **28**

Sog. „Kleinstunternehmen“, kleinen und mittleren Unternehmen (KMU) sollen der Begründung zur Richtlinie und der Gesetzesbegründung zufolge keine zusätzlichen Anforderungen auferlegt werden.³⁷ Gleichwohl ist nicht zu verkennen, dass die neuen Berichtsvorgaben mittelbare Auswirkungen auch auf diese Gesellschaften haben. Vor dem Hintergrund spezifischer Berichtspflichten der originären Adressaten zu deren Geschäftsbeziehungen, Produkten und Dienstleistungen nach § 289c Abs. 3 Nr. 4 HGB erfolgt vielfach eine Weitergabe von Berichtspflichten im Rahmen der Vertrags- bzw. Lieferkette auch an KMU. Schon bislang vereinbaren Unternehmen mit Geschäftspartnern vor Compliance- bzw. CSR-Hintergründen die Angabe spezifischer Informationen, um auf dieser Grundlage in der Folge eigenen (Selbst-)Verpflichtungen nachkommen zu können. Gerade größere Gesellschaften dringen mit solchen Anliegen vertraglicher Vereinbarungen aufgrund ihrer Marktposition regelmäßig durch; für KMU bedingt dieses Vorgehen dann Mehraufwände. Die Begründung zur CSR-Richtlinie merkt unter Erwägungsgrund 8 an, dass dieser Zusammenhang „nicht zu übermäßigem Verwaltungsaufwand für kleine und mittlere Unternehmen führen“ sollte. Die Zielrichtung greift das CSR-RUG ebenfalls auf. In seiner Begründung wird unter Hinweis auf zu vermeidende Belastungen für den deutschen Mittelstand, auf das dem deutschen Bilanzrecht innewohnende System der Abstufung von Berichtsanforderungen nach der Unternehmensgröße und auf Erwartungen der Allgemeinheit eine Ausweitung der Anwendung auf KMU als zumindest derzeit nicht angezeigt gewertet.³⁸ **29**

4. Berichtsansforderungen im Rahmen des Reportings nach der bislang geltenden CSR-Richtlinie

a) Berichtsvarianten: Die nichtfinanzielle Erklärung und der gesonderte Bericht

Der Lagebericht der von den bisherigen Berichtspflichten erfassten Unternehmen hat nach den §§ 289b Abs. 1, 289c HGB in einem besonderen Abschnitt *oder* vollständig in den Lagebericht integriert eine sogenannte nichtfinanzielle **30**

³⁶ BT-Drs. 18/9982, S. 60. Bemerkenswerterweise bildet sich diese Sicht indes im Referentenentwurf zum CSRD-Umsetzungsgesetz vom 22.3.2024, der Genossenschaften nicht adressiert, nicht ab.

³⁷ Richtlinie 2014/95/EU, Erwägungsgründe 8, 13, 14; BT-Drs. 18/9982, S. 2, 40, 51.

³⁸ BT-Drs. 18/9982, S. 44.

Erklärung mit Angaben zur Nachhaltigkeit des unternehmerischen Handelns aufzuweisen. Einzelne Mitgliedstaaten konnten nach der CSR-Richtlinie unter bestimmten Bedingungen einen „gesonderten Bericht“ anstelle der nichtfinanziellen Erklärung und damit außerhalb des Lageberichts anerkennen. Der deutsche Gesetzgeber machte von dieser Möglichkeit in § 289b Abs. 3 HGB Gebrauch und eröffnete – im Verhältnis zu den bisherigen handelsrechtlichen Informationspflichten – einen weiteren flexiblen Weg in der Berichterstattung. Nach dieser Norm sind berichtspflichtige Unternehmen von der Angabe einer nichtfinanziellen Erklärung im Lagebericht befreit, wenn ein gesonderter Bericht nach bestimmten Maßgaben erstellt und – spezifisch – veröffentlicht wird. Nach § 289b Abs. 3 HGB konnte der gesonderte nichtfinanzielle Bericht als eigenständiger Unternehmensbericht oder als Bestandteil eines anderen Unternehmensberichtes – wiederum als besonderer Abschnitt oder vollständige Integration – verfasst werden. Der gesonderte nichtfinanzielle Bericht hatte inhaltlich den Anforderungen an eine nichtfinanzielle Erklärung nach § 289c HGB zu entsprechen; auch die weiteren Rahmenbedingungen der nichtfinanziellen Erklärung gelten in dieser Variante der Berichterstattung (vgl. § 289b Abs. 3 Satz 2 HGB). Er muss sich auf dasselbe Geschäftsjahr beziehen, über das auch anderweitig berichtet wird, und ist entweder gemeinsam mit dem Lagebericht zu veröffentlichen oder – was eine gewisse Flexibilität mit sich bringen wird – binnen maximal vier Monaten nach dem Bilanzstichtag auf der Homepage des Unternehmens. In letzterem Falle ist im Lagebericht ein Verweis auf die Homepage-Veröffentlichung vorzusehen. Die Veröffentlichung ist ferner für mindestens 10 Jahre auf der Internetseite aufrechtzuerhalten, um ein hohes Maß an Transparenz für die Stakeholder herzustellen und eine nachhaltige Vergleichbarkeit in der Berichterstattung zu gewährleisten.

- 31 Die §§ 315b und 315c HGB regeln die entsprechenden Pflichten auf der Ebene der Mutterunternehmen. Der Konzernlagebericht ist nach näherer Maßgabe dieser Normen um eine nichtfinanzielle Konzernklärung zu erweitern oder es ist ein gesonderter nichtfinanzieller Konzernbericht zu erstellen. Die Gestaltung und der Inhalt haben der nichtfinanziellen Erklärung bzw. dem gesonderten nichtfinanziellen Bericht zu entsprechen; die §§ 289c ff. HGB finden deshalb entsprechende Anwendung.
- 32 Nach der CSR-Richtlinie sind die Mitglieder der Verwaltungs-, Leitungs- und Aufsichtsorgane des Unternehmens entsprechend den nationalen Zuständigkeitsvorschriften für die Erstellung und Veröffentlichung des CSR-Reportings verantwortlich.³⁹ Entsprechend dem deutschen Gesellschaftsrecht obliegt diese Aufgabe den gesetzlichen Vertretern des Unternehmens, d. h. bei einer AG dem Vorstand.⁴⁰

39 Art. 1 Nr. 4 RL 2014/95/EU zu Art. 33 Abs. 1 RL 2013/34/EU.

40 § 264 Abs. 1 Satz 1 und 3 HGB in Verbindung mit § 78 Abs. 1 Satz 1 AktG.

b) Inhalte, Relevanzmaßstab und Methodik des CSR-Reportings

Inhaltlich hat der nach der vormaligen CSR-Richtlinie erstellte Bericht nach § 289c Abs. 2 HGB einzugehen „zumindest“ auf Umwelt-, Arbeitnehmer- und Sozialbelange, auf die Achtung der Menschenrechte und auf die Bekämpfung von Korruption und Bestechung. Zu jedem dieser Themenfelder benennt die Norm beispielhaft und nicht abschließend spezifische, in der Erklärung grundsätzlich aufzugreifende Gesichtspunkte. Trotz Diskussion im Gesetzgebungsverfahren über die Aufnahme weiterer Mindestaspekte wie die „Belange von Verbraucherinnen und Verbrauchern als Vertragspartner“ des berichtspflichtigen Unternehmens,⁴¹ konnte sich dies nicht durchsetzen. Die Regelung ist aufgrund der Formulierung „zumindest“ nicht als abschließende Checkliste zu begreifen, sondern folgt eher einem prinzipienorientierten Ansatz. Unternehmensindividuell ist zu entscheiden, was über die normseitig benannten Belange hinaus für das Geschäftsmodell wesentlich ist; auch über diese wichtigsten sonstigen nichtfinanziellen Aspekte ist zu berichten. Es bleibt den bislang berichtspflichtigen Unternehmen daher unbenommen, über solche, weiteren CSR-Aspekte zu berichten, soweit sie diese als wesentlich betrachten. **33**

Relevant sind bezogen auf alle berichtspflichtigen CSR-Belange bzw. -Aspekte nur die Informationen, die nach § 289c Abs. 3 HGB für das „Verständnis des Geschäftsverlaufs, des Geschäftsergebnisses, der Lage der Kapitalgesellschaft sowie der Auswirkungen ihrer Tätigkeit [...] erforderlich sind“. Die Gesetzesbegründung spricht insoweit von einem Wesentlichkeitsvorbehalt; die Wesentlichkeit der Information über ein Risiko ist ein generelles Berichtserfordernis. Der hier anzuwendende Wesentlichkeitsvorbehalt geht jedoch über den des § 289 Abs. 3 HGB hinaus, indem die Angaben zusätzlich für das Verständnis der unternehmensspezifischen Auswirkungen der Geschäftstätigkeit auf nichtfinanzielle Aspekte im Sinne des § 289c Abs. 2 Nr. 1–5 HGB erforderlich sein muss.⁴² In erster Linie geht es damit um durch die Geschäftstätigkeit des Unternehmens verursachte spezifische Risiken für die nichtfinanziellen Voraussetzungen bzw. Grundlagen seiner weiteren Geschäftstätigkeit. **34**

Systematisch gibt bereits Art. 19a Abs. 1a–e der Richtlinie eine sinnvolle, aber nicht verpflichtende Berichtsstruktur vor. Diese wird zunächst von § 289c Abs. 1 und Abs. 3 Nr. 1, Nr. 2 HGB aufgegriffen: Nach einer kurzen Beschreibung des Geschäftsmodells des Unternehmens bedarf es bislang der Darlegung der in Bezug auf die spezifischen nichtfinanziellen Belange bzw. Aspekte nach § 289c Abs. 2 HGB verfolgten Konzepte, einschließlich der angewandten Due-Diligence-Prozesse sowie von Angaben zur Umsetzung der Konzepte („Ergebnisse“). „Konzepte“ im Sinne der Richtlinie – die englische Version spricht von **35**

41 Konzept des BMJV vom 27.4.2015 zur Umsetzung der CSR-Richtlinie – Reform des Lageberichts; <https://www.germanwatch.org/sites/default/files/announcement/11813.pdf>, Ziff. 3 (zuletzt abgerufen am 3.6.2024); Übersendungsschreiben des BMJV vom 11.3.2016 an die Verbände.

42 BT-Drs. 18/9982, S. 48 f.; *Kajüter*, DB 2017, 617, 620 f.

„Policies“ – sind im gegebenen Kontext als Grundsätze, Strategien oder Vorgehensweisen zu verstehen. Der deutsche Gesetzgeber stellte ab auf Zielsetzungen des Unternehmens, geplante Maßnahmen und deren Unterlegung mit (Due-Diligence-)Prozessen sowie die Einbindung der Geschäftsleitung.⁴³ Der Begriff der Due Diligence stammt aus dem Bereich der Risikofrüherkennung und steht für mit gebotener Sorgfalt durchgeführte Untersuchungs-, Bewertungs- und Überwachungsverfahren. Spezifische Due-Diligence-Anforderungen mit Blick auf nichtfinanzielle Aspekte fordert indes weder die Richtlinie noch das nationale Umsetzungsgesetz. Explizit geht es nur um „angewandte“ Prozesse. Zudem bezieht sich die Gesetzesbegründung auf Verfahren, die bereits im Unternehmen installiert sind, um Sorgfaltspflichten und -obliegenheiten zu identifizieren und zu erfüllen, also auf solche eines bestehenden Risikomanagements bzw. des internen Kontrollsystems. Bezogen auf die Ergebnisse der Konzepte geht es um eine Darlegung der tatsächlichen und wahrnehmbaren Auswirkungen des jeweiligen Konzepts; existieren solche nicht, ist auch dies zu berichten.⁴⁴ Weitergehender Erläuterungen über diese Fakten hinaus bedarf es nach den Vorgaben nicht; regelmäßig werden solche Informationen aber sinnvoll sein.

- 36 Zu erläutern sind nach § 289c Abs. 3 Nr. 3 HGB darüber hinaus im Zusammenhang mit den jeweiligen Aspekten die wesentlichen Risiken, die **mit der eigenen Geschäftstätigkeit des Unternehmens verknüpft** sind und die sehr wahrscheinlich schwerwiegende negative Auswirkungen auf die genannten Belange bzw. Aspekte haben oder haben werden, sowie die Handhabung dieser Risiken durch das Unternehmen. Der Risikobegriff ist durch ein Wesentlichkeitskriterium eingeschränkt. Im Rahmen der vorzunehmenden Risikobewertung geht es um die Wahrscheinlichkeit des Eintritts schwerwiegender Auswirkungen auf nichtfinanzielle Aspekte, um deren Ausmaß und Intensität. Während die relevante Schwelle nach Maßgabe der Richtlinie bereits bei nur „wahrscheinlich negativen Auswirkungen“ überschritten ist, bedarf es in der nationalen Umsetzung deutlich restriktiver „sehr wahrscheinlicher“ und „schwerwiegender negativer“ Auswirkungen. Anzumerken ist ferner, dass es nicht (mehr) nur um unternehmensbezogene, bilanzielle Risiken geht, sondern auch und gerade um Risiken für nichtfinanzielle Aspekte außerhalb des Unternehmens, also dessen gesellschaftlichen „Impact“. In Anbetracht dieser hohen Wesentlichkeitsschwelle, überrascht es nicht, dass über diesbezügliche Angaben kaum berichtet wird.⁴⁵
- 37 § 289c Abs. 3 Nr. 4 HGB verlangt – als Spezialregelung zu § 289c Abs. 3 Nr. 3 HGB – unter den vorstehend erörterten Bedingungen (Wesentlichkeitsvorbehalt, Risikorelevanz) weitergehend Angaben bezogen auf die wesentlichen Risiken, die **mit den Geschäftsbeziehungen des Unternehmens, seinen Produkten und seinen Dienstleistungen verknüpft** sind und deren Handhabung, sofern

43 BT-Drs. 18/9982, S. 49.

44 BT-Drs. 18/9982, S. 50.

45 PwC, Erstanwendung des CSR-Richtlinie-Umsetzungsgesetzes, Studie zur praktischen Umsetzung im DAX 160, S. 57.

diese Berichterstattung – explizit – als relevant und verhältnismäßig einzustufen ist. Im Wesentlichen geht es hier um Risiken, auf die das berichtspflichtige Unternehmen nur mittelbar Einfluss ausübt, da sie aus der Sphäre ihrer Geschäftspartner stammen.⁴⁶ Die hierin angelegte und vielfach zu erwartende Ausdehnung der Berichtspflichten auf Unternehmen der Vertrags- und Lieferkette begegnete schon im Rahmen des Gesetzgebungsprozesses vielfacher Kritik von Wirtschaftsverbänden (vgl. bereits → Rn. 29 am Ende). Nicht zu verkennen ist, dass Unternehmen, insbesondere größere und mit einer gewissen Marktmacht ausgestattete, bereits heute Teile ihrer Verantwortung im Zusammenhang mit Compliance- oder auch Nachhaltigkeits-Risiken auf vertraglichem Wege auf ihre Geschäftspartner verlagern. So sehr dieses Bedürfnis nach Absicherung anzuerkennen ist, führt eine solche Handhabung unweigerlich zu spürbaren Aufwänden bei vielen kleinen und mittleren, originär nicht berichtspflichteten Unternehmen; dies kommt insbesondere dann in Betracht, wenn diverse Vertragspartner ihnen unterschiedliche Anforderungen stellen. Wegen unterschiedlicher, unternehmensspezifisch ermittelter Berichtsschwerpunkte der Gesetzesadressaten werden oftmals überproportionale Aufwände bei Unternehmen entstehen, die sowohl nach den Begründungen zur CSR-Richtlinie als auch zum CSR-RUG explizit zu vermeiden sind. Die Berichterstattung soll hiernach „nicht zu übermäßigem Verwaltungsaufwand“ bei den KMU führen; der originär Berichtsverpflichtete soll die Größenklasse des Geschäftspartners angemessen berücksichtigen und damit Proportionalitätsgesichtspunkten Rechnung tragen. Ungeachtet dessen aber verweist der nationale Gesetzgeber in seinen Erwägungen auch auf das Interesse der Allgemeinheit, vom Normadressaten zu erfahren, ob seinerseits eine Wertschöpfungskette existiert und bis zu welcher Tiefe diesbezüglich nichtfinanzielle Angaben gemacht werden.⁴⁷

Entsprechend der CSR-Richtlinie sowie nach § 289c Abs. 3 Nr. 5 HGB bedarf es weitergehend generell der Angabe der für die konkrete Unternehmenstätigkeit wichtigsten nichtfinanziellen Leistungsindikatoren. Hierunter versteht man gemeinhin die im konkreten Kontext anzulegenden (Mess-)Kriterien und wesentlichen Kennzahlen eines Unternehmens, die zur Steuerung des Unternehmens dienen, umweltbezogen etwa den Energie-, Rohstoff- oder Wasserverbrauch. Waren diese Punkte bislang (vgl. § 289 Abs. 3 HGB) nur im Rahmen der Analyse von Geschäftsverlauf und -ergebnis zu betrachten, sind sie nun in ihrer Bedeutung selbstständig und präziser darzustellen. Überschneidungen oder Doppelungen in den Angaben werden sich indes in der gegenwärtigen Gesetzeskonzeption mit Blick auf bereits vorangehende Erläuterungen nicht vollständig vermeiden lassen, jedoch sind Verweise auf bestimmte Stellen des (Konzern-) Lageberichtes nach § 289b Abs. 1 Satz 3, Abs. 3 Satz 2 bzw. § 315b Abs. 1

38

46 BT-Drs. 18/9982, S. 50; *Rimmelspacher/Schäfer/Schönberger*, KoR 2017, 225, 228.

47 BT-Drs. 18/9982, S. 51; siehe auch gleichlautende Berichtsansforderungen zu den DNK-Kriterien 4 und 17: Rat für Nachhaltige Entwicklung, *Der Deutsche Nachhaltigkeitskodex*, „Texte Nr. 47“, 2015.

Satz 3, Abs. 3 Satz 2 HGB zulässig. Gefordert ist ein gesamthafter Überblick aller unternehmensspezifisch wichtigsten nichtfinanziellen Leistungsindikatoren, aus welchem Bereich auch immer sie stammen. Es erscheint empfehlenswert, weil zweckmäßig, die entsprechenden Darlegungen im Rahmen der nichtfinanziellen Erklärung vorzuziehen und die Leistungsindikatoren unmittelbar anschließend an die Erläuterungen zum Konzept im Rahmen des jeweiligen Belangs darzustellen. Ausweislich der Gesetzesbegründung ist die Reihenfolge der Angaben im Rahmen der Erklärung nach § 289c Abs. 3 HGB nicht zwingend an der gesetzlichen Abfolge der Berichtspunkte zu orientieren; diese sei nicht als Festlegung einer Priorität zu verstehen. Sie kann daher insbesondere unternehmensspezifischen Bedürfnissen folgen.⁴⁸

- 39** Die unverbindliche Leitlinie der EU-Kommission ist eine Orientierungshilfe zur Methodik der Berichterstattung – insbesondere zu den Grundsätzen der ordnungsgemäßen Lageberichterstattung sowie Ausführungen zum Inhalt der Angaben nach § 289c Abs. 3 HGB – und enthält Beispiele zu wichtigen nichtfinanziellen Leistungsindikatoren.⁴⁹ Im Hinblick auf Umweltbelange ist das ausführliche Update der Leitlinie, das sich explizit auf die „klimabezogene Berichterstattung“ bezieht, eine gute Hilfestellung bei der Erstellung des CSR-Berichtes.⁵⁰
- 40** Nur soweit für das Verständnis der nichtfinanziellen Erklärung im Zusammenhang mit dem Jahresabschluss erforderlich, sind schließlich nach § 289c Abs. 3 Nr. 6 HGB Hinweise auf einzelne im Jahresabschluss ausgewiesene Beträge und weitere diesbezügliche Erläuterungen zu geben. Auch wenn die EU-Kommission sich erklärtermaßen – und ähnlich wie der Gesetzgeber – (noch) von einer sogenannten integrierten Berichterstattung distanziert und diesen Ansatz lediglich „mit großem Interesse verfolgt“, ergibt sich durch Verknüpfungen nichtfinanzieller Informationen mit im Jahresabschluss ausgewiesenen Beträgen eine gewisse einfache Form des „Integrated Reportings“, also einer durchgängigen Verbindung der Finanzdaten eines Unternehmens mit den nichtfinanziellen Informationen.⁵¹

c) Muster: Struktur und Ansätze zur Gestaltung des CSR-Reportings

- 41** Die nichtfinanzielle Erklärung im Lagebericht kann inhaltlich bzw. strukturell wie folgt konzipiert werden. Die Reihenfolge der Behandlung der verschiedenen in § 289c Abs. 2 HGB genannten nichtfinanziellen Aspekte ist der Gesetzesbegründung zufolge nicht zwingend. Letztlich kommt es nur darauf an, sich konkret mit jedem Belang nach näherer Maßgabe des § 289c Abs. 3 HGB auseinanderzusetzen.

48 BT-Drs. 18/9982, S. 48.

49 ABl. 2017 C 215/01 v. 5.7.2017.

50 ABl. 2019 C 209/01 v. 20.6.2019.

51 Überblick zum Integrated Reporting: *Lanfermann*, in: Walden/Depping, CSR und Recht, S. 111.

derzusetzen. Auch einer Orientierung an anerkannten Rahmenwerken bedarf es nicht (vgl. § 289d HGB, der nur eine solche Möglichkeit eröffnet).

Hervorzuheben ist ferner, dass die Angaben zum Diversitätskonzept im Hinblick auf das vertretungsberechtigte Organ und den Aufsichtsrat nach § 289f Abs. 2 Nr. 6 HGB zukünftig gesondert in der Erklärung zur Unternehmensführung zu erfolgen haben – und damit außerhalb der nichtfinanziellen Erklärung. **42**

Das CSR-Reporting – Aufbau und Bestandteile:

43

- **Darstellung des Geschäftsmodells der Gesellschaft** (kurze Beschreibung);
- **Angaben zu Umweltbelangen**, „insbesondere, wenn angebracht“ zu: Treibhausgasemissionen, Wasserverbrauch, Luftverschmutzung, Nutzung erneuerbarer und nicht erneuerbarer Energien, Schutz biologischer Vielfalt – weitere Angaben, sofern unternehmensspezifisch relevant (Themenbeispiele: Abfallmanagement, Energieeinsatz und -effizienz, Finanzanlagen, Gesundheitsaspekte, Klimaschutz, Produkte, Rohstoff- und Materialverbrauch, Sicherheit)
- Konzept („Policy“: Grundsätze, Strategien oder Vorgehensweisen) im Umgang mit dem Themenfeld, einschließlich angewandter Due-Diligence-Prozesse,
- wichtigste nichtfinanzielle Leistungsindikatoren (zweckmäßigerweise im Kontext der Darstellung des jeweiligen Belangs und des Konzepts aufzunehmen; ausweislich der Gesetzesbegründung ist die Reihenfolge der Angaben in § 289c Abs. 3 HGB nicht zwingend; die Bearbeitung kann sich etwa an unternehmensspezifischen Bedürfnissen orientieren),
- Ergebnisse des Konzepts (Umsetzung in der Praxis, Funktionsfähigkeit etc.),
- wesentliche Risiken der Geschäftstätigkeit des Unternehmens mit potenziell negativen Auswirkungen im Zusammenhang mit Umweltbelangen sowie Umgang mit diesen Risiken; sofern relevant und angemessen auch explizit bezogen auf
 - die Geschäftsbeziehungen des Unternehmens, „einschließlich seiner Lieferkette und seiner Kette von Subunternehmern“⁵² sowie Abnehmer der Produkte und Dienstleistungen,⁵³
 - seine Produkte und
 - seine Dienstleistungen,

⁵² Richtlinie 2014/95/EU, Erwägungsgrund 8; BT-Drs. 18/9982, S. 51.

⁵³ ABl. 2019 C 209/01 v. 20.6.2019, S. 5.

- soweit für das Verständnis der nichtfinanziellen Erklärung erforderlich: Inbezugnahme im Jahresabschluss ausgewiesener Beträge und diesbezügliche Erläuterungen;
- 44** – **Angaben zu Arbeitnehmerbelangen** (ggf. wegen inhaltlicher Überschneidungen gemeinsam mit dem Themenfeld Sozialbelange zu bearbeiten), „insbesondere, wenn angebracht“ zu: Gewährleistung der Geschlechtergleichstellung, Arbeitsbedingungen, Achtung der Rechte der Arbeitnehmerinnen und Arbeitnehmer sowie der Gewerkschaften, Gesundheitsschutz, Arbeitssicherheit – weitere Angaben, sofern unternehmensspezifisch relevant (Themenbeispiele: Aufwendungen für Aus- und Weiterbildung, Ausfallzeiten, Berufskrankheiten, betriebliche Sozialleistungen)
- Konzept (wie vorstehend), einschließlich angewandter Due-Diligence-Prozesse,
 - wichtigste nichtfinanzielle Leistungsindikatoren (wie vorstehend),
 - Ergebnisse des Konzepts (wie vorstehend),
 - wesentliche Risiken (wie vorstehend),
 - soweit für das Verständnis der nichtfinanziellen Erklärung erforderlich: Inbezugnahme im Jahresabschluss ausgewiesener Beträge und diesbezügliche Erläuterungen;
- 45** – **Angaben zu Sozialbelangen** (ggf. wegen inhaltlicher Überschneidungen gemeinsam mit dem Themenfeld Arbeitnehmerbelange zu bearbeiten), „insbesondere, wenn angebracht“ zu: Dialog auf kommunaler oder regionaler Ebene, Schutz und Entwicklung lokaler Gemeinschaften – weitere Angaben, sofern unternehmensspezifisch relevant (Themenbeispiele: Beiträge zum Gemeinwesen – „Corporate Citizenship“, Beziehungen zur Gemeinde, Sozialstandards bei Dienstleistern)
- Konzept (wie vorstehend), einschließlich angewandter Due-Diligence-Prozesse,
 - wichtigste nichtfinanzielle Leistungsindikatoren (wie vorstehend),
 - Ergebnisse des Konzepts (wie vorstehend),
 - wesentliche Risiken (wie vorstehend),
 - soweit für das Verständnis der nichtfinanziellen Erklärung erforderlich: Inbezugnahme im Jahresabschluss ausgewiesener Beträge und diesbezügliche Erläuterungen;
- 46** – **Angaben zur Achtung der Menschenrechte**, „insbesondere, wenn angebracht“ zur Verhinderung von Menschenrechtsverletzungen (Themenbeispiele: Akzeptanz internationaler Standards, Maßnahmen zur Verhinderung von Zwangs- oder Kinderarbeit oder von Formen der Ausbeutung)
- Konzept (wie vorstehend), einschließlich angewandter Due-Diligence-Prozesse
 - wichtigste nichtfinanzielle Leistungsindikatoren (wie vorstehend),

- Ergebnisse des Konzepts (wie vorstehend),
- wesentliche Risiken (wie vorstehend),
- soweit für das Verständnis der nichtfinanziellen Erklärung erforderlich: Inbezugnahme im Jahresabschluss ausgewiesener Beträge und diesbezügliche Erläuterungen;
- **Angaben zur Bekämpfung von Korruption und Bestechung**, „insbesondere, wenn angebracht“ zu bestehenden Instrumenten zur Bekämpfung von Korruption und Bestechung (Themenbeispiele: fraud-spezifisches Compliance-Management-System, Gefährdungsanalyse, spezifisches Risk Assessment, Hinweisgebersystem, integritätsfördernde Unternehmenskultur, Richtlinien für Geschenke und Einladungen, Rolle des Managements, Schulungen) 47
- Konzept (wie vorstehend), einschließlich angewandter Due-Diligence-Prozesse,
- wichtigste nichtfinanzielle Leistungsindikatoren (wie vorstehend),
- Ergebnisse des Konzepts (wie vorstehend),
- wesentliche Risiken (wie vorstehend),
- soweit für das Verständnis der nichtfinanziellen Erklärung erforderlich: Inbezugnahme im Jahresabschluss ausgewiesener Beträge und diesbezügliche Erläuterungen;
- **Darstellung der wichtigsten sonstigen** (vgl. § 289c Abs. 2 Satz 1 HGB: „zumindest“) **nichtfinanziellen Aspekte**, die für die Geschäftstätigkeit des Unternehmens von Bedeutung sind (Themenbeispiele: Entwicklung und Forschung, Prozessmanagement, Kundenbelange (z. B. Kundenorientierung (allg.), Einhaltung Verbraucherschutzvorgaben, Datenschutz, Kundenansprache und Werbung, Kundengesundheit und -sicherheit, Beschwerdemanagement), Produktsicherheit, Reputation) 48
- Konzept(e) (wie vorstehend), einschließlich angewandter Due-Diligence-Prozesse,
- wichtigste nichtfinanzielle Leistungsindikatoren (wie vorstehend),
- Ergebnisse des(r) Konzept(s)e (wie vorstehend),
- wesentliche Risiken (wie vorstehend),
- soweit für das Verständnis der nichtfinanziellen Erklärung erforderlich: Inbezugnahme im Jahresabschluss ausgewiesener Beträge und diesbezügliche Erläuterungen.

d) Die Möglichkeit der Verwendung von Rahmenwerken

§ 289d HGB ermöglicht die Verwendung geeigneter nationaler, europäischer oder internationaler Standards. Hierdurch werden entsprechend der Genesis und der Zielsetzung der CSR-Richtlinie breit angelegte Gestaltungsmöglichkeiten eröffnet, jedoch zulasten des Ziels der Vergleichbarkeit der CSR-Berichterstat- 49

tung.⁵⁴ In Erwägungsgrund 9 der Richtlinie werden als anerkannte Rahmenwerke im Sinne dieser Vorgehensweise exemplarisch das Umweltmanagement- und -betriebsprüfungssystem (EMAS), der UN-Global Compact, die UN Leitprinzipien für Wirtschaft und Menschenrechte, die Leitlinie ISO 26.000 „Guidance on Social Responsibility“ der Internationalen Organisation für Normung, die Dreigliedrige Grundsatzerklärung der Internationalen Arbeitsorganisation zu multinationalen Unternehmen und zur Sozialpolitik, die OECD-Leitlinien für multinationale Unternehmen oder die Richtlinie der Global Reporting Initiative (GRI) genannt.⁵⁵

- 50** Darüber hinaus empfiehlt sich – auch nach der Begründung zum CSR-RUG⁵⁶ – eine Berichterstattung nach dem Deutschen Nachhaltigkeitskodex (DNK) des Rates für Nachhaltige Entwicklung (RNE),⁵⁷ der inhaltlich an den Prinzipien der vorgenannten Standards ausgerichtet ist. Die EU-Kommission hat den DNK ebenfalls ausdrücklich als einen zur CSR-Berichterstattung geeigneten Berichterstattungsstandard bezeichnet.⁵⁸ Das Berichtsinstrumentarium des DNK orientiert sich an den Standards der GRI und des europäischen Analystenverbandes EFFAS und ist damit insbesondere auch für Finanzanalysten und Investoren interessant. Der DNK ist gut strukturiert und wird seinem Anspruch gerecht, den deutschen Unternehmen angesichts der Vielzahl der einschlägigen Rahmenwerke Orientierung zu geben: Er eignet sich sowohl für „Neueinsteiger“ zur Erschließung der Materie als auch für „Fortgeschrittene“.⁵⁹ Der RNE verweist mit Blick auf die Kompatibilität des DNK mit der CSR-Richtlinie auf ein von ihm eigens eingeholtes Gutachten.⁶⁰
- 51** Das berichtspflichtige Unternehmen hat nach § 289d Satz 2 HGB in der nichtfinanziellen Erklärung anzugeben, welche(s) Rahmenwerk(e) es verwendet hat oder – sofern kein Rahmenwerk verwendet wurde – eine diesbezügliche Begründung. Ein Reporting nach Maßgabe von § 289d HGB „unter Anlehnung an oder unter Verwendung“ von Rahmenwerken setzt dem Wortlaut nach lediglich ein gewisses Maß an Orientierung an den entsprechenden Vorgaben voraus. Ein Rahmenwerk kann daher nur teilweise verwendet werden oder mehrere Rahmenwerke können kombiniert werden, soweit diesbezüglich eine deutliche Kenn-

54 Die Herstellung der Vergleichbarkeit der Berichte ist ein wesentliches Motiv für die Einführung der Berichterstattung nach der CSRD.

55 Vgl. www.unglobalcompact.org; www.iso.org; www.oecd.org; www.globalreporting.org.

56 BT-Drs. 18/9982, S. 46, 52.

57 Rat für Nachhaltige Entwicklung, Der Deutsche Nachhaltigkeitskodex, „Texte Nr. 47“, 2015.

58 IP/13/330 vom 16.4.2013.

59 Ausführlicher hierzu: *Beisheim*, in: Habersack/Huber/Spindler, FS Stilz, 2014, S. 55 ff.

60 Siehe <https://www.nachhaltigkeitsrat.de/aktuelles/mit-dem-dnk-die-neue-csr-berichtspflicht-erfuellen/> (zuletzt abgerufen am 3.6.2024); ein ähnliches Verfahren ist nach erfolgter Anpassung des DNK an die Anforderungen des CSDR/ESRS (geplant zum Jahreswechsel 2024/2025) vorgesehen.

zeichnung erfolgt.⁶¹ Der Gesetzesbegründung zufolge ist dem Gesetzgeber bewusst, dass manche der in Betracht zu ziehenden Standards nur Teilaspekte der inhaltlichen Mindestanforderungen abdecken. Die Normadressaten werden vor diesem Hintergrund explizit in die Verantwortung genommen, alle gesetzlich geforderten Berichtselemente auch im Rahmen dieses Berichtsansatzes abzudecken.⁶² Die Konkretisierungen in § 289c Abs. 2 HGB zu den einzelnen Belangen bzw. Themenfeldern haben demnach explizit auch den Zweck, im gegebenen Kontext eine Vergleichbarkeit der Berichterstattung zu gewährleisten. Hilfreich für den Berichtsersteller sind insoweit Begutachtungen, wie sie beispielsweise der RNE mit Blick auf die Kompatibilität des DNK mit den CSR-Vorgaben hat vornehmen lassen.

5. Nichtangaben, unrichtige Angaben und ihre Folgen

Vorstellbar ist, dass ein relevantes Unternehmen zu einem Themenfeld über kein einschlägiges Konzept verfügt und deshalb insoweit keine Angaben vorzunehmen vermag. Weitergehend könnte die nichtfinanzielle Erklärung, der gesonderte Bericht oder das Diversitätskonzept in Gänze fehlen oder ganz oder in Teilen unwahr bzw. unrichtig sein. **52**

a) Der „Comply or Explain“-Grundsatz

Die Richtlinie und § 289c Abs. 4 HGB verlangen grundsätzlich eine Bearbeitung aller vorgegebenen Themen, zumindest Angaben hinsichtlich der jeweils verfolgten Konzepte. Sind im Einzelfall oder generell keine Angaben zu Konzepten möglich, bedarf es einer eindeutigen und nachvollziehbaren Begründung im Wege einer zusätzlichen Erläuterung, warum konkret keine spezifische Darstellung möglich ist – eine schlichte „Fehlanzeige“ genügt also nicht. Jedoch muss nur das Fehlen eines gesamten Konzepts, nicht das Fehlen einzelner Konzeptteile – wie z. B. ein Due-Diligence-Prozess – begründet werden.⁶³ § 289c Abs. 4 HGB soll nach der Richtlinie und der Gesetzesbegründung damit den sog. „Comply or Explain“-Ansatz verfolgen, um ein hohes Maß an Transparenz zu gewährleisten, wie er sich ausweislich der Begründung zum CSR-RUG bereits im Rahmen der Corporate-Governance-Erklärung nach § 161 AktG bewährt hat.⁶⁴ Bedenkt man, aus welchem CSR-Verständnis heraus und mit welchen Zielsetzungen man die Normen auf EU-Ebene und national in die Umsetzung gebracht hat (siehe → Rn. 8 ff.), werden die verhaltenssteuernden Elemente dieses Ansatzes deutlich sichtbar. Es geht eben nicht nur um unternehmensinterne Risikomanagementansätze, sondern insgesamt um negativ wahrgenommene Auswirkungen des Unternehmens auf die Gesellschaft. Allen Stakeholdern – etwa Investoren, Kunden, **53**

61 BT-Drs. 18/9982, S. 49; *Kajüter*, DB 2017, 617, 623; *Winkeljohann/Schäfer*, in: Beck Bil-Komm., 11. Aufl. 2018, § 289d HGB Rn. 2.

62 BT-Drs. 18/9982, S. 46, 49, 52; *Kajüter*, DB 2017, 617, 623; *Klene*, WM 2018, 308, 313.

63 BT-Drs. 18/9982, S. 49, 52.

64 BT-Drs. 18/9982, S. 52.

Mitarbeitern und insbesondere auch der Öffentlichkeit gegenüber – soll Rechenschaft abgelegt werden über die nachhaltigkeitsbezogene Aufstellung des Unternehmens und ggf. verbundener Einheiten, über die der Geschäftstätigkeit inhärenten spezifischen Risiken und den unternehmensseitig vorgesehenen Umgang mit ihnen. Durch Herstellung angemessener Transparenz soll sichtbar werden, ob der Berichtsteller seiner gesellschaftlichen Verantwortung gerecht wird, in seinem Auftritt glaubwürdig erscheint und das Vertrauen der Stakeholder zu Recht in Anspruch nimmt. Glaubwürdigkeit und Vertrauen sind neben Zuverlässigkeit und Verantwortung wesentliche Grundlagen für eine gute Reputation des Unternehmens.

- 54 Andererseits hebt die Gesetzesbegründung die grundsätzliche Eigenverantwortung des Unternehmens bzw. seiner Organmitglieder im Umgang mit nichtfinanziellen Informationen hervor: Eine Anpassung bestehender Konzepte allein für Zwecke der Berichterstattung sei nicht intendiert. Das Unternehmen müsse selbst entscheiden, wie es mit nichtfinanziellen Themen umgehen möchte.⁶⁵
- 55 Tatsächlich enthält § 289c Abs. 4 HGB jedoch keinen echten „Comply-or-Explain“-Grundsatz. Der echte „Comply-or-Explain“-Grundsatz setzt untergesetzliche Verhaltensvorgaben voraus, die erklärtermaßen befolgt werden oder deren Nichtbefolgung zu begründen ist.⁶⁶ Mangels einheitlichem, kodifizierten Standard für CSR-Themen in Unternehmen oder gar einer „Best Practice“ existiert kein diesbezüglicher Referenzstandard.⁶⁷ Auch § 289c HGB selbst setzt keinen CSR-Standard, sondern kodifiziert lediglich eine Berichtspflicht.⁶⁸

b) Ein Sonderfall: Das (vorübergehende) Weglassen nachteiliger Angaben

- 56 Mit Blick auf einen Sonderfall vorübergehenden Geheimhaltungsbedarfs besteht nach der Richtlinie ein sogenanntes Mitgliedstaatenwahlrecht, das auch in Deutschland seine Anwendung findet: Einzelne EU-Länder können im Rahmen der nationalen Umsetzung Nichtangaben in begründeten Fällen ausnahmsweise dann und unter weiteren Bedingungen zulassen, wenn über Entwicklungen oder Belange Verhandlungen geführt werden und die Veröffentlichung diesbezüglicher Informationen dem Unternehmen „ernsthaft schaden würde“. ⁶⁹ Der deutsche Gesetzgeber greift diese Regelung in § 289e HGB auf. Die spezifische Berichtspflicht entfällt hiernach, wenn im Zusammenhang mit einem Themenfeld zukunftsgerichtet Gespräche mit Dritten geführt werden und diesbezügliche Angaben gegenüber der Öffentlichkeit „nach vernünftiger kaufmännischer Beurteilung“ geeignet sind, dem Unternehmen einen erheblichen Nachteil zuzufügen. Stets bedarf es zudem einer Bewertung dahingehend, ob das Weglassen der Angaben noch ein ausgewogenes (Gesamt-)Verständnis des Geschäftsverlaufs und

65 BT-Drs. 18/9982, S. 49.

66 *Leyens*, ZEuP 2016, 388, 389.

67 *Nietsch*, NZG 2016, 1330, 1333; *Mock*, ZIP 2017, 1195, 1198.

68 *Bachmann*, ZGR 2018, 231, 232 f.

69 Richtlinie 2014/95/EU, Art. 19a Abs. 1 Unterabs. 4.

-ergebnisses, der Lage der Gesellschaft und ihrer Tätigkeitsauswirkungen erlaubt (sog. „True and Fair View“-Prinzip). Im Kern ist hinsichtlich der betroffenen Angaben eine Interessenabwägung zwischen dem unternehmerischen Geheimhaltungsinteresse und dem Offenbarungsinteresse der Adressaten der CSR-Berichterstattung durch die Geschäftsleitung des Unternehmens durchzuführen.

Das Unternehmen kann sich hiernach nur in extremen Ausnahmefällen auf die Regelung berufen. Ohnedies besteht in der vorgesehenen Gestaltung ein sogenanntes Unternehmenswahlrecht, da es der Gesellschaft grundsätzlich freisteht, sich trotz bestehender bzw. als bestehend angenommener Berichtshindernisse überobligatorisch zu erklären. Nimmt das Unternehmen die Befreiungsmöglichkeit aber in Anspruch, hat es die Angaben im Rahmen des nächsten zu erstellenden Reportings nachzuholen (sog. „Nachholpflicht“). Ein willkürliches Absehen vom Reporting soll verhindert werden, die Transparenz und Vergleichbarkeit der Informationslage soll zumindest im Nachhinein sichergestellt sein.⁷⁰ **57**

c) Prüfungen

Art. 19a Abs. 5, 29a Abs. 5 und 34 Abs. 3 der CSR-Richtlinie fordern von den Mitgliedstaaten die Sicherstellung einer Überprüfung durch den Abschlussprüfer oder „die Prüfungsgesellschaft“ lediglich dahingehend, ob die nichtfinanzielle Erklärung oder der gesonderte Bericht vorgelegt wurde. Dies wurde vom deutschen Gesetzgeber in § 317 Abs. 2 Satz 4 HGB umgesetzt. Die Abschlussprüfung erfasst grundsätzlich nur den Aspekt des Vorliegens der Erklärung bzw. des Berichts („ob“). Im Falle eines nach § 289b Abs. 3 HGB möglichen, zeitlich verzögerten, gesonderten Berichts ist eine ergänzende Prüfung vorgesehen – unter entsprechender Ergänzung auch des Bestätigungsvermerks nach § 316 Abs. 3 Satz 2 HGB. **58**

Das Mitgliedstaatenwahlrecht nach Art. 19a Abs. 6, 29a Abs. 6 der CSR-Richtlinie hinsichtlich einer verpflichtenden inhaltlichen Überprüfung durch einen „unabhängigen Erbringer von Bestätigungsleistungen“ hat der deutsche Gesetzgeber in Anbetracht des Erfüllungsaufwands nicht ausgeübt.⁷¹ Berichtspflichtige Unternehmen – explizit dem Aufsichtsrat nach § 111 Abs. 2 Satz 4 AktG – steht es jedoch frei, eine freiwillige externe Prüfung durchführen zu lassen. Daran anknüpfend verlangen § 289b Abs. 4 bzw. § 315b Abs. 4 HGB für ab dem 1.1.2019 beginnende Geschäftsjahre die Veröffentlichung der Beurteilung des Prüfungsergebnisses in gleicher Weise wie das Reporting als solches. Die Allgemeinheit soll erkennen können, in welchem Umfang die Informationen geprüft wurden. Beauftragt das Unternehmen keine freiwillige inhaltliche Prüfung, ist dies hingegen nicht mitzuteilen. Als Prüfer kommen ein „unabhängiger Erbringer von Bestätigungsleistungen“, etwa Zertifizierungen anbietende NGOs, „ein Abschlussprüfer“ oder ein anderer Sachverständiger in Betracht. **59**

⁷⁰ BT-Drs. 18/11450, 44; BT-Drs. 18/9982, S. 53.

⁷¹ BT-Drs. 18/9982, S. 31; *Velte*, IRZ 2017, 325, 326.

- 60 Hervorzuheben ist ferner eine Erweiterung der Prüfungspflichten des Aufsichtsrats.⁷² Der Aufsichtsrat hat im Rahmen seiner Verantwortung sicherzustellen, dass die vorstandsseitige Rechnungslegung – und damit also auch die Anforderungen im Rahmen des nichtfinanziellen Reportings – den gesetzlichen Anforderungen entspricht. Nach § 170 Abs. 1 AktG bedarf es deshalb der unverzüglichsten Vorlage des gesonderten nichtfinanziellen Berichts nach § 289b HGB bzw. des entsprechenden Konzernberichts nach § 315b HGB an ihn; die Prüfungsverpflichtung seitens des Aufsichtsrats regelt § 171 Abs. 1 Satz 4 AktG. Die nichtfinanzielle Erklärung als solche wird bereits per se als Teil des Lageberichts bzw. des Konzernlageberichts von § 171 Abs. 1 Satz 1 HGB erfasst. Jedoch ist umstritten, welchen Prüfungsumfang der Aufsichtsrat hinsichtlich der Recht- und Ordnungsmäßigkeit des CSR-Reportings anzuwenden hat⁷³; Gleicher Prüfungsumfang wie im Rahmen der sonstigen Rechnungslegung,⁷⁴ „Plausibilitätskontrolle“⁷⁵ oder Ermessen hinsichtlich des eigenen Prüfungsumfangs.⁷⁶ Vor dem Hintergrund der bestehenden Rechtsunsicherheiten überrascht es nicht, dass Aufsichtsräte – auch zu ihrer eigenen Absicherung – überwiegend eine externe inhaltliche Prüfung des CSR-Reportings in Auftrag geben.⁷⁷
- 61 Sofern eine GmbH über einen Aufsichtsrat verfügt, bestehen entsprechende Pflichten über § 52 Abs. 1 GmbHG; für Genossenschaften gilt § 38 Abs. 1 Satz 5, Abs. 1b GenG.
- 62 Entsprechende Prüfanforderungen bestehen im Übrigen mit Blick auf das Diversitätskonzept nach § 289f Abs. 2, Abs. 5 HGB bzw. konzernbezogen nach § 315d HGB. Auch hier erfolgt die Prüfung nach § 317 Abs. 2 Satz 6 HGB lediglich eingeschränkt dahingehend, ob die Angaben gemacht wurden, nicht aber in inhaltlicher Hinsicht. Die Möglichkeit zur Beauftragung einer freiwilligen externen Prüfung der Erklärung zur Unternehmensführung ist zwar nicht explizit in § 111 AktG enthalten, kann aber als von der allgemeinen Ermächtigung in § 111 Abs. 2 Satz 2 AktG umfasst angesehen werden.⁷⁸ Hingegen besteht hier – im Gegensatz zum nichtfinanziellen Reporting (siehe → Rn. 59) – keine gesetzliche Pflicht zur Veröffentlichung der Beurteilung des Prüfungsergebnisses. Inwiefern

72 Zu Rolle und Aufgaben des Aufsichtsrats im Rahmen des Compliance Managements siehe *Leupolt*, in: Schulz, Compliance Management im Unternehmen, 1. Aufl. 2017, Kap. 17.

73 Hierzu insgesamt ausführlich *Velte*, AG 2018, 266, 269 ff.

74 IDW Positionspapier, Zukunft der Berichterstattung, Nachhaltigkeit, 14.6.2017, S. 7; *Mock*, ZIP 2017, 1195, 1201; *Klene*, WM 2018, 308, 313.

75 Ausführlich m. w. N. *Koch*, in: Hüffer/Koch, AktG, § 171 Rn. 8a; *Hennrichs/Pöschke*, NZG 2017, 121, 124 ff.; *Hirte*, BT-Plenarprotokoll 18/221, 22258.

76 BT-Drs. 18/11450, S. 47.

77 Global Compact Netzwerk Deutschland/econsense, Neuer Impuls für die Berichterstattung zu Nachhaltigkeit? – Studie zur Umsetzung des deutschen CSR-Richtlinie-Umsetzungsgesetzes, S. 16; EY, CSR-Richtlinie-Umsetzungsgesetz, Die nichtfinanzielle Erklärung – Lessons learned aus dem ersten Berichtsjahr 2017, S. 13; PwC, Erstanwendung des CSR-Richtlinie-Umsetzungsgesetzes, Studie zur praktischen Umsetzung im DAX 160, S. 64–65.

78 Ebenso *Velte*, AG 2018, 266, 269.

der Aufsichtsrat selbst die Erklärung zur Unternehmensführung – abgesehen von der ohnehin umstrittenen Frage des Prüfungsumfangs – zu prüfen hat ist umstritten. Das Meinungsspektrum reicht hier von der Verneinung einer Prüfungspflicht, über eine mittelbare Prüfung bis hin zur vollständigen materiellen Prüfungspflicht.⁷⁹

d) Verstöße, Säumnisse und Sanktionen

Nach Erwägungsgrund 10 zur CSR-Richtlinie sollten die Mitgliedstaaten sicherstellen, dass es „sachgerechte und wirksame Mechanismen“ zur Gewährleistung der Compliance mit der Richtlinie gibt. Art. 51 der dieser zugrunde liegenden Richtlinie 2013/34/EU fordert gar „abschreckende Sanktionen“. Wirksame nationale Verfahren sollten hierfür eingerichtet werden, die die Erfüllung der Pflichten sicherstellen und die allen natürlichen und juristischen Personen zur Verfolgung deren berechtigter Interessen im gegebenen Kontext offenstehen; letztere Formulierung zielt im Grunde ab auf die Einführung spezifischer Verbands- und Privatklageinstrumente. Der deutsche Gesetzgeber hat sich demgegenüber für eine Ausdehnung der bestehenden Straf- und Bußgeldvorschriften auf die Nichteinhaltung der Berichtspflichten zu den nichtfinanziellen Informationen entschieden.⁸⁰

Die Strafbarkeit der unrichtigen Wiedergabe oder Verschleierung der Verhältnisse der Kapitalgesellschaft bezieht in § 331 Abs. 1 Nr. 1 bzw. Nr. 2 HGB explizit auch die nichtfinanzielle Berichterstattung mit ein. Die Strafandrohung erfasst die Angaben in der nichtfinanziellen Erklärung, im gesonderten nichtfinanziellen Bericht sowie das entsprechende Berichtswesen auf Konzernebene und richtet sich an die Mitglieder des vertretungsberechtigten Organs und des Aufsichtsrats. Täter in Kreditinstituten und Versicherungen werden über die Verweisungsnormen der §§ 340m Abs. 1 Satz 1, 341m Abs. 1 Satz 1 HGB erfasst.

§ 334 Abs. 1 Nr. 3 und Nr. 4 HGB enthalten Bußgeldtatbestände mit Blick auf Verstöße gegen die in diesen Vorschriften konkret benannten Vorgaben zur nichtfinanziellen Berichterstattung. Für Kreditinstitute und Versicherungen gelten nach dem bereits bestehenden § 334 Abs. 5 HGB die speziellen Bußgeldvorschriften der §§ 340n und 341n HGB. Während der vorherige Bußgeldrahmen bis zu 50.000 EUR betrug, erfolgte eine Erhöhung des Bußgeldrahmens bei kapitalmarktorientierten Unternehmen. Geschäftsleitungs- und Aufsichtsratsmitglieder kapitalmarktorientierter Unternehmen droht nach § 334 Abs. 3 Satz 2 HGB ein Bußgeld von bis zu 2 Mio. EUR oder in Höhe des Zweifachen des aus der Ordnungswidrigkeit erlangten Vorteils. Dem kapitalmarktorientierten Unternehmen selbst droht nach § 334 Abs. 3a HGB ein Bußgeld von bis zu 10 Mio. EUR, in Höhe von 5% des jährlichen Umsatzes des vorausgegangenen Geschäftsjahres oder in Höhe des Zweifachen des aus der Ordnungswidrigkeit er-

⁷⁹ Ausführlich *Velte*, AG 2018, 266, 271 f.

⁸⁰ Kritisch mit Blick auf die Unbestimmtheit der Sanktionsandrohungen: *Nietsch/Muneretto*, CB 2016, 177, 182.

langten Vorteils. Maßgeblich für die Obergrenze ist stets der höchste dieser Beträge.

III. Die CSRD: Neue Anforderungen im Nachhaltigkeitsreporting

- 66** Im April 2021 veröffentlichte die EU-Kommission einen Vorschlag für eine Corporate Sustainability Reporting Directive (CSRD), die als sog. Änderungsrichtlinie insbesondere diverse Neuerungen in der sog. Bilanzrichtlinie (BilanzRL) vorsieht. Hintergrund für die Gesetzesinitiative auf EU-Ebene war insbesondere das hohe Ausmaß an Freiwilligkeit im Rahmen der bisherigen Anforderungen im Rahmen der Nachhaltigkeitsberichterstattung, insbesondere mit Blick auf die inhaltliche Ausgestaltung sowie die daraus resultierende geringe Vergleichbarkeit der Angaben. Ziel der neuen Regulierung ist es, dass in der EU tätige Unternehmen relevante, vergleichbare und verlässliche Nachhaltigkeitsinformationen offenlegen. Die CSRD löst in Verbindung mit der jeweiligen nationalen Gesetzgebung die bisherigen Grundlagen zur nichtfinanziellen Berichterstattung ab und gestaltet diese komplett neu.
- 67** Eine gravierende Änderung insoweit betrifft neben der zukünftig verpflichtend vorgegebenen Verortung der Nachhaltigkeitsberichterstattung im (Konzern-)Lagebericht insbesondere die deutliche Erweiterung des Kreises der unmittelbaren Adressaten der Regulierung. Er umfasst sodann, nach zuvor lediglich ca. 550 betroffenen Unternehmen, deutschlandweit geschätzt 15.000 Unternehmen und EU-weit gar annähernd 50.000 Unternehmen. Adressiert, und das lediglich unmittelbar, wird damit die Breite der Wirtschaft. Mittelbar werden die Pflichten weitere Unternehmen erreichen, da umfassend mit der Weitergabe entsprechender Informationsanforderungen durch unmittelbare Regulierungsadressaten zu rechnen ist. Die CSRD wurde nach Abschluss des Legislativ-Prozesses am 16.12.2022 im EU-Amtsblatt veröffentlicht. Gemäß Art. 7 der Richtlinie trat sie am 5.1.2023 in Kraft, am zwanzigsten Tag nach ihrer Veröffentlichung. Die CSRD ist als EU-Richtlinie bis zum 6.7.2024 in nationales Recht umzusetzen.⁸¹
- 68** Nach Art. 19a Abs. 2 BilanzRL n. F., der damit auf Ebene der Richtlinie auch eine Berichtsstruktur vorgibt, umfassen die geforderten Informationen Folgendes:
- Beschreibung des Geschäftsmodells und der Strategie, insb.
 - der Resilienz des Geschäftsmodells und der Strategie des Unternehmens gegenüber Risiken im Zusammenhang mit Nachhaltigkeitsbelangen;
 - der Chancen für das Unternehmen im Zusammenhang mit Nachhaltigkeitsbelangen;
 - der Pläne des Unternehmens, um sicherzustellen, dass sein Geschäftsmodell und seine Strategie mit dem Übergang zu einer nachhaltigen Wirt-

⁸¹ Letzter verfügbarer Stand mit Blick auf das deutsche CSRD-Umsetzungsgesetz ist ein am 22.3.2024 veröffentlichter Referentenentwurf, dargestellt unter → Rn. 111 ff. (Hinweis: Redaktionsschluss für dieses Werk war im Juli 2024, weswegen neuere Entwicklungen nicht mehr berücksichtigt werden konnten).

schaft und mit der Begrenzung der globalen Erwärmung auf 1,5 °C im Einklang mit dem Paris-Abkommen vereinbar sind;

- wie das Geschäftsmodell und die Strategie des Unternehmens den Interessen der Stakeholder des Unternehmens und den Auswirkungen des Unternehmens auf Nachhaltigkeitsbelange Rechnung tragen;
- wie die Strategie des Unternehmens in Bezug auf Nachhaltigkeitsbelange umgesetzt wurde.
- Beschreibung der Ziele, auch zeitbezogen, die sich das Unternehmen in Bezug auf Nachhaltigkeitsbelange gesetzt hat, und der Fortschritte, die das Unternehmen bei der Erreichung dieser Ziele gemacht hat.
- Beschreibung der Rolle der Verwaltungs-, Geschäftsführungs- und Aufsichtsorgane in Bezug auf Nachhaltigkeitsbelange (Fachwissen, spezifische Fähigkeiten, Anreizsysteme u.Ä.).
- Beschreibung der Unternehmensrichtlinien in Bezug auf Nachhaltigkeitsbelange.
- Beschreibung
 - des Due-Diligence-Verfahrens, das in Bezug auf Nachhaltigkeitsbelange durchgeführt wurde;
 - der wichtigsten tatsächlichen oder potenziellen nachteiligen Auswirkungen im Zusammenhang mit der Wertschöpfungskette des Unternehmens, einschließlich seiner eigenen Geschäftstätigkeit, seiner Produkte und Dienstleistungen, seiner Geschäftsbeziehungen und seiner Lieferkette;
 - aller ergriffenen Maßnahmen und das Ergebnis dieser Maßnahmen, um tatsächliche oder potenzielle nachteilige Auswirkungen zu verhindern, zu mindern oder zu beheben.
- Beschreibung der wichtigsten Risiken für das Unternehmen im Zusammenhang mit Nachhaltigkeitsbelangen, einschließlich der wichtigsten Abhängigkeiten des Unternehmens von solchen Belangen, und wie das Unternehmen mit diesen Risiken umgeht.
- Beschreibung der Verfahren zur Ermittlung der Informationen unter Berücksichtigung kurz-, mittel- und langfristiger Zeithorizonte.
- Indikatoren, die für die oben genannten Offenlegungen relevant sind.

Die in der CSRD verankerten Berichtspflichten werden weitergehend nach näherer Maßgabe der Art. 19b, 19c BilanzRL n.F. durch die European Sustainability Reporting Standards (ESRS) konkretisiert, die sich grundsätzlich inhaltlich an den klassischen ESG-Kriterien orientieren. Inhaltlich betreffen die Berichterstattungspflichten die in Art. 29b Abs. 2 BilanzRL n.F. spezifizierten sog. ESG-Faktoren (Umweltfaktoren, Sozial- und Menschenrechtsfaktoren, Governance-Faktoren).

69

- Die Umweltfaktoren nach Maßgabe der CSRD entsprechen den sechs Umweltzielen der EU-Umwelttaxonomie-VO:
 - Klimaschutz, auch in Bezug auf Scope-1-, Scope-2- und ggf. Scope-3-Treibhausgasemissionen,

Teil 2 Übergreifende Themen und Herausforderungen – ESG und Governance

- Anpassung an den Klimawandel,
- Wasser- und Meeresressourcen,
- Ressourcennutzung und die Kreislaufwirtschaft,
- Verschmutzung sowie
- Biodiversität und Ökosysteme.
- Die Sozial- und Menschenrechtsfaktoren sind in der CSRD umfangreicher ausformuliert und beinhalten folgende Aspekte:
 - Gleichbehandlung und Chancengleichheit für alle, einschl. Geschlechtergerechtigkeit und gleichen Lohn bei gleichwertiger Arbeit, Ausbildung und Kompetenzentwicklung, Beschäftigung und Inklusion von Menschen mit Behinderungen, Maßnahmen gegen Gewalt und Belästigung am Arbeitsplatz sowie Vielfalt;
 - Arbeitsbedingungen, einschließlich sicherer Beschäftigung, Arbeitszeit und angemessener Löhne, sozialer Dialog, Vereinigungsfreiheit, Existenz von Betriebsräten, Tarifverhandlungen, einschließlich des Anteils der Arbeitnehmer, für die Tarifverträge gelten, Informations-, Anhörungs- und Mitbestimmungsrechte der Arbeitnehmer, Vereinbarkeit von Beruf und Privatleben sowie Gesundheit und Sicherheit;
 - Achtung der Menschenrechte, Grundfreiheiten, demokratische Grundsätze und Standards, die in der Internationalen Charta der Menschenrechte und anderen grundlegenden Menschenrechtsübereinkommen der Vereinten Nationen, einschließlich des UN-Übereinkommens über die Rechte von Menschen mit Behinderungen und der Erklärung der Vereinten Nationen über die Rechte der indigenen Völker, sowie in der Erklärung der Internationalen Arbeitsorganisation (IAO) über grundlegende Prinzipien und Rechte bei der Arbeit und den grundlegenden Übereinkommen der IAO, der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten, der Europäischen Sozialcharta und der Charta der Grundrechte der EU festgelegt sind.
- Die Governance-Faktoren umfassen Folgendes:
 - Die Rolle der Verwaltungs-, Leitungs- und Aufsichtsorgane des Unternehmens im Zusammenhang mit Nachhaltigkeitsaspekten und ihre Zusammensetzung sowie ihr Fachwissen und ihre Fähigkeiten zur Wahrnehmung dieser Rolle oder ihr Zugang zu solchem Fachwissen und solchen Fähigkeiten;
 - die Hauptmerkmale der internen Kontroll- und Risikomanagementsysteme des Unternehmens in Bezug auf den Prozess der Nachhaltigkeitsberichterstattung und der Beschlussfassung;
 - Unternehmensethik und Unternehmenskultur, einschließlich der Bekämpfung von Korruption und Bestechung, des Schutzes von Hinweisgebern und des Tierwohls,
 - Tätigkeiten und Verpflichtungen des Unternehmens im Zusammenhang mit der Ausübung seines politischen Einflusses, einschließlich seiner Lobbytätigkeiten;

- die Pflege und die Qualität der Beziehungen zu Kunden, Lieferanten und Gemeinschaften, die von den Tätigkeiten des Unternehmens betroffen sind, einschließlich Zahlungspraktiken, insbes. in Bezug auf verspätete Zahlungen an kleine und mittlere Unternehmen.

Die ESRS werden nach Art. 49 Abs. 2 und 3a BilanzRL n. F. durch die European Financial Reporting Advisory Group mit Sitz in Brüssel (EFRAG) entwickelt und letztlich durch die EU-Kommission mittels sogenannter delegierter Rechtsakte erlassen. Sie sollen alle drei Jahre überprüft und ggf. überarbeitet werden und gewährleisten, dass das nachhaltigkeitsbezogene Reporting der Verpflichteten den Anforderungen an die Offenlegungen und den damit verbundenen Zielen der EU gerecht wird. Die im Nachhaltigkeitsbericht gemachten Angaben haben nach Art. 19b Abs. 2 Unterabs. 1, 19c Unterabs. 1 Satz 3 BilanzRL n. F. verständlich, relevant, repräsentativ, überprüfbar und vergleichbar zu sein. **70**

Eine solche Delegation zum Erlass von Rechtsakten ohne Gesetzescharakter ist zulässig, sofern im originären Gesetzgebungsakt, also in der CSRD, nicht nur Geltungsbereich und Dauer, sondern auch Ziel und Inhalt der Befugnisübertragung ausdrücklich festgelegt werden.⁸² Dabei sind die wesentlichen Aspekte eines Themengebiets dem Gesetzgebungsakt als solchem vorbehalten. Das ist auch der Hintergrund dafür, dass die CSRD bereits eine – wie vorstehend aufgezeigt – insgesamt recht ausführliche Beschreibung der Berichtsanforderungen enthält, dies etwa mit Blick auf die Berichtsgegenstände und -inhalte gemäß Art. 19a Abs. 1–3 BilanzRL n. F. **71**

Am 22.12.2023 wurde der delegierte Rechtsakt zum sogenannten Set 1 der ESRS, den sektoragnostischen Standards im EU-Amtsblatt veröffentlicht.⁸³ Die ESRS wurden zuvor ab April 2022 konsultiert und Ende Juli 2023 durch die Europäische Kommission angenommen. **72**

Zur Unterstützung der Anwender bei der anforderungskonformen Aufstellung der Unternehmen veröffentlichte die EFRAG am 31.5.2024 nach einer vorhergehenden Konsultation final sogenannte „Implementation Guidances“ bezogen auf das „Materiality Assessment“ (IG 1), „Value Chain“ (IG 2) und „Detailed ESRS Datapoints“ (IG 3).⁸⁴ Weitere „Implementation Guidances“, etwa bezogen auf „Training and Skills Development Metrics“, sind angekündigt; ferner existieren diverse weitere Hilfestellungen für die Erarbeitung der Berichte, auch in den ESRS selbst. **73**

Die ESRS sollen nach Art. 29b Abs. 1 Unterabs. 3 Nr. 2 BilanzRL n. F. auch sektorspezifische Nachhaltigkeitsthemen behandeln. Die EFRAG ist deshalb gebe- **74**

⁸² Art. 290 Abs. 1 AEUV.

⁸³ Delegierte Verordnung (EU) 2023/2772 der Kommission vom 31. Juli 2023 zur Ergänzung der Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates durch Standards für die Nachhaltigkeitsberichterstattung.

⁸⁴ Sämtlich verfügbar hier: <https://www.efrag.org/News/Public-524/Finalization-of-Three-EFRAG-ESRS-IG-Documents-EFRAG-IG-1-to-3-> (zuletzt abgerufen am 8.7.2024).

ten, auch solche Standards zu entwickeln. Ein bislang vorliegendes Arbeitspapier zur Sektorklassifikation („ESRS SEC“, weitere folgen) enthält eine Übersicht mit ca. 40 Sektoren in Orientierung an der NACE-Code Klassifizierung, für die nach aktuellem Stand bis Mitte 2026 sukzessive sektorspezifische ESRS erarbeitet und konsultiert werden sollen.⁸⁵ Die sektorspezifischen ESRS interpretieren und ergänzen die sektoragnostischen ESRS. Wegen des Kriteriums einer Zehn-Prozent-Grenze gemessen an den Außenumsatzerlösen des berichtenden Unternehmens nach ESRS 2.38 i.V.m. AR 12 kann ein Unternehmen rechnerisch bis zu neun Sektoren angehören bzw. deren spezifische Standards – wohlgemerkt stets unter Berücksichtigung des Grundsatzes der doppelten Wesentlichkeit – anzuwenden haben.⁸⁶

- 75 Weitere ESRS des sogenannten Set 2 werden die von der CSRD adressierten Unternehmen aus Drittstaaten mit nennenswerten Geschäftstätigkeiten in der EU und die kapitalmarktorientierten kleinen und mittleren Unternehmen (listed small and medium-sized entities, listed SMEs/LSMEs) betreffen. Ferner ist ein – freiwillig anwendbarer – Standard für nicht in den Anwendungsbereich der CSRD fallende, nicht-kapitalmarktorientierte SMEs in der Entwicklung (voluntary SMEs/VSMEs). Es ist derzeit vorgesehen, dass diese Standards seitens der EFRAG noch im Jahr 2024 an die EU-Kommission übergeben werden, damit eine Veröffentlichung in 2025 erfolgen kann. Die ESRS VSME sollen die Informationsbedarfe aufgreifen, die sich zum Beispiel aufgrund einer Zugehörigkeit der nicht-kapitalmarktorientierten SMEs zur Lieferkette von CSRD-Adressaten ergeben können. Die Standards sollen im Grundsatz den allgemeinen Standards zur Nachhaltigkeitsberichterstattung entsprechen; allerdings legt Art. 19a Abs. 6 BilanzRL n.F. fest, dass für SMEs geringere Anforderungen an die Berichterstattung zu gelten haben, sie sei „den Kapazitäten und Merkmalen kleiner und mittlerer Unternehmen angemessen“ auszugestalten.
- 76 Die NACE-Code Klassifizierung bildet ferner auch den Ausgangspunkt für die EU-Umwelttaxonomie, die von den der CSRD unterfallenden Unternehmen ebenfalls anzuwenden ist.⁸⁷ Die Unternehmen müssen zusätzlich zu den anderweitig zu machenden Nachhaltigkeitsangaben offenlegen, inwieweit ihre Wirtschaftsaktivitäten im Sinne dieser Taxonomie nachhaltig sind. Insbesondere haben sie nach Maßgaben separater delegierter Rechtsakte Angaben zu ökologisch nachhaltigen Umsatzerlösen, Investitions- und Betriebsausgaben zu machen.

1. Adressaten und Konzernprivileg

- 77 Die Einführung der Berichtspflichten erfolgt gestaffelt. Bereits seit dem 1.1.2024 sind in einem ersten Schritt diejenigen Unternehmen berichtspflichtig,

85 EFRAG SRB meeting: Exposure Draft ESRS SEC 1 vom 14.3.2023.

86 Eine Zugehörigkeit zu gar 10 Sektoren wäre wohl unrealistisch.

87 Verordnung (EU) 2020/852 des Europäischen Parlaments und des Rates vom 18. Juni 2020 über die Einrichtung eines Rahmens zur Erleichterung nachhaltiger Investitionen und zur Änderung der Verordnung (EU) 2019/2088 (ABl. L 198 vom 22.6.2020, S. 13) (TaxonomieVO).

die schon vormals vom Anwendungsbereich der CSR-Richtlinie erfasst waren (vgl. → Rn. 21 ff.). Sie haben ihren ersten Bericht im Jahre 2025 für das vorangegangene Geschäftsjahr zu erstatten.

Für Geschäftsjahre ab dem 1.1.2025 müssen sodann alle großen Kapitalgesell- **78**
schaften nach § 267 Abs. 3 HGB und ihnen über § 264a HGB gleichgestellte haftungsbeschränkte Personengesellschaften in 2026 berichten. Große Kapitalgesellschaften sind solche, die mindestens zwei der drei in § 267 Abs. 2 HGB bezeichneten Merkmale überschreiten: Bilanzsumme von 25 Mio. EUR, Umsatzerlöse von 50 Mio. EUR und Anzahl der Mitarbeitenden von mehr als 250. Diese Phase betrifft damit dann die Breite der Wirtschaft.

Im öffentlichen Sektor existieren zudem zahlreiche Gesellschaften, die nach **79**
Maßgabe ihrer Statuten verpflichtet sind, ihre Rechnungslegung „wie große Unternehmen“ vorzunehmen. Auch sie unterliegen aufgrund derartiger Vorgaben den Anforderungen. Die Berichterstattungspflicht für diverse weitere öffentliche Unternehmen ergibt sich unmittelbar aus spezifischen landes- oder auch bundesrechtlichen Vorschriften.⁸⁸

Ab dem 1.1.2026 erweitert sich der Adressatenkreis der CSRD ein weiteres Mal **80**
um gelistete KMU mit mehr als 10 Beschäftigten, mehr als 900.000 EUR Umsatz oder mehr als 450.000 EUR Bilanzsumme, um kleine und nicht komplexe Kreditinstitute, also in Deutschland oftmals kleinere Genossenschaftsbanken sowie Sparkassen, sowie firmeneigene Versicherungs- und Rückversicherungsunternehmen. Sie haben grundsätzlich in 2027 zu berichten, können indes eine Opt-out-Lösung in Anspruch nehmen und müssen dann erst in 2029 in einem ersten Bericht für das Geschäftsjahr 2028 berichten. In letztere Phase sind ebenfalls die Nicht-EU-Unternehmen mit einem Umsatz von mehr als 150 Mio. EUR innerhalb der EU und einer Zweigniederlassung oder einer Tochtergesellschaft in Form eines großen Unternehmens oder eines gelisteten KMU mit einem Umsatz von mehr als 40 Mio. EUR in der EU einzuordnen. Auch sie haben ihren ersten Bericht für das Geschäftsjahr 2028 in 2029 zu erstatten.

Unter bestimmten Bedingungen existiert ein sogenanntes Konzernprivileg, so- **81**
fern nicht ein einzubeziehendes Unternehmen selbst als groß und kapitalmarkt-orientiert anzusehen ist.⁸⁹ Tochterunternehmen werden gemäß Art. 19a Abs. 9 und 10, 37 BilanzRL n.F.⁹⁰ von der Pflicht zur Nachhaltigkeitsberichterstattung befreit. Für die Befreiung eines Mutterunternehmens, das auch selbst Tochterunternehmen ist, gilt Art. 29a Abs. 8 und 9 BilanzRL n.F.⁹¹ Voraussetzung ist in beiden Fällen unter anderem, dass die entsprechenden konzernzugehörigen Gesellschaften in den konsolidierten Nachhaltigkeitsbericht ihres EU- oder Non-

⁸⁸ Vgl. z. B. § 25 Eigenbetriebsverordnung für das Land Nordrhein-Westfalen (EigVO NRW): Pflicht zur Lageberichterstattung.

⁸⁹ *Lanfermann/Baumüller*, IRZ 2023, 89, 91; *Feisel/Makowka*, DB 2024, 65, 67.

⁹⁰ Siehe § 289b Abs. 2 HGB-Entwurf.

⁹¹ Siehe § 315b Abs. 2 HGB-Entwurf.

EU-Mutterunternehmens einbezogen sind und die Berichterstattung der Muttergesellschaft gemäß den Anforderungen der CSRD („gleichwertig“) geprüft und testiert erfolgt und veröffentlicht wird.

- 82** Mit Blick auf (nicht kapitalmarktorientierte und also nicht von der Regulierung erfasste) KMU ist von deren mittelbarer Betroffenheit über eine Weitergabe von Pflichten im Rahmen von Geschäftsbeziehungen mit unmittelbaren Adressaten auszugehen. Auch dessen ungeachtet ist darüber hinaus generell – und fraglos im Einklang mit den EU-Zielen der Transformation hin zu einer nachhaltigen Wirtschaft – mit einer Ausstrahlungswirkung der CSRD-Vorschriften auf kleinere Unternehmen als Nichtadressaten der Regulierung zu rechnen. Ein derzeit in Erarbeitung befindlicher Entwurf eines freiwilligen ESRS VSME richtet sich vor diesen Hintergründen speziell an KMU, die nicht direkt in den Anwenderkreis der CSRD fallen.⁹² Die Einführung eines europaweit gültigen Standards für die freiwillige Nachhaltigkeitsberichterstattung soll diese Unternehmen dabei unterstützen, den insoweit vielfältigen Anforderungen ihrer Stakeholder, etwa ihrer Mitarbeitenden, Geschäftspartner und Kapitalgeber, zu entsprechen und ihre Nachhaltigkeitsleistung auf eine Art und Weise darzustellen, die sowohl für alle Stakeholder relevant und verständlich ist als auch – zur Vermeidung einer Überforderung unterschiedlich großer KMU – den Prinzipien der Verhältnismäßigkeit und Flexibilität angemessen Rechnung trägt.
- 83** Der derzeit vorgeschlagene Entwurf für eine freiwillige Berichterstattung der KMU beruht auf einem modularen Ansatz und erfordert neben qualitativen Angaben beispielsweise zu Strategien, Maßnahmen und Zielen des Unternehmens zu bestimmten Nachhaltigkeitsaspekten auch quantitative Angaben, also Leistungskennzahlen, zu bestimmten grundlegenden Belangen. Insbesondere wird in ihm in bestimmten Datenpunkten auf die spezifischen Informationsbedürfnisse von Geschäftspartnern und Kapitalgebern eingegangen. Der Vorschlag ist indes wegen der ihm innewohnenden Komplexität großer Kritik ausgesetzt, eine Überarbeitung und Erleichterung in den Anforderungen scheint wahrscheinlich.

2. Überblick über die ESRS

- 84** Die Anforderungen an die Nachhaltigkeitsberichterstattung richten sich künftig maßgeblich nach den Vorgaben der einschlägigen European Sustainability Reporting Standards – ESRS, die von der EU-Kommission im Wege der Befugnis zu delegierten Rechtsakten erlassen und auch fortgeschrieben werden (Art. 29b und Art. 29c BilanzRL n. F.).⁹³
- 85** Die ESRS konkretisieren, welche Informationen die Unternehmen zukunftsgerichtet und vergangenheitsbezogen sowie qualitativ und quantitativ nach näherer Maßgabe der Vorgaben in Art. 19a (bzw. Art. 29a zur Konzernberichterstattung)

⁹² <https://www.efrag.org/News/Public-479/EFRAGs-public-consultation-on-two-Exposure-Drafts-on-sustainability-r> (zuletzt abgerufen am 8.7.2024).

⁹³ Vgl. bereits umfassend zu den ESRS: vorstehend unter → Rn. 66 ff.

und Art. 29b Bilanz-RL n. F. zu geben haben und in welcher Struktur diese Angaben zu erfolgen haben. Auch ist die gesamte Wertschöpfungskette in die Betrachtungen mit einzubeziehen. Die ESRS sind – auch nach der im Rahmen von deren Konsultation stark kritisierten und dann reduzierten Anzahl an Disclosure Requirements („DR“) – unverändert von einer insgesamt hohen inhaltlichen Komplexität bzw. Detailtiefe geprägt. Die Anzahl der DR wurde in dieser Phase von 137 auf 82 reduziert, mit Blick auf die reportingrelevanten qualitativen und quantitativen Datapoints erfolgte eine Reduktion von 2.161 auf 1.144 Datenpunkte.⁹⁴

U.a. müssen betroffene Unternehmen nachhaltigkeitsbezogenen Informationen zum Geschäftsmodell, zu Strategien, zu Konzepten bzw. Politiken und zu deren Ergebnissen offenlegen und zeitgebunden ihre Nachhaltigkeitsziele sowie -fortschritte beschreiben. Den Verwaltungs-, Leitungs- und Aufsichtsorganen kommt im Zusammenhang mit Nachhaltigkeitsaspekten eine große Bedeutung zu, weswegen es Darlegungen zu deren spezifischem Fachwissen, Fähigkeiten und etwaigen Anreizsystemen bedarf. Übergreifend ist eine Beschreibung der wichtigsten Auswirkungen der Geschäftstätigkeit sowie Risiken und Chancen gefordert, denen ein Unternehmen im Zusammenhang mit Nachhaltigkeitsaspekten ausgesetzt ist, einschließlich der wichtigsten Abhängigkeiten, Due-Diligence-Prozesse, Steuerungsmechanismen (Kennzahlen) und Maßnahmen – und dies stets auch unter Berücksichtigung der Wertschöpfungskette. **86**

a) Regelungsinhalte des Set 1 der ESRS

Das final veröffentlichte Set 1 der sektoragnostischen ESRS besteht letztlich aus zwei übergreifenden sogenannten Querschnittsstandards mit allgemeinen, also nicht auf einzelne Nachhaltigkeitsaspekte bezogenen Berichtsanforderungen, den ESRS 1 und 2, sowie aus zehn themenbezogenen Standards zu einzelnen ESG-Aspekten, konkret fünf zu Umwelt-Aspekten (ESRS E1-E5), vier zu Sozial-Aspekten (ESRS S1-S4) und einem Standard zu Governance-Aspekten (ESRS G1).⁹⁵ **87**

Die ESRS 1 und 2 beinhalten ergänzend zu den Inhalten der CSRD zum einen Festlegungen mit Blick auf die allgemeinen Anforderungen zur Erstellung und Darstellung der Nachhaltigkeitsberichte und zum anderen konkrete Berichtsanforderungen, die übergreifend alle Unternehmen betreffen – unabhängig von spezifischen Themen oder einer Sektorzugehörigkeit. Die themenspezifischen ESRS konkretisieren oder erweitern diese allgemeinen Anforderungen. Ihnen – und grundsätzlich auch dem ESRS 2 – ist gemein, dass den Darlegungen zu de- **88**

⁹⁴ Die Zahlenangaben hierzu in Fachveröffentlichungen differieren; offenbar hängt dies mit der Zählweise zusammen.

⁹⁵ Die EU Kommission hat am 18.4.2024 wegen verschiedener textlicher und redaktioneller Unzulänglichkeiten ein sog. Corrigendum zum ESRS Set 1 veröffentlicht, vgl. <https://www.drsc.de/en/news/berichtigungen-zum-esrs-set-1-veroeffentlicht/> (zuletzt abgerufen am 8.7.2024).

ren Zielsetzung und zu einer etwaigen Interaktion mit anderen Standards jeweils die Berichtsanforderungen (Disclosure Requirements) und abschließend Anhänge mit Definitionen und Anwendungsvorgaben bzw. -hilfen (Application Requirements) und anderen relevanten Aspekten folgen.

89 ESRS 1 enthält so u.a. die Anlage A „Anwendungsanforderungen“, die als „festen Bestandteil mit bindender Kraft“ unterteilt nach den Kategorien Thema, Unterthema und Unter-Unterthema⁹⁶ unter ESRS 1.AR16 eine Liste der Nachhaltigkeitsaspekte beinhaltet, die in den themenbezogenen ESRS behandelt werden.

90 Neben der Struktur der **Querschnittsstandards**:

- ESRS 1 „Allgemeine Anforderungen“:
 - ESRS-Kategorien, Berichterstattungsbereiche und Konventionen für die Ausarbeitung,
 - qualitative Merkmale von Informationen,
 - doppelte Wesentlichkeit,
 - Sorgfaltspflicht,
 - Wertschöpfungskette,
 - Zeithorizonte,
 - Erstellung und Darstellung von Nachhaltigkeitsinformationen,
 - Aufbau der Nachhaltigkeitserklärung,
 - Verknüpfungen mit anderen Teilen der Unternehmensberichterstattung,
- und ESRS 2 „Allgemeine Angaben“:
 - Grundlagen für die Erstellung der Nachhaltigkeitserklärung,
 - Governance (Rolle Verwaltungs-, Leitungs- und Aufsichtsorgane, Anreizsysteme, Risikomanagement, interne Kontrollen),
 - Strategie (Strategie, Geschäftsmodell und Wertschöpfungskette, Relevanz Stakeholder, wesentliche Auswirkungen, Risiken und Chancen und ihr Zusammenspiel mit Strategie und Geschäftsmodell),
 - Management der Auswirkungen, Risiken und Chancen (Verfahren zur Bewertung der Wesentlichkeit, Angaben zu Strategien und Maßnahmen),
 - Parameter und Ziele,
 - zugrunde zu legende Konzepte und Prinzipien für die Erstellung und Darstellung von Nachhaltigkeitsberichten,

beinhaltet die **Anlage A** des ESRS 1 eine **Übersicht zu den Inhalten der themenbezogenen ESRS des Set 1**, also zu den Umwelt-Aspekten, den Sozial-Aspekten und den Governance-Aspekten.

91 **Umweltaspekte:**

- ESRS E1 „Klimawandel“:
 - Angaben über Auswirkungen der Unternehmenstätigkeit mit Blick auf die Anpassung an den Klimawandel, Klimaschutz und Energie.

⁹⁶ Hier sprachlich und inhaltlich redigiert, inhaltliche Überschneidungen bleiben.

- ESRS E2 „Umweltverschmutzung“:
 - Angaben über Auswirkungen der Unternehmenstätigkeit auf Verschmutzung von Luft, Wasser, Boden, lebenden Organismen, Nahrungsressourcen;
 - Angaben über (besonders) besorgniserregende Stoffe, Mikroplastik.
- ESRS E3 „Wasser- und Meeresressourcen“:
 - Angaben über Auswirkungen der Unternehmenstätigkeit auf Wasser und Meere (inkl. Schutzmaßnahmen, Wasserverbrauch, Abwasser etc.);
 - Gewinnung und Nutzung von Meeresressourcen.
- ESRS E4 „Biologische Vielfalt und Ökosysteme“:
 - Angaben über den Beitrag der Unternehmenstätigkeit zu Biodiversitätsverlusten (Klimawandel, Landnutzungsänderungen, Süßwasser- und Meeresnutzungsänderungen, direkte Ausbeutung, Bedeutung invasiver gebietsfremder Arten, Umweltverschmutzung);
 - Auswirkungen auf den Zustand der Arten (Populationsgröße, Ausrottungsrisiko)
 - Auswirkungen auf den Umfang und den Zustand von Ökosystemen (Landdegradation, Verschlechterung der Ökosystemdienstleistungen des Bodens, Wüstenbildung, Bodenversiegelung);
 - Auswirkungen und Abhängigkeiten von Ökosystemdienstleistungen (Lebensgemeinschaften von Organismen); „Vorteile, die Menschen aus Ökosystemen beziehen“ (bestäubte Obstblüten, Reproduktion von Fischpopulationen als Nahrung o.Ä.);
- ESRS E5 „Ressourcennutzung und Kreislaufwirtschaft“:
 - Angaben über Auswirkungen der Unternehmenstätigkeit auf Ressourcenverbrauch (Ressourcenzuflüsse, einschließlich Ressourcennutzung, Ressourcenabflüsse, Abfälle);
 - Angaben über Maßnahmen zur Entkopplung von Ressourcenverbrauch und Wachstum.

Sozialaspekte:

92

- ESRS S1 „Eigene Belegschaft“:
 - Angaben über Auswirkungen der Unternehmenstätigkeit auf die eigene Belegschaft in Bezug auf Arbeitsbedingungen, Chancengleichheit und sonstige Arbeitnehmerrechte (Sichere Beschäftigung, Arbeitszeit, angemessene Entlohnung, sozialer Dialog, Vereinigungsfreiheit, Existenz von Betriebsräten, Mitwirkungsrechte, Tarifgebundenheit, Work-Life-Balance, Gesundheitsschutz und Sicherheit);
 - Gleichbehandlung und Chancengleichheit für alle (Gleichstellung der Geschlechter und gleicher Lohn für gleiche Arbeit, Schulungen und Kompetenzentwicklung, Beschäftigung und Inklusion von Menschen mit Behinderungen, Maßnahmen gegen Gewalt und Belästigung am Arbeitsplatz, Vielfalt);

Teil 2 Übergreifende Themen und Herausforderungen – ESG und Governance

- sonstige arbeitsbezogene Rechte (Kinderarbeit, Zwangsarbeit, angemessene Unterbringung, Datenschutz).
- ESRS S2 „Arbeitskräfte in der Wertschöpfungskette“:
 - Angaben über Auswirkungen der Unternehmenstätigkeit auf Mitarbeiter in der Wertschöpfungskette, also bezogen auf eigene, vor- und nachgelagerte Aktivitäten (Sichere Beschäftigung, Arbeitszeit, angemessene Entlohnung, sozialer Dialog, Vereinigungsfreiheit, Existenz von Betriebsräten, Mitwirkungsrechte, Tarifgebundenheit, Work-Life-Balance, Gesundheitsschutz und Sicherheit);
 - Gleichbehandlung und Chancengleichheit für alle (Gleichstellung der Geschlechter und gleicher Lohn für gleiche Arbeit, Schulungen und Kompetenzentwicklung, Beschäftigung und Inklusion von Menschen mit Behinderungen, Maßnahmen gegen Gewalt und Belästigung am Arbeitsplatz, Vielfalt);
 - sonstige arbeitsbezogene Rechte (Kinderarbeit, Zwangsarbeit, Angemessene Unterbringung, Wasser- und Sanitäreinrichtungen, Datenschutz).
- ESRS S3 „Betroffene Gemeinschaften“:
 - Angaben über Auswirkungen der Unternehmenstätigkeit auf lokale Gemeinschaften in der Wertschöpfungskette des Unternehmens;
 - wirtschaftliche, soziale und kulturelle Rechte von Gemeinschaften (Angemessene Unterbringung, angemessene Ernährung, Wasser- und Sanitäreinrichtungen, bodenbezogene Auswirkungen, sicherheitsbezogene Auswirkungen);
 - Bürgerrechte und politische Rechte von Gemeinschaften (Meinungsfreiheit, Versammlungsfreiheit, Auswirkungen auf Menschenrechtsverteidiger);
 - Rechte indigener Völker (Freiwillige und in Kenntnis der Sachlage erteilte vorherige Zustimmung zu Aktivitäten, Selbstbestimmung, kulturelle Rechte).
- ESRS S4 „Verbraucher und Endnutzer“:
 - informationsbezogene Angaben über Auswirkungen der Unternehmenstätigkeit bzw. Produkte oder Dienstleistungen auf Verbraucher und/oder Endnutzer (Datenschutz, Meinungsfreiheit, Zugang zu (hochwertigen) Informationen);
 - persönliche Sicherheit von Verbrauchern und/oder Endnutzern (Gesundheitsschutz und Sicherheit, persönliche Sicherheit, Kinderschutz);
 - soziale Inklusion von Verbrauchern und/oder Endnutzern (Nichtdiskriminierung, Zugang zu Produkten und Dienstleistungen, Verantwortliche Vermarktungspraktiken).

93 Governance-Aspekte:

- ESRS G1 Unternehmenspolitik:
 - Unternehmenskultur;
 - Schutz von Hinweisgebern (Whistleblowern);

- Tierschutz;
- politisches Engagement und Lobbytätigkeiten;
- Management der Beziehungen zu Lieferanten, einschließlich Zahlungspraktiken;
- Korruption und Bestechung (Vermeidung und Aufdeckung einschließlich Schulung, Vorkommnisse).

Nach Art. 2 Nr. 19, 19 Abs. 1 Unterabs. 4 der Bilanzrichtlinie n.F. bedarf es darüber hinaus der Offenlegung von Informationen über immaterielle Vermögenswerte (Abhängigkeiten, Wertschöpfungsquellen etc.). Insbesondere die Faktoren Human-Kapital (z.B. Altersstruktur, Fluktuation, Qualifikation & Weiterbildung, Erfahrung, Mitarbeiter-Zufriedenheit, Mitarbeiter-Gesundheit, Motivation, Innovationskraft der Mitarbeiter), Beziehungskapital (z.B. gute Beziehungen zu Kunden, Lieferanten, Investoren und anderen Stakeholdern sowie zur Öffentlichkeit, Förderung Zusammenhalt in der Gesellschaft) und Wissens- und Strukturkapital (z.B. geistiges Eigentum, F&E, Innovationen, funktionierende Prozesse in Fertigung und Administration, Produktqualität, Standortqualität/-faktoren, Medienpräsenz, Attraktivität als Arbeitgeber) erhalten so eine speziell größere Bedeutung im Rahmen der Rechnungslegung. **94**

b) Der Grundsatz der doppelten Wesentlichkeit und weitere Verfahrensvorgaben

Ausgehend von der Definition der Stakeholder des Unternehmens regeln ESRS 1.21 ff. den im Rahmen des zukünftigen Nachhaltigkeitsreportings elementaren Grundsatz der doppelten Wesentlichkeit. Grundsätzlich ist im Rahmen des Reportings nur zu den Querschnittsstandards verpflichtend zu berichten – wobei der ESRS 1 ohnehin eher nur allgemein gehaltene Vorgaben enthält und sich diese Berichtspflicht damit konkret auf ESRS 2 bezieht. Zu allen anderen ESRS hat das Unternehmen eine spezifische Wesentlichkeitsanalyse durchzuführen: Hierbei geht es um die Identifikation relevanter Themen nach Maßgabe einer sogenannten doppelten Wesentlichkeitsanalyse. Nur über die solchermaßen identifizierten Themen ist sodann zu berichten. **95**

Ein Nachhaltigkeitsthema ist wesentlich und damit also berichtspflichtig, wenn es sich entweder auf erhebliche tatsächliche oder potenzielle Auswirkungen des Unternehmens auf Mensch oder Umwelt bezieht (Inside-Out-Perspektive oder Impact Materiality) oder wenn es kurz-, mittel- oder langfristig erhebliche finanzielle Auswirkungen auf das Unternehmen, d. h. auf Entwicklung, Leistung und Position des Unternehmens hat oder haben kann (Outside-in-Perspektive oder Financial Materiality). Hervorzuheben ist, dass die doppelte Wesentlichkeit nicht auf einer „Und“- sondern auf einer „Oder“-Komponente beruht, sodass ein Aspekt nur hinsichtlich einer Dimension als wesentlich eingestuft werden muss, um bereits unter die Berichtspflicht zu fallen. **96**

Eine Ausnahme gilt lediglich für den ESRS E1 (Klimawandel). Bewertet ein Unternehmen diesen Aspekt als „nicht wesentlich“, muss es nach dem „Comply or **97**

Explain“-Prinzip genauer und unter Inbezugnahme der Ergebnisse der Wesentlichkeitsanalyse erläutern, warum auf Angaben zum Klimawandel verzichtet wird.

- 98 Die Beurteilung der Wesentlichkeit eines Nachhaltigkeitsthemas soll sich nach ESRS 1.62 auf im Unternehmen existente Due Diligence-Prozesse stützen. Als solche Prozesse sind die Verfahren definiert, derer sich das Unternehmen bedient, um die wesentlichen tatsächlichen und potenziellen nachteiligen Auswirkungen der Nachhaltigkeitsaspekte zu ermitteln, zu überwachen, zu verhüten, zu mildern, wiedergutzumachen oder zu beseitigen und den Umgang des Unternehmens mit diesen Auswirkungen festzulegen.⁹⁷ Die Berichtsinhalte der Nachhaltigkeitsberichterstattung hängen damit entscheidend von den implementierten Due-Diligence-Prozessen ab, die als solche auch darzustellen sind.
- 99 Grundsätzlich ergibt sich aus den qualitativen Merkmalen, dass für die Wesentlichkeitsanalyse nach den ESRS eine Brutto-Betrachtung zu erfolgen hat, bereits gesetzte Reaktionen bzw. Maßnahmen auf negative Auswirkungen und Risiken also nicht gegengerechnet werden dürfen.⁹⁸ Die Darstellungen haben damit vor den Effekten der sie adressierenden Strategien, Maßnahmen und Ziele zu erfolgen, da diese – auch im Hinblick auf ihre Milderungseffekte – gesondert dargestellt werden sollen. In ESRS 1.QC8. heißt es einerseits: „Informationen dürfen nicht aufgerechnet oder ausgeglichen werden, um sie neutral zu machen.“ Andererseits aber legt ESRS 1.QC8. fest, dass das Unternehmen „zusätzlich zu den Bruttowerten [...] aufgerechnete Informationen vorlegen [kann], sofern durch diese Darstellung keine relevanten Informationen verschleiert werden und wenn die Auswirkungen und die Gründe der Aufrechnung klar erläutert werden“. Wie grundsätzlich auch im Rahmen der Finanzberichterstattung sollte es daher zumindest dann, wenn ausschließliche Brutto-Betrachtungen ein insgesamt unzutreffendes oder irreführendes Bild abgeben, in Betracht kommen, von einer durchgehenden Brutto-Berichterstattung abzusehen. Dieses Vorgehen würde auch ganz generell dem bilanziellen Erfordernis der Sicherstellung der Konnektivität von Finanz- und Nachhaltigkeitsberichterstattung und konsistenter Informationen Rechnung tragen. Der Fachausschuss Nachhaltigkeitsberichterstattung des DRSC (FA) befasste sich insbesondere in seiner 21. Sitzung vom 16.10.2023 mit dem Thema und kam – wenngleich mit abweichend erklärten Ansichten – ausweislich des öffentlich verfügbaren Ergebnisberichts der Sitzung insoweit zu folgendem Ergebnis:⁹⁹

„Der FA positionierte sich mehrheitlich für die Zulässigkeit eines Nettoansatzes. Konsistent zu seiner Diskussion in der vergangenen Sitzung vom 12.9.2023 urteilte der FA, dass ein Nachhaltigkeitsthema nicht in jedem Fall allein deshalb grundsätzlich berichtspflichtig sein sollte, weil die hypotheti-

⁹⁷ Vgl. Erwägungsgrund 31 zur CSRD.

⁹⁸ Baumüller/Lopatta u. a., in: Freiberg/Lanfermann, ESRS, § 3 Rn. 64.

⁹⁹ <https://www.drsc.de/termine/21-sitzung-fa-nb/> (zuletzt abgerufen am 8.7. 2024).

sche Möglichkeit einer Auswirkung (z. B. eines Umweltschadens) bestehe. Bei hinreichend geringen Wahrscheinlichkeiten, z. B. aufgrund hochwirksamer Vermeidungsmaßnahmen, erscheine eine Berichterstattung nicht in jedem Fall zweckmäßig. Unter Umständen sei ein Nachhaltigkeitsbericht, welcher zahlreiche Themen beinhaltet, mit denen faktisch keine Risiken und Auswirkungen einhergehen, nicht informativ, weil den Adressaten dadurch relevante Informationen verborgen bleiben könnten. Zudem sprächen auch praktische Gründe deutlich gegen die Anwendung eines reinen Bruttoansatzes bei der Identifikation wesentlicher IROs. Eine Minderheit des FA folgte dieser Ansicht nicht. Der Fachausschuss konzidierte, dass eine Bruttobetrachtung in Einzelfällen jedoch notwendig sein könnte, z. B. wenn sich seitens der Stakeholder ein starkes Interesse an der Information zeige. Mehrere Fachausschussmitglieder drückten Bedenken gegen eine Regelung aus, welche ausschließlich eine Nettobetrachtung zulässt. Ein FA-Mitglied lehnte eine vollständige Nettobetrachtung ab.“

Die offengelegten Informationen sollen zukunftsorientierte und rückblickende Informationen sowie qualitative und quantitative Informationen enthalten und auch Informationen über die Wertschöpfungskette des Unternehmens, einschließlich der eigenen Geschäftstätigkeit, Produkte und Dienstleistungen, seiner Geschäftsbeziehungen und – explizit auch in diesem Rahmen nochmals hervorgehoben – seiner Lieferkette. ESRS 1.68 stellt bezogen auf die Wertschöpfungskette und den Tiefgang der Berichterstattung klar:

100

„The extension of the information about the reporting undertaking to include value chain information does not require information on each and every entity in the value chain, but the inclusion of material value chain information.“

Nach näherer Erläuterung durch die Implementation Guidance Value Chain (IG 2) mit Blick auf die Bedeutung der Value Chain gilt die Anforderung der Offenlegung von Informationen aus der Wertschöpfungskette überdies nicht für jede Angabepflicht.¹⁰⁰ Nur solche Informationen, die für das Verständnis der wesentlichen Auswirkungen, Risiken und Chancen notwendig sind, sind nach IG 2.20 anzugeben. Die Wertschöpfungskette ist unter diesen Maßgaben in die Wesentlichkeitsanalyse einzubeziehen und bildet gleichsam den Ausgangspunkt aller Überlegungen. Dem ESRS Glossar zufolge handelt es sich um „das gesamte Spektrum der Tätigkeiten, Ressourcen und Beziehungen im Zusammenhang mit dem Geschäftsmodell des Unternehmens und dem externen Umfeld, in dem es tätig ist“. Nach IG 2.79 empfiehlt es sich, sich auf die Bereiche der Wertschöpfungskette und die Geschäftsbeziehungen zu fokussieren, die am ehesten von wesentlichen Auswirkungen betroffen sind. Mit Blick auf den Unterschied zwischen der Wertschöpfungskette und der Lieferkette gilt generell Folgendes: Die Lieferkette besteht aus den Akteuren der Wertschöpfungskette, die dem berichtenden Unternehmen vorgelagert sind. Sie liefert Produkte, einschließlich Roh-

101

¹⁰⁰ IG 2, siehe → Rn. 73 und 100.

material, Komponenten oder Dienstleistungen, die bei der Entwicklung der Produkte oder Dienstleistungen des Unternehmens verwendet werden. Die Wertschöpfungskette umfasst auch nachgelagerte Einheiten sowie die Lieferkette als solche. Es gibt zudem auch andere Einrichtungen und Personen, die mit den Tätigkeiten, Produkten oder Dienstleistungen des Unternehmens lediglich in Verbindung stehen und gleichwohl zu berücksichtigen sind, ohne „Lieferanten“ zu sein. In diesem Fall besteht keine Geschäftsbeziehung, aber es gibt eine Auswirkung auf die Wertschöpfungskette, die die Wesentlichkeitsschwelle erreichen kann, wenn sie als schwerwiegend genug angesehen wird.

- 102** Grundsätzlich ist es ungeachtet der vorstehenden Ausführungen naheliegend, beim Reporting zunächst die auch in die Konzernberichterstattung einbezogenen Unternehmen zu berücksichtigen.¹⁰¹ Gesellschaften ohne Geschäftstätigkeit oder mit geringem Geschäftsumfang sind indes nicht per se auszuschließen. Denn der Kreis der in die konsolidierte Nachhaltigkeitsberichterstattung einzubeziehenden Unternehmen wird in der CSRD nicht weitergehend konkretisiert. Trotz einer scheinbar grundsätzlichen Orientierung an der Finanzberichterstattung, ergeben sich so gegenüber dem Finanzreporting Unterschiede bei der Einbeziehung von Informationen durch weiter gezogene Berichtsgrenzen.¹⁰² Die Tochterunternehmen können entweder zur eigenen Geschäftstätigkeit oder auch zur ebenfalls zu berücksichtigenden Wertschöpfungskette gehören.¹⁰³
- 103** Der Begriff des sogenannten eigenen Geschäftsbereichs eines Unternehmens wird bislang eher nur im Kontext des § 2 Abs. 6 LkSG diskutiert und ist definiert als „jede Tätigkeit des Unternehmens zur Erreichung des Unternehmensziels“. Jede Tätigkeit zur Herstellung und Verwertung von Produkten und zur Erbringung von Dienstleistungen, unabhängig davon, ob sie an einem Standort im In- oder Ausland vorgenommen wird, ist hiernach erfasst. Im Hinblick auf Konzernstrukturen ist grundsätzlich festzuhalten, dass in verbundenen Unternehmen eine konzernangehörige Gesellschaft dann zum eigenen Geschäftsbereich der Obergesellschaft gehört, wenn die Obergesellschaft einen bestimmenden Einfluss auf die konzernangehörige Gesellschaft ausübt. Relevant sind insoweit Kriterien wie eine hohe Mehrheitsbeteiligung an der Tochtergesellschaft, das Bestehen eines konzernweiten Compliance-Systems, die Übernahme von Verantwortung für die Steuerung von Kernprozessen im Tochterunternehmen, personelle Überschneidungen in der Führungsebene, ein bestimmender Einfluss auf das Lieferkettenmanagement der Tochtergesellschaft oder die Einflussnahme über die Haupt- bzw. Gesellschafterversammlung.
- 104** Über die Grenzen der Finanzberichterstattung hinaus sind damit auch Angaben zu Unternehmen in die nichtfinanzielle Berichterstattung zu integrieren, die Be-

101 Vgl. ESRS 1.62: „The sustainability statement shall be for the same reporting undertaking as the financial statements.“

102 *Lanfermann/Baumüller*, IRZ 2023, 89, 91; siehe auch ESRS 1.63, 1.67.

103 Vgl. auch IG 2.49 ff. zur Abgrenzung zwischen eigenem Geschäftsbereich und zur Wertschöpfungskette.

standteil der vorgelagerten (Lieferanten) oder nachgelagerten (Kunden) Wertschöpfungskette sind. In der Folge wird es bei der Umsetzung der anzuwendenden Berichtsgrenzen faktisch zu fließenden Übergängen zwischen einer konsolidierten und einer nichtkonsolidierten Berichterstattung kommen. Von großer Bedeutung wird jedoch die Wesentlichkeitsanalyse sein, die insoweit Spielräume eröffnet, als dem berichtenden Unternehmen insbesondere in der Anfangsphase des Reportings – in der Wertschöpfungskette und selbstverständlich eher nicht bezogen auf den eigenen Geschäftsbereich – nicht alle erforderlichen Angaben in der notwendigen Qualität vorliegen (können). Die CSRD gewährt vor diesem Hintergrund einen dreijährigen Übergangszeitraum, in dem Unternehmen auf die Berichterstattung von Informationen entlang der Wertschöpfungskette verzichten können, wenn diese nicht eingeholt werden konnten. Stattdessen soll nach ESRS 1.132 in dieser ersten Phase eher auf öffentlich verfügbare Daten und Schätzungen zurückgegriffen werden.

c) Verortung im Lagebericht und Prüfung

Die Nachhaltigkeitsberichterstattung einschließlich der Berichterstattung zur EU-Taxonomie ist künftig zwingender Bestandteil des Lageberichts bzw. Konzernlageberichts – und damit der Rechnungslegung – und hat nach Art. 19a Abs. 1, 29a Abs. 1 BilanzRL n.F. dort „mittels eines dafür vorgesehenen Abschnitts klar erkennbar“ zu sein. Es bedarf daher explizit eines gesonderten Abschnitts des Lageberichts. Einen „gesonderten nichtfinanziellen Bericht“ außerhalb des Lageberichts wird es nicht mehr geben. **105**

Der Lagebericht bzw. Konzernlagebericht von berichtspflichtigen Unternehmen ist nach Art. 29d BilanzRL n.F. in einem einheitlichen elektronischen und maschinenlesbaren Berichtsformat (European Single Electronic Format, ESEF) zu erstellen. Art. 3 ESEF-Verordnung (ESEF-VO)¹⁰⁴ legt fest, dass die Berichterstellung im sog. Extensible Hypertext Markup Language-Format (XHTML) zu erfolgen hat. Um die Nachhaltigkeitsangaben elektronisch auszeichnen zu können, sind sog. Taxonomien notwendig, die sich gegenwärtig in der Entwicklung befinden und zunächst die Themen „ESRS Set 1“ und „Angaben nach Art. 8 Umwelttaxonomie“ adressieren.¹⁰⁵ Die European Securities and Markets Authority (ESMA) erarbeitet sodann daraus einen Entwurf eines delegierten Rechtsaktes zur Änderung der ESEF-VO. **106**

Art. 34 BilanzRL n.F. sieht künftig eine externe inhaltliche Pflichtprüfung dahingehend vor, ob der Lagebericht nach den geltenden rechtlichen Anforderungen aufgestellt wurde. Die Prüfung erfolgt, um das Vertrauen und die Glaubwürdigkeit der Berichte zu steigern, und ist zunächst als Prüfung zur Erlangung begrenzter Prüfungssicherheit („limited assurance“) durch einen Abschlussprüfer oder einen unabhängigen Erbringer von Bestätigungsdienstleistungen, der **107**

¹⁰⁴ Delegierte Verordnung (EU) 2019/815.

¹⁰⁵ <https://www.efrag.org/Lab4> (zuletzt abgerufen am 3.6.2024).

einer gleichwertigen Regulatorik wie ein Wirtschaftsprüfer unterliegt, vorgehen. Insoweit besteht ein Mitgliedstaatenwahlrecht; dies auch mit Blick auf den Aspekt, dass ein anderer Abschlussprüfer oder eine andere Prüfungsgesellschaft als der- oder diejenige, der oder die die Abschlussprüfung durchführt, das Urteil abgibt.¹⁰⁶

d) Erleichterungen im Rahmen der Implementierung des Reportings

- 108** Bereits im Rahmen der Einführung der CSRD und der ESRS wurden verschiedentlich die Umsetzungsgeschwindigkeit und die dem Vorhaben innewohnende Komplexität der Regulierungsanforderungen kritisiert. Dieser Kritik, die zuletzt auch um den Aspekt des Bürokratieabbaus erweitert wurde, wurde in verschiedenen Umsetzungsstadien immer wieder Rechnung getragen, ursprünglich auch bereits mit der stufenweisen Einführung der Berichtspflichten als solcher. So wurde im Laufe des Verfahrens etwa die Anzahl der Offenlegungspflichten deutlich reduziert.¹⁰⁷ Ein Governance-Standard entfiel gar, wobei jedoch einige von dessen Inhalten Eingang in andere ESRS erhielten. Die Verabschiedung der sektorspezifischen ESRS wurde verschoben und soll nunmehr voraussichtlich erst bis Mitte 2026 erfolgen. Neben übergangsweisen Erleichterungen mit Blick auf die Einbindung der Wertschöpfungskette in den ersten drei Jahren der Berichtspflicht¹⁰⁸ gilt als ein besonders wichtiger Schritt zur Erleichterung des Umgangs mit den Vorgaben die nunmehr vorgesehene umfassende Anwendung des Wesentlichkeitsgrundsatzes auf alle Standards, abgesehen vom ESRS 2, und die damit vorgesehene Abstandnahme von der zwischenzeitlich angedachten widerlegbaren Vermutung dahingehend, dass einzelne themenbezogene Aspekte stets relevant seien.
- 109** Um kleineren Unternehmen angesichts der Tiefe der inhaltlichen Berichtsanforderungen entgegenzukommen, existieren anfänglich und zumindest in Teilbereichen der Vorgaben übergangsweise spezifische Erleichterungen, wobei die Gesellschaften im Weiteren berichtsverpflichtet bleiben. Berichtspflichtige Unternehmen mit weniger als 750 Mitarbeitern haben insofern beispielsweise nach näherer Maßgabe der Anlage C. zu ESRS 1 im ersten Berichtsjahr nur eingeschränkte Berichtspflichten, als die Angaben des ESRS E1 bezüglich der Scope 3- und der Gesamt-Treibhausgasemissionen sowie die Angaben des ESRS S1 grundsätzlich entfallen können. In den ersten zwei Berichtsjahren der erstmaligen ESRS-Anwendung sind für diese Unternehmen zudem die Angaben der

106 Nach dem Referentenentwurf zum CSRD-Umsetzungsgesetz sind in Deutschland nur Wirtschaftsprüfer (entweder der Prüfer des Jahresabschlusses oder ein gesondert bestellter Prüfer) zur Prüfung der Nachhaltigkeitsberichte zugelassen. Siehe → Rn. 118 (Hinweis: Redaktionsschluss für dieses Werk war im Juli 2024, weswegen neuere Entwicklungen nicht mehr berücksichtigt werden konnten).

107 Vgl. hierzu bereits → Rn. 84 ff., wobei deren zumindest partielle Abbildung zukünftig in den sektorspezifischen ESRS denkbar bleibt.

108 Siehe → Rn. 95 ff. und ESRS 1.132.

ESRS E4, ESRS S2, ESRS S3 und ESRS S4 vorbehaltlich bestimmter Minimumangaben entbehrlich.¹⁰⁹

Im gegebenen Kontext relevant, wenngleich begründet mit der zuletzt zeitweise hohen Inflationsrate, ist auch die verschiedentlich bereits angesprochene Anhebung der Kriterien für das Vorliegen großer Unternehmen auf nunmehr 25 Mio. EUR Bilanzsumme und 50 Mio. EUR Umsatzerlöse. **110**

IV. Der Referentenentwurf zum CSRD-Umsetzungsgesetz und ein weitergehender Ausblick

Am 22.3.2024 veröffentlichte das Bundesministerium der Justiz den Referentenentwurf des Gesetzes zur Umsetzung der CSRD (nachfolgend kurz: Referentenentwurf) nebst einer Synopse zum Abgleich der aktuellen und der vorgeschlagenen zukünftigen Normen.¹¹⁰ Der Gesetzesvorschlag wurde den Bundesländern, den kommunalen Spitzenverbänden, Fachkreisen und Verbänden mit der Bitte um deren Stellungnahmen bis zum 19.4.2024 zugeleitet, um sodann nach einer Überarbeitung und Umsetzung als Regierungsentwurf zur Prüfung an den Bundesrat übermittelt und in den Bundestag eingebracht zu werden. Inhaltliche Änderungen sind demnach im Zeitpunkt der Verfassung dieses Beitrags noch verschiedentlich möglich. **111**

Der Referentenentwurf sieht grundsätzlich eine 1:1-Umsetzung der CSRD vor und ändert insbesondere die relevanten handels- und gesellschaftsrechtlichen Normen. Folgende Regelungen des Gesetzesvorschlags sind in ihrer Bedeutung hervorzuheben. **112**

Nach §§ 289b Abs. 1, 315b Abs. 1 HGB-E soll die Pflicht zur Abgabe einer nichtfinanziellen (Konzern-)Erklärung durch die Pflicht zur Erweiterung des (Konzern-)Lageberichts um einen Nachhaltigkeitsbericht ersetzt werden. Dieser Bericht wird zum Bestandteil des (Konzern-)Lageberichts und hat in dessen Rahmen einen separaten, klar erkennbaren Abschnitt zu bilden. **113**

In den Nachhaltigkeitsbericht müssen – entsprechend dem Grundsatz der doppelten Wesentlichkeit und ggf. auf Konzernebene um weitere Angaben ergänzt – **114**

¹⁰⁹ Vgl. detaillierte Anlage C zu ESRS 1 „Liste der schrittweisen Angabepflichten“ (S. 34–37 Anlage ESRS Set 1).

¹¹⁰ Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2464 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 zur Änderung der Verordnung (EU) Nr. 537/2014 und der Richtlinien 2004/109/EG, 2006/43/EG und 2013/34/EU hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen. Auch angesichts der EU-seitig bestehenden Frist für die nationale Umsetzung bis zum 6.7.2024 hat das Bundeskabinett am 3.7.2024 den TOP CSRD-Umsetzung von der Tagesordnung seiner Sitzung genommen. Ein Regierungsentwurf wird damit voraussichtlich erst im Spätsommer 2024 (nach der sog. „Sommerpause“) vorliegen und im Herbst von Bundestag und Bundesrat behandelt werden. Folge für diese Fachveröffentlichung ist, dass das HGB in seiner vormaligen Fassung fortbesteht (Hinweis: Redaktionsschluss für dieses Werk war im Juli 2024, weswegen neuere Entwicklungen nicht mehr berücksichtigt werden konnten).

nach §§ 289c Abs. 1 und 2, 315c Abs. 1 HGB-E diejenigen Angaben aufgenommen werden, die für das Verständnis der Auswirkungen der Tätigkeiten der berichtspflichtigen Unternehmen bzw. Konzerne auf Nachhaltigkeitsaspekte sowie auf das Verständnis von deren Auswirkungen auf den Geschäftsverlauf, das Geschäftsergebnis und die Lage der betreffenden Gesellschaft erforderlich sind.

115 Die Angaben haben nach den §§ 289c Abs. 6, 315c Abs. 1 Nr. 2 HGB-E im Einklang mit den ESRS zu stehen. Wie schon zuvor können nachteilige Angaben nach Maßgabe der §§ 289e, 315c Abs. 1 HGB-E weggelassen werden (siehe → Rn. 56).

116 Konkret sind im Nachhaltigkeitsbericht folgende Angaben zu machen:

- Kurze Beschreibung von Geschäftsmodell und Strategie, inkl. folgender Angaben:
 - Widerstandsfähigkeit von Geschäftsmodell und Strategie gegenüber Risiken im Zusammenhang mit Nachhaltigkeitsaspekten,
 - Chancen im Zusammenhang mit Nachhaltigkeitsaspekten,
 - Art und Weise, wie sichergestellt werden soll, dass Geschäftsmodell und Strategie mit dem Übergang zu einer nachhaltigen Wirtschaft, der Begrenzung der Erderwärmung auf 1,5 °C und dem Ziel der Klimaneutralität bis 2050 vereinbar sind,
 - Art und Weise, wie den Belangen von Interessenträgern und den Auswirkungen der Unternehmenstätigkeit auf Nachhaltigkeitsaspekte in Geschäftsmodell und Strategie Rechnung getragen wird, und
 - Art und Weise, wie die Strategie im Hinblick auf Nachhaltigkeitsaspekte umgesetzt wird;
- Beschreibung der zeitgebundenen Nachhaltigkeitsziele;
- Beschreibung der Rolle der Geschäftsführungs-, Aufsichts- oder Verwaltungsorgane im Zusammenhang mit Nachhaltigkeitsaspekten;
- Beschreibung der Unternehmenspolitik hinsichtlich Nachhaltigkeit;
- Angaben über das Vorhandensein von Anreizsystemen mit Bezug zu Nachhaltigkeitsaspekten;
- Beschreibung
 - der durchgeführten nachhaltigkeitsbezogenen Sorgfaltspflichten,
 - der wichtigsten tatsächlichen oder potenziellen negativen Auswirkungen, die mit der eigenen Geschäftstätigkeit und der Wertschöpfungskette verknüpft sind, sowie der Maßnahmen zur Ermittlung und Überwachung, und
 - Maßnahmen zur Verhinderung, Minderung oder Behebung tatsächlicher oder potenzieller negativer Auswirkungen und des Erfolgs dieser Maßnahmen;
- Beschreibung der wichtigsten Risiken, denen das Unternehmen im Zusammenhang mit Nachhaltigkeitsaspekten ausgesetzt ist, inkl. der wichtigsten Abhängigkeiten in diesem Bereich, sowie der Handhabung dieser Risiken durch das Unternehmen; und
- Indikatoren, die für diese Angaben relevant sind.

Der (Konzern-)Lagebericht ist zudem gemäß §§ 289 Abs. 3a, 315a Abs. 3a HGB-E um Angaben zu den wichtigsten immateriellen Ressourcen im Kontext der Nachhaltigkeit zu erweitern (siehe → Rn. 87 ff.). Es ist über solche Ressourcen zu berichten, von denen das Geschäftsmodell grundlegend abhängt und die eine Wertschöpfungsquelle für das Unternehmen bzw. den Konzern darstellen. **117**

Gemäß den §§ 324b, 324c HGB-E ist der Nachhaltigkeitsbericht als Bestandteil des (Konzern-)Lageberichts zukünftig durch einen Wirtschaftsprüfer oder eine Wirtschaftsprüfungsgesellschaft inhaltlich zu prüfen. Auch der Abschlussprüfer kann nach § 324e HGB-E als Prüfer des Nachhaltigkeitsberichts bestellt werden. Sogenannte unabhängige Erbringer von Bestätigungsleistungen sind indes nicht zur Prüfung der Berichte zugelassen; insoweit würde Deutschland damit von einem Mitgliedstaatenwahlrecht Gebrauch machen. Die Prüfung als solche erfolgt bis auf Weiteres auf Basis einer prüferischen Durchsicht zur Erlangung begrenzter Prüfungssicherheit („limited assurance“). Im Grunde geht es insoweit um eine Prüfung der Plausibilität der im Nachhaltigkeitsbericht aufgeführten Informationen, was eine entsprechende Dokumentation seitens des Unternehmens erfordert. Beginnend mit einem Verständnis von den Prozessen hinsichtlich der Datenerhebung, gegebenenfalls der Datenkonsolidierung sowie dem nachhaltigkeitsbezogenen internen Kontrollsystem liegt die Prüfungstiefe für weitere Prüfungshandlungen im Ermessen des Abschlussprüfers. Die Richtigkeit und Vollständigkeit der Daten kann sowohl durch Befragungen als auch etwa durch Vorjahresvergleiche und/oder einzelne Stichproben geprüft werden. Eine mittelfristig zu erwartende Prüfung mit hinreichender Sicherheit („reasonable assurance“) entspricht demgegenüber vollumfänglich der Prüfung des Jahres-/Konzernabschlusses und umfasst insbesondere eine Wirksamkeitsprüfung der vorstehend dargestellten Prozesse, des IKS und gegebenenfalls der IT. Ferner sind die einzelnen Prüfungshandlungen im Umfang ausgeweitet. Über das Ergebnis der Prüfung ist nach näherer Maßgabe des § 324i Abs. 1 HGB-E in einem gesonderten Prüfvermerk zu berichten. In ihm hat der Prüfer des Nachhaltigkeitsberichts zu erklären, dass die von ihm durchgeführte Prüfung zu keinen Einwendungen geführt hat und dass der von den gesetzlichen Vertretern der Gesellschaft aufgestellte (Konzern-) Nachhaltigkeitsbericht nach den Erkenntnissen des Prüfers den gesetzlichen Vorschriften entspricht. Gegebenenfalls ist der Prüfungsvermerk einzuschränken oder zu versagen. **118**

Der (Konzern-)Lagebericht ist nach § 325 Abs. 1 und Abs. 3 HGB-E zusammen mit dem Prüfungsvermerk in deutscher Sprache beim Unternehmensregister offenzulegen. Der Bericht ist zu diesem Zweck im nach der ESEF-VO geforderten einheitlichen elektronischen Berichtsformat elektronisch zu übermitteln.¹¹¹ **119**

Durch Änderungen am Lieferkettensorgfaltspflichtengesetz (LkSG) sollen doppelte bzw. gleichgelagerte Berichtspflichten vermieden werden. Die Berichtspflicht für vom LkSG adressierte Unternehmen nach § 10 Abs. 2 LkSG soll nach **120**

111 Siehe → Rn. 105 ff.; § 11 Abs. 2 Unternehmensregisterverordnung-E.

§ 10 Abs. 5 und 6 LkSG-E entfallen, wenn ein solches Unternehmen einen Nachhaltigkeitsbericht nach den Vorgaben der CSRD/ESRS erstellt und dieser geprüft wird. Dies gilt selbst dann, wenn das Reporting, etwa im Vorgriff auf eine zu erwartende Berichtspflicht, freiwillig erstellt wird. Der Nachhaltigkeitsbericht ist dann gemäß § 12 Abs. 3 LKSG-E anstelle des LkSG-Berichts auf der Internetseite des Unternehmens zu veröffentlichen und beim BAFA einzureichen. Alle weiteren Pflichten nach dem LkSG bleiben bestehen. Um Unternehmen ausreichend Gelegenheit zu bieten, prüfen zu können, ob sie von der Ersetzungsmöglichkeit Gebrauch machen möchten, gelten Übergangsfristen gemäß § 12 Abs. 4 HGB-E.

- 121** Ein ähnliches Thema im Sinne einer Befreiung ergibt sich mit Blick auf Diversitätskonzepte: Während die diesbezügliche Berichterstattung derzeit zwingend in der Erklärung zur Unternehmensführung zu erfolgen hat, sollen nach § 289f Abs. 5 HGB-E die Informationen zukünftig alternativ auch im Nachhaltigkeitsbericht abgebildet werden können. In die Erklärung zur Unternehmensführung ist dann ein entsprechender Verweis aufzunehmen.
- 122** Mit Blick auf bestehende Arbeitnehmervertretungen besteht nach §§ 289b Abs. 6, 315b Abs. 5 HGB-E eine Unterrichts- und Erörterungspflicht bezogen auf das Nachhaltigkeitsreporting. Etwaige Stellungnahmen sind in der Folge an das Organ zu übermitteln, das für die Prüfung des (Konzern-)Lageberichts einschließlich des Nachhaltigkeitsberichts verantwortlich ist, in der Regel der Aufsichtsrat. Aktienrechtliche Anpassungen greifen diesen Aspekt auf und legen fest, dass das für die Prüfung zuständige Organ zukünftig auch die Nachhaltigkeitsberichterstattung kontrollieren und prüfen muss. Der Nachhaltigkeitsbericht ist explizit nach §§ 170 Abs. 3, 171 Abs. 1 AktG-E als Bestandteil des (Konzern-)Lageberichts Gegenstand der Prüfung durch den Aufsichtsrat. Auch ein Prüfungsausschuss hat sich im Rahmen der Überwachung des Rechnungslegungsprozesses gemäß § 107 Abs. 3 AktG-E zukünftig mit der Überwachung des Prozesses der Nachhaltigkeitsberichterstattung zu befassen.¹¹²
- 123** Der vormalige „Bilanzeid“ hinsichtlich des Jahresabschlusses (§ 264 Abs. 2 Satz 3 HGB) und der „Lageberichteid“ bezogen auf den Lagebericht bzw. auf Konzernebene der entsprechende „Konzernbilanzeid“ und „Konzernlageberichteid“ (§§ 289 Abs. 1 Satz 5 HGB, 297 Abs. 2 Satz 4, 315 Abs. 1 Satz 5 HGB) werden zukünftig in einer einheitlichen Erklärung zusammengefasst und beziehen die Aufstellung des Nachhaltigkeitsberichts mit ein. § 334 HGB-E wird mit Blick auf Sanktionen für Verstöße gegen die Anforderungen im Kontext der Nachhaltigkeitsberichterstattung angepasst.
- 124** Governance-bezogen wird sich damit zukünftig einiges in den Unternehmen ändern: Die neuen Vorgaben zur Berichterstattung führen zu einer schon seit Längerem angelegten, weiteren Verrechtlichung der Nachhaltigkeitsthemen. Sie

¹¹² Zu erwägen ist auch die Einrichtung eines gesonderten Nachhaltigkeitsausschusses des Aufsichtsrats.

geht einher mit einer diesbezüglich deutlichen Sensibilisierung in den Unternehmen und in der Zivilgesellschaft und bildet die Grundlage für die diesbezügliche Transformation der Wirtschaft. Deren oftmals spürbare Zurückhaltung gegenüber den neuen Berichtspflichten beruht ganz wesentlich und nachvollziehbar auf den mit einem solchen Reporting verbundenen Aufwänden. Fraglos ist es eher wünschenswert, dass die Unternehmen, wie es bislang schon verbreitet so gehandhabt wird, ihrer gesellschaftlichen Verantwortung aus einem inneren Antrieb und etwa zur Sicherstellung ihrer Wettbewerbsfähigkeit nachkommen – und nicht aus regulatorischen Zwängen heraus.

Dessen ungeachtet indes werden den mit der Regulierung verfolgten Zielen perspektivisch in den kommenden Jahren weitere gesetzgeberische Aktivitäten auf dem Gebiet der ESG folgen, dem globalen „Megatrend der Nachhaltigkeit“ wird regulatorisch weitergehend Rechnung getragen werden. Zu gegebener Zeit könnte dann indes die übergeordnete Frage aufgeworfen werden, ob die vorgesehene normative Verortung der Vorgaben im Bilanzrecht dem der Thematik innewohnenden Anspruch und den zunehmenden gesellschaftlichen Erwartungen in jeder Hinsicht gerecht wird oder ob sich andere Weichenstellungen wie gesonderte Regelungsbereiche empfehlen. **125**

Rein praktisch wird darüber hinaus in vielen Unternehmen unklar sein, wer sich zukünftig für die Organe auf operativer Ebene verantwortlich, mit einer vor reputativen und rechtlichen Hintergründen (Verantwortlichkeiten, Sanktionen, mediale Relevanz, etc.) wichtigen kritischen Sicht und mit einem breit angelegten Know-how als Querschnittseinheit um die Einhaltung der neuen Anforderungen kümmern sollte. Relevant sind – da nur wenige Unternehmen bislang über spezifische ESG-Einheiten verfügen oder diese gerade erst aufbauen – nach ersten Erfahrungen Einheiten wie Legal, Compliance, HR, Controlling und Rechnungswesen oder vorstandsnahe Stäbe. Schon diese Fragestellung offenbart, wie auch diverse unmittelbare inhaltliche Anknüpfungspunkte im Rahmen der bisherigen Arbeit, einige gute Gründe dafür, insbesondere bei Nichteinrichtung einer spezifischen ESG-Einheit die Compliance-Funktion mit der Sicherstellung und Überwachung der Einhaltung der ESG-Compliance als wesentliches Element einer guten Corporate Governance zu betrauen. **126**

17. Kapitel

Compliance im Kontext nachhaltigen Supply Chain Managements – Die betriebswirtschaftliche Perspektive

Unternehmen und Supply Chain Manager haben nicht nur die Aufgabe, Compliance mit diversen Nachhaltigkeitsstandards intern herzustellen und unterschiedlichen Anforderungen der Stakeholder gerecht zu werden, sondern auch ihre Lieferantennetzwerke diesbezüglich zu managen und gleichzeitig auf neue Lieferanten auszuweiten. Dieses Kapitel gibt einen Überblick über praktische Ansätze und zukünftige Herausforderungen aus der Sicht einkaufender Unternehmen und ihrer Lieferanten. 1

I. Einleitung

Aufgrund der Outsourcing- und Offshoring-Welle in den vergangenen Jahrzehnten werden je nach Industrie bis zu 80 % der Wertschöpfung von vorgelagerten Lieferanten betrieben.¹ Viele Unternehmen in Industrienationen haben die Erstellung von Produkten, Komponenten und ganzer Funktionen an Lieferanten in Entwicklungs- und Schwellenländer ausgelagert, um von den dort niedrigeren Lohnkosten zu profitieren.² Während die globale COVID-19-Pandemie sowie geopolitische Umbrüche³ diesen Trend verlangsamt haben und Stimmen lauter werden, die die Welt am Beginn einer neuen De-Globalisierungsphase sehen,⁴ bestehen moderne globale Lieferantennetzwerke durch die drastische Senkung der Wertschöpfungstiefe noch immer aus vielen einzelnen Unternehmensgliedern wie beispielsweise Rohmateriallieferanten, Produzenten, Distributoren, aber auch, Logistikdienstleistern, Handelsunternehmen und Endkunden. Aufgrund dieser spezialisierten und disaggregierten Wertschöpfungsstrukturen sind insbesondere Produzenten von hochwertigen Markengütern stark von der Kosten-, Qualitäts- und Lieferperformance ihrer direkten und indirekten Lieferanten abhängig.⁵ Gleichzeitig nehmen Nichtregierungsorganisationen wie Greenpeace oder Amnesty International, Stakeholdergruppen sowie aufgeklärte und nachhaltigkeitsbewusste Endkunden diese fokalen Unternehmen (d. i. das zentrale Unternehmen in einem Wertschöpfungsnetzwerk) in die Pflicht, für adäquate 2

1 Vgl. Carter/Rogers, *International Journal of Physical Distribution & Logistics Management* 2008, 360 ff.

2 Ehrhardt/Reimann/Kaufmann/Carter, *Journal of Business Ethics* 2011, 99 ff.

3 Bednarski/Roscoe/Blome/Schleper, *Production Planning & Control*, <https://doi.org/10.1080/09537287.2023.2286283>.

4 Di Sano/Gunnella/Lebastard, *European Central Bank* 2023.

5 Awayseh/Klassen, *International Journal of Operations & Production Management* 2012, 1246 ff.

Arbeitsschutzbedingungen und strikte Sozial- und Umweltstandards entlang der gesamten Lieferkette einzustehen.⁶

- 3 Die teils dramatischen Folgen, die hieraus für fokale⁷ Unternehmen resultieren, lassen sich an namhaften Beispielen festmachen: Im Jahr 2007 musste der Spielzeughersteller Mattel Inc. knapp eine Million Spielzeugartikel zurückrufen, da deren Farbanstrich für Kinder giftige Bleipartikel enthielt.⁸ Obwohl Mattel Inc. ein ambitioniertes Lieferantenmanagementprogramm betrieb, blieben die von einem Sublieferanten beigemischten verunreinigten Partikel zunächst unentdeckt. Die aus dem Vorfall resultierenden Rückrufrufen in Höhe von 30 Mio. USD und enorme Imageschäden sorgten dafür, dass die Aktie anschließend massiv an Wert verlor.
- 4 Um Imageschäden und finanzielle Einbußen zu vermeiden,⁹ haben fokale, im Blickpunkt der Öffentlichkeit stehende Unternehmen seit einiger Zeit damit begonnen, neben den traditionellen ökonomischen Faktoren zunehmend auch „grüne“ und soziale Aspekte hin zu einem ganzheitlich nachhaltigem Supply Chain Management¹⁰ zu integrieren. Dennoch ist es immer wieder zu tragischen Beispielen gekommen: Negativer Höhepunkt war 2013 der Zusammensturz der Rana Plaza Textilfabrik in Bangladesch, die überwiegend westliche fokale Unternehmen beliefert hat. Mehr als 1.100 Menschen starben bei dem Unglück und über 2.400 Personen wurden zum Teil schwer verletzt.¹¹ Einer der Hauptgründe für solche Vorfälle ist, dass die seitens der einkaufenden Unternehmen unternommenen Maßnahmen augenscheinlich nicht ausreichen, um Compliance mit Nachhaltigkeitsstandards und -anforderungen in ihren Lieferantennetzwerken sicherzustellen. Ein Grund warum gegen mit dem Unglück in Zusammenhang stehende Unternehmen von pakistanischen Textilarbeitern und Menschenrechtsgruppen vor deutschen Gerichten Klagen eingereicht wurden.¹² Zusätzlich sind Entscheidungsträger im Einkauf im Hinblick auf die tatsächliche Nachhaltigkeitsperformance ihrer Lieferanten vielfach immer noch großen Informationsdefiziten ausgesetzt.¹³ Supply Chain Manager sollten sich demnach kritisch die

6 Vgl. *Busse/Schleper/Weilenmann/Wagner*, International Journal of Physical Distribution & Logistics Management 2017, 18 ff.

7 Als „fokales Unternehmen“ wird ein zentrales oder führendes Unternehmen innerhalb eines Netzwerks von Unternehmen oder Lieferketten genannt, das maßgeblich die Strategien, Aktivitäten und Beziehungen der anderen beteiligten Unternehmen koordiniert und beeinflusst.

8 *Story*, New York Times 2007.

9 Vgl. *Hofmann/Busse/Bode/Henke*, Business Strategy and the Environment 2014, 160 ff.

10 Nachhaltiges Supply Chain Management wird in der Literatur zitiert als: „[...] management of material, information and capital flows as well as cooperation among companies along the supply chain while taking goals from all three dimensions of sustainable development, i.e., economic, environmental and social, into account which are derived from customer and stakeholder requirements“, *Seuring/Müller*, Journal of Cleaner Production 2008, 1700.

11 *Bajaj*, New York Times 2012.

12 *Dernbach*, Tagesspiegel 2019. Die Klage gegen das Textilunternehmen KiK wurde jedoch wegen Verjährung abgewiesen.

13 *Busse/Meinlschmidt/Förstl*, Journal of Supply Chain Management 2017, 87 ff.

Frage stellen, ob wirklich alle Lieferanten ihres Netzwerkes gemäß international anerkannter Umwelt- und Sozialstandards produzieren und wie Compliance effektiv gewährleistet werden kann.

Vor diesem skizzierten Hintergrund hat sich in der Betriebswirtschaftslehre ein vierstufiger Prozess herausgebildet, den fokale Unternehmen anwenden, um ihre Lieferantenbasis nachhaltiger zu gestalten: (1) Lieferantenbewertung, (2) Lieferantenentwicklung, (3) Lieferantenauswahl und (4) Lieferantenmonitoring. Das Verständnis dieses Prozesses ist auch im Zusammenhang mit den neuen regulatorischen Vorgaben für die Lieferketten-Compliance, insbesondere durch das Lieferkettensorgfaltspflichtengesetz (LkSG),¹⁴ hilfreich.

II. Nachhaltiges Lieferantenmanagement

Im Folgenden werden die einzelnen Elemente des nachhaltigen Lieferantenmanagements aus Sicht der Betriebswirtschaftslehre exemplarisch von links nach rechts erläutert (vgl. Abb. 1).

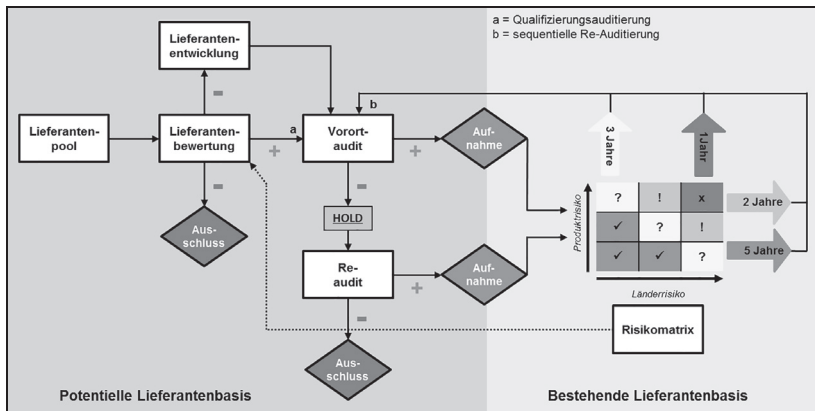


Abbildung 1: Prozessmodell des nachhaltigen Lieferantenmanagements

1. Lieferantenbewertung

Während die Auswahl geeigneter Lieferanten in der Vergangenheit zumeist auf den klassischen ökonomischen Kriterien Qualität und Preis der gekauften Ware sowie Liefertreue, -bedingungen und -risiken abzielten, spielt der Faktor Nachhaltigkeit mittlerweile für viele Unternehmen und deren Stakeholder eine wichtige Rolle in der Gesamtbetrachtung.¹⁵ Zusätzlich werden auf dieser Stufe die

¹⁴ Zum LkSG ausführlich → Heske, Kap. 18 sowie Schröder/Schulz, Praxisleitfaden Supply Chain Compliance, 2023.

¹⁵ Foerstl/Reuter/Hartmann/Blome, Journal of Purchasing and Supply Management 2010, 118 ff.

Compliance mit nationalen und internationalen Gesetzen, Regulierungen und Sorgfaltspflichten miteinbezogen.¹⁶

- 8 Aus einem Gesamtpool potenzieller Lieferanten einer Warengruppe werden die geeignetsten unterschiedlichen standardisierten Bewertungsverfahren unterzogen. Beispielsweise werden neben Selbstauskünften der Lieferanten verschiedene externe Informationsquellen genutzt (Auditierungsdienstleister, Nichtregierungsorganisationen und andere Stakeholdergruppen, öffentliche Informationen wie z. B. Code of Conducts, Nachhaltigkeitsberichte, etc. oder ggf. sogar Daten von Mitbewerbern), um ein umfassendes Bild der Nachhaltigkeitsperformance möglicher Lieferanten einzuholen. In diese Beurteilung fließen neben allgemeinen standardisierten Kriterien entlang der ökonomischen, ökologischen und sozialen Dimension, sektor- und produktspezifische Lieferantenbewertungskriterien¹⁷ sowie in bestimmten Fällen auch eine Sub-Lieferantenbewertung über mehrere Tierstufen ein. Oftmals wird dafür mittels eines risikobasierten Ansatzes eine Vorabidentifizierung von kritischen Lieferanten angestrebt. All dies führt dazu, dass Unternehmen weniger und gleichzeitig genauere Daten erheben, um Informationsdefizite in Bezug auf Nachhaltigkeit abzubauen. Fällt die Gesamtbeurteilung negativ aus, ergeben sich für das einkaufende Unternehmen zwei Möglichkeiten: Entweder der potenzielle Lieferant wird aus dem Bieterkreis ausgeschlossen oder aber es zeichnet sich aufgrund verschiedener Überlegungen ab, dass eine Kooperation mit dem in Frage kommenden Lieferanten vorteilhaft sein könnte.

2. Lieferantenentwicklung

- 9 Unter „Lieferantenentwicklung“ im Bereich der Nachhaltigkeit lassen sich alle Maßnahmen einordnen, die auf eine Verbesserung der Nachhaltigkeitsperformance und/oder von Nachhaltigkeitspotenzialen des Lieferanten zielen, um die einkaufsseitige Nachfrage kurz- und/oder langfristig sicherzustellen.¹⁸ Spezifische Aktivitäten bilden u. a. die Erarbeitung gemeinsamer Lösungen mit Lieferanten für nachhaltigkeitsbezogene Probleme, die Schaffung von Anreizen für Lieferanten mit besonders guter Nachhaltigkeitsperformance sowie die Bereitstellung kostenlosen technischen und organisationalen Know-hows oder in Einzelfällen gezielter Vorabinvestitionen zum Aufbau neuer Techniken und Prozesse. Diese Maßnahmen dienen sowohl der kontinuierlichen Entwicklung neuer als auch bestehender Lieferanten hinsichtlich „grüner“ und sozialer Kriterien und stellen so die Compliance mit allgemeinen internationalen Anforderungen und speziellen Bedarfen der Einkaufsseite sicher.

16 Zum LkSG ausführlich → *Heske*, Kap. 18 sowie *Schröder/Schulz*, Praxisleitfaden Supply Chain Compliance, 2023.

17 Bspw. sind der Ausschluss von Kinder- und Zwangsarbeit Hauptbewertungskriterien für Textilunternehmen, während die Reduzierung von Abwässern und des CO₂-Verbrauchs besonders für Chemie- und Pharmaunternehmen wichtig ist.

18 *Jia/Stevenson/Hendry*, Production Planning & Control 2023, 727 ff.

Da eine Entwicklung von Lieferanten jedoch eine erhöhte Investitionsbereitschaft bei gleichzeitig erhöhtem Verlustrisiko darstellt, wird diese zumeist nur in Situationen angewandt, in denen sich Lieferanten als kritisch für den Erfolg des einkaufenden Unternehmens erweisen und/oder keine alternativen Lieferanten zur Verfügung stehen.¹⁹ **10**

3. Lieferantenauswahl

Nachdem der jeweilige Lieferant entweder die Bewertungsphase direkt bestanden hat oder aber vom einkaufenden Unternehmen entwickelt wurde, kommt es in der Phase der Lieferantenauswahl zur Qualifizierungsauditierung, die vor Ort beim Lieferanten durchgeführt wird. Diese kann entweder durch den Kunden selbst oder aber eine dritte unabhängige Auditierungsorganisation geschehen. In einigen Fällen haben sich zudem Unternehmen einer Branche zusammengeschlossen und gemeinsame Auditierungsstandards entwickelt. Somit erkennen sie gegenseitig ihre bereits absolvierten Audits bei gemeinsamen Lieferanten an, um zeit- und kostenintensive²⁰ Mehrfach-Auditierungen zu vermeiden.²¹ **11**

Insofern ein solches Qualifizierungsaudit negativ beurteilt wird, wird der betroffene Lieferant auf „hold“ gestellt; d. h. er bekommt eine Karenzzeit eingeräumt, in der er die Möglichkeit erhält, die Mängel hinsichtlich des ersten Audits bis zu einem Re-Audit abzustellen. Nach einer positiven Beurteilung des Qualifikations- oder Re-Audits wird der neue Lieferant dann in die aktive Lieferantenbasis aufgenommen. **12**

4. Lieferantenmonitoring

Die Lieferantenbasis sollte von jedem Unternehmen hinsichtlich ihrer Nachhaltigkeitsperformance kontinuierlich beobachtet werden, da Reputationsrisiken und Imageschäden jederzeit durch Probleme im Lieferantennetzwerk auftreten können.²² Neben klassischen ökonomischen Kennzahlen wie bspw. Lieferzuverlässigkeit und Produktivitätsindikatoren gibt es eine Vielzahl ökologischer (CO₂-Ausstoß, Abwassermenge, Menge und Art eingesetzter gefährlicher Chemikalien etc.) und sozialer Indikatoren (Arbeitsunfälle, geleistete Überstunden, **13**

19 Busse/Schleper/Niu/Wagner, International Journal of Physical Distribution & Logistics Management 2016, 442 ff.

20 Für eine detaillierte Diskussion der Vorteile standardisierter Nachhaltigkeitsinstrumente siehe Schleper/Busse, Logistics Research 2013, 187 ff.

21 Sowohl in der chemisch-pharmazeutischen Industrie (Pharmaceutical Supply Chain Initiative), der Bekleidungsbranche (Detox Campaign), der elektronischen Industrie (Responsible Business Alliance, zuvor Electronic Industry Corporate Citizenship Initiative) als auch in Teilen der Chemiebranche (Together for Sustainability) gibt es Zusammenschlüsse von Unternehmen, die sich gegenseitig absolvierte Lieferantenaudits anerkennen.

22 Hofmann/Busse/Bode/Henke, Business Strategy and the Environment 2014, 160 ff.

durchschnittliche Bezahlung etc.), die Kunden hinsichtlich ihrer Lieferantenbasis regelmäßig überprüfen sollten.²³

- 14 Darüber hinaus sollten bestehende Lieferanten weiterhin hinsichtlich ihres Gesamtrisikos in Bezug auf Nachhaltigkeitsrisiken beurteilt und klassifiziert werden. Sowohl Länder- als auch Produktgruppenrisiken können sich verändern, so dass das nachhaltige Lieferantenmanagement als dynamischer Prozess verstanden werden muss. Die basal dargestellte Risikomatrix ermöglicht eine erste Einordnung, die je nach Risikoklasse sequenzielle Re-Auditierungen nach unterschiedlichen Zeiträumen vorsieht.²⁴

III. Unterschiede entlang der Lieferkette

- 15 Obwohl Nachhaltigkeit in den letzten Jahrzehnten einen enormen Aufschwung erlebt hat und nachhaltiges Supply Chain Management samt seiner Multiplikatorwirkung (siehe Abb. 2) in vielen Branchen, Industrien und Unternehmen in den Vordergrund gerückt ist, lassen sich im Hinblick auf die Intensität unternehmerischer Nachhaltigkeitsaktivitäten, sowohl intern als auch im Lieferantenmanagement, noch immer große Unterschiede konstatieren.

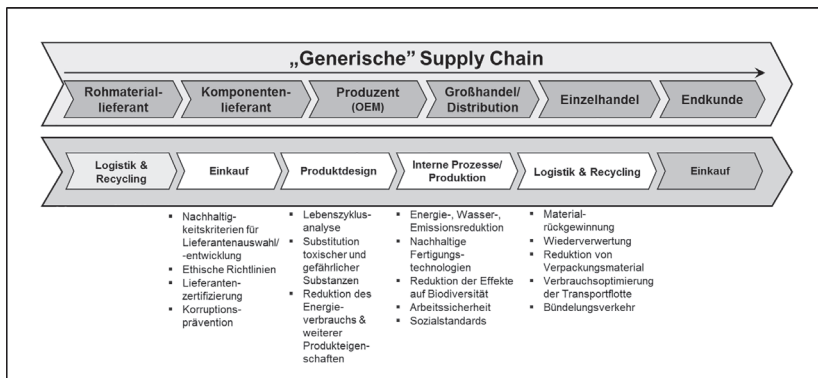


Abbildung 2: Funktionale Nachhaltigkeitspraktiken entlang der Lieferkette.

23 Für einen umfassenden Überblick solcher Indikatoren siehe bspw. die aktuelle Version der Global Reporting Initiative (GRI) 2022 oder die wissenschaftliche Diskussion in *Miemczyk/Johnsen/Macquet*, Supply Chain Management: An International Journal 2012, 485 ff.

24 Die in Abbildung 1 arbiträr gewählten Perioden dienen ausschließlich der Orientierung und sollen darauf hinweisen, dass riskantere Warengruppen und Lieferanten aus risikoreicheren Ländern (dunkelgelb/rot) tendenziell in kürzeren Abständen re-auditiert werden müssen als solche aus risikoarmen Ländern und Warengruppen (hellgelb/grün).

Studien legen nahe, dass die Lieferkettenposition eines Unternehmens in Bezug auf seine Nachhaltigkeitsaktivitäten dabei eine wichtige Rolle spielt.²⁵ Diese Vermutung ergibt sich aus einer Vielzahl möglicher Erklärungen:²⁶

16

- (a) Immer mehr Stakeholder, insbesondere Endkunden und NGOs üben den größten Druck auf exponierte Unternehmen mit starken Marken (fokale Unternehmen) aus. Dies geschieht hauptsächlich, weil diese Unternehmen am sichtbarsten sind und aufgrund ihrer exponierten Stellung auch am meisten Imageschaden zu fürchten haben.
- (b) Die produzierenden Unternehmen kontrollieren und managen sowohl das Produktdesign als auch die Produktentwicklung selbst. Somit haben sie einen starken Einfluss auf die nachhaltigen Produkteigenschaften und können gleichzeitig bewusst durch Lieferanten- und Standortwahl die Wertschöpfungsprozesse organisieren. Folglich sind es die Hersteller der Markenartikel, bei denen die Prozesse zusammenlaufen. In den Augen vieler Stakeholder haben sie daher auch die Verantwortung, dafür zu sorgen, dass in der gesamten Wertschöpfungskette keine Nachhaltigkeitsprobleme auftauchen.²⁷
- (c) Das Gros der Europäischen Umweltregularien wie etwa REACH²⁸ oder RoHS²⁹ sowie auf internationaler Ebene die Section 15 des Dodd-Frank Wall Street Reform and Consumer Protection Act³⁰ zielen auf jene Unternehmen ab, die das Endprodukt produzieren und/oder durch Import in Marktumlauf bringen. Dies sind in der Regel die Hersteller von Markenprodukten.
- (d) Ausgerechnet Unternehmen mit dem stärksten Umwelteinfluss und der höchsten körperlichen Arbeitsintensität – meist auf relativ niedrigem Qualifikations- und Bildungsniveau – sind häufig gegen den Druck von Stakeholdern und Imagekampagnen immun. Dieser paradoxe Effekt lässt sich darauf zurückführen, dass sie aufgrund ihrer geringen Sichtbarkeit ein lediglich geringes öffentliches Interesse wecken. Ein Umstand, der die Chance erhöht, dass ein Fehlverhalten seitens Lieferanten unentdeckt bleibt, und der Lieferanten einen Anreiz liefern kann, selbst nicht aktiv zu werden und somit die Kosten für etwaige Nachhaltigkeitsaktivitäten einzusparen. Dadurch werden

25 Vgl. z. B. Lo, *International Journal of Operations & Production Management* 2013, 93 ff. oder Schmidt/Schaltenbrand/Foerstl, *Journal of Supply Chain Management* 2017, 3 ff.

26 Für eine ausführliche Diskussion dieser Studie siehe Foerstl/Azadegan/Leppelt/Hartmann, *Journal of Supply Chain Management* 2015, 67 ff.

27 Hartmann/Moeller, *Journal of Operations Management* 2014, 281 ff.

28 Registration, Evaluation, Authorisation and Restriction of Chemicals. Europäische Chemikalienverordnung zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe.

29 RoHS: Restriction of Hazardous Substances. Beschränkung der Verwendung bestimmter gefährlicher Stoffe) in Elektro- und Elektronikgeräten.

30 US-amerikanische gesetzliche Verpflichtung des Nachweises über die Vermeidung von Konfliktmineralien innerhalb der Supply Chain für alle an die US Securities and Exchange Commission (SEC) berichtenden Unternehmen und ihre Zulieferer.

wiederum die fokalen produzierenden und großen Handelsunternehmen in die Pflicht genommen, ihre marktdominierende Stellung zu nutzen, um Nachhaltigkeitsstandards bei ihren Lieferanten durchzusetzen. Wenn nötig heißt dies auch, aktiv Entwicklungs- und Kooperationsprogramme zu kreieren und mit eigenen Ressourcen voranzutreiben.

- 17 Folglich wäre zu erwarten, dass produzierende und handelsnahe Unternehmen typischerweise stärker in ihr Nachhaltigkeitsengagement investieren als ihre Lieferanten. Gleichzeitig könnte man davon ausgehen, dass Unternehmen, die mehr in Nachhaltigkeit investieren, auch den größten ökonomischen Nutzen daraus ziehen.³¹
- 18 Wie in internationalen Studien bereits gezeigt wurde, wirken sich Investitionen in Nachhaltigkeitsaktivitäten positiv auf den Markterfolg und den Finanzerfolg von Unternehmen aus.³² Ein in Nachhaltigkeit investierter Euro wird sich also kurz bis mittelfristig durch gesteigerten Umsatz, ein verbessertes Unternehmensimage sowie gesteigerte Profitabilität verzinsen. Das ist nicht überraschend. Weiterhin lässt sich nachweisen, dass je näher die Lieferkettenposition den Endkunden kommt, desto mehr investieren Unternehmen in Nachhaltigkeitsengagement. Endkundenferne Unternehmen investieren dagegen signifikant weniger. Eine erhöhte Sichtbarkeit endkundennaher Unternehmen sollte also im Unternehmensalltag zu einem gesteigerten Bedarf an Nachhaltigkeitsengagement führen. Paradoxerweise nimmt jedoch zugleich die Erfolgswirkung von Nachhaltigkeitsinvestitionen mit steigender Endkundennähe ab.³³ Folglich sind die potenziell größten Profiteure im ökonomischen Sinne diejenigen, die am wenigsten für Nachhaltigkeit entlang der Lieferkette beitragen: endkundenferne Komponenten- und Rohmateriallieferanten. Dies hat in Bezug auf dringend anzugehende Themen wie die Menschenrechtsverletzungen jedoch gravierende Folgen.

IV. Menschenrechtsprobleme und Due Diligence – „beyond compliance“

- 19 Von Supply Chain Managern wird heutzutage nicht mehr nur verlangt, Compliance mit nachhaltigen Standards innerhalb ihrer Lieferantennetzwerke aufrechtzuerhalten und zu verbreiten, sondern sich zunehmend auch Aufgaben mitanzunehmen, die in der Vergangenheit unter originär staatlicher Gewalt standen.
- 20 Trotz zunehmender Regulierung, schaffen unterschiedliche gesetzliche Rahmenbedingungen in vielen Fällen noch immer ein legislatives Vakuum, das es ermöglicht, Produktionsstätten prinzipiell nicht nur dahin zu verlagern, wo die Kosten am geringsten sind, sondern gleichzeitig dort anzusiedeln, wo Menschenrechtsstandards, Umweltauflagen und Löhne am wenigsten in der Bilanz

31 Vgl. Schmidt/Schaltenbrand/Foerstl, Journal of Supply Chain Management 2017, 3 ff.

32 Vgl. Hoejmose/Brammer/Millington, Industrial Marketing Management 2012, 609 ff.

33 Schmidt/Schaltenbrand/Foerstl, Journal of Supply Chain Management 2017, 3 ff.

zu Buche schlagen.³⁴ Eine Konsequenz daraus ist, dass Menschenrechtsverletzungen in Zeiten von *failed states* und immer globaler agierender Unternehmen teilweise noch immer eher die Regel als die Ausnahme sind.³⁵

Da die Öffentlichkeit jedoch zunehmend auf die Belange der Betroffenen schaut und sich seit mehreren Dekaden unternehmerische Verantwortung als etabliertes und angesehenes Konzept durchgesetzt hat – nicht zuletzt durch nationale und internationale Initiativen wie etwa dem Lieferkettensorgfaltspflichtengesetz (LkSG)³⁶, dem UK Modern Slavery Act oder der OECD Guidelines for Multinational Enterprises –, sehen sich international agierende Unternehmen vor die Herausforderung gestellt, zumindest nachzuweisen, dass ihre immer globaleren Lieferantennetzwerke rechtskonform, nachhaltig und ethisch korrekt gemanagt werden. Darüber hinaus gibt es mittlerweile viele, zum Teil gewichtige Fürsprecher, die fordern, dass internationale Unternehmen dieses legislative Vakuum füllen.³⁷ Brennpunkte in der Diskussion um Menschenrechte und unternehmerische Verantwortung befassen sich u.a. mit den Themen Konfliktmineralien³⁸ und moderner Sklaverei.^{39,40}

Nicht zuletzt durch wachsende Anforderungen und Druck durch Stakeholder (Medien, Nichtregierungsorganisationen etc.) hat sich eine sog. Human Rights Due Diligence (dt. Sorgfaltspflicht) im Supply Chain Management etabliert.⁴¹ Diese orientiert sich primär an der OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas⁴² bzw. entsprechenden regulatorischen Vorgaben (wie LkSG oder der EU-Richtlinie zu Konfliktmineralien⁴³). Obwohl Due Diligence ursprünglich aus dem

34 Ehrgott/Reimann/Kaufmann/Carter, Journal of Business Ethics 2011, 99 ff.

35 Arnold, Business Ethics Quarterly 2010, 371 ff.

36 Zum LkSG ausführlich → Heske, Kap. 18 sowie Schröder/Schulz, Praxisleitfaden Supply Chain Compliance, 2023.

37 Eine ausführliche Diskussion bietet bspw. Ruggie, Innovations: Technology, Governance, Globalization 2008, 189 ff. Regulative Initiativen und Diskussionen umfassen bspw. auch das deutsche LkSG sowie die EU-weite „Lieferkettenrichtlinie“ (Directive on corporate sustainability due diligence).

38 Konfliktmineralien bezeichnen Rohstoffe, deren systematische Ausbeutung und Handel dazu beitragen, Menschenrechtsverletzungen im Land ihres Abbaus und angrenzenden Gebieten zu finanzieren. In erster Linie sind hier die Rohstoffe Gold, Wolfram, Tantal und Zinn aus dem Gebiet der Demokratischen Republik Kongo zu nennen.

39 Gold/Trautrim/Trodd, Supply Chain Management 2015, definieren Moderne Sklaverei (engl. „modern slavery“) als „[...] the exploitation of a person who is deprived of individual liberty anywhere along the supply chain, from raw material extraction to the final customer, for the purpose of service provision or production“ (S. 487).

40 Siehe z.B. Schleper/Blome/Stevenson/Thürer/Tusell, Transportation Research Part E: Logistics and Transportation Review 2022, 102801 ff.

41 Zu den Anforderungen nach dem LkSG → Heske, Kap. 18.

42 OECD, Organisation for Economic Cooperation and Development 2016.

43 Zur Konfliktmineralien-Verordnung und ähnlichen EU-Regelungen siehe etwa Kalss, ZfPW 2024, 181, 198 f.

M&A- (Mergers & Acquisitions) Bereich kommt⁴⁴ und dort eine vielseitige Untersuchung und Überprüfung der Finanzvorgänge eines Unternehmens vor Fusionen und Übernahmen beschreibt, wird das Konzept zunehmend auch im Lieferantenmanagement und dort vor allem im Nachhaltigkeitskontext angewandt.

- 23 Supply Chain Manager befinden sich somit immer öfter in der Position, angemessene Maßnahmen zu implementieren, die Konfliktmineralien und/oder moderne Sklaverei identifizieren und größtmögliche Transparenz über den Warenfluss von der Rohstoffgewinnung bis hin zum Endkunden gewährleisten. Viele der betroffenen Unternehmen versuchen bzw. sind rechtlich verpflichtet, diese Verantwortung in der Lieferkette an Zulieferer zu übertragen oder diese mit ihrer Marktmacht durchzusetzen.⁴⁵ Ein solcher „Verantwortungstransfer“ wird jedoch alleine kaum dazu führen, dass diese Probleme effektiv unterbunden werden können, insbesondere aus zwei Gründen: Auf der einen Seite führt das bereits erwähnte verbleibende regulative Vakuum dazu, dass Menschenrechtsverletzungen durch unternehmerische Akteure weiterhin stattfinden können, ohne dass diese oftmals dafür zur Verantwortung gezogen werden, d.i. eine „Non-Allokation von Verantwortungszuschreibungen“. Auf der anderen Seite scheuen sich viele Akteure jenseits rechtlicher Verpflichtungen teilweise immer noch, die dadurch zusätzlich entstehenden Compliance- und Regulierungskosten zu tragen.⁴⁶ Was daher benötigt wird ist vielmehr ein „Supply Chain Due Diligence“-Ansatz, unter dem einzelne Unternehmen und betroffene Stakeholder kooperativ Verantwortung tragen und gleichberechtigt zusammenarbeiten, um das Leben Betroffener zu verbessern.⁴⁷
- 24 Wichtig ist in diesem Zusammenhang, insbesondere die kleineren Zulieferer und betroffenen Individuen abseits der Endkonsumenten nicht auf sich allein gestellt zu lassen, da diese sich einem hohen ökonomischen Druck ausgesetzt sehen.⁴⁸ Dies ist jedoch selten der Fall: Auf der einen Seite versuchen die Hersteller und die Händler so viel Profit wie möglich zu generieren – zumeist auf Kosten der kleineren und schwächeren Stakeholder und Zulieferer. Auf der anderen Seite sollen diese jedoch ihre begrenzten Ressourcen in Due Diligence und Nach-

44 Für eine rechtliche Betrachtung von Compliance und Due Diligence in M&A-Transaktionen siehe in diesem Band → *Ullrich*, Kap. 26 Rn. 73 ff.

45 Wie etwa nach dem LkSG, siehe hierzu → *Heske*, Kap. 18 sowie zu vertraglichen Aspekten des LkSG *Wais*, JZ 2023, 429.

46 *Schleper/Blome/Stevenson/Thürer/Tusell*, Transportation Research Part E: Logistics and Transportation Review 2022, 102801 ff.

47 Für eine ausführliche Diskussion von Supply Chain Due Diligence im Rahmen der Konfliktmineralienthematik siehe *Hofmann/Schleper/Blome*, Journal of Business Ethics 2018, 115 ff. Für eine Diskussion des deutschen Lieferkettengesetzes siehe *Brandenburg/Warasthe/Seuring*, International Journal of Operations & Production Management 2024, 859 ff. Siehe ferner ausführlich → *Heske*, Kap. 18 sowie *Schröder/Schulz*, Praxisleitfaden Supply Chain Compliance, 2023. Für eine kritische Beurteilung der Erfolge solcher Initiativen siehe *LeBaron/Lister*, Review of International Political Economy 2022, 669 ff.

48 Zur Problematik der Lieferkettenregulierung für KMU siehe etwa *Kalss*, ZfPW 2024, 181, 198.

haltigkeitsaktivitäten investieren, damit das Einfallstor für Menschenrechtsprobleme, die fast immer am Beginn der Lieferketten liegen, so gering wie möglich gehalten wird. Diese doppelte Belastung führt jedoch selten zum Ziel. Werden schwächere Akteure ausgebeutet und werden ihnen gleichzeitig immer höhere Anforderungen an Nachhaltigkeit gestellt, kann dies schnell zu einem opportunistischen Verhalten führen.⁴⁹ Entweder versuchen die unter Druck stehenden Akteure abseits der Endkunden die abfließenden Profite und finanziellen Bürden durch andere Kanäle wieder hereinzuholen beispielsweise durch Minderungen bei Qualität und Sicherheit oder sie implementieren nur die nötigsten Mechanismen und „täuschen“ damit ein wahres Bekenntnis zu mehr Nachhaltigkeit nur vor. Was jedoch insbesondere in Situationen wie der unternehmensübergreifenden Menschenrechtsproblematik benötigt wird ist eine unternehmerische Praxis „beyond compliance“, d. i. eine auf ethischen und gerechten Grundsätzen basierende Problemlösungskultur.

V. Praxisrelevanz

Offensichtlich haben noch nicht alle endkundenferne Lieferanten das volle ökonomische Potenzial möglicher Nachhaltigkeitsaktivitäten für sich entdeckt. Insbesondere diese Unternehmen sollten erkennen, dass sie durch eine Verbesserung ihrer ökologischen und sozialen Bilanz auch ihre ökonomische Bilanz signifikant verbessern könnten. Grünes und soziales Wirtschaften steht somit seltener im Konflikt mit den ökonomischen Zielen des Unternehmens als oft behauptet. Folglich sollten die Lieferanten nicht abwarten bis ihre direkten Kunden sie drängen, Nachhaltigkeitskonzepte zu implementieren. Stattdessen sollten sie tragfähige Konzepte umsetzen und versuchen, Vorteile im Vergleich zu ihren zögerlichen Wettbewerbern zu erzielen. **25**

Weiterhin scheint es, dass die endkundennahen Unternehmen und Händler bereits ein höheres Niveau als ihre Lieferanten erreicht haben. Aufgrund des abnehmenden Grenznutzens wirken sich jedoch weitere Investitionen weniger positiv aus. Die tiefhängenden Früchte scheinen bereits gepflückt – was im Sinne der Nachhaltigkeit ein gutes Zeichen ist. Viele Produzenten und Handelsunternehmen versuchen ihre Ressourcen und ihr Know-how in branchenübergreifenden Organisationen einzubringen. Durch die gemeinsame Entwicklung von Nachhaltigkeitsstandards können heute mehr Lieferanten gefördert werden. So haben beispielsweise alle Mitglieder verschiedener Branchen und Industrien Abkommen geschlossen, in denen sie sich ihre Lieferantenaudits gegenseitig anerkennen (vgl. Fn. 21). Folglich können mit bestehenden Ressourcen quantitativ noch mehr Lieferanten nachhaltig entwickelt werden. Als positiver Nebeneffekt können alle Marktteilnehmer und Stakeholder transparent sehen, welche Unternehmen sich solchen Aktivitäten anschließen und welche nicht. **26**

49 Schleper/Blome/Wuttke, Journal of Business Ethics 2017, 97 ff.

- 27 Endkunden und Nichtregierungsorganisationen sollte dies alarmieren. Sie haben vieles richtig gemacht und durch kluge Kaufentscheidungen und effektive Kampagnen das Nachhaltigkeitsniveau gerade im vorderen, sichtbaren Teil der Lieferketten wesentlich erhöht. Nun jedoch sollte das Hauptaugenmerk stärker auf Lieferanten fallen, da auch sie durch nachhaltiges Verhalten Wettbewerbsvorteile generieren können. Im vorgelagerten Bereich der Lieferketten ist folglich noch viel Überzeugungsarbeit, aber auch Unterstützungsarbeit zu leisten. Wie das Beispiel der Menschenrechtsproblematiken gezeigt hat, muss es aber auch die Aufgabe der starken fokalen Unternehmen sein, die Zulieferer mit diesen Forderungen nicht allein zu lassen. Nur durch Vertrauen, faire Geschäftsbeziehungen und kooperatives Handeln lässt sich für beide Seiten ein profitables Unterfangen generieren. Auch die Zusammenarbeit mit NGOs, die auf einzelne Nachhaltigkeitsthemen spezialisiert sind, ist lohnenswert und befruchtet beide Seiten.

VI. Fazit

- 28 Zwar haben insbesondere die vorgelagerten Wertschöpfungsstufen Nachholbedarf im Hinblick auf ihr Nachhaltigkeitsengagement, doch auch der Konsument als das letzte Glied der Kette trägt große Verantwortung. Wird ein Nachhaltigkeitskandal durch Enthüllungsjournalismus oder engagierte Nichtregierungsorganisationen zu Tage gefördert, dann nützt ein kurzfristiger Kaufboykott auf lange Sicht wenig. Konsumenten müssen die zum Teil bereits vorhandenen Informationen zu Produkten und Unternehmen zu ihren Gunsten nutzen und eine Zahlungsbereitschaft für transparente, nachhaltig gefertigte Produkte entwickeln. Angesichts großer globaler Herausforderungen wie Klimawandel, Zerstörung von Biodiversität, Pandemien und geopolitischer Umwälzungen gilt dies heutzutage mehr denn je. Auch wenn es unmöglich ist, alle Wertschöpfungsprozesse entlang der Lieferkette detailgenau zu kennen, reicht es häufig aus, sich folgende Frage zu stellen: *Ist es möglich, dass dieses Produkt zu diesem Preis unter ordentlichen Arbeitsbedingungen und mit Rücksicht auf die Umwelt gefertigt wurde?* Kann man diese Frage mit „Ja“ beantworten, sollte man zusätzlich die Gegenprobe machen und überlegen, ob das gewünschte Produkt nicht vielleicht auch zu einem vergleichbaren Preis bei einem Anbieter mit nachweislich besserem Nachhaltigkeitsengagement zu erstehen ist.
- 29 Warum wird dies so deutlich betont? Der Endkunde ist integraler Bestandteil jeder Lieferkette. Mit seinem Verhalten bestimmt er nicht nur die Taktung der Lieferkette, sondern auch ihre Zusammensetzung (Lieferanten und Produktionstechnologien), ähnlich wie ein Dirigent nicht nur über den Takt seines Orchesters, sondern auch über die Musikanten und ihre Instrumente entscheidet. Gerade wenn es um das Thema Nachhaltigkeit geht, wird besonders deutlich, dass die viel zitierte Lieferkette eben in der Realität auch eine *Nachfragekette* ist, in der sich Angebot und Nachfrage treffen.

18. Kapitel

Lieferkettensorgfaltspflichtengesetz (LkSG) – Einführung und praktische Hinweise zur Umsetzung der Sorgfaltspflichten im Unternehmen

I. Wesentliche Regelungen des LkSG im Überblick

1. Entstehung, Zielsetzung und Anwendungsbereich

Das seit dem 1.1.2023 geltende „Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten“ (LkSG)¹ basiert auf den sogenannten „**Leitprinzipien für Wirtschaft und Menschenrechte**“ der Vereinten Nationen aus dem Jahr 2011. Die Umsetzung dieser Leitprinzipien wurde in Deutschland von 2016–2020 von der Bundesregierung im sogenannten Nationalen Aktionsplan (NAP)² vorangetrieben und überprüft. Das Ergebnis offenbarte eine mangelnde Integration menschenrechtlicher Sorgfalt in Unternehmensprozesse³ und führte dadurch zur gesetzlichen Regelung durch das LkSG. Am 25.7.2024 hat der EU-Gesetzgeber 2024 die EU-Lieferketten-Richtlinie (Corporate Sustainability Due Diligence Directive, CSDDD)⁴ verabschiedet, die von den Mitgliedstaaten bis zum 26.7.2026 umzusetzen ist. Das LkSG wird daher an die Vorgaben der CSDDD anzupassen sein (hierzu unter → Rn. 175).

Zielsetzung des LkSG ist die Achtung der Menschenrechte in den Lieferketten der verpflichteten Unternehmen, durch die Implementierung der Kernelemente der menschenrechtlichen Sorgfaltspflichten.⁵ Durch die Regulierung der vom Anwendungsbereich erfassten Unternehmen soll ein Schutzniveau in den Lieferketten sichergestellt werden, welches Staaten bis dato nicht allein herstellen können oder wollen.⁶ Damit kann das LkSG zugleich als Export des europäischen Verständnisses von Menschenrechten in viele Teile der Welt gesehen werden.⁷

Seit dem 1.1.2023 fielen zunächst Unternehmen mit mindestens 3.000 Arbeitnehmern in den **Anwendungsbereich** des Gesetzes, ungeachtet der Rechtsform, deren Hauptverwaltung, deren Hauptniederlassung, deren Verwaltungssitz oder

1 BGBl. 2021 I, S. 2959.

2 Siehe Nationaler Aktionsplan – Umsetzung der VN-Leitprinzipien für Wirtschaft und Menschenrechte (2016–2020), https://www.csr-in-deutschland.de/SharedDocs/Downloads/DE/NAP/nap-im-original.pdf?__blob=publicationFile (zuletzt abgerufen am 8.9.2024).

3 Abschlussbericht des NAP-Monitorings (2018–2020), S. 5.

4 Richtlinie (EU) 2024/1760 des Europäischen Parlaments und des Rates vom 13. Juni 2024 über die Sorgfaltspflichten von Unternehmen im Hinblick auf Nachhaltigkeit und zur Änderung der Richtlinie (EU) 2019/1937, ABl. L vom 5.7.2024, S. 1.

5 Vgl. BT-Drs. 19/28649, Problem und Ziel, S. 1.

6 Kritische Auseinandersetzung mit der LkSG-Zielerreichung in: *Passarge*, CB 2023, 171.

7 Vgl. *Passarge*, CB 2023, 171.

ob deren satzungsgemäßer Sitz sich im Inland befindet.⁸ Gleiches gilt für Unternehmen mit einer inländischen Zweigniederlassung (gemäß § 13d HGB). Der Schwellenwert reduzierte sich weiter seit dem 1.1.2024 auf 1.000 Arbeitnehmer.

- 4 In der Praxis empfiehlt es sich für Unternehmen daher, in einem ersten Schritt genau den eigenen Anwendungsbereich zu überprüfen und die Arbeitnehmerzahl exakt zu berechnen und zu dokumentieren. Dieses Vorgehen sollte jährlich wiederholt werden, wenn Unternehmen an der Schwelle des Anwendungsbereichs stehen.⁹
- 5 Maßgeblich ist die das Unternehmen prägende Personalstärke und damit die sogenannte „Stammbelegschaft“.¹⁰ Damit ist in Grenzfällen eine rückblickende Betrachtung und auch eine zukünftige Prognose entscheidend.¹¹ Sonderfälle (Leiharbeitnehmer und verbundene Unternehmen)¹² und Ausnahmen zur Berechnung der Arbeitnehmerzahl sind stets zu beachten.¹³
- 6 In Fällen, in denen die Arbeitnehmerzahl eines Unternehmens den Schwellenwert knapp unterschreitet, ist besondere Sorgfalt geboten. Es ist zu dokumentieren, dass zu Beginn des Geschäftsjahres die Arbeitnehmeranzahl geprüft und eine Anwendbarkeit verneint wurde.¹⁴ In dieser Situation sollte sich das Unternehmen vorsorglich Gedanken zur Erfüllung der gesetzlichen Sorgfaltspflichten machen, um im kommenden Geschäftsjahr bei Erreichen des Schwellenwerts nicht unvorbereitet in den Anwendungsbereich zu fallen.

2. Definition der Lieferkette

a) Lieferkette nach § 2 Abs. 5 LkSG

- 7 Wesentlich für die Umsetzung der gesetzlichen Sorgfaltspflichten des LkSG ist die Definition der **Lieferkette**.¹⁵ Je genauer Unternehmen die vom LkSG betroffenen eigenen Lieferketten identifizieren können, desto gezielter können sie die Anforderungen des LkSG umsetzen und eine ausufernde Anwendung der Sorgfaltspflichten vermeiden.
- 8 Die **Lieferkette** wird in § 2 Abs. 5 LkSG legaldefiniert und bezieht sich zunächst einmal auf alle Produkte und Dienstleistungen eines Unternehmens. Um-

8 Vgl. § 1 Abs. 1 LkSG.

9 Vgl. *Hagel/Wiedmann*, Menschenrechtsbeauftragte, S. 42.

10 Vgl. *Hagel/Wiedmann*, Menschenrechtsbeauftragte, S. 42.

11 Vgl. BT-Drs. 19/28649, Begründung zu § 1 Abs. 1 Nr. 2 LkSG.

12 Vgl. § 1 Abs. 2, 3 LkSG.

13 Siehe BAFA, Häufig gestellt Fragen (FAQ), III. Der Anwendungsbereich des Gesetzes, 2. Welche Arten von Arbeitnehmerinnen und Arbeitnehmern sind hier mitzuzählen?: https://www.bafa.de/DE/Lieferketten/FAQ/haeufig_gestellte_fragen_node.html (zuletzt abgerufen am 8.9.2024).

14 Vgl. *Hagel/Wiedmann*, Menschenrechtsbeauftragte, S. 42.

15 Abgrenzung zum Begriff der „Wertschöpfungskette“ überzeugend dargestellt in *Berg/Kramme/Charnitzky*, § 2 Rn. 155 f.

fasst sind alle Schritte im In- und Ausland, die zur Herstellung der Produkte oder zur Erbringung der Dienstleistung **erforderlich** sind.

Wie das einschränkende Merkmal der **Erforderlichkeit** auszulegen ist, ist streitig.¹⁶ Entgegen der Auffassung des Bundesamtes für Wirtschaft und Ausfuhrkontrolle (BAFA),¹⁷ das diesbezüglich eine weite Auffassung vertritt,¹⁸ sollte aus Sicht des Verfassers vielmehr davon ausgegangen werden, dass ausschließlich wesentliche Schritte, die zur Herstellung des Produkts bzw. zur Erbringung der Dienstleistung notwendig sind, erfasst sind.¹⁹ Reine **Hilfstätigkeiten**, wie beispielsweise Reinigungsleistungen oder der Betrieb einer Kantine wären demnach nicht Teil der Lieferkette.

In der Praxis kann Unternehmen empfohlen werden, zunächst den Rahmen der zwingend erforderlichen Schritte für die Produktherstellung oder die Dienstleistungserbringung zu konkretisieren und die eigene Einschätzung zu dokumentieren. Im Hinblick auf die weite Interpretation durch das BAFA sollten sodann vorsorglich auch Dienstleistungen wie der Betrieb der Kantine oder Reinigungsdienstleistungen berücksichtigt und dokumentiert werden.

Wesentlich ist die **konkrete Bestimmung der Lieferkette**. Für Produkte beginnt nach dem Gesetz die Lieferkette mit der Gewinnung der Rohstoffe und endet mit der Lieferung des Produkts an den Endkunden. Mangels Definition und zur Bestimmung der Lieferkette, sollte davon ausgegangen werden, dass als Endkunde der unmittelbare Abnehmer der Waren und Dienstleistungen²⁰ anzusehen ist. Dabei ist der Endkunde nicht unbedingt mit dem Endverbraucher gleichzusetzen.²¹ Typischerweise sollen die Phasen der Beschaffung, der Produktion und des Vertriebs umfasst sein.²²

b) Erfasste Handlungsbereiche im Rahmen der Lieferkette

Gesetzlich erfasst, als Bestandteil der Lieferkette gemäß § 2 Abs. 5 Nr. 1–3 LkSG, sind das Handeln im **eigenen Geschäftsbereich** sowie das zugerechnete Handeln von **unmittelbaren und mittelbaren Zulieferern**. Damit wird im Kern die ganze Lieferkette erfasst, die Sorgfaltspflichten folgen einem Stufenverhältnis

16 Vgl. etwa *Walden*, in: Depping/Walden, LkSG, 2022, § 2 Rn. 535 (nur produkt- bzw. dienstleistungsspezifische erforderlich Schritte); a. A. *Grabosch*, in: Grabosch, LkSG, § 2 Rn. 38; Zum Begriff der Erforderlichkeit siehe ferner *Gehling/Fischer*, in: Gehling/Ott, LkSG, § 2 Rn. 327 ff.

17 Das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) hat die gesetzliche Kontrolle zur Einhaltung der Vorgaben des LkSG übertragen bekommen.

18 Vgl. BAFA, LkSG-FAQ, II. Nr. 4. Siehe auch *Grabosch*, in: Grabosch, LkSG, § 2 Rn. 38.

19 Vgl. *Gehling/Ott/Lüneborg*, CCZ 2021, 230, 233; überzeugende Darstellung aus dem VCI-Papier bei *Brouwer*, CCZ 2022, 137, 141; Beispiele für erforderliche Schritte zur Produktherstellung in BT-Drs. 19/28649, Begründung zu § 2 Abs. 5.

20 Vgl. *Spindler*, ZHR 186 (2022), 67, 75; *Fleischer/Mankowski*, LkSG, § 2 Rn. 214; *Gergen/Fitzer*, CCZ 2024, 98, 100.

21 Vgl. *Gehling/Fischer*, in: Gehling/Ott, LkSG, § 2 Rn. 324

22 Vgl. BT-Drs. 19/28649, Begründung zu § 2 Abs. 5.

nis²³ mit unterschiedlich weitreichenden „Pflichtenkreisen“.²⁴ Im Unterschied zur CSDDD (→ hierzu unter Rn. 177) konzentriert sich das LkSG nur auf die vorgelagerte Wertschöpfungskette (sog. „Upstream“-Betrachtung)²⁵ und endet beim Endkunden. Eine pauschale Erweiterung der Sorgfaltspflichten auf die Absatzkette („Downstream“-Betrachtung) ist dem LkSG dagegen nicht zu entnehmen.²⁶

- 13** Der **eigene Geschäftsbereich** bezieht sich gemäß § 2 Abs. 6 LkSG auf jede Tätigkeit des Unternehmens zur Erreichung des Unternehmensziels. Eine Definition des Unternehmensziels (= Unternehmensgegenstand?) existiert nicht.²⁷ In der Literatur wird vertreten, dass darunter jede Tätigkeit zur Herstellung und Verwertung von Produkten und zur Erbringung von Dienstleistungen, unabhängig davon, ob sie an einem Standort im In- oder Ausland vorgenommen wird zu verstehen ist.²⁸ Zu beachten bleibt jedoch auch in diesem Fall, dass nur Handlungen des Unternehmens betroffen sind, die zur Herstellung der Produkte oder zur Erbringung der Dienstleistungen **erforderlich** sind.²⁹ Zu empfehlen ist insofern eine kritische Auseinandersetzung mit den unternehmenseigenen Gesellschaften und ihrem wesentlichen Beitrag im Rahmen der Herstellung der Produkte oder zur Erbringung der Dienstleistungen, um eine unkontrollierte Ausuferung zu vermeiden. Vor allem Gesellschaften mit vielen Mitarbeitenden, Produktionsstätten³⁰ oder Logistikzentren sollten dabei mit Priorität betrachtet werden.
- 14** Gemäß § 2 Abs. 5 Satz 1 LkSG umfasst der Begriff der Lieferkette auch das Handeln von unmittelbaren und mittelbaren Zulieferern.
- 15** **Unmittelbare Zulieferer** sind alle Vertragspartner über die Lieferung von Waren oder die Erbringung von Dienstleistungen, deren Zulieferung für die Herstellung des Produkts oder zur Erbringung und Inanspruchnahme der betreffenden Dienstleistung notwendig sind.³¹ Gemäß dieser Definition in § 2 Abs. 7 LkSG ist der gesamte Zulieferer mit allen Geschäftsbereichen in die Risikoanalyse mit aufzunehmen, auch wenn nicht jeder Geschäftsbereich für die Zulieferungen notwendig ist.³² Demnach wäre beispielsweise eine isolierte Betrachtung einer für das Unternehmen produzierenden Gesellschaft unzulässig, wenn die übergeordnete Holding beauftragt wurde.

23 Vgl. *Rothermel*, LkSG, § 2 Rn. 130.

24 Vgl. *Gehling/Ott/Lüneborg*, CCZ 2021, 230, 240.

25 Vgl. *Wüstemann/Büchner*, BB 2024, 579, 580.

26 Vgl. *Charnitzky*, in: *Berg/Kramme*, LkSG, § 2 Rn. 160.

27 Vgl. *Gergen/Fitzer*, CCZ 2024, 98, 100.

28 Vgl. *Charnitzky/Weigel*, RIW 2022, 12 ff., a. A. *Walden*, in: *Depping/Walden*, LkSG, § 2 Rn. 558 ff.

29 Vgl. *Bettermann/Hoes*, BKR 2022, 23, 24; ähnlich *Walden*, in: *Depping/Walden*, LkSG, § 2 Rn. 562.

30 Ausdrücklich genannt in BT-Drs. 19/28649 Begründung zu § 2 Abs. 6.

31 Vgl. § 2 Abs. 7 LkSG.

32 Vgl. *Charnitzky*, in: *Berg/Kramme*, LkSG, § 2 Rn. 193.

Auch **Tochtergesellschaften** können zum Kreis der unmittelbaren Zulieferer zählen, sofern es am bestimmenden Einfluss der Muttergesellschaft auf die Tochtergesellschaft mangelt.³³ Andernfalls sind sie dem eigenen Geschäftsbereich zuzuordnen. Diese Abgrenzung hat vor allem Auswirkungen im Rahmen der Abhilfemaßnahme im Inland (§ 7 Abs. 1 LkSG). 16

Die **Notwendigkeit** einer Zulieferung ist nicht definiert oder konkret beschrieben. Im Rahmen der Diskussion dürfte vieles dafür sprechen, die oben dargestellten Maßstäbe für das Merkmal der Erforderlichkeit auch hinsichtlich des Begriffs der Notwendigkeit heranzuziehen (vgl. oben → Rn. 9).³⁴ 17

Damit haben Unternehmen im ersten Schritt alle Vertragspartner zu sichten und in einem zweiten Schritt sodann die Notwendigkeit der Zulieferung für die eigene Produktherstellung oder Dienstleistungserbringung zu prüfen. Generell muss darauf geachtet werden, dass Zulieferer von **Nichtproduktionsmaterialien** nicht von der Definition ausgeschlossen sind und eine notwendige Zulieferung bzw. Dienstleistung erbringen können (bspw. Produktionsmaschinen oder Software). 18

Der sogenannte **mittelbare Zulieferer** wird nach § 2 Abs. 8 LkSG negativ abgegrenzt und umfasst alle Zulieferer mit notwendigen Zulieferungen, die nicht unmittelbare Zulieferer sind.³⁵ Damit können mittelbare Zulieferer keine Vertragspartner sein.³⁶ Im Kern dürfte im Rahmen einer Gesamtbetrachtung der Lieferkette der überwiegende Anteil unter die Definition der mittelbaren Zulieferer fallen, wobei nach dem LkSG – wie ausgeführt – ausschließlich die „Upstream“-Lieferkette zu betrachten ist.³⁷ Missbräuchliche Gestaltungen oder Umgehungsgeschäfte führen nach § 5 Abs. 1 Satz 2 LkSG allerdings dazu, dass mittelbare Zulieferer als unmittelbare Zulieferer im Rahmen der Risikoanalyse zu betrachten sind. 19

3. Menschenrechtliche und umweltbezogene Risiken und Pflichten

Die Sorgfaltspflichten für Unternehmen knüpfen zumeist an das Bestehen eines potenziellen **menschenrechtlichen oder umweltbezogenen Risikos** (bspw. Risikoanalyse in § 5 Abs. 1 LkSG) oder die eingetretene Verletzung einer **menschenrechtsbezogenen oder umweltbezogenen Pflicht** (bspw. Abhilfemaßnahmen, § 7 Abs. 1 LkSG) an. Ein umfangreicher, aber abgeschlossener 20

33 Vgl. *Wagner/Wagner/Schuler*, in: *Wagner/Ruttloff/Wagner*, LkSG, Rn. 66.

34 Vgl. auch *Gergen/Fitzer*, CCZ 2024, 98, 101.

35 Vgl. § 2 Abs. 8 LkSG.

36 Vgl. *Wagner/Wagner/Schuler*, in: *Wagner/Ruttloff/Wagner*, LkSG, Rn. 67.

37 Vgl. *Gergen/Fitzer*, CCZ 2024, 98, 101.

Katalog³⁸ von menschenrechtlichen und umweltbezogenen Verboten findet sich in § 2 Abs. 2 und 3 LkSG wieder.

- 21** In Bezug auf den Schutz der Menschenrechte, leiten sich die **geschützten Rechtspositionen** aus § 2 Abs. 1 LkSG ab, der auf den Anhang des LkSG (Nr. 1–11) und die aufgelisteten Übereinkommen zum Schutz der Menschenrechte verweist.

a) Menschenrechtliche Risiken

- 22** Ein **menschenrechtliches Risiko** ist ein Zustand bei dem aufgrund tatsächlicher Umstände mit hinreichender Wahrscheinlichkeit ein Verstoß gegen die in § 2 Abs. 2 Nr. 1–11 LkSG normierten Verbote droht.³⁹ Zu den Verboten gehören:
- Verbot zur Beschäftigung von **Kindern** unterhalb des zulässigen Mindestalters (Nr. 1);
 - Verbot der schlimmsten Formen der **Kinderarbeit** für Kinder unter 18 Jahren (Nr. 2);
 - Verbot der Beschäftigung von Personen in **Zwangsarbeit** (Nr. 3);
 - Verbot aller Formen der **Sklaverei** und sklavenähnlicher Praktiken (Nr. 4);
 - Verbot der Missachtung der Mindeststandards zum **Arbeitsschutz** (Nr. 5);
 - Verbot der Missachtung der **Koalitionsfreiheit** (Nr. 6);
 - Verbot der Ungleichbehandlung in Beschäftigung (**Diskriminierungsverbot**) (Nr. 7);
 - Verbot des Vorenthaltens eines **angemessenen Lohns** (Nr. 8);
 - Verbot der Herbeiführung bestimmter **Umwelteinwirkungen** (Nr. 9);
 - Verbot der widerrechtlichen **Zwangsräumung** und Entzug von Land (Nr. 10);
 - Verbot von bestimmten Verhaltensweisen durch **Sicherheitskräfte** (Nr. 11).

Darüber hinaus normiert § 2 Abs. 2 Nr. 12 LkSG eine Auffangklausel.⁴⁰ Darunter sind Fälle zu fassen, die nicht bereits unter die Verbote gemäß § 2 Abs. 2 Nr. 1–11 LkSG fallen, aber ihrer Art und Auswirkung nach eine gleichwertige Beeinträchtigung von im LkSG geschützten Rechtspositionen haben.⁴¹

b) Umweltbezogene Risiken

- 23** **Umweltbezogene Risiken** werden in § 2 Abs. 3 LkSG aufgeführt und sind im Rahmen der Sorgfaltspflichten zu beachten. Hierzu gehören:
- Verbot der **Herstellung von mit Quecksilber versetzten Produkten** (Nr. 1);
 - Verbot der **Verwendung von Quecksilber** und Quecksilberverbindungen bei Herstellungsprozessen (Nr. 2);
 - Verbot der unzulässigen Behandlung von **Quecksilberabfällen** (Nr. 3);

38 Vgl. BT-Drs. 19/28649 Begründung zu § 2 Abs. 1.

39 Verbote basieren auf den in der Anlage zum LkSG (zu § 2 Abs. 1, § 7 Abs. 3 Satz 2) aufgelisteten Übereinkommen zum Schutz der Menschenrechte.

40 Vgl. BT-Drs. 19/28649, Begründung zu § 2 Abs. 2 Nr. 12.

41 Vgl. Berg, in: Berg/Kramme, LkSG, § 2 Rn. 121.

- Verbot der **Produktion und Verwendung bestimmter Chemikalien** (Nr. 4);
- Verbot der nicht **umweltgerechten Handhabung, Sammlung, Lagerung und Entsorgung von Abfällen** (Nr. 5);
- Verbot der **Ausfuhr gefährlicher Abfälle** (Nr. 6 und 7);
- Verbot der **Einfuhr gefährlicher Abfälle und anderer Abfälle** (Nr. 8).

Insgesamt konzentriert sich das LkSG auf bestimmte Verbote aus dem Minamata-Übereinkommen, dem Stockholmer-Übereinkommen (POPs-Übereinkommen) und dem Basler-Übereinkommen.⁴² Unternehmen mit Berührungspunkten sollten eingehend ihre umweltbezogenen Risiken prüfen und entsprechende Sorgfaltspflichten beachten. 24

c) Menschenrechtsbezogene und umweltbezogene Pflichten

Werden **menschenrechtsbezogene oder umweltbezogene Pflichten** im Rahmen des LkSG verletzt, so ist darunter stets eine Verletzung der in § 2 Abs. 2, 3 LkSG genannten Verbote zu verstehen. Im Gesetz wird dieser Terminus zumeist dann verwendet, wenn eine Verletzung möglich erscheint (§ 3 LkSG) oder bereits eingetreten ist (§ 8 Abs. 1 LkSG) und folglich konkrete Abhilfemaßnahmen zu ergreifen sind. 25

II. Praktische Hinweise zur Umsetzung der Sorgfaltspflichten im Unternehmen

1. Verantwortlichkeiten im Rahmen der Einhaltung der Sorgfaltspflichten

Die Umsetzung und Einhaltung der Sorgfaltspflichten im Unternehmen verantwortet die Geschäftsleitung im Rahmen ihrer **Legalitätspflicht**.⁴³ Sie hat allgemein dafür Sorge zu tragen, dass das Unternehmen so organisiert wird, dass keine Gesetzesverstöße erfolgen.⁴⁴ 26

Im Wesentlichen erstreckt sich damit die Gesamtverantwortung der Geschäftsleitung des Unternehmens auf die **Umsetzung der menschenrechtlichen und umweltbezogenen Sorgfaltspflichten** gemäß § 3 Abs. 1 LkSG. Dabei steht es dem Unternehmen nach § 3 Abs. 2 LkSG grundsätzlich frei, die Sorgfaltspflichten in angemessener Weise umzusetzen, um etwaige Umstände des Einzelfalls bzw. die Charakteristika des Unternehmens zu berücksichtigen.⁴⁵ 27

Zur Einhaltung der Sorgfaltspflichten hat die Geschäftsleitung zudem eine Person zu benennen, die für die Überwachung des Risikomanagements zuständig 28

42 Vgl. Anlage zum LkSG (zu § 2 Abs. 1, § 7 Abs. 3 Satz 2).

43 Vgl. *Schröder/Schulz*, Praxisleitfaden Supply Chain Compliance, Rn. 7 ff.

44 Vgl. hierzu → *Schulz*, Kap. 1 Rn. 36 f. sowie LG München I, Urt. v. 10.12.2013 – 5 HK O 1387/10, NZG 2014, 345.

45 Vgl. *Fleischer*, CCZ 2022, 205, 208.

ist und der die „Funktion eines Bindeglieds“⁴⁶ zukommt. Vielfach folgen Unternehmen der gesetzlichen Empfehlung des LkSG und benennen einen **Menschenrechtsbeauftragten**.⁴⁷ Es ist jedoch nicht ausgeschlossen, die Überwachung des Risikomanagements auf mehrere Personen zu verteilen.⁴⁸ Vielfach werden hierfür auch Expertengremien gebildet. Die Schaffung einer solchen Funktion oder eines solchen Gremiums führt jedoch nicht zur Entlastung der Geschäftsleitung (im gesellschaftsrechtlichen Sinne) und befreit diese nicht von den eigenen Beaufsichtigungs- und Überwachungspflichten.⁴⁹

- 29 In der Praxis hängt die Benennung des Menschenrechtsbeauftragten oder eines Gremiums von den bereits etablierten Strukturen ab. Tatsächlich empfiehlt es sich, eine bereits bestehenden **Compliance-Funktion** im Unternehmen mit der Gesamtverantwortung zu betrauen und damit an bestehende Verantwortlichkeiten anzuknüpfen.⁵⁰ Die Überwachung der Einhaltung gesetzlicher Vorgaben, der Umgang mit Beschwerden und der Austausch mit Behörden lassen diesen Schluss naheliegen.
- 30 Die **Strafbarkeitsrisiken** des Menschenrechtsbeauftragten sind aufgrund der zumeist fehlenden Garantenstellung als gering zu betrachten.⁵¹

2. Sorgfaltspflichten im Unternehmen nach dem LkSG

- 31 Die tatsächliche Umsetzung der LkSG-Sorgfaltspflichten stellt die meisten Unternehmen vor große Herausforderungen. Neben der Einzigartigkeit jeder betrieblichen Organisation, der Lieferketten und der Produkte, ist auch die bereits bestehende Organisationsreife und damit die Ausgangslage der verpflichteten Unternehmen sehr unterschiedlich. Branchen, die bereits in der Vergangenheit stark mit Menschenrechtsthemen in Verbindung gebracht wurden, sind zumeist besser aufgestellt.
- 32 Dementsprechend unterscheiden sich Unternehmen bereits nach dem Reifegrad der Organisation, den bereits etablierten Strukturen und den personellen und finanziellen Kapazitäten. Damit verbietet sich ein genereller „Copy & Paste“-Ansatz bei der Umsetzung der Sorgfaltspflichten.
- 33 Jedoch lassen sich einige grundlegende **Strategien und Hinweise** zur erfolgreichen Implementierung und Umsetzung wie folgt zusammenfassen.

46 Vgl. *Wagner/Wagner*, in: *Wagner/Rutloff/Wagner*, LkSG, Rn. 488.

47 Vgl. § 4 Abs. 3 LkSG sowie ausführlich zu Rolle und Aufgaben des Menschenrechtsbeauftragten → *Hagel/Wiedmann*, Kap. 19.

48 Vgl. *Haag/Drodofsky*, CB 2024, 61, 63.

49 Vgl. *Rutloff/Wagner/Hahn/Freihoff*, CCZ 2022, 23 f.; *Kramer/Schunder*, BB 2024, 75, 77. Zu Umfang und Grenzen der Delegation von Compliance-Maßnahmen ferner → *Schulz*, Kap. 1 Rn. 56 f.

50 Bereits im Gesetzesentwurf vorgeschlagen, vgl. BT-Drs. 19/28649, Begründung zu § 4 Abs. 3; vgl. *Hembach*, Praxisleitfaden LkSG, III, S. 127.

51 Vgl. *Werner*, CB 2023, 245, 250.

a) Synergien erkennen – Compliance-Management-System nutzen

Ausgangspunkt der Umsetzung und Implementierung sollte die Suche nach Synergien im eigenen Unternehmen sein. Unternehmen die bereits dem „(Drei)-Säulen-Modell“ mit den Bereichen Recht, Compliance und ESG folgen,⁵² sollten die Einordnung der LkSG-Anforderungen genau prüfen. Etablierte Strukturen, Berichtslinien, erprobte Prozesse oder einzelne Sorgfaltspflichten und bestehende Maßnahmenkataloge sind dabei in die Abwägung mit einzubeziehen. Gleiches gilt für Kompetenzen und Kapazitäten in Bezug auf die nachhaltigkeitsbezogenen Anforderungen des LkSG.⁵³ Wenn bereits auf ein **bestehendes Compliance-Management-System (CMS)** zurückgegriffen werden kann, sollte genau geprüft werden, welche Sorgfaltspflichten oder Teile davon bereits implementiert sind oder alternativ in bestehende Strukturen integriert werden können.⁵⁴ 34

Besonders die LkSG-Sorgfaltspflichten rund um die Themen Risikoanalyse, Risikomanagement, Grundsatzzerklärung und Dokumentation sind bekannte und in prototypischer Weise **Elemente eines CMS**.⁵⁵ Gleiches gilt für die Systematik. Danach stellen die Sorgfaltspflichten einen sich wiederholenden Kreislauf von Verfahrensschritten dar, die aufeinander aufbauen und sich aufeinander beziehen.⁵⁶ Diese Vorgehensweise ist einem CMS nicht fremd, sondern erinnert an die bekannte Vorgehensweise in den ISO-Standards.⁵⁷ 35

Durch die Integration in bestehende Strukturen, kann im Idealfall auch die Bindung von Ressourcen⁵⁸ verhindert und auf den Aufbau von kostenintensiven Parallelstrukturen verzichtet werden. 36

b) Umsetzungsprojekt: Vorüberlegungen zur Implementierung der Sorgfaltspflichten

Im Rahmen der Vorbereitung müssen sich Unternehmen im Rahmen der **Zielsetzung** entscheiden, ob und in welchem Umfang das LkSG umgesetzt werden soll. Bei verpflichteten Unternehmen besteht hinsichtlich des „Ob“ keine Wahl. Unternehmen, die nicht oder derzeit nicht in den Anwendungsbereich fallen, sollten die Vor- und Nachteile genau abwägen und über eine (teilweise) Umsetzung trotz fehlender Verpflichtung nachdenken. Dies gilt vor allem dann, wenn sie Teil von Lieferketten sind, bei denen die Sorgfaltspflichten von Vertragspartnern weitergegeben werden (sog. Trickle-down-Effekt).⁵⁹ 37

⁵² Vgl. *Weihe*, CCZ 2024, 85, 86.

⁵³ Vgl. *Nietsch*, CCZ 2023, 61, 65.

⁵⁴ Vgl. *Schröder/Schulz*, Praxisleitfaden Supply Chain Compliance, Rn. 10, 140 ff., 494 ff.

⁵⁵ Vgl. *Nietsch*, CCZ 2023, 61, 66; siehe auch *Schröder/Schulz*, Praxisleitfaden Supply Chain Compliance, Rn. 131 ff.

⁵⁶ Vgl. BT-Drs. 19/28649, Begründung zu § 3 Abs. 1.

⁵⁷ Vgl. *Brauer/Busker*, CB, 2022, 472.

⁵⁸ Vgl. *Brauer/Busker*, CB, 2022, 472, 473.

⁵⁹ Vgl. *Hembach*, Praxisleitfaden LkSG, III, S. 162.

- 38 Die unternehmensinterne Umsetzung der LkSG-Sorgfaltspflichten setzt ein Bekenntnis der Geschäftsleitung zwingen voraus. Den „**Tone from the Top**“ vor allem im Hinblick auf eine klare Haltung mit Blick auf die Risikokultur vorzulegen und vorzuleben,⁶⁰ gibt allen weiteren Schritten die notwendige Legitimierung.
- 39 Die **Verantwortlichkeit** für die Umsetzung der Sorgfaltspflichten sollte von Beginn an, vor allem im Rahmen der internen Kommunikation, klar geregelt sein. In welchem Unternehmensbereich die Umsetzungsverantwortlichkeit liegt, hängt von etablierten Strukturen oder allgemeinen Zielsetzungen ab. Nicht zwingend, aber möglicherweise sinnvoll erscheint, dass dem zukünftigen Menschenrechtsbeauftragten die Verantwortung für die erstmalige Implementierung der Sorgfaltspflichten übertragen wird.⁶¹ Trotz seiner gesetzlich normierten Überwachungspflichten, darf die Anleitung der operativen Umsetzung dem nicht entgegenstehen. Vielmehr muss der Fokus darauf liegen, dass der Menschenrechtsbeauftragte bereits von Beginn an die Möglichkeit zur rechtskonformen Gestaltung der gesetzmäßigen Umsetzung der Sorgfaltspflichten hat. Dies setzt jedoch voraus, dass Verantwortlichkeiten im Rahmen der Implementierung später abgegeben werden und die Funktion der Überwachung eingenommen wird.
- 40 Wie die Umsetzung der Sorgfaltspflichten operativ organisiert wird, hängt von den vorgegebenen Prozessen im Unternehmen ab. Empfehlenswert ist eine koordinierte, gesteuerte und zentral organisierte Umsetzung im Rahmen eines **Projektes**. Hierzu muss die Geschäftsleitung die entsprechenden Ressourcen bereitstellen.
- 41 Unablässig bleibt im Rahmen der Vorbereitung eine **fundierte Kenntnis der Rechtslage**. Diese entscheidet zwangsläufig darüber, ob alle Sorgfaltspflichten gesetzeskonform umgesetzt und alle Chancen eines risikobasierten Ansatzes genutzt werden können. Die Zusammenarbeit mit Rechtsberatern, zumindest bei strategischen Überlegungen oder Detailfragen ist zu empfehlen.
- 42 Unausweichlich ist im Rahmen der Umsetzungsvorbereitung eine umfassende „**Gap-Analyse**“, also ein Vergleich des Ist- und Sollzustands in Bezug auf die Pflichten nach dem LkSG.⁶² Insgesamt empfiehlt sich ein detaillierter Blick in die Unternehmensstrukturen und -Prozesse, da Unternehmen zumeist einige Sorgfaltspflichten, beispielsweise die Einrichtung eines Beschwerdeverfahrens,⁶³ umgesetzt oder in anderen Prozessen integriert haben.

60 Vgl. *Fleischer*, CCZ 2022, 205, 213. Siehe hierzu auch → *Schulz*, Kap. 1 Rn. 69 f.

61 Zu Rolle und Aufgaben des Menschenrechtsbeauftragten ausführlich → *Hagel/Wiedmann*, Kap. 19.

62 Vgl. *Schröder/Schulz*, Praxisleitfaden Supply Chain Compliance, Rn. 174 ff. und Rn. 209.

63 Pflicht zur Einrichtung einer Meldestelle kann sich bereits unabhängig vom LkSG bspw. aus § 12 HinSchG ergeben.

Mit der Fertigstellung der Analyse wird erstmals deutlich welche derzeitigen Risiken das Unternehmen und die Geschäftsleitung tragen. Gleichzeitig zeigt sie aber auch zu einem frühen Stadium auf, welche Schwerpunkte ein Umsetzungsprojekt (bspw. Risikoanalyse und Präventionsmaßnahmen) haben muss. Dadurch wird neben der Planung der Ressourcen auch die Einschätzung der Umsetzungszeit erheblich erleichtert. 43

c) Die Sorgfaltspflichten im Überblick

Die Sorgfaltspflichten eines Unternehmens nach dem LkSG sind als **Bemühenspflichten** zu verstehen. Damit werden nur konkret machbare, mithin zumutbare, Regelungen vom Unternehmen verlangt.⁶⁴ Einer Erfolgspflicht oder gar einer Garantiehaftung sollen Unternehmen nicht ausgesetzt werden.⁶⁵ Ausnahmen, wie die Abhilfemaßnahmenvorschrift im eigenen, inländischen Geschäftsbe- reich durchbrechen aber bereits diesen Grundsatz.⁶⁶ 44

Insgesamt soll das **Prinzip der Angemessenheit** beachtet werden. Unternehmen sollen, ihren Möglichkeiten entsprechend, einen angemessenen Umfang an Maßnahmen zur Verhinderung von menschenrechtsbezogenen und umweltbezo- genen Pflichtverletzungen schaffen. Gleiche Maßnahmen können also bei un- terschiedlichen Unternehmen anders bewertet und gewichtet werden. 45

Unternehmen haben dementsprechend Prozesse oder ein System aufzusetzen, welches der eigenen Finanzkraft, Größe und Risikolage entsprechen. Orientie- rung kann (neben den Materialien der BAFA) dabei die Umsetzung der Sorg- faltspflichten des LkSG bei vergleichbaren Unternehmen geben. Als erste prak- tische Standortbestimmung kann der im Unternehmen aufgesetzte Plan zur Umsetzung stets mit dem Helpdesk für Wirtschaft und Menschenrechte⁶⁷ disku- tiert werden. 46

Entscheidend für die Umsetzung der gesetzlichen Sorgfaltspflichten ist ein strukturiertes Vorgehen. Zumeist schafft die Berichtsfrist eine natürliche „Dead- line“, bis wann ein **Umsetzungsprojekt** bzw. wesentliche Teile umgesetzt wer- den sollten. Im Rahmen der Umsetzung ist stets ein risikobasierter Ansatz zu verfolgen. Die größten Herausforderungen (zumeist im Rahmen der Risikoana- lyse) sollten zuerst angegangen werden. Erst im Anschluss daran sollten weitere Lücken geschlossen werden. Dadurch wird die Akzeptanz des Umsetzungspro- jekts im Unternehmen sichergestellt und eine Überforderung der internen Struk- turen vermieden. 47

64 Vgl. *Depping*, in: *Depping/Walden*, LkSG, § 3 Rn. 6.

65 Vgl. BT-Drs. 19/28649, Lösungen, S. 2.

66 Vgl. *Depping*, in: *Depping/Walden*, LkSG, § 7 Rn. 29.

67 Siehe Helpdesk für Wirtschaft und Menschenrechte: <https://wirtschaft-entwicklung.de/wirtschaft-menschenrechte/kostenfreie-beratung/?erfahren=&cHash=64e2816fbf6be884a76663d1e7cb0eea> (zuletzt abgerufen am 8.9.2024).

- 48 Umzusetzen sind die in § 3 Abs. 1 Nr. 1–9 LkSG genannten **Sorgfaltspflichten**. Dabei handelt es sich nicht um einen einmaligen Prozess, sondern um einen wiederholenden Kreislauf der in den §§ 4–10 LkSG aufgeführten Verfahrensschritte.⁶⁸
- 49 Bereits zu Beginn der Umsetzung empfiehlt es sich, die **fortlaufende Dokumentation** und damit die Umsetzung der Sorgfaltspflicht nach § 3 Abs. 1 Nr. 9 LkSG sicherzustellen.⁶⁹

aa) Angemessenes und wirksames Risikomanagement
(§ 3 Abs. 1 Nr. 1 LkSG)

- 50 Unternehmen müssen gemäß § 4 Abs. 1 LkSG ein **angemessenes und wirksames Risikomanagement** zur Einhaltung der Sorgfaltspflichten (§ 3 Abs. 1 LkSG) einrichten. Dieses muss der Risikolage des Unternehmens entsprechen⁷⁰ und umfasst neben dem eigenen Geschäftsbereich des Unternehmens auch dessen Lieferkette.⁷¹
- 51 Ein angemessenes **Risikomanagement** ist damit unternehmensspezifisch zu gestalten⁷² und den allgemeinen menschenrechtlichen und umweltbezogenen Risiken des Unternehmens, der Branche, der Größe, der internationalen Verflechtung und weiterer Parameter anzupassen. Entscheidend ist, wie sich die Unternehmenstätigkeit auf die Interessen der Betroffenen im eigenen Geschäftsbereich und in der Lieferkette auswirkt.⁷³ Damit ist eine „Inside-out-Perspektive“ einzunehmen.⁷⁴
- 52 Das Risikomanagement folgt (wie die übrigen Sorgfaltspflichten) stets dem in § 3 Abs. 1 LkSG formulierten sog. **Angemessenheitsprinzip**. Daher korreliert die Risikoaffinität des Unternehmens mit den zumutbaren Anstrengungen zur Erfüllung der Sorgfaltspflichten.⁷⁵ Dabei ist im Rahmen der Abwägung sicherzustellen, dass Unternehmen zum einen den gesetzlich aufgeführten Pflichten gerecht werden, jedoch die auch **Begrenzungen aus dem Angemessenheitsprinzip** nutzen.⁷⁶ Nach der Begründung will der Gesetzgeber mit den Sorgfaltspflichten zusätzliche Belastungen für kleine und mittlere Unternehmen vermeiden und sich auf Anforderungen an Großunternehmen beschränken, die

68 Vgl. BT-Drs. 19/28649, Begründung zu § 3 Abs. 1.

69 Vgl. zur Dokumentationspflicht etwa *Schröder/Schulz*, Praxisleitfaden Supply Chain Compliance, Rn. 350 ff.

70 Vgl. *Haag/Drodofsky*, CB 2024, 61, 64.

71 Vgl. BT-Drs. 19/28649, Begründung zu § 4 Abs. 2.

72 Vgl. *Wagner/Wagner*, in: *Wagner/Ruttloff/Wagner*, LkSG, Rn. 609.

73 Vgl. *Haag/Drodofsky*, CB 2024, 61, 64.

74 Vgl. *Walden*, in: *Depping/Walden*, LkSG, § 5 Rn. 9.

75 Vgl. *Mader*, in: *Gehling/Ott*, LkSG, § 3 Rn. 53.

76 Vgl. *Mader*, in: *Gehling/Ott*, LkSG, § 3 Rn. 57.

praktikabel, verhältnismäßig und ohne übermäßigen bürokratischen Aufwand umzusetzen sind.⁷⁷

Wie das Risikomanagement im Unternehmen im Einzelnen umgesetzt werden soll, lässt das LkSG allerdings offen. Denkbar ist eine Integration als Teil des allgemeinen Risikomanagements oder des Compliance-Management-Systems.⁷⁸ Es empfiehlt sich jedoch auf bestehende und etablierte Strukturen und Elemente zurückzugreifen,⁷⁹ um einen Gleichlauf der Risikosteuerung und die gesetzlich geforderte Verankerung in den Geschäftsabläufen im Unternehmen zu gewährleisten.

Die **Wirksamkeit** eines Risikomanagements besteht gemäß § 4 Abs. 1, 2 LkSG, wenn Maßnahmen implementiert wurden, um menschenrechtliche und umweltbezogene Risiken zu erkennen und zu minimieren sowie Verletzungen menschenrechtsbezogener oder umweltbezogener Pflichten zu verhindern, zu beenden oder deren Ausmaß zu minimieren. Wichtig dürfte in diesem Rahmen die Ergänzung der Gesetzesbegründung sein, die eine Wirksamkeit auch annimmt, wenn eine Beendigung der Rechtsgutsverletzung nicht möglich oder mit einem unverhältnismäßigen Aufwand verbunden ist.⁸⁰ Dementsprechend sind vor allem die Risikoanalyse, die vorgenommenen Präventionsmaßnahmen gemäß § 6 Abs. 2–4 LkSG und die Abhilfemaßnahmen nach § 7 LkSG im Rahmen der Wirksamkeitsbeurteilung von Bedeutung. Sofern die maßgeblichen Bestandteile des Risikomanagement für sich genommen wirksam sind, gilt dies auch für das Risikomanagement im Ganzen.

Ein Risikomanagement, dass nur auf dem Papier existiert, aber keine praktische Verknüpfung zum eigenen Geschäftsbereich und zur Lieferkette hat, wird niemals vollends wirksam sein können. Folglich sind zwar die theoretischen Überlegungen im Rahmen des Risikomanagements, hinsichtlich der Struktur oder der Prozesse, wesentlich. Entscheidend für den Grad der Wirksamkeit wird aber sein, reale und praktische Maßnahmen im Rahmen der Prävention und Abhilfe zu etablieren.

Wie die **Messung der Wirksamkeit** des Risikomanagements vorzunehmen ist, schreibt das LkSG nicht vor.⁸¹ Möglich dürfte die Heranziehung des international anerkannten Wirkungskettenmodells sein.⁸² Im Kern kann die Wirksamkeit wie üblich anhand zu definierender Key Performance Indicators (KPIs) gemessen werden.

Unternehmen haben zudem im Rahmen der Errichtung und der Umsetzung des Risikomanagements die **Interessen von Stakeholdern zu berücksichtigen**. Ge-

77 Vgl. BT-Drs. 19/28649, Begründung zu § 3 Abs. 1.

78 Vgl. Walden, in: Depping/Walden, LkSG, § 5 Rn. 5.

79 Vgl. Baumüller/Needham, DK 2022, 194, 199.

80 Vgl. BT-Drs. 19/28649, Begründung zu § 4 Abs. 2.

81 Vgl. Fitzer/Gergen, CB 2022, 327, 329.

82 Ausführliche Darstellung in Fitzer/Gergen, CB 2022, 327, 329.

nerell gilt, dass vor allem Stakeholder entsprechend der identifizierten Risiken aus der Risikoanalyse zu berücksichtigen sind.⁸³ Besonders vulnerable Gruppen, deren Rechte zumeist verstärkt bedroht sind, sollten berücksichtigt werden.⁸⁴

- 58 Darunter ist nicht zwingend zu verstehen, dass Unternehmen aktiv in den Austausch mit verschiedenen Interessenvertretern oder betroffenen Personen gehen oder sich stets eng mit ihnen abstimmen müssen. Stattdessen können die Interessen der betroffenen Stakeholder auch vom Unternehmen mitgedacht werden.⁸⁵ Dennoch ist der aktive Austausch oder die direkte Konsultation von betroffenen Personen oder Interessenvertretungen sinnvoll, um ein effektives Risikomanagement zu implementieren und eine zielgerichtete Herangehensweise dokumentieren zu können. Als Beteiligungsformen können sich neben Befragungen auch Workshops, Umfragen oder Veranstaltungen im Unternehmen anbieten.

bb) Festlegung einer betriebsinternen Zuständigkeit
(§ 3 Abs. 1 Nr. 2 LkSG)

- 59 Teil des Risikomanagements nach § 4 Abs. 3 LkSG ist die Festlegung einer **betriebsinternen Zuständigkeit** zur Überwachung des Risikomanagements. Die Person soll entsprechend den Empfehlungen des Gesetzes, der Geschäftsleitung unmittelbar unterstellt sein.⁸⁶ Dadurch können Kommunikationswege direkt und kurz gestaltet, die normierten Informationsrechte wahrgenommen bzw. ein ungehinderter Informationsaustausch sichergestellt werden.⁸⁷ Das Gesetz nennt hierfür beispielhaft den sogenannten **Menschenrechtsbeauftragten**, diese Person wird auch als Ansprechpartner der Aufsichtsbehörde fungieren.⁸⁸
- 60 Es ist darauf zu achten, dass diese Person über die fachliche Eignung und eine **arbeitsvertragliche Bestellung** verfügt.⁸⁹ Interessenkonflikte des Menschenrechtsbeauftragten gilt es zu vermeiden.
- 61 Darüber hinaus besteht gemäß § 4 Abs. 3 LkSG eine regelmäßige, mindestens jährliche **Informationspflicht** der Geschäftsleitung über die Arbeit des Menschenrechtsbeauftragten. In der Praxis wird sich vor allem bei großen und risikoexponierten Unternehmen eine kurzfristigere Taktung einstellen. Der Informationsaustausch muss dokumentiert werden.

83 Vgl. *Fitzer/Gergen*, CB 2022, 327, 330.

84 Vgl. BT-Drs. 19/28649, Begründung zu § 4 Abs. 4.

85 Vgl. *Grabosch*, in: *Grabosch*, LkSG, § 2 Rn. 80.

86 Vgl. BT-Drs. 19/28649, Begründung zu § 4 Abs. 3.

87 Vgl. *Gehling/Ott/Lüneborg*, CCZ 2021, 230, 235.

88 Siehe → *Hagel/Wiedmann*, Kap. 19; sowie *Hagel/Wiedmann*, Menschenrechtsbeauftragte, S. 56 ff.

89 Siehe → *Hagel/Wiedmann*, Kap. 19; sowie *Hagel/Wiedmann*, Menschenrechtsbeauftragte, S. 61 ff.

cc) Risikoanalyse (§ 3 Abs. 1 Nr. 3 LkSG)

Wesentlicher Bestandteil jedes Risikomanagements ist eine angemessene Analyse der für das Unternehmen einschlägigen menschenrechtlichen und umweltbezogenen Risiken. Damit besteht erstmals die gesetzliche Pflicht zur Durchführung einer menschenrechtlichen und umweltbezogenen Due Diligence. Im Gegensatz zu den bekannten Risikoanalysen (bspw. aus dem Geldwäschegesetz) ist nicht die Unternehmensperspektive einzunehmen, sondern sind die Belange der Personen, die von nachteiligen menschenrechtlichen Auswirkungen in der Lieferkette unmittelbar betroffen sein können, zu betrachten.⁹⁰ Das BAFA hat als Orientierungshilfe für betroffene Unternehmen eine Handreichung zur Umsetzung einer Risikoanalyse nach den Vorgaben des LkSG veröffentlicht.⁹¹ 62

Einzubeziehen sind nicht alle möglichen oder denkbaren Risiken. Vielmehr sind die Kriterien aus § 3 Abs. 2 LkSG heranzuziehen, um einen **angemessenen Umfang der Risikoanalyse** zu gewährleisten. 63

(1) Ziele der Risikoanalyse

Ziele der Risikoanalyse ist die **Identifizierung** von menschenrechtlichen und umweltbezogenen Risiken im Unternehmen, deren **Bewertung** und **Priorisierung**. 64

Dabei sollen Unternehmen zunächst die eigenen Beschaffungsprozesse und Lieferketten durchleuchten, um vertiefte **Kenntnis über die menschenrechtlichen und umweltbezogenen Risiken** zu erlangen.⁹² Die Bewertung der Ergebnisse und deren Priorisierung folgen im Anschluss. Hinsichtlich der vertieften Betrachtung und der Priorisierung der Risiken haben Unternehmen einen weiten Gestaltungsspielraum.⁹³ 65

(2) Bedeutung der Risikoanalyse und Vorüberlegungen

Die Risikoanalyse sollte in allen Unternehmen das **Herzstück** der gesetzlichen Sorgfaltspflichten darstellen und gilt als wesentlicher Bestandteil des Risikomanagements.⁹⁴ Sie ist der Ausgangspunkt und das Bindeglied für die Umsetzung und Erfüllung weiterer wesentlicher Sorgfaltspflichten, wie beispielsweise die Verankerung von Präventionsmaßnahmen. Bereits im Rahmen der Umsetzung sollte auf ihr der **Schwerpunkt** liegen. 66

⁹⁰ Vgl. Grabosch, in: Grabosch, LkSG, § 5 Rn. 27.

⁹¹ Siehe BAFA, Risikoanalyse: https://www.bafa.de/DE/Lieferketten/Risikoanalyse/risikoanalyse_node.html (zuletzt abgerufen am 8.9.2024), sowie allgemein zur Bedeutung der BAFA Handreichungen Harings/Beermann/Hörnig, CB 2023, 450, sowie Schröder/Schulz, Praxisleitfaden Supply Chain Compliance, Rn. 397 ff.

⁹² Vgl. BT-Drs. 19/28649, Begründung zu § 5 Abs. 1.

⁹³ Vgl. BAFA, LkSG-FAQ, VII., Nr. 3.

⁹⁴ Vgl. Lorenz/Krülls, CCZ 2023, 100, sowie Schröder/Schulz, Praxisleitfaden Supply Chain Compliance, Rn. 183 ff.

- 67 Wie Unternehmen in der Praxis die Risikoanalyse ausgestalten oder welche Methoden gewählt werden, steht im Ermessen der Unternehmen.⁹⁵ Genaue Vorgaben macht das LkSG hierzu nicht.⁹⁶ Wie oben ausgeführt, hat allerdings das BAFA inzwischen als Orientierungshilfe für betroffene Unternehmen eine Handreichung zur Umsetzung einer Risikoanalyse nach den Vorgaben des LkSG veröffentlicht.⁹⁷ Im Übrigen haben sich bislang noch keine Standards etabliert. Dementsprechend kann das Risiko ganzheitlich erhoben und dargestellt werden oder sich aus verschiedenen Teilanalysen zusammensetzen. Diese können ebenfalls von verschiedenen Abteilungen erstellt werden.
- 68 Empfehlenswert ist die Trennung zwischen den Risiken im eigenen Geschäftsbereich und denen der unmittelbaren Zulieferer. Dafür spricht, dass die tatsächlichen menschenrechtlichen und umweltbezogenen Risiken sich meist stark unterscheiden. Gleiches gilt für die sich anschließenden Sorgfaltpflichten und folglich auch für die damit einhergehenden, stärker ausgeprägten Compliance-Pflichten im eigenen Geschäftsbereich im Gegensatz zur Lieferkette.⁹⁸
- 69 Ob wesentliche Teile der Risikoanalyse durch eigene Mitarbeitende oder **externe Dienstleister** durchgeführt werden, spielt keine Rolle.⁹⁹ Empfehlenswert ist im Rahmen der Darstellung und zu Zwecken der Auswertung eine systemische IT-Lösung. In der einfachsten Form kann bereits ein Tabellenkalkulationsprogramm wirksam sein. Dies gilt vor allem im **eigenen Geschäftsbereich**. Für die **unmittelbaren Zulieferer** kann, je nach Anzahl, auch auf eine von einem externen Dienstleister durchgeführte Risikoanalyse zurückgegriffen werden. Das Unternehmen muss dabei stets eingebunden sein und kann nicht die gesamte Risikoanalyse nach außen delegieren.¹⁰⁰ Hintergrund ist die Einbettung der Risikoanalyse in die Prozesse des Unternehmens.
- 70 Dabei sollte immer darauf geachtet werden, dass auch die unternehmenstypischen Risiken abgebildet werden, und nicht auf allgemeine Risikofelder zurückgegriffen wird. Dies führt dazu, dass den gesetzlichen Anforderungen nachgekommen und die eigene Arbeitsbelastung und die der unmittelbaren Zulieferer in der Lieferkette reduziert wird.

(3) Umfang und Inhalt der Risikoanalyse

- 71 Von der Risikoanalyse umfasst und damit zwingend einzubeziehen sind alle für die Herstellung der Produkte oder zur Erbringung der Dienstleistung **erforderlichen eigenen Geschäftsbereiche und unmittelbaren Zulieferer**. Mittelbare Zulieferer sind nicht direkt von der Risikoanalyse nach § 5 Abs. 1 LkSG um-

95 Vgl. BAFA Handreichung Risikoanalyse, S. 6.

96 Vgl. *Lorenz/Krülls*, CCZ 2023, 100, 101.

97 Siehe BAFA, Risikoanalyse: https://www.bafa.de/DE/Lieferketten/Risikoanalyse/risikoanalyse_node.html (zuletzt abgerufen am 8.9.2024).

98 Vgl. *Kramer/Schunder*, BB 2024, 75, 76.

99 Vgl. *Hembach*, Praxisleitfaden LkSG, III, S. 134.

100 Vgl. *Hembach*, Praxisleitfaden LkSG, III, S. 136.

fasst, sondern müssen nur in Sonderfällen, entsprechend § 9 Abs. 3 Nr. 1 LkSG, mit einbezogen werden.

Zu beachten ist, dass nicht der komplette Datenbestand an Vertragspartnern (unmittelbare Zulieferer) eines Unternehmens ungefiltert in eine menschenrechtliche und umweltbezogene Risikoanalyse überführt werden sollte. Vielmehr sollte vorab Transparenz über die Lieferketten und die Beschaffungsstruktur hergestellt werden.¹⁰¹ Diese vorab durchgeführte „Strukturanalyse“¹⁰² ermöglicht eine **Identifikation der erforderlichen unmittelbaren Zulieferer** und schont Zeit und Ressourcen. Weiter können sich Unternehmen im Rahmen der Folgemaßnahmen, aufgrund der Ergebnisse der Risikoanalyse, dann auch auf die erforderlichen unmittelbaren Zulieferer konzentrieren. Generell bleibt zu beachten, dass Unternehmen aufgrund der reinen Bemühenspflicht nicht alle Details über jeden Zulieferer komplett ausermitteln müssen.¹⁰³ 72

Inhaltlich müssen die **menschenrechtlichen Risiken** nach § 2 Abs. 2 LkSG 73 und die **umweltbezogenen Risiken** nach § 2 Abs. 3 LkSG eines Unternehmens ermittelt werden. Dabei bietet sich eine mehrschichtige Risikobetrachtung an. Neben einer **abstrakten Betrachtung** der Risiken, muss auch eine **konkrete Betrachtung** des eigenen Geschäftsbereichs¹⁰⁴ und der unmittelbaren Zulieferer durchgeführt werden.¹⁰⁵ Wobei letztere Betrachtungsweise einen deutlich höheren Aussagewert hat. Zusammengefasst führen beide Betrachtungsweisen zu einer umfassenden und angemessenen Risikoidentifizierung.

Kriterien für eine **abstrakte Betrachtung** von menschenrechtlichen und umweltbezogenen Risiken sind vor allem **länder- oder branchenspezifische Risiken**. 74 Dadurch können insbesondere Zulieferer mit einem hohen Grundrisiko identifiziert werden. Wie Unternehmen die abstrakten Risiken bestimmen müssen, lässt der Gesetzgeber offen. Das BAFA legt in seiner Handreichung zur Risikoanalyse mit verschiedenen Übersichten die aus seiner Sicht maßgeblichen Kriterien und Schritte für die verschiedenen Arten von Risikoanalysen dar und empfiehlt den Unternehmen, auf einer ersten Stufe die Risiken abstrakt zu betrachten (und insbesondere die branchen- und länderspezifischen Risiken zu untersuchen) und sodann auf der zweiten Stufe die Risiken konkret zu ermitteln und anhand der Kriterien für die Angemessenheit (§ 3 Abs. 2 LkSG) zu gewichten und zu priorisieren.¹⁰⁶ Unternehmen können im Rahmen der abstrakten Be-

101 Vgl. BAFA Handreichung Risikoanalyse, S. 10.

102 Vgl. Bartz/Schmidt/Lehne, CCZ 2024, 25, 26.

103 Vgl. Bartz/Schmidt/Lehne, CCZ 2024, 25, 26.

104 Vgl. BAFA Handreichung Risikoanalyse, S. 12 f.

105 Vgl. BAFA Handreichung Risikoanalyse, S. 14.

106 Siehe BAFA, Risikoanalyse: https://www.bafa.de/DE/Lieferketten/Risikoanalyse/risikoanalyse_node.html (zuletzt abgerufen am 8.9.2024), sowie zur Bedeutung der BAFA Handreichungen Harings/Beermann/Hörnig, CB 2023, 450 sowie Schröder/Schulz, Praxisleitfaden Supply Chain Compliance, Rn. 397 ff.

trachtung beispielsweise auf verschiedene Indizes, öffentlich verfügbare Quellen¹⁰⁷ oder Berichte von NGOs (z. B. die ILO) und der OECD¹⁰⁸ zurückgreifen. Auch der Einsatz von externen, spezialisierten Dienstleistern ist möglich. Je nach Anzahl der zu prüfenden Zulieferer kann dies aus praktischen Erwägungen, vor allem hinsichtlich der Anzahl an Quellen und deren Aktualität, nahezu zwingend sein.

- 75 Besonders für europäische Länder wird im internationalen Vergleich, aufgrund der hohen Arbeitsschutz- und Umweltvorschriften, grundsätzlich ein niedrigeres abstraktes Risiko anzunehmen sein.¹⁰⁹ Es verbietet sich jedoch auch für diese Länder oder Rechtsräume (bspw. die Europäische Union), keine abstrakte Risikobetrachtung vorzunehmen.
- 76 Es ist festzuhalten, dass eine abstrakte Betrachtung eine erste Indikation der Risiken bei den eigenen Zulieferern gibt. Dadurch werden Unternehmen befähigt, zunächst Gruppen von Zulieferern zu priorisieren und weiter potenzielle Risiken bei dieser Gruppe besser zu identifizieren.¹¹⁰ Folglich können im Anschluss daran auch die Präventions- und Abhilfemaßnahmen besser gesteuert und risikoorientiert angepasst werden. Wichtig bleibt, dass regionale Probleme nicht zwangsläufig dazu führen, dass sämtliche Zulieferer „bemäkelt“ und im schlimmsten Fall auszuschließen sind.¹¹¹
- 77 Unverzichtbar bleibt stets die **konkrete Betrachtung** der Risiken der eigenen Geschäftsbereiche und der unmittelbaren Zulieferer.¹¹² Es muss eine Einzelbetrachtung erfolgen, sinnvollerweise nach fest definierten und damit vergleichbaren Parametern. Hinsichtlich der Einzelbewertung der Risiken kann noch einmal spezifiziert werden. Neben der Eintrittswahrscheinlichkeit, der Schwere der Verletzung, dem Verursachungsbeitrag, kann beispielsweise auch das Einflussvermögen des Unternehmens herangezogen werden.¹¹³
- 78 In der Lieferkettenpraxis dürfte sich im Rahmen der konkreten Betrachtung die Befragung der unmittelbaren Zulieferer mittels Fragebögen oder Selbstauskünfte durchgesetzt haben.¹¹⁴ Generell sind diese nach Produkt und Branche und dabei teilweise nach einzelnen Arbeitsschritten in der Lieferkette zu unterteilen. Fragebögen an Zulieferer sollten risikoorientiert angepasst werden. Schlussendlich können die konkreten Risiken auf unterschiedlichen Ebenen der Lieferkette völlig unterschiedliche Ausprägungen haben.

107 Konkrete Hinweise auf Quellen zur Bestimmung abstrakter Risiken in: BAFA Handreichung Risikoanalyse, Anhang II, S. 20.

108 Vgl. Lorenz/Krülls, CCZ 2023, 100, 101.

109 Vgl. Kramer/Schunder, BB 2024, 75, 77.

110 Vgl. Lorenz/Krülls, CCZ 2023, 100, 101.

111 Vgl. Werner, CB 2023, 245, 246.

112 Vgl. BAFA Handreichung Risikoanalyse, S. 12.

113 Vgl. Kramme/Ponholzer, in: Berg/Kramme, LkSG, § 5 Rn. 7.

114 Auch Empfehlung der BAFA Handreichung Risikoanalyse, S. 11.

Um ein **Gesamtbewertung** der menschenrechtlichen und umweltbezogenen Risiken im eigenen Geschäftsbereich und bei den unmittelbaren Zulieferern vornehmen zu können, müssen die identifizierten Risiken aus der konkreten und abstrakten Betrachtungsweise zusammengeführt, in Beziehung gesetzt und gewichtet werden.¹¹⁵ Mindestangaben sollten dabei stets eine Risikobeschreibung, ein Verantwortlicher, die Gewichtung, sowie die Präventions- und Abhilfemaßnahmen sein.¹¹⁶ Ob die Bewertung in Form einer „Heat-Map“,¹¹⁷ eines „Scorings“, einer klassischen Risikobewertung (low/medium/high oder rot/gelb/grün¹¹⁸) oder durch eine andere Unterteilung erfolgt, ist unerheblich.

Bedeutsam ist nur, dass die Bewertung eine Gewichtung und **Priorisierung** der Risikofaktoren und der einzelnen Geschäftsbereiche und Zulieferer zulässt. Dabei ist im Rahmen der Bewertung stets der Perspektive des Rechtsträgers zu folgen¹¹⁹ und damit das höchste menschenrechtliche und umweltbezogene Risiko zu priorisieren.

Im Ergebnis sollten alle Folgemaßnahmen an den priorisierten Risiken ausgerichtet werden. Dies gilt generell für den eigenen Geschäftsbereich und die unmittelbaren Zulieferer, speziell aber vor allem für Präventions- und Abhilfemaßnahmen. Folglich kann und muss es im Unternehmen eine differenzierte Behandlung der eigenen Geschäftsbereiche geben. Dies gilt erst recht für die unmittelbaren Zulieferer. Eine abweichende Vorgehensweise, stellt die Risikoanalyse und die Priorisierung durch das Unternehmen infrage.

Konzeptionell sollte im Rahmen der Risikobewertung und damit auch der Risikopriorisierung immer darauf geachtet werden, dass ungewollt entstandene Unschärfen aufgrund der Methodik etc. ausgeglichen werden können (Expert Judgement). Die Gründe für eine abweichende Betrachtung sind zu dokumentieren.

(4) Regelmäßige und anlassbezogene Risikoanalyse

Die Risikoanalyse ist gemäß § 5 Abs. 4 LkSG einmal im Jahr¹²⁰ durchzuführen und ist damit auf eine gewisse **Regelmäßigkeit** angelegt. Es handelt sich um einen dynamischen Prozess, der die Entwicklungen des Unternehmens stets zu berücksichtigen hat.¹²¹ Ob die Risikoanalyse immer identisch durchzuführen oder in welchem Umfang die jährliche Analyse zu wiederholen ist, ist nicht geregelt. Dementsprechend kann sich die Risikoanalyse in verschiedenen Jahren oder in einem bestimmten Rhythmus nach Umfang und Analysetiefe unterscheiden.

115 Vgl. BAFA Handreichung Risikoanalyse, S. 12, 14.

116 Vgl. *Haag/Drodofsky*, CB 2024, 61, 65.

117 Vgl. BAFA Handreichung Risikoanalyse, S. 12.

118 Vgl. *Fitzer/Gergen*, CB 2022, 327, 332.

119 Vgl. *Fitzer/Gergen*, CB 2022, 327, 332.

120 Zu verstehen als „Geschäftsjahr“, vgl. *Wagner/Wagner*, in: *Wagner/Ruttloff/Wagner*, LkSG, Rn. 641.

121 Vgl. *Wagner/Ruttloff*, NJW 2021, 2145, 2148.

- 84 In bestimmten Fällen muss zudem eine **anlassbezogene Risikoanalyse** durchgeführt werden, um den dynamischen Veränderungen im Unternehmen gerecht zu werden. Hierzu gehören nach § 5 Abs. 4 LkSG beispielsweise die Einführung neuer Produkte, Projekte oder ein neues Geschäftsfeld. Erkenntnisse aus beim Unternehmen eingegangenen Hinweisen sind ebenfalls zu berücksichtigen. Die umstrittene Frage, inwieweit sich die anlassbezogene Risikoanalyse bei einer Veränderung der Geschäftstätigkeit auch auf mittelbare Zulieferer erstreckt, wird vom BAFA ausdrücklich bejaht.¹²²
- 85 Eine Anpassung der Risikoanalyse ist jedoch nur für **wesentliche Änderungen** vorzunehmen, vor allem dann, wenn das Unternehmen mit veränderten oder erweiterten Risikolagen in der Lieferkette rechnen muss.¹²³ Damit kommt es auf eine wesentliche Abweichung der bekannten Risikolage und damit des Status quo an.¹²⁴ Schlussendlich wird damit nur bei signifikanten Veränderungen im Unternehmen die Pflicht zur Anpassung der Risikoanalyse ausgelöst. Dies ist in der Praxis meist auch sinnvoll, um aufgebauten Prozessen Kontinuität zu verleihen. Damit werden die meist begrenzten Ressourcen geschont und Vertrauen bei den ausführenden Personen geschaffen. Für Fälle, in denen keine Anpassung zwingend ist, sollte dies dokumentiert werden.

(5) Unternehmensinterne Kommunikation der Risikoanalyse

- 86 Gemäß § 5 Abs. 3 LkSG hat das Unternehmen die Ergebnisse der Risikoanalyse intern an die maßgeblichen Entscheidungsträger zu kommunizieren. Hier nennt das Gesetz beispielhaft den Vorstand oder die Einkaufsabteilung.
- 87 In der Praxis dürfte diese Kommunikation keine wesentliche Rolle spielen, da die maßgeblichen Entscheidungsträger zumeist an der Risikoanalyse beteiligt sind oder zumindest Präventions- oder Abhilfemaßnahmen umzusetzen haben. Ein entsprechender Überblick über die Risiken dürfte bestehen. Was bleibt ist die Dokumentation der Kommunikation, um den gesetzlichen Vorgaben zu entsprechen.

dd) Abgabe einer Grundsatzerklärung (§ 3 Abs. 1 Nr. 4 LkSG)

- 88 Die **Grundsatzerklärung** ist gemäß § 6 Abs. 2 LkSG eine wesentliche Präventionsmaßnahme des Unternehmens. Zwar ist die Grundsatzerklärung streng genommen keine Maßnahme,¹²⁵ sie hat aber eine wichtige Funktion. In der Erklärung werden die Maßnahmen des Unternehmens zusammengefasst und von der

122 Siehe BAFA, Risikoanalyse, https://www.bafa.de/DE/Lieferketten/Risikoanalyse/risikoanalyse_node.html (zuletzt abgerufen am 8.9.2024), sowie BAFA-FAQ, Ziffer VIII.6. Ebenso Grabosch, in: Grabosch, Das neue Lieferkettensorgfaltspflichtengesetz, § 5 Rn. 58; a. A. Rothermel, LkSG, § 5 Rn. 49; Schröder/Schulz, Praxisleitfaden Supply Chain Compliance, Rn. 202.

123 Vgl. BT-Drs. 19/28649, Begründung zu § 5 Abs. 4.

124 Vgl. Wagner/Wagner, in: Wagner/Ruttloff/Wagner, LkSG, Rn. 646.

125 Vgl. Hembach, Praxisleitfaden LkSG, III, S. 156.

Unternehmensleitung bestätigt (Tone from the top). Schlussendlich handelt es sich um ein Bekenntnis zur Einhaltung der Menschenrechte und zur Etablierung einer Menschenrechtsstrategie durch das Unternehmen.

Wesentlicher Bestandteil der Grundsatzerklärung ist die **Menschenrechtsstrategie**. Diese soll die Selbstverpflichtung und das Engagement des Unternehmens zur Achtung der Menschenrechte und der umweltbezogenen Pflichten zum Ausdruck bringen.¹²⁶ Die implementierte menschenrechtliche und umweltbezogene Due Diligence im Unternehmen sollte sich in der Strategie widerspiegeln.¹²⁷ Das Gesetz zeigt insgesamt nur wenige beispielhafte Elemente auf, die sich in der Menschenrechtsstrategie wiederfinden müssen.

Hierzu gehört die Beschreibung der **Verfahren zur Einhaltung der wesentlichen Sorgfaltspflichten**.¹²⁸ Darüber hinaus sind die in der Risikoanalyse **festgestellten prioritären menschenrechtlichen und umweltbezogenen Risiken** aufzunehmen. Abschließend sind die **menschenrechtlichen und umweltbezogenen Erwartungen**, die das Unternehmen an seine Beschäftigten und Zulieferer in der Lieferkette richtet, festzulegen. Die Grundlage und den Startpunkt bildet die Risikoanalyse. Dabei sollen Standards und Maßstäbe festgelegt werden, die das Unternehmen an seine Beschäftigten und vor allem Zulieferer anlegt.¹²⁹

Praxisorientiert sollten Unternehmen zudem noch die Person des Menschenrechtsbeauftragten und deren Kontaktdaten in der Grundsatzerklärung nennen. Neben einer gewissen Transparenz können so themenspezifische Fragen von Stakeholdern schnell und zielgerichtet adressiert werden.

Insgesamt ist Unternehmen zu empfehlen, die Inhalte der Grundsatzklärung besonders sorgfältig zu prüfen. Durch die geforderte **Veröffentlichung**¹³⁰ ist die Erklärung ein wesentliches **Aushängeschild der menschenrechtlichen und umweltbezogenen Aktivitäten** eines Unternehmens. Daneben besteht durch die Veröffentlichung von fehlerhaften Angaben ein latentes Risiko des sog. „Greenwashings“. Im Ergebnis sollte sich die Erfüllung aller Sorgfaltspflichten und die gesamte Strategie und Herangehensweise zur Achtung der Menschenrechte und der Umwelt, in dieser Erklärung wiederfinden.

Die Grundsatzklärung und die Menschenrechtsstrategie sind jährlich beziehungsweise anlassbezogen zu überprüfen. Vorgaben der europäischen Lieferkettenregulierung (Corporate Sustainability Due Diligence Directive – CSDDD,¹³²

126 Vgl. BT-Drs. 19/28649, Begründung zu § 6 Abs. 2.

127 Vgl. *Kramer/Schunder*, BB 2024, 75, 77.

128 Vgl. § 6 Abs. 2 Nr. 1 LkSG.

129 Vgl. BT-Drs. 19/28649, Begründung zu § 6 Abs. 2 Nr. 3.

130 Vgl. BT-Drs. 19/28649, Begründung zu § 6 Abs. 2.

131 Vgl. *Zeidler/Dürr*, CCZ 2022, 377, 380.

132 Richtlinie (EU) 2024/1760 des Europäischen Parlaments und des Rates vom 13. Juni 2024 über die Sorgfaltspflichten von Unternehmen im Hinblick auf Nachhaltigkeit und zur Änderung der Richtlinie (EU) 2019/1937, ABl. L vom 5.7.2024, S. 1.

die bis zum 26.7.2026 umzusetzen ist) können gegebenenfalls direkt aufgenommen werden.¹³³

ee) Verankerung von Präventionsmaßnahmen (§ 3 Abs. 1 Nr. 5 LkSG)

- 94 Unternehmen sind verpflichtet, gemäß § 6 LkSG angemessene Präventionsmaßnahmen zu ergreifen, wenn im Rahmen der Risikoanalyse menschenrechtliche oder umweltbezogene Risiken identifiziert werden. Damit bauen die Präventionsmaßnahmen auf den Erkenntnissen der Risikoanalyse auf¹³⁴ und müssen im Unternehmen unverzüglich etabliert werden.¹³⁵
- 95 Die in § 6 LkSG beschriebenen Präventionsmaßnahmen gelten zunächst nur für den eigenen Geschäftsbereich und die unmittelbaren Zulieferer. Neben der Grundsatzerklärung (siehe → Rn. 88 ff.), als übergeordnete Präventionsmaßnahme, wird konsequent zwischen den Maßnahmen für den eigenen Geschäftsbereich und die unmittelbaren Zulieferer unterschieden.

(1) Präventionsmaßnahmen im eigenen Geschäftsbereich (§ 6 Abs. 3 LkSG)

- 96 Unternehmen haben bei der Verankerung von Präventionsmaßnahmen im eigenen Geschäftsbereich risikobasiert vorzugehen. Nicht jeder Geschäftsbereich muss gleich gewichtet werden. Vielmehr sind die Maßnahmen auf **risikorelevante Geschäftsbereiche** wie beispielsweise die Personalabteilung, die Logistik oder die Beschaffung bzw. den Einkauf auszurichten.¹³⁶
- 97 Als angemessene **Präventionsmaßnahmen im eigenen Geschäftsbereich** gelten die in § 6 Abs. 3 LkSG genannten, aber nicht abschließend aufgelisteten, Maßnahmen. Diese sind unverzüglich zu ergreifen, wenn Risiken festgestellt werden.¹³⁷
- 98 Unternehmen haben die in der Grundsatzerklärung dargestellte **Menschenrechtsstrategie** in den relevanten Geschäftsabläufen umzusetzen. Hierzu gehört vor allem die interne Kommunikation der Strategie sowie die Ausrichtung der Unternehmensprozesse auf die wesentlichen Kernpunkte.
- 99 Die wohl wichtigste, aber schwierigste Präventionsmaßnahme ist die Entwicklung und Implementierung von geeigneten **Beschaffungsstrategien und Einkaufspraktiken**, um Risiken zu verhindern oder zu minimieren. Unternehmen haben dementsprechend ihre Strategien und Prozesse zunächst auf ihren Einfluss auf Menschenrechte und die Umwelt zu überprüfen. Bergen diese menschenrechtliche oder umweltbezogene Risiken in sich, so muss im nächsten Schritt deren Anpassung geprüft werden. Idealerweise werden die wesentlichen Risiken durch unternehmensinterne und externe Verhaltensvorschriften und

133 Vgl. *Wagner/Wagner*, in: *Wagner/Ruttloff/Wagner*, LkSG, Rn. 601.

134 Vgl. *Hembach*, Praxisleitfaden LkSG, III, S. 156.

135 Vgl. BT-Drs. 19/28649, Begründung zu § 6 Abs. 1.

136 Vgl. BT-Drs. 19/28649, Begründung zu § 6 Abs. 3 Nr. 1.

137 Vgl. *Wagner/Wagner*, in: *Wagner/Ruttloff/Wagner*, LkSG, Rn. 675.

Leitlinien adressiert,¹³⁸ um bereits vor Vertragsabschluss Risiken zu erkennen.¹³⁹ Neben einem Verhaltenskodex und Richtlinien für relevante Bereiche, sind besonders für die Beschaffung und den Einkauf sog. „Responsible Purchasing Practices“ zu empfehlen. Bei der Umsetzung sollte risikobasiert und priorisiert vorgegangen werden.

Zudem haben Unternehmen **Schulungen** in allen relevanten Geschäftsbereichen durchzuführen. Diese können Teil des allgemeinen Schulungskonzepts im Unternehmen, beispielsweise der allgemeinen Compliance-Schulungen, sein. Thematisch sollte zunächst ein Grundbewusstsein für die wesentlichen Risiken in den entsprechenden Bereichen geschaffen werden. Anschließend sind die wesentlichen Risiken und deren Ausprägung in den Unternehmensabläufen zu thematisieren. Alle Schulungen sollten dokumentiert und regelmäßig (jährlich und anlassbezogen) wiederholt werden. 100

Schlussendlich sind **risikobasierte Kontrollmaßnahmen** bzgl. der Einhaltung der Menschenrechtsstrategie vorzunehmen. Beispielsweise durch die interne Auditierung von Prozessen oder die regelmäßige Kontrolle und Aktualisierung von Vorgaben.¹⁴⁰ Je nach Ergebnis, kann die Nachbesserung bestehender oder die Umsetzung neuer Präventionsmaßnahmen erforderlich sein.¹⁴¹ 101

(2) Präventionsmaßnahmen gegenüber unmittelbaren Zulieferern (§ 6 Abs. 4 LkSG)

Das Gesetz regelt die Präventionsmaßnahmen gegenüber unmittelbaren Zulieferern in § 6 Abs. 4 LkSG. Für viele Unternehmen mit langen Lieferketten und Produktionsprozessen müssen die Maßnahmen zur Minimierung der identifizierten Risiken in diesem Bereich Priorität haben. Deren Umsetzung und Verankerung ist aufgrund des Einflusses um ein Vielfaches schwerer als im eigenen Geschäftsbereich. Dementsprechend muss die Priorisierung von Risiken, ein risikobasiertes Vorgehen und die Angemessenheit der Maßnahmen im Vordergrund stehen. 102

Für Unternehmen, die bislang keine Präventionsmaßnahmen zur Minimierung von menschenrechtlichen oder umweltbezogenen Risiken implementiert haben, empfiehlt es sich, zunächst zwischen sich anbahnenden und etablierten Vertragsbeziehungen zu unterscheiden. Die erstmalige Weitergabe oder Vereinbarung von Präventionsmaßnahmen ist in der Praxis um ein Vielfaches einfacher als das Nachverhandeln in einem bestehenden Vertragsverhältnis. Eine starke Priorisierung sollte vorgenommen werden. 103

Als wesentliche Präventionsmaßnahme müssen Unternehmen im Rahmen der **Zuliefererauswahl** menschenrechtliche und umweltbezogene Risiken evaluie- 104

138 Vgl. BT-Drs. 19/28649, Begründung zu § 6 Abs. 3 Nr. 2.

139 Vgl. *Haag/Drodofsky*, CB 2024, 61, 65.

140 Vgl. BT-Drs. 19/28649, Begründung zu § 6 Abs. 3 Nr. 4.

141 Vgl. *Haag/Drodofsky*, CB 2024, 61, 65.

ren und diese berücksichtigen. Der Prozess soll fester Bestandteil einer Lieferantenbewertung sein.¹⁴² Wie die Auswahl oder Lieferantenbewertung schlussendlich organisiert wird, wie Risiken gewichtet werden oder welche Kriterien zu einem Ausschluss eines Zulieferers führen, bleibt jedem Unternehmen überlassen. Sicher dürfte jedoch sein, dass menschenrechts- und umweltbezogene Kriterien im Auswahlprozess zwingend berücksichtigt werden müssen.¹⁴³

- 105** Unternehmen sollen zudem die **menschenrechtlichen und umweltbezogenen Erwartungen an ihre unmittelbaren Zulieferer weitergeben** und sich die Einhaltung im eigenen Geschäftsbereich des Zulieferers vertraglich zusichern lassen. Die Vereinbarung einer „**Weitergabeklausel**“ soll nach der Begründung des LkSG für Unternehmen und auch unmittelbare Zulieferer ausreichend sein.¹⁴⁴
- 106** Im Rahmen der Weitergabe von Verpflichtungen gemäß dem LkSG müssen Unternehmen stets die **AGB-rechtliche Zulässigkeit** prüfen, sofern sie LkSG-Klauseln oder die Einbeziehung von Dokumenten (bspw. des Lieferantenkodex) als vorformulierte Vertragsbedingungen für eine Vielzahl von Verträgen nutzen.
- 107** Die generelle Einbeziehung eines Lieferantenkodexes oder LkSG-Klauseln, die lediglich den gesetzlichen Mindeststandard verlangen, dürften nach § 305c BGB keine überraschende Klausel darstellen und damit zumeist wirksam und zulässig sein.¹⁴⁵
- 108** Inhaltlich können alle Pflichten, die zur Einhaltung der Sorgfaltspflichten im Unternehmen notwendig sind, vereinbart werden. Die wesentlichen Inhalte sollten die festgestellten Risiken der Risikoanalyse beinhalten.¹⁴⁶ Gleiches gilt für die Erwartungen gegenüber Zulieferern mit Blick auf die Kooperationsbereitschaft oder die Weitergabe an die vorgelagerte Lieferkette.¹⁴⁷ Neben Anforderungen an Arbeitsbedingungen, Sozialstandards und Umweltstandards, können aber auch Nachweispflichten über die Herkunft oder die Produktionsweise von Produkten Teil der Vereinbarung sein.¹⁴⁸ Zu berücksichtigen bleibt, dass jede übertragene Pflicht an den geltenden Maßstäben der §§ 305 ff. BGB zu messen ist.
- 109** Besonders zu beachten ist das Transparenzgebot (§ 307 Abs. 1 Satz 2 BGB) und damit die klare und verständliche Formulierung der Rechte und Pflichten. Hervorzuheben sind vor allem die Definition von Begrifflichkeiten, die Erwartungen im Rahmen von Maßnahmen und die Bereitstellung des Gesetzestextes.¹⁴⁹

142 Vgl. BT-Drs. 19/28649, Begründung zu § 6 Abs. 4 Nr. 1.

143 Vgl. *Hembach*, Praxisleitfaden LkSG, III, S. 160.

144 Vgl. BT-Drs. 19/28649, Begründung zu § 6 Abs. 4 Nr. 2.

145 Vgl. *Wagner*, in: *Wagner/Ruttloff/Wagner*, LkSG, Rn. 2144.

146 Vgl. *Windoffer*, CB 2023, 93, 94.

147 Vgl. *Windoffer*, CB 2023, 93, 94.

148 Vgl. BT-Drs. 19/28649, Begründung zu § 6 Abs. 4 Nr. 2.

149 Umfassende Ausführungen, vgl. *Passas/Holtz*, BB 2023, 387, 388 f.

Die Verpflichtung von unmittelbaren Zulieferern die Vorgaben des Unternehmens in die tiefere Lieferkette weiterzugeben, wird generell als zulässig erachtet. Dies setzt jedoch voraus, dass die Formulierung eine Bemühenspflicht (Best-Efforts-Klausel) statuiert.¹⁵⁰ 110

Der Inhalt der weitergegebenen Erwartungen an die Lieferanten sollte regelmäßig auf deren rechtliche Zulässigkeit überprüft werden. Dadurch sichern sich Unternehmen nicht nur im Vertragsverhältnis zu ihren Lieferanten rechtlich ab, sondern kommen gleichzeitig ihren eigenen Sorgfaltspflichten nach § 3 Abs. 1 Satz 2 Nr. 5 Alt. 2 LkSG nach. Eine unwirksame Klausel würde im schlimmsten Fall dafür sorgen, dass die LkSG-konforme Verankerung der Präventionsmaßnahmen beim Lieferanten fehlt und eine Verletzung der eigenen LkSG-Sorgfaltspflichten vorliegt.¹⁵¹ 111

Unternehmen die üblicherweise Lieferantenkodizes erhalten, sollten die ihnen auferlegten Pflichten genau prüfen und falls möglich eigene Standards entwickeln oder beibehalten. Ein bloßes „Abzeichnen“ fremder Kodizes birgt das Risiko, sich einer zivilrechtlichen Verpflichtung mit entsprechenden Schadens- und Kündigungsansprüchen auszusetzen.¹⁵² 112

Weiter sollen **Schulungen und Weiterbildungen** die Durchsetzung der vertraglichen Zusicherungen des unmittelbaren Zulieferers sicherstellen.¹⁵³ Inhaltlich müssen diese die wesentlichen Risiken des unmittelbaren Zulieferers thematisieren. Diese Pflicht kann entweder dem unmittelbaren Zulieferer übertragen oder durch das verpflichtete Unternehmen sichergestellt werden. Letztere Option schafft den Vorteil, dass Unternehmen die Inhalte vorgeben und Nachweise deutlich einfacher erbracht werden können. Darüber hinaus ist die Außenwirkung nicht zu unterschätzen. 113

Schlussendlich müssen **angemessene Kontrollen** zur Einhaltung der Menschenrechtsstrategie sowie deren Durchführung vereinbart werden. Zulieferer können aufgefordert werden, ein angemessenes Management- und Kontrollsystem vorzuhalten.¹⁵⁴ Üblicherweise wird in der Praxis das Recht zur Auditierung von Zuliefererbetrieben durch eigene oder externe Prüfer vereinbart. Alternativ können aber auch Kontrollnachweise durch anerkannte Zertifizierungsnachweise oder Auditzertifikate erbracht werden.¹⁵⁵ Unternehmen sollen sich dabei besonders auf strategisch relevante Zwischenhändler und Zulieferer fokussieren.¹⁵⁶ Dies muss vor allem von Fall zu Fall beurteilt werden, wenn diese Zulieferer im Rahmen der Risikoanalyse als unauffällig eingestuft werden. 114

150 Vgl. *Passas/Holtz*, BB 2023, 387, 390; *Wagner*, in: *Wagner/Ruttloff/Wagner*, LkSG, Rn. 2222.

151 Vgl. *Passas/Holtz*, BB 2023, 387, 388.

152 Vgl. *Windoffer*, CB 2023, 93, 96.

153 Vgl. § 6 Abs. 4 Nr. 3 LkSG.

154 Vgl. *Windoffer*, CB 2023, 93, 95.

155 Vgl. BT-Drs. 19/28649, Begründung zu § 6 Abs. 4 Nr. 4.

156 Vgl. BT-Drs. 19/28649, Begründung zu § 6 Abs. 4 Nr. 4.

(3) Wirksamkeit und Aktualisierung der Präventionsmaßnahmen
(§ 6 Abs. 5 LkSG)

- 115 Die **Wirksamkeit** der Präventionsmaßnahmen ist anlassbezogen, mindestens aber einmal jährlich zu überprüfen. In der Praxis empfiehlt sich ein Fristenplan zur Überprüfung der Wirksamkeit¹⁵⁷ und zur Dokumentation. Maßnahmen sind bei Bedarf zu aktualisieren, vor allem wenn Hinweise darauf bestehen, dass diese den präventiven Charakter verloren haben oder nicht mehr geeignet sind. Dies gilt für die verankerten Präventionsmaßnahmen im eigenen Geschäftsbereich sowie bei den unmittelbaren Zulieferern. Erkenntnisse aus Hinweisen sind einzubeziehen und können Schwachstellen im bisherigen Maßnahmenset aufzeigen.

ff) Abhilfemaßnahmen (§ 3 Abs. 1 Nr. 6 LkSG)

- 116 Unternehmen haben im Rahmen der Sorgfaltspflichten in bestimmten Fällen **unverzüglich Abhilfemaßnahmen** zu ergreifen. Dies setzt eine Kenntnis der Unternehmensleitung oder einer verantwortlichen Stelle im Unternehmen voraus.¹⁵⁸
- 117 Gemäß § 7 Abs. 1 LkSG muss eine **Verletzung einer menschenrechtsbezogenen oder umweltbezogenen Pflicht** im eigenen Geschäftsbereich oder bei einem unmittelbaren Zulieferer **bereits eingetreten sein oder unmittelbar bevorstehen**. Grundlage bleiben die Erkenntnisse der unternehmenseigenen Risikoanalyse.¹⁵⁹ Ziel ist es die Verletzung noch zu verhindern, diese zu beenden oder das Ausmaß der Verletzung zu minimieren. Dabei gilt als Faustformel im Rahmen der Maßnahmen, dass je näher das Unternehmen zur Verletzung steht oder je mehr es zu ihr beigetragen hat, desto größer müssen die eigenen Anstrengungen sein, diese zu beenden.¹⁶⁰

(1) Abhilfemaßnahmen im eigenen Geschäftsbereich (§ 7 Abs. 1 LkSG)

- 118 Abhilfemaßnahmen im eigenen Geschäftsbereich müssen im **Inland** zur **Beendigung der Verletzung** führen. Im **Ausland** verbleibt ein geringer Spielraum. Hier soll die Abhilfemaßnahme in der Regel die Beendigung herbeiführen. Festgestellte Verletzungen müssen unverzüglich und mit angemessenen Mitteln beendet werden.
- 119 Dabei begründet **§ 7 Abs. 1 LkSG keine Anspruchsgrundlage** auf Schadensersatz oder sonstige Kompensation für einen Geschädigten gegenüber dem Unternehmen.¹⁶¹

157 Vgl. *Wagner/Wagner*, in: *Wagner/Ruttloff/Wagner LkSG*, Rn. 688.

158 Vgl. *Wagner/Wagner*, in: *Wagner/Ruttloff/Wagner, LkSG*, Rn. 691.

159 Vgl. BT-Drs. 19/28649, Begründung zu § 7 Abs. 1.

160 Vgl. BT-Drs. 19/28649, Begründung zu § 7 Abs. 1.

161 Vgl. BT-Drs. 19/28649, Begründung zu § 7 Abs. 1.

(2) Abhilfemaßnahmen bei einem unmittelbaren Zulieferer (§ 7 Abs. 2 LkSG)

Verletzungen bei einem unmittelbaren Zulieferer sind ebenfalls unverzüglich zu beenden. Ist dies in absehbarer Zeit nicht möglich, so muss das Unternehmen ein Konzept zur Beendigung oder Minimierung erstellen und dieses umsetzen (sog. „nachgelagerte Sorgfaltspflicht“¹⁶²). Dabei liegt die Pflicht zur Konzeptionierung beim Unternehmen. Eine Beteiligung des Lieferanten an der Erarbeitung und Umsetzung des Abhilfemaßnahmenkonzepts sollte vertraglich vorab vereinbart worden sein.¹⁶³

120

Kernbestandteile eines Konzepts sind die notwendigen praktischen Schritte zur Beendigung oder Minimierung der Verletzung und ein konkreter und verbindlicher Zeitplan. Das Konzept selbst kann inhaltlich gemeinsam mit dem unmittelbaren Zulieferer (Verletzer) ausgearbeitet und umgesetzt werden. Dabei ist stets auch ein temporäres Aussetzen der Geschäftsbeziehung während der Bemühungen zur Risikominimierung in Betracht zu ziehen. Darüber hinaus sollten Erwägungen Teil des Konzepts sein, wann ein Abbruch der Geschäftsbeziehung notwendig ist.¹⁶⁴ In manchen Fällen kann auch die zukünftige Teilnahme an Brancheninitiativen und Branchenstandards zur Erhöhung des Einflusses auf den Verursacher beitragen. In der Praxis dürfte diese Option nur in wenigen Fällen bestehen, da Unternehmen sich nicht in jedem Land der Lieferkette und damit wirksam, an Initiativen und Standardisierungen beteiligen können.

121

Der **Abbruch einer Geschäftsbeziehung** mit einem unmittelbaren Zulieferer ist auch bei einer menschenrechtsbezogenen oder umweltbezogenen Pflichtverletzung nicht zwingend, sondern stellt vielmehr die Ultima Ratio dar. Dies gilt besonders für sog. Single-Source-Lieferanten.¹⁶⁵ Generell müssen neben einer sehr schwerwiegenden Verletzung, die Abhilfemaßnahmen(pläne) erfolglos geblieben sein und keine anderweitigen, mildernden Mittel in Betracht kommen, um die Geschäftsbeziehung zwingend abbrechen zu müssen.¹⁶⁶ Damit kann vom Grundsatz des Vorrangs der menschenrechtlichen Nachbesserung ausgegangen werden.¹⁶⁷ Ein Abbruch der Geschäftsbeziehung aufgrund der bloßen Vermutung scheidet aus, da stets die Umstände des Einzelfalls entscheidend sind.¹⁶⁸

122

Tragend ist das Prinzip „**Befähigung vor Rückzug**“. Dementsprechend soll die Behebung von Missständen stets Vorrang vor dem Rückzug aus einem Geschäftsfeld haben.¹⁶⁹ Dies gilt selbst dann, wenn Staaten die in der Anlage des LkSG aufgelisteten Übereinkommen nicht ratifiziert oder in nationales Recht umgesetzt haben. Unternehmen wird dadurch in der Praxis ein weiterer Spielraum

123

162 Vgl. *Haag/Drozdofsky*, CB 2024, 61, 66.

163 Vgl. *Wagner/Wagner*, in: *Wagner/Ruttloff/Wagner*, LkSG, Rn. 766 f.

164 Vgl. BT-Drs. 19/28649, Begründung zu § 7 Abs. 2.

165 Vgl. *Wagner/Wagner*, in: *Wagner/Ruttloff/Wagner* LkSG, Rn. 776.

166 Vgl. *Wagner/Wagner*, in: *Wagner/Ruttloff/Wagner* LkSG, Rn. 771 ff.

167 Vgl. *Ehmann*, ZVertriebsR 2021, 141, 148.

168 Vgl. *Johann/Sangi*, in: *Gehne/Humbert/Philippi*, LkSG, § 7 Rn. 48, 64.

169 Vgl. BT-Drs. 19/28649, Begründung zu § 7 Abs. 3.

eröffnet, solange sie an der gezielten Verbesserung von Missständen arbeiten. Ob in der Praxis Unternehmen schlussendlich aus Kostengründen oder Gründen der Rechtssicherheit diesem Prinzip folgen oder den „Rückzug vor Befähigung“ wählen,¹⁷⁰ wird sich in Zukunft zeigen.

- 124 Der Abbruch der Geschäftsbeziehung ist nach § 7 Abs. 3 LkSG gesetzlich nur gefordert, wenn **kumulativ** eine schwerwiegende Verletzung der geschützten Rechtspositionen oder umweltbezogenen Pflichten (siehe → Rn. 21 f.) vorliegt, das Konzept in der vorgesehenen Zeit keine Abhilfe bewirkt und das Unternehmen keine mildernden Mittel zur Verfügung stehen bzw. eine Erhöhung des Einflussbereichs nicht aussichtsreich erscheint. In der Praxis dürften daher nur die schlimmsten Verletzungen und schwerwiegende Versäumnisse beim unmittelbaren Zulieferer zu einem zwingenden Abbruch der Geschäftsbeziehung führen.

(3) Wirksamkeit und Aktualisierung der Abhilfemaßnahmen (§ 7 Abs. 4 LkSG)

- 125 Im Rahmen der Wirksamkeit und Aktualisierung der Abhilfemaßnahmen kann auf die Ausführungen zu den Präventionsmaßnahmen (siehe → Rn. 115) analog verwiesen werden.

gg) Einrichtung eines Beschwerdeverfahrens (§ 3 Abs. 1 Nr. 7 LkSG)

- 126 Im Rahmen der Sorgfaltspflichten haben Unternehmen gemäß § 8 LkSG ein **Beschwerdeverfahren** einzurichten. Es ist zwingender Teil des LkSG-Risikomanagements im Unternehmen.¹⁷¹ Das BAFA hat diesbezüglich im Rahmen einer Handreichung detaillierte Informationen zur gesetzeskonformen Umsetzung zur Verfügung gestellt.¹⁷²
- 127 Die Bereitstellung des Beschwerdeverfahrens kann durch interne Ressourcen oder durch die Beauftragung eines externen Dienstleisters erfolgen. Gleichwertig sind auch unternehmensübergreifende Beschwerdeverfahren von Branchenverbänden.¹⁷³ Bereits im Unternehmen implementierte Beschwerdeverfahren können genutzt und erweitert werden. Dies setzt vor allem die Umsetzung der formellen Anforderungen nach § 8 Abs. 1–4 LkSG voraus, die Öffnung des Verfahrens für den betroffenen Personenkreis (auch Dritte) und die notwendige Fachkunde des zuständigen Personals. In der Praxis werden viele Unternehmen bestehende Synergien nutzen und das Beschwerdeverfahren, soweit möglich, in bestehende Strukturen überführen.
- 128 Durch das Beschwerdeverfahren sollen Personen (Mitarbeiter, Kunden etc.) **Hinweise auf menschenrechtsbezogene oder umweltbezogene Pflichtverlet-**

170 Vgl. Ecker, CCZ 2023, 69, 74.

171 Vgl. Wagner/Wagner, in: Wagner/Ruttloff/Wagner, LkSG, Rn. 651.

172 Siehe BAFA Handreichung Beschwerdeverfahren: https://www.bafa.de/SharedDocs/Downloads/DE/Lieferketten/handreichung_beschwerdeverfahren.pdf?__blob=publicationFile&v=4 (zuletzt abgerufen am 8.9.2024).

173 Vgl. BT-Drs. 19/28649, Begründung zu § 8 Abs. 1.

zungen geben können, die durch das Handeln eines Unternehmens im eigenen Geschäftsbereich oder einen unmittelbaren Zulieferer entstanden sind. Gemäß § 9 Abs. 1 LkSG sind auch Pflichtverletzungen durch das wirtschaftliche Handeln eines mittelbaren Zulieferers einzubeziehen. Folglich muss das Beschwerdeverfahren auch für Dritte zugänglich sein.¹⁷⁴

Unternehmen müssen das Beschwerdeverfahren **transparent** und damit klar und verständlich darstellen. Informationen über die Erreichbarkeit, die Zuständigkeit und die Durchführung des Verfahrens sind Minimumstandards. Weiter muss ein **öffentlicher und barrierefreier Zugang** gewährleistet sein. Zu bedenken sind neben einem vielfältigen Zugang (E-Mail, Internet, Telefon¹⁷⁵) auch der Abbau von Zugangshindernissen wie mangelnde Kenntnis des Mechanismus, Sprache, Lese- und Schreibvermögen, Kosten, Standort und Furcht vor Repressalien.¹⁷⁶ In der Praxis werden Unternehmen alle notwendigen Informationen zum Beschwerdeverfahren transparent auf der eigenen Unternehmenswebsite zur Verfügung stellen¹⁷⁷ und Konzepte für die weitere Verbreitung in der eigenen Lieferkette prüfen und erarbeiten. **129**

Der Umgang mit Hinweisen ist in einer **Verfahrensordnung** in Textform festzulegen und zu veröffentlichen. Wesentliche Bestandteile sollten der Anwendungsbereich, die Nennung der Beschwerdekanaäle, der Ablauf des Verfahrens, die Ansprechpersonen und der Schutz des Hinweisgebenden sein.¹⁷⁸ **130**

Dem Hinweisgebenden ist der Eingang des Hinweises zu bestätigen. Der Sachverhalt muss mit dem Hinweisgebenden erörtert werden. Für anonyme postalische Hinweise kann dies selbstverständlich nicht gelten. **131**

Wesentlich ist die Zusicherung zur **Vertraulichkeit der Identität** des Hinweisgebenden und der wirksame **Schutz vor Benachteiligung oder Bestrafung** aufgrund der Beschwerde. Beide Punkte sind unerlässlich für die Akzeptanz und das Vertrauen in ein robustes Beschwerdeverfahren im Unternehmen. Wie der Schutz der Hinweisgebenden bei Zulieferern sicherzustellen ist, bleibt zunächst offen. Idealerweise lassen sich Unternehmen den Schutz von Hinweisgebenden im Rahmen der Weitergabe der Sorgfaltspflichten zusichern (siehe oben → Rn. 105). **132**

Die Durchführung des Verfahrens muss im Unternehmen Personen übertragen werden, die unparteiisch handeln dürfen. **Unabhängigkeit und Weisungsfreiheit** sind sicherzustellen. Neben einem besonderen vertraglichen Kündigungsschutz kann auch die Weisungsunabhängigkeit im Arbeits- oder Dienstvertrag verankert werden.¹⁷⁹ Gleiches gilt für die Verpflichtung zur **Verschwiegenheit**. **133**

174 Vgl. *Nietsch/Wiedmann*, CCZ 2021, 101, 108.

175 Vgl. *Grabosch*, in: Grabosch, LkSG, § 5 Rn. 127.

176 Vgl. BT-Drs. 19/28649, Begründung zu § 8 Abs. 2, 3, 4.

177 Hinweise zum Beschwerdeverfahren im sog. „Footer“ der Unternehmenswebseite dürften sich durchsetzen.

178 Vgl. BAFA Handreichung Beschwerdeverfahren, S. 8.

- 134 Die **Wirksamkeit** des Beschwerdeverfahrens ist anlassbezogen, mindestens aber einmal jährlich zu überprüfen. Die Anforderungen an die Wirksamkeitsprüfung legt das BAFA in seiner Handreichung zum Beschwerdeverfahren dar.¹⁸⁰ KPIs könnten danach die Anzahl der Beschwerden, der Anteil an gelösten Beschwerden oder die durchschnittliche Bearbeitungszeit sein.¹⁸¹ Dabei ist zu beachten, dass das Referenzieren auf reine Fallzahlen erst über einen längeren Vergleichszeitraum eine Aussagekraft hat.

hh) *Risiken bei mittelbaren Zulieferern (§ 3 Abs. 1 Nr. 8 LkSG)*

- 135 Das LkSG kennt ein **Regel-Ausnahme-Prinzip**. Danach fallen der eigene Geschäftsbereich und die unmittelbaren Zulieferer eines Unternehmens in der Regel unter die meisten normierten Sorgfaltpflichten. Der mittelbare Zulieferer fällt nur in Ausnahmefällen unter bestimmte Regelungen des LkSG. Wesentlich für die Einbeziehung der mittelbaren Zulieferer und die konkreten Sorgfaltpflichten sind die Regelungen gemäß § 9 Abs. 3 LkSG.

(1) Substantiierte Kenntnis (§ 9 Abs. 3 LkSG)

- 136 Der mittelbare Zulieferer ist nur in Ausnahmefällen von den Regelungen des LkSG umfasst. Maßgeblich ist nach § 9 Abs. 3 LkSG die sog. „**substantiierte Kenntnis**“ des Unternehmens. Danach müssen tatsächliche Anhaltspunkte vorliegen, die eine menschenrechtsbezogene oder umweltbezogene Pflichtverletzung möglich erscheinen lassen. Es gelten die Grundsätze der Wissenszurechnung, auch im Konzern.¹⁸²
- 137 **Tatsächliche Anhaltspunkte** beinhalten zumindest einen **verifizierbaren Tatsachenkern**, bloße Meinungen oder Gerüchte schaffen keine substantiierte Kenntnis.¹⁸³ Unternehmen ist daher zu empfehlen, bei der eigenen Kenntniserlangung strukturiert vorzugehen. Neben Informationsquellen wie dem eigenen Beschwerdeverfahren,¹⁸⁴ sonstigen eigenen Erkenntnissen und Informationen der zuständigen Behörden, genügen auch Hinweise auf eine schlechte Menschenrechtslage in Produktionsregionen.¹⁸⁵ Dies würde bedeuten, dass Unternehmen die eigene Lieferkette und ihre mittelbaren Zulieferer kennen müssen. Damit würde sich faktisch die Verpflichtung der Unternehmen zur Kenntnis der gesamten Lieferkette erstrecken, um potenzielle Verstöße überhaupt identifizieren und entsprechende Maßnahmen ergreifen zu können. Ob Unternehmen tatsächlich Kenntnis über alle mittelbaren Zulieferer haben müssen bzw. erlangen können, erscheint fraglich.¹⁸⁶ Besonders mit Blick auf die Ziele des LkSG, die

179 Vgl. BAFA Handreichung Beschwerdeverfahren, S. 9.

180 Vgl. BAFA Handreichung Beschwerdeverfahren, S. 16 f.

181 Vgl. BAFA Handreichung Beschwerdeverfahren, S. 17.

182 Vgl. BAFA, LkSG-FAQ, VI., Nr. 13.

183 Vgl. BAFA, LkSG-FAQ, VI., Nr. 13.

184 Vgl. Stemberg, CCZ 2022, 92.

185 Vgl. BT-Drs. 19/28649, Begründung zu § 9 Abs. 3.

einen praktikablen, verhältnismäßigen und unbürokratischen Ansatz¹⁸⁷ für Unternehmen zugrunde legen, kann davon ausgegangen werden, dass die Kenntnis aller mittelbarer Zulieferer nicht mit den Gesetzeszielen übereinstimmt.

Unternehmen sollten insgesamt die **Kenntniserlangung aktiv steuern**. Hierzu gehört vor allem die Ermittlung der branchenrelevanten nationalen und internationalen Informationsquellen zum Thema Menschenrechte und Umweltschutz. Informationen von Multi-Stakeholder- oder Brancheninitiativen, wie beispielsweise Handreichungen, Falllisten oder Datenbanken sind zu beachten.¹⁸⁸ Diese sollten regelmäßig, idealerweise institutionalisiert abgefragt und geprüft werden. Die Ergebnisse sind zu dokumentieren. 138

Ob Unternehmen darüber hinaus noch weitere, **freiwillige Analysen** zur Menschenrechtslage durchführen, ist fraglich.¹⁸⁹ Schlussendlich lösen alle weiteren tatsächlichen Anhaltspunkte Pflichten aus, denen sich das Unternehmen nicht verschließen kann. 139

(2) Maßnahmen nach Erlangung von substantiierter Kenntnis (§ 9 Abs. 3 LkSG)

Sobald Unternehmen substantiierte Kenntnis über eine mögliche menschenrechtsbezogene oder umweltbezogene Pflichtverletzung erlangt haben, müssen diese unverzüglich, aber anlassbezogen handeln. 140

Verpflichtende Maßnahmen sind danach die Durchführung einer Risikoanalyse gemäß § 5 Abs. 1–3 LkSG. Die identifizierten Risiken sind angemessen zu gewichten und zu priorisieren.¹⁹⁰ Weiter sind angemessene Präventionsmaßnahmen gegenüber dem Verursacher zu verankern und ein Konzept zur Verhinderung, Beendigung oder Minimierung zu erstellen und umzusetzen. Welche Maßnahmen zu ergreifen sind, liegt im Ermessen des Unternehmens, das sich aber an § 6 Abs. 4 LkSG, den Präventionsmaßnahmen gegenüber unmittelbaren Zulieferern, orientieren soll.¹⁹¹ 141

Unternehmen ist zu empfehlen, sofern möglich, bereits ein Maßnahmenpaket zu definieren, welches im Fall der Fälle genutzt werden kann. Um dies effektiv um- und durchzusetzen, müssen bereits in den Verträgen mit den unmittelbaren Zulieferern die Weichen gestellt und ein Durchgriff ermöglicht werden (siehe oben → Rn. 105 f.). 142

186 Zu Kritik und Diskussionsstand siehe *Depping*, in: *Depping/Walden*, LkSG, 2022, § 9 Rn. 16 ff.

187 Vgl. BT-Drs. 19/28649, Zielsetzung, S. 23.

188 Vgl. BAFA, LkSG-FAQ, VI., Nr. 14.

189 Vgl. auch *Wüstemann/Büchner*, BB 2024, 579, 582.

190 Vgl. BT-Drs. 19/28649, Begründung zu § 9 Abs. 3 Nr. 1.

191 Vgl. BT-Drs. 19/28649, Begründung zu § 9 Abs. 3 Nr. 2.

- 143 Bei Bedarf ist zudem die Grundsatzerklärung anzupassen und zu aktualisieren.

ii) Dokumentation und Berichterstattung (§ 3 Abs. 1 Nr. 9 LkSG)

- 144 Unternehmen haben gemäß § 10 Abs. 1 LkSG umfassende Dokumentationspflichten. Diese haben in der Praxis eine erhebliche Bedeutung, um eventuell Nachweise bei Verstößen zu erbringen und die Erfüllung der Sorgfaltspflichten zu einem gewissen Zeitpunkt zu belegen. Auch die Berichtspflicht sollte von Unternehmen äußerst ernst genommen werden.

(1) Dokumentationspflichten (§ 10 Abs. 1 LkSG)

- 145 Die Erfüllung der Sorgfaltspflichten nach § 3 LkSG ist unternehmensintern **fortlaufend zu dokumentieren** und mindestens **sieben Jahre lang aufzubewahren**. Eine Pflicht zur Veröffentlichung besteht nicht.
- 146 Für international tätige Unternehmen stellt sich von Beginn an die Frage wie dokumentiert werden kann. Dies beinhaltet die Klärung der **Struktur** und der **Dokumentationssprache**. Idealerweise existiert ein Dokument, in dem alle wesentlichen Maßnahmen zur Erfüllung der Sorgfaltspflichten beschrieben werden, welches dann mit Verweisen auf Detailausführungen in Unterordnern etc. versehen werden kann. Als Dokumentationssprache sollte stets die Unternehmenssprache gewählt werden, auch wenn gegenüber dem BAFA die Amtssprache (Deutsch) gilt. Im Ergebnis ist eine ad-hoc Übersetzung bei eventuellen Anfragen der Behörde, sprachlichen Barrieren in der Zusammenarbeit zwischen Fachbereichen vorzuziehen.

(2) Berichtspflicht (§ 10 Abs. 2 LkSG)

- 147 Unternehmen haben zudem jährlich einen Bericht gemäß den Vorgaben des § 10 Abs. 2 LkSG zu erstellen und diesen kostenfrei für einen Zeitraum von sieben Jahren öffentlich zugänglich zu machen. Darüber hinaus ist der Bericht spätestens vier Monate nach dem Schluss des Geschäftsjahrs in elektronischer Form gemäß § 12 LkSG einzureichen (siehe unten → Rn. 154 ff.). Die Berichtssprache ist Deutsch.
- 148 **Betriebs- und Geschäftsgeheimnisse** müssen dabei gemäß § 10 Abs. 4 LkSG im Bericht nicht offengelegt werden. Unternehmen haben damit stets abzuwägen, welche Informationen sie offenlegen wollen und sich damit angreifbar für einen Know-how-Abfluss machen bzw. darauf verzichten und ein Bußgeldrisiko eingehen.¹⁹²

¹⁹² Vgl. *Passarge*, CB 2023, 171, 174.

III. Das BAFA als zuständige Behörde für die Kontrolle und Durchsetzung der Regelungen des LkSG

Das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) ist die **zuständige Behörde** für die Kontrolle und Durchsetzung der Regelungen des LkSG.¹⁹³ Bei der Wahrnehmung der gesetzlichen Aufgaben verfolgt das BAFA gemäß § 18 Abs. 2 LkSG einen risikobasierten Ansatz. Dementsprechend haben besonders Unternehmen in Hochrisiko-Sektoren (Lebensmittel, Fischerei, Holz, Textil- und Bekleidung, Förderung mineralischer Rohstoffe etc.¹⁹⁴) mit verstärkten Kontrollen zu rechnen. 149

1. FAQs, Handreichungen und sonstige Informationsquellen

Besonders im Rahmen der erstmaligen Implementierung der Sorgfaltspflichten sollten die vom BAFA bereitgestellten Informationsquellen genauestens geprüft werden. Um ein allgemeines Verständnis der gesetzlichen Regelungen herzustellen, stellt das BAFA umfassende Hinweise und Erläuterungen zur Auslegung des LkSG für Unternehmen zur Verfügung (**FAQ**).¹⁹⁵ 150

Daneben gehören besonders die **Handreichungen**¹⁹⁶ des BAFA zu verschiedenen Themengebieten zur „Pflichtlektüre“ für Compliance- und Umsetzungsverantwortliche im Unternehmen. Neben Erläuterungen zu verschiedenen Problemstellungen wird auch ein gewisser Erwartungshorizont an Unternehmen verschriftlicht. Dabei ist zu beachten, dass die behördliche Interpretation des LkSG nicht auf gefestigter Rechtsprechung basiert. Vielmehr haben die Handreichungen nach § 20 LkSG einen empfehlenden Charakter¹⁹⁷ und geben einen Hinweis auf die zukünftige Auslegungspraxis des BAFA.¹⁹⁸ Abweichungen von dieser Praxis sollten begründet werden, genau wie die alternativ gewählten Maßnahmen zur Sicherstellung der Sorgfaltspflichten.¹⁹⁹ 151

Insgesamt sollten sich die Kerninhalte der Handreichungen in den implementierten Sorgfaltspflichten wiederfinden. Da die Handreichungen teilweise über die gesetzlich normierten Regelungen hinausgehen, sollten diese jedoch vielmehr 152

193 Vgl. § 18 Abs. 1 LkSG.

194 Vgl. Einschätzung der Risikosektoren in den Entwürfen der CSDDD können entsprechend angewandt werden.

195 Siehe BAFA, Häufig gestellt Fragen (FAQ): https://www.bafa.de/DE/Lieferketten/FAQ/haeufig_gestellte_fragen_node.html (zuletzt abgerufen am 8.9.2024).

196 Vgl. § 20 LkSG, bisher veröffentlichte Handreichungen: Risikoanalyse, Beschwerdeverfahren, Angemessenheit, Zusammenarbeit in der Lieferkette und Kredit- und Versicherungswirtschaft (Stand 8.1.2024). Zu den Handreichungen siehe auch *Harings/Beermann/Hörnig*, CB 2023, 450.

197 Vgl. *Harings/Beermann/Hörnig*, CB 2023, 450, 451.

198 Vgl. *Rung/Wenzel*, in: Berg/Kramme, LkSG, § 20 Rn. 1.

199 Vgl. *Ecker*, ESG 2023, 254.

als Best-Practice-Beispiele und nicht als verbindliche und zwingende Umsetzungsanweisungen angesehen werden.²⁰⁰

- 153 Neben den vom BAFA bereitgestellten Informationen sind insbesondere die vom **Helpdesk für Wirtschaft und Menschenrechte** bereitgestellten Unterstützungsangebote für eine praxisnahe Umsetzung des LkSG zu empfehlen. Vor allem die kostenlose Beratung, der kostenfrei bereitgestellte CSR Risiko-Check (Risikoeinschätzung der Menschenrechtssituation für Branchen und Länder) und die Schulungs- und Informationsangebote²⁰¹ können bei der LkSG-Umsetzung hilfreich sein.

2. Berichtspflicht und Kontrollen

a) Elektronische Berichtspflicht der Unternehmen

- 154 Besonders bedeutsam für Unternehmen ist die **Berichtspflicht** nach § 10 Abs. 2 LkSG. Verpflichtete Unternehmen müssen sich auf einem vom BAFA bereitgestellten Online-Portal registrieren und haben der eigenen Berichtspflicht durch das Ausfüllen eines „elektronischen Berichtsfragebogens“ nachzukommen. Der Bericht ist in deutscher Sprache zu erstellen²⁰² und muss bis spätestens vier Monate nach Schluss des Geschäftsjahres eingereicht werden.²⁰³ Die erste faktische Verschiebung der Berichtspflicht bis zum 31.12.2024²⁰⁴ und die Diskussionen über deren generelle Aussetzung sind von Unternehmen zukünftig genau zu beobachten.
- 155 Zudem muss der Bericht auch spätestens vier Monate nach Schluss des Geschäftsjahres auf der Internetseite des Unternehmens für einen Zeitraum von sieben Jahren kostenfrei öffentlich zugänglich sein.²⁰⁵ Eine strukturierte und chronologische Darstellung der Berichte und eine Einbettung in die sonstigen Nachhaltigkeitsaktivitäten empfiehlt sich, um den administrativen Aufwand über die Jahre möglichst gering zu halten. Die Möglichkeit die LkSG-Berichtspflicht mit der nichtfinanziellen Berichterstattung nach dem HGB zu kombinieren, besteht nicht.²⁰⁶
- 156 Den **Mindestinhalt des Berichts** legt § 10 Abs. 2 LkSG fest. Unternehmen haben zunächst Angaben zu den identifizierten menschenrechtlichen und umweltbezogenen Risiken und Pflichtverletzungen zu machen. Weiter ist darzustellen welche Maßnahmen zur Erfüllung der eigenen Sorgfaltspflichten das Unterneh-

200 Vgl. *Ecker*, CCZ 2023, 69.

201 Siehe Helpdesk für Wirtschaft und Menschenrechte: <https://wirtschaft-entwicklung.de/wirtschaft-menschenrechte/> (zuletzt abgerufen am 8.9.2024).

202 Vgl. § 12 Abs. 1 LkSG.

203 Vgl. § 12 Abs. 2 LkSG.

204 Siehe BAFA, Berichtspflicht: https://www.bafa.de/DE/Lieferketten/Berichtspflicht/berichtspflicht_node.html (zuletzt abgerufen am 8.9.2024).

205 Vgl. § 10 Abs. 2 LkSG.

206 Vgl. *Bartz/Schmidt/Weber*, CCZ 2024, 172, 176.

men unternommen hat und wie die Auswirkungen und die Wirksamkeit derselbigen zu bewerten ist. Zuletzt ist noch über die Schlussfolgerungen aus dieser Bewertung für zukünftige Maßnahmen zu berichten.

Zwar legt das LkSG den Berichtsinhalt fest, Unternehmen haben sich jedoch **157** zwingend an den erweiterten Fragen des **elektronischen Berichtsfragebogens** zu orientieren. Die im Bericht bereitgestellten Fragen decken alle wesentlichen Maßnahmen der §§ 4–9 LkSG ab und sind durch Multiple-Choice Fragen und Freifelder zu beantworten. Welche Anforderungen das BAFA an Unternehmen hinsichtlich Beantwortungsumfang und Detailgrad hat, bleibt offen.

Da aufgrund der Struktur des BAFA-Berichtsfragebogen kaum Rückschlüsse **158** auf potenzielle Menschenrechtsverletzungen gezogen werden können²⁰⁷ und dies wahrscheinlich nicht das Ziel der Behörde war, sollten sich Unternehmen vielmehr auf die Umsetzungsmaßnahmen im Hinblick auf die eigenen Sorgfaltspflichten konzentrieren. Folglich wäre zunächst das eigene Maßnahmenkonzept zu beschreiben und einen strukturierten Überblick über die aufgesetzten Prozesse zu geben, um der Behörde eine umfassende und strukturierte Umsetzung aller Sorgfaltspflichten aufzuzeigen.

b) Kontrollbefugnisse des BAFA

Das LkSG hat dem BAFA umfassende **Kontrollbefugnisse** übertragen, um Verstöße gegen die gesetzlichen Verpflichtungen aus §§ 3–10 Abs. 1 LkSG festzu- **159** stellen, zu beseitigen und zu verhindern.²⁰⁸ Dabei kann gemäß § 14 Abs. 1 LkSG die Behörde entweder von Amts wegen oder muss auf Antrag tätig werden.

Im Rahmen des **behördlichen Tätigwerdens von Amts wegen**, kann die Ein- **160** haltung bestimmter Pflichten hinsichtlich menschenrechtlicher und umweltbezogener Risiken oder die Verletzung einer menschenrechts- und umweltbezogenen Pflicht von der Behörde kontrolliert werden. Gleiches gilt, wenn Verstöße festzustellen, zu beseitigen oder zu verhindern sind. Dabei steht der Behörde ein Ermessen hinsichtlich der Ermittlungen zu.

In der Praxis bedeutet dies, dass Unternehmen grundsätzlich immer mit einer risikobasierten Kontrolle zu rechnen haben, da die Behörde Hinweise aus den Medien, der Wissenschaft, dem eigenen Beschwerdekanal²⁰⁹ oder anderen Quellen nutzen kann. **161**

Wird ein **Antrag** nach § 14 Abs. 1 Nr. 2 LkSG gestellt, muss die Behörde tätig **162** werden. Nur bei der Auswahl der Mittel steht ihr weiterhin ein Ermessen zu.²¹⁰ Antragsberechtigt sind nach § 14 Abs. 1 Nr. 2 LkSG natürliche und juristische

²⁰⁷ Vgl. *Wüstemann/Büchner*, BB 2024, 579, 583.

²⁰⁸ Vgl. § 15 LkSG.

²⁰⁹ Siehe BAFA, Lieferketten, Beschwerde einreichen: https://www.bafa.de/DE/Lieferketten/Beschwerde_einreichen/beschwerde_einreichen_node.html (zuletzt abgerufen am 8.9.2024).

²¹⁰ Vgl. BT-Drs. 19/28649, Begründung zu § 14 Abs. 1.

Personen,²¹¹ die substantiiert geltend machen können durch die Nichterfüllung einer Pflicht in einer geschützten Rechtsposition verletzt worden zu sein oder deren Verletzung unmittelbar bevorsteht. Derzeit wird aufgrund des gesetzlichen Wortlauts davon ausgegangen, dass ausschließlich Verletzungen menschenrechtsbezogener Rechtspositionen ein Antragsrecht begründen.²¹² Damit kann beispielsweise Mitarbeitern von verpflichteten Unternehmen, Beschäftigten aus der Lieferkette sowie Gewerkschaften²¹³ ein Antragsrecht zustehen.

- 163 Um die behördlichen Kontrollbefugnisse bei Bedarf wahrzunehmen, bestehen gemäß § 16 LkSG umfassende **Einsichts- und Betretungsrechte**. Dabei ermächtigt § 16 Satz 1 LkSG nicht zur Durchsuchung.²¹⁴

c) Anordnungen und Maßnahmebefugnisse des BAFA

- 164 Um Verstöße gegen die Sorgfaltspflichten festzustellen, zu beseitigen oder zu verhindern, ist das BAFA gemäß § 15 Satz 1 LkSG befugt, geeignete und erforderliche Anordnungen und Maßnahmen zu treffen. Neben dieser **ordnungsrechtlichen Generalklausel**, können den verpflichteten Unternehmen weitere – nicht abschließend aufgezählte – Anordnungen und Maßnahmen aufgegeben werden.
- 165 Zu beachten ist vor allem die Anordnung, Unternehmen einen fristgebundenen Plan zur Behebung von Missständen und dessen Umsetzung aufzugeben. In Zukunft können verpflichtete Unternehmen damit rechnen, dass das BAFA vor allem von dieser Anordnung Gebrauch machen wird. Neben der Entlastung der Behörde, stellt diese Anordnung auch die effektivste Möglichkeit dar, Pflichtverletzungen schnellstmöglich zu beenden und Abhilfe zu schaffen.
- 166 Flankiert werden die Anordnungen und Maßnahmen des § 15 LkSG mit umfassenden **Auskunfts- und Herausgabepflichten**.²¹⁵ Generell haben Unternehmen gemäß § 18 LkSG die behördlichen Maßnahmen zu dulden und bei der Durchführung mitzuwirken.

IV. Sanktionen

- 167 Bedeutend für ein unternehmensinternes Compliance-Management-System ist die Beurteilung der Haftungsrisiken und Sanktionen bei Gesetzesverstößen. Das LkSG kennt einen umfassenden Katalog an Sanktionen, der bei nicht oder nicht ordnungsgemäßer Umsetzung der Sorgfaltspflichten von der zuständigen Behörde genutzt werden kann.

211 Vgl. Engel/Schönfelder, in: Grabosch, LkSG, § 6 Rn. 19.

212 Vgl. Ruttloff/Hahn, in: Wagner/Ruttloff/Wagner, LkSG, Rn. 1424.

213 Vgl. BT-Drs. 19/28649, Begründung zu § 14 Abs. 1.

214 Vgl. Rung/Wenzel, in: Berg/Kramme, LkSG, § 16 Rn. 16.

215 Vgl. § 17 LkSG.

1. Bußgeld und Bemessungsgrundlage

Die Verhängung eines **Bußgeldes** setzt die Begehung einer in § 24 Abs. 1 LkSG genannten Ordnungswidrigkeit voraus. Dabei orientiert sich das Gesetz konsequent an den umzusetzenden Sorgfaltspflichten²¹⁶ und setzt den Bußgeldrahmen entsprechend der Tragweite des Verstoßes fest. Nicht oder nicht rechtzeitig ergriffene Maßnahmen zur Prävention oder zur Abhilfe von Verstößen werden deutlich härter geahndet als beispielsweise Verfehlungen im Rahmen der Berichterstattung.²¹⁷ Folglich bemisst sich das Bußgeld auch nach Art des Verstoßes von 100.000 EUR bis zu maximal 8 Mio. EUR.²¹⁸ Nach § 24 Abs. 3 LkSG kann die Behörde in besonderen Fällen eine umsatzabhängige Geldbuße (bis zu 2% des durchschnittlichen Jahresumsatzes) verhängen.

Die Bemessung der Geldbuße orientiert sich insbesondere an den in § 24 Abs. 4 LkSG genannten Umständen und Verhaltensweisen. Für Unternehmen ist besonders das Nachtatverhalten von Bedeutung, kann es doch bei der Bemessung des Bußgelds mindernd berücksichtigt werden.

2. Ausschluss von der Vergabe öffentlicher Aufträge

Darüber hinaus können Unternehmen neben einem Bußgeld noch von der Vergabe öffentlicher Aufträge (sog. **Vergabesperre**) ausgeschlossen werden, wenn die Voraussetzungen nach § 22 LkSG vorliegen. Unerheblich bleibt, ob der Auftragswert den unionsrechtlich vorgegebenen Schwellenwert erreicht oder nicht.²¹⁹

Voraussetzung für einen Vergabeausschluss ist gemäß § 22 Abs. 2 LkSG eine Geldbuße aufgrund eines rechtskräftig festgestellten Verstoßes nach § 24 Abs. 1 LkSG, die wenigstens 150.000 EUR beträgt. Damit fallen Verstöße nach § 24 Abs. 1 Nr. 9–12 i.V.m. Abs. 2 Nr. 3 LkSG²²⁰ bereits aus dem Anwendungsbereich, da der Bußgeldrahmen bei 100.000 EUR endet. Zu beachten bleibt, dass ein Ausschluss vom Vergabeverfahren aufgrund § 22 LkSG nur bis zum Nachweis der Selbstreinigung möglich ist.²²¹

Der Ausschluss darf nur innerhalb eines angemessenen Zeitraums von bis zu drei Jahren erfolgen. Damit hat der Auftraggeber alle Umstände des Einzelfalls zu beachten (intendiertes Ermessen).²²²

216 Vgl. §§ 4–10 LkSG.

217 Vgl. § 24 Abs. 2 Nr. 1, 3 LkSG.

218 Vgl. § 24 Abs. 2 i.V.m. § 30 Abs. 2 Satz 3 OWiG.

219 Vgl. *Freund/Krüger*, NVwZ 2022, 665, 668.

220 Hierzu gehören: § 24 Abs. 1 Nr. 9 LkSG – Dokumentation nicht oder nicht mindestens sieben Jahre aufbewahrt; § 24 Abs. 1 Nr. 10 LkSG – Bericht nicht richtig erstellt; § 24 Abs. 1 Nr. 11 LkSG – Bericht nicht oder nicht rechtzeitig zugänglich gemacht; § 24 Abs. 1 Nr. 12 LkSG – Bericht nicht oder nicht rechtzeitig eingereicht.

221 Vgl. Übersicht zur Selbstreinigung bei LkSG-Verstößen – *Schröder*, CB 2023, 15, 17.

222 *Engel/Schönfelder*, in: Grabosch, LkSG, § 6 Rn. 51.

V. Zivilrechtliche Haftung und Prozessstandschaft

- 173 Eine zivilrechtliche Haftung für Sorgfaltspflichtenverletzungen sieht das Gesetz nicht vor.²²³ Es schließt jedoch die allgemeine zivilrechtliche – vertragliche oder deliktische – Haftung für Menschenrechtsverletzungen oder Umweltverschmutzung in der eigenen Lieferkette nicht aus. Dementsprechend bleibt die Haftung nach ausländischem Recht auch vor deutschen Gerichten weiter möglich.²²⁴
- 174 Um möglichen Opfern die eigene Rechtsdurchsetzung von deutschen Gerichten zu erleichtern, schaffte das LkSG eine besondere Prozessstandschaft in § 11 LkSG. Gewerkschaften und Nichtregierungsorganisationen (NGOs) können danach zur Prozessführung ermächtigt werden. Bisher hat sich, entgegen den Befürchtungen vieler Unternehmen und Verbände, noch kein erheblicher Nutzen dieser besonderen Prozessstandschaft abgezeichnet.

VI. Auswirkungen der europäischen Lieferkettenregelung (CSDDD) – Anpassung des LkSG

- 175 Auf europäischer Ebene kündigt sich mit der Einführung der europäischen Lieferkettenrichtlinie (Corporate Sustainability Due Diligence Directive, nachfolgend CSDDD)²²⁵ eine Veränderung des LkSG an. Die CSDDD wird den bisherigen Rechtsrahmen für Lieferketten erweitern und auch aufgrund des Umsetzungsanfordernisses in nationales Recht zu einer Neufassung des LkSG führen.
- 176 Der **Anwendungsbereich der CSDDD** wird sich ab 2027 auf EU- und Nicht-EU-Unternehmen mit über 1.000 Mitarbeitern und einem Jahresumsatz von mehr als 450 Mio. EUR erstrecken.²²⁶ Die CSDDD ist bis zum 26.7.2026 in nationales Recht umzusetzen und sieht einen gestaffelten Anwendungsbereich vor: Auf Unternehmen mit mehr als 5.000 Beschäftigten und einem Mindestjahresumsatz von 1,5 Mrd. EUR ist sie nach drei Jahren,²²⁷ auf Unternehmen mit über 3.000 Mitarbeitern und einem weltweiten Umsatz von über 900 Mio. EUR ist sie nach vier Jahren anwendbar.²²⁸ Nach fünf Jahren ist die CSDDD auf alle Unternehmen mit 1.000 Mitarbeitern und einem Jahresumsatz von mehr als 450 Mio. EUR anwendbar. Kleinere und mittlere Unternehmen sind von der CSDDD zwar nicht direkt betroffen. Ebenso wie beim LkSG werden die Sorgfaltspflichten

223 Vgl. § 3 Abs. 3 LkSG.

224 Vgl. *Schröder/Schulz*, Praxisleitfaden Supply Chain Compliance, Rn. 431.

225 Richtlinie (EU) 2024/1760 des Europäischen Parlaments und des Rates vom 13. Juni 2024 über die Sorgfaltspflichten von Unternehmen im Hinblick auf Nachhaltigkeit und zur Änderung der Richtlinie (EU) 2019/1937, ABl. L vom 5.7.2024, S. 1.

226 Vgl. Art. 37 Abs. 1 lit. a und lit. c CSDDD.

227 Vgl. Art. 37 Abs. 1 lit. b CSDDD.

228 Vgl. Art. 37 Abs. lit. 1 lit. d CSDDD.

aber auch hier vermutlich von größeren Unternehmen weitergereicht werden („Trickle down“-Effekt).²²⁹

Die Sorgfaltspflichten der CSDDD werden über den Pflichtenbereich des LkSG deutlich hinausgehen.²³⁰ So ist etwa Bezugspunkt für die Sorgfaltspflichten bei der CSDDD nicht wie beim LkSG die Lieferkette, sondern die sog. „**Aktivitätskette**“,²³¹ die nicht nur vorgelagerte Schritte („upstream“), sondern auch nachgelagerte Schritte („downstream“) umfasst (bspw. Tätigkeiten der nachgelagerten Geschäftspartner im Zusammenhang mit dem Vertrieb). 177

Die von der CSDDD einbezogenen **Schutzgüter** werden im Vergleich zum LkSG noch einmal deutlich erweitert. Diese gilt sowohl für die menschenrechtlichen²³² als vor allem auch für die umweltbezogenen Schutzgüter.²³³ 178

Dagegen ähneln viele **Sorgfaltspflichten** denen des LkSG. Gemäß den Art. 7–11 CSDDD haben Unternehmen grundsätzlich (1) die Einbeziehung der Sorgfaltspflicht in die Unternehmenspolitik und die Risikomanagementsysteme sicherzustellen, (2) negative Auswirkungen ihrer Geschäftstätigkeit zu identifizieren und zu bewerten, (3) Auswirkungen zu priorisieren und Maßnahmen zu ergreifen. Elemente wie die Risikoanalyse, Präventions- und Abhilfemaßnahmen, das Beschwerdeverfahren oder die Berichtspflicht sind bereits aus dem LkSG bekannt. Neu hingegen ist die Erstellung und Umsetzung eines sogenannten Klimaschutzplans. 179

Wesentliche Veränderungen werden sich auch im Rahmen der **Sanktionen** ergeben.²³⁴ Die Mitgliedstaaten haben nach Art. 27 CSDDD Sanktionen für Verstöße, einschließlich Zwangsgeldern zu erlassen, wobei sich die Höhe der Zwangsgelder nach dem weltweiten Nettoumsatz des Unternehmens richten soll und bis zu 5% des weltweiten Nettoumsatzes des Unternehmens im Geschäftsjahr vor der Entscheidung über die Verhängung des Zwangsgelds betragen kann.²³⁵ 180

Neu wird auch die **zivilrechtliche Haftung** im Rahmen der CSDDD sein.²³⁶ Die Haftung eines Unternehmens tritt ein, wenn eine Rechtsgutsverletzung unmittelbar aus der Nichteinhaltung von Sorgfaltspflichten durch das Unternehmen resultiert.²³⁷ Eine Haftung für die Aktivitäten der Geschäftspartner in der Aktivitätskette ist ausgeschlossen.²³⁸ 181

229 Vgl. Bartz/Schmidt/Lehne, CCZ 2024, 172, 174; Schröder/Schulz, Praxisleitfaden Supply Chain Compliance, Rn. 1.

230 Vgl. Schäfer/Schütze, BB 2024, 1091, 1094.

231 Vgl. Art. 3 Abs. 1 lit. g i) CSDDD.

232 Vgl. Anhang Teil I CSDDD.

233 Vgl. Anhang Teil II CSDDD.

234 Vgl. Schäfer/Schütze, BB 2024, 1091, 1094.

235 Vgl. Art. 27 Abs. 4 CSDDD.

236 Vgl. Art. 29 CSDDD.

237 Vgl. Bartz/Schmidt/Lehne, CCZ 2024, 172, 175.

238 Vgl. Art. 29 Abs. 1 CSDDD.

- 182** Mit Blick auf die Praxis bleibt abzuwarten, wie die Regelungen der CSDDD konkret in nationales Recht überführt werden. Festzustellen ist, dass weitere Anforderungen auf die betroffenen Unternehmen zukommen. Bereits nach dem LkSG verpflichtete Unternehmen werden aber bereits diverse Anforderungen an das neue Lieferketten-Compliance-System umgesetzt haben und profitieren durch die Erstreckung der CSDDD auf Unternehmen außerhalb der EU zukünftig erstmals von einer Gleichbehandlung von Unternehmen in der EU (sog. „Level-Playing-Field“).

19. Kapitel

Menschenrechtsbeauftragte und Beschwerdebeauftragte nach dem LkSG

I. Einleitung

Das Lieferkettensorgfaltspflichtengesetz (LkSG) fügt der Liste der Beauftragten im Unternehmen¹ zwei weitere hinzu, nämlich die Menschenrechtsbeauftragten und die Beschwerdebeauftragten. Nachfolgend wird aufgezeigt, was sich hinter den neuen Begrifflichkeiten verbirgt, mit welchen Aufgaben sie betraut werden, welche Qualifikationen sie mitzubringen haben, wie sie organisatorisch einzubinden sind, ob ihnen arbeitsrechtliche Sonderrechte zustehen und wie sie für ihre Tätigkeiten haften.

II. Menschenrechtsbeauftragte

1. Begrifflichkeiten und gesetzliche Grundlagen

Der Begriff des Menschenrechtsbeauftragten wird im LkSG lediglich an einer Stelle verwendet, nämlich in § 4 Abs. 3 in Verbindung mit der Überwachung des Risikomanagements. Danach „hat das Unternehmen dafür zu sorgen, dass festgelegt ist, wer innerhalb des Unternehmens dafür zuständig ist, das Risikomanagement zu überwachen, etwa durch die Benennung eines Menschenrechtsbeauftragten“.

Darüber hinaus gibt es nur zwei weitere direkte Anknüpfungspunkte im LkSG an die betriebsinterne Überwachungszuständigkeit. Nach § 3 Abs. 1 Satz 2 Nr. 2 LkSG ist die Festlegung der betriebsinternen Zuständigkeit im Sinne von § 4 Abs. 3 LkSG eine menschenrechtliche und umweltbezogene Sorgfaltspflicht und in § 4 Abs. 3 Satz 2 LkSG wird zudem gefordert, dass sich die Geschäftsleitung regelmäßig, mindestens einmal jährlich über die Arbeit der zuständigen Person oder Personen zu informieren hat.

Durch die Verwendung des Wortes „etwa“ schreibt das Gesetz nicht vor, dass die betriebsinterne Zuständigkeit zwingend Menschenrechtsbeauftragter genannt werden muss. Ebenso empfiehlt die Gesetzesbegründung² lediglich, dass „die Einrichtung der Stelle eines Menschenrechtsbeauftragten, die unmittelbar der Geschäftsleitung unterstellt ist, zu empfehlen ist“, wenngleich an späterer Stelle auch von der Pflicht zur Bestellung eines Menschenrechtsbeauftragten gesprochen wird.³

1 Bspw. Datenschutzbeauftragte, Geldwäschebeauftragte, Arbeitsschutzbeauftragte, Umweltschutzbeauftragte (u. a. Immissionsschutz-, Strahlenschutz-, Gewässerschutz-, Abfall- und Gefahrgutbeauftragte).

2 BT-Drs. 19/28649, S. 43.

3 BT-Drs. 19/28649, S. 62.

- 5 Da die Benennung einer betriebsinternen Zuständigkeit eine menschenrechtliche und umweltbezogene Sorgfaltpflicht des Unternehmens ist⁴ und die Überwachungspflicht der zuständigen Person(en) sich sowohl auf menschenrechtliche Risiken als auch auf umweltbezogene Risiken bezieht, wäre die Bezeichnung „**Menschenrechts- und Umweltbeauftragter**“ zutreffender.⁵ Dies umso mehr, als die EU-Richtlinie über die Sorgfaltpflichten von Unternehmen im Hinblick auf Nachhaltigkeit (EU Directive on Corporate Sustainability Due Diligence, nachfolgend „CS3D“)⁶ den Katalog der umweltbezogenen Verbote und Verpflichtungen erheblich ausdehnt.⁷ Dies ist auch vom Gesetzgeber bei einer Integration der Vorgaben der CS3D in das LkSG zu berücksichtigen.⁸ Letztlich kommt es auf die tatsächliche Bezeichnung aber nicht an, solange zumindest eine Person benannt ist, die für die Überwachung des LkSG-Risikomanagements zuständig ist. In der Praxis hat sich jedoch die Bezeichnung Menschenrechtsbeauftragte durchgesetzt.⁹
- 6 Das Gesetz ermöglicht es auch, dass mehrere zuständige Personen ernannt werden, da § 4 Abs. 3 Satz 2 LkSG vorsieht, dass „sich die Geschäftsleitung regelmäßig, mindestens einmal jährlich, über die Arbeit der zuständigen Person oder Personen zu informieren hat“. Mit der Überwachung des LkSG-Risikomanagement kann also auch ein Menschenrechts-Komitee¹⁰ oder Menschenrechtsüberwachungsausschuss¹¹ beauftragt werden. Verschiedene Unternehmen haben dies auch getan.¹² Ebenso ist es denkbar, die Überwachung im Hinblick auf die menschenrechtsbezogenen und die umweltbezogenen Pflichten zu trennen,¹³ was Unternehmen auch schon praktisch umgesetzt haben.¹⁴ Letztlich kommt es nicht auf die Bezeichnung des oder der Zuständigen für die Überwachung des LkSG-

4 § 3 Abs. 1 Satz 1 LkSG.

5 So auch *Ruttloff/Wagner/Hahn/Freihoff*, CCZ 2022, 20, 22.

6 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401760 (zuletzt abgerufen am 17.8.2024).

7 Art. 15 CS3D sieht zwar die Überwachung des Risikomanagements vor, ohne jedoch Vorgaben für die Umsetzung durch die Unternehmen zu machen.

8 Vgl. die Verpflichtung der Bundesregierung bei der Evaluierung des LkSG unter Berücksichtigung der CS3D, BT-Drs. 19/28649, S. 32; ausführlich zur Anpassung des LkSG aufgrund der CS3D: *Hagel/Wiedmann*, CCZ 2024, 185 ff.

9 So haben u. a. fast alle Unternehmen der deutschen Automobilindustrie einen Menschenrechtsbeauftragten ernannt, bspw. Audi, BMW, Daimler Truck, Mercedes Benz und VW.

10 DICO Standard S16 – Lieferketten-Compliance-Management-System (L-CMS), https://www.dico-ev.de/wp-content/uploads/2022/08/S16_Lieferketten_CMS_2022_web.pdf (abgerufen am 1.7.2024).

11 *Harings/Jürgens*, LkSG, S. 93, für ein Gremium auch: *Herrmann/Rünz*, DB 2021, 3078, 3080.

12 Vgl. bspw. KION Group (Grundsatzerklärung vom 1.1.2023); Stadtwerke Düsseldorf, <https://www.swd-ag.de/ueber-uns/unternehmen/lieferkettengesetz/>; Traton, <https://traton.com/de/newsroom/stories/sensibilisierung-und-aktionen-ein-jahr-traton-menschenrechtsausschuss.html> (beide Quellen zuletzt abgerufen am 1.7.2024).

13 Vgl. hierzu: *Harings/Jürgens/Thalhammer*, CB 2022, 93 ff.

14 Vgl. bspw. Heidelberg Materials, Bericht zum LkSG vom 29.5.2024, S. 1.

Risikomanagements an,¹⁵ sondern auf die Tatsache, dass dafür eine oder mehrere Personen festgelegt wurden.¹⁶ Dies wird unterstrichen durch die Bußgeldbewehrung in § 24 Abs. 1 Nr. 1 LkSG, wonach das Versäumen der Festlegung eines Zuständigen für die Überwachung des LkSG-Risikomanagements nach § 4 Abs. 3 LkSG als Ordnungswidrigkeit geahndet und mit einem Bußgeld von bis zu 5 Mio. EUR belegt ist.¹⁷

Unabhängig davon, wie sich das Unternehmen entscheidet, und ohne dies zu präjudizieren, wird im Folgenden nur auf den Menschenrechtsbeauftragten Bezug genommen. 7

2. Überwachungsaufgaben

Die vom LkSG vorgesehene Aufgabe¹⁸ des Menschenrechtsbeauftragten ist die Überwachung der Angemessenheit und Wirksamkeit des LkSG-Risikomanagements, ohne dass näher beschrieben wird, ob er weitere beratende oder unterstützende Aufgaben wahrnehmen kann. 8

Zwar könnte seine Bezeichnung als „Beauftragter“ nahelegen, dass er auch in die Umsetzung der Sorgfaltspflichten involviert werden kann, doch dürfte dies zu Interessenkonflikten mit seiner Überwachungsaufgabe führen.²⁰ 9

Daher ist es sinnvoll, die Überwachungsaufgabe entsprechend dem Drei-Linien-Modell („**Three Lines Linie Model**“) einzuordnen.²¹ Folglich ist der Menschenrechtsbeauftragte für die Überwachung des LkSG-Risikomanagements der ersten²² und zweiten²³ Linie verantwortlich und führt risikobasiert Kontrollmaßnahmen durch. Zudem informiert er mindestens einmal jährlich die Geschäfts- 10

15 Aus Gründen der Transparenz wird aber eine Bezeichnung, aus der die Rolle der zuständigen Person(en) hervorgeht, empfohlen: *Harings/Jürgens/Thalhammer*, CB 2022, 93 ff.

16 Vgl. hierzu: *Hagel/Wiedmann*, BB 2023, Heft 19, Umschlagteil, I.

17 § 24 Abs. 2 Satz 1 Nr. 2 LkSG i.V.m. § 24 Abs. 2 Satz 2 LkSG, § 30 Abs. 2 Satz 3 OWiG.

18 Umfassende Aufgabenbeschreibung findet sich in *Hagel/Wiedmann*, Menschenrechtsbeauftragte, 2024.

19 Siehe hierzu *Häfeli*, ARP 2021, 299, 300.

20 Vgl. *Ghassemi-Tabar*, in: *Ghassemi-Tabar*, LkSG, § 4 Rn. 57, ebenso *Harings/Jürgens/Thalhammer*, CB 2022, 93, 94; a. A. *Bertke/Sandbrink*, NJW 2024, 319, 320 f.

21 Ausführlich *Ghassemi-Tabar*, in: *Ghassemi-Tabar*, LkSG, § 4 Rn. 58.

22 Die erste Verteidigungslinie besteht aus allen Fachbereichen des operativen Geschäfts, auf deren Tagesgeschäft sich unternehmerische Risiken auswirken können. Sie sind dafür zuständig, Risiken in ihrem Bereich frühzeitig zu erkennen, zu beurteilen, zu steuern, zu überwachen und zu reduzieren. Zur ersten Verteidigungslinie gehören in Bezug auf das LkSG insbesondere die Fachbereiche Einkauf, Personal, EHS.

23 Die zweite Verteidigungslinie umfasst alle Bereiche, die das operative Geschäft steuern und überwachen. Hierzu gehören die Festlegung von Methoden und Verfahren für das Risikomanagement, die Vorgaben durch Leit- und Richtlinien sowie das Reporting an die Unternehmensleitung. Zur zweiten Verteidigungslinie gehören in Bezug auf das LkSG insbesondere die Fachbereiche Compliance, Recht und Risikomanagement.

Teil 2 Übergreifende Themen und Herausforderungen – ESG und Governance

leitung über diese Aktivitäten.²⁴ Allerdings unterliegen er und sein Überwachungs- und Informationsprozess selbst der objektiven und unabhängigen Prüfungsinstanz der Internen Revision, sodass er zwischen der zweiten und dritten Linie anzusiedeln ist, quasi auf Linie 2,5.²⁵

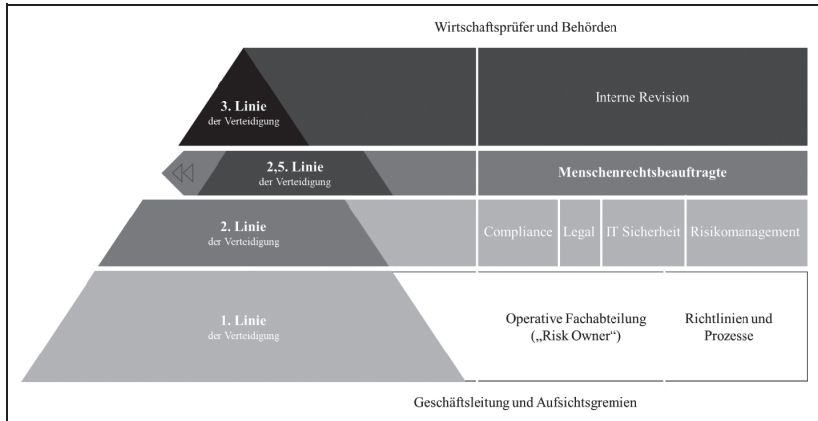


Abbildung 1: Der Menschenrechtsbeauftragte im Drei-Linien-Modell²⁶

- 11 Damit ist aber ausgeschlossen, dass der Menschenrechtsbeauftragte sowohl für die operative Umsetzung des Risikomanagements als auch für dessen Überwachung im Sinne eines zweigliedrigen Systems zuständig sein kann.²⁷ Dies könnte zu Interessenkonflikten führen, weshalb diese Frage auch regelmäßig Gegenstand des erweiterten Auskunftersuchens des BAFA ist.
- 12 Kein Interessenkonflikt dürfte vorliegen, wenn der Menschenrechtsbeauftragte neben seiner Überwachungsaufgabe LkSG-bezogene Mitarbeiterschulungen durchführt, an der Ausarbeitung der Grundsatzerklärung oder bei Abhilfemaßnahmen mitwirkt oder die Berichtspflicht koordiniert, da er bei diesen Aktivitäten seine Erkenntnisse aus der Überwachung des Unternehmens einfließen lassen kann. Dies setzt voraus, dass ihm dabei keine Entscheidungsbefugnisse eingeräumt werden.²⁸

²⁴ Vgl. § 4 Abs. 3 Satz 2 LkSG.

²⁵ So auch die Organisation bei Volkswagen, abrufbar unter <https://www.volkswagen-groupservices.com/ueber-uns/menschenrechte> (zuletzt abgerufen am 1.7.2024). Ausführlicher dazu: Hagel/Wiedmann, Menschenrechtsbeauftragte, S. 119 f.

²⁶ Abbildung aus Hagel/Wiedmann, Menschenrechtsbeauftragte, S. 121.

²⁷ Vgl. Ghassemi-Tabar, in: Ghassemi-Tabar, LkSG, § 4 Rn. 56.

²⁸ Ebenso im Hinblick auf Schulungen und Grundsatzerklärung Harings/Jürgens/Thalhammer, CB 2022, 93, 95; Hagel/Wiedmann, Menschenrechtsbeauftragte, S. 60 f.

Zur Erfüllung seiner Überwachungsaufgabe sollte der Menschenrechtsbeauftragte einen Jahresplan²⁹ erstellen, anhand dessen er das Vorliegen der folgenden LkSG-Vorgaben überprüft: **13**

1. Vorliegen einer regelmäßigen oder mindesten jährlichen Berichterstattung an die Geschäftsleitung (§ 4 Abs. 3 Satz 2 LkSG);
2. Verankerung des Risikomanagements in den maßgeblichen Geschäftsabläufen;³⁰
3. Überwachung der jährlich bzw. anlassbezogen durchzuführenden Risikoanalyse (§ 5 Abs. 4 Satz 1 LkSG);
4. Vorhandensein bzw. Aktualisierung der Grundsatzerklärung (§ 6 Abs. 2 LkSG);
5. Jährliche bzw. anlassbezogene Wirksamkeitsprüfung
 - a) der Präventionsmaßnahmen (§ 6 Abs. 5 Satz 1 LkSG),
 - b) der Abhilfemaßnahmen (§ 7 Abs. 4 Satz 1 LkSG),
 - c) des Beschwerdeverfahrens (§ 8 Abs. 5 Satz 1 LkSG);
6. Umsetzung von Sorgfaltspflichten in Bezug auf Risiken bei mittelbaren Zulieferern;
7. Dokumentation der Sorgfaltspflichten sowie ihre Aufbewahrung (§ 10 Abs. 1 LkSG);
8. Überwachung der jährlichen Berichtspflicht im Hinblick auf Vollständigkeit und Richtigkeit (§ 10 Abs. 2 LkSG).

3. Anforderungen an Menschenrechtsbeauftragte

a) Qualifikation

Das LkSG enthält keine speziellen Anforderungen zur Qualifikation des Menschenrechtsbeauftragten. Somit gelten die allgemeinen Organisations- und Aufsichtspflichten nach § 130 OWiG. Der Menschenrechtsbeauftragte muss in Bezug auf seine Aufgaben ordnungsgemäß ausgewählt werden und hinreichend qualifiziert sein. Dies erfordert die fachliche Sachkunde, Erfahrung und Vorbildung. Hinsichtlich seiner Tätigkeiten muss er zudem ordnungsgemäß instruiert und mit den notwendigen Ressourcen (Zeit, Geld und Personal)³¹ ausgestattet sein, um die angemessene Überwachung zu gewährleisten.³² **14**

Die Position des Menschenrechtsbeauftragten ist eine Querschnittsfunktion. Auch wenn sie Rechtskenntnis über die nationalen und internationalen Vorgaben erfordert, muss er kein Jurist sein. Zudem sollte er vertraut mit den Unternehmensabläufen und den Lieferketten des Unternehmens sein. Da seine Hauptaufgabe in der Informationsbeschaffung und -analyse besteht, sind Kommunikationsfähigkeiten einerseits und ein analytisches, konzeptionelles sowie **15**

²⁹ Vgl. *Hagel/Wiedmann*, Menschenrechtsbeauftragte, S. 60 f.

³⁰ Möglicher Bestandteil eines erweiterten Auskunftersuchens des BAFA.

³¹ Möglicher Bestandteil eines erweiterten Auskunftersuchens des BAFA.

³² Vgl. BT-Drs. 19/28649, S. 43; Fragen und Antworten zum Lieferkettengesetz (FAQ), VII.1.

fachübergreifend vernetztes Denken und Handeln andererseits von besonderer Bedeutung.

- 16 Zudem muss der Menschenrechtsbeauftragte dem Unternehmen gegenüber objektiv, loyal und verantwortungsbewusst handeln und seine Tätigkeit sorgfältig und ehrlich ausführen.

b) Unparteilichkeit, Unabhängigkeit und Weisungsungebundenheit

- 17 Das Gesetz macht keine Vorgaben zur Unabhängigkeit, Weisungsfreiheit und Verschwiegenheit des Menschenrechtsbeauftragten, anders als beispielsweise für die Beschwerdebeauftragten unter dem LkSG (siehe → Rn. 48 ff.). Auch für den Datenschutzbeauftragten besteht die Pflicht, sicherzustellen, dass er bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgabe erhält (Art. 38 Abs. 3 Satz 1 DSGVO). Um allerdings die Überwachungsfunktion sachgerecht wahrnehmen zu können, muss der Menschenrechtsbeauftragte über eine gewisse Unabhängigkeit verfügen³³ und er darf an der Ausübung der Überwachungstätigkeit nicht gehindert werden.³⁴
- 18 Übernimmt ein Mitarbeiter des Unternehmens (zusätzlich) die Position des Menschenrechtsbeauftragten, muss sichergestellt werden, dass kein Interessenskonflikt bezüglich der vorhergehenden oder parallelen Tätigkeit mit der Überwachungsaufgabe besteht. Bleibt der Mitarbeiter parallel in einem, der zu überwachenden Bereiche, scheidet diesbezüglich eine Überwachung aus und diese muss von einem anderen Mitarbeiter als Menschenrechtsbeauftragter übernommen werden. In solchen Konstellationen bietet es sich an, ein mehrköpfiges Menschenrechts-Komitee zu installieren, das die Überwachungsaufgaben übernimmt. Dabei ist wichtig, dass ein anderes Mitglied des Komitees die Überwachung des Bereiches vornimmt, dem ein Komiteemitglied angehört. Ähnlich sollte verfahren werden, wenn ein Mitarbeiter aus einem zu überwachenden Bereich ausscheidet und die Aufgabe des Menschenrechtsbeauftragten übernimmt; ggf. bietet sich hier auch eine angemessene Übergangsfrist an, bevor der Menschenrechtsbeauftragte den bisherigen Tätigkeitsbereich überwachen kann („cooling off“). Hierdurch wird sichergestellt, dass sachliche Beeinträchtigungen die Unabhängigkeit und Objektivität des Menschenrechtsbeauftragten nicht beeinträchtigen.³⁵

33 Nach *Harings/Jürgens*, LkSG, Kapitel, S. 95 „sollte der Menschenrechtsbeauftragte grundsätzlich nicht weisungsgebunden sein“; ähnlich: *Fleischer/Götz*, in: *Fleischer/Mankowski*, LkSG, § 4 Rn. 59: „weitgehende Unabhängigkeit“; weitergehend: *Sturm*, in: *Wagner/Rutloff/Wagner*, LkSG, § 6 Rn. 1007: „Seiner Überwachungsfunktion kann [...] nur nachkommen, wenn er unabhängig ist“; so auch *Frank/Edel/Heine/Heine*, BB 2021, 2165, 2167: „muss der Menschenrechtsbeauftragte ferner unabhängig arbeiten können.“

34 *Walden*, in: *Depping/Walden*, LkSG, § 4 Rn. 118.

35 Bei der mit der Funktion des Menschenrechtsbeauftragten vergleichbaren Internen Revision gilt eine Übergangsfrist von mindestens einem Jahr. Gemäß IPPF-Standard 1130.A1, https://www.diir.de/fileadmin/fachwissen/standards/downloads/IPPF_2017_Version_7_20190311.pdf (zuletzt abgerufen am 1.7.2024): „Beeinträchtigung von Unabhängigkeit oder Objek-

Gründe für Beeinträchtigungen der individuellen Unabhängigkeit und der persönlichen Objektivität können aber auch aus der geschützten Privatsphäre (z. B. Partner, Freunde) des Menschenrechtsbeauftragten resultieren. Sind seine Freunde oder Familienangehörige zu überwachen, sollte er die Beeinträchtigung seiner Unabhängigkeit anzeigen, wobei er nicht verpflichtet ist, die konkreten Gründe zu nennen.³⁶ **19**

Der Menschenrechtsbeauftragte darf an der Ausübung der Überwachungstätigkeit nicht gehindert werden.³⁷ Um seiner Überwachungspflicht nachkommen zu können, braucht der Menschenrechtsbeauftragte, ähnlich wie in der MaRisk der Bundesanstalt für Finanzdienstleistungsaufsicht³⁸ beschrieben, „Zugang zu allen für die Erfüllung seiner Aufgaben notwendigen Informationen, dazu zählen bspw. Dokumente (einschließlich Weisungen und Beschlüsse) der Geschäftsleitung, die für ihn von Bedeutung sein können, Einsicht in Prozesse und IT-Systeme sowie das Recht, relevante Mitarbeiter zu befragen“.³⁹ Das Recht und der Umfang der Informationsbeschaffung sollte in der Ernennungsurkunde des Menschenrechtsbeauftragten geregelt werden.⁴⁰ **20**

Des Weiteren muss er in der Lage sein, die Geschäftsleitung ungefiltert gemäß § 4 Abs. 3 Satz 2 LkSG zu informieren; dies sollte ebenfalls in der Ernennungsurkunde oder dem Arbeitsvertrag dokumentiert werden. **21**

c) Verschwiegenheit

Eine besondere Vertraulichkeit ist für den Menschenrechtsbefugten im LkSG nicht vorgesehen. Eine Verpflichtung zur Verschwiegenheit erscheint aber insoweit notwendig, als sich der Menschenrechtsbeauftragte auch mit Hinweisen aus dem Beschwerdeverfahren beschäftigt, da § 8 Abs. 3 LkSG fordert, dass die mit der Durchführung des Verfahrens betrauten Personen zur Verschwiegenheit zu verpflichten sind. **22**

tivität“ kann die Objektivität als beeinträchtigt angenommen werden, wenn ein Interner Revisor eine Aktivität prüft, für die er im Verlauf des vorangegangenen Jahres operativ verantwortlich war.

36 Schutz der Privatsphäre der Mitarbeitenden. Verhaltenskodizes der Unternehmen sehen meist Regelungen zu Interessenkollisionen wegen Freundschafts- oder Verwandtschaftsverhältnissen vor.

37 Walden, in: Depping/Walden, LkSG, § 4 Rn. 118.

38 MaRisk in AT 4.4.3 Ziffer 4 vom 16.8.2021, https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs1021_MaRisk_Erlaeuterungen.pdf?__blob=publicationFile&v=5 (zuletzt abgerufen am 1.7.2024).

39 Vgl. Hagel/Wiedmann, Menschenrechtsbeauftragte, S. 277.

40 Vgl. Musterernennungsurkunde in Hagel/Wiedmann, Menschenrechtsbeauftragte, S. 277 sowie weitere Musterklauseln bei Grabosch, in: Grabosch, LkSG, § 5 Rn. 37.

4. Ernennung

- 23 Das Unternehmen hat dafür zu sorgen, dass festgelegt ist, wer innerhalb des Unternehmens dafür zuständig ist, das LkSG-Risikomanagement zu überwachen (§ 4 Abs. 3 Satz 1 LkSG). Da das LkSG-Risikomanagement funktionsübergreifend ist,⁴¹ empfiehlt sich ein Beschluss der Geschäftsleitung. Die Ernennung ist nach dem Gesetz zwar formfrei möglich, Schriftform empfiehlt sich aber schon deswegen, weil die Erfüllung der in § 3 LkSG genannten Sorgfaltspflichten, zu denen auch die Benennung der zuständigen Person(en) für die Überwachung des LkSG-Risikomanagements gehört, nach § 10 Abs. 1 LkSG fortlaufend zu dokumentieren ist. Die Ernennung hat gegenüber dem Menschenrechtsbeauftragten zu erfolgen. Seine Rolle und Verantwortlichkeit kann ihm nicht ohne seine Zustimmung zugewiesen werden.⁴² Es empfiehlt sich zu Dokumentationszwecken, die **Ernennungsurkunde** von dem oder den Menschenrechtsbeauftragte(n) gegenzeichnen zu lassen. Die Ernennungsurkunde sollte auch den Aufgabenbereich und die notwendigen Befugnisse sowie Aussagen zur Vertraulichkeit und Weisungsungebundenheit und, falls vereinbart, zum Kündigungsschutz, vergleichbar zum Datenschutzbeauftragten (Art. 38 Abs. 3 Satz 2 DSGVO), enthalten. Sollten in Konzernen mehrere Gesellschaften unter den Anwendungsbereich des LkSG fallen, sollte jede dieser Gesellschaften aus Legimitationsgründen und zu Dokumentationszwecken jeweils eine Ernennungsurkunde ausstellen, auch wenn der Menschenrechtsbeauftragte personenidentisch ist.

5. Stellung im Unternehmen

- 24 Das Gesetz macht in § 4 Abs. 3 LkSG zur organisatorischen, insbesondere hierarchischen Einbindung des Menschenrechtsbeauftragten keine Angaben. Dies ist auch nicht verwunderlich, da die Benennung eines Menschenrechtsbeauftragten nur als eine Möglichkeit für die Festlegung einer zuständigen Person für die Überwachung des Risikomanagements genannt wird. Auch die Gesetzesbegründung empfiehlt lediglich die Einrichtung der Stelle des Menschenrechtsbeauftragten **direkt unter der Geschäftsleitung**.⁴³ Bei anderen betrieblichen Beauftragten sind die Regelungen unterschiedlich. Im Compliance-Bereich ist beispielsweise der Geldwäschebeauftragte nach § 7 Abs. 1 Satz 3 GwG zwingend der Geschäftsleitung direkt zu unterstellen, der Datenschutzbeauftragte berichtet nach Art. 38 Abs. 3 Satz 3 DSGVO unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters und der Compliance-Beauftragte nach Art. 11 Abs. 2 lit. a EUDR ist auf der Führungsebene zu ernennen.⁴⁴ Offener ist die hierarchische Anbindung in der Konfliktmi-

41 Zumindst unter Einbindung der folgenden Abteilungen, sofern vorhanden: Personal, EHS (Environment, Health and Safety), Einkauf, Compliance und Recht.

42 *Sturm*, in: Wagner/Ruttloff/Wagner, LkSG, § 6 Rn. 1008.

43 BT-Drs. 19/28649, S. 42.

44 Verordnung (EU) 2023/1115 über die Bereitstellung bestimmter Rohstoffe und Erzeugnisse, die mit Entwaldung und Waldschädigung in Verbindung stehen, auf dem Unionsmarkt und

neralienverordnung für Person(en), die damit betraut werden, den Prozess der Erfüllung der Sorgfaltspflicht in der Lieferkette zu überwachen. Nach Art. 4 lit. c der Konfliktmineralienverordnung sollen dies Mitglieder des gehobenen Managements sein.

In Ermangelung gesetzlicher Vorgaben kann der Menschenrechtsbeauftragte 25 theoretisch auch auf einer anderen (höheren oder niedrigeren) hierarchischen Ebene als direkt unter der Geschäftsleitung angesiedelt werden. Bei der hierarchischen Einordnung stellt sich für die Unternehmen die Frage der Angemessenheit ebenso wie die Frage der Zweckmäßigkeit.

Theoretisch kann der Menschenrechtsbeauftragte auch auf Geschäftsleitungsebene angesiedelt werden,⁴⁵ womit das Unternehmen die hohe Bedeutung seiner Position zum Ausdruck bringen würde. Allerdings ist die Geschäftsleitung verpflichtet, eine zuständige Stelle für die Überwachung des Risikomanagements im Unternehmen festzulegen und diese Stelle auszustatten und zu überwachen (§ 130 OWiG),⁴⁶ sodass die Geschäftsleitung ihre weitergehende Verantwortung nicht vollständig (z. B. auf einen Menschenrechtsbeauftragten) delegieren kann. Die Position des Menschenrechtsbeauftragten in der Geschäftsleitung würde diese Verantwortlichkeit auch nicht ersetzen. Verantwortet das Geschäftsleitungsmitglied zumindest auch teilweise die Umsetzung des LkSG, beispielsweise aufgrund der durch Geschäftsverteilungsplan zugewiesenen Verantwortung für die Funktionsbereiche Personal, EHS⁴⁷ oder Einkauf, kann es zumindest für diese Funktionsbereiche zu einem Interessenkonflikt kommen, wenn dieses Geschäftsleitungsmitglied zugleich die Verantwortung als Menschenrechtsbeauftragter innehat, da er als Menschenrechtsbeauftragter eine Überwachungsspflicht auch für „seine(n)“ Funktionsbereich(e) haben würde.⁴⁸ Zu bedenken ist aufgrund des umfangreichen Aufgabenkatalogs des Menschenrechtsbeauftragten auch, ob ein Geschäftsleitungsmitglied dafür ausreichend Kapazitäten hat. Empfehlenswert ist daher, einerseits die Verantwortung für die Einrichtung, Ausstattung und Überwachung des Menschenrechtsbeauftragten einem Mitglied der Geschäftsleitung im Geschäftsverteilungsplan zuzuweisen („**horizontale Delegation**“) und die Überwachung des LkSG-Risikomanagements auf einen unter dem Geschäftsleitungsmitglied angesiedelten Menschenrechtsbeauftragten zu übertragen („**vertikale Delegation**“). Soll die LkSG-Zuständigkeit eines Geschäftsleitungsmitglieds im Geschäftsverteilungsplan geregelt und einem Mitglied der Geschäftsführung als **Ressortverantwortlichkeit** zugewiesen werden,

ihre Ausfuhr aus der Union sowie zur Aufhebung der Verordnung (EU) Nr. 995/2010, <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32023R1115> (zuletzt abgerufen am 1.7.2024).

45 *Altenschmidt/Helling*, LkSG, § 4 Rn. 10; a. A. *Harings/Jürgens*, LkSG, S. 94 „sollte der Menschenrechtsbeauftragte nicht Mitglied der Geschäftsleitung sein“.

46 *Krais*, in: Pelz/Krais, LkSG, Kapitel 6 Rn. 10.

47 Steht für Environment, Health & Safety, im SCC-Regelwerk auch SGU (Sicherheits-, Gesundheits- und Umweltschutz) genannt.

48 *Harings/Jürgens*, LkSG, S. 93 f.

sollte dies klar und unmissverständlich erfolgen,⁴⁹ denn Unklarheiten führen dazu, dass die gesamte Geschäftsleitung verantwortlich bleibt.⁵⁰ Unklarheiten können sich beispielsweise dadurch ergeben, dass versucht wird, die Verantwortungsübertragung aus einem bestehenden Geschäftsverteilungsplan abzuleiten. Gibt es dort eine Geschäftsverteilung für die Bereiche Recht, Compliance und CSR auf unterschiedliche Mitglieder der Geschäftsleitung, so dürfte unklar sein, wem die Verantwortung für das LkSG-Risikomanagement obliegt. Es empfiehlt sich daher eine klare und dokumentierte Zuordnung der LkSG-Verantwortung auf ein Geschäftsleitungsmitglied.

- 27 Auch hinsichtlich der fachlichen Integration, also der Frage, welchem Funktionsbereich im Unternehmen die Stelle des Menschenrechtsbeauftragten zugeordnet wird, gibt es keine gesetzlichen Vorgaben. Der DICO-Standard zum Lieferketten-Compliance-Management-System („LCM“) enthält dazu folgende Ansatzpunkte in der Praxis:
- Verankerung bei Compliance (LCM als Teil des CMS): Für das Modell spricht die fachlich-juristische Beurteilungskompetenz aufgrund Verantwortung für weitere Compliance-Themenfelder, aber auch das Potenzial von Synergien mit bestehenden CMS-Elementen (z. B. Risikoanalyse, Hinweisgebersystem, etc.).
 - Verankerung bei Nachhaltigkeit (LCM als strategisch relevantes Thema): Zunächst spricht die thematische Nähe für dieses Modell, allerdings ist hervorzuheben, dass dort eher der strategische Fokus (geringe Nähe zum Umsetzungsnetzwerk) als der operative Bezug im Vordergrund steht. Ferner würde eine solche Verankerung zur Erhöhung der Komplexität durch Aufbau einer weiteren Compliance-Funktion führen.
 - Verankerung beim Einkauf (starke operationelle Einbindung): Dafür spricht zunächst die operative Nähe zu den Lieferanten, allerdings liegt dort wiederum der Fokus auf dem operationellen Geschäft und es entsteht ein Konfliktpotenzial.
- 28 Neben den im DICO-Standard genannten Beispielen gibt es weitere Möglichkeiten der fachlichen Integration, etwa in der Rechtsabteilung, oder die Schaffung eines eigenständigen Funktionsbereichs. Letztlich hat das Unternehmen nach sorgfältiger Abwägung unter Berücksichtigung der Grundsätze der Angemessenheit und Wirksamkeit zu entscheiden, welche funktionale Anbindung die Überwachung des LkSG-Risikomanagements unternehmensspezifisch am besten sicherstellt. Wichtig ist in jedem Fall, auf die Weisungsungebundenheit und die Vermeidung von Interessenkonflikten bezüglich Implementierung, Betrieb und Überwachung der Sorgfaltspflichten zu achten.⁵¹

49 Allgemein zur Klarheit der Ressortaufteilung im Geschäftsverteilungsplan: *Fleischer*, in: MünchKomm-GmbHG, § 43 Rn. 140; *Freund*, NZG 2021, 579, 586.

50 *Grabosch*, in: *Grabosch*, LkSG, § 4 Rn. 42.

51 Ebenso: Fragen und Antworten zum Lieferkettengesetz (FAQ), VII.1.

6. Arbeitsrechtlicher Schutz

Ein gesetzlicher **Kündigungsschutz** steht dem Menschenrechtsbeauftragten nicht zu, anders als etwa dem Geldwäschebeauftragte nach § 7 Abs. 7 Satz 2 GwG, bei dem eine Kündigung des Arbeitsverhältnisses nur zulässig ist, wenn Tatsachen vorliegen, die zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Zur Wahrung einer unabhängigen Überwachung des LkSG-Risikomanagements durch den Menschenrechtsbeauftragten empfiehlt sich allerdings eine entsprechende arbeitsvertragliche Regelung.⁵² **29**

7. Auslagerung der Funktion

Bei Unternehmen mit einer Vielzahl von Betriebsstätten in Form von Konzerngesellschaften und Standorten im In- und Ausland stellt sich die Frage, ob für jede Betriebsstätte ein Menschenrechtsbeauftragter ernannt werden muss („**dezentrale Integration**“) oder ob es ausreicht, einen konzernweit tätigen Menschenrechtsbeauftragten zu ernennen („**zentrale Integration**“). Den Unternehmen steht es frei, zu entscheiden, wie sie sich konzernintern organisieren. In der Praxis hat sich bewährt, dass Unternehmen einen Menschenrechtsbeauftragten für alle Betriebsstätten ernennen. In der Regel wird dieser durch LkSG-Verantwortliche in den einzelnen Unternehmensbereichen unterstützt.⁵³ **30**

Der Menschenrechtsbeauftragte muss dabei nicht im Inland sitzen, sondern kann auch bei einer Konzerngesellschaft im Ausland ansässig sein.⁵⁴ Dies ist oft der Fall, wenn die ausländische Muttergesellschaft im Rahmen ihrer Matrixorganisation diese Aufgabe durch einzelne Personen oder Teams übernimmt. **31**

Bei großen Konzernen mit vielen direkt unter das LkSG fallenden Konzerngesellschaften ist es mittlerweile auch üblich, einen Konzernmensenrechtsbeauftragten zu ernennen, an den die Menschenrechtsbeauftragten der unter das LkSG fallenden Konzerngesellschaften eine fachliche Berichtslinie haben, so bspw. im Volkswagen-Konzern. **32**

Im Gegensatz zu Regelungen für die Möglichkeit der Auslagerung der Beauftragtenfunktion auf Unternehmensexterne in anderen Gesetzen, bspw. für den Geldwäschebeauftragten (§ 6 Abs. 7 GwG) oder den Datenschutzbeauftragten (Art. 37 Abs. 6 DSGVO), enthält das LkSG keine ausdrückliche Erlaubnis der Auslagerung. Vielmehr sieht § 3 Abs. 1 Satz 2 Nr. 2 LkSG die Festlegung einer *betriebsinternen* Zuständigkeit vor. Auch § 4 Abs. 3 Satz 1 LkSG verlangt, dass festzulegen ist, wer *innerhalb* des Unternehmens für die Überwachung des LkSG-Risikomanagements zuständig ist. Insofern ist eine vollständige Auslage- **33**

⁵² Siehe hierzu: *Grabosch*, in: *Grabosch*, LkSG, § 5 Rn. 37.

⁵³ Im Ergebnis so auch: *Gehling*, CCZ 2023, 211, 217; *Theusinger/Gergen*, in: *Schall/Theusinger/Pour Rafsendsjani*, LkSG, § 4 Rn. 107, halten eine Benennung im Unternehmensverbund für zulässig.

⁵⁴ Ebenso: *Fragen und Antworten zum Lieferkettengesetz (FAQ)*, VII.1.

rung an einen Unternehmensexternen nicht möglich,⁵⁵ selbst wenn im Einzelfall eine Kontrolle durch einen Unternehmensexternen noch wirksamer und uneinflusster sein könnte.⁵⁶ Unbestritten ist, dass die Unterstützung des Menschenrechtsbeauftragten durch einen externen Dienstleister möglich⁵⁷ oder in Abhängigkeit des konkreten Risikoprofils und mit Blick auf den allgemeinen Angemessenheitsvorbehalt gar geboten ist.⁵⁸

8. Haftung

- 34** Da dem Menschenrechtsbeauftragten eine Überwachungsfunktion zukommt, stellt sich die Frage, ob damit auch eine besondere Haftung einhergeht. Hierbei ist einerseits an eine schuldrechtliche Haftung gegenüber dem Unternehmen zu denken, andererseits an eine bußgeldrechtliche Haftung.
- 35** Der Menschenrechtsbeauftragte haftet für Pflichtverletzungen aus seinem Arbeitsverhältnis. Pflichtverletzungen können aus Nichtleistung, verspäteter Leistung oder Schlechterfüllung bestehen. Bei Pflichtverletzungen kann seinem Arbeitgeber ein Recht zur Abmahnung/Kündigung und ein Anspruch auf Schadensersatz entstehen. Eine Entgeltminderung kennt das Arbeitsrecht hingegen nicht, ein Entfall der Pflicht zur Entgeltzahlung liegt nur in Ausnahmefällen vor.⁵⁹ Er haftet für schuldhaftes Pflichtwidrigkeiten in den Grenzen der Arbeitnehmerhaftung⁶⁰ nach den Grundsätzen der Rechtsprechung des BAG⁶¹:
- keine Haftung bei leichtester Fahrlässigkeit,⁶²
 - anteilige Haftung (mit dem Arbeitgeber) bei mittlerer Fahrlässigkeit,⁶³

55 Ruttloff/Wagner/Hahn/Freihoff, CCZ 2022, 20, 24; Rudkowski, in: BeckOK LkSG, § 4 Rn. 52; a. A. Kramme/Ponholzer, in: Berg/Kramme, LkSG, § 4 Rn. 24, Harings/Jürgens/Thalhammer, CB 2022, 93, 97; Gehling, CCZ 2023, 211, 217.

56 Aus diesem Grund für die zulässige Delegation an einen Unternehmensexternen: Harings/Jürgens/Thalhammer, CB 2022, 93, 97.

57 Ruttloff/Wagner/Hahn/Freihoff, CCZ 2022, 20, 24; Lorenzen, in: Kaltenborn/Krajewski/Rühl/Saage-Maaß, LkSG, § 4 Rn. 132; Theusinger/Gergen, in: Schall/Theusinger/Pour Rafsendjani, LkSG, § 4 Rn. 108.

58 DICO 30 FAQ zum Menschenrechtsbeauftragten (Antwort auf Frage 9), für Mitglieder abrufbar unter <https://www.dico-ev.de/2022/08/10/30-faq-zum-menschenrechtsbeauftragten/> (abgerufen am 30.6.2024); ebenso Fragen und Antworten zum Lieferkettengesetz (FAQ), VII.1.

59 Ausführlich dazu: Preis/Greiner, in: ErfK ArbR, § 619a Rn. 7.

60 Kraiss, in: Pelz/Kraiss, LkSG, Kapitel 6 Rn. 19.

61 BAG, 22.3.2018 – 8 AZR 779/16, NZA 2018, 1216 ff.; BAG, 15.11.2012 – 8 AZR 705/11, DB 2013, 705 ff.; ausführlich: Wullenkord, in: BeckOK ArbR, § 619a BGB Rn. 5 ff.; dazu und zum dreistufigen Haftungsmodell im Schrifttum (die ersten beiden Stufen der BAG-Rspr. werden ersetzt durch normale Fahrlässigkeit ohne Haftung): Griese, in: Küttner, ArbR, Arbeitnehmerhaftung Rn. 14.

62 Schaden beruht auf einem typischen Versehen (Sich-Versprechen, Vergreifen, Vertun): Wullenkord, in: BeckOK ArbR, § 619a BGB Rn. 10.

63 Außerachtlassung der im Verkehr erforderlichen Sorgfalt (objektiver Verschuldensbegriff): Wullenkord, in: BeckOK ArbR, § 619a BGB Rn. 11.

- in der Regel⁶⁴ volle Haftung bei grober Fahrlässigkeit,⁶⁵
- volle Haftung bei Vorsatz.

Bei leitenden Angestellten hat das BAG hingegen bisher eine Haftungserleichterung noch nicht ausdrücklich bejaht.⁶⁶ Leitende Angestellte und Betriebsbeauftragte können aber in die Vermögensschaden-Haftpflichtversicherung (D&O-Versicherung) des Unternehmens einbezogen werden.⁶⁷ Menschenrechtsbeauftragte, die zugleich leitende Angestellte sind, sollten sich hierzu vor Übernahme der Verantwortung informieren. 36

Nach den Anforderungen des LkSG ist der Menschenrechtsbeauftragte nicht für die Einhaltung der Sorgfaltspflichten verantwortlich, sondern für die Überwachung des Risikomanagementsystems.⁶⁸ Ihn trifft insofern auch keine Garantstellung. Ob er nach § 9 Abs. 2 Nr. 2 OWiG einem eigenen Bußgeldrisiko ausgesetzt ist, hängt von der konkreten Ausgestaltung seiner Aufgabenbeschreibung und der Einräumung einer eigenen Entscheidungsfreiheit ab.⁶⁹ 37

III. Beschwerdebeauftragte

1. Begrifflichkeiten und gesetzliche Grundlagen

Der Begriff des Beschwerdebeauftragten kommt, anders als der des Menschenrechtsbeauftragten, im LkSG nicht vor. Das Gesetz nennt in § 8 Abs. 1 und 3 LkSG nur „die von dem Unternehmen mit der Durchführung des Verfahrens betrauten Personen“. Diese werden in der Literatur als „**Beschwerdebeauftragte**“ bezeichnet.⁷⁰ Das Gesetz bestimmt zudem, dass diese Beschwerdebeauftragten Gewähr für unparteiisches Handeln bieten müssen, insbesondere müssen sie unabhängig und an Weisungen nicht gebunden sein.⁷¹ Sie sind zudem zur Verschwiegenheit verpflichtet,⁷² haben den Sachverhalt mit den Hinweisgebern zu erörtern⁷³ und können ein Verfahren der einvernehmlichen Beilegung anbieten.⁷⁴ Bei den mit der Durchführung des Beschwerdeverfahrens betrauten Personen ist 38

64 Außer bei existenzgefährdender Wirkung oder eklatantem Missverhältnis zwischen Vergütung und Schaden: *Wullenkord*, in: BeckOK ArbR, § 619a BGB Rn. 12.

65 Außerachtlassung der im Verkehr erforderlichen Sorgfalt in einem ungewöhnlich hohen Grad („hätte jedem anderen in der konkreten Situation einleuchten müssen“): *Wullenkord*, in: BeckOK ArbR, § 619a BGB Rn. 12.

66 *Wullenkord*, in: BeckOK ArbR, § 619a BGB Rn. 6.

67 *Grabosch*, in: Grabosch, LkSG, § 5 Rn. 40.

68 *Rothermel*, LkSG, § 4 Rn. 35; *Krais*, in: Pelz/Krais, LkSG, Kapitel 6 Rn. 19.

69 *Rothermel*, LkSG, § 4 Rn. 36; *Grabosch*, in: Grabosch, LkSG, § 4 Rn. 38; *Engel/Schönfelder*, in: Grabosch, LkSG, § 6 Rn. 38; *Altenschmidt/Helling*, LkSG, § 24 Rn. 8.

70 Vgl.: *Welling/Brouwer*, in: Spießhofer/Späth, LkSG, § 8 Rn. 46; *Stemberg*, in: Fleischer/Mankowski, LkSG, § 8 Rn. 81; *Bertke/Sandbrink*, NJW 2024, 319, 323.

71 § 8 Abs. 3 Satz 1 LkSG.

72 § 8 Abs. 3 Satz 2 LkSG.

73 § 8 Abs. 1 Satz 4 LkSG.

74 § 8 Abs. 1 Satz 5 LkSG.

zu unterscheiden zwischen „**verfahrensleitenden Personen**“ und „**verfahrensbegleitenden Personen**“.⁷⁵

2. Aufgaben

- 39 Die Beschwerdebeauftragten sind vom Unternehmen damit betraut, das LkSG-Beschwerdeverfahren durchzuführen. Das Verfahren ist vom Unternehmen in einer **Verfahrensordnung** festzuschreiben.⁷⁶ Aufgabe der Beschwerdebeauftragten ist die Leitung aller auf den Eingang der Beschwerde oder des Hinweises folgenden Phasen. Das LkSG trifft keine Aussagen dazu, wann das Beschwerdeverfahren endet. In § 17 HinSchG ist das Verfahren hingegen beschrieben und schließt nach § 17 Abs. 1 Nr. 6 auch die in § 18 HinSchG genannten Folgemaßnahmen ein:
1. interne Untersuchungen,
 2. Verweis an andere zuständige Stellen,
 3. Abschluss des Verfahrens aus Mangel an Beweisen oder aus anderen Gründen oder
 4. Abgabe des Verfahrens zwecks weiterer Untersuchungen im Unternehmen oder durch zuständige Behörden.
- 40 Nicht zum Beschwerdeverfahren gehören hingegen die Entscheidung über (Phase 9)⁷⁷ und Umsetzung von Präventions-,⁷⁸ Abhilfe-⁷⁹ oder Wiedergutmachungsmaßnahmen. Insofern ist der Beschwerdebeauftragte nicht mit der Durchführung dieser Schritte und Maßnahmen betraut und die durchführenden Personen⁸⁰ unterliegen, zumindest nach dem LkSG, nicht dem Erfordernis der Unparteilichkeit, Unabhängigkeit, Weisungsfreiheit und Verschwiegenheit.
- 41 Anders als das HinSchG⁸¹ trifft das LkSG keine Aussage dazu, ob auch **anonyme Hinweise** zu bearbeiten sind. Unabhängig davon ist die Geschäftsleitung auf der Grundlage des Legalitätsprinzips verpflichtet, Hinweisen auf Rechtsverletzungen nachzugehen, egal woher sie kommen oder in welcher Form sie getätigt wurden, sodass auch anonymen Hinweisen nachgegangen werden muss. Dann empfiehlt es sich aber, auch eine anonyme Nutzung des Verfahrens zu ermöglichen.⁸² Manche Meldende wollen anonym bleiben, weil sie der Unabhän-

75 Gläßer/Kühn, in: BeckOK LkSG, § 8 Rn. 165 f.; Kocher, in: Kaltenborn/Krajewski/Rühl/Saage-Maaß, LkSG, § 8 Rn. 37.

76 Nach § 8 Abs. 2 LkSG legt das Unternehmen eine Verfahrensordnung in Textform fest, die öffentlich zugänglich ist.

77 Siehe nachfolgende Abbildung des Beschwerdeverfahrens.

78 Siehe § 6 LkSG.

79 Siehe § 7 LkSG.

80 Abhängig vom Gegenstand der Beschwerde sind dies typischerweise die Geschäftsleitung und/oder die relevanten Fachabteilungen, bspw. die Personalabteilung.

81 § 16 Abs. 1 Satz 3 und 4 HinSchG.

82 BAFA, Handreichung, Beschwerdeverfahren nach dem Lieferkettensorgfaltspflichtengesetz, S. 9, https://www.bafa.de/SharedDocs/Downloads/DE/Lieferketten/handreichung_beschwerdeverfahren.html (zuletzt abgerufen am 1.7.2024).

gigkeit oder Verschwiegenheit der untersuchenden Stelle nicht trauen, Repressalien des Unternehmens fürchten oder nicht als Denunziant gelten möchten.⁸³

Der Eingang des Hinweises ist dem Hinweisgeber zu bestätigen. Bei systemgestützten Meldesystemen erfolgt dies automatisiert, ansonsten erfolgt eine Erstprüfung⁸⁴ und Dokumentation durch die Beschwerdebeauftragten (Phase 4) und nachfolgend eine **Eingangsbestätigung** (Phase 5). Dabei sollte die unter dem LkSG eigentlich nicht zwingende 7-Tagesfrist des HinSchG eingehalten werden.⁸⁵ 42

Nach dem HinSchG ist mit dem Hinweisgeber Kontakt zu halten.⁸⁶ Beschwerdebeauftragte sind darüber hinaus gehalten, den Sachverhalt mit dem Hinweisgeber zu erörtern.⁸⁷ Qualitativ unterscheiden sich die beiden Herangehensweisen. Aus praktischer Sicht empfiehlt es sich, diese situativ zu verschmelzen. Sofern der Untersuchungszweck nicht gefährdet wird, sollte mit dem Hinweisgeber während des ganzen Verfahrens Kontakt gehalten und der Verfahrensfortschritt erörtert werden. Für das Unternehmen geht es darum, dem Hinweis bestmöglich nachzugehen und zunächst den Sachverhalt umfassend zu ermitteln, um dann geeignete Maßnahmen ergreifen zu können, um dem gemeldeten Risiko vorzubeugen oder gemeldete Verletzungshandlungen abzustellen. Es geht auch darum, festzustellen, ob eine **Wiedergutmachung** möglich ist und, falls der Hinweisgeber zugleich Betroffener ist, wie diese gegebenenfalls aussehen könnte. Soweit erforderlich, oder falls vom Hinweisgeber gewünscht, sollte der Beschwerdebeauftragte den Hinweisgeber auch treffen, ob in Person oder virtuell (Phase 6).⁸⁸ 43

Der Beschwerdebeauftragte kann der hinweisgebenden Person auch ein Verfahren zur einvernehmlichen Beilegung anbieten.⁸⁹ 44

Auch wenn das LkSG, anders als das HinSchG (§ 17 Abs. 2 HinSchG), nicht vorsieht, dass der Hinweisgeber innerhalb von drei Monaten nach Erhalt der Eingangsbestätigung eine **Rückmeldung** über geplante sowie bereits ergriffene Maßnahmen zu erhalten hat, empfiehlt sich auch für Meldungen unter dem LkSG eine entsprechende Rückmeldung an den Hinweisgebenden. 45

83 Wiedmann/Hoppmann, CCZ 2023, 11, 16 unter Verweis auf Hauser/Bretti-Rainalter/Blumer, Whistleblowing Report 2021, S. 11, <https://www.integrityline.com/de/knowhow/white-paper/whistleblowing-report/> (zuletzt abgerufen am 1.7.2024).

84 Bei der Erstprüfung wird beispielsweise geprüft, ob der gemeldete Sachverhalt einen Anfangsverdacht eines Compliance-Verstoßes darstellen könnte und falls ja, ob dieser in den Anwendungsbereich des LkSG fällt, sodass die Regelungen von § 8 LkSG anwendbar sind oder andere gesetzliche (bspw. das HinSchG) oder betriebliche Verfahrensanforderungen zu berücksichtigen sind.

85 Vgl. § 8 Abs. 1 Satz 3 LkSG bzw. § 17 Abs. 1 Nr. 1 HinSchG.

86 § 17 Abs. 1 Nr. 3 HinSchG

87 Vgl. § 17 Abs. 1 Nr. 3 HinSchG bzw. § 8 Abs. 1 Satz 4 LkSG.

88 Nach § 16 Abs. 3 Satz 2 HinSchG steht dem Hinweisgeber ein entsprechender Anspruch zu.

89 § 8 Abs. 1 Satz 4 LkSG. Ausführlich zu den möglichen Verfahren: Hagel/Wiedmann, Menschenrechtsbeauftragte, S. 186 ff.

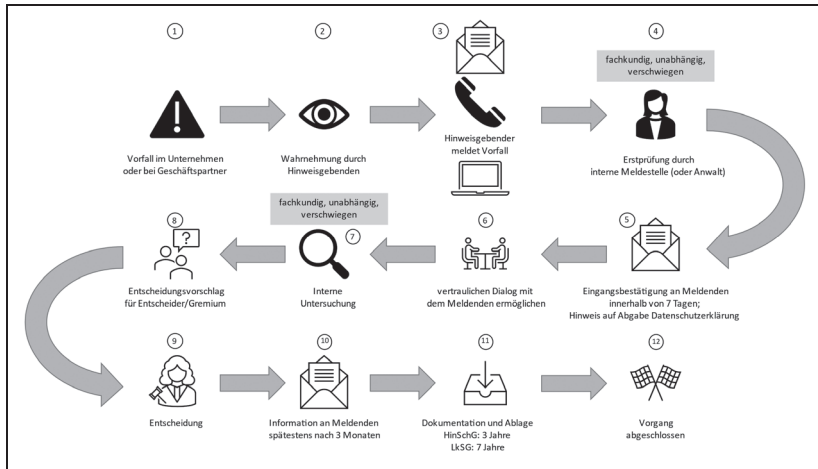


Abbildung 2: Ablauf des Beschwerdeverfahrens⁹⁰

3. Anforderungen an Beschwerdebeauftragte

a) Qualifikation

- 46** Das LkSG enthält keine Qualifikationsvorgaben für die mit der Durchführung des Beschwerdeverfahrens betrauten Personen, weder für verfahrensbegleitende noch für verfahrensleitende. Für die Wirksamkeit des Beschwerdeverfahrens ist es jedoch erforderlich, dass die Beschwerdebeauftragten eine ausreichende Qualifikation haben, um die Aufgaben in ihrem Verantwortungsbereich regelkonform ausgestalten zu können.⁹¹
- 47** Die Vorgaben für die Beschwerdebeauftragten sollten idealerweise im Arbeitsvertrag der Betroffenen verankert werden. Die Betroffenen selbst sollten über (1) eine gewisse Seniorität und Fachkunde verfügen, wie dies für die vergleichbare Position der Meldestellenbeauftragten auch in § 15 Abs. 2 HinSchG gesetzlich gefordert wird, (2) mit dem Umgang mit menschenrechtlichen und umweltbezogenen Risiken⁹² und entsprechenden Verletzungen⁹³ vertraut und (3) frei von Interessenkonflikten bezüglich des Sachverhalts und der involvierten Personen sein. Zudem sollten Beschwerdebeauftragte empathisch sein, beispielsweise bezüglich der oft heiklen Fragen im Hinblick auf Diskriminierung und (sexuelle) Belästigungen.⁹⁴ Eine gute Kommunikationsfähigkeit, einschließlich der Be-

⁹⁰ Übernommen aus Hagel/Wiedmann, Menschenrechtsbeauftragte, S. 185.

⁹¹ Gläßer/Kühn, in: BeckOK LkSG, § 8 Rn. 180.

⁹² § 2 Abs. 2 und 3 LkSG.

⁹³ § 2 Abs. 4 LkSG.

⁹⁴ Hagel/Wiedmann, KonfliktDynamik 2024, S. 266, 276.

herrschaft von Fragetechniken und des aktiven Zuhörens, sind insbesondere bei der Ermittlung des Sachverhaltes und der Anhörung der Meldenden und Beschuldigten notwendig.

b) Unparteilichkeit, Unabhängigkeit und Weisungsungebundenheit

Nach § 8 Abs. 3 Satz 1 LkSG müssen die Beschwerdebeauftragten „Gewähr für unparteiisches Handeln bieten, insbesondere müssen sie unabhängig und nicht an Weisungen gebunden sein“. Diese Anforderungen dienen dazu, sicherzustellen, dass die Beschwerdebeauftragten das Beschwerdeverfahren frei von Interessenkollisionen und unvoreingenommen durchführen können. Oberstes Gebot ist ein unparteiisches Handeln. Parteien des Beschwerdeverfahrens können die hinweisgebende Person sein, die zugleich in ihren eigenen Rechten betroffen sein kann, das Unternehmen, von dem das Risiko oder die Verletzung ausgeht, sowie seine unmittelbaren⁹⁵ und mittelbaren Zulieferer.⁹⁶ Aufgrund des Risikos parteiischen Handelns bei bestehender Abhängigkeit oder Weisungsgebundenheit, sind Beschwerdebeauftragte im jeweiligen Einzelfall automatisch vom weiteren Verfahren auszuschließen („müssen unabhängig und nicht an Weisungen gebunden sein“), selbst wenn sie das Verfahren tatsächlich unparteiisch führen (könnten) oder die Parteien mit der Fortsetzung der Tätigkeit des Beschwerdebeauftragten einverstanden sind.⁹⁷ Die Abhängigkeit kann sich auf die persönliche und/oder wirtschaftliche Abhängigkeit von den Parteien oder dem Ergebnis des Verfahrens beziehen. Auch wenn Mitarbeitende grundsätzlich dem Direktionsrecht des Arbeitgebers unterstehen, ist eine Weisungsunabhängigkeit eines betriebsinternen Beschwerdebeauftragten möglich, aber durch flankierende (vertragliche) Maßnahmen sicherzustellen,⁹⁸ beispielsweise durch einen Kündigungsschutz für die Zeit der Beauftragung als Beschwerdebeauftragter, eventuell mit anschließender Karenzzeit.⁹⁹

Neben den im Gesetz exemplarisch genannten Risiken für parteiisches Handeln kann sich **Befangenheit** der Beschwerdebeauftragten aber auch aus der Nähe zum Beschwerdegegenstand, beispielsweise durch eine Vorbefassung oder durch die tatsächliche, beispielsweise unfaire Verfahrensführung ergeben. Wird die Schwelle der Unvoreingenommenheit überschritten, hat der Beschwerdebeauftragte, sofern sie oder er es selbst feststellt, dies dem Unternehmen anzuzeigen und sich aus dem Beschwerdeverfahren zurückzuziehen („hat Gewähr zu leisten“) oder ist vom Unternehmen, gegebenenfalls auf Hinweis der Beteiligten, davon abzuziehen und durch andere Beschwerdebeauftragte zu ersetzen.

⁹⁵ § 2 Abs. 7 LkSG.

⁹⁶ § 2 Abs. 8 LkSG.

⁹⁷ Anders als beispielsweise in § 3 Abs. 1 MediationsG ist eine mögliche Zustimmung bei Offenlegung von Abhängigkeiten im LkSG nicht vorgesehen.

⁹⁸ BAFA (2022) Handreichung Beschwerdeverfahren, S. 9; *Grabosch*, in: Grabosch, LkSG, § 5 Rn. 128; *Rothermel*, LkSG, § 8 Rn. 29; *Stenberg*, in: Fleischer/Mankowski, LkSG, § 8 Rn. 85; *KKRS/Kocher* LkSG § 8 Rn. 40, 43 ff.

⁹⁹ Analog zum gesetzlichen Kündigungsschutz des Datenschutzbeauftragten.

c) Verschwiegenheit

- 50 Beschwerdebeauftragte sind nach § 8 Abs. 3 Satz 2 LkSG zur Verschwiegenheit verpflichtet. Dies erstreckt sich auf verfahrensleitende und verfahrensbegleitende Personen.¹⁰⁰ Dies dient vor allem dem Schutz der Hinweisgebenden vor Nachteilen¹⁰¹ und bezieht sich damit primär auf die Identität der Meldenden und sonstigen gefährdeten Verfahrensbeteiligten.¹⁰² Die Grenze der Verschwiegenheitspflicht ergibt sich aus dem Zweck des Beschwerdeverfahrens. So bleibt eine Weitergabe von Informationen, die zum Zwecke der Erfüllung der Sorgfaltspflichten (bspw. der Durchführung von Präventions- oder Abhilfemaßnahmen) notwendig sind, möglich („Need to know“-Basis).¹⁰³

4. Ernennung

- 51 Das Beschwerdeverfahren ist eine Sorgfaltspflicht (§ 3 Abs. 1 Nr. 7 LkSG), deren Erfüllung fortlaufend zu dokumentieren ist (§ 10 Abs. 1 LkSG). Dies gilt auch für die Benennung der mit der Durchführung des Verfahrens betrauten Person(en), sei es für die Durchführung eines einzelnen Verfahrens oder generell für die Durchführung eventueller Verfahren. Es empfiehlt sich, dies mit einer vom Beschwerdebeauftragten gegengezeichneten Ernennungsurkunde zu dokumentieren, in der zugleich die Weisungsfreiheit für die Durchführung der Verfahren bestätigt und die Verschwiegenheit vereinbart wird. Beim Beschwerdebeauftragten ist eine Stellvertreterregelung sinnvoll, um sicherzustellen, dass eventuell eingehende Beschwerden stets zeitnah bearbeitet werden können und insbesondere die Eingangsbestätigung zeitgerecht erfolgen kann, soweit nicht automatisiert.

5. Stellung im Unternehmen

- 52 Die mit der Durchführung des Beschwerdeverfahrens beauftragten Personen müssen nicht betriebsintern sein, vielmehr kann sich das Unternehmen an einem externen Beschwerdeverfahren beteiligen (§ 8 Abs. 1 Satz 6 LkSG) oder einen externen Dritten bitten, das interne Beschwerdeverfahren durchzuführen.
- 53 Bei betriebsinternen Beschwerdebeauftragten gibt es keine generelle organisatorische, fachliche oder hierarchische Einbindung in das Unternehmen. Beschwerdebeauftragte können daher allen Fachbereichen angehören, wobei Interessenkollisionen aber zwingend zu vermeiden sind.¹⁰⁴ Beschwerde- und Hinweisgeberverfahren sind häufig unter der Verantwortung der Compliance-Abteilung. Aufgrund des hohen Anteils personalbezogener Beschwerden werden auch

100 Gläßer/Kühn, in: BeckOK LkSG, § 8 Rn. 192, 5. Edition 15.3.2024.

101 Gläßer/Kühn, in: BeckOK LkSG, § 8 Rn. 187, 5. Edition 15.3.2024 unter Angabe weiterer Zwecke; Begründung RegE BT-Drs. 19/28649, S. 33.

102 Gläßer/Kühn, in: BeckOK LkSG, § 8 Rn. 199, 5. Edition 15.3.2024.

103 Gläßer/Kühn, in: BeckOK LkSG, § 8 Rn. 200, 5. Edition 15.3.2024.

104 Bertke/Sandbrink, NJW 2024, 319, 323.

Mitarbeitende aus der Personalabteilung mit der Durchführung der Beschwerdeverfahren eingesetzt, soweit nicht die Personalabteilung oder ihre Mitarbeitenden selbst Gegenstand der Beschwerde sind. Allerdings ist die Personalabteilung zugleich Disziplinarstelle, was bei potenziellen Hinweisgebern nicht vertrauensbildend ist und sie daher von Hinweisen abhalten könnte.¹⁰⁵

6. Arbeitsrechtlicher Schutz

Auch für den Beschwerdebeauftragten sieht das LkSG keine arbeitsrechtlichen Sonderrechte, wie beispielsweise einen Kündigungsschutz vor. Aufgrund der geforderten Weisungsfreiheit empfiehlt sich aber auch für den Beschwerdebeauftragten ein vertraglicher Kündigungsausschluss. Die Ausführungen zum Menschenrechtsbeauftragten gelten entsprechend auch für den Beschwerdebeauftragten. **54**

7. Haftung

Beschwerdebeauftragte sind zwar weisungsungebunden und frei, verfahrensleitende Entscheidungen zu treffen. Verfehlungen bei der Verfahrensleitung sind jedoch nicht Gegenstand der Ordnungswidrigkeiten nach § 24 LkSG. Dort sind lediglich das Fehlen der Einrichtung eines Beschwerdeverfahrens, die fehlende oder nicht rechtzeitige Wirksamkeitsprüfung des Beschwerdeverfahrens und die fehlende oder nicht rechtzeitige Aktualisierung des Beschwerdeverfahrens als Ordnungswidrigkeiten bußgeldbewehrt. Beschwerdebeauftragte sind keine Beauftragten im Sinne von § 9 OWiG und unterliegen daher keiner persönlichen Bußgeldhaftung.¹⁰⁶ **55**

8. Abgrenzung zum Meldestellenbeauftragten nach HinSchG

Neben dem LkSG gibt es weitere gesetzliche Bestimmungen zu Beschwerde- und Hinweisgebertverfahren. Von besonderer Bedeutung, auch hinsichtlich von Menschenrechtsverstößen und umweltbezogenen Pflichtverletzungen, ist das HinSchG, das im Juli 2023 in Kraft getreten ist. Der Anwendungsbereich des HinSchG überschneidet sich mit dem Anwendungsbereich des LkSG, insbesondere bei Verletzungen von menschenrechtlichen oder umweltbezogenen Verboten nach LkSG, die Straftaten darstellen oder (auch außerhalb des LkSG) bußgeldbewehrt sind, soweit die verletzte Vorschrift dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient (z. B. Arbeitsschutz, Mindestlohn). Das Beschwerdeverfahren nach § 8 LkSG geht dem HinSchG nicht vor, da es sich bei § 8 LkSG nicht um eine sektorspezifische Vorschrift im Sinne des HinSchG handelt¹⁰⁷ und es in **56**

¹⁰⁵ So auch: Götz, in: Maschmann/Fritz, Matrixorganisationen, Kapitel 6 Rn. 168.

¹⁰⁶ Bertke/Sandbrink, NJW 2024, 319, 324.

¹⁰⁷ Colneri/Gerdemann, in: BeckOK LkSG, LkSG, 3. Edition Stand 15.4.2024, § 8 Rn. 4.

der abschließenden Liste von § 4 HinSchG nicht genannt ist,¹⁰⁸ andererseits bleibt § 8 LkSG aber auch vom HinSchG unberührt.¹⁰⁹ Sofern Meldungen in den Anwendungsbereich sowohl des HinSchG als auch von § 8 LkSG fallen, gilt das jeweils höhere Schutzniveau,¹¹⁰ sodass beispielsweise der Beschwerdebeauftragte mit hinweisgebenden Personen den Sachverhalt zu erörtern hat (§ 8 Abs. 1 Satz 4 LkSG), ihnen Rückmeldung geben (§ 17 Abs. 2 HinSchG) und ein persönliches Treffen ermöglichen muss (§ 16 Abs. 3 Satz 3 HinSchG). Die Dokumentation ist dann auch sieben Jahre nach Erstellung aufzubewahren (§ 10 Abs. 1 Satz 2 LkSG) und ist nicht bereits drei Jahre nach Abschluss des Verfahrens zu löschen (§ 11 Abs. 5 HinSchG).

- 57 Das HinSchG sieht die Einrichtung einer internen Meldestelle vor (§ 12 Abs. 1 HinSchG) und, dass Personen mit den Aufgaben der internen Meldestelle zu beauftragen sind (§ 15 Abs. 1 Satz 1 HinSchG), sog. **Meldestellenbeauftragte**.¹¹¹ Die gleichzeitige Bestellung von Personen als Meldestellenbeauftragte nach HinSchG und Beschwerdebeauftragte nach LkSG ist möglich.¹¹²

IV. Verhältnis Menschenrechts- zu Beschwerdebeauftragtem

- 58 Der Menschenrechtsbeauftragte ist verantwortlich für die Überwachung des LkSG-Risikomanagements, das auch das Beschwerdeverfahren einschließt. Der Beschwerdebeauftragte ist hingegen für die Durchführung des Beschwerdeverfahrens zuständig. Bei Personenidentität würde dies bedeuten, dass die durchführende Person sich selbst hinsichtlich der Wirksamkeit überwachen müsste, was unweigerlich einen Interessenkonflikt verursacht. Sofern der Menschenrechtsbeauftragte zugleich Beschwerdebeauftragter sein soll, ist sicherzustellen, dass die Überwachung des Beschwerdeverfahrens und dessen Wirksamkeitskontrolle von einer anderen Person durchgeführt wird.¹¹³

108 Artikel 30 der CS3D sieht jedoch vor, dass die dem HinSchG zugrunde liegende Richtlinie (EU) 2019/1937 auf die CS3D sowie die Meldung entsprechender Verstöße und den Schutz von Hinweisgebern erstreckt wird, sodass nach einer Integration der CS3D in das LkSG von einem Gleichlauf der Verfahren auszugehen ist.

109 *Bleckmann*, in: Thüsing, HinSchG, § 4 Rn. 11.

110 Unzutreffend insoweit: *André/Hildner*, in: Fischer/Pellmann/Schoch, HinSchG, § 4 Rn. 11, wonach sich der Hinweisgebende zu entscheiden hat, ob er den Schutz des LkSG oder des HinSchG beanspruchen möchte. Gemeint war wohl, dass dem Hinweisgebenden der Schutz nach §§ 35–37 HinSchG nur dann zusteht, wenn die interne oder externe Meldestelle genutzt wurde (§ 33 Abs. 1 Nr. 1 HinSchG).

111 Vgl. hierzu: *Handel*, Meldestellenbeauftragte, S. 14.

112 Ebenso: *Michaelis*, in: Fischer/Pellmann/Schoch, HinSchG, § 17 Rn. 44.

113 Im Ergebnis ebenso: *Stemberg*, in: Fleischer/Mankowski, LkSG, § 8 Rn. 83; *Wiedmann/Hoppmann* CCZ 2023, 11, 14; a. A. wohl: *Welling/Brouwer*, in: Spießhofer/Späth, LkSG, § 8 Rn. 48; *Wagner/Wagner*, in: Wagner/Rutloff/Wagner, LkSG, § 4 Rn. 665; *Grambow/Cimino*, AnwaltSpiegel 5/2023, 7, 9.

V. Fazit

Mit dem Menschenrechtsbeauftragten und dem Beschwerdebeauftragten hat das LkSG zwei neue Beauftragte eingeführt, die sich schon aufgrund des ihnen gewidmeten Beschreibungsumfang im Gesetzestext unterscheiden, ebenso wie der Aufgaben, Qualifikationsmerkmale und der Möglichkeit der externen Besetzung. Ist der Menschenrechtsbeauftragte aufgrund seiner reinen Überwachungsfunktion in dieser Ausgestaltung ein Novum, hat der Beschwerdebeauftragte im Unternehmen ein Pendant im Meldestellenbeauftragten nach dem HinSchG. Während der Beschwerdebeauftragte zugleich Meldestellenbeauftragter sein kann, ist eine Kombination des Beschwerdebeauftragten und des Menschenrechtsbeauftragten in einer Person wegen des Interessenskonfliktes zwischen operativer Gestaltung und Ausführung einerseits und der Überwachungsaufgabe andererseits zumindest im Überschneidungsbereich nicht möglich. 59

Da im Juli 2024 die CS3D als europäische Richtlinie im menschenrechtlichen und umweltbezogenen Bereich in Kraft getreten und nun in nationales Recht der Mitgliedstaaten umgesetzt werden muss, wird das LkSG entsprechend angepasst.¹¹⁴ Die CS3D nennt weder Menschenrechts- noch Beschwerdebeauftragte. Gleichzeitig macht die CS3D Vorgaben zur Umsetzung in nationales Recht.¹¹⁵ Danach kann der deutsche Gesetzgeber den Begriff des Menschenrechtsbeauftragten aus dem LkSG streichen, muss es aber nicht. Die Aufgabe des Menschenrechtsbeauftragten, nämlich die Überwachung des Risikomanagements ist auch in der CS3D vorgesehen.¹¹⁶ Da sich die Überwachung des Risikomanagements durch eine unabhängige, frei von Interessenkonflikten, betraute Funktion bewährt hat, bietet es sich bei der Umsetzung der CS3D an, die in Deutschland mittlerweile herausgebildeten Praktiken, also die Ernennung eines Menschenrechtsbeauftragten oder die Einsetzung eines Komitees, beizubehalten. Wünschenswert wäre, wenn bei der Umsetzung der CS3D Vorgaben zur Unabhängigkeit, Weisungsfreiheit und Verschwiegenheit des Menschenrechtsbeauftragten gemacht werden. Beim Beschwerdebeauftragten, der im LkSG namentlich nicht benannt ist, können die Qualifizierungsmerkmale in § 8 Abs. 3 LkSG nicht gestrichen werden, da dies eine Absenkung des Schutzniveaus aus Anlass der Umsetzung der CS3D darstellen würde und daher dem Verschlechterungsverbot von Art. 1 Abs. 2 CS3D unterliegt.¹¹⁷ 60

¹¹⁴ Zum Anpassungsbedarf des LkSG aufgrund der CS3D: *Hagel/Wiedmann*, CCZ 2024, 185–198.

¹¹⁵ Eine Übersicht zum Verschlechterungsverbot (Art. 1 Abs. 2 CS3D), dem Subsidiaritätsprinzip (Art. 1 Abs. 3 CS3D), der Vollharmonisierung (Art. 4 Abs. 1 CS3D) und der Mindestharmonisierung (Art. 4 Abs. 2 CS3D) findet sich bei: *Hagel/Wiedmann*, CCZ 2024, 185, 188.

¹¹⁶ Art. 15 CS3D.

¹¹⁷ Ausführlich dazu: *Hagel/Wiedmann*, CCZ 2024, 185, 196.

Teil 3

Besondere Aufgaben und Anwendungsfelder

20. Kapitel

Die Compliance-Funktion in einem Kreditinstitut*

I. Einleitung: Was ist die Bedeutung des Begriffs Compliance?

Der Begriff Compliance leitet sich aus dem Englischen „to comply with“ (zu Deutsch: „befolgen“ oder „einhalten“) ab und bedeutet die Einhaltung sämtlicher für das jeweilige Unternehmen relevanter gesetzlicher Bestimmungen, regulatorischer und selbst gesetzter ethischer Standards und Anforderungen.¹ Compliance umfasst damit die Gesamtheit aller Maßnahmen, die das rechtmäßige Verhalten des Unternehmens, der Organisation und der Mitarbeiter im Blick auf alle gesetzlichen Gebote und Verbote, Richtlinien und freiwilligen Kodizes im Unternehmen sicherstellen.² Darüber hinaus ist unter Compliance auch eine Methode oder Herangehensweise zur Sicherstellung rechtmäßigen und richtlinienkonformen Verhaltens aller Beteiligten eines Unternehmens (Compliance-Management-System, CMS) zu verstehen. Zu diesem Zweck ist die Etablierung einer entsprechenden Organisation (Compliance-Organisation) inkl. eines Compliance-Beauftragten erforderlich.³ Bei Kreditinstituten erstreckt sich der Begriff Compliance neben den allgemeinen Vorschriften insbesondere auch auf die speziellen Vorschriften wie bspw. des WpHG, MAR, LkSG,⁴ des KWG und des KAGB, die für die Kreditwirtschaft die Compliance-Anforderungen auf diese Industriesäule branchenspezifisch vorgeben.

Auch die EBA-Leitlinien zur internen Governance⁵ zielen insbesondere darauf ab, die internen Governance Regelungen, Prozesse und Mechanismen der Banken in der Europäischen Union (EU) weiter zu harmonisieren, das Verhältnismä-

* Dieser Beitrag stellt ausschließlich die persönliche Meinung der Verfasser dar und ist nicht zwingend auch die Auffassung der jeweiligen Arbeitgeber.

1 Zum Begriffsverständnis siehe → *Schulz*, Kap. 1 Rn. 1 ff.; *Eisele/Faust*, in: Ellenberger/Bunte, Bankrechts-Handbuch, § 89, Rn. 1; *Rothenhöfer*, in: Kümpel/Mülbert/Früh/Seyfried, Bankrecht und Kapitalmarktrecht, Rn. 13.400.

2 Siehe → *Schulz*, Kap. 1 Rn. 1. Der Deutsche Corporate Governance Kodex (DCGK) bspw. Compliance als die in der Verantwortung des Vorstands liegende Pflicht zur Einhaltung der gesetzlichen Bestimmungen und unternehmensinternen Richtlinien, <https://www.dcgk.de/de/ko dex.html> (zuletzt abgerufen am 18.7.2024).

3 *Renz*, BvD-News 2/2014, 26, 26.

4 Zum LkSG siehe → *Heske*, Kap. 18 sowie → *Hagel/Wiedmann*, Kap. 19.

5 EBA/GL/2021/05 vom 2.7.2021, https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2021/EBA-GL-2021-05%20Guidelines%20on%20internal%20governance/translations/1021314/GL%20on%20internal%20governance%20under%20CRD_DE%20-%20updated.pdf (zuletzt abgerufen am 18.7.2024).

Bigkeitsprinzip zu stärken und zusätzliche Maßnahmen zur Reduzierung von Risiken im Bankenbereich zu treffen.⁶

- 3 Compliance ist als zentrale Leitungsaufgabe eine originäre Zuständigkeit der gesamten Geschäftsleitung.⁷ Daraus resultiert, dass die Geschäftsleitung rechtskonform handeln muss und die Gesamtverantwortung für die Compliance-Funktion trägt. Die Geschäftsleitung kann zur Erfüllung dieser Pflicht einzelne Kontrollaufgaben an eine Compliance-Funktion delegieren, die Gesamtverantwortung verbleibt aber in jedem Fall bei der Geschäftsleitung und kann nicht delegiert werden.⁸ Damit ist der Compliance-Beauftragte unmittelbar der Geschäftsleitung zu unterstellen und muss an diese berichten.⁹ Gemäß Grundsatz 5 in A. 3 des Deutschen Corporate Governance Kodex (DCGK)¹⁰ muss der Vorstand von börsennotierten Unternehmen für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien sorgen sowie auch auf deren Beachtung im Unternehmen hinwirken. Ferner ist die Geschäftsleitung für ein rechtskonformes Verhalten der Mitarbeiter verantwortlich (Legalitätsprinzip¹¹). Somit fallen zum einen die Einrichtung und Überwachung eines effektiven und effizienten Compliance-Systems sowie dessen Gestaltung, Umsetzung, Überwachung und Weiterentwicklung als Kernaufgabe in die Gesamtverantwortung der Geschäftsleitung.¹² Aufgrund der bestehenden Vorbildfunktion der Geschäftsleitung gegenüber ihren Mitarbeitern müssen und sollten sie sich an alle vorgeschriebenen Regelungen halten (Tone at the Top).¹³ Das U.S.-amerikanische Department of Justice (DOJ) spricht mittlerweile von einem sog. „Conduct at the Top“, da es in vielen (Compliance-)Fällen um einen „misconduct“ geht.¹⁴

II. Welche Compliance-Funktionen gibt es in einem Kreditinstitut?

- 4 Um einen umfassenden Compliance-Bereich in einem Kreditinstitut effizient aufzubauen und (aufsichts-)rechtlich konform auszugestalten, müssen verschie-

6 Renz/Brenner, in: Gebauer/Kirschhöfer/Repke, Compliance Miszellen – Dieter Eisele zum 80. Geburtstag gewidmet, S. 295.

7 Fleischer, CCZ 2008, 1, 3; Hauschka/Galster/Marschlich, CCZ 2014, 242, 243. Siehe auch → Schulz, Kap. 1 Rn. 2, 36 ff.

8 Koch, in: Koch, Aktiengesetz, 17. Aufl. 2023, §76 Rn. 12; Ghassemi-Tabar, in: Ghassemi-Tabar, DCGK, G5 Rn. 20 f.

9 Kramer/Renz/Hartz/Braun, BvD-News 1/2015, 12, 12.

10 Der DCGK fasst die wesentlichen gesetzlichen Vorgaben sowie die international und national anerkannten Standards zur Unternehmensleitung und -überwachung von börsennotierten Gesellschaften zusammen.

11 → Schulz, Kap. 1 Rn. 36 f. m. w. N.; → Böttger, Kap. 2 Rn. 116 m. w. N.

12 Bretschneider, in: Renz/Hense/Marbeiter, Wertpapier-Compliance in der Praxis, I.1. Rn. 10 ff.

13 Bretschneider, in: Renz/Hense/Marbeiter, Wertpapier-Compliance in der Praxis, I.1. Rn. 11; Wiedmann/Greubel, CCZ 2019, 88, 88. Siehe auch → Schulz, Kap. 1 Rn. 69.

14 U.S. Department of Justice Criminal Division – Evaluation of Corporate Compliance Programs (Updated March 2023), Seite 9; <https://www.justice.gov/criminal-fraud/page/file/937501/download> (zuletzt abgerufen am 18.7.2024).

dene Themengebiete und Aspekte berücksichtigt werden. Diese setzen sich aus den für Kreditinstitute allgemein gültigen Compliance-Anforderungen nach den Mindestanforderungen an das Risikomanagement (MaRisk) sowie den speziellen Anforderungen für Wertpapierdienstleistungsunternehmen nach §§ 63 ff. WpHG und den BaFin-Auslegungen zu den Mindestanforderungen an die Compliance-Funktion (MaComp) zusammen.¹⁵ Ferner müssen die Funktionen Datenschutz nach der Datenschutz-Grundverordnung (DSGVO), ein Hinweisgebersystem sowie die „Zentrale Stelle“ zur Koordination der Prävention von Geldwäsche, Terrorismusfinanzierung und sonstigen strafbaren Handlungen nach § 25h KWG ordnungsgemäß eingerichtet sein. Der Organisationsbereich Compliance umfasst demzufolge zusammenfassend im Wesentlichen fünf Säulen mit folgenden Themenbereichen:

1. Kapitalmarkt-Compliance,
2. Zentrale Stelle/sonstige strafbare Handlungen (inkl. Geldwäscheprävention) sowie Finanzsanktionen und Embargo (Anti-Financial Crime (AFC)),¹⁶
3. MaRisk-Compliance,
4. Hinweisgebersystem (Whistleblowing),
5. Datenschutz.

Daneben werden häufig noch andere Funktionen einer Compliance-Funktion zugeordnet wie bspw. Single Officer, IT-Security, Information Security, Auslagerungskontrollen der Second Line, Internes Kontrollsystem (IKS), Reputationsrisikomanagement, Verhaltensrisikomanagement (Conduct Risk), Kartell-Compliance etc., manchmal auch die ESG-Funktion oder auch die LkSG-Beauftragten-Funktion.

1. Kapitalmarkt-Compliance

Nach AT 6 der MaComp haben Wertpapierdienstleistungsunternehmen angemessene Grundsätze aufzustellen, Mittel vorzuhalten und Verfahren einzurichten, die darauf ausgerichtet sind, sicherzustellen, dass das Unternehmen selbst und seine Mitarbeiter den Verpflichtungen nach dem WpHG nachkommen. Dies erfordert insbesondere die Einrichtung einer dauerhaften und wirksamen, prozessbegleitenden als auch präventiv vorgehenden Kapitalmarkt-Compliance-Funktion, auch Kapitalmarkt-Compliance-Funktion genannt. Diese ist in Art. 22 Delegierte Verordnung (EU) 2017/565 i.V.m. BT 1 der MaComp geregelt und beschränkt sich im Gegensatz zu anderen Compliance-Organisationseinheiten ausschließlich auf Wertpapierdienstleistungen und -nebenleistungen sowie weiteren Vorschriften des WpHG, insbesondere die Marktmissbrauchsüberwachung.¹⁷ Die Geschäftsleitung hat einen Kapitalmarkt-Compliance-Beauf-

¹⁵ MaRisk in der Fassung vom 29.5.2024; MaComp in der Fassung vom 28.2.2024; Dokumente abrufbar unter www.bafin.de (zuletzt abgerufen am 18.7.2024).

¹⁶ Zur sog. Sanctions Compliance siehe → *Salathé/Moussaoui*, Kap. 24.

¹⁷ §§ 25 ff. WpHG.

tragten (Compliance-Beauftragter) zu ernennen, der gemäß § 87 Abs. 5 WpHG bei der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) mittels Meldung im BaFin-MVP Portal zu registrieren ist. Die Anzeige hat vor der tatsächlichen Aufnahme der Tätigkeit zu erfolgen. Ändern sich die von dem Wertpapierdienstleistungsunternehmen angezeigten Verhältnisse, sind die neuen Verhältnisse unverzüglich anzuzeigen. Dieser muss, ebenso wie die übrigen Mitarbeiter der Compliance-Funktion seine Aufgaben unabhängig wahrnehmen und ist lediglich der Geschäftsleitung unterstellt. Andere Bereiche unterhalb der Geschäftsleitung dürfen ihm daher keine Weisungen erteilen.¹⁸ Die Stellung der Compliance-Funktion spiegelt sich somit insbesondere in drei Säulen wider:¹⁹

1. **Unabhängigkeit:** Fachliche Unabhängigkeit, organisatorische und persönliche Unabhängigkeit;
 2. **Wirksamkeit:** Einbindung in Informationsflüsse, Fachkenntnisse, Personal- und Sachausstattung, Vertretung des Compliance-Beauftragten, Organisations- und Arbeitsanweisungen;
 3. **Dauerhaftigkeit.**
- 7 Nach den EBA-Leitlinien zur internen Governance²⁰ sollte der Compliance-Beauftragte ferner auch über einen angemessenen Status (Ansehen, Autorität und Befugnisse) verfügen und berechtigt sein, Compliance-Vorgaben in der Bank erfolgreich durchzusetzen und evtl. Interessenkonflikte zu entschärfen oder zu lösen.²¹
- 8 Eine Kombination der Kapitalmarkt-Compliance-Funktion mit weiteren Kontrolleinheiten (bspw. dem Risikocontrolling) eines Instituts ist grundsätzlich dann zulässig, wenn hierdurch die Wirksamkeit und Unabhängigkeit der Kapitalmarkt-Compliance-Funktion nicht beeinträchtigt wird.²² Dies ist gerade bei einer Kombination mit der Organisationseinheit für Datenschutz zweifelhaft, da sie der eigentlichen Funktion der Kapitalmarkt-Compliance zuwiderlaufen würde, sodass eine Kombination zu vermeiden ist. Möglich und zudem sinnvoll ist eine Kombination mit der MaRisk-Compliance-Funktion. Jedes Unternehmen muss jegliche Kombination unter Angabe der Gründe für die Kombination prüfungstechnisch nachvollziehbar dokumentieren.
- 9 Eine Anbindung an die Interne Revision ist grundsätzlich nicht statthaft, da diese die Kapitalmarkt-Compliance-Funktion neutral zu prüfen hat und durch eine Kombination beider Funktionen die erforderliche Unabhängigkeit nicht mehr gewährleistet wäre (vgl. BT 1.3.3.2 Tz. 2 der MaComp). Die Compliance-Funktion ist Teil des bankinternen IKS, wohingegen die Interne Revision nicht Teil

18 Röh, BB 2008, 398, 403; Spindler, WM 2008, 905, 911.

19 Schäfer, BKR 2011, 45, 45 f.

20 EBA/GL/2021/05, Nr. 204 ff.

21 Renz/Brenner, in: Gebauer/Kirschhöfer/Repke, Compliance-Miszellen, S. 295, 311.

22 Schäfer, BKR 2011, 187, 189.

des bankinternen IKS ist, sondern dieses prozessneutral auf seine Funktionsfähigkeit prüft.²³

Environmental, Social und Governance (ESG) (zu Deutsch Umwelt, Soziales und Unternehmensführung)²⁴ bezeichnet ein umfassendes Regelwerk zur Bewertung der nachhaltigen und ethischen Praxis von Unternehmen und hat in den letzten Jahren erheblich an Bedeutung gewonnen. Unternehmen erkennen nämlich zunehmend, dass ESG-Faktoren finanzielle Risiken und Chancen beeinflussen können. Durch die Integration von ESG-Kriterien in ihre Anlagestrategien können die Unternehmen identifiziert werden, die langfristig nachhaltig und erfolgreich sein können. **10**

Diese drei oben genannten ESG-Kriterien sollen sicherstellen, dass Unternehmen nachhaltig agieren. Zu den wesentlichen regulatorischen Vorgaben zählen hierbei insbesondere:²⁵ **11**

- BaFin Merkblatt zum Umgang mit Nachhaltigkeitsrisiken,²⁶
- Taxonomie-Verordnung,²⁷
- Offenlegungs-Verordnung,²⁸
- Corporate Sustainability Reporting Directive (CSRD, Nachhaltigkeitsberichterstattung),²⁹
- ESMA-Leitlinien zu Nachhaltigkeitspräferenzen im Wertpapierkundengeschäft:³⁰
 - Berücksichtigung von Nachhaltigkeitsrisiken in ihren organisatorischen Strukturen und im Risikomanagement;

23 Siehe hierzu § 25a Abs. 1 Satz 3 Nr. 3 KWG. Zum IKS siehe auch → *Bartuschka*, Kap. 11.

24 Siehe zu diesem Themenkomplex insbesondere: *Trickes/Renz*, in: *Bankrecht und Bankpraxis*, Kapitel 16.1 Compliance in der Fassung von 2024.

25 *Trickes/Renz*, in: *Bankrecht und Bankpraxis*, 2024, Kapitel 16.1, Rn. 22a.

26 BaFin, Merkblatt zum Umgang mit Nachhaltigkeitsrisiken, Stand 13.1.2020.

27 Die Verordnung 2020/852 (<https://eur-lex.europa.eu/eli/reg/2020/852/oj?locale=de>; zuletzt abgerufen am 18.7.2024) enthält Kriterien zur Bestimmung, ob eine Wirtschaftstätigkeit als ökologisch nachhaltig einzustufen ist (Taxonomie), um damit den Grad der ökologischen Nachhaltigkeit einer Investition ermitteln zu können.

28 Die Verordnung 2019/2088 (<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32019R2088>; zuletzt abgerufen am 18.7.2024) regelt die Offenlegungspflichten von Finanzdienstleistern bzgl. der Berücksichtigung von Nachhaltigkeitsthemen in ihren Strategien, Prozessen und Produkten. Die im Rahmen des Rechtsrahmens für nachhaltige Finanzierungen erlassene Verordnung über Offenlegungspflichten legt harmonisierte Transparenzvorschriften für Finanzmarktteilnehmer und Finanzberater fest, wie sie die Faktoren Umwelt, Soziales und eine gute Unternehmensführung in ihre Investitionsentscheidungen und Finanzberatung sowie in ihre allgemeinen und produktbezogenen Nachhaltigkeitsziele einbeziehen.

29 <https://www.csr-in-deutschland.de/DE/CSR-Allgemein/CSR-in-der-Praxis/CSR-Berichterstattung/Standards/standards.html> (zuletzt abgerufen am 18.7.2024). Siehe hierzu auch → *Beisheim*, Kap. 16.

30 Mit der Änderungsverordnung (EU) 2021/1253 wurden im April 2021 u. a. die Pflichten von Wertpapierdienstleistungsunternehmen in diesem Zusammenhang in die delegierte Verordnung (EU) Nr. 2017/565 zu MiFID II („DelVO“) aufgenommen.

Teil 3 Besondere Aufgaben und Anwendungsfelder

- Nachhaltigkeitspräferenzen im Rahmen ihrer Feststellungen zu Interessenkonflikten Rechnung zu tragen; und
 - Ermittlung von Nachhaltigkeitspräferenzen ihrer Kundinnen und Kunden insbesondere bei Erbringung der Anlageberatung oder Portfolioverwaltung.
- 12 Die Vielfältigkeit dieser regulatorischen Anforderungen führt nicht nur in der Kreditwirtschaft zu komplexen Prozessen in einer Organisation, die es auch und gerade durch eine holistisch agierende Compliance-Funktion in den Griff zu bekommen gilt. Auch auf diese Entwicklungen hat eine Compliance-Organisation in den jeweiligen Unternehmen einzugehen, auf die Einhaltung der relevanten Vorgaben hinzuwirken und sowohl ihre Schulungs- und Beratungsaktivitäten als auch vor allem ihre Überwachungstätigkeiten auszurichten.³¹
- 13 Am 29.6.2023 ist die Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (Markets in Crypto-Assets Regulation – MiCAR) in Kraft getreten. Die Europäische Kommission hatte den Legislativvorschlag zur MiCAR am 24.9.2020 als Teil des Pakets zur Digitalisierung des Finanzsektors (Digitalisierungspaket³²) im Europäischen Wirtschaftsraum (EWR) vorgelegt.
- 14 MiCAR verfolgt das Ziel, einen harmonisierten europäischen Regulierungsrahmen für Kryptowerte zu schaffen, der Innovationen fördert und die Nutzung des Potenzials von Kryptowerten unter Wahrung der Finanzstabilität und des Anlegerschutzes ermöglicht.³³ MiCAR gilt für alle natürlichen, juristischen Personen und andere Unternehmungen,³⁴ die Kryptowerte ausgeben, öffentlich anbieten und zum Handel anbieten oder sonstige Dienstleistungen im Zusammenhang mit Kryptowerten anbieten.³⁵ Grundsätzlich fällt damit jede öffentliche Aktivität in Bezug auf Kryptowerte unter das MiCAR-Regime.³⁶
- 15 Im Einzelnen regelt die MiCAR Transparenz- und Offenlegungspflichten für die Emission und den Handel mit Kryptowerten, die Zulassungspflicht und laufende Aufsicht über Kryptowerte-Dienstleister (Crypto Asset Service Provider –

31 *Trickes/Renz*, in: Bankrecht und Bankpraxis, 2024, Kapitel 16.1, Rn. 22a.

32 *Siadat*, RdF 2021, 12.

33 *Trickes/Renz*, in: Bankrecht und Bankpraxis, 2024, Kapitel 16.1, Rn. 90a.

34 Hierzu zählen bspw. Dezentrale Autonome Organisationen (DAOs); DAOs sind 1. Gemeinschaften im Besitz der Mitglieder ohne zentralisierte Führung; 2. ein sicherer Weg, um mit Internetfremden zusammenzuarbeiten; 3. ein sicherer Ort, um Geld für eine bestimmte Sache zu spenden. Eine DAO ist daher eine Blockchain-gesteuerte Organisation in kollektivem Besitz, die auf eine gemeinsame Mission hinarbeitet. DAOs ermöglichen es, mit Gleichgesinnten auf der ganzen Welt zusammenzuarbeiten, ohne einem wohlwollenden Führer bei der Verwaltung der Gelder oder des Betriebs zu vertrauen. Vgl. <https://ethereum.org/en/dao/> (zuletzt abgerufen am 18.7.2024).

35 Vgl. Art. 2 Abs. 1 MiCAR.

36 Vgl. Simmons+Simmons, Regulierung der Märkte für Krypto-Assets (MiCA) auf einen Blick, <https://www.simmons-simmons.com/en/publications/cl9fmmv9666h0b969l64d1dn/regulierung-der-markte-fur-krypto-assets-mica-auf-einen-blick> (zuletzt abgerufen am 18.7.2024).

CASP) und Emittenten von Kryptowerten. Ferner enthält die MiCAR Vorgaben für die ordnungsgemäße Geschäftsorganisation von Kryptowerte-Emittenten sowie Kryptowerte-Dienstleistern, Investoren- und Verbraucherschutzvorschriften für die Emission, den Handel und die Verwahrung von Kryptowerten sowie Vorschriften zur Bekämpfung von Marktmissbrauch auf Krypto-Handelsplätzen.³⁷

2. Zentrale Stelle/sonstige strafbare Handlungen (inkl. Geldwäscheprävention) sowie Finanzsanktionen und Embargo (Anti-Financial Crime (AFC))

Gemäß § 6 Abs. 1 GwG müssen Kreditinstitute angemessene interne Sicherungsmaßnahmen treffen, um zu verhindern, dass sie zur Geldwäsche und zur Terrorismusfinanzierung missbraucht werden können. Daher sind angemessene geschäfts- und kundenbezogene Sicherungssysteme zu schaffen, laufend zu aktualisieren und Kontrollen durchzuführen, die die Einhaltung dieser Sicherungssysteme gewährleisten. Zudem haben gemäß § 25h Abs. 2 KWG die Kreditinstitute angemessene Datenverarbeitungssysteme zu betreiben und zu aktualisieren, mittels derer sie in der Lage sind, Geschäftsbeziehungen und einzelne Transaktionen im Zahlungsverkehr zu erkennen, die aufgrund des öffentlichen und im Kreditinstitut verfügbaren Erfahrungswissens über die Methoden der Geldwäsche, der Terrorismusfinanzierung und sonstigen strafbaren Handlungen besonders komplex oder groß sind, ungewöhnlich ablaufen oder ohne offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck erfolgen. **16**

Des Weiteren sind den Kreditinstituten eine Vielzahl von Sorgfaltspflichten auferlegt. Sie müssen bspw. Informationen über die Identität ihrer Vertragspartner bzw. der wirtschaftlich Berechtigten einholen (Know-your-Customer-Prinzip)³⁸ und ihre Geschäftsbeziehungen auf Auffälligkeiten überwachen. Um diese Aufgaben zur Geldwäscheprävention erfüllen zu können, müssen Kreditinstitute nach § 7 Abs. 1 GwG einen der Geschäftsleitung unmittelbar nachgeordneten Geldwäschebeauftragten bestellen.³⁹ Seit dem am 1.1.2015 in Kraft getretenen § 25h Abs. 7 Satz 1 KWG werden die Funktion des Geldwäschebeauftragten und die Pflichten zur Verhinderung der sonstigen strafbaren Handlungen i. S. d. § 25h Abs. 1 Satz 1 nunmehr im Institut von einer Stelle wahrgenommen. Damit wurden die vormals getrennten Teilbereiche der Geldwäsche- und Betrugsprävention zur Zentralen Stelle zusammengefasst.⁴⁰ **17**

Auch in anderen Ländern bestehen umfangreiche Regelungen zur Verhinderung von Geldwäsche, Terrorismusfinanzierung oder sonstigen strafbaren Handlungen. Eines der schärfsten Anti-Korruptionsgesetze ist in Großbritannien zum **18**

³⁷ *Trickes/Renz*, in: Bankrecht und Bankpraxis, 2024, Kapitel 16.1, Rn. 90b.

³⁸ *Diergarten*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 34 Rn. 45 ff.

³⁹ *Grützner/Jakob*, in: Compliance von A–Z, „Geldwäschebeauftragter“.

⁴⁰ *Achtelik*, in: Fischer/Schulte-Mattler, KWG, CRR, § 25h KWG Rn. 26.

1.7.2011 in Kraft getreten. Der UK Bribery Act⁴¹ stellt neben der aktiven und passiven Bestechung für natürliche und juristische Personen auch die Bestechung ausländischer Amtsträger unter Strafe sowie das Versäumnis, Bestechung zu vermeiden. Eine Besonderheit liegt darin, dass er nicht nur für britische Unternehmen gilt, sondern für alle, die in irgendeiner Form in Großbritannien Geschäfte tätigen.⁴² Als Folge des UK Bribery Act wurde von Unternehmen fortan erwartet:⁴³

1. Risikobewertung der Korruptionsrisiken,
2. Verpflichtung der Mitarbeiter durch das Top-Management zur Korruptionsprävention,
3. Beachtung der gebührenden Sorgfalt bei Auswahl und Überwachung von Geschäftspartnern (Due Diligence),
4. klare, praktische und verfügbare Richtlinien und Vorgehensweisen,
5. effektive Einführung bzw. Umsetzung des Compliance-Programms,
6. Überwachung und (externe) Überprüfung des Compliance-Programms.

- 19 In den USA gilt der Foreign Corrupt Practices Act (FCPA),⁴⁴ ein Gesetz zur Korruptionsbekämpfung, das Zahlungen und Wertgeschenke an ausländische staatliche Amtsträger verbietet.⁴⁵ Darüber hinaus verpflichtet das Gesetz alle in den USA börsennotierten Unternehmen dazu, eine Buchführung vorzunehmen, die auf die Antikorruptionsregeln des FCPA abgestimmt ist.⁴⁶ Der Grund hierfür liegt darin, dass in der Vergangenheit Schmiergeldzahlungen jeweils entweder gar nicht in den Büchern der Unternehmen verzeichnet oder dort falsch ausgewiesen waren. Deshalb stellt der FCPA nicht allein das Zahlen von Bestechungsgeldern unter Strafe, sondern auch das Anlegen falscher oder irreführender Einträge in die Unternehmensunterlagen. Die Vorschriften zur Bestechungsbekämpfung des FCPA gelten für Emittenten, inländische Unternehmen und Personen sowie bestimmte natürliche bzw. juristische Personen, die in den territorialen Zuständigkeitsbereich fallen.⁴⁷ Die Bestimmungen verbieten US-Personen und US-Unternehmen, nach US-Recht gegründeten Unternehmen, Unternehmen mit Hauptniederlassung in den USA, Unternehmen, deren Aktien an US-Börsen notiert sind, und Unternehmen, die einer regelmäßigen Berichtspflicht gegenüber der US-Wertpapier- und Börsenaufsichtsbehörde SEC unterliegen, sowie bestimmten ausländischen natürlichen Personen und Unternehmen bei Tätigkeit im Hoheitsgebiet der USA, Korruptionszahlungen an ausländische Amtsträger zu leisten, um den Zuschlag für Geschäftsabschlüsse zu erhalten oder zu wahren.

41 <https://www.legislation.gov.uk/ukpga/2010/23> (zuletzt abgerufen am 18.7.2024).

42 Hugger/Röhrich, BB 2010, 2643, 2646.

43 Pörnbacher/Mark, NZG 2010, 1372, 1375.

44 <https://www.justice.gov/criminal-fraud/file/1292051/download> (zuletzt abgerufen am 18.7.2024).

45 Cohen/Holland, CCZ 2008, 7, 7.

46 Spehl/Grützner, CCZ 2013, 198, 201.

47 Passarge, in: Martinek/Semler/Flohr, Handbuch des Vertriebsrechts, § 79 Rn. 122.

Darüber hinaus sind immer Finanzsanktionen und Embargos zu berücksichtigen.⁴⁸ Embargos umfassen hoheitliche (Handels-)Maßnahmen (Totalembargos, Teilembargos und Waffenembargos) gegenüber anderen Staaten. Eine spezielle Form des Embargos sind dabei Finanzsanktionen. Damit soll der Zugang zu Finanzmitteln oder wirtschaftlichen Ressourcen gegenüber bestimmten Personen, Organisationen und Einrichtungen bewirkt werden. Grundlage deutscher Sanktionen können Entscheidungen der Vereinten Nationen, der Europäischen Union oder inländischer Behörden sein.⁴⁹ Der Verstoß gegen (Finanz-)Sanktionen kann als Ordnungswidrigkeit und in bestimmten Fällen auch als Straftat geahndet werden.⁵⁰ **20**

Seit dem 1.1.2023 gilt das Lieferkettensorgfaltspflichtengesetz (LkSG),⁵¹ das auch von Kreditinstituten einzuhalten ist und zusätzliche Maßnahmen erfordert, wie bspw. die Benennung eines Menschenrechtsbeauftragten. Ziel des Gesetzes ist, die Globalisierung von Lieferketten sozialer zu gestalten und damit Menschenrechte und die Umwelt zu schützen. Kreditinstitute sowie alle in Deutschland ansässigen relevanten Unternehmen müssen daher diverse Maßnahmen ergreifen, um Risiken in Bezug auf die Lieferkette und Dienstleister im Blick zu behalten. Das umfasst alle Produkte und Dienstleistungen des Unternehmens.⁵² Die Verantwortung für die Einhaltung des LkSG liegt in vielen Kreditinstituten in der Zentralen Stelle von Compliance. **21**

Der Menschenrechtsbeauftragte berichtet, wie der Geldwäsche- und Wertpapier-Compliance-Beauftragte auch, direkt an die Geschäftsleitung.⁵³ Ähnlich wie es auch die MaComp vorsieht, müssen Kreditinstitute ein Beschwerdeverfahren für potenziell Betroffene, etwa von Menschenrechtsverletzungen, einrichten. Hierfür verwenden Kreditinstitute bestehende Hinweisgebersysteme und passen diese auf die Anforderungen des LkSG an. **22**

In den Trilog-Verhandlungen zur Corporate Sustainability Due Diligence Directive („CSDDD“, auch CS3D) wurde diskutiert, ob der Finanzsektor, z. B. Kreditinstitute, Asset-Manager und Investmentfirmen, von der CSDDD ausgenommen werden soll. Aktuell sollen auch Unternehmen des Finanzsektors die Sorgfaltspflichten im eigenen Geschäftsbereich und gegenüber den Zulieferern **23**

48 Generell hierzu: *Eggers/Haak*, CB 2022, 416 sowie → *Salathé/Moussaoui*, Kap. 24. Zu den Aufgaben der Compliance-Funktion hierzu: Deutsche Bundesbank, Merkblatt zur Einhaltung von Finanzsanktionen, Stand Juli 2021, S. 9 f.

49 Unternehmen mit US-Nexus sollten auch die Vorgaben des Office of Foreign Assets Control (OFAC) beachten, siehe Home Office of Foreign Assets Control (treasury.gov) (zuletzt abgerufen am 18.7.2024).

50 Deutsche Bundesbank, Merkblatt zur Einhaltung von Finanzsanktionen, Stand von Juli 2021, S. 3.

51 Vgl. zu den Inhalten des LkSG und dem Einsatz von ISO-Standards *Renz/Spallek*, *Comply* 202, 26 ff. sowie → *Heske*, Kap. 18.

52 https://www.bafa.de/DE/Lieferketten/FAQ/haeufig_gestellte_fragen_node.html (zuletzt abgerufen am 18.7.2024).

53 Zu Menschenrechtsbeauftragten siehe → *Hagel/Wiedmann*, Kap. 19.

(upstream) erfüllen und im Rahmen eines Übergangsplans dazu beitragen, das Klimaschutzziel des Pariser Klimaabkommens zu erreichen; die Kommission wird überprüfen, ob der Finanzsektor zukünftig vollständig unter die CSDDD fallen wird.⁵⁴

3. MaRisk-Compliance

- 24** Basierend auf den damals durch die CRD IV⁵⁵ (Capital Requirements Directive – EU-Eigenkapitalrichtlinie) veranlassten KWG-Änderungen wurde über die daraus folgende MaRisk-Novelle in 2017 eine neue erweiterte Compliance-Funktion für Kreditinstitute geschaffen. Gemäß AT 4.4.2 der MaRisk muss jedes Kreditinstitut über eine Compliance-Funktion verfügen, um den Risiken, die sich aus der Nichteinhaltung rechtlicher Regelungen ergeben können, entgegenzuwirken. Die Compliance-Funktion bekam daher erstmals den Status einer besonderen Funktion i. S. d. MaRisk und wird systematisch auf Augenhöhe mit den Funktionen Risikocontrolling und Interne Revision eingeordnet.⁵⁶ Somit kommt es zu einer Bündelung und zentralen Identifizierung aller rechtlichen Regelungen und Vorgaben, denen das Unternehmen im Rahmen der Ausübung seiner verschiedenen Aufgaben auf unterschiedlichen Märkten unterliegt. Im Zuge der damaligen 5. MaRisk-Novelle haben systemrelevante Institute für die Compliance-Funktion zwingend eine eigenständige Organisationseinheit einzurichten.⁵⁷
- 25** Zur Erreichung der vorgenannten Ziele und Gewährleistung einer effektiven Wahrnehmung ihrer Aufgaben müssen der MaRisk-Compliance-Funktion ausreichende Befugnisse und uneingeschränkter Informationszugang eingeräumt werden.⁵⁸ Die MaRisk-Compliance-Funktion ist unabhängig und nach AT 4.4.2 Tz. 3 der MaRisk unmittelbar der Geschäftsleitung zu unterstellen und ist dieser gegenüber berichtspflichtig. Dieser Bericht hat Ausführungen zur Angemessenheit und Wirksamkeit der aufbau- und ablauforganisatorischen Regelungen, die die Einhaltung der identifizierten wesentlichen rechtlichen Regelungen und Vorgaben gewährleisten sollen, zu enthalten. Darüber hinaus müssen in dem Bericht auch festgestellte Mängel sowie Maßnahmen zu deren Behebung enthalten sein.

54 Siehe zu diesem Komplex *Gergen/Fitzer/Theusinger/Pour Rafsendjani*, in: Noerr, Europäisches Lieferkettengesetz (CSDDD) auf der Zielgerade, abzurufen unter Europäisches Lieferkettengesetz (CSDDD) auf der Zielgeraden (noerr.com) (zuletzt abgerufen am 18.7.2024).

55 Am 7.6.2019 wurde die CRD V veröffentlicht und die CRD VI/CRR III wurden am 19.6.2024 veröffentlicht, CRD VI: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_2024016916; CRR III: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401623 (beides zuletzt abgerufen am 18.7.2024).

56 *Weber-Rey*, CCZ 2014, 97, 97.

57 *Hannemann/Steinbrecher/Weigl*, Mindestanforderungen an das Risikomanagement (MaRisk), AT 4.4 Rn. 6.

58 *Schäfer*, in: Park, Kapitalmarktrecht, Teil 2, Kap. 2.2 Rn. 85.

Die MaRisk-Compliance-Funktion hat auf die Implementierung wirksamer Verfahren zur Einhaltung der für das Institut wesentlichen rechtlichen Regelungen und Vorgaben und entsprechender Kontrollen hinzuwirken und dies aufgrund ihrer Stellung als Second Line im Rahmen des IKS zu überwachen.⁵⁹ Wesentlich sind danach alle Regelungen, deren Nichteinhaltung zur Gefährdung des Vermögens des Instituts führen kann, womit nicht sämtliche Regelungen, die ein Institut zu beachten hat, in den Aufgabenbereich der Compliance-Funktion fallen.⁶⁰ Die Identifizierung der wesentlichen rechtlichen Regelungen und Vorgaben, deren Nichteinhaltung zu einer Gefährdung des Vermögens des Instituts führen kann, erfolgt unter Berücksichtigung von Risikogesichtspunkten in regelmäßigen Abständen durch die Compliance-Funktion.⁶¹ Das bedeutet, dass die Compliance-Funktion (1) die wesentlichen rechtlichen Regelungen und Vorgaben identifizieren muss, (2) eine Risikoanalyse im Hinblick auf ihre Einhaltung durch die betroffenen Einheiten zu erstellen lassen hat, (3) sich mitteilen lassen muss, ob es einen Kontrollrahmen der betreffenden Einheiten zur Einhaltung der wesentlichen rechtlichen Regelungen und Vorgaben gibt, (4) Angaben zu möglichen Defiziten und zu Maßnahmen zu deren Behebung einholen muss und (5) in ihrem Bericht an die Geschäftsleitung, den Aufsichtsrat und die Interne Revision festhalten muss. Der Fokus der wesentlichen rechtlichen Regelungen und Vorgaben soll nicht nur auf neuen bzw. zukünftigen Regelungen liegen, sondern auch bereits bestehende rechtliche Regelungen und Vorgaben (inkl. Rechtsprechung) umfassen, sofern diese Einfluss für das Compliance-Risiko für das Institut haben können.⁶² Die inhaltlichen rechtlichen Themenbereiche der MaRisk-Compliance-Funktion sind demnach nach einem proportional angemessenen Ansatz umzusetzen. Diesem Ansatz wird man dadurch gerecht, indem das Institut die Compliance-Risiken identifiziert. Eine konkrete Definition hierfür existiert nicht, wobei sie sich insbesondere dadurch auszeichnen, dass bei einer Nichtbeachtung von rechtlichen Regelungen und Vorgaben vor allem Strafen (Bußgelder), Schadensersatzansprüche und/oder die Nichtigkeit von Verträgen drohen, die zu einer Gefährdung des Vermögens des Instituts führen können. Somit ist eine fortlaufende Bestandsaufnahme im Hinblick auf alle relevanten Regelungsbereiche und Vorgaben der MaRisk-Compliance-relevanten Bereiche und Aufgabengebiete institutsspezifisch erforderlich. Dies kann zur Folge haben, dass einige Themengebiete schon durch andere Kontroll- und Stabseinheiten abgedeckt sind und wiederum andere Themengebiete bereits Aufgabe von speziellen Compliance-Funktionen sind (Kapitalmarkt-Compliance-Funktion, Zentrale Stelle etc.). Die bislang in einem Kreditinstitut noch nicht zugewiesenen Aufgaben und Verantwortlichkeiten werden von der MaRisk-Compliance-Funktion auf Basis der für das Institut bestehenden rechtlichen Regularien im Rahmen einer Risikoanalyse einer Risikobetrachtung unterzogen und das Ergeb-

59 *Boldt/Büll/Voss*, CCZ 2013, 248, 251.

60 *Gebauer/Niermann*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 48 Rn. 22.

61 *Braun*, in: Fischer/Schulte-Mattler, KWG, CRR-VO, KWG § 25a Rn. 435.

62 *Renz*, in: Schäfer/Sethe/Lang, Handbuch der Vermögensverwaltung, § 16 Rn. 93.

nis wird an den Vorstand berichtet. Zudem wirkt die MaRisk-Compliance-Funktion darauf hin, dass für alle identifizierten wesentlichen rechtlichen Regelungen und Vorgaben eindeutige Zuständigkeiten bestehen und bei ggf. bestehenden Risiken eine Risikoverantwortung zugeordnet ist.⁶³ Damit stellt die MaRisk-Compliance-Funktion eine Klammerfunktion zu bereits bestehenden Compliance-Funktionen dar.

- 27 Die MaRisk-Compliance-Funktion befasst sich als Teil des bankweiten Risikomanagements mit der Vermeidung von Compliance-Risiken. Daher obliegt der MaRisk-Compliance-Funktion die Überwachung der Fachbereiche dahingehend, ob diese ihren Pflichten nachkommen und rechtliche relevante Regelungsbereiche mit Handlungsbedarf „zugewiesen“ werden. Die Durchführung von Kontrollhandlungen durch die Compliance-Funktion ist nach dem Wortlaut der MaRisk zwar nicht gesondert vorgeschrieben. Dennoch ist es unter MaRisk-Aspekten ebenfalls erforderlich,⁶⁴ analog zu den MaComp, die explizit einen Überwachungsplan und daraus abgeleitete risikobasierte Überwachungshandlungen fordern, dass die MaRisk-Compliance-Funktion Kontrollhandlungen durchführt und ihr die hierfür notwendigen Kontrollrechte eingeräumt werden. Die MaRisk-Compliance-Funktion kann nur dann (weitestgehend) auf eigene Prüfprozesse verzichten, wenn die anderen bereits genannten Funktionen eigene Kontrollhandlungen vornehmen und diese risikobasiert ausreichend sind.

4. Hinweisgebersystem (Whistleblowing)

- 28 Hinweise sind ein sehr wichtiges Instrument zur Aufdeckung von Verstößen gegen aufsichtsrechtliche Bestimmungen und Missständen im Unternehmen.⁶⁵ Hinweisgeber können daher wertvolle Beiträge dazu leisten, das Fehlverhalten einzelner Personen oder ganzer Unternehmen aufzudecken und die negativen Folgen dieses Fehlverhaltens einzudämmen bzw. zu korrigieren. Damit potenzielle Hinweisgeber die von ihnen wahrgenommenen Missstände aufdecken, bedürfen sie allerdings eines effektiven gesetzlich gewährleisteten Schutzes. Im Finanzsektor wird ein solcher Schutz durch verschiedene Regelungen gewährleistet.
- 29 Seit dem 1.1.2014 besteht gemäß § 25a Abs. 1 Satz 6 Nr. 3 KWG die Verpflichtung zur Einrichtung eines Hinweisgebersystems für Kreditinstitute. Damit wurde ein weiterer verpflichtender Bestandteil einer Compliance-Organisation eingeführt, der als eine ordnungsgemäße Geschäftsorganisation u. a. einen Prozess zur Verarbeitung anonymen Hinweise von Mitarbeitern (Whistleblowing) um-

63 Baumert, CCZ 2013, 265, 267.

64 Renz/Frankenberger, CB 2015, 420, 420–425; Schmitt/Stränger, in: Schmidt, Compliance-Funktion nach MaRisk, 2015, Rn. 486 f.; Renz, in: Schäfer/Sethe/Lang, Handbuch der Vermögensverwaltung, § 16 Rn. 94.

65 Zu Hinweisgebersystemen siehe → Block/Sonnenberg, Kap. 5.

fasst. Bereits nach Section 301 des Sarbanes-Oxley Act (SOA) besteht eine solche Verpflichtung für Unternehmen, die in den USA börsennotiert sind.⁶⁶

Nach Art. 32 Abs. 1 der in 2016 in Kraft getretenen Marktmissbrauchsverordnung (MAR)⁶⁷ müssen einerseits die zuständigen nationalen Behörden wirksame Mechanismen schaffen, um die Meldung tatsächlicher oder möglicher Verstöße gegen diese Verordnung zu ermöglichen. Andererseits müssen nach Art. 32 Abs. 3 der MAR Unternehmen, die durch die Finanzdienstleistungsregulierung geregelt werden, angemessene interne Verfahren einrichten, über die ihre Mitarbeiter Verstöße gegen diese Verordnung melden können. Die Meldung von Verstößen ist erforderlich, damit die zuständigen Behörden Marktmissbrauch aufdecken und Sanktionen verhängen können. Maßnahmen in Bezug auf Mitteilungen von Informanten sind erforderlich, um die Aufdeckung von Marktmissbrauch zu erleichtern und den Schutz und die Einhaltung der Rechte des Informanten und der Person, gegen die sich die Vorwürfe richten, sicherzustellen.

Nicht nur in der Finanzindustrie besteht die Verpflichtung zur Einrichtung einer internen Meldestelle. Am 2.7.2023 ist das Hinweisgeberschutzgesetz in Kraft getreten, das Unternehmen mit mehr als 50 Beschäftigten verpflichtet, ein internes Hinweisgebersystem einzurichten. Mit dem neuen Gesetz erfolgt die Umsetzung der EU-Hinweisgeberrichtlinie⁶⁸ aus dem Jahre 2019 in deutsches Recht. Ziel des Gesetzes ist der Schutz von Whistleblowern, also von Personen, die Hinweise auf Missstände in Unternehmen geben, und die Sicherstellung, dass ihnen im Rahmen der Vorgaben dieses Gesetzes keine Benachteiligungen drohen.

Die Ausgestaltung des Whistleblowing-Prozesses hängt gemäß § 25a Abs. 1 Satz 6 Nr. 3 KWG von Art, Umfang, Komplexität und Risikogehalt der Geschäftstätigkeit ab. Die Hinweise können auf ein schädigendes Verhalten hindeuten und bspw. Verstöße gegen das Gesetz oder eine aufgrund des Gesetzes erlassenen Verordnung, strafbare Handlungen innerhalb des Unternehmens, Verstöße gegen interne Richtlinien und Verfahren, Verstöße, die dem Image der Bank abträglich sein können (auch unethisches Verhalten) oder unerlaubte Weitergabe von Informationen betreffen. Ein Hinweisgebersystem bietet daher die Chance, relevante Informationen und Kenntnisse über Abläufe, aktuell oder zukünftig schädigende Angriffe, Missstände, Manipulationen oder ähnliches, die damit verbundenen handelnden Personen und deren Motivation zu erhalten.⁶⁹

66 Moosmayer, Compliance, Rn. 181; Passarge, in: Martinek/Semler/Flohr, Handbuch des Vertriebsrechts, § 79 Rn. 120. Zu Aufbau und Management von Hinweisgebersystemen siehe ferner → Block/Sonnenberg, Kap. 5.

67 Verordnung (EU) Nr. 596/2014; https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=cele_x%3A32014R0596 (zuletzt abgerufen am 18.7.2024).

68 <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L1937> (zuletzt abgerufen am 18.7.2024).

69 Benz, ZRFC 2015, 126, 127.

- 33** Die Institute haben bei der Ausgestaltung des Whistleblowing-Verfahrens eine weitgehende Gestaltungsfreiheit im Hinblick auf den Adressaten der Meldung.⁷⁰ So sind z. B. interne oder externe Anlaufstellen möglich. Hinweisgeber können anonym per Telefon oder E-Mail Verstöße gegen Gesetze und/oder Compliance-Richtlinien an eine (unternehmensinterne oder externe) Zentrale Stelle melden (Whistleblower-Hotline). Hierzu bedarf es eines unabhängigen und höchst vertraulichen Kommunikationsprozesses. Die Whistleblower-Hotline sammelt Informationen, geht ihnen nach und informiert die zuständigen Stellen. Ähnliches erfolgt bei einem Ombudsmann (oftmals Externer).⁷¹ Dieser sammelt ebenfalls die Informationen und gibt sie nach einer Prüfung weiter. Durch die Implementierung eines solchen Hinweisgebersystems wird das Entdeckungsrisiko von Straftaten erhöht und eine positive Außendarstellung ermöglicht.
- 34** Voraussetzung für eine wirksame Whistleblower-Hotline ist neben geeigneten Prozessen das Vertrauen und die Akzeptanz der Mitarbeiter in einem Unternehmen. Hierzu ist neben einem CMS eine etablierte Compliance-Kultur erforderlich, die die Mitarbeiter motiviert, intern Hinweise zu geben und grobe Missstände und Gefahren abzustellen.

5. Datenschutz

- 35** Bei der Ausgestaltung des Compliance-Bereichs eines Kreditinstituts spielt auch die Gewährleistung des Datenschutzes (Compliance im weiteren Sinne) eine wesentliche Rolle. Kreditinstitute sind, wie jedes Unternehmen auch, dazu verpflichtet Maßnahmen zu ergreifen, die die Einhaltung der Datenschutzbelange der eigenen Mitarbeiter sowie der Kunden gewährleistet.⁷² Demgegenüber steht die grundsätzliche Zielsetzung der Compliance-Funktion, möglichst viele Daten zu sammeln und auszuwerten, um die Einhaltung von Regelungen und Maßnahmen zu überwachen. Problematisch sind im Allgemeinen weniger die Regelungen und Maßnahmen als solche, die im jeweiligen Unternehmen zur grundsätzlichen Vermeidung von Regelverstößen getroffen werden, sondern vielmehr die Vorgehensweisen, die im Unternehmen eingesetzt werden, um Compliance-Verstöße aufzudecken.
- 36** Die Aufgabenwahrnehmung der Funktionen Kapitalmarkt-Compliance und Datenschutz sowie die Verhinderung bzw. angemessene Verminderung von Interessenkonfliktpotenzialen beider Funktionen erfordert eine detaillierte Schnittstellendefinition. Die unterschiedlichen Maßstäbe und Ansätze beider Funktionen werden damit, soweit sinnvoll und möglich, aufeinander abgestimmt und eine Zusammenarbeit beider Beauftragten erleichtert.

⁷⁰ Hannemann/Steinbrecher/Weigl, Mindestanforderungen an das Risikomanagement (MaRisk), AT 4.4.2 Rn. 33.

⁷¹ Moosmayer, Compliance, Rn. 186.

⁷² Brandt, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 29 Rn. 27. Zum Datenschutz im Compliance Management siehe ausführlich → Becker/Böhlke/Fladung, Kap. 12.

Eine Schnittstelle besteht für beide Funktionen insofern, dass der Grundsatz der Datensparsamkeit gilt. Häufig werden im Rahmen von Compliance-Maßnahmen personenbezogene Daten verarbeitet, wie etwa Auswertungen von Personen- und Kommunikationsdaten von Mitarbeitern oder Transaktionen, die Bestandteil der Aufgaben einer „Compliance-Organisation“ sind.⁷³ Dies ist z. B. bei unternehmensinternen Untersuchungen der Fall, bei denen Verbindungsnachweise kontrolliert und mithilfe der E-Mail-Korrespondenz Sachverhalte rekonstruiert werden. Bei solchen Handlungen muss das Unternehmen neben dem BDSG, der DSGVO auch das TTDSG und das DDG beachten. Gerade in diesem Bereich bestehen sehr hohe einfachgesetzliche und grundrechtliche Hürden, da hier in der Regel Grundrechte betroffen sind, deren rechtswidrige Verletzung strafrechtliche Folgen haben können. Nach § 26 BDSG ist bspw. die Nutzung und Übermittlung von Daten des Arbeitnehmers beschränkt. Im Rahmen von Compliance-Maßnahmen darf keine Totalkontrolle der Beschäftigten mit umfassenden Auswertungen erfolgen. Der Umfang der Kontrollmaßnahmen muss verhältnismäßig sein und eine Betrachtung der Geeignetheit, Erforderlichkeit und Angemessenheit der Datenverarbeitung einschließen.⁷⁴

Eine weitere Schnittstelle zwischen den Funktionen Kapitalmarkt-Compliance-Funktion und Datenschutz besteht dahingehend, dass beide Funktionen der Geschäftsleitung, die für beide Funktionen die Gesamtverantwortung trägt, unmittelbar nachgeordnet sein müssen. Beide Beauftragten müssen somit unmittelbar an die Geschäftsleitung berichten. Diese Gesamtverantwortung beinhaltet auch, dass die Verpflichtung der Geschäftsleitung zum Aufbau einer effizienten Datenschutz- und Compliance-Organisation besteht.⁷⁵ Damit sind ein Kapitalmarkt-Compliance- und Datenschutzbeauftragter zu ernennen. Voraussetzung für die Ernennung ist, dass der Beauftragte sowohl sachkundig als auch zuverlässig ist.⁷⁶ Weiterhin hat die Geschäftsleitung die Unabhängigkeit der Datenschutz- und Kapitalmarkt-Compliance-Beauftragten sicherzustellen. Während der Kapitalmarkt-Compliance-Beauftragte nur gegenüber der Gesamtgeschäftsleitung weisungsgebunden ist, ist der Datenschutzbeauftragte gemäß Art. 38 Abs. 3 DSGVO in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei.

Im Übrigen sind beide Beauftragte nicht für die Umsetzung und Einhaltung von Regeln verantwortlich (AT 6 Tz. 2 der MaComp). Gemäß AT 6 Tz. 3 der MaComp obliegt dem Kapitalmarkt-Compliance-Beauftragten insbesondere die Überwachung der Einhaltung der Vorschriften des WpHG, wohingegen der Da-

⁷³ Boldt/Büll/Voss, CCZ 2013, 248, 252.

⁷⁴ Thüsing, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 3 Rn. 17.

⁷⁵ LG München, 10.12.2013 – 5 HK O 1387/10, NZG 2014, 345 (sog. „Neubürger-Urteil“).
Siehe hierzu auch → Schulz, Kap. 1 Rn. 39.

⁷⁶ Brandt, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 29 Rn. 41 f.

tenschutzbeauftragte die Einhaltung datenschutzrechtlicher Grundsätze und Regelungen innerhalb des Unternehmens überwacht.⁷⁷

- 40 Ein Unterschied zwischen beiden Funktionen besteht im Hinblick auf Mitarbeiterschulungen. Nach BT 1.2.3 Tz. 2 der MaComp hat der Compliance-Beauftragte Mitarbeiterschulungen zu unterstützen, ist jedoch nicht primär für Mitarbeiterschulungen verantwortlich (vgl. arg. ex. AT 6.2 der MaComp). Damit obliegt es der Compliance-Funktion zu entscheiden, ob sie diesem Beratungsauftrag risikobasiert nachkommt oder dies bspw. den Fachbereichen selbst überlässt.

6. Auslagerung der Compliance-Funktion oder von einzelnen Compliance-Tätigkeiten

- 41 Compliance ist eine originäre Pflicht der Unternehmensleitung, die ein unternehmensadäquates und dauerhaftes Compliance-Management sicherzustellen hat. Eine vollständige Delegation der Compliance-Verantwortung scheidet aus.⁷⁸
- 42 Wertpapierdienstleistungsunternehmen ist es allerdings unter den Voraussetzungen des § 25b KWG und § 80 Abs. 6 WpHG i.V.m. BT 1.3.4 MaComp erlaubt, die Compliance-Funktion teilweise oder vollständig auszulagern. Voraussetzung hierfür ist jedoch nach BT 1.3.4 Tz. 1 MaComp, dass alle einschlägigen aufsichtsrechtlichen Anforderungen eingehalten werden.
- 43 Grundsätzlich ist eine Auslagerung innerhalb des Konzerns möglich. Darüber hinaus kann bei kleinen Instituten eine Übertragung einzelner Funktionen oder von Teilen derer auf Dritte, bspw. auf andere Banken, Kanzleien, Beratungsfirmen und IT-Dienstleister, erfolgen. Übertragen werden können insbesondere die Beratungs- sowie die Überwachungsfunktion, solange die Vertraulichkeit gesichert ist.⁷⁹
- 44 Wie ausgeführt, verbleibt trotz der Auslagerung einzelner Compliance-Tätigkeiten die nicht delegierbare Gesamtverantwortung für die Compliance-Funktion stets bei der Geschäftsleitung des auslagernden Unternehmens.⁸⁰ Diese muss das

⁷⁷ Oberlin/Bossardt, CB 2017, 245, 246.

⁷⁸ Siehe → Schulz, Kap. 1 Rn. 37, 56 f. Zu Besonderheiten bei Finanzdienstleistungsunternehmen siehe Wagner, in: Szesny/Kuthe, Kapitalmarkt Compliance, 15, Rn. 83 ff.

⁷⁹ Vgl. EG-Organisationsrichtlinie Artikel 13–15 (Richtlinie 2006/73/EG der Kommission vom 10.8.2006 zur Durchführung der Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates in Bezug auf die organisatorischen Anforderungen an Wertpapierfirmen und die Bedingungen für die Ausübung ihrer Tätigkeit sowie in Bezug auf die Definition bestimmter Begriffe für die Zwecke der genannten Richtlinie); Trickes/Renz, in: Bankrecht und Bankpraxis, 2024, Kapitel 16.1, Rn. 112.

⁸⁰ EG-Organisationsrichtlinie, Artikel 14 Abs. 1 lit a (Richtlinie 2006/73/EG der Kommission vom 10.8.2006 zur Durchführung der Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates in Bezug auf die organisatorischen Anforderungen an Wertpapierfirmen und die Bedingungen für die Ausübung ihrer Tätigkeit sowie in Bezug auf die Definition bestimmter Begriffe für die Zwecke der genannten Richtlinie); Trickes/Renz, in: Bankrecht und

Auslagerungsunternehmen sorgfältig auswählen.⁸¹ Daher ist die Geschäftsleitung weiterhin für die Erfüllung der Anforderungen, insbesondere für eine Einrichtung der ganz oder teilweise ausgelagerten Compliance-Funktion verantwortlich. Damit verbleibt es bei dem Grundsatz der Alleinverantwortung der Geschäftsleitung.⁸² Um eine angemessene Aufgabenerfüllung durch den Dienstleister zu gewährleisten, ist eine fortlaufende Überwachung der Qualität als auch der Quantität der Dienstleistung erforderlich.⁸³ Diese Auslagerungskontrolle obliegt ebenfalls der Geschäftsleitung, die jedoch unternehmenszugehörige Personen mit der laufenden Beaufsichtigung und Überwachung beauftragen kann.⁸⁴ Diese handelt dann im Namen der Geschäftsleitung. Eine Auslagerung ist seit der 5. MaRisk-Novelle (2017) nur noch dann zulässig, wenn das auslagernde Institut weiterhin über Kenntnisse und Erfahrungen verfügt, die eine wirksame Überwachung der erbrachten Dienstleistungen gewährleistet.⁸⁵

Eine Vollausslagerung der Compliance-Funktion ist jedoch nach dem Proportionalitätsprinzip nur bei kleineren und evtl. mittelgroßen Instituten möglich. Systemrelevante Institute können diese Möglichkeit nach aktueller Aufsichtspraxis nicht nutzen. **45**

III. Inhalt und Aufgabe einer modernen Compliance-Funktion

Weltweit finden Rechtsverstöße von Wirtschaftsunternehmen eine immer größere Aufmerksamkeit. Insbesondere die Themen Wirtschaftskriminalität, (Arbeitnehmer-)Datenschutz und Korruption rücken stärker in das öffentliche Bewusstsein. Die sich hieraus u. a. ergebende Zunahme von Haftungsrisiken, (indirekten) Schadenersatzforderungen und Imageschäden haben für das Unternehmen und deren Management zur Folge, dass es an Bedeutung gewinnt, sich im Einklang mit gesetzlichen Vorschriften zu verhalten.⁸⁶ Somit gewinnt die Compliance-Funktion immer stärker an Bedeutung. **46**

Die Aufgabe der Compliance-Funktion besteht daher insbesondere darin, eine bestimmte Compliance-Kultur i. S. e. Wertekultur zu implementieren und zu fördern.⁸⁷ Ziel der Compliance-Kultur ist nicht nur ein umfassendes Umfeld zu entwickeln, in dem Compliance-Angelegenheiten behandelt werden, sondern darüber hinaus Mitarbeiter mit den Grundsätzen des verbesserten Anlegerschutzes **47**

Bankpraxis, 2024, Kapitel 16.1, Rn. 113. sowie *Wagner*, in: Szesny/Kuthe, Kapitalmarkt Compliance, 15, Rn. 84.

81 *Schäfer*, in: Krimphove, MaComp, MaComp, BT 1.3.4 Rn. 1271.

82 *Schäfer*, in: Krimphove, MaComp, BT 1.3.4, Rn. 1222. Zu Delegationsfragen siehe auch → *Schulz*, Kap. 1 Rn. 56 f.

83 *Schäfer*, in: Krimphove, MaComp, BT 1.3.4, Rn. 1290 ff.

84 *Schäfer*, in: Krimphove, MaComp, BT 1.3.4, Rn. 1294 f.

85 *Hannemann/Steinbrecher/Weigl*, Mindestanforderungen an das Risikomanagement (MaRisk), AT 4.4.2 Rn. 67.

86 *Salvenmoser/Hauschka*, NJW 2010, 331, 331 f.

87 Zur Bedeutung der Compliance-Kultur → *Schulz*, Kap. 1 Rn. 68 ff.

vertraut zu machen.⁸⁸ Gemäß BT 1.1 Tz. 5 der MaComp fördert und bestärkt das Wertpapierdienstleistungsunternehmen eine unternehmensweite Compliance-Kultur, durch die Rahmenbedingungen für eine Förderung des Anlegerschutzes durch die Mitarbeiter und eine angemessene Wahrnehmung von Compliance-Angelegenheiten geschaffen werden. Eine adäquate Wertekultur mindert somit die Risiken, dass Mitarbeiter eines Instituts gegen gesetzliche Vorgaben verstoßen wollen. Schulung und Trainingsmaßnahmen dienen dazu, diese Anforderungen transparent zu machen, sodass die Motivation eines jeden Mitarbeiters gefördert wird, sich an die Vorgaben zu halten. Ferner bestimmt BT 1.3.1.2 Tz. 2 der MaComp, dass der Compliance-Beauftragte neben den eingehenden Kenntnissen hinsichtlich der Organisation und der Entscheidungsprozesse des Wertpapierdienstleistungsunternehmens auch über die Unternehmenskultur eingehende Kenntnisse haben muss. Dies bedeutet, dass er seine Beratungs- und Überwachungsaktivitäten anhand der durch die Geschäftsleitung vorgegebenen Unternehmenskultur i. S. e. Compliance-Kultur ausrichten kann und auch muss. Um dies umzusetzen, ist es wichtig, dass sowohl die aufsichtsrechtlichen Vorgaben als auch die gesetzlichen Normen sowie die Werte des Unternehmens i. S. e. Unternehmens- und Compliance-Kultur kommuniziert werden. Kommunikation ist eine der wesentlichen Aufgaben einer Compliance-Funktion, zum einen innerhalb der Compliance-Funktion selbst, sodass alle Mitarbeiter anhand gleicher Maßstäbe beraten, überwachen sowie die Risiken steuern können. Zum anderen ist aber auch die Kommunikation ins eigene Unternehmen hinein einer der wesentlichen Grundpfeiler als Aufgabe einer Compliance-Funktion. Compliance-Funktionen sind Dienstleister für das eigene Unternehmen und beraten sowohl Mitarbeiter als auch die Geschäftsleitung zu den aufsichtsrechtlichen Vorgaben als auch zur Vermeidung von Compliance-Risiken. Gerade diese Compliance-Risiken, die durch die Compliance-Funktion evaluiert und gesteuert werden, sind es, die die Basis für die Tätigkeit der Compliance-Funktion darstellen. Die Ausrichtung der Compliance-Funktion ist durch das Management von Compliance-Risiken somit ein Teil des unternehmensinternen Risikomanagements mit speziellem Fokus auf qualitative Compliance-Risiken, die es über Key Performance Indicator (KPIs) quantifizierbar und damit steuerbar zu machen gilt.

IV. Das Compliance-Management-System (CMS)

- 48 Der Einsatz strukturierter, robuster und dauerhaft ausgerichteter Compliance-Management-Systeme (CMS) ist für die Einhaltung regulatorischer Vorgaben einerseits, aber auch für die Reduzierung von Haftungsrisiken von Unternehmen handelnden Personen und Organen andererseits unerlässlich geworden. Für die Einrichtung eines CMS erweisen sich international anerkannte Management (ISO) als auch lokale Prüfungsstandards als hilfreich.

⁸⁸ ESMA, Leitlinien zu einigen Aspekten der MiFID-II-Anforderungen an die Compliance-Funktion, 06/04/2021 ESMA35-36-1952, Rn. 34. [guidelines_on_certain_aspects_of_mifid_ii_compliance_function_requirements_de.pdf](#) (europa.eu) (zuletzt abgerufen am 18.7.2024).

Die Norm ISO 37301⁸⁹ aus dem Jahre 2021, die die Norm ISO 19600 ersetzt, ist als internationaler Leitfaden⁹⁰ anerkannt und enthält Anforderungen und Richtlinien zur Einrichtung eines wirksamen und effektiven CMS.⁹¹ Die Anforderungen sollen die Organisationen dabei unterstützen, Compliance-Ziele zu erreichen, Compliance-Risiken zu identifizieren, zu bewerten und zu managen, Verantwortlichkeiten zu verwalten und einen Rahmen zu entwickeln, der darauf abzielt, ein CMS kontinuierlich zu verbessern.

Der Hauptunterschied zwischen ISO 37301 und ISO 19600 besteht darin, dass ISO 37301 zertifizierbar ist. Auch wenn die Einhaltung von ISO-Standards und die Durchführung von CMS-Prüfungen freiwillig sind, gewährleistet die Umsetzung, Prüfung und Zertifizierung nach ISO 37301 auf der Grundlage der CMS-Prüfungsgrundsätze ein höheres Maß an Governance und ein geringeres Maß an organisatorischen Risiken. Mittlerweile werden gerade an Geschäftspartner, an Unternehmen in Lieferketten aber auch an vertriebsbezogene Unternehmen(s-einheiten) Forderungen mit Blick auf die Einhaltung international anerkannter Standards im Geschäftsalltag gerichtet.⁹²

Ein Prüfungsstandard ist bspw. der Compliance-Prüfungsstandard IDW PS 980, der speziell in Deutschland ein generell standardisierter Maßstab für die Prüfung von CMS ist und Prinzipien und Best Practices für Auditoren bereitstellt. Er wurde im September 2022 vom Institut der Wirtschaftsprüfer in Deutschland überarbeitet⁹³ und konzentriert sich auf Elemente, die als grundlegende Faktoren betrachtet werden, die, wenn sie erfüllt sind, als Beweiserleichterung dafür dienen können, dass Organisationen ihre Sorgfaltspflicht wahrgenommen haben.⁹⁴

Dieser Standard konzentriert sich auf Elemente, die als grundlegende Faktoren betrachtet werden, die, wenn sie erfüllt sind, als objektiver Beweis dafür dienen, dass Organisationen ihre Sorgfaltspflicht wahrgenommen haben. Zu diesen Elementen gehören die folgenden sieben Kategorien:⁹⁵

1. **Compliance-Kultur:** Grundeinstellung und Verhaltensweisen des Vorstands und des Verwaltungsrats („Tone at the Top“, „Conduct at the Top“);

89 Der ISO 37301 ist ein Standard für Compliance-Systeme, der IDW PS 980 ist ein Standard für externe Wirtschaftsprüfer.

90 ISO 37301: 2021 Compliance Management Systems – Guidelines, <https://www.iso.org/standard/75080.html> (zuletzt abgerufen am 18.7.2024). Zum Vergleich zwischen IDW PS 980 und ISO 19600 ausführlich *Withus*, in: Schulz (Hrsg.), *Compliance Management im Unternehmen*, 1. Aufl. 2017, Kap. 6, Rn. 6 ff. Zur ISO 19600 siehe auch → *Uhlig/Federmann*, Kap. 7.

91 *Withus/Kunz*, BB 2015, 685, 688; *Makowicz*, CB 2015, 45, 48.

92 Vgl. zum Einsatz von ISO-Standards bspw. *Renz/Spallek*, *Comply* 202, 26 ff.

93 Siehe Institut der Wirtschaftsprüfer (IDW) am 6.12.2022 „IDW PS 980 n.F. (09.2022) zur Prüfung von Compliance Management Systemen verabschiedet“ (zuletzt abgerufen am 18.7.2024).

94 Zur Anforderung an wirksame Compliance-Management-Systeme siehe auch → *Schulz*, Kap. 1 Rn. 52 ff.

95 Siehe hierzu auch → *Schulz*, Kap. 1 Rn. 52 ff.; *Wolf*, DStR 2011, 997, 998 ff.

2. **Compliance-Ziele:** Festlegung relevanter Teilbereiche und dort einzuhalten-der Regeln;
 3. **Compliance-Organisation:** Festlegung der Verantwortlichkeiten, Aufbau- und Ablauforganisation, Ressourcenplanung;
 4. **Compliance-Risiken:** Identifikation von Risiken und systematische Risiko-erkennung anhand einer Risikoanalyse;
 5. **Compliance-Programm:** Einführung von Grundsätzen und Maßnahmen zur Risikominimierung, Vermeidung von Regelverstößen und Behandlung von Verstößen;
 6. **Compliance-Kommunikation:** Information von Mitarbeitern und ggf. Drit-ten, Berichtswege für identifizierte Risiken, Regelverstöße und Hinweise;
 7. **Compliance-Verbesserung:** Überwachung der Angemessenheit und Wirk-samkeit der CMS-Einrichtung von Abläufen zur Berichterstattung und sys-tematischen Verbesserung des CMS.
- 53 Basierend auf den Grundsätzen Good Governance, Nachhaltigkeit, Transparenz und Verhältnismäßigkeit folgt dieser Prüfungsstandard einem Vier-Phasen-Prinzip, „Plan-Do-Check-Act“,⁹⁶ wie dies auch der ISO 37301 voraussetzt. Somit ist das CMS – ähnlich den drei wesentlichen Bestandteilen der Prävention, Kontrolle und Reaktion – in vier Phasen gegliedert: Planung, Handlung, Kontrolle und Maßnahme. Gemäß dem IDW PS 980 versteht man unter einem CMS die gewählte Organisationsform eines Unternehmens, die auf die Sicherstellung eines regelkonformen Verhaltens der Führungskräfte und Mitarbeiter des Unter-nehmens abzielt. Ziel jedes CMS ist es damit, Verstöße gegen definierte Pflich-ten zu vermeiden bzw. wesentlich zu erschweren und eingetretene Verstöße zu erkennen und zu behandeln. Das CMS stellt damit einen wesentlichen Bestand-teil des Risikomanagements eines Kreditinstituts dar.⁹⁷ Damit die Anforderun-gen des Compliance-Standards erfüllt werden können, muss ein Unternehmen eine systematische Compliance-Organisation (CMS) einführen, dokumentieren, umsetzen und aufrechterhalten. Hierfür ist der Compliance-Beauftragte verant-wortlich.⁹⁸
- 54 Der IDW PS 980 dient als Prüfungsstandard dazu, die Gundsätze externer ord-nungsgemäßer Prüfung von CMS zur Bewertung der Wirksamkeit von CMS si-cherzustellen. Der ISO 37301 zielt hingegen darauf ab, Organisationen beim Aufbau eines CMS zu unterstützen und ist daher als Voraussetzung zum IDW PS 980 und Konkretisierung der dort formulierten sieben Grundelemente zu se-hen.⁹⁹
- 55 Das zu errichtende CMS muss sich an der Risikolage des Unternehmens orien-tieren. Daraus folgt unmittelbar, dass die Unternehmensleitung die spezifische

96 Kayser, CB 2015, 441, 442; Renz/Marbeiter, ZfgK 23/2023, 11.

97 Bank, in: Patzina/Bank/Schimmer/Simon-Widmann, Haftung von Unternehmensorganen, 1. Aufl. 2010, Kap. 6 Rn. 329 ff.

98 Zu Stellung und Aufgaben des Compliance-Beauftragten siehe Wolf, DStR 2011, 997, 998.

99 Withus, BB 2015, 685, 685 ff.; Schmidt/Wermelt/Eibels Häuser, CCZ 2015, 18, 18 ff.

Risikosituation des Unternehmens beurteilen und darauf aufbauend ein individuelles CMS erarbeiten muss.¹⁰⁰ Ein generell gültiges und für alles Unternehmen passendes CMS kann es daher nicht geben.

Um auch neue regulatorische Anforderungen schneller verorten und umsetzen zu können, sind klare, durch die Geschäftsleitung zugewiesene Prozessverantwortlichkeiten zwingende Voraussetzung. Denn wer die regulatorischen Anforderungen effizient beherrscht, verschafft sich Wettbewerbsvorteile.¹⁰¹ Prozessuale Schwachstellen, auch bei der Erschließung neuer Geschäftsfelder, lassen sich mit einem effektiven und effizienten CMS innerhalb des IKS schneller erkennen und beheben. Compliance-Risiken können auf diese Weise erfolgreich minimiert werden. Sollten CMS und IKS nicht ausreichend ausgestaltet und funktionsfähig sein, stünde dies einer Ausweitung oder Veränderung des strategischen Geschäftsmodells mangels Beherrschbarkeit der Risiken entgegen. In der regulatorischen Weiterentwicklung ist für zukünftige Anforderungen der Fokus erkennbar, der Wirksamkeit von IKS-Systemen, der internen Governance und den Compliance-Funktionen eine noch höhere Bedeutung beizumessen. Damit soll sichergestellt werden, dass Kreditinstitute Risiken erkennen und beherrschen.¹⁰² **56**

Ein CMS ist effektiv und wirksam, wenn allgemein und in risikobehafteten Prozessen des Institutes keine Gesetzesverstöße begangen (Prävention) und etwaige Gesetzesverstöße aufgedeckt werden (effektive Kontrolle) und auf diese mit wirksamen Maßnahmen reagiert wird (Reaktion). **57**

Im Hinblick auf die Prävention ist im Unternehmen darauf zu achten, dass Compliance nicht lediglich in der Verantwortlichkeit des Vorstandes liegt, sondern dieser auch eine Vorbildfunktion („Tone at the Top“,¹⁰³ „Conduct at the Top“¹⁰⁴) innehat – ungeachtet der Aufstellung von Verhaltensregeln für alle Mitarbeiter. Der Compliance-Beauftragte ist zwecks Prävention von Risiken sowohl für die Identifikation risikobehafteter Prozesse als auch für die Identifizierung der allgemeinen und branchen- oder unternehmensspezifischen Risikobereiche, in denen sich das Unternehmen bewegt, verantwortlich, welche dann an den Vorstand berichtet werden.¹⁰⁵ Darüber hinaus ist die Erstellung detaillierter Arbeitsanweisungen für die Mitarbeiter eines Instituts im Bereich risikobehafteter Prozesse und die Auswahl von besonders zuverlässigem Personal in diesen Bereichen im Rahmen der präventiven Ausrichtung des CMS von Bedeutung. Des Weiteren **58**

100 *Ghassemi-Tabar*, in: *Ghassemi-Tabar*, DCGK, G5, Rn. 13. Zum Risikomanagement siehe auch → *Romeike*, Kap. 9.

101 *Powilleit*, GWR 2010, 28, 28 ff.

102 *Bergmoser*, BB Special 4 (zu BB 50/2010), 2, 5.

103 *Sandmann*, CCZ 2015, 70, 72; *Wolf*, DStR 2011, 997, 998.

104 Siehe → Rn. 3 sowie → *Schulz*, Kap. 1 Rn. 69 f.

105 Siehe *Wolf*, BB 2011, 1353, 1354 ff.

Teil 3 Besondere Aufgaben und Anwendungsfelder

hat der Compliance-Beauftragte sicherzustellen, dass Mitarbeiter über die Risiken etwa durch Mitarbeiterschulungen aufgeklärt sind.¹⁰⁶

- 59 Zur Erfüllung der Kontrollfunktion eines wirksamen CMS ist besonders auf eine klare Struktur der Compliance-Organisation hinzuwirken. Im Rahmen dessen sind klare Kontrollzuständigkeiten festzulegen und dafür ausreichende Kontrollbefugnisse zu erteilen. Auch ist sowohl eine regelmäßige als auch anlassbezogene Überprüfung risikobehafteter compliance-relevanter Prozesse durchzuführen. Damit wird auch ein etwaiger Anpassungsbedarf des CMS – etwa aufgrund veränderter Risikolage oder Vorfällen – erkannt.
- 60 Die reagierende Ausrichtung der Compliance-Funktion dient der Aufklärung von Pflichtverletzungen sowie deren Ursachen und soll eventuelle Konsequenzen – organisatorischer oder ggf. personeller Natur – tragen. Denn lediglich durch die Anpassung des CMS kann die Wirksamkeit des CMS auf Dauer sichergestellt werden.

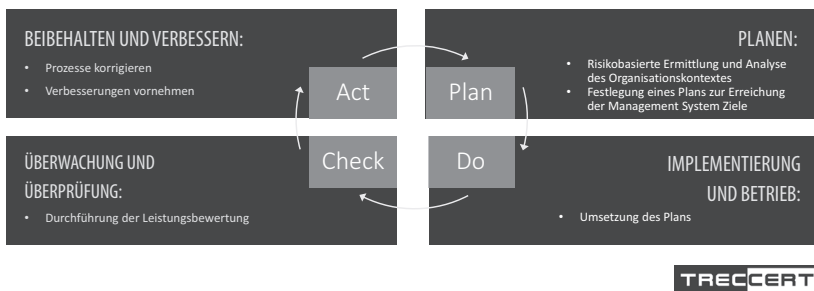


Abbildung 1: Plan-Do-Check-Act-Zyklus (PCDA) im Sinne des ISO 37301 – Compliance Management System

V. Schnittstellen zu anderen Funktionen

- 61 Compliance-Risiken setzen sich aus verschiedenen Aspekten des rechtlichen und damit des operationellen Risikos sowie des Reputationsrisikos zusammen. Für das Management dieser Risiken sind bei Kreditinstituten diverse Fachbereiche zuständig (bspw. Rechtsbereich, Compliance-Organisationseinheit, Interne Revision), sodass teilweise zahlreiche Schnittstellen sowie ähnlich gelagerte Aufgaben bestehen. Nicht zuletzt durch die hinzugekommene Verpflichtung, eine übergreifende MaRisk-Compliance-Funktion i. S. e. Klammerfunktion zu implementieren, ist die Fragestellung der Ausgestaltung von Schnittstellen noch komplexer geworden. Dies erfordert für Kreditinstitute, die einzelnen Aufgabenstellungen der vorgenannten Organisationseinheiten voneinander abzugrenzen, die Schnittstellen optimal auszugestalten und einen effizienten Informationsaus-

¹⁰⁶ Tüllner, BB 2012, 2551, 2551.

tausch zwischen den einzelnen Funktionen und Organisationseinheiten zu gewährleisten. Damit sollen einerseits Doppelarbeiten und andererseits Überwachungslücken durch fehlende Zuordnungen vermieden werden.¹⁰⁷ Für eine effektive Aufgabenerfüllung der Compliance-Funktion ist es jedenfalls sinnvoll und zweckmäßig, mit vielen Schlüsselfunktionen, auf die im Nachfolgenden näher eingegangen wird, intensiv und effizient zusammenzuarbeiten.

1. Fachbereiche

Compliance dient der proaktiv präventiven Beratung der operativen Einheiten zur Einhaltung regulatorischer und sonstiger Vorgaben. Zur Sicherstellung der Einhaltung der Vorgaben überwacht die Compliance-Funktion daher die Fachbereiche und die dort implementierten Kontrollhandlungen. Compliance-Risiken werden somit evaluiert und gesteuert. Eine optimale und zweckdienliche Beratung der Fachbereiche durch die Compliance-Funktion ist jedoch nur dann möglich, wenn entsprechende Sachkundevoraussetzungen für Mitarbeiter der Compliance-Funktion und für den Compliance-Beauftragten vorliegen. Die Sachkundevoraussetzungen für den Compliance-Beauftragten sind in § 3 WpHG-Mitarbeiteranzeigeverordnung normiert. Neben rechtlichen Kenntnissen muss der Compliance-Beauftragte auch über fachliche Kenntnisse verfügen. Daneben müssen gemäß BT 1.3.1.3 Tz. 1 der MaComp auch die Mitarbeiter der Compliance-Funktion über die erforderlichen Fachkenntnisse für den jeweils zugewiesenen Aufgabenbereich verfügen. Die entsprechende Sachkunde muss vorhanden sein, damit sich die Compliance-Funktion mit den Fachbereichen auf Augenhöhe unterhalten kann. Zudem ist nur bei Verstehen der eigenen Produkte und Vertriebswege eine optimale und zielgerichtete Beratung der Fachbereiche durch die Compliance-Funktion überhaupt erst möglich. Um Fehler von Anfang an zu vermeiden, gerät die Beratung grundsätzlich immer stärker in den Fokus, „denn wer besser berät, muss weniger überwachen“.¹⁰⁸

2. Rechtsbereich

Der Rechtsbereich ist wie die Compliance-Organisationseinheit, das Risikomanagement/-controlling, die Finance-Abteilung sowie die Personalabteilung eine Funktion der sog. Second Line,¹⁰⁹ je nach Ausgestaltung der unternehmensspezifischen Aufbau- und Ablauforganisation.¹¹⁰ Die Aufgaben der Compliance-Or-

107 *Faust*, in: *Ellenberger/Bunte, Bankrechts-Handbuch*, Bd. II, 5. Aufl. 2017, § 109 Rn. 112. Zur „Schnittstellen-Funktion“ von Compliance siehe ausführlich → *Rau*, Kap. 3.

108 *Schäfer*, BKR 2011, 187, 191.

109 *Hannemann/Steinbrecher/Weigl*, Mindestanforderungen an das Risikomanagement (MaRisk), AT 4.4, Rn. 13.

110 Die EBA Guideline 2021/05 zur internen Governance bei Kreditinstituten sieht allerdings nur die Compliance-Funktion (inkl. der Geldwäschepräventionsfunktion) und die Risikomanagement-Funktion als Teil der Internen Kontrollfunktionen und somit sog. Second Line, siehe dort Rn. 169.

ganisationseinheit mit denen des Rechtsbereichs überschneiden sich dahingehend, dass es bei beiden im Wesentlichen um die Einhaltung rechtlicher Vorgaben geht. Dennoch gibt es diverse Unterschiede.¹¹¹

- 64 Ein wesentlicher Unterschied besteht darin, dass die Compliance-Organisationseinheit einen präventiven, viel stärker prozessbezogenen und überwachenden prozessualen Ansatz verfolgt und nicht nur Beratungs-, sondern auch Kontrollfunktionen wahrnimmt, wohingegen der Rechtsbereich im Regelfall auf Anfrage und im Einzelfall tätig wird.¹¹² Ein weiterer Unterschied besteht darin, dass beide Bereiche für unterschiedliche Rechtsgebiete zuständig sind. Während sich bspw. die Kapitalmarkt-Compliance-Funktion im Wesentlichen mit Regelungen/Vorgaben befasst, die einen Bezug zum Wertpapiergeschäft aufweisen, so würdigt der Rechtsbereich diverse Rechtsgebiete, wie bspw. Zivilrecht oder auch Gesellschaftsrecht. Im Übrigen unterscheidet sich die Zielrichtung beider Organisationseinheiten. Der Rechtsbereich, der insbesondere für die Vertragsgestaltung und Haftungsrisiken verantwortlich ist, vertritt ausschließlich die Interessen des jeweiligen Instituts. Hierbei hat die Geschäftsleitung im Rahmen ihrer Legalitätspflicht für die Einhaltung von gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und auf deren Beachtung durch alle Mitarbeiter ihres Instituts hinzuwirken. Ein Legal Counsel kann sich durch Warnhinweise exkulpieren, während ein Compliance Officer bei Verfehlungen sofort eingreifen, handeln und das Fehlverhalten unterbinden muss.¹¹³ Die Compliance-Organisationseinheit ist neutraler und berücksichtigt bei der Wahrnehmung ihrer Beratungs- und Überwachungsfunktion insbesondere auch die Kundeninteressen.¹¹⁴ Die Compliance-Organisationseinheit handelt daher nicht nur nach Legalitätsaspekten, sondern auch nach dem Legitimitätsprinzip. Sie stellt durch organisatorische Maßnahmen sicher, dass potenzielle oder bestehende Compliance-Risiken reduziert bzw. ausgeschlossen werden.
- 65 Enge Zusammenarbeit und regelmäßiger Austausch beider Organisationseinheiten sind erforderlich, um gemeinsam bestehende oder potenzielle Compliance- und Rechtsrisiken minimieren zu können.¹¹⁵ Auch wenn die Zuständigkeiten beider Bereiche grundsätzlich klar abgegrenzt sind, ist im Einzelfall zu entscheiden, ob nicht die jeweils andere Abteilung in einen Beratungsvorgang einzubinden ist. Ein von dem Rechtsbereich beratener Vertriebsvertrag kann bspw. wettbewerbsbeschränkende Klauseln enthalten, sodass insofern eine grundsätzliche oder einzelfallbezogene Abstimmung mit der Compliance-Organisationseinheit

111 Zu Schnittstellen mit dem Rechtsbereich und anderen Unternehmensfunktionen siehe auch → *Schulz*, Kap. 1 Rn. 85 sowie ausführlich → *Rau*, Kap. 3.

112 *Wiedmann/Greubel*, CCZ 2019, 88, 90; *Faust*, in: *Ellenberger/Bunte*, Bankrechts-Handbuch, Bd. II, § 109 Rn. 112a.

113 *Warneke*, NStZ 2010, 312, 313.

114 Diese sowohl nach außen (Kunden-, Anleger-, Verbraucherschutz) als auch nach innen (Unternehmens-, Arbeitnehmerschutz als auch Schutz der Geschäftsleitung vor Haftungsrisiken) gerichtete Tätigkeit stellt in dieser Funktion ein innewohnendes Spannungsfeld dar.

115 Siehe hierzu auch → *Rau*, Kap. 3.

erfolgen sollte, wenn dieser das Thema der kartellrechtlichen Compliance zugewiesen ist.¹¹⁶

3. Risikocontrolling-Funktion

Die Risikocontrolling-Funktion hat die Aufgabe, eine Risikoinventur durchzuführen und daraus ein Risikogesamtprofil der wesentlichen Risiken gemäß MaRisk abzuleiten.¹¹⁷ Hierbei sind neben Risiken aus innerbetrieblichen Vorgängen auch solche erfasst, die aus der Interaktion von Unternehmensprozessen mit der Umwelt herrühren. Aufgrund ihrer Spezialisierung auf einzelne Risikomanagementaspekte und einer laufenden Überwachung der Risikosituation können Risikoentwicklungen frühzeitig erkannt und gegen diese äußert effektiv und effizient vorgegangen werden.¹¹⁸ Ein wesentlicher Aspekt der Compliance-Funktion beim Management von Compliance-Risiken ist neben der Vermeidung aufsichtsrechtlicher Sanktionen i. S. v. Bußgeldern das Steuern und Vermeiden von Reputationsrisiken. Reputationsrisiken stellen qualitative Compliance-Risiken dar, die aufgrund des eigenen Verhaltens einer Bank bzw. seiner Mitarbeiter von innen heraus entstehen. Dies unterscheidet die Compliance-Funktion, die im Wesentlichen ein sog. qualitatives Risikomanagement wahrnimmt, auch von der klassischen Risikocontrolling-Funktion. Diese stellt eine quantitative, auf Zahlen basierte Risikocontrolling-Funktion dar und fokussiert bei Reputationsrisiken eher äußere Risiken, bspw. Marktpreisrisiken, die das Risiko der Bank von außen beeinflussen können. Zudem ist die Compliance-Funktion primär auf die Erreichung der Ordnungsmäßigkeit ausgerichtet, wohingegen die Risikocontrolling-Funktion im Wesentlichen die Aspekte der Risikoerkennung zur Vermeidung von Vermögensschäden sowie der Strategiekonformität berücksichtigt.

Eine enge Zusammenarbeit zwischen der Risikocontrolling- und der Compliance-Funktion ist zwingend notwendig, da nur eine ganzheitliche Betrachtung von Risiken zu deren dauerhafter Minimierung führen kann.¹¹⁹

4. Interne Revision

Die Interne Revision als Third Line im Rahmen der internen Kontrollverfahren ist primär nicht auf die Prävention und (zeitnahe) Aufdeckung von Unregelmäßigkeiten oder (Compliance-)Verstößen ausgerichtet, sondern auf die Prüfung der Funktionsfähigkeit und Wirksamkeit des IKS im Besonderen sowie des Risi-

¹¹⁶ *Klahold/Lochen*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 37, Rn. 72.

¹¹⁷ *Braun*, in: Boos/Fischer/Schulte-Mattler, KWG, 5. Aufl. 2016, § 25a Rn. 211 f.; *Schmidt*, in: Schmidt, Compliance-Funktion nach MaRisk, Rn. 33. Zum Risikomanagement siehe → *Romeike*, Kap. 9.

¹¹⁸ *Hannemann/Steinbrecher/Weigl*, Mindestanforderungen an das Risikomanagement (MaRisk), AT 4.4.1 Rn. 28 ff.

¹¹⁹ EBA/GL/2021/05, Nr. 95.

komanagements eines Unternehmens im Allgemeinen.¹²⁰ Somit prüft die Interne Revision auch die Compliance-Organisationseinheit, sodass eine strikte Trennung von Überwachenden und Überwachten sicherzustellen ist. Auch wenn die Prävention und die Aufdeckung von Unregelmäßigkeiten ein bedeutender Bestandteil der risikoorientierten Prüfungsplanung und -durchführung ist, liegt der Schwerpunkt der Internen Revision auf prozessunabhängigen Ex-Post-Prüfungen.¹²¹ Diese werden nach Einführung bzw. Veränderung von Geschäftsprozessen zeitlich, zum Teil deutlich nachgelagert durchgeführt. In Abhängigkeit vom Prüfungsintervall und dem gewählten Prüfungsumfang kann dies bedeuten, dass Geschäftsvorfälle in Stichproben erst nach Jahren näher geprüft werden. Der Prüfungsturnus der Internen Revision beträgt in der Regel drei Jahre und kann risikobasiert auf zwei bzw. ein Jahr reduziert werden.¹²² Bei einer derartigen Vorgehensweise der Internen Revision erfolgt eine zeitnahe Aufdeckung von möglichen Unregelmäßigkeiten oder (Compliance-)Verstößen im Zweifel verspätet. Für die Compliance-Organisationseinheit besteht hingegen ein jährlicher Überwachungsturnus aller relevanten Verfahren, insbesondere im Rahmen der Kapitalmarkt-Compliance-Funktion. Auch wenn die von der Compliance-Funktion implementierten bzw. vorzunehmenden Kontrollen zwar zum Teil auch zeitlich nachgelagert sind, sind sie dennoch zeitnah, teilweise auch prozessintegriert am jeweiligen Geschäftsvorfall orientiert, sodass Risiken minimiert werden können und ggf. sogar noch Möglichkeiten zur Verhinderung drohenden Schadens bestehen.¹²³ Die Compliance-Organisationseinheit ist zudem in den täglichen Geschäftsbetrieb durch eine proaktive Beratung zeitnah eingebunden. Diese folgt einem präventiven, prozessbegleitenden Ansatz. Damit sich die Compliance-Funktion und die Interne Revision, die ebenfalls Kontrollhandlungen durchführen,¹²⁴ optimal ergänzen, ist es erforderlich, dass die Kommunikation funktioniert und Informationen ausgetauscht werden.

- 69** Im Übrigen ist der Fokus der Internen Revision deutlich weiter gefasst als der Aufgabenbereich der Kontrolleinheiten. Neben dem Aspekt der Ordnungsmäßigkeit auf den ersten beiden Linien (First und Second Line) werden bei den Prüfungshandlungen der Internen Revision auch Aspekte der Sicherheit, Wirtschaftlichkeit und Zweckmäßigkeit aufgegriffen.¹²⁵ Damit stehen das Auffinden von Schwachstellen, die Verminderung von Risiken ebenso im Fokus der Internen Revision wie auch die Schaffung von Mehrwert für das Institut.

120 *Faust*, in: Ellenberger/Bunte, Bankrechts-Handbuch, Bd. II, § 109 Rn. 112c. Siehe auch → *Bartuschka*, Kap. 11 Rn. 21.

121 *Faust*, in: Ellenberger/Bunte, Bankrechts-Handbuch, Bd. II, § 109 Rn. 112c.

122 *Renz/Frankenberger*, CB 2015, 420, 423.

123 *Hauschka/Galster/Marschlich*, CCZ 2014, 242, 244; *Faust*, in: Ellenberger/Bunte, Bankrechts-Handbuch, Bd. II, § 109 Rn. 112c.

124 *Obermayr*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 44 Rn. 65 ff.

125 *Obermayr*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 44 Rn. 69.

VI. Compliance als Teil des IKS eines Kreditinstituts

Das IKS ist ein wichtiges Führungsinstrument eines jeden Unternehmens.¹²⁶ Im Jahr 2021 wurde mit dem Finanzmarktintegritätsstärkungsgesetz für börsennotierte Aktiengesellschaften in § 91 Abs. 3 AktG die Pflicht zur Schaffung eines IKS mit aufgenommen. Für nicht-börsennotierte Unternehmen kann sich eine Pflicht zur Einrichtung eines IKS weiterhin aus der Sorgfaltspflicht nach § 93 Abs. 1 AktG ergeben.¹²⁷ Hier ist der Vorstand einer AG verpflichtet, geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, um den Fortbestand der Gesellschaft gefährdende Entwicklungen frühzeitig erkennen und ihnen entgegenwirken zu können. Viele Kreditinstitute und Wertpapierdienstleistungsinstitute verfügen über ein IKS, wobei die Anforderungen an die internen Kontrollen und die Prüfung des IKS in den letzten Jahren stark gestiegen sind. Grund hierfür war insbesondere die Wirtschafts- und Finanzmarktkrise der letzten Jahre, die Schwachstellen im IKS von Kreditinstituten offengelegt haben.¹²⁸ Aufgrund dieser Ereignisse wurden striktere regulatorische Anforderungen – u. a. in Form der MiFID II/MiFIR, EMIR oder MAR – an Finanzinstitute erlassen, um die Risiken, die zur Finanzkrise geführt haben, zu minimieren.¹²⁹ Daneben wurden auch Eigenkapital- bzw. Reportingverpflichtungen erweitert. Die EBA verfolgt bspw. einen ganzheitlichen SREP-Ansatz (Supervisory Review and Evaluation Process) der die Beurteilung der Schlüsselindikatoren, des Geschäftsmodells, der Kapital- und Liquiditätsrisiken als auch der Governance einschließt. Zu den Vorgaben zählt dabei auch eine regelmäßige Berichterstattung über die Prozesse zur internen Governance und zur Wirksamkeit von Compliance.¹³⁰

Obgleich die Anforderungen an und die Herausforderungen für Finanzinstitute stetig steigen, bieten diese Änderungen gleichzeitig eine Chance, die Effizienz der internen Organisation grundlegend zu verbessern. Zur Wahrnehmung dieser stetig steigenden Herausforderungen und um die spezifischen Risiken, denen jedes Unternehmen aufgrund der Produkt- oder Dienstleistungspalette, der Märkte oder des Ressourceneinsatzes ausgesetzt ist, zu managen und insbesondere zu minimieren, ist ein wirksames IKS unerlässlich und von großer Bedeutung.

126 Siehe auch → *Bartuschka*, Kap. 11 Rn. 21 ff.

127 BT-Drs. 19/26966, S. 115.

128 *Boldt/Büll/Voss*, CCZ 2013, 248, 254. Zum Zusammenhang zwischen Governance, Risk und Compliance Management siehe auch → *Bartuschka*, Kap. 11 Rn. 2 ff.

129 MiFIR: Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rates vom 15.5.2014; MiFID II: Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15.5.2014; MAR: Verordnung (EU) Nr. 596/2014 des Europäischen Parlaments und des Rates vom 16.4.2014; MAD II: Richtlinie 2014/57/EU des Europäischen Parlaments und des Rates vom 16.4.2014; EMIR: Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4.7.2012.

130 *Wittig*, WM 2010, 2337, 2342.

- 72 Das IKS umfasst alle in einem Unternehmen eingeführten, aufeinander abgestimmten Grundsätze, Methoden und Maßnahmen (Regelungen), die dazu dienen, einen ordnungsgemäßen Ablauf des betrieblichen Geschehens sicherzustellen.¹³¹ Aus den Ergebnissen der Überwachung und Beurteilung von Risiken werden risikobasiert weitere interne Kontrollen abgeleitet. Weil es sich auf die gesamte Geschäftstätigkeit und damit auf alle wesentlichen Geschäftsprozesse des Unternehmens richtet, trägt das IKS zur Einhaltung der unternehmerischen Ziele bei. In jedem Institut sind in Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten gemäß dem Proportionalitätsprinzip innerhalb des IKS:
- Regelungen zur Aufbau- und Ablauforganisation zu treffen,
 - Risikosteuerungs- und -controlling-Prozesse zur Identifizierung, Beurteilung, Steuerung, Überwachung sowie Kommunikation der Risiken einzurichten und
 - eine Risikocontrolling-Funktion sowie eine angemessene, unabhängige, dauerhafte und wirksame Compliance-Funktion zu implementieren.¹³²
- 73 Die Einrichtung, Ausgestaltung, Steuerung und Überwachung eines wirksamen IKS sind Aufgabe der Geschäftsleitung.¹³³ Die Verantwortung – sowohl Letzt- als auch Gesamtverantwortung – für die Sicherstellung der Errichtung und Überwachung wirksamer interner Kontrollverfahren liegt damit bei der Geschäftsleitung und ist als solche – wie auch die Verantwortung für die Compliance – nicht delegierbar.¹³⁴ Dahingehend hat die Geschäftsleitung sicherzustellen, dass überprüft wird, ob diejenigen internen Vorgaben und Geschäftsprozesse, welche die Einhaltung der zu beachtenden Gesetze und Verordnungen sowie der aufsichtsbehördlichen Anforderungen gewährleisten sollen, eingehalten werden und somit die Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit sichergestellt werden können.¹³⁵
- 74 Für Kreditinstitute bestehen verpflichtende Regelungen zur Implementierung des IKS und dessen Ausgestaltung. So schreibt § 25a Abs. 1 Satz 3 Nr. 3 KWG vor, dass eine ordnungsgemäße Geschäftsorganisation insbesondere angemessene Kontrollverfahren zu umfassen hat, die aus einem IKS und einer Internen Revision bestehen. Die Verpflichtung der Institute zur Einrichtung einer Internen Revision wird durch den Abschnitt BT 2 der MaRisk, der die Anforderungen an die Ausgestaltung der Internen Revision behandelt, konkretisiert. Das IKS, das alle Unternehmensebenen inkl. ausgelagerter Prozesse umfasst, ist vom Institut stets auf dem neuesten Stand zu halten und weiterzuentwickeln sowie auf alle Prozesse auszudehnen, um neue gesetzliche oder

131 *Dierks/Sandmann/Herre*, CCZ 2013, 164, 166. Siehe auch → *Bartuschka*, Kap. 11 Rn. 21.

132 *Bürkle*, in: *Bürkle*, Compliance in Versicherungsunternehmen, § 2 C. III. Rn. 90.

133 *Wimmer*, BKR 2006, 146, 147.

134 *Bürkle*, CCZ 2008, 50, 50.

135 § 25a Abs. 1 Satz 1 und 2 KWG.

weitere regulatorische Bestimmungen und die damit einhergehenden potenziellen Risiken zu minimieren.¹³⁶

Die Hauptziele des IKS sind:¹³⁷

75

1. die Sicherstellung der Effektivität und Effizienz der Geschäftsprozesse sowie auch Prozessoptimierung und Identifizierung von operativen Schwachstellen innerhalb der Prozesse;
2. das Hinwirken auf ein erhöhtes Risikobewusstsein auf Mitarbeiterebene; u. a. bei bevorstehenden Personalwechseln;
3. das Sicherstellen der Einhaltung der relevanten Gesetze und Vorschriften und dahingehend
4. die Reduzierung der für Unternehmen bestehenden Risiken, die insbesondere durch Verstöße gegen regulatorische und gesetzliche Vorschriften drastisch erhöht werden.

Man unterscheidet zwischen drei Kontrollverantwortlichkeiten:

76

1. „**First Line**“:¹³⁸ Fachbereiche
 - Verantwortung eines jeden Fachbereichs für die Einhaltung von Gesetzen, aufsichtsrechtlichen Vorgaben und internen Richtlinien in seinem Zuständigkeitsbereich- und Aufgabenbereich.
 - Verantwortung der Fachbereiche für die Implementierung angemessener Mechanismen und Systeme, um ihrer Verantwortung nachzukommen und die in ihren verantworteten Bereichen bestehenden Risiken und Prozesse zu steuern.
 - Kontrollhandlungen.
2. „**Second Line**“:¹³⁹ Compliance-, Risikomanagement- und Controlling-Funktionen
 - Überwachungshandlungen.
3. „**Third Line**“:¹⁴⁰ Interne Revision
 - Regelmäßige Regel- und Sonderprüfungen der First Line und unabhängige Prüfung und Bewertung der Second Line-Kontroll- und Überwachungshandlungen.
 - Prüfungshandlungen.

¹³⁶ Dierks/Sandmann/Herre, CCZ 2013, 164, 166 f.

¹³⁷ Renz/Frankenberger, CB 2015, 420, 420. Siehe auch → Bartuschka, Kap. 11 Rn. 21 ff.

¹³⁸ Welsch/Foshag, in: Renz/Hense/Marbeiter, Wertpapier-Compliance in der Praxis, I.5. Rn. 17.

¹³⁹ Boldt/Büll/Voll, CCZ 2013, 248, 250 f.

¹⁴⁰ Hannemann/Steinbrecher/Weigl, Mindestanforderungen an das Risikomanagement (MaRisk), AT 4.4 Rn. 16.

Teil 3 Besondere Aufgaben und Anwendungsfelder

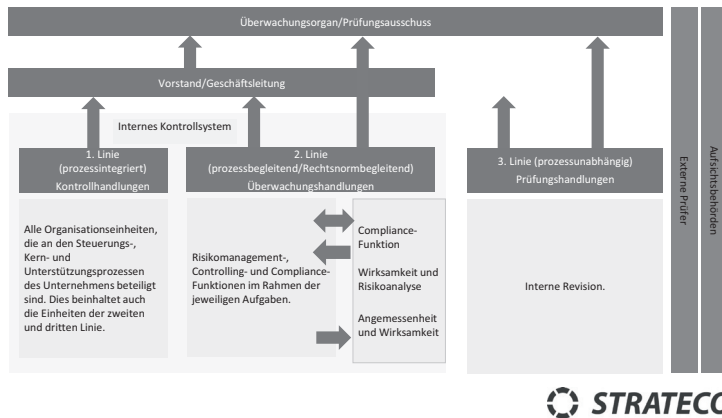


Abbildung 2: „Three Lines Modell“: Rahmenwerk für ein wirksames Internes Kontrollsystem (IKS) und Compliance-Funktion

- 77 Die erste Linie („First Line“) – die Fachbereiche – erstellt fachbereichsspezifische Organisations- und Arbeitsanweisungen, welche die Prozesse innerhalb des Fachbereiches definieren und bestimmen.¹⁴¹ Des Weiteren sind die Fachbereiche für das Treffen von strategischen Entscheidungen zuständig. Dahingehend entscheiden diese etwa über die Erschließung neuer Geschäftsfelder, Dienstleistungen, Märkte und Handelsplätze oder über die Auflage neuer Finanzprodukte sowie die Einführung neuer Werbestrategien für das Angebot von Wertpapierdienstleistungen. Solche Entscheidungen sind unter Berücksichtigung der damit verbundenen Risiken zu treffen, sodass die Einhaltung der anzuwendenden Vorschriften nicht gefährdet ist. Gemäß AT 6 Ziffer 2 der MaComp sind die operativen Bereiche für die Einhaltung der Vorschriften und die Durchführung von eigenen Kontrollen (Selbstkontrollen) verantwortlich. Somit besteht eine Pflicht der Fachbereiche zur Durchführung von eigenen Kontrollen (etwa der aufgestellten Abläufe und Prozesse). Des Weiteren sind nach AT 5 der MaRisk geeignete Kontrollen für die Identifizierung, Beurteilung und Steuerung der operativen Risiken einzurichten und entsprechend zu dokumentieren. Diese Kontrollen dienen neben der Vermeidung bzw. Steuerung von Risiken regelmäßig auch der Überwachung der Prozessqualität und der Überprüfung der Strategiekonformität. Die Fachbereiche haben demzufolge Prozesse und Maßnahmen zur Minimierung von Risiken und zur Qualitätssicherung einzurichten bzw. einzuleiten.
- 78 Die zweite Linie („Second Line“) – primär die Risikocontrolling-Funktion und die Compliance-Funktion – ist insbesondere für die Beratung und Überwachung der Fachbereiche als erster Linie und deren Kontrollprozesse verantwortlich.¹⁴² Die Compliance-Funktion berät und unterstützt insbesondere bei der Ausgestal-

¹⁴¹ Boldt/Büll/Voss, CCZ 2013, 248, 251.

¹⁴² Renz/Frankenberger, CB 2015, 420, 423.

tung neuer Produkte und Dienstleistungen.¹⁴³ Zudem analysiert und bewertet sie die von den verantwortlichen Fachbereichen erstellten Kontrollberichte der Geschäftsfelder. Darüber hinaus führt die zweite Linie regelmäßige als auch risikobasierte Kontroll- und Überwachungshandlungen durch. Diese umfasst die Überwachung der Abläufe, Prozesse, (Selbst-)Kontrollen sowie die Einhaltung interner (etwa Arbeits- und Organisationsanweisungen) sowie externer Vorgaben (etwa Gesetze, Richtlinien) durch angemessene und wirksame interne Verfahren. Daneben werden bestimmte Geschäftsaktivitäten direkt durch den Compliance-Beauftragten überwacht. Dazu zählen Mitarbeitergeschäfte und der Eigenhandel hinsichtlich der Einhaltung des Insiderhandelsverbots. Bei diesen Prozessen ist die Compliance-Funktion somit „Process Owner“ und damit in diesen Überwachungsprozessen, die eigentlich Kontrollprozesse sind, First Line. Darüber hinaus überwacht die Compliance-Funktion, ob die betroffenen Bereiche angemessene und wirksame Verfahren eigenverantwortlich einrichten und ihren Pflichten nachkommen. Umfasst sind auch ausländische Niederlassungen/Zweigstellen, die nach dem Prinzip der Herkunftslandaufsicht dem KWG und dem WpHG unterliegen.¹⁴⁴ Die Compliance-Funktion hat die Ergebnisse (insbesondere festgestellte Schwächen und Handlungsempfehlungen) ihrer Überwachung neben den zuständigen Fachbereichen auch der Geschäftsleitung und dem Aufsichtsorgan über Berichte mitzuteilen.¹⁴⁵ Dies kann risikobasiert im Rahmen der Regelberichterstattung, aber auch insbesondere bei schwerwiegenden Verstößen gegen compliance-relevante Vorschriften durch Ad-hoc-Berichte¹⁴⁶ erfolgen. Die Geschäftsleitung leitet im Falle von schwerwiegenden Verstößen geeignete Gegenmaßnahmen ein, die zeitnah von den jeweiligen Fachbereichen umzusetzen sind. Die Überwachung (der Einhaltung) dieser Maßnahmen liegt in der Verantwortlichkeit der Compliance-Funktion.

Zusammenfassend hat die Compliance-Funktion folgende Aufgaben im Rahmen des IKS:¹⁴⁷ **79**

1. Beratung¹⁴⁸ der Fachbereiche und der Geschäftsleitung: Beratung beim Einrichten neuer Verfahren, z. B. bei der Implementierung neuer Prozesse oder der Aufnahme neuer Produkte in den Vertrieb.
2. Überwachung
 - a) First-Line-Kontrollen und Prozesse, einschließlich risikobasierter Kontrolle von deren Ergebnissen;
 - b) Einhaltung der externen Vorgaben und Gesetze durch Vorhalten angemessener Prozesse und Verfahren;

143 *Welsch/Foshag*, in: Renz/Hense/Marbeiter, Wertpapier-Compliance in der Praxis, 2012, I.5. Rn. 18.

144 *Eisele/Faust*, in: Ellenberger/Bunte, Bankrechts-Handbuch, § 89, Rn. 120.

145 *Schäfer*, in: Krimphove, MaComp, BT 1.2.2, Rn. 409.

146 *Schockenhoff*, NZG 2015, 409, 411; *Schäfer*, in: Krimphove, MaComp, BT 1 Rn. 459 f.

147 Siehe grundlegend *Renz/Frankenberger*, CB 2015, 420 ff.

148 *Schäfer*, in: Krimphove, MaComp, BT 1.2.4, Rn 678.

- c) Einhaltung interner Arbeitsanweisungen und Verpflichtungen durch die Fachbereiche;
 - d) Maßnahmen zur Behebung von erheblichen Mängeln und Feststellungen;
 - e) Durchführung von Vor-Ort-Prüfungen.
3. Regelmäßige Berichterstattung an die Geschäftsleitung und das Aufsichtsorgan;
4. Unverzügliche Information an die Geschäftsleitung bei erheblichen Mängeln und Feststellungen;
5. Maßnahmen zur Vermeidung der Risiken.¹⁴⁹
- 80** Die dritte Linie („Third Line“) – die Interne Revision – ist vorwiegend für die Ex-Post-Prüfung, die sich auf alle Aktivitäten und Prozesse eines Institutes erstreckt, verantwortlich. Nach Einführung bzw. Veränderung von Geschäftsprozessen prüft die Interne Revision diese neuen Prozesse, welche zeitlich, zum Teil deutlich, nachgelagert sind. Die Interne Revision bewertet objektiv, prozessunabhängig die Wirksamkeit der Risikomanagement- und Steuerungsprozesse sowie des Überwachungssystems und prüft die Wirksamkeit des IKS, d.h. sowohl die Erfüllung der Aufgaben und Pflichten durch die Compliance-Funktion als zweite Linie und durch die einzelnen Fachbereiche als erste Linie.¹⁵⁰ Zur Wahrnehmung ihrer Aufgaben verfügt die Interne Revision über ein vollständiges und uneingeschränktes Informationsrecht gegenüber allen Fachbereichen.¹⁵¹

VII. Übertragung der Struktur/des Ansatzes auf andere Industriesäulen – und umgekehrt

- 81** Die Compliance-Funktion ist in der Finanzindustrie bereits fest etabliert, in der „Nicht-Banken-Industrie“ fehlen häufig noch der prozessuale Ansatz sowie die zur Einhaltung der Vorgaben notwendige Überwachungsfunktion durch Compliance. Zudem sind gerade in Industriebereichen, die nicht dem Finanzdienstleistungssektor zuzuordnen sind, Themenkomplexe der Compliance-Funktion zugeordnet, die sich so im Bankensektor noch nicht ausreichend wiederfinden. Hierzu gehört bspw. die Kartell-Compliance, die in der Industrie typischerweise in der Compliance-Funktion fest verankert ist.¹⁵² In Unternehmen des Finanzdienstleistungssektors wird das Thema Kartellrecht jedoch noch häufig den Rechtsbereichsfunktionen zugeordnet. Da es durchaus sinnvoll ist, kartellrechtliche Verfahren und Prozesse so im Unternehmen zu implementieren, dass Kartellabsprachen und Kartellverstöße nicht vorkommen können, ist dieses Thema aufgrund des prozessualen Ansatzes eindeutig der Compliance-Funktion zuzuordnen. Ferner ist das Thema Business Partner Due Diligence und damit die Überprüfung von Teilnehmern der Wertschöpfungskette im Vertrieb und in der

¹⁴⁹ Vgl. BaFin, MaComp, BT 1.2.2 Nr.7 lit. d.

¹⁵⁰ Welsch/Foshag, in: Wertpapier-Compliance in der Praxis, 2012, I.5. Rn. 15.

¹⁵¹ Hannemann/Steinbrecher/Weigl, Mindestanforderungen an das Risikomanagement (MaRisk), AT 4.4.3 Rn. 72 f.

¹⁵² Eufinger, WM 2014, 1113, 1114.

Herstellung der Produkte in Industrieunternehmen üblich und dort auch selbstverständlich der Compliance-Funktion zugeordnet.¹⁵³ Diese Compliance-Sicht entwickelte sich durch die „Product-Governance-Vorgaben“¹⁵⁴ gemäß § 80 WpHG, wonach Produktüberwachungsprozesse regelmäßig zu überprüfen sind.

Umgekehrt bestehen in der Finanzdienstleistungsindustrie Prozesse in der Compliance-Funktion, von denen auch die Industrie-Compliance profitieren kann. Hierzu gehört insbesondere der prozessuale Ansatz einer Compliance-Funktion im Finanzdienstleistungssektor.¹⁵⁵ Die Compliance-Funktion denkt und agiert in Prozessen und Verfahren, wohingegen Compliance-Funktionen in Industrieunternehmen häufig noch nach Rechtsbereichsthemen und Rechtsproblematiken denken und handeln. Das Denken in Prozessen macht durchaus Sinn, da durch die Implementierung eines wirksamen IKS Verantwortlichkeiten für Prozesse und Verfahren geschaffen werden, die so in der Industrie häufig noch nicht ausreichend vorhanden sind. Dadurch werden Verantwortlichkeiten klar gesetzt und diese auch entsprechenden Bereichen zugeordnet. Die Verantwortlichkeit für die Prozesse liegt dabei typischerweise gerade nicht in der Compliance-Funktion, sondern in den jeweils für den Prozess zuständigen Fachbereichen.¹⁵⁶ Ferner ist, teilweise aufsichtsrechtlich getrieben, im Finanzdienstleistungssektor die Compliance-Funktion von Legitimitätsgrundsätzen geprägt. Dies bedeutet, die Compliance-Funktion prüft, ob es opportun ist, rechtlich einwandfreie ausgestaltete Produkte und Dienstleistungen dennoch bestimmten Kundenkreisen anzubieten bzw. zu verkaufen. Dieser Schutzaspekt des Kunden i. S. v. Kundenschutz, Anlegerschutz und Verbraucherschutz ist so in der klassischen Industrie häufig noch nicht verankert. Hier ist die Compliance-Funktion im Wesentlichen darauf ausgerichtet, Risiken vom eigenen Unternehmen fernzuhalten, ohne dabei Kundenschutz-Themen zu berücksichtigen. Ein weiterer wesentlicher Punkt, der in der Finanzdienstleistungsindustrie mittlerweile „State of the Art“ ist, ist die Notwendigkeit der Sachkundevoraussetzungen für Compliance-Mitarbeiter und für den Compliance-Beauftragten.¹⁵⁷ Dies ist zwingend notwendig, da ohne Verständnis der Produkte, der Vertriebswege bzw. der Herstellungsprozesse der Produkte eine optimale und zweckdienliche Beratung der Fachbereiche durch die Compliance-Funktion überhaupt nicht möglich ist. Ferner ist das Verständnis für Vertriebswege notwendig, um korruptiven Verhaltensweisen proaktiv präventiv begegnen zu können. Dieses Verständnis zu den Sachkundevoraussetzungen für Compliance-Mitarbeiter bzw. für den Compliance-Beauftragten ist so in der Industrie noch nicht verankert. Dies führt häufig dazu, dass Compliance-Beauftragte die Prozesse im eigenen Hause nicht kennen, nicht verstehen und auch die Produkte nicht bis ins Detail beurteilen können. Dies ist aber notwendig, um

153 Liese, BB Special 4 (zu BB 50/2010), 27, 29.

154 Siehe hierzu Renz/Marbeiter, ZfGK 23/2023, 10 ff.

155 Hammer, BB 2013, 1175, 1178.

156 Wolff/Schroeren/Martin, CCZ 2014, 86, 88.

157 Hauschka/Galster/Marschlich, CCZ 2014, 242, 244.

Compliance-Risiken, die aus den Produkten, Dienstleistungen und Vertriebswegen entstehen können, adäquat beurteilen zu können, um im Rahmen einer Risikoanalyse diese auch an den Vorstand berichten zu können. Nicht ausreichende Sach- und Fachkunde bei Compliance-Mitarbeitern und dem Compliance-Beauftragten in der Industrie weist häufig auf eine schwachen Compliance-Funktion hin. Nur bei entsprechenden Kenntnissen können die Prozesse hinterfragt, Risiken gesehen und entsprechend transparent gemacht werden und auch zur Verminderung bzw. zur Vermeidung von Compliance-Risiken beigetragen.

VIII. Fazit/Ausblick

- 83** Es stellt sich also gerade nicht die Frage, ob die Compliance-Funktion im Finanzdienstleistungssektor besser ausgestaltet ist als im Nicht-Finanzdienstleistungssektor oder umgekehrt. Vielmehr sollte der Fokus beider Seiten das gegenseitige voneinander Profitieren sein. Dies beinhaltet insbesondere, wie die jeweiligen Vorteile der Compliance-Funktion des jeweils anderen Industriebereichs in die Überlegungen einzufließen lassen sind, wie im eigenen Unternehmen die Compliance-Funktion optimal zum Schutz des Unternehmens, der Mitarbeiter des Unternehmens aber auch der Kunden des Unternehmens ausgestaltet sein kann.
- 84** Der große Vorteil im Finanzdienstleistungssektor und der Finanzwirtschaft ist, dass die Einrichtung eines CMS durch spezielle Rechtsgrundlagen geregelt wird und Vorgaben zu einem strukturierten IKS existieren. Insbesondere bei Kreditinstituten ist das IKS aufsichtsrechtlich zwingend vorgegeben, was zur Folge hat, dass die Compliance-Funktion als Second Line zwingend innerhalb des IKS vorgeschrieben ist. Somit bestehen bei Kreditinstituten feste Strukturen, die im Nicht-Finanzdienstleistungssektor hingegen mangels gesetzlicher Vorschriften bislang nicht so ausgeprägt sind. Das IKS mit klar geregelten Prozessverantwortlichkeiten und Überwachungshandlungen durch die Compliance-Funktion ist Bestandteil der Governance-Struktur der Banken. Damit ist das CMS Bestandteil des IKS und demzufolge ähnlich strukturiert wie das IKS. Von diesem im Finanzdienstleistungssektor bestehenden strukturellen Ansatz können andere Branchen profitieren und die in Banken vorhandene Struktur im jeweiligen Unternehmen ganz oder teilweise übernehmen.

21. Kapitel

Produktbezogenes Compliance- und Risikomanagement im Treasury

I. Einleitung

Die Nutzung von Finanz- und Kapitalmarktprodukten durch Unternehmen der sogenannten Realwirtschaft birgt Risiken, die den Bestand des Unternehmens gefährden können. In der Regel handelt es sich um Risiken, die keinen Bezug zum Kerngeschäft des Unternehmens aufweisen und deshalb nur schwer oder gar nicht eingeschätzt werden können. Hinzu kommt, dass neben die marktbezogenen Risiken weitere Risiken treten, die sich aus der Konstruktion des Produkts ergeben. Selbst ein CFO mit Bankhintergrund, der im Unternehmen als Generalist tätig ist, wird damit auf ein ausgefeiltes Risikomanagementsystem angewiesen sein, um seinen Leitungspflichten nachkommen und die persönliche Haftung vermeiden zu können. Das Compliance-Management-System, das die Einrichtung und den Betrieb des Risikomanagementsystems begleitet, muss mit diesem eng verzahnt sein. Im Folgenden wird daher als „Best Practice“ davon ausgegangen, dass ein Unternehmen sich für ein integriertes Compliance- und Risiko-Management-System entscheidet (ICRM), das sich konzeptionell auch im Bankbereich zum Standard entwickelt. 1

Das vorliegende Kapitel befasst sich in Abschnitt II zunächst mit den relevanten Finanz- und Kapitalmarktprodukten und deren spezifischen Risiken (→ Rn. 3 ff.). Hierbei werden die Charakteristika genauso wie die spezifischen Risiken vor dem Hintergrund der Einordnung als „einfaches“ oder als „komplexes“ Finanzprodukt bestimmt. In Abschnitt III (→ Rn. 15 ff.) werden zunächst die Risikomanagement- und Compliance-Pflichten der regulierten Marktteilnehmer (Finanzinstitute) beschrieben. In einem zweiten Schritt wird dargestellt, unter welchen Voraussetzungen Unternehmen, die keiner Regulierung unterliegen, im Finanzbereich ein Risikomanagementsystem nach Bankvorbild einrichten müssen, das im Idealfall in einem ICRM aufgeht. In Abschnitt IV (→ Rn. 42 ff.) werden die verschiedenen Komponenten – „Tools“ – eines Risikomanagementsystems für Finanz- und Kapitalmarktprodukte erläutert und die Frage erörtert, ob und unter welchen Bedingungen die Risikomanagement- und Compliance-Pflichten im Finanzbereich an Dritte ausgelagert werden können. Ergänzt wird das Kapitel in Abschnitt V (→ Rn. 58 ff.) um die Erörterung von Haftungsfragen, die sich ergeben, wenn die Verantwortlichen es entweder unterlassen haben, erforderliche Systeme zu installieren oder ihnen Fehler im Umgang mit den Systemen oder den Finanzprodukten unterlaufen sind. Betrachtet werden auch die haftungsrechtlichen Implikationen des Einsatzes künstlicher Intelligenz im Finanzbereich. Es schließt sich in Abschnitt VI. ein Fazit an (→ Rn. 64). 2

II. Finanz- und Kapitalmarktprodukte; Risiken

1. „Einfache“ Produkte

- 3 Im Rahmen einer Risikoinventur ist es erforderlich, den Bestand an genutzten Finanz- und Kapitalmarktprodukten zu bestimmen. Um Verhaltenspflichten ableiten zu können, empfiehlt es sich zunächst, Kategorien zu bilden. Hierbei kann zwischen Produkten unterschieden werden, die als „einfach“ und solchen, die als „komplex“ einzustufen sind. „Einfache“ Produkte lassen sich im Gegensatz zu „komplexen“ Produkten häufig nicht in verschiedene Komponenten teilen.¹ Die Tatsache, dass ein Produkt nicht „strukturiert“ ist, lässt häufig den Schluss darauf zu, dass die Risiken begrenzt sind. „Einfache“ Produkte sind beispielsweise:

Produkte	Eigenschaften
Zahlungsverkehr	Auftragsgemäße Abwicklung eines Zahlungsstroms
Darlehen mit fester/variabler Verzinsung	Abwicklung eines bis zur Endfälligkeit festgelegten Zahlungsstroms; beim variabel verzinslichen Darlehen gebunden an allgemein verbindliche Referenz (z. B. EURIBOR)
Aval/Akkreditiv	Standardisierte Abwicklung von Lieferung/Zahlung über Bank unter Herausnahme des Kundenrisikos
Factoring	Abwicklung eines Zahlungsstroms aus dem Kerngeschäft; die Risiken bestimmen sich im Wesentlichen nach der Kundenbonität
Bestimmte standardisierte Derivate, soweit sie ausschließlich der Risikoabsicherung einer Einzelposition dienen, über Clearing-Stellen abgewickelt werden, keine Stillhalterrisiken begründen und deutschem Recht unterliegen	„Spiegelung“ eines Zahlungsstroms zu Absicherungszwecken; „Null-Summen-Spiel“

- 4 Betrachtet man die Beispiele, so wird deutlich, dass die Risiken der jeweiligen Produkte recht transparent sind. Im Zahlungsverkehr geht es regelmäßig um einen Auftrag an die Bank, der dann ohne weiteren Eingriff Dritter und ohne Ermessensspielräume der Bank auszuführen ist. Auch Darlehen sind grundsätzlich

¹ Im angelsächsischen Sprachgebrauch werden „einfache“ Finanzprodukte als „plain vanilla“ bezeichnet. Im Derivatebereich werden häufig die Begriffe „komplex“, „exotisch“ oder auch „strukturiert“ als Gegensatz zu „plain vanilla“ verwendet. Siehe zu komplexen Finanzderivaten z. B. *de Corbavia-Perisc/Maier*, in: Zerey, Finanzderivate, S. 101 ff.

„einfach“ strukturiert. Zwar müssen die Bedingungen verhandelt und dokumentiert werden. Jedoch hat das Unternehmen als Darlehensnehmer über die Laufzeit bis zur Endfälligkeit keine besonderen Risiken aus der Sphäre Dritter zu tragen, sieht man einmal vom Referenzzinssatz beim variabel verzinslichen Darlehen ab. Bei der Nutzung von Avalen und den darauf aufbauenden Finanzprodukten (z. B. Garantie oder Akkreditiv) geht es im Wesentlichen um die Ausschaltung des Kunden- oder des eigenen Bonitätsrisikos, das auch ohne das jeweilige Finanzprodukt zu überwachen wäre und dem Kerngeschäft zuzuordnen ist. Das Factoring ist in dieser Hinsicht auch als „einfaches“ Produkt zu bewerten, weil die Forderungen gegen Kunden mit einem Abschlag aber regresslos an die Factoring-Bank verkauft werden („echtes Factoring“). Auch im Laufe der Factoring-Transaktion ist das Unternehmen nur Forderungen ausgesetzt, die aus der eigenen oder der Bonität von Kunden (Kerngeschäft) resultieren. Zudem sind die Forderungen regelmäßig über einen Warenkreditversicherer abgesichert.² Bestimmte standardisierte Derivate sind nach der Reform des Derivatemarktes durch die European Market Infrastructure Regulation (EMIR)³ als „einfach“ einzustufen, sofern sie der Einzelabsicherung dienen, über Clearing-Stellen abgewickelt werden, keine Stillhalterrisiken begründen und deutschem Recht unterliegen.

2. „Komplexe“ Produkte

a) Überblick

„Komplexe“ Produkte sind in der Regel zusammengesetzt und/oder beziehen sich auf einen Basiswert, der vom Unternehmen entweder nicht überwacht oder nicht beeinflusst werden kann. Die spezifische Gefährlichkeit solcher Produkte besteht darin, dass die Risiken aus sämtlichen Komponenten des Produkts und deren Wechselwirkung berücksichtigt werden müssen. Komplexe Produkte sind beispielsweise:

2 Näher zum Factoring im Unternehmensbereich: von Bodungen, in: Kessler, Unternehmensfinanzierung Mittelstand, S. 277 f.

3 Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4.7.2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister, ABl. L 201 vom 27.7.2012, S. 1, ergänzt durch das Gesetz zur Einführung von Sondervorschriften für die Sanierung und Abwicklung von zentralen Gegenparteien und zur Anpassung des Wertpapierhandelsgesetzes an die Unterrichts- und Nachweispflichten nach den Artikeln 4a und 10 der Verordnung (EU) Nr. 648/2012, BGBl. I 2020, S. 529.

Teil 3 Besondere Aufgaben und Anwendungsfelder

Produkte	Eigenschaften
Cash-Pooling- und Payment-Factroy-Lösungen	Software-basierte und damit automatische Abwicklung von konzerninternen Zahlungsströmen (auch unter Einsatz von künstlicher Intelligenz), die rechtlichen Restriktionen unterliegen
Darlehen mit separater Zinssicherung	Zwar Abwicklung eines festen Zahlungsstromes unter dem Darlehen, aber separater Zahlungsstrom mit unbegrenztem Risiko über den Kapitaleinsatz hinaus unter dem Zins-Swap/-Cap
ABS (= Asset Backed Securities)	Verkauf eines Kundenzahlungsstroms an eine Zweckgesellschaft (SPV) – grundsätzlich wie Factoring, aber unter Einbindung von Kapitalmarktinstrumenten („Kapitalmarkt-Factoring“)
Strukturierte Schuldscheine, Anleihen und Kreditderivate	Abwicklung eines Zahlungsstromes, der von der Bonität Dritter und dem Kapitalmarkt abhängig ist sowie rechtlich anspruchsvoll dokumentiert wird
Derivate, welche die oben unter 1. erläuterten Kriterien nicht erfüllen	Häufig Begründung von Zahlungsströmen mit unbegrenztem Verlustrisiko, die sich nicht auf gegenläufige Zahlungsströme aus dem Kerngeschäft beziehen (kein Hedging)
Sonstige zusammengesetzte Produkte	s. o.

- 6 Die Schwierigkeit bei dem Einsatz von Cash-Pooling- und Payment-Factory Lösungen ergibt sich im Konzern bereits daraus, dass regelmäßig taggleich über die vorhandene Liquidität aller Konzerngesellschaften verfügt wird, obgleich unter Kapitalerhaltungsgesichtspunkten (§§ 30, 31 GmbHG; § 57 AktG) jedenfalls in der Kapitalgesellschaft im Einzelfall über die Kreditgewährung an die Muttergesellschaft unter Bonitätsgesichtspunkten entschieden werden müsste.⁴ Darüber hinaus sind viele Funktionen der marktüblichen Payment-Factory-Lösungen software-basiert und damit automatisiert, sowohl im Hinblick auf das „Pooling“ an sich und die weitere Verwendung von Finanzprodukten wie zum Beispiel den Einsatz von Derivaten zur Absicherung von bestimmten Risiken.
- 7 Darlehen mit separater Zinssicherung sind regelmäßig so strukturiert, dass ein variabel verzinsliches Darlehen mit einem Swap oder einem Cap verbunden wird. Hierdurch tauscht (Swap) das Unternehmen gegen Gebühr den variablen gegen einen festen Zins. Bei der Verwendung eines Caps erwirbt das Unternehmen gegen Zahlung einer Gebühr das Recht, über einen bestimmten Zinssatz hinaus kein höheres Zinsrisiko zu tragen, weil der Vertragspartner des Cap ein-

4 Zu den Pflichten der Geschäftsführung bei der Nutzung von Cash-Pooling: *Gesell/Seulen*, in: Kessler, Unternehmensfinanzierung Mittelstand, S. 140.

springt. Häufig werden diese Gestaltungen bei der Finanzierung von gewerblichen Immobilien (aber auch darüber hinaus) eingesetzt. Nicht selten ist die darlehensgebende Bank zugleich Vertragspartner der Zinssicherung. Die swap-basierte Variante wird gefährlich, wenn das Darlehen vorzeitig fällig wird, entweder weil die Immobilie veräußert wurde, das Unternehmen gekündigt hat oder die Bank das Darlehen vorzeitig fällig gestellt hat. In einem solchen Fall ist nicht nur die Darlehensvaluta zurückzuzahlen, sondern es sind auch die Forderungen aus dem Derivat zu erfüllen, die grundsätzlich der Höhe nach nicht begrenzt sind. Hat sich das Zinsniveau während der Laufzeit des Darlehens entsprechend markant und gegenläufig verändert, ist der Ausgleichsanspruch des Vertragspartners entsprechend hoch, ohne dass sich etwas an der Hauptforderung der Bank geändert hätte.⁵

Die Ausgabe von Asset Backed Securities (ABS) in der Form der Verbriefung von Handelsforderungen dient grundsätzlich dem gleichen Zweck wie Factoring, nämlich der Veräußerung von Kundenforderungen zur Liquiditätsgewinnung. Der Unterschied besteht darin, dass die Forderungen zwar regresslos verkauft werden, der Käufer aber keine Bank ist, welche die Forderungen zum Einzug auf ihre Bilanz nimmt, sondern eine Zweckgesellschaft, die ihrerseits Anleihen am Kapitalmarkt begibt, um den Kaufpreis zu refinanzieren.⁶ Die Bedingungen des Forderungsverkaufs und die Zahlungsströme, die damit verbunden sind, müssen entsprechend gestaltet werden und auf Rating-Erfordernisse muss Rücksicht genommen werden. Die Transaktion kann grundsätzlich vom Arrangeur bzw. der Zweckgesellschaft gekündigt werden, wenn diese sich am Kapitalmarkt nicht mehr zu den ursprünglich festgelegten Konditionen refinanzieren kann. Unter anderem trägt das Unternehmen daher neben dem Bonitätsrisiko des Arrangeurs, der die Zweckgesellschaft zusätzlich absichert, auch das allgemeine Kapitalmarktrisiko. Beide Risiken kann das Unternehmen nicht steuern.

Derivate, die als „komplex“ einzustufen sind, dienen häufig nicht der Absicherung von Einzelpositionen, sondern beziehen sich auf Portfoliorisiken. Ein solches „Makro Hedging“ kann sinnvoll sein, wenn bestimmte Portfoliorisiken sich bereits gegenseitig aufheben (zum Beispiel im Wege des „Netting“, der Verrechnung von gegenseitigen Ansprüchen). Es werden zudem immer wieder Fälle bekannt, in denen Unternehmen mit Derivaten spekuliert haben, um Zusatzertrag zu generieren. Bekannt geworden ist zum Beispiel der Fall eines mittelständischen Unternehmens, das einen sogenannten „Spread Ladder Swap“ von der Deutschen Bank erworben hatte, um auf die Differenz zwischen kurz- und langfristigen Zinsen zu wetten.⁷ Neben erheblichen Kosten, die im Produkt versteckt waren, bestand ein praktisch unbegrenztes Verlustrisiko.

⁵ Siehe auch unten → Rn. 46 ff. zu den Auswirkungen des Marktrisikos auf den Wert des Swap.

⁶ Zur Funktionsweise siehe von Bodungen, in: Kessler, Unternehmensfinanzierung Mittelstand, S. 281 ff.

⁷ BGH, Urt. v. 22.3.2011 – XI ZR 33/10, BGHZ 189, 13 („Zinswette“).

b) Risiken im Einzelnen

- 10** Neben den Marktpreisrisiken, die sich materialisieren, wenn die entsprechende Prognose nicht eintritt, weisen vor allem die „komplexen“ Produkte häufig auch weitere Risiken auf. So erwähnt zum Beispiel das bankbetriebliche Risikobild zusätzlich zum Marktpreisrisiko Adressenausfall-, Liquiditäts- und operationelle Risiken⁸ und bezieht diese Risiken auf Finanzinstrumente, aber auch auf den Bankbetrieb selbst. Adressenausfallrisiko wird häufig auch als Kreditrisiko bezeichnet. Es beschreibt das Risiko des bonitätsbedingten Ausfalls der Gegenpartei und lässt sich, wieder bankbetrieblich geprägt, weiter ausdifferenzieren.⁹ Liquiditätsrisiko bezieht sich vorwiegend auf diejenigen Finanzprodukte, die an einer Börse gehandelt werden. Fehlt es dort an Liquidität, wird die Fähigkeit des Unternehmens eingeschränkt, sich von einem verlustbringenden Instrument zu trennen. Hierdurch können weitere Verluste (bis hin zum Totalverlust) entstehen.
- 11** Der Begriff „operationelles Risiko“ wird häufig aus Bankensicht verwendet, um diejenigen Risiken zu beschreiben, die durch einen „Fehler“ im weitesten Sinne entstanden sind. Das Paradebeispiel hierfür ist eine fehlerhafte Geschäftsorganisation oder der Verstoß gegen rechtliche Gebote und Verbote („Rechtsrisiko“). Jedenfalls aus Bankensicht fallen rechtliche Defekte der Dokumentation von vertriebenen Finanzprodukten ebenfalls in den Bereich des Rechts- und damit des operationellen Risikos. Auch aus Unternehmenssicht trägt eine eigenständige Risikokategorie „operationelles Risiko“. Das Rechtsrisiko muss allerdings etwas anders definiert werden, weil ein Unternehmen Finanzprodukte nutzt und nicht selbst vertreibt. Ein rechtlicher Defekt der Dokumentation begründet danach Rechtsrisiko, wenn er sich nachteilig für das Unternehmen auswirkt, zum Beispiel wenn eine das Unternehmen schützende Vertragsbestimmung unwirksam ist. Häufig sind „komplexe“ Produkte aus Unternehmenssicht auch rechtlich riskant.¹⁰
- 12** Betrachtet man die Beispiele oben (→ Rn. 5 ff.), so ergeben sich neben den marktbezogenen folgende weitere, rechtliche Risiken:

⁸ Näher *Kessler*, BB 2013, 1098, 1099.

⁹ *Bessis*, Risk Management in Banking, 2010, 28, unter Verweis auf die weiteren aufsichtsrechtlich vorgegebenen Risikokategorien innerhalb des Adressenausfallrisikos.

¹⁰ Zu den Rechtsrisiken im Derivatebereich ausführlich *Kessler*, Das Strukturrisiko von Finanzderivaten, S. 231 ff. (Dokumentation unter Deutschem Rahmenvertrag und ISDA Master Agreement). Lesenswert – weil unerwartet – BGH, Urt. v. 9.6.2016 – IX ZR 314/14 (zitiert nach juris) (DRV teilweise unwirksam).

Produkte	Rechts- und Dokumentationsrisiken
Cash-Pooling- und Payment-Factor-Lösungen	Umfangreiche Vertragsdokumentation, die von allen GF der Konzerngesellschaften nach Schulung über das Kapitalerhaltungsrecht unterzeichnet werden muss; keine Standards ersichtlich; Verknüpfung mit Software-Lösungen Bank und i. d. R. SAP erforderlich
Darlehen mit separater Zinssicherung	Dokumentation des Darlehens nach deutschem Recht oder LMA-Standard (Loan Market Association Standard), teilweise englisches Recht; Dokumentation des Swaps/Caps häufig nach englischem oder New Yorker Recht (ISDA – International Swaps and Derivatives Association); Verknüpfung der Rechtssysteme erforderlich, sonst „Mismatch“ (Unwirksamkeit einzelner Bestimmungen)
ABS (= Asset Backed Securities)	Umfangreiches Vertragswerk, das mehreren Rechtsordnungen unterliegt (Unternehmen, Bank, Zweckgesellschaft, „Kapitalmarkt“)
Strukturierte Schuldscheine, Anleihen und Kreditderivate	Umfangreiches Vertragswerk, das in der Regel angelsächsischen Standards folgt und häufig nicht deutschem Recht unterliegt
Derivate, welche die oben unter 1. erläuterten Kriterien nicht erfüllen	Entweder individuelle Dokumentation (selten) oder Verwendung von DRV (Deutscher Rahmenvertrag für Finanztermingeschäfte) oder ISDA, Letztere nach englischem oder New Yorker Recht; Besicherung der Transaktionen mit hohem „Mismatch“-Risiko, wenn nach den Besicherungsanhängen Sicherheiten verwendet werden, die sammelverwahrt werden
Bestimmte Equity-Instrumente	s. o.

Sicherlich lassen sich Dokumentationsfehler vermeiden, doch erfordern komplexe Produkte dann den Einsatz entsprechend erfahrener interner oder externe Rechtsanwälte. Häufig wird aber der Aufwand gescheut und man verlässt sich auf die Aussagen der jeweiligen Gegenpartei oder man beauftragt den angestammten Berater, der nicht notwendigerweise Erfahrung mit den relevanten Produkten hat. Viele Risiken, die sich aus der Dokumentation von Finanz- und Kapitalmarktprodukten ergeben, verstärken sich gegenseitig. Diese Risiken stehen wiederum im Verhältnis der Wechselwirkung zu den marktbezogenen Risiken und begründen eine eigene Risikokategorie, das Strukturrisiko.¹¹ Häufig ist

13

11 Grundlegend: *Kessler*, Das Strukturrisiko von Finanzderivaten, S. 46 ff.

zum Beispiel nicht bekannt, dass eine finanzierte Immobilie auch dann verwertet werden kann, wenn der Darlehensnehmer zwar den Darlehensvertrag erfüllt, also Zins und Tilgung leistet, aber den negativen Marktwert eines zusätzlich abgeschlossenen Zinssicherungsinstruments nicht durch entsprechende Sicherheiten abdeckt oder, im Rahmen einer Umfinanzierung, ausgleicht. In diesem Fall verwirklicht sich das Strukturrisiko dergestalt, dass ein Marktpreisrisiko (Veränderung der Zinsen) mit einem Rechtsrisiko (riskante vertragliche Verknüpfung zweier Finanzinstrumente) zusammentrifft und dadurch einen hohen Schaden verursachen. Im schlimmsten Fall kann eine solche Konstellation für das Unternehmen bestandsgefährdend sein.

- 14 Es ist in diesem Zusammenhang auch zu berücksichtigen, dass es wissenschaftlich allgemein akzeptierte Methoden der Risikobestimmung nicht gibt. Marktpreisrisiken werden regelmäßig „approximiert“ (geschätzt) und zwar im Rahmen von Value-at-Risk-Modellen, die letztlich die „Gauß'sche Normalverteilung“ abbilden.¹² Operationelle und damit auch Rechtsrisiken lassen sich allerdings gar nicht über mathematische Verfahren bestimmen. Hier bedarf es der Analyse von Wirkungsketten. Es liegt auf der Hand, dass eine solche Betrachtung zeit- und ressourcenintensiv ist und bei der Verwendung von Finanzprodukten auf Unternehmensseite mangels eigener Ressourcen in der Regel ausscheidet.

III. Rechtliche Anforderungen an das Risikomanagement- und Compliance-System

1. Anforderungen an Finanzinstitute

a) Aufsichtsrechtliche Anforderungen

- 15 Finanzunternehmen unterliegen strengen Anforderungen beim Risikomanagement und bei der Compliance.¹³ Das gilt verstärkt seit den Gipfelbeschlüssen von Pittsburgh 2009, die sich zum Ziel gesetzt haben, durch eine verstärkte Regulierung der relevanten Marktteilnehmer eine neue Finanzkrise zu verhindern.¹⁴ Grundsätzlich ergeben sich die Anforderungen für regulierte Kapitalgesellschaften aus dem Gesellschaftsrecht (§ 91 Abs. 2 AktG; § 43 Abs. 2 GmbHG; DCGK) und, weitergehend, aus dem Aufsichtsrecht, das wiederum nach der Art des Geschäftsbetriebs und der jeweiligen Schutzrichtung (Institut oder Kunde) variiert. Rechtsquellen sind hier insbesondere das KWG inklusive MaRisk BA, das WpHG, die Delegierte Verordnung (EU) 2017/565, die

12 Dazu näher unten → Rn. 46 ff. und Kessler, BB 2013, 1098, 1099.

13 Siehe hierzu auch → Renz/Frankenberger, Kap. 20.

14 Die Erklärung des G20-Gipfels von Pittsburgh zur Finanzmarktregulierung findet sich unter <https://www.bundesregierung.de/resource/blob/975254/474982/ba28f22bea0df3b25beec209cd62f936/g20-erklaerung-pittsburgh-2009-de-data.pdf?download=1> (zuletzt abgerufen am 6.2.2024).

WpDVerOV sowie die MaComp¹⁵ und die entsprechenden weiteren europarechtlichen Vorgaben, häufig in der Form der „Technischen Ausführungsstandards“ oder als sonstige administrative Konkretisierungen. Das Risikomanagement von Instituten erstreckt sich, anders als die Compliance-Funktion, die umfassender ist, auf die Überwachung der Erreichung und Erhaltung des regulatorischen Kapitals nach der europäischen Capital Requirements Regulation (CRR).¹⁶

Die Risikomanagement- und Compliance-Pflichten ergeben sich für Institute im Einzelnen aus § 25a KWG in Verbindung mit den Bestimmungen der „Mindestanforderungen für das Risikomanagement“ (MaRisk BA),¹⁷ die auch für Versicherungen¹⁸ und Kapitalverwaltungsgesellschaften¹⁹ in ähnlicher Form als Rundschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht Bindungswirkung entfalten. **16**

Die MaRisk BA, die im vorliegenden Beitrag exemplarisch betrachtet werden soll, besteht aus einem „allgemeinen Teil“ (AT) und einem „besonderen Teil“ (BT), der in verschiedene Module aufgeteilt ist, die sich an den jeweiligen Geschäftsarten des Instituts orientieren. AT 3, als Generalklausel, enthält die sich auch aus dem Gesellschaftsrecht ergebende Verpflichtung der Geschäftsleitung, „... die Risiken beurteilen zu können“. Wie dies im Einzelnen geschieht, regeln die weiteren Bestimmungen des AT und des BT. Insbesondere schreiben AT 5 bis 7 Dokumentationspflichten vor und enthalten Anforderungen an die technische und personelle Ausstattung. Das Modul BTR enthält Regelungen für die relevanten Risikosteuerungs- und Controlling-Prozesse und bezieht diese auf die bereits erwähnten Risikopositionen Adressenausfallrisiko, Marktpreisrisiko, Liquiditätsrisiko und operationelles Risiko. Zur unabhängigen Überwachung der Prozesse muss nach AT 4.4.1 eine Risikocontrolling- und nach AT 4.4.2 eine Compliance-Funktion geschaffen werden. Letztere ist von einem Compliance-Beauftragten zu verantworten. **17**

Entscheidend sind neben den Anforderungen der MaRisk BA die Konkretisierungen, die sich kundenseitig aus den §§ 63 ff. WpHG, den Art. 21 ff. der Delegierten Verordnung (EU) 2017/565 und der MaComp ergeben. Betrachtet man **18**

15 Rundschreiben 05/2018 (WA) – Mindestanforderungen an die Compliance-Funktion und weitere Verhaltens-, Organisations- und Transparenzpflichten vom 19.4.2018 in der Fassung vom 30.6.2023.

16 Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26.6.2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 646/2012 und Verordnung (EU) Nr. 876/2019 des Europäischen Parlaments und des Rates vom 20.5.2019 zur Änderung der Verordnung (EU) Nr. 575/2013 und der Verordnung (EU) Nr. 648/2012 („CRR 2“).

17 Rundschreiben 05/2023 (BA) der BaFin zu den Mindestanforderungen an das Risikomanagement, Stand 18.10.2023. Siehe hierzu auch → *Renz/Frankenberger*, Kap. 20 Rn. 37 ff.

18 Rundschreiben 2/2017 (VA) der BaFin zu den Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo), Stand 2.3.2018.

19 Rundschreiben 01/2017 (WA) der BaFin zu den Mindestanforderungen an das Risikomanagement von Kapitalverwaltungsgesellschaften (KAMaRisk), Stand 10.1.2017.

zusätzlich die WpDVerOV, die für bestimmte Bereiche das kundenbezogene Wertpapiergeschäft gilt, ergeben sich ähnliche Anforderungen, insbesondere im Hinblick auf Konzeptionierung und den Vertrieb von Produkten. Es müssen weitreichende organisatorische Anforderungen erfüllt werden. Hierzu gehört in allen relevanten Bereichen die Einrichtung einer qualifizierten Compliance-Funktion, die von einem Compliance-Beauftragten verantwortet werden muss. Auch wenn die WpDVerOV in erster Linie sicherstellen soll, dass die Interessen der Kunden in spezifischen Situationen wie z. B. der Honorar-Anlageberatung geschützt werden, entfaltet sie, wie WpHG und die dazugehörige Delegierte Verordnung, auch interne Wirkung. Geschäftsprozesse, die den Anforderungen des Kundenschutzes genügen, wirken sich auch langfristig positiv für das Institut aus.

b) „Best Practice“ und praktische Ausgestaltung

- 19 In der Praxis haben sich sowohl für Finanzinstitute nach der MaRisk BA als auch kundenseitig und für Wertpapierdienstleister nach WpHG, Delegierter VO, Ma-Comp und WpDVerOV „Standards“ bzw. eine „Best Practice“ herausgebildet, wie mit den aufsichtsrechtlichen Anforderungen umzugehen ist. Hierbei ist auf der rechtlichen Ebene noch zwischen Risikomanagement einerseits und Compliance andererseits zu unterscheiden.²⁰ Inhaltlich sind die Anforderungskreise in der Praxis schon weitgehend verschmolzen. Auch die für die Abschlussprüfung relevanten IDW-Standards, hier IDW PS 980 (Stand: 09/2022), gehen von einem thematisch integrierten Konzept aus, obwohl sich IDW PS 980 streng genommen nur auf die Prüfung eines Compliance-Management-Systems bezieht.²¹

aa) Risikomanagement

- 20 Im Bereich des Risikomanagements sind die Bestimmungen der MaRisk umzusetzen, damit die Risikotragfähigkeit des Instituts sichergestellt werden kann. Das geschieht nach AT 2.2 MaRisk BA zunächst durch Erstellung eines Gesamtrisikoprofils, das vor allem die wesentlichen Risiken für die Vermögens-, Ertrags- und Liquiditätslage identifizieren muss. Darüber hinaus müssen wegen des nicht abschließenden Charakters der Risikoauflistungen in der MaRisk weitere Risiken identifiziert werden, wobei insgesamt Methodenfreiheit besteht.²²
- 21 Nach AT 4.1 MaRisk BA besteht die Pflicht, einen internen Prozess einzurichten, der sicherstellt, dass die Risikoidentifikation und -bewertung nach den Regeln der MaRisk BA gewährleistet ist. Dieser interne Prozess muss die nach § 25a Abs. 1 Satz 3 KWG erforderlichen Elemente eines Risikomanagement-

20 Inwieweit diese Unterscheidung mit dem Übergang zu ICRM in der Praxis regulatorisch in der Zukunft entfällt, muss abgewartet werden.

21 Hinzu tritt letztlich noch der Einrichtungsstandard ISO 19600, der sich grundsätzlich auch auf Compliance-Systeme bezieht.

22 I. E. auch *Braun*, in: Fischer/Schulte-Mattler, KWG CRR, § 25a Rn. 102 unter Verweis auf die zunehmende Normendichte in diesem Bereich und die weiter konkretisierenden Anforderungen aus den Rundschreiben der BaFin.

systems, nämlich Risikomanagementstrategie, Risikotragfähigkeitskonzept, interne Kontrollverfahren, personelle und technische Ausstattung, Notfallkonzept und nachhaltiges Vergütungssystem nach der InstitutsVergV, enthalten. Die einzelnen Komponenten stellen sich wie folgt dar:

(1) Risikomanagementstrategie

Die Risikomanagementstrategie dient der Verwirklichung des Risikomanagements auf Gruppenebene, d. h. der Erfassung und Reduzierung aller wesentlichen Risiken im Rahmen der Geschäfts- und Risikostrategie.²³ Das konkrete Risikomanagementsystem und damit auch die Risikomanagementstrategie hängen von den Geschäftsaktivitäten der Gruppe ab und sind damit auch produktbezogen zu entwickeln. Praktisch heißt das, dass allgemeine sowie produktbezogene Risikomanagement- und Controlling-Prozesse aufzusetzen sind.²⁴ Für komplexe Finanzprodukte wird zunächst danach zu differenzieren sein, ob das Institut als Anbieter oder als Nutzer des Produkts auftritt. Die Risikomanagementstrategie unterscheidet sich naturgemäß danach, ob ein komplexes Finanzprodukt originär bilanzielle Risiken begründet (Kapitalrelevanz) oder das Institut einer Eventualverbindlichkeit, nämlich einer möglichen Haftung gegenüber dem Kunden, aussetzt.

Betrachtet man die Risikomanagementstrategie und das damit verbundene Compliance-Management vor dem Hintergrund einer Nutzung komplexer Finanzprodukte, die zu Kapitalthemen nach der CRR führt, sind die Anforderungen nicht nur in § 25a KWG und der MaRisk BA zu suchen, sondern auch in der CRR selbst, die Instituten vorschreibt, wie und wie viel Kapital vorgehalten werden muss, um die Geschäftsrisiken abzudecken. Die CRR erwähnt in den Offenlegungsbestimmungen (Art. 435 Abs. 1 CRR) vor allem die Bereiche Risikosteuerung, Risikomanagement, Risikoberichts- und Messsysteme sowie Risikoabsicherung und -minderung, die mit konkreten Angaben zu unterlegen sind. Die jeweiligen Maßnahmen beziehen sich dann wieder auf die vorerwähnten Risikotypen Markt-, Adressenausfall-, Liquiditäts- und operationelles Risiko.

(2) Risikotragfähigkeitskonzept

Das Risikotragfähigkeitskonzept enthält dementsprechend Elemente der Informationssammlung und -verarbeitung, der Risikobestimmung und -analyse sowie der Anwendung kapitalbezogener und anderer Anforderungen aus § 25a KWG, der MaRisk BA und der CRR und wird damit wiederum Teil der Risikomanagementstrategie. Entscheidend für die Ausgestaltung des Risikotragfähigkeitskonzepts ist – jedenfalls bei der Nutzung von Finanzprodukten – die Bewertung und das Management von Marktrisiken.

²³ Näher hierzu: *Braun*, in: Fischer/Schulte-Mattler, KWG CRR, § 25a Rn. 148 ff.

²⁴ Siehe hierzu die Übersicht der WP-Gesellschaft Deloitte bei *Braun*, in: Fischer/Schulte-Mattler, KWG CRR, § 25a Rn. 94.

(3) Interne Kontrollverfahren

- 25** Die internen Kontrollverfahren („Risiko-Controlling“) sollen sicherstellen, dass die bestehenden Risiken richtig eingeschätzt und behandelt werden. Insofern beinhaltet das Risiko-Controlling Prozesse zur Identifizierung, Beurteilung, Steuerung und Überwachung der Risiken,²⁵ die von der internen Revision validiert und nachgeprüft werden. Die Compliance-Funktion dagegen prüft, ob das Risiko-Controlling selbst den gesetzlichen Anforderungen genügt.

(4) Personelle und technische Ausstattung

- 26** Das Institut muss tatsächlich in der Lage sein, die Anforderungen an das Risikomanagement zu erfüllen. In erster Linie stellt es dazu sicher, dass es über Mitarbeiter und technische Systeme verfügt, die dafür geeignet sind. „Geeignet“ bedeutet in diesem Zusammenhang, dass ausreichend Mitarbeiter vorhanden sind, die über das nötige Know-how verfügen, um Risiken entdecken und bewerten zu können (quantitative und qualitative Komponente). Dies muss durch die Einstellungspolitik, durch Schulungen, Neuproduktprozesse und Handbücher sichergestellt werden. Technische Systeme und damit vor allem das IT-System müssen nach gängigen Standards aufgebaut sein und die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten gewährleisten.²⁶

(5) Notfallkonzept

- 27** Im Rahmen eines Notfallkonzepts sind Vorkehrungen vor allem im Bereich der IT-Systeme aber auch darüber hinaus zu treffen. So sind Redundanzen zu schaffen, die sicherstellen, dass der Geschäftsbetrieb und damit auch das Risikomanagement in Krisenzeiten aufrechterhalten werden kann. Das Notfallkonzept muss regelmäßig getestet werden und geeignet sein, die zu erwartenden Schäden erheblich zu reduzieren.²⁷ Das Konzept muss auch Wiederanlaufpläne enthalten.²⁸

(6) Nachhaltiges Vergütungssystem

- 28** Die Einrichtung eines nachhaltigen und transparenten Vergütungssystems soll sicherstellen, dass nur solche Risiken eingegangen werden, die den langfristigen Unternehmenserfolg nicht gefährden. Die InstitutsVergV wurde insofern als vom Financial Stability Board (FSB) empfohlene Maßnahme mit den Inhalten der CRD II-Richtlinie²⁹ ursprünglich im Jahr 2010 von der BaFin erlassen und

²⁵ *Hellstern*, in: Luz/Neus/Schaber/Schneider/Wagner/Weber, KWG mit CRR, § 25a KWG Rn. 11.

²⁶ *Braun*, in: Fischer/Schulte-Mattler, KWG CRR, § 25a Rn. 622 f., wobei die technischen Standards solche sind, die nicht ausschließlich im Bankbereich gelten wie z. B. das Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik und ISO 17799.

²⁷ *Braun*, in: Fischer/Schulte-Mattler, KWG CRR, § 25a Rn. 640.

²⁸ *Braun*, in: Fischer/Schulte-Mattler, KWG CRR, § 25a Rn. 642.

²⁹ Richtlinie 2009/111/EG des Europäischen Parlaments und des Rates vom 16.9.2009 zur Änderung der Richtlinien 2006/48/EG, 2006/49/EG und 2007/64/EG hinsichtlich Zentralorga-

gilt nunmehr in der Fassung vom 28.8.2013. Sie geht grundsätzlich davon aus, dass höhere Risiken von den Mitarbeitern und Organen eingegangen werden, wenn sie von variablen Gehaltsbestandteilen abhängig sind. Die InstitutsVergV soll sicherstellen, dass Mitarbeiter und Organe nur entsprechend der Risikolage des Instituts vergütet werden und diesbezüglich keine Manipulationsmöglichkeiten gegeben sind, z. B. durch Absicherungsmaßnahmen im Interesse des Vergütungsempfängers.³⁰ Primär verantwortlich ist an dieser Stelle nicht das Risiko-Controlling, sondern die Compliance-Funktion.

bb) Compliance

(1) MaRisk BA-Compliance

Die Compliance-Pflicht aus der MaRisk soll sicherstellen, dass neben der MaRisk selbst alle für das Institut geltenden gesetzlichen Bestimmungen eingehalten werden, wobei der Begriff der „gesetzlichen Bestimmungen“ grundsätzlich weit auszulegen ist.³¹ Dies gilt auch nach dem IDW PS 980-Standard, der in der Anwendung auch auf solche Regeln erstreckt wird, die keinen bankaufsichtsrechtlichen Hintergrund haben (z. B. Arbeitsrecht). Der Überwachung der Compliance-Pflichten aus der MaRisk und dem sonstigen Gesetzesrecht dient die Compliance-Organisation, die seit der CRD IV-Richtlinie auch einen „Whistleblower-Prozess“ beinhalten muss.³² Wie diese Compliance-Funktion im Einzelnen auszugestalten ist, hängt von der Art des Instituts und der Natur der von ihm betriebenen Geschäfte ab.

Compliance Management bedeutet in diesem Zusammenhang nicht, die Aufgaben des Risikomanagements bzw. Risiko-Controllings zu duplizieren, sondern dafür zu sorgen, dass die jeweiligen Systeme im weitesten Sinne den gesetzlichen Anforderungen entsprechen. Ohne detaillierte Kenntnisse der Risiken und der Risikotragfähigkeit des Instituts lassen sich die Risikomanagementsysteme durch die Compliance-Funktion nicht bewerten. Deshalb geht der Trend – wie bereits unter III.1.b) erwähnt – zu integrierten Compliance- und Risikomanagementprozessen in Form des ICRM, die einen einheitlichen Risikomanagement- und Compliance-Rahmen schaffen.

nisationen zugeordneter Banken, bestimmter Eigenmittelbestandteile, Großkredite, Aufsichtsregelungen und Krisenmanagement.

30 Näher die Auslegungshilfe der BaFin vom 16.2.2018 zur InstitutsVergV und die FAQ (Entwurf vom 21.6.2023).

31 Siehe *Glawischnig-Quinke*, in: Szesny/Kuthe, Kapitalmarkt Compliance, S. 443 ff. zu den besonderen Organisationspflichten; enger *Braun*, in: Fischer/Schulte-Mattler, KWG CRR, § 25a Rn. 44 (keine Ausdehnung auf Vorschriften, die keinen Bezug zum Bank- und Finanzdienstleistungsrecht aufweisen). Siehe zur MaRisk-Compliance auch → *Renz/Frankenberger*, Kap. 20 Rn. 24 ff.

32 Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26.6.2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG.

- 31** Neben den klassischen Compliance-Themen Geldwäsche und Betrugsprävention erstreckt sich die MaRisk BA-Compliance auf sämtliche regulatorische Themen und dort vor allem auf die Risikomanagementfunktion, auf die Finanzfunktion (Treasury), auf die Personalfunktion und auf die Informationssicherheitsfunktion. Aufbauend auf den internen Systemen ist ein Compliance-Handbuch zu erstellen, das es jedem Mitarbeiter ermöglicht, innerhalb kurzer Zeit einen Überblick über die einzuhaltenden Anforderungen zu gewinnen.³³

(2) MaComp-Compliance

- 32** Für den Wertpapierbereich (also kundenseitig) sind nach § 80 Abs. 1 WpHG i. V. m. der MaComp (Mindestanforderungen an die Compliance-Funktion)³⁴ detaillierte Anforderungen zu erfüllen. Hierbei ist einerseits sicherzustellen, dass sämtliche Anforderungen des WpHG beachtet werden. Zudem müssen Interessenkonflikte erkannt und vermieden und im Übrigen dürfen Interessen der Kunden nicht beeinträchtigt werden. Hierzu gehört auch, dass Systeme vorhanden sind, die sicherstellen, dass Kunden über Risiken von Wertpapieren – soweit erforderlich – nach den gesetzlichen Bestimmungen aufgeklärt werden.
- 33** Die zu schaffende Compliance-Funktion muss nach der MaComp unabhängig, wirksam und dauerhaft sein. Das heißt, dass der Compliance-Funktion hinreichende Befugnisse eingeräumt werden müssen. Weil die Compliance-Funktion präventiv und prozessleitend tätig ist, müssen die Mitarbeiter über ein hohes Fachwissen in allen geschäftsrelevanten Bereichen verfügen. Zum Beispiel bedeutet das für einen Compliance-Beauftragten einer großen Bank, dass er Kenntnisse in allen Bereichen des WpHG-relevanten Wertpapiergeschäfts hat. Auch komplexe Finanzprodukte wie strukturierte Derivate muss er verstehen und deren Risiken einschätzen können.
- 34** Das „aufsichtsrechtliche“ und das „wertpapierhandelsrechtliche“ Compliance-Management-System muss wiederum auf übergeordneter Ebene zusammengeführt werden, weil sich die Risiken aus den verschiedenen Geschäftsbereichen möglicherweise gegenseitig beeinflussen. Regelmäßig wird ein „Chief Compliance Officer“ das auf Vorstandsebene tun.

2. Anforderungen an Unternehmen

a) Normativer Rahmen und Übertragbarkeit

- 35** Unternehmen als Kunden von Finanzdienstleistern werden bei der Nutzung von Finanzprodukten bereits durch die aufsichtsrechtlichen Anforderungen des Finanzbereichs geschützt (siehe oben → Rn. 15 ff.).³⁵ Ein solcher Schutz reicht

³³ Siehe *Braun*, in: Fischer/Schulte-Mattler, KWG CRR, § 25a Rn. 45.

³⁴ Oben → Fn. 15.

³⁵ Ein solcher Schutz ergibt sich vor allem aus den WpHG- und MaComp-Bestimmungen. Teilweise ergeben sich hieraus und aus dem allgemeinen Zivilrecht Schadenersatzansprüche bei Verletzung der Pflichten.

aber regelmäßig nicht aus, weil die von Unternehmen verwendeten Finanzprodukte nur teilweise unter die §§ 31 ff. WpHG fallen. Cash-Pooling-Systeme, verbundene Darlehen, ABS und teilweise auch Derivate werden zwar von einem Finanzinstitut „begleitet“, aber nicht als Wertpapier vertrieben oder nur im Rahmen eines sogenannten „Execution Only“-Geschäfts, das keine Beratungs- und Aufklärungspflichten auslöst.³⁶ Es besteht insofern eine Schutzlücke, wenn Unternehmen mit Finanz- und Kapitalmarktprodukten umgehen.

Ob sich deshalb für Unternehmen aus § 91 Abs. 2 AktG, § 43 Abs. 2 GmbHG **36** die Pflicht ergibt, Risikomanagement- und Compliance-Systeme zu installieren, die denjenigen von Finanzinstituten entsprechen, wird im juristischen Schrifttum noch immer kontrovers diskutiert.³⁷ Kern dieser Kontroverse ist die Frage, was der Gesetzgeber in § 91 Abs. 2 AktG unter der Formulierung „... ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“ versteht. Ältere Gerichtsentscheidungen, die sich mit der Problematik auseinandersetzen, beziehen sich auf nicht verallgemeinerungsfähige Sachverhalte.³⁸ Im Rahmen des Siemens-Neubürger-Urteils des LG München aus dem Jahr 2014 wurden Anforderungen an ein bestehendes Compliance-System thematisiert.³⁹ Die h.L. im juristischen Schrifttum geht immer noch davon aus, dass es sich bei dem einzurichtenden Überwachungssystem nicht notwendigerweise um ein Risikomanage- bzw. Compliance-System handeln muss, jedenfalls nicht um ein System, dass die branchenspezifischen Anforderungen aus dem Finanzsektor aufgreift.⁴⁰ Als Argument wird im Wesentlichen vorgebracht, dass der Wortlaut kein solches System fordere und die Art und Weise, wie bestandsgefährdende Risiken erkannt und ausgeschaltet werden, im Leitungsermessen des Vorstands liege.⁴¹ Ein Teil der Literatur spricht sich gleichwohl dafür aus, im Umgang mit Finanzrisiken Unternehmen die Pflicht aufzuerlegen, Vorgaben des § 25a KWG und damit der MaRisk BA „punktuell und selektiv“ heranzuziehen.⁴² Zudem ist zu beachten, dass der Gesetzgeber die Norm des § 91 AktG infolge des „Wirecard-Skandals“ im Jahr 2021 um einen Abs. 3 erweitert hat, wonach der Vorstand einer börsen-

36 Unter einem „Execution Only“-Geschäft versteht man ein beratungsfreies Geschäft im Kundenauftrag, durch das weder aufsichtsrechtliche noch allgemein zivilrechtliche Beratungspflichten des Dienstleisters ausgelöst werden. Für das Rechtsverhältnis zwischen Kunde und Discountbroker BGH, Urt. v. 19.3.2013, IX ZR 431/11, BGHZ 196, 370.

37 Siehe *Spindler*, in: MünchKomm-AktG, § 91 Rn. 77 ff. Grundsatz 5 S. 2 DCGK 2022 verlangt ausdrücklich die Einführung eines Compliance-Management-Systems.

38 OLG Celle, WM 2008, 1745 ff., legt sich nicht fest und das VG Frankfurt am Main, WM 2004, 2157 ff., („Bruderhilfe“) bezieht sich auf ein Versicherungsunternehmen, das ohnehin in den Anwendungsbereich der aufsichtsrechtlichen Vorschriften fällt (seinerzeit MaRisk VA).

39 LG München I, AG 2014, 332. Siehe hierzu → *Schulz*, Kap. 1 Rn. 39.

40 Siehe *Spindler*, in: MünchKomm-AktG, § 91, Rn. 84.

41 Unter Verweis auf die Gesetzesbegründung *Krieger/Sailer-Coceani*, in: Schmidt/Lutter, AktG, § 91 Rn. 14 m. w. N.

42 So z. B. KölnKomm-AktG/*Mertens/Cahn*, Bd. 2/1, § 91 Rn. 31.; i. E. wohl auch *Spindler-MünchKomm-AktG*, § 91 Rn. 78.

notierten Aktiengesellschaft ein im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames internes Kontrollsystem und Risikomanagementsystem einzuführen hat.⁴³

- 37 Betriebswirtschaftlich geprägte Autoren sprechen sich unter Praktikabilitätsgesichtspunkten beim Umgang mit Finanzrisiken überwiegend für eine konkrete Pflicht zum Risikomanagement aus und wenden die Grundsätze des § 25a KWG und der MaRisk BA direkt an.⁴⁴ Zwar kann eine solche Anwendung von bankbetrieblichen Regeln nicht grenzenlos erfolgen (siehe unten → Rn. 40 f.), doch erscheint das MaRisk BA-Instrumentarium am ehesten geeignet, verlässliche Standards für den Umgang mit Risiken aus dem Finanzbereich zu setzen. Zumindest werden hierdurch die Risikokategorien definiert und die gängigen Risikobewertungsprozesse eingeführt. Die Notwendigkeit hierfür hat sich in der Aufarbeitung der Finanzkrise der Jahre 2008 ff. gezeigt. Gerade im Umgang mit Finanzderivaten haben Unternehmen durch Marktpreisfluktuationen erhebliche Verluste erlitten, die nur teilweise auf den Vertragspartner (die Bank) abgewälzt werden konnten. Relevant werden diese Fragestellungen wiederum im Zuge der Marktstörungen, die durch die Corona-Pandemie und im Energiemarkt durch den Ukraine-Krieg eingetreten sind.⁴⁵ Es wird sich zeigen, ob die Verbesserung der Risikomanagementprozesse im Nachgang zur sogenannten Finanzkrise ausreichend sind, um auch exogene Schocks dieser Größenordnung auffangen zu können.
- 38 Unabhängig davon, ob die zu treffenden Maßnahmen bei der Nutzung von Finanzprodukten im Leitungsermessen des Vorstands liegen oder ob MaRisk BA-Regeln punktuell angewendet werden oder ob ein bankentypisches Risikomanagement insgesamt zu übernehmen ist, muss die Geschäftsleitung die Risiken der genutzten Finanzprodukte einschätzen und überwachen können. Neben den Folgen für das Unternehmen muss nämlich auch die eigene Haftung im Blick behalten werden. Zwar werden unternehmerische Entscheidungen und dementsprechend auch die Nutzung eines Finanzprodukts von der „Business Judgement Rule“ in § 93 Abs. 1 Satz 2 AktG (und entsprechend in § 43 Abs. 2 GmbHG) privilegiert, sodass Verluste nicht direkt zu einer Haftung des Geschäftsleiters führen müssen. Jedoch muss der Entscheider die verfügbaren Informationsquellen rechtlicher und tatsächlicher Natur ausschöpfen und auf dieser Basis eine abgewogene Entscheidung treffen.⁴⁶ Die Gesetzesbegründung zum UMAG,⁴⁷ durch das § 93 Abs. 1 Satz 2 AktG eingefügt worden ist, verweist darauf, dass die Informationen zwar nicht allumfassend sein können, aber innerhalb der betriebs-

43 Siehe hierzu → *Bartuschka*, Kap. 11 Rn. 40; → *Renz/Frankenberger*, Kap. 20 Rn. 70. Zur Erweiterung des § 91 Abs. 3 AktG vgl. *Roth*, NZG 2022, 53; *Fischer/Schuck*, NZG 2021, 534.

44 So z. B. *Preußner*, NZG 2008, 574, 575.

45 Instrukтив zu den Folgen einer Pandemie auf Vertragsverhältnisse *Weller/Lieberknecht/Habrich*, NJW 2020, 1017. Zu Pandemien und Risikomanagement ferner → *Romeike*, Kap. 9 Rn. 4 f.

46 So v. a. *Baums*, ZGR 2011, 218, 235 f.

47 Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts vom 22.9.2005, BGBl. I, S. 2802.

wirtschaftlichen Schwerpunkte unter Berücksichtigung anerkannter betriebswirtschaftlicher Verhaltensmaßstäbe bestimmt werden müssen.⁴⁸ Diejenigen betriebswirtschaftlichen Verhaltensmaßstäbe, die der Gesetzgeber im Blick hatte, umfassen im Umgang mit komplexen Finanzprodukten auch ein professionelles, produktbezogenes Risikomanagement.

Die Pflicht zur Compliance im Unternehmensbereich, die sich auch auf das Risikomanagement erstreckt, ist das Ergebnis der Organisationspflichten, die ihren Ursprung in der Legalitätspflicht haben.⁴⁹ **39**

b) Grenzen

Bei der Anwendung der MaRisk BA-Regeln im Unternehmensbereich sind solche auszulassen, die sich, wie zum Beispiel das Modul BTO (Kreditgeschäft), auf bankspezifische Risiken beziehen, die im Unternehmen nicht existieren. Andererseits müssen die übertragbaren Bestimmungen der MaRisk BA und ggf. der WpDVerOV durch solche Regeln ergänzt werden, die speziell für Unternehmen erforderlich sind. Zu denken ist in diesem Zusammenhang vor allem an interne Schulungs- und Risikoaufklärungspflichten, weil in Bezug auf Finanzprodukte regelmäßig weniger Know-how zur Verfügung steht als in Finanzinstituten. **40**

Zu bedenken ist auch, dass der Bezug zu bankaufsichtsrechtlichen Pflichten und deren Erfüllung alleine noch nicht ausreichen, um den Vorstand oder die Geschäftsführung über die Business Judgement Rule zu enthaften. Vielmehr ist in diesem Rahmen immer eine Einzelfallbetrachtung durchzuführen. **41**

IV. Ausgestaltung des Risikomanagement- und Compliance-Systems im Unternehmensbereich

1. Finanzproduktbezogenes Risikomanagement und Compliance – Überblick

Grundsätzlich müssen sich das finanzproduktbezogene Risikomanagement und auch die nachfolgende Compliance-Organisation in das Gesamtkonzept einfügen. Insofern müssen Schnittstellen definiert und Zuständigkeiten übertragen werden. Im folgenden Abschnitt wird die Betrachtung auf den Umgang mit Finanzprodukten beschränkt. Im Unternehmensbereich ist es wenig sinnvoll, verschiedene Risikomanagement- und Compliance-Systeme zu installieren, die dann auf höherer Ebene wieder zusammengeführt werden. Vielmehr sollte – so wie es der Bankpraxis heute schon entspricht – ein integriertes Risikomanagement und Compliance-System entwickelt werden, in das die verschiedenen geschäftsbezogenen Module integriert werden. Am Beispiel der oben (→ Rn. 40 f.) **42**

⁴⁸ Begr. RegE, BT-Drs. 15/5092, S. 12.

⁴⁹ Zur Legalitätspflicht im Rahmen von § 93 Abs. 1 AktG und ihren Grenzen: *Koch*, AktG, 17. Aufl. 2023, § 93 Rn. 11. Zur Compliance-Organisationspflicht ferner → *Schulz*, Kap. 1 Rn. 36 ff.

Teil 3 Besondere Aufgaben und Anwendungsfelder

erläuterten komplexen Finanzprodukte soll skizziert werden, welche Elemente ein solches ICRM-Modul für die jeweiligen Risikoarten enthalten muss. Im Überblick ergibt sich das folgende Modell:

Instrument	Wesentliche Risiken	ICRM
Cash Pooling und Payment Factory	Adressenausfall-/Kreditrisiko; operationelles/Rechtsrisiko	– Kreditrisiko-Tool („Treasury Portal“) – rechtliche Einzelfallprüfung und fortlaufende Prüfungen (ggf. unter Einbindung künstlicher Intelligenz) – Einweisung und fortlaufende Schulung von GF und V
Darlehen mit separater Zinssicherung	Marktrisiko, Adressenausfall-/Kreditrisiko; operationelles/Rechtsrisiko	– Kreditrisiko-Tool (Darlehenskomponente) – rechtliche Einzelfallprüfung und Monitoring der Covenants („Treasury Portal“) – Liquiditäts- und Marktrisiko-Tool (Zinssicherung) – ggf. Kreditrisiko-Tool (Zinssicherung) – erweiterte rechtliche Prüfung der Dokumentation (Zinssicherung)
ABS	Marktrisiko, Adressenausfall-/Kreditrisiko; Liquiditätsrisiko, operationelles/Rechtsrisiko	– erweiterte rechtliche Prüfung (wegen Komplexität und fremden Rechtsordnungen) – Kreditrisiko-Tool (Darlehens- und Anleihekomponenten; Liquiditätslinie Issuer) – rechtliches und wirtschaftliches Monitoring der Covenants („Treasury Portal“) – Liquiditäts- und Marktrisiko-Tool (Zinssicherung und weitere Derivate)
Strukturierte Schuldscheine, Anleihen, Kreditderivate	Marktrisiko, Adressenausfall-/Kreditrisiko; Liquiditätsrisiko, operationelles/Rechtsrisiko	– erweiterte rechtliche Prüfung (wegen Komplexität und häufig fremden Rechtsordnungen) – Kreditrisiko-Tool (Darlehens- und Anleihekomponenten; Kreditderivat) – rechtliches und wirtschaftliches Monitoring der Covenants („Treasury Portal“) – Liquiditäts- und Marktrisiko-Tool (Zinssicherung und weitere Derivate)
Derivate	Marktrisiko, Adressenausfall-/Kreditrisiko; operationelles/Rechtsrisiko	– Liquiditäts- und Marktrisiko-Tool – Kreditrisiko-Tool (Zinssicherung) – erweiterte rechtliche Prüfung der Dokumentation – fortlaufende rechtliche Prüfung der Dokumentationsstandards

2. Die Ausgestaltung der wichtigsten ICRM-Komponenten im Einzelnen

a) Rechtliche Einzelfallprüfung: Covenant-Tool

Bei Covenants handelt es sich in Darlehensverträgen um Pflichten des Darlehensnehmers. Häufig wird ein bestimmtes Reporting vereinbart, aber auch bonitätsbezogene und rechtliche bzw. organisatorische Verpflichtungen spielen eine Rolle. Neben diese allgemeinen Covenants treten in aller Regel sogenannte Financial Covenants, also finanzielle Kennzahlen oder „Kapitalstrukturauflagen“, die vom Darlehensnehmer eingehalten werden müssen.⁵⁰ Sie dienen der fortlaufenden Überprüfung der Rahmendaten, die für die Kreditentscheidung erheblich waren.⁵¹ Ein Verstoß gegen diese Covenants führt regelmäßig zu einem vertraglichen Kündigungsrecht des Darlehensgebers und begründet dann eine erhebliche Insolvenzgefahr für den Darlehensnehmer. Insofern ist es wichtig, die Einhaltung der Financial Covenants im Rahmen des ICRM fortlaufend zu überwachen.

Üblich sind Eigenkapitalklauseln, die verlangen, dass das Eigenkapital des Darlehensnehmers nicht unter eine bestimmte Quote absinkt. Weiterhin kommen verschuldungsabhängige Kennzahlen zum Einsatz, welche die Verschuldung des Darlehensnehmers ins Verhältnis zu seinem Eigenkapital setzen. Es wird zudem regelmäßig verlangt, dass der Darlehensnehmer seine Netto-Finanzverbindlichkeiten ins Verhältnis zum EBITDA setzt und damit sicherstellt, dass die Verbindlichkeiten in einem angemessenen Zeitraum zurückgeführt werden können. Wichtig ist in diesem Zusammenhang die Feststellung des Schuldendienstdeckungsgrads, der bestimmt, ob die Aufwendungen für die eingegangene Verschuldung überhaupt getragen werden können. Schließlich muss sich der Darlehensnehmer verpflichten, eine bestimmte Liquidität vorzuhalten, um über die Laufzeit des Darlehens die Illiquidität zu vermeiden.⁵²

Das Covenant Tool kann eine simple Excel-Tabelle sein, die alle eingegangenen Finanzierungen enthält und die Financial Covenants beinhaltet. Es muss dann in regelmäßigen Abständen „händisch“ überprüft werden, ob die meist unterschiedlichen Covenants eingehalten worden sind. Besser ist es, eine Verknüpfung mit dem allgemeinen Reporting des Unternehmens herzustellen, sodass jedenfalls an den jeweiligen Stichtagen (zumeist zum Ende eines jeden Quartals, teilweise halbjährlich oder jährlich) die notwendigen Kennzahlen von der Finanzabteilung im richtigen Format geliefert werden.

50 Näher von Bodungen, in: Kessler, Unternehmensfinanzierung Mittelstand, S. 165.

51 von Bodungen, in: Kessler, Unternehmensfinanzierung Mittelstand, S. 165.

52 Zu den Financial Covenants näher von Bodungen, in: Kessler, Unternehmensfinanzierung Mittelstand, S. 167 f.

b) Kreditrisiko-Tool

- 46 Das Kreditrisiko-Tool dient der Überwachung des jeweiligen Gegenparteirisikos und muss vor allem dann das Gegenparteirisiko im Blick haben, wenn das Unternehmen selbst Gläubiger der Forderung ist oder werden kann. Normalerweise ist das bei einfachen Finanzierungen nicht der Fall, weil das Unternehmen regelmäßig unter einem Darlehensvertrag Zins und Tilgung schulden wird. Ist zur Zins-sicherung aber ein Derivat abgeschlossen worden oder ist das Unternehmen Teil einer komplexeren Struktur (wie zum Beispiel bei ABS), muss das Gegenparteirisiko beachtet werden. Grundsätzlich kann das individuell erfolgen, indem die Gegenpartei bereits vertraglich verpflichtet wird, selbst bestimmte Finanzinformationen zu liefern. Häufig wird die Gegenpartei jedoch ein Finanzinstitut sein, das einem externen Rating unterliegt. Dann wird das Rating im Rahmen des Kreditrisiko-Tools mit zu überwachen sein. Im Bankbereich spielt das Kredit- oder Adressenausfallrisiko bei der Risikogewichtung von Bilanzpositionen zur Bestimmung von Eigenmittelanforderungen eine wesentliche Rolle, sodass die Bewertungsstandards entsprechend ausgefeilt sind. Anders als im Unternehmensbereich, der unreguliert ist, bestehen im Bankbereich allerdings Vorgaben, welche Positionen als besonders risikoarm oder besonders riskant anzusehen sind;⁵³ diese Vorgaben lassen sich im Unternehmensbereich nicht anwenden. Allerdings wird auch im Bankbereich darüber hinaus und unter bestimmten Bedingungen auf Ratings anerkannter Agenturen (sogenannte ECAI⁵⁴) abgestellt werden. Wie das zu geschehen hat, richtet sich danach, ob die kurz- oder langfristige Bonität der Gegenpartei zu beurteilen ist. Die Einteilung in die gängigen Ratingklassen AAA (geringstes Ausfallrisiko) bis CCC+ (hohes Ausfallrisiko) kann grundsätzlich im Unternehmen übernommen werden. Einzig der „Cut off“, das heißt diejenige Schwelle, unter der eine Gegenpartei nicht mehr akzeptabel ist, muss individuell festgelegt werden und sich an der Risikoneigung und Risikotragfähigkeit des Unternehmens orientieren.
- 47 Handelt es sich bei der Gegenpartei um eine Zweckgesellschaft (SPV) oder ein sonstiges, nicht geratetes Unternehmen, werden Aussagen nur schwer schematisiert zu treffen sein und müssen durch die individuelle Analyse des Kreditrisikos ersetzt und durch strukturelle Maßnahmen flankiert werden. Eine Zweckgesellschaft, die zum Beispiel im Rahmen einer ABS-Transaktion Vertragspartner wird, muss so strukturiert sein, dass sie neben den Verbindlichkeiten im Rahmen der eingegangenen Transaktion keine weiteren zu tragen hat und entsprechend kein Risiko besteht, dass externe Einflussfaktoren zu ihrem Zusammenbruch und damit zum Ausfall des Unternehmens führen („Insolvency Remoteness“). Diese strukturellen Themen lassen sich im Rahmen des Kreditrisiko-Tools nur durch die Hinterlegung einer regelmäßig von Anwälten und Wirtschaftsprüfern zu aktualisierenden „Legal Opinion“ erfassen.

53 Siehe hierzu insbesondere Art. 114 ff. CRR.

54 ECAI sind „External Credit Assessment Institutions“. Zum Beispiel erfüllen Fitch, Standard & Poors und Moodys die Kriterien und sind als ECAI zugelassen.

c) Marktrisiko-Tool

Marktrisiko wohnt allen Finanzprodukten inne, die Marktpreisen unterliegen. Hierbei kann es sich um die Tranche eines Darlehens handeln, das der Darlehensgeber am Markt veräußert, ohne dass dies vom Darlehensnehmer gewünscht ist. Es kann sich um Derivate zur Zinssicherung handeln, die einen eigenen Marktwert haben, der durchaus auch – je nach Zinsentwicklung – negativ sein kann. Eigene Schuldscheine, Anleihen und Equity-Instrumente haben Marktpreise, die das Unternehmen als Schuldner nur mittelbar betreffen, aber unmittelbare Auswirkungen auf die Bonität und den Ruf des Unternehmens haben (z. B. wenn eine vom Unternehmen begebene Anleihe weit unter dem Nominalwert notiert und damit Geschäftspartner auf eine Schieflage aufmerksam werden).

48

Die Bestimmung von Marktrisiko ist nicht trivial. Es geht letztlich darum vorherzusagen, wie sich ein Marktpreis in der Zukunft entwickelt und insbesondere, mit welcher Wahrscheinlichkeit Verluste eintreten, die unter Risikomanagementgesichtspunkten für das Unternehmen relevant sind. Betrachtet man zum Beispiel das Risiko eines Zins-Swaps, so hängt der Marktwert des Swaps eng mit dem Basiswert und damit mit der Zinsentwicklung zusammen. Tauscht das Unternehmen einen variablen Zahlungsstrom in einen fixen Zahlungsstrom, zahlt es eine Prämie dafür, dass der Kontrahent das Zinsrisiko übernimmt. Die Höhe der Prämie hängt davon ab, wie der Markt die Zinsentwicklung über die Laufzeit einschätzt. Wird der Swap während der Laufzeit aufgelöst, etwa weil der Darlehensnehmer das Darlehen anderweitig refinanzieren möchte (oder muss), ergibt sich ein positiver Marktwert, wenn das Zinsniveau weiter angestiegen ist, als der vom Darlehensnehmer „gekaufte“ Zinssatz. Ein negativer Marktwert ergibt sich, wenn das Zinsniveau unter den „gekauften“ Zinssatz abgesunken ist. Dann ist der Swap, den die Bank als Kontrahent am Markt „refinanziert“ hat, wertlos und es droht die Pflicht, eine Ausgleichszahlung zu leisten, welche den Kontrahenten in die Lage versetzt, seine Verpflichtungen gegenüber seiner Gegenpartei zu erfüllen. Grundsätzlich besteht dieser Ausgleichsanspruch unbegrenzt.

49

Die Regeln der CRR, die teilweise auch im Unternehmensbereich angewendet werden müssen, sind produkt- und risikobezogen ausgestaltet. Im Rahmen der Marktpreisrisiken wird zwischen Allgemeinem Zinsrisiko, Spread-Risiko, Währungsrisiko, Rohwarenrisiko, Aktienrisiko, Ausfallrisiko und Optionsrisiko unterschieden.⁵⁵ Risikopositionen sind nach Marktpreis zu bestimmen (Art. 94 Abs. 2 CRR). Insofern findet sich durchaus eine bankaufsichtsrechtliche Kategorie für alle von Unternehmen verwendeten Finanz- und Kapitalmarktprodukte. Die Bestimmung des zukünftigen Marktwerts eines Kapitalmarktinstruments und die damit verbundene Risikoeinschätzung ist jedoch keine exakte Wissen-

50

⁵⁵ Einen guten Überblick über die Risikopositionen geben die Offenlegungsvorschriften der CRR (Art. 431–435).

schaft, weil die Zukunft unbekannt ist. Insofern stützen sich die Finanzmathematik und damit auch die Regulierung auf Verfahren, die auf vergangenen Daten beruhen. Ein Beispiel hierfür ist das Value-at-Risk-Verfahren (VaR), das im Bankbereich im Rahmen der Marktrisikomodelle angewendet wird.⁵⁶ Der Value-at-Risk beschreibt denjenigen Verlust, der innerhalb einer bestimmten Zeitspanne nur mit einer bestimmten Wahrscheinlichkeit überschritten wird.⁵⁷ Grundsätzlich obliegt es dem Risikomanagement im Unternehmen, Zielwerte festzulegen und insbesondere zu bestimmen, welcher VaR unter Risikotragfähigkeitsgesichtspunkten noch akzeptabel ist. Dieser Wert muss dann mit gängigen, software-basierten Berechnungs- und Überwachungsverfahren eingehalten werden.

d) Liquiditätsrisiko-Tool

- 51 Grundsätzlich muss ein Unternehmen sicherstellen, dass es „liquide“ bleibt, um eine Insolvenz zu vermeiden. Um diese Liquidität geht es beim Umgang mit Finanz- und Kapitalmarktprodukten jedoch nicht. Finanzinstrumente, die an einem Markt gehandelt werden, weisen ein Liquiditätsrisiko auf. Es handelt sich dabei im Gegensatz zum Risiko der Illiquidität des Unternehmens um das Risiko, dass ein Handel in einem bestimmten Wertpapier oder Anlagegegenstand nicht zustande kommt, weil ein Verkäufer oder Käufer fehlt. Ist das Unternehmen in einer solchen Situation eines wenig liquiden Marktes gezwungen, ein Wertpapier zu verkaufen, kann es dies, wenn überhaupt, nur zu einem schlechten Preis tun und wird Verluste erleiden. Grundsätzlich muss es deshalb die Veräußerbarkeit gehaltener Finanz- und Kapitalmarktprodukte sicherstellen oder für „illiquide“ Vermögenswerte entsprechend Rückstellungen bilden, wenn sich deren Marktwert verringert.
- 52 Ein Liquiditätsrisiko-Tool sollte täglich das Handelsvolumen in den relevanten Produkten genauso im Auge behalten, wie die Volatilität des Marktes und des Produkts.

3. Delegation des Risikomanagements und Compliance

- 53 Die Wahrscheinlichkeit ist hoch, dass ein komplexes Finanzprodukt von einem Finanzinstitut vertrieben worden ist. In den meisten Fällen haben Unternehmen und Finanzinstitut dann zumindest konkludent einen Beratungsvertrag⁵⁸ geschlossen, sodass zum Zeitpunkt des Vertragsschlusses Informationen zu Funk-

56 Siehe *Neus*, in: Luz/Neus/Schaber/Schneider/Wagner/Weber, KWG mit CRR, Einführung Rn. 43.

57 Siehe *Neus*, in: Luz/Neus/Schaber/Schneider/Wagner/Weber, KWG mit CRR, Einführung Rn. 43.

58 Die Obergerichte nehmen in ständiger Rechtsprechung an, dass die Bank Rechtsbindungswillen zum Abschluss eines Beratungsvertrages hat und ein solcher zustande kommt, wenn sie an den Kunden herantritt und dieser das Gespräch aufnimmt, vgl. nur BGH, Urt. v. 22.3.2011 – XI ZR 33/10 BGHZ 189, 13 („Zinswette“); auch die Vorinstanz: OLG Frankfurt

tionsweise und Risiko des Produkts übermittelt worden sind, und zwar in der Form eines Beratungsgesprächs und/oder eines Prospekts. Der Beratungsvertrag wirkt aber nicht in die Zukunft, sodass grundsätzlich keine Pflicht des beratenden Instituts besteht, nach Vertragsschluss die Risiken für den Vertragspartner zu überwachen. Ganz im Gegenteil, die Bank hätte sogar, wenn sie Vertragspartner bliebe, einen Interessenkonflikt, wenn sie die gegenläufige Position hält. Unabhängig von der vertraglichen Gestaltung erwog die EU-Kommission jedoch im Rahmen der MiFID-Reform,⁵⁹ die Wohlverhaltensregeln für Finanzinstitute dergestalt zu ändern, dass auch während der Laufzeit zum Beispiel eines Derivatevertrages Hinweis- und Warnpflichten gegenüber einem strukturell unterlegenen Marktteilnehmer bestünden.⁶⁰ Dieser Ansatz ist jedoch bei der weiteren Umsetzung der Reform fallengelassen worden.

Ohne gesetzliche Vorgabe müssten Finanzinstitut und Unternehmen ein regelmäßiges, risikoorientiertes Reporting vereinbaren. Ein solcher Geschäftsbesorgungsvertrag würde dazu führen, dass ein Dritter, der über umfangreiches institutionelles Know-how im Umgang mit den relevanten Produkten und Risiken verfügt, die Pflichten des Vorstands nach § 91 Abs. 2 AktG übernehmen würde. Grundsätzlich würde eine solche Dienstleistung wohl wegen des inhärenten Interessenkonfliktes von einer Abteilung des Vertragspartners durchgeführt werden müssen, die von der Handelsabteilung organisatorisch getrennt ist (Chinese Walls). Ob der Interessenkonflikt gänzlich behebbar ist, wird von den Umständen des Einzelfalles abhängen. Auf der Bankenseite jedenfalls wäre die Auslagerung der Risikoüberwachungsfunktion für laufende Finanzprodukte nach § 25a KWG i. V. m. AT 9 MaRisk BA unter den dort festgeschriebenen Voraussetzungen (insbesondere Nr. 6) ausdrücklich zulässig. **54**

Der Vorstand kann im Rahmen von § 91 Abs. 2 AktG Pflichten grundsätzlich intern und auch extern delegieren, wobei ein bestimmter Kernbestand bei ihm bestehen bleibt, der nicht delegierbar ist.⁶¹ Folgt man der hier vertretenen Auffassung, dass im Rahmen des § 91 Abs. 2 AktG für das Risikomanagement von komplexen Finanzprodukten soweit wie möglich die Regeln der MaRisk BA bzw. der CRR heranzuziehen sind, dann wird man die schriftliche Fixierung des **55**

a. M., ZIP 2010, 921 unter Verweis auf BGH, Urt. v. 4.3.1987 – IVa. ZR 122/85, BGHZ 100, 117 ff.

59 Die MiFID-Richtlinie (Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15.5.2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU – Markets in Financial Instruments Directive – MiFID II) ist am 12.6.2014 im Amtsblatt der EU veröffentlicht worden. Das Konsultationspapier aus dem Jahr 2011 sah eine solche Hinweis- und Warnpflichtpflicht als „Idee“ vor.

60 Die Frage, ob ein Marktteilnehmer, auch wenn er geeignete Gegenpartei im Sinne von § 31a WpHG ist, strukturell unterlegen ist („strukturelles Ungleichgewicht“), bestimmt sich danach, ob seine institutionelle, durch das Aufsichtsrecht vermittelte, Kompetenz hinter derjenigen seines Vertragspartners zurückbleibt – näher *Kessler*, Das Strukturrisiko von Finanzderivaten, S. 277 ff. m. w. N.

61 *Baums*, ZGR 2011, 219, 268, beschreibt diesen Kernbestand als „Residualpflichten“.

Risikomanagementkonzepts und der Anforderungen an den Dienstleister (regulierte Bank, hohe institutionelle Kompetenz) zwar als sogenannte Residualpflicht des Vorstands begreifen, aber gegen eine vertragliche Auslagerung der Ausführung unter den Voraussetzungen des AT 9 MaRisk BA keine Einwände haben. In Fällen, in denen die Einrichtung eines bankenüblichen Risikomanagementsystems für Unternehmen zu aufwendig ist, empfiehlt es sich, auf der Grundlage der Informationen, die im Rahmen der Beratung übermittelt worden sind (Stichwort: Informationssymmetrie), ein Auslagerungskonzept schriftlich zu fixieren. Im nächsten Schritt muss mit dem Vertragspartner oder einer anderen Bank auf dieser Grundlage ein unabhängiges Risiko-Controlling mit entsprechenden Hinweis-, Warn- und Berichtspflichten vereinbart werden, die wiederum die oben unter 1. erläuterten Risiko-Tools umfassen.

- 56 Den Interessenkonflikt, der typischerweise entsteht, wenn der Vertriebspartner Aufgaben des Risikomanagements übernimmt, lässt sich durch die Wahl eines bankenunabhängigen Dienstleisters vermeiden. Dieser kann im Rahmen des ICRM und eines Auslagerungskonzepts häufig sogar direkter eingebunden werden, als ein Finanzinstitut, dessen Kerngeschäft die operative software-basierte Begleitung seiner Kunden häufig nicht ist. Grundsätzlich gelten für einen solchen externen Dienstleister dieselben Grundsätze wie für eine Auslagerung an ein Finanzinstitut.
- 57 Die Compliance-Funktion wird, wie im Bankbereich auch, im Rahmen des ICRM-Ansatzes die aufgesetzten Prozesse plausibilisieren und die Einhaltung der Anforderungen an das Risikomanagement überwachen.⁶²

V. Haftungsfragen

- 58 Grundsätzlich zieht die Verletzung der Rechtspflicht zum Risikomanagement und auch zur Compliance eine Haftung nach § 93 Abs. 2 AktG bzw. § 43 Abs. 2 GmbHG nach sich. Zur Bestimmung der bereichsspezifischen Anforderungen müssen jedoch die verschiedenen Komponenten des ICRM wieder getrennt betrachtet werden. Im Bereich des Risikomanagements werden Pflichten verletzt, wenn der Vorstand entweder kein Risikomanagementsystem installiert hat, obwohl es erforderlich war, oder bestandsgefährdende Risiken durch die Verwendung von Finanz- und Kapitalmarktprodukten in Fällen nicht erkannt worden sind, in denen kein Risikomanagementsystem erforderlich war. Im Bereich der Compliance geht es um Verstöße gegen die Legalitätspflicht, die zu einem Schaden im Unternehmen führen.

1. Verstoß gegen die Pflicht zum Risikomanagement

- 59 Es ist im juristischen Schrifttum zunächst anerkannt, dass die Umstände des Einzelfalles zu betrachten sind. Weder ergibt sich aus der Einrichtung eines „allum-

62 Näher zu den Schnittmengen von Risikomanagement und Compliance *Schulz/Galster*, in: Bürkle/Hauschka, *Der Compliance Officer*, 1. Aufl. 2015, § 4 Rn. 64.

fassenden“ Systems (sofern das überhaupt möglich ist) eine Enthftung des Vorstands noch führt das Fehlen eines solchen Systems in jedem Fall zur Haftung.⁶³ Es gilt insofern die Privilegierung des § 93 Abs. 1 Satz 2 AktG (die sog. „Business Judgement Rule“ – BJR). Hiernach haftet ein Vorstand (oder auch ein GmbH-Geschäftsführer) nicht, wenn er bei einer unternehmerischen Entscheidung richtige Annahmen getroffen hat. „Unternehmerisch“ ist eine Entscheidung immer dann, wenn der Vorstand im Rahmen seines Leitungsermessens unter Unsicherheit, entscheidet.⁶⁴ Das wird typischerweise bei der Nutzung von Finanz- und Kapitalmarktprodukten genauso der Fall sein, wie bei der Frage, ob ein banktypisches Risikomanagementsystem einzurichten ist oder nicht (jedenfalls, wenn man der h. L. in der Literatur folgt – siehe oben → Rn. 36 f.). Die Annahmen, die der Vorstand trifft, müssen auf der Basis angemessener Information getroffen werden. Das ist der Fall, wenn der Vorstand die für eine sachgerechte Entscheidung nötigen Informationen einholt, wobei die routinemäßige Anforderung von Sachverständigengutachten nicht erforderlich ist.⁶⁵ Bei der Nutzung von Finanz- und Kapitalmarktprodukten treten regelmäßig zwei Grundkonstellationen auf. Es ist einerseits denkbar, dass der Vorstand es verabsäumt hat, ein produktspezifisches Risikomanagementsystem einzurichten und dadurch im weiteren Verlauf nicht genügend Informationen hatte, um Verluste zu vermeiden. Andererseits ist auch denkbar, dass der Vorstand auf der Grundlage angemessener Information, die auf einem funktionalen Risikomanagementsystem beruht, eine Entscheidung getroffen hat, die zu Verlusten geführt hat. Im letzteren Fall ist er über die BJR privilegiert und, vorausgesetzt, die Entscheidung war zum Wohle der Gesellschaft gedacht, haftungsfrei. Begibt er sich allerdings der Einschätzungsmöglichkeit, weil er die Systeme nicht installiert, die erforderlich gewesen wären, um ermessensfehlerfreie Entscheidungen zu treffen, haftet er, auch wenn er zum Beispiel durch den Verzicht auf ein Risikomanagementsystem Kosten zum Wohle der Gesellschaft sparen wollte.

In diesem Zusammenhang gilt, dass die Maßnahmen des Risikomanagements der Gefährlichkeit der verwendeten Produkte entsprechen müssen. Der Vorstand braucht beim Erwerb der Aktien eines DAX 30-Unternehmens wohl nicht mehr zu tun, als täglich den Kurs und die im Rahmen der Kapitalmarktpublizität veröffentlichten Emittenteninformationen zur Kenntnis zu nehmen. Anders ist die Lage aber beim Abschluss eines Vertragswerks für eine ABS-Transaktion mit einer Reihe von Vertragspartnern und verschiedenen Kapitalmarktinstrumenten, deren Risiken das Unternehmen direkt ausgesetzt ist. In diesem Zusammenhang gilt es zu beachten, dass Stimmen im juristischen Schrifttum in Folge der Finanzkrise davon ausgegangen sind, es gäbe finanzmarktbezogene Risiken, die grundsätzlich eine Privilegierung nach der BJR ausschließen, etwa weil sie

60

63 Krieger/Sailer-Coceani, in: Schmidt/Lutter, AktG, § 91 Rn. 14 m. w. N. Zu den positiven Effekten effektiver Compliance-Maßnahmen siehe → Schulz, Kap. 1.

64 Spindler, in: MünchKomm-AktG, § 93 Rn. 48.

65 Spindler, in: MünchKomm-AktG, § 93 Rn. 57.

„übergroß“ seien.⁶⁶ Dieser Auffassung ist entgegenzutreten. Wenn der Vorstand die eingegangenen Risiken versteht und sachgerecht kontrollieren kann, haftet er nicht. Das heißt allerdings nicht, dass der Vorstand sich allein auf finanzwirtschaftliche Informationen, wie z. B. Ratings, verlassen darf, ohne diese kritisch zu würdigen.⁶⁷

2. Verstoß gegen die Pflicht zur Compliance

- 61** Die Haftung für Compliance-Verstöße – die auch an § 93 Abs. 1 Satz 2 AktG zu messen sind – ist mit dem Siemens-Neubürger-Urteil des LG München⁶⁸ erheblich verschärft worden. Gestützt hat das Gericht die Entscheidung auf die Legalitätspflicht des Vorstands (es ging um Schmiergelder) und im Leitsatz festgestellt, dass eine Pflicht zur Einrichtung einer auf Schadensprävention und Risikokontrolle angelegten Compliance-Organisation besteht, wenn eine entsprechende Gefährdungslage vorliegt.⁶⁹
- 62** Ob für die Nutzung von Finanz- und Kapitalmarktprodukten hieran angeknüpft werden kann, ist allerdings fraglich. Verabsäumt der Vorstand die Einrichtung eines Risikomanagementsystems, obwohl er nach § 91 Abs. 2 AktG dazu verpflichtet ist, verletzt er eine Organisationspflicht, die nach innen gerichtet ist. Ein Verstoß gegen die Legalitätspflicht setzt aber voraus, dass nicht nur ein Verstoß gegen innen-, sondern auch gegen nach außengerichtete Pflichten vorliegt.⁷⁰ Das wäre bei der Nutzung von Finanzprodukten z. B. der Fall, wenn ein regulierter Marktteilnehmer gegen Bank- oder Kapitalmarktaufsichtsrecht verstoßen würde und es kein Compliance-System gäbe, das einen solchen Verstoß hätte verhindern können. Es ist insofern anzunehmen, dass Fehler im ICRM oder das Fehlen eines Compliance-Elements im Unternehmensbereich jedoch nicht zum Wegfall der Privilegierungen durch die BJR führen würden.

3. Einsatz von Künstlicher Intelligenz

- 63** Neben automatisierten Lösungen im Treasury-Bereich kommen verstärkt KI-Lösungen zum Einsatz, welche auf der Basis bestimmter Regeln und Algorithmen selbstständig Entscheidungen treffen. Nach einer Ausarbeitung der Wirtschaftsprüfungsgesellschaft KPMG finden sich diese Lösungen derzeit in den Bereichen Cash Management, Betrugsprävention und im Wertpapierhandel.⁷¹ Der Einsatz von künstlicher Intelligenz ist aber auch darüber hinaus denkbar, z. B. ließe sich das gesamte Cash-Pooling perspektivisch unter Einsatz von

66 Z. B. Lutter, ZIP 2007, 841, 845.

67 Spindler, in: MünchKomm-AktG, § 93 Rn. 60 m. w. N.

68 LG München I, AG 2014, 332. Siehe hierzu → Schulz, Kap. 1 Rn. 39.

69 LG München I, AG 2014, 332.

70 Zur Differenzierung und den haftungsrechtlichen Folgen siehe Nietsch, ZGR 2015, 631, 651 f.

71 KPMG Corporate Treasury News, Ausgabe 136, September 2023, <https://kpmg.com/de/home/themen/2023/09/treasury-automatisierung-ki.html> (zuletzt abgerufen am 7.2.2024).

künstlicher Intelligenz genauso automatisieren wie die Marktrisikooanalyse von Derivaten und anderen Finanzprodukten. Die Pflichten des Vorstands zur Überwachung der spezifischen Risiken der verwendeten Finanzprodukte erstrecken sich naturgemäß auch auf Entscheidungen, welche von autonomen Systemen eigenständig getroffen werden, sei es im Rahmen der Analyse von Daten oder des Eingehens von Handelsgeschäften. Das ICRM muss so strukturiert sein, dass der Vorstand selbst die Kontrolle über seine Funktionsweise (sein datenbasiertes Modell) behält. Umgekehrt wird ein Risikomanagement-Tool, das unter Einbindung von künstlicher Intelligenz eine effizientere Überwachung von Risikopositionen ermöglicht, die haftungsrechtliche Situation von Vorständen verbessern, wenn es durch die Analyse größerer Datenmengen präzisere Entscheidungen ermöglicht.

VI. Fazit

Die Nutzung von Finanz- und Kapitalmarktprodukten im Unternehmen muss sowohl durch ein Risikomanagement- wie auch durch ein Compliance-System unterstützt werden. Es muss im Unternehmen abgewogen werden, ob unabhängige Systeme oder ein einheitliches ICRM installiert werden. Unabhängig von der organisatorischen Ausgestaltung variieren die Anforderungen je nach genutztem Produkt, wobei die Risiken komplexer Produkte besonders „gemanagt“ und überwacht werden müssen. Neben Marktpreisrisiken stehen insbesondere Rechtsrisiken, die bei vorwiegend angelsächsisch geprägter Dokumentation von Finanz- und Kapitalmarktprodukten ein eigenständiges Risikomanagement erfordern. Aber auch im Bereich der banküblichen Risiken sind entsprechende „Tools“ in das jeweilige System zu integrieren. Hierbei muss sich das Unternehmen an den „Best Practice“-Vorgaben der MaRisk BA, der CRR und des WpHG bzw. der MaComp orientieren, wobei ein externer Dienstleister im Rahmen eines Auslagerungsvorgangs beauftragt werden kann, den Vorstand zu unterstützen. Der Einsatz künstlicher Intelligenz wirkt nicht per se haftungsverschärfend, sondern kann perspektivisch sogar helfen, die Risiken im Treasury-Bereich effektiv zu kontrollieren und damit die haftungsrechtliche Situation zu verbessern. Der Vorstand ist – unabhängig vom eingesetzten Tool – im Regelfall durch die BJR privilegiert und haftet nur, wenn entweder die Systeme keine ausreichende Informationslage schaffen oder wenn Systeme gar nicht existieren und der Vorstand deshalb nur ermessensfehlerhaft entscheiden kann. Die verschärfte Haftung nach der Neubürger-Entscheidung trifft den Vorstand bei der Verletzung seiner Organisationspflichten nicht, weil kein Verstoß gegen das Legalitätsprinzip „im Außenverhältnis“ stattfindet.

64

22. Kapitel

Der Geldwäschebeauftragte – Stellung und Aufgaben

I. Der Geldwäschebeauftragte

Viele Unternehmen innerhalb und außerhalb des Finanzsektors haben qua Gesetz einen Geldwäschebeauftragten und einen Stellvertreter im Rahmen ihrer Sicherungsmaßnahmen gegen Geldwäsche zu bestellen. Vom „üblichen“ Compliance Officer unterscheidet er sich in mehrerlei Hinsicht: So sind Rolle, Aufgaben, Rechte, Verantwortung und Haftung gesetzlich vorgeschrieben und teilweise nicht von innerbetrieblicher Aufbau- und Ablauforganisation oder gar individueller Delegation abhängig. Der Geldwäschebeauftragte agiert nicht ausschließlich im Unternehmens-, sondern teils in hoheitlichem Interesse.¹ Hinsichtlich vieler Aspekte seines Handelns ist seine Rolle und Funktion deshalb eher vergleichbar mit der eines Datenschutzbeauftragten.

Der Geldwäschebeauftragte² ist dennoch – mangels öffentlichem Beleihungsakt – kein öffentlich Beliehener, sondern agiert ausschließlich privatrechtlich, wenn auch im öffentlichen Interesse. Seine Rechte und Stellung im Unternehmen, Befugnisse und Schutzrechte sind weitgehend gesetzlich geregelt und in einer untergesetzlichen Verwaltungspraxis detailliert ausgestaltet.

Innerhalb der Finanzindustrie haben sich hierzu jahrzehntelang Industriestandards herausgebildet, teils induziert durch die Branchenverbände (in der Finanzindustrie namentlich das ZKA (heute DK)),³ teils durch die Verwaltungspraxis der Aufsichtsbehörden, namentlich der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)⁴ sowie – vor allem – deren Vorgängerbehörde Bundesaufsichtsamt für das Kreditwesen (BAKred)⁵ und der entsprechenden europäischen Behörden und politischen Instanzen.⁶

Wie zu zeigen sein wird, war der „Geldwäschebeauftragte“ in seiner Ausprägung über Jahre eine reine Kreation der Verwaltungsbehörden, zu der über lange

1 Vgl. näher *Kaetzler*, in: Zentes/Glaab, GwG, § 7 Rn. 26 ff. mit weiteren Ausführungen. Zu Rolle und Aufgaben des Compliance Officers vgl. → *Rau*, Kap. 3; → *Schulz*, Kap. 1 Rn. 77 m. w. N.

2 Das in diesem Aufsatz verwendete Genus soll nicht diskriminierend wirken. Insbesondere in der Kreditwirtschaft ist vielmehr zu beobachten, dass der Frauenanteil unter den Geldwäschebeauftragten stetig ansteigt.

3 Vgl. z. B. die Auslegungs- und Anwendungshinweise der DK vom 1.2.2014, Ziff. 82 ff.

4 Vgl. BaFin, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz vom Oktober 2021, Ziff. 3.2.

5 BAKred Rundschreiben Nr. 1/1998 vom 30.12.1997 (*Kleinhans/Reischauer*, KWG, Ziff. 948) und die Verlautbarung vom 30.3.1998, Z-5 E 100 Nr. 35 (leider nicht mehr öffentlich verfügbar).

6 Ein Überblick über die weiteren normsetzenden Organe der Exekutive und der Legislative findet sich bei *Wende*, in: Zentes/Glaab, GwG, Geschichte der Geldwäschebekämpfung, Rn. 4 ff.

Jahre hinreichende gesetzliche Eingriffsgrundlagen fehlten. Dies änderte sich für die Kreditwirtschaft und weitere Unternehmen der Finanzindustrie i. w. S. erst 2011. Mit den Änderungen des GwG im Jahr 2017 wurden schließlich weitere Verpflichtete außerhalb des Finanzsektors in den Pflichtenkreis einbezogen und mussten einen Geldwäschebeauftragten bestellen. Außerhalb des Finanzsektors existieren seitdem zwar rudimentäre eigene Verwaltungspraxen zur Notwendigkeit, wann und unter welchen Umständen ein Geldwäschebeauftragter bestellt werden muss und wann nicht. Zur näheren Ausgestaltung von dessen Rolle – insbesondere in den finanzfernen Branchen und Wirtschaftssektoren (etwa im Handel und bei Immobilienmaklern) – bestehen jedoch nur höchst allgemeine Vorgaben oder Rechtsanwendungstraditionen zur eigentlichen Funktion und Rolle des Geldwäschebeauftragten. Das mit der Umsetzung der 2. EU-Geldwäscherichtlinie angestrebte „level playing field“ zwischen den Wirtschaftssektoren mit dem Ziel, alle relevanten Wirtschaftszweige gleichsam unattraktiv für Geldwäsche zu machen, hat sich hinsichtlich Normdurchsetzung und Rechtspraxis leider bisher nicht einstellen können, was die Geldwäschebeauftragten im Nichtfinanzsektor nicht selten ohne spezielle gewerberechtliche „Guidance“ in Sektoren wie dem Edelmetallhandel, dem Immobiliengewerbe, Verbrauchs- und Konsumgüterhandel oder Glücksspiel relativ⁷ alleine lässt.

- 5 Die ursprünglich für den Finanzsektor entwickelte Funktion des Geldwäschebeauftragten wurde mit der Umsetzung der 2. und 3. EU-Geldwäscherichtlinie einfach auf immer weitere Felder des Nichtfinanzsektors erstreckt, ohne dass deren Sinn und Zweck in einzelnen Branchen hinterfragt wurde. Deshalb orientieren sich Geldwäschebeauftragte aller Sektoren bis heute an ihren Kollegen in den Kreditinstituten und den regulatorischen Vorgaben für Kreditinstitute.
- 6 Der Geldwäschebeauftragte blickt also, anders als der „bloße“ Compliance Officer, auf eine lange Rechtstradition und Regulierung jedenfalls im Finanzsektor zurück, die es wenigstens grob zu verstehen gilt, um Tätigkeit, Pflichten und Rolle des Geldwäschebeauftragten überhaupt verstehen zu können. Ein wenig geldwäschegeschichtliches Verständnis mag zudem manch rechtspraktische Auslegungsfälle sicherlich einfacher beantworten lassen.

1. Warum eigentlich ein Geldwäschebeauftragter? – Geschichte einer besonderen Funktion

- 7 Mit dem Banking Secrecy Act 1970⁸ wurde in den USA ein unter Datenschutzgesichtspunkten drastisches Mittel zur Bekämpfung von organisierter Kriminalität eingeführt: Dokumentationspflichten für Bankkunden und Bankgeschäfte

7 Die – wenigen – Publikationen beschränken sich im Wesentlichen auf eine nicht industriespezifische Wiedergabe der Regeln im Finanzsektor. Sie sind in der Rechtsanwendungspraxis für die Sektoren außerhalb der Finanzindustrie weitgehend wertlos.

8 PUBLIC LAW, 91-508-OCT. 26, 1970, „An Act to amend the Federal Deposit Insurance Act to require insured banks to maintain certain records, to require that certain transactions in U.S. currency be reported to the Department of the Treasury, and for other purposes.“

sowie der sogenannte „Currency Transaction Report“ (CTR). Finanzinstitute wurden qua Gesetz verpflichtet, bei Transaktionen jenseits des Schwellenwertes von 10.000 USD und bei bestimmten Forex-Transaktionen einen „Schwellenreport“ zur Nachverfolgung von Transaktionen (den sogenannten „paper trail“) abzusetzen. Anders als in modernen Geldwäschepräventionssystemen wurden solche Meldungen unabhängig von Verdachtsmomenten, unabhängig von Relevanz und Größenordnung und regelmäßig bei Schwellenüberschreitungen bei einzelnen Transaktionen abgesetzt („Regelansatz“). Dies geschah, um rein repressiv, nicht präventiv, Finanzkriminalität durch Beweissicherung zu bekämpfen. Ein solcher Versuch, organisierter und cleverer Finanzkriminalität mit rein beweisorientierten Maßnahmen zu begegnen, mag aus heutiger Sicht erstaunlich oder gar rückständig erscheinen, war in den 1970er Jahren in den USA (und anderswo) aber Mittel der Wahl.

Versetzt man sich in die Zeit der 1970er Jahre, wird schnell die Dimension der Aufgabe klar: Insbesondere für Großbanken war das Meldewesen schon aufgrund der schieren Anzahl von Transaktionen (und den beschränkten technischen Möglichkeiten der Zeit) eine logistische Herausforderung. Clearinghäuser und große Institute hatten folglich mehrere zehntausend Meldungen am Tag abzusetzen, größtenteils ohne IT-Infrastruktur, sondern auf Basis von Einzelbelegen, bestenfalls Microfiche oder Lochstreifen, erst später mit Computern. Anfragen von Behörden und die Rückverfolgung des „paper trail“ waren entsprechend langsam zu bearbeiten und erforderten „manpower“.

Um diese organisatorischen und logistischen Herausforderungen des Regelmeldewesens zu bändigen, wurde im amerikanischen Rechtskreis die zunächst nicht im Gesetz verankerte Funktion des „Money Laundering Reporting Officer“ (MLRO) geboren, der die Organisation des Dokumentations- und Schwellenwertmeldewesens organisierte. Zunächst war der Geldwäschebeauftragte also kaum mehr als ein Koordinator ziemlich unspektakulärer (Standard-)Meldevorgänge an die Finanzbehörden. Kam ein Verdachtsfall auf, war er der im Institut Verantwortliche, um den zuständigen Behörden Informationen aus der Bank zu verschaffen. Auf Überprüfung von Identität oder gar wirtschaftliche Berechtigung an Transaktionen kam es damals (noch) nicht an.

Mit Inkrafttreten des US Money Laundering Control Act 1986⁹ wurde die Teilnahme an Geldwäschetransaktionen unter Strafe gestellt. Ebenso wurde das strukturierte Unterschreiten der CTR und FTR unter Strafe gestellt – ebenso die Mitwirkung hieran. Entsprechend sahen sich Kreditinstitute veranlasst, binnenorganisatorische Vorkehrungen zu treffen, um gezielte Schwellenwertunter-

9 PUBLIC LAW 99-570 – OCT. 27, 1986 100 STAT. 3207, „An Act to strengthen Federal efforts to encourage foreign cooperation in eradicating illicit drug crops and in halting international drug traffic, to improve enforcement of Federal drug laws and enhance interdiction of illicit drug shipments, to provide strong Federal leadership in establishing effective drug abuse prevention and education programs, to expand Federal support for drug abuse treatment and rehabilitation efforts, and for other purposes.“

schreitungen durch Strukturierungen zu erkennen und um Identitäten zu verifizieren. In der Folge wurde – wiederum rein faktisch durch die Markt- und Verwaltungspraxis, nicht von Gesetzes wegen veranlasst – die Rolle des MLRO zunehmend institutionalisiert und weiter gefasst. Insbesondere entwickelte sich der MLRO zur zentralen Instanz für Rückfragen und Nachforschungen von Behörden und innerhalb der Institute selbst, wenn Kundenbeziehungen verschleiert werden oder eben die Regelmeldungen durch geschickte Transaktionsstrukturierungen („Smurfing“, „Structuring“) umgangen werden sollten, was naturgemäß Dokumentationsaufgaben und Analyseleistungen zur wahren wirtschaftlichen Berechtigung hinter Transaktionen mit sich brachte. Wenngleich noch nicht gesetzlich geregelt, erweiterte sich die Funktion des „MLRO“ inhaltlich also stetig.

- 11 Wie der vormalige Name der Funktion erahnen lässt, war die Rolle des „MLRO“ ursprünglich also im Wesentlichen darauf fokussiert, das Schwellenmeldewesen in amerikanischen Instituten zu organisieren und dann – ab 1986 – auch Verdachtsfälle hinsichtlich der Verschleierung von ansonst meldepflichtigen Transaktionen zu identifizieren und als Ansprechpartner für die Informationsbeschaffung durch staatliche Stellen zu fungieren. Vom modernen Verständnis eines „Compliance Officers“ im Sinne eines Risikomanagers war er aber weit entfernt. Durch die Änderungen des US Money Laundering Control Act wurde auch die Identifizierung und die Prüfung von Inhabern von Bankkonten und Depots zur Aufgabe des Instituts, was vom Geldwäschebeauftragten überwacht werden musste.
- 12 In Europa wurden entsprechende Praktiken von der Finanzindustrie übernommen. Schon lange galten in vielen Europäischen Staaten Identifikationspflichten gegenüber Bankkunden, wie andernorts auch in Deutschland, aber eher steuerrechtlich indiziert als geldwäscherechtlich.¹⁰
- 13 Als Anfang und Mitte der 1990er Jahre auf Basis der 1. EU-Geldwäscherichtlinie¹¹ die ersten europäischen Geldwäschegesetze erlassen wurden, wurden Institute zwar verpflichtet, angemessene Maßnahmen zur Bekämpfung der Geldwäsche zu erlassen und Ermittlungsbehörden durch Personen, die Teil dieser Organisation sein sollten,¹² die notwendigen Informationen zur Verfügung zu stellen; eine ausdrückliche Bestellung eines Geldwäschebeauftragten sah die Richtlinie allerdings nicht vor.

10 Vgl. z. B. zum Prinzip der „Kontenwahrheit“ die Identifikationspflichten nach § 154 Abgabenordnung. Das Gesetz war bereits 1977 in Kraft getreten und zwang Institute, zum Zwecke der Erfassung korrekter Besteuerungsgrundlagen den Konteninhaber zu identifizieren.

11 Richtlinie des Rates vom 10. Juni 1991 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche (91/308/EWG).

12 Vgl. Art. 3 und 11 der 1. EU-Geldwäscherichtlinie.

Anders verhielt es sich dann mit den einzelstaatlichen Umsetzungsgesetzen.¹³ In Deutschland war mit § 14 Abs. 2 des ersten Geldwäschegesetzes 1993¹⁴ erstmals eine gesetzliche Pflicht kodifiziert, „eine leitende Person zu bestimmen, die Ansprechpartner für die Strafverfolgungsbehörden bei der Verfolgung der Geldwäsche ist“. Analog dem US-Vorbild beschränkte sich die Haupttätigkeit dieser „leitenden Person“ also zunächst darauf, Ansprechpartner für die Strafverfolgungsbehörden zu sein und das Meldewesen zu organisieren. Anders als in den USA hatte in Europa das Regelmeldewesen allerdings nie Fuß fassen können. Mit dem Inkrafttreten der ersten Geldwäschegesetze wurden Institute verpflichtet, ausschließlich verdächtige Transaktionen zu melden;¹⁵ auch diese zu entdecken war Aufgabe der „leitenden Person“.

Im Rest der Welt entwickelte sich seit den 1990er Jahren durch den Dialog US-amerikanischer Finanzbehörden mit deren internationalen, insbesondere europäischen, Kollegen das Gegenmodell zum Regelansatz, der sogenannte „Risikoansatz“.

Nach dem Risikoansatz („risk based approach“) fand Geldwäschebekämpfung nicht durch eine regelmäßige Meldung und Rückverfolgung von Transaktionsdaten statt, sondern war darauf ausgerichtet, besonders risikobehaftete Konstellationen schon während der Anbahnung oder Abwicklung von Transaktionen genauer zu untersuchen, Verdachtsfälle unter den Transaktionen schon in der Anbahnung oder während der Durchführung zu erkennen, die Transaktionen anzuhalten oder zu unterbinden und ggf. den Strafverfolgungsbehörden als „verdächtige Transaktion“ zu melden (Suspicious Transaction Reports (STR)).

Durch diese in Europa favorisierten Geldwäschebekämpfungsmaßnahmen wurde die Rolle des Geldwäschebeauftragten vom „Reporting Officer“ durch die erste Geldwäscherichtlinie faktisch weiterentwickelt hin zu einer Art „Transaktions- und Kundenrisikomanager“. Man gestand dem Geldwäschebeauftragten zu, Risiken von Transaktionen selbst einzustufen, KYC-Prozesse auf Inkonsistenzen zu überprüfen und im Rahmen des neugeschaffenen Risikoansatzes verdächtige Transaktionen und zugehörige Kundenbeziehungen anzuhalten, abzulehnen und/oder zu melden. Anders als nach den US-basierten Regelmeldesystemen wurde mehr Gewicht auf institutsindividuelle Risikoexposition, individuellen Risikoappetit, geschäftsimmanente Risiken, die von Institut zu Institut divergierten, gelegt. Der Geldwäschebeauftragte wurde also – zunächst in begrenztem Umfang –

13 Vgl. z. B. in U.K., wo im Nachgang zum Erlass des dortigen Money Laundering Acts in 1993 dann im Folgejahr das Erfordernis eingeführt wurde, eine „adequate person“ mit den genannten Aufgaben zu betreuen. 2002 wurde aus der „adequate person“ dann ein „designated officer“; vgl. die historische Schilderung bei *Abdullahi Usman Bello*, Improving Anti-Money Laundering Compliance, S. 41 mit zahlreichen Nachweisen für U.K.

14 Bundesgesetzblatt Jahrgang 1993 Teil I Nr. 56, ausgegeben am 29.10.1993, S. 1770, „Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz – GwG)“ vom 25.10.1993.

15 Vgl. § 1 GwG in der Fassung von 1993.

als Risikomanager tätig, der besonders risikorelevante Geschäftsbereiche beobachtete, besonders risikoträchtige Transaktionen und Kunden identifizierte, manage und im Extremfall sogar beendete und anzeigte.

- 18 Zunächst galt dies in Deutschland aber allein in der Finanzindustrie; durch eine „Umstrukturierung“ der Verpflichtungen des GwG wurden die Zentralnormen des „Ur-GwG“ in einen „generellen Teil“ (GwG) und die (Fach- bzw.) Spezialgesetze wie das KWG und das VAG aufgeteilt.¹⁶ Der Geldwäschebeauftragte befand sich – wie die übrigen Sicherungsmaßnahmen gegen Geldwäsche – nunmehr im Kredit- und Versicherungsaufsichtsrecht wieder.
- 19 Wie eingangs erwähnt, hatte in der Folge die Verwaltungspraxis der Finanzaufsichtsbehörden wesentlichen Anteil an der Ausprägung der Rolle und der Pflichtenkreise des Geldwäschebeauftragten. Zunächst war seine Rolle wie geschildert darauf beschränkt, Ansprechpartner für die Strafverfolgungsbehörden zu sein. In Deutschland institutionalisierte sich die Rolle des Geldwäschebeauftragten dann aber vor allem in den Jahren nach 1998 durch die Verwaltungspraxis der BaFin, zunächst für „Finanzdienstleistungsinstitute“ im altrechtlichen Sinn, später dann für die komplette Finanzwirtschaft.
- 20 Obgleich in der Verlautbarung des BAKred 1/1998 vom Dezember 1997, gerichtet an die Finanzdienstleistungsinstitute, noch „Bestellung eines Geldwäschebeauftragten als Ansprechpartner“ in der Überschrift zu finden ist,¹⁷ legt das BAKred auf den folgenden Seiten der Verlautbarung sehr weit reichende Kompetenzen und Pflichten fest, die ein Geldwäschebeauftragter als Ansprechpartner haben bzw. erfüllen müsse.¹⁸ Insbesondere gehöre zu den Aufgaben des Geldwäschebeauftragten,
 - die Bearbeitung der internen Verdachtsmeldungen und Entscheidung über die Weiterleitung dieser Meldungen gem. § 11 GwG an die zuständigen Ermittlungsbehörden,
 - die Zuständigkeit für die Entwicklung, Aktualisierung und Durchführung interner Grundsätze, Verfahren und Kontrollen zur Verhinderung der Geldwäsche,
 - die Schulung und zeitnahe Unterrichtung der Beschäftigten über Methoden der Geldwäsche und den Pflichtenkatalog des Geldwäschegesetzes,

16 Diese Aufteilung wurde viel später, nämlich mit der Umsetzung der 4. EU-Geldwäscherichtlinie wieder umgekehrt; vgl. das Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen vom 23. Juni 2017, BGBl. I, S. 1822.

17 Vgl. Verlautbarung 1/1998 vom 30.12.1997 (Ziff. VII Rn. 35), zitiert nach *Reischauer/Klein-hans*, KWG, Nr. 948, S. 16 ff.

18 Bei der „Verlautbarung“ des BAKred handelte es sich um eine konkretisierende Verwaltungspraxis zur Durchführung der Pflichten nach dem GwG durch die verpflichteten Institute, die aufgrund § 16 GwG a.F. durch die zuständige Verwaltungsbehörde zu konkretisieren und zu veröffentlichen waren. Die „Verlautbarung“ vom Dezember 1997 war allerdings in ihrer Rechtsnatur noch weniger verbindlich als das folgende „Rundschreiben GW“.

- die Schaffung schriftlicher interner Organisationsanweisungen und technischer Systeme, die gewährleisten, dass diejenigen unbaren/baren Transaktionen, Geschäftsarten und Dienstleistungen, die aus Sicht des einzelnen Finanzdienstleistungsinstituts als besonders geeignet anzusehen sind, mit Geldwäsche verbunden zu sein, mit besonderer Aufmerksamkeit behandelt und auf ihre Geldwäscherelevanz untersucht werden. Dabei reiche es aus, wenn derartige Anti-Geldwäsche-Systeme mit bereits institutsintern für andere Zwecke bestehenden technischen Systemen (z. B. zum Risk Management, Kundenakquisition, Minimierung von Betrugsfällen) verbunden werden.
- Um der Innenrevision sowie dem mit einer Jahresabschlussprüfung bzw. mit einer Prüfung gem. § 44 Abs. 1 KWG beauftragten Prüfer die Ergebnisse dieser Researcharbeit nachvollziehbar zu machen, seien diese (vom Geldwäschebeauftragten) zu dokumentieren.
- Die Überwachung einer auffälligen Geschäftsbeziehung sei ebenso Aufgabe des Geldwäschebeauftragten, wobei dieser die Ergebnisse dieser Überwachung ebenso zu dokumentieren habe.
- Den Geldwäschebeauftragten treffe ferner eine Pflicht zur laufenden Kontrolle der Einhaltung des Geldwäschegesetzes und der internen Grundsätze zur Verhinderung der Geldwäsche. Diese Kontrollpflicht bestehe unabhängig von den retrospektiven Prüfungspflichten der Innenrevision bzw. der Funktion der von der Innenrevision beauftragten externen Stelle.

Schon aus den vorgenannten Pflichtenkreisen ergibt sich also, dass der Geldwäschebeauftragte weitaus mehr sein sollte als lediglich der „Ansprechpartner für Strafverfolgungsbehörden“, wie es noch reichlich naiv in der Überschrift anmuten ließ. Das moderne, bis heute bestehende Rollenverständnis des Geldwäschebeauftragten war geboren. **21**

Wenige Wochen später, nämlich am 30.3.1998, wurden inhaltlich weitgehend gleich gerichtete Grundsätze für die Kreditinstitute festgelegt.¹⁹ In der weiteren Verlautbarung wurde für die Kreditinstitute nochmals ausführlich dargelegt, dass dem Geldwäschebeauftragten insbesondere Entscheidungen im Zusammenhang mit der Bearbeitung und Erstattung von Verdachtsmeldungen, zum Anlass von unternehmensinternen Weisungen (auf Einzelanweisung, Arbeitsanweisung, Organisationsrichtlinien) sowie zur Stornierung von Transaktionen und der Kündigung der Geschäftsverbindung zustünden. **22**

Ferner äußerte sich die Verlautbarung vom 30.3.1998 auch dahingehend, dass der Geldwäschebeauftragte eine leitende Position unterhalb der Geschäftsleiter-ebene haben, im Falle mehrerer Tätigkeiten jedoch nicht zwingend in der zweiten Hierarchieebene angesiedelt sein solle. Im Wesentlichen wurden allerdings die Funktionen und Aufgaben des Geldwäschebeauftragten den für Finanzdienstleistungsinstitute geltenden Regeln angepasst. Obgleich durch die ständige Verwaltungspraxis tief in die Binnenorganisation der Verpflichteten – und somit in **23**

¹⁹ BAKred, Verlautbarung vom 30.3.1998 Z 5 E-100.

die Gewerbebefreiheit und sogar in Grundrechtspositionen – eingegriffen wurde, handelte es sich bei den vorgenannten rechtlichen Vorgaben um „soft law“ im Rahmen der Verwaltungspraxis der Finanzaufsicht. „Verlautbarungen“ waren nach damaligem Verständnis zwar die Ausprägung einer allgemeinen Verwaltungspraxis, die an die betroffenen Institute eben in Form von allgemeinen Hinweisen kommuniziert wurde. Aus rechtsstaatlicher Sicht (im Rahmen der Gewerbebefreiheit²⁰ bedürfen Eingriffe einer gesetzlichen Grundlage²¹) war dieses Vorgehen des BAKred bemerkenswert robust: Zwar waren die Institute faktisch verpflichtet, Geldwäschebeauftragte zu bestellen und ihre Binnenorganisation an die Verwaltungspraxis anzupassen. Es mangelte hierfür aber schlicht an einer hinreichenden rechtlichen Eingriffsgrundlage. Inhaltlich war das Vorpreschen der Aufsichtsbehörden aber völlig richtig.

- 24 Auch mit der 2.²² und 3. EU-Geldwäscherichtlinie²³ und deren einzelstaatlicher Umsetzung änderte sich an einer fehlenden formalrechtlichen Grundlage zunächst nichts; es war den Verpflichteten aus europäischer Sicht – nunmehr auch denjenigen außerhalb des Finanzsektors – qua Richtlinie lediglich aufgebürdet, „interne Strukturen“ zu schaffen, die die Einhaltung der geldwäscherechtlichen Pflichten sicherstellen sollten; von einem förmlichen Erfordernis eines ausgewiesenen „Beauftragten“ sprachen die Richtlinien einstweilen nicht.
- 25 2003 wurde schließlich die Rolle des Geldwäschebeauftragten formalgesetzlich festgelegt. Durch das Geldwäschebekämpfungsverbesserungsgesetz²⁴ wurden die Verpflichteten innerhalb (und, soweit damals schon verpflichtet, auch außerhalb) des Finanzsektors nunmehr qua Gesetz angehalten, einen „der Geschäftsleitung unmittelbar nachgeordneten Geldwäschebeauftragten zu bestimmen“, der Ansprechpartner für die Behörden sein sollte. Der Makel fehlender Eingriffsgrundlage war geheilt.
- 26 In den späten 1990er und frühen 2000er Jahren verschob sich die Rolle des Geldwäschebeauftragten – getrieben durch die Verwaltungspraxis – immer weiter. Waren es vormalig – basierend auf dem Gedanken des Regelansatzes – vornehmlich „Transaktionen“, die ein Tätigwerden des Geldwäschebeauftragten erforderten, wurden auffällige Kundenprofile, Inkonsistenzen im Kundenverhalten und verdächtige und fragwürdige Verhaltensmuster im Kundenverhalten primäres

20 *Erbs/Kohlhaas*, Strafrechtliche Nebengesetze, § 1 GewO Rn. 1.

21 BVerfG, NJW 1970, 1591; BVerwGE 38, 209 ff. (NJW 1971, 1475). Aufgrund der bundesweiten Geltung des Geldwäscherechts ist hier auf das Erfordernis einer bundesgesetzlichen Norm abzustellen.

22 Richtlinie 2001/97/EG des Europäischen Parlaments und des Rates vom 4. Dezember 2001 zur Änderung der Richtlinie 91/308/EWG des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche.

23 Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung.

24 Gesetz zur Verbesserung der Bekämpfung der Geldwäsche und der Finanzierung des Terrorismus (Geldwäschebekämpfungsgesetz) vom 8.8.2002 (BGBl. I, S. 3105).

Ziel des staatlichen Interesses. Mithin wurden nicht nur einzelne verdächtige Transaktionen anzeigepflichtig („Suspicious Transaction Reporting“ (STR)), sondern jegliche geldwäscheverdächtige Aktivität eines (Bank-)Kunden („Suspicious Activity Reporting“ (SAR)). Die verdächtige Gesamtaktivität eines oder mehrerer Kunden, nicht mehr nur noch einzelne verdächtige Transaktionen zu erkennen, wurde somit zur weiteren Aufgabe des Geldwäschebeauftragten. Hierzu musste der Geldwäschebeauftragte Monitoringsysteme einrichten und betreiben, mit deren Hilfe die Kundenprofile analysiert und besonders risikoträchtige Geschäftsbeziehungen herausgefiltert werden mussten. Das Tätigkeitsprofil des Geldwäschebeauftragten, insbesondere in der Finanzindustrie, entwickelte sich zu einer IT-lastigen Funktion weiter; der Geldwäschebeauftragte war für die Einrichtung und vor allem die institutsspezifische Kalibrierung der IT-Systeme verantwortlich. Hierdurch wurde das Tätigkeitsprofil des Geldwäschebeauftragten mehr und mehr auf eine Tätigkeit als „Risikomanager“ zur Abwehr von Gefahren für den Verpflichteten weit im Vorfeld eigentlich verdächtiger Transaktionen ausgerichtet.

Im Jahr 2011 wurde die Pflicht, einen Geldwäschebeauftragten zu bestellen, in das Geldwäschegesetz aufgenommen, während es vorher nur in den Fachgesetzen für die Finanzbranche vorgeschrieben war.²⁵ Leider waren die Begrifflichkeiten des Gesetzes unklar bzw. ließen deutlichen Raum für Interpretation. Hierdurch wurde für viele Verpflichtete jedenfalls unklar oder strittig, ob diese einen Geldwäschebeauftragten zu ernennen hatten. **27**

Die Umsetzung der 4. EU-Geldwäscherichtlinie²⁶ in das deutsche GwG²⁷ im Jahr 2017 war schließlich für die Figur des Geldwäschebeauftragten in dreierlei Hinsicht eine wesentliche Zäsur: Zum einen wurde die Bestellung des Geldwäschebeauftragten unter die Unterüberschrift „Risikomanagement“ in den Zweiten Abschnitt des GwG eingeführt, die oben beschriebene Rolle als „Risikomanager“ mithin fest im Gesetz verankert. Zum anderen wurden auch – dies war in den vorherigen Gesetzesfassungen vielfach streitig – zahlreiche weitere Verpflichtete nochmals ausdrücklich aufgefordert, einen Geldwäschebeauftragten zu bestellen bzw. Härtefallregelungen aufgenommen, um unsachgerechte Konstellationen zu vermeiden (siehe hierzu sogleich unten → Rn. 38 ff.). **28**

Durch die Einführung einer „Transparenzkultur“ durch das Umsetzungsgesetz zur 4. EU-Geldwäscherichtlinie erweiterte sich aber die Rolle des Geldwäsche- **29**

25 Vgl. das „Gesetz zur Optimierung der Geldwäscheprävention“ vom 22.12.2011 (BGBl. I, S. 2959).

26 Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission.

27 GwG in der Fassung des Gesetzes zur Umsetzung der 4. EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen vom 23. Juni 2017 (BGBl. I, S. 1822).

beauftragten erneut. Im Nachgang zu einigen Steuer-Skandalen²⁸ rückte die Transparenz von Eigentümerstrukturen und die wirtschaftliche Kontrolle über an Transaktionen beteiligte Personen in den Vordergrund.

- 30** Spätestens mit dem Umsetzungsgesetz zur Änderungsrichtlinie zur 4. EU-Geldwäscherichtlinie,²⁹ dort durch § 23a GwG n. F., erweiterte sich das Aufgabenspektrum des Geldwäschebeauftragten weiter. Schon nach der bisherigen Rechtslage war es eine wesentliche Aufgabe, die Eigentümer- und Kontrollstruktur von Kunden zu ermitteln, allerdings bisher allein als Folge einer eigenen, gewerberechtlichen Verpflichtung zur Abwehr einer eigenen Geldwäscheverantwortlichkeit des Unternehmens. Mit der Einfügung der Pflicht zur Abgabe von Unstimmigkeitsmeldungen (§ 23a GwG) wird die neue Rolle des Geldwäschebeauftragten „im Dienste der Transparenzkultur“ weiter ausgestaltet. Über eine reine unternehmensbezogene Tätigkeit zur Abwehr von geldwäscheverdächtigen Kunden und Transaktionen im eigenen Risiko wird die Funktion eines Überwachers von Unternehmens- und Eigentümertransparenz im öffentlichen Interesse in Zukunft stärker werden.
- 31** Rückblickend sind Rolle und Aufgaben des Geldwäschebeauftragten also immer weiter gefasst worden – teils wegen der technischen Entwicklung, zum weitaus größeren Teil aber im Zuge der Reformen der Geldwäschebekämpfung, die sich nach deutschrechtlichem Verständnis in der Rolle des Geldwäschebeauftragten als unmittelbar verantwortlicher Person heraus kristallisieren.

2. Verpflichtete Unternehmen

- 32** Wie oben dargestellt traf die Pflicht zur Einsetzung eines Geldwäschebeauftragten erst seit der Umsetzung der 4. EU-Geldwäscherichtlinie wesentliche Teile der Gesamtverpflichteten, vorher nur die Finanzindustrie. Dennoch sind einzelne Abstufungen im Gesetz vorgesehen, um der Geldwäschesensibilität und den Eigenheiten einiger Sektoren Rechnung tragen zu können.

a) Qua Gesetz

- 33** Nach § 7 Abs. 1 GwG müssen zunächst die „Kernverpflichteten“ aus der Finanzindustrie, nämlich
- Kreditinstitute nach § 1 Abs. 1 des Kreditwesengesetzes, mit Ausnahme der in § 2 Abs. 1 Nr. 3 bis 8 des Kreditwesengesetzes genannten Unternehmen, und im Inland gelegene Zweigstellen und Zweigniederlassungen von Kreditinstituten mit Sitz im Ausland,

28 Vgl. RL (EU) 2018/843 des Europäischen Parlaments und des Rates vom 30.5.2018 zur Änderung der RL (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der RL 2009/138/EG und 2013/36/EU, ABl. EU Nr. L 156/43 vom 19.6.2018.

29 Gesetz zur Umsetzung der Änderungsrichtlinie zur 4. EU-Geldwäscherichtlinie vom 12. Dezember 2019 (BGBl. I, S. 2602).

- Finanzdienstleistungsinstitute nach § 1 Abs. 1a des Kreditwesengesetzes, mit Ausnahme der in § 2 Abs. 6 Satz 1 Nr. 3 bis 10 und 12 und Abs. 10 des Kreditwesengesetzes genannten Unternehmen, und im Inland gelegene Zweigstellen und Zweigniederlassungen von Finanzdienstleistungsinstituten mit Sitz im Ausland, und
 - Zahlungsinstitute und E-Geld-Institute nach § 1 Abs. 3 des Zahlungsdienstleistungsgesetzes und im Inland gelegene Zweigstellen und Zweigniederlassungen von vergleichbaren Instituten mit Sitz im Ausland,
- einen Geldwäschebeauftragten bestellen. Vor dem oben geschilderten historischen Hintergrund der Funktion ist dies auch nur konsequent.

Ferner müssen Finanzunternehmen im Sinne des § 1 Abs. 24 GwG sowie im Inland gelegene Zweigstellen und Zweigniederlassungen von Finanzunternehmen mit Sitz im Ausland, soweit sie nicht bereits aus anderen Gründen hierzu verpflichtet sind, einen Geldwäschebeauftragten bestellen. Diese Pflicht war – wie die Erfassung von Finanzunternehmen ehemals im Sinne des § 1 Abs. 3 KWG – über viele Jahre hoch umstritten, da nach alter Lesart auch reine Industrieholdings jedenfalls theoretisch in den Verpflichtetenkreis fallen konnten.³⁰ Erst eine klarstellende Gesetzesänderung hat mit Wirkung vom Januar 2020 dies – zutreffenderweise – verneinend klargestellt.³¹

Die Versicherungswirtschaft ist neben der Kreditwirtschaft zwar ein Kernverpflichteter, aber nur sofern Geldwäscherisiken tatsächlich bestehen, was z. B. bei Sach- oder Transportversicherungen sicherlich anders eingeschätzt werden muss als bei kapitalbildenden Lebensversicherungen. Konsequenterweise erfasst das GwG von vornherein nur solche Versicherungen, die besonders risikobehaftete Produkte vertreiben oder makeln. Insbesondere handelt es sich hierbei um Lebensversicherungen, Unfallversicherungen mit Prämienrückgewähr, Darlehen im Sinne des Kreditwesengesetzes oder Kapitalisierungsprodukte. Folglich sind Versicherungsunternehmen, die entsprechende Produkte anbieten, verpflichtet, einen Geldwäschebeauftragten zu bestellen; die Verpflichtung gilt wiederum für inländische Versicherungen und Niederlassungen ausländischer Unternehmen. Für Versicherungsmakler gilt dies aber nur auf Anordnung im Einzelfall (→ Rn. 44 ff.).

Kapitalverwaltungsgesellschaften nach dem KAGB sind ebenso verpflichtet, Geldwäschebeauftragte zu bestellen, wie inländische Niederlassungen ausländischer KVGn. Aufgrund des komplexen Passporting-Verfahrens bei KVGn gelten für Konstellationen mit Auslandsberührung jedoch komplexere Regeln.³²

30 Vgl. eine Übersicht über den Problemkreis bei *Brian/Frey/Krais*, CCZ 2019, 245 mit zahlreichen aktuellen Nachweisen.

31 Vgl. § 1 Abs. 24 Satz 2 GwG n.F.; über den Gesetzeswortlaut wird es hinsichtlich Minderheitsbeteiligungen an Unternehmen des Finanzsektors wohl noch zu Auseinandersetzungen kommen.

32 Der Grund hierin liegt in komplexeren „Passporting“-Konstellationen bei Fonds, wo zwischen Produkt- und Dienstleistungspassporting, bspw. als Fondsmanager oder Vertriebsmitt-

- 37** Ferner müssen Veranstalter und Vermittler von Glücksspielen Geldwäschebeauftragte bestellen, soweit es sich nicht um Betreiber von Geldspielgeräten nach § 33c der Gewerbeordnung handelt, Vereine, die das Unternehmen eines Totalisatoren nach § 1 des Rennwett- und Lotteriegesetzes betreiben, oder im Falle von Lotterien, die nicht im Internet veranstaltet werden und für die die Veranstalter und Vermittler über eine staatliche Erlaubnis der in Deutschland jeweils zuständigen Behörde verfügen. Ausgenommen sind ferner Soziallotterien.

b) Freistellungsmöglichkeit (§ 7 Abs. 2 GwG)

- 38** Für die genannten Verpflichtetengruppen besteht die Möglichkeit, bei der zuständigen Aufsichtsbehörde eine Freistellung von der Verpflichtung, einen Geldwäschebeauftragten bestellen zu müssen, zu beantragen (§ 7 Abs. 2 GwG). Eine entsprechende Befreiungsmöglichkeit ist auch in den internationalen Quellen vorgesehen; die FATF z.B. empfiehlt den FATF-Mitgliedstaaten sogar, aus Verhältnismäßigkeitsgründen eine entsprechende, breit gefasste Härteklausel aufzunehmen.³³
- 39** Eine Härteausnahme kommt vor allem für kleine und kleinste Unternehmen in Betracht. Hierzu müssen nach dem Gesetz die folgenden Voraussetzungen kumulativ erfüllt sein:
- Die Gefahr von Informationsverlusten aufgrund arbeitsteiliger Unternehmensstruktur besteht nicht und
 - risikobasiert wurden anderweitige Vorkehrungen getroffen, um Geschäftsbeziehungen und Transaktionen zu verhindern, die mit Geldwäsche oder Terrorfinanzierung zusammenhängen.
- 40** Sofern die spezifische Risikolage eines Verpflichteten dem nicht entgegensteht, sollen durch die Möglichkeit einer Befreiung wie gesagt nur unangemessene Härtefälle vermieden werden; flächendeckende Ausnahmen sind auch in der Rechtsanwendungspraxis nicht zu beobachten.
- 41** Unter dem Erfordernis, dass „die Gefahr von Informationsverlusten und -defiziten aufgrund der Unternehmensstruktur nicht besteht“, ist zu verstehen, dass die zur Geldwäscheprävention wesentlichen Erkenntnisse über Kunden, Produkte, Vertriebskanäle, Zahlungen etc. bei einer anderen Person als dem Geldwäschebeauftragten zusammenfließen bzw. dies jedenfalls eingerichtet werden kann.³⁴ Gerade bei Kleinstunternehmen mit zwei oder drei Mitarbeitern ist dies in der Regel der Fall. Hinter dem zweiten Erfordernis, dass jedenfalls „anderweitige Vorkehrungen“ getroffen werden, um Geldwäsche zu verhindern, ist zu verstehen, dass die förmlichen Sicherungsmaßnahmen und die förmlichen Risikoanalysen, wie sie das GwG vorschreibt, schlicht nicht risikoangemessen und des-

ler, unterschieden wird. Zu den technischen Details vgl. *Kaetzler*, in: Zentes/Glaab, GwG, § 2 Rn. 155 ff.

33 Vgl. FATF Recommendations 2012–2017, Interpretive Note zu Recommendation 18, Rn. 3.

34 Vgl. *Herzog*, in: Herzog, GwG, § 7 Rn. 7.

halb nicht notwendig sind. Kann ein Unternehmen mithin beides darlegen, kommt eine Befreiung von der Verpflichtung, einen Geldwäschebeauftragten zu bestellen, in Betracht.

Hinsichtlich des Finanz- und Versicherungssektors hat die Vorschrift allerdings kaum praktische Relevanz. Die BaFin hat in ihren Auslegungs- und Anwendungshinweisen klargestellt, dass § 7 Abs. 2 GwG als Ausnahmenvorschrift allenfalls für kleine und kleinste Finanzdienstleister überhaupt in Betracht kommen dürfte;³⁵ Ausnahmegenehmigungen beschränken sich auf ein paar Handvoll Institute, meistens kleinste Spezialinstitute. **42**

Außerhalb des Finanzsektors spielt die genannte Vorschrift allerdings eine relevante Rolle, insbesondere bei Güterhändlern,³⁶ welche nur sehr vereinzelt Transaktionen jenseits der Bargeldschwelle des § 4 Abs. 5 GwG vornehmen, bei Beteiligungsgesellschaften und Finanzholdings i. S. d. § 1 Abs. 24 GwG und in ähnlichen Konstellationen. **43**

c) Anordnung der Behörden

Nach dem Gesetz kann die zuständige Aufsichtsbehörde (vgl. § 50 GwG) anordnen, dass auch einzelne Verpflichtete weiterer Verpflichtetengruppen einen Geldwäschebeauftragten zu bestellen haben, für die dies das Gesetz regelmäßig nicht vorsieht. Die Schwelle hierfür liegt relativ niedrig; eine Anordnung kann erfolgen, wenn die Behörde dies für „angemessen“ erachtet. **44**

Insbesondere handelt es sich hierbei um die Verpflichteten nach § 2 Abs. 1 Nr. 4, 5, 8, 10 bis 14 und 16 GwG, mithin also Zahlungs- und E-Geld-Agenten bzw. Gewerbetreibende, die E-Geld vertreiben oder rücktauschen, Versicherungsvermittler, soweit das GwG für sie anwendbar ist, Rechtsanwälte bei der Wahrnehmung von Katalogmandaten sowie nicht verkammerte Rechtsbeistände, „Trust-Service-Provider“ bei der Ausübung einer Katalogdienstleistung, Immobilienmakler und Güterhändler. Bei Letzteren soll eine Anordnung erfolgen, wenn die Haupttätigkeit des entsprechenden Güterhändlers im Handel mit hochwertigen Gütern, insbesondere Edelmetallen, Edelsteinen, Schmuck oder Kunstgegenständen, liegt, vgl. § 1 Abs. 10 GwG. **45**

Erfolgt eine solche behördliche Anordnung, hat der Geldwäschebeauftragte die gleiche Stellung und die gleichen Pflichten, wie sie § 7 GwG für den Geldwäschebeauftragten bei den Kernverpflichteten vorsieht, wobei die Aufsichtsbehörde hierzu konkretisierende Anordnungen treffen kann, vgl. § 51 GwG. Die Anordnung nach § 7 Abs. 3 GwG ist ein den jeweiligen Verpflichteten belastender Verwaltungsakt, gegen den der Rechtsweg (Widerspruch und Anfechtungsklage) möglich ist; Rechtsmittel haben allerdings keine aufschiebende Wirkung (§ 51 Abs. 2 Satz 3 GwG). **46**

³⁵ BaFin, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz 2021, Ziff. 3.2, S. 20 unten.

³⁶ Zur Geldwäscheprävention bei Güterhändlern siehe → *Komma*, Kap. 23 m. w. N.

- 47 In der Vergangenheit haben verschiedene Aufsichtsbehörden vor allem im Wege der Allgemeinverfügung entsprechende Anordnungen erlassen.³⁷ In der Praxis darf erwartet werden, dass Aufsichtsbehörden von einer Anordnung allerdings dann absehen, wenn schon aufgrund der Unternehmensstruktur und des geringen Geldwäscherisikos eigentlich eine Befreiung nach § 7 Abs. 2 GwG in Betracht kommen könnte.³⁸

3. Anforderungen an den Geldwäschebeauftragten und Bestellung

- 48 Nach dem Gesetz müssen der Geldwäschebeauftragte und sein Stellvertreter die erforderliche Sachkunde und Zuverlässigkeit zur Ausführung dieses Amtes besitzen (§ 7 Abs. 4 Satz 2 GwG). Wie unten zu zeigen sein wird, ist er aufgrund des ihm von Gesetz und Verwaltungspraxis zugewiesenen Pflichtenkreises gleichzeitig Beschützer und zum kleineren Teil auch Überwachergarant.³⁹ Dies und die oben geschilderte fortschreitende öffentlich-rechtliche Prägung seines Tätigkeitsbereiches erfordern – branchenspezifisch – hinreichende Sachkunde und, selbstverständlich aufgrund der Sensibilität der Tätigkeit, eine unzweifelhafte Integrität.
- 49 Unter hinreichender „fachlicher Eignung“ versteht das Gesetz, dass der Geldwäschebeauftragte und sein Stellvertreter die notwendigen theoretischen Kenntnisse sowie praktische Erfahrungen, insbesondere Leitungserfahrung, aufweisen können. Ein Berufsanfänger wird in keiner Branche Geldwäschebeauftragter werden können. Innerhalb der verschiedenen zu verpflichtenden Gruppen werden allerdings jeweils höchst unterschiedliche Anforderungen gestellt.
- 50 Die erforderlichen theoretischen Kenntnisse setzen bis heute keinen Hochschulabschluss voraus. Der Geldwäschebeauftragte muss jedoch nachweisen können, dass er – etwa durch geeignete Fortbildungen – die notwendigen rechtlichen Grundlagen, insbesondere die gesetzlichen regulatorischen Anforderungen sowie regulatorische Rahmengesetze (z. B. das KWG, das VAG oder weitere gewerberechtliche Grundvorschriften) kennt und deren Auswirkungen auf die Ablauforganisation einordnen kann.⁴⁰
- 51 Insbesondere bei den Kernverpflichteten besteht ferner die Anforderung, dass eine gewisse Berufserfahrung, gekoppelt mit „praktischer Leitungserfahrung“, besteht. Unter solcher praktischer Leitungserfahrung ist vor allem zu verstehen, dass der Betreffende über praktische Anwendungserfahrung in geldwäsche-rechtlich relevanten Tätigkeitsfeldern verfügt. Hierbei muss es sich nicht zwin-

37 Vgl. hierzu *Roth*, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, S. 108 f. m. w. N.; *Kaetzler*, in: Zentes/Glaab, GwG, § 7 Rn. 21 ff. m. w. N. sowie *Herzog*, GwG, § 7 Rn. 9.

38 Vgl. *Roth*, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, S. 109 Rn. 25.

39 Vgl. *Kaetzler*, in: Zentes/Glaab, GwG, § 7 Rn. 26 m. w. N.

40 Vgl. *Roth*, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, S. 110 Rn. 30 ff.; *Kaetzler*, in: Zentes/Glaab, GwG, § 7 Rn. 33 ff.

gend um eine Tätigkeit in einer Compliance- oder Geldwäscheabteilung handeln; auch langjährige Erfahrungen, z. B. im Bereich der Debitorenbuchhaltung, der Stammdatenanlage, der Finanzbuchhaltung, des Controllings oder der Innenrevision dürften hierzu in der Regel ausreichen; in der Finanzwirtschaft werden hinreichende Branchenkenntnisse und Branchenerfahrung erwartet. Wesentlich ist weiterhin, dass sich der Geldwäschebeauftragte – dies sehen die Verwaltungspraxen durchgehend vor – in angemessener Form laufend weiterbildet. Es ist zu empfehlen, diese Weiterbildung zu dokumentieren und entsprechend nachzuhalten. Der Geldwäschebeauftragte und sein Stellvertreter haben aufgrund dieser Anforderungen einen im Gesetz angelegten Anspruch auf Kostenerstattung, selbstverständlich nur solange die Kosten angemessen sind.⁴¹

Da der Geldwäschebeauftragte in der Regel seine Tätigkeit „im Inland ausüben“ **52** muss, sind hinreichende deutsche Sprachkenntnisse, die z. B. die angemessene Koordination mit den Aufsichtsbehörden oder der FIU ermöglichen, Grundvoraussetzung. Eine ständige Anwesenheit im Inland ist wünschenswert, nicht zwingend Voraussetzung, wird aber gerne von den Aufsichtsbehörden gesehen.

Unter „Zuverlässigkeit“ ist zu verstehen, dass der Geldwäschebeauftragte und sein Stellvertreter die Gewähr bieten, sich stets rechtstreu zu verhalten und keine strafrechtlich relevanten Verstöße zu begehen. Der Begriff rekurriert allerdings **53** nur teilweise auf die Legaldefinition in § 1 Abs. 20 GwG, welcher die Zuverlässigkeit von Mitarbeitern regelt. Die Anforderungen an den Geldwäschebeauftragten dürften hinsichtlich der Sensibilität seiner Tätigkeit inhaltlich deutlich über die Vorgaben des § 1 Abs. 20 GwG hinausgehen.⁴² In Übereinstimmung mit verschiedenen Industriestandards ist entsprechend zu fordern, dass der Geldwäschebeauftragte jedenfalls innerhalb der letzten fünf Jahre vor Bestellung nicht wegen eines Verbrechens oder wegen eines Vermögens- oder Urkundsdelikts, einer Insolvenzstraftat oder einer Steuerhinterziehung rechtskräftig verurteilt worden ist.⁴³ In der Finanzindustrie gelten in der Praxis deutlich höhere Maßstäbe; selbst eine Einstellung nach § 153a StPO innerhalb der letzten Jahre stellt faktisch einen Hinderungsgrund dar, ebenso wie ein einschlägiges Bußgeld. Aufgrund der gestiegenen Sanktionsaktivität der Aufsichtsbehörden wird diesem Punkt in Zukunft erhebliches Gewicht zukommen.

Die förmliche Bestellung des Geldwäschebeauftragten im Unternehmen ist gesetzlich geregelt, vgl. § 7 Abs. 4 GwG. Die Verpflichteten haben der zuständigen **54** Aufsichtsbehörde, vgl. § 50 GwG, die Bestellung des Geldwäschebeauftragten und seines Stellvertreters sowie ihre Entpflichtung vorab anzuzeigen. Würde ein externer Geldwäschebeauftragter bestellt, sind zusätzlich die Anforderungen an

⁴¹ Vgl. *Kaetzler*, in: Zentes/Glaab, GwG, § 7 Rn. 38 m. w. N.

⁴² Vgl. hierzu *Kaetzler*, in: Zentes/Glaab, GwG, § 7 Rn. 40 ff.; abweichend ausdrücklich *Roth*, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, S. 112 Rn. 39 ff.

⁴³ Dieser Rückschluss ergibt sich aus den für die Kreditwirtschaft geltenden Mindestanforderungen an die Compliance-Organisation „MaComp“, dort BT Ziff. 1.3.1.4, Rn. 1.

Auslagerungen von Sicherungsmaßnahmen nach § 6 Abs. 7 GwG, mithin eine zweiwöchige Voranzeige und inhaltliche Darlegung, erforderlich. Die Anzeige selbst ist formlos, muss aber Schriftformerfordernissen genügen. Während außerhalb des Finanzsektors kurze Anschreiben genügen bzw. sogar Formblätter existieren, besteht im Finanzsektor darüber hinaus eine explizite Darlegungspflicht zur Funktion bzw. zu den Abberufungsgründen.⁴⁴

- 55 Zusammengefasst ist jedoch anzumerken, dass die Voraussetzungen, insbesondere an die Vorbildung und Vorerfahrung des Geldwäschebeauftragten und seines Stellvertreters stark zwischen den einzelnen verpflichteten Gruppen divergieren. Während z. B. im Handel lediglich eine minimale Vorbildung, z. B. durch Seminare etc. und eine Tätigkeit auf „Marktfolgeseite“ nachgewiesen werden muss, bestehen im Finanzsektor, insbesondere bei großen oder gar systemrelevanten Instituten, deutlich erhöhte Anforderungen, die nur durch langjährige einschlägige Vortätigkeiten und ein makelloses Führungszeugnis erfüllt werden können. Sofern eingangs geschildert wurde, dass bis heute zwar ein einschlägiges Hochschulstudium grundsätzlich nicht nötig ist, wird dies faktisch bei Großbanken und Versicherungskonzernen vorausgesetzt.

4. Kompetenzen und Stellung im Unternehmen

- 56 Anders als beim „normalen“ Compliance Officer sind Stellung im Unternehmen, Kompetenzen und Befugnisse des Geldwäschebeauftragten gesetzlich geregelt. Auskunft hierzu gibt § 7 Abs. 5 GwG.
- 57 Der Geldwäschebeauftragte muss u. a. seine Tätigkeit im Inland ausüben. Unter „im Inland ausüben“ versteht das Gesetz zwar keine strenge Residenzpflicht, jedoch eine angemessene Anwesenheitspflicht im Inland. Eine grenzüberschreitende Auslagerung der Funktion ist entsprechend nur dann möglich, wenn im Inland ein „Geldwäscheansprechpartner“ verbleibt. Zum Teil wird dieses Erfordernis sogar durch das Gesetz selbst begründet:
- 58 „Er muss Ansprechpartner sein für die Strafverfolgungsbehörden, für die für Aufklärung, für Hütung und Beseitigung von Gefahren zuständigen Behörden, für die Zentralstelle für Finanztransaktionsuntersuchungen und für die Aufsichtsbehörde in Bezug auf die Einhaltung der einschlägigen Vorschriften.“
- 59 Das Gesetz verlangt also eine relative Verfügbarkeit im Inland für Behörden, was wie angesprochen hinreichende deutsche Sprachkenntnisse voraussetzt. Ein weiterer Grund für das Erfordernis, dass der Geldwäschebeauftragte seine Tätigkeit im Inland ausüben muss, liegt jedoch darin, dass aufgrund des Territorialitätsprinzips erwartet wird, dass der Geldwäschebeauftragte hinreichenden Kontakt zu den im Inland belegenen Organisationsteilen, den im Inland vertriebenen Produkten und Leistungen hat, um seine Tätigkeit als „Risikomanager“ zielfüh-

44 Vgl. hierzu *Herzog*, in: *Herzog*, GwG, § 7 Rn. 10 m. w. N.; *Roth*, in: *Gehra/Gittfried/Lienke*, Prävention von Geldwäsche und Terrorismusfinanzierung, S. 113 Rn. 45.

rend ausüben zu können. Die Anwesenheit in unvorhergesehenen Eil- und Auskunftsfällen muss ebenso sichergestellt sein.

Nach dem Gesetz sind dem Geldwäschebeauftragten (und seinem Stellvertreter) ferner ausreichend Befugnisse und die für eine ordnungsgemäße Durchführung seiner Funktion notwendigen Mittel einzuräumen. Liegen Defizite bei der personellen oder sachlichen Ausstattung vor, kann dies zu einer unzureichenden Delegation im haftungsrechtlichen Sinne führen, welche als Organisationsverstoß in einem Geldwäschefall die Haftung des zuständigen Geschäftsleiters wieder aufleben lässt.⁴⁵ Aus Sicht des Geldwäschebeauftragten empfiehlt es sich deshalb, schwerwiegende Ausstattungsdefizite revisionssicher beim zuständigen Mitglied der Leitungsebene zu monieren. Welche Sach- und Betriebsmittel „notwendig“ sind, bestimmt sich nach der Größe, dem Geschäftsmodell und der Risikosituation des jeweiligen Verpflichteten. Allgemeingültige konkrete Regeln können kaum erstellt werden; dies gilt sowohl im Hinblick auf die erforderliche personelle Ausstattung wie auch die sachliche Ausstattung.⁴⁶ **60**

Nach dem Gesetz sind dem Geldwäschebeauftragten und dem Stellvertreter auch „umgehender Zugang zu sämtlichen Informationen, Daten, Aufzeichnungen und Systemen zu gewähren oder zu verschaffen, die im Rahmen der Erfüllung seiner Aufgaben von Bedeutung sein können“. **61**

Die angemessene Einbindung des Geldwäschebeauftragten in die Informationsarchitektur des Unternehmens ist von herausragender Bedeutung. Der Geldwäschebeauftragte muss – zur effektiven Delegation von Verantwortlichkeit vom Geschäftsleiter auf den Geldwäschebeauftragten – in sämtliche Informationsflüsse, die für seine Arbeit von Bedeutung sein können, eingebunden werden. Nach stehender Verwaltungspraxis im Finanzsektor ist ihm auch Zugang zu Prüfberichten der internen Revision und von externen Prüfern zu gewähren.⁴⁷ **62**

In der Verwendung der entsprechenden Daten, die dem Geldwäschebeauftragten zur Verfügung gestellt werden, ist der Geldwäschebeauftragte selbstverständlich beschränkt; nach § 7 Abs. 6 darf der Geldwäschebeauftragte Daten und Informationen ausschließlich zur Erfüllung seiner Aufgaben verwenden. **63**

Ferner legt das Gesetz fest, dass der Geldwäschebeauftragte der Geschäftsleitung unmittelbar zu berichten hat. Hierin liegt ein Eingriff in die Gewerbefreiheit und die Freiheit einer Selbstorganisation von Gewerbebetrieb und freien Berufen. Er ist auf „Führungsebene“ zu bestellen und der Geschäftsleitung – in seinem Kompetenzbereich – unmittelbar nachgeordnet (§ 7 Abs. 1 GwG). Hintergrund der Vorschrift ist, dass der Gesetzgeber den Geldwäschebeauftragten als „starke Funktion“ im Unternehmen sehen will. Der Begriff der „Führungs-“ **64**

45 Vgl. Kaetzler, in: Zentes/Glaab, GwG, § 7 Rn. 57 und 66.

46 Vgl. BaFin, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz 2021, Ziff. 3.2 oder *Achtelik*, in: Boos/Fischer/Schulte-Mattler, KWG/CRR-VO, § 25 h KWG Rn. 27 m. w. N.

47 Vgl. BaFin, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz 2021, Ziff. 3.2.

ebene“ ist legal definiert, vgl. § 1 Abs. 15 GwG. Der Geldwäschebeauftragte muss mithin eine „Führungskraft oder ein leitender Mitarbeiter“ mit ausreichenden Qualifikationen und Befugnissen sein. Er muss – ausweislich der Gesetzes-systematik und der Gesetzesbegründung⁴⁸ – in dieser leitenden Funktion vor allem Kenntnisse und Erfahrungen aufweisen; „leitend“ ist hier also durchaus qualitativ, nicht hierarchisch zu verstehen.

- 65 Dass ein gewerberechtlich orientiertes Gesetz die Stellung eines Beauftragten sogar nach der Hierarchieebene definiert, mag bemerkenswert erscheinen. Begründet ist dies jedoch in einer langen Rechtstradition, in welcher insbesondere die Verwaltungspraxis anstrebt, dem Geldwäschebeauftragten eine hinreichend exponierte Stellung zu verschaffen, die ihm insbesondere Entscheidungsbefugnisse und Weisungsbefugnisse gegenüber nachgeordneten Mitarbeitern verschafft. Durch die Klarstellung, dass der Geldwäschebeauftragte lediglich in seiner Funktion (als „dotted line“) der Geschäftsleitung unmittelbar nachgeordnet ist, hält sich der Eingriff in die Binnenorganisation der Gewerbetreibenden in verhältnismäßigen Grenzen.
- 66 Oftmals übt der Geldwäschebeauftragte allerdings weitere Tätigkeiten aus. Dies ist selbstverständlich zulässig. Die hierarchische Nachordnung zur Geschäftsleitung darf durch die parallelen Tätigkeiten jedoch nicht entwertet werden.
- 67 Ebenso ist es üblich, den Geldwäschebeauftragten – z. B. in disziplinarisch/organisatorischer Hinsicht – an andere Unternehmenseinheiten als die Geschäftsleitung anzubinden. Insbesondere außerhalb des Finanzsektors ist zu beobachten, dass eine Einbindung an Rechtsabteilungen oder andere Marktfolgeeinheiten üblich ist. Dies ist so lange nicht zu beanstanden, wie es nicht zu Interessenkonflikten führt. Aus diesen Gründen wird z. B. schon seit langem vertreten, dass der Geldwäschebeauftragte nicht gleichzeitig in der Innenrevision eines Verpflichteten tätig sein darf.⁴⁹ EBA und BaFin vertreten für den Finanzsektor mit sehr guten Gründen, dass eine Einbindung an die Innenrevision unzulässig sei.⁵⁰
- 68 Eine gleichzeitige Ausübung der Funktion des Datenschutzbeauftragten ist – aufgrund der evidenten Interessenkollision zwischen Datenschutz und Geldwäsche – unzulässig. Eine in der Vergangenheit vertretene Ansicht, dass eine Doppelfunktion durch eine Person ausgeübt werden könne, sofern diese die Pflichtenkreise jeweils differenziere, ist mittlerweile verworfen.⁵¹

48 Vgl. die Abweichung zum Referentenentwurf zur Umsetzung der 4. EU-Geldwäscherichtlinie 2017 vom 15.12.2016, S. 17. Auf Intervention der Kreditwirtschaft wurde das Erfordernis zurückgenommen.

49 Vgl. Roth, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, S. 120 Rn. 87 ff., insbesondere 120 ff.

50 EBA/GL/2017/11, Leitlinie zur internen Governance gem. Art. 16 VO (EU) 1093/2010, Rn. 159; BaFin, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz 2021, Ziff. 3.2.

51 Vgl. Roth, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, S. 125 Rn. 122 ff.; zudem Kaetzler, in: Zentes/Glaab, GwG, § 7 Rn. 51 m. w. N.

Eine gleichzeitige Funktionswahrnehmung in der Rechtsabteilung ist grundsätzlich möglich. Sofern die Rechtsabteilung auf „Marktseite“ tätig wird, sind hier jedoch auch Interessenkollisionen evident und müssen durch geeignete organisatorische Maßnahmen ausgeschlossen werden; bei größeren Einheiten sowie bei Kernverpflichteten wie größeren Kreditinstituten oder Versicherungsgesellschaften ist eine gleichzeitige Einbindung in die Rechtsabteilung in fachlicher Hinsicht generell untunlich. Eine solche kann wie erörtert selbstverständlich in rein disziplinarischer oder organisatorischer Hinsicht erfolgen, solange die Bereichsautonomie nicht beeinträchtigt ist. **69**

In kleineren Unternehmen, insbesondere außerhalb des Finanzsektors, ist eine gleichzeitige Wahrnehmung einer Funktion als Syndikusanwalt jedoch noch weit verbreitet. Hiermit möglicherweise einhergehende Interessenkollisionen verantwortet der Geldwäschebeauftragte in eigenem Risiko, sofern nicht ein „Delegationsverschulden“ vorliegt, bei dem eine entsprechende Haftung des zuständigen Geschäftsleiters aufgrund mangelhafter Geschäftsorganisation fortbesteht. Dies wird – außerhalb des Finanzsektors – bei kleinen Unternehmen jedoch in der Regel zu verneinen sein. **70**

Allerdings ist hierbei zu beachten, dass Syndikusanwälte als Rechtsanwälte gemäß § 2 Abs. 1 Nr. 10 GwG selbst Geldwäscheverpflichtete sind, sofern sie in einem Katalogmandat tätig sind. Hierdurch entstehen Überlappungen der Verpflichtetenkreise, die im Unternehmen durch gezielte Maßnahmen geregelt werden müssen. Nach einer vermeintlich klarstellenden Abgrenzung zu den Pflichtenkreisen des Syndikusanwalts in § 10 Abs. 8a GwG, wonach bei der Wahrnehmung der Pflichten bei den allgemeinen Kundensorgfaltspflichten auf das Unternehmen, nicht den Syndikusanwalt, abzustellen sei, entstand die Frage, ob dies auch für die Sicherungsmaßnahmen und die Risikoanalyse gelte. Richtigerweise wird hierbei auf den Rechtsgedanken des § 6 Abs. 3 GwG abzustellen sein, der Ähnliches für die Sicherungsmaßnahmen regelt. Für Risikoanalysen nach § 5 GwG ist dies allerdings offen; hier sind pragmatische Lösungen gefragt. Wichtig ist, dass der Syndikusrechtsanwalt Tätigkeiten für andere Mandanten als seinen Arbeitgeber genau von seiner Tätigkeit für das Unternehmen abgrenzt. **71**

Dem Geldwäschebeauftragten sind nach Gesetz wie genannt „ausreichende Befugnisse einzuräumen und insbesondere Zugang zu allen Informationen einzuräumen, die zur Wahrnehmung seiner Aufgabe notwendig sind“ (§ 7 Abs. 5 Satz 3 und 4 GwG). **72**

In der Praxis verbirgt sich hinter dieser leichtfüßig anmutenden Anordnung des Gesetzes oftmals die sehr komplexe Folgefrage, ob dem Geldwäschebeauftragten eigene Entscheidungsbefugnisse, z. B. zum Abbruch oder Beendigung einer Geschäftsbeziehung und hiermit kumulierende Weisungsrechte zustehen sollen. Während der „normale Compliance-Beauftragte“ oftmals durch Festschreibung einer entsprechenden Delegation die Frage in seinem Arbeitsvertrag klärt, ist bei dem Pflichtenkatalog des Geldwäschebeauftragten (aufgrund der Haftung, siehe **73**

hierzu unten → Rn. 130 ff.) der gewerberechtliche Einschlag der Vorschrift des § 7 GwG zu berücksichtigen.

- 74 Aus Sicht der Geldwäschebeauftragten wird hierzu natürlich oftmals angemerkt, dass das Bestehen von Weisungsrechten, insbesondere Kündigungsrechten, in einer Geschäftsbeziehung zu einer deutlich erweiterten Haftung führt. In der Kreditwirtschaft haben sich hierzu – nach langem Ringen – mittlerweile sachgerechte Verwaltungspraxen herausgebildet: Das Bundesaufsichtsamt für das Kreditwesen (BAKred) hat in seiner Verlautbarung vom 30.3.1998 an die Kreditinstitute, dort Teilziffer 35, noch gefordert, dass ein Geldwäschebeauftragter beispielsweise mit entsprechenden Kündigungsrechten gegenüber Dritten ausgestattet sein müsse. Die entsprechende Verlautbarung ist mittlerweile durch Rundschreiben 2/2009 vom 13.1.2009 aufgehoben. Nach heute überwiegender Praxis werden Geldwäschebeauftragte mit solchen, über das eigene Tätigkeitsfeld hinausgehenden Kompetenzen nicht mehr ohne eine ausdrückliche Delegation durch die Geschäftsleitung ausgestattet sein. Außerhalb des Finanzsektors ist eine entsprechende Kompetenz in der Praxis kaum vorzufinden. Eine Delegation entsprechender Rechte ist mithin möglich, aber nicht mehr zwingend notwendig. Dies hat die moderne Verwaltungspraxis mittlerweile so aufgegriffen. Die Entscheidung über den Abbruch einer Geschäftsbeziehung sei lediglich „unter Einbeziehung der Geschäftsleitung zu treffen“.⁵²
- 75 Anders gestaltet sich die Frage der Weisungsbefugnis im Unternehmen. Hier wird anzunehmen sein, dass dem Geldwäschebeauftragten jedenfalls hinreichende Weisungsbefugnisse zur Erfüllung seiner Aufgaben zu gewähren sind;⁵³ die Auslegungs- und Anwendungshinweise der BaFin verlangen allerdings lediglich die Kompetenz, dass dem Geldwäschebeauftragten seine Aufgabenwahrnehmung „mit Nachdruck“ ermöglicht werden soll. Nach hiesigem Verständnis schließt dies innerbetriebliche Weisungsbefugnisse ein.
- 76 Darüber hinausgehende Kompetenzen zum Eingreifen in innerbetriebliche Abläufe können dem Geldwäschebeauftragten mithin eingeräumt werden. Ein ausdrückliches gewerberechtliches Erfordernis hierzu ergibt sich aus § 7 Abs. 5 Satz 3 GwG jedoch nicht.

5. Aufgaben des Geldwäschebeauftragten

- 77 Wie oben dargelegt, entwickelte sich das Aufgabenspektrum des Geldwäschebeauftragten historisch stets weiter. Nach dem Gesetz ist er zentraler Ansprechpartner für sämtliche Fragen der Geldwäscheprävention, nicht nur für Behörden, sondern auch für Mitarbeiter und die Geschäftsleitung. Wie oben geschildert, hat

52 Vgl. DK, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz 2014, Zeile 85, S. 60.

53 Die bisherige Kommentarliteratur schweigt sich hierzu aus, vgl. *Herzog*, in: *Herzog*, GwG, § 7 Rn. 18.

sich der historische Aufgabenbereich des Geldwäschebeauftragten hin zu einem modernen „Risikomanager“ entwickelt.

In der Finanzindustrie gibt es seit langem typische „Tätigkeitskataloge“, die die Pflichtenkreise jedenfalls im Finanzsektor gut umreißen.⁵⁴ **78**

Für Unternehmen außerhalb des Finanzsektors können die Tätigkeits- und Pflichtenkataloge der Finanzwirtschaft jedenfalls dahingehend herangezogen werden, dass die folgend dargestellten Pflichten und Tätigkeiten von Geldwäschebeauftragten, jedenfalls dem Grunde nach, hier jedoch industrieabhängig, zu erfüllen sind. Auch hier ist die Tätigkeit des Geldwäschebeauftragten jedoch sehr stark vom Sektor bzw. der Industrie des jeweiligen Verpflichteten abhängig. So treten außerhalb des Finanzsektors insbesondere vertriebsbezogene Risiken, die erfasst und gemanagt werden wollen, Lieferungen und Leistungen und deren Risiken sowie weitere Faktoren hinzu, die die Risikolage mit Blick auf Geldwäsche- und Terrorismusfinanzierung beeinträchtigen können, welche ggf. mit ganz eigenen Sicherungsmaßnahmen gemanagt und überwacht werden wollen. Dem Grunde nach kann sich ein Geldwäschebeauftragter außerhalb des Finanzsektors aber an den unten dargestellten Richtlinien orientieren: **79**

a) Risikoanalyse

Gem. § 5 GwG haben Verpflichtete eine Risikoanalyse zu erstellen. Hierbei sind die Risiken der Geldwäsche für das konkrete Unternehmen individuell zu erheben und zu bewerten. Diese Aufgabe, zumindest jedoch die Verantwortung hierfür, kommt in der Regel dem Geldwäschebeauftragten zu. **80**

Da die Durchführung der Risikoanalyse gem. § 5 GwG sozusagen den „Nukleus“ für Sicherungsmaßnahmen nach § 6 GwG darstellt, kommt dieser Funktion in den letzten Jahren erhebliche Aufmerksamkeit – auch aus Perspektive der Wirtschaftsprüfer – zu. **81**

In der Verwaltungspraxis haben sich zahlreiche Anforderungen zur Erstellung der Risikoanalyse herausgeprägt.⁵⁵ **82**

b) Sicherungsmaßnahmen

Der Geldwäschebeauftragte ist ferner verpflichtet, basierend auf den Ergebnissen der Risikoanalyse, risikoangemessene interne Grundsätze und Verfahren zur Verhinderung von Geldwäsche und Terrorismusfinanzierung zu schaffen. Dies umfasst die Erstellung und Aktualisierung von internen Organisations- und Arbeitsanweisungen für den jeweiligen Verpflichteten, z. B. durch geeignete Richtlinien, Arbeitsplatzbeschreibungen, ablauf- und aufbauorganisationstechnische **83**

⁵⁴ BaFin, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz 2021, Ziff. 2.3; DK, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz 2014, Zeile 84; Roth, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, S. 129 ff. m. w. N.

⁵⁵ Vgl. Zentes, in: Zentes/Glaab, GwG, § 5 Rn. 1 ff. mit zahlreichen weiteren Nachweisen.

Maßnahmen. Letztere sind selbstverständlich in Absprache mit der Geschäftsleitung zu erstellen und durch diese in Kraft zu setzen.

- 84** Innerhalb größerer Einheiten, insbesondere in der Finanzwirtschaft, ist der Geldwäschebeauftragte auch für die Selbstorganisation der entsprechenden Abteilung zuständig. Innerhalb der Kompetenzen, die Gesetz und Geschäftsleitung dem Geldwäschebeauftragten zuweisen, ist eine Weiterdelegation an nachgeordnete Mitarbeiter selbstverständlich möglich. Soweit nicht die Residualverantwortung des zuständigen Geschäftsleiters greift, ist der Geldwäschebeauftragte jedoch als Beschützer- und Überwachergarant qua Gesetz auch für solche Aufgaben weiter verantwortlich, die er im Wege der Delegation auf nachgeordnete Mitarbeiter übertragen hat.
- 85** Vom Geldwäschebeauftragten wird hierbei selbstverständlich nicht erwartet, dass er dafür einzustehen hat, dass sämtliche Fälle von Geldwäsche beim Verpflichteten unterbleiben. Er hat vielmehr durch geeignete und risikoangemessene Maßnahmen ein geldwäscheaverses Umfeld im Unternehmen zu schaffen, welches risikoangemessen ist. Im Übrigen kann auf die einschlägigen Kommentierungen zu § 6 GwG verwiesen werden.

c) Antizipation und Implementierung neuer rechtlicher und verwaltungspraktischer Vorschriften

- 86** Der Geldwäschebeauftragte fungiert ferner in seinem eigenen Verantwortungsbereich als „Radarstation“ für neue gesetzliche Anforderungen. Die genannte Pflicht besteht in der Finanzindustrie übrigens parallel zur inhaltlich gleichlaufenden Pflicht für MaRisk-Compliance-Beauftragte, die gemäß Ziff. 4.2. der MaRisk eine entsprechende Beobachtungs- und Organisationspflicht trifft.
- 87** Außerhalb des Finanzsektors besteht eine solche Beobachtungspflicht selbstverständlich ebenfalls. Hier wird sie – mangels Anknüpfung an § 25a KWG – auf allgemeine Legalitätspflichten⁵⁶ gestützt. Wie auch hinsichtlich der internen Aufbau- und Ablauforganisation müssen etwaige Änderungen in Übereinkunft mit der Geschäftsleitung entwickelt und durch diese im Unternehmen formell umgesetzt werden.
- 88** Insbesondere wegen der hohen Geschwindigkeit von Reformen im Geldwäscherecht, der Überlappung verschiedener Aufsichtsbehörden und weiterer normsetzender Instanzen im Geldwäscherecht und des schieren Volumens neuer Regulierung darf diese Aufgabe in ihrer Komplexität nicht unterschätzt werden. Praktische Hilfe kommt – da wesentliche und zeitnahe Unterstützung insbesondere bei Rechtsänderungen durch die Verwaltungsbehörden außerhalb des Finanzsektors nicht zu erwarten ist – von Verbänden, Dienstleistern und Auslagerungsunternehmen, die die „Radarstation“ unterstützen.

⁵⁶ Vgl. Ziff. 4.1.3 DCGK; ebenso die Kommentierungen zu § 93 AktG.

d) Kontinuierliche Überwachung von Geschäftsbeziehungen/„Monitoring“

Den Geldwäschebeauftragten trifft die in § 10 Abs. 1 Nr. 5 GwG normierte Pflicht, die bestehenden Geschäftsbeziehungen, einschließlich aller Transaktionen, kontinuierlich zu überwachen. **89**

Während innerhalb der Finanzindustrie (vgl. § 25h Abs. 2 KWG) im Wesentlichen elektronische Datenverarbeitungssysteme zur kontinuierlichen Überwachung eingesetzt werden müssen, existiert eine solche Pflicht außerhalb des Finanzsektors nicht. **90**

Ob mit oder ohne EDV-gestützten Systemen muss der Geldwäschebeauftragte jedenfalls in der Lage sein, Indizien und Indikatoren zu bestimmen, wann er Transaktionen oder Geschäftsbeziehungen als risikobehaftet ansehen möchte bzw. von derart gestiegenen Geldwäscherisiken ausgehen muss, dass eine Geschäftsbeziehung beendet und/oder Verdachtsmeldungen abgegeben werden. Die Organisation einer entsprechenden Struktur ist eine weitere Kernaufgabe eines Geldwäschebeauftragten. **91**

Es ergibt sich aus der Natur der Aufgabe, dass diese enorm von der Industrie, der Größe des Unternehmens und der Zahl der zu überwachenden Kunden- und Geschäftsbeziehungen sowie der geschäftlichen Tätigkeit des Verpflichteten abhängt. **92**

Hinsichtlich der Risikoträchtigkeit für den Verpflichteten und den Geldwäschebeauftragten selbst handelt es sich hierbei um die wohl wichtigste Tätigkeit des Geldwäschebeauftragten, der naturgemäß bei Geldwäschefällen im Unternehmen in den Fokus der untersuchenden Behörden gerät und sich nicht selten rechtfertigen, in Extremfällen sogar gegen strafrechtliche Verfolgung verteidigen muss. **93**

In regelmäßigen Abständen hat sich der Geldwäschebeauftragte zudem davon zu überzeugen, dass die gewählten Monitoringsysteme wirksam sind. Der Geldwäschebeauftragte kann zur Überwachung eigene risikobasierte Prüfungshandlungen durchführen und/oder Prüfungshandlungen bzw. Prüfungsergebnisse durch Dritte (interne oder externe Revision) in Bezug nehmen und auswerten. **94**

e) Verdachtsfälle und Verdachtsmeldewesen/Unstimmigkeitsmeldungen

Wie oben anhand der historischen Herleitung berichtet, ist die Pflicht des Geldwäschebeauftragten zur Vornahme von Verdachtsmeldungen die historisch älteste. Zweifelhafte oder ungewöhnliche Sachverhalte muss der Geldwäschebeauftragte untersuchen; dies im Übrigen unabhängig davon, ob eine Transaktion angetragen, durchgeführt oder bereits abgewickelt ist. Der Geldwäschebeauftragte bearbeitet die Verdachtsfälle intern wie extern, stellt möglicherweise Verdachtsmeldungen und Strafanzeigen und ist erster Ansprechpartner im Institut für Strafverfolgungs- und Polizeibehörden. **95**

- 96 In der Praxis steht dem Geldwäschebeauftragten bei der Beurteilung, ob ein konkreter Sachverhalt oder eine Transaktion im Rahmen einer Verdachtsmeldung nach § 43 GwG zu melden ist, ein – allerdings begrenztes – Einschätzungsermessen zu. Die Literatur ist sich insoweit einig, dass es sich bei einer Verdachtsmeldung nicht um eine Strafanzeige nach § 158 StPO handelt, weshalb der Verdachtsgrad auch geringer als der eines Anfangsverdachts nach § 152 StPO sein muss.⁵⁷ Es ist gerade nicht Aufgabe eines Geldwäschebeauftragten, insbesondere weit in die Möglichkeit einer Bemakelung bzw. sogar in Vortaten hinein zu untersuchen, die möglicherweise mit einer Transaktion oder einer Geschäftsbeziehung in Verbindung stehen könnten.⁵⁸
- 97 Die Meldung hat nach § 43 Abs. 1 GwG unverzüglich, also ohne schuldhaftes Zögern, zu erfolgen. In einer weit beachteten Entscheidung hat das OLG Frankfurt am Main⁵⁹ erhebliche Anforderungen an die Unverzüglichkeit gestellt und einen Geldwäschebeauftragten sogar mit einem Bußgeld belegt.
- 98 Zur Einreichung der Verdachtsmeldungen wurde bei der Financial Intelligence Unit ein eigenes IT-Portal (GoAML) eingerichtet. Die Anlage eines eigenen Profils für jeden Verpflichteten ist auch unabhängig von einer Verdachtsmeldung anzuraten.
- 99 Mit dem Inkrafttreten des Gesetzes zur Umsetzung der Änderungsrichtlinie zur 4. EU-Geldwäscherichtlinie im Jahr 2020 ist neben die Pflicht zur Abgabe einer Verdachtsmeldung die Pflicht zur Abgabe einer Unstimmigkeitsmeldung (§ 23a GwG) getreten. Stellt ein Verpflichteter bei der Prüfung der Eigentümer- und Kontrollstrukturen, insbesondere bei der Überprüfung des wirtschaftlich Berechtigten (§ 3 GwG) fest, dass die im Transparenzregister enthaltenen Eintragungen nicht mit den Ergebnissen des Verpflichteten übereinstimmen, muss – bußgeldbewehrt – eine Unstimmigkeitsmeldung abgegeben werden. Hierdurch wird ein weiterer Pflichtenkreis des Geldwäschebeauftragten begründet, welchen dieser zwar durch Delegation auf andere Mitarbeiter übertragen kann; letzten Endes haftet er jedoch auch für die Abgabe und die inhaltliche Richtigkeit einer solchen Unstimmigkeitsmeldung. Inhaltlich sind kaum praktische Erfahrungen mit Unstimmigkeitsmeldungen vorhanden. Tendenziell wird allerdings zu erwarten sein, dass durch die Prüfpraxis, vor allem im Finanzsektor, zukünftig wesentlich größeres Augenmerk auf die rechtssichere Feststellung wirtschaftlich Berechtigter gelegt werden wird. Hierzu wird es unerlässlich sein, dass die Verpflichteten Zugang zu werthaltigen Informationen über Eigentümer- und Kontrollstrukturen durch qualifizierte Informationsdienstleister erhalten. Anderenfalls läuft die – inhaltlich sicherlich richtige – Rolle des Geldwäschebeauftragten als Wächter über die Transparenz juristischer Personen und rechtlicher Gestaltungen ins Leere.

57 Vgl. Roth, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, S. 137 Rn. 191 m. w. N.

58 Vgl. OLG Frankfurt v. 10.4.2018, 2 Ss-OWi, 1059/2017.

59 Vgl. OLG Frankfurt v. 10.4.2018, 2 Ss-OWi, 1059/2017.

Je nach Schwere des Verdachtsgrades muss der Geldwäschebeauftragte anschließend über den Abbruch einer Geschäftsbeziehung bzw. das Anhalten einer Transaktion entscheiden; wie oben geschildert, geschieht dies allerdings in der Regel mangels entsprechender eigener Weisungs- und Entscheidungsrechte „unter Einbindung“ entsprechend befugter Hierarchieebenen bzw. der Geschäftsleitung. Allerdings genießt der Geldwäschebeauftragte – im Rahmen des Verdachtsmelde- und Prüfwesens – besondere arbeitsrechtliche Privilegien (vgl. hierzu → Rn. 107 ff.). **100**

f) Berichtswesen, Bericht an Geschäftsleitung und Aufsichtsorgan

Nach § 7 Abs. 5 Satz 5 GwG muss der Geldwäschebeauftragte der Geschäftsleitung „unmittelbar“ berichten. In der Finanzindustrie hat sich hierzu eine Verwaltungspraxis verfestigt, wonach der Geldwäschebeauftragte mindestens einmal jährlich einen – schriftlichen – Bericht über seine Tätigkeit, insbesondere über die Risikosituation, etwaige Verdachtsfälle und erfolgte und beabsichtigte Maßnahmen zur Umsetzung der geldwäscherechtlichen Pflichten abgeben muss.⁶⁰ **101**

Neben die periodische Berichterstattungspflicht tritt selbstverständlich eine anlassbezogene Berichterstattung, die „Ad hoc“-Meldung an die Geschäftsleitung. **102**

Von besonderer praktischer Bedeutung war in den vergangenen Jahren die Frage, ob und inwieweit der Geldwäschebeauftragte – ähnlich dem Compliance Officer – bei konkretem Fehlverhalten oder bei Organisationsverschulden der Geschäftsleitung direkt an den Aufsichtsrat zu berichten habe. Mittlerweile prägt sich jedenfalls im Finanzsektor eine Verwaltungspraxis heraus, wonach dem Aufsichtsorgan nicht nur ein eigenes Auskunftsrecht gegenüber dem Geldwäschebeauftragten zusteht, sondern nach der in extremen Fällen, z. B. bei dauerhaftem Widersetzen der Geschäftsleitung gegen Empfehlungen des Geldwäschebeauftragten oder bei strukturellen Defiziten, der Geldwäschebeauftragte sich direkt und unmittelbar an das Aufsichtsorgan wenden darf.⁶¹ Lediglich die Form der Einbeziehung der Geschäftsleitung ist noch nicht abschließend geklärt. Aufgrund allgemeiner Legalitätserwägungen und der gesetzlich ausgeprägten Stellung des Geldwäschebeauftragten verhält sich dies für Verpflichtete außerhalb des Finanzsektors ähnlich. **103**

g) Mitarbeiterschulungen

Der Geldwäschebeauftragte ist ferner verpflichtet, die vom Gesetz in § 6 Abs. 2 Nr. 6 GwG vorgesehene Unterrichtungspflicht gegenüber den Mitarbeitern des Verpflichteten zu erfüllen. **104**

60 Vgl. Roth, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, S. 136 Rn. 182 mit Verweis auf die Auslegungs- und Anwendungshinweise der BaFin zum Geldwäschegesetz aus 2021, Ziff. 3.2; vgl. zum Berichtswesen eingehend auch Kaetzler, in: Zentes/Glaab, GwG, § 7 Rn. 111 ff.

61 Vgl. Kaetzler, in: Zentes/Glaab, GwG, § 7 Rn. 118.

- 105** Hierbei hat der Geldwäschebeauftragte die relevanten Geschäftsbereiche und Mitarbeiter des Unternehmens mit Blick auf die Risiken, etwaige Stereotypen und Pflichten zur Verhinderung von Geldwäsche und Terrorismusfinanzierung zu schulen. Der Geldwäschebeauftragte kann die Schulungen selbst vornehmen oder delegieren/auslagern.
- 106** Auch über die Schulungspflicht hinaus steht der Geldwäschebeauftragte als „Vertrauensmann“ den Mitarbeitern des Verpflichteten als Ansprechpartner und „Berater“ zur Verfügung.⁶²

6. Arbeitsrechtlicher Schutz des Geldwäschebeauftragten und Teilausnahme vom Direktionsrecht des Arbeitgebers

- 107** Im Hinblick auf die besondere Interessenlage zwischen den Verpflichteten als Arbeitgeber und dem Geldwäschebeauftragten als Stellvertreter staatlicher Interessen im Unternehmen genießt der Geldwäschebeauftragte mittlerweile erhebliche arbeitsrechtliche Sonderrechte. Mit dem Umsetzungsgesetz zur 4. EU-Geldwäscherichtlinie verbesserte sich der Status des Geldwäschebeauftragten 2017 in dieser Hinsicht deutlich.
- 108** Schon seit langem hatte in Deutschland und Europa zuvor eine Diskussion darüber geschwelt, ob der Geldwäschebeauftragte nicht – ähnlich dem Datenschutzbeauftragten – einen höheren arbeitsrechtlichen Schutz in Anspruch nehmen können solle. Mit dem Umsetzungsgesetz zur 4. EU-Geldwäscherichtlinie wurde der arbeitsrechtlich privilegierte Status des Geldwäschebeauftragten (und selbstverständlich seines Stellvertreters) gewerberechtlich schließlich festgesetzt. Lediglich im Finanzsektor herrschte zuvor bereits ein gewisser faktischer Schutz des Geldwäschebeauftragten, da die Abberufung desselben den Aufsichtsbehörden angezeigt und Gründe transparent gemacht werden mussten.⁶³ Schließlich wurde in Erwägungsgrund 41 und Art. 38 der 4. EU-Geldwäscherichtlinie ein Benachteiligungsschutz in arbeitsrechtlicher Hinsicht formalisiert. Ziel des Gesetzgebers bei der Umsetzung der 4. EU-Geldwäscherichtlinie war es, den Schutz des Geldwäschebeauftragten in arbeitsrechtlicher Hinsicht dem des Datenschutzbeauftragten gleichzustellen.⁶⁴ Flankiert wird der arbeitsrechtliche Schutz durch eine Ausnahme vom Direktionsrecht und ein allgemeines Benachteiligungsverbot.

a) Sonderkündigungsschutz

- 109** Der in § 7 Abs. 7 GwG enthaltene Sonderkündigungsschutz ist stark an den Regelungen für den Datenschutzbeauftragten orientiert. Wie auch beim Datenschutzbeauftragten beschränkt sich der Sonderkündigungsschutz – ebenso wie

62 Vgl. Roth, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, S. 140 Rn. 212 f.

63 Vgl. DK, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz 2014, Zeile 83.

64 Vgl. Gesetzesbegründung in BT-Drs. 18/11555, S. 113 ff.

das Benachteiligungsverbot – auf solche Kündigungsgründe, die unmittelbar aus der Funktion als Geldwäschebeauftragter bzw. als Stellvertreter „herrühren“. Für „freiwillig“ bestellte Geldwäschebeauftragte gilt der Sonderkündigungsschutz nicht; ebenso für die nicht ausdrücklich als Geldwäschebeauftragter oder Stellvertreter bestimmten Mitarbeiter entsprechender Abteilungen.

Bei der Frage, ob eine Kündigung aus der Funktion als Geldwäschebeauftragter herrührt, ist insbesondere in Fällen, in denen Kündigungsgründe aus einer anderen Tätigkeit herrühren, aber in die Funktion als Geldwäschebeauftragter hineinragen, grundsätzlich anzudenken, eine Teilkündigung auszusprechen, die die Funktion des Geldwäschebeauftragten ggf. unberührt lässt.⁶⁵ Sofern ein Geldwäschebeauftragter aber einen ganz wesentlichen Teil seiner Arbeitszeit der Funktion widmet, die Stellung des Geldwäschebeauftragten der Tätigkeit des betroffenen Arbeitnehmers also „das Gepräge“ gibt, sind die Kündigungsmöglichkeiten des Arbeitgebers allerdings deutlich erschwert.⁶⁶ **110**

Auch für den externen Geldwäschebeauftragten (siehe zur Ausgestaltung einer solchen Funktion sogleich → Rn. 121 ff.) gilt der Sonderkündigungsschutz nicht. Hier werden entsprechende Erwägungen jedoch nach §§ 242, 315 BGB in den Auslagerungs- bzw. Geschäftsbesorgungsvertrag hineinzulesen sein. **111**

b) Benachteiligungsverbot

Nach dem Gesetzeswortlaut darf dem Geldwäschebeauftragten und seinem Stellvertreter wegen der Erfüllung seiner Aufgaben keine Benachteiligung im Beschäftigungsverhältnis entstehen (§ 7 Abs. 7 Satz 1 GwG). Hinter diesem generellen Benachteiligungsverbot steht die Erwägung, dass der Gesetzgeber den Geldwäschebeauftragten in seiner Unabhängigkeit und vor Nachteilen und Repressionen durch den Arbeitgeber schützen will.⁶⁷ Das Benachteiligungsverbot erstreckt sich auf das gesamte Tätigkeitsfeld des Geldwäschebeauftragten und des Stellvertreters innerhalb ihrer Funktion. **112**

Der Begriff der „Benachteiligung“ ist weit auszulegen; zur Begriffsbestimmung können die allgemeinen arbeitsrechtlichen Grundsätze herangezogen werden.⁶⁸ **113**

Hinter der Norm steht auch die – regulatorische – Erwartung, dass der Geldwäschebeauftragte seine Funktion „robust“ ausüben kann. Sollten entsprechende Ungleichbehandlungen evident werden, kann der Geldwäschebeauftragte dies einer Ombudsstelle bei der BaFin mitteilen. Dieselbe hat in der Konsequenz die in § 51 GwG genannten Möglichkeiten (in Extremfällen sicherlich durch Ermessensreduktion eine Pflicht), auf die entsprechenden Verpflichteten hinzuwirken. **114**

65 Vgl. – für eine ähnlich gelagerte Konstellation beim Datenschutzbeauftragten – BAG, DB 2007, 1198.

66 Vgl. Kaetzler, in: Zentes/Glaab, GwG, § 7 Rn. 147 ff. m. w. N.

67 Vgl. Gesetzesbegründung in BT-Drs. 18/11555, S. 114.

68 Vgl. Schlachter, in: ErfK ArbR, AGG § 3 Rn. 2 ff.

c) Ausnahme vom Direktionsrecht

- 115** In den Gesetzgebungsverfahren zur Umsetzung der 4. EU-Geldwäscherichtlinie war zwar beabsichtigt, die Stellung des Geldwäschebeauftragten möglichst nah derjenigen des Datenschutzbeauftragten anzugleichen. Anders als der Datenschutzbeauftragte ist der Geldwäschebeauftragte allerdings nicht im Rahmen seiner gesamten Tätigkeiten vom Direktionsrecht befreit.
- 116** Der Grund hierfür liegt darin, dass der Datenschutzbeauftragte eine – auch nominal – besondere öffentlich-rechtliche Stellung trägt, die – anders als beim Geldwäschebeauftragten – weiter mit zudem ausdrücklich auch so benannten hoheitlichen Funktionen durchsetzt ist. Der Geldwäschebeauftragte ist hingegen nur dann vom Direktionsrecht ausgenommen, „soweit [er] die Erstattung einer Meldung nach § 43 Abs. 1 beabsichtigt oder ein Auskunftersuchen der Zentralstelle für Finanztransaktionsuntersuchungen nach § 30 Abs. 3 beantwortet“.
- 117** In diesem historischen „Kernbereich“ des Tätigwerdens des Geldwäschebeauftragten manifestieren sich die unterschiedlichen Interessen zwischen Arbeitgeber und Geldwäschebeauftragten besonders deutlich.
- 118** Nach der funktionalen Auslegung des Geldwäschegesetzes erstreckt sich die Weisungsausnahme auf Vorbereitungs- und Untersuchungshandlungen des Geldwäschebeauftragten im Vorfeld der Prüfungen; anderenfalls liefe der Sinn des Gesetzes leer.
- 119** Auch hinsichtlich der Ausnahme vom Direktionsrecht im Hinblick auf „Auskunftersuchen“ sind Vorbereitungshandlungen derselben mit von der Privilegierung erfasst. Inhaltlich beschränkt sich die Ausnahme vom Direktionsrecht allerdings auf förmliche Auskunftersuchen nach § 30 Abs. 3 GwG; „informelle“ Auskunftersuchen und Auskunftersuchen anderer Behörden als solche der FIU sind nicht umfasst. Diesbezüglich können Geschäftsleiter also noch Weisungen erteilen.
- 120** Die Weisungsfreiheit erstreckt sich – innerhalb des eng umfassten Anwendungsbereiches – auch auf die Stellvertreter und die Mitarbeiter des Geldwäschebeauftragten. Dies ist aus einer Parallelschau mit dem Datenschutzbeauftragten abzulesen.

7. Auslagerung der Funktion

- 121** Die Funktion des Geldwäschebeauftragten sowie des Stellvertreters kann – allerdings nur unter engen gesetzlichen Voraussetzungen – ausgelagert werden. Gegenüber der allgemeinen Auslagerungsfähigkeit nach § 6 Abs. 7 GwG gelten jedoch für die Auslagerung der Funktion des Geldwäschebeauftragten einige rechtliche Besonderheiten. Diese sind in § 7 Abs. 5 Satz 1 GwG niedergelegt; teilweise ergeben dieselben sich aber aus Nachbarnormen innerhalb des Geldwäschegesetzes.

Eine Auslagerung der Funktion des Geldwäschebeauftragten auf eine geeignete (mithin fachlich geeignete, mit Leitungserfahrung versehene, zuverlässige → Rn. 48 ff.) Person ist nach – formloser – schriftlicher Anzeige mit mindestens zwei Wochen Vorlauf möglich. **122**

Eine bloße Übersendung des Auslagerungsvertrages reicht hierzu i. d. R. nicht aus; im Rahmen des Finanzsektors ist es mittlerweile durch entsprechende Verwaltungspraxis klargestellt.⁶⁹ Vielmehr soll genau erläutert werden, welche Sicherungsmaßnahmen aufgrund des konkreten Geschäftsmodells des auslagernden Unternehmens erforderlich sind und wie die Ablauforganisation des Auslagerungsunternehmens mit dem des auslagernden Unternehmens zusammenspielt.⁷⁰ **123**

Die Übertragung der Funktionen und Aufgaben des Geldwäschebeauftragten erfolgt über einen Auslagerungsvertrag. Dieser ist in der Grundfassung ein „Service Level Agreement“, also ein Geschäftsbesorgungsvertrag, der dienstvertragliche und werkvertragliche Elemente enthält. Zwar sind nach § 6 Abs. 7 GwG „sämtliche Sicherungsmaßnahmen“ auslagerungsfähig. Dies stimmt jedoch nur zum Teil. Aufgrund eines Missverständnisses in der Gestaltung der EU-Geldwäscherichtlinie ist z. B. das laufende „Monitoring“ in einer Geschäftsbeziehung, insbesondere von Kundendaten, nicht ohne Weiteres auslagerungsfähig, sondern muss beim auslagernden Verpflichteten verbleiben. Hier ist der Gesetzgeber dringend gefordert. **124**

Wie in der Kreditwirtschaft auch, muss sich der Verpflichtete auch außerhalb des Finanzsektors gewisse Steuerungsmöglichkeiten zurückbehalten. Grund hierfür ist die Residualverantwortlichkeit des zuständigen Mitglieds der Leitungsebene (§ 1 Abs. 15 GwG), die nicht auf einen externen Dienstleister „wegdelegiert“ werden kann. **125**

Insbesondere müssen entsprechende Auslagerungsverträge Überwachungsmöglichkeiten, ein detailliertes Reporting, Überwachungs- und Prüfrechte, einschließlich Zutrittsrechten für den Verpflichteten und seine Prüfer, mithin also auch für die Aufsichtsbehörden, vorsehen. Der zuständigen Behörde (§ 50 GwG) müssen zudem Kontrollmöglichkeiten beim Dienstleister eingeräumt werden. **126**

Auf die Anzeige hin hat die zuständige Behörde die Möglichkeit, die Auslagerung zu untersagen, insbesondere wenn das Auslagerungsunternehmen/der externe Dienstleister nicht über die erforderliche Zuverlässigkeit oder Sachkunde verfügt. **127**

Hinsichtlich besonderer Verschwiegenheitspflichten sind die Verpflichtungen nach der Datenschutzgrundverordnung über entsprechende Datenschutzklauseln **128**

⁶⁹ Vgl. BaFin, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz 2021, Ziff. 3.10.

⁷⁰ Vgl. hierzu ausführlich Roth, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, S. 113 Rn. 45.

auf das Auslagerungsunternehmen zu erstrecken. Gleiches gilt für Geschäfts-/Bankgeheimnisse, wo anwendbar.

- 129** Allerdings verbleibt auch bei Bestellung eines externen Geldwäschebeauftragten die Residualverantwortung für die Erfüllung der Sicherungsmaßnahmen gem. § 6 Abs. 7 Satz 4 GwG beim Verpflichteten selbst. Entsprechend ist eine – engmaschige – Überwachung des externen Geldwäschebeauftragten nach Risikogesichtspunkten anzuraten. Innerhalb der Kreditwirtschaft bestehen hierzu detaillierte „Best Practices“;⁷¹ außerhalb des Finanzsektors existieren solche „Best Practices“ nicht. Hier werden die zuständigen Aufsichtsbehörden außerhalb des Finanzsektors in den kommenden Jahren eine entsprechende Verwaltungspraxis entwickeln müssen.

8. Haftung

- 130** „Der Geldwäschebeauftragte ist für die Einhaltung der geldwäscherechtlichen Vorschriften zuständig; [...]“.
- 131** Die in § 7 Abs. 1 Satz 2 Hs. 1 GwG genannte Zuständigkeitsregelung deutet an, dass der Geldwäschebeauftragte möglicherweise besondere Obhutspflichten wahrnehmen muss. Es liegt nahe, dass er in strafrechtlicher Hinsicht möglicherweise Beschützer- und zu einem kleineren Anteil auch Überwachergarant ist.⁷² Hinsichtlich der besonderen persönlichen Merkmale i. S. d. § 14 StGB liegen solche sicherlich gehäuft beim Geldwäschebeauftragten vor, wenn es um entsprechende Organisations- und Funktionsverstöße geht. Ob aus der vorgenannten Vorschrift eine harte, gesetzliche Garantenstellung „herauszulesen“ ist, wird abzuwarten bleiben.
- 132** Die Frage der persönlichen Haftung des Geldwäschebeauftragten ist nicht neu. Schon im Jahre 1995 wurde in der Literatur bei der genannten Stellung des Geldwäschebeauftragten diskutiert und diese jedenfalls als persönliches Risiko für denselben wahrgenommen.⁷³
- 133** Durch die im Rahmen der Umsetzung der 4. EU-Geldwäscherichtlinie eingefügte verschärfende Formulierung kommt eine Garantenstellung jedenfalls in Betracht. Zu beachten ist allerdings, dass – wenn man eine solche Annahme – die Residualverantwortlichkeit der Leitungspersonen hierdurch nicht überlagert oder präkludiert werden darf. Das Nähere werden die Gerichte in Zukunft klären müssen.

71 Vgl. Roth, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, S. 117 mit zahlreichen Beispielen.

72 Vgl. Kaetzler, in: Zentes/Glaab, GwG, § 7 Rn. 26 m. w. N.

73 Otto, wistra 1995, 323.

In arbeitsrechtlicher Hinsicht gelten die allgemeinen Haftungsregelungen für Arbeitnehmer. Bei etwaigen verursachten Schäden kommen die Prinzipien des „innerbetrieblichen Schadensausgleichs“⁷⁴ zum Tragen. **134**

Erste Ordnungswidrigkeitenverfahren gegen Geldwäschebeauftragte im Zusammenhang mit Pflichtverstößen⁷⁵ verdeutlichen das deutlich erhöhte Risiko des Geldwäschebeauftragten im Umgang mit seinen Aufgaben. In der Konsequenz ist den Geldwäschebeauftragten dringend anzuraten, die durch gesetzliche Aufgabenverteilung vorgesehene „Globaldelegation“ durch eine möglichst genaue Definition des Verantwortungskreises im Arbeitsvertrag oder in entsprechenden Stellenbeschreibungen zu begrenzen. **135**

Während beim „normalen“ Compliance Officer mangels gesetzlicher Vorgaben einzig die Delegation durch die residual verantwortlichen Leitungsorgane den Pflichtenkreis bestimmt, ist es beim Geldwäschebeauftragten wie oben geschildert mithin anders. Eine Delegation auf den Geldwäschebeauftragten hat mithin nur ausgestaltenden Charakter; die zwingenden gesetzlichen Vorgaben der o. g. Zuständigkeitsbereiche dürfen lediglich ausgeführt, nicht verändert werden. Anderenfalls läge ein Delegationsverschulden beim zuständigen Leitungsorgan vor. **136**

9. Der Geldwäschebeauftragte – gefangen zwischen hoheitlicher und unternehmerischer Tätigkeit?

Aus den vorgenannten Erwägungen wird deutlich, dass den Geldwäschebeauftragten eine besondere Funktion innerhalb des verpflichteten Unternehmens trifft. Wenngleich seine Tätigkeit an die des Datenschutzbeauftragten angelehnt ist, entspricht sie ihm – mangels ausdrücklicher Beleihung – nicht vollumfänglich. **137**

Der Geldwäschebeauftragte wird wie geschildert teils in hoheitlichem, teils im privatrechtlichen Interesse tätig. Während in den 1990ern und frühen 2000er Jahren der Schwerpunkt der Tätigkeit und der Verantwortung des Geldwäschebeauftragten noch darin gesehen wurde, Straftaten des Unternehmens, mithin des Verpflichteten abzuwehren, treten spätestens seit der Erweiterung des Pflichtenkatalogs um die Unstimmigkeitsanzeigen klare öffentlich-rechtliche, ordnungsrechtliche, ggf. sogar polizeirechtliche Aufgaben hinzu. Rolle, Pflichtenkreis und gesetzliche Stellung im Unternehmen haben sich – wie geschildert – sehr weit von einem „MLRO“ fortentwickelt; die Abwehr von Strafbarkeitsrisiken und Schäden für das eigene Unternehmen steht ausweislich der hinzugeetretenen erweiterten Anzeigepflichten nicht mehr im Mittelpunkt des Handelns. **138**

Nicht selten gerät ein Geldwäschebeauftragter hierdurch in einen Entscheidungskonflikt, der zwar durch die geschilderte arbeitsrechtliche Sonderstellung **139**

⁷⁴ Vgl. *Preis/Greiner*, in: *ErfK ArbR*, BGB, § 619a Rn. 10 ff.

⁷⁵ OLG Frankfurt, Beschl. v. 10.4.2018, 2 Ss-OWi 1059/17 mit Besprechung von *Komma*, CB 2019, 197.

Teil 3 Besondere Aufgaben und Anwendungsfelder

etwas abgefedert werden kann. Im Grunde genommen wird der Geldwäschebeauftragte durch die zahlreichen öffentlich-rechtlichen Durchsetzungen seiner Rolle oftmals gegen das Unternehmensinteresse entscheiden müssen.

- 140** Ob ein Tätigwerden im öffentlichen Interesse zukünftig bei etwaigen Schadensfällen durch Gerichte berücksichtigt werden wird, darf auch außerhalb der Haftungsfreistellungsnormen des GwG und des allgemeinen Straf- und Ordnungswidrigkeitenrechts abzuwarten bleiben.

23. Kapitel

Geldwäsche-Compliance in Industrie und Handel

I. Einführung in die Geldwäscheprävention

Geldwäsche ist seit Längerem kein exklusives Thema der Finanzindustrie mehr. 1
Gesetzgeberische Aktivitäten, Maßnahmen von Aufsichtsbehörden und nicht zuletzt eine vermehrte öffentliche Berichterstattung rückten den Fokus der Geldwäsche und deren Verhinderung vermehrt auf Unternehmen aus Industrie und Handel. Dies ist nicht zuletzt auch der Erkenntnis der letzten Jahre geschuldet, dass Unternehmen aus Industrie und Handel an Geldwäschehandlungen beteiligt waren, teilweise ohne davon überhaupt Kenntnis erlangt zu haben.

Aufgrund ihrer Relevanz für das System der Geldwäscheprävention sind Industrie- 2
und Handelsunternehmen Regelungsadressaten des Geldwäschegesetzes („GwG“), in dem sie als „Güterhändler“ bezeichnet werden. Das GwG verlangt von seinen Adressaten, den Verpflichteten, die Implementierung zahlreicher Maßnahmen, die zum Ziel haben, Vorgänge im Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung¹ zu erkennen und an die zuständigen Behörden zu melden.²

Die Geldwäsche-Compliance ist daher – anders als andere klassische Compliance-Bereiche wie die Korruptionsprävention – primär darauf ausgerichtet zu 3
verhindern, dass außenstehende Dritte das Unternehmen zu Geldwäschezwecken missbrauchen. Allerdings spielt auch der Aspekt, Straftaten im eigenen Unternehmen zu verhindern, mit Blick auf die leichtfertige Geldwäsche gem. § 261 Abs. 6 StGB eine nicht nur untergeordnete Rolle und muss in ein Geldwäsche-Compliance-System entsprechend aufgenommen werden.

1. Begriff und Methoden der Geldwäsche

Der Begriff der Geldwäsche soll ursprünglich auf den berühmten amerikanischen Gangsterboss *Al Capone* zurückgehen, der illegal beschafftes Geld aus 4
vornehmlich Glücksspiel, Prostitution, Schutzgelderpressung und illegalem Alkoholhandel in Waschsalons investiert haben soll, um damit seine Einnahmen legal erscheinen zu lassen.³ Dafür schienen Waschsalons prädestiniert, denn sie erwirtschafteten Bargeldumsätze ohne Quittung, Ware oder nachhaltige Leistung und eigneten sich somit hervorragend für Umsatzlegenden und die Vermitt-

1 Das zweite gesetzliche Ziel des GwG, die Verhinderung von Terrorismusfinanzierung, wird in diesem Kapitel nicht gesondert dargestellt. Einen gesonderten Maßnahmenkatalog zur Verhinderung der Terrorismusfinanzierung sieht das GwG auch nicht vor.

2 Entsprechend der „drei Säulen der Geldwäscheprävention“ mit der die Pflichten der Adressaten zusammengefasst werden: Risikomanagement, Kundensorgfaltspflichten und Verdachtsmeldewesen.

3 *Bausch/Voller*, Geldwäsche-Compliance für Güterhändler, S. 1.

schung von bemakeltem mit sauberem Geld.⁴ Die Wortschöpfung „Geldwäsche“ erklärt aber auch bereits bildlich den wesentlichen Kern des Geldwäschevorgangs: „Schmutzige“ Gelder oder Vermögenswerte sollen von ihrer kriminellen Herkunft reingewaschen werden.

- 5 Nach der kriminologischen Definition ist Geldwäsche die Einschleusung kriminell erworbener Vermögenswerte in den legalen Wirtschaftskreislauf unter Verschleierung der wahren Herkunft, um diese zu einem späteren Zeitpunkt als scheinbar legales Vermögen im regulären Geschäftsverkehr zu verwenden.⁵
- 6 Ausgehend von dieser Definition lässt sich die Funktionsweise der Geldwäsche in anschaulicher, wenn auch in etwas simplifizierter Weise, mit dem sog. „Dreiphasenmodell“ erklären.⁶ Die drei Phasen, die in der Regel nacheinander, jedoch auch zeitgleich ablaufen können, werden Einspeisung („Placement“), Verschleierung („Layering“) und Integration („Integration“) genannt.
- 7 Die erste Phase der Einspeisung bezeichnet den Vorgang, Gelder oder Vermögenswerte aus kriminellen Aktivitäten in den Wirtschaftskreislauf einzubringen unter Ausnutzung der Einzahlungswege von Kreditinstituten oder durch sonstige Unternehmen. Auf die Einspeisung folgt die eigentliche Phase der Geldwäsche, die Verschleierung. Dabei soll die Herkunft der illegal erworbenen Gelder oder Vermögenswerte durch komplexe Finanztransaktionen und Handlungsketten sowie durch die Vermischung mit legal erworbenen Vermögen verschleiert werden, um es den Strafverfolgungsbehörden unmöglich zu machen, die Papierspur des schmutzigen Geldes gerichtsfest zu belegen. In der dritten Phase, der Integration, werden die nunmehr „gewaschenen“ Gelder und Vermögenswerte von den Kriminellen investiert, insbesondere in hochwertige Konsum- und Luxusgüter und hochwertige Immobilien, aber auch in Geschäftsbeteiligungen, Bauprojekte oder Lebensversicherungen.⁷
- 8 Auch wenn sich das Dreiphasenmodell als praktikables Erklärungsmodell der Geldwäsche durchgesetzt hat, muss berücksichtigt werden, dass es noch aus den Anfangszeiten der Geldwäschebekämpfung Ende der 1980er Jahre stammt, als es im Wesentlichen um das Waschen von Bargeldern aus Straftaten der Drogenkriminalität ging.⁸ Heute sind die relevanten Vortaten einer Geldwäsche hingegen längst nicht mehr auf die klassischen Delikte der organisierten Kriminalität begrenzt, sondern erfassen auch zahlreiche Straftaten der Wirtschaftskriminalität. Auch spielt Bargeld in der modernen Geldwäschekriminalität eine weitaus geringere Rolle. Die Methoden der Geldwäsche haben sich unter Einfluss neuer Technologien wie beispielsweise virtuelle Währungen vervielfältigt. Das zeigt

4 Herzog/Achtelik, in: Herzog/Achtelik, GwG, Einleitung Rn. 2.

5 Herzog/Achtelik, in: Herzog/Achtelik, GwG, Einleitung Rn. 3.

6 Das Dreiphasenmodell wurde 1989 von der damaligen US-Zollbehörde zur Bekämpfung des Drogenhandels entwickelt, vgl. Herzog/Achtelik, in: Herzog/Achtelik, GwG, Einleitung Rn. 7 Kaetzler, in: Wohlschlägl-Aschberger, Geldwäscheprävention, S. 482.

7 Krais, Geldwäsche und Compliance, 2. Aufl. 2022, S. 19.

8 Krais, Geldwäsche und Compliance, S. 19.

schon ein Blick auf die zahlreichen Publikationen zu den Methoden der Geldwäsche.⁹ Im Grunde eignet sich jedoch jedes Geschäftsmodell dazu, Geldwäsche zu betreiben, also illegal erworbene Vermögenswerte in den Wirtschaftskreislauf zu schleusen. Nichtsdestotrotz sieht der Gesetzgeber in bargeldintensiven Geschäften weiterhin ein hohes Geldwäscherisiko und setzt Anreize für Unternehmen, Bargeldgeschäfte in größerem Umfang auszuschließen (siehe dazu → Rn. 28).

2. Die Geldwäschebekämpfung

a) Geldwäschebekämpfung auf internationaler Ebene: FATF

Auch wenn Geldwäsche als Phänomen bereits seit den 1920er Jahren existierte, erfolgten erste gesetzgeberische Aktivitäten erst Mitte der 1980er Jahre in den USA mit der Einführung einer Strafnorm zur Geldwäsche.¹⁰ Im gleichen Zeitraum gab es auf internationaler Ebene Bemühungen, Regeln für die Geldwäschebekämpfung zu schaffen. Dabei ging es in erster Linie darum, die Drogenkriminalität zu bekämpfen. Entsprechend heißt das erste internationale Vertragswerk der UN zur Geldwäschebekämpfung „Übereinkommen gegen den unerlaubten Verkehr mit Suchtstoffen und psychotropen Stoffen“ aus dem Jahr 1988 („UN-Suchtstoffübereinkommen“).¹¹

Mit der Zielsetzung über die Bekämpfung des Drogenhandels hinaus, Offshore-Finanzplätze zu kontrollieren und die organisierte Kriminalität zu bekämpfen, einigten sich die Staats- und Regierungschefs der G-7-Staaten im Jahr 1989 in Paris darauf, mit der Financial Action Task Force on Money Laundering („**FATF**“) eine besondere Ad-hoc-Expertengruppe einzusetzen, die Empfehlungen zur Bekämpfung der Geldwäsche in allen Bereichen erarbeiten sollte.¹² Das bei der OECD in Paris angegliederte Gremium ist heute der internationale Standardsetzer für die Bekämpfung von Geldwäsche, Terrorismusfinanzierung und Proliferationsfinanzierung.

Die FATF veröffentlichte 1990 erstmals Empfehlungen zur Bekämpfung von Geldwäsche („The FATF Recommendations“), die fortlaufend aktualisiert werden.¹³ Auch wenn die insgesamt 40 Empfehlungen rechtlich nicht bindend sind, entfalten sie eine politische Druckwirkung auf die Teilnehmerstaaten. Denn die FATF prüft diese turnusgemäß im Rahmen der FATF-Länderevaluationen auf die Einhaltung der internationalen Standards zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung und veröffentlicht ihre Ergebnisse in einem aus-

⁹ Vgl. die Liste der Publikationen zu Methoden und Trends der Geldwäsche unter: <https://www.fatf-gafi.org/en/topics/methods-and-trends.html> (zuletzt abgerufen am 2.2.2024).

¹⁰ Herzog/Achtelik, in: Herzog/Achtelik, GwG, 5. Aufl. 2023, Einleitung Rn. 60.

¹¹ BGBl. 1993 II, S. 1136.

¹² Herzog, in: Herzog/Achtelik, GwG, Einleitung Rn. 62.

¹³ Letzte Aktualisierung im November 2023, vgl. <https://www.fatf-gafi.org/en/publications/fatfrecommendations.html> (zuletzt abgerufen am 2.2.2024).

fürlichen Evaluierungsreport.¹⁴ Die letzte Evaluation der Bundesrepublik Deutschland im Jahr 2021 bescheinigte der Bundesrepublik Versäumnisse bei der Geldwäschebekämpfung insbesondere auf staatlicher Ebene und führte zu einer Umstrukturierung der behördlichen Aufsichts- und Ermittlungslandschaft im Bereich der Geldwäscheprevention.

- 12 Daneben stellt die FATF auf ihrer Homepage regelmäßig Veröffentlichungen zu aktuellen Methoden und Trends, „Best Practices“ zum Thema Geldwäsche- und Terrorismusfinanzierung zur Verfügung und unterhält eine Liste mit sog. Hochrisikostaaten bzw. nicht kooperativer Länder und Territorien („High Risk and non-cooperative Jurisdictions“).¹⁵ Diesen Ländern bescheinigt die FATF einen gravierenden Mangel bei ihren Maßnahmen zur Geldwäsche- und Terrorismusfinanzierung. Die EU-Kommission folgt bei der Benennung der Drittländer mit hohem Risiko in der Regel der FATF-Länderlistung.
- 13 Die FATF Recommendations und sonstigen Veröffentlichungen haben einen großen Einfluss auf die EU-Geldwäscherichtlinien, die wiederum maßgeblich für das deutsche Geldwäscherecht sind. Teilweise werden die Empfehlungen wortgleich von der EU in die Geldwäscherichtlinien übernommen. Ein Blick auf die Publikationen der FATF stellt also gelegentlich einen Blick in die Zukunft der deutschen Geldwäschegesetzgebung dar. So veröffentlichte die FATF bereits im Juni 2014 einen Bericht zu den Risiken virtueller Währungen, bevor der deutsche Gesetzgeber zu Beginn des Jahres 2020 virtuelle Währungen regulierte.¹⁶ Das deutsche Geldwäscherecht ist damit ganz wesentlich von den Empfehlungen der FATF geprägt. Bei der Auslegung der Normen des GwG sind daher neben den EU-Richtlinien auch die FATF-Recommendations und die entsprechenden „Interpretive Notes“ heranzuziehen.¹⁷

b) Geldwäschebekämpfung in der deutschen Gesetzgebung

- 14 Entsprechend den internationalen Entwicklungen nahm die deutsche Gesetzgebung das Thema Geldwäschebekämpfung zu Beginn der 1990er Jahre auf die Agenda mit der Einführung des Straftatbestandes der Geldwäsche in § 261 StGB.¹⁸ Seitdem erfuhr die Strafnorm zahlreiche Anpassungen. Die letzte große Novellierung der Strafnorm erfolgte mit Wirkung zum 18. März 2021, mit der

14 Vgl. <https://www.fatf-gafi.org/en/topics/mutual-evaluations.html> (zuletzt abgerufen am 2.2.2024).

15 Vgl. unter <https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html> (zuletzt abgerufen am 2.2.2024).

16 Vgl. <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> (letzter Zugriff am 2.2.2024).

17 Die „Interpretive Notes“ schließen sich direkt an die FATF Recommendations im selben Dokument an, vgl. <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> (zuletzt abgerufen am 15.5.2020).

18 Die Einführung erfolgte durch das Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität v. 15.7.1992 (OrgKG), BGBl. 1992 I, S. 1302.

u. a. der Vortatenkatalog abgeschafft wurde und seitdem jede Straftat taugliche Vortat der Geldwäsche sein kann.¹⁹

Neben der strafrechtlichen Norm ist insbesondere das GwG seit 1993 das gesetzgeberische Instrument der Geldwäscheprävention. Das GwG ist ein gewerbe-rechtliches Instrument mit weitgehend präventivem Charakter.²⁰ Deren Vorschriften sind wie bereits erwähnt ganz wesentlich durch die entsprechenden EU-Richtlinien geprägt. Die letzte Umsetzung der nunmehr 5. EU-Geldwäscherichtlinie²¹ erfolgte am 1.1.2020. Anschließend änderte der deutsche Gesetzgeber mit mehreren nationalen Gesetzen das GwG, insbesondere im Bereich des Transparenzregisters, zuletzt durch das Gesetz zur Stärkung der risikobasierten Arbeitsweise der Zentralstelle für Finanztransaktionsuntersuchungen (FIU) am 18.11.2023.²² **15**

Das GwG ist historisch gesehen und mit Blick auf seine Anforderungen, Terminologien und nicht zuletzt seiner Systematik (immer noch) ein Gesetz, dem man ansieht, dass es ursprünglich für den Finanzsektor geschaffen wurde. Mit der Umsetzung der 4. EU-Geldwäscherichtlinie²³ hat sich der deutsche Gesetzgeber dafür entschieden, die EU-Vorgaben wieder in ein einheitliches Gesetzbuch zu gießen.²⁴ Dabei hat der Gesetzgeber wohl einige Inkonsistenzen in Kauf gekommen, die im Laufe dieses Kapitels noch thematisiert werden, sofern sie Güterhändler betreffen. **16**

Das deutsche und europäische Geldwäscherecht steht vor großen Veränderungen. Auf EU-Ebene steht die Verabschiedung eines umfassenden Gesetzespaketes bevor, das neben der Einrichtung einer europäischen Anti-Geldwäschebehörde eine Vollharmonisierung der zentralen Geldwäscheregelungen beinhaltet. Von entscheidender Bedeutung für Güterhändler ist, dass die veröffentlichten Gesetzesentwürfe vorsehen, nur noch Güterhändler vom geldwäscherechtlichen Anwendungsbereich zu erfassen, wenn sie mit Edelmetallen und Edelsteinen han- **17**

19 Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche, BGBl. 2021 I, S. 327.

20 *Krais*, Geldwäsche und Compliance, S. 9.

21 Richtlinie (EU) 2018/843 des Europäischen Parlaments und des Rates vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU.

22 BGBl. 2023 I, S. 311.

23 Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung.

24 Anders als beispielsweise Österreich, wo die EU-Richtlinie in jeweils branchenspezifische Gesetzbücher umgesetzt wurde, z. B. in das Finanzmarkt-Geldwäschegesetz, das Glücksspielgesetz oder die Gewerbeordnung.

deln.²⁵ In Deutschland würden damit auf einen Schlag Unternehmen aus Industrie und Handel keinen Pflichten mehr zur Verhinderung von Geldwäsche unterliegen. Die einschlägige EU-Verordnung²⁶ wurde am 19.6.2024 im Amtsblatt der EU veröffentlicht und tritt am 10.6.2027 in Kraft.

3. Geldwäscherisiken für Industrie- und Handelsunternehmen

- 18** Mit Blick auf das Dreiphasenmodell können Unternehmen aus Industrie und Handel in jeder Phase mit Geldern oder Vermögenswerten aus illegalen Quellen in Berührung kommen. Bei der Einspeisung wird dies in der Regel durch Bargeldgeschäfte geschehen. In der Folge wird das Bargeld mit Einzahlung auf das Konto des Unternehmens in den Finanzkreislauf eingeschleust. In der Verschleierungsphase können Unternehmen dafür genutzt bzw. missbraucht werden, durch den Vertrieb schnell umschlagfähiger Güter oder sonstiger Wirtschaftssubjekte Verschleierungstransaktionen durchzuführen, mit der Folge, dass die Herkunft des Vermögens kaum noch bestimmt werden kann.²⁷ Dafür eignen sich insbesondere solche Güter, die einen hohen Wiederverkaufswert haben. Nach dem ursprünglichen Vorstellungsbild des Dreiphasenmodells besteht das höchste Risiko für Industrie- und Handelsunternehmen in der Integrationsphase, in der Kriminelle die „gewaschenen“ Gelder oder Vermögenswerte in teure Statussymbole und Konsumgüter investieren möchten.²⁸ Aufgrund ihres hohen Wiederverkaufswerts eignen sich einige Luxusgüter (insbesondere Edelmetalle und Schmuck) aber auch für die Verschleierung.
- 19** Wenn man sich diese Erwägungen vor Augen führt, wird schnell deutlich, dass Missbrauchsgefahren für Industrie- und Handelsunternehmen nicht nur im Zusammenhang mit bargeldintensiven Geschäften bestehen. In der jüngeren Vergangenheit haben das eindrucksvoll die Geldwäscheskandale gezeigt, die öffentlich als „Russian Laundromat“,²⁹ „Troika Laundromat“³⁰ oder „Danske Bank Skandal“³¹ bekannt wurden. Auch wenn der Fokus der Berichterstattung und der Ermittlungen im Danske Bank Skandal auf dem Finanzsektor lag, waren zahlreiche Industrie- und Handelsunternehmen von den Vorgängen betroffen. Als 2018

25 Art. 1 Nr. 3 lit. e des Vorschlages für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung (COM(2021) 420 final).

26 Verordnung (EU) 2024/1624 des Europäischen Parlaments und des Rates vom 31. Mai 2024 zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung.

27 Kaetzler, in: Wohlschlägl-Aschberger, Geldwäscheprävention, S. 483.

28 Kraus, Geldwäsche und Compliance, S. 19.

29 Vgl. <https://www.sueddeutsche.de/wirtschaft/geldwaesche-die-russische-geldwaschaschine-1.3427580> (zuletzt aufgerufen am 2.2.2024).

30 Vgl. <https://www.sueddeutsche.de/politik/laundromat-geldwaesche-russland-1.4354499> (zuletzt aufgerufen am 2.2.2024).

31 Vgl. <https://www.faz.net/aktuell/finanzen/so-lief-der-geldwaesche-skandal-der-danske-bank-1853314.html> (zuletzt aufgerufen am 2.2.2024).

bekannt wurde, dass über eine Filiale der Danske Bank in Tallin zwischen 2007 und 2015 Gelder aus Russland und ehemaligen Sowjetrepubliken in Milliardenhöhe gewaschen wurden, ergaben Nachforschungen in Deutschland die Involvierung zahlreicher bekannter deutscher Unternehmen.³² Über die Konten bei der estnischen Filiale flossen insgesamt 31 Mio. EUR offenbar unbemerkt auf deutsche Firmenkonten. In der Mehrzahl der Fälle wurden mit den Geldern Warenlieferungen nach Russland bezahlt. Die Empfänger der Handelsgüter waren allerdings nicht identisch mit den Firmen, die für die Warenlieferungen bezahlt hatten. Auch ließen sich keine unmittelbaren Geschäftsbeziehungen zwischen den beteiligten Firmen nachweisen. Bei den gelieferten Gütern handelte es sich unter anderem um Industrieausrüstungen, Hausgerätetechnik, Stoffe, Aquarientechnik, Ersatzteile oder Autos. Auch wenn die Vorfälle für die beteiligten Unternehmen – soweit bekannt – keine strafrechtlichen oder sonstigen behördlichen Ermittlungen oder Sanktionen nach sich zogen, war der Reputationsschaden aufgrund der Presseberichterstattung beträchtlich.

Der Danske Bank Skandal liefert einige Erkenntnisse für die Risikoexposition von Unternehmen aus Industrie und Handel, die teilweise mit veralteten Vorstellungen zum Geldwäscherisiko außerhalb der Finanzbranche brechen: **20**

- Zunächst ist die pauschale Aussage, bargeldlose Geschäftsaktivitäten wiesen ein geringe(re)s Risiko der Geldwäsche auf, nicht korrekt. Die Transaktionen auf die Firmenkonten erfolgten bargeldlos mittels Kontoüberweisungen.
- Die betroffenen Unternehmen produzierten allesamt keine Waren oder Güter, die gemeinhin als „geldwäscheexponiert“ angesehen werden, wie beispielsweise Schmuck und Uhren, Kraftfahrzeuge, Schiffe und Motorboote oder Kunst und Antiquitäten.
- Im Danske Bank Skandal waren insbesondere exportorientierte Unternehmen aus dem deutschen Mittelstand betroffen. Es spricht einiges dafür, dass diese Unternehmen gezielt ausgewählt wurden, möglicherweise da ihnen – im Gegensatz zu den Unternehmen aus der Automobil- oder Luxusgüterbranche – generell hin ein geringes Geldwäscherisiko bescheinigt wurde und entsprechende Sicherungsmaßnahmen weniger stark ausgeprägt waren.

Die Geldwäscheskandale der letzten Jahre haben gezeigt, dass Industrie- und Handelsunternehmen verstärkt in der „Layering-Phase“ genutzt bzw. benutzt werden, um durch den Kauf bestimmter Waren die Herkunft der dazu eingesetzten Gelder zu verschleiern. Dieses Ausnutzen von internationalen Warenströmen zu Geldwäschezwecken ist insgesamt allerdings kein neues Phänomen. Das sog. „Trade-based Money Laundering“ ist vielmehr seit vielen Jahrzehnten bekannt und hat inzwischen viele Erscheinungsformen angenommen. Bereits im Jahr 2006 veröffentlichte die FATF zu diesem Thema.³³ Tatsächlich eignet sich der **21**

32 Vgl. <https://www.nzz.ch/wirtschaft/danske-bank-steckt-tief-im-geldwaescherei-sumpf-ld.1400914> (zuletzt aufgerufen am 2.2.2024).

33 Vgl. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade%20Based%20Money%20Laundering.pdf.coredownload.pdf> (zuletzt abgerufen am 2.2.2024).

globalisierte Weltmarkt mit seinen internationalen Warenströmen und Finanztransaktionen sehr gut dafür, die illegale Herkunft von Geldern und Vermögenswerten zu verschleiern. Damit kann jedoch nicht pauschal ein erhöhtes Risiko für Industrie und Handel angenommen werden. Vielmehr kommt es bei der Bestimmung des Geldwäscherisikos auf die Eignung der Produkte zu Geldwäschezwecken, Art und Größe des Geschäfts sowie auf die Kunden und Geschäftspartner an.

II. Industrie- und Handelsunternehmen im GwG: Der Begriff des Güterhändlers

- 22 Mit Blick auf die soeben geschilderte Risikoexposition ist die Einbeziehung von Industrie- und Handelsunternehmen in die gesetzliche Geldwäschebekämpfung konsequent. Diese sind nach § 1 Abs. 9 GwG Güterhändler, wenn sie gewerblich Güter veräußern, unabhängig davon in wessen Namen oder auf wessen Rechnung. Normadressaten sind sowohl natürliche Personen als auch juristische Personen und rechtsfähige Personengesellschaften.³⁴
- 23 Voraussetzung ist, dass die Person gewerblich handelt. Darunter ist ein Gewerbe i. S. d. GewO zu verstehen, also jede selbstständige, erlaubte, auf Gewinnerzielungsabsicht gerichtete und auf Dauer angelegte Tätigkeit, die nicht der Urproduktion, den freien Berufen oder der bloßen Verwaltung von eigenem Vermögen zuzurechnen ist.³⁵ Damit fallen private oder nur gelegentliche Veräußerungsgeschäfte nicht in den Anwendungsbereich.³⁶ Neben dem Eigenhandel (eine Person veräußert eigene Güter in eigenem Namen) sind auch Kommissionsgeschäfte und Auktionatoren (in eigenem Namen auf fremde Rechnung) und Vermittlergeschäfte (in fremdem Namen auf fremde Rechnung) von dem Begriff erfasst.³⁷
- 24 Güterhändler sind nicht nur An- und Wiederverkäufer von Waren, sondern auch Industriebetriebe, die Waren und Güter herstellen und vertreiben.³⁸ Auf einen Absatz an Endkunden kommt es nicht an, sodass in einer Weiterveräußerungskette jeder involvierte Händler ein Güterhändler i. S. d. GwG ist.³⁹ Gewerbliche Dienstleister sind hingegen nicht erfasst.⁴⁰ Auch Güterhändler, die im Rahmen ihrer Tätigkeit Dienstleistungen ausüben, unterliegen dabei nicht den geldwäscherechtlichen Pflichten.
- 25 Der Begriff der „Güter“ wird sehr weit ausgelegt. Nach der Gesetzesbegründung sind Güter alle beweglichen und nicht beweglichen Sachen, unabhängig von ih-

34 BT-Drs. 19/13827, S. 63.

35 Kaetzler, in: Wohlschlägl-Aschberger, Geldwäscheprävention, S. 492.

36 Kaetzler, in: Wohlschlägl-Aschberger, Geldwäscheprävention, S. 490, 493.

37 BT-Drs. 18/11555, S. 103.

38 Kraus, Geldwäsche und Compliance, S. 47.

39 Kaetzler, in: Wohlschlägl-Aschberger, Geldwäscheprävention, S. 493.

40 Kraus, Geldwäsche und Compliance, S. 52.

rem Aggregatzustand, die einen wirtschaftlichen Wert haben und deshalb Gegenstand einer Transaktion sein können.⁴¹ Danach fallen körperliche als auch unkörperliche Gegenstände (z. B. Gas und Strom) sowie auch Immobilien nach dem Willen des Gesetzgebers unter den Güterbegriff.⁴²

Daneben unterhält das GwG eine Definition für hochwertige Güter. Nach § 1 Abs. 10 GwG sind darunter Gegenstände zu verstehen, die sich aufgrund ihrer Beschaffenheit, ihres Verkehrswertes oder ihres bestimmungsgemäßen Gebrauchs von Gebrauchsgegenständen des Alltags abheben oder die aufgrund ihres Preises keine Alltagsanschaffung darstellen. Hochwertige Güter sind insbesondere Edelmetalle wie Gold, Silber und Platin, Edelsteine, Schmuck und Uhren, Kunstgegenstände und Antiquitäten, Kraftfahrzeuge, Schiffe und Motorboote sowie Luftfahrzeuge.⁴³ Aufgrund ihrer höheren Risikoexposition unterliegen Händler mit hochwertigen Gütern strengeren Vorschriften. **26**

Eine schwierige Abgrenzungsfrage kann dann entstehen, wenn Dienstleistungsunternehmen (auch) Geschäfte tätigen, die sie als Güterhändler qualifizieren könnten. Nach § 2 Abs. 1 GwG sind Personen oder Unternehmen Verpflichtete, soweit sie in Ausübung ihres Gewerbes oder Berufes als Angehörige der genannten Instituts- oder Berufsgruppen handeln. Zur Bestimmung der Verpflichteteigenschaft aufgrund einer bestimmten Tätigkeit kommt es auf die gewerbliche bzw. freiberufliche Tätigkeit im Kern an.⁴⁴ Sofern also vereinzelt Verkaufsgeschäfte nicht von der gewerblichen Tätigkeit des Unternehmens gedeckt sind, führen sie nicht dazu, dass das Unternehmen zum Güterhändler wird und entsprechende Pflichten nach dem GwG in der Geschäftsbeziehung zu erfüllen hat. Mit Blick auf § 4 Abs. 5 Nr. 1 GwG kann dieses Unterscheidungsmerkmal auch für die Abgrenzung herangezogen werden, ob ein Unternehmen über seine Stellung als Güterhändler hinaus als Kunsthändler oder als Edelmetallhändler bestimmt werden kann und unter niedrigeren Voraussetzungen ein Risikomanagement einführen muss. **27**

III. Die Pflichten der Güterhändler im GwG

Güterhändler sind in Deutschland unabhängig von einer Bargeldbeschränkung stets Verpflichtete nach dem GwG. Das ist deshalb erwähnenswert, weil die EU-Geldwäscherichtlinien nur Güterhändler verpflichten, die Zahlungen in Höhe von 10.000 EUR oder mehr in bar tätigen oder entgegennehmen.⁴⁵ Entsprechend müssen in vielen anderen EU-Ländern Unternehmen aus Industrie und Handel überhaupt nur dann geldwäscherechtliche Pflichten erfüllen, wenn sie Bargeldgeschäfte in dieser Höhe tätigen. Der deutsche Gesetzgeber hat sich dagegen zu **28**

⁴¹ BT-Drs. 18/11555, S. 103.

⁴² BT-Drs. 18/11555, S. 103; *Gehrmann/Wengenroth*, BB 2019, 1035, 1037.

⁴³ Vgl. den nicht abschließenden Katalog in § 1 Abs. 10 Nr. 2 Satz 2 GwG.

⁴⁴ *Kaetzler*, in: *Zentes/Glaab*, GwG, § 2 Rn. 2.

⁴⁵ Art. 2 Abs. 1 Nr. 3 lit. e der 4. EU-Geldwäscherichtlinie.

einer „überschießenden“ Umsetzung der 4. EU-Geldwäscherichtlinie entschieden mit der Folge, dass Güterhändler unabhängig von Bargeldgeschäften verpflichtet sind. Sofern sie jedoch Bargeldgeschäfte von über 10.000 EUR ausschließen, sind Güterhändler von der Pflicht befreit, ein Risikomanagement durchzuführen. Sie müssen jedoch in bestimmten Situationen Sorgfaltspflichten gegenüber ihren Kunden und Geschäftspartnern durchführen und verdächtige Sachverhalte an die Zentralstelle für Finanztransaktionsuntersuchungen (Financial Intelligence Unit – „FIU“) melden.

1. Die privilegierte Verpflichtetenstellung von Güterhändlern

- 29 Eine zentrale Norm für Güterhändler ist § 4 Abs. 5 Nr. 1 GwG. Sie gibt vor, unter welchen Voraussetzungen Güterhändler die Vorschriften zur Errichtung eines Risikomanagements zu erfüllen haben. An dieser Stelle kommt dem Ausschluss von Bargeldtransaktionen über mindestens 10.000 EUR eine wesentliche Bedeutung zu. Denn nur Güterhändler, die Bartransaktionen über Güter über mindestens 10.000 EUR selbst oder durch Dritte tätigen oder entgegennehmen, müssen kein Risikomanagement einführen. Für Händler mit Edelmetallen wie Gold, Silber und Platin gilt eine Bargeldschwelle von 2.000 EUR. Güterhändler, die mit Kunstgegenständen handeln, müssen bei Transaktionen über Kunstgegenstände von mindestens 10.000 EUR – unabhängig davon, ob diese bar oder unbar erfolgen – ein Risikomanagement einführen. Bei dieser Vorschrift wird die Ansicht des Gesetzgebers deutlich, dass unternehmensinterne Bargeldbeschränkungen in besonderem Maße geeignet sind, in präventiver Weise Geldwäscherisiken entgegenzuwirken.⁴⁶ Güterhändler können sich also mit einem Ausschluss von Bartransaktionen in entsprechender Höhe davon befreien, die formellen Vorgaben zum Risikomanagement einzuhalten und in der Folge insb. keine Risikoanalyse erstellen oder interne Sicherungsmaßnahmen vorhalten zu müssen.

a) Praktische Umsetzung des Bargeldausschlusses

- 30 In der Praxis stellt sich regelmäßig die Frage, was ein Unternehmen oder eine Unternehmensgruppe beachten muss, um die Entgegennahme oder Durchführung von Bargeldtransaktionen in Höhe von 10.000 EUR (bzw. 2.000 EUR) wirksam auszuschließen. Auch ohne explizite gesetzliche Vorgabe bietet es sich aus Dokumentations- und Darlegungszwecken gegenüber Behörden an, eine entsprechende Bargeldregelung in einer Richtlinie, Arbeitsanweisung oder einer sonstigen Kommunikation zu verschriftlichen. Darüber hinaus muss regelmäßig kontrolliert werden, ob die Regelung auch tatsächlich eingehalten wird.⁴⁷

46 BT-Drs. 19/15196, S. 45.

47 Auslegungs- und Anwendungshinweise zum Geldwäschegesetz (GwG) für Güterhändler, Immobilienmakler und andere Nichtfinanzunternehmen (Regierungspräsidien in Hessen) im Rahmen der Gemeinsamen Auslegungs- und Anwendungshinweisen der Länder der Bundesrepublik Deutschland (Stand Mai 2023), Ziff. 2.4.

Bei der konkreten Ausgestaltung der Regelung muss inhaltlich beachtet werden, dass vom Transaktionsbegriff in § 1 Abs. 5 Satz 1 GwG erfasst sind „eine oder, soweit zwischen ihnen eine Verbindung zu bestehen scheint, mehrere Handlungen, die eine Geldbewegung oder eine sonstige Vermögensverschiebung bezweckt oder bezwecken oder bewirkt oder bewirken“. Der Transaktionsbegriff erfasst somit auch mehrere zusammenhängende Geldbewegungen oder sonstige Vermögensverschiebungen, soweit zwischen ihnen eine Verbindung besteht. Damit sollen insbesondere solche Transaktionen erfasst werden, die künstlich aufgeteilt werden, um einen möglichen Schwellenbetrag zu unterschreiten (sog. „Smurfing“). Maßgeblich ist ein von der Verkehrsanschauung logisch als zusammenhängend zu betrachtender Vorgang.⁴⁸ **31**

Eine Bargeldregelung muss diesen Gedanken aufgreifen um sicherzustellen, dass der Schwellenwert von 10.000 EUR nicht durch mehrere einzelne aber zusammenhängende Bartransaktionen überschritten wird. Umstritten ist, ob bereits eine einzige den Schwellenwert übersteigende Bargeldtransaktion ausreicht, um die Pflichten in Abschnitt 2 des GwG auszulösen. Mit der Umsetzung der 5. EU-Geldwäscherichtlinie zum 1.1.2020 hat sich der Wortlaut in § 4 Abs. 5 GwG dahingehend geändert, dass nunmehr Transaktionen (Plural) im Wert von mindestens 10.000 EUR vorliegen müssen. Die alte Gesetzeslage sprach von einer Transaktion (Singular). Daher kann nach aktueller Rechtslage wohl nicht mehr davon ausgegangen werden, dass bereits eine Bartransaktion die Pflicht zur Einrichtung eines Risikomanagements auslöst. In ihren Auslegungs- und Anwendungshinweisen zum GwG scheinen die Aufsichtsbehörden hingegen weiterhin davon auszugehen, dass bereits eine den Schwellenwert übersteigende Transaktion den Pflichtenkatalog in Abschnitt 2 des GwG auslöst.⁴⁹ In der Praxis führt die Unsicherheit zur Bestimmung von zusammenhängenden Barzahlungen oftmals dazu, dass – je nach Geschäftsmodell – Güterhändler Barzahlungen vollständig ausschließen oder intern einen Schwellenwert benennen, der weit unter der 10.000-EUR-Grenze liegt. **32**

Für Güterhändler von großer Relevanz ist § 4 Abs. 5 Nr. 1 lit. c GwG, wonach die Norm auch Bartransaktionen über mindestens 10.000 EUR erfasst, die durch Dritte getätigt oder entgegengenommen werden. Unklar ist, was unter dem Zusatz „durch Dritte“ zu verstehen ist.⁵⁰ Es spricht einiges dafür, dass der deutsche Gesetzgeber solche Umgehungskonstellationen erfassen wollte, in denen Güterhändler über eine von ihnen eingeschaltete Hilfsperson Barzahlungen entgegennehmen oder tätigen lassen, um nicht selbst eine pflichtenauslösende Bartrans- **33**

⁴⁸ Kaetzler, in: Zentes/Glaab, GwG, § 1 Rn. 64.

⁴⁹ Vgl. Auslegungs- und Anwendungshinweise zum Geldwäschegesetz (GwG) für Güterhändler, Immobilienmakler und andere Nichtfinanzunternehmen (Regierungspräsidien in Hessen) im Rahmen der Gemeinsamen Auslegungs- und Anwendungshinweisen der Länder der Bundesrepublik Deutschland (Stand Mai 2023), Ziff. 2.3.1 ff.

⁵⁰ Weder die 4. noch die 5. EU-Geldwäscherichtlinie noch die für Güterhändler relevanten FATF Recommendations Nr. 22 und Nr. 23 sowie die dazugehörigen Interpretive Notes geben vor, dass Transaktionen durch Dritte erfasst sein sollen.

aktion durchzuführen. Die Veranlassung und Weisung des Dritten durch den Güterhändler muss sich zumindest auch auf die Annahme von Bargeld in Höhe von mehr als 10.000 EUR beziehen, da die Gesetzesbegründung davon spricht, dass „der Schwellenbetrag unabhängig davon greift, ob Bargeld tatsächlich zwischen dem Güterhändler und dem Vertragspartner ausgetauscht wird oder insoweit Dritte eingeschaltet werden“.⁵¹ Die Auffassung der Aufsicht ist hingegen weiter und wertet bereits Bareinzahlungen eines Kunden auf das Konto des Verpflichteten regelmäßig als Annahme von Bargeld durch den Verpflichteten.⁵² Diese Auffassung ist kritikwürdig, denn wie soll ein Güterhändler effektiv verhindern können, dass seine Kunden Bareinzahlungen auf eines seiner Konten tätigt? Am Ende wird Güterhändlern nichts anderes übrig bleiben, als gegenüber ihren Geschäftspartnern klarzustellen, dass Barzahlungen gar nicht oder nur in einer Höhe unterhalb der Schwellenwerte möglich sind, wenn sie von der Pflichtenreduzierung in § 4 Abs. 5 Nr. 1 GwG profitieren wollen.

b) Konsequenzen bei Einführung einer Bargeldbeschränkung

- 34 Mit Einführung einer Bargeldgrenze entfällt für Güterhändler die Pflicht, über ein wirksames Risikomanagement zu verfügen. Mit dem Ausschluss müssen Güterhändler auch keine gruppenweiten Pflichten nach § 9 GwG erfüllen.
- 35 Die Kundensorgfaltspflichten müssen Güterhändler mit Bargeldausschluss oder -beschränkung nach § 10 Abs. 3 GwG lediglich bei Vorliegen von Tatsachen durchführen, die darauf hindeuten, dass es sich bei Vermögensgegenständen, die mit einer Transaktion oder Geschäftsbeziehung im Zusammenhang stehen, um den Gegenstand von Geldwäsche handelt oder die Vermögensgegenstände im Zusammenhang mit Terrorismusfinanzierung stehen (sog. „**Verdachtsfall**“), siehe unten → Rn. 71 ff. Unbeschränkt ist die Pflicht für Güterhändler, bei Vorliegen eines Verdachtsfalles eine Verdachtsmeldung nach § 43 Abs. 1 GwG an die FIU abzugeben (siehe → Rn. 71).
- 36 Güterhändler müssen also in der Regel erst mit Vorliegen eines Verdachtsfalls die formellen Vorgaben des GwG erfüllen. Daher ist es für Güterhändler von hoher Bedeutung, Verdachtsfälle erkennen zu können. Das wiederum setzt voraus, dass Güterhändler ihre unternehmensspezifischen geldwäscherelevanten Risiken kennen, um verdächtige Sachverhalte überhaupt erkennen zu können. Solche kritische und pflichtenauslösende Sachverhalte erkennen Unternehmen am ehesten, wenn sie sich im Rahmen einer Risikoanalyse (siehe → Rn. 40) mit ihren Kunden und Geschäftspartnern, Produkten und Dienstleistungen sowie Vertriebsländern und Vertriebswegen auseinandergesetzt haben.

51 BT-Drs. 19/13827, S. 70.

52 Auslegungs- und Anwendungshinweise zum Geldwäschegesetz (GwG) für Güterhändler, Immobilienmakler und andere Nichtfinanzunternehmen (Regierungspräsidien in Hessen) im Rahmen der Gemeinsamen Auslegungs- und Anwendungshinweisen der Länder der Bundesrepublik Deutschland (Stand Mai 2023), Ziff. 2.3.1.

Wie eingangs geschildert, können Unternehmen aus Industrie und Handel auch ohne Bargeldgeschäfte von Geldwäsche betroffen sein. Denn Geldwäscherisiken bestehen in Unternehmen je nach Tätigkeitsfeld unabhängig von Verdachtsschwellen für Kundenidentifizierungs- und Risikomaßnahmen im GwG.⁵³ Die praktische Konsequenz der Ausnahme nach § 4 Abs. 5 Nr. 1 GwG ist daher nicht, dass Güterhändler komplett auf sämtliche Maßnahmen des Risikomanagements verzichten können.⁵⁴ Empfehlenswert ist, anhand der Vorschriften im zweiten Abschnitt des GwG geeignete Elemente der Geldwäscheprävention aufzugreifen und in die allgemeine Compliance-Organisation zu integrieren (siehe → Rn. 47 ff.).

Dies ist nicht nur aus der Perspektive des gewerberechtlichen GwG ratsam. Schließlich darf nicht vernachlässigt werden, dass die Strafnorm der Geldwäsche in § 261 StGB jede Straftat als Vortat der Geldwäsche einstuft, zahlreiche Tathandlungen umfasst und auch leichtfertiges Handeln pönalisiert. Um Mitarbeiter nicht der Gefahr auszusetzen, leichtfertig Geldwäsche zu betreiben und um der Legalitätspflicht der Unternehmensführung besser gerecht zu werden, empfiehlt es sich, auch ohne formale Pflicht nach dem GwG organisatorische Maßnahmen zur Geldwäscheprävention einzurichten.

2. Risikomanagement

Das Risikomanagement besteht gemäß § 4 Abs. 2 GwG aus einer Risikoanalyse und den internen Sicherungsmaßnahmen. Damit umfasst das Risikomanagement im Grunde diejenigen Maßnahmen, die auch Bestandteil eines allgemeinen Compliance-Management-Systems sind.

a) Risikoanalyse

Die Analyse der Compliance-Risiken ist das Kernstück eines jeden Compliance-Management-Systems.⁵⁵ Nur wer seine Risiken kennt, kann ihnen angemessen und wirksam begegnen. Daher ist die Erstellung einer Risikoanalyse für Güterhändler empfehlenswert, auch wenn sie formell nicht dazu verpflichtet sind (siehe oben → Rn. 28 ff.). Güterhändler finden inzwischen u. a. gute und übersichtliche Muster auf den Internetseiten ihrer Aufsichtsbehörden, anhand derer sie eine eigene Risikoanalyse erstellen können.⁵⁶

Eine Risikoanalyse nach § 5 Abs. 1 GwG erfolgt üblicherweise in mehreren Schritten. Nach einer ersten Bestandsaufnahme, in der die Situation des Unter-

⁵³ Kaetzler, in: Wohlschlägl-Aschberger, Geldwäscheprävention, S. 487 f.

⁵⁴ Kaetzler, in: Zentes/Glaab, GwG, § 4 Rn. 38 zum Risikomanagement grundsätzlich auch → Romeike, Kap. 9.

⁵⁵ Vgl. → Schulz, Kap. 1 Rn. 60 ff.

⁵⁶ Vgl. für das Regierungspräsidium Darmstadt <https://rp-darmstadt.hessen.de/sicherheit-und-kommunales/gefahrenabwehr/geldwaesche> (zuletzt abgerufen am 2.2.2024); zu den Grundlagen und Anforderungen eines Risikomanagements siehe → Romeike, Kap. 9.

Teil 3 Besondere Aufgaben und Anwendungsfelder

nehmens konkret erfasst wird, erfolgt die Risikoidentifizierung. In diesem zweiten Schritt erfolgt die Beschreibung der konkreten Geldwäscherisiken des Unternehmens. Als Ausgangspunkt für die Risikoidentifizierung werden in der Praxis bestimmte Risikoklassen herangezogen. Diese wurden zwar ursprünglich für die Finanzindustrie entwickelt, können aber durchaus auch in Industrie und Handel herangezogen werden. Grundsätzlich bestehen die folgenden Risikoklassen:

- Kunden- und Geschäftspartnerrisiken,
- Produktrisiken,
- Transaktionsrisiken und
- Länderrisiken, die aber auch z. B. beim Kundenrisiko mit thematisiert werden können.

- 42 Die Risikoklassen bestehen selbst aus einzelnen Risikofaktoren, die in abstrakter Form Fälle von erhöhtem Geldwäscherisiko beschreiben. Das GwG nennt in den Anlagen 1 und 2 einige Faktoren, die potenziell ein geringeres oder höheres Geldwäscherisiko darstellen. Sie sind neben den Ergebnissen der Ersten Nationalen Risikoanalyse,⁵⁷ die im Oktober 2019 veröffentlicht wurde, zwingend in der Risikoanalyse zu berücksichtigen. Viele der „klassischen“ geldwäschespezifischen Risikofaktoren sind jedoch auf den Finanzsektor zugeschnitten und nur bedingt für Güterhändler geeignet. Eine gute Hilfestellung bilden insoweit die fortlaufend aktualisierten Typologie-Papiere der FIU, die neben allgemeinen Typologien für den Nicht-Finanzsektor auch branchenspezifische Auffälligkeiten beispielsweise für die Automobilbranche oder für den Immobiliensektor benennt.
- 43 Im Rahmen der Risikoanalyse muss sich das Unternehmen also bewusst machen, inwieweit sein Geschäft diesen Risikofaktoren potenziell ausgesetzt ist. Ist es beispielsweise in Ländern aktiv, in denen ein hohes Risiko für Geldwäsche existiert, muss es sein Länderrisiko entsprechend hoch gewichten. Dagegen sprechen Geschäftspartner, die als börsennotierte Gesellschaften organisiert sind und ihren Sitz in der EU haben, für ein geringes Geschäftspartnerrisiko.⁵⁸ Risikofaktoren spielen nicht nur bei der Erstellung und Aktualisierung der Risikoanalyse eine Rolle. Sofern sie in einem konkreten Einzelfall auftauchen, sind sie maßgeblich für die Frage, ob ein Verdachtsfall vorliegt, welcher der FIU angezeigt werden muss (siehe zur Verdachtsmeldepflicht unten → Rn. 71 ff.).
- 44 Im dritten Schritt müssen die identifizierten Risiken kategorisiert und gewichtet werden. Hierbei geht es darum, die im Laufe der Geschäftstätigkeit auftretenden Kunden und Geschäftspartner, Transaktionen und Produkte in (abstrakte) Risikogruppen einzuteilen. In der Regel sind drei Risikokategorien ausreichend:

57 Vgl. https://www.bundesfinanzministerium.de/Content/DE/Downloads/Broschueren_Bestellservice/2019-10-19-erste-nationale-risikoanalyse_2018-2019.pdf?__blob=publicationFile&v=14 (zuletzt abgerufen am 2.2.2024).

58 Siehe Nr. 1 lit. a und Nr. 3 lit. a der Anlage 1 zum GwG.

Geringes Risiko – Mittleres Risiko – Hohes Risiko

Die Kategorisierung kann anhand folgender Kriterien erfolgen:⁵⁹

45

- Hohes Risiko: Alle Fallkonstellationen, die entweder unter die vom Gesetzgeber definierten Hochrisikoklassen (§ 15 GwG) oder aufgrund der eigenen Risikoeinschätzung unter Berücksichtigung der Anlage 2 zum GwG oder sonstiger Informationen ebenfalls in diese Klassifizierung fallen.
- Mittleres Risiko: Alle Fallkonstellationen, die aufgrund der eigenen Risikoeinschätzung des Verpflichteten nicht in die Klassifizierung „hoch“ oder „gering“ fallen.
- Geringes Risiko: Alle Fallkonstellationen, in denen unter Beachtung der Anforderungen des § 14 GwG, der Anlage 1 des GwG oder sonstiger Informationen aufgrund einer nachvollziehbaren Risikoanalyse ein geringes Risiko angenommen werden kann.

Das Ergebnis dieser Risikoanalyse ist die Grundlage für die zu ergreifenden Präventionsmaßnahmen, die in § 6 GwG als interne Sicherungsmaßnahmen bezeichnet und aufgelistet werden. Hierbei gilt, wie im gesamten GwG, ein risikobasierter Ansatz: Je höher das festgestellte Risiko zu bewerten ist, desto strenger und größer müssen die entsprechenden Abwehrmaßnahmen ausfallen.

46

b) Interne Sicherungsmaßnahmen

Nach § 6 Abs. 1 GwG haben Verpflichtete angemessene geschäfts- und kundenbezogene interne Sicherungsmaßnahmen zu schaffen, um die Risiken von Geldwäsche und von Terrorismusfinanzierung in Form von Grundsätzen, Verfahren und Kontrollen zu steuern und zu mindern. Angemessen sind solche Maßnahmen, die der jeweiligen Risikosituation entsprechen, die in der Risikoanalyse herausgearbeitet wurde, und diese hinreichend abdecken.⁶⁰ Die Verpflichteten haben die Funktionsfähigkeit der internen Sicherungsmaßnahmen zu überwachen und sie bei Bedarf zu aktualisieren. Nach § 6 Abs. 2 GwG gehören zu den internen Sicherungsmaßnahmen unter anderem die Bestellung eines Geldwäschebeauftragten,⁶¹ die Durchführung von Mitarbeiterschulungen in Bezug auf Typologien und aktuelle Methoden der Geldwäsche oder die Einrichtung eines Hinweisgebersystems.

47

Güterhändler mit Bargeldbegrenzung sind nicht dazu verpflichtet, interne Sicherungsmaßnahmen gemäß § 6 GwG zu errichten. Es empfiehlt sich allerdings aus oben genannten Gründen, auch mit einer eingeführten Bargeldgrenze im angemessenen Umfang geeignete Maßnahmen zur Geldwäscheprävention zu ergreifen. In § 6 Abs. 2 GwG sind nicht abschließende Regelbeispiele für interne Si-

48

⁵⁹ Angelehnt an die beispielhafte Risikoeinstufung in den Auslegungs- und Anwendungshinweisen der BaFin, vgl. BaFin, Auslegungs- und Anwendungshinweise, Oktober 2021, S. 12 f.

⁶⁰ Kaetzler, in: Zentes/Glaab, GwG, § 6 Rn. 22.

⁶¹ Zu Stellung und Aufgaben des Geldwäschebeauftragten siehe → Kaetzler, Kap. 22.

cherungsmaßnahmen genannt. Viele sind auch für Güterhändler gut umsetzbar, z. B. die Ausarbeitung von internen Grundsätzen, Verfahren und Kontrollen.

- 49 Aufgrund der grundsätzlichen Risikoexposition von Güterhändlern haben sich folgende spezifische Sicherungsmaßnahmen für Güterhändler etabliert, die nur zum Teil im Katalog des § 6 Abs. 2 GwG niedergeschrieben sind:

aa) Richtlinie zur Prävention von Geldwäsche

- 50 Empfehlenswert ist eine separate oder in eine allgemeine Compliance-Richtlinie eingegliederte Richtlinie zur Prävention von Geldwäsche. Im GwG ist diese Sicherungsmaßnahme als „interner Grundsatz“ in § 6 Abs. 2 Nr. 1 GwG genannt. Eine enge Orientierung an § 6 Abs. 2 Nr. 1 GwG ist durchaus sinnvoll; neben allgemeinen Ausführungen zum Begriff und Erscheinungsformen von Geldwäsche sollten Sorgfalts- und Dokumentationspflichten sowie die Erfüllung der Meldepflicht nach § 43 Abs. 1 GwG thematisiert werden. Letzterer Punkt beinhaltet nicht nur den Hinweis auf die Pflicht zur Abgabe von Verdachtsmeldungen, sondern auch die Beschreibung klarer Verantwortlichkeiten und Eskalationswege für den Fall, in dem ein verdächtiger Sachverhalt im Unternehmen bekannt wurde (sog. internes Verdachtsmeldewesen).⁶² Die Erstellung einer Geldwäschepräventionsrichtlinie ist für Güterhändler auch mit Bargeldgrenze empfehlenswert, da sie im Verdachtsfall dazu verpflichtet sind, Sorgfaltspflichten gegenüber ihren Kunden oder Geschäftspartnern durchzuführen. Daher sollten entsprechende Prozesse, Verantwortlichkeiten und Formulare zur Dokumentation im Unternehmen vorherrschen.

bb) Überprüfung von Geschäftspartnern

- 51 Die Überprüfung von Geschäftspartnern erfolgt in der Regel im Hinblick auf Korruptionsrisiken und dient dazu, das Unternehmen vor Reputations- und Haftungsrisiken zu schützen, die sich aus in- und ausländischen Korruptionsstraftatbeständen ergeben. Geschäftspartnerprüfungen decken gleichzeitig viele Elemente ab, die auch im Rahmen der Sorgfaltspflichten nach §§ 10 ff. GwG gefordert werden und stellen insofern einen Prüfungsprozess dar, der auch der Geldwäscheprävention dient. Zudem sind Geschäftspartnerprüfungen dazu geeignet, verdächtige Sachverhalte aufzudecken, die eine Verdachtsmeldung nach § 43 Abs. 1 GwG erforderlich machen können.

cc) Überwachung von Zahlungseingängen

- 52 Zahlungen aus einer unbekannten Quelle oder von einem unbekannten Konto sind ein Risikofaktor für Geldwäsche, der in der Praxis für Industrie- und Handelsunternehmen eine große Rolle spielt. Auch wenn mit der ungeprüften An-

62 Die BaFin hat in ihren Auslegungs- und Anwendungshinweisen die Voraussetzungen für das interne Verdachtsmeldewesen ausführlich beschrieben, woran sich Güterhändler gut orientieren können, vgl. BaFin, Auslegungs- und Anwendungshinweise, Oktober 2021, S. 75 ff.

nahme von Geldern aus illegaler Quelle nicht zwingend eine Strafbarkeit nach § 261 Abs. 6 StGB wegen leichtfertiger Geldwäsche einhergeht, kann damit zumindest ein erheblicher Reputationsschaden entstehen (siehe oben → Rn. 19). Unternehmen in Industrie und Handel, die eine gewisse Risikoexposition aufweisen, prüfen daher automatisiert oder stichprobenartig, ob Zahlungseingänge durch den Vertragspartner und von dem vorher festgelegten Konto des Vertragspartners erfolgen oder nicht. Inwieweit aus einer Zahlung durch unbekannte Dritte oder von einem unbekannten Konto ein Verdachtsfall erwächst, der an die FIU zu melden ist (siehe unten → Rn. 71 ff.).

Darüber hinaus bestehen vielfach schon Prozesse und Maßnahmen in Unternehmen, die auch der Geldwäscherprvention dienen, wie beispielsweise Sanktionslisten screenings,⁶³ Einholung von Kreditauskünften über Geschäftspartner oder eingerichtete Hinweisgebersysteme. **53**

c) Gruppenweite Pflichten

Verpflichtete, die Mutterunternehmen einer Gruppe sind, müssen nach § 9 Abs. 1 GwG eine Risikoanalyse für alle gruppenangehörigen Unternehmen nach § 1 Abs. 16 Nr. 2 bis 4 GwG durchführen und auf dieser Grundlage weitere gruppenweite Sicherungsmaßnahmen ergreifen. Normadressat ist nur das ultimative Mutterunternehmen einer Gruppe und nicht eine Zwischenobergesellschaft (vgl. § 1 Abs. 25 GwG). Die Erfüllung von gruppenweiten Pflichten gemäß § 9 GwG trifft zunächst nur diejenigen Güterhändler, die zur Einrichtung eines Risikomanagements verpflichtet sind (siehe § 4 Abs. 5 GwG).⁶⁴ **54**

In die gruppenweit zu erstellende Risikoanalyse sind gruppenangehörige Unternehmen miteinzubeziehen, soweit sie geldwäscherechtlichen Pflichten unterliegen. Gruppenangehörige Unternehmen, die als Güterhändler Bargeldgeschäfte über 10.000 EUR abgeschlossen haben und daher kein Risikomanagement inklusive Sicherungsmaßnahmen einführen müssen, sind daher ebenso wenig erfasst, wie ausländische Tochtergesellschaften, die nach ihrem lokalen Recht nicht Verpflichtete sind. Güterhändler, die Mutterunternehmen einer Gruppe sind, jedoch aufgrund eines Bargeldausschlusses kein Risikomanagement einführen müssen, unterliegen auch dann nicht den Pflichten nach § 9 Abs. 1 GwG, wenn ihre in- oder ausländischen Tochtergesellschaften weiter Bargeldgeschäfte **55**

63 Das Screening von Geschäftspartnern und auch Mitarbeitern wird irrtümlicherweise oft als Pflicht aus dem GwG gesehen. Rechtsgrundlagen sind jedoch die entsprechenden EU-Vorordnungen, deren Verstoß nach dem AWG sanktioniert wird, sowie die entsprechenden US-Sanktionslisten. Bei einem Treffer sollte, neben der Meldung an die Bundesbank, aber auch eine Verdachtsmeldung nach § 43 GwG abgegeben werden.

64 Im Referenten- und auch im Regierungsentwurf für ein Gesetz zur Umsetzung der 5. EU-Geldwäscherichtlinie war noch die Rede davon, dass die Privilegierung für Güterhändler nicht für die gruppenweiten Pflichten gelte. Erst nach Protest aus der Wirtschaft wurde die Rückausnahme nach Beratung im Finanzausschuss des Bundestages wieder gestrichen und stattdessen der klarstellende Passus in § 4 Abs. 5 GwG „einschließlich gruppenweiter Verfahren“ eingefügt.

tätigen. Allerdings müssen in dieser Konstellation aufgrund der Regelung des § 9 Abs. 4 GwG die gruppenangehörigen Unternehmen, deren Muttergesellschaft weder nach § 9 Abs. 1 GwG noch nach dem Recht ihres Sitzlandes gruppenweite Maßnahmen zu erfüllen hat, die Regelungen des § 9 GwG befolgen, sofern ihnen mindestens ein anderes Tochterunternehmen untergeordnet ist. Der Gesetzgeber hat diese Übertragung der gruppenweiten Pflichten aufgenommen, um Umgehungen der gruppenweiten Pflichten durch die Gründung einer Muttergesellschaft, die ohne operatives Geschäft nicht Verpflichtete ist, zu vermeiden.⁶⁵

- 56** Im Falle von EU-ausländischen Zweigstellen oder gruppenangehörigen Unternehmen müssen deutsche Mutterunternehmen sicherstellen, dass die in dem jeweiligen EU-Mitgliedstaat geltenden geldwäscherechtlichen Rechtsvorschriften eingehalten werden (§ 9 Abs. 2 GwG). Deutsche Mutterunternehmen, die über Zweigstellen oder gruppenangehörige Unternehmen in (Nicht-EU-)Drittstaaten verfügen, müssen unter Umständen nach § 9 Abs. 3 GwG sicherstellen, dass die Anforderungen nach dem deutschem Geldwäscherecht erfüllt sind, soweit das Recht des Drittstaates dies zulässt. Insoweit gilt das deutsche GwG also extraterritorial.

3. Kundensorgfaltspflichten

- 57** Die Sorgfaltspflichten in Bezug auf Kunden gehören zu den Kernpflichten der Geldwäscheprävention. Anders als die Überschrift des Dritten Abschnitts vermuten lässt, sind nicht nur auf Kunden Sorgfaltspflichten anzuwenden, sondern ganz grundsätzlich auf alle Vertrags- und Geschäftspartner. Entsprechend steht das Akronym „KYC“, das „Know Your Customer“ bedeutet, außerhalb der Finanzindustrie immer öfter für „Know Your Counterparty“. Die Sorgfaltspflichten bestehen aus den allgemeinen, verstärkten und vereinfachten Sorgfaltspflichten. Bereits die allgemeinen Sorgfaltspflichten umfassen eine umfangreiche Prüfung des Geschäftspartners samt Eigentums- und Kontrollstruktur bei juristischen Personen, Personengesellschaften und anderen Rechtsgestaltungen, im Rahmen derer nicht nur Angaben erhoben, sondern auch mittels offizieller Dokumente und ggf. Drittquellen überprüft werden müssen.

a) Auslösetatbestände der Sorgfaltspflichten für Güterhändler

- 58** Güterhändler müssen nicht bei jeder neu begründeten Geschäftsbeziehung Sorgfaltspflichten erfüllen, sondern nur in den in § 10 Abs. 6a Nr. 1 GwG genannten Fällen, also bei Transaktionen im Wert von mindestens 10.000 EUR über Kunstgegenstände, Transaktionen über Edelmetalle, bei welchen sie Barzahlungen über mindestens 2.000 EUR selbst oder durch Dritte tätigen oder entgegennehmen oder Transaktionen über sonstige Güter, bei welchen sie Barzahlungen über mindestens 10.000 EUR selbst oder durch Dritte tätigen oder entgegennehmen.

65 BT-Drs. 19/13827, S. 72.

Die Norm ist *lex specialis* zu § 10 Abs. 3 GwG, der die allgemeinen Eröffnungstatbestände für die Sorgfaltspflichten benennt.⁶⁶ § 10 Abs. 6a GwG ist identisch aufgebaut wie § 4 Abs. 5 GwG, der die Pflichten zur Einführung eines Risikomanagements regelt (siehe oben → Rn. 28 ff.). Auch hier zeigt sich wieder, dass der Gesetzgeber diejenigen Güterhändler privilegieren möchte, die keine Bargeldgeschäfte über 10.000 EUR tätigen.

Daneben müssen Güterhändler gemäß § 10 Abs. 3 Nr. 3 GwG auch im Verdachtsfall Sorgfaltspflichten erfüllen. Mit der Gesetzesnovellierung zum 1.1.2020 ist zwar der Verweis in der Spezialregelung § 10 Abs. 6a GwG für Güterhändler auf § 10 Abs. 3 Nr. 3 GwG unerklärlicherweise weggefallen. Letztere gilt jedoch ungeachtet etwaiger nach dem GwG oder anderen Gesetzen bestehender Ausnahmeregelungen, Befreiungen oder Schwellenbeträge und damit ungeachtet der Spezialregelung in § 10 Abs. 6a GwG. **59**

Die Durchführung der Sorgfaltspflichten bei Vorliegen eines Verdachtsfalls geht also regelmäßig mit der Abgabe einer Verdachtsmeldung einher. Letztere muss gemäß § 43 Abs. 1 GwG unverzüglich, also ohne schuldhaftes Zögern, erfolgen. Während also eine Verdachtsmeldung binnen kurzer Zeit abgegeben werden muss, ist die Durchführung der Sorgfaltspflichten in der Regel zeitaufwändiger und überdauert regelmäßig die bereits abgegebene Verdachtsmeldung. Sofern der Kunde oder Geschäftspartner nicht überobligatorisch identifiziert wurde, wird der meldende Güterhändler im Zeitpunkt der Meldung noch gar keine bzw. nicht ausreichende Informationen über beispielsweise die Eigentums- oder Kontrollstruktur, wirtschaftlich Berechtigte oder deren „PEP-Eigenschaften“ besitzen. In der Folge kann ein Güterhändler in der Regel nur eine mehr oder weniger unsubstantiierte Verdachtsmeldung abgeben und erst nach Durchführung allgemeiner Sorgfaltspflichten mit einer Mitteilung an die FIU ergänzende Informationen nachreichen. Der Geldwäschebekämpfung ist mit dieser Vorgehensweise kaum gedient.⁶⁷ **60**

Viel gravierender ist, dass der Verdachtsfall den Güterhändler regelmäßig vor ein Dilemma stellt. Denn die Durchführung der Sorgfaltspflichten bringt es mit sich, dass bei dem Geschäftspartner eine Reihe von Identifizierungsmerkmalen sowie Angaben zu den wirtschaftlich Berechtigten abgefragt werden. Ein Vertragspartner mit Grundkenntnissen im deutschen Geldwäscherecht könnte dadurch schnell misstrauisch werden und auf den Gedanken kommen, dass der Nachfragende eine Verdachtsmeldung erstattet hat.⁶⁸ Das in § 47 Abs. 1 GwG statuierte Verbot der Informationsweitergabe („Tipping Off-Verbot“)⁶⁹ verbietet es jedoch, den betroffenen Vertragspartner von einer beabsichtigten oder erstatteten Verdachtsmeldung in Kenntnis zu setzen. Die Durchführung von Sorgfaltspflichten nach einer zuvor erstatteten Verdachtsmeldung erhöht somit ganz wesentlich das **61**

⁶⁶ *Krais*, Geldwäsche und Compliance, S. 140.

⁶⁷ *Komma*, CB 2019, 197, 201.

⁶⁸ *Krais*, Geldwäsche und Compliance, S. 142.

⁶⁹ Zum Verbot der Informationsweitergabe im Detail unten → Rn. 80 ff.

Risiko, gegen das bußgeldbewehrte Verbot der Informationsweitergabe zu verstoßen. Da die nicht richtige oder nicht vollständige Durchführung von Sorgfaltspflichten ebenfalls bußgeldbewehrt ist, kann die spezielle Regelung für Güterhändler im GwG diese in die missliche Lage eines Befolgungskonflikts bringen, in dem sie entscheiden müssen, welche Norm sie befolgen bzw. verletzen.

- 62 Eine klare Handlungsempfehlung in diesem Dilemma existiert von Seiten der Aufsichtsbehörden derzeit nicht. Ein gangbarer Ausweg könnte sein, die Sorgfaltspflichten bei einem zu hohen Risiko, gegen das Verbot der Informationsweitergabe zu verstoßen, auszusetzen. So gibt es zumindest die „Interpretative Note“ zu Empfehlung 10 der FATF Recommendations vor, nach der sich der Verpflichtete in dem Fall, dass die Durchführung der Sorgfaltspflichten den (potenziellen) Kunden warnt, dafür entscheiden kann, diese Sorgfaltspflichten nicht durchzuführen und eine Verdachtsmeldung abzugeben.⁷⁰

b) Ausgewählte Aspekte der allgemeinen Sorgfaltspflichten

- 63 Die allgemeinen Sorgfaltspflichten sind im Wesentlichen von der Identifizierung des Vertragspartners und gegebenenfalls der für ihn auftretenden Personen sowie von etwaigen wirtschaftlich Berechtigten geprägt. Eine Identifizierung besteht aus der Feststellung der Identität durch die Erhebung von Angaben und die Überprüfung der Identität mittels durch das GwG vorgeschriebenen Dokumente und Unterlagen, wie beispielsweise Ausweisdokumente und Handelsregisterauszüge.
- 64 Insbesondere die Bestimmung des wirtschaftlich Berechtigten kann sich auch für routinierte Akteure aus dem Finanzsektor als aufwendig und kompliziert herausstellen. In ihren Auslegungs- und Anwendungshinweisen zum GwG nennen die Aufsichtsbehörden der Länder gesetzliche Konkretisierungsbeispiele und gibt eine Prüfungsabfolge für mehrstufige Beteiligungsstrukturen vor, an die sich Güterhändler bei der Bestimmung von wirtschaftlich Berechtigten halten sollten.⁷¹
- 65 Die identifizierten natürlichen Personen müssten darüber hinaus auf ihre Eigenschaft als politisch exponierte Person („PEP“), als Familienmitglied einer PEP oder als bekanntermaßen nahestehende Person einer PEP geprüft werden. Wie auch die Bestimmung der wirtschaftlich Berechtigten kann die Abklärung der PEP-Eigenschaft nicht nur über Internet-Recherchen oder kommerzielle Auskunftsdienste erfolgen, sondern auch mittels Selbstauskunftsbogen des Geschäftspartners. Inwieweit sich Verpflichtete allerdings auf die Selbstauskünfte

70 FATF (2012), The FATF Recommendations, Interpretative Note zu Empfehlung 10, A.3; *Barreto da Rosa*, in: Herzog/Achtelik, GwG, § 47 Rn. 5.

71 Auslegungs- und Anwendungshinweise zum Geldwäschegesetz (GwG) für Güterhändler, Immobilienmakler und andere Nichtfinanzunternehmen (Regierungspräsidien in Hessen) im Rahmen der Gemeinsamen Auslegungs- und Anwendungshinweisen der Länder der Bundesrepublik Deutschland (Stand Mai 2023), Ziff. 4.5.2 ff.

eines Geschäftspartners ohne weitere Recherchen in unabhängigen Quellen verlassen dürfen, ist eine Frage der Risikobewertung des Geschäftspartners.

c) Ausgewählte Aspekte der vereinfachten und verstärkten Sorgfaltspflichten

Neben den allgemeinen Sorgfaltspflichten können Güterhändler auch vereinfachte oder müssen verstärkte Sorgfaltspflichten unter den jeweiligen Voraussetzungen erfüllen.⁷² Die vereinfachten Sorgfaltspflichten spielen für Güterhändler regelmäßig keine Rolle, wenn man sich vor Augen führt, dass Güterhändler erst im Verdachtsfall oder bei Bargeldtransaktionen über 10.000 EUR überhaupt Sorgfaltspflichten zu erfüllen haben. In beiden Fällen erlaubt es das mit diesen Vorgängen einhergehende Risiko nicht, lediglich vereinfachte Sorgfaltspflichten durchzuführen. **66**

Anders sieht es hingegen bei den sogenannten verstärkten Sorgfaltspflichten aus. Verpflichtete haben zusätzlich zu den allgemeinen Sorgfaltspflichten in den folgenden Situationen verstärkte Sorgfaltspflichten zu erfüllen: **67**

- Der Vertragspartner oder der wirtschaftlich Berechtigte ist ein PEP, ein Familienmitglied einer PEP oder eine bekanntermaßen nahestehende Person einer PEP.
- In der Geschäftsbeziehung oder Transaktion ist ein Drittstaat mit hohem Risiko oder eine in diesem Drittstaat ansässige natürliche oder juristische Person beteiligt.
- Eine Transaktion liegt vor, die im Vergleich zu ähnlichen Fällen besonders komplex oder ungewöhnlich groß ist, einem ungewöhnlichen Transaktionsmuster folgt oder keinen offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck hat.
- Bei der vorliegenden Transaktion/Geschäftsbeziehung ist aufgrund der Risikoanalyse oder im Einzelfall ein erhöhtes Risiko festgestellt worden.

Die anschließend durchzuführenden „verstärkten“ Maßnahmen unterscheiden sich nach dem jeweiligen oben aufgezählten Auslösetatbestand. Bei Involvierung einer PEP oder einem im Einzelfall erhöhten Risiko muss beispielsweise ein Mitglied der Führungsebene der Begründung oder Fortführung der Geschäftsbeziehung zustimmen, die Herkunft der Vermögenswerte mit angemessenen Maßnahmen bestimmt und die Geschäftsbeziehung einer verstärkten kontinuierlichen Überwachung unterzogen werden.⁷³ Die Durchführung der zu ergreifenden Maßnahmen kann also durchaus aufwendig und zeitintensiv werden. **68**

Das Vorliegen eines oder mehrerer der Auslösetatbestände in § 15 GwG bedeutet für Güterhändler jedoch nur dann die Pflicht zur Erfüllung von verstärkten Sorgfaltspflichten, wenn auch die Voraussetzungen für die allgemeinen Sorgfaltspflichten vorliegen. **69**

⁷² BT-Drs. 18/11555, S. 117.

⁷³ Vgl. § 15 Abs. 4 Satz 1 GwG.

pflichten gegeben sind, also ein Verdachtsfall oder eine Bargeldtransaktion von über 10.000 EUR. Eine Geschäftsbeziehung in einen Drittstaat mit hohem Risiko ohne verdachtsfallbegründete Auffälligkeiten oder Bargeldzahlungen löst für Güterhändler formell gesehen also keine verstärkten Sorgfaltspflichten aus.

- 70 Güterhändler, die regelmäßig erst bei einem Verdachtsfall den Sorgfaltspflichten nachkommen, müssen sich fragen, ob ein Verdachtsfall nicht dazu führen muss, neben den allgemeinen auch die verstärkten Sorgfaltspflichten nach § 15 GwG durchzuführen, da ein im Einzelfall erhöhtes Risiko besteht. Nach der hier vertretenen Ansicht löst ein Verdachtsfall gemäß § 43 Abs. 1 GwG für Güterhändler nicht automatisch die Pflicht aus, nach § 15 GwG verstärkte Sorgfaltspflichten durchzuführen, sofern nicht zusätzlich eine der Fallgruppen in § 15 Abs. 3 GwG einschlägig ist.⁷⁴ Außerhalb der fallbasierten Auslösetatbestände in § 15 GwG kommt es auf die individuelle Risikoeinschätzung des Verpflichteten an, ob ein Sachverhalt zu verstärkten Sorgfaltspflichten führt oder nicht. Ein Verdachtsfall kann einzelfallbezogen ein erhöhtes Risiko i. S. v. § 15 Abs. 2 Satz 1 GwG darstellen und damit verstärkte Sorgfaltspflichten auslösen. Allerdings löst ein Verdachtsfall nicht stets verstärkte Sorgfaltspflichten aus. Ein Auslöseautomatismus besteht insofern nicht. Der Gesetzgeber schreibt in § 10 Abs. 3 Satz 1 Nr. 3 GwG lediglich vor, dass im Verdachtsfall zwingend die allgemeinen Sorgfaltspflichten von allen Verpflichteten zu erfüllen sind, nicht aber zwingend verstärkte Sorgfaltspflichten.

4. Pflicht zur Abgabe von Verdachtsmeldungen

- 71 Die zweite zentrale Pflicht für Güterhändler ist die Meldung verdächtiger Sachverhalte an die FIU. Die Meldung erfolgt elektronisch über das online Meldeportal goAML.⁷⁵ Grundlage einer jeden Verdachtsmeldung ist der Verdachtsfall. Zum 1.1.2024 mussten sich alle Adressaten des GwG unabhängig von der Abgabe einer Verdachtsmeldung auf dem Portal registrieren.⁷⁶ Für Güterhändler, die nicht mit Kunst, Schmuck, Uhren, Edelmetall, Edelsteinen, Kraftfahrzeugen, Schiffen, Motorbooten oder Luftfahrzeugen handeln, besteht die Pflicht zur Registrierung jedoch erst ab dem 1.1.2027.⁷⁷

a) Verdachtsfall und typische Verdachtsmomente

- 72 Wann ein Verdachtsfall vorliegt, kann eine Frage von Nuancen sein und ist häufig nicht leicht zu beantworten. In praktischer Hinsicht werden in den existierenden Typologie-Papieren und -Aufzählungen bestimmte Auffälligkeiten dargestellt, die Anhaltspunkte für einen Geldwäscheverdacht geben. Typologien sind je nach Kunde, Geschäft oder anderen Umständen ganz unterschiedlich zu be-

⁷⁴ Kraiss, in: BeckOK GwG, 16. Ed., § 10 Rn. 68.

⁷⁵ Vgl. <https://goaml.fiu.bund.de/Home> (zuletzt abgerufen am 2.2.2024).

⁷⁶ § 45 Abs. 1 Satz 2 i. V. m. § 59 Abs. 6 Satz 1 GwG.

⁷⁷ § 45 Abs. 1 Satz 2 i. V. m. § 59 Abs. 6 Satz 3 GwG.

werten. Teilweise ist bereits ein Anhaltspunkt ausreichend, um einen Verdachtsfall zu bejahen, in einem anderen Sachverhalt können hingegen selbst mehrere Anhaltspunkte keine Abgabe einer Verdachtsmeldung rechtfertigen. Als Regel gilt jedoch, je mehr Anhaltspunkte vorliegen, desto wahrscheinlicher ist ein Verdachtsfall.

Folgende Risikofaktoren kommen in der Praxis von Industrie- und Handelsunternehmen regelmäßig vor und können für sich genommen oder kumulativ einen Verdachtsfall begründen:⁷⁸

73

- **„untypisches“ oder „wirtschaftlich unsinniges“ Geschäft:** Das Geschäft passt nicht zu dem üblichen Geschäftsbereich des Kunden oder Geschäftspartners oder erscheint vor dem Hintergrund der sonstigen dahingehenden Geschäfte als für den Kunden wirtschaftlich nachteilig.
- **Angaben des Kunden stehen im Widerspruch zu anderweitig bekannten Informationen:** Angaben des Kunden widersprechen Auskünften von Dritten, z. B. Geschäftspartnern, Registern oder Datenbanken.
- **Unerwartete und nicht plausible Veränderung des Kunden-/Transaktionsverhaltens:** Kunde steigert die Bestellgrößen, ohne dass es dafür konkrete Anhaltspunkte gibt.
- **Kunde nutzt eine Vielzahl ähnlicher Adressen/Postfächer/Sammeladresse/Briefkastenfirmen:** Der Kunde nutzt bei verschiedenen Aufträgen verschiedene Rechnungs- oder Lieferadressen, ohne dafür einen nachvollziehbaren Grund zu offenbaren.
- **Zweifel an der Echtheit von zur Identifizierung vorgelegten Ausweisdokumenten:** Das vorgelegte Dokument erscheint z. B. wenig wertig in Bezug auf Auflösung und Gestaltung.
- **Angaben zur Identität des Vertragspartners, wirtschaftlich Berechtigten oder zu Zahlungsmodalitäten werden mehrfach korrigiert:** Der Kunde ändert ständig seine Aussagen bzgl. des Vertragspartners, ohne dass es dafür nachvollziehbare Gründe gibt.
- **Kunde weicht Nachfragen aus und/oder macht ungenaue oder nicht nachvollziehbare Angaben:** Der Kunde antwortet auf Anfragen, z. B. per E-Mail, nicht, oder weicht Nachfragen aus.
- **Abweichender Zahlungsleistender:** Die Überweisung selbst wird nicht von dem Kunden, sondern einem unbekannten Dritten (aus einem Drittstaat) geleistet, ohne dass dies angekündigt wurde oder plausibel ist.
- **Eingehende Bestellungen sind jeweils mit anderen Zahlungsmodalitäten versehen:** Der Kunde nutzt wiederholt unterschiedliche Bankverbindungen zur Zahlung, die nicht als Stammdaten erfasst wurden.

⁷⁸ Vgl. auch die Liste von typischen Verdachtskonstellationen für Güterhändler bei *Kaetzler*, in: Wohlschlägl-Aschberger, Geldwäscheprävention, S. 510 und die kommentierte Liste von Anhaltspunkten für mögliche Verdachtsfälle bei *Krais*, Geldwäsche und Compliance, 2. Aufl. 2022, S. 251 ff.

- 74 Den Verpflichteten wird bei der Einordnung und Bewertung von Anhaltspunkten im Hinblick auf einen Verdachtsfall ein gewisser Ermessensspielraum eingeräumt.⁷⁹ Dieser notwendige Ermessensspielraum resultiert daraus, dass der Gesetzgeber auf eine enumerative Aufzählung möglicher Konstellationen, in denen ein Verdachtsfall zu bejahen ist, bewusst verzichtet hat. Denn die Methoden der Geldwäsche sind einem raschen Wandel unterworfen und zu vielgestaltig, um im Einzelnen dargestellt zu werden.
- 75 In der Beurteilungsphase ist es Unternehmen nicht per se verwehrt, dem Kunden oder Geschäftspartner Fragen zu stellen, um eine Auffälligkeit zu plausibilisieren. In der Regel wird ihnen als kurzfristige Maßnahme zur Informationsbeschaffung oftmals auch nur die Kontaktaufnahme mit dem Kunden übrigbleiben. Viele auffällige Sachverhalte lassen sich auch oft überhaupt nur mit Hilfe des Vertragspartners aufklären.⁸⁰ Hier muss jedoch stets das Verbot der Informationsweitergabe beachtet werden (siehe unten → Rn. 80 ff.).
- 76 Die zeitliche (Ober-)Grenze der Aufklärungs- und Beurteilungsphase setzt § 43 Abs. 1 GwG fest, wonach Verdachtsmeldungen unverzüglich abgegeben werden müssen. Zwar gilt dieses Unverzüglichkeitsgebot nur für die Abgabe einer Verdachtsmeldung, wirkt sich aber auch auf den vorgelagerten Aufklärungs- und Beurteilungszeitraum aus, der ebenfalls „schnellstmöglich abgeschlossen“ werden muss.⁸¹

b) Folgen einer Verdachtsmeldung

- 77 Die Abgabe einer Verdachtsmeldung hat strafbefreiende Wirkung, führt jedoch auch dazu, dass der Verpflichtete eine Drei-Tages-Frist abwarten muss, um weiter eine Transaktion durchzuführen. Schließlich muss bei einer beabsichtigten oder bereits abgegebenen Verdachtsmeldung das Verbot der Informationsweitergabe beachtet werden.

aa) Strafbefreiende Wirkung

- 78 Eine Verdachtsmeldung gilt gemäß § 43 Abs. 4 GwG zugleich als strafbefreiende Selbstanzeige i. S. v. § 261 Abs. 8 StGB, wenn sie die für eine Anzeige nach § 261 Abs. 8 StGB erforderlichen Angaben enthält. Eine zusätzliche Anzeige nach § 261 Abs. 8 StGB zur Sicherstellung der Strafbefreiung von Verpflichteten und den sachbefassten Mitarbeitern ist daher nicht notwendig. Selbstverständlich bleibt es dem Verpflichteten unbenommen, neben der Verdachtsmeldung eine Strafanzeige nach § 158 StPO zu stellen.⁸²

79 BMF, Auslegungshinweise zur Handhabung des Verdachtsmeldewesens vom 6.11.2014, S. 3.

80 Ausführlich zur Beurteilungsphase für Güterhändler: *Komma*, CB 2019, 197.

81 BMF, Auslegungshinweise zur Handhabung des Verdachtsmeldewesens vom 6.11.2014, S. 3.

82 Vgl. hierzu *Rothe/Schlombs*, ZRFC 2018, 266, 271.

bb) Transaktionssperrfrist § 46 GwG

Nach einer abgegebenen Verdachtsmeldung ist die Transaktionssperrfrist nach § 46 Abs. 1 GwG einzuhalten. Der Verpflichtete darf Transaktionen frühestens durchführen, wenn ihm dazu die Zustimmung der FIU oder einer Staatsanwaltschaft erteilt wurde oder der dritte Werktag nach dem Abgangstag der Meldung verstrichen ist, ohne dass die Durchführung der Transaktion durch die FIU oder einer Staatsanwaltschaft untersagt wurde. In der Praxis kommt es selten vor, dass Behörden nach einer abgegebenen Verdachtsmeldung Güterhändler kontaktieren, sodass in der Regel nach Ablauf der Drei-Tages-Frist Transaktionen durchgeführt werden können. **79**

cc) Verbot der Informationsweitergabe (Tipping Off-Verbot)

Eine ganz wesentliche Regelung im Geldwäscherecht und für Güterhändler von großer Bedeutung ist das in § 47 Abs. 1 GwG statuierte Verbot der Informationsweitergabe. Es besagt, dass ein Verpflichteter weder dem Vertragspartner, dem Auftraggeber der Transaktion noch einem sonstigen Dritten über eine beabsichtigte oder erstattete Verdachtsmeldung in Kenntnis setzen darf. Das Verbot erfasst zudem Ermittlungsverfahren infolge einer Verdachtsmeldung und einem Auskunftsverlangen der FIU. Zweck des in § 47 Abs. 1 GwG statuierten Verbots ist es, staatsanwaltliche oder polizeiliche Ermittlungen nicht zu gefährden und zu verhindern, dass kriminelle Beweismittel unterdrückt werden (Verdunkelungsgefahr).⁸³ **80**

Ein „In Kenntnis setzen“ ist nicht nur bei ausdrücklichen, sondern auch bei stillschweigenden („impliziten“) Hinweisen anzunehmen.⁸⁴ In praktischer Hinsicht bedeutet das für Güterhändler eine sehr zurückhaltende Kommunikation in Geschäftsbeziehungen, in deren Verlauf eine Verdachtsmeldung abgegeben wurde. Es darf nicht der Anschein erweckt werden, dass eine Verdachtsmeldung beabsichtigt wird oder bereits abgegeben wurde. Dies ist insbesondere in solchen Situationen problematisch, in denen der Geschäftspartner oder Kunde wegen einer dringend benötigten Warenlieferung bereits nachfragt, der Güterhändler allerdings die Transaktionssperrfrist abwarten muss. Das Verbot der Informationsweitergabe hindert den Güterhändler daran, den wahren Grund der Verzögerung zu nennen. Daher sollten Güterhändler bei Nachfragen wenn möglich liefer- oder buchhalterische Gründe vorschieben, um die Verzögerung zu erklären. **81**

Mit der Umsetzung der 5. EU-Geldwäscherichtlinie ist für Güterhändler bzw. Güterhändlergruppen eine neue Problemdimension mit Blick auf das „Tipping Off“-Verbot hinzugekommen. Während nach alter Gesetzeslage das Verbot der Informationsweitergabe zwischen allen Verpflichteten, also auch Güterhändlern, die derselben Gruppe angehören, nicht galt, gilt seit dem 1.1.2020 diese Ausnahme nicht mehr für Güterhändlergruppen. Da andere gruppenangehörige **82**

⁸³ BT-Drs. 16/9038, S. 46.

⁸⁴ *Krais*, Geldwäsche und Compliance, S. 240.

Unternehmen als „sonstige Dritte“ anzunehmen sind, dürfen sich innerhalb einer Güterhändlergruppe die einzelnen Gesellschaften nicht mehr über beabsichtigte oder erstattete Verdachtsmeldungen austauschen. Der Geldwäscheprevention dient diese Änderung nicht. Aus Konzernsicht wäre es vielmehr gerade wünschenswert, dass sich gruppenangehörige Verpflichtete zu geldwäscheverdächtigen Sachverhalten umfassend austauschen und gegenseitig informieren, um einen Missbrauch der einzelnen Tochtergesellschaften zu Geldwäschezwecken zu verhindern. Mit § 9 Abs. 1 Nr. 3 GwG besteht für das Mutterunternehmen einer Gruppe i. S. v. § 1 Abs. 16 GwG sogar die Pflicht, Verfahren für den Informationsaustausch innerhalb der Gruppe zur Verhinderung von Geldwäsche und Terrorismusfinanzierung zu schaffen. Zu den Informationen gehören grundsätzlich auch Verdachtsmeldungen.⁸⁵ Eine denkbare Lösung könnte sein, über Auslagerung der Verdachtsmeldepflicht nach § 45 Abs. 4 i. V. m. § 6 Abs. 7 GwG zumindest einen gewissen Informationsfluss aufrechtzuerhalten.

IV. Fazit

- 83** Das deutsche Geldwäscherecht ist für Güterhändler eine Disziplin mit Licht und Schatten. Einerseits werden sie – anders als in vielen anderen EU-Ländern – durch ihre uneingeschränkte Einbeziehung in den Adressatenkreis des GwG überbordend verpflichtet. Im internationalen Wettbewerb kann das durchaus ein Nachteil sein, zumal die gesetzlichen Vorschriften und Terminologien vielfach nicht selbsterklärend sind. Zudem pönalisiert die Strafnorm des § 261 Abs. 6 StGB bereits die leichtfertige Verkenntung der illegalen Herkunft eines Gegenstandes und erhöht somit die Strafbarkeits- und Bußgeldrisiken in und von Unternehmen.
- 84** Andererseits können sich Güterhändler mit vergleichsweise einfachen Mitteln vielen gewerberechtlichen Pflichten entziehen und mit verhältnismäßig geringem Aufwand ihre Pflichten erfüllen. In der Einhaltung der für sie obligatorisch zu beachtenden Vorschriften des GwG sollten Güterhändler daher eine Chance sehen. Denn bereits mit dem Erkennen und Melden verdächtiger Sachverhalte sowie den anlassbezogenen Prüfungen von Kunden und Geschäftspartnern schützen sich Unternehmen, deren Geschäftsleitung und die einzelnen Mitarbeiter vor straf- und bußgeldrechtlichen Sanktionen.
- 85** Mit Blick auf die zahlreichen Erscheinungsformen der Geldwäsche und die daraus resultierenden Risiken für Unternehmen ist ein Blick in das GwG auch über die obligatorisch zu erfüllenden Pflichten hinaus ratsam. Denn ein wesentlicher Vorteil der Geldwäscheprevention im Vergleich zu anderen klassischen Compliance-Feldern ist, dass mit dem GwG im Grunde eine gesetzlich legitimierte und regelmäßig aktualisierte Mustervorlage zur Einrichtung einer wirksamen Präventionsstrategie existiert, die den Güterhändlern das Rüstzeug zur Einrichtung einer wirksamen Geldwäsche-Compliance-Organisation an die Hand gibt. Ins-

⁸⁵ Lang, in: Zentes/Glaab, GwG, § 9 Rn. 14.

besondere Unternehmen mit einem erhöhten Geldwäscherisiko sollten diese Gelegenheit nutzen, indem sie Elemente der Geldwäscheprävention aus dem GwG in ihr Compliance-Management-System integrieren.

24. Kapitel

Sanktions-Compliance als Teil eines effektiven Compliance-Management-Systems

I. Einleitung

Man denke nur an den nunmehr seit Februar 2022 andauernden Angriffskrieg Russlands gegen die Ukraine,¹ den durch den breitflächigen Terroranschlag der radikalislamistischen Hamas auf Israel am 7.10.2023 ausgelösten Krieg in Gaza,² zunehmende Spannungen zwischen den Vereinigten Staaten und deren Verbündeten auf der einen und China auf der anderen Seite,³ um festzustellen, dass die globale geopolitische Lage immer komplexer wird.

Sanktionen werden von vielen Staatenverbünden oder Einzelstaaten als probates Mittel erachtet, um als richtig empfundene politische oder humanitäre Ziele durchzusetzen.⁴

Für Wirtschaftsteilnehmer, insbesondere solche, die im Außenhandel tätig sind, ist es daher unabkömmlich, sich mit den Auswirkungen des für sie bzw. ihre Geschäftspartner anwendbaren Sanktionsrechts auseinanderzusetzen.

Neben evidenten Reputationsrisiken, die mit Geschäften einhergehen, die Diktatoren, Oligarchen oder bloß in bestimmten Ländern ansässige Geschäftspartner einbeziehen, können bestimmte Geschäfte oder Geschäfte mit bestimmten Geschäftspartnern zivil-, oder strafrechtliche Haftungsrisiken auslösen oder zum Ausschluss von öffentlichen Vergabeverfahren durch den Sanktionsgeber führen.⁵

Um solche Schäden von Organen, Mitarbeitern oder Gesellschaftern eines Unternehmens fernzuhalten, bietet es sich in der Praxis an, die Vermeidung von Sanktionsverstößen in das Compliance-Management-System einzubeziehen.

1 Siehe Zeit Online v. 25.2.2022, <https://www.zeit.de/politik/ausland/2022-02/russland-ukraine-invasion-krieg-chronik> (zuletzt abgerufen am 22.5.2024).

2 Siehe DW v. 9.11.2023, <https://www.dw.com/de/israel-hamas-krieg-eine-chronologie-der-eskalation/a-67345154> (zuletzt abgerufen: 22.5.2024).

3 Siehe FAZ v. 12.2.2021, <https://www.faz.net/aktuell/politik/ausland/china-und-usa-ringen-um-die-vorherrschaft-in-der-welt-17193014.html> (zuletzt abgerufen: 22.5.2024).

4 Vgl. Art. 1 Abs. 1 der Charta der Vereinten Nationen (UN-Charta) i.V.m. Art. 41 und 42 UN-Charta (Maßnahmen zur Wahrung oder Wiederherstellung des Weltfriedens und der internationalen Sicherheit).

5 Zu den Risiken und Nachteilen der Non-Compliance siehe → *Schulz*, Kap. 1 Rn. 11 m. w. N. Zu den Risiken der Non-Compliance im Zusammenhang der Exportkontrolle → *von Bodungen*, Kap. 25.

1. Terminologien und Begriffsverständnis

- 6 Im Bereich des Sanktionsrechts stößt man auf eine Vielzahl unterschiedlicher, definitionsbedürftiger Begriffe, etwa Embargos, Sanktionen, restriktive Maßnahmen oder Boykotte.⁶ Während diese zum Teil durch entsprechende Sanktionsverordnungen definiert werden, sind andere schlicht historisch gewachsen.
- 7 Trotz der denkbar langen Geschichte entsprechender Phänomene, die teils in das antike Griechenland rückverfolgbar sind,⁷ mangelt es noch immer an einem einheitliches Begriffsverständnis.⁸ So kommt es, dass, auch wenn sich die genannten Begriffe in Nuancen unterscheiden mögen, sie in der Praxis dennoch oftmals nahezu synonym verwendet werden.
- 8 Die wohl gängigste Unterscheidung ist diejenige zwischen Embargos und Sanktionen. Während Embargos sich nur auf die Beschränkung von Staaten fokussieren, richten sich Sanktionen auch gegen Individuen.⁹
- 9 Die Europäische Union (EU) bezeichnet hingegen sowohl Embargos als auch Sanktionen einheitlich als restriktive Maßnahmen.¹⁰
- 10 Als sinnvoll erachten wir die nachfolgend dargestellte Begriffsabgrenzung:
- 11 Ein Embargo ist eine Maßnahme, die sich allein gegen einen Staat richtet, während Sanktionen weitergehend verstanden werden.¹¹ Zusammenfassend lässt sich der Begriff der Sanktionen als Maßnahme eines Staates oder eines Staatenverbundes gegen einen anderen Staat verstehen, die dazu dient, den betroffenen Staat durch entsprechende Nachteile zu einer Verhaltensänderung zu bewegen.
- 12 Dieser Beitrag befasst sich vornehmlich mit einer Unterform von Sanktionen, den sog. Finanzsanktionen, die gegen bestimmte gelistete Individuen oder Organisationen gerichtet sind und maßgeblich deren Vermögenswerte mit Einfriergebieten belegen bzw. die Bereitstellung von Vermögenswerten an gelistete Individuen oder Organisationen mit Sanktionen belegen (vgl. → Rn. 47).

6 Vgl. *Alten*, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, Kap. 9 A. II, Rn. 5 ff.; *Sachs*, in: Sachs/Pelz, Außenwirtschaftsrecht, 3. Auflage 2024, I. Begriffe, Rn. 1; zum Begriff des „Boykotts“: *Pfeil/Mertgen*, Compliance im Außenwirtschaftsrecht, § 5 Rn. 205.

7 Zur historischen Entwicklung siehe: *Sachs*, in: Sachs/Pelz, Außenwirtschaftsrecht, II. Historische Entwicklung, Rn. 4.

8 *Alten*, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, Kap. 9 II, Rn. 5.

9 *Alten*, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, Kap. 9 II, Rn. 8.

10 Vgl. Grundprinzipien für den Einsatz restriktiver Maßnahmen (Sanktionen) <https://data.consilium.europa.eu/doc/document/ST-10198-2004-REV-1/de/pdf> (zuletzt abgerufen am 22.3.2024).

11 So auch: *Alten*, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, II., Rn. 7, welcher zu Recht auf die Ungenauigkeit etwaig in der Praxis üblicher Abgrenzung hinweist.

2. Sanktionen: Historie, Gründe und Ziele

Während in der ursprünglichen Form zunächst sog. Totalembargos verhängt wurden, welche den Wirtschaftsverkehr mit dem betroffenen Staat vollkommen untersagten,¹² entwickelt sich das moderne Sanktionsrecht zunehmend hin zu zielgerichteten Maßnahmen, Teilembargos bzw. sogenannten Smart Sanctions.¹³ Dieser Entwicklung liegt das Ziel zugrunde, die teilweise fatalen Folgen eines Totalembargos für die Zivilbevölkerung eines Staates zu reduzieren und stattdessen zielgerichtet die für den jeweiligen Missstand als verantwortlich anzusehenden politischen Eliten oder sonstigen Einflusssträger zu adressieren.¹⁴

Die Entwicklung hin zu Smart Sanctions lässt sich bereits am aktuellen Beispiel der Russland-Sanktionen der EU veranschaulichen. Gegen Russland wurde kein Totalembargo verhängt, sondern gezielte Maßnahmen gegen einzelne Sektoren¹⁵ oder Personen bzw. Organisationen.¹⁶

Gleichwohl lässt der – im erfolgten Umfang rechtlich nicht gebotene – Rückzug vieler international tätiger Unternehmen aus Russland ab Februar 2022¹⁷ vermuten, dass über die bloße Einhaltung verbindlichen Rechts hinaus auch die Vermeidung von Reputationsrisiken bzw. die Wahrnehmung als sog. Good Corporate Citizen für die Unternehmen von besonderem Stellenwert ist.¹⁸ Ein möglicher wirtschaftlicher Verlust durch die Einstellung der Tätigkeit wird daher häufig über das rechtlich erforderliche Maß hinaus in Kauf genommen. Dieser vorsichtige Ansatz erscheint allzu verständlich, schaut man sich die Presseberichterstattung über Unternehmensgruppen an, die ihre Tätigkeit (rechtskonform) fortsetzen.¹⁹

12 Grützner/Jakob, Compliance von A-Z, Embargo.

13 Zu der geschichtlichen Entwicklung des Sanktionsrechts, vgl. Sachs, in: Sachs/Pelz, Außenwirtschaftsrecht, IV. Rn. 4 ff.

14 Sanktionsleitlinien, S. 8 Ziff. 13; Nestler, in: Esser/Rübenstahl/Saliger/Tsambakakis, Wirtschaftsstrafrecht, § 18 AWG Rn. 17.

15 VO (EU) Nr. 833/2014.

16 VO (EU) Nr. 269/2014.

17 Z. B. McDonald's, vgl. tagesschau.de v. 16.5.2022, <https://www.tagesschau.de/wirtschaft/unternehmen/mcdonalds-russland-rueckzug-101.html#:~:text=Endgültiger%20Rückzug%20McDonald%27s%20verkauft%20russische%20Filialen&text=Nach%20über%2030%20Jahren%20in,Verkaufs%20wird%20McDonald%27s%20sie%20bezahlen> (zuletzt abgerufen am 17.3.2024), zahlreiche Unternehmen aus der Automobilindustrie, darunter Stellantis, Volkswagen, BMW, Mercedes-Benz Group, vgl. tagesschau.de v. 26.1.2023, <https://www.tagesschau.de/wirtschaft/unternehmen/russland-rueckzug-unternehmen-103.html> (zuletzt abgerufen am 17.3.2024).

18 Zur Bedeutung des Reputationsmanagements siehe → Schulz, Kap. 1 Rn. 23 ff. m. w. N.

19 Z. B. Unilever, vgl. Der Spiegel v. 5.7.2023, <https://www.spiegel.de/wirtschaft/unternehmen/ukraine-setzt-unilever-auf-ihre-liste-der-internationalen-kriegssponsoren-a-95155fa2-00e2-42cb-809e-0aead04a7f59> Bericht; Metro, vgl. Stern v. 10.7.2023, <https://www.stern.de/wirtschaft/russland-trotz-krieg-verdient-metro-vor-ort-geld-fuer-den-kreml-33634766.html> und unter Nennung verschiedener Unternehmensgruppen Frankfurter Rundschau v. 23.2.2024, <https://www.fr.de/wirtschaft/ukraine-krieg-sanktionen-russland-putin-handel-unternehmen->

II. Rechtsrahmen

- 16 Ein erster Schritt für die Beachtung von Sanktionen im Unternehmen sollte die Bestandserfassung derjenigen Sanktionsregime sein, die für ein Unternehmen potenziell relevant sind.
- 17 Als „Faustregel“ sollte immer und unbedingt das Sanktionsrecht des jeweiligen Sitzstaates bzw. des übergeordneten Staatenverbundes beachtet werden.
- 18 Wichtige Sanktionsregime können aber auch solche sein, die von Staaten(-verbünden) verhängt werden, mit denen ein Unternehmen einen bedeutenden Teil seines Umsatzes erwirtschaftet. Typischerweise beachten global agierende Unternehmen mit Sitz in Deutschland (im zulässigen Umfang) auch Sanktionsregime der Vereinigten Staaten von Amerika (US) oder Großbritanniens (UK).
- 19 Zudem kann es ratsam sein, die Sanktionsregime solcher Staaten zu beachten, in denen ein Unternehmen Tochterunternehmen, Joint Ventures oder Repräsentanten unterhält.
- 20 Für Unternehmensvertreter können darüber hinaus auch Sanktionsregime von Drittstaaten relevant werden, etwa wenn sie deren Staatsbürgerschaften oder Aufenthaltstitel besitzen.

1. UN-Sanktionen

- 21 Im Allgemeinen dürften die Vereinten Nationen (UN) wohl als der wichtigste globale Sanktionsgeber betrachtet werden. In Bezug auf Russland steht die UN gleichwohl vor dem Problem, dass der Beschluss entsprechender Resolutionen regelmäßig am Gebrauch des Vetorechts Russlands als ständiges Mitglied des UN-Sicherheitsrates scheitert (Art. 27 Abs. 3 i.V.m. Art. 23 Abs. 1 der UN-Charta).²⁰ Die Mitgliedstaaten wurden daher eigenständig tätig.
- 22 Zuständiges Gremium für die Verhängung von UN-Sanktionen ist der UN-Sicherheitsrat, der gemäß Art. 24 der UN-Charta die Verantwortung für die Wahrung des Weltfriedens und der internationalen Sicherheit innehat. Als solches kann der UN-Sicherheitsrat gemäß Art. 39 UN-Charta feststellen, ob eine Bedrohung bzw. ein Bruch des Friedens oder eine Angriffshandlung vorliegt, und ist berechtigt, Maßnahmen nach Art. 41 und 42 der UN-Charta zu beschließen.
- 23 Jenseits des ausgeschlossenen Einsatzes von Waffengewalt sieht Art. 41 UN-Charta beispielhaft die vollständige oder teilweise Unterbrechung der Wirtschaftsbeziehungen vor, um Beschlüssen des UN-Sicherheitsrates Wirksamkeit zu verleihen. Demgegenüber sieht Art. 42 der UN-Charta sogar militärische Einsätze als mögliche Maßnahme vor, sollte der UN-Sicherheitsrat der Auffassung

geschaefte-verluste-wirtschaft-zr-92851228.html Bericht vom 23.2.2024 (alle hier genannten Quellen zuletzt abgerufen am 17.3.2024).

20 Vgl. etwa Zeit online v. 26.2.2022, <https://www.zeit.de/politik/ausland/2022-02/krieg-ukraine-un-sicherheitsrat-resolution-veto-russland-china> (zuletzt abgerufen am 22.3.2024).

sein, dass die in Art. 41 der UN-Charta vorgesehenen Maßnahmen unzulänglich seien oder sich als unzulänglich erwiesen hätten.

Sollte der UN-Sicherheitsrat eine Maßnahme, etwa eine Sanktionsmaßnahme im Sinne des Art. 41 der UN-Charta, beschließen, so entfalten die UN-Sanktionen grundsätzlich und aus sich heraus zunächst keine unmittelbare Rechtswirkung für natürliche oder juristische Personen in Deutschland.²¹ Die Mitgliedstaaten der UN sind gleichwohl verpflichtet, beschlossene UN-Sanktionen umzusetzen (Art. 25, 48 UN-Charta). Deutschland hat als Mitgliedstaat der EU die Umsetzungspflicht auf diese delegiert (unten → Rn. 39). Zudem sind UN-Sanktionen neuerdings in Deutschland auch schon vor Umsetzung durch Rechtsakt der EU bindend, vgl. § 5a Außenwirtschaftsgesetz (AWG) (unten → Rn. 109).

Sanktionen der UN ist schließlich aufgrund ihrer Aktualität, der Umsetzungspflicht durch ihre Mitgliedstaaten sowie des Vorbildcharakters für andere Staaten eine erhöhte Bedeutung beizumessen. **25**

2. EU-Sanktionen

Von herausgehobener Bedeutung für deutsche Wirtschaftsteilnehmer sind auch und insbesondere die Sanktionen der EU. **26**

Sanktionen der EU werden übergreifend auch als restriktive Maßnahmen²² bezeichnet, die überall dort Anwendung finden sollen, wo eine Verbindung zur EU besteht (→ Rn. 28 ff.).²³ **27**

a) Anwendungsbereich

Der Anwendungsbereich der EU-Sanktionen²⁴ wird über territoriale Anknüpfungspunkte (Territorialprinzip)²⁵ oder personelle Anknüpfungspunkte (Personalprinzip)²⁶ eröffnet. Nach den Standardklauseln der EU-Sanktionsleitlinien²⁷ finden EU-Sanktionen unter anderem Anwendung **28**

²¹ Sattler, JuS 2019, 18, 18.

²² Grundprinzipien für den Einsatz restriktiver Maßnahmen (Sanktionen) (7.6.2004), S. 1 ff.

²³ Sanktionsleitlinien, Ratsdokument Nr. 5664/18 vom 4.5.2018 (**Sanktionsleitlinien**), S. 19 Ziff. 51 5.

²⁴ EU-Sanktionen werden durch Verordnungen ergriffen, die gemäß Art. 288 Abs. 2 Satz 1 Vertrag über die Arbeitsweise der Europäischen Union (**AEUV**) allgemeine Geltung entfalten. Sie sind in all ihren Teilen verbindlich und gelten unmittelbar in jedem Mitgliedstaat, Art. 288 Abs. 2 Satz 2 AEUV.

²⁵ Alten, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, 2. Territoriale Anknüpfung, Rn. 25.

²⁶ Sachs, in: Sachs/Pelz, Außenwirtschaftsrecht, 3. Anwendungsbereich, Rn. 342; Alten, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, Kap. 9, Rn. 30.

²⁷ Sanktionsleitlinien, S. 42, Ziff. 88.

Teil 3 Besondere Aufgaben und Anwendungsfelder

- im Gebiet der Union, einschließlich ihres Luftraums, an Bord der Luftfahrzeuge und Schiffe, die der Hoheitsgewalt eines Mitgliedstaats unterstehen,
 - sowie für natürliche Personen, die die Staatsangehörigkeit eines Mitgliedstaats besitzen – hierzu zählen auch doppelte Staatsangehörigkeiten²⁸ – oder
 - für juristische Personen, Organisationen und Einrichtungen, die nach dem Recht eines Mitgliedstaats gegründet worden sind,
 - innerhalb und außerhalb des Gebiets der Union
 - sowie für alle juristischen Personen, Organisationen oder Einrichtungen hinsichtlich aller Geschäfte, die ganz oder teilweise innerhalb der Union betrieben werden.
- 29 Dies bedeutet, dass sich alle natürlichen Personen, im Ergebnis also etwa auch Reisende aus Drittstaaten, welche sich nur vorübergehend im Hoheitsgebiet eines EU-Mitgliedstaats aufhalten, an das gültige Sanktionsrecht halten müssen. Dies ergibt sich aus dem Territorialprinzip.²⁹
- 30 Aus dem Personalprinzip ergibt sich wiederum, dass Wirtschaftsteilnehmer aus der EU, unabhängig vom derzeitigen Aufenthalts- bzw. Wohnsitzort, EU-Sanktionsrecht zu beachten haben.³⁰ Für deutsche natürliche Personen sind daher die EU-Sanktionen stets relevant.
- 31 Gleiches gilt für juristische Personen, welche nach deutschem Recht gegründet worden sind.
- 32 In der Praxis stellt sich in diesem Zusammenhang oft die Frage, ob etwa auch Tochtergesellschaften in Nicht-EU-Staaten das EU-Sanktionsrecht zu beachten haben. Bei der Beantwortung dieser Frage ist ein gewisses Feingefühl gefragt. Während die ausländische Tochtergesellschaft mangels territorialen oder personalen Anknüpfungspunkts grundsätzlich nicht selbst dem EU-Sanktionsrecht unterfällt, könnten Organmitglieder oder sachbefasste Mitarbeiter aufgrund der Staatsbürgerschaft eines EU-Mitgliedstaats in den Anwendungsbereich von EU-Sanktionen fallen, bestimmte Handlungen Vertretern des in Deutschland bzw. einem anderen EU-Mitgliedstaat ansässigen Mutterunternehmens zugerechnet werden (z. B. bei Gesellschaftervorbehalten oder weil Vertreter des Mutterunternehmens im Beirat oder Aufsichtsorgan der Tochtergesellschaft sitzen) oder Geschäfte als ganz oder teilweise innerhalb der EU betrieben angesehen werden.³¹
- 33 Eine Besonderheit hierzu gilt für die restriktiven Maßnahmen aus der Verordnung (EU) Nr. 833/2014 (Russland-Sanktionen). Durch die Verabschiedung der Verordnung (EU) 2024/1745 des Rates vom 24.6.2024 (**14. Sanktionspaket**) sind EU-Rechtsunterworfenen verpflichtet, sich „nach besten Kräften“ zu bemü-

28 Pfeil/Mertgen, in: Compliance im Außenwirtschaftsrecht, § 5 Rn. 14.

29 Alten, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, Kap. 9 II, Rn. 25.

30 Alten, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, Kap. 9 II, Rn. 30 ff.

31 Wiedmann/Will, RIW 2022, 173, 174.

hen sicherzustellen, dass außerhalb der Union niedergelassene juristische Personen, Organisationen oder Einrichtungen, die sich in ihrem Eigentum befinden oder unter ihrer Kontrolle stehen, nicht an Aktivitäten beteiligt sind, die die restriktiven Maßnahmen untergraben (vgl. Art. 8a der Verordnung (EU) 833/2014). Nach dem Erwägungsgrund 30 des 14. Sanktionspakets werden unter „Bemühen nach besten Kräften“ diejenigen Handlungen verstanden, welche geeignet und notwendig sind, um zu erreichen, dass die restriktiven Maßnahmen der Verordnung (EU) 833/2014 nicht untergraben werden.

Damit ist etwa gemeint, dass EU-Rechtsunterworfenen geeignete Strategien, Kontrollen und Verfahren implementieren, um die Untergrabung der restriktiven Maßnahmen zu verhindern. Abzuwarten bleibt, welche konkreten Anforderungen die EU noch an ein „Bemühen nach besten Kräften“ stellen wird. Auch wenn Erwägungsgrund 30 den Umfang der erforderlichen Maßnahmen auf solche eingrenzt, die durchführbar sind und damit auf den Verhältnismäßigkeitsgrundsatz anspielt, dürften EU-Unternehmen gut daran tun, die Undurchführbarkeit und Unverhältnismäßigkeit nicht vorschnell anzunehmen. Eine fehlende Durchführbarkeit dürfte dann angenommen werden, wenn die in Drittstaaten ansässigen Tochtergesellschaften gegenläufigem Sanktionsrecht des Staates unterworfen sind, in dem sie ihren Sitz haben. Davon abgesehen dürfte es bereits derzeit vielerorts gelebter Praxis entsprechen, in Drittstaaten ansässige Tochterunternehmen über unternehmensinterne Richtlinien an die Einhaltung von EU-Sanktionen zu binden. Eine solche grundsätzliche Bindung an EU-Sanktionen bietet sich aus Sicht der Verfasser an, um ein „Bemühen“ nachzuweisen. **34**

Insgesamt scheint sich die EU hierbei den „Secondary Sanctions“ anzunähern, welche aus US-Sanktionsprogrammen bekannt sind und seitens EU in der Vergangenheit teils scharf kritisiert wurden (vgl. → Rn. 132). Zwar verpflichtet Art. 8a der Verordnung (EU) 833/2014 keine Nicht-EU-Rechtsunterworfenen zur Einhaltung des EU-Rechts, faktisch wird allerdings die Einhaltung über die Verpflichtung des Mutterunternehmens erreicht. Damit dürfte, ähnlich wie bei der Verhängung von „Secondary Sanctions“, ein extritorialer Effekt einhergehen, dessen Vereinbarkeit mit dem Völkerrecht zumindest angezweifelt werden darf. **35**

b) Grundlage der EU-Sanktionen

Die restriktiven Maßnahmen der EU³² basieren in der Regel auf UN-Resolutionen und werden durch Beschlüsse der Gemeinsamen Außen- und Sicherheitspolitik (**GASP-Beschlüsse**) gem. Art. 29 Satz 1 EU-Vertrag verhängt.³³ **36**

Neben solchen Sanktionen, welche auf UN-Sanktionen beruhen, kann die EU auch eigenständige Sanktionen durch GASP-Beschlüsse festsetzen.³⁴ **37**

32 Grundprinzipien für den Einsatz restriktiver Maßnahmen (Sanktionen) (7.6.2004), S. 1 ff.

33 Sanktionsleitlinien, S. 6, Ziff. 7.

34 Sanktionsleitlinien, S. 5, Ziff. 3 und 4, Grundprinzipien für den Einsatz restriktiver Maßnahmen (Sanktionen) (7.6.2004), S. 1, Ziff. 1.

- 38 Nachdem die Maßnahmen, wie etwa Finanzsanktionen oder sektorbezogene Maßnahmen, in den GASP-Beschlüssen verhängt wurden, werden sie gem. Art. 215 Vertrag über die Arbeitsweise der Europäischen Union (AEUV) durch EU-Verordnungen umgesetzt.³⁵
- 39 Solche EU-Verordnungen haben gemäß Art. 288 Abs. 2 Satz 1 AEUV allgemeine Geltung. Sie sind gemäß Art. 288 Abs. 2 Satz 2 AEUV in all ihren Teilen verbindlich und gelten unmittelbar in jedem Mitgliedstaat.³⁶
- 40 Demgegenüber gibt es allerdings auch solche restriktiven Maßnahmen, welche nur einzelstaatlich durchgesetzt werden können. Hierzu zählen etwa Waffenembargos,³⁷ aber auch Einreisebeschränkungen. Solche einzelstaatlich durchzusetzende Maßnahmen werden durch die Mitgliedstaaten selbst beschlossen, welche wiederum rechtlich verpflichtet sind, im Einklang mit den GASP-Beschlüssen des Rates zu handeln.³⁸

c) Auslegung der EU-Sanktionen

- 41 Für die Auslegung von EU-Sanktionen gilt die klassische juristische Methodenlehre,³⁹ bei der der Wortlaut im Vordergrund steht. Da die Auslegung den Rechtsanwender zum Teil vor Hürden stellt, hat die EU für Fragen hinsichtlich der Anwendung und Auslegung des Sanktionsrechts zahlreiche unverbindliche Arbeitshilfen entworfen, die in der Praxis als sog. „Soft Law“ angesehen werden sollten.⁴⁰
- 42 Hierzu zählen etwa das Best-Practice-Dokument,⁴¹ der Kommissionsleitfaden⁴² sowie in Bezug auf Russland-Sanktionen die Commission Consolidated FAQs.⁴³
- 43 Zusätzlich gibt es Arbeits- und Auslegungshilfen von nationalen Behörden wie etwa dem Bundesamt für Ausfuhrkontrolle in Bezug auf sektorbezogene Sanktionen (BAFA)⁴⁴ oder Hilfen der Bundesbank in Bezug auf Finanzsanktionen

35 *Niedernhuber*, GSZ-Sonderausgabe 2022, 32, 33.

36 Sanktionsleitlinien, S. 6, Ziff. 7.

37 Eine Liste der Länder, gegen welche Embargos verhängt wurden, ist unter https://www.bafa.de/DE/Aussenwirtschaft/Ausfuhrkontrolle/Embargos/embargos_node.html abrufbar (zuletzt abgerufen am 22.3.2024).

38 Sanktionsleitlinien, S. 6, Ziff. 7.

39 Vgl. zur juristischen Methodenlehre im Unionskontext, *Rehbahn*, ZfPW 2016, 281.

40 <https://www.consilium.europa.eu/de/policies/sanctions/> (zuletzt abgerufen am 22.3.2024).

41 EU, Aktualisierung der vorbildlichen Verfahren der EU für die wirksame Umsetzung restriktiver Maßnahmen (Sanktionen), Dok.-Nr. 10572/22 v. 27.6.2022.

42 Vermerk der Kommission v. 25.8.2017, Leitfaden der Kommission für die Anwendung bestimmter Vorschriften der VO (EU) Nr. 833/2014, Abl. EU Nr. L 229/1 v 31.7.2014, Dok.-Nr. C (2017) 5738.

43 https://finance.ec.europa.eu/document/download/66e8fd7d-8057-4b9b-96c2-5e54bf573cd1_en?filename=fags-sanctions-russia-consolidated_en.pdf, Stand: 1.3.2024 (zuletzt abgerufen am 22.3.2024).

44 https://www.bafa.de/DE/Aussenwirtschaft/Ausfuhrkontrolle/Arbeitshilfen/arbeitshilfen_node.html (zuletzt abgerufen am 22.3.2024).

bzw. den Finanz- oder Kapitalmarktsektor betreffende Sanktionen.⁴⁵ Für den Fall, dass UK-Sanktionen Relevanz entfalten, sollten zusätzlich die Arbeitshilfen des Office of Financial Sanctions Implementation HM Treasury (OFSI) herangezogen werden.⁴⁶ Diese können in der Praxis, mit Blick auf die EU-Vergangenheit Großbritanniens und daraus hervorgehende Parallelen zu EU-Sanktionen, auch ohne UK-Bezug im Hinblick auf mögliche Auslegungsschwierigkeiten als zusätzliche Interpretationshilfe herangezogen werden.

3. Aufbau der EU-Sanktionen

Die Sanktionen der EU sind als sogenannte Smart Sanctions ausgestaltet und basieren im Regelfall auf einer Art „Baukastenprinzip“. Dies bedeutet, dass zahlreiche bereits entwickelte Sanktionsmaßnahmen in ähnlicher Form je nach Sanktionsziel eingesetzt werden können. Diese erarbeiteten Maßnahmen sind aus Effektivitätsgründen standardisiert. Im Ergebnis wurden einheitliche Definitionen und Standardformulierungen erarbeitet, welche die EU in den Sanktionsleitlinien darstellt und beschreibt.⁴⁷ **44**

Allerdings sind darüber hinausgehende neue Maßnahmen denkbar, da die Maßnahmenkataloge des Baukastenprinzips nicht abschließend sind.⁴⁸ **45**

Im hiesigen Kontext bietet es sich an, sich auf die Standardmaßnahmen mit höchster Relevanz für die breite Masse der Anwender zu fokussieren. Diese dürften zum einen in Ein- und Ausfuhrbeschränkungen zu sehen sein,⁴⁹ zum anderen, und hier wohl am wichtigsten, im Bereich der Finanzsanktionen bzw. Finanzrestriktionen. **46**

a) Listenprinzip

Da die als Smart Sanctions ausgestalteten Sanktionen nicht einen Staat als Ganzes, sondern nur bestimmte Personen, Güter oder Bereiche betreffen, arbeitet die EU oftmals mit Listen,⁵⁰ welche als Anhänge zu den Verordnungen beigelegt sind. Auf solchen Listen sind die entsprechenden Güter oder Personen, die von den Maßnahmen betroffen sind, niedergeschrieben (sogenanntes „**strenges Listenprinzip**“).⁵¹ **47**

45 Bspw. Häufig gestellte Fragen zum Thema Finanzsanktionen, abzurufen unter <https://www.bundesbank.de/de/service/finanzsanktionen> (zuletzt abgerufen am 22.3.2024).

46 OFSI, UK Financial Sanctions: General Guidance, Stand 8.2022; OFSI, Russia Guidance, Stand 3.2023.

47 Vgl. Sanktionsleitlinien.

48 Dies ergibt sich schon aus den Grundprinzipien, nach welchen der Rat an der Weiterentwicklung des Sanktionsinstrumentariums arbeiten und dieses dabei auch an das neue Sicherheitsumfeld anpassen wird. Vgl. Grundprinzipien für den Einsatz restriktiver Maßnahmen (Sanktionen), Ziff. 7f.

49 Siehe auch → von Bodungen, Kap. 25.

50 Nestler, in: Esser/Rübenstahl/Saliger/Tsambikakis, Wirtschaftsstrafrecht, § 18 AWG Rn. 18.

51 Sattler, JuS 2019, 18, 20.

- 48** Wegen des strengen Listenprinzips sind im Grundsatz nur die gelisteten Personen, Organisationen und Einrichtungen von den Sanktionen betroffen. Ein Screening des Geschäftspartners ist zwingend erforderlich, um das Risiko, gegen Finanzsanktionen zu verstoßen, zu reduzieren (→ Rn. 214 ff.).
- 49** Dies bedeutet für Unternehmen allerdings nicht, dass nur der direkte Geschäftspartner nicht gelistet ist. Vielmehr muss darüber hinaus auch bedacht werden, dass ein Verstoßrisiko besteht, wenn der Geschäftspartner eine ausreichend enge Verbindung zu einer gelisteten Person, Organisation oder Einrichtung aufweist.⁵² Hierbei sei etwa an Streckengeschäfte, komplexe Beteiligungsstrukturen, Strohmankonstellationen oder mögliche Umgehungstaktiken gedacht (→ Rn. 84).
- 50** Wegen des strengen Listenprinzips ist daher ein Screening sehr wichtig. Nur so kann die Einhaltung der Sanktionen, insbesondere der Finanzsanktionen gelingen.

b) Finanzsanktionen

- 51** Unter Finanzsanktionen versteht man die Einschränkungen des Kapital- und Zahlungsverkehrs. Diese können in der Anwendung unterschiedlich ausgestaltet sein. So ist beispielsweise an bestimmte Genehmigungsvorbehalte, Verbote oder Ausschlüsse von Handelsplätzen zu denken.
- 52** Inhaltlich haben Finanzsanktionen aber das Ziel gemeinsam, die wirtschaftliche Freiheit der sanktionierten Person, Organisation oder Einrichtung einzuschränken.
- 53** Hierbei sind insbesondere das Einfriergebot (vgl. → Rn. 90 ff.) und das Bereitstellungsverbot (vgl. → Rn. 77 ff.) als Finanzsanktionen im engeren Sinne und schwerwiegendste restriktive Maßnahmen zu nennen.
- 54** Das Einfriergebot und das Bereitstellungsverbot werden zusammen als restriktive Maßnahme gegen sanktionierte Personen beschlossen. So kann nämlich erreicht werden, dass die sanktionierte Person zum einen nicht mehr über relevante wirtschaftliche Mittel verfügen kann, und zum anderen, dass diese keine neuen wirtschaftlichen Mittel von Dritten erhält. In Kombination führen das Einfriergebot und das Bereitstellungsverbot daher zu einem effektiven Ausschluss der sanktionierten Person vom Wirtschaftsleben. Allerdings sieht jede Verordnung Befreiungen und Ausnahmen, maßgeblich zu humanitären Zwecken, vor.⁵³

aa) Begriffsdefinitionen

- 55** Die EU-Sanktionen arbeiten an vielen Stellen mit Legaldefinitionen. Diese gibt es sowohl im Zusammenhang mit dem Bereitstellungsverbot als auch mit dem

⁵² *Vogt/Arend*, in: Sachs/Pelz, Außenwirtschaftsrecht, 1. Einfriergebot und Bereitstellungsverbot, Rn. 125.

⁵³ Vorbildliche Verfahren der EU für die wirksame Umsetzung restriktiver Maßnahmen, S. 13.

Einfriergebot. Solche Legaldefinitionen sind zumeist zu Beginn der jeweiligen EU-Verordnung in Artikel 1 bei den Begriffsbestimmungen zu finden.

Nachfolgend einige Definitionen, die im Zusammenhang mit dem Bereitstellungsverbot und dem Einfriergebot maßgeblich sind. **56**

(1) Gelder

Unter „Geldern“ sind finanzielle Vermögenswerte und Vorteile jeder Art zu verstehen, die folgendes einschließen, aber nicht darauf beschränkt sind.⁵⁴ **57**

- Bargeld, Schecks, Geldforderungen, Wechsel, Zahlungsanweisungen und andere Zahlungsmittel,
- Einlagen bei Finanzinstituten oder anderen Einrichtungen, Guthaben auf Konten, Zahlungsansprüche und verbrieft Forderungen,
- öffentlich und privat gehandelte Wertpapiere und Schuldtitel einschließlich Aktien und Anteilen, Wertpapierzertifikate, Obligationen, Schuldscheine, Optionsscheine, Pfandbriefe und Derivate,
- Zinserträge, Dividenden und andere Einkünfte oder Wertzuwächse aus Vermögenswerten,
- Kredite, Rechte auf Verrechnung, Bürgschaften, Vertragserfüllungsgarantien und andere finanzielle Ansprüche,
- Akkreditive, Konnossemente, Übereignungsurkunden und
- Dokumente zur Verbriefung von Anteilen an Fondsvermögen oder anderen Finanzressourcen.

Die Definition zeigt, dass der Begriff der Gelder sehr weit zu verstehen ist und sich nicht nur auf Bargeld oder Giralgeld bezieht. In der Praxis bedeutet dies, dass Mitarbeiter entsprechend geschult werden und erkennen können, dass als Gelder nicht nur, wie möglicherweise landläufig angenommen, Bargelder oder Gelder von Konten gemeint sind. **58**

(2) Wirtschaftliche Ressourcen

Wirtschaftliche Ressourcen sind gemäß der Standarddefinition derart definiert, als es sich hierbei um Vermögenswerte jeder Art handelt – unabhängig davon, ob materielle oder immaterielle, bewegliche oder unbewegliche –, die keine „Gelder“ sind, aber für den Erwerb von „Geldern“, Waren oder Dienstleistungen verwendet werden können.⁵⁵ Diese Begriffsbestimmung findet sich beispielhaft in Art. 1 d) VO (EU) Nr. 269/2014. **59**

Es kommt im Ergebnis darauf an, ob der Vermögenswert im Rechtsverkehr einen irgendwie gearteten Gegenwert besitzt oder sonstigen Vorteil verschaffen kann. Der Begriff soll einen möglichst umfassenden, lückenlosen Ausschluss der Zielperson vom Wirtschaftsverkehr in der Union gewährleisten. Durch das weite Be- **60**

⁵⁴ Siehe auch Sanktionsleitlinien, S. 26, Ziff. 60 und Art. 1 g) VO (EU) Nr. 269/2014.

⁵⁵ Siehe auch Sanktionsleitlinien, S. 26, Ziff. 61.

griffsverständnis, aber auch durch die zusätzliche Erwähnung der wirtschaftlichen Ressourcen neben dem Begriff der Gelder, soll verhindert werden, dass wirtschaftliche Ressourcen als Ersatz- oder Parallelwährung verwendet werden, um so die Sanktionsbestimmungen zu umgehen. Sanktionsgelistete Personen sollen vielmehr keinen finanziellen oder sonstigen Nutzen aus Vermögenswerten ziehen dürfen, der für Zwecke eingesetzt werden kann, die den Zielen der entsprechenden Sanktionsverordnung zuwiderlaufen.⁵⁶

- 61 Als Faustformel und sehr vereinfacht lässt sich als wirtschaftliche Ressource all das definieren, was gegen Entgelt veräußert oder überlassen werden kann.⁵⁷
- 62 Dennoch ist auch der Begriff der wirtschaftlichen Ressource nicht uferlos. So zählen etwa Güter des täglichen Lebens oder Leistungen mit Verbrauchscharakter nicht dazu, weil hierdurch bereits nicht die Teilnahme am Wirtschaftsverkehr betroffen ist.⁵⁸
- 63 Trotz oder möglicherweise gerade wegen der Weite des Begriffs stellt die Auslegung des Begriffs Rechtsanwender vor eine Vielzahl von Detailfragen und Auslegungsschwierigkeiten.
- 64 So ist etwa umstritten, ob Dienstleistungen, wie etwa Beförderungen von Personen, Beratungen oder Vermittlungen, als wirtschaftliche Ressourcen zu werten sind.⁵⁹

(3) Einfrieren von Geldern und wirtschaftlichen Ressourcen

- 65 Der Ausdruck „Einfrieren von Geldern“ bezeichnet die Verhinderung jeglicher Form der Bewegung, des Transfers, der Veränderung und der Verwendung von Geldern sowie des Zugangs zu ihnen oder ihres Einsatzes, wodurch das Volumen, die Höhe, die Belegenheit, das Eigentum, der Besitz, die Eigenschaften oder die Zweckbestimmung der Gelder verändert oder sonstige Veränderungen bewirkt werden, die die Nutzung der Gelder, einschließlich der Portfolioverwaltung, ermöglichen.⁶⁰
- 66 Der Ausdruck „Einfrieren wirtschaftlicher Ressourcen“ bezeichnet das Verhindern der Verwendung wirtschaftlicher Ressourcen für jedwede Art der Beschaffung von Geldern, Waren oder Dienstleistungen, was auch den Verkauf, das Ver-

56 *Vogt/Arend*, in: Sachs/Pelz, Außenwirtschaftsrecht, 1. Einfriergebot und Bereitstellungsverbot, Rn. 97.

57 So etwa: BAFA-Merkblatt „Länderunabhängige Embargomaßnahmen zur Terrorismusbekämpfung“, S. 5.

58 BAFA-Merkblatt „Länderunabhängige Embargomaßnahmen zur Terrorismusbekämpfung“, 28.9.2009, Nr. 2, S. 5; *Wagner*, in: MünchKomm-StGB, 3. Aufl. 2019, § 18 AWG Rn. 32.

59 Vgl. zum Streit: *Vogt/Arend*, in: Sachs/Pelz, Außenwirtschaftsrecht, 1. Einfriergebot und Bereitstellungsverbot, Rn. 99 m. w. N.

60 Sanktionsleitlinien, S. 26, Ziff. 60.

mieten oder das Verpfänden dieser Ressourcen einschließt, sich aber nicht darauf beschränkt.⁶¹

Die Standardformulierung der EU hierzu lautet: 67

Sämtliche Gelder und wirtschaftlichen Ressourcen, die im Besitz oder im Eigentum der in Anhang X aufgeführten [einzelne Mitglieder der Regierung von (Land) und] [mit ihnen verbundenen] natürlichen oder juristischen Personen, Organisationen oder Einrichtungen stehen oder von diesen gehalten oder kontrolliert werden, werden eingefroren.⁶² Eben jene Definition wird beispielhaft auch in Art. 1 f) der Verordnung (EU) Nr. 269/2014 verwendet. 68

(4) Eigentum und Besitz

Die Finanzrestriktionen knüpfen immer an die Eigentümerstellung, aber auch an die Besitzstellung von Personen an. Insoweit kann auf die sachenrechtlichen Begriffsbestimmungen zurückgegriffen werden.⁶³ 69

Weder für die Annahme von relevantem Eigentum noch für relevanten Besitz ist ein Alleineigentum bzw. ein Alleinbesitz erforderlich.⁶⁴ 70

Maßgebliches Kriterium für die Frage der Eigentümerstellung der sanktionierten Person ist hierbei, ob dieser Person mindestens 50 % der Eigentumsrechte zusteht oder eine Mehrheitsbeteiligung besteht oder nicht.⁶⁵ 71

Die Finanzrestriktionen können demnach auch nicht sanktionierte Personen ausnahmsweise treffen, wenn diese Miteigentümer einer Sache sind, welche im Eigentum einer sanktionierten Person stehen. In einem solchen Fall steht dem nicht sanktionierten Dritten ein Aussonderungsrecht bezogen auf seinen Miteigentumsanteil zu, falls eine Trennung der Eigentumsanteile möglich ist, und ebenso kann die Genehmigung für die Verwendung der Gelder und wirtschaftlichen Ressourcen von jener Person beantragt werden.⁶⁶ 72

(5) Halten und Kontrollieren

Da sowohl das Einfriergebot als auch das Bereitstellungsverbot nicht nur auf Eigentums- und Besitzverhältnisse abstellt, kommt dem Begriff des „Kontrollierens“ besondere Bedeutung zu. 73

61 Sanktionsleitlinien, S. 26, Ziff. 61.

62 Sanktionsleitlinien, S. 35, Ziff. 82.

63 Vgl. etwa zum Begriff des Eigentums: *Fritzsche*, in: BeckOK BGB, 68. Ed. 1.8.2023, § 903 BGB Rn. 4.

64 *Allen*, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, 1. Einfriergebot, Rn. 63.

65 Sanktionsleitlinien, S. 20, Ziff. 55a.

66 Restriktive Maßnahmen (Sanktionen) – Aktualisierung der vorbildlichen Verfahren der EU für die wirksame Umsetzung restriktiver Maßnahmen, S. 14, Ziff. 36.

- 74** Unter „Halten“ oder „Kontrollieren“ sind alle Fälle zu verstehen, in denen eine benannte Person oder Organisation, die über keine Eigentumsrechte verfügt, rechtlich in der Lage ist, Gelder oder wirtschaftliche Ressourcen, die ihr nicht gehören, zu veräußern oder zu transferieren, ohne dass der rechtmäßige Eigentümer vorab zustimmen muss.⁶⁷
- 75** Im Ergebnis werden eigentumsähnliche Verfügungsbefugnisse als Maßstab herangezogen.⁶⁸ Demnach wird eine Kontrolle vermutet, wenn die sanktionierte Person oder Organisation:⁶⁹
- a) das Recht oder die Befugnis hat, die Mehrheit der Mitglieder des Verwaltungs-, Leitungs- oder Aufsichtsorgans der juristischen Person oder der Organisation zu bestellen oder abzuwählen;
 - b) allein durch die Ausübung ihrer Stimmrechte die Mehrheit der Mitglieder des Verwaltungs-, Leitungs- oder Aufsichtsorgans der juristischen Person oder der Organisation für das laufende und das vorhergehende Geschäftsjahr bestellt;
 - c) allein über die Mehrheit der Stimmrechte der Anteilseigner bzw. Mitglieder der juristischen Person oder der Organisation aufgrund einer Vereinbarung mit anderen Anteilseignern bzw. Mitgliedern derselben verfügt;
 - d) das Recht hat, auf die juristische Person oder die Organisation aufgrund eines mit ihr geschlossenen Vertrags oder aufgrund einer in ihrer Gründungsurkunde oder Satzung niedergelegten Bestimmung einen beherrschenden Einfluss auszuüben, sofern das Recht, dem die juristische Person oder die Organisation unterliegt, es zulässt, dass sie solchen Verträgen oder Bestimmungen unterworfen wird;
 - e) die Befugnis hat, von dem Recht zur Ausübung eines beherrschenden Einflusses im Sinne des Buchstabens d Gebrauch zu machen, ohne dieses Recht selbst innezuhaben;
 - f) das Recht hat, die Gesamtheit oder einen Teil der Vermögenswerte der juristischen Person oder der Organisation zu verwenden;
 - g) die Geschäfte der juristischen Person oder der Organisation auf einer einheitlichen Grundlage mit Erstellung eines konsolidierten Abschlusses führt; oder
 - h) gesamtschuldnerisch für die finanziellen Verbindlichkeiten der juristischen Person oder der Organisation haftet oder für sie bürgt.
- 76** Ist eines dieser Kriterien erfüllt, so ist davon auszugehen, dass die juristische Person oder Organisation von der anderen Person oder Organisation kontrolliert wird, sofern sich nicht im Einzelfall das Gegenteil beweisen lässt.

67 Restriktive Maßnahmen (Sanktionen) – Aktualisierung der vorbildlichen Verfahren der EU für die wirksame Umsetzung restriktiver Maßnahmen, S. 14, Ziff. 34.

68 Bundesbank FAQs, S. 12, B.4a.

69 Vgl. Sanktionsleitlinien, S. 20, Ziff. 55b.

bb) Bereitstellungsverbot

Ziel des Bereitstellungsverbots ist es, die sanktionierten Personen an der Teilhabe am Wirtschafts- und Geschäftsleben in weiten Teilen auszuschließen.⁷⁰ **77**

Dies sei am Beispiel der Russland-Sanktionen veranschaulicht: Gemäß Art. 2 Abs. 2 der Verordnung (EU) Nr. 269/2014 des Rates vom 17.3.2014 über restriktive Maßnahmen angesichts von Handlungen, die die territoriale Unversehrtheit, Souveränität und Unabhängigkeit der Ukraine untergraben oder bedrohen (**VO (EU) Nr. 269/2014**), dürfen (i) den in Anhang I aufgeführten natürlichen Personen oder (ii) mit diesen in Verbindung stehenden natürlichen oder juristischen Personen, Einrichtungen oder Organisationen weder unmittelbar noch mittelbar Gelder oder wirtschaftliche Ressourcen zur Verfügung gestellt werden oder zuzugute kommen. **78**

(1) Bereitstellung

Der Begriff der Bereitstellung umfasst gemäß ständiger Rechtsprechung des Gerichtshofs der Europäischen Union jede Handlung, die nach dem anwendbaren nationalen Recht erforderlich ist, damit eine sanktionierte Person tatsächlich die vollständige Verfügungsbefugnis über die betreffende Sache erlangen kann.⁷¹ **79**

Insgesamt ist der Begriff der Bereitstellung weit auszulegen.⁷² **80**

Nur so kann dem dem Sanktionsrecht innewohnenden Effektivitätsgrundsatz (effet utile) Rechnung getragen werden.⁷³ **81**

Als Faustformel kann man von einer Bereitstellung ausgehen, wenn wirtschaftliche Ressourcen der sanktionierten Person tatsächlich zufließen und sie darauf Zugriff nehmen kann. Auf welche Weise dies geschieht, ist ohne Bedeutung.⁷⁴ **82**

Die Auslotung, wann die Grenze zur Bereitstellung erreicht ist, stellt sich in der Praxis als schwierig dar. Einem vorsichtigen Ansatz folgend, sollte die Schwelle lieber zu früh als zu spät als überschritten angesehen werden. So ist beispielsweise auch die Frage, ob ein Vertragsschluss unter das Bereitstellungsverbot zu fassen ist, umstritten.⁷⁵ Hierbei gibt es Ansichten, nach welchem der Vertragsschluss oder bloße Vorbereitungshandlungen noch nicht als Bereitstellen zu qualifizieren sind.⁷⁶ Demnach sei der Realakt, also der tatsächliche Vorgang des Zur-Verfügung-Stellens, der dazu führt, dass einer sanktionsgelisteten Partei ein **83**

⁷⁰ Hildebrandt/Koch, IWRZ 2016, 152, 155.

⁷¹ EuGH, Slg 2007, I-08361, Rn. 51 – Möllendorf; EuGH, Slg 2010, I-0621, 3 Rn. 67 – E und F.

⁷² EuGH, Urt. v. 11.10.2007 – C-117/06 = EuZW 2007, 737, 739; EuGH, Urt. v. 17.1.2019 – C-168/17, BeckRS 2019, 105 Rn. 51.

⁷³ Sachs, in: Sachs/Pelz, Außenwirtschaftsrecht, I. Einleitung, Rn. 46.

⁷⁴ Pelz, in: Sachs/Pelz, Außenwirtschaftsrecht, 3. Zuwiderhandlung nach Abs 1 Nr. 1 lit. a, Rn. 15; B.7. Bundesbank FAQs.

⁷⁵ Hierzu: Vogt/Arend, in: Sachs/Pelz, Außenwirtschaftsrecht, 1. Einfriergebot und Bereitstellungsverbot, Rn. 108.

⁷⁶ Wagner, in: MünchKomm-StGB, 3. Aufl. 2019, § 18 AWG Rn. 32.

wirtschaftlicher Vorteil zugutekommt,⁷⁷ entscheidend. Wann dieser tatsächliche Vorgang einschlägig ist, bedarf einer Betrachtung des Einzelfalls.⁷⁸ Andererseits gibt es auch die nach hiesiger Ansicht vorzugswürdige Auffassung, wonach auch vertragliche Ansprüche als wirtschaftliche Ressource zu erfassen sind, wenn es sich um Ansprüche auf Leistung, die nicht auf Zahlung ausgerichtet sind, also beispielsweise Herausgabe, handelt. Hierfür spricht, dass solche vertraglichen Erfüllungsansprüche, zumindest nach deutschen zivilrechtlichen Grundsätzen, leicht abtretbar sind und damit zur Teilnahme am Wirtschaftsverkehr genutzt werden können.⁷⁹

(2) Mittelbare Bereitstellung

- 84** Während das Risiko der unmittelbaren Bereitstellung von Unternehmen in der Regel wegen des strengen Listenprinzips, durch Listenscreening des Vertragspartners, handhabbar sind, stellt die Einhaltung etwaiger mittelbarer Bereitstellungsverbote Wirtschaftsteilnehmer regelmäßig vor größere Herausforderungen.
- 85** Unter Fällen der mittelbaren Bereitstellung sind solche Fallkonstellationen zu verstehen, in welchen die Bereitstellung nicht direkt an die sanktionierte Person erfolgt, sondern an einen Dritten, der unter der Kontrolle der sanktionierten Person steht oder auf dessen Weisung handelt.⁸⁰ Eine typische Fallkonstellation der mittelbaren Bereitstellung liegt etwa vor, wenn Gelder oder wirtschaftliche Ressourcen unmittelbar einer nicht (namentlich) sanktionierten Person bereitgestellt werden, diese jedoch im Eigentum oder unter der Kontrolle der sanktionierten Person bzw. in einem Abhängigkeitsverhältnis zu einer sanktionierten Person steht oder auf deren Weisung handelt.⁸¹
- 86** Maßgebliches Kriterium für die Frage der Eigentümerstellung der sanktionierten Person ist hierbei, ob ein Besitz von mindestens als 50% der Eigentumsrechte oder eine Mehrheitsbeteiligung besteht oder nicht.⁸²
- 87** Anders als etwa bei US-Sanktionen (vgl. unten → Rn. 123) werden hierbei Mit-eigentumsanteile anderer sanktionierter Personen grundsätzlich nicht hinzuge-

77 BGH, Beschl. v. 23.4.2010 – 3 StE 1/10-1, Rn. 23; *Vogt/Arend*, in: Sachs/Pelz, Außenwirtschaftsrecht, 1. Einfriergebot und Bereitstellungsverbot, Rn. 139; *Wagner*, in: MünchKomm-StGB, § 18 AWG Rn. 35.

78 BGH, Beschl. v. 11.8.2021 – 3 StR 173/21, BeckRS 2021, 33671 Rn. 6 = BeckRS 2021, 33671, Rn. 6.

79 *Harings/Loets*, RdTW, 2015, 321, 322.

80 BGH, Beschl. v. 5.3.2019 – 3 StR 413/18 = NStZ 2019, 736, 737.

81 EuGH, Urt. v. 17.1.2019 – C-168/17, BeckRS 2019, 105 Rn. 61 ff.; BGH, Beschl. v. 5.3.2019 – 3 StR 413/18, NStZ 2019, 736, 737; *Diemer*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 238. EL September 2021, AWG, § 18 Rn. 9; BGH, Beschl. v. 5.3.2019 – 3 StR 413/18, NStZ 2019, 736, 737.

82 Sanktionsleitlinien, S. 20, Ziff. 55a; restriktiver hierzu FAQ der Bundesbank, Stand: 5.9.2023, z. B. unter B.4a, B.5b.

rechnet, also so behandelt, als sei jede sanktionierte Person ausschlaggebend.⁸³ Sollte eine juristische Person oder Organisation allerdings von mehreren sanktionierten Personen jeweils unterhalb der Mehrheitsbeteiligungsschwelle von 50 % gehalten werden und es bestehen Anzeichen für ein kollusives Zusammenwirken der sanktionierten Personen, kann auch bei EU-Sanktionen eine Zusammenrechnung in Betracht gezogen werden.⁸⁴

Demgegenüber ist eine Kontrolle anzunehmen, wenn zwar keine Mehrheitsbeteiligung besteht, die sanktionierte Person dennoch gewisse Einflussmöglichkeiten hat (vgl. oben → Rn. 73 ff.). Es genügt hierbei auch, wenn der sanktionierten Person durch Lieferung die Zugriffsmöglichkeit auf den Vermögenswert eingeräumt wird.⁸⁵ **88**

Hierbei ist darauf hinzuweisen, dass bei Vermögenswerten, welche juristischen Personen oder Organisationen zur Verfügung gestellt werden, die sich im Eigentum oder unter der Kontrolle einer sanktionierten Person befinden, vermutet wird, dass diese zugleich der sanktionierten Person mittelbar zur Verfügung gestellt werden.⁸⁶ Diese Vermutung kann jedoch erschüttert werden, wenn im Einzelfall nach vernünftigem Ermessen mittels eines risikobasierten Ansatzes und unter Berücksichtigung aller relevanten Umstände festgestellt werden kann, dass die betreffenden Gelder oder wirtschaftlichen Ressourcen nicht von der sanktionierten Person oder Organisation verwendet werden oder ihr zugute kommen.⁸⁷ Bei dieser Feststellung ist unter anderem die Eigenschaft der bereitgestellten Gelder oder wirtschaftlichen Ressourcen, einschließlich ihrer möglichen praktischen Verwendung durch die sanktionierte Person und der Unkompliziertheit eines Transfers an die sanktionierte Person zu berücksichtigen.⁸⁸ **89**

cc) Einfriergebot

Das Einfrieren von Geldern bezeichnet die Verhinderung jeglicher Form der Bewegung, des Transfers, der Veränderung und der Verwendung von Geldern sowie des Zugangs zu ihnen oder ihres Einsatzes, wodurch das Volumen, die Höhe, die Belegenheit, das Eigentum, der Besitz, die Eigenschaften oder die Zweckbestimmung der Gelder verändert oder sonstige Veränderungen bewirkt werden, die die Nutzung der Gelder, einschließlich der Portfolioverwaltung, ermöglichen.⁸⁹ **90**

⁸³ Bundesbank FAQ B.6.

⁸⁴ Bundesbank FAQ B.6.

⁸⁵ *Alten*, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, 3. Mittelbares Bereitstellungsverbot, Rn. 86 ff.

⁸⁶ Europäische Union, Aktualisierung der vorbildlichen Verfahren der EU für die wirksame Umsetzung restriktiver Maßnahmen v. 27.6.2022, 10572/22, Ziff. 66.

⁸⁷ Europäische Union, Aktualisierung der vorbildlichen Verfahren der EU für die wirksame Umsetzung restriktiver Maßnahmen v. 27.6.2022, 10572/22, Ziff. 66.

⁸⁸ Europäische Union, Aktualisierung der vorbildlichen Verfahren der EU für die wirksame Umsetzung restriktiver Maßnahmen v. 27.6.2022, 10572/22, Ziff. 66.

⁸⁹ Siehe auch Sanktionsleitlinien, S. 26, Ziff. 60 und Art. 1 f) VO (EU) Nr. 269/2014.

- 91** Vom Einfriergebot sind sämtliche Gelder und wirtschaftlichen Ressourcen umfasst, die sich im Besitz oder im Eigentum von benannten Personen und Organisationen befinden oder von diesen gehalten oder kontrolliert werden.⁹⁰ Ein „Halten“ oder „Kontrollieren“ ist anzunehmen, wenn die benannte Person in der Lage ist, auf die Gelder zuzugreifen oder über diese verfügen zu können (vgl. oben → Rn. 73 ff.).
- 92** Zusammengefasst ist es das Ziel des Einfrierens von Geldern, jegliche Form der Verwendung, der Bewegung und des Transfers von Geldern sowie des Zugangs zu oder des Einsatzes von diesen zu verhindern.
- 93** Durch das Einfrieren werden die Eigentumsrechte der sanktionierten Person nicht berührt.⁹¹ Dies bedeutet, dass die sanktionierten Personen trotz des Einfriergebots weiterhin Eigentümer der Gelder und wirtschaftlichen Ressourcen bleiben und keine Enteignung, sondern lediglich eine Verfügungsbeschränkung mit dem Einfriergebot verbunden ist.⁹²

dd) Ausnahmen

- 94** Die EU-Sanktionsverordnungen enthalten zahlreiche Ausnahmen bezüglich des Einfriergebots und Bereitstellungsverbots.
- 95** Um die Grundrechte der betroffenen Personen zu wahren, werden in der Regel auch hinsichtlich der Finanzrestriktionen einige Ausnahmen statuiert.
- 96** Ausnahmen im Bereich der Finanzrestriktionen können sein:⁹³
- Ausnahmen zur Deckung der Grundbedürfnisse der benannten Personen, auch in Bezug auf die Bezahlung von Nahrungsmitteln, Mieten oder Hypotheken, Medikamenten und ärztlicher Behandlung, Steuern, Versicherungsprämien und Gebühren öffentlicher Versorgungseinrichtungen;
 - Ausnahmen für die Wahrnehmung der Verteidigungsrechte in Bezug auf Ausgaben im Zusammenhang mit der Bereitstellung von Rechtsdienstleistungen;
 - das Eigentumsrecht der benannten Person oder Organisation (da das Einfrieren von Vermögenswerten nicht das Eigentum der benannten Person oder Organisation berührt, sondern die Fähigkeit, über die Gelder zu verfügen);
 - Ausnahmen betreffend die Eigentumsrechte der nicht sanktionierten juristischen Person bzw. Organisation, bei der die eingefrorenen Gelder gehalten werden;
 - Ausnahmen betreffend das Eigentumsrecht sowohl der benannten Person oder Organisation als auch einer nicht benannten Person oder Organisation in Bezug auf vor der Benennung zwischen ihnen abgeschlossene Verträge;

90 Sanktionsleitlinien, S. 36, Ziff. 82.

91 Vorbildliche Verfahren der EU, Restriktive Maßnahmen (Sanktionen) – Aktualisierung der vorbildlichen Verfahren der EU für die wirksame Umsetzung restriktiver Maßnahmen, S. 14.

92 *Vogt/Arend*, in: Sachs/Pelz, Außenwirtschaftsrecht, Kap. IV Rn. 133.

93 Restriktive Maßnahmen (Sanktionen) – Aktualisierung der vorbildlichen Verfahren der EU für die wirksame Umsetzung restriktiver Maßnahmen, Ziff. 76.

- Ausnahmen in Bezug auf das internationale Recht über diplomatische und konsularische Beziehungen;
- Ausnahmen über die menschliche Sicherheit und den Umweltschutz; oder
- Ausnahmen zu humanitären Zwecken wie beispielsweise die Durchführung oder Erleichterung von Hilfeleistungen, einschließlich medizinischer Versorgung, Nahrungsmittellieferungen oder des Transports humanitärer Helfer und damit verbundener Hilfe, oder Evakuierungen aus einem betroffenen Land.

Solche Ausnahmetatbestände sind bereits in den Standardformulierungen enthalten und werden im Bereich des Einfriergebots und Bereitstellungsverbots eingesetzt.⁹⁴ **97**

4. Deutschland

Wegen der Übertragung der Kompetenzen für den Erlass der Sanktionen der Mitgliedstaaten auf die EU (vgl. Art. 215 AEUV) setzt der Rat der EU UN-Sanktionen um und erlässt darauf basierende, aber auch davon unabhängige EU-Sanktionen. Diese sind für natürliche Personen deutscher Staatsangehörigkeit, aber auch für in Deutschland ansässige juristische Personen, Organisationen und Einrichtungen bindend. **98**

Neben den in der Praxis weitaus relevanteren EU-Sanktionen ist parallel auch nationales Sanktionsrecht zu beachten. **99**

Die wichtigsten Vorschriften diesbezüglich finden sich im AWG und in der Außenwirtschaftsverordnung (AWV) sowie in den Sanktionsdurchsetzungsgesetzen. **100**

a) Außenwirtschaftsgesetz und Außenwirtschaftsverordnung

Für deutsche Personen, Organisationen und Einrichtungen, sind neben etwaigen strafrechtlichen Normen und Ordnungswidrigkeitstatbeständen (vgl. §§ 17 ff. AWG) vor allem die §§ 4 bis 7 AWG von Bedeutung. **101**

Diese Vorschriften sind größtenteils auf Empfehlungen der Financial Action Taskforce (FATF) zurückzuführen. Diese hatte schon vor der Veröffentlichung des FATF-Berichts 2022⁹⁵ gefordert, dass die Umsetzung von UN-Sanktionen unverzüglich zu erfolgen habe.⁹⁶ Da die Umsetzung der UN-Sanktionen im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik (GASP) der EU erfolgt und dieser Umsetzungsprozess einige Zeit in Anspruch nimmt, erachtete die FATF die Umsetzungspraxis als nicht unverzüglich. **102**

⁹⁴ Vgl. Sanktionsleitlinien, S. 36, Ziff. 83.

⁹⁵ Siehe <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-germany-2022.html> (zuletzt abgerufen am 22.3.2024).

⁹⁶ Vgl. die FATF-Recommendations Nr. 6 und 7 sowie die „Immediate Outcomes“ Nr. 10 und 11.

- 103** Um dennoch eine solch unverzügliche Umsetzung zu gewährleisten, wurde § 6 AWG durch das Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie vom 12.12.2019 entsprechend angepasst.⁹⁷ Durch § 6 AWG besteht für deutsche Behörden die Möglichkeit, durch Verwaltungsakte entsprechende Sanktionsmaßnahmen anzuordnen. Nach dieser Norm können Verwaltungsakte erlassen werden, durch welche Rechtsgeschäfte oder Handlungen beschränkt werden, oder Handlungspflichten angeordnet werden, um eine bestehende Gefahr für bestimmte Rechtsgüter abzuwenden. Insbesondere können (i) die Verfügung über Gelder und wirtschaftliche Ressourcen bestimmter Personen oder Personengesellschaften oder (ii) das Bereitstellen von Geldern und wirtschaftlichen Ressourcen zugunsten bestimmter Personen oder Personengesellschaften beschränkt werden.
- 104** Die so erlassenen Verwaltungsakte dürfen gemäß § 6 Abs. 1 lit. a AWG öffentlich bekannt gemacht werden. Entsprechend der allgemeinen Regelung des § 43 Abs. 1 Satz 1 Verwaltungsverfahrensgesetzes, wird der Verwaltungsakt, wie dies auch § 6 Abs. 1a Satz 3 AWG klarstellt, mit Bekanntmachung wirksam.
- 105** Inhaltlich ähneln die in § 6 Abs. 1 AWG genannten Maßnahmen schon allein wegen des Wortlauts stark dem Einfriergebot und Bereitstellungsverbot der EU-Sanktionen.
- 106** Zusätzlich sind auch Beschränkungen und Handlungspflichten, welche durch Rechtsverordnung nach § 4 AWG angeordnet wurden, in der täglichen Praxis zu beachten. Solche sind jedoch in der Praxis gegenüber EU-Sanktionen von untergeordneter Relevanz, da die Möglichkeit der Beschränkungen und Eingriffe in den Außenwirtschaftsverkehr der EU-Mitgliedstaaten durch Kompetenzübertragung nach Art. 207 AEUV bei der EU liegt.⁹⁸

b) Sanktionsdurchsetzungsgesetze

- 107** Trotz der Regelung der §§ 4 bis 7 AWG statuierte die FATF in ihrem Bericht von 2022, dass die Umsetzung immer noch nicht unverzüglich erfolgt sei. Hierbei betont die FATF, dass es seitens der EU Verzögerungen in der Umsetzung gebe, wenn die UN Sanktionen unmittelbar vor dem Wochenende oder vor Feiertagen erlasse.⁹⁹ Dies führe dazu, dass die Sanktionen nicht unverzüglich umgesetzt würden, was in einem finanzstarken Staat wie Deutschland besonders problematisch sei. Zwar gebe es nationale Mechanismen, um die Verzögerung im EU-Rahmen abzumildern, allerdings erlaube der derzeitige Rahmen keine unverzügliche Umsetzung von Sanktionen.¹⁰⁰

⁹⁷ Art. 17, Gesetz v. 12.12.2019 – BGBl. I 2019, Nr. 50 v. 19.12.2019, S. 2602.

⁹⁸ Thoms, in: Dorsch, Zollrecht, § 4 AWG 2013 Rn. 2.

⁹⁹ FATF Report, S. 245.

¹⁰⁰ Vgl. Gesetzesbegründung: S. 66.

Deutschland reagierte hierauf noch Ende des Jahres 2022 mit dem Zweiten Gesetz zur effektiveren Durchsetzung von Sanktionen (Sanktionsdurchsetzungsgesetz II), durch welches § 5a AWG in das Gesetz eingefügt wurde.¹⁰¹ **108**

Damit sollte die etwaige zeitliche „Umsetzungslücke“ in Deutschland geschlossen werden. § 5a AWG erlaubt es nun, vorläufig und vorübergehend Verfügungs- und Bereitstellungsverbote, welche auf neuen UN-Sanktionen basieren, Geltung zu verschaffen. Im Ergebnis sind die UN-Sanktionen mithin direkt anwendbar, bis ein Umsetzungsrechtsakt seitens der EU verabschiedet wird.¹⁰² **109**

Diese Änderungen erachtet die FATF als ausreichend, um im Follow-up-Report Deutschland zu bescheinigen, dass die Anforderungen erfüllt seien.¹⁰³ **110**

Hintergrund für die rasche Umsetzung ist wohl neben dem FATF-Report, dass eine im Jahr 2022 errichtete Taskforce aufgrund des Angriffskriegs von Russland gegen die Ukraine aufzeigte, dass die damaligen Mechanismen für die Sanktionsdurchsetzung weder angemessen noch ausreichend waren.¹⁰⁴ Nach Einschätzung der Taskforce seien die wesentlichen Probleme etwa unklare Kompetenzen, Schwierigkeiten bei der Identifizierung von Vermögenswerten von sanktionierten Personen und fehlende Kommunikationsmöglichkeiten.¹⁰⁵ **111**

Angesichts der schnell erkannten Probleme wurde das Erste Gesetz zur effektiveren Durchsetzung von Sanktionen (Sanktionsdurchsetzungsgesetz I) mit „heißer Nadel“ gestrickt und ist bereits am 24.5.2022 in Kraft getreten. Im Wesentlichen schaffte das Sanktionsdurchsetzungsgesetz I neue Eingriffsbefugnisse für Behörden zur Ermittlung und Sicherstellung von Geldern und wirtschaftlichen Ressourcen. Zudem wurden Datenzugriffs- und Datenaustauschbefugnisse geschaffen. Die aufsehenerregendste Änderung war die Schaffung einer Anzeigepflicht sanktionierter Personen (vgl. § 23a AWG). **112**

Das Sanktionsdurchsetzungsgesetz II knüpft an das Sanktionsdurchsetzungsgesetz I an und soll nach dem Wunsch des Gesetzgebers für strukturelle Verbesserungen sorgen, nachdem mit dem Sanktionsdurchsetzungsgesetz I bereits kurzfristig umsetzbare Maßnahmen zur Verbesserung der Sanktionsdurchsetzung realisiert worden seien.¹⁰⁶ Insbesondere die Errichtung der neuen mit zahlreichen Befugnissen ausgestatteten Behörde, der Zentralstelle für Sanktionsdurchsetzung, welche ein bundeseinheitliches und effektives Vorgehen ermöglichen **113**

101 Zweites Gesetz zur effektiveren Durchsetzung von Sanktionen (Sanktionsdurchsetzungsgesetz II) BGBl. I, S. 2606, S. 100.

102 *Sachs*, in: *Sachs/Pelz*, Außenwirtschaftsrecht, 2. Rechtsgrundlagen und Rechtssetzungsverfahren, Rn. 27.

103 FATF, Follow-up Report 2023 – Germany, S. 3.

104 <https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Europa/Krieg-in-der-Ukraine/taskforce-zur-umsetzung-der-sanktionen.html> (zuletzt abgerufen am 22.3.2024).

105 <https://www.tagesschau.de/inland/sanktionen-russland-kanzleramt-101.html> (zuletzt abgerufen am 22.3.2024).

106 Referentenentwurf, BT-Drs. 20/4326, S. 1.

soll, dürfte eine sinnvolle Änderung sein, welche mit dem Sanktionsdurchsetzungsgesetz II einhergeht. So ist gemäß § 1 Abs. 1 Nr. 1 Sanktionsdurchsetzungsgesetz II unter anderem Aufgabe der Zentralstelle für Sanktionsdurchsetzung, Gelder und wirtschaftliche Ressourcen von sanktionierten Personen und Personengesellschaften zu ermitteln und sicherzustellen. Gemäß § 1 Abs. 1 Nr. 2 Sanktionsdurchsetzungsgesetz II ist auch die Überwachung der Einhaltung von Bereitstellungsverböten und Verfügungsverboten Aufgabe der Zentralstelle für Sanktionsdurchsetzung.

5. Ausblick: Deutschland und EU

- 114** Perspektivisch werden die Pflichten zur Umsetzung präventiver Sanktionsmaßnahmen erheblich ausgeweitet. Während derzeit außerhalb des streng regulierten Finanzsektors keine Pflichten zu präventiven Maßnahmen (insb. „Sanktionslistenscreenings“) bestehen, sieht die EU mit der Verordnung (EU) 2024/1624 des europäischen Parlaments und Rates vom 31.5.2024 zur Verhinderung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung (**EU-Anti-Geldwäscheverordnung**), die am 10.7.2027 Geltung erlangen wird, vor, Maßnahmen zur Prävention von Geldwäsche und Terrorismusfinanzierung um Maßnahmen zur Bekämpfung von Verstößen gegen Finanzsanktionen¹⁰⁷ zu ergänzen.
- 115** Gemäß Art. 9 Abs. 1 lit. b der EU-Anti-Geldwäscheverordnung müssen die nach der Verordnung als Verpflichtete geltenden Wirtschaftsteilnehmer über interne Strategien, Verfahren und Kontrollen verfügen, um – insbesondere zusätzlich zu der Pflicht, Finanzsanktionen anzuwenden – das Risiko der Nichtumsetzung und Umgehung von Finanzsanktionen zu mindern und zu steuern. Ebenso wird das Sanktionsrecht Teil der Risikoanalyse werden (vgl. Art. 10 Abs. 1 der EU-Anti-Geldwäscheverordnung). Dies sind, neben der Prüfpflicht, „ob der Kunde oder die wirtschaftlichen Eigentümer gezielten finanziellen Sanktionen unterliegt bzw. unterliegen, und im Fall eines Kunden oder einer Partei einer Rechtsvereinbarung, bei der es sich um eine juristische Person handelt, ob natürliche oder juristische Personen, die gezielten finanziellen Sanktionen unterliegen, die juristische Person kontrollieren oder einzeln oder kollektiv mehr als 50% der Eigentumsrechte oder eine Mehrheitsbeteiligung an dieser juristischen Person haben“ (vgl. Art. 20 Abs. 1 lit. d der EU-Anti-Geldwäscheverordnung), nur einige neue Anforderungen, welche es in Zukunft zu beachten gilt.
- 116** Diese Entwicklung veranschaulicht das bereits eingangs gezeichnete Bild einer weiterhin zunehmenden Bedeutung des Sanktionsrechts in einer stetig komplexer werdenden Welt.

107 Die EU-Geldwäscheverordnung nennt Finanzsanktionen aus dem Englischen „targeted financial sanctions“ übersetzt „gezielte finanzielle Sanktionen“.

6. US-Sanktionen**a) Grundlagen**

Die US-Sanktionen weisen teilweise Ähnlichkeiten zu solchen der EU auf, stellen sich für die Wirtschaftsteilnehmer in der Praxis aber als teils wesentlich komplexer und schwieriger „greifbar“ dar. **117**

Die Komplexität ist auch der Tatsache geschuldet, dass in den USA mehrere Behörden Sanktionen zu den gleichen beziehungsweise zu ähnlichen, sich teilweise inhaltlich überschneidenden Themengebieten erlassen. **118**

Der Großteil der Sanktionen wird durch Präsidialdekrete, sog. Executive Orders (E.O.), unmittelbar durch den US-Präsidenten erlassen.¹⁰⁸ Ebenso sind förmliche Gesetze durch den Kongress denkbar. **119**

Das Pendant zu den Finanzsanktionen erlässt in den USA das beim Finanzministerium (Department of the Treasury) ansässige Office of Foreign Asset Control (OFAC). Das OFAC bietet für die Auslegung der Sanktionsprogramme, ähnlich wie die EU, Hilfestellungen an. Hierzu zählen etwa die umfangreichen FAQs oder sowie allgemeine Informationen zu allen Sanktionsprogrammen.¹⁰⁹ **120**

Ebenso wie die EU-Sanktionen sind auch US-Sanktionen zu einem Großteil als Smart Sanctions ausgestaltet. Im Unterschied zu der EU ist allerdings erkennbar, dass die US-Sanktionen oftmals weitergehend sind und tiefgreifendere Einschränkungen vornehmen. Zudem verhängen die USA auch umfassende Verbote (Comprehensive Sanctions), welche den Handel mit bestimmten Staaten oder Territorien gänzlich verbieten.¹¹⁰ **121**

Deutliche Ähnlichkeiten zwischen US-Sanktionen und EU-Sanktionen fallen insbesondere im Hinblick auf einzelnen Maßnahmen auf. So gibt es auch bei den US-Sanktionen ein Einfriergebot und ein Bereitstellungsverbot (blocking of property and property interests).¹¹¹ Die jeweilige Wirkung kann hierbei, je nach Sanktionsprogramm, unterschiedlich ausgestaltet sein. In der Tendenz ist diese noch weitreichender als die von EU-Sanktionsprogrammen, so kann beispielsweise etwa auch die Annahme von Geldern von sanktionierten Personen verboten sein.¹¹² **122**

Ein wesentlicher Unterschied, der auch für das Sanktionslisten-Screening relevant ist, ist die Berechnung des beherrschenden Einflusses. Nach der Logik von US-Sanktionsprogrammen existiert eine strenge sogenannte 50-Prozent-Lösung **123**

108 *Alten*, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, Kap. 9 C. II, Rn. 166.

109 Siehe <https://ofac.treasury.gov/faqs/topic/1501> (zuletzt abgerufen am 22.3.2024).

110 Etwa Iran-Sanktionen: Iranian Transactions Regulations, 31 C.F.R. part 560; Kuba-Sanktionen: Cuban Assets Control Regulations, 31 C.F.R. Part 515.

111 C.f. Executive Order 13660, Sec 1.

112 *Alten*, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, I. Blocking Sanctions, Rn. 193.

(50 Percent Rule), welche rein mathematisch berechnet wird.¹¹³ Diese strenge mathematische Lösung gilt es zu beachten, wenn der Geschäftspartner überprüft wird und in seiner Beteiligungsstruktur mit einem Beteiligungsanteil von 50% oder mehr sanktionierte Gesellschafter stehen. Nach dieser Logik gelten Unternehmen, deren Anteile zu 50% oder mehr von einer oder mehreren sanktionierten Personen gehalten werden, als ebenfalls sanktioniert.¹¹⁴

- 124** Im Ergebnis wird dann auch das Eigentum und die Beteiligung an Eigentum eines solchen Unternehmens unabhängig davon blockiert, ob das Unternehmen selbst im Anhang zu einer Durchführungsverordnung aufgeführt ist oder anderweitig Sanktionen unterliegt. Dementsprechend darf eine US-Person im Allgemeinen keine Geschäfte mit einer solchen Person tätigen, es sei denn, das OFAC hat dies genehmigt.
- 125** Wegen der Schwierigkeiten, die diese Regelung nach sich zieht, die teilweise Parallelen zu den Schwierigkeiten des „mittelbaren Bereitstellungsverbots“ (vgl. oben → Rn. 84 ff.) aufweisen, veröffentlicht das OFAC Auslegungshilfen und Beispiele bezüglich dieser Regelung.¹¹⁵

b) Anwendungsbereich

aa) Primärsanktionen

- 126** US-Sanktionen sind zunächst überall dort relevant, wo ein US-Bezug, auch als *US-Nexus* bezeichnet, besteht. Diese Sanktionen werden als Primärsanktionen (Primary Sanctions) bezeichnet.
- 127** Ein Anknüpfungspunkt für solche Primärsanktionen besteht beispielsweise, wenn US-Personen involviert sind. US-Personen sind wegen des personellen Anknüpfungspunktes vollumfänglich den Pflichten des US-Sanktionsrechts unterworfen.
- 128** Ungeachtet des derzeitigen Aufenthaltsorts müssen natürliche Personen, welche US-Staatsangehörige sind, stets die US-Sanktionen beachten. Neben US-Staatsangehörigen gilt dies auch regelmäßig für Ausländer mit dauerhaftem Aufenthaltstitel (Permanent Resident Aliens), Inhaber einer Green Card und Personen, die sich – wenn auch nur vorübergehend – im Hoheitsgebiet der USA aufhalten.¹¹⁶

¹¹³ Revised guidance on entities owned by persons whose property and interest in property are blocked, <https://ofac.treasury.gov/media/6186/download?inline> (zuletzt abgerufen am 29.10.2024).

¹¹⁴ *Allen*, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, 1. Blocking Sanctions, Rn. 194.

¹¹⁵ Vgl. etwa: OFAC FAQ Nr. 401.

¹¹⁶ OFAC FAQ, Basic Information on OFAC and Sanctions, Ziff. 11; <https://home.treasury.gov/policy-issues/financial-sanctions/frequently-asked-questions/ofac-consolidated-frequently-asked-questions> (zuletzt abgerufen am 31.12.2023).

Bei bestimmten Sanktionsprogrammen, wie etwa dem Kuba-Sanktionsprogramm,¹¹⁷ müssen auch ausländische Tochtergesellschaften, die sich im Besitz oder unter der Kontrolle von US-Unternehmen befinden, die Vorschriften einhalten. **129**

Ebenso kann ein US-Bezug bestehen, wenn eine Transaktion in US-Dollar abgewickelt wird oder die Ware US-Ursprung hat. Ob dies ein ausschlaggebender Faktor ist, kommt auf das entsprechende Sanktionsprogramm an. **130**

Insgesamt sind Verstöße gegen US-Sanktionsrecht mit erheblichen Strafen bedroht. Dies können etwa zivil- und strafrechtliche Strafen von mehreren Millionen Dollar sein.¹¹⁸ Ebenso sind Freiheitsstrafen denkbar.¹¹⁹ **131**

bb) Sekundär-Sanktionen

Ohne erkennbare Anknüpfungspunkte beanspruchen manche US-Sanktionsprogramme sogar extraterritoriale Wirkung. Hierbei handelt es sich um die außerhalb der Vereinigten Staaten weitgehend einhellig als völkerrechtswidrig angesehene US-Praxis der Sekundärsanktionen (Secondary Sanctions).¹²⁰ **132**

Während die Primärsanktionen auf den US-Bezug abstellen und das Personal- und Territorialprinzip ähnlich wie EU-Sanktionen berücksichtigen (vgl. oben → Rn. 28), reichen die US-Sekundärsanktionen weiter. Diese richten sich explizit gegen natürliche und juristische Personen, die nach der jeweiligen Definition eines extraterritoriale Anwendung beanspruchenden Sanktionsprogramms keine „US-Persons“ sind, nicht in den USA ansässig sind und bei welchen auch sonst kein US-Bezug erkennbar ist.¹²¹ **133**

Die ohnehin weit zu verstehenden und umfassend anzuwendenden US-Sanktionen erfahren hierbei eine wesentliche Erweiterung, die dazu führt, dass es auch Personen, die nicht als „US-Persons“ zu klassifizieren sind, verboten ist, mit sanktionierten Personen Geschäfte einzugehen. Andernfalls droht ihnen eine eigene Listung als sog. Specially Designated Nationals (SDN).¹²² **134**

117 Cuban Assets Control Regulations, 31 C.F.R. § 515, 329, <https://www.ecfr.gov/current/title-31/subtitle-B/chapter-V/part-515> (zuletzt abgerufen am 22.3.2024).

118 OFAC FAQ, Basic Information on OFAC and Sanctions, Ziff. 12; <https://home.treasury.gov/policy-issues/financial-sanctions/frequently-asked-questions/ofac-consolidated-frequently-asked-questions> (zuletzt abgerufen am 31.12.2023).

119 Alten, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, 2. Strafrechtliche Folgen, Rn. 208.

120 Vgl. Denga, RIW 2022, 93, 94 m. w. N.

121 Denga, RIW 2022, 93, 93.

122 OFAC, Specially Designated Nationals and Blocked Persons List (SDN), Stand: 15.3.2024; <https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists> (zuletzt abgerufen am 17.3.2024).

- 135** Auch Nicht-US-Personen, die wesentliche Geschäfte mit SDN wissentlich unterstützen („knowingly facilitate a significant transaction“),¹²³ laufen Gefahr, im Rahmen der Sekundärsanktionen selbst als SDN gelistet zu werden oder vergleichbaren Beschränkungen zu unterfallen.¹²⁴
- 136** Die Gefahr einer eigenen Sanktionslistung entfaltet regelmäßig eine erhebliche Abschreckungswirkung, die Unternehmen dazu bewegt, von nach US-Sanktionsprogrammen missbilligten Geschäften „freiwillig“ Abstand zu nehmen und US-Sanktionsprogramme damit auch ohne rechtlichen Anknüpfungspunkt zu beachten.¹²⁵ Zwar gelten die Sekundärsanktionen nur in Bezug auf bestimmte als wesentlich (significant) betrachtete Geschäfte, die Abgrenzung von solchen wesentlichen zu unwesentlichen Geschäften weist trotz Auslegungshilfen der OFAC in der Praxis allerdings Schwierigkeiten auf, die zumindest die qualifizierte Einschätzung eines Einzelfalls durch spezialisierte US-Rechtsanwälte erfordern. Wir erkennen in der Praxis daher die Tendenz, aus Vorsichtsgründen von jeglicher Art des Geschäfts abzusehen, das mit der Gefahr verbunden wäre, gegen Sekundärsanktionen zu verstoßen.
- 137** Solche Sekundärsanktionen gilt es etwa im Zusammenhang mit Transaktionen mit dem Iran oder Kuba zu beachten.¹²⁶ In Bezug auf Russland-Sanktionen bestehen derzeit indes bislang keine Sekundärsanktionen, was mit dem weitreichenden Interessengleichlauf der USA und der EU zu erklären ist.

c) Funktionsweise der US-Sanktionen

- 138** Ähnlich wie die EU arbeiten auch die US-Behörden mit Sanktionslisten. Bezüglich der US-Sanktionen besteht jedoch der Vorteil, dass die Suche nach sanktionierten Personen in stärker digitalisierter Form möglich ist, da eine entsprechende Suchmaske bereitgestellt wird, welche es erlaubt, gezielt nach Namen und Personen zu suchen.¹²⁷
- 139** US-gelistete Personen, darunter derzeit zahlreiche russische Oligarchen und deren Familienangehörige,¹²⁸ werden von den USA als sog. SDN gelistet.¹²⁹ Solche

¹²³ OFAC FAQ, Basic Information on OFAC and Sanctions, Ziff. 574; <https://home.treasury.gov/policy-issues/financial-sanctions/frequently-asked-questions/ofac-consolidated-frequently-asked-questions> (zuletzt abgerufen am 31.12.2023).

¹²⁴ *Alten*, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, 2. Relevanz für Nicht-US-Personen, Rn. 183.

¹²⁵ Vgl. *Alten*, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, Kap. 9 II, Rn. 184.

¹²⁶ *Roeder/Schlutz/Hille/Havlik/Conte*, CCZ 2023, 337, 338.

¹²⁷ <https://sanctionssearch.ofac.treas.gov/> (zuletzt abgerufen am 22.3.2024).

¹²⁸ Basierend insb. auf Ukraine Freedom Support Act of 2014 (UFSA), E.O. 13660, E.O. 13661, E.O. 13662, E.O. 13685, vgl. OFAC FAQ, Basic Information on OFAC and Sanctions, Ziff. 574; <https://home.treasury.gov/policy-issues/financial-sanctions/frequently-asked-questions/ofac-consolidated-frequently-asked-questions> (zuletzt abgerufen am 31.12.2023).

¹²⁹ <https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists> (zuletzt abgerufen am 22.3.2024).

Personen unterliegen dadurch umfassenden Finanzsanktionen. Ebenso gibt es Personen, welche nur teilweise in ihrem Handeln beschränkt wurden, die Non-SDN.¹³⁰ Diese sind auf den sogenannten Non-SDN-Listen zu finden.¹³¹

Sonstige Erklärungen von Abkürzungen, sogenannten „Codes“ oder „Tags“, finden sich auf der Seite der OFAC.¹³² **140**

7. Anti-Boycott-Regelungen

a) EU-Blocking-Verordnung

Aufgrund der soeben aufgezeigten Reichweite von US-Sanktionen besteht insbesondere für Unternehmen mit Tochtergesellschaften in den USA oder umfangreichem US-Geschäft ein hoher Anreiz, diese vollumfänglich zu beachten. Bei pauschaler Beachtung bestünde jedoch die Gefahr, gegen für deutsche Unternehmen anwendbares Anti-Boycott-Recht zu verstoßen. Ein Verstoß, wie etwa ein solcher gegen Art. 5 Abs. 1 EU-Blocking-VO, ist im deutschen Recht gem. § 82 Abs. 2 Satz 1 AWV i.V.m § 19 Abs. 4 Satz 1 Nr. 1, Abs. 6 AWG eine Ordnungswidrigkeit und mit einem Bußgeld von bis zu 500.000 EUR bewehrt. **141**

aa) Hintergrund der EU-Blocking-Verordnung

Hintergrund der EU-Blocking-Verordnung¹³³ ist, dass die Sekundärsanktionen nach herrschender und auch zutreffender Meinung gegen das Völkerrecht verstoßen.¹³⁴ **142**

Um die Souveränität der EU-Mitgliedstaaten zu schützen, wurde deshalb im Jahr 2018 der Anhang der Verordnung (EG) Nr. 2271/96 des Rates vom 22.11.1996 zum Schutz vor den Auswirkungen der extraterritorialen Anwendung von einem Drittland erlassener Rechtsakte sowie von darauf beruhenden oder sich daraus ergebenden Maßnahmen (**EU-Blocking-Verordnung**) geändert. Die Änderung betraf die bereits im Jahr 1996 verabschiedete (ursprüngliche) EU-Blocking-Verordnung, welche als Reaktion auf die unrechtmäßigen Auswirkungen extraterritorialer Rechtsakte der Vereinigten Staaten (mit denen Sanktionen gegen Kuba, Iran und Libyen erlassen wurden) verabschiedet wurde.¹³⁵ **143**

130 <https://ofac.treasury.gov/consolidated-sanctions-list-non-sdn-lists/non-sdn-menu-based-sanctions-list-ns-mbs-list> (zuletzt abgerufen am 22.3.2024).

131 <https://ofac.treasury.gov/consolidated-sanctions-list-non-sdn-lists> (zuletzt abgerufen am 22.3.2024).

132 <https://ofac.treasury.gov/specially-designated-nationals-list-sdn-list/program-tag-definitions-for-ofac-sanctions-lists> (zuletzt abgerufen am 22.3.2024).

133 Verordnung (EG) Nr. 2271/96 des Rates vom 22.11.1996 zum Schutz vor den Auswirkungen der extraterritorialen Anwendung von einem Drittland erlassener Rechtsakte sowie von darauf beruhenden oder sich daraus ergebenden Maßnahmen.

134 Pelz, in: Sachs/Pelz, Außenwirtschaftsrecht, D. Rechtsquellen des US-Reexportkontroll- und Sanktionsrechts, Rn. 90; Schwendinger/Rehle, RdTW 2022, 382 Rn. 7.

135 Leitfaden: Fragen und Antworten: Annahme der aktualisierten Blocking-Verordnung, I. 1. [https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52018XC0807\(01\)](https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52018XC0807(01)) (zuletzt abgerufen am 22.3.2024).

bb) Regelungen der EU-Blocking-Verordnung

- 144** Nach den Regelungen der EU-Blocking-Verordnung ist es EU-Wirtschaftsteilnehmern verboten, die in dem Anhang der EU-Blocking-Verordnung gelisteten extraterritorialen Rechtsakte, einschließlich darauf beruhender Entscheidungen, Urteile oder Schiedssprüche, einzuhalten, da die EU die Anwendbarkeit und die Auswirkungen solcher Rechtsakte auf EU-Wirtschaftsteilnehmer nicht anerkennt (vgl. Artikel 5 Absatz 1 der EU-Blocking-Verordnung).
- 145** Die zentrale „Blocking-Regel“ stellt Art. 5 Abs. 1 der EU-Blocking-Verordnung dar. Nach Art. 5 Abs. 1 der EU-Blocking-Verordnung darf keine der in Art. 1 genannten Personen (im Wesentlichen „EU-Personen“) selbst oder durch einen Vertreter oder einen anderen Vermittler aktiv oder durch bewusste Unterlassung Forderungen oder Verbote, einschließlich Aufforderungen ausländischer Gerichte, nachkommen, die direkt oder indirekt auf den im Anhang aufgeführten Gesetzen oder den darauf beruhenden oder sich daraus ergebenden Maßnahmen beruhen oder sich daraus ergeben. Die Regelung statuiert somit ein Befolungsverbot.
- 146** Allerdings ist dieser Regelung nicht zu entnehmen, dass Geschäftsbeziehungen nicht aufgrund freier geschäftspolitischer Entscheidung beendet werden dürfen. Dies würde auch der durch die Verordnung geschützten Vertragsfreiheit zuwiderlaufen.¹³⁶
- 147** Erklärtes Ziel der Verordnung ist nämlich, sicherzustellen, „dass Geschäftsentscheidungen weiterhin frei getroffen werden können und EU-Wirtschaftsteilnehmern nicht durch die gelisteten extraterritorialen Rechtsakte, deren Anwendbarkeit auf EU-Wirtschaftsteilnehmer im Unionsrecht nicht anerkannt wird, aufgezwungen werden“. Eine freie Entscheidung liegt jedoch gerade nicht vor, wenn das Bestehen der Sanktion für die Entscheidung maßgeblich war.¹³⁷
- 148** Eine nicht erfolgte Kündigung wegen Angst vor einem Verstoß gegen die Verordnung ist nämlich auch nicht als eine freie Entscheidung zu werten.
- 149** Es kommt daher maßgeblich darauf an, ob der EU-Wirtschaftsteilnehmer die Sanktion als solche anerkennen wollte oder nicht. Um daher Verstöße gegen die EU-Blocking-Verordnung zu vermeiden, bietet es sich an, die Verträge entsprechend auszugestalten. Die Gestaltungsrechte sollten daran geknüpft sein, ob Sanktionen zu Störung des Vertragsverhältnisses führen, ohne hierbei entsprechende Sanktionsregime anzuerkennen. Die geschaffene nachteilige Lage durch die Sanktionsprogramme dürfte nämlich, sofern nicht missbräuchlich zur Kündigung genutzt, nicht als Anerkennung dieser gelten. Eine entsprechende ver-

¹³⁶ Vgl. zur Vertragsfreiheit: Frage 5 des EU-Leitfadens der Kommission: Fragen und Antworten: Annahme der aktualisierten Blocking-Verordnung; EuGH (Große Kammer), Urt. v. 21.12.2021, Rs. C-124/20 = RIW 2022, 117, 122.

¹³⁷ LG Hamburg, Urt. v. 15.10.2018 – 318 O 330/18 = BeckRS 2018, 31002 Rn. 40; *Bierwagen*, RIW 2020, 584, 586.

tragliche Regelung schränkt weder den freien Außenhandel ein, noch berührt sie die außenpolitischen Interessen der Bundesrepublik Deutschland.¹³⁸

Bei einer erklärten oder zu erklärenden Kündigung ist allerdings zu beachten, dass nach der Rechtsprechung des EuGH die Beweislast, dass die Kündigung nicht wegen der Einhaltung einer Sanktion erfolgt, bei dem Kündigenden liegt.¹³⁹ **150**

Die Blocking-Verordnung gilt für die im Anhang der Verordnung aufgeführten extraterritorialen Rechtsakte („gelistete extraterritoriale Rechtsakte“). **151**

Im Ergebnis ist die EU-Blocking-Verordnung daher (Stand Februar 2024) nur relevant, soweit es sich um Geschäfte mit Iran- und/oder Kuba-Bezug handelt. **152**

b) § 7 AWV

Mehr Relevanz dürfte für deutsche Wirtschaftsteilnehmer § 7 AWV aufweisen.¹⁴⁰ **153**

§ 7 Satz 1 AWV untersagt es Inländern, im Außenwirtschaftsverkehr eine Erklärung abzugeben, durch die er sich an einem Boykott (hier gleichbedeutend mit Sanktionen) gegen einen anderen Staat beteiligt. **154**

Ziel des Boykottverbots aus § 7 AWV ist es, Störungen der auswärtigen Beziehungen der Bundesrepublik Deutschland zu vermeiden, welche eintreten würden, wenn sich Inländer an einen Boykott gegen einen anderen Staat beteiligten.¹⁴¹ **155**

Diesem Ziel folgend statuiert § 7 Satz 2 AWV auch eine Ausnahme von dem Verbot derart, dass das Boykottverbot nicht gilt, wenn eine Erklärung abgegeben wird und auch der Sicherheitsrat der UN (§ 7 Satz 2 Nr. 1 AWV), der Rat der EU im Rahmen des Kapitels 2 des Vertrags über die Europäische Union (EUV) (§ 7 Satz 2 Nr. 2 AWV) oder die Bundesrepublik Deutschland (§ 7 Satz 2 Nr. 3 AWV) wirtschaftliche Sanktionsmaßnahmen beschlossen hat. **156**

Dieser Ausnahmetatbestand ist beispielsweise in Bezug auf Russland wegen der beschlossenen EU-Sanktionen erfüllt. **157**

Hierbei ist es für die Erfüllung des Ausnahmetatbestands schon ausreichend, dass überhaupt Sanktionsmaßnahmen gegen den betroffenen Staat beschlossen wurden, wobei die inhaltliche Reichweite dieser gleichgültig ist.¹⁴² Dies ergibt **158**

138 Bälz, NJW 2020, 878, 883.

139 EuGH (Große Kammer), Urt. v. 21.12.2021, Rs. C-124/20 = RIW 2022, 117, 122.

140 Zur AWV siehe auch → Rn. 100 ff. sowie → von Bodungen, Kap. 25 Rn. 9 ff. m. w. N.

141 Hoffmann, AW-Prax 2019, 88, 88.

142 Bälz, NJW 2020, 878, 882; Hoffmann, EuZW 2019, 315, 318; Jungkind/Winkler, AW-Prax 2019, 354, 355.

sich nicht nur aus dem Wortlaut von § 7 Satz 2 AWV selbst,¹⁴³ sondern auch aus der Verordnungsbegründung.¹⁴⁴

- 159** Das Ziel der Norm, die Störung auswärtiger Beziehungen zu vermeiden, kann nämlich nicht erreicht werden, wenn diese Beziehungen ohnehin schon durch entsprechende Maßnahmen der UN, der EU oder der Bundesrepublik belastet sind.¹⁴⁵ Aus diesem Grund dürfte in einer Vielzahl von Fällen kein Verstoß gegen § 7 Satz 1 AWV zu befürchten sein.
- 160** Wegen der Ausnahme in § 7 Satz 2 AWV wird die Norm in der Praxis kaum im Fokus von deutschen Unternehmen stehen bzw. nur in besonders gelagerten Fällen, etwa wenn etwa das Mutterunternehmen aus einer anderen Jurisdiktion außerhalb Europas stammt, von Relevanz sein.

8. Weitere Sanktionen anderer Staaten und Organisationen

- 161** Neben den hier beschriebenen Sanktionsprogrammen bestehen noch zahlreiche weitere Sanktionsprogramme, etwa solche der Schweiz, solche des Vereinigten Königreichs (UK) oder Chinas.
- 162** Es ist daher von hoher Bedeutung zu wissen, welches Sanktionsprogramm auf das jeweilige Geschäft möglicherweise anwendbar ist. Gerade die Sanktionsprogramme der UK ähneln, nicht nur wegen der EU-Vergangenheit, solchen der EU. Dennoch sind etwaige Unterschiede zu beachten.
- 163** Zudem kann es von Relevanz sein, drittstaatliche Sanktionsregimes zu beachten, wenn ein Unternehmen den dortigen Markt bedient. Denn auch außerhalb des streng juristischen Anwendungsbereichs können Sanktionsprogramme Wirkung entfalten, etwa durch den Ausschluss von öffentlichen Vergabeverfahren, der lokale Tochtergesellschaften oder Repräsentanzen vor wirtschaftliche Probleme stellen könnte.
- 164** Ein wichtiger Schritt beim Aufbau des Compliance-Management-Systems eines Unternehmens ist es daher, zu evaluieren, welches Sanktionsrecht einschlägig ist. Nur so können etwaige Gebote und Verbote befolgt werden.
- 165** Sollten drittstaatliche Sanktionsregimes Relevanz entfalten, so sollten sie nicht vorbehaltlos beachtet werden, sondern zunächst sollte abgewogen werden, ob ihre Beachtung seinerseits das Risiko eines Verstoßes gegen anwendbare Anti-Boikottregelungen birgt. Sollte dies der Fall sein, gibt es häufig Wege, um dieses Risiko seinerseits zu reduzieren.

¹⁴³ So auch *Jungkind/Winkler*, AW-Prax 2019, 354, 355.

¹⁴⁴ Begründung zur Zwölften Verordnung zur Änderung der Außenwirtschaftsverordnung, Stand: 6.12.2018, S. 8.

¹⁴⁵ Begründung zur Zwölften Verordnung zur Änderung der Außenwirtschaftsverordnung, Stand: 6.12.2018, S. 8.

III. Konsequenzen und Haftung

Da sich dieses Handbuch vor allem an deutsche Rechtsanwender richtet, werden im Folgenden nur die Konsequenzen und die Haftung bezüglich des wohl am häufigsten einschlägigen Sanktionsrechts, des EU-Sanktionsrechts unter Berücksichtigung von nationalen deutschen Vorschriften vorgestellt. Hierbei beschränken sich die Ausführungen auf solche Vorschriften, die für die Mehrzahl der Leser aus Sicht der Verfasser von erhöhter Relevanz sind. **166**

Dies bedeutet allerdings nicht, dass deutsche Rechtsanwender andere Sanktionsregimes komplett außer Acht lassen dürfen. Vielmehr ist stets sorgsam darauf zu achten, ob personelle oder territoriale Anknüpfungspunkte bestehen, welche den Anwendungsbereich anderer Sanktionsregimes eröffnen. **167**

1. Straf- und ordnungswidrigkeitsrechtliche Folgen

In Deutschland sind die Vorschriften über Straftaten und Ordnungswidrigkeiten in Bezug auf Sanktionsverstöße in §§ 17 ff. AWG i.V.m. 80 ff. AWV geregelt. **168**

a) § 17 AWG

Gemäß § 17 Abs. 1 AWG wird der Verstoß gegen eine Rechtsverordnung nach § 4 Abs. 1 AWG, die der Durchführung einer vom Sicherheitsrat der Vereinten Nationen nach Kapitel VII der Charta der Vereinten Nationen (§ 17 Abs. 1 Nr. 1 AWG) oder der Durchführung einer vom Rat der Europäischen Union im Bereich der Gemeinsamen Außen- und Sicherheitspolitik (§ 17 Abs. 1 Nr. 1 AWG) dient, mit einer Freiheitsstrafe von einem Jahr bis zu zehn Jahren bestraft. **169**

§ 17 Abs. 2 AWG stellt einen Qualifikationstatbestand dazu dar, für den Fall, dass in den Fällen des Abs. 1 für den Geheimdienst einer fremden Macht (Nr. 1) oder gewerbsmäßig oder als Mitglied einer Bande gehandelt wird, die sich zur fortgesetzten Begehung solcher Taten verbunden hat (Nr. 2). **170**

Erwähnenswert dürfte auch § 17 Abs. 6 AWG sein, wonach auch ein leichtfertiges Handeln mit Strafen von bis zu drei Jahren oder Geldstrafe bedroht ist. Ein solch leichtfertiges Handeln ist mit einem zivilrechtlichen grob fahrlässigen Handeln vergleichbar.¹⁴⁶ Es liegt vor, wenn sich die Sachlage geradezu aufdrängt und der Täter gleichwohl handelt, weil er dies aus besonderer Gleichgültigkeit oder grober Unachtsamkeit außer Acht lässt.¹⁴⁷ **171**

b) § 18 AWG

In der Praxis dürfte allerdings § 18 AWG im Vergleich zu § 17 AWG für Unternehmen von erhöhter Relevanz sein. **172**

¹⁴⁶ *Kudlich*, in: BeckOK StGB, 59. Ed. 1.11.2023, § 15 StGB Rn. 32.

¹⁴⁷ BGH, Urt. v. 24.6.2008 – 5 StR 89/08 = NJW 2008, 2516, 2517; *Neuheuser*, in: Münch-Komm-StGB, § 261 Rn. 108; BGH, Urt. v. 9.11.1984 – 2 StR 257/84 = NJW 1985, 690.

- 173** Nach § 18 Abs. 1 Nr. 1 AWG wird unter anderem mit Freiheitsstrafen von drei Monaten bis zu fünf Jahren bestraft, wer einem Ausfuhr-, Einfuhr-, Durchfuhr-, Verbringungs-, Verkaufs-, Erwerbs-, Liefer-, Bereitstellungs-, Weitergabe- oder Investitionsverbot (vgl. § 18 Abs. 1 Nr. 1 lit. a), einem Sende-, Übertragungs-, Verbreitungs- oder sonstigen Dienstleistungsverbot (§ 18 Abs. 1 Nr. 1 lit. b) oder einem Verfügungsverbot über eingefrorene Gelder und wirtschaftliche Ressourcen (§ 18 Abs. 1 Nr. 1 lit. c) eines im Amtsblatt der Europäischen Gemeinschaften oder der Europäischen Union veröffentlichten und unmittelbar geltenden Rechtsaktes der Europäischen Gemeinschaften oder der Europäischen Union zuwiderhandelt, welcher der Durchführung einer vom Rat der Europäischen Union im Bereich der gemeinsamen Außen- und Sicherheitspolitik beschlossenen wirtschaftlichen Sanktionsmaßnahme dient.
- 174** § 18 Abs. 1 Nr. 2 AWG sieht das gleiche Strafmaß bei einem Verstoß gegen die dort genannten Genehmigungspflichten vor.
- 175** Die Zuwiderhandlung gegen einen Verwaltungsakt nach § 6 AWG (vgl. oben → Rn. 103 ff.) ist gemäß § 18 Abs. 1a AWG ebenfalls mit einem Strafmaß von Freiheitsstrafen von drei Monaten bis zu fünf Jahren bedroht.
- 176** Auch wenn Verstöße gegen die von der EU statuierten Umgehungsverbote, wegen der Unbestimmtheit der Begrifflichkeiten,¹⁴⁸ seit der Änderung des AWG durch das Gesetz zur Modernisierung des Außenwirtschaftsrechts im Jahr 2013¹⁴⁹ nicht mehr geahndet werden, sollte stets auch wegen der sehr weiten Auslegung der sanktionsrechtlichen Begriffe hinterfragt werden, ob die angedachte Handlung missbräuchlich wäre oder gar eine Umgehung seien könnte. In solchen Fällen könnte beispielsweise auch das Risiko einer strafrechtliche Teilnahmehandlung bestehen.

c) § 19 AWG

- 177** Die Ordnungswidrigkeitentatbestände sind in § 19 AWG geregelt.
- 178** Gemäß § 19 Abs. 1 AWG handelt ordnungswidrig, wer eine in § 18 Abs. 1 AWG, § 18 Abs. 1a AWG, § 18 Abs. 2 Nr. 1–7 AWG, § 18 Abs. 3 AWG, § 18 Abs. 4 AWG, § 18 Abs. 5 AWG oder § 18 Abs. 5a AWG oder § 18 Abs. 1b AWG oder § 18 Abs. 2 Nr. 8 AWG bezeichnete Handlung fahrlässig begeht.
- 179** Ebenso handelt gemäß § 19 Abs. 3 AWG ordnungswidrig, wer vorsätzlich oder fahrlässig einer Rechtsverordnung nach § 4 Abs. 1 AWG (§ 19 Abs. 3 Nr. 1 AWG) zuwiderhandelt.
- 180** Darüber hinaus ist der Tatbestand des § 19 Abs. 5 AWG von Bedeutung, wonach ordnungswidrig handelt, wer vorsätzlich oder fahrlässig einem im Amtsblatt der Europäischen Gemeinschaften oder der Europäischen Union veröffentlichten unmittelbar geltenden Rechtsakt der Europäischen Gemeinschaften oder der Eu-

148 BGH, Beschl. v. 23.4.2010 – AK 2/10 = NJW 2010, 2370, 2373.

149 BT-Drs. 519/12, S. 75.

ropäischen Union, der der Durchführung einer vom Rat der Europäischen Union im Bereich der Gemeinsamen Außen- und Sicherheitspolitik beschlossenen wirtschaftlichen Sanktionsmaßnahme dient, zuwiderhandelt, indem er eine Information nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt (§ 19 Abs. 5 Nr. 1 AWG), eine Vorabanmeldung nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig abgibt (§ 19 Abs. 5 Nr. 2 AWG), eine Aufzeichnung von Transaktionen nicht oder nicht für die vorgeschriebene Dauer aufbewahrt oder nicht oder nicht rechtzeitig zur Verfügung stellt (§ 19 Abs. 5 Nr. 3 AWG) oder eine zuständige Stelle oder Behörde nicht oder nicht rechtzeitig unterrichtet (§ 19 Abs. 5 Nr. 1 AWG).

Gemäß § 19 Abs. 6 AWG kann die Ordnungswidrigkeit in den Fällen von § 19 Abs. 1 AWG, von § 19 Abs. 3 Nr. 1 lit. a AWG und von § 19 Abs. 4 AWG 4 Satz 1 Nr. 1 AWG mit einer Geldbuße von bis zu fünfhunderttausend Euro, in den übrigen Fällen mit einer Geldbuße von bis zu dreißigtausend Euro geahndet werden. **181**

Neben der Vermeidung möglicher Strafbarkeiten und/oder Ordnungswidrigkeiten aufgrund der spezialgesetzlichen Rechtsgrundlagen muss zusätzlich bedacht werden, dass die Pflicht zur sanktionsrechtlichen Compliance auch schon aus der allgemeineren Norm des § 130 OWiG erwächst.¹⁵⁰ **182**

d) Vermeidung von Verstößen

Zur Vermeidung von Verstößen gegen die genannten Tatbestände ist es – insbesondere für global agierende Unternehmen – unerlässlich, über ein risikoangemessenes, wirksames und effektives Sanktions-Compliance-Management-System zu verfügen. **183**

Darüber hinaus können Risiken von Verstößen, insbesondere im Hinblick auf ausländische Tochterunternehmen, bereits dadurch reduziert werden, dass natürliche Personen mit Staatsangehörigkeit eines EU-Mitgliedstaats von Geschäften und Entscheidungen, welche das Risiko eines Sanktionsverstosses bergen könnten, von Anfang an ferngehalten werden. Eine Tochtergesellschaft, welche nach dem Recht eines Nicht-EU-Staates gegründet wurde, müsste sich nämlich selbst nicht an die EU-Sanktionen halten. Dennoch besteht bei Mitwirkung von Mitarbeitern, welche eine Staatsangehörigkeit eines Mitgliedstaats haben, ein Risiko, dass diese gegen das von ihnen persönlich einzuhaltende EU-Sanktionsrecht verstoßen. **184**

2. Zivilrechtliche Folgen

Zivilrechtlich sind bei Einhaltung von Sanktionen innerhalb der EU keine Haftungen zu befürchten. **185**

¹⁵⁰ So auch zutreffend: *Wiedmann/Will*, RIW 2022, 173, 179.

- 186** Verträge mit sanktionierten Personen, die gegen Sanktionsrecht verstoßen und die nach Inkrafttreten von EU-Sanktionen geschlossen werden, sind gemäß § 134 BGB nichtig.¹⁵¹
- 187** Hierbei sollte schon das Verpflichtungsgeschäft, einem vorsichtigen Ansatz folgend, als Verstoß gegen das Bereitstellungsverbot anzusehen sein. Schließlich können schon Erfüllungsansprüche wirtschaftliche Ressourcen darstellen (vgl. oben → Rn. 59 ff.). Zudem zieht die Nichtigkeit des Erfüllungsgeschäfts regelmäßig die Nichtigkeit des Verpflichtungsgeschäfts nach sich,¹⁵² weshalb bereits das Eingehen einer entsprechenden vertraglichen Verpflichtung als Verstoß gegen das Bereitstellungsverbot anzusehen und damit von einer Nichtigkeit gemäß § 134 BGB auszugehen ist.¹⁵³
- 188** Hinsichtlich der eingefrorenen und von Sanktionen betroffenen Vermögenswerte, Gelder und wirtschaftlichen Ressourcen statuieren die Verbote selbst schon absolute Verfügungsverbote.¹⁵⁴ Vorsorglich sollte daher, auch wenn der Vertrag ohnehin nichtig wäre, überobligatorisch und zur Klarstellung die Kündigung des Vertrags erklärt werden.
- 189** Hierbei ist besonders zu beachten, dass dem sanktionierten Vertragspartner die bereits erbrachten Leistungen nicht zurückgegeben werden dürfen, da eine solche Rückgabe mit hoher Wahrscheinlichkeit vom Einfriergebot oder Bereitstellungsverbot erfasst ist.¹⁵⁵
- 190** Sollte ein Vertrag schon vor der Sanktionierung geschlossen worden sein, so ist die nunmehrige Erfüllung der vertraglich geschuldeten Leistungen als rechtlich unmöglich i. S. d. § 275 Abs. 1 BGB zu erachten.¹⁵⁶ Insgesamt sollten daher vertragliche Leistungen nicht erbracht werden, der Vertrag sollte also nicht erfüllt werden.
- 191** Der Vertragspartei der sanktionierten Person, welche das gültige Sanktionsrecht beachtet, erwachsen aus ihrem rechtmäßigen Verhalten bei EU-Geschäftspartnern auch keine Nachteile, da die EU zahlreiche sogenannte Haftungsausschlussklauseln bzw. „No Claim Clauses“ vorsieht.¹⁵⁷ Solche sind als Standardformulierungen beispielsweise derart formuliert, dass natürliche und juristische Personen, Organisationen und Einrichtungen sowie ihre Führungskräfte und Beschäftigten, die im guten Glauben, im Einklang mit dieser Verordnung zu handeln, Gelder oder wirtschaftliche Ressourcen einfrieren oder ihre Zurverfügungstellung ablehnen, hierfür nicht haftbar gemacht werden können, es sei denn, es

¹⁵¹ *Niedernhuber*, GSZ-Sonderausgabe 2022, 32, 36.

¹⁵² Vgl. BGH, Urt. v. 14.11.1960 – VIII ZR 116/59 = BeckRS 1960, 31188674.

¹⁵³ *Harings/Loets*, RdTW 2015, 321, 322

¹⁵⁴ *Niedernhuber*, GSZ-Sonderausgabe 2022, 32, 36.

¹⁵⁵ *Niedernhuber*, GSZ-Sonderausgabe 2022, 32, 35 m. w. N.

¹⁵⁶ *Harings/Loets*, RdTW 2015, 321, 323.

¹⁵⁷ Vgl. hierzu Ziff. 37, S. 15 Restriktive Maßnahmen (Sanktionen) – Aktualisierung der vorbildlichen Verfahren der EU für die wirksame Umsetzung restriktiver Maßnahmen.

ist nachgewiesen, dass das Einfrieren oder das Zurückhalten der Gelder oder wirtschaftlichen Ressourcen auf Fahrlässigkeit beruht.¹⁵⁸

Dieser Schutz wirkt allerdings nur in der EU. Außerhalb des Geltungsbereichs von EU-Recht drohen daher den Wirtschaftsteilnehmern mögliche Klagen auf Schadensersatz und Erfüllung.¹⁵⁹ **192**

Vor diesen Gefahren gilt es sich präventiv und privatrechtlich mit eigenen Sanktionsschutzklauseln bei Vertragsschluss abzusichern (vgl. unten → Rn. 200). **193**

3. Schadensersatz

EU-Rechtsunterworfenen sollten ein besonderes Augenmerk auf die Änderungen des 14. Sanktionspakets legen, wenn sie verlangen möchten, dass potenzielle Schäden ersetzt werden. **194**

Mit Art. 11a der Verordnung (EU) 833/2014 und Art. 11b der Verordnung (EU) 833/2014 hat die EU nämlich Normen geschaffen, die es EU-Rechtsunterworfenen erlauben Schadenersatzansprüche in der Union gerichtlich gegenüber russischen Schädigern geltend machen zu können. **195**

Art. 11a Verordnung (EU) 833/2014 begründet hierbei einen Anspruch auf Ausgleich derjenigen Schäden, die dem EU-Rechtsunterworfenen entstanden sind, weil dieser sich nicht wirksam gegen die gerichtliche Inanspruchnahme in einem Drittland im Zusammenhang mit einem Vertrag oder einem Geschäft, dessen Erfüllung von den mit der Verordnung (EU) 833/2014 verhängten Maßnahmen betroffen war, verteidigen konnte, weil ihr Zugang zu wirksamen Rechtsbehelfen versperrt war. **196**

Art. 11b Verordnung (EU) 833/2014 betrifft demgegenüber den Ausgleich von Schäden, die EU-Rechtsunterworfenen dadurch erlitten haben, dass der russische Schädiger in völkerrechtswidriger Weise oder unter Verstoß gegen bilaterale Investitionsabkommen zulasten des EU-Rechtsunterworfenen von der Anordnung vorübergehender Verwaltung von Vermögenswerten im Zusammenhang mit dem russischen Präsidialerlass vom 25.4.2023 über die Verwaltung von Vermögenswerten von Investoren aus „unfreundlichen Staaten“ oder vergleichbaren russischen Rechtsakten profitiert hat. **197**

4. Sonstige Folgen

Auch wenn Strafen und Bußgelder für alle Wirtschaftsteilnehmer Anreiz genug sein sollten, eine ordnungsgemäße Sanktions-Compliance zu pflegen, sollten auch die weiteren Folgen eines Sanktionsverstößes bedacht werden. **198**

¹⁵⁸ Sanktionsleitlinien S. 40 (F. 1.).

¹⁵⁹ *Allen*, in: Gehra/Gittfried/Lienke, Prävention von Geldwäsche und Terrorismusfinanzierung, I. Zivilrechtliche Folgen von Sanktionen, Rn. 132.

- 199** Für viele Unternehmen dürfte der Reputationsschaden, der mit Sanktionsverstößen einhergeht, eine hohe Abschreckungswirkung entfalten.¹⁶⁰ Solche Schäden, die etwa durch negative Presseberichterstattung und dadurch beeinflusste (potenzielle) Kunden entstehen, sind kaum bezifferbar, erweisen sich jedoch angesichts der Distanzierung vieler Neu-, aber auch Bestandskunden als gravierend für Unternehmen.
- 200** Außerdem können Sanktionsverstöße privatrechtliche Folgen haben, da viele Geschäftspartner entsprechende Sanktionsklauseln nutzen. Diese Klauseln sehen vor, dass sich die Geschäftspartner an gültiges Sanktionsrecht halten müssen und Verstöße entsprechende zivilrechtliche Folgen nach sich ziehen. Diese Folgen können, je nach privatautonomer Ausgestaltung solcher Klauseln, zur Beendigung des Vertrags, zu Vertragsstrafen oder zu Schadensersatzansprüchen führen.
- 201** Sollte das Unternehmen an Vergabeverfahren teilnehmen, gilt es ebenso zu beachten, dass eine Folge der Nichteinhaltung von Sanktionsrecht auch der Ausschluss von Vergabeverfahren der entsprechenden Jurisdiktion sein kann.¹⁶¹
- 202** Insgesamt zeigt sich daher, dass die negativen Folgen sich nicht nur auf Bußgelder und Strafen begrenzen lassen, sondern weitergehend auch an nachteilige wirtschaftliche Folgen zu denken ist.

IV. Maßnahmen zur Umsetzung eines Sanktions-Compliance-Management-Systems

- 203** Um der mannigfaltigen Risiken, die Verstöße gegen (Finanz-)Sanktionen nach sich ziehen, Herr zu werden, ist deren Berücksichtigung im Rahmen des Compliance-Management-Systems eines Unternehmens unabdingbar.¹⁶² Dies gilt insbesondere vor dem Hintergrund der steigenden globalen geopolitischen Komplexität und der antizipierten parallelen Zunahme an Anforderungen im Bereich der Sanctions-Compliance.
- 204** Eine Orientierungshilfe zur Umsetzung eines solchen Programms bieten auf Unionsebene die Empfehlung für ein internes Compliance-Programm in Bezug auf Dual-Use Güter¹⁶³ sowie auf nationaler Ebene das BAFA mit seinem Merkblatt

160 Zur Bedeutung der Reputationssicherung → *Schulz*, Kap. 1 Rn. 23 ff. m. w. N.

161 Dies ist auch bei Nichteinhaltung der US-Secondary-Sanctions zu bedenken, *Jungkind/Winkler*, AW-Prax 2019, 354, 356.

162 Zu den Kriterien für ein wirksames Compliance Management → *Schulz*, Kap. 1 Rn. 52 ff. m. w. N. Allgemein zur Exportkontrolle als Bestandteil eines Compliance-Management-Systems → *von Bodungen*, Kap. 25.

163 Empfehlung (EU) 2019/1318 der Kommission vom 30.7.2019 zu internen Compliance-Programmen für die Kontrolle des Handels mit Gütern mit doppeltem Verwendungszweck (Dual-Use-Güter) nach Maßgabe der Verordnung (EG) Nr. 428/2009 des Rates.

Firmeninterne Exportkontrolle (ICP).¹⁶⁴ Während beide Dokumente warenbezogene Sanktionen in den Fokus nehmen, erlangen die dort niedergelegten Grundsätze darüber hinaus auch Geltung für den Umgang mit Finanzsanktionen.

1. Risikobewertung

Um angemessene Maßnahmen ergreifen zu können, müssen Wirtschaftsteilnehmer zunächst ihr individuelles Risikoprofil kennen. Hierfür bietet sich die Ermittlung des Bruttoisikos nach den allgemeinen Grundsätzen zur Durchführung einer Risikoanalyse an.¹⁶⁵ Betrachtet werden sollten dabei die Produktpalette, die Kundenstruktur (→ Rn. 211 ff.), Vertriebs- und Transaktionskanäle, Länderisiken und Besonderheiten der Geschäftstätigkeit, kurzum alle Bereiche, die von Sanktionsrisiken betroffen sein können.¹⁶⁶ Dabei weisen die Risikofaktoren teilweise (größere) Schnittmengen mit Risikofaktoren einer allgemeinen Compliance-Risikoanalyse oder einer Geldwäsche-Risikoanalyse (gem. § 5 GwG) auf. Es kann sich daher anbieten – gerade mit Blick auf die geplante Einbeziehung präventiver Sanctions-Compliance-Maßnahmen in das Geldwäscherecht –, die Sanktionsrisiken in der Geldwäsche-Risikoanalyse zu berücksichtigen.

Kundenbezogene Risiken können etwa sein:¹⁶⁷

- Der Kunde ist selbst sanktioniert oder hat Kontakt zu sanktionierten Personen.
- Der Kunde hat seinen Sitz in einem Land, dessen Regierungs- und Wirtschaftsvertreter weitgehend Ziel restriktiver Maßnahmen sind.
- Kundendaten enthalten Personen, Adress- oder Telefonnummern, die mit Sanktionslisten übereinstimmen oder verdächtig ähnlich sind.
- Neugründung eines Unternehmens durch Fusion mit einer sanktionierten Entität bzw. einer mit sanktionierten Personen verbundenen Entität oder Änderung der Eigentümerstruktur im zeitlichen Zusammenhang mit neuen Listungen;
- bekannter Kunde verändert überraschend sein Einkaufsverhalten und fragt ohne erkennbare Begründung in hohem Umfang Produkte an;
- Verdacht auf bewusste Verschleierung der Eigentümerstruktur;
- ungewöhnlich komplexe Beteiligungsstrukturen, u. a. mit Gesellschaften, die ihren Sitz in Ländern haben, deren Regierungs- und Wirtschaftsvertreter weitgehend Ziel restriktiver Maßnahmen sind.

¹⁶⁴ BAFA Merkblatt Firmeninterne Exportkontrolle (ICO) (3. Aufl./April 2022), https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_icp.html (zuletzt abgerufen am 17.3.2024).

¹⁶⁵ Zu den Grundlagen und Anforderungen eines Risikomanagements → *Romeike*, Kap. 9.

¹⁶⁶ Vgl. <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019H1318&rid=8> (zuletzt abgerufen am 22.3.2024), vgl. Risikobewertung.

¹⁶⁷ Vgl. https://www.bmwk.de/Redaktion/DE/Downloads/S-T/sanktionsumgehung-hinweispa-pier-fuer-unternehmen.pdf?__blob=publicationFile&v=8 (zuletzt abgerufen am 22.3.2024).

- 207** Produktbezogene Risiken können sein:
- Kunden bevorzugen Produkte, die Anonymität begünstigen;
 - Kunden bevorzugen Produkte, die schnell verwertbar sind bzw. kurze Laufzeiten aufweisen;
 - die Güter und/oder deren Menge sind für die angegebene oder anderweitig bekannte Verwendung nicht plausibel.
- 208** Transaktionsbezogene Risiken können sein:
- Eine Transaktion wird zu marktunüblichen Preisen abgewickelt;
 - eine Transaktion wird, ohne erkennbar plausiblen Grund, unter Einschaltung Dritter abgewickelt;
 - eine Transaktion wird, ohne erkennbar plausiblen Grund, in mehrere kleine Teilbeträge aufgeteilt;
 - ein Kunde äußert einen Barzahlungswunsch, der in Bezug auf das Geschäft und dessen Volumen ungewöhnlich erscheint.
- 209** Geografische Risiken können sein:
- Kunde/Gesellschafter des Kunden/Geschäft/für Transaktion eingesetztes Bankkonto weist einen Bezug zu einem Staat auf, dessen Regierungs- und Wirtschaftsvertreter weitgehend Ziel restriktiver Maßnahmen sind.
- 210** Die interne Evaluierung sollte daher ein Augenmerk darauf legen, welches Sanktionsrecht einzuhalten ist und in welchen Bereichen und Geschäftsbeziehungen Risiken der Nichteinhaltung drohen. Die Ergebnisse dieser Risikobewertung haben maßgeblichen Einfluss auf die notwendigen Maßnahmen und möglichen Lösungen für die Entwicklung oder Umsetzung der unternehmensspezifischen Compliance-Verfahren.

2. Know Your Business Partner/Know Your Customer/Risikoanalyse

- 211** Abseits strengerer Regelungen für den Finanzsektor bestehen derzeit (noch) keine spezialgesetzlichen präventiven Prüfpflichten zur Vorbeugung von Sanktionsverstößen. Diese ist gleichwohl aus der allgemeinen Legalitätspflicht für Unternehmen¹⁶⁸ herleitbar und – nicht zuletzt – aus dem gesunden Eigeninteresse eines jeden Geschäftsleiters, Haftungsrisiken vom Unternehmen fernzuhalten.
- 212** Da Prüfpflichten nicht ins Unendliche reichen können, sollten für den Umfang präventiver Prüfungen haftungsreduzierende Aspekte berücksichtigt werden.¹⁶⁹ Nach der Haftungsklausel in den Standardformulierungen der EU¹⁷⁰ etwa können natürliche oder juristische Personen, Organisationen oder Einrichtungen für ihre Handlungen nicht haftbar gemacht werden, wenn sie nicht wussten und ver-

¹⁶⁸ Vgl. → *Schulz*, Kap. 1.

¹⁶⁹ So auch: *Hildebrandt/Koch*, IWRZ 2016, 152, 156.

¹⁷⁰ Haftungsausschlussklausel (Ziffer F.).

nünftigerweise nicht wissen konnten, dass sie mit ihrem Handeln gegen die in den Verordnung festgelegten Maßnahmen verstoßen würden.

Um dieser Pflicht gerecht zu werden, ist die Kenntnis des Geschäftspartners von elementarer Bedeutung. **213**

Schließlich steht und fällt die Wirksamkeit eines jeden Sanktions-Compliance-Management-Systems mit einer angemessenen Geschäftspartnerüberprüfung, auch als Business-Partner-Screening, bekannt. **214**

Die Überprüfung des Geschäftspartners dürfte vielen Wirtschaftsteilnehmern schon bekannt sein. Beispielsweise ist wegen des Lieferkettensorgfaltspflichtengesetzes die Kenntnis der Geschäftspartner in den Fokus vieler Wirtschaftsteilnehmer gerückt. Ebenso trifft etwa Verpflichtete nach dem Geldwäschegesetz unter anderem die Pflicht, ihre Geschäftspartner zu kennen (vgl. §§ 10 ff. GwG). **215**

In der Praxis hat sich oftmals schon ein Vier-Phasen-Modell für Business-Partner-Checks bewährt. **216**

a) Phase 1: Informationsbeschaffung

Die eigene Kenntnis des Geschäftspartners sollte bestimmte Informationen unbedingt umfassen. Hierbei bietet sich eine Orientierung an dem gesetzlich etablierten Vorbild, den Anforderungen aus dem Geldwäschegesetz, an. Dies hat für viele Wirtschaftsteilnehmer den Vorteil, dass sie als Verpflichtete nach dem GwG die jeweiligen Informationen ohnehin einholen müssen. **217**

Zu empfehlen ist daher, in Bezug auf Vertragspartner und gegebenenfalls für diese auftretende Personen folgende Angaben in einer ersten Phase, der Informationsbeschaffungsphase, zu erheben: **218**

- bei einer natürlichen Person:
 - a) Vorname und Nachname,
 - b) Geburtsort,
 - c) Geburtsdatum,
 - d) Staatsangehörigkeit und
 - e) eine Wohnanschrift oder, sofern kein fester Wohnsitz mit rechtmäßigem Aufenthalt in der Europäischen Union besteht und die Überprüfung der Identität im Rahmen des Abschlusses eines Basiskontovertrags im Sinne von § 38 ZKG erfolgt, die postalische Anschrift, unter der der Vertragspartner sowie die gegenüber dem Verpflichteten auftretende Person erreichbar sind;
- bei einer juristischen Person oder bei einer Personengesellschaft:
 - a) Firma, Name oder Bezeichnung,
 - b) Rechtsform,
 - c) Registernummer, falls vorhanden,
 - d) Anschrift des Sitzes oder der Hauptniederlassung und

Teil 3 Besondere Aufgaben und Anwendungsfelder

- e) die Namen der Mitglieder des Vertretungsorgans oder die Namen der gesetzlichen Vertreter und, sofern ein Mitglied des Vertretungsorgans oder der gesetzliche Vertreter eine juristische Person ist, von dieser juristischen Person die Daten nach den Buchstaben a) bis d);
 - Zusätzlich sollten noch folgende Informationen eingeholt werden:
 - a) Handelsregisternummer(n),
 - b) Informationen zur Beteiligung von sog. politisch exponierten Personen (PEPs) i. S. d. § 1 Abs. 12 GwG,
 - c) Informationen zu bekannten/relevanten Risikofaktoren.
- 219** Diese Angaben sollten mittels eines standardisierten Fragebogens von dem Geschäftspartner selbst eingeholt und mit Unterschrift bestätigt werden.
- 220** In einem weiteren Schritt sollten sodann Informationen über die Geschäftsbeziehung eingeholt werden. Die folgenden Fragen sollten beantwortet werden:
- Was ist der Geschäftszweck?
 - Wie hoch ist der Wert der Transaktion?
 - Wer ist Empfänger des Geldes/der Ware?
 - Welche Zahlungsmodalitäten werden genutzt?
 - Sind weitere Geschäfte dieser Art in Zukunft geplant?
- 221** Generell gilt: Je mehr Informationen in diesem ersten Schritt gesammelt werden, desto effektiver wird sich der Business-Partner-Check insgesamt gestalten.

b) Phase 2: Überprüfung

- 222** Nachdem die Informationen eingeholt wurden, müssen sie auch überprüft werden. Hierzu sollten die jeweiligen Angaben in der zweiten Phase, der Überprüfungsphase, mittels glaubhafter Unterlagen wie etwa Auszügen aus dem Handelsregister oder notariellen Beglaubigungen oder durch Informationen aus Unternehmensdatenbanken verglichen werden.
- 223** Je nachdem, wie viele Informationen in dem ersten Schritt bereits gesammelt werden konnten, kann sich dieser Schritt auch als reine Verifizierung der vorhandenen Information darstellen. Ebenso denkbar ist jedoch, dass die Informationen aus der Vorbereitungsphase noch lückenhaft waren, weshalb es in diesem Schritt auch vorkommen kann, dass weitere Personen nunmehr zu identifizieren sind, welche ebenso zu überprüfen wären.
- 224** Unter Umständen kann es sogar vorkommen, dass die Hintergrundüberprüfung Abweichungen von den Informationen aus der Informationsbeschaffungsphase zutage fördert. In diesem Fall müssen die Gründe der Abweichungen plausibilisiert werden.
- 225** Zum Zwecke der Überprüfung hat sich der Einsatz kommerzieller Datenbanken bewährt.

c) Phase 3: Risikoeinschätzung

Nachdem die Informationen gesammelt und überprüft wurden, sollte in der Risikoklassifizierungsphase eine (Erst-)Einschätzung und Risikoklassifizierung vorgenommen werden. **226**

In diesem Schritt ist zu überprüfen, ob schon anhand der bisherigen Daten und Informationen bestimmte Risikofaktoren erkennbar sind. Ebenso sind die Geschäftspartner und alle beteiligten Personen gegen Sanktionslisten zu prüfen (**Sanktionslisten-Screening**). **227**

Dem Sanktionslisten-Screening kommt gerade bei Finanzsanktionen wegen des vorherrschenden Listenprinzips eine hervorgehobene Stellung innerhalb der durchzuführenden Compliance-Maßnahmen zu. Bei sehr großen Unternehmen mit vielen Kunden bietet sich der Einsatz eines EDV-gestütztes Screeningtools an. Bei problematischen Fällen sollte zusätzlich stets noch ein manueller Abgleich erfolgen. **228**

Sollte ein Sanktionslistentreffer festgestellt werden, gilt es zunächst zu überprüfen, ob die geprüfte Person auch tatsächlich die sanktionierte Person ist oder ob der Treffer ein sogenannter „false positive“ ist. Solche „false positives“ sind vermeintliche Treffer, welche auf einer Namensähnlichkeit beruhen, jedoch mangels Personenidentität keine echten Treffer darstellen. **229**

Da sich die Sanktionierung von Personen durch neue Entwicklungen ändern kann, sollten die Sanktionslistenprüfungen fortlaufend erfolgen. Das Überprüfungsintervall sollte hierbei risikoangemessen festgelegt werden. Hierbei gilt es zu beachten, dass die Zeiten enger zu fassen sind, je umfassender neue Sanktionsregimes sind. Dies kann sogar soweit führen, dass bei sehr umfassenden oder sehr neuen bzw. erstmaligen Sanktionen eine Ad-hoc-Prüfung notwendig wird. **230**

d) Phase 4: Entscheidung

Falls im Rahmen des Business-Partner-Checks eine Beteiligung bzw. ein Mitwirken einer sanktionierten Person festgestellt wird oder nicht auszuschließen ist, muss überlegt werden, ob ein Verstoß gegen das anwendbare Sanktionsrecht zu befürchten steht. Die Einschätzung diesbezüglich ist unbedingt zu dokumentieren. Sollte das Risiko eines Sanktionsverstößes nicht auszuschließen sein, sollte von der Geschäftsbeziehung Abstand genommen werden. **231**

3. Interne Meldeprozesse und Ablauforganisation

Gerade große Unternehmen stehen vor der Hürde, dass die große Anzahl von Vorfällen und Kunden, welche möglicherweise Risiken bergen, wenig überschaubar ist. Aber auch kleine Unternehmen können bei problematischen Fällen schnell den Überblick verlieren. **232**

Um dies zu vermeiden, hilft es, ein System zu etablieren und gewisse Standards im Unternehmen einzuführen. **233**

- 234** Die Etablierung des Systems beginnt zunächst damit, dass die interne Verantwortlichkeit für das Thema Sanktionsrecht geklärt wird.
- 235** Im Unternehmen sollte es, je nach Größe, eine Person oder eine (Unter-)Abteilung mit vertieftem Fachwissen zu sanktionsrechtlichen Fragen geben. Diese Personen sollten auch bei dem Entwurf der internen Richtlinien eingebunden und in diesen benannt werden. In der Praxis bietet es sich an, die Zuständigkeiten innerhalb der Compliance-Abteilung zu verorten, wobei in größeren Unternehmen, maßgeblich solchen des Finanzsektors, auch sog. Anti-Financial-Crime-Units bestehen, die die Prävention von Geldwäsche, Terrorismusfinanzierung, Sanktionsverstößen und sonstigen strafbaren Handlungen betreuen.
- 236** Alle relevanten Entscheidungen bezüglich sanktionsrechtlicher Themen sollten sodann nur noch unter Einbeziehung dieser Personen getroffen werden. Ebenso sollte die Kommunikation mit Behörden nur über diese Personen erfolgen.
- 237** Um die Einbindung der Personen zu gewährleisten, müssen interne Berichtslinien etabliert und entsprechend kommuniziert werden. Dies kann beispielsweise auch durch entsprechende Fixierung in den Richtlinien geschehen.¹⁷¹ Um die Strukturen und Berichtslinien noch einfacher darzustellen, bietet sich eine Visualisierung mittels eines Organigramms an.
- 238** Der primär Verantwortliche sollte, ähnlich wie der Geldwäschebeauftragte, der obersten Führungsetage angehören. Die Person muss insbesondere mit der Weisungsbefugnis ausgestattet sein, fragliche Transaktionen zu stoppen und von Mitarbeitern alle Informationen betreffend solcher Vorgänge anzufordern.
- 239** Ebenso sollten interne Abläufe und Meldungen nach standardisierten Prozessen erfolgen. Dies minimiert die Fehleranfälligkeit, da aufgrund der Standardisierung ein gewisses Qualitätslevel gehalten werden kann und die Mitarbeiter in ihrer Arbeit routiniert sind. Diese Standardprozesse sollten derart ausgestaltet sein, dass die meisten Risiken hinsichtlich etwaiger Sanktionsverstöße schon bei Beachtung des Standardprozesses erkannt und vermieden werden können. Beispielsweise könnten für das Kunden-Onboarding standardisierte und vorgedruckte Fragebögen verwendet werden. Eben jene Standardprozesse sind in Richtlinien festzuhalten (vgl. Unterabschnitt darunter).

4. Tone from the Top and Guidance

- 240** Wie in jedem Compliance-Management-System ist für den Erfolg des Sanktions-Compliance-Managements der „Tone from the Top“ sowie der „Conduct at the Top“¹⁷² entscheidend.¹⁷³ Nur wenn die Führungsebene die herausgehobene

171 Firmeninterne Exportkontrolle Betriebliche Organisation im Außenwirtschaftsverkehr, 2.3.

172 Moosmayer, Compliance, Rn. 144.

173 Vgl. → Schulz, Kap. 1 Rn. 69. Betriebliche Organisation im Außenwirtschaftsverkehr, S. 9, 2.1.

Relevanz der Einhaltung des Sanktionsrechts betont und vorlebt, werden die Mitarbeiter die Einhaltung der sanktionsrechtlichen Regelungen ernst nehmen.

Um die Wichtigkeit der Einhaltung des Sanktionsrechts zu unterstreichen, bietet sich eine Erwähnung im Code of Conduct an.¹⁷⁴ Dieser sollte dann auch entsprechend gelebt werden und ist durch nachgeordnete Richtlinien zu präzisieren. Verbindliche Richtlinien sind an dieser Stelle unersetzlich, da sie zweierlei Vorteile bieten. Zum einen wird wegen des verbindlichen Charakters der internen Richtlinien einem jedem Mitarbeiter die Wichtigkeit der Einhaltung des Sanktionsrechts bewusst gemacht. Zum anderen haben betriebsinterne Richtlinien den Vorteil, dass die Mitarbeiter nach entsprechender Anleitung handeln und im Zweifelsfall in den Richtlinien Antworten auf offene Fragen finden können. Um diese Funktion zu erfüllen, müssen die Richtlinien möglichst einfach, aber dennoch umfassend formuliert sein. Die Richtlinie darf sich nicht nur darauf beschränken, die einschlägigen Gesetze wiederzugeben. Vielmehr muss die Richtlinie für den einzelnen Mitarbeiter eine Art Anleitung sein, nach welcher er sich bei seiner täglichen Arbeit richten kann. 241

Besonders wichtig ist, dass die Richtlinien für alle Mitarbeiter leicht zugänglich sind. Dies kann beispielsweise durch ein Upload in das Intranet des Unternehmens bewerkstelligt werden. 242

5. Mitarbeiterzuverlässigkeit

Überprüfungen der Mitarbeiterzuverlässigkeit sind den meisten Unternehmen bekannt. Hierbei wird häufig nicht beachtet, dass auch bei Einstellung eines Mitarbeiters das Risiko besteht, dass dieser auf einer Sanktionsliste geführt wird. Dies gilt insbesondere für Mitarbeiter, die die oben genannten personellen Risikofaktoren aufweisen (vgl. → Rn. 206). Eine Auszahlung von Arbeitslohn gegenüber einer sanktionierten Person kann einen Verstoß gegen das Bereitstellungsverbot begründen. 243

Um eben jenem Risiko zu begegnen, sind daher nicht nur potenzielle Geschäftspartner, sondern in ähnlicher Art und Weise die eigenen Mitarbeiter beim Onboarding und während des laufenden Arbeitsverhältnisses kontinuierlich gegen Sanktionslisten zu prüfen. Eine Zuverlässigkeitsüberprüfung sollte nicht nur bei Einstellung, sondern auch während des laufenden Arbeitsverhältnisses durchgeführt werden. In der Praxis haben sich für diese (allgemeine) Zuverlässigkeitsüberprüfung die Vorlage eines polizeilichen Führungszeugnisses, die Vorlage der Ausweisdokumente und Steuernummer bei Berufseinstieg, aber auch gezielte Fragen während des Bewerbungsprozesses etabliert. Während des bestehenden Arbeitsverhältnisses bieten sich Leistungsbeurteilungen an sowie – zum Zwecke der Sicherstellung der Zuverlässigkeit – zusätzliche Schulungen (vgl. → Rn. 245 ff.). 244

¹⁷⁴ Zur Funktion eines Code of Conduct → Benkert, Kap. 4.

6. Schulungen

- 245** Schulungen versetzen Mitarbeiter in die Lage, einschlägiges Sanktionsrecht zu kennen und Verstöße zu vermeiden.
- 246** Neu eingestellte Mitarbeiter sollten schon in der Anfangszeit entsprechend geschult werden. Hierbei darf es allerdings nicht verbleiben. Vielmehr ist es geboten, dass Mitarbeiter in regelmäßigen Abständen an Schulungen teilnehmen. Die Schulungsintervalle sind hierbei variabel. Eine jährliche Schulung scheint allerdings, angesichts der Komplexität des Themas, angemessen. Zudem sollte über Ad-hoc-Schulungen nachgedacht werden, wenn es wesentliche Neuerungen gibt.
- 247** Mitarbeiterschulungen sollten sowohl rechtliche Grundlagen des Sanktionsrechts beinhalten als auch – und vor allem – unternehmensspezifische Risikofaktoren berücksichtigen, um die Mitarbeiter auf „Schwachstellen“ des Unternehmens zu sensibilisieren. Eine persönlich durchgeführte Schulung bietet häufig auch den Vorteil, dass der Dozent – als für Sanktions-Compliance verantwortliche Kraft – Hinweise aus der Belegschaft erhält, die auf weitere Risikofaktoren hindeuten könnten.
- 248** Es bietet sich an, einen Schulungsplan zu erstellen, der – nach allgemeinen Grundsätzen – festlegt, welche Mitarbeiter (Abteilung und Hierarchiestufe) in welchen Intervallen Schulungen unterzogen werden müssen.¹⁷⁵ Mitarbeiter in Führungsfunktionen und/oder in risikosensiblen Positionen sollten vertieften Schulungen unterzogen werden, während es für risikofernere Positionen ausreichen kann, Sanktions-Compliance im Rahmen einer allgemeinen Compliance-Schulung zu unterrichten.

7. Überprüfung

- 249** Letztlich muss das bestehende Sanktions-Compliance-Management-System fortlaufend überprüft werden.
- 250** Hierbei muss das Augenmerk insbesondere auf die Ordnungsgemäßheit der Abläufe, die Qualität der Arbeit, aber auch auf etwaige Schwachstellen gelegt werden.
- 251** Um eine einfache, zuverlässige, aber auch vollständige Kontrolle gewährleisten zu können, sollte ein Kontrollplan, ähnlich wie für Verfahren des Geldwäschebeauftragten, entwickelt werden.
- 252** Hierbei sollten die Prüfschritte und Prüfintervalle festgelegt werden. Außerdem muss das Unternehmen entscheiden, ob wegen der möglicherweise hohen Anzahl von Vorfällen, Stichproben gezogen werden sollen oder ob eine vollumfängliche Kontrolle stattzufinden hat.¹⁷⁶

¹⁷⁵ Zu Schenkungen siehe → *Hastenrath*, Kap. 6 sowie → *Schulz* Kap. 1 Rn. 78 ff.

¹⁷⁶ Zur Einrichtung von Kontrollen → *Schulz*, Kap. 1 Rn. 86.

Sollte sich das Unternehmen für eine Stichprobenprüfung entscheiden, so ist es von besonderer Wichtigkeit, eine repräsentative Anzahl von Stichproben zu wählen. Die Anzahl hängt hierbei zum einen von den festgestellten Risiken, zum anderen aber auch von der Anzahl der Geschäftsvorfälle an sich ab. **253**

8. Rechtliche Unterstützung

Für grundlegende Fragen, besondere Risikofälle oder bei Fragen zu ausländischen Rechtsordnungen sollte stets auch erwogen werden, externe rechtliche Beratung hinzuzuziehen. Gerade hinsichtlich etwaig bestehender (straft-)rechtlicher Haftungsrisiken kann eine externe Rechtsberatung, sei es zu konkreten Fragen oder auf abstrakter Ebene, einen hohen Mehrwert bieten. **254**

9. Einsatz von IT-Hilfen/Technik

Auch wenn es außerhalb des Finanzsektors derzeit keine Verpflichtung zum Einsatz technischer Unterstützung oder eines EDV-Monitorings gibt, ist davon auszugehen, dass ein Sanktionsrechts-Compliance-System, das der (stetig steigenden) Komplexität des Themengebiets und den (zumeist begrenzten) innerbetrieblichen Ressourcen gerecht werden will, nicht umhin kommt, sich technischer Hilfe zu bedienen. **255**

Hierbei bieten sich Abgleiche mit Datenbanken ebenso wie ein EDV-Monitoring der Kundenstammdaten an. Insgesamt sollte sichergestellt werden, dass ein Sanktionslistentreffer nicht übersehen wird. Wegen der unmittelbaren Geltung der entsprechenden Sanktionsregimes, beispielsweise solcher der EU, muss insbesondere Wert auf die Aktualität der Systeme und technischen Hilfen gelegt werden. Hierfür muss sichergestellt werden, dass die verwendeten Informationen laufend aktualisiert werden. **256**

10. Dokumentation und Aufbewahrung

Ebenso unerlässlich wie ein ordnungsgemäßes Handeln ist eine ordnungsgemäße Dokumentation und Aufbewahrung. **257**

Die einzelnen Prüfschritte sind in sämtlichen Stadien eines Vorhabens genau zu dokumentieren; hierbei empfiehlt sich eine Orientierung an den Dokumentations- und Aufbewahrungspflichten des GwG (§ 8 GwG), sofern anwendbar. **258**

Im Ernstfall kann die Dokumentation herangezogen werden, um den Nachweis zu stützen, dass ein Verstoß unverschuldet erfolgt ist. Denn kaum etwas eignet sich besser, um einem Fahrlässigkeitsvorwurf entgegenzutreten, als eine umfassende, ordnungsgemäße Dokumentation.¹⁷⁷ **259**

177 Vgl. → *Schulz*, Kap. 1 Rn. 90.

V. Checkliste

- 260** Um es Unternehmen zu ermöglichen, schnell und einfach eine Selbstevaluierung hinsichtlich des eigenen Sanktions-Compliance-Managements vorzunehmen, bietet sich eine Prüfung mittels einer Checkliste an.
- 261** Hierbei kann sich etwa an den nützlichen Fragen der EU zum ICP eines Unternehmens orientiert werden.¹⁷⁸
- 262** Es bietet sich an, die folgenden Fragen „abzuklopfen“:
- 1. Wurde eine Risikobewertung vorgenommen?**
 - Wurde das Sanktionsrisiko unter Beachtung aller Parameter analysiert?
 - Stehen alle relevanten Informationen zur Verfügung?
 - Ist der Geschäftspartner bekannt?
 - Wurde der Geschäftspartner überprüft?
 - Ist bekannt, welches Sanktionsrecht einzuhalten ist? Sind mitunter auch Sanktionsprogramme von Drittstaaten relevant?
 - 2. Interne Meldeprozesse und Ablauforganisation**
 - Sind die internen Zuständigkeiten klar definiert?
 - Sind die zuständigen Mitarbeiter ausreichend geschult?
 - Haben die zuständigen Mitarbeiter ausreichende Mittel und Befugnisse?
 - Ist sichergestellt, dass die zuständigen Mitarbeiter in die relevanten Vorgänge eingebunden sind?
 - Gibt es standardisierte und qualitativ hochwertige interne Prozesse?
 - Funktionieren die Berichtsprozesse?
 - 3. Gibt es ein Bekenntnis der Geschäftsleitung zu Sanktions-Compliance (Tone from the Top)?**
 - Hat sich die Führungsebene eindeutig zur Einhaltung von Sanktionsrecht verpflichtet?
 - Ist die Wichtigkeit der Einhaltung ausreichend klar kommuniziert?
 - Haben alle Mitarbeiter Zugang zu dieser Erklärung?
 - Ist Sanktions-Compliance Bestandteil des Code of Conduct?
 - 4. Mitarbeiterzuverlässigkeit**
 - Wurden die Mitarbeiter bei Einstellung auf Zuverlässigkeit geprüft?
 - Werden Sanktionslisten-Screenings der Mitarbeiter vorgenommen?
 - Sind die erhobenen Daten der Mitarbeiter vollständig und aktuell?
 - Wird die Zuverlässigkeit laufend sichergestellt?
 - 5. Schulungen**
 - Werden die (risikorelevanten) Mitarbeiter regelmäßig und ausreichend qualifiziert geschult?
 - Werden die Schulungsunterlagen regelmäßig aktualisiert?

¹⁷⁸ <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019H1318&rid=8>
(zuletzt abgerufen am 22.3.2024).

- Haben die Mitarbeiter innerhalb der festgelegten Intervalle an den Schulungen teilgenommen?

6. Kontrollen

- Gibt es interne Kontrollen?
- Gibt es einen internen Kontrollplan?
- Werden zu ergreifende Maßnahmen aus den Ergebnissen der internen Kontrolle abgeleitet?

7. Rechtliche Unterstützung

- Gibt es einen kompetenten Ansprechpartner, falls weitere rechtliche Beratung nötig ist?

8. Einsatz von IT

- Wird IT zur Unterstützung eingesetzt?
- Ist die IT-Sicherheit gewährleistet? Bestehen Cybersicherheitsmaßnahmen für den Schutz von Software und Technologie?

9. Dokumentation und Aufbewahrung

- Werden alle relevanten Vorgänge nachvollziehbar und vollständig dokumentiert?
- Werden alle relevanten Vorgänge für mindestens fünf Jahre aufgezeichnet?

25. Kapitel

Exportkontrolle und Compliance

I. Einleitung

Der Außenhandel ist eine tragende Säule der deutschen Wirtschaft und hat in den letzten Jahren – nicht zuletzt vor dem Hintergrund der weltweiten Globalisierungsprozesse – beeindruckende Zuwachsraten offenbart.¹ Die ausgeprägte Exportorientierung deutscher Unternehmen bringt es mit sich, dass sich diese vielfach mit den Vorgaben und Verboten des Exportkontrollrechts vertraut machen müssen. Darunter ist diejenige Teilmenge des Außenwirtschaftsrechts zu verstehen, die aus außen- und sicherheitspolitischen Erwägungen auf die besondere staatliche Überwachung der Ausfuhr von Gütern, Dienstleistungen sowie Geld- und Vermögenswerten abzielt.

Das Exportkontrollrecht ist ein komplexes Regelungsgefüge nationaler, europäischer sowie internationaler Rechtsnormen, die zugleich Gegenstand dynamischer Änderungen und Anpassungen sind. Ausgangspunkt ist dabei auf nationaler wie internationaler Ebene die Freiheit des Warenverkehrs.² Gleichwohl sind – weitreichende – exportkontrollrechtliche Beschränkungen und Verbote denkbar, sofern dies zur Wahrung höherrangiger Schutzgüter erforderlich ist.³ So bedarf die Ausfuhr von Rüstungsgütern und gelisteten sog. „Dual-Use-Gütern“ (d.h. Gütern, die sowohl zivilen als auch militärischen Zwecken zugeführt werden können) nach der – im Jahr 2021 neugefassten – europäischen Dual-Use-Verordnung⁴ regelmäßig der Genehmigung. In besonderen Fällen können Güterlieferungen ins Ausland sogar ausgeschlossen sein. Anknüpfungspunkte für exportkontrollrechtliche Restriktionen sind das Exportgut selbst, dessen Destination, der Empfänger sowie die bezweckte Endverwendung.⁵

Zentrales Ziel der Überwachung des Außenhandels ist es, einer Bedrohung Deutschlands und seiner Bündnispartner durch konventionelle Waffen und Massenvernichtungswaffen wirksam vorzubeugen.⁶ Nicht zuletzt in Anbetracht schwerwiegender Exportskandale in der Vergangenheit sollen überdies Ausfuhr-

1 Vgl. Statistisches Bundesamt, Außenhandel – Gesamtentwicklung des deutschen Außenhandels ab 1950, 2023, 3, https://www.destatis.de/DE/Themen/Wirtschaft/Aussenhandel/Tabelle/gesamtentwicklung-aussenhandel.pdf?__blob=publicationFile (zuletzt abgerufen am 27.3.2024).

2 Vgl. § 1 Abs. 1 Satz 1 AWG und Art. 34 f. AEUV.

3 Vgl. § 4 Abs. 1 AWG und Art. 36 AEUV.

4 Verordnung (EU) 2021/821 über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung, der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck, ABl. (EU) 2021 Nr. L 206/1; dazu eingehend BAFA, Die neue EU-Dual-Use-Verordnung (Verordnung (EU) 2021/821), Stand: September 2021, sowie unter → Rn. 15 ff.

5 BAFA, Exportkontrolle und das BAFA, 9. Aufl. 2022, 6; *Wolffgang/Witte*, CB 2015, 138.

6 BAFA, Exportkontrolle und das BAFA, 9. Aufl. 2022, 6; *dass.*, CB 5/2015, 168.

ren der deutschen Wirtschaft im Ausland weder konfliktverstärkende Wirkungen zeitigen noch Menschenrechtsverletzungen Vorschub leisten.⁷ Schließlich ist die Bundesrepublik Deutschland als Mitglied der internationalen Staatengemeinschaft durch vielfältige Vereinbarungen und Beschlüsse verpflichtet, supranationale Vorgaben zum Exportkontrollrecht einzuhalten bzw. im nationalen Recht umzusetzen.⁸

- 4 Die Einhaltung ausfuhrrechtlicher Vorgaben obliegt zuvörderst den Wirtschaftsbeteiligten selbst. Diesen wird im Bereich der Exportkontrolle die Beachtung vielzähliger Bestimmungen und Beschränkungen abverlangt. Im Verletzungsfall drohen empfindliche Sanktionen bis hin zu Freiheits- und Geldstrafen. Gleichwohl muss die Exportkontrolle nicht nur als lästiges Hemmnis begriffen werden. Vielmehr schafft sie Rechtssicherheit und Planbarkeit hinsichtlich der Durchführbarkeit von Exporten und sonstigen Handlungen im Außenwirtschaftsverkehr.⁹ Die Exportkontrolle stellt sich insofern als integraler Bestandteil eines gewissenhaften Compliance-Risikomanagements dar und schützt Unternehmen vor falschen Investitionsentscheidungen und Rechtsverletzungen.¹⁰ Unbesehen der für jeden Normadressaten bestehenden Pflicht zur Einhaltung geltenden Rechts ist exportorientierten Unternehmen anzuraten, durch entsprechende Organisation ihrer innerbetrieblichen Abläufe die Wahrung des an sie gerichteten Exportkontrollrechts sicherzustellen. Nicht zuletzt kann eine funktionierende Exportkontroll-Compliance dazu beitragen, Auslandsmärkte zu sichern und Reputations- sowie Imageschäden zu verhindern.¹¹ Wie sich ein wirkungsvolles Compliance-System unternehmensspezifisch etablieren lässt, wird in diesem Kapitel näher dargelegt. Dazu bedarf es vorab einer – gerafften – Darstellung der exportkontrollrechtlichen Rechtsgrundlagen sowie der einschlägigen Genehmigungspflichten und -verfahren.

II. Rechtsgrundlagen der Exportkontrolle in Deutschland

1. Supranationale Vorgaben

- 5 Das von deutschen Unternehmen zu beachtende Exportkontrollrecht fußt weitestgehend auf internationalen Vorgaben. In vielen Fällen ist es in unmittelbar geltenden Exportkontrollvorschriften der EU kodifiziert. Grund hierfür ist, dass die Effektivierung der Exportkontrolle in einer zunehmend globalisierten Welt

7 BAFA, Exportkontrolle und das BAFA, 9. Aufl. 2022, 6; *dass.*, CB 5/2015, 168.

8 BAFA, Praxis der Exportkontrolle, 5. Aufl. 2023, 3; *dass.*, CB 5/2015, 168.

9 BAFA, Praxis der Exportkontrolle, 5. Aufl. 2023, 2.

10 BAFA, Praxis der Exportkontrolle, 5. Aufl. 2023, 8. Zur Notwendigkeit eines systematischen Compliance-Risikomanagements siehe → *Schulz*, Kap. 1 Rn. 60 ff. sowie *Kark*, Compliance-Risikomanagement, 3. Aufl. 2024.

11 BAFA, Praxis der Exportkontrolle, 5. Aufl. 2023, 8. Zu Reputations- und Imageschutz als Bestandteil des Compliance Managements siehe → *Schulz*, Kap. 1 Rn. 23 ff.

ein abgestimmtes Vorgehen auf internationaler bzw. europäischer Ebene erforderlich macht.¹²

Weitreichende Genehmigungspflichten werden auf EU-Ebene im Rahmen der bereits angesprochenen Dual-Use-Verordnung für solche Güter statuiert, die sowohl zivilen als auch militärischen Zwecken zugeführt werden können. Solche genehmigungspflichtigen Dual-Use-Güter sind beispielsweise Analysatoren für Funksignale, die sich sowohl in der zivilen als auch in der militärischen Luftfahrt einsetzen lassen. 6

Flankierend treten die unmittelbar geltenden EU-Embargoverordnungen hinzu, die die außenwirtschaftsrechtlichen Genehmigungspflichten der Dual-Use-Verordnung überlagern und umfassende Beschränkungen von Wirtschaftsaktivitäten bis hin zu Verboten im Außenhandelsverkehr mit bestimmten Staaten statuieren.¹³ Genannt seien beispielhaft das – inzwischen freilich gelockerte – Embargo gegen den Iran aufgrund der Verordnung (EU) Nr. 267/2012¹⁴ sowie die seit dem Jahr 2014 gegen die Russische Föderation verhängten Wirtschaftsanktionen.¹⁵ Die Handelsbeschränkungen und Finanzsanktionen anlässlich der von der EU gegen die Russische Föderation angeordneten Embargo-Regelungen finden sich für die deutsche Exportwirtschaft nunmehr auch in einem offiziellen Merkblatt zum Außenwirtschaftsverkehr mit der Russischen Föderation zusammengefasst.¹⁶ 7

Ebenso können – ohne dass es insoweit überhaupt auf einen Exportvorgang ankäme – personenbezogene Restriktionen Platz greifen, wie sie sich beispielsweise in den EU-Terrorismusverordnungen wiederfinden.¹⁷ Den in diesen Verordnungen gelisteten Personen oder Organisationen dürfen weder Gelder noch wirtschaftliche Ressourcen zur Verfügung gestellt werden (sog. „Bereitstellungsverbot“). Verstöße gegen solche Wirtschaftsembargos und -sanktionen der EU können mit Freiheitsstrafe von bis zu fünf Jahren sanktioniert werden.¹⁸ 8

12 BAFA, Praxis der Exportkontrolle, 5. Aufl. 2023, 12.

13 Zur Relevanz von Embargos und Finanzsanktionen für Kreditinstitute bei der Durchführung des nationalen und internationalen Kapital- und Zahlungsverkehrs ausführlich → *Renz/Frankenberger*, Kap. 20 Rn. 15 ff.

14 ABl. (EU) 2012 Nr. L 88/1.

15 Verordnung (EU) Nr. 833/2014 vom 31.7.2014 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren.

16 BAFA, Merkblatt zum Außenwirtschaftsverkehr mit der Russischen Föderation, Stand: 20.2.2024; dazu auch *Müller-Ibold/Herrmann*, EuZW 2022, 1085, 1089. Zur sog. Sanktions-Compliance siehe → *Salathé/Moussaoui*, Kap. 24.

17 Vgl. u. a. die zwischenzeitlich wiederholt angepasste Verordnung (EG) Nr. 881/2002 betreffend Maßnahmen gegen das Al-Qaida-Netzwerk (ABl. [EG] 2002, Nr. L 139/9) sowie Verordnung (EG) Nr. 2580/2001 betreffend Maßnahmen gegen sonstige Terrorverdächtige (ABl. [EG] 2001, Nr. L 344/70). Siehe auch → *Salathé/Moussaoui*, Kap. 24.

18 Vgl. § 18 Abs. 1 AWG.

2. Nationale Vorgaben

- 9 Stellt sich das vorrangige EU-Recht als lückenhaft dar oder enthält es Öffnungsklauseln für einzelstaatliche Regelungen, kommt nationales Exportkontrollrecht zur Anwendung. In Deutschland ist dieses hauptsächlich im Außenwirtschaftsgesetz (AWG) und in der Außenwirtschaftsverordnung (AWV) geregelt. Das AWG spannt den außenwirtschaftsrechtlichen Rahmen auf, ordnet aber selbst keine Beschränkungen des Außenwirtschaftsverkehrs an. Die Kompetenz hierzu überantwortet es vielmehr – aus Gründen der Flexibilität und schnelleren Reaktionsfähigkeit auf aktuelle politische und wirtschaftliche Entwicklungen – der Exekutive.¹⁹ Die für den Anwender relevanten Verbote und Genehmigungspflichten sind denn auch in der Außenwirtschaftsverordnung enthalten. Beide Rechtstexte wurden im Jahr 2013 grundlegend überarbeitet und modernisiert, um ihre Anwendung in der Praxis zu erleichtern und solche Vorschriften zu streichen, die die deutschen Exporteure in der Vergangenheit gegenüber der europäischen Konkurrenz benachteiligt hatten.²⁰
- 10 Ergänzend ist das Gesetz über die Kontrolle von Kriegswaffen (sog. „Kriegswaffenkontrollgesetz“ – KrWaffKontrG) zu nennen, welches deren Herstellung, Beförderung und Inverkehrbringen einer Genehmigungspflicht unterstellt. Beim Export von Kriegswaffen können sich Überschneidungen ergeben und Genehmigungspflichten sowohl nach dem KrWaffKontrG als auch nach der Außenwirtschaftsverordnung zu beachten sein.²¹

3. Relevanz ausländischen Exportkontrollrechts

a) Allgemeines

- 11 Unternehmen in Deutschland müssen neben deutschem und europäischem Exportkontrollrecht unter Umständen auch die Exportkontrollvorschriften anderer Rechtsordnungen wahren. Dies gilt insbesondere im Hinblick auf das Recht des jeweils in Rede stehenden Einfuhrlandes. Aber auch andere Rechtsordnungen, zu denen ein spezifischer Bezug (sog. „genuine link“) besteht, können Relevanz erlangen. Eine solche Verknüpfung kann sich beispielsweise daraus ergeben, dass ein bestimmtes Gut durch das Hoheitsgebiet einer anderen Rechtsordnung befördert wird (sog. „Durchfuhr“) oder das exportierende Unternehmen dort eine Zweigniederlassung hat.

b) Insbesondere: US-Re-Exportkontrolle

- 12 Das US-Exportkontrollrecht ist bekannt dafür, dass es bereits entferntere Anknüpfungspunkte genügen lässt, um auch außerhalb des eigenen Hoheitsgebietes

19 Stein/Thoms, in: dies., Außenwirtschaftsgesetz, Einführung Rn. 20.

20 Vgl. insoweit die Darstellungen bei Kollmann, AW-Prax 2013, 267 ff., und Niestedt/Trennt, BB 2013, 2115 ff.

21 Bender, in: Paschke/Graf/Olbrisch, Hamburger Handbuch des Exportrechts, Abschnitt 37 Rn. 6 u. 10.

sowie gegenüber Nicht-US-Bürgern seinen – insoweit extraterritorialen – Geltungsanspruch zu erheben.²² Insbesondere kommt es aus Sicht des US-Rechts nicht zwingend darauf an, dass das US-Territorium als Import-, Export- oder Transitland berührt ist. Vielmehr kann es genügen, dass Waren von einem Exportvorgang betroffen sind, die US-amerikanischen Ursprungs sind oder einen Mindestwertanteil US-amerikanischer Komponenten – im Regelfall 25 % bzw. 10 % bei Ausfuhren in US-Embargoländer – aufweisen, selbst wenn sich der in Rede stehende Exportvorgang erst zu einem späteren Zeitpunkt als die ursprüngliche Ausfuhr aus den USA ereignet und sich vollständig außerhalb der USA abspielt (sog. „Re-Export“).²³ Das US-Recht verlangt den an einem solchen Re-Export beteiligten Personen ab, die von ihm statuierten Genehmigungserfordernisse und sonstigen Beschränkungen zu beachten.

Das US-Außenwirtschaftsrecht kennt überdies zahlreiche Listen, in denen Län- **13**
der, Personen, Organisationen und Vereinigungen spezifiziert werden, die Adressaten von Handels- und Finanzsanktionen sind.²⁴ Diese Listen sind mit den bereits angesprochenen Embargo- und Sanktionslisten auf europäischer Ebene nicht deckungsgleich. Das US-Embargorecht erhebt gleichwohl auch gegenüber ausländischen Unternehmen Geltungsanspruch.²⁵ Für europäische Unternehmen besteht die Herausforderung insbesondere auch darin, die Fülle der Listen mit den verbotenen oder kritischen Empfängern fortlaufend im Blick zu haben, was sich ohne EDV-Unterstützung schwerlich zuverlässig bewerkstelligen lässt.²⁶

Zwar knüpft die deutsche bzw. europäische Ausfuhrkontrolle an Verstöße gegen **14**
US-(Re-)Exportkontrollrecht oder US-Listentreffer keine unmittelbaren Rechtsfolgen. So ist die Notwendigkeit der Einholung einer US-Exportgenehmigung für die Behörden in Deutschland schon kein Prüfungspunkt. Die Nichtbeachtung von US-Recht kann für ein in Deutschland ansässiges Unternehmen gleichwohl gravierende Beeinträchtigungen zur Folge haben. Das gilt zunächst für Unternehmensangehörige, die die US-amerikanische Staatsangehörigkeit besitzen oder sich in den USA aufhalten. Aber auch dann, wenn einem Unternehmen mangels Präsenz auf dem US-Markt dort keine Geldbußen oder sonstigen Strafen drohen, ist zu besorgen, dass die US-Behörden das Unternehmen auf eine schwarze Liste (sog. „Denied-Persons-List“) setzen und es damit allen US-amerikanischen Unternehmen untersagen, Geschäftsabschlüsse mit ihm zu tätigen.²⁷

22 Eingehend zu diesen Anknüpfungspunkten jüngst *Haellmigk*, CCZ 2019, 135, 136 f.; *Roe-der/Schlutz/Hille/Havlik/Conte*, CCZ 2023, 337, 338.

23 *Hohmann*, AW-Prax 2007, 456, 457; *Pfeil/Mertgen*, Compliance im Außenwirtschaftsrecht, § 4 Kap. D Rn. 181 ff.

24 *Merz*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 32 Rn. 49; *Pfeil/Mertgen*, Compliance im Außenwirtschaftsrecht, § 5 Kap. F Rn. 94 ff.

25 Eingehend zu diesen sog. secondary sanctions jüngst *Haellmigk*, CCZ 2019, 135, 138.

26 *Merz*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 32 Rn. 80.

27 *Melchior*, in: Wecker/Ohl, Compliance in der Unternehmenspraxis, S. 91; *Sachs/Krebs*, CCZ 2013, 60, 64.

III. Exportkontrollrechtliche Genehmigungspflichten

1. Allgemeines

- 15 Ausfuhrrechtliche Genehmigungspflichten ergeben sich nach den vorstehenden Ausführungen insbesondere aus der Dual-Use-Verordnung sowie der Außenwirtschaftsverordnung. Wichtig ist aus Sicht der betroffenen Unternehmen, dass die Ausfuhrkontrolle nicht allein Warenexportgeschäfte im engeren Sinne erfasst. Neben physischen Gütern kann vielmehr auch die Übertragung von Software und Technologie exportkontrollrechtlichen Beschränkungen unterworfen sein.²⁸ Anknüpfungspunkte für Genehmigungspflichten können zudem – über die Ausfuhr inkriminierter Güter hinaus – auch deren Verbringung bzw. Durchfuhr, Handels- und Vermittlungstätigkeiten sowie die Erbringung technischer Unterstützungsleistungen sein.
- 16 Für die Zwecke der Exportkontrolle ist unerheblich, auf welche Weise das Ausfuhrgut in einen anderen Staat verbracht wird. Ob Software und Technologie in verkörperter Form (etwa in Papierform oder als CD bzw. DVD) ins Ausland geliefert oder auf elektronischem Wege (insbesondere also per E-Mail oder etwa durch Verlagerung eines firmeneigenen Servers) dorthin übermittelt wird, macht genehmigungsrechtlich keinen Unterschied.²⁹ Vor diesem Hintergrund kann sogar die Bereitstellung von Software und Technologie im unternehmenseigenen Intranet oder einer externen Cloud ausfuhrrechtlich relevant sein, wenn auf diese Weise der Zugriff von einem Drittstaat aus möglich wird.³⁰
- 17 Die Einholung einer behördlichen Genehmigung kommt freilich nur in Betracht, wenn nicht bereits ein – insoweit vorrangiges – exportkontrollrechtliches Verbot Anwendung findet. Neben den bereits angesprochenen länderbezogenen Embargos und personenspezifischen Sanktionen ist insbesondere das in §§ 17 f. KrWaffKontrG normierte Verbot (u. a.) der Ausfuhr atomarer, biologischer und chemischer Waffen zu beachten.

2. Genehmigungspflichten bei Ausfuhren in Länder außerhalb der EU

a) Gelistete Güter

- 18 Die Dual-Use-Verordnung gilt einheitlich in allen EU-Mitgliedstaaten und führt in ihrem Anhang I diejenigen Güter mit doppeltem Verwendungszweck auf, deren Ausfuhr ins außereuropäische Ausland unter Genehmigungsvorbehalt gestellt ist. Die in Anhang I gelisteten Positionen zeichnen sich durch detaillierte Leistungsbeschreibungen aus, welche u. a. Güter aus den Kategorien kerntechnische Materialien und Anlagen, allgemeine Elektronik, Rechner, Sensoren und

28 Vgl. die Definition von „Ausfuhr“ in § 2 Abs. 3 Nr. 2 AWG.

29 Huber/Huetz, Handbuch Import- und Exportrecht, S. 222.

30 BAFA, Exportkontrolle und das BAFA, 9. Aufl. 2022, 20; eingehend zu den exportkontrollrechtlichen Fragestellungen beim (Cloud-)Datentransfer auch Haellmigk/Vulin, CR 2013, 350; Haellmigk, CCZ 2016, 28 ff.

Laser sowie Luftfahrt und Antriebssysteme umfassen. Für die Listung genügt die bloße Möglichkeit einer militärischen Verwendung, auch wenn tatsächlich eine zivile Nutzung intendiert ist.

Anhang I der Dual-Use-Verordnung wird durch – ebenfalls genehmigungspflichtige – nationale Dual-Use-Sonderpositionen ergänzt. Diese finden sich in Teil I Abschnitt B der Anlage 1 zur Außenwirtschaftsverordnung, welche auch als Ausfuhrliste (AL) bezeichnet wird. Überdies finden sich in Teil I Abschnitt A der Ausfuhrliste Waffen, Munition und Rüstungsmaterial aufgeführt, deren Ausfuhr auf Ebene des nationalen Rechtes einer Genehmigungspflicht unterstellt wird. Den ausführenden Unternehmen obliegt es, die Listung eines Gutes zu erkennen, wobei im jeweiligen Einzelfall die Prüfung der europäischen *und* der nationalen Güterliste erforderlich ist. **19**

b) Nicht gelistete Güter

Auch wenn ein bestimmtes Gut weder in der Dual-Use-Verordnung gelistet noch auf der nationalen Ausfuhrliste aufgeführt ist, kann es gleichwohl Gegenstand außenhandelsrechtlicher Restriktionen sein, die auf einem bestimmten – kritischen – Verwendungszweck fußen. Sensitiv ist aus Sicht der Dual-Use-Verordnung beispielsweise eine Verwendung im Zusammenhang mit der Entwicklung, Herstellung, Lagerung, Ortung und Verbreitung von chemischen, biologischen oder Kernwaffen.³¹ Entsprechendes gilt bei militärischer Endverwendung, wenn gegen das Käufer- bzw. Bestimmungsland ein Waffenembargo verhängt ist.³² Des Weiteren ist nach der Dual-Use-Verordnung nunmehr die Genehmigung der Ausfuhr von bestimmten Gütern der digitalen Überwachung verpflichtend, sofern diese im Empfangsstaat für schwerwiegende Menschenrechtsverletzungen bestimmt sein können.³³ Schließlich sind bei nicht gelisteten Gütern nationale Genehmigungspflichten angeordnet, wenn sie für den Bau oder Betrieb einer Anlage für kerntechnische Zwecke in bestimmten – kritischen – Ländern vorgesehen sind.³⁴ **20**

Voraussetzung der Genehmigungspflichtigkeit eines konkreten Exportvorhabens gemäß den vorstehend beschriebenen Auffangtatbeständen (sog. „Catch-All“) ist, dass die zuständigen Behörden den Ausführer von der kritischen Verwendung – ggf. in Verbindung mit einem als problematisch eingestuften Länderkreis – in Kenntnis gesetzt haben. Eigene Kenntnis des Ausführers von diesen Umständen verpflichtet ihn seinerseits zur Unterrichtung der zuständigen Behörden.³⁵ Auf eigene Unkenntnis kann er sich in diesem Zusammenhang vor allem dann nicht berufen, wenn auf der Hand liegende Fakten und offensichtliche **21**

³¹ Vgl. Art. 4 Abs. 1 lit. a Dual-Use-Verordnung.

³² Vgl. Art. 4 Abs. 2 lit. b Dual-Use-Verordnung.

³³ Vgl. Art. 5 Abs. 1 Dual-Use-Verordnung.

³⁴ Vgl. § 9 Abs. 1 AWV.

³⁵ Vgl. Art. 4 Abs. 2, Art. 5 Abs. 2 Dual-Use-Verordnung; § 9 Abs. 2 Satz 1 AWV.

Möglichkeiten zur Kenntnisnahme in Rede stehen.³⁶ Die Ausfuhr hat in diesem Fall bis zur behördlichen Entscheidung über die Genehmigungspflicht zu unterbleiben.³⁷

3. Genehmigungspflichten bei Verbringungen

- 22** Die Lieferung von Waren, Software und Technologie aus dem Inland in das übrige Zollgebiet der EU wird im Gegensatz zur Ausfuhr als Verbringung bezeichnet.³⁸ Sie unterliegt grundsätzlich weniger strengen Anforderungen als die Ausfuhr.

a) Verbringungen bei Endverbleib in der EU

- 23** Die Verbringung von Dual-Use-Gütern in andere Mitgliedstaaten der EU ist grundsätzlich genehmigungsfrei. Der Verbringer hat den Empfänger lediglich darauf hinzuweisen, dass es sich um in Anhang I der Dual-Use-Verordnung gelistete Güter handelt und deren Ausfuhr aus der EU kontrollpflichtig ist.³⁹ Der Genehmigung bedarf allerdings die Verbringung der in Anhang IV der Dual-Use-Verordnung aufgeführten – als besonders sensibel eingestuft – Güter (u. a. Güter der Tarn- bzw. Stealth-Technologie, bestimmte Sprengstoffe, Raketenantriebssysteme und kerntechnische Materialien).⁴⁰ Dies gilt ebenso für die Verbringung von Rüstungsgütern, die sich in Teil I Abschnitt A der deutschen Ausfuhrliste genannt finden.⁴¹

b) Verbringungen mit anschließender Ausfuhr

- 24** Besonderheiten sind zu beachten, wenn der Lieferung eines Gutes innerhalb der EU die Ausfuhr in ein Drittland außerhalb der EU folgen soll. Für die national gelisteten Dual-Use-Güter in Teil I Abschnitt B der deutschen Ausfuhrliste besteht in diesem Fall – vorbehaltlich einiger Ausnahmen⁴² – eine Genehmigungspflicht, sofern der Verbringer Kenntnis vom endgültigen Bestimmungsziel außerhalb der EU hat.⁴³ Ebenso kann in Konstellationen der nachgelagerten Ausfuhr bereits die Verbringung solcher Güter der Genehmigung bedürfen, die weder in Anhang I der Dual-Use-Verordnung noch in der deutschen Ausfuhrliste aufgeführt und daher an sich als unkritisch eingestuft sind. Dies ist der Fall, wenn der Verbringer behördlicherseits darüber unterrichtet worden ist, dass diese Güter ganz oder teilweise für bestimmte kerntechnische Zwecke vorge-

36 *Schwendinger/Bender*, in: Paschke/Graf/Olbrisch, *Hamburger Handbuch des Exportrechts*, Abschnitt 35 Rn. 23.

37 Vgl. § 9 Abs. 2 Satz 3 AWV.

38 Vgl. § 2 Abs. 21 Nr. 1 AWG.

39 Vgl. Art. 11 Abs. 9 Dual-Use-Verordnung.

40 Vgl. Art. 11 Abs. 1 Satz 1 Dual-Use-Verordnung.

41 Vgl. § 11 Abs. 1 Satz 1 AWV.

42 Vgl. § 11 Abs. 5 AWV.

43 Vgl. § 11 Abs. 2 AWV.

sehen sind bzw. sein können und zudem ein inkriminiertes Bestimmungsland in Rede steht.⁴⁴ Sind dem Verbringer diese Umstände bekannt, hat er seinerseits die Verbringung auszusetzen und die zuständige Behörde zu unterrichten, damit diese über die Genehmigungspflichtigkeit befinden kann.⁴⁵

4. Sonstige Genehmigungspflichten

a) Handels- und Vermittlungsgeschäfte

Dass die Exportkontrolle nicht nur Ausfuhren und Verbringungen zum Gegenstand hat, zeigt sich daran, dass auch bestimmte damit im Zusammenhang stehende Handels- und Vermittlungsgeschäfte der Genehmigung bedürfen. Hierunter fallen Vermittlung, Aushandlung und Abschluss von Verträgen über den Erwerb oder das Überlassen bestimmter Güter sowie der Nachweis einer Gelegenheit zum Abschluss solcher Verträge.⁴⁶ 25

Die Dual-Use-Verordnung statuiert eine Genehmigungspflicht für drittlandbezogene Vermittlungstätigkeiten aus der EU heraus, wenn der Vermittler eines in Anhang I der Verordnung gelisteten Gutes mit doppeltem Verwendungszweck von der zuständigen Behörde unterrichtet worden ist, dass das Gut bestimmten – kritischen – Verwendungszwecken im Zusammenhang mit der Entwicklung, Herstellung, Lagerung und Verbreitung von chemischen, biologischen oder atomaren Waffen zugeordnet ist oder sein kann.⁴⁷ Ist dies dem Vermittler seinerseits bekannt geworden, obliegt ihm eine Informationspflicht gegenüber der Behörde.⁴⁸ 26

Die auf EU-Ebene statuierten Genehmigungs- und Unterrichtungspflichten werden im deutschen Recht dahingehend ausgeweitet, dass sie die vorstehend beschriebenen – kritischen – Handels- und Vermittlungsgeschäfte auch dann erfassen, wenn diese von Deutschen nicht aus der EU heraus, sondern unmittelbar in einem Drittland vorgenommen werden,⁴⁹ wobei Drittland alle Gebiete außerhalb des EU-Zollgebiets sind.⁵⁰ Überdies ordnet das nationale Recht für Handels- und Vermittlungsgeschäfte über Rüstungsgüter und bestimmte Kriegswaffen eine Genehmigungspflicht an.⁵¹ 27

b) Technische Unterstützung

Schließlich müssen exportierende Unternehmen sich des Umstandes gewahr sein, dass unter bestimmten Voraussetzungen auch die Erbringung technischer 28

⁴⁴ Vgl. § 11 Abs. 3 AWV.

⁴⁵ Vgl. § 11 Abs. 4 AWV.

⁴⁶ Vgl. Art. 2 Nr. 7 Dual-Use-Verordnung; § 2 Abs. 14 AWG.

⁴⁷ Vgl. Art. 6 Abs. 1 i.V.m. Art. 4 Abs. 1 Dual-Use-Verordnung.

⁴⁸ Vgl. Art. 6 Abs. 2 Dual-Use-Verordnung.

⁴⁹ Vgl. § 47 Abs. 2, 3 AWV.

⁵⁰ Vgl. § 2 Abs. 8 AWG.

⁵¹ Vgl. §§ 46 Abs. 1, 47 Abs. 1 AWV.

Unterstützung der Genehmigung bedarf. Betroffen kann – sehr weitreichend – jede technische Dienstleistung sein, wie etwa Reparatur, Wartung, Entwicklung, aber auch die Weitergabe praktischer Fähigkeiten und Kenntnisse etwa vermittelt durch Beratung und Ausbildung.⁵² Technische Unterstützung erfasst auch mündliche, fernmündliche und elektronische Formen der Hilfeleistung, weshalb bereits ein informelles Telefonat exportkontrollrechtliche Relevanz besitzen kann. Dies kann sogar für eine technische Hilfeleistung gelten, die ohne grenzüberschreitenden Bezug in Deutschland selbst – etwa auf einer Messe oder bei einer Betriebsbesichtigung – erbracht wird, sofern der Empfänger eine bestimmte ausländische Staatsangehörigkeit besitzt.⁵³

- 29 Eine Genehmigungspflicht ist in den vorstehend genannten Fällen davon abhängig, dass der Dienstleister von der zuständigen Behörde informiert worden ist, dass seine technische Unterstützung im Zusammenhang mit ABC-Waffen steht.⁵⁴ Hat er seinerseits Kenntnis von diesem Zweck, so hat er die zuständige Behörde zu informieren, welche sodann über die Genehmigungspflichtigkeit und -fähigkeit der technischen Unterstützung befindet.⁵⁵ Dieser Unterrichtsmechanismus zwischen Behörde und Dienstleister gilt ebenso für Support-Dienstleistungen im Zusammenhang mit einer militärischen Endverwendung in einem Embargoland.⁵⁶ Eine vergleichbare Regelung findet sich in der Außenwirtschaftsverordnung schließlich auch für technische Unterstützung beim Bau und Betrieb kerntechnischer Anlagen sowie hinsichtlich bestimmter Güter der Kommunikationsüberwachung.⁵⁷

IV. Exportkontrollrechtliches Genehmigungsverfahren

1. Zuständigkeit des BAFA

- 30 Sofern sich ein konkretes Exportvorhaben gemäß den vorstehend dargestellten Vorschriften als genehmigungspflichtig darstellt, ist die behördliche Erteilung einer entsprechenden Genehmigung zu beantragen. Zuständige deutsche Exportkontrollbehörde ist regelmäßig das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) in Eschborn bei Frankfurt/Main.⁵⁸ Das BAFA ist insbesondere zu involvieren, wenn eine genehmigungspflichtige Ausfuhr nach der Dual-Use-Verordnung in Rede steht und der Ausführer in Deutschland niedergelassen ist (sog. „Niederlassungsprinzip“).⁵⁹ Fußt die Genehmigungspflicht auf den Bestimmungen der Außenwirtschaftsverordnung, ist das BAFA für die Erteilung

52 Vgl. § 2 Abs. 16 AWG; ferner BAFA, Exportkontrolle und das BAFA, 9. Aufl. 2022, 25.

53 Vgl. § 51 Abs. 1 Nr. 2, Abs. 3 AWV.

54 Vgl. §§ 49 Abs. 1, 51 Abs. 1 AWV.

55 Vgl. §§ 49 Abs. 2, 51 Abs. 3 AWV.

56 Vgl. § 50 Abs. 1, 2, § 51 Abs. 2, 3 AWV.

57 Vgl. §§ 52, 52a, 52b AWV.

58 Vgl. § 13 Abs. 1 AWG.

59 Vgl. Art. 12 Abs. 2 Dual-Use-Verordnung.

der Genehmigung vor allem dann zuständig, wenn sich das zu liefernde Gut im Inland befindet (sog. „Belegenheitsprinzip“).⁶⁰

Hauptaufgabe des BAFA ist die Überprüfung, ob konkrete Exportvorhaben genehmigungspflichtig und -fähig sind. Für Fragen zum US-Exportkontrollrecht ist das BAFA dagegen nicht zuständig (vgl. insoweit oben → Rn. 12 ff.). Entsprechendes gilt für die Überwachung des Kapital- und Zahlungsverkehrs, welche – etwa im Hinblick auf die einschlägigen Embargoverordnungen – der Deutschen Bundesbank obliegt.⁶¹ Weitere ausschließliche Zuständigkeiten liegen beim Bundesministerium für Wirtschaft und Energie, das unter anderem auch Genehmigungsbehörde im Bereich der Kriegswaffenkontrolle ist.⁶² **31**

2. Ablauf des Genehmigungsverfahrens

Das deutsche Exportkontrollsystem fußt maßgeblich auf dem Gedanken der Eigenverantwortung der ausführenden Unternehmen.⁶³ Damit korreliert seitens der Unternehmen das Erfordernis, sich über die rechtlichen Beschränkungen und Genehmigungspflichten im Außenwirtschaftsverkehr zu informieren. **32**

Hilfreich ist insoweit das äußerst reichhaltige Informationsangebot des BAFA, welches den Wirtschaftsbeteiligten online zur Verfügung steht.⁶⁴ Insbesondere die vielzähligen Merkblätter des BAFA zu den einschlägigen Vorschriften im Exportkontrollbereich erleichtern den Einstieg in diese komplexe Materie. Die Handreichungen des BAFA können allerdings die Prüfung im jeweiligen Einzelfall nicht ersetzen, weshalb für exportierende Unternehmen eine eigenverantwortliche Befassung mit den sie treffenden Genehmigungspflichten unerlässlich bleibt, damit Ausfuhrvorhaben rechtssicher und möglichst effektiv realisiert werden können.⁶⁵ **33**

Die meisten der im Ausfuhrbereich erforderlichen Genehmigungsanträge sind beim BAFA auf elektronischem Wege über das Ausfuhrportal ELAN-K2 („Elektronische Antragserfassung und -kommunikation“) zu stellen. In diesem Zusammenhang erforderliche Dokumente sind dem BAFA mittels Uploads zur Verfügung zu stellen, sodass die Antragstellung im Regelfall vollständig papierlos erfolgt.⁶⁶ Dies gilt insbesondere im Hinblick auf die bei gelisteten Gütern beizubringenden Dokumente, die deren technische Qualifizierung nach den maßgeblichen Güterlisten erlauben, sowie den erforderlichen Nachweis über den End- **34**

60 Schwendinger/Bender, in: Paschke/Graf/Olbrisch, Hamburger Handbuch des Exportrechts, Abschnitt 36 Rn. 3.

61 Vgl. § 13 Abs. 2 Nr. 1 AWG.

62 Vgl. § 13 Abs. 2 Nr. 2 AWG u. § 11 Abs. 2 Nr. 4 KrWaffKontrG.

63 BAFA, Exportkontrolle und das BAFA, 9. Aufl. 2022, 5.

64 Abrufbar unter https://www.bafa.de/DE/Aussenwirtschaft/Ausfuhrkontrolle/Arbeitshilfen/arbeitshilfen_node.html (zuletzt abgerufen am 27.3.2024).

65 BAFA, Exportkontrolle und das BAFA, 9. Aufl. 2022, 5.

66 Siehe eingehend zur Antragstellung sowie den sich in der Praxis dabei typischerweise zeigenden Fehlern BAFA, Praxis der Exportkontrolle, 5. Aufl. 2023, 74 ff.

empfänger, den Endverbleib und den Verwendungszweck.⁶⁷ Gerade mit Blick auf die vom Empfänger beizubringende Bestätigung über die zivile Endverwendung hat das BAFA bereits seit dem Jahr 2017 zahlreiche neue Formularmuster samt Ausfüllanleitungen online bereitgestellt und laufend aktualisiert, die zu einem optimierten Ablauf des Genehmigungsverfahrens beitragen sollen. Auch die vertraglichen Vereinbarungen des deutschen Ausführers mit dem Empfänger im Ausland sind hochzuladen, setzt doch die Erteilung einer Ausfuhrgenehmigung im Regelfall einen verbindlichen Vertragsschluss zwischen beiden Parteien voraus.⁶⁸

3. Genehmigungstypen

- 35** Ausfuhrgenehmigungen können als Individual- bzw. Einzelgenehmigung beantragt werden. Eine Einzelgenehmigung gestattet die Lieferung einer bestimmten Anzahl an Gütern aufgrund eines Ausfuhrantrages an einen Empfänger.⁶⁹ Die Erteilung der Genehmigung hängt insbesondere von der Zuverlässigkeit des Antragstellers ab.⁷⁰ Maßgeblich ist insoweit die behördliche Einschätzung, dass der Ausführer willens und in der Lage ist, die ihm obliegenden Verpflichtungen des Exportkontrollrechts einzuhalten.⁷¹ Insoweit kommt es vor allem darauf an, dass das Unternehmen einen Ausfuhrverantwortlichen gegenüber dem BAFA benannt hat.⁷² Einen Sonderfall der Einzelgenehmigung bildet die sog. Höchstbetragsgenehmigung, die dem Ausführer im Rahmen einer festen Geschäftsbeziehung mit dem Empfänger Lieferungen bis zu einem bestimmten Gesamtumfang gestattet.⁷³
- 36** Die Globalausfuhr- bzw. Sammelgenehmigung reicht auf der Rechtsfolgenreite weiter und gestattet die Ausfuhr einer Vielzahl von Gütern an einen oder mehrere genau bestimmte Empfänger oder Drittländer.⁷⁴ Ihre Erteilung fußt nach der neugefassten Dual-Use-Verordnung allerdings – verschärfend – darauf, dass der Ausführer dem BAFA die Existenz eines hinreichenden innerbetrieblichen Exportkontrollsystems (sog. „Internal Compliance Programme“ – ICP) nachgewiesen hat.⁷⁵ Das Compliance-System muss ihn in die Lage versetzen, Verstößen gegen exportkontrollrechtliche Vorschriften schon im Vorfeld durch geeignete organisatorische Vorkehrungen vorzubeugen.⁷⁶ Die Wirksamkeit des unterneh-

67 Vgl. Art. 12 Abs. 4 Dual-Use-Verordnung; § 21 Abs. 2 Satz 1 AWV.

68 Pfeil/Mertgen, Compliance im Außenwirtschaftsrecht, § 6 Kap. F Rn. 72.

69 BAFA, Exportkontrolle und das BAFA, 9. Aufl. 2022, 30.

70 Vgl. § 8 Abs. 2 Satz 1 AWG.

71 Pfeil/Mertgen, Compliance im Außenwirtschaftsrecht, § 6 Kap. F Rn. 57.

72 Siehe zum Ausfuhrverantwortlichen noch unter → Rn. 45 ff.

73 Harnischmacher, in: Ovie/Berger/Harnischmacher, Praxishandbuch Transport, S. 480 f.

74 Vgl. Art. 12 i. V. m. Art. 2 Nr. 13 Dual-Use-Verordnung sowie § 4 AWV; ferner BAFA, Praxis der Exportkontrolle, 5. Aufl. 2023, 44.

75 Art. 12 Abs. 4 UAbs. 3 Dual-Use-VO; BAFA, Sammelgenehmigungen für Dual-Use-Güter, 2018, 14 f.

76 BAFA, Exportkontrolle und das BAFA, 9. Aufl. 2022, 30.

mensintern installierten Exportkontrollsystems wird vom BAFA zunächst im Antragsverfahren und sodann fortlaufend während des Gültigkeitszeitraums der Sammelgenehmigung – unter anderem durch Besuche vor Ort – überprüft.

Allgemeingenehmigungen werden vom BAFA im Bundesanzeiger veröffentlicht und gelten (nur) für den darin genannten Güter- und Länderkreis. Fällt eine beabsichtigte Ausfuhr unter eine nationale Allgemeingenehmigung, erleichtert dies das Verfahren signifikant, weil es nicht der Beantragung einer Einzelgenehmigung bedarf. Vielmehr genügt es, wenn sich der Ausführer bzw. Verbringer beim BAFA registriert hat.⁷⁷ Die Prüfung, ob eine Ausfuhr von einer Allgemeingenehmigung gedeckt ist, liegt dann allerdings ebenso beim registrierten Unternehmen wie das Risiko einer Fehleinschätzung. Dies gilt in gleicher Weise für die acht allgemeinen Ausfuhrgenehmigungen der EU, die als Anhang II zur Dual-Use-Verordnung erlassen worden sind⁷⁸ und zu denen das BAFA ergänzende Nebenbestimmungen veröffentlicht hat.⁷⁹ **37**

Zweifel, ob ein konkretes Ausfuhrvorhaben genehmigungspflichtig ist, lassen sich vermittels Erteilung eines Nullbescheids durch das BAFA ausräumen. Darin wird rechtsverbindlich festgestellt, dass ein bestimmtes Ausfuhrvorhaben im Hinblick auf einen bestimmten Empfänger weder verboten noch genehmigungspflichtig ist. Der Nullbescheid entfaltet allerdings keine Präcedenzwirkung für andere oder künftige Ausfuhrvorhaben, selbst wenn diese identische oder vergleichbare Güter bzw. Empfänger zum Gegenstand haben.⁸⁰ Nullbescheide sind wie Ausfuhrgenehmigungen zu beantragen. Folglich sind dafür alle relevanten Antragsunterlagen beizubringen. **38**

Schließlich kommt die Erteilung von unverbindlichen „sonstigen Auskünften“ zum Außenwirtschaftsverkehr durch das BAFA in Betracht. Insoweit genügt die formlose Beantragung, die ggf. auch telefonisch erfolgen kann.⁸¹ Trotz fehlender Rechtsverbindlichkeit bieten derartige Auskünfte durch das BAFA den Vorteil, dass sie häufig schneller ergehen als ein vergleichbarer förmlicher Bescheid.⁸² **39**

4. Sanktionen bei exportkontrollrechtlichen Verstößen

Vorsätzliche Verstöße gegen das Erfordernis der Genehmigung von Ausfuhren gelisteter Dual-Use-Güter sind Straftaten und werden mit Freiheitsstrafe von bis zu fünf Jahren oder Geldstrafe bestraft.⁸³ Fahrlässige Verstöße werden dagegen als Ordnungswidrigkeiten mit einer Geldbuße von bis zu fünfhunderttausend **40**

77 BAFA, Exportkontrolle und das BAFA, 9. Aufl. 2022, 30.

78 Vgl. Art. 12 Abs. 1 S. 1 lit. d i. V. m. Anhang II Abschnitte A–H Dual-Use-VO.

79 BAFA, Exportkontrolle und das BAFA, 9. Aufl. 2022, 30.

80 BAFA, Exportkontrolle und das BAFA, 9. Aufl. 2022, 36.

81 BAFA, Exportkontrolle und das BAFA, 9. Aufl. 2022, 21 u. 36.

82 Pfeil/Mertgen, Compliance im Außenwirtschaftsrecht, § 6 Kap. F Rn. 100 f.

83 Vgl. § 18 Abs. 2 Nr. 1, Abs. 5 Satz 1 Nr. 1 AWG.

Euro geahndet.⁸⁴ Adressat ist die für den Verstoß verantwortliche natürliche Person. Zwar besteht bei bestimmten exportkontrollrechtlichen Verstößen seit einigen Jahren die Möglichkeit eines Bußgeldausschlusses aufgrund freiwilliger Selbstanzeige.⁸⁵ Allerdings gehören zu den anzeigefähigen Verfehlungen insbesondere nicht – vorsätzliche oder fahrlässige – Verstöße gegen Genehmigungspflichten, sondern (nur) die fahrlässige Verletzung von Form- und Verfahrensrecht bei der Abwicklung von Ausfuhren, die keiner Genehmigungspflicht unterfallen bzw. von einer Genehmigung gedeckt sind.⁸⁶

- 41 Daneben kann gegen die Unternehmensleitung eine Geldbuße von bis zu einer Million Euro wegen Verletzung von Aufsichtspflichten verhängt werden, sofern die – etwa durch die Existenz eines Compliance-Programms dokumentierte – Vornahme gehöriger Aufsichtsmaßnahmen exportkontrollrechtsbezogene Straftaten von Mitarbeitern verhindert oder wesentlich erschwert hätte.⁸⁷ In diesem Fall besteht zugleich Gefahr, dass gegen das Unternehmen selbst eine (Verbands-)Geldbuße von bis zu zehn Millionen Euro festgesetzt wird.⁸⁸ Existenzbedrohend kann ferner die Einziehung des Wertes von Taterträgen aus inkriminierten Geschäften ohne Abzugsmöglichkeit für die dafür getätigten Aufwendungen sein (sog. „Verfall“).⁸⁹ Dies gilt ebenso für die Versagung künftiger Ausfuhrgenehmigungen mangels Zuverlässigkeit sowie einen Eintrag im Gewerbezentralregister, der sich u. a. in einem Ausschreibungsverfahren nachteilig auswirken kann.

V. Exportkontrollrechtliche Compliance-Strukturen

1. Allgemeines

- 42 Eine allgemeine Rechtspflicht zur Einrichtung eines Compliance-Systems ist im geltenden Außenwirtschaftsrecht bislang nicht normiert. Wie die Wirtschaftsbeteiligten ihre Exportkontrollprozesse organisieren, um außenwirtschaftsrechtliche Verstöße zu verhindern, bleibt ihnen vielmehr im Grundsatz selbst überlassen.⁹⁰
- 43 Bereits dargelegt wurde indes, dass die Zuverlässigkeit des Exporteurs bei der Erteilung von Ausfuhrgenehmigungen für Dual-Use-Güter ausschlaggebende Be-

84 Vgl. § 19 Abs. 1 u. 6 AWG. Nach § 17 Abs. 4 OWiG kann das gesetzliche Höchstmaß freilich auch überschritten werden, sofern es nicht ausreicht, um den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, abzuschöpfen.

85 Vgl. § 22 Abs. 4 AWG; siehe zur bußgeldbefreienden Selbstanzeige eingehend auch *Prieß/Arend*, AW-Prax 2013, 71 ff.; *Krause/Prieß*, NSTZ 2013, 688 ff.; *Pelz/Hofschneider*, AW-Prax 2013, 173 ff.; *dies.*, wistra 2014, 1 ff.; *Bünnigmann*, CCZ 2016, 60 ff.

86 *Prieß/Arend*, AW-Prax 2013, 71, 72; *Pelz/Hofschneider*, AW-Prax 2013, 173, 174.

87 Vgl. § 130 Abs. 1, Abs. 3 Satz 1 OWiG.

88 Vgl. § 30 Abs. 1, Abs. 2 Satz 2 u. 3 i. V. m. § 130 Abs. 3 Satz 2 OWiG.

89 Vgl. § 73 StGB u. § 29a OWiG.

90 *Schwendinger/Bender*, in: *Paschke/Graf/Olbrisch*, *Hamburger Handbuch des Exportrechts*, Abschnitt 36 Rn. 68.

deutung besitzt und es insoweit vor allem auf die Bestellung eines Ausfuhrverantwortlichen ankommt (siehe insoweit → Rn. 35). Weitergehend hat das BAFA bei der Erteilung von Globalausfuhrgenehmigungen nach der Dual-Use-Verordnung zu berücksichtigen, ob der Ausführer über ein internes Programm für rechtskonformes Verhalten bzw. ICP verfügt.⁹¹ Insofern kommt es bei der Erteilung von Globalausfuhr- bzw. Sammelgenehmigungen (siehe insoweit bereits → Rn. 36) durch das BAFA darauf an, ob laufende, wirksame, geeignete und verhältnismäßige Strategien und Verfahren existieren, um die Wahrung der Bestimmungen und Ziele der Dual-Use-Verordnung sowie der Bedingungen der auf ihrer Basis erteilten Genehmigungen zu fördern.⁹² Hintergrund ist, dass die vom Erfordernis der Einholung einer Genehmigung im Wege des Einzelantragsverfahrens dispensierten Unternehmen im Außenwirtschaftsverkehr besondere Verantwortung tragen.⁹³ Die Etablierung und Aufrechterhaltung eines innerbetrieblichen Compliance-Programms ist insoweit unverzichtbares Gegenstück zur Inanspruchnahme der mit Globalausfuhr- bzw. Sammelgenehmigungen einhergehenden Vereinfachung und Flexibilisierung der Ausfuhrabwicklung.⁹⁴ Schließlich sieht die sog. „Verteidigungsgüterrichtlinie“⁹⁵ ein Zertifizierungsverfahren für Unternehmen vor, die als Empfänger bestimmter Rüstungsgüter die maßgebliche Allgemeingenehmigung⁹⁶ des Lieferlandes für Verbringungen innerhalb der EU in Anspruch nehmen und sich auf diese Weise vom Erfordernis einer Einzelgenehmigung freizeichnen wollen. Der Aufwand für die – zur Erlangung der Zertifizierung erforderliche – Errichtung eines Compliance-Systems ist auch hier der Preis für die angestrebte Verfahrensvereinfachung und -optimierung. Die aufgrund der Verteidigungsgüterrichtlinie an die Betriebsorganisation zu stellenden Anforderungen⁹⁷ werden vom BAFA – (weit) über den eigentlichen Anwendungsbereich der Richtlinie hinaus – auch bei der Bewertung sonstiger Exportkontroll-Compliance-Systeme herangezogen (siehe hierzu → Rn. 48 ff.).

In der Zusammenschau spielen Compliance-Strukturen in Genehmigungsverfahren vor dem BAFA eine wichtige Rolle.⁹⁸ Insbesondere die mit ihnen einhergehenden Verfahrenserleichterungen schaffen – jenseits der Erteilung von Globalausfuhr- bzw. Sammelgenehmigungen – zwar keinen rechtlichen, wohl aber einen faktischen Zwang zur Etablierung effektiver innerbetrieblicher Exportkontrollsysteme.

44

91 Vgl. Art. 12 Abs. 4 UAbs. 3 Dual-Use-Verordnung.

92 Vgl. Art. 2 Nr. 1 Dual-Use-Verordnung.

93 *Beutel/Anders/Hötzl*, in: Ehlers/Wolffgang, *Recht der Exportkontrolle*, S. 399, 410.

94 *Sachs/Krebs*, CCZ 2013, 12, 14; *Wolffgang/Witte*, CB 2015, 138, 140.

95 Richtlinie 2009/43/EG zur Vereinfachung der Bedingungen für die innergemeinschaftliche Verbringung von Verteidigungsgütern, ABl. (EG) 2009 Nr. L 146/1.

96 Siehe zur Allgemeingenehmigung bereits → Rn. 37.

97 Vgl. Art. 9 Abs. 2 der Verteidigungsgüterrichtlinie sowie § 9 AWG i.V.m. § 2 Abs. 2 AWV.

98 *Wolffgang/Witte*, CB 2015, 138, 139.

2. Der Ausfuhrverantwortliche

- 45 Wie bereits dargelegt, wird ein Antrag auf Ausfuhr oder Verbringung exportkontrollierter Güter beim BAFA nur dann Erfolg haben, wenn die Zuverlässigkeit des Ausführers gewährleistet ist.⁹⁹ In diesem Zusammenhang sind die „Grundsätze der Bundesregierung zur Prüfung der Zuverlässigkeit von Exporteuren von Kriegswaffen und rüstungsrelevanten Gütern“¹⁰⁰ samt der flankierenden Bekanntmachung des BAFA¹⁰¹ von Belang. Danach erfassen die Grundsätze der Bundesregierung – über ihre insoweit zu enge Bezeichnung hinaus – sämtliche Dual-Use-Güter.¹⁰² Zugleich schreiben sie in ihrem Anwendungsbereich zwingend die Benennung eines Ausfuhrverantwortlichen gegenüber dem BAFA vor.¹⁰³ Die zuständigen Behörden verweigern in der Praxis die Erteilung von Ausfuhrgenehmigungen, sofern kein Ausfuhrverantwortlicher bestellt ist.¹⁰⁴ In Anbetracht dieser Verwaltungspraxis wirken die – lediglich als Verwaltungsanweisungen formulierten – Grundsätze der Bundesregierung für Antragsteller wie unmittelbar verbindliche Rechtsvorschriften.¹⁰⁵ Will ein Unternehmen gelistete Güter – seien es Rüstungsgüter, seien es Dual-Use-Güter – ausführen, gelingt dies im Ergebnis nur bei Bestellung eines Ausfuhrverantwortlichen.
- 46 Die Grundsätze der Bundesregierung bestimmen ferner, dass der Ausfuhrverantwortliche ein für die Durchführung der Ausfuhr verantwortlich zeichnendes Mitglied des Vorstands, ein Geschäftsführer oder ein vertretungsberechtigter Gesellschafter sein muss.¹⁰⁶ Diese „Verortung“ auf höchster Leitungsebene folgt dem Grundsatz „Exportkontrolle ist Chefsache“ und soll die Einhaltung und verbindliche Durchsetzung der unternehmensinternen Export-Compliance-Maßnahmen gewährleisten.¹⁰⁷ Nicht zulässig ist es daher, einen Prokuristen, Compliance Manager oder Abteilungsleiter als Ausfuhrverantwortlichen zu benennen.

99 Vgl. nochmals § 8 Abs. 2 Satz 1 AWG.

100 Bekanntmachung des Bundesministeriums für Wirtschaft und Technologie vom 25.7.2001, BAAnz. 17, 177 (nachfolgend als „Grundsätze der Bundesregierung“ bezeichnet).

101 Bekanntmachung zu den Grundsätzen der Bundesregierung zur Prüfung der Zuverlässigkeit von Exporteuren von Kriegswaffen und rüstungsrelevanten Gütern vom 27.7.2015 (nachfolgend als „BAFA-Bekanntmachung“ bezeichnet), https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_ausfuhrverantwortlicher_bekanntmachung.html (zuletzt abgerufen am 27.3.2024).

102 Vgl. Ziff. 1 Abs. 2 BAFA-Bekanntmachung.

103 Vgl. Ziff. 2 Abs. 1 Satz 1 Grundsätze der Bundesregierung („muss“).

104 Kritisch in Anbetracht dieses – unter dem Gesichtspunkt der Außenwirtschaftsfreiheit nicht unbedenklichen – Zwanges zur Benennung eines Ausfuhrverantwortlichen *Schwendinger/Bender*, in: Paschke/Graf/Olbrisch, *Hamburger Handbuch des Exportrechts*, Abschnitt 36 Rn. 73.

105 *Beutel/Anders/Hötzl*, in: Ehlers/Wolffgang, *Recht der Exportkontrolle*, S. 399, 404.

106 Vgl. Ziff. 1 Abs. 1 Satz 2 BAFA-Bekanntmachung.

107 *Wolffgang/Witte*, CB 2015, 138, 141. Zum Compliance Management als Bestandteil der Leitungsverantwortung siehe → *Schulz*, Kap. 1 Rn. 36 ff. m. w. N.

Der Ausführungsverantwortliche steht persönlich für die innerbetriebliche Einhaltung des Exportkontrollrechts in der Verantwortung. So verzichtet das BAFA im Einzelantragsverfahren auf eine eigene Prüfung und lässt sich stattdessen vom Ausführungsverantwortlichen versichern, dass dieser alle erforderlichen Maßnahmen trifft, damit die außenwirtschaftsrechtlichen Ge- und Verbote gewahrt werden.¹⁰⁸ Insbesondere hat der Ausführungsverantwortliche bei genehmigungspflichtigen Gütern vermittels einer geeigneten Binnenorganisation, Personalauswahl und -weiterbildungsmaßnahmen sowie entsprechender Überwachung sicherzustellen, dass es zu keinen Verstößen gegen ausfuhrrechtliche Bestimmungen kommt.¹⁰⁹ Diese Vorgaben sind zugleich der Nukleus bei der sogleich zu erörternden Etablierung einer funktionierenden Compliance-Organisation im Bereich der Exportkontrolle.¹¹⁰

3. Modell eines innerbetrieblichen Exportkontrollsystems

Auch soweit die neugefasste Dual-Use-Verordnung für Exporteure, welche Globalausfuhr- bzw. Sammelgenehmigungen nutzen, das Vorhandensein eines ICP vorschreibt (siehe insoweit auch → Rn. 36 u. 43), bleibt es den Mitgliedstaaten überlassen, welchen Anforderungen eines solches innerbetriebliches Exportkontrollsystem zu genügen hat.¹¹¹ Das BAFA hat ausgehend von den dargestellten Pflichten des Ausführungsverantwortlichen und vor dem Hintergrund der Vorgaben für die Zertifizierung nach der Verteidigungsgüterrichtlinie Kriterien herausgearbeitet, die sich als Richtschnur für alle außenwirtschaftsrechtlich motivierten Compliance-Programme begreifen lassen.¹¹² Ergänzend sind die – freilich nicht bindenden – Leitlinien der Europäischen Kommission für die Etablierung von Compliance-Konzepten im Dual-Use-Handel von Belang.¹¹³ Die darin aufgezeigten Kernelemente interner Compliance-Programme werden zwar in zum Teil divergierender Abfolge erläutert, sind inhaltlich aber (nahezu) identisch mit den Kriterien des BAFA, sodass sich für in Deutschland ansässige Unternehmen keine beachtenswerten Änderungen ergeben.¹¹⁴ Das überrascht schon deshalb nicht, weil das BAFA – gleichsam im Vorgriff auf die jüngere Empfehlung der Europäischen Kommission – die Diskussionen auf der EU-Ebene zur

108 Beutel/Anders/Hötzl, in: Ehlers/Wolffgang, Recht der Exportkontrolle, S. 399, 404.

109 Vgl. Ziff. 2 Abs. 1 Satz 1 BAFA-Bekanntmachung.

110 Merz, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 32 Rn. 13; Wolffgang/Witte, CB 2015, 138, 139.

111 Art. 12 Abs. 4 UAbs. 4 Dual-Use-Verordnung.

112 Das insoweit relevante Merkblatt des BAFA „Firmeninterne Exportkontrolle“ (3. Aufl. 2022) ist abrufbar unter https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_icp.html (zuletzt abgerufen am 27.3.2024).

113 Empfehlung (EU) 2019/1318 vom 30.7.2019 zu internen Compliance-Programmen für die Kontrolle des Handels mit Gütern mit doppeltem Verwendungszweck (Dual-Use-Gütern) nach Maßgabe der Verordnung (EG) Nr. 428/2009 des Rates, ABl. (EU) 2019 Nr. L 205/15; siehe hierzu auch die Darstellung von Jungkind/Bormann, AW-Prax 2020, 103 ff.

114 So bereits die Einschätzung von Jungkind/Bormann, AW-Prax 2020, 103, 106.

Schaffung einheitlicher Standards für innerbetriebliche Compliance im Dual-Use-Bereich bei der Überarbeitung der eigenen Kriterien im Jahre 2018 bereits berücksichtigt hatte.¹¹⁵ Vor diesem Hintergrund liegt aus deutscher Perspektive der spezifische Mehrwert der nachfolgend durch die EU verabschiedeten Leitlinien denn auch vornehmlich darin, dass auf diese Weise die Harmonisierung auf europäischer Ebene befördert wird, was – etwa mit Blick auf die Etablierung von Compliance in europaweit verzweigten Konzernstrukturen – signifikante Erleichterungen mit sich bringen dürfte. Für die Zwecke dieser Darstellung bedeutet dies zugleich, dass eine Erörterung der Kriterien des BAFA als der für in Deutschland ansässige Unternehmen vornehmlich relevanten Exportkontrollbehörde ausreichend ist.

a) Überblick über die relevanten Strukturelemente

- 49 Zuvörderst ist die Gesamtverantwortung für die Exportkontrolle im Unternehmen eindeutig zuzuweisen. Bei Unternehmen, die gelistete Güter exportieren, liegt diese naturgemäß beim Ausfuhrverantwortlichen (siehe insoweit auch → Rn. 45). Dessen Verantwortlichkeit und die nachgelagerten Verantwortlichkeiten für die Exportkontrolle sind zum einen im Organigramm des Unternehmens (sog. „Aufbauorganisation“) transparent zu hinterlegen, zum anderen durch geeignete Arbeitsabläufe, Informations- und Weisungsrechte (sog. „Ablauforganisation“) zu effektuieren.¹¹⁶ Aufbau- und Ablauforganisation sind mit den tatsächlichen Abläufen im Unternehmen mittels eines Prozesshandbuchs zu verknüpfen, welches als das Herzstück einer jeden Exportkontrollorganisation begriffen wird.¹¹⁷ Entscheidend kommt es darauf an, die betriebsinterne Exportkontrolle vor Konflikten mit geschäftspolitischen Interessen zu schützen, indem deren Mitarbeiter schon organisatorisch nicht etwa dem Vertriebs- oder Finanzbereich zugeordnet werden.¹¹⁸ Die Exportkontrollstelle sollte ferner über ein direktes Berichtsrecht an den Vorstand bzw. die Geschäftsführung verfügen und gegenüber anderen Geschäftsbereichen weisungsbefugt sein, um ausfuhrrechtlich bedenkliche Transaktionen jedenfalls bis zum Abschluss einer umfassenden Überprüfung aufhalten zu können (sog. „Stopp-Funktion“).¹¹⁹ Schließlich ist die Exportkontrolle dergestalt in die Geschäftsabläufe zu integrieren, dass ggf. er-

115 BAFA, Firmeninterne Exportkontrolle, 3. Aufl. 2022, 4.

116 BAFA, Firmeninterne Exportkontrolle, 3. Aufl. 2022, 8 f., 10 ff.; *Umnuß*, Corporate Compliance Checklisten, Kap. 4 Rn. 41; *Schwendinger/Bender*, in: Paschke/Graf/Olbrisch, Hamburger Handbuch des Exportrechts, Abschnitt 36 Rn. 75.

117 BAFA, Firmeninterne Exportkontrolle, 3. Aufl. 2022, 10; *Merz/Witte*, in: Ehlers/Wolffgang, Recht der Exportkontrolle, S. 431, 443. Zur Bedeutung einer prozessorientierten Vorgehensweise im Compliance Management ausführlich *Muth*, in: Schulz (Hrsg.), Compliance Management im Unternehmen, 1. Aufl. 2017, Kap. 5 Rn. 2 ff.

118 BAFA, Firmeninterne Exportkontrolle, 3. Aufl. 2022, 8; *Prieß/Thoms*, AW-Prax 2013, 110, 111.

119 *Prieß/Thoms*, AW-Prax 2013, 110, 111; *Merz*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 32 Rn. 103. Zu vergleichbaren Rechten des Compliance Officers vgl. *Schulz/Galster*, in: Bürkle/Hauschka/Schieffer, Der Compliance Officer, § 4 Rn. 37.

forderliche Genehmigungen rechtzeitig vor dem vereinbarten Liefertermin beantragt werden, kann doch die Genehmigungserteilung durch das BAFA je nach Empfänger, Destination und Endverwendung im Einzelfall mehrere Monate in Anspruch nehmen.¹²⁰

Was die in den außenwirtschaftsrechtlich relevanten Bereichen eines Unternehmens eingesetzten Mitarbeiter anbelangt, ist bei deren Auswahl darauf zu achten, dass sie persönlich zuverlässig sind und über die erforderliche Sach- und Fachkenntnis verfügen.¹²¹ Die betreffenden Mitarbeiter sollen nach Empfehlung des BAFA Ausführen und Verbringungen mithilfe von elektronischen Datenverarbeitungssystemen abwickeln, welche im Fall der Beantragung von Sammelgenehmigungen sogar verpflichtend vorgegeben sind.¹²² Entsprechende Softwarelösungen sind insbesondere dann unverzichtbar, wenn Geschäftspartner mit den – fortlaufender Aktualisierung unterworfenen – EU-Embargo- und Terrorismusverordnungen (siehe hierzu bereits → Rn. 7 f.) abzugleichen sind.¹²³ Nur auf diese Weise lässt sich der Forderung des BAFA verlässlich Rechnung tragen, dass dem Exportkontrollpersonal die maßgeblichen Rechtstexte samt Güter- und Personenlisten in jeweils aktueller Fassung zur Verfügung stehen müssen.¹²⁴

Ebenso ist die innerbetriebliche Exportkontrolle darauf auszurichten, dass das involvierte Personal stets über die aktuellen Entwicklungen im Außenwirtschaftsbereich informiert ist. Der Ausfuhrverantwortliche und seine Mitarbeiter müssen sich im Exportbereich ständig fortbilden, weshalb sie in regelmäßigen Abständen externe Seminare oder Inhouse-Schulungen zu besuchen haben.¹²⁵ Überdies sind Mitarbeiter, die im Unternehmen mit dem Exportgeschäft befasst sind, fortlaufend für die beträchtliche Reichweite exportkontrollrechtlicher Vorgaben zu sensibilisieren. So kann sich etwa ein scheinbar unverfänglicher und ohne eigenes wirtschaftliches Interesse erfolgter Hinweis gegenüber einem Dritten auf potenzielle Geschäftspartner im Ausland bei näherer Betrachtung als genehmigungspflichtige Vermittlungstätigkeit darstellen (siehe hierzu bereits → Rn. 25 ff.).

Um die Einhaltung der festgelegten Arbeitsabläufe im täglichen Betriebsablauf sicherzustellen, müssen interne Exportkontrollprogramme nach dem Kriterienkatalog des BAFA prozessbezogene Kontrollmechanismen vorsehen.¹²⁶ Als besonders wirksam werden in diesem Zusammenhang die Etablierung des „Vier-Augen-Prinzips“ bei Freigaben sowie turnusmäßige Sitzungen der mit der Ex-

120 BAFA, Exportkontrolle und das BAFA, 9. Aufl. 2022, 16, siehe dazu auch *Umnuß*, Corporate Compliance Checklisten, Kap. 4 Rn. 41.

121 BAFA, Firmeninterne Exportkontrolle, 3. Aufl. 2022, 9.

122 BAFA, Firmeninterne Exportkontrolle, 3. Aufl. 2022, 9.

123 *Umnuß*, Corporate Compliance Checklisten, Kap. 4 Rn. 43.

124 BAFA, Firmeninterne Exportkontrolle, 3. Aufl. 2022, 10.

125 BAFA, Firmeninterne Exportkontrolle, 3. Aufl. 2022, 15; *Merz*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 32 Rn. 105.

126 BAFA, Firmeninterne Exportkontrolle, 3. Aufl. 2022, 16.

portkontrolle betrauten Mitarbeiter erachtet, in deren Rahmen sich kritische Exportvorhaben ebenso erörtern lassen wie organisatorische Unzulänglichkeiten und Optimierungspotenziale.¹²⁷ Überdies sind stichprobenartige Prüfungen vonnöten, die der Ausfuhrverantwortliche entweder selbst vornehmen oder anderen Unternehmensbereichen bzw. Mitarbeitern überantworten kann. Eine solche Delegation entbindet den Ausfuhrverantwortlichen allerdings nicht davon, sich in regelmäßigen Abständen sowie anlassbezogen (etwa bei bedeutsamen Transaktionen) selbst ein Bild davon zu machen, inwieweit seine Vorgaben umgesetzt werden, um etwaige Missstände unverzüglich korrigieren zu können.¹²⁸ Darüber hinaus haben systembezogene Kontrollen stattzufinden, die das innbetriebliche Exportkontrollsystem ganzheitlich bezüglich Konzeption, Angemessenheit und Wirksamkeit in den Blick nehmen und nach den Vorgaben des BAFA idealerweise einmal jährlich, mindestens aber alle drei Jahre vorzunehmen sind.¹²⁹

- 53 Schließlich ist der physische und technische Schutz gelisteter Güter gegen unerlaubte Wegnahme durch unternehmensangehörige Personen oder Dritte unerlässlich und lässt sich etwa durch Zugangskontrollen oder alternative Berechtigungskonzepte implementieren.¹³⁰ Ebenso ist die Führung und Aufbewahrung ausfuhrrechtlich relevanter Unterlagen unverzichtbares Element eines funktionierenden Exportkontrollsystems. Das gilt selbstredend im Hinblick auf gesetzlich angeordnete Aufbewahrungspflichten.¹³¹ Aber auch jenseits dieser Vorgaben bedarf es einer lückenlosen Nachweisführung und -aufbewahrung. Das betrifft beispielsweise auch die Fortbildungsmaßnahmen der Mitarbeiter, die im Rahmen behördlicher Überprüfungen möglichst ohne großen Rechercheaufwand, zweifelsfrei und lückenlos belegbar sein sollten.¹³²

b) Umsetzung im Einzelfall

- 54 Die vorstehend dargestellten Strukturelemente sind für die Errichtung eines jeden internen Exportkontrollsystems belangvoll. Gleichwohl gibt es kein Muster, das unesehen auf jedes Unternehmen übertragen werden könnte.¹³³ Vielmehr muss eine effektive Exportkontrolle unternehmensspezifisch ausgerichtet sein. Insoweit kommt es ausschlaggebend auf Art, Größe, Geschäftsfelder, geografische Präsenz sowie organisatorische Komplexität des betreffenden Unternehmens an.¹³⁴ Handelt ein Unternehmen mit ausschließlich zivil nutzbaren Gütern, entfallen beispielsweise Genehmigungserfordernisse nach den Dual-Use-Be-

127 BAFA, Firmeninterne Exportkontrolle, 3. Aufl. 2022, 16; *Merz/Witte*, in: Ehlers/Wolffgang, Recht der Exportkontrolle, S. 431, 441.

128 *Merz*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 32 Rn. 104.

129 BAFA, Firmeninterne Exportkontrolle, 3. Aufl. 2022, 16 f.

130 BAFA, Firmeninterne Exportkontrolle, 3. Aufl. 2022, 15.

131 Vgl. u. a. Art. 27 Abs. 3 u. 4 Dual-Use-Verordnung; § 22 Abs. 3 AWW.

132 *Merz/Witte*, in: Ehlers/Wolffgang, Recht der Exportkontrolle, S. 431, 440.

133 BAFA, Firmeninterne Exportkontrolle, 3. Aufl. 2022, 4.

134 BAFA, Firmeninterne Exportkontrolle, 3. Aufl. 2022, 4; *Schwendinger/Bender*, in: Paschke/Graf/Olbrich, Hamburger Handbuch des Exportrechts, Abschnitt 36 Rn. 68.

stimmungen, womit auf die Ernennung eines Ausfuhrverantwortlichen verzichtet werden kann.

Ausgangspunkt bei der Etablierung eines Exportkontrollsystems muss stets die Identifizierung aller ausfuhrrechtlichen Bestimmungen sein, welche das jeweilige Unternehmen denkbarerweise betreffen können.¹³⁵ Zwar mag die Anwendbarkeit der Dual-Use-Bestimmungen oftmals auf den ersten Blick fernliegend erscheinen. Da für die Klassifizierung als Dual-Use-Gut allerdings bereits ausreichend ist, dass Güter – etwa Pumpen, Werkzeugmaschinen oder Ventile – im Zusammenhang mit der Entwicklung, Herstellung oder Verwendung von Rüstungsgütern eingesetzt werden können, sind im Ergebnis vielzählige Industrieprodukte betroffen. Es ist Exporteuren daher dringlich anzuraten, die „Aufgriffsschwelle“ eher niedrig anzusetzen und Zurückhaltung bei der Einschätzung zu üben, dass sich bestimmte Produkte keinesfalls (auch) für militärische Zwecke verwenden lassen.¹³⁶ **55**

Sind die einschlägigen außenwirtschaftsrechtlichen Bestimmungen identifiziert, ist im nächsten Schritt das unternehmensspezifische Risiko ihrer Verletzung zu bewerten, wobei jeweils von der Eintrittswahrscheinlichkeit eines Verstoßes sowie dessen denkbaren Schadensfolgen auszugehen ist.¹³⁷ Sodann ist der Exportkontrollprozess spezifisch auf die erkannten Risiken und risikobehafteten Geschäftsbereiche auszurichten.¹³⁸ Wird die Risikoexposition für Rechtsverstöße im Exportgeschäft – etwa im Hinblick auf bestimmte Rechtsordnungen – als nicht vertretbar eingestuft, kann dies auch zur Folge haben, dass sich Unternehmen aus bestimmten Geschäftsfeldern zurückziehen. Schließlich bedarf die Risikosituation fortlaufender Überwachung, da sie sich im Laufe der Zeit wandeln kann.¹³⁹ Ergibt sich dabei eine geänderte Risikoeinschätzung, muss das innerbetriebliche Exportkontrollprogramm ggf. angepasst werden, weshalb es keinesfalls als statisches Gebilde begriffen werden darf, sondern vielmehr in einem kontinuierlichen Prozess fortzuentwickeln ist. **56**

Zu den bei der Ausgestaltung der innerbetrieblichen Exportkontrolle maßgeblichen Unternehmensspezifika zählen insbesondere auch die jeweiligen Ausfuhrmengen. Fallen diese eher gering aus, kann es genügen, einige wenige Mitarbeiter im Unternehmen *zusätzlich* mit Aufgaben im Bereich der Exportkontrolle zu betrauen. Eine solche Lösung wird dagegen bei größeren Produktions- und Ausfuhrvolumina regelmäßig nicht tragfähig sein. Hier wird es vielmehr erforderlich sein, einer größeren Anzahl von Mitarbeitern ausschließlich Aufgaben der Exportkontrolle zuzuweisen.¹⁴⁰ Wurde ein Ausfuhrverantwortlicher im Unternehmen benannt, wird dieser zumeist schon aufgrund seiner vielfältigen weite- **57**

135 Gündel/Feiler, CB 2013, 236, 238.

136 BAFA, Praxis der Exportkontrolle, 5. Aufl. 2023, 19.

137 Gündel/Feiler, CB 2013, 236, 238.

138 BAFA, Firmeninterne Exportkontrolle, 3. Aufl. 2022, 7; Gündel/Feiler, CB 2013, 236, 239.

139 BAFA, Firmeninterne Exportkontrolle, 3. Aufl. 2022, 7.

140 Merz/Witte, in: Ehlers/Wolffgang, Recht der Exportkontrolle, S. 431, 440.

ren Aufgaben bei der Unternehmensführung die operative Wahrnehmung der Exportkontrolle aus Kapazitätsgründen nicht alleine bewältigen können.¹⁴¹ Um die Exportkontrolle im operativen Geschäft zu effektuieren, bedarf es dann einer nachgelagerten Unternehmensorganisation mit klar festgelegten und unmissverständlich kommunizierten Zuständigkeiten und Delegierungen. Typischerweise wird die Exportkontrolle auf der Ebene unterhalb der Geschäftsführung bei einem Exportkontrollbeauftragten – häufig „Export Control Compliance Officer“ oder „Export Control Manager“ – verortet, welcher in Abstimmung mit dem Ausfuhrverantwortlichen die Exportkontrolle im Tagesgeschäft verantwortet, kontrolliert und weiterentwickelt.¹⁴²

- 58** Auch die vom BAFA herausgearbeiteten sonstigen Standardelemente der innerbetrieblichen Exportkontrolle sind jeweils unternehmensspezifisch zu adaptieren. Nicht zu übersehen ist, dass es dabei des Einsatzes nicht unerheblicher personeller und technischer Mittel bedarf, um eine exportkontrollrechtliche Organisationsstruktur zu errichten, die sich in der Praxis zu bewähren vermag. Beispielhaft sei hier die Abbildung von Embargo- und Sanktionsmaßnahmen in den betriebsinternen Exportprozessen genannt, um bei kritischen Bestimmungsländern und Empfängern rechtzeitig eine vertiefte Prüfung und ggf. die Anordnung eines Ausfuhrstopps sicherzustellen. Ohne eine ausgereifte „EDV-Landschaft“ lässt sich diesem Erfordernis jedenfalls bei größeren Ausfuhrvolumina kaum verlässlich Rechnung tragen.

VI. Zusammenfassung und Ausblick

- 59** Das Außenwirtschaftsrecht ist eine vielschichtige, komplexe und in ständigem Fluss befindliche Materie. Erfasst sind vielfältige Geschäftsaktivitäten, an denen ganz unterschiedliche Akteure mitwirken. Belastbare Kenntnisse der einschlägigen Rechtsnormen auf deutscher, europäischer und drittstaatlicher Ebene sind ebenso unverzichtbar wie ein profundes technisches Verständnis der für die Ausfuhr vorgesehenen Güter. Weitreichende exportkontrollrechtliche Verbote und Genehmigungsvorbehalte knüpfen – kumulativ oder alternativ – an exportkontrollierte Güter, kritische Bestimmungsländer, inkriminierte Verwender und sensitive Verwendungen an. Dadurch schränken sie die – dem Grundsatz nach unbegrenzte – Freiheit im Außenwirtschaftsverkehr nicht unerheblich ein. Bei Verstößen drohen den Unternehmen selbst sowie den für die Verstöße verantwortlichen Personen empfindliche Sanktionen, die bis zu mehrjährigen Freiheitsstrafen reichen können. Für exportierende Unternehmen können Verstöße gegen außenwirtschaftliche Regelungen zudem einen generellen Ausschluss vom kontrollierten Außenhandel zur Folge haben.¹⁴³

141 Merz, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 32 Rn. 113.

142 Sachs/Krebs, CCZ 2013, 60, 66; Merz, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 32 Rn. 113.

143 Roeder/Schultz/Havlik/Conte, CCZ 2023, 377, 341.

Vor diesem Hintergrund wird ein effektives innerbetriebliches Exportkontrollsystem auch in Zukunft von Vorteil sein. Zwar besteht grundsätzlich keine Rechtspflicht zu dessen Errichtung. Gleichwohl erlaubt vielfach überhaupt erst die Etablierung durchgängiger und belastbarer Exportkontrollprozesse den Zugang zum genehmigungspflichtigen Außenhandel. Überdies hängt hiervon die Inanspruchnahme vielzähliger Verfahrensprivilegierungen ab, welche für eine effektive Teilnahme am Außenwirtschaftsverkehr unerlässlich sein können. So haben Ausführer, die die Erteilung einer Sammel- bzw. Globalausfuhrgenehmigung beantragen wollen, nach der neugefassten Dual-Use-Verordnung grundsätzlich über ein internes Programm für rechtskonformes Verhalten (ICP) zu verfügen (hierzu bereits → Rn. 36 und 43). Das BAFA gibt den Unternehmen insoweit die Strukturelemente für ein effektives Exportkontrollprogramm vor. Deren Umsetzung in der Unternehmenswirklichkeit obliegt gleichwohl den Wirtschaftsbeteiligten selbst. **60**

26. Kapitel

Compliance in M&A-Transaktionen

I. Einleitung

Eine Vielzahl rechtlicher Regeln kann sich im Fall ihrer Nichtbeachtung nachteilig auf M&A-Transaktionen auswirken. Insofern ist zu differenzieren: Einerseits 1
gibt es Regeln, die auf den M&A-Prozess selbst Anwendung finden (prozessuale M&A-Compliance). Dabei handelt es sich beispielsweise um das kartellrechtliche Vollzugsverbot oder das Erfordernis, vor der Offenlegung vertraulicher Informationen in Bezug auf die Zielgesellschaft mit dem Erwerber eine Vertraulichkeitserklärung abzuschließen.

Neben der Bewältigung prozessualer Compliance-Themen stellt sich die Frage, 2
wie mit Risiken aufgrund der Nichteinhaltung von rechtlichen Regeln jeglicher Art durch die Zielgesellschaft umzugehen ist (materielle M&A-Compliance). Im Kern stehen hier die Fragen, ob und wenn ja, inwieweit eine Pflicht besteht, im Rahmen der Due Diligence nach derartigen Risiken zu suchen und welche Möglichkeiten es gibt, mit etwaigen materiellen Compliance-Risiken in einer M&A-Transaktion umzugehen. Die materielle M&A-Compliance hat bislang deutlich weniger Beachtung gefunden, als die prozessuale M&A-Compliance.

Freilich sind prozessuale und materielle M&A-Compliance nicht immer scharf 3
voneinander abzugrenzen: Streng genommen ist die Frage nach der Pflicht zur Durchführung einer Compliance-Due Diligence (ebenso wie die Frage nach der Pflicht zur Due Diligence ganz allgemein) zumindest auch eine prozessuale Frage. Inhaltlich geht es aber um potenzielle materielle Compliance-Themen der Zielgesellschaft, weshalb die Frage nach der Pflicht zur Durchführung einer Compliance-Due Diligence hier als eine solche der materiellen M&A-Compliance behandelt wird.

Kaum der Erwähnung bedarf wohl die erhebliche praktische Relevanz der 4
M&A-Compliance – und zwar sowohl der prozessualen wie der materiellen. M&A-Transaktionen sind komplex und häufig großvolumig, was betragsmäßig zu einem hohen Schadenspotenzial führt.¹ Man stelle sich nur vor, der Geschäftsbereich der Siemens AG, in dem sich der der Siemens/Neubürger-Entscheidung² zugrunde liegende Sachverhalt abspielte, wäre (vor Bekanntwerden der korruptiven Handlungen) Gegenstand einer M&A-Transaktion gewesen. Der Erwerber hätte sich Risiken in Höhe von ca. 2,5 Milliarden EUR eingekauft.³ Auch wird die tatsächliche Entdeckungswahrscheinlichkeit von Compliance-Verstößen durch M&A-Transaktionen erheblich erhöht, z. B. aufgrund von

1 Liese, BB 2010, 27.

2 LG München I, 10.12.2013, 5 HK O 1387/10, BB 2014, 850.

3 Handelsblatt v. 22.4.2014, [https://archiv.handelsblatt.com/document/HBON__HB%2097900/hitlist/0?all=\(zuletzt%20abgerufen%20am%202.4.2024\)](https://archiv.handelsblatt.com/document/HBON__HB%2097900/hitlist/0?all=(zuletzt%20abgerufen%20am%202.4.2024)).

Zufallsfunden in Unterlagen, die im Zusammenhang mit der Prüfung des Zusammenschlussvorhabens von Kartellbehörden angefordert wurden. Aber nicht nur die materielle M&A-Compliance ist haftungsträchtig: Beispielsweise können unterlassene oder verspätete Ad-hoc-Mitteilungen oder Verstöße gegen das kartellrechtliche Vollzugsverbot erhebliche Bußgelder nach sich ziehen. Im Fall unterlassener oder verspäteter Ad-hoc-Mitteilungen drohen zudem (erhebliche) Schadensersatzforderungen. Insiderhandel ist für die betroffenen Individuen sogar strafbar und es kann auch im Zusammenhang mit der Durchführung einer M&A-Transaktion selbst zu korruptiven Handlungen kommen: So hatte etwa jedes dritte Verfahren nach dem US-amerikanischen Foreign Corrupt Practices Act (FCPA) im Kern einen M&A-Sachverhalt.⁴

II. Prozessuale M&A-Compliance – Einhaltung von Rechtsvorschriften im M&A-Verfahren

1. Strukturierung der Transaktion

a) Auktions- und Einzelbieterverfahren

- 5 In einem ersten Schritt wird sich der Veräußerer Gedanken zur Transaktionsstruktur machen müssen, sowohl hinsichtlich des Kaufgegenstands als auch des Prozesses. Prozessual spielt vor allem die Frage eine Rolle, ob der Verkauf als Auktionsverfahren mit mehreren Bietern aufgesetzt oder exklusiv mit einem einzelnen Bieter verhandelt werden soll. Empirische Untersuchungen deuten darauf hin, dass der Kaufpreis in einem Auktionsverfahren maximiert werden kann. Im Einzelfall mag es dessen ungeachtet gewichtige Gründe geben, mit nur einem Bieter exklusiv zu verhandeln. Die Entscheidung gegen ein Bieterverfahren sollte aus Sicht der handelnden Organe aber sorgfältig abgewogen und dokumentiert werden, um sich gegen den etwaigen Vorwurf wehren zu können, die Zielgesellschaft sei zu günstig (oder zu unnötig nachteiligen Konditionen im Übrigen) veräußert worden.⁵ Eine Pflicht zur Veräußerung zu einem möglichst hohen Preis kann jedoch nicht angenommen werden. So findet die mitunter angeführte Revlon-Doktrin⁶ aus dem angelsächsischen Recht, wonach die Direktoren einer Zielgesellschaft – deren Verkauf feststeht – zur Erzielung des höchsten Kaufpreises verpflichtet sind, hier keine Grundlage.⁷ Die Unternehmensleitung ist vielmehr den Unternehmens- und jedenfalls nicht allein den Eigentümerinteressen verpflichtet.

4 Schwarz, BB 2012, 136, 138.

5 Vgl. Liese/Theusinger, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 27 Rn. 8. Zur haftungsprivilegierenden Wirkung der Business Judgement Rule sowie deren Voraussetzungen, siehe → Rn. 84.

6 Revlon, Inc. v. MacAndrews & Forbes Holdings, Inc., 506 A.2d 173 (Del. 1986).

7 Fleischer, Geschäftsleiterpflichten bei der Veräußerung von Unternehmensbeteiligungen, in: Grunewald/Koch/Tielmann (Hrsg.), FS Vetter, S. 144 ff.

b) Transaktionsgegenstand

Als Transaktionsgegenstand kommen einerseits die Gesellschaftsanteile der Zielgesellschaft („Share Deal“) und andererseits die Vermögensgegenstände der Zielgesellschaft („Asset Deal“) in Betracht. Die Wahl hat steuerliche Auswirkungen und kann weiterhin dazu dienen, den Übergang von materiellen Risiken der Zielgesellschaft zu steuern (siehe dazu → Rn. 98). Allerdings hat die Wahl der Strukturierung der Transaktion als Asset oder Share Deal weitere compliance-relevante Implikationen, die ebenfalls bedacht werden müssen. 6

Z.B. kann es regelmäßig durch die Übertragung von Vermögensgegenständen im Rahmen eines Asset Deals zu einer Verarbeitung von personenbezogenen Daten kommen (Art. 4 Nr. 2 DSGVO). Bereits die Erhebung solcher Daten unterliegt einer Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO). Die Verarbeitung darf nicht über diesen ursprünglich festgelegten Zweck (bei Kundendaten das Geschäftsverhältnis) hinausgehen. Gerechtfertigt kann eine Verarbeitung jedoch dann sein, wenn (i) die betroffene Person in die Verarbeitung einwilligt oder (ii) ein überwiegendes berechtigtes Interesse an der Verarbeitung besteht (Art. 6 Abs. 1 lit. a, f DSGVO). Eine Einwilligung ist bei der möglichen hohen Anzahl der betroffenen Personen, der gewünschten Geheimhaltung der Transaktion und dem ursprünglich verfolgten Zweck kaum praktikabel. 7

Sind hingegen Gesellschaftsanteile Gegenstand der M&A-Transaktion, werden durch die Transaktion selbst keine Daten an einen Dritten übermittelt, da die Identität desjenigen, der die Daten gespeichert hat und sie verarbeitet – nämlich der Zielgesellschaft –, nicht berührt wird. Die (Kunden-)Daten verbleiben beim ursprünglichen Verantwortlichen im Sinne des Art. 4 Nr. 7 DSGVO.⁸ 8

Im Fall einer unbefugten Verarbeitung von personenbezogenen Daten kann durch die Aufsichtsbehörde eine Geldbuße von bis zu 20 Mio. EUR oder 4 % des gesamten weltweit erzielten Jahresumsatzes verhängt werden (Art. 83 Abs. 5 lit. a DSGVO). Zudem sind Reputationsschäden zu erwarten, weshalb hier vorsichtig vorgegangen werden sollte.⁹ 9

2. Offenlegung von Informationen**a) Offenlegungs- und Aufklärungspflichten des Veräußerers**

Der Veräußerer haftet für unterlassene oder unvollständige Auskünfte aus der Verletzung eines vorvertraglichen Schuldverhältnisses, soweit ihn besondere Offenlegungs-, Aufklärungs- oder Informationspflichten treffen (§§ 280 Abs. 1, 311 Abs. 2 Nr. 1, 241 Abs. 2 BGB). Dabei ist zwischen der Offenlegung einer- 10

8 Plath/Struck/Hazeborg, Verkauf von Kundendaten im Asset Deal, CR 2020, 9, 10 (hier auch ausführlich zu Rechtfertigungsoptionen beim Asset Deal).

9 Siehe zum Thema Datenschutz ausführlicher unten → Rn. 22 ff. sowie ausführlich → Becker/Böhlke/Fladung, Kap. 12.

seits und der Aufklärung andererseits zu unterscheiden.¹⁰ Nach ganz überwiegender Auffassung ist unter einer Offenlegung nur die Bereitstellung der Informationen zu verstehen. Eine Aufklärung beinhaltet auch aktive Hinweise auf bestimmte Sachverhalte, um die Kenntnisnahme durch die andere Partei sicherzustellen.¹¹ Grundsätzlich hat der Veräußerer nur eine Pflicht zur Offenlegung wesentlicher Umstände.¹² Darüber hinaus trifft den Veräußerer in zwei Fällen eine Pflicht zur Aufklärung: Erstens, wenn wegen der besonderen Umstände des Einzelfalls davon auszugehen ist, dass der Erwerber die Verhältnisse nicht durchschaut.¹³ Zweitens hat der Veräußerer im Rahmen der Verhandlungen ungefragt über solche Umstände aufzuklären, die den Vertragszweck des Erwerbers vereiteln könnten und daher für seinen Entschluss von wesentlicher Bedeutung sind.¹⁴ Dies gilt jedoch nur, sofern der Erwerber die Mitteilung nach der Verkehrsauffassung erwarten darf.¹⁵

- 11** Indem der Veräußerer in einem (virtuellen) Datenraum Unterlagen für die Due Diligence zur Verfügung stellt und damit dem Erwerber die Möglichkeit gibt, sich Kenntnis vom offenbarungspflichtigen Umstand zu verschaffen, kommt er seinen Offenlegungspflichten nach, nicht aber automatisch seinen hiervon zu unterscheidenden Aufklärungspflichten.¹⁶ Hierzu kann es weiterer Informationen und Hinweise bedürfen, wobei es nach einer aktuellen Entscheidung des BGH maßgeblich darauf ankommt, ob der Veräußerer die berechnete Erwartung haben darf, dass der Erwerber (allein) durch Einsichtnahme in den (virtuellen) Datenraum Kenntnis von dem offenbarungspflichtigen Umstand erlangen wird.¹⁷ Dabei ist je nach Einzelfall abzuwägen, ob eine derartige Erwartung berechtigt ist.¹⁸ Insbesondere ist zu berücksichtigen, ob und in welchem Umfang eine Due Diligence auf Erwerberseite durchgeführt wird, wie der Datenraum und der Zugriff auf diesen strukturiert und organisiert sind, welche Vereinbarun-

10 Göthel, in: Göthel, Grenzüberschreitende M&A-Transaktionen, § 2 Rn. 83.

11 Göthel, in: Göthel, Grenzüberschreitende M&A-Transaktionen, § 2 Rn. 83, 85; Möller, NZG 2012, 841, 846, auch mit Nachweisen zur a. A.

12 Due Diligence-Anforderungslisten des Erwerbers dürften allenfalls ein Indiz dafür sein, was wesentlich ist, da der Erwerber die Zielgesellschaft regelmäßig noch nicht kennt und er diese Frage mithin im Zweifelsfall nur abstrakt, nicht aber unternehmensspezifisch beurteilen kann; anders wohl Liese/Theusinger, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 27 Rn. 34.

13 BGH, Urt. v. 14.6.2007, III ZR 269/06, NJW-RR 2007, 1503, 1504; Göthel, in: Göthel, Grenzüberschreitende M&A-Transaktionen, § 2 Rn. 83.

14 BGH, Urt. v. 28.11.2001, VIII ZR 37/01, NZG 2002, 298, 300; Tamcke/Dembinski, GWR 2023, 338, 339.

15 BGH, Urt. v. 28.11.2001, VIII ZR 37/01, NZG 2002, 298, 300; Göthel, in: Göthel, Grenzüberschreitende M&A-Transaktionen, § 2 Rn. 83.

16 BGH, Urt. v. 15.9.2023, V ZR 77/22, NJW 2023, 3423, 3426; Göthel, in: Göthel, Grenzüberschreitende M&A-Transaktionen, § 2 Rn. 90.

17 BGH, Urt. v. 15.9.2023, V ZR 77/22, NJW 2023, 3423, 3427; Keller/Schümmer, NJW-Spezial 2023, 719.

18 BGH, Urt. v. 15.9.2023, V ZR 77/22, NJW 2023, 3423, 3427; Mallmann/Henke, NJW 2023, 3398.

gen zwischen den Parteien getroffen wurden und um welche Art der Information es sich handelt.¹⁹ In einem anderen vom BGH entschiedenen Fall²⁰ war die allgemein gehaltene Information seitens des Veräußerers ausreichend, dass die Zielgesellschaft in der geführten Form ein Verlustgeschäft sei, da der Erwerber sonst alle erfragten Informationen erhalten hatte und sachkundig war. Ungefragt bedurfte es darüber hinaus keiner Darstellung der Verluste der einzelnen Geschäftsjahre. Denn von einem hinreichend sach- und branchenkundigen Erwerber wäre zu erwarten gewesen, dass er auf den Hinweis hin, es handele sich um ein Verlustgeschäft, Bilanzen, Gewinn- und Verlustrechnungen, betriebswirtschaftliche Auswertungen oder ähnliche Unterlagen anfordert, wenn dies für ihn von Interesse gewesen wäre.²¹

b) Rechtliche Grenzen der Offenlegung von Informationen

Neben kartellrechtlichen Schranken für die Informationsweitergabe in M&A-Transaktionen (dazu → Rn. 32 ff.) können sich Grenzen weiterhin aus dem Gesellschaftsrecht (unter → Rn. 13 ff.), aus von der Zielgesellschaft geschlossenen Verträgen (unter → Rn. 19 ff.) und datenschutzrechtlichen Bestimmungen (unter → Rn. 22 ff.) ergeben. **12**

aa) Gesellschaftsrechtliche Zulässigkeit der Offenlegung von Informationen gegenüber Dritten

Im Rahmen der Verhandlung einer M&A-Transaktion werden in vielfältiger Weise vertrauliche Informationen in Bezug auf die Zielgesellschaft offengelegt. In diesem Zusammenhang stellt sich die Frage, unter welchen Voraussetzungen dies den Organen der Zielgesellschaft mit Blick auf ihre eigenen dienstvertraglichen und gesetzlichen Verschwiegenheitspflichten (§§ 93 Abs. 1 Satz 3, 404 AktG, vgl. § 85 GmbHG) gestattet ist. Die Vertraulichkeitspflichten der Organe gelten nicht absolut; vielmehr dürfen vertrauliche Informationen dann offengelegt werden, wenn das Organ nach einer Abwägung zu dem Ergebnis kommen durfte, dass die Offenlegung im Interesse der Zielgesellschaft ist.²² Dabei kann die Veräußerung aus Sicht der Zielgesellschaft insbesondere deshalb von Vorteil sein, weil sie sich als Bestandteil der Gruppe des Erwerbers neue Märkte, Finanzierungsquellen oder Know-how erschließt.²³ Allerdings sind bei der Offenlegung bestimmte Voraussetzungen einzuhalten. **13**

19 BGH, Urt. v. 15.9.2023, V ZR 77/22, NJW 2023, 3423, 3427; Keller/Schümmer, NJW-Spezial 2023, 719.

20 BGH, Urt. v. 28.11.2001, VIII ZR 37/01, NZG 2002, 298, 300.

21 BGH, Urt. v. 28.11.2001, VIII ZR 37/01, NZG 2002, 298, 300.

22 Schiffer/Bruß, BB 2012, 847, 849; K. J. Müller, NJW 2000, 3452, 3453; vgl. aber die Mindermeinung von Lutter, ZIP 1997, 613, 617, nach dem der Vorstand einer Aktiengesellschaft eine umfassende Due Diligence nur dann zulassen dürfe, wenn ein anders nicht erreichbares überragend wichtiges unternehmerisches Interesse der Gesellschaft dies gebiete.

23 K. J. Müller, NJW 2000, 3452, 3453.

- 14 Die Organe der Zielgesellschaft sind zunächst gehalten, mit dem Erwerber eine Vertraulichkeitsvereinbarung abzuschließen.²⁴ Zwar wird durch die Aufnahme von Verhandlungen zwischen Veräußerer und Erwerber regelmäßig ein vorvertragliches Schuldverhältnis begründet (§ 311 Abs. 2 Nr. 1 BGB), aus dem die Verpflichtung des Erwerbers folgt, ihm zur Verfügung gestellte Informationen vertraulich zu behandeln.²⁵ Dessen ungeachtet sollten diese Pflichten in Form einer ausdrücklichen schriftlichen Vertraulichkeitsvereinbarung konkretisiert werden, um Streit über Beginn und Inhalt der Geheimhaltungsverpflichtung zu vermeiden (Beweis- und Dokumentationsfunktion) und um ggf. Regelungen zu treffen, die über die gesetzlichen Pflichten des Informationsempfängers hinausgehen.²⁶ Trotz dieser grundsätzlichen Pflicht zum Abschluss einer Vertraulichkeitsvereinbarung sollte man sich der Tatsache bewusst sein, dass eine solche häufig nur wenig Schutz vor einer unerlaubten Offenlegung vertraulicher Informationen bieten kann. Denn es wird in der Praxis regelmäßig zu Beweisschwierigkeiten hinsichtlich (i) der Person desjenigen, der die vertrauliche Information konkret offengelegt hat, und (ii) des durch die Offenlegung eingetretenen Schadens kommen (soweit keine pauschalierte Vertragsstrafe vereinbart wird).
- 15 Neben dem Abschluss einer Vertraulichkeitsvereinbarung mit dem Erwerber sowie eines Gesellschafterbeschlusses ist die Offenlegung von Informationen nur zulässig, soweit der Erwerber ein ernsthaftes Interesse an einem möglichen Erwerb der Zielgesellschaft hat. Dies wird typischerweise durch den Abschluss einer Absichtserklärung (Letter of Intent, Term Sheet, Memorandum of Understanding o. Ä.) dokumentiert.²⁷
- 16 Weiterhin ist es im Fall einer GmbH den Geschäftsführern der Zielgesellschaft anzuraten, einen Beschluss der Gesellschafterversammlung hinsichtlich der Informationsweitergabe einzuholen, da jedenfalls eine umfassende Due Diligence angesichts ihrer Bedeutung für die Gesellschaft keine Angelegenheit der laufenden Geschäftsführung darstellt.²⁸ Im Fall einer Aktiengesellschaft bedarf es eines Beschlusses des Gesamtvorstands der Zielgesellschaft, da die Entschei-

24 Göthel, in: Göthel, Grenzüberschreitende M&A-Transaktionen, § 2 Rn. 119 f.; K. J. Müller, NJW 2000, 3452, 3455. Für Muster siehe nur Seibt, in: Seibt, Beck'sches Formularbuch Mergers & Acquisitions, B.I. 1 und 2.

25 Seibt, in: Seibt, Beck'sches Formularbuch Mergers & Acquisitions, Anm. 1 zu B.I.1, 36; von Werder/Kost, BB 2010, 2903, 2905.

26 Linke/Fröhlich, GWR 2014, 449; Seibt, in: Seibt, Beck'sches Formularbuch Mergers & Acquisitions, Anm. 1 zu B.I.1, 36.

27 K. J. Müller, NJW 2000, 3452, 3455.

28 Ganz überwiegende Auffassung, siehe nur Fleischer, in: MünchKomm-GmbHG, § 43 Rn. 260 m. w. N. Nach der wenig überzeugenden, aber wohl überwiegenden Meinung ist dieser Beschluss einstimmig zu fassen, LG Köln, Urt. v. 26.3.2008, 90 O 11/08, GmbHR 2009, 261; Lutter, ZIP 1997, 613, 615; dagegen Göthel, in: Göthel Grenzüberschreitende M&A-Transaktionen, § 2 Rn. 119; Liese/Theusinger, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 27 Rn. 36; Stephan/Tieves, in: MünchKomm-GmbHG, § 37 Rn. 147 jeweils m. w. N.

dung über die Zulassung der Due Diligence aufgrund ihrer Bedeutung regelmäßig die Ressortkompetenz eines einzelnen Vorstandsmitglieds übersteigt.²⁹

Ist der Kaufinteressent ein (potenzieller) Wettbewerber des Zielunternehmens, bedarf die Offenlegung der wettbewerbsrechtlich sensiblen Informationen besonderer Vorkehrungen (siehe dazu → Rn. 34 ff.). Welche Informationen wettbewerbsrechtlich sensibel sind, sollte in der Vertraulichkeitsvereinbarung klargestellt werden (z. B. als Unterdefinition von vertraulichen Informationen).³⁰ Als wettbewerbsrelevante Informationen sind vor allem einzustufen: Angaben zu Preisen, Rabatten, Preisgestaltung, Informationen über aktuelle oder erwartete Angebote, kundenspezifische Informationen, Kosten für strategische Waren oder Kosten, die von strategischen Subunternehmen verlangt werden, sowie die Kapazitätsauslastung.³¹ **17**

Im Fall von Transaktionen, an denen eine börsennotierte Gesellschaft beteiligt ist, kommt dem Abschluss einer Vertraulichkeitsvereinbarung Bedeutung weiterhin deshalb zu, da ab Vorliegen einer Insidertatsache grundsätzlich eine Ad-hoc-Mitteilung zu erfolgen hat (Art. 17 Abs. 1 Marktmissbrauchsverordnung)³² und die Möglichkeit des Emittenten, sich von dieser Pflicht selbst zu befreien (Art. 17 Abs. 4 Marktmissbrauchsverordnung), u. a. voraussetzt, dass die Vertraulichkeit der Insiderinformation gewährleistet werden kann.³³ Es bedarf jedoch einer genauen Abwägung, ob eine Vertraulichkeitsvereinbarung notwendig ist, da auch diese selbst einen Anlass zur Prüfung der Ad-hoc-Publizitätspflicht geben kann.³⁴ **18**

bb) Vertraulichkeitsbestimmungen in Verträgen mit Dritten

In Verträgen mit Dritten wird die Zielgesellschaft häufig Bestimmungen über die Vertraulichkeit des betroffenen Vertrags aufgenommen haben, über die sie nicht einseitig disponieren kann.³⁵ Ein solches mit einem Dritten vereinbartes Verbot der Offenlegung steht in diametralem Widerspruch zum Interesse des Erwerbers, z. B. wichtige Verträge mit Kunden und Lieferanten zu prüfen. Wird dem Erwerber der Zugang zu aus seiner Sicht wesentlichen Informationen verwehrt, so kann dies die Organe des Erwerbers unter Umständen dazu zwingen, von der Transaktion Abstand zu nehmen (siehe → Rn. 49). **19**

29 K. J. Müller, NJW 2000, 3452, 3455; Meincke, WM 1998, 749, 751; Schroeder, DB 1997, 2161, 2163.

30 Linke/Fröhlich, GWR 2014, 449, 451.

31 Linke/Fröhlich, GWR 2014, 449, 451.

32 Zur Frage, wann eine Insiderinformation vorliegt, siehe → Rn. 41.

33 Zur Selbstbefreiung nach Art. 17 Abs. 4 Marktmissbrauchsverordnung siehe → Rn. 42.

34 Hasselbach/Stepper, BB 2020, 203, 205 mit Hinweis darauf, dass die BaFin in Einzelfällen dazu neigt, schon in einem sehr frühen Stadium einer Transaktion die Publizitätspflicht anzunehmen.

35 Auch ohne eine ausdrückliche Vertraulichkeitsbestimmung kann eine entsprechende Nebenpflicht bestehen, Liese/Theusinger, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 27 Rn. 47; Werder/Kost, BB 2010, 2903, 2905.

- 20** Vertraulich ist dabei über den Inhalt des Vertrags mit dem Dritten hinaus häufig sogar die Existenz des Vertrags als solchem. Neben einer Offenlegung entgegenstehender Interessen des Dritten wird eine ausdrückliche Zustimmung zur Offenlegung seitens des Dritten häufig schon daran scheitern, dass die Planung einer (wie auch immer gearteten) Transaktion – gerade gegenüber Vertragspartnern wie Kunden oder Lieferanten – zunächst geheim gehalten werden soll.³⁶ Selbst im unwahrscheinlichen Fall, dass die geplante Transaktion gegenüber Dritten offengelegt werden kann, könnten sich seitens des Dritten Fragen zu den Hintergründen der Offenlegung und dem Erwerber ergeben, deren Beantwortung nicht erwünscht ist.
- 21** In einer idealen Welt würde man vor diesem Hintergrund bereits bei Vertragsabschluss Vertraulichkeitsbestimmungen dahingehend einschränken, dass der Vertrag bei einem berechtigten Interesse des Veräußerers gegenüber Dritten offengelegt werden darf (ggf. wenn und soweit der Dritte selbst zur Vertraulichkeit verpflichtet ist). Häufig ist es dafür aber zu spät, wenn die Due Diligence ansteht. Auch kann es sein, dass sich der Vertragspartner auf eine derartige Regelung nicht einlässt. Um im Fall einer Offenlegung entgegenstehenden Vertraulichkeitsbestimmungen nicht gegenüber dem Dritten vertragsbrüchig zu werden und Vertragsstrafen, Schadensersatzforderungen und/oder den Abbruch der Geschäftsbeziehung als mögliche Konsequenzen in Kauf nehmen zu müssen, kommt lediglich noch die Schwärzung des Vertrags (z. B. zur Anonymisierung) oder die Erstellung einer Zusammenfassung durch den Veräußerer bzw. dessen Berater in Betracht.³⁷ Dabei wird im Einzelnen zu prüfen sein, inwieweit hierdurch die Anforderungen der Vertraulichkeitsabrede mit dem Dritten gewahrt werden. Auch kann sich dabei das Problem stellen, dass die Schwärzung faktisch einer unterbliebenen Offenlegung gleichkommt.³⁸

cc) Datenschutzrechtliche Anforderungen für die Offenlegung von personenbezogenen Daten

- 22** Von der Transaktion selbst und der Übertragung von Assets oder Anteilen ist die Due Diligence als eigener Verarbeitungstatbestand zu unterscheiden. Werden Daten des Zielunternehmens in einem Datenraum zur Verfügung gestellt, wird sowohl beim Share als auch beim Asset Deal regelmäßig eine Verarbeitung (im Sinne einer Übermittlung) von Daten gegeben sein. Insbesondere personenbezogene Arbeitnehmerdaten sind hier betroffen, anhand derer die Zulässigkeit der Offenlegung dargestellt werden soll. Dafür ist zunächst zu erörtern, auf welcher Grundlage die Daten überhaupt im Rahmen einer Due Diligence offengelegt werden dürfen. Soweit es sich bei der Verarbeitung von Daten um personenbezogene Daten (z. B. Name, Familienstand, Leistungsverhalten und Gesundheitszustand) handelt (Art. 4 Nr. 1 DSGVO), findet auch die DSGVO Anwendung. Eine

³⁶ Vgl. auch *Schiffer/Bruß*, BB 2012, 847, 851.

³⁷ *Schiffer/Bruß*, BB 2012, 847, 851.

³⁸ Vgl. *Schiffer/Bruß*, BB 2012, 847, 851.

Verarbeitung nach Art. 4 Nr. 2 DSGVO liegt immer dann vor, wenn die Daten in einen digitalen oder elektronischen Datenraum eingestellt werden (vgl. Art. 2 Abs. 1 DSGVO).³⁹ Zulässig ist diese Verarbeitung nach vorheriger Einwilligung oder durch eine gesetzliche Erlaubnis (Art. 6 Abs. 1 DSGVO). Eine Einwilligung wird meist schon aus rein praktischen Gründen nur schwer einholbar sein, beachte man die Anzahl betroffener Personen und das Interesse der Geheimhaltung einer geplanten Veräußerung.⁴⁰ Eine gesetzliche Rechtfertigung ergibt sich aus Art. 6 Abs. 1 lit. f DSGVO, wenn (i) berechnete Interessen des Verantwortlichen vorliegen, die (ii) die Interessen des Betroffenen in Bezug auf seine Grundfreiheiten und Grundrechte, die seine personenbezogenen Daten schützen, überwiegen.⁴¹

Während sich das berechnete Interesse als wirtschaftliches Interesse an einer möglichst vorteilhaften Veräußerung des Unternehmens gut begründen lässt, bedarf es bei der Abwägung mit den Interessen der Betroffenen einer Einzelfallbetrachtung.⁴² Darüber hinaus ist die Offenlegung bestimmter Informationen für eine Transaktion zwar zwingend erforderlich, doch gilt es auch bei besonderen personenbezogenen Kategorien (Gesundheitszustand, Religionszugehörigkeit, Gewerkschaftszugehörigkeit etc.) die strengeren Vorgaben des Art. 9 Abs. 2 DSGVO zu beachten.⁴³ Unter dieser Prämisse bleibt nur die Anonymisierung und Pseudonymisierung der Daten, um einen Verstoß zu vermeiden. Es ist jedoch zu beachten, dass ein Rückschluss auf die Person ausgeschlossen sein muss. Ist dieser weiterhin möglich, bleibt die DSGVO anwendbar. Die Abwägung der Interessen kann nun jedoch zu Gunsten der Unternehmensinteressen ausfallen, da personenbezogene Daten geschwärzt wurden.⁴⁴ Das gleiche Problem entsteht in sehr kleinen Betrieben, in denen die Pseudonymisierung und Schwärzung häufig daran scheitert, dass stets eine Re-Individualisierung mög-

23

39 Plath, in: v. d. Bussche/Voigt, Konzerndatenschutz, Teil 6 Datenschutz bei M&A Transaktionen, Rn. 13 f. Zur Rolle des Datenschutzes im Rahmen des Compliance Managements ausführlich → Becker/Böhlke/Fladung, Kap. 12.

40 Tribess/Spitz, GWR 2019, 261, 263.

41 Plath, in: v. d. Bussche/Voigt Konzerndatenschutz, Teil 6 Datenschutz bei M&A Transaktionen, Rn. 18. Umstr. ist in diesem Zusammenhang, ob eine verweigerte, unwirksame oder widerrufene Einwilligung im Verhältnis zu anderen Rechtfertigungsgründen Sperrwirkung entfalten. Hiergegen wird jedoch zurecht eingewandt, die Transparenz- und Informationspflichten der Art. 12 ff. DSGVO würden diesem Umstand bereits angemessene Rechnung tragen. Darüber hinaus ließen sich entsprechende Anhaltspunkte weder dem Wortlaut von Art. 6 Abs. 1 DSGVO noch dem von Art. 17 Abs. 1 lit. b a. E. DSGVO entnehmen. Zuletzt ist darauf hinzuweisen, dass eine Sperrwirkung Datenverarbeiter dazu motivieren könnte, auf die Einwilligung seltener zurückzugreifen, was kaum im Sinne des Gesetzgebers liegen dürfte; vgl. zu diesem Thema auch Albers/Veit, in: BeckOK DatenschutzR, 46. Ed. 1.11.2023, DS-GVO Art. 6 Rn. 25. m. w. N.

42 Plath, in: v. d. Bussche/Voigt Konzerndatenschutz, Teil 6 Datenschutz bei M&A Transaktionen, Rn. 21.

43 Tribess/Spitz, GWR 2019, 261, 263 f.

44 Plath, in: v. d. Bussche/Voigt Konzerndatenschutz, Teil 6 Datenschutz bei M&A Transaktionen, Rn. 29 f.

lich wäre.⁴⁵ Dann könnte eine Interessenabwägung dazu führen, dass die Übertragung personenbezogener Daten der gesamten Belegschaft zulässig ist, wenn anders keine Transaktion möglich wäre.

- 24 Demgegenüber ist die Übermittlung personenbezogener Daten der Organmitglieder und Führungskräfte regelmäßig erforderlich und zwingende Voraussetzung für eine erfolgreiche Transaktion. Denn die genaue Kenntnis dieser Schlüsselmitarbeiter, einschließlich ihres Werdegangs sowie der Einzelheiten ihrer Verträge, insbesondere Kündigungsfristen und Change-of-Control-Klauseln (auch „Golden Parachute“), ist für den Erwerber von besonderer Bedeutung. Werden diese Daten nicht an den Erwerber übermittelt, dürfte dies – mit Blick auf die grundsätzlich bestehende Pflicht zur Durchführung einer Due Diligence (dazu → Rn. 45 f.) – die Chancen eines Abschlusses der M&A-Transaktion erheblich beeinträchtigen.⁴⁶ Auch wenn die Interessenabwägung grundsätzlich dazu führt, dass die Offenlegung personenbezogener Daten von Organmitgliedern und Führungskräften erforderlich ist, kann es geboten sein, diese Daten als mildestes Mittel nur einem kleinen Kreis von Personen auf Seiten des Erwerbers in einem Bereich des (virtuellen) Datenraums zur Verfügung zu stellen, der besonderen Zutrittsbeschränkungen unterliegt.⁴⁷
- 25 Weiterhin sind bei einer Übermittlung von personenbezogenen Daten in der Regel vertragliche Vereinbarungen zur Sicherung des Datenschutzes zu treffen. Diese sollten neben der vertraulichen Behandlung der zur Verfügung gestellten Daten die Zweckbestimmung der Verwendung klar regeln und sicherstellen, dass die Daten allein zum Zweck der Due Diligence genutzt sowie nach Abschluss der Vertragsverhandlungen unverzüglich vernichtet werden. Ebenso sollte, im Hinblick auf die Informationspflicht aus Art. 13, 14 DSGVO gegenüber dem Betroffenen über die Verarbeitung seiner Daten, genau dokumentiert werden, aus welchem Grund eine solche Information unterblieben ist. Aus den vorgenannten Gründen liegt es ebenso nicht im Interesse des Veräußerers die Betroffenen auf die Verarbeitung hinzuweisen. Ein Rechtfertigungsgrund besteht jedoch bereits im Falle einer drohenden Vereitelung der Transaktion (Art. 14 Abs. 5 lit. b DSGVO) oder aus dem Geheimhaltungsinteresse des Dritten (Art. 29 Abs. 1 S. 1 BDSG).⁴⁸

3. Kartellrechtliche M&A-Compliance – Vollzugsverbot, Marktmachtmissbrauch und Informationsaustausch

a) Anmeldepflicht und Vollzugsverbot

- 26 Unternehmenskaufverträge unterliegen nach deutschem Recht der Fusionskontrolle (§§ 35 ff. GWB), die vom Bundeskartellamt ausgeübt wird. Jeder Zusam-

45 *Braun/Wybitul*, BB 2008, 782, 785.

46 Vgl. *Braun/Wybitul*, BB 2008, 782, 785.

47 *Braun/Wybitul*, BB 2008, 782, 785.

48 *Treibess/Spitz*, GWR 2019, 261, 264.

menschluss, der einen der Zusammenschlusstatbestände erfüllt (§ 37 GWB) und bestimmte Umsatzschwellen erreicht (§ 35 GWB), ist vor Vollzug beim Bundeskartellamt anzumelden und darf vor dessen Freigabe bzw. dem Ablauf von bestimmten Wartefristen nicht vollzogen werden (präventive Fusionskontrolle, § 41 Abs. 1 GWB). Bei Zusammenschlussvorhaben, die aufgrund der Umsätze der am Zusammenschlussvorhaben beteiligten Unternehmen gemeinschaftsweite Bedeutung haben, erfolgt eine Fusionskontrolle nach europäischem Recht (Verordnung Nr. 139/2004 des Rates vom 20.1.2004 über die Kontrolle von Unternehmenszusammenschlüssen (EG-Fusionskontrollverordnung) – FKVO). Soweit eine europäische Fusionskontrolle nach der FKVO stattfindet, ist die Anwendung des deutschen Kartellrechts im Übrigen ausgeschlossen (sog. „One-Stop-Shop-Prinzip“, Art. 21 Abs. 2, 3 FKVO, § 35 Abs. 3 GWB). Auch soweit europäisches Recht anwendbar ist, darf ein Zusammenschluss nicht vollzogen werden, solange er von der Kommission nicht freigegeben worden ist (Art. 7 Abs. 1 FKVO). Eine in die Einzelheiten gehende Darstellung der fusionskontrollrechtlichen Bestimmungen kann hier nicht erfolgen; insofern sei auf die einschlägige kartellrechtliche Literatur verwiesen.⁴⁹

Verstöße gegen das fusionskontrollrechtliche Vollzugsverbot (bzw. ein etwaiges Anmeldeerfordernis in anderen Jurisdiktionen) werden in der Praxis von den Kartellbehörden zunehmend verfolgt und sanktioniert.⁵⁰ Dabei setzt die Verhängung eines Bußgeldes nicht voraus, dass das Zusammenschlussvorhaben materiell-rechtlich nicht freigabefähig ist; ausreichend ist vielmehr der – rechtliche oder tatsächliche – Vollzug ohne erforderliche Anmeldung.⁵¹ In zwei Fällen eines solchen Frühstarts (sog. „Gun Jumping“) hat die EU-Kommission in der Vergangenheit Bußgelder in Höhe von jeweils 20 Mio. EUR verhängt; in einem der beiden Fälle wurde die Bußgeldhöhe vom EuGH bestätigt.⁵² Jüngst verhängte die EU-Kommission ein Rekordbußgeld in der Höhe von 432 Mio. EUR⁵³ sowie erstmalig ein Bußgeld gegen ein Zielunternehmen.⁵⁴ In früheren Fällen verhängte die Kommission Bußgelder in der Höhe von 124,5 Mio. EUR⁵⁵

49 Siehe nur *Seeliger/Crozals*, in: *Schalast/Raettig*, Grundlagen des M&A-Geschäftes, 2019, Kap. 14, S. 431 ff.; zur kartellrechtlichen Compliance außerhalb von M&A-Transaktionen siehe → *Seeliger/Mross/Seydel*, Kap. 27 sowie *Haus/Erne*, ZWH 2016, 162.

50 *Steger*, DB 2014, 1857, 1858.

51 *Badtke*, KStZ 2011, 418, 420, der m.w.N. auch darauf hinweist, dass sich der Umstand, dass keine wettbewerblichen Bedenken gegen das Zusammenschlussvorhaben bestehen, jedoch bußgeldmindernd auswirken kann.

52 EuGH, 3.7.2015, Rs. C-84/13 P, ECLI:EU:C:2014:2040 – *Electrabel/Compagnie Nationale du Rhône*; KOM, ABl. 2014 C 455, 5 – *Marine Harvest/Morpol* (M.7184).

53 Fall M. 10483 *Illumina/GRAIL*, Entscheidung vom 12.7.2023, Pressemitteilung https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3773 (zuletzt abgerufen am 15.4.2024).

54 Fall M. 10483 *Illumina/GRAIL*, Entscheidung vom 12.7.2023, Pressemitteilung https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3773 (zuletzt abgerufen am 15.4.2024); Das Bußgeld gegen *Illumina* betrug nur 1.000 EUR, da die Kommission erstmalig ein Bußgeld gegen ein Zielunternehmen verhängte.

und 28 Mio. EUR.⁵⁶ Darüber hinaus sind gegen das Vollzugsverbot verstoßende Rechtsgeschäfte grundsätzlich unwirksam (§ 41 Abs. 1 Satz 2 GWB). Um zu überprüfen, ob im Zusammenhang mit einer M&A-Transaktion gegen das Vollzugsverbot verstoßen wurde, kommt es mitunter sogar zu Durchsuchungen durch die Kartellbehörden.⁵⁷

- 28** Der genaue Inhalt des Vollzugsverbots ist nicht gesetzlich festgelegt, aber es ist anerkannt, dass neben der rechtlichen auch die tatsächliche Vollendung des Zusammenschlussvorhabens erfasst ist, d.h. Handlungen, die die wirtschaftlichen Wirkungen des Zusammenschlusses vorwegnehmen.⁵⁸ Das ist von besonderer Bedeutung für die Integrationsplanung. Verständlicherweise würde der Erwerber nach erfolgter Unterzeichnung des Unternehmenskaufvertrags gerne sofort mit der – mitunter langwierigen – Integration der Zielgesellschaft beginnen. Soweit die Transaktion aber der Fusionskontrolle unterliegt, wird man sich zwingend auf vorbereitende Maßnahmen beschränken müssen. Verboten sind grundsätzlich die organisatorische Zusammenführung, die Aufnahme gemeinsamer Geschäftsaktivitäten, die Implementierung gemeinsamer Reporting- und Organisationsstrukturen, die Befolgung interner Weisungen der zukünftigen Geschäftsführung/Anteilseigner, die Abstimmung und Anpassung von Produkten sowie der beiderseitigen Marketing- und Absatzbemühungen und ein gemeinsamer Vertrieb.⁵⁹ Allenfalls in Randbereichen können derartige Aktivitäten ausnahmsweise als Integrationsvorbereitung zulässig sein, wobei die Abgrenzung im Einzelnen komplex ist.⁶⁰ Das Vollzugsverbot des GWB kann dabei in bestimmten Fällen strenger ausgelegt werden, als das in der FKVO was auch explizit in Art. 3 Abs. 3 Wettbewerbsregeln DVO (Verordnung (EG) Nr. 1/2003 des Rates vom 16. Dezember 2002 zur Durchführung der in den Artikeln 81 und 82 des Vertrags niedergelegten Wettbewerbsregeln) festgehalten ist.
- 29** Vor dem Hintergrund der vorstehenden (beispielhaften) Aufzählung unzulässiger Integrationsmaßnahmen ergibt sich eine weitere Haftungsfalle durch unbeabsichtigte Verstöße gegen das Vollzugsverbot: Der Erwerber wird dem Veräußerer regelmäßig Verhaltenspflichten für die Leitung der Zielgesellschaft in der Zeit zwischen Vertragsunterzeichnung und Vollzug auferlegen und jedenfalls wesentliche Maßnahmen an seine vorherige Zustimmung knüpfen wollen (sog.

55 EuGH, 3.7.2015, Rs. C-84/13 P, ECLI:EU:C:2014:2040 – Electrabell/Compagnie Nationale du Rhône; KOM, ABl. 2014 C 455, 5 – Marine Harvest/Morpol (M.7184).

56 Fall M.8179, Entscheidung vom 27.6.2019, https://ec.europa.eu/competition/mergers/cases/decisions/m8179_759_3.pdf (zuletzt abgerufen am 15.4.2024).

57 *Steger*, DB 2014, 1857, 1858.

58 BGH, Beschl. v. 17.7.2018 – KVR 64/17 (OLG Düsseldorf), NZKart 2018, 541; statt vieler *Badtke*, KSzW 2011, 418, 419 m. w. N.

59 *Badtke*, KSzW 2011, 418 m. w. N.

60 *Badtke*, KSzW 2011, 418, 419 m. w. N.

„Conduct of Business Covenants“).⁶¹ Das Fusionskontrollrecht erkennt den Schutzzweck derartiger Klauseln grundsätzlich an. Diese dürfen jedoch nicht zu einer De-facto-Integration führen. Das wäre insbesondere dann der Fall, wenn der Erwerber die Möglichkeit eingeräumt bekäme, über die Geschäftspolitik der Zielgesellschaft insgesamt zu entscheiden und beispielsweise der Geschäftsführung Weisungen erteilen könnte.⁶²

In der Praxis empfiehlt es sich, die mit der Verhandlung und Durchführung einer Transaktion betrauten Personen von dem fusionskontrollrechtlichen Anmeldeerfordernis und Vollzugsverbot sowie deren Implikationen in Kenntnis zu setzen (z.B. durch Erstellung einer Übersicht der kartellrechtlichen „Dos“ und „Don'ts“) und frühzeitig Experten heranzuziehen. Dies dient einerseits dazu Haftungsfallen zu erkennen und andererseits, um frühzeitig zu verhindern, dass übertriebene Darstellungen der Transaktion erstellt werden, die den Parteien später kartellrechtlich „auf die Füße fallen“ können. Das kann auch bei rein internen Unterlagen – wie z.B. Vorstandsvorlagen – der Fall sein, die die Kartellbehörden zur Prüfung des Zusammenschlussvorhabens anfordern können. Dies dürfte aber in Deutschland die Ausnahme sein.⁶³

Weiterhin kann die frühzeitige Einschaltung von Beratern eine Verzögerung des Vollzugs vermeiden. Dies gilt insbesondere bei Transaktionen, an denen Unternehmen mit (signifikanten) Umsätzen in vielen Ländern beteiligt sind: Derzeit gibt es weltweit mehr als 100 Jurisdiktionen, die ggf. im Hinblick auf ein Anmelde- oder zumindest Notifizierungserfordernis geprüft werden müssen.⁶⁴ Zudem gibt es auf europäischer Ebene ein formalisiertes Pränotifizierungsverfahren und im Idealfall kann auch auf nationaler Ebene bereits vor Abschluss des Unternehmenskaufvertrags die fusionskontrollrechtliche Anmeldung entworfen werden und eine mündliche Vorabstimmung mit der zuständigen Behörde stattfinden (sog. „Courtesy Call“). Spätestens mit Unterzeichnung des Unternehmenskaufvertrags kann dann die Anmeldung des Zusammenschlussvorhabens mit dem Ziel einer zügigen Freigabe erfolgen.

b) Informationsaustausch

Das Kartellrecht hat jedoch nicht nur Auswirkungen auf den Vollzug einer M&A-Transaktion, sondern auch auf Transaktionsstadien vor Abschluss des Unternehmenskaufvertrags, namentlich den Austausch wettbewerbsrelevanter Informationen im Rahmen der Due Diligence. Denn eine kartellrechtswidrige Vereinbarung (Art. 101 AEUV, § 1 GWB) kann schon in einer unmittelbaren oder mittelbaren Fühlungnahme zwischen Unternehmen liegen, die bezweckt oder

61 Vgl. nur *Schrader*, in: Seibt, Beck'sches Formularbuch Mergers & Acquisitions, C.II.2, § 13.1, 411 sowie die Erläuterungen in Fn. 135, 454.

62 *Badtke*, KSzW 2011, 418, 424 m. w. N.

63 *Badtke*, KSzW 2011, 418, 419, mit dem plastischen Beispiel einer Aussage wie „[w]ir steigen mit dem Deal zum absoluten Weltmarktführer auf“.

64 *Steger*, DB 2014, 1857, 1858.

bewirkt, das Marktverhalten eines Wettbewerbers zu beeinflussen oder ihn über das eigene beabsichtigte Marktverhalten in Kenntnis zu setzen.⁶⁵ Auch insofern ist von einer erheblichen praktischen Relevanz auszugehen, da sich der Fokus sowohl des Bundeskartellamtes als auch der Kommission seit einigen Jahren neben den sog. Hardcore-Kartellen auch auf den Austausch wettbewerbsrelevanter Informationen erstreckt.⁶⁶

- 33** Für den Austausch von wettbewerbsrelevanten Informationen im Zusammenhang mit einer M&A-Transaktion lassen sich die folgenden Grundregeln formulieren: Ein transaktionsbezogener Informationsaustausch ist grundsätzlich dann unbedenklich, wenn es sich bei den beteiligten Unternehmen nicht um (potenzielle) Wettbewerber handelt und sie auch nicht auf denselben einander vor- oder nachgelagerten Marktstufen tätig sind.⁶⁷ Dies trifft häufig insbesondere auf M&A-Transaktionen unter Beteiligung von Finanzinvestoren zu, soweit sich in deren Portfolio noch kein Wettbewerber der Zielgesellschaft oder ein Unternehmen auf einem vor- oder nachgelagerten Markt befindet.⁶⁸ Unbedenklich ist ein Informationsaustausch im Rahmen der Due Diligence weiterhin grundsätzlich dann, wenn die Informationen öffentlich verfügbar sind (in Geschäftsberichten etc.).⁶⁹
- 34** Sind die beteiligten Unternehmen (potenzielle) Wettbewerber und handelt es sich nicht um öffentlich verfügbare Informationen, ist der gemeinsame Marktanteil und die Art der Informationen entscheidend: Ein Austausch soll nach der Literatur, die die sog. De-Minimis-Bekanntmachung der Kommission⁷⁰ heranzieht, dann unbedenklich sein, wenn der gemeinsame Marktanteil der beteiligten Unternehmen unter 10 % liegt und eine Wettbewerbsbeschränkung nicht bezweckt wird. Im Falle eines reinen Vertikalverhältnisses (d. h. einer Leistungsbeziehung zwischen einem Unternehmen und seinen Lieferanten) gilt das Gleiche, wenn der Marktanteil der beteiligten Unternehmen auf ihren jeweiligen Märkten 15 % nicht überschreitet. Handelt es sich um einen kumulativen Marktabstottungseffekt (durch nebeneinander bestehende Netze von Vereinbarungen), sinkt die Marktanteilsschwelle auf 5 %.⁷¹ Auch in diesen Fällen ist jedenfalls aus Sicht der

65 EuGH, Urt. v. 28.5.1998, C-7/95, Slg. 1998 I-3111, Rn. 87 – John Deere; EuGH, Urt. v. 4.6.2009, C-8/08, Slg. 2009 I-4529, Rn. 36 – T-Mobile.

66 Vgl. noch zur alten Bekanntmachung: *Besen/Gronemeyer*, CCZ 2013, 137; *Bischke/Brack*, NZG 2018, 696; zurückhaltender *Liese/Theusinger*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 27 Rn. 40.

67 *Besen/Gronemeyer*, CCZ 2013, 137, 142.

68 *Besen/Gronemeyer*, CCZ 2013, 137, 142 m. w. N.

69 *Besen/Gronemeyer*, CCZ 2013, 137, 142.

70 Vgl. Bekanntmachung über Vereinbarungen von geringer Bedeutung, die im Sinne des Art. 101 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union den Wettbewerb nicht spürbar beschränken (De-minimis-Bekanntmachung) (2014/C 291/01) Rn. 8–10.

71 *Besen/Gronemeyer*, CCZ 2013, 137, 142.

Kommission aber ein Austausch von solchen Informationen unzulässig, die das beabsichtigte Preis- oder Mengenverhalten betreffen.⁷²

In allen anderen Fällen ist die Zulässigkeit davon abhängig, inwiefern der Informationsaustausch für die beabsichtigte Transaktion erforderlich und angemessen ist,⁷³ was naturgemäß zu einem nicht unerheblichen Maß an Rechtsunsicherheit führt. Insofern gilt grundsätzlich, dass eine Preisgabe von Informationen umso eher zulässig ist, (i) je weiter die Verhandlungen fortgeschritten sind (in einem späteren Stadium steigt einerseits die Notwendigkeit einer genauen Kenntnis der Zielgesellschaft und andererseits sinkt die Gefahr des Scheiterns der Transaktion und damit das wettbewerbliche Gefährdungspotenzial), (ii) je weniger Unternehmen noch an dem Auktionsverfahren beteiligt sind (soweit es sich bei der geplanten Transaktion um ein solches handelt) und (iii) je weniger wettbewerbssensibel die konkreten Informationen sind.⁷⁴ **35**

Dabei sollte sichergestellt sein, dass die Informationen nur so weit verbreitet werden, wie dies zum Zweck der Bewertung der Transaktion durch den Erwerber erforderlich ist. Insbesondere sollten die wettbewerbsrelevanten Informationen nur solchen Mitarbeitern oder Beratern des Erwerbers zugänglich gemacht werden, die an der Transaktion beteiligt sind und die Informationen daher tatsächlich benötigen („Need to know“-Basis). Diese Mitarbeiter sollten darüber hinaus nicht mit dem operativen Geschäft befasst sein und keinen Einfluss auf das Wettbewerbsverhalten haben, z. B. indem sie an der Preisgestaltung mitwirken. Nur so kann sichergestellt werden, dass die ausgetauschten Informationen sich nicht auf das Marktverhalten des Erwerbers auswirken. Diejenigen Mitarbeiter des Erwerbers, die über die Durchführung der M&A-Transaktion entscheiden und zugleich Verantwortung für die operative Tätigkeit tragen, sollten die betroffenen wettbewerbsrelevanten Informationen zunächst (d. h. vor Durchführung der Transaktion) lediglich in Form aggregierter Berichte erhalten. Auf diesem Weg kann vermieden werden, dass einzelne Mitarbeiter des Erwerbers in der Folge ihrer Kenntniserlangung mit einer Sperre belegt werden müssten, während der sie nicht in das operative Geschäft des Erwerbers eingreifen dürfen.⁷⁵ Dies kann insbesondere dann überaus unangenehm sein, wenn die geplante Transaktion noch auf der Zielgeraden scheitert. In diesem Fall kann die Sperre nicht mit Vollzug der geplanten Transaktion enden, sondern muss fort dauern. **36**

Organisatorisch kann die erforderliche Begrenzung des Kreises der Personen, an die wettbewerbsrelevante Informationen in nicht aggregierter Form weitergegeben werden, durch die Einrichtung eines sog. „Clean Teams“ umgesetzt werden.⁷⁶ Teil des Clean Teams werden Mitarbeiter, die nicht (mehr) operativ tätig sind, gleichzeitig aber über die nötige Marktkennntnis verfügen (z. B. pensionierte **37**

⁷² Besen/Gronemeyer, CCZ 2013, 137, 142.

⁷³ Badtke, KSzW 2011, 418, 421 m. w. N.; Besen/Gronemeyer, CCZ 2013, 137, 142.

⁷⁴ Besen/Gronemeyer, CCZ 2013, 137, 142 m. w. N.

⁷⁵ Zum Ganzen: Besen/Gronemeyer, CCZ 2013, 137, 143 (insbesondere Fn. 70).

⁷⁶ Badtke, KSzW 2011, 418, 422 m. w. N.; Besen/Gronemeyer, CCZ 2013, 137, 144.

Führungskräfte). Dabei kann es sich – insbesondere zu Dokumentationszwecken – anbieten, von den Mitgliedern des Clean Teams ungeachtet ihrer entsprechenden arbeitsvertraglichen (oder im Fall „reaktiver“ ehemaliger Führungskräfte in deren Beratervertrag verankerter) Vertraulichkeitspflichten spezielle persönliche Vertraulichkeitserklärungen einzuholen. Ferner sollten Informationsbarrieren (auch sog. „Ethical“ oder „Chinese Walls“) innerhalb der Organisation des Erwerbers implementiert werden.⁷⁷

- 38 Schließlich kann sich auch die Einbindung von externen Beratern anbieten: Die wettbewerbsrelevanten Informationen können – statt von einem unternehmensinternen Clean Team – von einer Wirtschaftsprüfungsgesellschaft oder Anwaltskanzlei gesichtet und nur anonymisiert oder aggregiert an den Erwerber weitergegeben werden.⁷⁸ Dies kommt insbesondere dann in Betracht, wenn auf Seiten des Erwerbers keine oder nicht ausreichend geeignete Clean Team-Mitglieder vorhanden sind⁷⁹ oder wenn es sich um hochsensible Daten handelt.⁸⁰
- 39 Die wettbewerbsrelevanten Daten können naturgemäß nicht im allgemein zugänglichen (virtuellen) Datenraum offengelegt werden, sondern sind in einen speziellen Teilbereich des (virtuellen) Datenraums einzustellen, der nur den Mitgliedern des Clean Teams zugänglich ist (sog. „Red Data Room“).⁸¹ Einer detaillierten Dokumentation der Maßnahmen, die ergriffen wurden, um zu verhindern, dass wettbewerbsrelevante Daten operativ tätigen Mitarbeitern des Erwerbers zugänglich gemacht werden, kommt dabei entscheidende Bedeutung zu, falls eine Wettbewerbsbehörde Ermittlungen anstellt. In inhaltlicher Hinsicht wird zu prüfen sein, inwiefern die wettbewerbsrechtliche Brisanz der offengelegten Informationen durch eine Steuerung der Qualität der Daten minimiert werden kann. In Betracht kommt hier, sensible Preis- und Kundendaten nicht in der jeweils aktuellen Fassung offenzulegen.⁸² Im Falle des Scheiterns der Transaktion sind die wettbewerbsrelevanten Daten zu vernichten. Dies ist bereits bei Offenlegung der Daten in der zwischen Veräußerer und Erwerber abzuschließenden Vertraulichkeitsvereinbarung (siehe → Rn. 14 f.) entsprechend zu regeln.

4. Kapitalmarktrechtliche M&A-Compliance

a) Informationsweitergabe im Rahmen der Due Diligence

- 40 Die Weitergabe von Informationen im Rahmen einer Due Diligence durch börsennotierte Zielgesellschaften bzw. Zielgesellschaften, deren Obergesellschaft eine börsennotierte Gesellschaft ist, wird nach allgemeiner Auffassung nicht

77 Besen/Gronemeyer, CCZ 2013, 137, 144, dort auch zu Vorschlägen für konkrete organisatorische Maßnahmen.

78 Besen/Gronemeyer, CCZ 2013, 137, 144.

79 Besen/Gronemeyer, CCZ 2013, 137, 144.

80 Badtke, KSzW 2011, 418, 422 m. w. N.

81 Link/Fröhlich, GWR 2014, 449, 451.

82 Badtke, KSzW 2011, 418, 422 m. w. N.

durch das Verbot der Offenlegung von Insiderinformationen (Art. 14 Marktmissbrauchsverordnung) ausgeschlossen.⁸³

b) Ad-hoc-Pflicht

Wann die beabsichtigte Durchführung einer M&A-Transaktion eine präzise Information über nicht öffentlich bekannte Umstände wird, die sich auf einen Emittenten von Insiderpapieren bezieht und geeignet ist, im Falle ihres öffentlichen Bekanntwerdens den Börsen- oder Marktpreis der Insiderpapiere erheblich zu beeinflussen – es sich mithin um eine Insiderinformation handelt (Art. 7 Abs. 1 Marktmissbrauchsverordnung) – ist umstritten und stark vom Einzelfall abhängig.⁸⁴ Insbesondere auf Veräußererseite kann bereits die Tatsache für sich, dass eine M&A-Transaktion geplant ist, oder die Einleitung erster Schritte eine konkrete Information sein, die bei Kurserheblichkeit dem Grunde nach Veröffentlichungspflichtig ist, ohne dass es auf die hinreichende Wahrscheinlichkeit des Vertragsabschlusses ankommt.⁸⁵ Denn nach dem Urteil des EuGH in der Rechtssache *Geltl/Daimler* können auch Zwischenschritte für sich eine Insiderinformation darstellen, vgl. Art. 7 Abs. 3 Marktmissbrauchsverordnung.⁸⁶ Die Abgrenzung zwischen veröffentlichungspflichtigen Zwischenschritten und bloßen Planungs- und Vorbereitungshandlungen führt hier häufig zu Rechtsunsicherheit. Der Emittentenleitfaden der BaFin versucht Orientierung zu bieten und zählt Umstände auf, die zumindest Anlass zur Prüfung des Vorliegens einer Insiderinformation geben sollen (bspw. Übersendung eines Term Sheets, Abschluss einer Vertraulichkeitsvereinbarung, Durchführung einer Due Diligence).⁸⁷ Entscheidend bleibt weiterhin, ob es sich um eine (i) präzise Information handelt, die (ii) Kursbeeinflussungspotenzial aufweist. Je weiter der Übernahmeprozess vorangeschritten ist, umso höher muss dieses Potenzial auch angesehen werden. Nicht zuletzt vor dem Hintergrund der Pflicht, Aktionären etwaige Schäden zu ersetzen, die durch eine unterlassene Ad-hoc-Mitteilung entstanden sind (§§ 97, 98 WpHG), sowie der Möglichkeit zur Selbstbefreiung (dazu sogleich) sollte im Zweifel jedoch aus Gründen der Vorsicht eine Ad-hoc-Pflicht angenommen werden.

Liegt eine Insiderinformation vor, kann sich die betroffene Gesellschaft in zulässiger Weise von ihrer Pflicht zur Veröffentlichung einer Ad-hoc-Mitteilung durch einen entsprechenden Beschluss des Vorstands selbst befreien. Voraussetzung hierfür ist nach Art. 17 Abs. 4 Marktmissbrauchsverordnung, dass (i) die

41

42

83 *Banerjee*, ZIP 2003, 1730, 1737; *K. J. Müller*, NJW 2000, 3452, 3456; vgl. BT-Drs. 12/6679 zu § 14 Abs. 1 WpHG, 47; vgl. auch *Liese/Theusinger*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 27 Rn. 29 f., die die Zulässigkeit implizit voraussetzen.

84 Ausführlich zur umfassenden Kasuistik und insb. auch zur Due Diligence: *Hasselbach/Stepper*, BB 2020, 203, 206 ff.

85 Vgl. v. *Bonin/Böhmer*, EuZW 2012, 694, 697.

86 EuGH, Urt. v. 28.6.2012, C-19/11 – *Markus Geltl/Daimler AG*, DB 2012, 1496.

87 BaFin-Konsultation, Nr. 14/2019, Entwurf Emittentenleitfaden, Modul C (Stand 1.7.2019), S. 27 f.

Offenlegung die berechtigten Interessen des Emittenten an der Geheimhaltung der Information zu beeinträchtigen geeignet wäre (beispielsweise weil laufende Verhandlungen beeinträchtigt würden), (ii) die Aufschiebung nicht geeignet wäre, die Öffentlichkeit irrezuführen (der Emittent darf während des Befreiungszeitraums nicht selbst aktiv Signale hinsichtlich des Gegenstands des Selbstbefreiungsbeschlusses setzen, z.B. durch Dementi, die zu der noch nicht veröffentlichten Information in Widerspruch stehen) und (iii) die Geheimhaltung gewährleistet ist. Es ist fortlaufend zu überprüfen, ob die Voraussetzungen für eine Selbstbefreiung weiter vorliegen und bei Entfallen ist die Ad-hoc-Mitteilung unverzüglich nachzuholen (Art. 17 Abs. 7 Marktmissbrauchsverordnung). Der Emittent hat unmittelbar im Anschluss an die aufgeschobene Veröffentlichung der Ad-hoc-Mitteilung der Bundesanstalt für Finanzdienstleistungsaufsicht den Aufschub als solchen und die Gründe für die Befreiung mitzuteilen (Art. 17 Abs. 4 Unterabs. 2 Marktmissbrauchsverordnung).

- 43 Neben der Veröffentlichung einer Ad-hoc-Mitteilung bzw. der Selbstbefreiung von einer entsprechenden Pflicht hierzu hat der Vorstand der börsennotierten Aktiengesellschaft die Insiderliste gemäß Art. 18 Marktmissbrauchsverordnung ergänzen zu lassen, sobald eine Insiderinformation vorliegt. Zudem muss er die Insider auf ihre gesetzliche Pflicht zur Beachtung des Insiderrechts hinweisen und mit ihnen eine Vertraulichkeitsvereinbarung schließen (lassen), soweit sie nicht bereits standesrechtlich zur Verschwiegenheit verpflichtet sind.

c) Übernahmerechtliche M&A-Compliance

- 44 Bei der Übernahme einer börsennotierten Gesellschaft sind insbesondere die Bestimmungen des WpÜG zu beachten, dessen Ziele es sind, (i) ein Übernahmeverfahren ohne Forderung und Behinderung einer Unternehmensübernahme zu schaffen, (ii) Information und Transparenz für die Aktionäre und Arbeitnehmer der Zielgesellschaft zu verbessern, (iii) die rechtliche Stellung der Minderheitsaktionäre bei einer Unternehmensübernahme zu stärken und (iv) international übliche Standards zu implementieren.⁸⁸ Die Veröffentlichungspflicht nach WpÜG bezieht sich auf die Entscheidung zur Abgabe eines Angebots (§ 10 Abs. 1 WpÜG). Das Konkurrenzverhältnis zu § 17 Abs. 1 Marktmissbrauchsverordnung, der deutlich früher eine Veröffentlichungspflicht auferlegt, wird über § 10 Abs. 6 WpÜG gelöst. Hier wird bezüglich dieser speziellen Entscheidung nur das WpÜG für anwendbar erklärt.⁸⁹ Hinsichtlich der übernahmerechtlichen Einzelfragen wird auf die einschlägige Literatur verwiesen.⁹⁰

88 *Beisel*, in: *Beisel/Klumpp*, Unternehmenskauf, § 14 Rn. 26.

89 *Hasselbach/Stepper*, BB 2020, 203, 209 f.

90 Siehe nur zum Einstieg *Beisel*, in: *Beisel/Klumpp*, Unternehmenskauf, § 14, sowie *Schwark/Zimmer* (Hrsg.), Kapitalmarktsrechts-Kommentar, WpÜG, passim.

5. Pflicht zur Durchführung einer rechtlichen Due Diligence

a) Regelfall

Jedenfalls bei Transaktionen von grundsätzlicher Bedeutung geht die herrschende Auffassung von einer Pflicht der Organe des Erwerbers zur Durchführung einer Due Diligence aus, um dem Erfordernis einer sorgfältigen Entscheidungsvorbereitung zu genügen.⁹¹ Hierbei handelt es sich allerdings nicht um eine absolute Pflicht. Vielmehr ist der erforderliche Umfang der Informationsbeschaffung für eine Transaktion – insbesondere im Wege der Due Diligence – von der Geschäftsleitung des Erwerbers im Einzelfall abzuwägen.⁹² 45

Bei der somit grundsätzlich bestehenden Pflicht der Organe des Erwerbers, eine Due Diligence durchzuführen, handelt es sich allerdings nur um eine ihrer eigenen Gesellschaft geschuldete Sorgfaltspflicht und ausdrücklich nicht um eine solche gegenüber dem Veräußerer. Auch handelt es sich nicht um eine Obliegenheit des Erwerbers, deren Nichtbeachtung etwa zu einem Rechtsverlust gegenüber dem Veräußerer führen würde: Denn nach deutschem Kaufrecht gibt es grundsätzlich keine Prüfungspflicht des Erwerbers.⁹³ Soweit die M&A-Transaktion für beide Seiten ein Handelsgeschäft ist, könnte zwar grundsätzlich eine gesetzliche Untersuchungs- und Rügeobliegenheit bestehen (§ 377 Abs. 1 HGB). Die Anwendbarkeit einer solchen Obliegenheit auf Unternehmenskäufe wird jedoch von der wohl herrschenden Auffassung abgelehnt.⁹⁴ Im Übrigen werden die Norm sowie ihr zugrunde liegende Rechtsgedanken in der Praxis regelmäßig im Unternehmenskaufvertrag (höchstvorsorglich) abgedungen. Zudem würde eine Untersuchungsobliegenheit erst ab Ablieferung der Kaufsache (d.h. wohl dem Vollzug der M&A-Transaktion) bestehen und somit jedenfalls nicht zu einer Pflicht zu einer Due Diligence vor Vertragsunterzeichnung führen.⁹⁵ Allenfalls in extremen Ausnahmefällen könnte man bei Unterlassen einer Due Diligence an ein Mitverschulden des Erwerbers (§ 254 Abs. 1 BGB) denken.⁹⁶ 46

91 LG Hannover, 23.2.1977, 1 O 123/75, AG 1977, 198 f.; Böttcher, NZG 2005, 49, 50 (für den Vorstand einer AG); Liese, BB 2010, 27, 28; Spindler, in: MünchKomm-AktG, § 93 Rn. 82; vgl. auch Schiffer/Bruß, BB 2012, 847, 848.

92 Schiffer/Bruß, BB 2012, 847, 848.

93 BGH, Urt. v. 15.9.23, V ZR 77/22, NJW 2023, 3423, 3427 f.; Göthel, in: Göthel, Grenzüberschreitende M&A-Transaktionen, § 2 Rn. 89; Schiffer/Bruß, BB 2012, 847, 848; Beisel, in: Beisel/Klumpp, Unternehmenskauf, § 2 Rn. 8.

94 Siehe nur Göthel, in: Göthel, Grenzüberschreitende M&A-Transaktionen, § 2 Rn. 89 (Fn. 140); a. A. Beisel, in: Beisel/Klumpp, Unternehmenskauf, § 2 Rn. 10.

95 BGH, Urt. v. 15.9.2023, V ZR 77/22, NJW 2023, 3423, 3428; Göthel, in: Göthel, Grenzüberschreitende M&A-Transaktionen, § 2 Rn. 89 (Fn. 140).

96 Zusammenfassend Fleischer/Körber, BB 2001, 841, 848 f.

b) Besonders gelagerte Fälle

- 47 Die Rechtsprechung erkennt ausdrücklich an, dass es Ziel der Due Diligence nur sein kann, die „vorhandenen Risiken zumindest in einem gewissen, mit zumutbarem Aufwand erreichbaren Umfang zu begrenzen“.⁹⁷ Während diese Abwägung – wie eingangs erläutert – im Regelfall dazu führen wird, dass es einer Due Diligence bedarf, kann in besonders gelagerten Fällen die Geschäftsleitung des Erwerbers durchaus zu dem Ergebnis kommen, nur eine stark eingeschränkte oder auch keine Due Diligence durchzuführen.⁹⁸ Das kann insbesondere dann der Fall sein, wenn der Erwerber die Zielgesellschaft hinreichend kennt, beispielsweise weil er bereits deren Gesellschafter ist. Denkbar ist auch, dass es sich um eine feindliche Übernahme handelt, bei der die Zielgesellschaft naturgemäß keine Informationen zur Verfügung stellen wird. Ein vollständiger Verzicht auf eine Due Diligence ist in diesem Fall gleichwohl nicht angezeigt; vielmehr sind alle öffentlich zugänglichen Erkenntnisquellen auszuschöpfen.⁹⁹ Diese sind bei börsennotierten Unternehmen vielfältig, da sie ungleich mehr Berichtspflichten unterliegen als nicht-börsennotierte Unternehmen. Zu nennen sind in diesem Zusammenhang beispielsweise Ad-hoc-Mitteilungen oder der Abschnitt zur Compliance-Berichterstattung im Jahresabschluss.¹⁰⁰
- 48 Grundsätzlich kommt ein Verzicht auf eine Due Diligence bei einer Transaktion mit sehr geringem Volumen in Betracht.¹⁰¹ Allerdings ist auch dabei sicherzustellen, dass – ungeachtet des geringen Volumens – keine unbekannten Risiken eingekauft werden, die ggf. das Volumen der Transaktion übersteigen und unter Umständen sogar auf den Erwerber „durchschlagen“ (etwa aufgrund von Reputationsschäden). Denn auch „kleine“ Transaktionen können große Risiken bergen. Bei sehr großvolumigen Transaktionen können nach sorgfältiger Abwägung bestimmte Schwellenwerte festgelegt werden, unterhalb derer Verträge nicht oder nur eingeschränkt geprüft werden. Auch die Kosten der Durchführung einer Due Diligence,¹⁰² zeitliche Aspekte¹⁰³ sowie die fehlende Bereitschaft des Veräußerers, Informationen offenzulegen, können in die Abwägungsentscheidung hinsichtlich des Umfangs der Informationsbeschaffung einbezogen werden.
- 49 Allein der Verweis auf die Eilbedürftigkeit einer Transaktion kann allerdings kaum hinreichender Grund sein, auf die Durchführung einer Due Diligence zu verzichten. Denn praktisch jede Transaktion ist aus Sicht der Handelnden eilbe-

97 OLG Oldenburg, 22.6.2006, 1 U 34/03, BB 2007, 66, 68; vgl. auch *Schwarz*, BB 2012, 136 ff.; *Andras/Szesny*, Deutscher AnwaltSpiegel 20/2015, 3, 4.

98 *Schiffer/Bruß*, BB 2012, 847, 848.

99 *Schwarz*, BB 2012, 136.

100 Vgl. *Schwarz*, BB 2012, 136.

101 *Hölters*, AktG, § 93 Rn. 162.

102 *Nauheim/Goette*, DStR 2013, 2520, 2525; *Schiffer/Bruß*, BB 2012, 847, 848.

103 *Nauheim/Goette*, DStR 2013, 2520, 2525; *Schiffer/Bruß*, BB 2012, 847, 848; *Böttcher*, NZG 2007, 481, 483 f.

dürftig.¹⁰⁴ Auch kann die fehlende Bereitschaft des Veräußerers zur Offenlegung von wesentlichen Informationen für sich alleine kaum eine ausreichende Begründung für die Geschäftsleitung des Erwerbers sein, die Due Diligence zu unterlassen oder unangemessen einzuschränken. Im Regelfall müssen weitere Umstände hinzutreten, die es aus Sicht der Geschäftsleitung des Erwerbers angemessen erscheinen lassen, die Transaktion auch ohne Due Diligence durchzuführen. Dies kann beispielsweise dann der Fall sein, wenn der Kaufpreis sehr attraktiv ist und die maximalen Risiken auch ohne (eingehende) Due Diligence abgeschätzt werden können. Im Zweifelsfall wird es aber so liegen, dass die Geschäftsleitung von einer Transaktion Abstand nehmen muss, wenn ihr nicht die Möglichkeit eingeräumt wird, in dem erforderlichen Maß Due Diligence zu betreiben, wie es im Einzelfall geboten ist – zumal dies gerade ein Indiz für wesentliche Risiken sein könnte, die unentdeckt bleiben sollen.

Auch die Tatsache, dass (umfangreiche) Garantien im Unternehmenskaufvertrag vereinbart werden, kann für sich allein in der Regel kein Argument sein, auf eine Due Diligence zu verzichten. Denn typischerweise sind jedenfalls operative Garantien höhenmäßig auf einen bestimmten Prozentsatz des Kaufpreises (sog. „Cap“) beschränkt und erst ab einer bestimmten Höhe ersatzfähig (sog. „De minimis“). Auf Rechtsfolgenrechte wird entgangener Gewinn jedenfalls auf Ebene des Erwerbers häufig als ersatzfähiger Schaden ausgeklammert und es wird vereinbart, dass bei der Schadensberechnung keine EBIT(DA)-Multiplikatoren (sog. „Multiples“) berücksichtigt werden dürfen, selbst wenn diese bei der Berechnung des Kaufpreises zugrunde gelegt wurden. Weiterhin unterliegen Garantien der (typischerweise kenntnisunabhängigen) Verjährung. Schließlich stellt sich auch immer die Frage der tatsächlichen Beweis- und Durchsetzbarkeit etwaiger Ansprüche aus der Verletzung von Garantien. Vor diesem Hintergrund muss der Unternehmenskaufvertrag stark vom marktüblichen Standard abweichen, um für sich alleine genommen einen Verzicht oder eine unangemessene Einschränkung der Due Diligence rechtfertigen zu können. Statt Garantien müsste der Unternehmenskaufvertrag wohl eher – umfassende, d. h. alle denkbaren Risiken abdeckende – Freistellungen auf Euro-für-Euro-Basis zugunsten des Erwerbers vorsehen. Im Fall eines Garantieverstoßes muss der Erwerber die Garantieverletzung einschließlich des eingetretenen Schadens darlegen und ggf. beweisen; im Fall einer Freistellung muss der Erwerber hingegen nur das Vorliegen der vertraglich vereinbarten Freistellungs Voraussetzungen – beispielsweise die Geltendmachung eines Anspruchs gegen die Zielgesellschaft durch einen Dritten – darlegen und beweisen.¹⁰⁵ Schließlich werden Freistellungen auch nicht von etwa vertraglich vereinbarten oder gesetzlichen Einschränkungen für solche Schäden erfasst, die der Erwerber kannte oder hätte kennen müssen. Die

104 Insbesondere in Bieterverfahren wird absichtlich Zeitdruck generiert, *Nauheim/Goette*, DSStR 2013, 2520, 2525.

105 Vgl. *Schrader*, in: Seibt, Beck'sches Formularbuch Mergers & Acquisitions, Anm. 101 zu C.II.1, 313.

tatsächliche Durchsetzbarkeit von Schadensersatzansprüchen müsste in besonders weitgehendem Maße abgesichert sein (z. B. durch eine Hinterlegung eines nicht unerheblichen Teils des Kaufpreises auf einem Treuhandkonto).

- 51 Abschließend ist noch einmal hervorzuheben, dass – wie eingangs formuliert – das Ergebnis der Abwägungsentscheidung hinsichtlich des erforderlichen Informationsumfangs immer von den Umständen des Einzelfalls abhängt und die vorstehenden Überlegungen nur Erwägungen hinsichtlich des Regelfalls sind.

c) Nachgelagerte Due Diligence (Post-Closing Due Diligence)

- 52 Soweit es ausnahmsweise zulässig ist, vor Vertragsunterzeichnung auf die Durchführung einer Due Diligence zu verzichten, wird diese in aller Regel nach Vollzug des Erwerbs als sog. „Post-Closing Due Diligence“ jedenfalls in dem Umfang nachzuholen sein, wie dies erforderlich ist, um festzustellen, ob Ansprüche unter Freistellungsvereinbarungen oder Garantien bestehen. Dies hat vor Ablauf der Verjährungsfristen zu erfolgen.¹⁰⁶ Hinweise, die den Verdacht auf Gesetzesverstöße begründen oder eine unzureichende Einhaltung von Compliance- und Kartellrechtsanforderungen nahelegen, sind weitere Gründe für eine nachgelagerte Due Diligence mit dem Ziel, fortgesetzte Verstöße zu identifizieren und abzustellen.¹⁰⁷

6. (Abbruch der) Vertragsverhandlungen

- 53 Durch die Aufnahme von Verhandlungen zwischen Veräußerer und Erwerber wird regelmäßig ein vorvertragliches Schuldverhältnis begründet (§ 311 Abs. 2 Nr. 1 BGB). Dieses vorvertragliche Schuldverhältnis kann durch den treuwidrigen Abbruch von Vertragsverhandlungen verletzt werden. Ein Schadensersatzanspruch (§§ 280 Abs. 1, 241 Abs. 2 BGB) soll nach der Rechtsprechung dabei aber ausnahmsweise nur dann entstehen, wenn eine Partei der anderen fälschlicherweise ihre Bereitschaft zum Abschluss eines Unternehmenskaufvertrags vorgespiegelt hat und die andere Partei dadurch zu Aufwendungen veranlasst wurde.¹⁰⁸ Eine solche Haftung kann allerdings von den Parteien dadurch ausgeschlossen werden, dass im Letter of Intent,¹⁰⁹ im Term Sheet¹¹⁰ oder einem den Ablauf eines Bieterverfahrens beschreibenden Process Letter¹¹¹ deutlich gemacht wird, dass keine solche Abschlussbereitschaft besteht.
- 54 Weiterhin ist ausdrücklich darauf hinzuweisen, dass die Aufgabe einer zunächst vorhandenen Erwerbsabsicht nicht mit dem Vorspiegeln einer gar nicht vorhan-

106 Vgl. von Busekist/Timmerbeil, CCZ 2013, 225, 228; Hölters, AktG, § 93 Rn. 162; zur Post-Closing Due Diligence siehe auch → Rn. 93 f.

107 Spindler, in: MünchKomm-AktG, § 93 Rn. 83.

108 BGH, Urt. v. 29.3.1996, V ZR 332/94, NJW 1996, 1884, 1885; Göthel, in: Göthel, Grenz-überschreitende M&A-Transaktionen, § 2 Rn. 93.

109 Geyrhalter/Zirngibl/Strehle, DStR 2006, 1559, 1562.

110 Göthel, in: Göthel, Grenzüberschreitende M&A-Transaktionen, § 2 Rn. 25.

111 Liese/Theusinger, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 27 Rn. 19.

denen Erwerbsabsicht verwechselt werden darf und grundsätzlich keine Haftung auslöst. Zu einer Haftung kann es aber dann kommen, wenn nicht nur eine Abschlussbereitschaft signalisiert wird, sondern darüber hinaus der Eindruck erweckt wird, dass es mit Sicherheit zu einem Vertragsabschluss kommen wird, anschließend die Verhandlungen aber dessen ungeachtet ohne triftigen Grund abgebrochen werden.¹¹² Die Haftung setzt dabei nicht voraus, dass sich die Parteien bereits über sämtliche Punkte des Vertrags geeinigt hatten, kommt aber umso eher in Betracht, je weiter die Verhandlungen bereits gediehen waren.¹¹³ An die Annahme eines wichtigen Grundes, der den Abbruch von Vertragsverhandlungen zu rechtfertigen vermag, dürfen indes keine hohen Anforderungen gestellt werden. Jede vernünftige Erwägung genügt für einen legitimen Abbruch der Verhandlungen.¹¹⁴ Beispiele sind das bessere Angebot eines anderen Interessenten, eine Verschlechterung der Geschäftschancen der Zielgesellschaft, die es nahelegt, von dem beabsichtigten Geschäft Abstand zu nehmen, oder der Umstand, dass sich der andere Vertragspartner dem begründeten Verdacht der Korruption in Zusammenhang mit dem intendierten Vertragsabschluss ausgesetzt hat.¹¹⁵

Die vorstehenden Ausführungen gelten dabei nur eingeschränkt bei beurkundungsbedürftigen Verträgen. Denn das Gesetz behält den Vertragsparteien bis zur Beurkundung die volle Entscheidungsfreiheit vor, da dem Schutzzweck des Formerfordernisses nur Rechnung getragen werden kann, wenn auch kein indirekter Zwang zur Vornahme des beurkundungsbedürftigen Geschäfts besteht.¹¹⁶ Lediglich in Fällen einer vorsätzlichen Treupflichtverletzung kommt eine Haftung wegen des Abbruchs der Verhandlungen über einen beurkundungsbedürftigen Vertrag in Betracht. Denn allein die Formbedürftigkeit eines Vertrages gibt einer Partei noch kein Recht zu illoyalem Verhalten gegenüber dem Verhandlungspartner.¹¹⁷ Ein Beurkundungserfordernis ergibt sich bei vielen M&A-Transaktionen, z. B. im Fall der Abtretung von Geschäftsanteilen einer GmbH (§ 15 Abs. 3 GmbHG) und bei der Veräußerung (nahezu) des gesamten Vermögens einer Gesellschaft (§ 311b Abs. 3 BGB).

Die bewusste und gewollte Vorspiegelung falscher Tatsachen, die zu einer Vermögensverfügung führt, kann auch strafrechtlich relevant sein (§ 263 Abs. 1 StGB); ggf. in Form eines Versuchs, wenn kein Vermögensschaden eingetreten ist (§§ 263 Abs. 1 und 2, 22, 23 Abs. 1 Var. 2 StGB). In Betracht kommt insofern

112 St. Rspr., BGH, Urt. v. 8.6.1978, III ZR 48/76, NJW 1979, 1802, 1804; BGH, Urt. v. 7.2.1980, III ZR 23/78, NJW 1980, 1683, 1684; BGH, Urt. v. 9.11.2012, V ZR 182/11, NJW 2013, 928 Rn. 7 f.; *Emmerich*, in: MünchKomm-BGB, § 311 Rn. 195.

113 *Emmerich*, in: MünchKomm-BGB, § 311 Rn. 193.

114 BGH, Urt. v. 10.1.1996, VIII ZR 327/94, DtZ 1996, 113, 114; *Emmerich*, in: MünchKomm-BGB, § 311 Rn. 195.

115 *Emmerich*, in: MünchKomm-BGB, § 311 Rn. 195.

116 BGH, Urt. v. 20.1.1987, 4 U 22/86, NJW-RR 1987, 801.

117 BGH, Urt. v. 20.1.1987, 4 U 22/86, NJW-RR 1987, 801; BGH, Urt. v. 9.11.2012, V ZR 182/11, NJW 2013, 928.

beispielsweise die Vorspiegelung einer tatsächlich nicht vorhandenen Abschlussbereitschaft (dazu bereits → Rn. 54). Aber auch Angaben betreffend die Zielgesellschaft oder die Behauptung, es befänden sich weitere Bieter im Auktionsverfahren, kommen insofern in Betracht. Wenngleich strafrechtlichen Bestimmungen in regulär verlaufenden Transaktionen keine große praktische Bedeutung zukommt, ist auch zu bedenken, dass eine Strafanzeige aus Sicht eines Erwerbers, der mit seinem Investment unzufrieden ist und sich betrogen fühlt, ein Mittel zur Informationsgewinnung sein kann. Mitunter wird zur Vorbereitung eines späteren zivilgerichtlichen (Schieds-)Verfahrens versucht, die Arbeit der – zur Amtsermittlung verpflichteten und mit behördlichen Befugnissen versehenen – Staatsanwaltschaft zur „Sachverhaltsaufbereitung“ fruchtbar zu machen. Auch ein frustrierter und sich betrogen fühlender Erwerber wird sich allerdings gut überlegen müssen, ob er wirklich die Staatsanwaltschaft einschalten will. Denn M&A-Transaktionen sind für die meisten Unternehmen keine singulären Ereignisse und mit einer Involvierung der Staatsanwaltschaft wird man Gefahr laufen, den eigenen Ruf als verlässlicher Vertragspartner zu riskieren, wenn nicht tatsächlich ganz massive Anhaltspunkte für betrugsrelevante Sachverhalte vorliegen.

7. Zustimmungserfordernisse

- 57 Eine M&A-Transaktion kann Gegenstand einer Vielzahl potenzieller Zustimmungserfordernisse sein, die unterschiedlichsten Rechtsgebieten entspringen können, insbesondere dem Gesellschaftsrecht, dem öffentlichen Recht und dem Familien- und Erbrecht (auch die kartellrechtliche Freigabe kann man hierunter fassen, die jedoch unter → Rn. 26 ff. separat behandelt wurde).¹¹⁸ Um die erforderlichen Zustimmungen rechtzeitig zu erhalten, sollten etwaige Zustimmungsvorbehalte möglichst früh ermittelt werden.¹¹⁹
- 58 Nachfolgend sollen lediglich zwei erfahrungsgemäß besonders praxisrelevante Zustimmungserfordernisse in der gebotenen Kürze näher beleuchtet werden, nämlich gesellschaftsrechtliche Zustimmungserfordernisse und das Erfordernis der Zustimmung von Ehegatten und gleichgeschlechtlichen Lebenspartnern i. S. d. Lebenspartnerschaftsgesetzes.

a) Zustimmung von Aufsichtsgremien und/oder der Gesellschafter

- 59 Oft wird eine M&A-Transaktion jedenfalls ab einem bestimmten Volumen der Zustimmung der Gesellschafterversammlung, der Hauptversammlung und/oder eines Aufsichts- oder Beirats bedürfen. Ein solches Erfordernis kann sich aus dem Gesetz, der Satzung oder einer Geschäftsordnung für den Vorstand bzw. die Geschäftsführer ergeben. Ein gesetzliches Erfordernis wird dabei für die AG ins-

118 Vgl. die ausführliche Checkliste bei *Seibt*, in: *Seibt*, Beck'sches Formularbuch Mergers & Acquisitions, A. III., 17 ff., sowie *Beisel*, in: *Beisel/Klump*, Unternehmenskauf, § 8.

119 *Liese/Theusinger*, in: *Hauschka/Moosmayer/Lösler*, Corporate Compliance, § 27 Rn. 11.

besondere aus § 179a AktG resultieren, soweit eine Veräußerung (nahezu) des ganzen Vermögens erfolgt. Auch bei Verbleib erheblichen Anlagevermögens ist die Vorschrift anzuwenden, wenn bisherige Unternehmensziele nicht weiter verfolgt werden können.¹²⁰ Darüber hinaus kann nach der sog. Holzmüller-Rechtsprechung des BGH eine ungeschriebene Zustimmungspflicht der Hauptversammlung einer AG bestehen, wenn eine M&A-Transaktion die Mitgliedschaftsrechte der Aktionäre ganz wesentlich beeinträchtigt (sog. „Mediatisierungseffekt“).¹²¹ Die Einzelheiten sind umstritten, aber man wird ab einer Veräußerung von 80 % des Gesellschaftsvermögens von einer entsprechenden Zustimmungspflicht ausgehen dürfen. Im Einzelfall – etwa der Veräußerung des wertvollsten Unternehmensteils – kann eine ungeschriebene Hauptversammlungskompetenz aber auch bei Werten unterhalb dieser Schwelle entstehen.¹²² Erwerbsvorgänge fallen nach herrschender Auffassung hingegen nicht in die Kompetenz der Hauptversammlung des Erwerbers, sondern sind dem Vorstand zugewiesene Maßnahmen der Vermögensverwendung.¹²³

Eine analoge Anwendung des § 179a Abs. 1 Satz 1 AktG auf die GmbH hat der BGH hingegen im Jahr 2019, entgegen der wohl herrschenden Meinung in der Literatur, abgelehnt.¹²⁴ Ein Zustimmungserfordernis der Gesellschafterversammlung ergibt sich, soweit es sich um ein bedeutsames Geschäft handelt, hingegen aus § 49 Abs. 2 GmbHG. Hiernach ist die Gesellschafterversammlung einzuberufen, wenn es im Interesse der Gesellschaft erforderlich scheint, was bei einer Veräußerung wesentlicher Anteile stets zutrifft. Auch aus dem Gesellschaftsvertrag ergibt sich, als ungeschriebene Vorlagepflicht gem. § 37 Abs. 1 GmbHG, ein Zustimmungserfordernis. Den Beschluss der Gesellschafterversammlung hat der Geschäftsführer dann selbstständig herbeizuführen.¹²⁵

Aus Sicht der handelnden Organe sollte bereits bei Einleitung des M&A-Prozesses ein (Grundsatz-)Beschluss der Gesellschafter (im Fall der GmbH) bzw. des Aufsichtsrats (im Fall der AG) hinsichtlich der Transaktion herbeizuführen sein. Dies ist aus Sicht des handelnden Organs (Geschäftsführung, Vorstand) auch zur

120 *Beisel*, in: *Beisel/Klump*, Unternehmenskauf, § 8 Rn. 70.

121 BGH, Urt. v. 25.2.1982, II ZR 174/80, DB 1982, 795; statt vieler: *Beisel*, in: *Beisel/Klump*, Unternehmenskauf, § 8 Rn. 80 f.

122 *Beisel*, in: *Beisel/Klump*, Unternehmenskauf, § 8 Rn. 80 f., 83.

123 OLG Frankfurt, Urt. v. 7.12.2010, 5 U 29/10, ZIP 2011, 75; zusammenfassend *Beisel*, in: *Beisel/Klump*, Unternehmenskauf, § 8 Rn. 82 m. w. N., auch zur a. A.

124 BGH, Urt. v. 8.1.2019 – II ZR 364/18, GmbHR 2019, 528; ausführliche Besprechung: *Müller*, NZG 2019, 807. Dem Argument der Literatur, die Gesellschafter einer GmbH seien in gleicher Weise schutzwürdig wie Aktionäre, tritt das Gericht entgegen, und verweist auf die erheblich einflussreichere Stellung eines GmbH-Gesellschafters gegenüber der Geschäftsführung im Vergleich zur AG. Ferner betont das Gericht, dass es sich mit Blick auf die Rechtfolge des § 179a AktG nicht um eine verallgemeinerungsfähige Norm i. S. e. Prinzip des Verbandsrechts handle. Die Gegenansicht berücksichtige nur unzureichend die Kollision mit dem tragenden handelsrechtlichen Prinzip, wonach Geschäftsleiter von Handelsgesellschaften im Außenverhältnis grds. unbeschränkbare Vertretungsmacht inne hätten.

125 BGH, Urt. v. 8.1.2019 – II ZR 364/18, GmbHR, 2019, 528, 533 f.

Vermeidung der eigenen Haftung empfehlenswert.¹²⁶ Insbesondere deshalb weil entgegen der eigenen Verschwiegenheitspflicht des Organs möglicherweise in erheblichem Umfang vertrauliche Informationen offengelegt werden¹²⁷ und zudem durch den M&A-Prozess erhebliche Kosten entstehen können, die eine vorbehaltene Maßnahme darstellen könnte. Letzteres ist auch im Fall des Erwerbers bedeutsam. Erwerbsnebenkosten (etwa für die Due Diligence), die leicht sechsstellige Beträge erreichen, können bereits allein aufgrund ihrer Höhe – d. h. ungeachtet sonstiger spezieller Zustimmungserfordernisse für M&A-Transaktionen – eine Zustimmungspflicht der Gesellschafterversammlung nach der Satzung oder Geschäftsordnung des Erwerbers auslösen. Zudem besteht das Risiko auf Erwerberseite aus der Transaktion aufgrund des fehlenden Gesellschaftsbeschlusses keine vertraglichen Rechte und Einwendungen herleiten zu können.

- 62** In der AG wirkt sich die Unwirksamkeit im Innenverhältnis aufgrund eines fehlenden Beschlusses, mit dem einer Übertagung (im Wesentlichen) des Ganzen Vermögens gem. § 179a AktG zugestimmt wird, immer auch auf das Außenverhältnis aus. Für die GmbH sieht § 37 Abs. 2 Satz 1 GmbHG zwar einen Verkehrsschutz vor und die Beschränkung der Geschäftsführerbefugnis (hier durch den erforderlichen Gesellschafterbeschluss) entfaltet keine Wirkung gegenüber Dritten. Dieser Verkehrsschutz wirkt aber nur gegenüber demjenigen, der auch schutzbedürftig ist. Ein bösgläubiger Geschäftspartner kann sich nicht auf die Unwirksamkeit im Außenverhältnis berufen. Das Vertrauen des Geschäftspartners auf den Bestand des Geschäfts ist hierbei nach der Rechtsprechung des BGH als nicht schutzwürdig einzustufen, wenn es sich diesem geradezu aufdrängen müsse, dass der Geschäftsführer seine Vertretungsmacht missbrauche; ohne Einfluss sei hingegen, ob der Geschäftsführer zum Nachteil der Gesellschaft handle.¹²⁸
- 63** Zu trennen von der Frage der Erforderlichkeit eines Zustimmungsbeschlusses, ist die Frage der erforderlichen Form dieses Beschlusses. Nahm die herrschende Meinung vor dem Urteil des BGH aus dem Jahr 2019 eine Beurkundungspflicht auch für GmbHs an,¹²⁹ so ist diesem Ansatz – soweit die Herleitung auf einer analogen Anwendung des § 179a AktG (i.V.m. § 130 AktG) beruhte – durch das

126 Zu den Risiken eines fehlenden Beschlusses: BGH, Urt. v. 8.1.2019 – II ZR 364/18, GmbHR, 2019, 528, 534.

127 So die entsprechende Empfehlung bei *Seibt*, in: *Seibt, Beck'sches Formularbuch Mergers & Acquisitions*, Anm. 1 zu B.I.1, 35; für ein Muster eines entsprechenden Grundsatzbeschlusses *Seibt*, in: *Seibt, Beck'sches Formularbuch Mergers & Acquisitions*, 3. Aufl. 2018, B.IX. 3, 178 ff.

128 BGH, Urt. v. 8.1.2019 – II ZR 364/18, GmbHR, 2019, 528, 534; BGH, Hinweisbeschluss v. 10.4.2006 – II ZR 337/05, NZG 2006, 626, 627.

129 *Weitnauer*, GWR 2018, 3 f. mit zusammenfassendem Verweis auf *Priester*, in: *Scholz, GmbHG*, 11. Aufl. 2014, § 53 Rn. 176.

Urteil die Grundlage entzogen worden.¹³⁰ Jedoch gab es auch vor Ablehnung der Analogie bereits andere Ansätze, die Beurkundungspflicht zu begründen.¹³¹

So konzentriert sich die Diskussion um die Beurkundungspflicht von Gesellschafterbeschlüssen, mit denen der Veräußerung des (im Wesentlichen) gesamten Vermögens einer GmbH zugestimmt wird, nunmehr auf die Frage, ob bereits durch den Beschluss eine (faktische) Satzungsänderung vorliegt, die zu einer Anwendung des § 53 Abs. 2 GmbHG (analog) führt.¹³² Der BGH befasste sich in seinem Urteil mit dieser Frage nicht. Er äußerte sich weder zur Beurkundungspflicht des Beschlusses noch zu seinem Charakter als gegebenenfalls satzungsdurchbrechend in Bezug auf den Unternehmensgegenstand. Nach hier vertretener Auffassung stellt der Beschluss allein, auch über den Verkauf des gesamten Gesellschaftsvermögens, für sich noch keine Satzungsänderung dar.¹³³

64

Eine Beurkundungspflicht wird weiterhin auch auf die wesentliche Bedeutung des Beschlusses für das Unternehmen gestützt.¹³⁴ Die Ableitung einer Beurkundungspflicht aus der Rechtsprechung in Sachen Holzmüller/Gelatine geht jedoch fehl. Zum einen weist der BGH bezüglich des Beschlussbedürfnisses auf die Beschränkung der Geschäftsführungsbefugnis aus § 37 Abs. 1 GmbHG hin und begründet ein Zustimmungserfordernis (aber keine Beurkundungspflicht) bereits aus § 49 Abs. 2 GmbHG im Falle einer fehlenden Regelung oder Beschränkung in der Satzung aufgrund der Bedeutung des Geschäfts.¹³⁵ Zum anderen lässt sich aus der Holzmüller/Gelatine-Rechtsprechung nur die Erforderlichkeit eines Beschlusses und nicht seine Form ableiten.¹³⁶

65

Die analoge Anwendung des § 53 Abs. 2 GmbHG auf einer Veräußerung des (im Wesentlichen) ganzen Vermögens zustimmende Gesellschafterbeschlüsse wird mit dem Charakter des Beschlusses als faktische Satzungsänderung begründet.¹³⁷ Jedoch ist hier genau zu differenzieren, inwieweit die Veräußerung von einem wesentlichen Teil oder dem gesamten Gesellschaftsvermögen noch vom

66

130 So noch vor dem Urteil des BGH, *Harbarth*, in: MünchKomm-GmbHG, 3. Aufl. 2018, § 53 Rn. 229 mit Verweis auf *Priester*, in: Scholz, GmbHG, 11. Aufl. 2014, § 53 GmbHG Rn. 176.

131 *Schnorbus*, in: Rowedder/Schmidt-Leithoff, GmbHG, § 53 GmbHG Rn. 25.

132 *Müller*, NZG 2019, 807, 812; so bereits einige Stimmen vor der Entscheidung des BGH: vgl. *Müller*, NZG 2019, 807, 811.

133 So die allg. Auffassung: *Noack*, in: Noack/Servatius/Haas/Noack § 53 Rn. 26, auch vor dem Urteil des BGH: *Harbarth*, in: MünchKomm-GmbHG, 3. Aufl. 2018, § 53 Rn. 230; *Altmep-pen*, in: Roth/Altmep-pen, GmbHG, 9. Aufl. 2019, § 53 Rn. 18, *Schnorbus*, in: Rowedder/Schmidt-Leithoff, GmbHG, § 53 GmbHG Rn. 25.

134 Vgl. *Decker*, NZG 2018, 447, 449; *Altmep-pen*, in: Altmep-pen, GmbHG, 11 § 53 Rn. 18.

135 BGH, Urt. v. 8.1.2019 – II ZR 364/18, GmbHR 2019, 528, 533 f.

136 *Decker*, NZG 2018, 447, 449.

137 *Heckschen*, AG 2019, 420, 422; *Trölitzsch*, in: BeckOK GmbHG, 58. Ed. 1.11.2023, § 53 Rn. 8.3 m. w. N.

bisherigen Unternehmensgegenstand gedeckt ist oder nicht.¹³⁸ Nur in dem Fall, dass der Unternehmensgegenstand die Veräußerung nicht umfasst oder aber dieser durch die Veräußerung nicht mehr verfolgt werden kann, kann eine faktische Satzungsänderung überhaupt erwogen werden. Es bleiben darüber hinaus berechnete Zweifel, ob für eine Analogie in diesen Fällen ausreichend Raum besteht. Der Annahme einer planwidrigen Regelungslücke kann entgegengehalten werden, dass der Schutzzweck des § 53 Abs. 2 GmbHG dadurch erfüllt ist, dass das Vollzugsgeschäft als tatsächliche und nicht bloß faktische Satzungsänderung zu einem späteren Zeitpunkt beurkundet wird.¹³⁹ Durch den vorherigen Beschluss allein werden noch keine Gesellschafterrechte so stark betroffen sein, dass die Schutz- und Warnfunktion der notariellen Beurkundung notwendig erscheint und der Beschluss stellt noch nicht sicher, dass die Veräußerung am Ende auch durchgeführt wird.

- 67 Eine Tendenz im Schrifttum zur Beurkundungsbedürftigkeit des Beschlusses lässt sich folglich nicht erkennen.¹⁴⁰ Vielmehr wird allein auf die satzungsändernde Wirkung des Beschlusses verwiesen. Solange diese bloß faktisch wirkt, ist eine Beurkundungspflicht schwer zu begründen. Als Vorsichtsmaßnahme¹⁴¹ muss die Beurkundung mit den entstehenden Kosten abgewogen werden. Umfasst der Unternehmensgegenstand hingegen auch die Veräußerung des Gesellschaftsvermögens oder kann dieser weiterhin verfolgt werden, erscheint die Beurkundung auch aus dieser Perspektive nicht erforderlich.

b) Zustimmung von Ehegatten oder Lebenspartnern

- 68 Soweit ein Veräußerer im gesetzlichen Güterstand der Zugewinnngemeinschaft oder der Gütergemeinschaft lebt, bedarf die Veräußerung (nahezu)¹⁴² des Vermögens im Ganzen der Zustimmung des Ehegatten (§ 1365 Abs. 1 Satz 1 BGB bei Zugewinnngemeinschaft, § 1423 Satz 1 BGB bzw. §§ 1419 Abs. 1, 1422 ff., 1450 ff. BGB bei Gütergemeinschaft) bzw. des gleichgeschlechtlichen Lebenspartners (§§ 6 und 7 LPartG i.V.m. den für die Zugewinn- bzw. Gütergemeinschaft einschlägigen Normen des BGB). Insbesondere das Zustimmungserfordernis für Lebenspartner i. S. d. LPartG wird in der Praxis häufig übersehen. Da der Zweck der einschlägigen Normen ist, die materiellen Grundlagen der Ehe bzw. Lebenspartnerschaft in ihrem Bestand zu schützen, bestehen diese Zustim-

138 Decker, NZG 2018, 447, 450 ff. und DNotI-Report 2019, 193, 194 mit jew. differenzierten Abgrenzungskriterien zur Beurteilung.

139 So wohl auch Decker, NZG 2018, 447, 450 f., Keller, NJW-Spezial 2019, 271, 272 differenzierend zwischen Beschluss und tatsächlicher Satzungsänderung.

140 So aber DNotI-Report 2019, 193, 195 mit einzigem Verweis auf Bayer, in: Lutter/Hommelhoff, GmbHG, § 53 Rn. 3.

141 DNotI-Report 2019, 193, 196: vorsorgliche Beurkundung in Holzmüller/Gelatine Fällen.

142 Siede, in: Grüneberg, BGB, § 1365 Rn. 6 (allg. Meinung).

machungserfordernisse unabhängig davon, ob die Gegenleistung äquivalent zu den veräußerten Gesellschaftsanteilen ist.¹⁴³

Um nicht die Vermögensverhältnisse eines Veräußerers ausforschen zu müssen, empfiehlt es sich in der Praxis, Zustimmungserklärungen losgelöst von den (vermeintlichen) Vermögensverhältnissen und damit der Frage einer Veräußerung (nahezu) des gesamten Vermögens immer dann einzuholen, wenn natürliche Personen Veräußerer sind. Sollte das im Einzelfall nicht in Betracht kommen – etwa weil die Ehegatten oder Lebenspartner zerstritten sind –, muss die Vermögenslage des Veräußerers näher analysiert werden, was z. B. anhand eines vom Steuerberater erstellten Vermögensstatus geschehen kann. **69**

Die Einwilligung kann grundsätzlich formlos erklärt werden.¹⁴⁴ Zu Beweiszw- **70**
ecken empfiehlt es sich jedoch, eine schriftliche Erklärung einzuholen, die als Anlage zum Unternehmenskaufvertrag genommen wird. In inhaltlicher Hinsicht ist zu beachten, dass sich die Einwilligung des Ehegatten oder gleichgeschlechtlichen Lebenspartners auf den Mindestinhalt des konkreten Rechtsgeschäfts des konkret anstehenden Geschäfts beziehen muss („essentialia negotii“; bei einem Kaufvertrag in der Regel Kaufsache, Kaufpreis und Vertragspartner).¹⁴⁵ Andernfalls könnte die Einwilligung als Generaleinwilligung einzustufen sein, die – als Ausnahme vom Grundsatz der Formfreiheit – jedenfalls dann der notariellen Niederschrift bedarf, wenn sie unwiderruflich erklärt wird (§§ 1413, 1410 BGB).¹⁴⁶ Eine Unwiderruflichkeit bietet sich regelmäßig deshalb an, weil die Einwilligung ansonsten vor Unterzeichnung oder Vollzug des Unternehmenskaufvertrags jederzeit widerrufen werden könnte.¹⁴⁷ Wurde der Widerruf abbedungen, ist die Einwilligung nur noch aus wichtigem Grund widerrufbar.¹⁴⁸ Vor diesem Hintergrund empfiehlt es sich, die Einwilligung zwar unwiderruflich auszugestalten, sie jedoch erst zu einem Zeitpunkt einzuholen, in dem die essentialia negotii – insbesondere der Kaufpreis – bereits feststehen. Es ist allerdings nicht erforderlich, dass die essentialia negotii auch ausdrücklich in der Erklärung genannt werden, um eine Einstufung als Generaleinwilligung zu vermeiden.¹⁴⁹

143 *Siede*, in: Grüneberg, BGB, § 1365 Rn. 6; die Höhe der Gegenleistung spielt aber für die Frage eine wichtige Rolle, ob eine etwaige Verweigerung berechtigt war und die fehlende Zustimmung gerichtlich ersetzt werden kann, *Siede/Cziupka*, in: Bamberger/Roth/Hau/Poseck, BGB, 4. Aufl. 2019, § 1365 Rn. 31.

144 *Siede/Cziupka*, in: Bamberger/Roth/Hau/Poseck, BGB, 4. Aufl. 2019, § 1365 Rn. 23.

145 *Siede/Cziupka*, in: Bamberger/Roth/Hau/Poseck, BGB, 4. Aufl. 2019, § 1365 Rn. 23 a. E.

146 *Siede*, in: Grüneberg, BGB, § 1365 Rn. 15.

147 Unter Umständen kann sich ein redlicher Geschäftspartner aber auf den Schutz der §§ 170 ff. BGB berufen, *Siede/Cziupka*, in: Bamberger/Roth/Hau/Poseck, BGB, 4. Aufl. 2019, § 1365 Rn. 24 m. w. N.

148 *Bayreuther*, in: MünchKomm-BGB, § 183 Rn. 16.

149 Ob die Erklärung die essentialia negotii abdeckt, ist in diesem Fall durch Auslegung zu ermitteln, *Siede/Cziupka*, in: Bamberger/Roth/Hau/Poseck, BGB, 4. Aufl. 2019, § 1365 Rn. 23 m. w. N.

8. Vereinbarung von Wettbewerbsverboten im Unternehmenskaufvertrag

- 71 Wettbewerbsverbote sind als den Wettbewerb beschränkende Abreden grundsätzlich unzulässig (Art. 101 AEUV, § 1 GWB). Im Zusammenhang mit der Veräußerung eines Unternehmens können dem Veräußerer jedoch in kartellrechtlich zulässiger Weise vertraglich vereinbarte Wettbewerbsverbote auferlegt werden.¹⁵⁰ Das Bedürfnis für und die Zulässigkeit derartiger Wettbewerbsverbote ergeben sich daraus, dass der Erwerber zumindest in gewissem Umfang vor Wettbewerb durch den Veräußerer geschützt werden muss, damit er den vollständigen Wert der Zielgesellschaft bzw. der veräußerten Vermögensgegenstände erhält.¹⁵¹ Denn aufgrund seines Know-hows und seiner Kundenbeziehungen wäre es dem Veräußerer in vielen Transaktionen ein Leichtes, innerhalb kurzer Zeit ein Konkurrenzunternehmen aufzubauen und so den wirtschaftlichen Erfolg der Transaktionen zu torpedieren.
- 72 Voraussetzung für die Zulässigkeit entsprechender Wettbewerbsverbote ist allerdings, dass sie sachlich, räumlich und zeitlich auf das zur Durchführung des Vertragszwecks erforderliche Maß begrenzt sind.¹⁵² In sachlicher Hinsicht ist dies der Fall, wenn das Wettbewerbsverbot auf diejenigen Waren und Dienstleistungen beschränkt ist, die Geschäftsgegenstand der Zielgesellschaft sind.¹⁵³ In zeitlicher Hinsicht gilt, dass Wettbewerbsverbote für eine Dauer von bis zu drei Jahren gerechtfertigt sind, wenn – neben Vermögensgegenständen und Goodwill – auch Know-how übertragen wird.¹⁵⁴ Wird zwar kein Know-how, aber – neben Vermögensgegenständen – zumindest auch Goodwill übertragen, soll eine Dauer von zwei Jahren zulässig sein.¹⁵⁵ Werden hingegen ausschließlich materielle Vermögensgegenstände und/oder gewerbliche Schutzrechte (nicht aber Know-how oder Goodwill) übertragen, ist es zweifelhaft, ob überhaupt ein Wettbewerbsverbot vereinbart werden darf.¹⁵⁶ In diesem Fall dürfte der Erwerber kein schützenswertes Interesse daran haben, die übertragenen Maschinen, Grund-

150 *Badtke*, KSzW 2011, 418, 422 m. w. N.; *Baron/Trebing*, BB 2016, 131, 133 m. w. N.

151 *Badtke*, KSzW 2011, 418, 422.

152 *Badtke*, KSzW 2011, 418, 423 m. w. N.

153 Vgl. Bekanntmachung der KOM über Einschränkungen des Wettbewerbs, die mit der Durchführung von Unternehmenszusammenschlüssen unmittelbar verbunden und für diesen notwendig sind, ABl. 2005 C 56/03, Rn. 18; *Badtke*, KSzW 2011, 418, 423.

154 Vgl. Bekanntmachung der KOM über Einschränkungen des Wettbewerbs, die mit der Durchführung von Unternehmenszusammenschlüssen unmittelbar verbunden und für diesen notwendig sind, ABl. 2005 C 56/03, Rn. 20; *Badtke*, KSzW 2011, 418, 423.

155 KOM v. 12.4.1999, IV/M.1482 Rn. 26 – *Kingfisher/Großlabor*; KOM v. 14.12.1997, IV/M.884, Rn. 17 – *KNP BT/Bunzl*; Bekanntmachung der KOM über Einschränkungen des Wettbewerbs, die mit der Durchführung von Unternehmenszusammenschlüssen unmittelbar verbunden und für diesen notwendig sind, ABl. 2005 C 56/03, Rn. 20; *Badtke*, KSzW 2011, 418, 423.

156 Vgl. Bekanntmachung der KOM über Einschränkungen des Wettbewerbs, die mit der Durchführung von Unternehmenszusammenschlüssen unmittelbar verbunden und für diesen notwendig sind, ABl. 2005 C 56/03, Rn. 21; *Badtke*, KSzW 2011, 418, 423.

stücke oder gewerblichen Schutzrechte frei von Wettbewerb zu nutzen. Denn in der Regel gewähren sie bereits nach dem Gesetz ihrem Eigentümer bzw. Inhaber das Recht zur ausschließlichen Nutzung und ihr Wert kann nicht durch die Nutzung anderer vergleichbarer Wirtschaftsgüter (die nicht mitveräußert wurden) durch den Veräußerer torpediert werden. In räumlicher Hinsicht sollten sich Wettbewerbsverbote auf das Gebiet beschränken, in denen die Zielgesellschaft ihre Waren oder Dienstleistungen anbietet oder anzubieten plant, wobei es nach der EU-Kommission in diesem Fall erforderlich sein soll, dass bereits Investitionen für die geplante Expansion getätigt wurden.¹⁵⁷

III. Materielle M&A-Compliance – Prüfung von/Umgang mit Compliance in der Zielgesellschaft

1. Due Diligence

a) Erfordernis einer Compliance-Due Diligence

aa) Einführung unter besonderer Beachtung von ESG/CSR

Neben dem Begriff der Compliance-Due Diligence, also der Überprüfung der Einhaltung rechtlicher Regeln durch die Zielgesellschaft, erfahren in jüngerer Zeit auch die Begriffe ESG (Environmental, Social, Governance) und CSR (Corporate Social Responsibility) zunehmend Aufmerksamkeit auch und gerade im Kontext von M&A-Transaktionen. **73**

ESG versteht sich als übergeordneter Begriff für nachhaltige Investitionen und Nachhaltigkeitsrisiken im Zusammenhang mit Finanzinvestitionen, ohne jedoch einer präzisen gesetzlichen Bestimmung oder gar Definition zu unterliegen.¹⁵⁸ Große institutionelle Investoren stellen die Relevanz solcher Faktoren durch die Aufnahme in ihre Veröffentlichungsanforderungen an Portfolio-Gesellschaften heraus und verstehen ESG in ihren Portfolios als Mittel zur Risikominimierung.¹⁵⁹ In der EU findet auf bestimmte Finanzdienstleister die EU-Taxonomie-Verordnung bzw. die SFDR (Sustainable Finance Disclosure Regulation) Anwendung. Hierunter fallende Investoren sind verpflichtet, über negative ESG-Auswirkungen ihrer Anlagestrategien bzw. Kriterien zur Bewertung der ökologischen Nachhaltigkeit von Wirtschaftstätigkeiten zu berichten. **74**

CSR-Anforderungen bilden ein Normsystem, das Lücken zwischen Völkerrecht und nationalem Recht schließen will, um z. B. die Ausbeutung von Drittländern unter Missachtung von Sozial- und Umweltstandards zu verhindern.¹⁶⁰ Als **75**

¹⁵⁷ Vgl. Bekanntmachung der KOM über Einschränkungen des Wettbewerbs, die mit der Durchführung von Unternehmenszusammenschlüssen unmittelbar verbunden sind und für diesen notwendig sind, ABl. 2005 C 56/03, Rn. 22; *Badtke*, KSzW 2011, 418, 423.

¹⁵⁸ *Eberius*, WM 2019, 2143, 2143.

¹⁵⁹ *Watchell, Lipton, Rosen & Katz*, ESG Memo: The Coming Impact of ESG on M&A, 18.2.2020, <https://www.wlrk.com/webdocs/wlrknew/ClientMemos/WLRK/WLRK.26787.20.pdf> (zuletzt abgerufen am 14.4.2024).

¹⁶⁰ *Spießhofer*, NZG 2018, 441, 443. Siehe ferner → *Stehr/Knopp*, Kap. 15.

Oberbegriff versteht sich CSR auch als Konzeption, die Ausprägungen in Unternehmenszielbestimmungen, der Business Judgment Rule (siehe dazu → Rn. 84 f.), dem DCGK und den oben bereits behandelten ESG-Kriterien findet.¹⁶¹

- 76 Durch das CSR-Richtlinien-Umsetzungsgesetz wurden CSR- und ESG-Aspekte in § 289b HGB aufgenommen. Kapitalmarktorientierte Unternehmen, Banken und Versicherungen (börsenorientiert und mehr als 500 Mitarbeiter) werden hierdurch verpflichtet, in ihre Lageberichte auch nichtfinanzielle Erklärungen abzugeben.¹⁶² Diese unterliegen dann, auch wegen ihrer erheblichen wirtschaftlichen Risikobehaftung durch Reputationsverlust bei Nichteinhaltung,¹⁶³ häufig auch einer Prüfung im Zusammenhang mit der Due Diligence. Darüber hinaus trat am 1.1.2023 das Lieferkettensorgfaltspflichtengesetz (LkSG) für Unternehmen mit einer Mitarbeiteranzahl von mindestens 3.000 Personen (seit 1.1.2024 mindestens 1.000 Personen) in Kraft.¹⁶⁴
- 77 In Due Diligence-Prüfungen rücken insbesondere die risikobezogenen ESG/CSR-Faktoren in den Fokus, beispielsweise der Umgang mit Korruption, Privatsphäre und Datensicherheit, Klimawandel, Treibhausgasemissionen, Diversität und Arbeitsbedingungen.¹⁶⁵ Diese Aufzählung zeigt bereits eine große Schnittmenge mit anderen Bereichen der (Compliance-)Due Diligence und verdeutlicht die fehlende Trennschärfe der Begrifflichkeiten: Inwieweit die unter ESG/CSR gefassten Anforderungen über eine übliche Compliance hinausgehen, muss auch vom jeweiligen Bezugsraum abhängig gemacht werden. So kann im europäischen Rechtsraum durchaus davon ausgegangen werden, dass jedenfalls CSR-Standards im engeren Sinne vielfach nicht über den bereits bestehenden Rechtsrahmen hinausgehen oder aber (wie z. B. durch die CSR-Richtlinie) bereits umgesetzt sind.¹⁶⁶
- 78 Es wird erwartet, dass die ESG-Performance zukünftig einen wesentlichen Einfluss auf die Unternehmensbewertung haben wird.¹⁶⁷ Da die Validierung des indikativen Kaufpreises eine der Kernaufgaben der Due Diligence ist, deutet dies in der Tat auf eine zunehmende Bedeutung der ESG-Due Diligence hin.
- 79 Soweit mitunter auch von einer „Integrity-Due Diligence“ die Rede ist, wird dieser Begriff teilweise synonym mit dem der Compliance-Due Diligence verwen-

161 *Spießhofer*, NZG 2018, 441, 445.

162 *Eberius*, WM 2019, 2143, 2152.

163 Siehe umfangreich zu möglichen Risiken: Merkblatt zum Umgang mit Nachhaltigkeitsrisiken, BaFin 13.1.2020, https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/dl_mb_Nachhaltigkeitsrisiken.html (zuletzt abgerufen am 2.2.2024).

164 *Arntzen/Abele*, BB 2023, 2823, 2826. Zum LkSG siehe auch → *Heske*, Kap. 18.

165 *Arntzen/Abele*, BB 2023, 2823; *Roeder/Werthmüller/Havlik*, CCZ 2024, 13. Zum Zusammenhang zwischen CSR und Compliance-Aspekten siehe → *Stehr/Knopp*, Kap. 15.

166 *Spießhofer*, NZG 2018, 441, 444.

167 *Arntzen/Abele*, BB 2023, 2823, 2826; *Roeder/Werthmüller/Havlik*, CCZ 2024, 13.

det.¹⁶⁸ Naheliegender scheint indes ein enges Verständnis, das auf die Integrität der Gesellschafter und/oder Manager der Zielgesellschaft abzielt. So wird z. B. in der Folge des Weinstein-Skandals jedenfalls in den USA im Kontext von M&A-Transaktionen zunehmend um Offenlegung von Informationen über Anschuldigungen sexuellen Missverhaltens gegenüber leitenden Angestellten gebeten (was datenschutzrechtlich nicht immer unproblematisch ist).¹⁶⁹

bb) Erfordernis der Durchführung einer Compliance-Due Diligence

Vor dem Hintergrund, dass eine – nicht in jedem Fall besonders aufwendige (einge- **80**
hend dazu → Rn. 87 ff.) – Compliance-Due Diligence oft noch immer unterbleibt, soll nachfolgend dargestellt werden, weshalb in vielen Fällen die Durchführung einer Compliance-Due Diligence den handelnden Organen des Erwerbers anzuraten ist oder sogar eine entsprechende Pflicht besteht.

Lediglich standardmäßig getroffene Regelungen im Unternehmenskaufvertrag – insbesondere Garantien – reichen regelmäßig nicht zur hinreichenden Absicherung des Erwerbers gegen Risiken aus Compliance-Verstößen aus. So kann der Schaden aus Compliance-Verstößen vereinbarte Haftungshöchstsummen leicht übersteigen.¹⁷⁰ Denn Compliance-Garantien werden in Unternehmenskaufverträgen häufig den operativen Garantien zugeordnet und als solche einer Haftungshöchstgrenze („Cap“) von oft nur 25% des Kaufpreises oder weniger unterworfen (wobei die Vereinbarung eines Caps und dessen Höhe stets Verhandlungssache ist).¹⁷¹ Zudem sind Reputationsschäden,¹⁷² entgangener Gewinn (z. B. aufgrund von Vergabesperrn) und/oder die Kosten für interne Untersuchungen häufig nicht vom Schadensbegriff des Unternehmenskaufvertrags erfasst, da dieser – je nach der Verteilung der Verhandlungsmacht im Einzelfall – auf bestimmte direkte Schäden beschränkt wird und Posten wie interne Kosten oder entgangenen Gewinn ausschließt. Deshalb müssen Compliance-Verstöße durch eine Due Diligence aufgedeckt oder zumindest hinreichend plausibilisiert werden, um in den Vertragsverhandlungen zumindest eine (der Höhe nach nicht begrenzte) Freistellung für damit in Zusammenhang stehende Schäden auf Euro-für-Euro-Basis durchsetzen zu können (sofern nicht weitergehende Maßnahmen zu ergreifen sind, dazu → Rn. 82 ff.). Damit dient eine Compliance-Due-Diligence nicht nur der Absicherung des Erwerbers durch die Ermöglichung **81**

168 Vgl. *Liese*, BB 2010, 27, 28 m. w. N., der die Bezeichnung noch als Oberbegriff für die Compliance-Due Diligence verwendet.

169 *Watchell, Lipton, Rosen & Katz*, ESG Memo: The Coming Impact of ESG on M&A, 18.2.2020, <https://www.wlrk.com/webdocs/wlrknew/ClientMemos/WLRK/WLRK.26787.20.pdf> (zuletzt abgerufen am 14.4.2024).

170 *Liese*, BB 2010, 27, 30. Zu den zahlreichen Nachteilen von Non-Compliance siehe → *Schulz*, Kap. 1 Rn. 6.

171 Eine derartige Haftungshöchstgrenze gilt regelmäßig selbst bei käuferfreundlichen Unternehmenskaufverträgen, vgl. nur *Seibt*, in: *Seibt, Beck'sches Formularbuch Mergers & Acquisitions*, C.II.2 Fn. 113, 450, Anm. 125 zu C.II.1, 317.

172 *Liese*, BB 2010, 27, 30.

einer tatsächlichen Aufdeckung von Compliance-Risiken, sondern u.U. auch der Stärkung der eigenen Verhandlungsposition mit dem Ziel der Vereinbarung einer Freistellung für lediglich vermutete Verstöße.

- 82** Zudem kann es im Fall des Unterlassens einer Compliance-Due Diligence zu einem Verstoß gegen die Legalitätspflicht der (ggf. neuen) Geschäftsleiter der Erwerberin/Zielgesellschaft oder – aufgrund ihrer Konzernleitungspflicht¹⁷³ – sogar der Geschäftsleiter der Konzernobergesellschaft kommen, wenn es in der Zielgesellschaft nach Vollzug der M&A-Transaktion zu fortgesetzten Compliance-Verstößen kommt.¹⁷⁴ In der Rechtsprechung wird mitunter davon ausgegangen, dass eine allgemeine Verpflichtung der Geschäftsleiter zur Einrichtung eines Compliance-Management-Systems aus der Überwachungspflicht bestehe.¹⁷⁵ Nach einem Urteil des OLG Nürnbergs aus dem Jahr 2022 folge aus dieser Überwachungspflicht zudem das Erfordernis einer hinreichenden Kontrolle eines solchen Systems, die nicht erst dann erfolgen dürfe, wenn Missstände tatsächlich entdeckt werden.¹⁷⁶ Sind Tatsachen bekannt, die Verdachtsmomente begründen, haben die Geschäftsleiter nach Ansicht des Gerichts unverzüglich Nachforschungen anzustellen.¹⁷⁷ Ferner seien – nach Maßgabe der Umstände des Einzelfalls – mehr als nur gelegentliche Kontrollen des Compliance-Management-Systems durchzuführen.¹⁷⁸ Neben dieser allgemeinen Überwachungspflicht seien die Geschäftsleiter verpflichtet, dafür Sorge zu tragen, dass auch ohne eine direkte und dauerhafte Kontrolle Compliance-Verstöße unterbleiben.¹⁷⁹
- 83** Gemäß der Literatur muss nach deutschem Recht sichergestellt sein, dass die Geschäfte (unmittelbar) nach Abschluss der Transaktion unter Beachtung aller einschlägigen rechtlichen Voraussetzungen fortgeführt werden.¹⁸⁰ Ein nur schrittweises Abstellen von jeglichem als rechtswidrig erkannten Verhalten sei nicht mit dem Legalitätsprinzip vereinbar.¹⁸¹ In anderen Jurisdiktionen wird dies mitunter großzügiger gesehen und dem Erwerber unter bestimmten Vorausset-

173 Die Einzelheiten einer Konzernleitungspflicht sind umstritten; das LG München I hat in seiner Siemens/Neubürger-Entscheidung (LG München I, 10.12.2013, 5 HK O 1387/10, BB 2014, 850) die Existenz einer Konzernleitungspflicht ohne weitere Begründung unterstellt; vgl. zum Kartellrecht *Baron/Trebing*, BB 2016, 131, 135 m. w. N.

174 *Roeder/Schlutz/Havlik*, CCZ 2023, 269, 270. Für nach Vollzug begangene Kartellrechtsverstöße haftet nach Europäischem Recht – neben der Zielgesellschaft selbst – ab Vollzug auch der Erwerber; und zwar kenntnisunabhängig, *Baron/Trebing*, BB 2016, 131, 134. Zur Legalitätspflicht siehe ferner → *Schulz*, Kap. 1 Rn. 36 ff.

175 OLG Nürnberg, NZG 2022, 1058, 1062; OLG Zweibrücken, NZG 2023, 330, 332; *Roeder/Schlutz/Havlik*, CCZ 2023, 269, 270 f.

176 OLG Nürnberg, NZG 2022, 1058, 1062; *Roeder/Schlutz/Havlik*, CCZ 2023, 269, 271.

177 OLG Nürnberg, NZG 2022, 1058, 1062; *Reuter*, NZG 2023, 322, 324.

178 OLG Nürnberg, NZG 2022, 1058, 1062; *Reuter*, NZG 2023, 322, 324. Zu den Anforderungen an wirksame Compliance-Management-Systeme → *Schulz*, Kap. 1.

179 OLG Nürnberg, NZG 2022, 1058, 1062; *Reuter*, NZG 2023, 322, 324.

180 *Schwarz*, BB 2012, 136, 142.

181 *Schwarz*, BB 2012, 136, 142.

zungen einige Wochen oder Monate Zeit gegeben, um sicherzustellen, dass die Zielgesellschaft etwaige Compliance-Verstöße abstellt.¹⁸²

cc) (Eigen-)Interesse der Geschäftsleitung (Business Judgement Rule)

Überdies sollte die Durchführung einer Compliance-Due Diligence ein ureigenes Interesse der Geschäftsleiter sein: Eine Pflichtverletzung eines Geschäftsleiters liegt nicht vor, wenn er bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf Grundlage angemessener Informationen zum Wohle der Gesellschaft zu handeln (§ 93 Abs. 1 Satz 2 AktG, „Business Judgement Rule“). Bei einer M&A-Transaktion handelt es sich typischerweise um eine solche unternehmerische Entscheidung und das wichtigste Mittel zur Schaffung einer angemessenen Informationsgrundlage ist die Due Diligence. Das Unterlassen einer Compliance-Due Diligence kann dazu führen, dass die Haftungsprivilegierung der Business Judgement Rule nicht in Anspruch genommen werden kann, weil nicht auf angemessener Informationsgrundlage gehandelt wurde.¹⁸³ Die Nichtanwendbarkeit der Business Judgement Rule muss zwar nicht automatisch zu einer Pflichtverletzung führen,¹⁸⁴ verschlechtert aber die haftungsrechtliche Position des Geschäftsleiters erheblich – ein unangenehmes Szenario für jeden Geschäftsleiter; man denke in diesem Zusammenhang nur an den in der Einleitung skizzierten – fiktiven – Fall, dass der Geschäftsbereich, in dem sich der Sachverhalt der Siemens/Neubürger-Entscheidung¹⁸⁵ abspielte, Gegenstand einer M&A-Transaktion gewesen wäre. Der Erwerber hätte sich ein Risiko in Milliardenhöhe eingekauft (siehe → Rn. 4).

Eines der Ziele der Due Diligence ist es weiterhin, die Kosten für die rechtliche, organisatorische, technische und personelle Eingliederung der Zielgesellschaft in die Gruppe des Erwerbers (Integrationskosten) zu berechnen. Ist bei der Zielgesellschaft die Einführung oder Überarbeitung eines Compliance-Management-Systems (CMS) erforderlich, so erfordert dies Investitionen.¹⁸⁶ Durch eine Compliance-Due Diligence können die hierfür ggf. erforderlichen Investitionen geschätzt und in der Kalkulation des Kaufpreises berücksichtigt werden.¹⁸⁷

182 Schwarz, BB 2012, 136, 138 (am Beispiel einer Entscheidung des US-amerikanischen DoJ betreffend eine öffentliche Übernahme durch den US-Konzern Halliburton nach englischem Recht).

183 Von Busekist/Timmerbeil, CCZ 2013, 225, 227 f.; Roeder/Schlutz/Havlik, CCZ 2023, 269, 271.

184 Allg. Meinung, siehe nur Spindler, in: MünchKomm-AktG, § 93 Rn. 47 m. w. N.

185 LG München I, 10.12.2013, 5 HK O 1387/10, BB 2014, 850.

186 Zur Pflicht, ein Compliance Management einzuführen, siehe den Beitrag von → Schulz, Kap. 1.

187 Andras/Szesny, Deutscher AnwaltSpiegel 20/2015, 3, 5; von Busekist/Timmerbeil, CCZ 2013, 225, 226; Liese, BB 2010, 27, 28.

dd) Normative Kraft des Faktischen

- 86 Schließlich macht es die Jelinek'sche „normative Kraft des Faktischen“ immer häufiger erforderlich, eine Compliance-Due Diligence durchzuführen. Zum einen ist in der Praxis vermehrt zu beobachten, dass die die M&A-Transaktion ggf. finanzierenden Banken Compliance als Bestandteil der von der rechtlichen Due Diligence umfassten Gebiete einfordern. Zum anderen versichern sog. Warranty & Indemnity-Versicherer typischerweise nur solche Risiken aus Garantien und Freistellungen in einem Unternehmenskaufvertrag, die im Rahmen der Due Diligence untersucht wurden. Ferner sind grob fahrlässige Pflichtverstöße in aller Regel ein Ausschlussstatbestand für die sog. D&O-Versicherung der Geschäftsleiter. Allerdings dürfte das Unterlassen einer Compliance-Due Diligence allenfalls in besonders gelagerten Fällen grob fahrlässig sein; etwa dann, wenn offensichtliche, massive, sich aufdrängende Compliance-Risiken nicht untersucht und auch keine hinreichenden Freistellungen vereinbart wurden.

b) Vorgehensweise: Abgestufte, risikobasierte Compliance-Due Diligence

aa) Rechtlicher Rahmen

- 87 Die Rechtsprechung erkennt es ausdrücklich an, dass Ziel der Due Diligence nur sein kann, die vorhandenen Risiken in einem gewissen, mit zumutbarem Aufwand erreichbaren Umfang zu begrenzen.¹⁸⁸ Vor diesem Hintergrund erscheint es vertretbar, den Umfang einer Compliance-Due Diligence entsprechend den Anforderungen der Transaktion sowie einem zu ermittelnden spezifischen Risikoprofil der Zielgesellschaft auszugestalten, also einen abgestuften, risikobasierten Ansatz zu wählen,¹⁸⁹ der im Folgenden erläutert wird.
- 88 Anders als bei einer rechtlichen Due Diligence in anderen Bereichen existiert für die Compliance-Due Diligence noch kein gefestigtes Verständnis hinsichtlich der konkreten Vorgehensweise.¹⁹⁰ In der Praxis sollte sich der „Scope“ der Compliance-Due Diligence auf alle Bereiche erstrecken, in denen potenziell Rechtsverstöße von einigem Gewicht auftreten können. Neben den nachfolgend exemplarisch hervorgehobenen Korruptions- und Bestechungstatbeständen sind dies vor allem das Kartellrecht und der Datenschutz¹⁹¹ sowie das Vergaberecht.¹⁹² Dabei werden Verstöße gegen Datenschutzrecht im Vergleich zu Hardcore-Kartellen, Fällen wettbewerbswidrigen Informationsaustauschs sowie Kor-

188 OLG Oldenburg, 22.6.2006, 1 U 34/03, BB 2007, 66; vgl. auch Schwarz, BB 2012, 136 ff.; Andras/Szesny, Deutscher AnwaltSpiegel 20/2015, 3, 4.

189 Vgl. auch Schwarz, BB 2012, 136, 137.

190 Siehe aber von Busekist/Timmerbeil, CCZ 2013, 225; Störk/Görtz, in: Beisel/Andreas, Beck'sches Mandatshandbuch Due Diligence, 3. Aufl. 2017, § 41 Rn. 11; Schwarz, BB 2012, 136, 140 f.; Ullrich/von Hesberg, CB 2015, 233, 234.

191 Vgl. von Busekist/Timmerbeil, CCZ 2013, 225, 228. Zum Compliance-Risikomanagement ferner → Schulz, Kap. 1 Rn. 60 ff.

192 Roeder/Schlutz/Havlik, CCZ 2023, 269, 270. Zur Relevanz des Vergaberechts siehe → Scherer, Kap. 28.

ruptions- und Bestechungstatbeständen erheblich leichter zu identifizieren sein. Denn es muss insofern nicht nach der „Nadel im Heuhaufen“ gesucht werden, sondern es können alle Datenverarbeitungsprozesse der Zielgesellschaft schlicht im Hinblick auf ihre Rechtskonformität überprüft werden.

Deutlich hervorzuheben ist, dass eine den Anforderungen der Transaktion sowie einem zu ermittelnden spezifischen Risikoprofil der Zielgesellschaft angemessene, sorgfältig geplante und durchgeführte Due Diligence nicht zwingend zeit- und kostenintensiv sein muss. Wenn die spezifischen Compliance-Risiken der Zielgesellschaft vor dem Hintergrund der Natur des Geschäftsbetriebs, der Sektoren und Länder, in denen sie tätig wird sowie weiterer Faktoren sehr niedrig sind, kann es ausreichend sein, sich in einem strukturierten Prozess und in dokumentierter Weise zu vergewissern, dass dem so ist. Dann bedarf es im Rahmen der Compliance-Due Diligence als weitere Maßnahme neben der Erstellung des Risikoprofils möglicherweise nur noch der Prüfung, ob die Zielgesellschaft ein Compliance-Management-System (CMS) hat und dieses auch gelebt wird. Bei einem sehr hohen Risikoprofil wird die Compliance-Due Diligence hingegen umfangreicher ausfallen müssen. Das mag aus Sicht der Geschäftsleiter des Erwerbers störend sein, ist bei erheblichen Risiken aber angemessen. Man denke in diesem Zusammenhang nur an die Worte des früheren US-amerikanischen Deputy Attorney General *Paul McNulty*: „If you think compliance is expensive, try non-compliance“.¹⁹³

bb) Ermittlung des Risikoprofils der Zielgesellschaft

In einem ersten Schritt sind die konkreten Korruptions- und Bestechungsrisiken in der Zielgesellschaft fundiert einzuschätzen (Risikoprofil). Die für die Risikobewertung maßgeblichen Faktoren sind (i) unternehmensbezogene Risiken, wie z. B. in der Vergangenheit aufgetretene Compliance-Verstöße oder enge Geschäftsbeziehungen mit Amtsträgern, (ii) geschäftsmodellbezogene Risiken, wie z. B. die Abhängigkeit von öffentlich-rechtlichen Erlaubnissen und/oder öffentlichen Aufträgen und (iii) das geografische Tätigkeitsgebiet sowie die Geschäftsfelder, in denen die Zielgesellschaft tätig ist (geografische und sektorspezifische Risiken).¹⁹⁴ Zur Bewertung dieser Risikofaktoren müssen zunächst Informationen zur Zielgesellschaft eingeholt werden. Dies werden zumeist mindestens sämtliche öffentlich zugänglichen Informationen aus dem Internet, Presseerzeugnissen oder weiteren allgemein zugänglichen Quellen sein, wie z. B. der sog. „Blacklist“ der Weltbank („Desktop Review“). Auch die Heranziehung von (kostenpflichtigen) Datenbanken (sog. „Negative Press Databases“, wie z. B. Acuity oder Worldcheck) kann in diesem Stadium sinnvoll sein, um Compliance-Verstöße in der Vergangenheit aufzudecken. Weiterhin kann es bei Trans-

¹⁹³ Zitiert nach *Doug Cornelius*, McNulty Keynote on a Tale of Two Sectors, <https://www.compliancebuilding.com/2009/06/04/mcnulty-keynote-on-a-tale-of-two-sectors/> (zuletzt abgerufen am 2.2.2024).

¹⁹⁴ Im Einzelnen *Ullrich/von Hesberg*, CB 2015, 233, 234 f.

aktionen mit Auslandsberührung angezeigt sein, bereits zu diesem Zeitpunkt zu versuchen, über lokale Berater Informationen zur Zielgesellschaft bzw. deren Tochtergesellschaften im Ausland und dem relevanten Marktumfeld zu erhalten (handelt es sich um eine besonders korruptionsanfällige Branche, ist die Zielgesellschaft in besonders korruptionsanfälligen Ländern tätig?).¹⁹⁵ Diese Informationen werden zwar nur selten definitive Antworten auf die Frage nach möglichen Compliance-Verstößen liefern, erlauben es aber, eine Risikoanalyse durchzuführen und bestehende Risiken besser einzuschätzen, um sodann ggf. eine tiefergehende Due Diligence für besonders risikoaffine Bereiche durchzuführen.

cc) Risikobewertung und Dokumentation

- 91 Zweitens hat eine Risikobewertung auf Grundlage der ermittelten Informationen zu erfolgen, die z. B. in Form einer Matrix dargestellt werden kann und zu Beweis Zwecken hinreichend dokumentiert werden sollte. Ergebnis der Bewertung sollte ein Überblick über die Zielgesellschaft sein, der einzelne Geschäftsbereiche in Risikoklassen untergliedert und damit den Umfang für den (weiteren) Ablauf der Prüfung vorgibt.

dd) Eigentliche Due Diligence

- 92 Der dritte Schritt liegt dann in der Durchführung der eigentlichen Due Diligence. Hier können – je nach Risikoprofil – neben Fragebögen und Interviews auch unternehmensinterne Dokumente zu sichten sowie in Extremfällen sogar umfangreiche E-Searches – also die strukturierte, technologie-unterstützte Sichtung elektronischer Daten, insbesondere E-Mails und Chatnachrichten – durchzuführen sein. Dieser Schritt kann somit auch im Fall einer abgestuften, risikobasierten Vorgehensweise sehr aufwendig sein, wenn die Zielgesellschaft bzw. einzelne Geschäftsbereiche ein sehr hohes Risikoprofil aufweisen. Umgekehrt kann ein niedriges Risikoprofil aber dazu führen, dass neben dem „Desktop Review“, der zunächst der Bestimmung des Risikoprofils diene, keine oder nur wenige, minimalinvasive weitere Maßnahmen vorzunehmen sind.¹⁹⁶

c) Due Diligence nach Vollzug

- 93 Wurden keine oder nicht ausreichend Informationen zu Compliance-Themen von der Zielgesellschaft bereitgestellt, sollte eine Untersuchung im angemessenen Umfang unmittelbar nach Vollzug der Transaktion in einer sogenannten Post-Closing oder auch Confirmatory-Due Diligence nachgeholt werden.¹⁹⁷ In rechtlicher Hinsicht ergibt sich die Pflicht zur Durchführung der Due Diligence

¹⁹⁵ Roeder/Schlutz/Kemper, CCZ 2023, 310, 312.

¹⁹⁶ Liese/Theusinger, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 27 Rn. 60 f.

¹⁹⁷ Andras/Szesny, Deutscher AnwaltSpiegel 20/2015, 3, 5; Störk/Görtz, in: Beisel/Andreas, Beck'sches Mandatshandbuch Due Diligence, 3. Aufl. 2017, § 41 Rn. 12; Benz, BOARD 4/2012, 137, 139; Schwarz, BB 2012, 136, 142.

nach Vollzug (Post-Closing Due Diligence) im Fall solcher Informationsdefizite zunächst aus der Legalitätspflicht der Organe, die die rechtmäßige Fortführung des Geschäftsbetriebs sicherzustellen haben.¹⁹⁸ Zudem gilt es, etwaige Ansprüche aus Garantien oder Freistellungen zu identifizieren und geltend zu machen, bevor eine im Unternehmenskaufvertrag vereinbarte (regelmäßig kenntnisunabhängige) Verjährung eintritt.¹⁹⁹ Auch wenn kartellrechtliche Risiken erst nach Vollzug der Transaktion aufgedeckt werden, kann über die Inanspruchnahme der sog. Kronzeugenregelung versucht werden, einen Erlass oder wenigstens eine Reduzierung von Bußgeldern zu erreichen.²⁰⁰ Dabei ist jedoch ausdrücklich darauf hinzuweisen, dass eine Post-Closing Due Diligence keinesfalls die Due Diligence vor Abschluss des Unternehmenskaufvertrags ersetzt (soweit diese erforderlich ist, was nicht zwingend der Fall sein muss, → Rn. 49), sondern ergänzend neben diese tritt.

Eine Post-Closing Due Diligence dürfte also vor allem dann erforderlich sein, wenn z.B. aufgrund eines Bieterverfahrens oder einer öffentlichen Übernahme die (Compliance-)Due Diligence zulässigerweise in einem geringeren Umfang erfolgt ist, als es mit Blick auf das spezifische Risikoprofil der Zielgesellschaft grundsätzlich erforderlich gewesen wäre und es so zu Informationsdefiziten gekommen ist. **94**

2. Umgang mit bekannten/bekanntgewordenen Compliance-Verstößen/-Risiken

Werden im Rahmen einer Due Diligence mögliche oder tatsächliche Compliance-Verstöße identifiziert, so stellt sich die Frage, wie mit derartigen Risiken umzugehen ist. Regelmäßig besteht die Sorge, dass jegliche Compliance-Risiken potenziell zu einem Abbruch der Verhandlungen führen können. Angesichts des gravierenden Schadenspotenzials vieler Compliance-Verstöße kann es durchaus Fälle geben, in denen das Risiko derart groß ist, dass sinnvollerweise von dem Abschluss der M&A-Transaktion Abstand genommen werden sollte. In der überwiegenden Mehrzahl der Transaktionen wird es aber so sein, dass durch die Strukturierung der Transaktion oder Regelungen im Unternehmenskaufvertrag auch noch nicht bis ins letzte Detail scharf umrissene Compliance-Risiken beherrscht werden können. **95**

a) Risikobewertung

In einem ersten Schritt gilt es, (i) die Eintrittswahrscheinlichkeit sowie (ii) die potenzielle Schadenshöhe der identifizierten Compliance-Risiken so gut wie **96**

198 Für nach Vollzug begangene Kartellrechtsverstöße haftet nach Europäischem Recht – neben der Zielgesellschaft selbst – ab Vollzug auch der Erwerber; und zwar kenntnisunabhängig, *Baron/Trebing*, BB 2016, 131, 135.

199 *Liese/Theusinger*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 27 Rn. 95; *Schwarz*, BB 2012, 136, 142.

200 *Baron/Trebing*, BB 2016, 131, 135.

möglich zu beziffern. Dabei sollten alle Aspekte in die Bewertung mit einbezogen werden, die den potenziellen Schaden bei Realisierung des relevanten Risikos beeinflussen können. Zunächst stellt sich insofern die Frage, inwiefern das Geschäftsmodell der Zielgesellschaft auf unlauterem Verhalten aufbaut (zu erwartender Umsatzeinbruch bei Änderung der illegitimen Geschäftspraxis). Bedeutsam ist auch, in welchen Jurisdiktionen Compliance-Verstöße (potenziell) begangen wurden, ob in der (oder den) betroffenen Jurisdiktion(en) eine Anzeigepflicht besteht und wie sich dort die Durchsetzungspraxis der betroffenen Behörden gestaltet (drohen Bußgelder, Gewinnabschöpfung, Steuernach- und/oder -strafzahlungen oder Vergabesperren (sog. „Blacklisting“)?). Auch Schadensersatzklagen von Kunden und/oder Wettbewerbern oder – in der Praxis natürlich schwer zu bemessende – Reputationsschäden können zu Schäden der Zielgesellschaft oder sogar des Erwerbers führen. Haben Schlüsselmitarbeiter Compliance-Verstöße begangen, muss ihnen u. U. gekündigt werden, was sich nachteilig auf das Geschäft auswirken kann. Ist der (vermutete) Compliance-Verstoß die Folge eines allgemein unzureichenden Compliance-Management-Systems (CMS), handelt es sich bei dem (vermuteten) Verstoß also nicht um einen „Ausreißer“, so muss das Compliance-Management-System (CMS) überarbeitet werden (sog. „Remedial Action“). Dies erfordert Investitionen.

b) Umgang mit bekannten/entdeckten Compliance-Risiken

- 97 Wurde das identifizierte Compliance-Risiko hinsichtlich der Höhe und der Eintrittswahrscheinlichkeit so gut es geht beziffert, stellt sich in einem zweiten Schritt die Frage, wie mit Blick auf die Eigenart des Risikos und die potenzielle Schadenshöhe damit umzugehen ist. Naheliegend ist zunächst die Überlegung, erwartete direkte Schäden wie z. B. Bußgelder, Gewinnabschöpfung und Steuernachzahlungen oder indirekte Schäden wie z. B. entgangener Gewinn durch Vergabesperren oder Reputationsschäden, einzupreisen, wobei eine Multiplikation der Schadenshöhe mit der Eintrittswahrscheinlichkeit erfolgen sollte. Inwiefern diese Vorgehensweise praktisch durchsetzbar ist, wird vor allem davon abhängen, ob (i) die zu erwartenden Schäden und deren Eintrittswahrscheinlichkeit im Zeitpunkt der Kaufpreisfindung überhaupt schon beziffert werden können und (ii) es die Verteilung der Verhandlungsmacht dem Erwerber erlaubt, seine Preisvorstellungen durchzusetzen. Dabei wird sich häufig das faktische Problem stellen, dass der Erwerber im Rahmen seines (Non-)Binding Offers bzw. bei Unterzeichnung des Letter of Intent oder Term Sheets bereits ein indikatives Kaufpreisangebot abgegeben hat. Fällt der Kaufpreis wegen der identifizierten Compliance-Risiken nun niedriger aus, so wird dies vom Veräußerer typischerweise als Kaufpreisreduktion wahrgenommen, wenngleich der indikative Kaufpreis unter den Vorbehalt der Due Diligence gestellt wurde.
- 98 Wurden sehr konkrete Risiken oder sogar belegbare Compliance-Verstöße bekannt, kann versucht werden, die Transaktion so zu strukturieren, dass die Risiken nicht mitveräußert werden. In Betracht kommt hier insbesondere die Struk-

turierung als Erwerb einzelner Vermögensgegenstände (sog. „Asset Deal“) anstelle der Geschäftsanteile der Zielgesellschaft (sog. „Share Deal“). Hierbei wird aber im Einzelfall sehr sorgfältig zu prüfen sein, ob der Übergang etwaiger Compliance-Risiken auf diesem Wege tatsächlich ausgeschlossen werden kann.²⁰¹ Es könnte z.B. zu einem gesetzlichen Übergang von Verbindlichkeiten kommen (§§ 25 Abs. 1 Satz 1 HGB, 75 Abs. 1 Satz 1 AO, 613a Abs. 1 Satz 1 BGB) und bei „Nahezu-Identität“ von übertragenem Vermögen und dem sonstigen Vermögen des Erwerbers kann selbst die Strukturierung als Asset Deal die Haftung für etwaige kartellrechtliche Bußgelder nicht ausschließen.²⁰²

Häufig wird es so liegen, dass die Compliance-Due Diligence Verdachtsmomente zutage gefördert hat, der Informationsstand aber noch nicht ausreicht, um die Risiken zu beziffern. Lehnt es der Veräußerer mit Blick auf die Zeitschiene oder aus Vertraulichkeitserwägungen ab, dem Erwerber eine weitergehende Compliance-Due Diligence zu gestatten, hält der Erwerber es aber dessen ungeachtet (ggf. wegen im Unternehmenskaufvertrag vereinbarter Sicherungsmechanismen wie z.B. Freistellungen, dazu sogleich) für vertretbar, den Unternehmenskaufvertrag zu unterzeichnen, so kommt unter Umständen eine Fortsetzung der Compliance-Due Diligence zwischen Unterzeichnung und Vollzug des Unternehmenskaufvertrags in Betracht. Das hat natürlich nur dann Sinn, wenn der Unternehmenskaufvertrag Möglichkeiten vorsieht, die Ergebnisse einer solchen vertieften Due Diligence auch nach Unterzeichnung noch zu reflektieren. Denkbar wäre es beispielsweise, im Fall der Strukturierung der M&A-Transaktion als Asset Deal zu vereinbaren, dass Vermögensgegenstände (ggf. sogar ganze Geschäftsbereiche), die sich als (in hohem Maße) risikobehaftet herausstellen, unter entsprechender Reduzierung des Kaufpreises zwischen Abschluss der Transaktion und Vollzug aussortiert werden können (sog. „Clean gate“-Struktur). Dabei stellen sich natürlich wiederum die vorstehend geschilderten Risiken, dass auch ein Asset Deal nicht in jedem Einzelfall den Übergang von Compliance-Risiken auszuschließen vermag. Denkbar wäre weiterhin eine Rücktrittsmöglichkeit für den Erwerber vor Vollzug bei Identifizierung gravierender Compliance-Risiken im Zeitraum zwischen Abschluss und Vollzug des Unternehmenskaufvertrags. Naturgemäß wird der Veräußerer einem solchen Vorschlag kritisch gegenüberstehen, da dies die Transaktionssicherheit beeinträchtigt, sich möglicherweise aber damit einverstanden erklären, wenn die Transaktion sonst scheitern würde.

Hat die Due Diligence lediglich Risiken von Compliance-Verstößen zutage gefördert und ist eine vertiefte Due Diligence nach Unterzeichnung des Kaufvertrags nicht gewünscht oder erfolgversprechend, bietet sich die Vereinbarung

99**100**

201 *Liese/Theusinger*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 27 Rn. 75. Zu den Grundlängen des Risikomanagements siehe ferner → *Romeike*, Kap. 9.

202 Zuletzt BGH, Urt. v. 27.1.2015, KRB 39/14, NZKart 2015, 276 – Kaffeekartell (Melitta), dies bestätigend: BVerfG, Beschl. v. 20.8.2015 – 1 BvR 980/15 NJW 2015, 3641; → *Seeliger/Mross/Seydel*, Kap. 27 Rn. 97 sowie *Baron/Trebing*, BB 2016, 131, 134.

einer Compliance-Freistellung an, die gegenüber der standardmäßig in Unternehmenskaufverträgen vereinbarten Compliance-Garantie eine Reihe von Vorteilen aufweist (siehe dazu → Rn. 50). Compliance-Freistellungen sind in der Praxis bislang eher ungewöhnlich. Aus Sicht des Erwerbers ist die Interessenlage aber jedenfalls im Fall eines mittleren bis hohen Risikos von Compliance-Verstößen mit der für unbekannte Steuerverbindlichkeiten²⁰³ oder Bodenlasten – zwei typische Risiken, die regelmäßig durch Freistellungen abgesichert werden – vergleichbar. In sämtlichen Fällen ist zumindest mit hinreichender Sicherheit zu erwarten, dass in der Zeit vor Vollzug der M&A-Transaktion Risiken entstanden sind, von denen jedoch bei Abschluss der Transaktion noch nicht absehbar ist, ob und wenn ja, in welchem Ausmaß sie sich materialisieren. Dies ist die typische Konstellation, in der eine Freistellung vereinbart wird.²⁰⁴ Insbesondere vor dem Hintergrund der aus Sicht des Veräußerers mit einer Compliance-Freistellung verbundenen Risiken sowie der Tatsache, dass derartige Freistellungen bislang eher selten anzutreffen sind, wird sich der Veräußerer in der Praxis wohl nur bei einer entsprechend starken Verhandlungsposition des Erwerbers oder bei sehr konkreten Risiken darauf einlassen. Soweit eine Compliance-Freistellung vereinbart wird, besteht umfangreicher Regelungsbedarf. So gilt es zu klären, wie z. B. entgangener Gewinn berechnet werden soll. Mit Blick auf die bisweilen horrenden Untersuchungskosten wird der Erwerber fordern, dass er insbesondere auch von den Kosten für (weitere) interne Untersuchungen freigestellt wird. Dies kann der Veräußerer regelmäßig allenfalls bei hinreichenden Verdachtsmomenten für (weitere) Verstöße akzeptieren und wird in diesem Zusammenhang einen Mechanismus zur Überprüfung durch einen unabhängigen Dritten (z. B. eine unbeteiligte Anwaltskanzlei oder einen Schiedsgutachter) sowie eine höhenmäßige Begrenzung fordern.

- 101** Für die Zeit nach Vollzug wäre schließlich denkbar, ein Rücktrittsrecht oder eine Put-Option für den Erwerber für den Fall zu vereinbaren, dass sich wider Erwarten doch (neue) Compliance-Risiken materialisieren.²⁰⁵ Diese Idee mag insofern zunächst überraschend erscheinen, als jedenfalls für die Zeit nach Vollzug ein Rücktritt oder eine irgendwie geartete Rückabwicklung des Unternehmenskaufvertrags in aller Regel gerade nicht gewollt und mit großen praktischen Schwierigkeiten verbunden ist, und deshalb explizit ausgeschlossen wird. Man muss sich aber vor Augen halten, dass die Vereinbarung entsprechender Rücktrittsrechte allenfalls dann in Betracht kommen wird, wenn der Erwerber erhebliche Bedenken aufgrund zumindest von ihm gesehener Compliance-Risiken hat und die M&A-Transaktion kurz vor dem Scheitern steht. In einem solchen Szenario kommt auf den ersten Blick ungewöhnlich erscheinenden Lösungen die Funktion zu, andernfalls nicht zustande kommende Transaktionen zu ermöglichen.

203 Benz, BOARD 2012, 137, 139.

204 Schrader, in: Seibt, Beck'sches Formularbuch Mergers & Acquisitions, Anm. 101 zu C.II.1 313 f.

205 Schwarz, BB 2012, 136, 142.

IV. Zusammenfassung

M&A-Transaktionen sind – ungeachtet eines zunehmenden Grades der Standardisierung – komplexe Prozesse, auf die eine Vielzahl von rechtlichen Regelungen aus unterschiedlichsten Bereichen Anwendung finden, deren Nichtbeachtung hohes Schadenspotenzial birgt. Neben Bestimmungen, die auf den M&A-Prozess selbst Anwendung finden, besteht die Gefahr, dass ein Erwerber sich mit einem Unternehmen(-steil) unbekannte Compliance-Risiken einkauft, die den Wert der erworbenen Beteiligung stark mindern und schlimmstenfalls sogar die gesamte Gruppe des Erwerbers nachteilig beeinträchtigen können. 102

Prozessuale Compliance-Risiken sind grundsätzlich gut beherrschbar. Die wesentliche Aufgabe der am M&A-Prozess beteiligten Personen liegt insofern darin, den Überblick über mögliche Haftungsfallen zu behalten und frühzeitig zu erkennen, ob ein Spezialist für bestimmte Rechtsgebiete wie z. B. Kartell- oder Datenschutzrecht heranzuziehen ist. Materielle Compliance-Risiken aus M&A-Transaktionen bergen hingegen regelmäßig viele Unwägbarkeiten und haben bislang weder im Schrifttum noch in der Praxis die ihnen gebührende Aufmerksamkeit erfahren. Ungeachtet der Tatsache, dass in vielen Fällen eine rechtliche Verpflichtung der Geschäftsleiter des Erwerbers zur Durchführung einer Compliance-Due Diligence besteht oder das Unterlassen zumindest Nachteile wie den Verlust der Haftungsprivilegierung der Business Judgement Rule für sie nach sich ziehen dürfte, unterbleibt sie häufig. Die Gründe hierfür sind vielfältig; insbesondere dürften fehlendes Problembewusstsein oder fehlendes Know-how und die Sorge vor dem (vermeintlichen) Aufwand sowie einem möglichen Scheitern der Transaktion ausschlaggebend sein. Diese Befürchtungen sind häufig unbegründet, denn eine (Compliance-)Due Diligence muss nicht zwingend sehr umfangreich ausfallen. Es ist vielmehr zulässig, den Umfang in angemessener Weise zu beschränken. Bei einem sehr hohen Risikoprofil der Zielgesellschaft kann der rechtlich gebotene Umfang der Compliance-Due Diligence allerdings durchaus erheblich ausfallen. Man wird sich jedoch vor Augen halten müssen, dass in den betroffenen Fällen ganz massive Compliance-Risiken bestehen. Insofern kommt einer eingehenden Compliance-Due Diligence hier eine Ermöglichungsfunktion zu: Ohne eine fundierte Risikoeinschätzung wäre jedenfalls in derartigen Hochrisikofällen die einzige Alternative für den Erwerber, Abstand von der Transaktion zu nehmen. Gleiches gilt für die sich an die Erforschung der Compliance-Risiken anschließende Frage nach dem Umgang mit ebendiesen. Zwar mögen vertragliche Vereinbarungen wie Rücktrittsrechte oder Compliance-Freistellungen auf den ersten Blick (noch) ungewöhnlich erscheinen, können aber durchaus geeignet sein, einer M&A-Transaktion trotz (erheblicher) Compliance-Risiken zum Abschluss zu verhelfen. 103

27. Kapitel

Kartellrechts-Compliance*

I. Überblick über die Kartellrechts-Risiken

1. Einleitung

Kartellrechts-Compliance stellt eine wichtige Herausforderung für rechtskonforme Geschäftstätigkeiten von Unternehmen im nationalen und internationalen Geschäftsverkehr dar und gilt als einer der „klassischen“ Compliance-Themenbereiche. 1

Kein Unternehmen kann es sich heute noch leisten, in seinem Compliance-System angemessene Maßnahmen zum Umgang mit seinen spezifischen Kartellrechtsrisiken auszusparen. In immer mehr Jurisdiktionen wird eine verschärfte Kartellverfolgung vorangetrieben. Die Kartellbußgelder erreichen dabei mitunter Rekordhöhen.¹ Darüber hinaus gibt es in mehr als 50 Staaten Kronzeugenprogramme zur Förderung der Aufdeckung von kartellrechtswidrigen Vereinbarungen. Hinzu kommen anonyme Hinweisgebersysteme in Unternehmen² und bei Wettbewerbsbehörden. Diese arbeiten besonders eng im Netzwerk der Europäischen Wettbewerbsbehörden (ECN) unter Führung der Europäischen Kommission zusammen. Darüber hinaus erfolgt auf internationaler Ebene ein Austausch im Rahmen von Arbeitsgruppen im International Competition Network (ICN).³ 2

Kartellrechts-Compliance richtet sich traditionell vorrangig an die Vertriebsabteilungen, sollte aber auch andere Unternehmensabteilungen einschließen. Insbesondere Bereiche, die unmittelbar oder auch nur mittelbar in Kontakt mit Wettbewerbern stehen oder die Geschäftsbeziehungen mit Kunden und Lieferanten gestalten oder strategisch bestimmen, sollten – neben der Unternehmensleitung – mit betrachtet werden. Bereits der Umstand, dass ein Unternehmen von kartellrechtlichen Ermittlungen der Wettbewerbsbehörden betroffen ist, kann gravierende Folgen haben. Ziel der Kartellrechts-Compliance muss es deshalb 3

* Die Autoren danken Frau Dr. Antje Heinen, die in den beiden Voraufagen als Co-Autorin an der Bearbeitung dieses Kapitels beteiligt war. Frau Dorothee de Crozals, Herrn Aurélien Hömann und Herrn Markus Pohlmann danken sie für ihre wertvolle Unterstützung.

1 Z. B. verhängte die Europäische Kommission im Bereich der Kartellverfahren in der Vergangenheit Bußgelder in Höhe von 1 Mrd. EUR gegen Daimler, 880 Mio. EUR gegen Scania, 750 Mio. EUR gegen DAF und 670 Mio. EUR gegen Volvo/Renault (jeweils LKW), 715 Mio. EUR gegen Saint Gobain (Autoglas), 705 Mio. EUR gegen Philips und 688 Mio. EUR gegen LG Electronics (jeweils Bildschirmröhren), und 466 Mio. EUR gegen die Deutsche Bank (Kreditderivate). Siehe www.ec.europa.eu/competition/cartels/statistics/statistics.pdf zu grafischen Darstellungen, die z. B. auch in Compliance-Schulungen eingesetzt werden können (zuletzt abgerufen am 25.4.2024).

2 Zu aktuellen Entwicklungen und Anforderungen bei Hinweisgebersystemen → *Block/Sonnenberg*, Kap. 5.

3 Im ICN arbeiten inzwischen über 140 nationale Kartellbehörden zusammen (siehe www.internationalcompetitionnetwork.org).

sein, schon präventiv jedem Anschein eines möglichen Kartellrechtsverstoßes so weit wie möglich vorzubeugen.

- 4 Die vorangehenden Abschnitte könnten bereits der Start in eine Ihrer Compliance-Schulungen sein. Denn das Stichwort „Risikopotenzial“ ist ein guter Auftakt für eine lebhafte Diskussion auch zum Thema Kartellrechts-Compliance.
- 5 Eine Besonderheit des Kartellrechts ist, dass einzelne Geschäftsvorgänge kartellrechtlich oftmals nicht eindeutig in die Kategorien „erlaubt“ (grün) oder „verboten“ (rot) einsortiert werden können, sondern häufig „orange“ mit unterschiedlichen Schattierungen sind. Jeder weiß, dass die Absprache von Preisen zwischen Wettbewerbern dem Kunden/Endverbraucher gegenüber verboten ist. Aber wenn im Verband über Rohstoffpreiserhöhungen – und wie der Einzelne damit umgeht – diskutiert wird, was dann? Hier können Nuancen entscheidend sein, ob ein schwerwiegender Kartellrechtsverstoß (Hardcore-Kartell) oder ein noch erlaubter allgemeiner Informationsaustausch vorliegt – und die Behörden weiten ihr Aufgreifermessen zunehmend aus. Gerade dies führt zu einem erhöhten Beratungsbedarf bei Ansprechpartnern insbesondere im Vertrieb, aber auch z. B. im Marketing, Einkauf, im Programm/Product Management, in der F&E, der Unternehmensstrategie und auch bei der Geschäftsführung sowie den Kontrollgremien. Bei Diskussionen zur rechtlichen Einschätzung kann es zuweilen hilfreich sein, das eigene „Bauchgefühl“ zu erspüren bzw. den „gesunden Menschenverstand“ walten zu lassen. Auf jeden Fall ist der Sachverhalt, also die Umstände des Einzelfalls, möglichst umfassend zu erfragen.
- 6 Vonnöten sind gute rechtliche und im Einzelfall passende Compliance-Materialien im Unternehmen. Aus welchem Blickwinkel lesen Sie das Kapitel zur Kartellrechts-Compliance? Konzipieren Sie Ihre Strategie zu Compliance-Schulungen, stehen Sie vor dem Entwurf von Kartellrechts-Richtlinien, suchen Sie einen Leitfaden für Beratungen im Tagesgeschäft oder möchten Sie sich zur Vorgehensweise bei etwaigen internen Untersuchungen informieren? Dies sind einige der Aspekte der Kartellrechts-Compliance, die in diesem Kapitel im Fokus stehen.
- 7 Im Folgenden werden zunächst die wichtigsten kartellrechtlich relevanten Risiken aufgelistet (→ Rn. 8 ff.). In vielen Veröffentlichungen wird bei der Darstellung der kartellrechtlichen Themen eine Gliederung nach horizontalen Vereinbarungen (mit Wettbewerbern) auf der einen Seite und vertikalen Vereinbarungen (mit Lieferanten/Kunden) auf der anderen Seite vorgenommen. Bewusst erfolgt im Folgenden eine Gliederung nach Gewichtung des Ausmaßes der möglichen Risiken (zunächst „sehr hohe Risiken“, dann „weniger hohe Risiken“). Mit den aufgelisteten Risiken sind dann auch die Inhalte abgedeckt, die – je nach kartellrechtlichem Risikoprofil des Unternehmens – in Compliance-Schulungen und Richtlinien behandelt werden sollten. Abschnitt I.3. (→ Rn. 80 ff.) befasst sich mit der Frage, welche Handlungen von natürlichen Personen einem Unternehmen als eigener Verstoß zugerechnet werden. Unter Abschnitt I.4. (→ Rn. 89 ff.) werden Art und Umfang der kartellrechtlichen Haf-

tung geschildert. In Teil II. (→ Rn. 110 ff.) werden Bausteine der – insbesondere präventiven – Steuerung der Kartellrechtsrisiken in der Praxis dargestellt. Teil III. (→ Rn. 153 ff.) der Abhandlung behandelt behördliche Durchsuchungen. Es werden die Ermittlungsbefugnisse der Wettbewerbsbehörden und der typische Ablauf einer solchen Durchsuchung dargestellt. Den Abschluss bildet eine Auflistung von Verhaltensregeln für die Unternehmen vor, während und nach einer möglichen Durchsuchung (→ Rn. 180 ff.). Dieser Teil nimmt einen relativ breiten Raum ein. Dies aus zwei Gründen: Zum einen stoßen Durchsuchungen in Compliance-Schulungen tendenziell auf großes Interesse der Mitarbeiter und der Geschäftsführung, vor allem, wenn dieser Teil durch – leidvolle – Erfahrungsberichte belebt wird. Dann steigen in vielen Fällen auch Interesse und Aufmerksamkeit für die notwendigen sonstigen präventiven Maßnahmen der Kartellrechts-Compliance. Zum anderen mag es sinnvoll sein, diese rein hypothetische Situation, die im Ernstfall eine Stresssituation darstellt, einmal in Ruhe zu durchdenken.

2. Kartellrechts-Risikokategorien

Bei der Einteilung in verschiedene Risikokategorien ist vor allem das Verfolgungs- bzw. Sanktionsrisiko zu berücksichtigen. 8

Den weitaus größten Teil möglicher Kartellrechtsverstöße bilden Vereinbarungen oder Abstimmungen eines Unternehmens mit anderen Unternehmen zu Inhalten, die für das Wettbewerbsverhalten der Unternehmen relevant sind. Soweit durch eine solche Vereinbarung oder Abstimmung der Wettbewerb spürbar beeinträchtigt wird, handelt es sich um ein Kartell im Rechtssinn.⁴ Auch einseitige Handlungen eines Unternehmens können einen Wettbewerbsverstoß darstellen, wenn das Unternehmen eine marktbeherrschende Stellung hat und sein Verhalten als Missbrauch zu bewerten ist.⁵ In beiden Fällen sind im Folgenden als „sehr hohe Risiken“ alle Verstöße eingestuft, die von den Wettbewerbsbehörden verstärkt verfolgt und üblicherweise mit empfindlichen Bußgeldern geahndet werden. Im Gegensatz dazu sind „weniger hohe Risiken“ alle Verstöße, die grundsätzlich weniger stark im Fokus der Wettbewerbsbehörden stehen und bei denen im Regelfall nicht mit einem Bußgeld, sondern nur mit einer Untersagung (Verbot) zu rechnen ist. Zum Kartellrecht im weiteren Sinn gehört außerdem die Kontrolle von Zusammenschlüssen von Unternehmen, deren Umsätze eine bestimmte Größenordnung übersteigen (Fusionskontrolle).⁶ In diesem Zusammen- 9

4 Rechtsgrundlage sind insoweit Art. 101 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) für das europäische Recht und der inhaltlich identische § 1 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) für das deutsche Recht. Entsprechende Vorschriften gibt es grundsätzlich in den Kartellrechtsgesetzen anderer Länder.

5 Letzteres ist geregelt in Art. 102 AEUV für das europäische Recht und den teilweise weitergehenden Bestimmungen in den §§ 18 ff. GWB für das deutsche Recht. Ähnliche Vorschriften gibt es wiederum in den Kartellrechtsgesetzen anderer Länder.

6 Vgl. dazu für das europäische Recht die Verordnung (EG) Nr. 139/2004 des Rates vom 20.1.2004 über die Kontrolle von Unternehmenszusammenschlüssen, ABl. L 24/1 vom

hang sind ebenfalls Wettbewerbsverstöße denkbar, die von den zuständigen Wettbewerbsbehörden mit Sanktionen geahndet werden können.⁷

a) Das Verbot wettbewerbsbeschränkender Vereinbarungen: Absprachen mit anderen Unternehmen

- 10** Durch wettbewerbsbeschränkende Vereinbarungen wird der Wettbewerb der Unternehmen eingeschränkt oder verfälscht. Geschädigte sind die Kunden und letztlich die Verbraucher, die vor allem in Form höherer Preise die Nachteile zu tragen haben. Die Bekämpfung von wettbewerbsbeschränkenden Vereinbarungen ist deshalb ein Schwerpunkt der Kartellbehörden.

aa) Vereinbarung, abgestimmtes Verhalten oder Beschluss

- 11** Kartelle sind Absprachen zwischen zwei oder mehreren Unternehmen über das Verhalten im Wettbewerb („Vereinbarungen“). Gegenstand der Absprache kann alles sein, was für das Verhalten eines Unternehmens im Markt, also gegenüber Kunden und Lieferanten, von Bedeutung ist. Meist geht es um den Vertrieb von Produkten an Unternehmenskunden oder Endverbraucher. Aber auch Vereinbarungen mit anderen Unternehmen über die Produktion, den Einkauf oder die Forschung und Entwicklung können betroffen sein. Ein besonders gravierender Verstoß ist der (gegenseitige oder einseitige) Verzicht auf Wettbewerb (z.B. Preisabsprachen, Markt-, Kunden- oder Projektaufteilungen).
- 12** Für die Art und Weise, wie eine Vereinbarung zustande kommt, gibt es keine Einschränkungen. Es kann sich um ein formelles Rechtsgeschäft handeln, mit dem eine rechtliche Bindung bewirkt werden soll.⁸ Wenn den Beteiligten bewusst ist, dass ihre Absprachen kartellrechtlich verboten sind, werden sie häufig geheim gehalten. In der Praxis kann den Unternehmen jedenfalls schon allein die Tatsache zur Last gelegt werden, dass sie bei einem Treffen anwesend waren, bei dem ein Kartellrechtsverstoß be- bzw. abgesprochen wurde.
- 13** Was häufig Mitarbeitern im Unternehmen nicht bewusst ist: Kartellrechtsverstöße können auch auf einem sog. „abgestimmten Verhalten“ von Unternehmen beruhen. Wenn Unternehmen Kontakt mit Wettbewerbern hatten und anschließend ihr Verhalten im Wettbewerb anpassen, wird von den Wettbewerbsbehörden häufig vermutet, dass eine kartellrechtlich unzulässige Verhaltensabstimmung vorliegt. Diesen Anschein gilt es dann im Einzelfall ggf. zu entkräften. Nur dann, wenn sich ein Unternehmen aufgrund eigener Entscheidung im Wettbewerb nach dem Verhalten eines anderen Unternehmens ausrichtet, ohne sich mit diesem abzustimmen, ist ein solches „Parallelverhalten“ kartellrechtlich zulässig.

29.1.2004 – Fusionskontrollverordnung (FKVO). Im deutschen Recht sind die §§ 35 ff. GWB maßgeblich. Ähnliche Regelungen gibt es in den Rechtsordnungen anderer Länder.

7 Siehe dazu → Ullrich, Kap. 26 Rn. 26 ff.

8 Eine kartellrechtswidrige Vereinbarung ist aber von Rechts wegen unwirksam und erzeugt daher keine rechtlich wirksame Bindung (Art. 101 Abs. 2 AEUV; § 1 GWB i.V.m. 134 BGB).

Grundsätzlich ist deshalb bei allen Kontakten mit Wettbewerbern Vorsicht geboten.

Für das Kartellrecht gilt die Regel: Solange die Unternehmen im Wettbewerb ihre Entscheidung eigenverantwortlich und ohne Abstimmung mit Wettbewerbern treffen, sind sie frei, die Bedingungen für ihre geschäftlichen Aktivitäten (z.B. Preise, Mengen, Qualität, Auswahl der Kunden) nach eigenem Belieben festzusetzen.⁹ Jede Verständigung (Austausch oder einseitige Offenlegung) über eine solche Entscheidung mit einem Wettbewerber birgt das Risiko, dass die Behörden ein abgestimmtes Verhalten annehmen. Die Kartellbehörden wollen effektiv verhindern, dass einzelne Unternehmen ihr unternehmerisches Risiko durch Absprachen oder Abstimmungen mit Wettbewerbern verringern und dadurch den Wettbewerb zulasten anderer beeinträchtigen. Deshalb stellt auch der bloße Austausch (oder die einseitige Offenlegung) von Informationen ein hohes Risiko dar, wenn die Informationen für das Wettbewerbsverhalten eines oder mehrerer Unternehmen von Bedeutung sind. Dies wurde jüngst bei einer Durchsuchung deutlich, bei der die Kommission den Vorwurf einer Preisabstimmung über öffentliche Verlautbarungen untersucht.¹⁰ 14

bb) Bezweckte oder bewirkte Wettbewerbsbeschränkung

Schwerwiegende Verstöße, bei denen die Erfahrung dafür spricht, dass hierdurch der Wettbewerb beeinträchtigt wird, gelten als „bezweckte Wettbewerbsbeschränkung“. ¹¹ Hier liegt der Verstoß bereits in der Absprache als solcher. Auf die Auswirkungen im konkreten Fall kommt es nicht an. Ein Unternehmen kann sich auch nicht damit verteidigen, es habe an dem Verstoß nicht aktiv mitgewirkt, es habe die Absprache gar nicht eingehalten oder die Vereinbarung habe sich nicht auf die Marktverhältnisse ausgewirkt. Diese Verstöße werden von den Wettbewerbsbehörden in der Regel mit empfindlichen Bußgeldern geahndet (dazu siehe → Rn. 91 ff.). Im Folgenden werden sie als „sehr hohe Risiken“ bezeichnet. 15

Im Unterschied dazu ist bei den weniger gravierenden Verstößen im Einzelnen zu untersuchen, ob der Wettbewerb tatsächlich beeinträchtigt wurde. Bei diesen Verstößen handelt es sich um Verhaltensweisen, bei denen der Erfahrung nach eine Wettbewerbsbeschränkung zwar möglich, aber nicht unbedingt zu vermuten 16

9 Sowohl in der Rechtsprechung des EuGH als auch in der Entscheidungspraxis des Bundeskartellamtes ist dieses „Selbstständigkeitspostulat“ wesentlicher Maßstab bei der Beurteilung, ob eine kartellrechtswidrige Absprache oder Abstimmung vorliegt. Vgl. z.B. EuGH, 8.7.1999 – Rs. C-49/92 P, ECLI:EU:C:1999:356 – Anic Partecipazioni SpA; 16.12.1975 – Rs. 40–48/73, 50/73, 54–56/73, 111/73, 113 u. 114/73, ECLI:EU:C:1975:174 – Suiker Unie; Bunte, Kartellrecht, § 1 GWB Rn. 106.

10 Europäische Kommission, Pressemitteilung vom 30.1.2024, Kommission führt unangekündigte Nachprüfungen bei Anbietern von Autoreifen durch, https://ec.europa.eu/commission/presscorner/detail/de/ip_24_561 (zuletzt abgerufen am 25.4.2024).

11 EuGH, 13.12.2012 – Rs. C-226/11, ECLI:EU:C:2012:795 – Expedia; EuGH, 11.9.2014 – Rs. C-67/13P, ECLI:EU:C:2014:2204 – Cartes Bancaires.

ist. Man nennt diese „bewirkte Wettbewerbsbeschränkungen“.¹² Bei ihrer Beurteilung müssen jeweils die konkreten Umstände des Sachverhalts ermittelt und bewertet werden. Bußgelder wurden in der Vergangenheit hier nur in Ausnahmefällen verhängt. Im Folgenden werden sie als „weniger hohe Risiken“ eingestuft.

cc) *Sehr hohe Risiken*

(1) „Hardcore-Kartelle“

- 17 Sogenannte „Hardcore-Kartelle“ sind die „klassischen“ Kartelle, bei denen Wettbewerber untereinander Preise, Mengen oder die Zuteilung von Kunden, Märkten oder Projekten absprechen. Auch der Verzicht auf Wettbewerb ist davon erfasst. Dabei handelt es sich um eine Verständigung der Unternehmen, dass sie künftig z. B. die Preise ihrer Wettbewerber nicht unterbieten oder sich gegenseitig keine Kunden abwerben wollen. Ein Preiskartell liegt nicht nur bei der Absprache über Endkundenpreise vor. Es reicht in der Regel schon aus, wenn Preisbestandteile, Preiserhöhungen, Margen oder wesentliche Kostenfaktoren abgestimmt werden. In einem konkreten Fall hatten die Unternehmen beispielsweise nur die Referenzpreise ausgetauscht, mit denen sie jeweils die Preisverhandlungen mit ihren Kunden begonnen hatten. Die Europäische Kommission und das EuG haben hierin trotzdem einen Kartellverstoß gesehen, da aus ihrer Sicht die laufende Information über die Referenzpreise zusammen mit anderen Faktoren zumindest Tendenzaussagen über die tatsächlichen Kundenpreise ermöglichte und den Unternehmen „mehr“ Sicherheit in ihren bilateralen Verhandlungen mit dem Kunden gab.¹³ In derartigen Fällen werden die Behörden auch immer strenger und rücken „orange“ Bereiche mehr und mehr in „rote“ Bereiche.
- 18 Schwierigkeiten bereitet oft auch die Entscheidung, welches Unternehmen in welchem Zeitraum an der Kartellabsprache beteiligt war. Kartelle können sich über Jahre erstrecken und eine Vielzahl von Märkten umfassen. Auch wenn ein Unternehmen nicht an allen Absprachen unmittelbar mitgewirkt hat, ist es nach Ansicht der Behörden grundsätzlich für alle Verstöße im gesamten Zeitraum und auf allen Märkten verantwortlich.¹⁴ Eine Ausnahme gilt nur dann, wenn es entweder an bestimmten Abschnitten des Gesamtkartells nicht teilgenommen oder sich von bestimmten Absprachen für die anderen Unternehmen erkennbar distanziert hat.

12 EuGH, 13.12.2012 – Rs. C-226/11, ECLI:EU:C:2012:795 – Expedia.

13 EuG, 14.3.2013 – Rs. T-588/08, ECLI:EU:T:2013:130 – Dole Food und Dole Germany; EuGH, 19.3.2015 – Rs. C-286/13P, ECLI:EU:C:2015:184 – Dole Food Company Inc. und Dole Fresh Fruit Europe. In gleicher Weise beurteilte die Kommission auch Absprachen zu „Bruttolistenpreisen“ als Grundlage für die Preisbildung im sog. LKW-Kartell, Europäische Kommission, Pressemitteilung vom 19.7.2016, https://ec.europa.eu/commission/presscorner/detail/de/ip_16_2582 (zuletzt abgerufen am 25.4.2024).

14 Man spricht dann von einer einheitlichen fortgesetzten Handlung.

(2) Ausschreibungen

Heimliche Absprachen von Unternehmen, die an einer Ausschreibung teilnehmen, verfälschen den Wettbewerb und stellen somit nach den allgemeinen Regeln ein Kartell dar. 19

Beispiel: Der Geschäftsführer A des Unternehmens X und der Geschäftsführer des Wettbewerbers B treffen sich zum Tennisspiel. Im Gespräch nach dem Spiel stellt sich heraus, dass X nur bei einem von 20 Angeboten, die es im Norden des Landes abgibt, den Zuschlag bekommt. Das Unternehmen von B erhält hingegen in demselben Gebiet bei jedem dritten Angebot den Zuschlag. Andererseits scheint X im Süden des Landes (anteilmäßig) viel mehr Zuschläge zu bekommen als das Unternehmen von B. Die Preise in beiden Gebieten werden jedoch durch den Wettbewerb zwischen ihnen gedrückt. Deswegen vereinbart A mit B, dass A im Norden des Landes und B im Süden des Landes keine Angebote oder nur „erhöhte“ Angebote abgeben werden. Diese Vereinbarung ist eine Marktaufteilung und ein schwerer Kartellrechtsverstoß. 20

Bei unzulässigen Absprachen im Rahmen von (öffentlichen) Ausschreibungen gilt die Besonderheit, dass es sich für die handelnden Personen um eine Straftat handelt.¹⁵ Das führt zu einer Aufteilung der Verfahren. Der Verstoß der Unternehmen wird als Ordnungswidrigkeit vom Bundeskartellamt verfolgt und mit einem Bußgeld geahndet. Gegen die handelnden Personen ermittelt die Staatsanwaltschaft und leitet ggf. durch eine Anklage ein gerichtliches Strafverfahren ein, an dessen Ende eine Verurteilung zu einer Gefängnis- oder Geldstrafe stehen kann. 21

Eine weitere Besonderheit besteht darin, dass kleine und mittlere Unternehmen häufig die Ausschreibungsbedingungen nicht allein erfüllen können. In diesem Fall dürfen sie andere Unternehmen zu ihrem Angebot hinzuziehen, sofern sie dadurch in die Lage versetzt werden, ein wirksames Angebot abzugeben. Man spricht dann von einer sogenannten Arbeitsgemeinschaft. Der Wettbewerb wird durch diese Zusammenarbeit nicht beschränkt, vielmehr wird hierdurch die Beteiligung an der Ausschreibung erst ermöglicht. Sofern die Voraussetzungen einer Arbeitsgemeinschaft vorliegen, ist diese somit wettbewerbsfördernd und kein Kartellverstoß. Hier besteht aber in der Praxis ein erheblicher Graubereich, unter welchen Bedingungen und aus welchen Gründen es Unternehmen unmöglich ist, ein eigenständiges Angebot abzugeben (fehlende finanzielle/personelle Ressourcen, fehlendes Know-how etc.).¹⁶ 22

¹⁵ Rechtsgrundlage ist § 298 StGB.

¹⁶ Siehe hierzu z. B. BKartA, Pressemitteilung zu Verbandsleitlinien für Liefergemeinschaften vom 4.7.2019, https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilung/2019/04_07_2019_Verbandsleitlinien_Transportbeton.html (zuletzt abgerufen am 25.4.2024).

- 23 Beispiel:** Ein Kunde hat X zur Abgabe eines Angebots für einen Auftrag von über 700 Mio. EUR aufgefordert. Aufgrund des Auftragsumfangs (und der hierfür erforderlichen Fachkenntnisse) wäre X nicht in der Lage, ihn allein auszuführen. Deshalb entschließt sich X, eine Arbeitsgemeinschaft mit zwei anderen Unternehmen zu gründen (die ebenfalls allein kein Angebot abgeben können) und legt auf dieser Basis ein Angebot vor. Das Konsortium erhält den Zuschlag. Eine derartige Arbeitsgemeinschaft (die es X erlaubt, einen Auftrag auszuführen, den es allein nicht bewältigen könnte) verstößt als solche nicht gegen das Kartellrecht. Voraussetzung dafür ist jedoch, dass der Kunde von der Arbeitsgemeinschaft weiß und sich der Informationsaustausch zwischen den Unternehmen auf die Geschäftstätigkeit der Arbeitsgemeinschaft beschränkt.

(3) Informationsaustausch

- 24** Im Rahmen von Kartellabsprachen teilen sich die beteiligten Unternehmen in der Regel eine Vielzahl von Informationen mit, die für die Durchführung des Kartells notwendig sind. Diese Art des Informationsaustauschs ist Teil des Kartells, zu dem er gehört, und kein gesonderter Kartellverstoß.
- 25** Bei einem reinen Informationsaustausch ohne Bezug zu weitergehenden (Kartell-)Absprachen kann eine Wettbewerbsbeschränkung darin bestehen, dass durch die Verständigung mit Wettbewerbern die wirtschaftliche Unsicherheit und die unternehmerischen Risiken beseitigt oder verringert werden, die mit einer Tätigkeit im Markt üblicherweise verbunden sind (Verstoß gegen das Selbstständigkeitspostulat) (dazu siehe → Rn. 14). Dabei ist es regelmäßig eine verbotene Kartellabsprache, wenn die ausgetauschten Informationen geeignet sind, das Marktverhalten zumindest eines Unternehmens (beispielsweise hinsichtlich der Forderung eines gemeinsamen Kunden) zu beeinflussen. Dieser Umstand macht die meisten Kontakte und Treffen zwischen Wettbewerbern sehr risikoreich.
- 26** Es gibt keine allgemeine Regel, wie zwischen einem verbotenen und einem erlaubten Informationsaustausch zu unterscheiden ist. Dies hängt vom Thema des Treffens/Gesprächs im Einzelfall ab. Grundsätzlich unzulässig („roter Bereich“) sind Hinweise zum aktuellen und künftigen geschäftlichen Verhalten der Unternehmen. Dies umfasst nicht nur Geschäftsgeheimnisse im engeren Sinn, sondern alle sensiblen Unternehmensdaten, die die Geschäftspolitik betreffen. Dazu zählen vor allem preisbezogene Informationen, aber auch Angaben zu einzelnen Kunden, aktuellen Aufträgen und konkreten (Liefer- oder Bezugs-)Konditionen einzelner Geschäfte. Grundsätzlich zulässig („grüner Bereich“) ist ein Austausch, wenn die Informationen öffentlich zugänglich, nicht mehr aktuell oder so aggregiert sind, dass Rückschlüsse auf einzelne Wettbewerber/Kunden oder

Geschäftsabschlüsse nicht mehr möglich sind.¹⁷ Dazwischen („oranger Bereich“) liegt eine große Bandbreite an Informationen, bei denen es umso mehr auf die Umstände des Einzelfalls ankommt. Bei einer Offenlegung von Unternehmensdaten an Wettbewerber ist immer besondere Vorsicht geboten. Das soll nicht jeder Art von Benchmarking oder Verbandstreffen pauschal einen Riegel vorschieben, da es eine Vielzahl an Themen und Informationen gibt, die in legitimer Weise besprochen und ausgetauscht werden dürfen. Als Faustregel sollte gelten: Immer dann, wenn die Information Einfluss auf die unternehmerischen Entscheidungen auch nur eines einzigen Beteiligten haben könnte, sollte sie Wettbewerbern nicht offengelegt werden. Die Grenze der zulässigen Information ist rasch überschritten und bei Verstößen können empfindliche Bußgelder drohen. Hier ist die Entscheidungspraxis der Kartellbehörden im vergangenen Jahrzehnt deutlich strenger geworden.

Fragen zu zulässigem oder unzulässigem Informationsaustausch werden in vielen Unternehmen einen wichtigen Teil des Beratungsalltags und der Compliance-Schulungen ausmachen. Gerade dies sind auch Aspekte, die einen Teilnehmerkreis über die Vertriebsteams hinaus betreffen, z. B. auch die Abteilungen Einkauf, F&E, Marketing, Unternehmensstrategie und die Geschäftsführung. 27

Die Wettbewerbsbehörden und Gerichte haben den Kreis des verbotenen Informationsaustauschs immer weiter gezogen. Selbst die einmalige Information eines Wettbewerbers kann als Kartellverstoß geahndet werden.¹⁸ Es muss sich auch nicht unbedingt um einen Austausch handeln. Auch die einseitige Unterrichtung gilt als Kartellabsprache, wenn die Information für das Marktverhalten relevant ist und der Empfänger die Mitteilung widerspruchslos entgegennimmt. Umgekehrt kann auch für den Empfänger die einseitige Entgegennahme der Äußerung eines Wettbewerbers, die wettbewerbslich sensible Informationen enthält, kartellrechtlich verboten sein. 28

Beispiel: Vertriebsmitarbeiter A des Unternehmens X steht schweigend in der Bar an der Theke und trinkt ein Bier. Vertriebsmitarbeiter B des Unternehmens Y sitzt schweigend daneben. A sagt in die Luft: „Nächste Woche gehen wir [mit den Preisen] 2 % hoch.“ B sagt nichts, trinkt sein Bier aus und geht. 29

Ebenso wenig kommt es darauf an, ob die Informationen direkt zwischen den Beteiligten ausgetauscht werden oder ob der Austausch über eine dritte Partei erfolgt. Ein Kartellverstoß liegt z. B. vor, wenn die Unternehmen ihre Daten an einen Verband oder ein Marktforschungsinstitut/Beratungsunternehmen übersenden und diese die Daten so aufbereiten, dass Rückschlüsse auf das geschäft- 30

¹⁷ Nach der Entscheidungspraxis müssen zu diesem Zweck die Angaben von mindestens fünf Unternehmen zusammengefasst werden.

¹⁸ EuGH, 4.6.2009 – Rs. C-8/08, ECLI:EU:C:2009:343 – T-Mobile Netherlands u. a.

liche Verhalten einzelner Unternehmen möglich bleiben.¹⁹ Ein weiterer Problemereich sind schließlich Informationen, die zur Unterrichtung der Öffentlichkeit bestimmt sind. Zulässig sind nicht nur vorgeschriebene Mitteilungen z. B. aufgrund börsenrechtlicher Vorschriften, sondern auch eine sachgerechte Unterrichtung der Kunden und der Öffentlichkeit z. B. über eine bevorstehende Preiserhöhung wegen gestiegener Rohstoffpreise. Wenn diese Mitteilung aber tatsächlich einer wie auch immer gearteten Abstimmung mit Wettbewerbern unterliegt, wäre dies eine verbotene Preisabsprache. Insoweit bedürfen auch öffentliche Verlautbarungen stets einer genauen Prüfung.²⁰

(4) Verbandsarbeit

- 31 Die Mitwirkung an der Verbandsarbeit ist eine legitime Aufgabe der Unternehmen, die die Mitglieder bei der Ausübung ihrer operativen Tätigkeit erheblich unterstützt. Zu den legitimen Themen zählen z. B. allgemeine Gespräche zu regulatorischen Anforderungen, zu Qualität und Normierung, zum Umweltschutz, zu technischen Entwicklungen, zu Messen und zur Positionierung im Lobbying.
- 32 Teilnehmern an Verbandstreffen wird sich aber in einigen Fällen die Frage stellen, wie sie dafür sorgen können, dass der Kontakt mit Wettbewerbern bei Verbandstreffen kartellrechtskonform verläuft und keine kartellrechtswidrigen Themen besprochen werden. Die meisten Verbände haben inzwischen eigene Kartellrechtsleitfäden, die inhaltliche und organisatorische Vorgaben für den Ablauf von Verbandssitzungen enthalten.²¹ Oft ist auch ein Verbandsmitarbeiter bei Arbeitstreffen anwesend, der unter anderem die Einhaltung des Kartellrechtsleitfadens sicherstellen soll. Dennoch sollten Unternehmen die Einhaltung des Kartellrechts nicht der Verbandsorganisation überlassen, sondern ihre ohnehin bestehende Verantwortung für das kartellrechtskonforme Verhalten ihrer Vertreter wahrnehmen.
- 33 (Potenzielle) Mitglieder in Verbänden bekommen z. B. durch das ICC Toolkit zur kartellrechtlichen Compliance hilfreiche Leitlinien an die Hand, die bei einer „Due Diligence“ im Zusammenhang mit Verbänden unterstützen.
- 34 Selten, aber nicht ausgeschlossen sind formelle Verbandsbeschlüsse, die eine Wettbewerbsbeschränkung darstellen. Das größere Risiko bergen separate Gespräche am Rande oder bei Gelegenheit von Verbandsveranstaltungen, insbeson-

19 So ermittelte die finnische Kartellbehörde zu Informationsaustausch auf Grundlage von AC Nielsen ScanTrack-Daten; *Rivas/Van De Walle De Ghelcke*, e-Competitions, N°43913.

20 Siehe nur Europäische Kommission, Pressemitteilung vom 30.1.2024, Kommission führt unangekündigte Nachprüfungen bei Anbietern von Autoreifen durch, https://ec.europa.eu/commission/presscorner/detail/de/ip_24_561 (zuletzt abgerufen am 25.4.2024).

21 Z. B. BDI Leitfaden Kartellrecht, https://bdi.eu/media/themenfelder/wettbewerb/publikationen/201510_Leitfaden-Kartellrecht.pdf, sowie Leitfaden Kartellrecht im VDA, <https://www.vda.de/aktuelles/publikationen/publication/leitfaden-kartellrecht-im-vda> (beide Quellen zuletzt abgerufen am 25.4.2024).

dere wenn der Teilnehmerkreis beschränkt ist. Hier finden die allgemeinen Beurteilungsregeln insbesondere zum Informationsaustausch Anwendung.

Häufig ist es Aufgabe der Verbände, Statistiken und Übersichten zu ihrem Wirtschaftszweig auszuarbeiten und zu veröffentlichen. Dabei müssen alle sensiblen inhaltlichen Angaben so aggregiert werden, dass keine Rückschlüsse auf einzelne Unternehmen und ihr Geschäftsverhalten möglich sind (siehe → Rn. 26). Kein Unternehmen darf Einblick in die nicht aggregierten Daten erhalten. 35

(5) Preisbindungen und Preisempfehlungen

Vereinbarungen zwischen Herstellern und Händlern über den Vertrieb von Produkten oder Dienstleistungen werden als vertikale Beziehungen bezeichnet. Sie sind i. d. R. wettbewerblich weniger bedenklich als horizontale Absprachen zwischen Wettbewerbern. Aber auch bei (vertikalen) Vertriebsvereinbarungen sind Hardcore-Kartellverstöße möglich und werden sowohl von der Europäischen Kommission als auch vom Bundeskartellamt, aber auch von vielen weiteren Kartellbehörden weltweit verstärkt verfolgt. 36

Keine Anwendung findet das Kartellrecht auf den Eigenvertrieb des Herstellers, da er nicht auf Absprachen mit anderen Unternehmen beruht. Gleiches gilt für den Vertrieb durch Handelsvertreter, wenn es sich um „echte“ Handelsvertreter i. S. d. Kartellrechts handelt.²² Ihnen ist in Bezug auf den Vertrieb der Produkte kein oder nur ein geringes Risiko auferlegt. Sie gelten dann als „verlängerter Arm“ des Auftraggebers und unterliegen insoweit nicht dem Kartellrecht. 37

Zu den wichtigsten vertikalen „Hardcore-Kartellen“ gehört die Preisbindung durch den Hersteller gegenüber seinen Händlern.²³ Der Hersteller darf seine Händler in der Gestaltung der Wiederverkaufspreise nicht beschränken oder in irgendeiner Form hierauf Einfluss nehmen. Die unzulässigen Vorgaben des Herstellers können eine rechtliche oder auch nur faktische Bindung der Händler bewirken, z. B. indem der Hersteller erkennen lässt, dass der Händler, wenn er den Wünschen oder Erwartungen des Herstellers nicht Rechnung trägt, mit Konsequenzen rechnen muss. Unter dieser Voraussetzung sind auch bloße Preisempfehlungen verboten, gleichgültig ob sie als unverbindlich bezeichnet werden. Der Händler muss völlig frei bleiben, der Preisempfehlung des Herstellers zu folgen oder nicht. Auch hier geht das Bundeskartellamt sehr weit und hat bereits 38

²² Europäische Kommission, Leitlinien für vertikale Beschränkungen, ABl. C 248/1, vom 30.6.2022, Rn. 29 ff.

²³ So verhängte die Europäische Kommission Bußgelder in Höhe von 111 Mio. EUR wegen Preisbindungsmaßnahmen im Vertikalverhältnis gegen Elektronikhersteller, Pressemitteilung vom 24.7.2018. Das Bundeskartellamt ahndete Preisbindungen zuletzt in den Bereichen Schutzkleidung (783.900 EUR, Pressemitteilung vom 13.3.2024), Unterhaltungselektronik (7 Mio. EUR, Pressemitteilung vom 2.12.2021), Schulrucksäcke (2 Mio. EUR, Pressemitteilung vom 1.10.2021) und Musikinstrumente (21 Mio. EUR, Pressemitteilung vom 17.8.2021).

mehrmalige telefonische oder direkte Kontakte des Herstellers mit seinen Händlern als eine unzulässige Druckausübung angesehen.²⁴

- 39 Die Preisbindung muss sich nicht unbedingt auf einen bestimmten Preis bzw. einen Mindest- oder Wiederverkaufspreis beziehen. Untersagt sind alle Absprachen des Herstellers, die den Händler in Bezug auf preisbezogene Elemente einschränken. Dazu gehören z. B. Rabatte, Margen, Spannen etc.
- 40 Zulässig sind dagegen Vereinbarungen über Höchstpreise. Es muss sich aber um echte Obergrenzen handeln, d. h. eine Preisunterschreitung muss für den Händler möglich und wirtschaftlich sinnvoll sein.

(6) Marktaufteilungen beim Vertrieb

- 41 Die Europäische Kommission verfolgt seit Langem mit besonderem Nachdruck alle Praktiken von Unternehmen, die auf eine künstliche Abschottung innerhalb des einheitlichen europäischen Binnenmarktes hinauslaufen.²⁵ Die klarste Form sind Im- und Exportverbote, die den Händlern vom Hersteller auferlegt werden, wenn sie auch sogenannte passive Verkäufe einschließen. Um einen passiven Verkauf handelt es sich dann, wenn die Initiative zum Kauf vom Kunden ausgeht, der Kunde sich also aus eigener Entscheidung an den Händler wendet (auch als „Komm-Kunde“ bezeichnet). Grundsätzlich erlaubt ist es dagegen, wenn dem Händler nur die Akquisition von Kunden z. B. durch gezielte Ansprache untersagt wird (sog. aktive Verkäufe).²⁶

- 42 **Beispiel:** Ein Kunde in Frankreich bestellt bei X zu einem in Frankreich üblichen Marktpreis. X befürchtet, dass die Produkte zum Weiterverkauf in Belgien bestimmt sind, wo der Marktpreis höher liegt. Der Kunde macht dort bedeutende Umsätze und kann die Preise seiner Wettbewerber unterbieten. Um seinen Umsatz und seine Kundenbeziehungen in Belgien zu schützen, beliefert X den Wiederverkäufer unter der Bedingung, dass dieser die Produkte nicht an Kunden in Belgien verkauft. Eine solche pauschale Kundenkreisbeschränkung stellt einen schweren Verstoß gegen das Kartellrecht dar. Hätte sich X die Belieferung von Kunden in Belgien ausschließlich selbst vorbehalten oder einem anderen Händler zugewiesen, wäre ein Verbot aktiver Verkäufe unter Umständen zulässig (passive Verkäufe jedoch in keinem Fall).

24 Das Bundeskartellamt hat seine Praxis im „Hinweispapier Preisbindung im Lebensmitteleinzelhandel“ vom 12.7.2017 im Einzelnen erläutert, abrufbar unter www.bundeskartellamt.de.

25 So verhängte sie zuletzt Bußgelder in Höhe von 6,7 Mio. EUR gegen die Hotelkette Meliá wegen Beschränkungen der Reiseveranstalter in Bezug auf die Vermittlung von Hotelunterkünften abhängig vom Wohnsitz der Verbraucher, Pressemitteilung vom 21.2.2020. Ebenso erging ein Bußgeld in Höhe von 14,3 Mio. EUR gegen NBC Universal wegen per-se Beschränkungen des Verkaufs außerhalb zugewiesener Gebiets- bzw. Kundengruppen, Pressemitteilung vom 30.1.2020.

26 Voraussetzung für die Zulässigkeit solcher Gebiets- oder Kundenschutzklauseln in Alleinvertriebsverträgen ist allerdings, dass die Marktanteile beider Parteien weniger als 30 % betragen; siehe dazu → Rn. 57.

In derselben Weise verfolgt die Kommission alle Maßnahmen, die im Ergebnis eine vergleichbare Marktabstottung bewirken. So will die Kommission grundsätzlich vermeiden, dass ein Hersteller seinen Händlern vorschreibt oder ihnen nahelegt, dass sie an Kunden aus anderen Staaten nicht oder nur zu einem höheren Preis verkaufen dürfen. Gleiches würde aus Sicht der Kommission für regional begrenzte Marktabstottungen gelten (z.B. kein Verkauf an Kunden aus einer anderen Stadt). Eine unzulässige Behinderung kann auch darin liegen, dass der Hersteller dem Händler nur eine solche Menge an Produkten zur Verfügung stellt, dass er nur seine festen Kunden und keine neuen zusätzlichen Kunden beliefern kann.²⁷ Mit einer solchen Praxis kann der Hersteller bezwecken, einen für ihn unerwünschten Parallelhandel bzw. Grauiimporte aus anderen Staaten zu unterbinden. Grundsätzlich ist die Behinderung von Parallelimporten oder von Grauiporten durch den Hersteller eine von der Kommission nicht gewünschte Wettbewerbsbeschränkung.²⁸

Schwierig kann in diesen Fällen die Feststellung sein, ob es sich um gemeinsame Absprachen oder einseitige Handlungen des Herstellers handelt. Letztere sind keine Vereinbarungen und unterfallen deshalb nicht dem Verbot wettbewerbsbeschränkender Vereinbarungen. Ordnet also der Hersteller ohne Abstimmung mit den Händlern bestimmte Maßnahmen an, ist dies als einseitiges Verhalten kein Kartellverstoß. Hier ist aber Vorsicht geboten. Denn die Rechtsprechung nimmt in solchen Fällen mitunter eine stillschweigende Zustimmung der Händler an, die als Vereinbarung gewertet wird und zur Anwendung des Kartellrechts führt.²⁹ Eine stillschweigende Zustimmung kann vorab erteilt sein, z.B. durch Klauseln im Händlervertrag, die den Hersteller zu den getroffenen Maßnahmen berechtigen. Sie kann aber auch nachträglich erfolgen, indem die Händler die Anordnungen des Herstellers tatsächlich befolgen.

(7) Internet-Behinderungen

Zunehmend aktuell, aber im Einzelnen auch schwierig zu beurteilen sind Behinderungen des Internetvertriebs. Die EU-Kommission hat hierzu eine umfangreiche Sektoruntersuchung durchgeführt.³⁰ Im Abschlussbericht vom Mai 2017 stellte sie fest, dass Hersteller mit ihren Internet-Händlern vielfach Vereinbarungen trafen, die den Wettbewerb in problematischer Weise beschränkten. Hersteller wollen generell häufig das Image ihrer Produkte schützen, indem sie alle oder

27 Voraussetzung ist, dass es sich hierbei nicht um eine einseitige Maßnahme des Herstellers handelt. Vgl. dazu EuGH, 6.1.2004 – Rs. C-2/01 P, ECLI:EU:C:2004:2 – Bayer/Kommission und den nachfolgenden Absatz.

28 Ausnahmen sind dann denkbar, wenn staatliche Preisregelungen, wie dies z.B. bei Medikamenten der Fall ist, zu starken Wettbewerbsverzerrungen führen. In einem solchen Fall kann es dem Hersteller erlaubt sein, sich hiergegen zu schützen, vgl. EuGH, 6.1.2004 – Rs. C-2/01 P, ECLI:EU:C:2004:2, Rn. 53 ff. – Bayer/Kommission.

29 Siehe dazu z.B. EuGH, 6.1.2004 – Rs. C-2/01 P, ECLI:EU:C:2004:2 – Bayer/Kommission.

30 Einzelheiten zur Sektoruntersuchung E-commerce finden sich auf der Internetseite der GD Wettbewerb der Europäischen Kommission.

bestimmte Internetverkäufe durch Händler verbieten. Dies ist jedoch nicht uneingeschränkt möglich. Der Hersteller kann zwar von seinen Händlern verlangen, dass sie ein festes Verkaufslokal ordnungsgemäß einrichten („Brick and click“-Klausel). Er darf jedoch seinen Händlern, die ein solches Verkaufslokal besitzen, nicht ohne Grund untersagen, daneben auch über das Internet zu vertrieben. Ergänzend zu den bislang geltenden Regeln wurde 2018 eine sog. Geoblocking-Verordnung³¹ erlassen. Diese verbietet es Händlern, Kunden aus anderen Mitgliedstaaten vom Zugang zu ihren Internet-Portalen auszuschließen.³²

- 46** Verboten sind wie beim passiven Verkauf (siehe dazu → Rn. 41 f.) alle Vereinbarungen, die den Vertrieb des Händlers über das Internet ausschließen oder erheblich behindern. Zulässig sind dagegen andere Beschränkungen des Online-Verkaufs, die nicht auf ein faktisches Verbot abzielen. Die Abgrenzung ist problematisch und z. T. umstritten. Für etwas Klarheit gesorgt haben aber mittlerweile die neuen Vertikal-Leitlinien der Europäischen Kommission, die Beispiele aufzählen. Zulässig sind demnach u. a. Vorgaben des Herstellers, die Mindestanforderungen an den Internetauftritt vorschreiben (sog. Qualitätsanforderungen), wie z. B. Vorgaben an die Gestaltung des Internetauftritts, die Verpflichtung der Händler, bestimmte Mengen vorrätig zu halten und die Lieferfristen einzuhalten, Anforderungen an die Beratung beim Kauf sowie den Service nach dem Kauf, aber auch die Anforderung, dass der Händler neben dem Onlineshop auch physische Verkaufsstätten betreiben muss. Solche Klauseln sind wettbewerbsrechtlich zulässig.³³ Grundsätzlich ist danach zu fragen, ob die Einschränkung darauf abzielt, die wirksame Nutzung des Internets durch den Händler zu verhindern. Das ist beispielsweise dann der Fall, wenn dem Händler die Nutzung von Preisvergleichsdiensten oder anderen Online-Werbekanälen gänzlich verboten wird.³⁴ Unterschiedliche Preise für den Offline- und den Online-Vertrieb (sog. Dual Pricing) darf der Hersteller nur verlangen, soweit dies als Anreiz zu Investitionen in den jeweiligen Vertriebskanal erforderlich oder durch konkrete Kostenunterschiede gerechtfertigt ist. Außerdem muss er in allen Fällen darauf achten, dass die Einschränkungen diskriminierungsfrei für alle Händler und ggf. auch für ihn selbst in gleicher Weise gelten. Die Wettbewerbsbehörden waren bislang bei der Verhängung von Bußgeldern zurückhaltend.³⁵ Es steht allerdings zu erwarten, dass die Behörden angesichts der stetig wachsen-

31 Verordnung (EU) 2018/302 des Europäischen Parlaments und des Rates vom 28. Februar 2018, ABl. L 60 I/1.

32 Hierbei geht es um einseitige Maßnahmen der Händler, die mangels einer Vereinbarung von den allgemeinen Regeln des Wettbewerbsrechts nicht erfasst werden.

33 Europäische Kommission, Leitlinien für vertikale Beschränkungen, ABl. C 248/1, vom 30.6.2022, Rn. 208.

34 Europäische Kommission, Leitlinien für vertikale Beschränkungen, ABl. C 248/1, vom 30.6.2022, Rn. 206.

35 Bereits im Jahr 2009 hat das Bundeskartellamt allerdings einem Kontaktlinsenhersteller ein Bußgeld in Höhe von 11,5 Mio. EUR auferlegt, nachdem dieser u. a. den Internetvertrieb gänzlich untersagt hatte. BKartA, Pressemitteilung vom 25.9.2009, B3-123/08 – CIBA Vision.

den Bedeutung des Online-Vertriebs und des Plattformgeschäfts als auch der stärkeren Regulierungen auch in diesem Bereich aktiver werden.

Unterschiedliche Auffassungen bestehen zwischen den nationalen Wettbewerbsbehörden, inwieweit Betreiber von Plattformen mit den Anbietern vereinbaren dürfen, dass ihnen jeweils die günstigsten Konditionen eingeräumt werden (sog. „Bestpreisklauseln“).³⁶ Dies betraf vor allem Hotelvermittlungsdienste wie HRS und Booking.com, die für ihre Kunden immer den „besten Preis“ sicherstellen wollten. Während sog. weite Bestpreisklauseln übereinstimmend als kartellrechtlich unzulässig beurteilt werden,³⁷ ist dies für enge Bestpreisklauseln nicht pauschal zu beantworten. Solche Klauseln untersagen es den Anbietern lediglich, über eigene Buchungswege günstigere Konditionen anzubieten als über die Plattform. Der BGH hat eine solche Klausel eines Hotelvermittlungsdienstes zuletzt für unzulässig erachtet, da im konkreten Einzelfall die wettbewerbsbeschränkende Wirkung der Klausel nicht gerechtfertigt gewesen sei.³⁸ In der Vorinstanz war diese noch als notwendige Nebenabrede betrachtet worden, um Trittbrettfahrer-Effekte zu vermeiden und so den fairen Leistungsaustausch zwischen Plattform- und Hotelbetreiber zu gewährleisten.³⁹ Auch nach Ansicht der Europäischen Kommission können Bestpreisklauseln unter gewissen Voraussetzungen vom Kartellverbot freigestellt sein.⁴⁰ Nach der neuen Vertikal-GVO kann nämlich eine Freistellung erfolgen, wenn eine Bestpreisklausel nicht unter die neue Spezialregelung zu weiten Bestpreisklauseln von Online-Vermittlern fällt.⁴¹ Jedenfalls aber bedürfen sie einer umfassenden Prüfung im Einzelfall, bei der unter anderem auch die Marktmacht des Plattformbetreibers eine Rolle spielt.⁴² Ein weiterer Schwerpunktbereich mit z. T. noch offenen Fragen sind vertragliche Vereinbarungen von Herstellern und Händlern, in denen die Verwendung aller oder bestimmter Internet-Plattformen (z. B. Amazon, Ebay) für den Vertrieb untersagt wird. Im Vorlageverfahren Coty hat der EuGH im Dezember 2017 entschieden, dass Drittplattformverbote in selektiven Vertriebssystemen dann mit dem Kartellrecht vereinbar sind, wenn die Anforderungen zum Schutz der Aura bzw. des Luxuscharakters des Produkts erforderlich sind, diskriminierungsfrei angewendet werden und nicht über das notwendige Maß hinausge-

47

36 Zur deutschen Entscheidungspraxis siehe sogleich. Zur Entscheidungspraxis der französischen, italienischen und schwedischen Wettbewerbsbehörde siehe *Weitbrecht/Mühle*, EuZW 2016, 172, 175 m. w. N.

37 Im Verfahren HRS ist dies durch das OLG Düsseldorf in vollem Umfang bestätigt worden, OLG Düsseldorf, 9.1.2015 – VI-Kart. 1/14 (V), BB 2015, 593 ff.

38 BGH, 18.5.2021 – KVR 54/20 – Booking.com.

39 OLG Düsseldorf, 4.6.2019 – VI-Kart 2/16 (V), NZKart 2019, 379 – Enge Bestpreisklausel II.

40 Europäische Kommission, Leitlinien für vertikale Beschränkungen, ABl. C 248/1, vom 30.6.2022, Rn. 253.

41 *Wegner/Schwenker/Altdorf*, ZWer 2022, 243, 278; *Kohm/Eppelmann*, GRUR-Prax 2022, 458.

42 Europäische Kommission, Leitlinien für vertikale Beschränkungen, ABl. C 248/1, vom 30.6.2022, Rn. 369 ff.

hen.⁴³ Plattformverbote stellen auch keine Kernbeschränkung dar, sofern es den Händlern unbenommen bleibt, die Produkte über ihre eigenen Internetseiten zu vertreiben (unter Berücksichtigung der Qualitätsanforderungen). Die grundsätzliche Zulässigkeit von Plattformverboten unter diesen Voraussetzungen ist mittlerweile auch in der Vertikal-GVO 2022 kodifiziert worden. Für das Bundeskartellamt ist ein wichtiger Gesichtspunkt, ob die vom Plattformverbot betroffenen Händler andere wirtschaftlich sinnvolle Möglichkeiten haben, das Internet für ihren Vertrieb zu nutzen. Einer Übertragung auf andere Produkte als Luxusgüter steht das Amt skeptisch gegenüber.⁴⁴ Die Europäische Kommission vertritt dagegen die Auffassung, dass auch der Vertrieb anderer hochwertiger oder hochtechnologischer Produkte Drittplattformverbote rechtfertigen könne. Insofern hat sie die im *Coty*-Urteil aufgestellten Kriterien für die Zulässigkeit von Plattformverboten übernommen und sogar erweitert.⁴⁵ Ein Risiko besteht für Hersteller vor allem dann, wenn sie selbst über Plattformen vertreiben oder das Plattformverbot nicht konsequent anwenden, z. B. den Vertrieb über einzelne Billiganbieter zulassen.⁴⁶

(8) Boykott

- 48** Der Boykott ist eine zwischen mehreren Unternehmen abgestimmte Liefer- oder Bezugssperre, die sich gegen ein anderes Unternehmen richtet.⁴⁷ Sie stellt einen schwerwiegenden Wettbewerbsverstoß dar. Auch dieses Verbot ist weit auszulegen. Die Liefer- oder Bezugssperre kann nicht nur im Abbruch bestehender, sondern auch in der Nichtaufnahme neuer Geschäftsbeziehungen bestehen.

(9) Personalbereich

- 49** Zuletzt nach dem Vorbild der USA sind auch in der EU Absprachen zwischen Unternehmen im Personalbereich in den Fokus gerückt. Die Bewertung der kartellrechtlichen Zulässigkeit hängt dabei von der konkreten Absprache ab. Unterschieden werden kann zwischen Nichtanstellungsvereinbarungen („No-hire Agreements“), Abwerbeverboten („No-poaching Agreements“), Gehaltsabsprachen („Wage Fixing“) und anderem Informationsaustausch zwischen Personalverantwortlichen.⁴⁸ Derartige Absprachen können sowohl eine unzulässige Marktaufteilung, einen Boykott zulasten der Mitarbeiter, ein letztlich mit Preisabsprachen gleichzusetzendes Kartell als auch einen unzulässigen Informations-

43 EuGH, 6.12.2017 – Rs. C-230/16.

44 Siehe dazu z. B. den auf seiner Internetseite veröffentlichten Beitrag zum Thema „Wettbewerbsbeschränkungen im Internetvertrieb nach *Coty* und *Asics* – wie geht es weiter?“, Oktober 2018.

45 Europäische Kommission, Leitlinien für vertikale Beschränkungen, ABl. C 248/1, vom 30.6.2022, Rn. 149.

46 Europäische Kommission, Leitlinien für vertikale Beschränkungen, ABl. C 248/1, vom 30.6.2022, Rn. 342.

47 Rechtsgrundlage im deutschen Recht ist § 21 Abs. 1 GWB.

48 *Steinle/Fuhrer*, CB 2023, 201, 202 f.

austausch darstellen. Die EU-Kommissarin für Wettbewerb *Vestager* stellte ebenfalls klar, dass derartige Absprachen ein Kartell darstellen können.⁴⁹

Einschlägige Verfahren sind bisher vorwiegend auf nationaler Ebene bekannt geworden.⁵⁰ Die Europäische Kommission hat bei entsprechendem Verdacht aber zuletzt ebenfalls Nachprüfungen durchgeführt.⁵¹ Es scheint sich eine Tendenz abzuzeichnen, dass die Wettbewerbsbehörden jedenfalls bei Gehaltsabsprachen und Nichtanstellungsvereinbarungen eine bezweckte Wettbewerbsbeschränkung annehmen.⁵² Darüber hinaus gab etwa die portugiesische Kartellbehörde bereits ein „Best Practice“-Papier zu der Thematik heraus.⁵³ 50

Das Bundeskartellamt beschäftigte sich mit dem Arbeitsmarkt bislang lediglich am Rande. So wurde im Rahmen eines mit einem Bußgeld sanktionierten Informationsaustauschs auch die anzusetzenden Personalkostensätze für freie Mitarbeiter erwähnt.⁵⁴ Im Rahmen eines Leitfadens zur Fusionskontrolle stellt das Bundeskartellamt zudem klar, dass es für die Vereinbarung eines Abwerbverbots wichtiger Mitarbeiter einer Erforderlichkeit für ein solches im konkreten Fall bedarf.⁵⁵ Auch hier dürfte zu erwarten sein, dass derartige Vereinbarungen künftig zunehmend in den Fokus der Wettbewerbsbehörden gelangen. 51

dd) Weniger hohe Risiken

(1) Horizontale Kooperationen

Das Kartellrecht erfasst nicht nur Kartelle im engeren Sinn, sondern findet grundsätzlich auch Anwendung auf vielfältige Formen der betrieblichen oder geschäftlichen Zusammenarbeit mit anderen Unternehmen. Kartellrechtlich vertiefter Analyse bedürfen dabei in der Regel nur Kooperationen von Unternehmen, die im Wettbewerb stehen oder bei denen ein Wettbewerbsverhältnis zumindest möglich ist (potenzieller Wettbewerb). Gegenstand der Zusammenarbeit können alle Unternehmenstätigkeiten sein. In der Praxis finden sich Kooperationen vor allem in den Bereichen F&E, Produktion, Einkauf, Vermarktung und Lizenzierung. 52

49 *Vestager*, Rede vom 22.10.2021, SPEECH/21/7877, https://ec.europa.eu/commission/presscorner/detail/en/speech_21_7877 (zuletzt abgerufen am 25.4.2024), „can create a cartel“.

50 Für eine Übersicht: *Steinle/Fuhrer*, CB 2023, 201, 204 f.

51 Europäische Kommission, Pressemitteilung vom 21.3.2023, IP/23/5944, https://ec.europa.eu/commission/presscorner/detail/de/ip_23_5944 (zuletzt abgerufen am 25.4.2024).

52 OECD (2020), *Competition in Labour Markets*, S. 28, <https://web-archiv.oecd.org/2020-03-10/546723-competition-in-labour-markets-2020.pdf> (zuletzt abgerufen am 25.4.2024).

53 AdC, *Best Practices in preventing Anticompetitive Agreements in Labor Markets*, <https://www.concurrencia.pt/en/public-consultations/public-consultation-draft-report-labor-market-agreements-and-competition> (zuletzt abgerufen am 25.4.2024).

54 BKartA, Fallbericht vom 12.9.2016 zur Entscheidung vom 26.6.2016, B12–23/15 – Fernsehstudiotreiber.

55 BKartA, Leitfaden Zusagen in der Fusionskontrolle (2017), Rn. 102.

- 53 Die Wettbewerbsbeschränkungen sind in diesen Fällen meist nicht bezweckt, sondern es handelt sich um bewirkte Wettbewerbsbeschränkungen. Hier ist in jedem Einzelfall konkret festzustellen, ob die Vereinbarung tatsächlich den Wettbewerb beschränkt und nicht – im Gegenteil – fördert. Es kommt also darauf an, ob die Kunden/Verbraucher oder andere Marktteilnehmer nachweisbar durch die Absprache geschädigt sind und Nachteile erleiden. Nach dem neueren wirtschaftlichen Ansatz der Wettbewerbsbehörden (sog. „More Economic Approach“) setzt dies voraus, dass die Unternehmen über ein gewisses Maß an Marktmacht verfügen.⁵⁶ Das ist eine Abkehr von dem früheren rein juristischen Ansatz, der allein darauf abstellte, dass die Zusammenarbeit von Wettbewerbern zu einer Verringerung des Wettbewerbs führt. Zur Ermittlung der Spürbarkeit gelten die sog. Bagatellbekanntmachungen der Europäischen Kommission und des Bundeskartellamtes.⁵⁷ Aus Gründen der Praktikabilität kann danach eine Spürbarkeit verneint werden, wenn der gemeinsame Marktanteil der beteiligten Unternehmen weniger als 10 % beträgt. Sind die Marktanteile höher, bedeutet dies nicht automatisch, dass eine Wettbewerbsbeschränkung spürbar ist; dies muss im Einzelfall konkret festgestellt werden.
- 54 Für einzelne Formen der Kooperation gibt es Sonderregelungen (z. B. sog. Gruppenfreistellungsverordnungen).⁵⁸ Die horizontalen Gruppenfreistellungsverordnungen über F&E und Spezialisierungsvereinbarungen, begleitet von Leitlinien (sog. Horizontalleitlinien) wurden erst jüngst von der Europäischen Kommission überarbeitet und sind am 1.7.2023 in Kraft getreten. Die Gruppenfreistellungsverordnungen sollen den Unternehmen die Feststellung erleichtern, ob eine Wettbewerbsbeschränkung vorliegt und ob diese spürbar ist. Dazu können nur einige allgemeine Hinweise gegeben werden. In allen Zweifelsfällen sollte der Rat von Experten eingeholt werden.
- **Forschung und Entwicklung:** Die Zusammenarbeit im Bereich Forschung und Entwicklung stellt in vielen Fällen keine Wettbewerbsbeschränkung dar. Sie ist unkritisch, wenn die Unternehmen keine Wettbewerber sind, es sich um eher marktferne Grundlagenforschung handelt oder keine gemeinsame Ver-

56 Vgl. Europäische Kommission, Leitlinien zur Anwendbarkeit von Artikel 101 AEUV auf Vereinbarungen über horizontale Zusammenarbeit, ABl. C 164/1 vom 19.4.2022.

57 Bekanntmachung der Europäischen Kommission über Vereinbarungen von geringer Bedeutung, die im Sinne des Artikel 101 Absatz 1 AEUV den Wettbewerb nicht spürbar beeinträchtigen (De-minimis-Bekanntmachung), ABl. C 291/1 vom 30.8.2014; Bekanntmachung Nr. 18/2007 des Bundeskartellamtes über die Nichtverfolgung von Kooperationsabreden mit geringer wettbewerbsbeschränkender Bedeutung vom 13.3.2007, abrufbar unter www.bundeskartellamt.de.

58 Z. B. Verordnung (EU) Nr. 1067/2023 der Kommission vom 1.6.2023 über die Anwendung von Artikel 101 Absatz 3 AEUV auf bestimmte Gruppen von **Spezialisierungsvereinbarungen**, ABl. L 143/20 vom 2.6.2023 und Verordnung (EU) Nr. 1066/2023 der Europäischen Kommission vom 1.6.2021 über die Anwendung von Artikel 101 Absatz 3 AEUV auf bestimmte Gruppen von **Vereinbarungen über Forschung und Entwicklung**, ABl. L 143/9 vom 2.6.2023. Siehe dazu auch KOM, Leitlinien zur Anwendbarkeit von Artikel 101 AEUV auf Vereinbarungen über horizontale Zusammenarbeit, ABl. C 164/1 vom 19.4.2022.

marktung der Forschungsergebnisse vereinbart ist. Liegt eine Wettbewerbsbeschränkung vor, ist diese freigestellt, wenn der gemeinsame Marktanteil der beteiligten Unternehmen weniger als 25 % beträgt. In diesem Fall ist auch der gemeinsame Vertrieb der Produkte durch die beteiligten Unternehmen oder einen beauftragten Dritten zulässig. Voraussetzung für die Freistellung ist, dass die Unternehmen in ihrer eigenen F&E-Tätigkeit in keiner Weise eingeschränkt sind. Soweit es gesetzliche Vorschriften zu technischen Standards gibt und den Herstellern eine Übererfüllung technisch möglich ist, kann eine (implizit) vereinbarte Nichteinführung eine Wettbewerbsbeschränkung darstellen, soweit der (fehlenden) Umsetzung auch eine wettbewerbliche Relevanz zukommt. Dies gilt selbst dann, wenn die zugrunde liegende Kooperation im Ausgangspunkt nicht zu beanstanden war.⁵⁹

- **Gemeinsame Produktion bzw. Spezialisierung:** In diesen Fällen liegt meist eine Wettbewerbsbeschränkung vor, da die Zusammenarbeit einen umfangreichen Austausch von Informationen erfordert und eine erhebliche Kostenangleichung bewirken wird. Dennoch sind diese Vereinbarungen vom Kartellverbot freigestellt, wenn der gemeinsame Marktanteil der Parteien nicht mehr als 20 % beträgt und gewisse Anforderungen erfüllt sind.⁶⁰ Die Kooperation kann sowohl in der gemeinsamen Produktion als auch in einer Spezialisierung bestehen, in der die Unternehmen die Produktion untereinander aufteilen. Mit freigestellt ist in beiden Fällen der gemeinsame Vertrieb durch die Parteien oder einen beauftragten Dritten.
- **Gemeinsamer Einkauf:** Einkaufskooperationen stellen grundsätzlich keine Wettbewerbsbeschränkung dar, wenn der gemeinsame Marktanteil der beteiligten Unternehmen sowohl beim Einkauf als auch bei der Vermarktung nicht mehr als 15 % beträgt. Oberhalb dieser Schwelle und in Abhängigkeit von Art und Gegenstand des Austauschs bzw. der Vereinbarung auf der Einkaufsseite besteht jedoch das Risiko der Annahme eines Verstoßes. So verhängte die Kommission Bußgelder gegen die Abnehmer der Chemikalie Ethylen,⁶¹ ebenso wie gegen Abnehmer des chemischen Zwischenproduktes Styrolmonomer.⁶² Diese sprachen sich jeweils ab, um den Referenzpreis, den sogenannten „Monthly Contract Price“, und so in der Konsequenz die von den Einkäufern zu zahlenden Preise zu beeinflussen.
- **Gemeinsame Vermarktung:** Vereinbarungen über eine gemeinsame Vermarktung der Produkte sind unzulässig, wenn hierbei die Preise abgestimmt oder Kunden bzw. Gebiete unter den beteiligten Unternehmen aufgeteilt werden. In den anderen Fällen, in denen keine solche „Hardcore-Kartellabspra-

⁵⁹ von Köckritz/Wessely, in: Schröter/Klotz/von Wendland, Europäisches Wettbewerbsrecht, Art. 101 AEUV Rn. 376.

⁶⁰ Die Parteien dürfen z. B. keine Preise für den Verkauf der Produkte außerhalb eines gemeinsamen Vertriebs festsetzen oder Märkte oder Kunden untereinander aufteilen.

⁶¹ Europäische Kommission, 14.7.2020 – AT 40410 – Ethylen.

⁶² Europäische Kommission, 29.11.2022 – AT.40547 – Styrol.

che“ vorliegt, ist die gemeinsame Vermarktung freigestellt, wenn der Marktanteil der beteiligten Unternehmen insgesamt 15 % nicht übersteigt.

- **Nachhaltigkeitsvereinbarungen:** Vereinbarungen zwischen Wettbewerbern, die Nachhaltigkeitsziele verfolgen, finden die zunehmende Beachtung der Wettbewerbsbehörden.⁶³ Die Europäische Kommission gibt nun in den neuen Horizontalleitlinien erstmals Hinweise und Beispiele, welche Vereinbarungen schon nicht gegen das Kartellverbot verstoßen oder jedenfalls hiervon freigestellt sein können.⁶⁴ Hinsichtlich einer solchen möglichen Freistellung unterliegen Nachhaltigkeitsvereinbarungen ggf. zunächst den sie betreffenden Gruppenfreistellungsverordnungen, bspw. für Forschung und Entwicklung (F&E). Im Übrigen kommt eine Freistellung im Einzelfall in Betracht, wenn die betreffende Vereinbarung zur Erreichung von Effizienzgewinnen unerlässlich ist, an denen die Verbraucher ohne Ausschaltung des Wettbewerbs angemessen beteiligt werden. Zusätzlich zu diesen allgemeinen Hinweisen will die Kommission aber auch informelle Orientierungshilfen für neue oder ungeklärte Fragen im Einzelfall geben. Auch die nationalen Wettbewerbsbehörden setzen einen Fokus auf Nachhaltigkeitsthemen. Dies wird zum einen durch eine stetig wachsende Entscheidungspraxis deutlich. So sah das Bundeskartellamt einen vereinbarten Rückgriff auf Referenzpreise der Entwicklungshilfeforschung bei dem Einkauf bei Kakaobauern als unbedenklich an.⁶⁵ Zugleich werden aber auch kartellrechtliche Grenzen aufgezeigt: Aufgrund vom Bundeskartellamt geäußerter wettbewerbllicher Bedenken entschloss sich die Initiative Tierwohl nach einer Übergangsphase, die verpflichtenden Preisaufschläge für die Abnehmer der teilnehmenden Erzeugerbetriebe abzuschaffen.⁶⁶ Ein dem Bundeskartellamt vorgelegtes Finanzmodell des Agrardialogs Milch, welches Preisaufschläge in der Milchwirtschaft vorsah, erklärte das Bundeskartellamt für kartellrechtlich unzulässig, da es keine anerkannten Gemeinwohlziele feststellen konnte.⁶⁷ Zum anderen geben die nationalen Wettbewerbsbehörden ebenfalls verstärkt Leitlinien und Handreichungen an die

63 Zur zunehmenden Berücksichtigung von ESG-Kriterien im Kartellrecht siehe *Seeliger/Gürer*, DB-Beilage 2023, 58; *Holle*, ZHR 188, 98.

64 Europäische Kommission, Leitlinien zur Anwendbarkeit von Artikel 101 AEUV auf Vereinbarungen über horizontale Zusammenarbeit, ABl. C 259/1 vom 21.7.2023, Rn. 515 ff.

65 BKartA, Pressemitteilung vom 13.6.2023, Forum Nachhaltiger Kakao – Bundeskartellamt sieht keine Veranlassung für tiefergehende Prüfung, https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2023/13_06_2023_Kakaoforum.html (zuletzt abgerufen am 25.4.2024).

66 BKartA, Pressemitteilung vom 25.5.2023, Mehr Wettbewerb für die Initiative Tierwohl – Bundeskartellamt erwirkt Abschaffung des verpflichtenden Preisaufschlags, https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2023/25_05_2023_ITW.html (zuletzt abgerufen am 25.4.2024).

67 BKartA, Pressemitteilung vom 25.1.2022, Preisaufschläge ohne mehr Nachhaltigkeit in der Milchwirtschaft: Bundeskartellamt zeigt kartellrechtliche Grenzen auf, https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2022/25_01_2022_Agrardialog.html (zuletzt abgerufen am 25.4.2024).

Unternehmen heraus, um insoweit für eine gesteigerte Rechtssicherheit von Kooperationen zu sorgen.⁶⁸

(2) Vertriebsbeschränkungen

In Vereinbarungen zwischen dem Hersteller und seinen Händlern sind in vielen Fällen wettbewerbsbeschränkende Regelungen enthalten. Sie können sowohl den Wettbewerb zwischen den Händlern desselben Produkts (Intrabrand-Wettbewerb) als auch den Wettbewerb zwischen verschiedenen Produkten (Interbrand-Wettbewerb) betreffen. Wettbewerbsbeschränkungen im Vertikalverhältnis zwischen Hersteller und Händlern können aber eine wettbewerbsfördernde Wirkung entfalten, wenn sie z. B. dazu beitragen, dass die Händler vermehrte Anstrengungen für eine bessere Versorgung der Kunden oder eine höhere Qualität bei den Serviceleistungen unternehmen. **55**

Vertikale Wettbewerbsbeschränkungen sind daher durch die Gruppenfreistellungsverordnung für vertikale Vereinbarungen (Vertikal-GVO),⁶⁹ die mitsamt begleitender Leitlinien⁷⁰ in ihrer aktuellen Fassung seit Juni 2022 gilt, grundsätzlich freigestellt, mit Ausnahme der bereits erwähnten Hardcore-Kartelle, insbes. der Preisbindung und der Beschränkungen von passiven Verkäufen sowohl im stationären als auch im Internet-Handel.⁷¹ Die Freistellung setzt voraus, dass der Marktanteil sowohl des Herstellers als auch des Händlers für die betroffenen Produkte nicht mehr als 30 % beträgt.⁷² In diesem Fall kommt es nicht darauf an, ob eine Wettbewerbsbeschränkung vorliegt, da die Vereinbarung wegen der Freistellung auf jeden Fall zulässig ist. Bei einem höheren Marktanteil ist dagegen zu prüfen, ob der Intra- oder Interbrand-Wettbewerb eingeschränkt oder behindert wird. Wenn das zu bejahen ist, muss weiter geprüft werden, ob die Vereinbarung zu Effizienzen (z. B. einer besseren Versorgung der Kunden) führt und ob diese Vorteile in angemessenem Umfang an die Verbraucher weitergegeben wer- **56**

68 Siehe hierzu z. B. The Netherlands Authority for Consumers and Markets, Guidelines regarding Sustainability claims vom 13.6.2023, <https://www.acm.nl/en/publications/guidelines-regarding-sustainability-claims>; Österreichische Bundeswettbewerbsbehörde, Leitlinien zur Anwendung von § 2 Abs 1 KartG auf Nachhaltigkeitskooperationen von 1.6.2022, https://www.bwb.gv.at/fileadmin/user_upload/Leitlinien_zur_Anwendung_von___2_Abs_1_KartG_auf_Nachhaltigkeitskooperationen___Nachhaltigkeits-LL___final.pdf (beide Quellen zuletzt abgerufen am 25.4.2024).

69 Verordnung (EU) Nr. 720/2022 der Kommission vom 10.5.2022 über die Anwendung von Artikel 101 Absatz 3 AEUV auf Gruppen von vertikalen Vereinbarungen und abgestimmten Verhaltensweisen, ABl. L 134/4 vom 11.5.2022 (Vertikal-GVO); einen Überblick über die praxisrelevanten Neuerungen in der Vertikal-GVO 2022 geben auch *Schultze/Pautke/Wagener*, WuW 2023, 646 und WuW 2024, 70; für bereits bestehende Verträge galt eine Übergangsfrist bis zum 31.5.2023.

70 Europäische Kommission, Leitlinien für vertikale Beschränkungen, ABl. C 248/1, vom 30.6.2022.

71 Sie werden in der Vertikal-GVO als Kernbeschränkungen (Art. 4) bezeichnet. Im Einzelnen siehe dazu → Rn. 38 ff.

72 Zur Definition des relevanten Marktes siehe die Ausführungen unter → Rn. 63 ff.

den. Außerdem dürfen die Wettbewerbsbeschränkungen nicht über das unbedingt erforderliche Maß hinausgehen und den Wettbewerb nicht vollständig ausschließen.⁷³

57 Für die wichtigsten Vertriebsformen gilt im Einzelnen:

- **Alleinvertrieb:** Wenn der Hersteller nur einen einzigen Händler oder einen kleinen Kreis von maximal fünf ausgewählten Händlern mit dem Vertrieb beauftragt, liegt immer eine (intra-brand-)Wettbewerbsbeschränkung vor. Für die Freistellung ist die Marktanteilsschwelle von 30 % besonders wichtig. Bei höheren Marktanteilen, insbesondere bei Marktmacht oder einer marktbeherrschenden Stellung des Herstellers, sind solche Vereinbarungen grundsätzlich verboten.
- **Alleinbelieferung:** Vereinbarungen, durch die sich der Hersteller verpflichtet, sein Produkt nur an einen einzigen Abnehmer in der EU zu liefern, sind bis zur Marktanteilsschwelle von 30 % (jeweils für Hersteller und Händler) freigestellt. Sie können insbesondere in Zulieferbeziehungen von Bedeutung sein. Wenn sich ein Zulieferer verpflichtet, ein (Zwischen-)Produkt, das er im Auftrag des Endherstellers gefertigt hat, nur an diesen Endhersteller zu liefern, kann dies sogar unabhängig von den Marktanteilen wirtschaftlich gerechtfertigt und zulässig sein.⁷⁴
- **Exklusivvertrieb:** Ein Hersteller kann seinen Vertrieb so organisieren, dass für ein bestimmtes Gebiet oder einen bestimmten Kreis von Kunden immer nur ein Händler ausschließlich zuständig ist. Eine solche Vereinbarung ist grundsätzlich zulässig. Wichtig ist aber, dass insoweit nur der aktive Verkauf exklusiv ausgestaltet ist. Passive Verkäufe⁷⁵ dürfen nur ausnahmsweise insoweit eingeschränkt werden, als dem Alleinvertriebshändler untersagt wird, an andere Händler in einem Gebiet zu verkaufen, in dem der Anbieter ein selektives Vertriebssystem betreibt; auch darf einem Alleinvertriebshändler, der auf der Großhandelsstufe tätig ist, der passive Verkauf an Endverbraucher untersagt werden.⁷⁶ Auch für sich selbst darf der Hersteller ein Gebiet oder einen Kundenkreis vorbehalten. Die Freistellung gilt in allen Fällen nur bis zu der Marktanteilsschwelle von 30 % für Hersteller und Händler.
- **Selektiver Vertrieb:** Der Hersteller kann bestimmte Auswahlkriterien für seine Händler festlegen, um auf diese Weise für eine gleichmäßig hohe Qualität der Händler zu sorgen. Das ist vor allem bei hochwertigen Markenprodukten weit verbreitet. Wenn es sich um reine Qualitätsanforderungen handelt (qualitative Selektion), ist eine solche Vereinbarung keine Wettbewerbsbeschränkung, wenn folgende Voraussetzungen erfüllt sind: Die Anforderungen müssen im Hinblick auf die Eigenart des Produktes angemessen sein, dürfen

⁷³ Dies ist im Einzelnen in Art. 101 Abs. 3 AEUV und § 2 Abs. 1 GWB geregelt.

⁷⁴ Rechtsgrundlage ist insoweit die Zulieferbekanntmachung der Kommission vom 18.12.1978, die immer noch gültig ist (ABl. 1979 C 1/2 vom 3.1.1979).

⁷⁵ Zu diesem Begriff siehe → Rn. 41.

⁷⁶ Dies ergibt sich aus Art. 4 lit. b Ziff. 2 und 4 Vertikal-GVO.

nicht über das erforderliche Maß hinausgehen und müssen diskriminierungs- frei in gleicher Weise auf alle Händler angewandt werden.⁷⁷ Falls die Auswahl nicht für alle Händler einheitlich erfolgt oder die Zahl der Händler begrenzt ist (quantitative Selektion), gilt die Freistellung bis zur doppelten Marktanteilsschwelle von 30 % (jeweils für Hersteller und Händler). Jedem Händler ist es dann untersagt, an Außenseiter, die nicht dem System angehören, zu liefern; selbst passive Verkäufe dürfen dann ausnahmsweise untersagt werden.⁷⁸ Andererseits ist jeder Händler berechtigt, an andere Händler im System oder an Endverbraucher zu verkaufen. Dieses Recht darf vom Hersteller nicht eingeschränkt werden.

- **Franchising:** Vereinbarungen, durch die ein Hersteller seinen Händlern umfangreiches Know-how und meist auch die Nutzung seiner Marke (Firmennamen) zur Verfügung stellt, stellen keine Wettbewerbsbeschränkung dar, wenn die Beschränkungen nicht über das hinausgehen, was zum Schutz des Know-hows erforderlich ist.⁷⁹ Bei weitergehenden Einschränkungen gilt die Freistellung bis zur doppelten Marktanteilsschwelle von 30 % (jeweils für Hersteller und Händler).

(3) Wettbewerbsverbote (Markenzwang); Alleinbezugsverpflichtungen

Nicht selten verlangen Hersteller von ihren Händlern, dass diese keine konkurrierenden Produkte anderer Hersteller vertreiben.⁸⁰ Eine vergleichbare Wirkung haben Vereinbarungen, die den Händler dazu verpflichten, seinen Bedarf ausschließlich oder ganz überwiegend (d. h. zu mehr als 80 %) von dem vorgeschriebenen Anbieter zu beziehen (Alleinbezugsverpflichtungen). Derartige Vereinbarungen sind bis zur doppelten Marktanteilsschwelle von 30 % (jeweils für Hersteller und Händler) freigestellt. Voraussetzung ist aber, dass die Bindung des Händlers eine Dauer von fünf Jahren nicht übersteigt. Neuerdings zulässig ist die Vereinbarung einer automatischen stillschweigenden Verlängerung über diesen Zeitraum hinaus, wenn dem Abnehmer eine angemessene Kündigungsfrist und die Möglichkeit, die Vertragskonditionen neu auszuhandeln, eingeräumt wird. In den „orangenen“ Bereich fallen dabei Klauseln, die nach fünf Jahren eine Bezugsverpflichtung von knapp unter 80 % vorsehen, da sie als missbräuchliche Umgehung gewertet werden könnten.

58

77 So die Definition der Kommission in den Leitlinien für vertikale Beschränkungen, ABl. C 248/1, vom 30.6.2022, Rn. 149; Vgl. auch EuGH, 11.12.1980 – Rs. C-31/80, ECLI:EU:C:1980:289, Rn. 15 f. – L'Oréal/PVBA; 25.10.1977 – Rs. C-26/76, ECLI:EU:C:1977:167, Rn. 21 f. – Metro I; 25.10.1983 – Rs. C-107/82, ECLI:EU:C:1983:293, Rn. 35 – AEG/Kommission.

78 Dies ergibt sich aus dem Wortlaut von Art. 4 lit. c und lit. d Vertikal-GVO.

79 EuGH, 28.1.1986 – Rs. C-161/84, ECLI:EU:C:1986:41 – Pronuptia.

80 Solche Wettbewerbsverbote werden von der Europäischen Kommission auch als Markenzwang bezeichnet, vgl. Europäische Kommission, Leitlinien für vertikale Beschränkungen, ABl. C 248/1, 30.6.2022, Rn. 298 ff.

- 59** Ist ein Marktanteil höher als 30 % oder übersteigt die Dauer des Wettbewerbsverbots bzw. der Alleinbezugsverpflichtung fünf Jahre, ist eine Einzelfallprüfung einer möglichen Freistellung erforderlich.

b) Machtmissbrauch (einseitige Handlungen)

aa) Allgemeine Voraussetzungen

- 60** Während das Verbot wettbewerbsbeschränkender Vereinbarungen nur Vereinbarungen von zwei oder mehr Unternehmen erfasst, gilt das Missbrauchsverbot auch für einseitige Handlungen eines Unternehmens.⁸¹ Dies kann auch der Abschluss einer Vereinbarung sein; dann gelten das Kartell- und das Missbrauchsverbot nebeneinander. Anders als das Verbot wettbewerbsbeschränkender Vereinbarungen richtet sich das Missbrauchsverbot nicht an alle Unternehmen, sondern nur an den kleinen Kreis von Unternehmen, die auf dem relevanten Markt, d.h. unter Umständen für ein Produkt/eine Produktgruppe, über eine marktbeherrschende Stellung verfügen. Kartellrechtlich ist die Erlangung einer marktbeherrschenden Stellung nicht untersagt, sofern dies auf der eigenen geschäftlichen Tüchtigkeit und dem damit verbundenen marktwirtschaftlichen Erfolg beruht.⁸² Wird eine marktbeherrschende Stellung dagegen durch den Zusammenschluss mit einem anderen Unternehmen begründet oder verstärkt,⁸³ greift die Fusionskontrolle.
- 61** Marktbeherrschende Unternehmen dürfen wie jedes andere Unternehmen ihre geschäftlichen Interessen am Markt wahrnehmen. Sie müssen auch nicht auf günstige neue Geschäftsfelder verzichten, selbst wenn sie dadurch ihre Marktposition weiter ausbauen. Aber sie tragen eine besondere Verantwortung, weil der Wettbewerb durch ihre marktbeherrschende Stellung bereits eingeschränkt ist. Ihnen sind deshalb alle Handlungen untersagt, die ihnen nur durch ihre Marktmacht möglich sind und zu denen ein „normales“ Unternehmen nicht in der Lage wäre.
- 62** Um einen Verstoß gegen das Missbrauchsverbot zu begründen, müssen somit zwei Voraussetzungen erfüllt sein. Das Unternehmen muss eine marktbeherrschende Stellung haben, und es muss diese Stellung missbräuchlich ausgenutzt haben. Zahlenmäßig spielen diese Verstöße in der Entscheidungspraxis keine große Rolle. Gleichwohl werden die Grundregeln hier erläutert, weil es durchaus Nischenmärkte gibt, in denen Unternehmen marktbeherrschend sind, ohne es immer selber so analysiert zu haben.

81 Rechtsgrundlage ist im europäischen Recht Art. 102 AEUV, im deutschen Recht sind es §§ 18 ff. GWB.

82 Dies wird auch als internes Wachstum bezeichnet.

83 In diesem Fall handelt es sich um externes Wachstum.

(1) Marktbeherrschende Stellung

Auch diese Prüfung erfolgt in zwei Schritten: Zunächst muss ermittelt werden, wie der relevante Markt abzugrenzen ist. Danach ist festzustellen, ob das Unternehmen auf diesem Markt eine beherrschende Stellung hat. Die Definition des relevanten Marktes gehört zu den schwierigsten Aufgaben im Kartellrecht. Die Wettbewerbsbehörden stellen dabei in zahlreichen Fällen auf die Perspektive der Nachfrager ab. Entscheidend ist dann, ob die Verbraucher für ihren Bedarf auf andere Anbieter ausweichen können. Der Bedarf der Verbraucher wird nur durch Produkte erfüllt, die hinsichtlich Zweck und Qualität, u. U. auch beim Preis bestimmte Eigenschaften erfüllen und vom Kunden als austauschbar angesehen werden. Das kann zu einer engen Abgrenzung der sachlichen und räumlichen Märkte führen.⁸⁴ **63**

Es empfiehlt sich, in Compliance-Schulungen auf die Produkte des eigenen Unternehmens abzustellen und die Teilnehmer diskutieren zu lassen. Ein guter Start in die Diskussion kann die Schilderung eines plakativen Beispiels sein, z. B. die Frage, ob Bananen einen separaten Produktmarkt bilden oder mit anderen frischen Früchten, z. B. Äpfeln, zu einem weiteren Markt gehören. Es kann analysiert werden, wie man aus Verbrauchersicht argumentieren kann („Denken Sie an die Alten, Kranken, Babys und sonstige Zahnlose.“⁸⁵). **64**

Ins Gewicht fallen können aber auch Aspekte der Angebotsumstellungsflexibilität, d. h. der Austauschbarkeit auf der Seite des Anbieters. Sie ist dann gegeben, wenn die Anbieter ihre Produktion ohne spürbare Zusatzkosten und Risiken innerhalb kurzer Frist auf andere Erzeugnisse umstellen können. Dies ist im Einzelfall zu prüfen. **65**

Eine marktbeherrschende Stellung liegt vor, wenn das Unternehmen auf dem so abgegrenzten sachlichen und räumlichen Markt keinem wirksamen Wettbewerb ausgesetzt ist und sein Verhalten im Wesentlichen unabhängig von den Wettbewerbern bestimmen kann. In der Praxis spielen Marktanteile eine wichtige Rolle. Im deutschen Recht wird eine marktbeherrschende Stellung vermutet, wenn das Unternehmen einen Marktanteil von mindestens 40 % hat.⁸⁶ Im europäischen Recht gibt es keine gesetzliche Vermutung; regelmäßig wird jedoch bei einem Marktanteil ab 50 % von Marktbeherrschung ausgegangen. Die Höhe der Marktanteile ist aber nicht das einzige Kriterium. Letztlich entscheidet eine Gesamtabwägung aller für die Wettbewerbssituation wesentlichen Umstände. Dies hängt stark von den Umständen des jeweiligen Einzelfalls ab. Für die Feststellung, ob ein Unternehmen eine marktbeherrschende Stellung hat, ist deshalb die Einschaltung von Experten zu empfehlen. **66**

84 Im Februar 2024 veröffentliche die Kommission die erste Überarbeitung der Bekanntmachung über die Marktdefinition seit deren Publikation im Jahr 1997 (C/2023/6789 OJ C, C/2024/1645, 22.2.2024).

85 Vgl. EuGH, 14.2.1978 – Rs. C-27/76, ECLI:EU:C:1978:22 – United Brands & Co and United Brands Continental BV (Chiquita Bananas).

86 Vgl. § 18 Abs. 4 GWB.

(2) Missbräuchliche Ausnutzung

- 67 Ein Missbrauch liegt vor, wenn die Unternehmen ihre Marktmacht ausgenutzt haben, um gegenüber ihren Abnehmern oder ihren Wettbewerbern Konditionen durchzusetzen, die nicht mit dem normalen Leistungswettbewerb vereinbar sind.⁸⁷ Auch diese Beurteilung ist immer von den Umständen des Einzelfalls abhängig. Eine weitere Schwierigkeit ist, dass sowohl zu hohe als auch zu niedrige Preise einen Missbrauch darstellen können. In der Entscheidungspraxis der Gerichte und Behörden sind bestimmte Fallgruppen entwickelt worden, bei denen ein Verstoß grundsätzlich vermutet wird, wenn die Unternehmen nicht besondere Gründe für die Rechtfertigung ihres Verhaltens nachweisen können. Sie gelten als „Per-se-Verbote“.⁸⁸ In diesen Fällen besteht ein hohes Risiko, dass die Behörden bei einem Verstoß ein Bußgeld verhängen. Unternehmen, bei denen eine marktbeherrschende Stellung möglich ist, sollten die Per-se-Verbote unbedingt beachten oder sich ausreichend absichern, dass ihr Verhalten ausnahmsweise gerechtfertigt ist. In den anderen Fällen haben die Behörden zwar wiederholt Untersagungen ausgesprochen, aber bisher keine Bußgelder verhängt. Hier sind die Risiken somit weniger hoch.

bb) Sehr hohe Risiken

(1) Behinderung/Ausgrenzung von Wettbewerbern

- 68 Verhaltensweisen eines marktbeherrschenden Unternehmens, deren Zweck erkennbar darauf ausgerichtet ist, Wettbewerber vom Markt zu verdrängen oder sie in ihrer geschäftlichen Entwicklung zu behindern, sind stets als Missbrauch anzusehen. Eine objektive Rechtfertigung kommt in diesen Fällen normalerweise nicht in Betracht.⁸⁹ Vielfach werden solche Handlungen unter eine der folgenden Kategorien fallen. Darauf kommt es aber nicht an, wenn eine Behinderung der Wettbewerber bei objektiver Betrachtung bezweckt ist. Beispiele für einen Missbrauch, die nicht einer besonderen Gruppe von Per-se-Verstößen zuzuordnen sind, sind Maßnahmen, die Wettbewerber vom Zugang zu notwendigen Rohstoffen ausschließen oder sie beim Absatz von einem geschäftlich nicht unerheblichen Kundenkreis abschneiden.

87 EuGH, st. Rspr.; 13.2.1979 – Rs. 85/76, ECLI:EU:C:1979:36 – Hoffmann-La Roche.

88 Siehe den folgenden Abschnitt zu diesen Fallgruppen. Vgl. Europäische Kommission, Erläuterungen zu den Prioritäten der Kommission bei der Anwendung von Artikel 82 des EG-Vertrags auf Fälle von Behinderungsmissbrauch durch marktbeherrschende Unternehmen, 2009/C 45/02. Derzeit arbeitet die Kommission zudem an Leitlinien für die Anwendung des Missbrauchsverbots, die hier in Zukunft für mehr Sicherheit sorgen könnten.

89 Vgl. Europäische Kommission, Erläuterungen zu den Prioritäten der Kommission bei der Anwendung von Artikel 82 des EG-Vertrags auf Fälle von Behinderungsmissbrauch durch marktbeherrschende Unternehmen, 2009/C 45/02.

(2) Kundenbindung, Treuerabatte

Diese Gruppe gehört zu den häufigsten Verstößen gegen das Missbrauchsverbot. Unbedenklich sind Mengenrabatte, die allein an abgenommene Volumina geknüpft sind. Verboten sind aber sog. „Treuerabatte“, die einem Abnehmer dafür gewährt werden, dass er seinen gesamten Bedarf oder erhebliche Teile desselben bei dem marktbeherrschenden Unternehmen deckt.⁹⁰ Eine ähnliche „Sogwirkung“ haben Rabatte, die an einen bestimmten Mindestumsatz über einen längeren Zeitraum hinweg geknüpft sind. Das trifft bereits bei einer Kundenbindung für ein Jahr zu.⁹¹ Die in der Praxis verbreiteten Jahresumsatzrabattstaffeln sind deshalb für marktbeherrschende Unternehmen verboten. **69**

(3) Squeeze-out von Wettbewerbern, Kosten-Preis-Schere

Diese Kategorie betrifft Fälle, in denen gewerbliche Abnehmer auf die Produkte des marktbeherrschenden Unternehmens angewiesen sind (z. B. unabhängige Mineralöhländler, die das Benzin bei den großen Markenherstellern beziehen). Der Missbrauch besteht in diesen Fällen darin, dass das marktbeherrschende Unternehmen von den gewerblichen Abnehmern so hohe Entgelte fordert, dass sie im Wettbewerb nicht mehr bestehen können, weil sie die notwendige Verdienstspanne nicht mehr erwirtschaften können. Dies ist insbesondere der Fall, wenn die Preise für die gewerblichen Abnehmer gleich oder annähernd gleich hoch sind wie die Preise, die das marktbeherrschende Unternehmen von seinen eigenen Endkunden verlangt. Denkbar ist aber, dass die Preissetzung durch besondere Umstände, die das marktbeherrschende Unternehmen nicht beeinflussen kann, ausnahmsweise gerechtfertigt ist. **70**

(4) Kopplung von Angeboten

Eine unzulässige Kopplung liegt dann vor, wenn mehrere Produkte nur gemeinsam erworben werden können, ohne dass es dafür einen vernünftigen wirtschaftlichen oder technischen Grund gibt. Die Europäische Kommission hat bereits extrem hohe Bußgelder wegen der unzulässigen Kopplung von verschiedenen Produkten verhängt.⁹² **71**

90 EuGH, 13.2.1979 – Rs. 85/76, ECLI:EU:C:1979:36 – Hoffmann-La Roche; 16.12.1975 – Rs. 40-48/73, 50/73, 54-56/73, 111/73, 113 u. 114/73, ECLI:EU:C:1975:174 – Suiker Unie; 9.11.1983 – Rs. 322/81, ECLI:EU:C:1983:313 – Michelin I.

91 EuGH, 9.11.1983 – Rs. 322/81, ECLI:EU:C:1983:313 – Michelin I.

92 So erging z. B. im Jahr 2018 im Fall Google Android ein Bußgeld in Höhe von 4,34 Mrd. EUR wegen der unzulässigen Kopplung des Betriebssystems mit vorzuinstallierenden Apps (Google-Suche und ihrem Browser Chrome), Europäische Kommission, Pressemitteilung vom 18.7.2018.

cc) Weniger hohe Risiken

(1) Ausbeutungsmissbrauch, Kundenpreisdifferenzierung

- 72** Ein Ausbeutungsmissbrauch ist dadurch gekennzeichnet, dass ein marktbeherrschendes Unternehmen von seinen Abnehmern oder den Endverbrauchern überhöhte Preise fordert, die bei normalem Wettbewerb nicht durchsetzbar gewesen wären. Der Nachweis unangemessen hoher Preise ist meist ausgesprochen schwierig. Im Regelfall stützen sich die Wettbewerbsbehörden auf die Preise anderer vergleichbarer Anbieter oder auf vergleichbaren Märkten (Vergleichsmarktkonzept). Ist dies nicht möglich, muss ermittelt werden, ob Preise und Kosten in einem angemessenen Verhältnis stehen.⁹³
- 73** Ein Sonderfall des Ausbeutungsmissbrauchs ist die Preisdifferenzierung zwischen verschiedenen Kunden. Marktbeherrschenden Unternehmen ist dies anders als „normalen“ Unternehmen grundsätzlich untersagt, es sei denn die Benachteiligung einzelner Kunden oder Kundenkreise ist durch besondere Umstände gerechtfertigt.

(2) Niedrigpreisstrategien

- 74** Häufiger sind die Fälle, dass ein marktbeherrschendes Unternehmen versucht, durch unangemessen niedrige Preise Wettbewerber aus dem Markt zu verdrängen oder sie zumindest in ihrer Entfaltung zu behindern (sog. „Preisdumping“ oder „Kampfpreise“). Grundsätzlich kommt es darauf an, ob ein Unternehmen, das nicht marktbeherrschend aber ebenso leistungsfähig wie das marktbeherrschende Unternehmen ist, Preise dieser Höhe im Wettbewerb durchsetzen könnte. In der Praxis stützt man sich auf einfache festzustellende Kriterien. Sind die Preise so hoch, dass sowohl die variablen als auch die anteiligen Fixkosten des marktbeherrschenden Unternehmens gedeckt sind, scheidet ein Missbrauch aus. Reichen dagegen die Erlöse nicht einmal für die (vermeidbaren) durchschnittlichen variablen Kosten des Produkts aus, sind die Preise als missbräuchlich anzusehen. In dem Zwischenbereich, in dem zwar die variablen, nicht aber auch die anteiligen Fixkosten des Produkts gedeckt sind, ist jeweils eine Einzelfallprüfung erforderlich. Entscheidend ist, ob das marktbeherrschende Unternehmen die Absicht verfolgt hat, Wettbewerber aus dem Markt zu drängen oder von ihm fernzuhalten.⁹⁴

93 Besondere Bedeutung hat die Missbrauchsaufsicht über die Energiepreise in Deutschland. Für die Preise von Strom, Fernwärme und Gas gibt es eine derzeit bis Ende 2027 befristete Sonderregelung (jeweils für Hersteller und Händler) in § 29 GWB. Dadurch waren Strom- und Gasanbieter in vielen Fällen genötigt, ihre Endverbraucherpreise z. T. deutlich abzusenken.

94 *Huttenlauch/Lübbig*, in: Loewenheim/Meessen/Riesenkampff/Kersting/Meyer-Lindemann, Kartellrecht, Art. 102 AEUV Rn. 225 ff. m. w. N.

(3) Lieferverweigerung; wesentliche Einrichtungen („Essential Facilities“)

Auch marktbeherrschende Unternehmen können grundsätzlich frei entscheiden, welche Abnehmer sie beliefern wollen. In besonderen Fällen kann aber eine Lieferverweigerung missbräuchlich sein. Das ist vor allem der Fall, wenn die Belieferung für den Nachfrager unerlässlich ist, um seine Geschäftstätigkeit weiter ausüben zu können, und es keine sachlichen Gründe für die Lieferverweigerung gibt. Dabei sind an die Rechtfertigung des Abbruchs einer bestehenden Lieferbeziehung höhere Anforderungen zu stellen als an die Weigerung, Geschäftsbeziehungen zu neuen Kunden aufzunehmen.⁹⁵ In Ausnahmefällen kann auch ein Anspruch auf Erteilung einer Lizenz für ein patentgeschütztes Produkt des marktbeherrschenden Unternehmens bestehen (Zwangslizenz).⁹⁶ 75

Eine Lieferverweigerung kann vor allem im Fall der sog. „Essential Facilities“ einen Missbrauch darstellen. Das sind Einrichtungen, auf die andere Unternehmen bei ihrer Geschäftstätigkeit angewiesen sind und die ihrer Natur nach nicht doppelt oder mehrfach vorgehalten werden können. Typische Beispiele sind Netze z. B. in der Telekommunikation, im Energiebereich oder im Schienenverkehr. Das marktbeherrschende Unternehmen muss den Unternehmen, die auf die Einrichtung angewiesen sind, grundsätzlich die Nutzung der Einrichtung gegen angemessenes Entgelt gestatten. Es darf dies nur dann verweigern, wenn dies durch besondere sachliche Gründe hinreichend gerechtfertigt ist. 76

(4) Ausschließlichkeitsbindungen

Ein marktbeherrschendes Unternehmen handelt missbräuchlich, wenn es mit seinen Abnehmern vereinbart, dass diese ihren Gesamtbedarf oder einen beträchtlichen Teil davon (z. B. mehr als 80 %) bei ihm selbst eindecken. Die Bindung kann rechtlicher Art sein, aber auch rein faktisch auf Anreizen (wie z. B. entsprechenden Rabatten) oder wirtschaftlichem Zwang (z. B. als Voraussetzung für eine Belieferung) beruhen. Wendet ein marktbeherrschendes Unternehmen solche Klauseln in größerem Umfang an, wird dadurch der Markt für die Wettbewerber weitgehend verschlossen. 77

(5) Diskriminierung abhängiger Unternehmen

Dieses Verbot betrifft nicht nur marktbeherrschende Unternehmen, sondern auch marktstarke Unternehmen, die gegenüber anderen Unternehmen über eine 78

⁹⁵ Mitteilung der Europäischen Kommission – Erläuterungen zu den Prioritäten der Kommission bei der Anwendung von Artikel 82 des EG-Vertrags auf Fälle von Behinderungsmissbrauch durch marktbeherrschende Unternehmen, ABl. C 45/7 vom 24.2.2009, Rn. 84; siehe auch Europäische Kommission, 24.3.2004 – COMP/37.792, Rn. 556, 558 – Microsoft; *Fuchs*, in: Immenga/Mestmäcker, EU-Wettbewerbsrecht, Art. 102 AEUV Rn. 312, 320.

⁹⁶ EuGH, 6.4.1995 – verb. Rs. C-241/91 P und C-242/92 P, ECLI:EU:C:1995:98 – Radio Telefís Éireann (RTE) und Independent Television Publications Ltd (ITP)/Kommission („Magill“); EuGH, 29.4.2004 – Rs. C-418/01, ECLI:EU:C:2004:257 – IMS Health/NDC Nealth. Siehe auch *Fuchs*, in: Immenga/Mestmäcker, EU-Wettbewerbsrecht, Art. 102 AEUV Rn. 329.

erhebliche Marktmacht verfügen (relative Marktmacht).⁹⁷ Diese Unternehmen dürfen, ebenso wie marktbeherrschende Unternehmen, andere Unternehmen, die von ihnen abhängig sind, nicht unbillig benachteiligen. Abhängigkeit ist im Wirtschaftsleben ein häufiges Phänomen. Die Vorschrift hat daher eine große praktische Bedeutung. Beispiele sind u. a. Händler, die sich auf den Vertrieb bestimmter Produkte spezialisiert haben; Fachhändler, die im Hinblick auf ihr Standing die Produkte der Spitzengruppe in ihrem Sortiment führen müssen; umgekehrt Hersteller, die darauf angewiesen sind, dass ihre Produkte vom Handel gelistet werden; oder schließlich Zulieferer, die für die Herstellung ihrer Produkte erhebliche Investitionen getätigt haben. Marktbeherrschende oder marktstarke Unternehmen dürfen von solchen abhängigen Unternehmen keine ungünstigeren Preise oder Konditionen verlangen, als dies andere Unternehmen in vergleichbarer Lage tun.⁹⁸

(6) Behinderung von kleineren Wettbewerbern; Verkauf unter Einstandspreis

- 79** Marktbeherrschende oder marktstarke⁹⁹ Unternehmen dürfen kleine und mittlere Wettbewerber nicht unbillig behindern.¹⁰⁰ Dieses Verbot hat in der Praxis keine große Bedeutung. Ein Sonderfall mit erheblichen Auswirkungen ist das Verbot des Verkaufs unter Einstandspreis. Marktstarke Unternehmen wie z. B. die großen Handelsketten dürfen ihre Waren unter bestimmten Voraussetzungen nicht unter ihrem eigenen Einstandspreis verkaufen. Auf den (meist erheblich höheren) Einstandspreis der kleinen und mittleren Wettbewerber kommt es nicht an. Erlaubt ist ein Verkauf unter Einstandspreis im Allgemeinen, wenn er nur gelegentlich erfolgt oder durch besondere Umstände gerechtfertigt ist (z. B. Notverkäufe kurz vor dem Ablaufdatum). Im Jahr 2007 wurde die Vorschrift für den Lebensmittelhandel in § 20 Abs. 3 Nr. 1 GWB weiter verschärft.¹⁰¹ Die zeitliche Befristung der Sonderregelung in diesem Sektor wurde aufgehoben.

3. Haftungssubjekte (Wer haftet für wen?)

a) Unternehmenshaftung

- 80** Für Kartellverstöße haften in erster Linie die Unternehmen, die an der wettbewerbsbeschränkenden Vereinbarung mitgewirkt haben. Nach Ansicht der Kartellbehörden ist es für die Haftung ohne Bedeutung, dass das Unternehmen die Kartellabsprachen nicht eingehalten hat oder nicht einhalten wollte, wenn das

⁹⁷ Im deutschen Recht ist dies in § 19 Abs. 2 Nr. 1 i. V. m. § 20 Abs. 1 GWB ausdrücklich geregelt. Eine vergleichbare Vorschrift für marktstarke Unternehmen gibt es im europäischen Recht nicht.

⁹⁸ Art. 102 Abs. 2 lit. c AEUV.

⁹⁹ Zur Definition siehe → Rn. 78.

¹⁰⁰ Rechtsgrundlage ist im deutschen Recht § 20 Abs. 3 Satz 1 GWB.

¹⁰¹ Siehe dazu § 20 Abs. 3 Nr. 1 GWB.

für die anderen beteiligten Unternehmen nicht eindeutig erkennbar war.¹⁰² Meistens bestehen Kartelle über einen längeren Zeitraum. Dann kommt es wiederum aus Sicht der Kartellbehörden nicht darauf an, ob sich die Durchführung des Kartells im Laufe der Zeit geändert hat oder vorübergehend unterbrochen worden ist. Wichtig ist nur, dass der Zweck der Kartellabsprache grundsätzlich, wenn auch mit etwaigen notwendigen Anpassungen, unverändert gewahrt bleibt.¹⁰³ Jedes Unternehmen haftet dann im Grundsatz, wenn es die Kartellabsprache kannte oder kennen musste, für alle Verstöße während des gesamten Zeitraums. Um die Haftung zu beenden, reicht es nicht, dass das Unternehmen seine Mitwirkung am Kartell einstellt. Es muss sich offen von der Absprache distanzieren und die anderen Beteiligten davon in Kenntnis setzen, dass es fortan an dem Kartellrechtsverstoß nicht mehr beteiligt ist. Die Haftung gilt nicht nur für die eigentlichen „Täter“; auch Unternehmen, die nur Hilfestellung geleistet haben, z.B. durch Beratung bei der Ausführung des Kartellrechtsverstoßes ohne selbst Wettbewerber zu sein, haften mit.¹⁰⁴ Das unterschiedliche Ausmaß der Beteiligung und des Umfangs des verursachten Schadens findet zwar bei der Haftung keine Berücksichtigung, ist aber für die Bemessung des Bußgeldes ein wesentlicher Faktor (dazu siehe → Rn. 91 ff.).

b) Persönliche Haftung

Im deutschen Recht steht neben der Unternehmenshaftung die persönliche Haftung der am Kartellverstoß beteiligten Personen.¹⁰⁵ Das ist bei allen Verfahren des Bundeskartellamtes von Bedeutung. Für die Haftung spielt es keine Rolle, ob der Mitarbeiter für die Handlungen zuständig und befugt war. Voraussetzung für die Haftung ist ein Verschulden. Verantwortlich ist auch derjenige, der einen Kartellverstoß schuldhaft nicht verhindert hat, obwohl ihm dies aufgrund seiner Aufsichtspflicht möglich gewesen wäre.¹⁰⁶ Für die Leitungspersonen eines Unternehmens ist es deshalb wichtig, durch ein effektives Compliance-Programm so weit wie möglich dafür zu sorgen, dass es nicht zu einem Kartellrechtsverstoß kommt.

Für die Unternehmenshaftung ist Voraussetzung, dass mindestens ein Mitarbeiter schuldhaft an dem Kartellverstoß mitgewirkt hat.¹⁰⁷ Die handelnde Person muss nicht der Leitungsebene angehören. Welchen Rang und welche Kompetenzen

81

82

102 EuG, 8.7.2008 – Rs. T-53/03, ECLI:EU:T:2008:254, Rn. 82 – BPB/Kommission; EuGH, 12.7.1979 – Rs. C-32/87, ECLI:EU:C:1979:191 – BMW-Belgium/Kommission; EuGH, 29.10.1980 – Rs. C-209/78, ECLI:EU:C:1980:248 – van Landewyck u. a./Kommission.

103 Vgl. dazu im Einzelnen EuG, 12.12.2007 – Rs. T-101/05, ECLI:EU:T:2007:380 – BASF und UCB/Kommission.

104 EuGH, 22.10.2015 – Rs. C-194/14 P – AC Treuhand, WuW 2016, 71 ff.

105 Die persönliche Haftung ist im deutschen System der Ordnungswidrigkeiten eigentlich die primäre Haftung (vgl. § 81a Abs. 1 Satz 1 GWB). Die Unternehmenshaftung folgt als Annex aus der persönlichen Haftung der Unternehmensangehörigen (§ 30 OWiG).

106 Dies ist im deutschen Recht in § 130 OWiG ausdrücklich geregelt.

107 Im deutschen Recht ist dies in den §§ 9, 30 OWiG geregelt.

zen der Mitarbeiter hat, ist unerheblich. Die Haftung des Unternehmens entfällt auch nicht deshalb, weil das Unternehmen alle denkbaren Compliance-Anstrengungen unternommen hat, um den Verstoß zu verhindern. Neuerdings stellen nach deutschem Recht jedoch „Vorkehrungen zur Vermeidung und Aufdeckung von Zuwiderhandlungen“ einen gesetzlichen Milderungsgrund dar, der zu einer Verringerung der Geldbuße führt.¹⁰⁸ Nach der Praxis der Europäischen Kommission ist dies bislang nicht einmal ein Milderungsgrund.¹⁰⁹

c) Haftung im Konzern („Wirtschaftliche Einheit“)

- 83 Zusätzliche Regeln gelten für die Haftung von Unternehmen im Konzern, wenn zwischen der Konzernobergesellschaft (Mutter) und den Tochtergesellschaften eine sog. „wirtschaftliche Einheit“ besteht. Nach der Praxis der Europäischen Kommission und der europäischen Gerichte beruht eine solche wirtschaftliche Einheit darauf, dass die Tochtergesellschaft ihr Verhalten im Geschäftsverkehr nicht autonom bestimmt, sondern im Wesentlichen Weisungen der Mutter befolgt oder sich aus eigener Entscheidung nach den Interessen der Mutter ausrichtet.¹¹⁰ Dies wird vermutet, wenn die Mutter (nahezu) 100 % der Anteile besitzt.¹¹¹ Eine Widerlegung dieser Vermutung ist theoretisch möglich, in der Praxis aber meist sehr schwierig. Mutter und Tochter gelten in diesem Fall als ein einheitliches Unternehmen; auf die rechtliche Selbstständigkeit der Tochter kommt es dann nicht an. Die Mutter haftet für Handlungen der Tochtergesellschaft wie für Handlungen ihrer eigenen Mitarbeiter, unabhängig davon, ob sie Kenntnis von dem Verhalten oder Einfluss darauf gehabt hat. Ein eigenes Verschulden der Mutter ist nicht erforderlich; es reicht das Verschulden eines Mitarbeiters der Tochtergesellschaft.

108 Dies ergibt sich seit Verabschiedung der 10. GWB-Novelle aus § 81d Abs. 1 Satz 2 Nr. 4 GWB. Damit wurde letztlich die bisherige Rechtsprechung kodifiziert, vgl. grundlegend BGH, 9.5.2017 – 1 StR 265/16, NZWiSt 2018, 379; zuletzt OLG Düsseldorf, 19.12.2023 – 6 Kart 9/19 (OWi), WuW 2024, 220 – Süßwarenkartell.

109 Vgl. *Trüg/Ruppert*, ZWeR 2020, 69, 88; *Baur/Holle*, NZG 2018, 14; *Eufinger*, NZG 2018, 327. Eine wachsende Zahl von ausländischen Wettbewerbsbehörden berücksichtigt aber – wie nun auch das Bundeskartellamt – ausreichende Compliance-Anstrengungen bei der Bemessung der Geldbuße (sog. compliance defence); so z.B.: Autorité de la concurrence, Framework document of 23 May 2022 on competition compliance programmes, https://www.autoritedelaconcurrence.fr/sites/default/files/2022-06/Conformite_nouveau%20doc-cadre_VEN.pdf (zuletzt abgerufen am 25.4.2024).

110 Siehe z.B. EuGH, 14.7.1972 – Rs. C-48/69, ECLI:EU:C:1972:70, Rn. 132, 135 – ICI; EuGH, 10.9.2009 – Rs. C-97/08 P, ECLI:EU:C:2009:536, Rn. 58 – Akzo Nobel; EuGH, 10.4.2014 – Rs. C-231/11 P bis C-233/11 P, ECLI:EU:C:2014:256, Rn. 46 – Siemens.

111 St. Rspr. seit EuGH, 25.10.1983 – Rs. 107/82, ECLI:EU:C:1983:293, Rn. 50 – AEG. Siehe u.a. EuGH, 10.4.2014 – Rs. C-247/11 P, ECLI:EU:C:2014:257 Rn. 32 – Areva.

Mit der 9. GWB-Novelle¹¹² erfolgte durch den deutschen Gesetzgeber eine Angleichung an die europäische Praxis.¹¹³ Demzufolge kann die Muttergesellschaft eines Konzerns nicht mehr nur dann vom Bundeskartellamt mit einer Geldbuße belegt werden, wenn ihr ein eigenes Verschulden nachgewiesen wird. Vielmehr haftet sie fortan verschuldensunabhängig. Voraussetzung für eine konzernweite Haftung ist, dass der Verstoß von einer Leitungsperson der Tochtergesellschaft i. S.d. § 30 OWiG begangen wurde und eine tatsächliche Ausübung eines bestimmenden Einflusses durch die Muttergesellschaft vorlag.¹¹⁴ Gerade im Hinblick auf die erfolgte Haftungsausweitung ist ein effektives – konzernweites – Compliance-Management-System wichtig.

84

d) Haftung bei Gemeinschaftsunternehmen

Eine „wirtschaftliche Einheit“ kann auch bei einem Gemeinschaftsunternehmen (GU; englisch: Joint Venture) im Verhältnis zwischen den Muttergesellschaften und dem GU vorliegen. Dabei kann die wirtschaftliche Einheit sowohl zwischen dem GU und einer Mutter als auch zwischen dem GU und mehreren oder allen Müttern bestehen.¹¹⁵ Voraussetzung ist, dass die eine Mutter allein oder die verschiedenen Mütter gemeinsam die Geschäftstätigkeit des GU tatsächlich so stark beeinflussen, dass dieses im Wesentlichen ihren Weisungen folgt oder sich auch ohne ausdrückliche Weisung nach den Interessen der Mutter bzw. der Mütter ausrichtet.¹¹⁶ Liegt eine wirtschaftliche Einheit vor, gelten die beteiligten Unternehmen wiederum als ein einheitliches Unternehmen. Die Mutter haftet also für einen Kartellverstoß des GU wie für einen eigenen Verstoß, auch wenn sie kein eigenes Verschulden trifft.

85

e) Haftung für Beauftragte

In der europäischen Praxis ist die „wirtschaftliche Einheit“ auf Fälle ausgedehnt worden, in denen ein Handelsvertreter für einen Auftraggeber tätig ist.¹¹⁷ Auch hier ist es typischerweise so, dass der Handelsvertreter seine Geschäftstätigkeit auf die Interessen des Auftraggebers ausrichtet. Wird dies im Einzelfall festgestellt, gelten Auftraggeber und Handelsvertreter im Hinblick auf den Kartellverstoß ebenfalls als ein einheitliches Unternehmen. Das kann auch dann der Fall sein, wenn der Handelsvertreter noch für einen oder mehrere andere Auftraggeber tätig ist, sofern die finanziellen Risiken – wie dies üblich ist – vom Auftrag-

86

112 Neuntes Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen vom 1.6.2017, BGBl. 2017, Teil I Nr. 33, ausgegeben am 8.6.2017, S. 1416 ff.

113 Einen guten Überblick über die Regelungsänderung geben *Timmerbeil/Blome*, BB 2017, 1544, sowie *Mäger/von Schreitter*, NZKart 2017, 264.

114 Vgl. § 81 Abs. 3a GWB.

115 Vgl. dazu EuGH, 26.9.2013 – Rs. C-172/12P, ECLI:EU:C:2013:601 – El du Pont de Nemours.

116 Die Vermutung im Fall von (nahezu) 100% des Anteilsbesitzes kann hier nicht zum Tragen kommen, da keine der Mütter bei einem GU einen Anteil in dieser Höhe besitzen kann.

117 EuG, 15.7.2015 – Rs. T-418/10, ECLI:EU:T:2015:516 – Voestalpine.

geber getragen werden.¹¹⁸ Der Auftraggeber haftet dann für die Pflichtverletzung des Handelsvertreters so, als wenn ein eigener Mitarbeiter die Tat begangen hätte. Dabei spielt es wiederum keine Rolle, ob er von den Aktivitäten des Handelsvertreters Kenntnis hatte oder sie hätte verhindern können. Die gleichen Grundsätze gelten für sonstige Beauftragte, wenn die Voraussetzungen einer wirtschaftlichen Einheit erfüllt sind, d.h. der Beauftragte sein Verhalten im Wesentlichen nach den Interessen des Auftraggebers ausrichtet oder dessen Weisungen befolgt.

f) Haftung bei Rechtsnachfolge

- 87** Probleme können sich ergeben, wenn ein Unternehmen, nachdem es den Kartellverstoß begangen hat, aufgelöst oder umgewandelt wird und auf einen Rechtsnachfolger übergeht. Im europäischen ebenso wie im deutschen Recht bleibt die Haftung des Kartellunternehmens unberührt, solange es als Rechtssubjekt fortbesteht.¹¹⁹ Bestand eine wirtschaftliche Einheit mit der früheren Mutter, bleibt auch deren Haftung unberührt. Der Erwerber haftet nicht, solange das erworbene Unternehmen rechtlich fortbesteht, selbst wenn er Kenntnis von dem Kartellverstoß gehabt hat. Löst der Erwerber das Kartellunternehmen auf oder wandelt es so um, dass es seine bisherige Rechtspersönlichkeit verliert, geht die Haftung nach dem Grundsatz der wirtschaftlichen Kontinuität auf den Erwerber über (Gesamtrechtsnachfolge).¹²⁰ Dies betrifft vor allem gesellschaftsrechtliche Transaktionen wie die Umwandlung oder Verschmelzung.
- 88** Schwieriger ist die Rechtslage, wenn das für das Kartell verantwortliche Unternehmen nur formal weiterbesteht, aber seine Vermögenssubstanz auf ein anderes Unternehmen übertragen wird, sodass es das Bußgeld nicht mehr bezahlen kann. Typischerweise erfolgt dies durch die Übertragung der Vermögenswerte des Kartellunternehmens auf ein anderes Unternehmen im Konzern.¹²¹ Im europäischen Recht gilt insoweit der Grundsatz der wirtschaftlichen Identität: Die Haftung geht immer dann auf das erwerbende Unternehmen über, wenn das Bußgeld gegen das übernommene Unternehmen nicht mehr durchgesetzt werden kann. In der deutschen Praxis gab es in diesem Fall eine Sanktionslücke, die üblicherwei-

¹¹⁸ EuG, 15.7.2015 – Rs. T-418/10, ECLI:EU:T:015:516, Rn. 142 ff. – Voestalpine.

¹¹⁹ So z.B. EuGH, 24.9.2009 – Rs. C-125/07, C-133/07, C-135/07 und C-137/07, ECLI:EU:C:2009:576, Rn. 79 – Lombardclub; OLG Düsseldorf, 15.4.2013 – VI-4 Kart 2 – 6/10 (OWi).

¹²⁰ Europäische Kommission, 28.1.2009 – COMP/39.406 Rn. 352 ff. – Marineschläuche; Europäische Kommission, 19.10.2011 – COMP/39.605 Rn. 6 und 60 – CRT-Glas; EuG, 14.12.2006 – Rs. T-259/02 bis T-264/02 und T-271/02, ECLI:EU:T:2006:396, Rn. 332–336 – Lombardclub; bestätigt durch EuGH, 24.9.2009 – Rs. C-125/07, C-133/07, C-135/07 und C-137/07, ECLI:EU:C:2009:576, Rn. 79 – Lombardclub.

¹²¹ Zum Grundsatz der wirtschaftlichen Kontinuität vgl. u. a. EuG, 11.3.1999 – Rs. T-134/94, Slg. 1999, II-239 – NMH Stahlwerke; EuG, 30.9.2009 – T-161/05, ECLI:EU:T:2009:366 – Hoechst.

se als „Wurst-Lücke“¹²² bezeichnet wurde. Durch die 9. GWB-Novelle wurde das deutsche Recht hinsichtlich der Gesamtrechts- und der Einzelrechtsnachfolge an das europäische Recht angepasst.¹²³ Eine Kartellgeldbuße kann nunmehr auch gegen lediglich wirtschaftliche Nachfolger festgesetzt werden. Damit ist es grundsätzlich nicht mehr möglich, dass sich ein Unternehmen durch interne Umorganisation oder Veräußerung von Vermögensteilen einem Kartellbußgeld entziehen kann. Für Kartellrechtsverstöße, die vor Inkrafttreten der 9. GWB-Novelle begangen wurden, besteht außerdem in § 81e GWB eine Übergangsregelung, nach der auch in diesen Fällen eine Umstrukturierung keine Flucht vor dem Bußgeld mehr ermöglicht.

4. Art und Umfang der Haftung

a) Strafrechtliche Sanktionen

Strafrechtliche Sanktionen sind die schwerwiegendste Form der Ahndung von Rechtsverstößen.¹²⁴ Nicht nur die Strafe, schon allein die Einleitung eines Strafverfahrens ist meist eine schwere Belastung für die Betroffenen. Bei Kartellverstößen sind im europäischen Recht strafrechtliche Sanktionen nicht vorgesehen. Die Europäische Kommission kann also weder selbst Strafen verhängen noch gerichtliche Strafverfahren einleiten. Sie kann auch nicht die nationalen Behörden einschalten und diese auffordern, strafrechtliche Schritte gegen die persönlich Verantwortlichen zu veranlassen. Es bleibt allein bei den Unternehmensbußgeldern der Europäischen Kommission. 89

Auch im deutschen Recht sind Kartellverstöße in aller Regel Ordnungswidrigkeiten und keine Straftaten. Lediglich der Ausschreibungs- oder Submissionsbetrug ist als Straftatbestand ausgestaltet.¹²⁵ Hier führt das Bundeskartellamt das Verfahren als Ordnungswidrigkeit gegen die Unternehmen, während die Staatsanwaltschaft für das strafrechtliche Verfahren gegen die persönlich Verantwortlichen zuständig ist. Im Gegensatz zu kartellrechtlichen Verfahren haben Strafverfahren wegen Ausschreibungsbetrugs in der Praxis bislang keine große Bedeutung erlangt. Häufig enden die Verfahren, wenn es überhaupt dazu kommt, mit Geldstrafen oder einer Verfahrenseinstellung. Ein großer Nachteil ist allerdings, dass dem Täter in diesen Fällen die Kronzeugenvergünstigung des Bundeskartellamtes nicht zugutekommt. Es kann also sein, dass das Unternehmen als Kronzeuge straffrei bleibt, die persönlich Handelnden aber strafrechtlich zur Verantwortung gezogen werden. In Deutschland wird darüber diskutiert, ob schwerwiegende Kartellvergehen generell als kriminelles Unrecht ausgestal- 90

122 Der Name rührt daher, dass diese Lücke erstmals im Rahmen des Wurst-Kartells tatsächlich relevant geworden ist.

123 § 81a Abs. 2 und 3 GWB.

124 Zu den strafrechtlichen Risiken bei „Non-Compliance“ ausführlich → Böttger, Kap. 2 Rn. 31 ff.

125 § 298 StGB.

tet werden sollten, um die Abschreckungswirkung zu erhöhen.¹²⁶ Mit einer grundlegenden Änderung des Sanktionssystems ist jedoch auf absehbare Zeit nicht zu rechnen.

b) Bußgelder

- 91 Es ist ein weltweites Phänomen, dass die Behörden die Bußgelder im Lauf der letzten Jahre z. T. dramatisch erhöht haben. Auch die von der Europäischen Kommission und dem Bundeskartellamt verhängten Bußgelder erreichen inzwischen regelmäßig mehrstellige Millionenbeträge.¹²⁷ Sowohl in der deutschen wie in der europäischen Praxis haben die Behörden Leitlinien für die Bemessung der Bußgelder veröffentlicht.¹²⁸ Letztlich hängt die Höhe der Sanktion aber ganz wesentlich von den Umständen des Einzelfalls ab. Die folgenden Erläuterungen können keine Anleitung geben, aus der sich die Höhe der Geldbuße mit einiger Genauigkeit errechnen ließe. Ziel kann es nur sein, einige Hinweise zur Größenordnung möglicher Sanktionen bei Kartellverstößen zu geben.

aa) EU-Recht

- 92 Die Höhe des Bußgeldes bemisst sich im europäischen Recht nach Schwere und Dauer der Zuwiderhandlung.¹²⁹ In der Entscheidungspraxis hat dabei der Grundsatz einer ausreichenden Abschreckungswirkung des Bußgeldes Priorität.¹³⁰ Bei der Festsetzung des Betrags ist zwischen der Bemessung des Bußgeldes und dem zulässigen Höchstbetrag zu unterscheiden. Für die Bemessung wird zunächst ein Grundbetrag ermittelt, der sich aus dem Umsatz mit den kartellbefangenen Produkten im europäischen Binnenmarkt im letzten Jahr vor der Entscheidung ableitet. Maßgeblich ist dabei nicht nur der Umsatz mit den Produkten, die Gegenstand des Kartells waren; vielmehr sind alle Produkte einzubeziehen, auf die sich der überhöhte Kartellpreis unmittelbar oder mittelbar ausgewirkt hat

126 Dafür hatte sich die Monopolkommission ausgesprochen (Zwanzigstes Hauptgutachten 2012/2013, Rn. 118 ff. und Sondergutachten 72 „Strafrechtliche Sanktionen bei Kartellverstößen“, 2015, www.monopolkommission.de).

127 Siehe dazu → Fn. 1 und die Jahresberichte des Bundeskartellamts; Im Jahr 2022 lagen die vom Bundeskartellamt verhängten Bußgelder bei 24 Mio. EUR gegen 20 Unternehmen, nach 105 Mio. EUR im Jahr 2021. Im Jahr 2023 betrug das verhängte Bußgeld EUR 77 Mio. EUR, siehe Jahresrückblick des Bundeskartellamts 2023, https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2023/21_12_23_Jahresrueckblick.html (zuletzt abgerufen am 25.4.2023). Die bislang höchsten Gesamtbußgelder wurden im Jahr 2014 in Höhe von 1,1 Mrd. EUR verhängt.

128 Leitlinien der Kommission für das Verfahren zur Festsetzung von Geldbußen gemäß Artikel 23 Absatz 2 Buchstabe a) der Verordnung (EG) Nr. 1/2003, ABl. C 210/2 vom 1.9.2006 und Leitlinien des Bundeskartellamtes für die Bußgeldzumessung in Kartellordnungswidrigkeitenverfahren vom 11.10.2021, www.bundeskartellamt.de.

129 Vgl. Art. 23 Abs. 3 VO 1/2003.

130 Dies hat die Rechtsprechung in zahlreichen Entscheidungen immer wieder betont. Vgl. z. B. EuGH, 7.6.1983 – Rs. C-100/80, ECLI:EU:C:1983:158 – *Musique Diffusion Française*; EuGH, 17.6.2010 – Rs. C-413/08P, ECLI:EU:C:2010:346 – *Lafarge*.

oder haben könnte. Bei vertikal integrierten Unternehmen müssen auch die internen Umsätze mit den Tochtergesellschaften mit einbezogen werden.¹³¹ Falls kein Umsatz erzielt wurde, weil die Unternehmen z. B. auf Lieferungen in die EU verzichtet haben, ist der Umsatz zugrunde zu legen, der ohne die Kartellabsprache erzielt worden wäre. Auch in anderen Fällen ist der Umsatz so anzupassen, dass er der wirtschaftlichen Bedeutung des Kartells und der beteiligten Unternehmen entspricht.¹³² Für die Bestimmung des Grundbetrags wird danach von dem so ermittelten kartellbefangenen Umsatz ein bestimmter Prozentsatz festgelegt, der je nach Schwere des Verstoßes bis zu 30 % betragen kann.¹³³ In den meisten Fällen bewegt er sich in der Größenordnung um 20 %. Dieser Grundbetrag wird mit der Anzahl der Jahre des Kartells multipliziert, was häufig zu einer ganz erheblichen Ausweitung des Bußgeldes führt. Außerdem kann die Europäische Kommission einen Aufschlag (die sog. „Eintrittsgebühr“) in Höhe von 15–25 % festsetzen.¹³⁴

In einem zweiten Schritt wird der Grundbetrag im Hinblick auf erschwerende oder mildernde Umstände angepasst. So ist im Wiederholungsfall ein Zuschlag von bis zu 100 % oder bei Großunternehmen ein Zuschlag in nicht begrenzter Höhe möglich. Auch die Art und Weise, wie das Unternehmen mit der Behörde im Verfahren kooperiert, kann erschwerend oder entlastend berücksichtigt werden. Das so ermittelte Bußgeld darf einen Höchstbetrag von 10 % des weltweiten Konzernumsatzes nicht übersteigen.¹³⁵ Ist dies der Fall, ist es auf den zulässigen Höchstbetrag zu reduzieren (sog. Kappungsgrenze). Für die Praxis ist wichtig, dass das Bußgeld aus den Netto-Einkünften zu bezahlen ist. Eine steuerliche Berücksichtigung ist nicht zulässig. Grundsätzlich ist es unerheblich, ob das Bußgeld die finanzielle Leistungsfähigkeit des Unternehmens übersteigt. Nur wenn andere Unternehmen (Abnehmer, Lieferanten) Nachteile erleiden oder Arbeitslosigkeit die Folge ist, kommt eine Reduzierung des Bußgeldes in Betracht.¹³⁶ Im Übrigen kann die Europäische Kommission bei Zahlungsunfähigkeit („inability to pay“)¹³⁷ bestimmte Erleichterungen gewähren.

bb) Deutsches Recht

Auch im deutschen Recht bestimmt sich das Bußgeld nach Schwere und Dauer der Zuwiderhandlung.¹³⁸ Nach dem Gesetz beträgt der Mindestsatz 5 EUR, der

131 Vgl. EuG, 12.11.2014 – Rs. C-580/12P, EU:C:2014:2363 – Guardian.

132 Vgl. z. B. EuGH, 7.6.1983 – Rs. C-100/80, ECLI:EU:C:1983:158 – Musique Diffusion Française; EuG, 18.5.2006, Rs. – C-397/03P, EU:C:2006:328408 – Archer Daniels Midland und Archer Daniels Midland Ingredients/Kommission.

133 Bußgeldleitlinien der Europäischen Kommission, Rn. 21.

134 Bußgeldleitlinien der Europäischen Kommission, Rn. 25.

135 Art. 23 Abs. 2 Unterabs. 2 VO 1/2003.

136 EuG, 15.7.2015 – Rs. T-393/10, ECLI:EU:T:2015:515, Rn. 295 ff. – Spannstahl-Kartell (Westfälische Drahtindustrie).

137 Vgl. dazu die Bußgeldleitlinien der Europäischen Kommission, Rn. 35.

138 § 81 Abs. 4 Satz 6 GWB.

Höchstbetrag 10 % des Konzernumsatzes. Für die Berechnung der Unternehmensbußgelder hat das Bundeskartellamt ähnliche Leitlinien wie die Europäische Kommission veröffentlicht.¹³⁹ Ein wichtiger Unterschied zu den Leitlinien der Kommission besteht darin, dass das Bundeskartellamt nur einen Ausgangswert für das Bußgeld festlegt. Dieser wird dann einer Gesamtabwägung zugrunde gelegt, bei der tat- und täterbezogene Kriterien Berücksichtigung finden.¹⁴⁰ Der Ausgangswert bestimmt sich nach dem tatbezogenen Umsatz und dem Gesamtumsatz des Unternehmens und steigt mit zunehmendem Gesamtumsatz. So werden für Unternehmen mit Umsätzen unter 100 Mio. EUR 10–15 % des tatbezogenen Umsatzes als Ausgangswert herangezogen, bei Unternehmen mit über 100 Mrd. EUR Umsatz jedoch über 30 %.¹⁴¹ In der Regel betrachtet das Bundeskartellamt ein Bußgeld bis zum Doppelten des so bestimmten Wertes als angemessen.¹⁴²

- 95 Nach der gesetzlichen Regelung darf das Bußgeld 10 % des weltweiten Konzernumsatzes im letzten Geschäftsjahr nicht übersteigen.¹⁴³ Im Unterschied zum europäischen Recht ist dies aber keine Kappungsgrenze, sondern gilt als Höchstbetrag des Bußgeldes. Die 10%-Grenze darf also nur in den denkbar schwersten Fällen erreicht werden. Normalerweise muss das Bußgeld deutlich weniger betragen. Insgesamt ist es noch weniger als in der europäischen Praxis möglich, das Bußgeld vorauszuberechnen. Dafür sind die Bußgelder in der Regel deutlich niedriger als die der Europäischen Kommission. Das Bundeskartellamt kann auch die finanzielle Leistungsfähigkeit des Unternehmens berücksichtigen.¹⁴⁴ Außerdem kann es Zahlungserleichterungen gewähren, insbesondere in Form eines Besserungsscheins (d.h. das Unternehmen muss das Bußgeld nur zahlen, wenn sich seine finanzielle Situation verbessert). Praktisch immer stellt das Bundeskartellamt im Bußgeldbescheid fest, dass das Bußgeld der Ahndung des Verstoßes (und nicht der Vorteilsabschöpfung) dient. Dann ist eine steuerliche Berücksichtigung ausgeschlossen und das Bußgeld aus den Netto-Einkünften zu bezahlen. Die deutschen Gerichte haben die Berechnungsweise des Bundeskartellamtes nicht akzeptiert und legen stattdessen den gesetzlichen Höchstbetrag von 10 % des weltweiten Gesamtumsatzes zugrunde. Das führt dazu, dass sie den vom Bundeskartellamt festgesetzten Bußgeldbetrag in einigen Fällen deutlich heraufgesetzt haben. Der bislang deutlichste Fall betraf das Verfahren im Fall Rossmann, in dem das OLG Düsseldorf die Geldbuße von 5 Mio. EUR auf 20 Mio. EUR erhöhte.¹⁴⁵ Im Jahr 2017 hatte das OLG die vom Bundeskartellamt

139 Abrufbar unter www.bundeskartellamt.de.

140 Bußgeldleitlinien des Bundeskartellamtes, Rn. 14.

141 Bußgeldleitlinien des Bundeskartellamtes, Rn. 8.

142 Bußgeldleitlinien des Bundeskartellamtes, Rn. 15.

143 § 81c Abs. 2 Satz 2 GWB.

144 Bußgeldleitlinien des Bundeskartellamtes, Rn. 16.

145 OLG Düsseldorf, 11.11.2022 – V 1 Kart 1/22 OWi. Ursprünglich hatte das Gericht das Bußgeld sogar auf 30 Mio. EUR erhöht, dieses Urteil wurde vom BGH jedoch aus formellen Gründen aufgehoben.

verhängten Bußgelder im Tapetenkartellverfahren¹⁴⁶ um 30–40 % und im Süßwarenkartell um 50–60 % heraufgesetzt.¹⁴⁷

Für die persönlichen Bußgelder beträgt der Höchstbetrag 1 Mio. EUR bzw. bei leichteren Verstößen 100.000 EUR.¹⁴⁸ Auch diese Grenze darf nur in den denkbar schwersten Fällen erreicht werden. Bei fahrlässigen Handlungen beträgt der Höchstbetrag die Hälfte.¹⁴⁹ In der Praxis wird vielfach ein Brutto-Jahresgehalt als Maßstab zugrunde gelegt. In den meisten Fällen setzt das Bundeskartellamt neben dem Unternehmensbußgeld auch Bußgelder gegen die persönlich Verantwortlichen fest. Es ist dazu aber nicht verpflichtet.

c) Schadensersatz

Schadensersatzforderungen haben als Risikofaktor für Kartellunternehmen erheblich an Gewicht gewonnen. Dabei liegt das Schadensersatzrisiko oftmals um ein Vielfaches höher als das Bußgeldrisiko. Dieses Risiko besteht insbesondere auch, wenn ein Unternehmen von einer Kronzeugenregelung Gebrauch gemacht hat und deshalb von einer Geldbuße befreit ist oder wenn Unternehmen sich einvernehmlich mit der Wettbewerbsbehörde einigen. Die erhöhte Wahrscheinlichkeit eventueller Schadensersatzforderungen – und deren signifikante Höhe – muss daher bei diesen Schritten immer mitberücksichtigt werden. Der EuGH hat klargestellt, dass auch der wirtschaftliche Nachfolger eines Unternehmens für kartellrechtlichen Schadensersatz haftet. Der Unternehmensbegriff ist hier wie im Rahmen der Bußgeldhaftung als wirtschaftliche Einheit zu verstehen und somit einheitlich im europäischen Recht anzuwenden.¹⁵⁰

Ist ein Unternehmen durch ein Kartell geschädigt, gehört es heute zu den geschäftlichen Pflichten der Leitungsorgane, die Geltendmachung von Schadensersatzansprüchen zu prüfen. Dadurch ist die Geltendmachung von Schadensersatzansprüchen zunehmend übliche Praxis. Künftig ist mit einem weiteren Anstieg der Geltendmachung solcher Schadensersatzforderungen zu rechnen. Diese werden in der Regel gegen die am Kartell beteiligten Unternehmen geltend gemacht; sie können sich aber auch gegen die persönlich Verantwortlichen, die schuldhaft gehandelt haben, richten.

aa) Individualansprüche

Das Schwergewicht liegt in Deutschland und den anderen europäischen Ländern auf der individuellen Geltendmachung von Schadensersatzforderungen durch die Geschädigten. Jeder, der durch ein Kartell geschädigt ist, hat Anspruch auf

146 OLG Düsseldorf, 12.10.2017 – V-2 Kart 1/17 (Owi).

147 OLG Düsseldorf, 26.1.2017 – V-4 Kart 6/15 (Owi). Diese Entscheidung wurde jedoch vom BGH wegen einer lückenhaften Beweiswürdigung zurückverwiesen, BGH, 21.6.2019 – KRB 10/18.

148 § 81c Abs. 1 Satz 1 GWB.

149 § 17 Abs. 2 OWiG.

150 EuGH, 14.3.2019 – Rs. C-724/17, ECLI:EU:C:2019:204 – Skanska.

vollständigen Ersatz seines Schadens.¹⁵¹ Um die Durchsetzung von Schadensersatzansprüchen auf europäischer Ebene zu vereinheitlichen und weiter zu verbessern, hatte die EU eine europäische Richtlinie zur Geltendmachung von Schadensersatzansprüchen wegen Kartellrechtsverstößen beschlossen.¹⁵² Die Richtlinie ist in Deutschland durch die 9. GWB-Novelle in nationales Recht umgesetzt worden.

- 100** Die §§ 33a ff. GWB enthalten nun eine Vielzahl von materiellrechtlichen Vorschriften zur Schadensersatzpflicht bei Kartellverstößen, die als Spezialnormen vor allem den §§ 249 ff. und 251 BGB vorgehen. Außerdem sind in den §§ 89b ff. GWB die verfahrensrechtlichen Besonderheiten geregelt, die von den allgemeinen Vorschriften in der ZPO, der StPO und dem OWiG abweichen.
- 101** Meist braucht der Kläger einen Kartellverstoß nicht nachzuweisen, da dieser durch die Behörde bindend festgestellt ist.¹⁵³ Wohl aber muss er als Anspruchsteller nach den Regeln der deutschen Zivilprozessordnung seinen Schaden konkret darlegen. Zu den neuen Vorschriften im GWB gehört nunmehr eine widerlegliche Vermutung, dass ein Kartell einen Schaden verursacht. Im Schienenkartellverfahren lehnte der BGH jedoch einen Anscheinsbeweis für Kartellschäden und die Kartellbefangenheit bei Quoten- und Kundenschutzkartellen ab.¹⁵⁴ Es könne nicht in jedem Fall unterstellt werden, dass Absprachen erfolgreich umgesetzt werden, sodass die Beweislast auf der Klägerseite verbleibe. Offen ist, ob diese Grundsätze auch bei anderen Hardcore-Absprachen, insbesondere Preisabsprachen, anwendbar sind. Allerdings gilt die BGH-Entscheidung nur für kartellrechtliche Schadensersatzansprüche, die vor dem 27.12.2016 entstanden sind. Für jüngere Fälle greift die (widerlegliche) gesetzliche Vermutung nach § 33a Abs. 2 GWB.
- 102** Ferner ist dem mittelbar Geschädigten (z. B. einem Einzelhändler oder einem Weiterverarbeiter), der das Kartellprodukt von einem Großhändler zu dem überhöhten Kartellpreis erworben hat, ein gleichberechtigter Schadensersatzanspruch eingeräumt (passing on). Es gilt die widerlegliche Vermutung zugunsten des mittelbaren Abnehmers, dass der Preisaufschlag durch den Erstabnehmer auf ihn abgewälzt wurde.
- 103** Mehrere Kartellunternehmen haften gesamtschuldnerisch.¹⁵⁵ Insoweit sind allerdings dem Kronzeugenunternehmen gewisse Vergünstigungen eingeräumt. Kleinere und mittlere Unternehmen sind unter bestimmten Voraussetzungen von

151 EuGH, 20.9.2001 – Rs. C-453/99, ECLI:EU:C:2001:465 – Courage.

152 Richtlinie des Europäischen Parlaments und des Rates über bestimmte Vorschriften für Schadensersatzklagen nach nationalem Recht wegen Zuwiderhandlungen gegen wettbewerbsrechtliche Bestimmungen der Mitgliedstaaten und der Europäischen Union, ABl. L 349, S. 1 ff. vom 5.12.2014.

153 Vgl. § 33 Abs. 4 GWB.

154 BGH, 11.12.2018 – KZR 26/17.

155 Vgl. § 33d GWB.

der gesamtschuldnerischen Haftung ausgenommen. Weiterhin ist vorgesehen, dass alle Schadensersatzansprüche erst nach Ablauf von fünf Jahren verjähren.

Eine weitere wichtige Neuerung besteht in dem Offenlegungsanspruch nach § 33g GWB. Danach kann der Geschädigte vom Kartellunternehmen oder auch einem unbeteiligten Dritten verlangen, dass diese alle Unterlagen vorlegen oder alle Auskünfte erteilen, die der Geschädigte für den Nachweis seines Schadensersatzanspruchs zwingend benötigt (sog. Disclosure). Dabei ist allerdings das Vertraulichkeitsinteresse insbesondere von Kronzeugen, die Unterlagen freiwillig an die Behörde herausgegeben haben, und von Betriebs- und Geschäftsgeheimnissen abzuwägen. Unter bestimmten Voraussetzungen kann der Geschädigte auch von Behörden die Herausgabe von Unterlagen oder die Erteilung von Auskünften verlangen.¹⁵⁶ Ein allgemeines Recht auf Akteneinsicht steht dem Geschädigten aber nicht zu. Der Schadenersatzkläger kann seinen Offenlegungsanspruch entweder im anhängigen Schadenersatzprozess¹⁵⁷ oder in einem gesonderten Verfahren geltend machen.

bb) Kollektiver Rechtsschutz

In den USA sind die sog. Class Actions die bei Weitem wirksamste Sanktion bei Kartellverstößen. Derartige Sammelklagen gab es bislang in Deutschland und den meisten anderen europäischen Ländern nicht. Seit der Umsetzung der EU-Verbandsklagenrichtlinie¹⁵⁸ in deutsches Recht besteht in Gestalt der Abhilfeklage gemäß § 1 Abs. 1 Nr. 1 VDuG erstmals ein Instrument zur kollektiven Durchsetzung von Kartellschadenersatzansprüchen.¹⁵⁹ Verbraucherverbände können demnach nun nicht mehr nur Unterlassungs- und Mehrerlösabführungsansprüche (an die Staatskasse) geltend machen, sondern auch die Schadensersatzansprüche einzelner Verbraucher bündeln und im sog. Abhilfeverfahren kollektiv geltend machen. Ob sich diese neue Möglichkeit der Anspruchsdurchsetzung großer Beliebtheit erfreuen wird (und somit auch die entsprechenden Risiken für kartellbeteiligte Unternehmen signifikant erhöhen wird), muss sich noch in der Praxis zeigen.¹⁶⁰

Daneben Bedeutung erlangt hat die Durchsetzung von Kartellschadenersatzansprüchen mithilfe von Inkassodienstleistern. Dabei treten Geschädigte ihre Schadensersatzansprüche kollektiv an hierauf spezialisierte Dienstleistungsunternehmen ab, die dann deren klageweise Durchsetzung betreiben (sog. Abtre-

156 Einzelheiten ergeben sich insbesondere aus § 33g Abs. 4 und 5 GWB. Zusätzlich kann das Gericht nach § 89c GWB auf Antrag die Vorlegung von Urkunden oder Gegenständen aus den Akten der Wettbewerbsbehörde fordern.

157 Die Entscheidung erfolgt nach § 89b Abs. 3 GWB in diesem Fall durch Zwischenurteil.

158 Richtlinie 2020/1828 vom 25.11.2020 über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG, Abl. L 409/1 vom 4.12.2020.

159 Zu den Einzelheiten der neuen Regelung: *Schläfke/Lühmann*, NJW 2023, 3385; *Hornkohl*, NZKart 2024, 2.

160 Eher pessimistisch *Schneider/Conrady/Kapoor*, BB 2023, 2179.

tungsmodell). Die Zulässigkeit dieses Modells nach dem Rechtsdienstleistungsgesetz wurde jedoch mehrfach von deutschen Gerichten verneint, bis der BGH die grundsätzliche Zulässigkeit in einem nicht-kartellrechtlichen Verfahren festgestellt hat.¹⁶¹ Zweifelhaft ist aber weiterhin, ob dies auch für Kartellschadensersatzansprüche gilt. In Frage gestellt wurde das u. a. vom Landgericht Dortmund, das diese Frage im Jahr 2023 dem EuGH zur Vorabentscheidung vorgelegt hat.¹⁶² Eine Entscheidung hierüber steht noch aus. Sollte der EuGH das Abtretungsmodell für zulässig halten, erhöht dies die Rechtsschutzmöglichkeiten für Geschädigte – und auf der Gegenseite das Schadensersatzrisiko für Kartellanten – jedenfalls weiter.

cc) Schadensausgleich im Innenverhältnis

- 107** Der Geschädigte kann seinen Schaden in voller Höhe gegen jedes Unternehmen einklagen, das am Kartell beteiligt ist bzw. war. Dabei liegt es nahe, dass er mit Vorliebe das Unternehmen als Beklagten auswählt, das sich im Rahmen eines Kronzeugenantrags als erstes schuldig bekannt hat. Das zum Schadensersatz verurteilte Unternehmen muss im Rückgriff einen anteiligen Ausgleich durch die anderen Kartellunternehmen einfordern. In dieser Hinsicht besteht noch erhebliche Rechtsunsicherheit, vor allem nach welchen Kriterien die Anteile im Innenverhältnis bemessen werden.¹⁶³ Auch droht u. U. eine Verjährung der Ausgleichsansprüche, wenn die Schadensersatzklage lange Zeit in Anspruch genommen hat. Hinzu kommt, dass gegen ausländische Unternehmen ein Schadensausgleich möglicherweise gar nicht durchgesetzt werden kann.¹⁶⁴ Das Unternehmen, das als erstes auf Schadensersatz verklagt wird, befindet sich daher häufig in einer misslichen Lage. Ähnliche Probleme und Unsicherheiten bestehen bei einer vertraglichen, außergerichtlichen Einigung über Schadensersatzzahlungen.

d) Sonstige Nachteile

- 108** Neben den Bußgeldern und Schadensersatzverpflichtungen können Kartellverstöße eine Vielzahl weiterer Nachteile zur Folge haben, die im Ergebnis ein erhebliches Ausmaß erreichen können: Dazu zählt insbesondere der Zeit- und Kostenaufwand, der durch die Aufdeckung des Kartellrechtsverstosses und die Verteidigung im Behörden- und Gerichtsverfahren anfällt. Auch führt die Verurteilung wegen eines Kartellrechtsverstosses meist zu einer Schädigung der Reputation, die sich bei börsennotierten Unternehmen erheblich auf den Börsenkurs auswirken kann. Hinzukommen können auch vergabe- und gewerberechtliche Sanktionen. Für die persönlich Verantwortlichen stehen die arbeitsrechtlichen

¹⁶¹ BGH, 13.7.2021 – II ZR 84/20, NZKart 2021, 515 – Sammelklage-Inkasso.

¹⁶² LG Dortmund, 13.3.2023, 8 O 7/20 (Kart) – NZKart 2023, 229 – Rundholzkartell NRW (anhängig unter Rs. C-253/23); zur Zulässigkeit des Abtretungsmodells zuletzt OLG München, 28.3.2024 – 29 U 1319/20 (LKW-Kartell).

¹⁶³ Zu diesen Fragen ausführlich *Gänswein*, NZKart 2016, 51 ff.

¹⁶⁴ Im amerikanischen Rechtssystem ist ein Schadensausgleich im Innenverhältnis bei Kartellverstößen überhaupt nicht vorgesehen.

Konsequenzen im Vordergrund, die bis zur fristlosen Kündigung reichen können. In bestimmten Fällen ist sogar ein Berufsverbot wegen erwiesener Unzuverlässigkeit nicht ausgeschlossen.¹⁶⁵

Weitere Folgen können sich für Unternehmen im Bereich der öffentlichen Auftragsvergabe ergeben. Bereits im Juli 2017 wurde in Deutschland ein Wettbewerbsregistergesetz verabschiedet.¹⁶⁶ Öffentliche Auftraggeber können seitdem in einem bundesweiten Wettbewerbsregister (einer sog. „schwarzen Liste“) nachprüfen, ob ein Unternehmen wettbewerbsrelevante Delikte begangen hat. Seit Juni 2022 sind sie ab einem Auftragswert von 30.000 EUR sogar dazu verpflichtet. Kartellrechtsverstöße werden ab einem Bußgeldbescheid i. H. v. 50.000 EUR eingetragen. Anders als bei anderen Verstößen erfolgt die Eintragung bereits vor Rechtskraft. Der öffentliche Auftraggeber kann aber nach freiem Ermessen entscheiden, ob der Kartellverstoß zu einem Ausschluss vom Bieterverfahren führt. Die Eintragung wird nach drei bis fünf Jahren automatisch oder vorzeitig bei Nachweis einer sog. Selbstreinigung gelöscht. Zu den Voraussetzungen zählen wirksame Compliance-Maßnahmen.¹⁶⁷ In seinen „Leitlinien zur vorzeitigen Löschung einer Eintragung aus dem Wettbewerbsregister wegen Selbstreinigung“ hat das Bundeskartellamt Hinweise gegeben, welche technische, organisatorische und personelle Maßnahmen geeignet sind, weiteres Fehlverhalten zu vermeiden.¹⁶⁸ Von dem bundesweiten Wettbewerbsregister, das beim Bundeskartellamt geführt wird, wird rege Gebrauch gemacht: Täglich werden dort durchschnittlich zwischen 800 und 1.000 Abfragen durchgeführt. Nach Angaben des Bundeskartellamts ergeben diese jede Woche mehrere Treffer. Ein Treffer bedeutet, dass Angaben zu einem Fehlverhalten übermittelt worden sind, die im Register aufgeführt sind.¹⁶⁹

109

II. Management der Kartellrechtsrisiken in der Praxis

Wie sieht nun ein wirksames Kartellrechts-Compliance-Programm aus? Welche Maßnahmen muss es und welche kann es haben? Wovon hängt das ab? Dass sich

110

165 Im Einzelnen vgl. dazu *Seeliger/Mross*, in: Jaeger/Kokott/Pohlmann/Schroeder/Seeliger, Frankfurter Kommentar zum Kartellrecht, Stand 5/2024, E. Kartellrechts-Compliance, Rn. 31 ff., 55 ff. und 69 ff.

166 Gesetz zur Einführung eines Wettbewerbsregisters vom 18.7.2017, BGBl. I 2017, S. 2739. Siehe dazu auch → *Scherer*, Kap. 28 Rn. 18, 32.

167 § 8 Abs. 1 Satz 3 WRegG i.V.m. § 125 Abs. 1 Satz 1 Nr. 3 GWB; siehe im Allgemeinen *Hooghoff*, WuW 2021, 551, 556 f. Zu den Anforderungen an wirksame Compliance-Maßnahmen auch → *Schulz*, Kap. 1 Rn. 52 ff.

168 Siehe Leitlinien zur vorzeitigen Löschung einer Eintragung aus dem Wettbewerbsregister wegen Selbstreinigung aus November 2021, https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/WettbewReg/Leitlinien_vorzeitige_Loeschung.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 25.4.2024); siehe zur Selbstreinigung und den neuen Leitlinien auch *Herrlinger/Ahlenstiehl*, WuW 2022, 396; *Koll*, NZBau 2023, 491. Zur sog. Selbstreinigung ausführlich → *Scherer*, Kap. 28 Rn. 41 ff.

169 Bundeskartellamt, Jahresbericht 2022/23, S. 69.

jedes Unternehmen mit der Frage beschäftigen sollte, ob und in welchem Umfang seine Geschäftsaktivitäten kartellrechtlichen Risiken ausgesetzt sind, dürfte unbestritten sein. Wie tiefgehend sich ein Unternehmen mit dieser Frage befasst und wie umfangreich letztlich die kartellrechtlichen Compliance-Maßnahmen sind, hängt von dem individuellen Ergebnis der Risikoanalyse ab (dazu unter 1., → Rn. 112 ff.). Diese bildet die Grundlage für die konkreten Maßnahmen zur Vorbeugung (dazu unter 2., → Rn. 121 ff.) und Kontrolle/Aufdeckung (dazu unter 3., → Rn. 146 ff.).

- 111** Festzuhalten ist: Weder Gesetzgeber noch Kartellbehörden sehen einen detaillierten Anforderungskatalog von zwingenden, konkreten Maßnahmen eines Kartellrechts-Compliance-Programms oder Compliance-Management-Systems vor. Allgemeine Standards und Mindestanforderungen – sowohl übergreifend für Compliance-Bereiche¹⁷⁰ (damit auch anwendbar auf das Kartellrecht) als auch speziell für das Kartellrecht¹⁷¹ – gibt es zunehmend; inhaltlich sind sie weitestgehend deckungsgleich und konsistent.¹⁷² Öffentliche Hilfestellungen zur Ausgestaltung von Compliance-Programmen gibt beispielsweise die internationale Handelskammer (International Chamber of Commerce, ICC) und die OECD: Die ICC hat 2013 und 2015 Toolkits zur kartellrechtlichen Compliance als Leitfaden für (mittelständische) Unternehmen herausgegeben;¹⁷³ die OECD hat 2021 ein Competition Compliance Programmes Discussion Paper herausgegeben.¹⁷⁴ Auch zahlreiche Kartellbehörden haben solche Hilfestellungen zu kartellrechtlichen Compliance-Programmen veröffentlicht.¹⁷⁵

170 Beispielhaft: ISO 37301, IDW PS 980 n. F. aus 09.2022. Zu den Mindestanforderungen an wirksame Compliance-Management-Systeme → *Schulz*, Kap. 1 Rn. 52 ff.

171 Beispielhaft zuletzt (Juli 2019) „Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations“ der Antitrust Division des US Department of Justice (DoJ), <https://www.justice.gov/atr/page/file/1182001/download> (zuletzt abgerufen am 25.4.2024). Siehe auch DICO Standard 15 Grundsätze eines kartellrechtlichen CMS von April 2022.

172 Siehe insgesamt zu Vorgaben und Standards zur Kartellrechts-Compliance: *Seeliger/Mross*, in: Jaeger/Kokott/Pohlmann/Schroeder/Seeliger, Frankfurter Kommentar zum Kartellrecht, Stand 5/2024, E. Kartellrechts-Compliance, Rn. 137 ff. Zu den Kernelementen eines wirk samen Compliance Managements siehe → *Schulz*, Kap. 1 Rn. 52 ff.

173 Beide abrufbar unter www.iccwbo.org.

174 Abrufbar unter <https://web.archive.org/2021-10-31/591205-competition-compliance-programmes-2021.pdf> (zuletzt abgerufen am 25.4.2024).

175 Beispielsweise das US DoJ (Antitrust Division) „Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations“; die britische CMA „Quick Guide to Complying with Competition Law“; die französische Autorité de la concurrence „Framework Document on Competition Compliance Programmes“; die spanische CNMC „Antitrust Compliance Programmes Guidelines“; die brasilianische CADE „Guidelines – Competition Compliance Programs“; das kanadische CBC „Guidance on the core principles of a credible and effective compliance program“ (alle Dokumente online abrufbar).

1. Risikoanalyse: Identifizierung und Bewertung

Um kartellrechtliche Risiken durch angemessene Compliance-Maßnahmen zu steuern, ist es zunächst erforderlich, dass die im ersten Teil beschriebenen potenziellen Risikobereiche im Unternehmen identifiziert und in Bezug auf Relevanz und mögliches Schadenspotenzial bewertet werden. Dabei sind regelmäßig verschiedene Unternehmensabteilungen involviert, wie z.B. die Rechtsabteilung (sofern ihr nicht die kartellrechtliche Compliance-Funktion ohnehin zugeordnet ist), das Risikomanagement, die Interne Revision und der Bereich des Controlling. Entscheidend ist, dass die verschiedenen Abteilungen effektiv zusammenarbeiten. Ein adäquates Schnittstellenmanagement ist dabei unerlässlich.¹⁷⁶ 112

a) Kartellrechtliches Risikoprofil

Kartellrechtliche Risiken können je nach Art, Umfang und Internationalität der Geschäftstätigkeit, Struktur der Märkte, Organisation und Marktstellung des Unternehmens unterschiedlich gelagert und ausgeprägt sein. Es gibt z.B. Märkte, die aufgrund ihres Konzentrationsgrades, Produktstandardisierungen oder der Stabilität anfälliger als andere Märkte für Kartellverstöße sind. Das kartellrechtliche Risikoprofil sollte ggf. für jeden Unternehmensbereich und jede Region getrennt ermittelt werden. Etwaige Abweichungen von einer konzernweiten Risikolage sollten überprüft und festgehalten werden. Denn zum einen können sich im Unternehmensbereich A Risiken ergeben (Schwerpunkt: Kooperationen/Kontakte mit Wettbewerbern), die es im Unternehmensbereich B nicht gibt, und umgekehrt (dort Schwerpunkt: Marktbeherrschung). Zum anderen stellen sich die Risiken in einem Land mit intensiver Kartellverfolgung durch die nationale Wettbewerbsbehörde und starker Unternehmenspräsenz (viel Umsatz, viele Kunden, viele Standorte) anders dar als in einem Land ohne bzw. mit einer wenig „aktiven“ Kartellbehörde und geringer Unternehmenspräsenz (kaum Umsatz, wenige Kunden, kein oder nur kleiner Standort).¹⁷⁷ 113

b) Geschäftstätigkeit und Geschäftsbeziehungen

Ausgangspunkt der Risikobestimmung sind in der Regel die (typischen) Geschäftstätigkeiten, bei denen die im ersten Teil genannten kartellrechtlichen Risiken bestehen. Dabei kann nach den Schwerpunkten horizontaler und vertikaler Beziehungen (d.h. Verhältnis zu Wettbewerbern einerseits und Verhältnis zu Kunden/Lieferanten und sonstigen Geschäftspartnern andererseits) vorgegangen werden. Ein Teil der kartellrechtlichen Risiken kann im laufenden Vertragsmanagement angesiedelt werden. Aber nicht alle kartellrechtlichen Risiken – gerade nicht die mit einem besonders hohen Schadenspotenzial – tauchen im Zusammenhang mit der Vertragsgestaltung auf. Insbesondere die kartellrechtlich 114

¹⁷⁶ Schulz, CB 9/2015, 1, 5. Zum Schnittstellenmanagement ferner → Schulz, Kap. 1 Rn. 85, → Rau, Kap. 3, → Renz/Frankenberger, Kap. 20 Rn. 60 ff.

¹⁷⁷ Siehe dazu auch Heckenberger/Schulz, in: Moosmayer, Compliance-Risikoanalyse, § 9 Rn. 18 f.

relevanten Berührungspunkte mit Wettbewerbern außerhalb von vertraglich vereinbarten Kooperationen (z.B. im Rahmen der Verbandsarbeit und bei Benchmarking-Aktivitäten) sind separat zu erfassen. Von einer pauschalen Ausgrenzung bestimmter Risikobereiche, z.B. in Bezug auf Risiken beim Missbrauch einer marktbeherrschenden Stellung, ist abzuraten. Auch hier sollte das Risikoprofil grundsätzlich – zumindest in grober Form – ermittelt und anschließend bei der Bewertung angemessen eingeordnet werden. So wird dokumentiert, dass man ein Risiko erkannt und bestimmt, aber – aus anzugebenden Gründen – als weniger relevant angesehen hat.

- 115** Für jedes Unternehmen ist es wichtig, eine individuelle Bestandsaufnahme durchzuführen.¹⁷⁸ Neben den allgemeinen Hilfsmitteln zur Compliance-Risikoanalyse¹⁷⁹ stehen dem Praktiker dabei auch kartellrechtsspezifische Hilfsmittel zur Verfügung. Das ICC Toolkit zur kartellrechtlichen Compliance z.B. zählt beispielhaft einige Punkte auf, die bei der Identifizierung der unternehmenseigenen Risiken berücksichtigt werden können, und gibt auch Beispiele für die Bewertung dieser Risiken (Risiko-Register).¹⁸⁰ Auch Kartellbehörden stellen Checklisten und Informationen für die Risikoidentifizierung und -bewertung online.¹⁸¹

c) Risikokategorisierung und Risikobewertung

- 116** Bei der Bewertung wird in der Regel zwischen unterschiedlichen Risikokategorien unterschieden (vgl. → Rn. 8 ff.). Diese lassen sich z.B. in hohe und weniger hohe Risiken einteilen, je nach Schwere der Sanktion bzw. des Schadenspotenzials und Wahrscheinlichkeit des Verstoßes. Ein risikoerhöhender Umstand ist z.B. eine etwaige Kartellhistorie in der Branche oder sogar im Unternehmen selbst oder das Bestehen vielfältiger Wettbewerberkontakte (auch im Rahmen von Kooperationen, Gemeinschaftsunternehmen, Verbänden). Risikoidentifizierung und -bewertung sollten in regelmäßigen Abständen oder ad hoc bei besonderen Anlässen (z.B. neuen Geschäftsfeldern, neuen Gesetzen/Gesetzesände-

178 Zur Risikoidentifizierung siehe z.B. *Reimer/Brack/Schmidt*, CCZ 2016, 83; *Pautke*, in: *Schultze, Compliance-Handbuch Kartellrecht*, Teil B, Rn. 1. Zur Bedeutung des unternehmensspezifischen Risikoprofils ferner → *Schulz*, Kap. 1 Rn. 60 ff.

179 Vgl. z.B. DICO, Standard 09 – Compliance Risikoanalyse (veröffentlicht im März 2020), sowie L02 – Kriterien zur internen Qualitätssicherung von CM-Systemen, 11. Siehe hierzu auch *Ebersoll/Stork*, CCZ 2013, 129 ff.; *Hauschka/Moosmayer/Lösler*, in: *Hauschka/Moosmayer/Lösler, Corporate Compliance*, § 1 Rn. 8 ff.; *Pyrcek*, in: *Umnuß*, § 13 Rn. 64 ff.

180 ICC Toolkit zur kartellrechtlichen Compliance, 35 ff., Anhang 2. Siehe ebenso ICC SME Toolkit, S. 7. Hilfreiche Checklisten finden sich auch z.B. bei *Pautke*, in: *Schultze, Compliance-Handbuch Kartellrecht*, 1. Aufl. 2013, Teil B VI, Rn. 152, VII, Rn. 201 und VIII Rn. 278.

181 Z.B. Dokumente der Competition and Markets Authority (GB), z.B. *Competition Law Checklist* und *Competition Law Risk – A Short Guide* sowie die Broschüre der Europäischen Kommission „Compliance matters“, 2012 (beide abrufbar im Internet).

rungen) wiederholt und aktualisiert werden, um die früheren Einschätzungen und Ergebnisse zu überprüfen.

Entscheidend für eine realistische Risikoidentifizierung und -bewertung ist eine Verknüpfung von kartellrechtlicher Expertise mit Kenntnissen über das operative Geschäft mit allen Produkten, Vertriebswegen, Marktverhältnissen und sonstigen Abläufen, Prozessen und Aktivitäten. Fehlt ersteres oder letzteres, besteht die Gefahr, dass bestehende Risiken nicht erkannt oder unzureichend bewertet werden. Dabei ist für die kartellrechtliche Expertise ggf. auf externe Berater zurückzugreifen. 117

d) Einführung eines Top-down-Ansatzes

Bei der (erstmaligen) Risikoanalyse empfiehlt es sich in der Regel, dem Grundsatz „vom Allgemeinen zum Konkreten“ zu folgen und zunächst nach dem Top-down-Ansatz eine Analyse aus zentraler Funktion (mit kartellrechtlicher Expertise) anzufertigen, bevor diese Ergebnisse lokal mit häufig umfangreichen und Ressourcen-aufwendigen Workshops und Interviews überprüft, ergänzt und vervollständigt werden. 118

Die Ergebnisse der Risikoanalyse sollten angemessen und nachvollziehbar dokumentiert werden (zumindest im Excel-Format, sofern kein spezifisches IT-Tool Anwendung findet). Dabei ist aber gerade bei der Formulierung äußerste Sorgfalt zu wahren, um falsche Darstellungen und Fehlinterpretationen zu vermeiden. 119

Zur Methodik und Dokumentation der Risikoanalyse sollte etwaigen fachbereichsübergreifenden Vorgaben zum Risikomanagement bzw. internen Kontrollsystem gefolgt werden, um von der unternehmenseigenen Fach-Expertise zu profitieren und Konsistenz mit Risikoanalysen in anderen Unternehmensbereichen, insbesondere Compliancebereichen, zu wahren. 120

2. Präventive Maßnahmen

Kartellrechts-Compliance ist im Wesentlichen präventive Arbeit. Kartellrechtsrisiken können nur in beschränktem Umfang durch Maßnahmen der Kontrolle gesteuert werden (im Unterschied zu anderen Compliance-Bereichen, die insbesondere elektronische Geschäftsvorgänge oder sonstige prozessgesteuerte Aktivitäten zum Gegenstand haben, in denen automatische oder manuelle Kontrollpunkte gesetzt werden können). Vielmehr ist bei allen betroffenen Mitarbeitern das Bewusstsein für die kartellrechtlichen Risikofelder durch Maßnahmen der Aufklärung und Instruktion zu schaffen und zu erhalten. Wichtige präventive Maßnahmen stellen Richtlinien (einschließlich Leitfäden, Checklisten, Verhaltensregeln etc., nachfolgend → Rn. 122 ff.) und Schulungen (nachfolgend → Rn. 133 ff.) dar. Darüber hinaus ist die Beratung der Mitarbeiter durch einen unternehmensinternen Ansprechpartner für das Kartellrecht von herausragender Bedeutung. Richtlinien und Schulungen werden den Mitarbeitern nur Grund- 121

kenntnisse und ein allgemeines Verständnis für die relevanten kartellrechtlichen Regelungen und Risiken vermitteln können. Darüber hinaus muss ein Mitarbeiter im Arbeitsalltag jederzeit die Möglichkeit haben, bei Zweifeln/Fragen im Einzelfall Rechtsrat einzuholen. Dafür muss der Kartellrechtsexperte als Ansprechpartner einerseits im Unternehmen hinreichend für die relevanten Risikogruppen bekannt sein und andererseits durch Ausgestaltung entsprechender Unternehmensprozesse formalisiert eingebunden sein (siehe → Rn. 146 f.).

a) Richt- und Leitlinien zum Kartellrecht

- 122** Die Leitlinien zum Kartellrecht werden sich – sofern bereits vorhanden – in das grundsätzliche Gerüst zum Richtlinienmanagement im Unternehmen einfügen.¹⁸² In manchen Fällen wird durch sie aber vielleicht auch ein Anstoß gesetzt, das Richtlinienmanagement weiter zu professionalisieren. Auch bei dem Aufsetzen von Richtlinien für das Kartellrecht wird die Orientierung an grundsätzlichen Kriterien hilfreich sein.¹⁸³ Festzuhalten ist: Bei Richtlinien gilt nicht „viel hilft viel“. Die schönste Richtlinie trägt nicht zu einem effektiven Compliance-System bei, wenn sie nicht gelesen und verstanden wird. „Kurz und knackig“ sollte die Devise sein – und das Format sollte in die Unternehmenskultur passen. Für den Ersteller von Regelungen kann ein aktueller Überblick über allgemeine, nicht kartellrechtsspezifische Leitlinien der Compliance-Verbände hilfreich sein.¹⁸⁴
- 123** Diese Richtlinien werden sich fortlaufend weiterentwickeln und Inhalte können z.B. nach Durchführung des „Roll-outs“ von Schulungen, sofern erforderlich, erneut angepasst werden (z.B. an einigen Stellen gekürzt oder detaillierter werden). Regelmäßige Aktualisierungen im Hinblick auf etwaige Gesetzesentwicklungen und neue Entscheidungspraxis sind auch hier selbstverständlich.
- 124** Je nach Format der allgemeinen Richtlinienstruktur des Unternehmens und Relevanz für das Unternehmen oder besonders betroffene Unternehmensbereiche/-funktionen kommen schlanke, allgemeine oder aber ausführliche Richtlinien zu Spezialthemen des Kartellrechts in Betracht, welche die folgenden Themen aufgreifen:

182 Zur Einführung von Richtlinien im Unternehmen vgl. *Stork*, CB 2013, 89.

183 Vgl. z.B. zur thematischen Abdeckung, Anwendbarkeit, rechtsverbindlichen Implementierung, Formalanforderungen: DICO, Leitlinie L02 – Kriterien zur internen Qualitätssicherung von CM-Systemen, 19.

184 Vgl. z.B. DICO, Leitlinie L01 – Geschäftspartner-Compliance.

- Allgemeines zum Kartellrecht;
- Informationsaustausch mit Wettbewerbern;
- Austausch von Informationen bei Transaktionen (M&A);
- Verbands- und Gremienarbeit;
- Unverbindliche Preisempfehlungen.

Auch wenn die Richt- und Leitlinien für jedes Unternehmen individuell zugeschnitten sein sollten, so können die Ersteller neuer Regelwerke auf zahlreiche „Muster“ als Orientierungsgrundlage zurückgreifen. Muster werden teilweise von Verbänden zur Verfügung gestellt und finden sich auch in Handbüchern und weiteren Aufsätzen und Veröffentlichungen, z. B.:

- Unternehmensrichtlinie für Compliance-Untersuchungen;¹⁸⁵
- Leitfaden für Mitarbeiter zu richtigem Verhalten bei kartellbehördlichen Ermittlungen und Merkblatt für den Empfang;¹⁸⁶
- Leitlinie „Kartellrechtliche Compliance“;¹⁸⁷
- Beispiele sogenannter kartellrechtlicher Dos and Don'ts.¹⁸⁸

Zusätzlich kann auch durch Recherchen im Internet nach öffentlich zugänglichen Kartellrechtsregelungen anderer Unternehmen eine Art „Benchmark“ vorgenommen werden.¹⁸⁹

Neben der klassischen Richtlinie können ergänzende Dokumente wie FAQs, „Dos and Don'ts“, Merkzettel, Checklisten im Visitenkartenformat o. Ä. den Mitarbeitern eine wertvolle Hilfe im Arbeitsalltag bieten, um auch in prägnanter Form einen schnellen Zugriff auf die wesentlichen Verhaltensregeln zu gewährleisten. In der Praxis sind pragmatische „Dos and Don'ts“-Übersichten ein Format, das den Adressaten in der Operative besonders entgegenkommt, erkennbar an Rückfragen wie z. B. „Sie hatten doch diese Ampelliste ...“.

Richtlinien und ergänzende Dokumente können auch auf einen bestimmten Adressatenkreis zugeschnitten sein, um Mitarbeiter gezielt in ihren jeweiligen Verantwortlichkeiten anzusprechen. So können spezielle Unterlagen z. B. für den Vertrieb, den Einkauf oder die Forschung und Entwicklung erstellt werden, oder zur Unterzeichnung vor Verbandstreffen.

Inhaltlich ist es empfehlenswert, die durchaus abstrakten und komplexen kartellrechtlichen Regeln in möglichst klare Verhaltensanweisungen umzusetzen – und dies in verständlicher Sprache (keine Rechtsbegriffe) und mit anschaulichen

185 ICC Toolkit zur kartellrechtlichen Compliance, Anhang 3 sowie ICC SME Toolkit.

186 Hauschka, in: Formularbuch Compliance, 2013, § 21 Rn. 1 und 2.

187 Vgl. z. B. die DICO-Leitlinie L06 – Kartellrechtliche Compliance von Mai 2016. Für weitere Informationen siehe www.dico-ev.de. Dazu Reimers/Hainz, CCZ 2016, 188.

188 Z. B. bei Schröder, CCZ 2015, 63, 67; DICO/Bundesverband Materialwirtschaft, Einkauf und Logistik e. V., Arbeitspapier A05, Kartellrechtliche Compliance, Beispielhaftes kartellrechtliches Regelwerk („Dos & Don'ts“).

189 So verweist Moosmayer – neben der Schilderung der Regelungen bei Siemens – auf Regelwerke von Bosch und Bayer, Moosmayer, Compliance, Rn. 154 ff.

Beispielen aus dem Arbeitsalltag der betroffenen Abteilungen. Dabei gilt: Die Mitarbeiter sollen nicht durch ein möglichst umfassendes Werk zu Kartellrechtsexperten fortgebildet werden, die sämtliche – oftmals komplexen – kartellrechtlichen Fragestellungen aus dem Arbeitsalltag selbstständig abschließend beurteilen und lösen können. Vielmehr sollen sie in gebotener Kürze, Prägnanz und Anschaulichkeit ein grundsätzliches Verständnis und Gefühl für kartellrechtlich relevante „Problemstellungen“ erlangen und, soweit notwendig, den Ansprechpartner für Kartellrecht im Unternehmen kontaktieren.

- 130** Es hat sich ebenfalls bewährt, in Richtlinien, in einem separaten Dokument oder einer Videobotschaft ein Bekenntnis der Geschäftsführung zur Relevanz der Einhaltung der kartellrechtlichen Vorschriften i. S. d. sog. „Tone from the Top“ zu integrieren.¹⁹⁰ Wie in anderen Compliance-Bereichen gilt, dass ohne eine entsprechende überzeugende und glaubwürdige Unterstützung durch die Geschäftsleitung und Führungskräfte auf allen Ebenen, Richtlinien und andere Compliance-Maßnahmen Gefahr laufen, wirkungslos zu bleiben.
- 131** Obwohl die Kartellgesetze weltweit zwar die grundlegenden Arten von Wettbewerbsbeschränkungen gleich oder zumindest ähnlich beurteilen, gibt es im Detail auch unterschiedliche Bestimmungen und Entscheidungspraxis der Behörden und Gerichte. Dies stellt die Unternehmen vor Herausforderungen bei der Erarbeitung von konzernweit geltenden Richtlinien mit einem einheitlichen Bewertungsmaßstab. Unvermeidbar ist jedenfalls bei der Anwendung eines „strengen“ Maßstabs, der sich an den Kartellgesetzen z. B. in Deutschland bzw. der EU, den USA und China/Japan orientieren kann, dass auf die Nutzung eines gewissen Spielraums, den ein lokaler Rechtsrahmen geben könnte, verzichtet wird. Dieser Nachteil wird aber in der Regel durch die Effizienz der Erstellung und Geltung einer konzernweiten Regelung und den Zweck der möglichst sicheren Verhinderung von Kartellrechtsverstößen mehr als kompensiert.¹⁹¹ Zudem kann gezielt im Rahmen einer Einzelfallbetrachtung der mögliche lokale Spielraum bewertet und ggf. genutzt werden.
- 132** Nicht vergessen werden darf die Erwähnung der grundlegenden kartellrechtlichen Ge- und Verbote in kurzer, verständlicher Form im Verhaltenskodex (Code of Conduct) des Unternehmens, da in diesem Dokument in der Regel nicht nur allgemein die Einhaltung von Recht und Gesetz von den Mitarbeitern eingefordert wird, sondern auch die wesentlichen Vorgaben für die zentralen Compliance-Bereiche – wie Kartellrecht – enthalten sind.¹⁹²

190 Zum „Tone from the Top“ als Bestandteil der Compliance-Kultur ausführlich → *Schulz*, Kap. 1 Rn. 69.

191 Zur Empfehlung konzernweiter kartellrechtlicher Compliance-Maßnahmen unter Beachtung regionaler Besonderheiten vgl. *Seeliger/Mross*, CB 2017, 304, 305.

192 Siehe dazu *Hess*, in: *Rübenstahl u. a.*, *Kartell Compliance*, 25. Kap., Rn. 4 f.

b) Schulungen (Präsenzs Schulungen und Webinars/E-Learning)

Für Kartellrechts-Compliance gelten bei der Gestaltung von Schulungen, seien es Präsenzs Schulungen oder Webinars¹⁹³/E-Learning, die allgemeinen Regeln.¹⁹⁴ **133**

Die Inhalte der Kartellrechtsschulungen sollten nach Durchführung einer Risikoanalyse zugeschnitten werden. In der Praxis ist aber auch eine schrittweise Festlegung und Weiterentwicklung eines ganzheitlichen Schulungskonzepts nach dem folgenden Schema möglich: **134**

- Erster Startpunkt bei der Geschäftsführung mit der Vorstellung des allgemeinen Schulungskonzepts und Gespräch zur Vertiefung des „Tone from the Top“, Darstellung wichtigster Inhalte von Schulungen (high-level);
- Weiterentwicklung des Konzepts und der Inhalte der Schulungen auf Grundlage dieses Gesprächs;
- Start von Compliance-Schulungen auf Führungskräfte-Ebene (wichtigste Inhalte zu allgemeinen Themen wie Organisation effektiver Compliance, Risikopotenzial Kartellrecht, Verbot wettbewerbsbeschränkender Vereinbarungen, Informationsaustausch, Leitlinien für Verbandstreffen, Preisempfehlungen und -bindungen, Verbot des Missbrauchs einer marktbeherrschenden Stellung) mit intensiven Diskussionsrunden und Feedback-Gesprächen;
- Zuschnitt anschließender Detail-Schulungen für die jeweiligen Teams dieser Führungskräfte nach kurzem Vorbereitungsgespräch mit den bereits geschulten Führungskräften („Bei Orientierung an der Führungskräfte-Schulung: Welche Themen sollten im Schwerpunkt geschult werden, welche Themen sehen Sie zusätzlich? Sind im Team Besonderheiten zu beachten – z. B. Vorlieben für interaktive Parts? Gab es im Team besondere Fragestellungen, die aufgenommen werden sollten?“);
- Durchführung („Ausrollen“) der Compliance-Schulungen zunächst in „Fokusgruppen“ (Start in einer Pilot-Jurisdiktion, in einem „Fokusteam“, z. B. im Vertrieb);
- Schulungen in weiteren Teams, dabei fortlaufende Anpassungen;
- Schulungen auch in weiteren Jurisdiktionen.

Auf dieser Grundlage kann dann die Konzeption eines E-Learning-Moduls erfolgen, das in regelmäßigen Abständen für eine Auffrischung des Bewusstseins der Mitarbeiter für die kartellrechtlichen Risikobereiche sorgt und eine rasche Schulung von neu ankommenden Mitarbeitern ermöglicht.¹⁹⁵ Detailarbeit ist hier wichtig, wenn es darum geht, für Vollständigkeit des Adressatenkreises zu **135**

193 Damit sind Telefon- oder Videokonferenzen gemeint, bei denen sich die Teilnehmer von ihrem Arbeitsplatz zuschalten und die Schulung visuell (Präsentation am Bildschirm) und akustisch verfolgen.

194 Siehe zu Rolle und Formaten von Schulungen ausführlich → *Hastenrath*, Kap. 6; DICO, Leitlinie L05 – Zielgruppenorientiertes Schulungskonzept. Speziell zum Kartellrecht *Hess*, in: *Rübenstahl u. a.*, *Kartell Compliance*, 25. Kap., Rn. 24 ff.

195 Zur Gestaltung von Compliance-Schulungen mittels E-Learning ausführlich → *Hastenrath*, Kap. 6.

sorgen: Erfolgt eine automatische Verknüpfung der Mitarbeiternamen für die festgelegten Abteilungen (z. B. Vertrieb, Einkauf) aus dem HR-System (z. B. SAP) mit der E-Learning-Datenbank? Falls nicht, wer sorgt für eine manuelle Verknüpfung und stete Aktualisierung – die Personal- oder die Compliance-Abteilung oder die/der Vorgesetzte? Hier ist die Zuständigkeit zu klären.

- 136 Ebenso gut kann in umgekehrter Weise das Schulungsprogramm mit dem konzernweiten Roll-out eines E-Learning-Moduls an einen zielgerichteten Adressatenkreis begonnen werden, um auf diesem Weg schnell und umfassend für eine Grundinstruktion aller betroffenen Mitarbeiter zu sorgen. Darauf aufbauend können dann vertiefte Themen und Diskussionen Gegenstand von Präsenzs Schulungen mit bestimmten Zielgruppen sein.
- 137 Beim Entwurf der Schulungspräsentation kann es hilfreich sein, fortlaufend eine „Master-Schulung“ weiterzuentwickeln, die dann die Grundlage für maßgeschneiderte Schulungen verschiedener Teams bildet. Denn zum Thema sollten nicht nur der Vertrieb, sondern z. B. auch die Abteilungen Marketing, Einkauf, F&E etc. geschult werden – u. a. zu den Aspekten Informationsaustausch und Verbandstreffen.
- 138 Beim Zuschnitt der Inhalte mag dieses Kapitel selbst unterstützen, aber auch die Webseiten der Kartellbehörden.¹⁹⁶
- 139 Beispielsfolien für Compliance-Schulungen werden durch Verbände und in Handbüchern zugänglich gemacht, z. B.:
 - DICO-Leitlinie „Kartellrechtliche Compliance“;¹⁹⁷
 - Einbindung der oben erwähnten Dos and Don'ts.¹⁹⁸
- 140 Bei der Formulierung gibt erneut das ICC Toolkit zur kartellrechtlichen Compliance Hilfestellung an die Hand.¹⁹⁹
- 141 Die eigenen Schulungsfolien können – über die in diesem Kapitel enthaltenen Beispiele hinaus – z. B. auch durch weitere Beispiele aus öffentlich zugänglichen Leitfäden angereichert werden.²⁰⁰ Die Schilderung von konkreten Fällen, die für den Industriezweig des Unternehmens von Relevanz sind oder bei denen die Teilnehmer sich durch Ortsnähe oder wegen eines konkreten Produkts, das sie in

196 Z. B. Europäische Kommission, Compliance with competition rules und Bundeskartellamt (beides abrufbar über das Internet).

197 DICO, Leitlinie L06 – Kartellrechtliche Compliance von Mai 2016. Für weitere Informationen siehe www.dico-ev.de.

198 Z. B. in Schröder, CCZ 2015, 63, 67; DICO/Bundesverband Materialwirtschaft, Einkauf und Logistik e. V., Arbeitspapier A05, Kartellrechtliche Compliance, Beispielhaftes kartellrechtliches Regelwerk („Dos & Don'ts“).

199 ICC Toolkit zur kartellrechtlichen Compliance, 45.

200 Beispiele z. B. im BDI-Leitfaden Kartellrecht, https://bdi.eu/media/themenfelder/wettbewerb/publikationen/201510_Leitfaden-Kartellrecht.pdf (zuletzt abgerufen am 25.4.2024) oder auch bei Schultze, Compliance Handbuch Kartellrecht, 2. Aufl. 2021, Teil E.II. – Standardinhalte für Schulungspräsentationen.

ihrem Alltag verwenden, angesprochen fühlen, stoßen ebenfalls in der Regel auf erhöhte Aufmerksamkeit von Teilnehmern an Compliance-Schulungen.²⁰¹ Auch im Kartellrecht können Inhalte gut in Form eines Quiz vermittelt werden, z. B. orientiert an einer aktuellen Fernsehshow.²⁰²

Schließlich kann der Praktiker auch bei der Erstellung von Compliance-Schulungen eine „Benchmark-Studie“ vornehmen und nach öffentlich zugänglichen Präsentationen Ausschau halten. Neben Schulungsunterlagen aus Schulungen für Compliance Officer und Rechtsabteilungen ermöglicht auch bereits eine rasche Suche im Internet den Zugriff auf Beispielsfolien und Webinar-Unterlagen. 142

Auch hier gilt wieder: Viel hilft *nicht* viel. Weniger Text (nur Kernbotschaften), mehr anschauliche Bilder. Zu viele Folien/Seiten führen eher zu einem Redescript und verhindern die Interaktion zwischen Vortragendem und den Teilnehmern. 143

Ebenso gilt es zu beachten: Nicht nur die kartellrechtlichen Verbote betonen, sondern auch zulässige Verhaltensweisen (Lösungen, Optionen) vorstellen, um nicht als „Geschäftsverhinderer“, sondern „Business Enabler“ oder zumindest als „Trusted Adviser“ angesehen zu werden. 144

Beim Nachhalten der durchgeführten Schulungen (insbesondere Teilnehmer, Inhalte, geplanter Turnus) und Einbinden von neuen Mitarbeitern gelten auch für das Kartellrecht die grundsätzlichen Regeln.²⁰³ 145

3. Maßnahmen zur Kontrolle/Aufdeckung

Maßnahmen zur Kontrolle und Aufdeckung zielen im Wesentlichen darauf ab, einerseits etwaige Kartellrechtsverstöße durch organisatorische oder prozessuale Maßnahmen zu verhindern oder zumindest frühzeitig aufzudecken und zu korrigieren und andererseits sicherzustellen, dass das Compliance-Management-System für diese Thematik allgemein angemessen ausgestaltet und wirksam ist.²⁰⁴ 146

Als klassische organisatorische und prozessuale Maßnahmen kommen Genehmigungs-/Freigabe-/Konsultationsvorbehalte in Betracht (sofern dies kapazitativ abdeckbar ist, z. B. für Wettbewerberkontakte/Verbandsmitgliedschaften, Informationsaustausch im Rahmen von M&A-Prozessen, Änderung von Preisstrategien, Entwürfe von Verträgen zu Kooperationen mit Wettbewerbern und Vertriebs-/Vertriebsmittlerveträgen etc.). Die Einbindung in Vertragsprüfungen dürfte verbreitet sein. Kataloge genehmigungs- oder zustimmungspflichtig 147

201 Z. B. Pressemeldungen und Fallberichte unter www.bundeskartellamt.de. Zum Nutzen konkreter Praxisbeispiele bei Schulungen → *Hastenrath*, Kap. 6.

202 Für eine interaktive Wissensvermittlung sprechen sich auch aus *Reimers/Brack/Modest*, NZKart 2018, 453, 457 f.

203 Vgl. → *Hastenrath*, Kap. 6.

204 Zu den möglichen Auswirkungen eines Compliance-Management-Systems auf eine drohende Kartellgeldbuße vgl. ausführlich *Trüg/Ruppert*, ZWeR 2020, 69, 88 ff.

tiger Tätigkeiten bieten sich aber ebenfalls an, um die Kartellrechtsrisiken über ausschließlich instruktive Maßnahmen (Richtlinien/Schulungen) angemessen zu steuern.

- 148** Ein erster pragmatischer Ansatz zur Überwachung ist es, die regelmäßigen Compliance-Schulungen für Rückkoppelungen zum Verständnis der Teilnehmer zu Compliance-Regelungen zu nutzen.²⁰⁵
- 149** Darüber hinaus kann auch auf fortlaufende Risikoidentifizierungen und -bewertungen durch andere Bereiche (z. B. durch das Risikomanagement, die Interne Revision im Rahmen der Jahresplanung) zurückgegriffen werden.²⁰⁶ Dies könnte bereits durch eine Anregung der Erweiterung des Fragenkatalogs erreicht werden.
- 150** Je nach Risikohöhe kann ein „Monitoring“ auch über das Ausfüllen von Selbst-Zertifizierungen für Mitarbeiter, Führungskräfte und/oder Geschäftsführer erfolgen. Auch Dokumentations- und Berichterstattungspflichten, z. B. über bestimmte Arten von Wettbewerberkontakten (z. B. Benchmark-Aktivitäten außerhalb von Verbänden), können hilfreich sein. Eine (stichprobenartige) Durchsicht von Agenden/Protokollen von Verbandssitzungen und sonstigen Treffen mit Wettbewerbern/Kunden/Lieferanten ist ebenfalls eine mögliche Maßnahme.²⁰⁷
- 151** Schließlich kommt in Betracht, interne nicht anlassbezogene Audits mit detaillierten Fragekatalogen durchzuführen – mit einem Fokus auf bestimmte Abteilungen/Gesellschaften, ggf. in bestimmten Ländern/Regionen und unter Berücksichtigung des Risikoprofils im Unternehmen. Eine Kurz-Checkliste, die im Fall einer internen Untersuchung als Orientierungshilfe dient, und die z. B. in Abstimmung zwischen Compliance-/Rechtsabteilung, Personal- und Revisionsabteilung erarbeitet werden kann, kann hier gute Dienste leisten.²⁰⁸
- 152** An Bedeutung gewonnen haben außerdem unternehmensinterne Hinweisgebersysteme, die immer wieder hilfreiche Meldungen zu möglichen Kartellrechtsverstößen liefern.²⁰⁹ Durch das im Jahr 2023 verabschiedete Hinweisgeberschutzgesetz (HinSchG)²¹⁰ sind Unternehmen nunmehr sogar verpflichtet, interne Meldestellen einzurichten.²¹¹ Daneben liegt es auch im eigenen Interesse der Unternehmen, durch niedrigschwellige Meldesysteme mögliche Kartell-

205 Vgl. → *Hastenrath*, Kap. 6.

206 Zum erforderlichen „Schnittstellenmanagement“ der Compliance-Funktion mit anderen Unternehmensfunktionen → *Rau*, Kap. 3.

207 Zu Verbandsregister und -analyse siehe *Hess*, in: *Rübenstahl u. a.*, *Kartell Compliance*, 25. Kap., Rn. 47 ff.

208 Siehe hierzu auch die Literatur zum letztlich nicht in Kraft getretenen Verbandssanktionsgesetz. Praxisnahe Übersicht bei *Teicke*, CCZ 2019, 298 ff.

209 Zu aktuellen Entwicklungen und Anforderungen bei Hinweisgebersystemen → *Block/Sonnenberg*, Kap. 5.

210 BGBl. 2023 I Nr. 140 vom 2.6.2023.

211 § 12 Abs. 1 HinSchG. Zu den maßgeblichen Vorgaben im Einzelnen *Steinhauser/Saalwächter-Hirsch/Trouvain*, ESG 2023, 9 sowie → *Block/Sonnenberg*, Kap. 5.

rechtsverstöße eigenständig ermitteln zu können, um Verstöße abstellen und möglicherweise von der Kronzeugenregelung profitieren zu können, bevor interne Hinweisgeber sich veranlasst sehen, unmittelbar externe Meldestellen (z. B. das Bundeskartellamt) zu informieren. Auch die Förderung einer allgemeinen „Speak-up Culture“ im Unternehmen wirkt sich hier positiv aus.²¹²

III. Behördliche Untersuchungen

Kartellbehördliche Durchsuchungen (sog. „Dawn Raids“) werden in Deutschland entweder vom Bundeskartellamt oder der Europäischen Kommission („Kommission“) durchgeführt. Ob die Kommission oder das Bundeskartellamt wegen des Verdachts kartellrechtswidrigen Verhaltens einschreitet, hängt in erster Linie davon ab, ob es sich um einen rein nationalen oder grenzüberschreitenden Sachverhalt handelt. 153

Das Bundeskartellamt ist als nationale Behörde sowohl für die Durchsetzung der deutschen als auch der europäischen kartellrechtlichen Rechtsvorschriften (insbesondere §§ 1, 2, 18 ff. GWB und Artikel 101, 102 AEUV) zuständig. Folglich können Unternehmen in Deutschland bei Verdacht kartellrechtswidriger Absprachen immer vom Bundeskartellamt durchsucht werden. Bei Auswirkungen in anderen Mitgliedstaaten obliegt die Verfolgung den jeweiligen nationalen Kartellbehörden. Innerhalb der Europäischen Union arbeiten diese dabei intensiv im Rahmen des sog. „European Competition Network“ (ECN) zusammen. 154

Neben dem parallelen Einschreiten mehrerer nationaler Behörden besteht auch die Möglichkeit, dass die Kommission als zentrale Behörde wegen des Verdachts von Verstößen mit grenzüberschreitendem Bezug ermittelt. Ein grenzüberschreitender Bezug ist in vielen Fällen gegeben, sodass aus Unternehmenssicht grundsätzlich nicht absehbar ist, ob die nationale Behörde oder die Kommission vor der Tür stehen wird. Wenn die Kommission einschreitet, sind die betroffenen Verhaltensweisen von einer Verfolgung durch die nationalen Behörden ausgenommen. Auch wenn in diesen Fällen die Kommissionsbeamten oftmals von Beamten der nationalen Behörden unterstützt werden, bleibt es bei einem Verfahren nach europäischem Recht. 155

Unabhängig davon, welche Behörde ermittelt, ist es für die betroffenen Unternehmen von entscheidender Bedeutung, sich während einer Durchsuchung richtig zu verhalten bzw. bereits im Vorfeld Maßnahmen für den Fall einer Durchsuchung zu treffen.²¹³ Denn eine unzureichende Kooperation bzw. „Pannen“ während der Durchsuchung können zusätzliche Bußgelder bis zu 1 % des Kon- 156

212 Zur Compliance-Kultur als Erfolgsfaktor für das Compliance Management → *Schulz*, Kap. 1 Rn. 57 ff.

213 Zur unternehmensinternen Aufklärung von Fehlverhalten durch Mitarbeiter im oder aus dem Unternehmen heraus durch Interne Untersuchungen ausführlich → *Wettner/Walter*, Kap. 8.

zernumsatzes nach sich ziehen.²¹⁴ Alternativ wird ein solcher Umstand bei der Bußgeldbemessung erschwerend berücksichtigt.²¹⁵

1. Durchsuchungen der EU-Kommission

a) Zuständigkeit

- 157** Die Kommission ist aufgrund der Kartellverfahrensverordnung zu Durchsuchungen von Unternehmen (Nachprüfungen oder „Dawn Raids“) ermächtigt.²¹⁶ Die Beamten handeln in der Regel aufgrund einer sog. „Nachprüfungsentscheidung“. Diese muss hinreichend bestimmt sein und insbesondere den Gegenstand und Zweck der Nachprüfung bezeichnen.²¹⁷ Das Unternehmen muss aus der Entscheidung eindeutig entnehmen können, worauf sich der Verdacht der Kommission richtet. Erforderlich ist eine Nachprüfung nur, wenn es Anhaltspunkte für einen konkreten Kartellverstoß gibt.²¹⁸ Die Verdachtsmomente müssen mit dem Gegenstand der Durchsuchungsentscheidung übereinstimmen.²¹⁹ Dadurch sollen berechnete Nachprüfungen von unzulässigen sog. „Fishing Expeditions“ abgegrenzt werden.
- 158** Nach abschließender europäischer Rechtsprechung ist eine vorherige richterliche Anordnung zur Durchsuchung der Geschäftsräume von Unternehmen nicht erforderlich.²²⁰ Nach Ansicht der europäischen Gerichte wird effektiver Rechtsschutz in ausreichendem Maße dadurch gewährleistet, dass die Nachprüfungsentscheidung nachträglich vor dem EuG angefochten werden kann.²²¹ Soll sich die Durchsuchung allerdings auch auf private Räumlichkeiten erstrecken, darf

214 Art. 23 Abs. 1 VO 1/2003 und § 81c Abs. 2 i.V.m. § 81 Abs. 2 GWB. Zu Behinderungen von Durchsuchungen siehe z. B. KOM, 28.3.2012 – COMP/39.793 – EPH und andere (Umleiten von E-Mails), bestätigt durch EuG, 26.11.2014 – Rs. T-272/12, ECLI:EU:T:2014:995; EuGH, 22.11.2012 – Rs. C-89/11, ECLI:EU:C:2012:738 – E.ON Energie AG/Kommission (Siegelbruch).

215 Vgl. Europäische Kommission, 13.9.2006 – COMP/F/38.456 – Bitumen Niederlande (Erhöhung des Bußgeldes um 10 % wegen Verweigerung des Zutritts zu Räumlichkeiten und bestimmten Büros), bestätigt durch EuG, 27.9.2012 – Rs. T-357/06, ECLI:EU:T:2012:488, Rn. 252 ff. – Koninklijke Wegenbouw Stevin BV (KWS)/Kommission.

216 Art. 20, 21 der Verordnung (EG) Nr. 1/2003 des Rates vom 16.12.2002 zur Durchführung der in den Artikeln 81 und 82 des Vertrages niedergelegten Wettbewerbsregeln, ABl. L 1/1 vom 4.1.2003.

217 Art. 20 Abs. 3 f. VO 1/2003.

218 Ähnlich dem „Anfangsverdacht“ im deutschen Strafrecht.

219 EuGH, 18.6.2015 – Rs. C-583/13 P, ECLI:EU:C:2015:404 – Deutsche Bahn AG u. a./Kommission.

220 EuGH, 18.6.2015 – Rs. C-583/13 P, ECLI:EU:C:2015:404 – Deutsche Bahn AG u. a./Kommission.

221 EuG, 6.9.2013 – Rs. T-289/11, ECLI:EU:T:2013:404, Rn. 111 – Deutsche Bahn AG u. a./Kommission; EuGH, 18.6.2015 – Rs. C-583/13 P, ECLI:EU:C:2015:404, Rn. 26 – Deutsche Bahn AG u. a./Kommission.

die Nachprüfungsentscheidung nur mit der vorherigen Genehmigung des nationalen Gerichts vollzogen werden.²²²

b) Befugnisse

Die Beamten dürfen das Betriebsgelände, sämtliche Geschäftsräume und Transportmittel betreten und durchsuchen sowie die Inhalte von Schränken, Schreibtischen oder anderen Aufbewahrungsgegenständen (z.B. Aktentaschen etc.) überprüfen. Bei Vorliegen einer entsprechenden Berechtigung sind auch Privatgrundstücke und Wohnungen von Mitarbeitern und Führungskräften erfasst. Die Beamten sind berechtigt, Bücher und sonstige Geschäftsunterlagen – unabhängig in welcher Form sie vorliegen – einzusehen und zu kopieren. Zu den Geschäftsunterlagen gehören damit auch elektronische Dokumente (siehe dazu im Einzelnen → Rn. 162 ff.). Da eine Durchsuchung mehrere Tage andauern kann, dürfen die Beamten Räume oder Gegenstände (z.B. Unterlagen oder Laptops) versiegeln, wenn dies für die Nachprüfung erforderlich ist.²²³

159

Das Unternehmen trifft bei einer Nachprüfung durch die Kommission eine Mitwirkungspflicht. Die Mitarbeiter müssen Zugang zu Räumlichkeiten und Dokumenten verschaffen und bestimmte Informationen erteilen.²²⁴ Die Befugnisse der Beamten sind jedoch nicht unbegrenzt. Nicht erfasst sind Dokumente, die außerhalb des Untersuchungsgegenstands liegen sowie rechtlich privilegierte Dokumente. Nach europäischem Recht ist jedwede Kommunikation zwischen dem Unternehmen und externen Rechtsanwälten innerhalb des EWR, die sich auf den Gegenstand der Nachprüfung bezieht, privilegiert und darf somit nicht eingesehen werden.²²⁵ Interne Dokumente, die die Kommunikation mit dem Unternehmensjuristen betreffen, sind grundsätzlich nicht geschützt. Eine Ausnahme gilt jedoch für den Fall, dass „Inhouse-Juristen“ lediglich den Inhalt eines rechtlich privilegierten Dokumentes wiedergeben. Zudem können Dokumente geschützt sein, die vor Einschaltung von externen Rechtsanwälten alleine im Hinblick auf den einzuholenden Rechtsrat zur Verteidigung der Unternehmensrechte erstellt wurden.²²⁶

160

Die Beamten haben das Recht, Ad-hoc-Fragen zu jeglichen Dokumenten und Fakten im Rahmen der Nachprüfung zu stellen.²²⁷ Ein Auskunftsverweigerungsrecht in Bezug auf die für das Verfahren relevanten Tatsachen hat der Europäische Gerichtshof nicht anerkannt.²²⁸ Die Mitwirkungspflicht findet ihre Grenze

161

²²² Art. 21 Abs. 3 VO 1/2003.

²²³ Art. 20 Abs. 2 lit. d VO 1/2003. Nach Erwägungsgrund 25 zur VO 1/2003 soll die Versiegelung in der Regel 72 Stunden nicht überschreiten. Der Bruch des Siegels kann mit einem Bußgeld geahndet werden.

²²⁴ EuGH, 18.10.1989 – Rs. C-374/87, ECLI:EU:C:1989:387, Rn. 22 – Orkem.

²²⁵ EuGH, 18.5.1982 – Rs. C-155/79, ECLI:EU:C:1982:157 – AM&S/Kommission.

²²⁶ Siehe zum Anwaltsprivileg auch *Schnichels/Resch*, EuZW 2011, 47.

²²⁷ Art. 20 Abs. 2e VO 1/2003.

²²⁸ EuGH, 18.10.1989 – Rs. C-374/87, ECLI:EU:C:1989:387, Rn. 37 f. – Orkem.

in dem Verbot der Selbstbeichtigung, d. h. – über die Aufklärung von Tatsachen hinaus – in dem Eingeständnis, dass eine Zuwiderhandlung begangen wurde. Die Beamten können z. B. Auskünfte über Termine und Teilnehmer an Sitzungen verlangen, nicht dagegen die Angabe, ob das Ziel solcher Treffen die Festsetzung von Preisen gewesen ist.²²⁹

c) Elektronische Durchsuchung

- 162** Mit Zunahme des elektronischen Geschäftsverkehrs haben sich die Durchsuchungen der Kartellbehörden bereits seit geraumer Zeit zu sog. „E-Raids“ entwickelt. Der Schwerpunkt der Ermittlungen liegt heutzutage eindeutig auf dem elektronischen Datenbestand der Unternehmen. Zum Teil werden elektronische Daten wie E-Mail-Postfächer ausdrücklich in der Nachprüfungsentscheidung benannt. Die Kommission hat ihren Leitfaden für die Durchführung von Nachprüfungen zuletzt im März 2024 überarbeitet, der sich vorrangig mit der Durchsuchung der IT-Systeme befasst.²³⁰ Sie hat zudem ihre digitalen Ermittlungsinstrumente weiter ausgebaut und verfügt über ein spezielles Referat „Datenanalyse und Technologie“, das u. a. mit ermittlungstechnischen Analysen und forensischer IT-Unterstützung betraut ist und aus Experten zur Erfassung, Analyse und Auswertung digitaler Spuren besteht.²³¹ Mithilfe ihrer forensischen IT-Tools kann die Kommission Daten kopieren, durchsuchen und wiederherstellen und dabei die Integrität der Systeme und Daten der Unternehmen wahren.²³² Seit 2012 nutzt die Kommission bei ihren Ermittlungen spezielle Software des IT-Unternehmens NUIX.
- 163** Die Kommission führt in ihren Erläuterungen aus, dass grundsätzlich alle Arten von elektronischen Dokumenten oder Daten unabhängig vom Speichermedium von der Durchsuchung erfasst sind.²³³ Dies schließt lokale Geräte wie Desktop-PCs, mobile Endgeräte wie Laptops oder Tablets, Mobiltelefone, Smartphones, USB-Sticks oder externe Festplatten (auch ehemaliger Mitarbeiter) mit ein. Sie benennt nunmehr auch ausdrücklich Server und Cloud-Dienste sowie BYOD-Endgeräte, d. h. private Geräte, die auch zu geschäftlichen Zwecken genutzt werden. Zu den elektronischen Daten gehören insbesondere E-Mails, aber auch Of-

229 EuG, 8.3.1995 – Rs. T-34/93, ECLI:EU:T:1995:46, Rn. 75 – Société Générale; EuG, 20.2.2001, Rs. T-112/98, ECLI:EU:T:2001:61, Rn. 67 – Mannesmannröhren-Werke.

230 Explanatory Note on Commission inspections pursuant to Article 20(4) of the Council Regulation No 1/2003, 11.3.2024, https://competition-policy.ec.europa.eu/index/inspections_en (zuletzt abgerufen am 25.4.2024). Dieser Leitfaden wird den Unternehmen regelmäßig vor Beginn der Durchsuchung ausgehändigt.

231 Siehe im Einzelnen die Berichte der Kommission über die Wettbewerbspolitik 2022 (S. 13 f.) und 2023 (S. 49; jeweils in englischer Fassung und abrufbar unter https://competition-policy.ec.europa.eu/publications/annual-reports_en (zuletzt abgerufen am 25.4.2024) sowie Seeliger/Gänswein, BB 2014, 1027.

232 Explanatory Note on Commission inspections pursuant to Article 20(4) of the Council Regulation No 1/2003, 11.3.2024, Rn. 10.

233 Ebenda.

Office-Dokumente wie z.B. Textdateien, Tabellenkalkulationen und Präsentationen einschließlich Dokumente im PDF-Format. Bei der Durchsuchung des Datenbestands werden auch Metadaten, ältere Versionen von Dokumenten und gelöschte Objekte erfasst. Sie sind oftmals von besonderem Interesse, da anhand dieser Informationen interne Entscheidungsprozesse („Wer hat welche Zeile in die Excel-Tabelle eingefügt?“) nachvollzogen werden können.

Die Kommission hat kein Recht, die IT-Hardware oder Datenträger zu beschlagnehmen und mitzunehmen.²³⁴ Wie auch bei Dokumenten in Papierform muss sie entsprechende elektronische Kopien der für sie relevanten Daten (z. B. auf CD-ROMs, USB-Sticks oder externen Festplatten) anfertigen.

164

d) Typischer Ablauf

Durchsuchungen der Kommission starten in der Regel morgens zur üblichen Geschäftszeit der Unternehmen. Nach Vorlage der Ermächtigungsgrundlage verschaffen sich die Beamten und IT-Experten in einem ersten Schritt Zugang zum Gelände des zu durchsuchenden Unternehmens und zu den Büros der betroffenen Mitarbeiter sowie den Räumlichkeiten, in denen sich die IT-Infrastruktur befindet. Ein Anspruch auf die Anwesenheit externer Rechtsanwälte besteht nicht, auch wenn die Beamten sich gegebenenfalls für eine gewisse Zeit zum Warten bereit erklären. Dazu sind die Beamten grundsätzlich eher bereit, wenn kein Unternehmensjurist anwesend ist. Eine 47-minütige Wartezeit wurde jedoch bereits als Behinderung der Durchsuchung gewertet und mit einem gesonderten Bußgeld in Höhe von 1,71 Mio. EUR sanktioniert.²³⁵ Während die Beamten die physischen Dokumente durchsehen (z. B. Aktenordner, Notizbücher, Arbeitsplätze etc.), kümmern sich die IT-Spezialisten um die elektronischen Daten. Nach Erläuterungen zur IT-Infrastruktur lassen sie sich in der Regel Administratorenrechte einräumen und sperren (zumindest vorübergehend) den Zugang zu elektronischen Daten wie z.B. E-Mail-Konten. Aufgrund der Kooperationspflicht muss das Unternehmen nicht nur geeignete IT-Mitarbeiter zur Verfügung stellen, sondern auch Auskunft über Standorte von Servern geben und Passwortsperrern überwinden.²³⁶ Hält sich das Unternehmen nicht an die Vorgaben, droht ein Bußgeld. Auch aus diesem Grund empfiehlt es sich, die IT-Abteilung schon vorab in Schulungen zu Durchsuchungen einzubinden.

165

Zunächst fertigt die Kommission elektronische Kopien der als relevant angesehenen Datenträger bzw. Datensätze an (Imaging). In der Regel benutzt sie dafür eigene Speichermedien (Laptops). Sie lässt dann über die Kopie der Daten eine Suchsoftware laufen, die unter der Verwendung bestimmter Suchbegriffe be-

166

234 Sie sind lediglich nach Art. 20 Abs. 2 lit. c VO 1/2003 dazu ermächtigt, Kopien zu erstellen; siehe auch Explanatory Note on Commission inspections pursuant to Article 20(4) of the Council Regulation No 1/2003, 11.3.2024, Rn. 10.

235 Siehe EuG, 27.9.2012 – Rs. T-357/06, ECLI:EU:T:2012:488, Rn. 233 – KWS/Kommission.

236 Explanatory Note on Commission inspections pursuant to Article 20(4) of the Council Regulation No 1/2003, 11.3.2024, Rn. 11.

weisrelevante Daten herausfiltern soll (Indexierung). Dieser Vorgang kann mehrere Stunden, ggfs. auch die Nacht in Anspruch nehmen. Die Kommission gibt die Liste der Suchbegriffe nicht heraus. Sie ist der Ansicht, dass die Suchbegriffe nur Hilfsmittel zur Identifizierung beweisrelevanter Informationen sind. Typischerweise reduziert die Vorfilterung den relevanten Datenbestand auf einige tausend Dateien. Nach der Indexierung werden die Daten von den Beamten manuell durchgesehen. Die verwendeten Suchbegriffe können seitens des externen Rechtsanwalts bzw. des Unternehmensmitarbeiters, der der behördlichen Durchsuchungsperson zugewiesen ist (sog. „Shadowing“), notiert werden. Sie sind bei der Eingabe in die Suchmaske oder anhand der Markierung bestimmter Wörter in den relevanten Dokumenten zu erkennen. Auf diese Weise lassen sich die Verdachtsmomente der Kommission für das betroffene Unternehmen in diesem frühen Verfahrensstadium konkretisieren. Nicht-relevante bzw. privilegierte Daten werden aussortiert, der Rest wird markiert (Tagging/Flagging). Das Unternehmen erhält dann eine Liste der markierten Dokumente, um diese durchzugehen und auf Relevanz und Privilegierung zu prüfen.

- 167** Am Ende der Durchsuchung erstellt die Kommission eine forensische Kopie der von ihr erfassten Daten für das Unternehmen, zwei Kopiesätze nimmt sie mit. Zuvor wird die Authentizität der Daten gesichert und die Daten werden verschlüsselt. Sollte die Kommission Daten auf eigene Hardware kopiert haben, so werden diese Datenträger vor Ort gelöscht (Wiping).
- 168** In Ausnahmefällen kann es zu einer sogenannten „fortgesetzten Durchsuchung“ kommen, wenn potenziell beweis erhebliche Datenträger erst zu einem späten Zeitpunkt aufgefunden werden und eine Auswertung vor Ort zeitlich nicht mehr möglich erscheint oder es Streitigkeiten über die Relevanz eines Dokuments gibt. Die Dokumente werden in einem Umschlag verwahrt und können zu einem späteren Zeitpunkt entweder in Anwesenheit von Unternehmensvertretern in den Räumlichkeiten der Kommission oder des Unternehmens geprüft werden.²³⁷

2. Durchsuchungen des Bundeskartellamts

a) Zuständigkeit

- 169** Die Zuständigkeit des Bundeskartellamts richtet sich nach den allgemeinen strafprozessualen Vorschriften.²³⁸ Die Beamten handeln aufgrund eines richterlich angeordneten Durchsuchungsbeschlusses. Die richterliche Anordnung ist nach deutschem Recht aufgrund des grundrechtsbeschränkenden Zwangscharakters der Durchsuchung notwendig. Voraussetzung für den Durchsuchungsbeschluss ist, dass das Bundeskartellamt einen begründeten Tatverdacht schlüssig

²³⁷ Explanatory Note on Commission inspections pursuant to Article 20(4) of the Council Regulation No 1/2003, 11.3.2024, Rn. 16.

²³⁸ Insbesondere §§ 102, 103, 110 StPO, die über die Verweisungsnormen der §§ 82 Abs. 1 Nr. 3, 48 GWB i.V.m. §§ 36 Abs. 1 Nr. 1, 46 OWiG anwendbar sind.

darlegt. Lediglich bei Gefahr im Verzug darf das Bundeskartellamt eine Durchsuchung selbst anordnen.²³⁹

Aufgrund begrenzter interner Ermittlungskapazitäten insbesondere im IT-Bereich lassen sich die Beamten des Bundeskartellamts regelmäßig von Mitarbeitern des Landeskriminalamtes begleiten. 170

b) Befugnisse

Die Beamten des Bundeskartellamts haben ähnliche Befugnisse wie die Kommissionsbeamten. Die Ermittlungsbefugnisse des Bundeskartellamts wurden in den vergangenen Jahren, vor allem durch die 10. GWB-Novelle 2021 und die Neuregelung der Vorschrift zu Auskunftsverlangen (§ 59 GWB) und einer neuen Vorschrift für kartellrechtliche Durchsuchungen (§ 59b GWB) erheblich gestärkt.²⁴⁰ Die Erweiterungen der Ermittlungsbefugnisse des Bundeskartellamts dienen der Umsetzung einer europäischen Richtlinie, nämlich von Art. 6 ff. der „ECN+-Richtlinie“,²⁴¹ und sorgen für eine Angleichung der kartellbehördlichen Ermittlungsbefugnisse auf nationaler und europäischer Ebene. Im Gegensatz zum europäischen Recht waren Unternehmen lange nicht zur Kooperation mit dem Bundeskartellamt verpflichtet, sondern es bestand lediglich eine passive Duldungspflicht.²⁴² Diese Duldungspflicht gilt nach § 59b Abs. 5 Satz 2 GWB zwar weiterhin, wurde im Rahmen der 10. GWB-Novelle jedoch durch eine zumindest eingeschränkte aktive Mitwirkungspflicht ergänzt. Gemäß § 59 Abs. 1 GWB gilt daher nun eine umfassende Pflicht für Unternehmen und Unternehmensvereinigungen zur Erteilung all jener Auskünfte, die für die Erfüllung der Aufgaben des Bundeskartellamts erforderlich sind. Die Beamten haben nun das Recht, Informationen und Erläuterungen zu verlangen und zu Protokoll zu nehmen, die mit dem Gegenstand und dem Zweck der Durchsuchung in Verbindung stehen oder Zugang zu Beweismitteln ermöglichen könnten. Die neuen §§ 59, 59b GWB gelten sowohl im Verwaltungs- als auch im Bußgeldverfahren (vgl. § 82b Abs. 1 GWB). 171

Die Mitarbeiter sollten und müssen weiterhin nicht von sich aus Unterlagen anbieten oder ungefragt Auskünfte erteilen. Neu ist aber, dass Mitarbeiter bei Durchsuchungen des Bundeskartellamts ihre Mitwirkung umgekehrt nicht mehr 172

239 § 105 Abs. 1, Satz 1 Halbs. 2 StPO sowie § 59b Abs. 2, 4 GWB für eine Durchsuchung während der Geschäftszeit. Allerdings muss dies ausreichend begründet werden, z. B. mit der konkreten Gefahr eines Beweismittelverlustes und dem gescheiterten Versuch, den Ermittlungsrichter zu erreichen.

240 Überblicksartig dazu *Hartmann-Rüppel/Nagel*, CB 2022, 230.

241 Richtlinie (EU) 2019/1 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 zur Stärkung der Wettbewerbsbehörden der Mitgliedstaaten im Hinblick auf eine wirksamere Durchsetzung der Wettbewerbsvorschriften und zur Gewährleistung des reibungslosen Funktionierens des Binnenmarkts, ABl. L 11/3 vom 14.1.2019.

242 S. dazu noch *Klusmann*, in: Wiedemann, Handbuch des Kartellrechts, § 57 Rn. 24. Zur Kooperationspflicht nach europäischem Recht siehe z. B. EuGH, 21.9.1989 – verb. Rs. C-46/87 und 227/88, ECLI:EU:C:1989:337, Rn. 31 – Hoechst/Kommission.

generell verweigern können. Stattdessen können sie dazu verpflichtet sein, Auskunft zum Aufbewahrungsort bestimmter Dokumente und deren Inhalte geben zu müssen. Anders als bisher müssen sie sich dabei unter Umständen sogar selbst belasten, wenn und weil sich das Bundeskartellamt verpflichtet, kein Bußgeldverfahren gegen sie einzuleiten (sog. Nichtverfolgungszusage). Das Bundeskartellamt kann allerdings – anders als die Kommission – Maßnahmen zwangsweise durchsetzen und z. B. Firmenserver beschlagnahmen, was zu einer erheblichen Störung des Geschäftsbetriebs führen kann.²⁴³ Es ist also durchaus im Interesse des Unternehmens, soweit zu kooperieren, dass die Durchsuchung im Großen und Ganzen reibungslos ablaufen kann. In jedem Fall sollten die Ermittlungen nicht behindert oder erschwert werden, z. B. durch bewusst falsche Angaben oder das Verstecken/Vernichten von Beweismitteln, was strafscharfend berücksichtigt werden kann.

- 173** Die Beamten sind berechtigt, alle vom Durchsuchungsbeschluss umfassten Räumlichkeiten, Personen und Gegenstände zu untersuchen, Unterlagen einzusehen und Räume zu versiegeln. Über das Kopieren von Unterlagen hinaus dürfen sie – anders als die Kommission – Beweismittel vorläufig sicherstellen oder beschlagnahmen, wenn sie nicht freiwillig herausgegeben werden.²⁴⁴ In der Praxis legen die Beamten eher selten gleichzeitig mit dem Durchsuchungsbeschluss eine Beschlagnahmeanordnung vor. Eine erforderliche genaue Auflistung der zu beschlagnahmenden Gegenstände ist vor der Durchsuchung meist nicht möglich. Bei Gefahr im Verzug kann das Bundeskartellamt die Beschlagnahme aber selbst anordnen. In der Regel werden schriftliche Unterlagen von der Behörde beschlagnahmt, IT-Asservate dagegen vorläufig sichergestellt (siehe dazu im Einzelnen → Rn. 176 f.).
- 174** Die Beamten dürfen ebenso sogenannte Zufallsfunde mitnehmen.²⁴⁵ Dabei handelt es sich um Unterlagen, auf die das Bundeskartellamt während der Durchsuchung stößt, die aber nicht vom Durchsuchungsgegenstand erfasst sind und möglicherweise auf eine andere Ordnungswidrigkeit oder Straftat hindeuten. Eine systematische Suche nach solchen Unterlagen ist jedoch unzulässig. Eine rechtliche Privilegierung von Anwalts-Mandanten-Korrespondenz dürften die Unternehmen im Rahmen einer Durchsuchung des Bundeskartellamtes grundsätzlich nicht geltend machen können. Zwar gibt es im deutschen Recht bestimmte Beschlagnahmeverbote, deren enge Voraussetzungen liegen jedoch in der Regel bei Durchsuchungen des Bundeskartellamtes nicht vor. Der deutsche

243 Zur Verhältnismäßigkeit der Beschlagnahme siehe z. B. *Klusmann*, in: Wiedemann, Handbuch des Kartellrechts, § 57 Rn. 26 f.

244 Unter einer freiwilligen Herausgabe versteht man den Verzicht des Unternehmens auf eine Beschlagnahmeanordnung (z. B. wegen Gefahr im Verzug). Dies sollte gut überlegt werden, da das Unternehmen so verschiedene (nachträgliche) Rechtsschutzmöglichkeiten aufgibt.

245 § 108 Abs. 1 Satz 1 StPO.

Gesetzgeber hat es jedenfalls – trotz Art. 3 Abs. 1 der ECN+-Richtlinie – versäumt, das europäische Legal Professional Privilege zu kodifizieren.²⁴⁶

Die Beamten haben das Recht, Mitarbeiter und Betroffene während der Durchsuchung zu befragen. Fragen zur Person müssen grundsätzlich beantwortet werden. Mögliche Betroffene des Ermittlungsverfahrens haben unter Umständen das Recht, auf Fragen kartellbehördlicher Durchsuchungspersonen zur Sache zu schweigen. Die sogenannte Selbstbelastungsfreiheit wurde durch die letzte Gesetzesänderung jedoch eingeschränkt (siehe dazu → Rn. 171). Über das Aussageverweigerungsrecht sind sie vom Bundeskartellamt zu belehren. Nicht betroffene Mitarbeiter (z. B. das IT-Personal) können als Zeugen befragt werden. Zu beachten ist, dass falsche, unvollständige, verspätete oder unzulässig verweigernde Antworten als Verfahrensverstöße empfindliche Bußgelder nach sich ziehen können. Insofern kann es für Unternehmen sinnvoll sein, den Befragten frühzeitig externe Verteidiger zur Seite zu stellen. 175

c) Elektronische Durchsuchung

Auch das Bundeskartellamt konzentriert sich bei seinen Ermittlungen auf den elektronischen Datenbestand des Unternehmens. In der Praxis treffen die Beamten jedoch während der Durchsuchung im Unternehmen allenfalls eine grobe Vorauswahl der relevanten Daten, z. B. nach Geschäftsbereichen und betroffenen Mitarbeitern. Eine detaillierte Sichtung der Daten findet in der Regel vor Ort nicht statt. 176

Die Beamten sind grundsätzlich berechtigt, die IT-Hardware (Computer/Server) vorläufig mitzunehmen und sicherzustellen.²⁴⁷ Aus Gründen der Verhältnismäßigkeit fertigen sie jedoch häufig mit Zustimmung des Unternehmens und mithilfe forensischer Software elektronische Kopien an, entweder in Form einer Spiegelung des gesamten Datenbestands oder aber selektiv von bestimmten Datensätzen (z. B. E-Mail-Postfächern). Dafür verwenden sie in der Regel eigene Hardware, die sie an das IT-System des Unternehmens anschließen. 177

Mobile Endgeräte wie Smartphones oder Laptops werden meistens von den Beamten vorläufig sichergestellt. Nach Kopie der Daten im Bundeskartellamt erhalten die Betroffenen die Geräte zurück. Die detaillierte Sichtung des Datenbestands in der Behörde gilt noch als Teil der Durchsuchung.²⁴⁸ Sie kann durchaus mehrere Wochen oder Monate in Anspruch nehmen, eine zeitliche Begrenzung gibt es nicht. 178

246 Krit. dazu *Wirtz*, in: Immenga/Mestmäcker, § 59b GWB Rn. 35 („Umsetzungsdefizit“); für eine Anwendbarkeit ohne Anknüpfung an das deutsche Recht: *Klusmann*, in: Wiedemann, Handbuch des Kartellrechts, § 57 Rn. 35.

247 §§ 102, 103 StPO; *Vollmer*, WuW 2006, 235, 240.

248 Vgl. *Saller*, CCZ 2012, 189, 190.

d) Typischer Ablauf

- 179** Mit Ausnahme der detaillierten Durchsicht elektronischer Daten in der Behörde²⁴⁹ ähneln die wesentlichen Stationen einer Durchsuchung durch das Bundeskartellamt grundsätzlich dem Ablauf der Ermittlungen der Kommission. Nach Vorlage der Ermächtigungsgrundlage verteilen sich die Beamten auf die relevanten Räumlichkeiten zur Sichtung der Unterlagen und des Datenbestands. Sie befragen Mitarbeiter sowie das IT-Personal und durchsuchen Arbeitsplätze und Papiere. Die grob gesichtete IT-Hardware wird entweder vorläufig sichergestellt oder in Form von elektronischen Kopien auf Speichermedien des Bundeskartellamts zur weiteren Untersuchung mitgenommen. Am Ende der Durchsuchung vor Ort erstellen die Beamten ein sogenanntes Durchsuchungsprotokoll, in dem die wesentlichen Punkte festgehalten werden. Ebenso fertigen sie ein Asservatenverzeichnis über die sichergestellten oder beschlagnahmten Papierunterlagen und IT-Kopien an. Sowohl von dem Protokoll als auch von dem Verzeichnis sollte das Unternehmen eine Kopie verlangen. Bei der weiteren Sichtung des elektronischen Datenbestands in der Behörde geben die Beamten bestimmte Suchbegriffe und Stichworte ein, um die beweis erheblichen Daten zu identifizieren. Auch wenn den Unternehmen dabei kein Anwesenheitsrecht zusteht, ist davon auszugehen, dass das Bundeskartellamt dies im Einzelfall in der Praxis möglich machen wird. Nach Abschluss der Sichtung des Datenbestands erhält das Unternehmen eine Kopie der als relevant identifizierten Daten und eine Kopie der Liste der Suchbegriffe. Gleichzeitig wird das Unternehmen gefragt, ob es die Daten freiwillig herausgibt. Bei einer Weigerung muss das Bundeskartellamt die förmliche Beschlagnahme beim Amtsgericht beantragen. Dem Unternehmen bleiben dann etwaige Rechtsmittel gegen die Beschlagnahme von potenziell unerheblichen Daten erhalten.²⁵⁰

3. Verhaltensregeln für die Unternehmen

a) Vor der Durchsuchung

- 180** Angesichts der drohenden Bußgelder und des möglichen Imageschadens ist das Krisenmanagement der Unternehmen im Fall einer Durchsuchung von entscheidender Bedeutung. Dieses setzt bereits im Vorfeld und damit bei der Compliance-Arbeit an.
- 181** Unternehmen sollten Dawn-Raid-Schulungen für vorrangig betroffene Mitarbeiter durchführen (lassen) und – angepasst an die unterschiedlichen Entscheidungsträger im Unternehmen – über die wesentlichen Befugnisse der Behörden und die Abläufe informieren. Dies schließt sowohl Führungskräfte als auch das IT- und Empfangspersonal/Werkschutz mit ein. Schulungen können vor Ort oder

²⁴⁹ Diese gängige Praxis ausdrücklich ablehnend: LG Bonn, 30.3.2023 – 64 Qs 53/22, NZKart 2024, 50 – Ermittlungsverfahren Kabel I.

²⁵⁰ § 98 Abs. 2 Satz 2 StPO. Zum Verfahren des Bundeskartellamts insgesamt siehe *Saller*, CCZ 2012, 189; *Vollmer*, WuW 2006, 235.

auch im Wege des E-Learning vorgenommen werden. Sie sollten im Wege der Compliance-Arbeit, insbesondere nun nach dem Inkrafttreten der weitreichenden Änderungen durch die 10. GWB-Novelle regelmäßig überprüft und aufgefrischt werden (beispielsweise sind nun die Duldungs- durch Mitwirkungspflichten zu ersetzen). In jedem Fall empfiehlt sich die Aufstellung eines Notfall-Teams, das aus Vertretern der Führungsebene, der Rechts- bzw. Compliance-Abteilung, der IT, der Revisionsabteilung, der Finanz- und Steuerabteilung, des Empfangspersonals/Werkschutzes und der Abteilung Unternehmenskommunikation besteht. Jedem Vertreter sollten bestimmte Verantwortlichkeiten zugewiesen werden. Darüber hinaus sollten entsprechende Anweisungen, Leitlinien bzw. Dos and Don'ts vorab verteilt werden. Auch bei diesen Dokumenten ist auf die Aktualität der Unterlagen zu achten.

Es ist weiterhin sinnvoll, konkrete Telefonlisten und E-Mail-Verteiler zu erstellen (und diese mindestens jährlich zu aktualisieren), damit die zuständigen Personen im Falle einer Durchsuchung schnellstmöglich informiert werden können und auch in diesem Bereich keine Verzögerungen oder Pannen entstehen. Dies kann Kontakte externer Rechtsberater z. B. über eine von diesen angebotenen Dawn-Raid-Hotline mit einschließen. Ein entsprechender interner „Kommunikationsplan“ kann dabei helfen. Dieser kann bereits Muster für die interne Kommunikation im Unternehmen sowie für eine eventuell herauszugebende Presseerklärung enthalten. **182**

Aufgrund der Bedeutung der Durchsuchung elektronischer Daten ist es unerlässlich, die IT in den Notfallplan zu integrieren. Unternehmen sollten bereits im Vorfeld ihre IT-Landschaft „kartieren“ und festhalten, welche Datenträger es gibt (z. B. Server, Back-up Tapes, Laptops), wo sich diese befinden (im Unternehmen oder an einem anderen Standort) und wie der Zugriff erfolgt (wie Passwortsperrern überwunden werden etc.). Des Weiteren sollte geklärt sein, wie der E-Mail-Verkehr bestimmter Nutzerkonten bzw. insgesamt im Notfall blockiert werden kann. **183**

b) Während der Durchsuchung

Bei Ankunft der Beamten werden diese in der Regel nach der Geschäftsleitung fragen, um die Nachprüfungsentscheidung bzw. den Durchsuchungsbeschluss auszuhändigen. Es empfiehlt sich, die Beamten in einen vom laufenden Geschäftsbetrieb getrennten Raum zu bitten, um dort auf einen Vertreter der Unternehmensführung und eventuell auch auf das Eintreffen externer Rechtsanwälte zu warten.²⁵¹ Der „Kommunikationsplan“ des Unternehmens sollte unmittelbar umgesetzt werden, d. h. die entsprechenden Kontaktpersonen in der Unternehmensführung, der Rechtsabteilung, IT, Unternehmenskommunikation etc. müssen zügig informiert werden. Im nächsten Schritt sollte sich das Unternehmen **184**

²⁵¹ Sollten sie jedoch sofortigen Zutritt verlangen, muss dieser gewährt werden (siehe → Rn. 160).

die Dienstausweise der Beamten vorlegen lassen, die Namen notieren und äußerst sorgfältig die Ermächtigungsgrundlage prüfen. Sollten noch keine externen Rechtsanwälte vor Ort sein, empfiehlt es sich, diesen die Ermächtigungsgrundlage vorab zukommen zu lassen. Auch die Mitglieder des Notfall-Teams sollten eine Kopie oder Scan der Ermächtigungsgrundlage erhalten. Bei der Prüfung der Grundlage für die Durchsuchung ist insbesondere zu beachten, ob sich die Entscheidung an das fragliche Unternehmen richtet, die betroffenen Geschäftsräume genannt sind und ob Gegenstand und Zweck der Durchsuchung hinreichend bestimmt sind.

- 185** Sobald dies geklärt ist, sollte das Notfall-Team die Durchsuchung soweit wie möglich begleiten. Da die Beamten sich im Unternehmen aufteilen, sollte jedem Beamten eine unternehmenseigene Begleitperson oder ein externer Rechtsanwalt zugeordnet werden, die weitestgehend protokolliert, welche Büros, Computer, Dokumente etc. der jeweilige Beamte durchsucht und welche Mitarbeiter er befragt. Bei Unklarheiten sollten die Mitarbeiter entweder beim Mitglied der Rechtsabteilung oder den externen Rechtsanwälten Rat einholen. Ein IT-Mitarbeiter sollte als zentraler Ansprechpartner für IT-Fragen fungieren, vorzugsweise gemeinsam mit einem externen Rechtsanwalt oder einem Mitglied der Rechtsabteilung. Es empfiehlt sich, die entsprechenden Notfallnummern alsbald derart zu kommunizieren, dass die Mitarbeiter diese ohne Verzögerung auffinden (beispielsweise auf vorgefertigten Protokollmöglichkeiten). Zeitgleich sollten ggf. bestimmte Mitarbeiter des Unternehmens über die Durchsuchung informiert werden, damit eine Behinderung der Ermittlungen vermieden wird.
- 186** Grundsätzlich stellt sich bereits zu Beginn der Durchsuchung die Frage, ob das Unternehmen einen Kronzeugenantrag stellen soll und dafür einen sogenannten „Marker“ bei den Behörden setzt, um gegebenenfalls die Reduktion eines möglichen Bußgelds zu erhalten.²⁵² Die Beamten des Bundeskartellamtes händigen dem Unternehmen zu Beginn oder während der Durchsuchung ein Merkblatt zur sogenannten Bonusregelung aus. Das Stellen eines Kronzeugenantrags sollte gemeinsam mit den externen Rechtsberatern erörtert werden.
- 187** Dauert die Durchsuchung mehrere Tage an und werden Räume von den Beamten versiegelt, sollte das Unternehmen sicherstellen, dass die Siegel nicht gebrochen bzw. beschädigt werden. Die Siegel sind in der Regel nicht sehr groß, sodass eine zusätzliche Absicherung durch das Unternehmen sinnvoll sein kann. Sicherungsmaßnahmen sollten gemeinsam mit den Beamten protokolliert werden. Unter Umständen empfiehlt es sich, über Nacht die versiegelten Räume überwachen zu lassen. In jedem Fall sollte etwaiges Sicherheits- und Reinigungspersonal über die Versiegelung informiert werden, da ein (auch fahrlässiger) Siegelbruch in den Risikobereich des Unternehmens fällt und hohe Bußgelder nach

252 Der Marker kann schriftlich oder mündlich in deutscher oder englischer Sprache gesetzt werden.

sich ziehen kann, unabhängig davon, ob die Räumlichkeiten tatsächlich betreten oder Dokumente entwendet wurden.²⁵³

Am Ende der Durchsuchung sollte sichergestellt sein, dass das Unternehmen einen Überblick über die von den Beamten durchgesehenen, kopierten und sichergestellten bzw. beschlagnahmten Dokumente und Datenträger hat und alle Fragen und Antworten protokolliert sind. 188

c) Nach der Durchsuchung

Wenn die Beamten das Unternehmen verlassen haben, sollte eine Besprechung mit allen an der Durchsuchung beteiligten Mitarbeitern und den externen Rechtsanwälten abgehalten werden, um das weitere Vorgehen zu erörtern. Das Unternehmen sollte dafür sorgen, dass ein vollständiges internes Protokoll angefertigt wird, einschließlich aller Streitpunkte mit den Beamten. Falls nicht schon während der Durchsuchung erfolgt, sollte spätestens jetzt erörtert werden, ob das Unternehmen einen Kronzeugenantrag stellen will. 189

Darüber hinaus ist es ratsam zu prüfen, ob die zur Verfügung gestellten Dokumente und Erklärungen eine komplette und korrekte Antwort auf die aufgeworfenen Fragen geben oder weitere Details ergänzt oder Dokumente zur Verfügung gestellt werden sollten. Sofern das Unternehmen nicht von allen Dokumenten Kopien erhalten hat, kann es beim Bundeskartellamt Akteneinsicht in die eigenen Unterlagen beantragen. 190

Die Tatsache, dass eine Durchsuchung stattgefunden hat, bleibt selten geheim. In den meisten Fällen erscheinen Presseberichte bereits wenige Tage nach der Durchsuchung, oftmals geben die Kartellbehörden auch selbst Pressemitteilungen hinaus. Zusätzlich zu einer eigenen kurzen Pressemitteilung des Unternehmens kann es sinnvoll sein, sich auf Fragen von außenstehenden Personen vorzubereiten bzw. zusätzliche Mitteilungspflichten zu prüfen.²⁵⁴ Bei der genauen Formulierung sollten spezialisierte Anwälte hinzugezogen werden. 191

Die Hauptaufgabe nach der Durchsuchung ist die Aufarbeitung des Sachverhalts durch das Unternehmen und die Entwicklung einer entsprechenden Verteidigungsstrategie. Zusätzlich zu den Anhaltspunkten aus der Durchsuchung selbst und der Durchsicht der relevanten Unterlagen empfiehlt es sich, Interviews mit den betroffenen Mitarbeitern und der Geschäftsführung zu führen. Die lückenlose Aufklärung des Sachverhaltes erfordert grundsätzlich die vollständige Kooperation der Mitarbeiter. Eine Sanktionierung über arbeitsrechtliche Maßnahmen 192

253 Im Jahr 2008 verhängte die Kommission gegen E.ON ein Bußgeld in Höhe von 38 Mio. EUR wegen Siegelbruchs, siehe Pressemitteilung P/08/108, bestätigt durch EuGH, 22.11.2012 – Rs. C-89/11, ECLI:EU:C:2012:738 – E.ON Energie AG/Kommission; siehe ebenso Europäische Kommission vom 24.5.2011 – COMP/39.796, in der die Kommission Suez Environment ein Bußgeld wegen Siegelbruchs in Höhe von 8 Mio. EUR auferlegte.

254 Insbesondere börsennotierte Unternehmen unterliegen bestimmten Mitteilungspflichten (z. B. nach § 15 WpHG).

Teil 3 Besondere Aufgaben und Anwendungsfelder

ist insofern abzuwägen. Da nach deutschem Recht auch einzelnen Personen Bußgelder auferlegt werden können, ist es unter Umständen sinnvoll, einem betroffenen Mitarbeiter separaten Rechtsbeistand für das Kartellverfahren zur Seite zu stellen. Auch die Freistellung von einem Bußgeld oder von beruflichen Konsequenzen kann vereinbart werden, dies ist jedoch nicht unstrittig und im Einzelfall zu klären.

28. Kapitel

Compliance-Anforderungen im Wettbewerb um öffentliche Aufträge

I. Einleitung

Compliance ist auch im Zusammenhang mit der durch das Vergaberecht geregelten öffentlichen Auftragsvergabe zu beachten. Im Rahmen eines Vergabeverfahrens muss der Auftraggeber nicht nur die Wirtschaftlichkeit des Angebots, sondern auch die Eignung und Zuverlässigkeit der Unternehmen, die sich um Aufträge bewerben, prüfen. Verstöße gegen Recht und Gesetz oder sonstige Anforderungen können zum Ausschluss vom Verfahren oder zur Auftragsperre führen. Das hat mitunter existenzielle Folgen für Unternehmen, wenn deren Geschäft vornehmlich auf die Erbringung von Liefer-, Bau- oder Dienstleistungen für die öffentliche Hand oder sonstige öffentliche Auftraggeber ausgerichtet ist, wie beispielsweise in den Bereichen Straßen- und Ingenieurbau oder in der Verteidigungsindustrie. 1

Die rechtlichen Anforderungen ergeben sich für Aufträge, deren geschätzter Auftragswert oberhalb bestimmter Schwellenwerte liegt, aus dem GWB und den aufgrund dieses Gesetzes erlassenen Rechtsverordnungen. Zur Bestimmung der Schwellenwerte verweist § 106 Abs. 2 GWB auf die einschlägigen Ermächtigungen zur Anpassung der Werte durch die Europäische Kommission,¹ die alle zwei Jahre erfolgt. Das untergesetzliche Regelwerk umfasst insbesondere die Verordnung über die Vergabe öffentlicher Aufträge (VgV), die für Bauaufträge größtenteils auf Abschnitt 2 der VOB/A verweist. Teils von den Regelungen der VgV abweichende Bestimmungen enthalten die Sektorenverordnung (SektVO) für Sektorauftraggeber i. S. d. § 100 GWB,² die Vergabeverordnung Verteidigung und Sicherheit (VSVgV) für verteidigungs- und sicherheitsspezifische öffentliche Aufträge i. S. d. § 104 GWB und die Konzessionsvergabeverordnung (KonzVgV) für Konzessionen i. S. d. § 105 GWB.³ 2

Unterhalb dieser Schwellenwerte beurteilt sich die Vergabe von Aufträgen durch die öffentliche Hand nach Haushaltsrecht und dazu erlassenen Verwaltungsvorschriften. Auf Bundesebene schreibt § 55 BHO eine Öffentliche Ausschreibung 3

1 Ab 1.1.2024 gelten folgende Schwellenwerte (ohne USt): für Bauleistungen 5.538.000 EUR, für Lieferungen und sonstige Dienstleistungen 221.000 EUR, bei Bundesaufträgen 143.000 EUR. Abweichende Schwellenwerte gelten für soziale und bestimmte andere Dienstleistungen (§ 130 GWB) sowie für Sektoraufträge, den Verteidigungs- und Sicherheitsbereich sowie Konzessionen. Näher dazu: *Alexander*, in: Pünder/Schellenberg, Vergaberecht, § 106 GWB Rn. 11 ff.; *Greb*, in: Ziekow/Völlink, Vergaberecht, § 106 GWB Rn. 10 ff.

2 Bestimmte Auftraggeber aus einem der Bereiche für Sektorentätigkeiten (Wasser, Elektrizität, Gas und Wärme, Verkehr, Häfen und Flughäfen, fossile Brennstoffe).

3 Aus Vereinfachungsgründen wird nachfolgend allein auf die Regelungen für öffentliche Aufträge abgestellt, die keinem dieser Sonderbereiche unterliegen.

oder eine Beschränkte Ausschreibung mit Teilnahmewettbewerb für den Abschluss von Verträgen über Lieferungen und Leistungen vor, sofern nicht die Natur des Geschäfts oder besondere Umstände eine Ausnahme rechtfertigen. Die Voraussetzungen und das Verfahren werden durch die Verwaltungsvorschriften zu § 55 BHO konkretisiert. Diese verweisen insoweit für die Vergabe von Liefer- und Dienstleistungen auf die Verfahrensordnung für die Vergabe öffentlicher Liefer- und Dienstleistungsaufträge unterhalb der EU-Schwellenwerte (Unterschwellenvergabeordnung, UVgO) und für die Vergabe von Bauleistungen auf Abschnitt 1 der VOB/A. Auf Landes- und kommunaler Ebene gelten entsprechende Regelungen und die einschlägigen Vorgaben der Landes-Vergabegesetze.⁴

II. Anforderungen an Unternehmen in Vergabeverfahren

- 4 Gemäß § 122 Abs. 1 GWB werden öffentliche Aufträge nur an fachkundige und leistungsfähige Unternehmen vergeben, die nicht nach den §§ 123 und 124 GWB ausgeschlossen worden sind. Der öffentliche Auftraggeber ist daher gehalten, die Unternehmen, die sich um öffentliche Aufträge bewerben und ein Angebot zur Erbringung von Leistungen abgeben oder abgeben wollen, zu prüfen.
- 5 Gegenstand dieser Unternehmensprüfung ist einerseits die Eignung des Unternehmens für die Erbringung der vom öffentlichen Auftraggeber nachgefragten Leistung. Diese umfasst gemäß § 122 Abs. 2 GWB die Befähigung und Erlaubnis zur Berufsausübung, die wirtschaftliche und finanzielle Leistungsfähigkeit sowie die technische und berufliche Leistungsfähigkeit. Der Auftraggeber muss diese Eignungskriterien auftragsbezogen konkretisieren und die von den Bewerbern vorzulegenden Eignungsnachweise vorgeben.
- 6 Daneben umfasst die Unternehmensprüfung auch die Prüfung, ob Ausschlussgründe vorliegen. Über diese Anforderung wird eine Prüfung, ob ein potenzieller Auftragnehmer compliant ist, in das Vergabeverfahren integriert. Vor der Vergaberechtsnovelle 2016 war dies Teil der Eignungsprüfung unter dem Eignungskriterium der Zuverlässigkeit. Diese Systematik wurde zur Angleichung an die EU-Vergaberichtlinien aufgegeben, hat allerdings in den Regelungen über Bauaufträge im „Unterschwellenbereich“ noch überlebt.⁵
- 7 Die Unternehmensprüfung erfolgt im offenen Verfahren (vgl. § 15 VgV) mit der Prüfung des Angebots. Grundsätzlich ist die Unternehmensprüfung der eigentlichen Angebotsprüfung vorgelagert. Gemäß § 42 Abs. 3 VgV kann der öffentli-

4 Aus Vereinfachungsgründen wird nachfolgend allein auf die Regelungen abgestellt, die für Aufträge mit einem geschätzten Wert oberhalb der Schwellenwerte gelten, da die für den Unterschwellenbereich geltenden Vorschriften weitestgehend auf diese Regelungen verweisen oder vergleichbare Anforderungen enthalten, vgl. insb. § 31 UVgO und die Regelungen zur Zuverlässigkeit in Abschnitt 1 der VOB/A; näher dazu *Scherer*, in: Heuvels/HöB/Kuß/Wagner, Vergaberecht, § 31 UVgO Rn. 4 ff. und § 6a VOB/A Rn. 8 f.

5 Vgl. § 2 Abs. 3 und § 6a VOB/A; näher dazu *Scherer*, in: Heuvels/HöB/Kuß/Wagner, Vergaberecht, § 6a VOB/A Rn. 8.

che Auftraggeber die Angebotsprüfung vorziehen, was sich insbesondere anbietet, wenn eine große Anzahl von Angeboten eingereicht wurde und die Angebote einzelner Bieter schon aussortiert werden können, weil sie unwirtschaftlich sind und bereits deshalb für den Zuschlag sicher nicht in Betracht kommen. In den anderen Verfahrensarten, dem nicht offenen Verfahren (vgl. § 16 VgV), dem Verhandlungsverfahren (vgl. § 17 VgV), dem wettbewerblichen Dialog (vgl. § 18 VgV) und der Innovationspartnerschaft (vgl. § 19 VgV), erfolgt die Unternehmensprüfung in einem vorgelagerten Teilnahmewettbewerb. Hierzu lädt die Vergabestelle interessierte Unternehmen entweder durch eine öffentliche Bekanntmachung zur Beantragung der Teilnahme am Wettbewerb ein oder fordert die Unternehmen, die nach einem Interessenbekundungsverfahren ihr Interesse bekundet haben, auf, dieses Interesse zu bestätigen. Die Auftragsbekanntmachung bzw. die Aufforderung zur Interessenbestätigung muss gemäß § 48 Abs. 1 VgV die Nachweise angeben, die die Bewerber zum Nachweis des Nichtvorliegens von Ausschlussgründen vorlegen müssen.

In der Regel wird zum Nachweis die Vorlage einer Eigenerklärung verlangt. 8 Hierbei handelt es sich meist um ein Formular, das die verschiedenen Ausschlussgründe aufzählt und mit dem die Bewerber bestätigen, dass keiner dieser Ausschlussgründe vorliegt. Diese Eigenerklärung muss jeder Einzelbewerber, jedes Mitglied einer Bewerbungsgemeinschaft und jeder Dritte, der etwa als Unterauftragnehmer in die Angebotserstellung einbezogen ist, mit seiner Unterschrift oder elektronischen Signatur abgeben. Gemäß § 48 Abs. 3 VgV muss die Vergabestelle die Einheitliche Europäische Eigenerklärung nach § 50 VgV als zumindest vorläufigen Nachweis akzeptieren.⁶ Der Auftraggeber prüft die Unterlagen. Er kann die Bewerber zur Erläuterung der vorgelegten Unterlagen auffordern (§ 48 Abs. 7 VgV) und Unterlagen nachfordern (§ 56 Abs. 2 VgV).⁷ Gemäß § 122 Abs. 3 GWB kann der Nachweis über das Nichtvorliegen von Ausschlussgründen auch über eine Teilnahme an einem Präqualifizierungssystem erfolgen.⁸

Anhand der vorgelegten Informationen und Nachweise muss die Vergabestelle 9 prüfen, ob einer der Ausschlussgründe vorliegt. Ist das nicht der Fall, steht dieser Aspekt der weiteren Teilnahme des Unternehmens am Verfahren nicht mehr entgegen. Geht die Vergabestelle vom Vorliegen eines Ausschlussgrundes aus, muss sie zudem prüfen, ob (erstens) sich das Unternehmen nicht bereits gemäß § 125 GWB selbst gereinigt hat und (zweitens) dem Ausschluss auch nicht ein Fristablauf nach § 126 GWB entgegensteht. Die Vergabestelle darf im weiteren Verlauf des Vergabeverfahrens nur wieder in die Unternehmensprüfung einstei-

6 Zu weiteren Belegen, die von der Vergabestelle akzeptiert werden müssen, vgl. § 48 Abs. 4 bis 6 und 8 VgV.

7 Zu den Anforderungen und Grenzen der Nachforderung von Unterlagen vgl. Pauka/Krüger, in: MünchKomm-Wettbewerbsrecht, Bd. 3, § 56 VgV Rn. 23 ff.

8 Vgl. hierzu Opitz, in: Burgi/Dreher/Opitz, Beck'scher Vergaberechtskommentar, Bd. 1, § 122 GWB Rn. 107.

gen, wenn sich Umstände ergeben, die die Frage (der Eignung oder) des Nichtvorliegens von Ausschlussgründen neu aufwerfen.⁹

III. Ausschlussgründe

- 10** Das GWB unterscheidet zwingende und fakultative Ausschlussgründe. Die zwingenden Ausschlussgründe sind in § 123 GWB geregelt und der Auftraggeber ist verpflichtet, das Unternehmen auszuschließen, wenn ein solcher Grund vorliegt. Demgegenüber muss die Vergabestelle bei Vorliegen eines fakultativen Ausschlussgrundes ein Ermessen ausüben, bevor sie ein Unternehmen ausschließt.¹⁰ Dieses Ermessen ist allerdings durch die Vergaberechtsgrundsätze des § 97 GWB vorgeprägt. Insbesondere das Diskriminierungsverbot und der Wettbewerbsgrundsatz lenken das Ermessen i. d. R. dergestalt, dass ein Ausschluss geboten erscheint.¹¹

1. Zwingende Ausschlussgründe

a) Straftatbestände

- 11** § 123 Abs. 1 GWB zählt eine Reihe von Straftatbeständen auf. Diese beruhen auf einer Liste von Ausschlussstatbeständen der EU-Vergaberichtlinien,¹² die in deutsches Recht umgesetzt wurden, indem auf die jeweiligen Straftatbestände des StGB und des Gesetzes zur Bekämpfung internationaler Bestechung verwiesen wird. Diese Liste ist abschließend und enthält Straftatbestände wie
- Terrorismusfinanzierung;
 - Geldwäsche;
 - Betrug oder Subventionsbetrug gegen die EU;
 - Bestechlichkeit und Bestechung im geschäftlichen Verkehr;
 - Bestechlichkeit und Bestechung von Mandatsträgern;
 - Vorteilsgewährung und Bestechung;
 - Bestechung ausländischer Abgeordneter.
- 12** Der Ausschlussgrund liegt erst vor, wenn eine rechtskräftige strafgerichtliche Verurteilung vorliegt. Da nach deutschem Strafrecht nur natürliche Personen verurteilt werden können, stellt das Gesetz auf die Verurteilung einer Person ab, deren Verhalten dem Unternehmen zuzurechnen ist. Das ist gemäß § 123 Abs. 3 GWB der Fall, wenn eine Person den Straftatbestand verwirklicht hat, die als für die Leitung des Unternehmens verantwortliche Person gehandelt hat, also insbe-

9 OLG Düsseldorf, 15.12.2008 – I-27 U 1/07, LS 2, juris; *Hölzl*, in: MünchKomm-Wettbewerbsrecht, Bd. 3, § 122 GWB Rn. 33 f.

10 *Stolz*, in: Ziekow/Völlink, Vergaberecht, § 124 GWB Rn. 2.

11 *Opitz*, in: Burgi/Dreher/Opitz, Beck'scher Vergaberechtskommentar, Bd. 1, § 124 GWB Rn. 19.

12 Insbesondere Art. 57 Abs. 1, 2 und 3 Unterabs. 1 und Abs. 5 der RL 2014/24/EU des Europäischen Parlaments und des Rates v. 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der RL 2004/18/EG; vgl. *Kaufmann*, in: Pünder/Schellenberg, Vergaberecht, § 123 GWB Rn. 1.

sondere Mitglieder eines Vorstands oder der Geschäftsführung. Erfasst sind aber auch Personen, die für die Überwachung der Geschäftsführung verantwortlich sind oder in sonstiger Weise Kontrollbefugnisse in leitender Stellung ausüben, wie beispielsweise Mitglieder von Aufsichtsräten.¹³

Unter bestimmten Voraussetzungen kann bei Vorliegen eines strafrechtlichen Delikts auch eine Geldbuße gegen ein Unternehmen selbst verhängt werden. Die Voraussetzungen sind in § 30 OWiG geregelt und setzen insbesondere voraus, dass der Straftatbestand von einer leitenden Person verwirklicht wurde.¹⁴ Wird nach dieser Regelung eine Geldbuße gegen ein Unternehmen wegen einer der in § 123 Abs. 1 GWB genannten Straftaten rechtskräftig festgesetzt, muss dieses Unternehmen ebenfalls ausgeschlossen werden. Sollte es in Zukunft zur Verabschiedung eines Verbandssanktionengesetzes¹⁵ kommen, würde voraussichtlich die rechtskräftige Verhängung von Sanktionen nach diesem Gesetz wegen solcher Straftaten ebenfalls den Ausschluss nach sich ziehen; insoweit bleibt die weitere Rechtsentwicklung abzuwarten.¹⁶

Nach § 123 Abs. 5 Satz 1 GWB kann die Vergabestelle ausnahmsweise von einem Ausschluss absehen, wenn zwingende Gründe des öffentlichen Interesses dies gebieten. Eine solche Ausnahme kann angenommen werden, wenn der öffentliche Auftraggeber auf ein bestimmtes Produkt oder eine bestimmte Dienstleistung zur Erfüllung seiner öffentlichen Aufgaben dringend angewiesen ist und die Beschaffung nur bei einem Unternehmen möglich ist, das auszuschließen wäre, z. B. im Zusammenhang mit der Beschaffung von Ersatzteilen für ein Feuerwehrfahrzeug.

b) Steuer- und Abgabentatbestände

Nach § 123 Abs. 4 Satz 1 GWB ist ein Unternehmen auch auszuschließen, wenn es seinen Verpflichtungen zur Zahlung von Steuern, Abgaben oder Beiträgen zur Sozialversicherung nicht nachgekommen ist und dies durch eine rechtskräftige Gerichtsentscheidung festgestellt wurde, etwa einer Verurteilung wegen Steuerhinterziehung nach § 370 AO oder Vorenthalten von Beiträgen des Arbeitnehmers zur Sozialversicherung nach § 266a StGB. Daneben können auch Bußgeldbescheide wegen Steuerordnungswidrigkeiten, etwa wegen leichtfertiger Steuerverkürzung nach § 378 AO, oder Verwaltungsentscheidungen der zuständigen Behörden, in denen festgestellt wird, dass die Zahlung der Steuer, der Abgabe oder des Beitrags noch aussteht, den Ausschluss nach sich ziehen. Der zwingende Ausschlussgrund ist insoweit erst verwirklicht, wenn die Verwaltungsentscheidung bestandskräftig ist, sie also insbesondere nach Ablauf der

13 Näher hierzu *Scherer*, in: Heuvels/Höb/Kuß/Wagner, Vergaberecht, § 123 Rn. 9 ff.

14 *Rogall*, in: Karlsruher Kommentar zum OWiG, § 30 Rn. 1. Siehe auch → *Böttger*, Kap. 2 Rn. 31 ff. m. w. N.

15 Vgl. zu dem in der 19. Legislaturperiode gescheiterten Gesetzentwurf: *Schulz/Block*, CCZ 2020, 49.

16 → *Böttger*, Kap. 2 Rn. 143 ff.

Rechtsbehelfsfristen nicht mehr angefochten werden kann. Wurden Rechtsbehelfe gegen solche Verwaltungsentscheidungen eingelegt, ist der Ausschluss geboten, sobald diese rechtskräftig abgewiesen wurden.

- 16** Im Vergleich zu den Straftatbeständen des § 123 Abs. 1 GWB ist der Ausschluss wegen der Abgabentatbestände einerseits zusätzlich erleichtert. Nach § 123 Abs. 4 Satz 1 Nr. 2 GWB bedarf es für einen zwingenden Ausschluss keiner Gerichts- oder Verwaltungsentscheidung. Es genügt, wenn der Vergabestelle sonstige Nachweise vorliegen.
- 17** Andererseits kann das Unternehmen den Ausschluss gemäß § 123 Abs. 4 Satz 2 GWB recht einfach abwenden, indem es die Zahlung nachholt. Es genügt bereits, dass es sich verpflichtet, die Steuern, Abgaben und Beiträge zur Sozialversicherung einschließlich Zinsen, Säumnis- und Strafbzuschlägen zu zahlen. Auch die Ausnahme wegen dringender öffentlicher Interessen (siehe → Rn. 14) gilt in diesem Zusammenhang und wird durch § 123 Abs. 5 Satz 2 GWB zusätzlich auf die Fälle ausgedehnt, in denen ein Ausschluss unverhältnismäßig wäre.

2. Fakultative Ausschlussgründe

a) Verstoß gegen umwelt-, sozial- oder arbeitsrechtliche Verpflichtungen

- 18** Gemäß § 124 Abs. 1 Nr. 1 GWB können Unternehmen ausgeschlossen werden, die bei der Ausführung öffentlicher Aufträge nachweislich gegen geltende umwelt-, sozial- oder arbeitsrechtliche Verpflichtungen verstoßen haben. Unter den Begriff der umwelt-, sozial- oder arbeitsrechtlichen Verpflichtungen fallen sowohl europäische und internationale als auch deutsche Rechtsvorschriften¹⁷ sowie Tarifverträge und Übereinkommen.¹⁸ Auch die ILO-Kernarbeitsnormen oder Zahlungsverpflichtungen gegenüber tarifvertraglichen Sozialkassen werden von dem Ausschlussstatbestand erfasst. Der Ausschlussgrund wird dadurch eingeschränkt, dass die Rechtsverstöße bei der Ausführung öffentlicher Aufträge verwirklicht worden sein müssen. Wiegt der Verstoß schwer, kann zugleich ein Ausschlussgrund nach § 124 Abs. 1 Nr. 3 GWB vorliegen. Der Pflichtverstoß muss vom öffentlichen Auftraggeber nachgewiesen werden. Bloße Verdachtsmomente genügen nicht. Bestimmte sozial- und arbeitsrechtliche Verstöße sind in das Wettbewerbsregister beim Bundeskartellamt einzutragen (siehe dazu → Rn. 32),¹⁹ wenn eine rechtskräftige Bußgeldentscheidung mit einer bestimmten Mindesthöhe des Bußgelds oder eine strafgerichtliche Verurteilung mit einem bestimmten Mindeststrafmaß vorliegt (vgl. § 2 Abs. 1 Nr. 2 WRegG). Typische Verstöße gegen sozial- und arbeitsrechtliche Verpflichtungen sind Verstöße gegen die in § 124 Abs. 2 GWB genannten Gesetze: das AEntG, das AufenthG, das MiLoG und das SchwarzArbG. Seit 2021 bezieht § 124 Abs. 2 GWB auch das LkSG mit ein, das am 1.1.2023 in Kraft getreten ist und insbesondere

¹⁷ *Summa*, NZBau 2012, 729, 732.

¹⁸ Amtliche Begründung BT-Drs. 18/6281, S. 105.

¹⁹ Vgl. *Scherer-Leydecker*, CB 2017, 261, 262.

umwelt- und sozialrechtliche Verpflichtungen aufstellt.²⁰ Die in § 124 Abs. 2 GWB aufgeführten Gesetze enthalten eigene Regelungen zu Auftragssperren.²¹ Diese gelten neben den Ausschlussgründen nach § 124 Abs. 1 GWB aber nur, soweit sie nicht über einschlägiges EU-Recht hinausgehen.²²

b) Insolvenz und Liquidation

Gemäß § 124 Abs. 1 Nr. 2 GWB ist ein Ausschluss möglich, wenn über das Vermögen des Unternehmens das Insolvenzverfahren eröffnet ist oder ein Insolvenzantrag mangels Masse abgelehnt wurde. Dem gleichgestellt sind die Beantragung der Eröffnung des Insolvenzverfahrens und die Zahlungsunfähigkeit des Unternehmens. Hierdurch wird dem Umstand Rechnung getragen, dass es zum Zeitpunkt der Eröffnung eines Insolvenzverfahrens bereits zu spät sein kann und ein Zuwarten dem öffentlichen Auftraggeber nicht zumutbar ist. Ein Unternehmen gilt gemäß § 17 Abs. 2 InsO als zahlungsunfähig, wenn es nicht in der Lage ist, die fälligen Zahlungspflichten zu erfüllen, was i. d. R. anzunehmen ist, wenn es seine Zahlungen eingestellt hat. Eine Vergabestelle, die sich auf diese Tatbestandsalternative stützt, muss die materiellen Voraussetzungen der Zahlungsunfähigkeit darlegen und beweisen können. **19**

Von den Insolvenztatbeständen zu trennen ist der ebenfalls im Rahmen des § 124 Abs. 1 Nr. 2 GWB geregelte Ausschluss wegen einer Liquidation der Gesellschaft oder der Einstellung der Geschäftstätigkeit des Unternehmens. Mit der Liquidation wird eine juristische Person oder Personengesellschaft, die aufgelöst werden soll, abgewickelt. Im Rahmen der Liquidation werden die Verbindlichkeiten des Unternehmens beglichen und das verbleibende Vermögen verteilt, etwa gem. §§ 60 ff. GmbHG bei der GmbH. Hierzu wird ein Liquidator bestellt und die Liquidation (i.L.) im Handelsregister vermerkt. Der Liquidation als Ausschlussgrund gleichgestellt ist die Einstellung der Geschäftstätigkeit, die in der Sache von dem öffentlichen Auftraggeber festgestellt werden muss, wenn er sich auf diesen Ausschlussgrund berufen will. **20**

c) Schwere Verfehlung im Rahmen beruflicher Tätigkeit

Voraussetzung des Ausschlussgrundes nach § 124 Abs. 1 Nr. 3 GWB ist, dass nachweislich eine schwere Verfehlung vorliegt, die im Rahmen der beruflichen Tätigkeit begangen wurde. Verfehlung ist jeder Verstoß gegen einschlägiges Recht. Der Ausschlussgrund hat daher Überschneidungen mit den zwingenden Ausschlussgründen des § 123 GWB sowie dem Ausschlussgrund des § 124 Abs. 1 Nr. 1 GWB betreffend Verstöße gegen umwelt-, sozial- oder arbeitsrechtliche Verpflichtungen. Anders als nach § 123 GWB verlangt § 124 Abs. 1 Nr. 3 GWB keine rechtskräftige Verurteilung oder Verwaltungsentscheidung. Der **21**

20 Friton, in: BeckOK Vergaberecht, § 124 GWB Rn. 97. Zu diesem Gesetz siehe auch → Hesse, Kap. 18; Hagel/Wiedmann, Kap. 19.

21 Kaufmann, in: Pünder/Schellenberg, Vergaberecht, § 124 GWB Rn. 108 ff.

22 Friton, in: BeckOK Vergaberecht, § 124 GWB Rn. 98.

Nachweis kann daher wie bei § 123 Abs. 4 Satz 1 Nr. 2 GWB auch auf sonstige Weise erbracht werden. Der öffentliche Auftraggeber muss den Sachverhalt ermitteln und aufgrund der ihm vorliegenden Erkenntnisse und Belege zu der Überzeugung kommen, dass der Rechtsverstoß begangen wurde. Einen Ausschluss rechtfertigen nur Verfehlungen, die eine solche Schwere aufweisen, dass sie die Integrität des Unternehmens in Frage stellen, und die im Rahmen einer beruflichen Tätigkeit (nicht nur im privaten Bereich) begangen wurden. Die Pflichtverstöße werden dem Unternehmen gemäß § 124 Abs. 1 Nr. 3 Hs. 2 GWB i.V.m. § 123 Abs. 3 GWB nach den gleichen Maßstäben wie bei den zwingenden Ausschlussgründen zugerechnet (siehe → Rn. 12).

- 22 Etwaige Erkenntnisse können sich auch aus der Einsichtnahme in das Gewerbezentralregister oder im Hinblick auf Personen, die dem Unternehmen i.S.d. § 123 Abs. 3 GWB zurechenbar sind, aus dem Bundeszentralregister ergeben. Seit der Schaffung des Wettbewerbsregisters muss bzw. kann der öffentliche Auftraggeber nach § 6 Abs. 1, 2 WRegG auch die Eintragungen in diesem Register abrufen (siehe → Rn. 36f.).²³ Für einen Übergangszeitraum kann die Vergabestelle auf beide Register zurückgreifen, da ältere Verstöße im Gewerbezentralregister, aber noch nicht im Wettbewerbsregister dokumentiert sind. Zukünftig wird in Vergabeverfahren nur noch das speziell dafür geschaffene Wettbewerbsregister abgerufen.

d) Wettbewerbsbeschränkende Vereinbarungen oder abgestimmte Verhaltensweisen

- 23 Der Ausschlussgrund des § 124 Abs. 1 Nr. 4 GWB greift den Grundsatz des Verbots wettbewerbsbeschränkender Vereinbarungen und abgestimmter Verhaltensweisen nach § 1 GWB auf. Er umfasst nicht nur wettbewerbswidriges Verhalten im laufenden Verfahren, sondern liegt auch vor, wenn das Unternehmen unabhängig davon einen Verstoß begangen hat. Der Umstand allein, dass polizeiliche, kartellrechtliche oder staatsanwaltliche Ermittlungsmaßnahmen eingeleitet wurden, oder der bloße Verdacht gegen das Unternehmen reichen hingegen nicht aus. Andererseits muss (anders als bei § 124 Abs. 1 Nr. 1 und 3 GWB) kein Nachweis vorliegen. Es genügen hinreichende Anhaltspunkte. Dem wird im Rahmen der Eintragung von Bußgeldbescheiden nach § 81 Abs. 1 Nr. 1 oder Abs. 2 Nr. 1 GWB ins Wettbewerbsregister dadurch Rechnung getragen, dass diese gem. § 2 Abs. 2 WRegG bereits mit Festsetzung erfolgt und die Rechtskraft nicht erforderlich ist.²⁴
- 24 Der Begriff der wettbewerbsbeschränkenden Vereinbarung ist in § 124 Abs. 1 Nr. 4 GWB mit nahezu dem gleichen Wortlaut wie in § 1 GWB definiert. Der Vereinbarungs-begriff wird von der herrschenden Lehre weit ausgelegt.²⁵ Einsei-

²³ Vgl. dazu *Scherer-Leydecker*, CB 2017, 261, 263.

²⁴ Vgl. amtliche Begründung zum WRegG, BT-Drs. 18/12051, S. 27; vgl. auch → Rn. 33.

²⁵ *Zimmer*, in: *Immenga/Mestmäcker*, Wettbewerbsrecht, Bd. 2, § 1 GWB Rn. 36.

tige Maßnahmen sind dagegen grundsätzlich keine Vereinbarung. Eine abgestimmte Verhaltensweise beinhaltet ein koordinierendes Element, etwa die vorherige Information der Wettbewerber zur Risikominimierung, das von bloß reaktivem Verhalten abzugrenzen ist.²⁶ Die Vereinbarung oder abgestimmte Verhaltensweise wird wettbewerbsbeschränkend, indem sie die Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs bezweckt oder bewirkt.

e) Interessenkonflikt

Nach § 124 Abs. 1 Nr. 5 GWB können Interessenkonflikte einer bei der Durchführung des Vergabeverfahrens für die Vergabestelle oder einen sie unterstützenden Beschaffungsdienstleister tätigen Person einen Ausschluss rechtfertigen. Das Vorliegen eines Interessenkonflikts setzt voraus, dass die Person (auch) andere Interessen als die Interessen des öffentlichen Auftraggebers wahrnimmt und dies geeignet ist, die Unparteilichkeit und Unabhängigkeit dieser Person im Zusammenhang mit der Durchführung des Vergabeverfahrens zu beeinträchtigen. Nicht erforderlich ist, dass die Person sich bereits parteilich oder abhängig verhalten hat. Es genügt, wenn die Situation das Potenzial birgt, dass diese Person in einer Weise handelt, die den diskriminierungsfreien Wettbewerb gefährdet. Nach § 6 Abs. 1 VgV muss die Vergabestelle allerdings zuvor geeignete Maßnahmen zur wirksamen Verhinderung, Aufdeckung und Behebung von Interessenkonflikten treffen, um Wettbewerbsverzerrungen zu vermeiden und eine Gleichbehandlung aller Bieter zu gewährleisten. Ein Ausschluss kommt daher nur in Betracht, wenn dies nicht möglich ist. **25**

f) Vorbefassung

Der in § 124 Abs. 1 Nr. 6 GWB geregelte fakultative Ausschlussgrund der Vorbefassung betrifft die sog. „Projektantenproblematik“. Nach dieser Vorschrift kann ein Unternehmen, das bei der Vorbereitung des laufenden Verfahrens mit eingebunden war und dadurch einen Wettbewerbsvorteil erlangt haben könnte, ausgeschlossen werden. Bevor der öffentliche Auftraggeber einen Ausschluss in Betracht zieht, hat er weniger einschneidende Maßnahmen zur Vermeidung einer Wettbewerbsverzerrung zu ergreifen. Angesichts der mit der Vorbefassung verbundenen Gefährdung des diskriminierungsfreien Wettbewerbs hat der Auftraggeber nach § 7 Abs. 1 VgV insbesondere sicherzustellen, dass ein Informationsvorsprung des vorbereiteten Unternehmens ausgeglichen wird und bei der Ausgestaltung der Leistungsbeschreibung und Eignungskriterien darauf geachtet wird, dass der Wettbewerb auch anderen Bietern offensteht. Gemäß § 7 Abs. 2 VgV sind die anderen Bewerber oder Bieter über die dem vorbereiteten Unternehmen zur Verfügung gestellten Informationen zu unterrichten und ihnen angemessene Fristen zur Verarbeitung der Informationen einzuräumen.²⁷ Das vorbereitete Unternehmen darf nur dann von der Vergabe ausgeschlossen wer- **26**

²⁶ Zimmer, in: Immenga/Mestmäcker, Wettbewerbsrecht, Bd. 2, § 1 GWB Rn. 41 f.

²⁷ Tomerius, in: Pünder/Schellenberg, Vergaberecht, § 7 VgV Rn. 5.

den, wenn eine geeignete Maßnahme zur Verhinderung der Wettbewerbsverfälschung nicht ersichtlich ist.²⁸ Vor einem Ausschluss muss dem Bieter nach § 7 Abs. 3 VgV in jedem Fall die Möglichkeit eingeräumt werden, sich zu äußern und gegebenenfalls nachzuweisen, dass aus seiner Vorbefassung mit dem laufenden Vergabeverfahren keine Verzerrung des Wettbewerbs resultieren würde.²⁹

g) Mangelhafte Leistung bei Ausführung früherer Aufträge

- 27 Der Ausschluss nach § 124 Abs. 1 Nr. 7 GWB betrifft Fälle, in denen bei der Ausführung eines öffentlichen Auftrages oder einer Konzession in der Vergangenheit Mängel aufgetreten sind. Wegen der Schwere der Folge für das Unternehmen müssen die Mängel bei der vorherigen Vertragsausführung erheblich sein. Das Unternehmen muss wesentliche Anforderungen des öffentlichen Auftrages oder der Konzession erheblich oder fortlaufend mangelhaft erfüllt haben.³⁰ Auch sonstige Vertragsverletzungen können einen erheblichen Mangel darstellen, wie zum Beispiel ein Verstoß gegen die Verpflichtung zur Vertraulichkeit oder gegen wesentliche Sicherheitsauflagen. Darüber hinaus muss die mangelhafte Erfüllung oder Vertragsausführung kumulativ zu einer vorzeitigen Beendigung, Schadensersatz oder einer vergleichbaren Rechtsfolge geführt haben. Eine vorzeitige Beendigung kann durch Kündigung, Rücktritt, Anfechtung oder einvernehmliche Vertragsaufhebung erfolgen, muss aber auf der Mangelhaftigkeit der Leistung beruhen. Allein die Kündigungs- oder Rücktrittserklärung durch den Auftraggeber genügt nicht, wenn sie unberechtigt ist und den Vertrag nicht wirksam beendet hat.³¹ Dabei muss es sich nicht um einen vorherigen Auftrag desselben öffentlichen Auftraggebers handeln. Eine Schlechtleistung mit einer der vorgenannten Folgen bei der Ausführung des Auftrages eines anderen öffentlichen Auftraggebers ist ausreichend. Bevor das betroffene Unternehmen ausgeschlossen wird, muss der öffentliche Auftraggeber eine Prognoseentscheidung dahingehend treffen, ob von dem Unternehmen trotz einer vorherigen Schlechtleistung im Hinblick auf die Zukunft zu erwarten ist, dass der nunmehr zu vergebende Auftrag ordnungsgemäß durchgeführt wird.³²

h) Schwerwiegende Täuschung bei Eignungsprüfung

- 28 § 124 Abs. 1 Nr. 8 GWB ermächtigt zum Ausschluss solcher Bewerber, die im Vergabeverfahren unzutreffende Erklärungen in Bezug auf ihre Eignung oder

28 So auch schon EuGH, 3.3.2005 – Rs C-21/03 und C-34/03 – *Fabricom*; *Kupczyk*, NZBau 2010, 21, 22.

29 So die amtliche Begründung BT-Drs. 18/6281, S. 106.

30 *Hausmann/von Hoff*, in: Röwekamp/Kus/Portz/Prieß, Kommentar zum GWB-Vergaberecht, § 124 GWB Rn. 71 ff.

31 *Summa*, in: Heiermann/Zeiss/Summa, jurisPK-Vergaberecht, § 124 GWB Rn. 141 ff.

32 VK Rheinland-Pfalz, 31.10.2019 – VK 1-17/19, Rn. 67 f.; noch zur alten Rechtslage: VK Südbayern, 11.9.2014 – Z3-3-3194-1-34-07/14; VK Nordbayern, 18.12.2007 – 21.VK-3194-47/07; a. A. *Opitz*, in: Burgi/Dreher/Opitz, Beck'scher Vergaberechtskommentar, Bd. 1, § 124 GWB Rn. 104.

Ausschlussgründe abgegeben haben. Dem gleichgestellt sind die Fälle, in denen es der Bewerber unterlässt, Erklärungen abzugeben oder Auskünfte zu erteilen, obwohl diese offensichtlich für die Beurteilung der Eignung oder das Vorliegen von Ausschlussgründen von Bedeutung sind.³³ Ein bloßes Unterlassen vermag einen fakultativen Ausschlussstatbestand nur zu erfüllen, wenn der Bewerber bzw. Bieter zur Erklärung oder Aufklärung erkennbar verpflichtet ist. Grundsätzlich handelt es sich nämlich bei dem Vergabeverfahren um ein stark formalisiertes Verfahren und der Bewerber bzw. Bieter kann darauf vertrauen, dass er mit den abgefragten Angaben und Nachweisen das seinerseits Erforderliche getan hat und dem Auftraggeber die aus dessen Sicht notwendigen Informationen zur Beurteilung der Eignung oder des Vorliegens von Ausschlussgründen beigebracht hat. Aus den Vergabeunterlagen müssen sich konkrete Anhaltspunkte ergeben, die es als missbräuchlich erscheinen lassen, bestimmte Informationen zurückzuhalten.

Zusätzlich ist ein Ausschluss möglich, wenn das Unternehmen nicht in der Lage ist, die erforderlichen Nachweise zu übermitteln. Im Hinblick auf diese Alternative ist der Ausschlussgrund unklar formuliert. Mit Blick auf die Regelung in Art. 57 Abs. 4 lit. h i.V.m. Art. 59 der RL 2014/24/EU des Europäischen Parlaments und des Rates v. 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der RL 2004/18/EG ist diese Tatbestandsalternative dahingehend auszulegen, dass sie sich ausschließlich auf die Nachreichung der Unterlagen erstreckt, die wegen der Vorlage einer Einheitlichen Europäischen Eigenklärung (EEE) noch nicht eingereicht werden mussten. Gemäß § 48 Abs. 3 VgV muss der öffentliche Auftraggeber die EEE als vorläufigen Eignungsnachweis akzeptieren. Er kann gemäß § 50 Abs. 2 VgV die Vorlage weiterer Unterlagen nur verlangen, wenn dies für die ordnungsgemäße Verfahrensdurchführung notwendig ist oder vor Zuschlagserteilung. Ist dem Bieter die Vorlage nicht möglich, kann er ausgeschlossen werden. **29**

i) Unzulässige Einflussnahme

Gemäß § 124 Abs. 1 Nr. 9 lit. a GWB kann ein Unternehmen ausgeschlossen werden, das versucht hat, den öffentlichen Auftraggeber in unzulässiger Weise zu beeinflussen. Das setzt voraus, dass das Unternehmen den Tatentschluss, also Vorsatz, hatte, den öffentlichen Auftraggeber in unzulässiger Weise zu beeinflussen, und hierzu bereits unmittelbar angesetzt hat (vgl. § 22 StGB). Gleiches gilt gemäß § 124 Abs. 1 Nr. 9 lit. b GWB, wenn das Unternehmen versucht hat, vertrauliche Informationen zu erhalten, mit dem Ziel, sich dadurch Vorteile im Verfahren zu verschaffen. Da die Tatvollendung immer auch die Merkmale eines Versuchs einschließt, liegt der Ausschlussgrund auch vor, wenn die Beeinflussung **30**

33 Vgl. VK Hessen, 28.6.2005 – 69d VK 07/2005; *Opitz*, in: Burgi/Dreher/Opitz, Beck'scher Vergaberechtskommentar, Bd. 1, § 124 GWB Rn. 111; *Hänsel*, in: Ziekow/Völlink, Vergaberecht, § 6 VOL/A Rn. 8. Zum Täuschen durch Unterlassen auch *Kling*, in: Immenga/Mestmäcker, Wettbewerbsrecht, Bd. 4, § 124 GWB Rn. 104.

sung bereits erfolgt ist oder das Unternehmen die Information erhalten hat. Gemäß § 124 Abs. 1 Nr. 9 lit. c GWB kann ein Unternehmen zudem ausgeschlossen werden, wenn es vorsätzlich oder fahrlässig irreführende Informationen übermittelt, um sich Vorteile zu verschaffen, oder dies versucht.

IV. Wettbewerbsregister

1. Einrichtung des Wettbewerbsregisters

- 31 Zur Erleichterung der Prüfung der Ausschlussgründe durch die Vergabestellen hat der Gesetzgeber die Grundlagen für die Einrichtung eines Wettbewerbsregisters beim Bundeskartellamt in Bonn in Form einer elektronischen Datenbank, die ein automatisiertes, elektronisches Abrufverfahren ermöglicht,³⁴ geschaffen. Nach einer gestaffelten Inbetriebnahme ist das Wettbewerbsregister inzwischen vollständig in Betrieb. Inhaltliche und technische Vorgaben für die Datenbank finden sich in der WRegV, die auf § 10 WRegG beruht und am 23.4.2021 in Kraft getreten ist.³⁵ Seit seiner Inbetriebnahme löst das Wettbewerbsregister die zahlreichen in den Ländern existierenden Korruptionsregister und vergleichbare Datenbanken ab.³⁶

2. Eintragung von Rechtsverstößen

- 32 In das Register sind die in § 2 WRegG abschließend aufgezählten Rechtsverstöße einzutragen, die im Zusammenhang mit der Vergabe öffentlicher Aufträge oder Konzessionen relevant sind. Einzutragen sind gem. § 2 Abs. 1 WRegG insbesondere rechtskräftige strafgerichtliche Verurteilungen und Strafbefehle sowie rechtskräftige Bußgeldentscheidungen wegen
- der in § 123 Abs. 1 GWB aufgeführten Straftaten,
 - Betrugs i. S. d. §§ 263, 264 StGB, der sich gegen öffentliche Haushalte richtet,
 - Vorenthaltens und Veruntreuens von Bestandteilen des Arbeitsentgelts nach § 266a StGB,
 - Steuerhinterziehung nach § 370 AO,
 - wettbewerbsbeschränkender Absprachen bei Ausschreibungen nach § 298 StGB,
 - Entscheidungen nach § 8 Abs. 1 Nr. 2, §§ 10 bis 11 SchwarzArbG, § 404 Abs. 1 und 2 Nr. 3 SGB III, §§ 15, 15a, 16 Abs. 1 Nr. 1, 1c, 1d, 1f und 2 AÜG, § 21 Abs. 1 Nr. 1 bis 8, 10 und 11 sowie Abs. 2 MiLoG oder § 23 Abs. 1 Nr. 1 bis 9 und 11 sowie Abs. 2 AEntG, jeweils wenn auf Freiheitsstrafe von mehr als drei Monaten oder Geldstrafe von mehr als 90 Tagessätzen erkannt oder eine Geldbuße von wenigstens 2.500 EUR festgesetzt worden ist.

34 Vgl. amtliche Begründung zum WRegG, BT-Drs. 18/12051, S. 33.

35 *Opitz*, in: Burgi/Dreher/Opitz, Beck'scher Vergaberechtskommentar, Bd. 1, § 1 WRegG Rn. 2 ff.

36 Überblick in amtlicher Begründung zum WRegG, BT-Drs. 18/12051, S. 16 f.

Seit einer Novelle des WRegG Anfang 2023 sind auch rechtskräftige Bußgeldentscheidungen, die wegen Ordnungswidrigkeiten nach § 24 Abs. 1 LkSG ergangen sind, einzutragen, wenn ein Bußgeld von wenigstens 175.000 EUR festgesetzt worden ist.

Des Weiteren sind nach § 2 Abs. 2 WRegG Bußgeldentscheidungen einzutragen, die wegen Ordnungswidrigkeiten nach § 81 Abs. 1 Nr. 1 und Abs. 2 Nr. 1 i.V.m. § 1 GWB verhängt wurden, wenn eine Geldbuße von wenigstens 50.000 EUR ergangen ist. Insoweit wird keine Bestandskraft des Bußgeldbescheids vorausgesetzt (vgl. auch → Rn. 23).³⁷ **33**

Soweit sich die Gerichts- oder Verwaltungsentscheidungen gegen Privatpersonen richten, erfolgt die Eintragung, wenn die Tat einem Unternehmen zuzurechnen ist.³⁸ Die Zurechnungsregelung nach § 2 Abs. 3 WRegG entspricht derjenigen in § 123 Abs. 3 GWB (siehe → Rn. 12). **34**

Um sicherzustellen, dass die Verfehlungen auch zeitnah eingetragen werden, sind die Strafverfolgungsbehörden und die zur Verfolgung von Ordnungswidrigkeiten berufenen Behörden gemäß § 4 Abs. 1 WRegG verpflichtet, ihnen bekannte eintragungsrelevante Rechtsverstöße unverzüglich dem Register mitzuteilen. Den von einer Eintragung betroffenen Unternehmen ist nach § 5 Abs. 1 WRegG eine zweiwöchige Frist zur Stellungnahme einzuräumen, bevor die Eintragung erfolgt. Kann ein Unternehmen schlüssig darlegen, dass eine angekündigte oder bereits vorgenommene Eintragung unrichtig ist, so hat die Registerbehörde die Eintragung mit einem Sperrvermerk zu versehen, solange sich weder die Richtigkeit noch die Unrichtigkeit der Eintragung feststellen lässt. Wird die Unrichtigkeit der Eintragung festgestellt, ist die Eintragung unverzüglich zu löschen. Jedes Unternehmen und jede Person hat gemäß § 5 Abs. 2 Satz 1 WRegG einen Anspruch auf Auskunft über den sie betreffenden Inhalt des Registers, dies umfasst nach § 5 Abs. 6 WRegG auch das unbeschränkte Akteneinsichtsrecht eines bevollmächtigten Rechtsanwaltes.³⁹ **35**

3. Einbindung in das Vergabeverfahren

Der Eintrag in das Wettbewerbsregister zieht nicht automatisch eine Auftrags-sperre nach sich.⁴⁰ Vielmehr dient das Register dem öffentlichen Auftraggeber zu der Beschaffung relevanter Informationen. Er ist nach wie vor gehalten, anhand aller ihm zugänglichen Informationen einschließlich der Angaben aus dem Wettbewerbsregister eine eigenständige Entscheidung über einen Ausschluss zu **36**

37 Vgl. amtliche Begründung zum WRegG, BT-Drs. 18/12051, S. 27; dazu *Scherer-Leydecker*, CB 2017, 261, 263.

38 Dazu *Eufinger*, CB 2017, 240, 242.

39 Vgl. amtliche Begründung, BT-Drs. 18/12583, S. 11.

40 Amtliche Begründung zum WRegG, BT-Drs. 18/12051, S. 31; *Scherer-Leydecker*, CB 2017, 261, 263 f.

treffen und im Hinblick auf die fakultativen Ausschlussgründe sein Ermessen pflichtgemäß auszuüben.

- 37 Die Vergabestelle ist bei Aufträgen mit einem geschätzten Auftragswert ab 30.000 EUR ohne Umsatzsteuer nach § 6 Abs. 1 WRegG verpflichtet, vor Zuschlagserteilung bei der Registerbehörde abzufragen, ob es Eintragungen zu dem bietenden Unternehmen gibt. Öffentliche Auftraggeber, die Aufträge mit einem Auftragswert unter 30.000 EUR vergeben wollen, sind berechtigt, aber nicht verpflichtet, die Einträge über das Unternehmen bei der Registerbehörde abzufragen. Ausgenommen von der Abfragepflicht sind zudem Sachverhalte, die vom Vergaberecht ausgenommen sind, sowie Vergaben durch Auslandsdienststellen.⁴¹ Im Hinblick auf Sektorenauftraggeber und Konzessionsgeber ist die Abfragepflicht abgeschwächt.

4. Löschung von Eintragungen

- 38 Eintragungen werden gem. § 7 Abs. 1 WRegG teilweise nach fünf Jahren, teilweise nach drei Jahren ab Rechts- oder Bestandskraft der Entscheidung gelöscht. Die Löschfristen orientieren sich an den nach § 126 GWB zulässigen Höchstfristen für einen Ausschluss vom Vergabeverfahren.⁴² Soweit sich die Eintragung auf einen der zwingenden Ausschlussgründe des § 123 Abs. 1 und Abs. 4 GWB bezieht, erfolgt eine Löschung spätestens fünf Jahre nach dem Tag der Rechtskraft der Entscheidung. In den übrigen Fällen gilt eine Drei-Jahres-Frist ab dem Tag des Erlasses des Bußgeldbescheides bzw. der Unanfechtbarkeit der eintragungspflichtigen Gerichts- oder Bußgeldentscheidung.
- 39 Zudem kann das Unternehmen nach § 8 Abs. 1 WRegG eine vorzeitige Löschung unter Darlegung der von ihm ergriffenen Selbstreinigungsmaßnahmen nach § 125 GWB⁴³ sowie nach § 123 Abs. 4 Satz 2 GWB verlangen. Ein entsprechender Antrag ist nach § 8 Abs. 1 Satz 2 WRegG zulässig, wenn das Unternehmen ein berechtigtes Interesse an der vorzeitigen Löschung glaubhaft macht. Hierüber entscheidet die Registerbehörde von Amts wegen, wobei sie sich auf die Prüfung der Angaben und Nachweise des Unternehmens beschränken kann. Die Behörde kann nach § 8 Abs. 2 Satz 2 WRegG vom Antragsteller auch die Vorlage des Gutachtens eines Wirtschaftsprüfers oder eines Rechtsanwalts oder anderer geeigneter Unterlagen verlangen. Daneben kann sie die Strafverfolgungsbehörde oder die Behörde, die für die Verfolgung von Ordnungswidrigkeiten zuständig ist, gem. § 8 Abs. 3 WRegG um Auskunft ersuchen.

41 Amtliche Begründung zum WRegG, BT-Drs. 18/12051, S. 30; *Scherer-Leydecker*, CB 2017, 261, 263.

42 *Scherer-Leydecker*, CB 2017, 261, 263.

43 Vgl. *Stolz*, in: Ziekow/Völlink, Vergaberecht, § 125 GWB Rn. 5 ff.

5. Rechtsbehelfe

Gegen die Entscheidungen der Registerbehörde ist nach § 11 Abs. 1 WRegG die Beschwerde zum Oberlandesgericht zulässig, das gemäß § 171 GWB bereits für Vergabesachen zuständig ist.⁴⁴ Als Gegenstand der Beschwerde kommen insbesondere die Vornahme einer Eintragung durch die Registerbehörde oder die Ablehnung einer vorzeitigen Löschung wegen Selbstreinigung in Betracht.⁴⁵ **40**

V. Selbstreinigung

Gemäß § 125 Abs. 1 GWB dürfen Unternehmen, bei denen ein Ausschlussgrund vorliegt, nicht ausgeschlossen werden, wenn sie eine hinreichende Selbstreinigung nachgewiesen haben. Da die Selbstreinigungsmaßnahmen jeweils an ein Fehlverhalten des Unternehmens anknüpfen, kommt eine Selbstreinigung auch nur im Hinblick auf Ausschlussgründe in Betracht, die auf Verfehlungen des Unternehmens beruhen, also nicht im Hinblick auf die Ausschlussgründe nach § 124 Abs. 1 Nr. 2, 5 und 6 GWB. **41**

1. Selbstreinigung im Vergabeverfahren**a) Prüfung durch Vergabestelle**

Dem Unternehmen steht es offen, im konkreten Vergabeverfahren der Vergabestelle darzulegen und nachzuweisen, dass es Selbstreinigungsmaßnahmen ergriffen hat, die sicherstellen, dass seine Integrität wieder hergestellt ist.⁴⁶ Durch das Fehlverhalten hat das Unternehmen die Notwendigkeit einer Selbstreinigung ausgelöst, sodass es auch sachgerecht ist, ihm die Nachweispflicht für die erfolgte Selbstreinigung aufzuerlegen. Der Nachweis kann nach Maßgabe der einschlägigen Vorgaben etwa in § 50 VgV mit der Einheitlichen Europäischen Eigenenerklärung (EEE) erbracht werden.⁴⁷ Das Formular für die EEE⁴⁸ sieht vor, dass das Unternehmen Angaben zu etwaigen Selbstreinigungsmaßnahmen macht, wenn es auf die Fragen betreffend Verfehlungen bejahend antwortet.⁴⁹ Das betroffene Unternehmen hat ein Recht auf Prüfung durch den öffentlichen Auftraggeber, ob es ausreichende Maßnahmen nach dem Katalog des § 125 GWB getroffen hat, um seine Integrität wiederherzustellen. Diese Prüfung ist von dem öffentlichen Auftraggeber in die allgemeine Prüfung über das Vorliegen von Ausschlussgründen in Bezug auf das Unternehmen einzubeziehen.⁵⁰ **42**

44 Vgl. amtliche Begründung zum WRegG, BT-Drs. 18/12051, S. 34.

45 *Scherer-Leydecker*, CB 2017, 261, 264.

46 *Dreher/Hoffmann*, NZBau 2014, 150, 154.

47 Vgl. *Tomerius*, in: Pünder/Schellenberg, Vergaberecht, § 50 VgV Rn. 1 ff.

48 Durchführungsverordnung (EU) 2016/7, ABl. EU 2016, L3, S. 16.

49 Zu beachten ist, dass das Unternehmen spätestens bei beabsichtigter Auftragserteilung konkrete Nachweise vorlegen muss. Vgl. *Voppel*, in: *Voppel/Osenbrück/Bubert*, VgV, § 50 Rn. 16.

50 *Schnitzler*, BB 2016, 2115, 2119.

Das Fehlen von Nachweisen und eine etwaige Verweigerung der Mitwirkung bei der Ermittlung des Sachverhaltes gehen zulasten des Unternehmens.⁵¹

b) Prüfung durch Wettbewerbsregister

- 43** Ein Unternehmen kann die Selbstreinigungsmaßnahmen gemäß § 8 WRegG in dem Verfahren über die vorzeitige Löschung der Verfehlung aus dem Wettbewerbsregister auch gegenüber dem Bundeskartellamt, dem die Führung des Wettbewerbsregisters obliegt, nachweisen. Das Lösungsverfahren muss von dem Unternehmen beantragt werden und ist gebührenpflichtig. Da die zentrale Selbstreinigung im Rahmen des Lösungsverfahrens erfolgt, kommt sie auch nur im Hinblick auf Verfehlungen in Betracht, die gem. § 2 WRegG eintragungspflichtig sind. Gemäß § 8 Abs. 1 Satz 3 und Abs. 4 Satz 1 WRegG prüft die Registerbehörde das Vorliegen der Selbstreinigung nach den Maßstäben des § 125 GWB unter Berücksichtigung der Schwere und der besonderen Umstände der Straftat oder des Fehlverhaltens.⁵²

2. Kriterien der Selbstreinigung

- 44** Eine wirksame Selbstreinigung setzt voraus, dass das Unternehmen, das auszuschießen wäre, nachweist, dass es die in § 125 Abs. 1 Satz 1 Nr. 1 bis 3 GWB aufgezählten Maßnahmen ergriffen hat. Die Maßnahmen sind kumulativ zu ergreifen. Die Gewichtung der jeweiligen Maßnahmen und deren Umfang hängt vom konkreten Einzelfall des begangenen Verstoßes und der Tatbeiträge innerhalb des Unternehmens ab und ist individuell zu beurteilen.⁵³

a) Ausgleich des Schadens

- 45** Das betroffene Unternehmen ist verpflichtet, den gesamten durch die Straftat oder das Fehlverhalten verursachten Schaden auszugleichen. Das Unternehmen kann den Schadensausgleich durch Zahlung bewirken oder sich zum Schadensausgleich verpflichten.⁵⁴ Beide Alternativen stehen in § 125 Abs. 1 Satz 1 Nr. 1 GWB gleichberechtigt nebeneinander, obwohl qualitativ ein erheblicher Unterschied zwischen der bereits geleisteten Ausgleichszahlung und dem Eingehen einer bloßen Verpflichtung, die gegebenenfalls durchgesetzt werden muss, besteht. Probleme bereitet der Schadensausgleich, wenn der öffentliche Auftraggeber zur Bestimmung des entstandenen Schadens auf die Mitwirkung des Unternehmens angewiesen ist. Bereits nach der bisherigen Rechtsprechung war angenommen worden, dass Voraussetzung für eine wirksame Selbstreinigung die Mitarbeit bei der Berechnung der Schadenshöhe und bei der Aufklärung des

⁵¹ VK Lüneburg, 14.2.2012 – VgK-05/2012.

⁵² Dazu *Scherer-Leydecker*, CB 2017, 261, 263 f.

⁵³ *Schnitzler*, BB 2016, 2115, 2119.

⁵⁴ Dazu auch schon LG Berlin, 22.3.2006 – 23 O 118/04.

für die Schadensermittlung maßgeblichen Sachverhalts ist.⁵⁵ Dem wird entgegengehalten, Vergaberecht könne nicht missbraucht werden, um die Beweislastverteilung nach Zivilrecht umzukehren, die verlangt, dass der Geschädigte die Höhe des Schadens darlegt und beweist.⁵⁶ Die Kooperationspflicht ist in § 125 Abs. 1 Satz 1 Nr. 2 GWB nunmehr ausdrücklich vorgeschrieben (siehe → Rn. 46).

b) Zusammenarbeit zur Aufklärung

Gemäß § 125 Abs. 1 Satz 1 Nr. 2 GWB erfordert eine wirksame Selbstreinigung, dass das Unternehmen alle Tatsachen und Umstände sowie die dadurch verursachten Schäden⁵⁷ aufklärt und mit den Ermittlungsbehörden und dem öffentlichen Auftraggeber zusammenarbeitet.⁵⁸ Die Selbstreinigungsmaßnahme nach § 125 Abs. 1 Satz 1 Nr. 2 GWB umfasst zwei zu trennende Schutzrichtungen. Einerseits verlangt eine Selbstreinigung die aktive Zusammenarbeit mit den Ermittlungsbehörden. Das sind insbesondere Staatsanwaltschaft, zuständige Ordnungsbehörden und Kartellbehörden. Andererseits verlangt § 125 Abs. 1 Satz 1 Nr. 2 GWB auch Aufklärung und Zusammenarbeit mit dem öffentlichen Auftraggeber. Diese zweite Alternative ist in Art. 57 Abs. 6 Unterabs. 2 RL 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der RL 2004/18/EG nicht ausdrücklich angelegt und beruht auf der nationalen Umsetzung durch den deutschen Gesetzgeber. Inzwischen hat der EuGH klargestellt, dass diese Bestimmung des deutschen Rechts mit EU-Recht in Einklang steht und ein Wirtschaftsteilnehmer in bestimmten Fällen auch mit dem öffentlichen Auftraggeber zusammenarbeiten muss, um den Nachweis der Wiederherstellung seiner Zuverlässigkeit zu erbringen.⁵⁹ Hierbei beschränkt er die Pflicht zur Zusammenarbeit jedoch auf Maßnahmen, die unbedingt erforderlich sind, damit das Ziel der Prüfung der Integrität des Unternehmens verfolgt werden kann.⁶⁰

Es sind alle mit dem Fehlverhalten in Bezug stehenden Umstände aufzuklären. Das Unternehmen muss sich zur Erfüllung dieser Voraussetzung des § 125 Abs. 1 Satz 1 Nr. 2 GWB aktiv, ernsthaft und nach außen erkennbar bemühen.⁶¹ Eine selektive Einlassung des Unternehmens oder reine Lippenbekenntnisse sind nicht ausreichend. Es muss der ernstgemeinte Wille zur Wiedergutmachung

55 VK Lüneburg, 14.2.2012 – VgK-05/2012; 24.3.2011 – VgK-04/2011.

56 Vgl. *Oetker*, in: MünchKomm-BGB, § 249 Rn. 481.

57 *Stolz*, in: Ziekow/Völlink, Vergaberecht, § 125 GWB Rn. 7.

58 LG Berlin, 22.3.2006 – 23 O 118/04; *Mutschler-Siebert/Dorschfeldt*, BB 2015, 642, 645.

59 EuGH, 24.10.2018 – C-124/17, Rn. 33; a. A. VK Südbayern, 7.3.2017, Z3-3-3194-1-45-11/16, Rn. 88.

60 EuGH, 24.10.2018 – C-124/17, Rn. 28, 33.

61 OLG Düsseldorf, 9.6.2010 – VII-Verg 14/10; LG Berlin, 22.3.2006 – 23 O 118/04; *Schnitzler*, BB 2016, 2115, 2119.

des Fehlverhaltens vorhanden und erkennbar sein. Dies muss anhand der konkreten Umstände des Einzelfalls beurteilt werden.

c) Technische, organisatorische und personelle Maßnahmen

- 48 Nach § 125 Abs. 1 Satz 1 Nr. 3 GWB sind technische, organisatorische und personelle Maßnahmen des Unternehmens erforderlich, um nicht weiterhin von den Vergabeverfahren ausgeschlossen zu werden. Diese Maßnahmen müssen sowohl abstrakt als auch konkret geeignet sein zu gewährleisten, dass weiteres Fehlverhalten oder Straftaten für die Zukunft ausgeschlossen sind. § 125 Abs. 1 Satz 1 Nr. 3 GWB ist zukunftsgerichtet, indem er die Prävention weiterer Verstöße regelt. Präventive Maßnahmen nach § 125 Abs. 1 Satz 1 Nr. 3 GWB bilden das Herzstück der Selbstreinigung, da sie darauf gerichtet sind, zukünftige Verstöße durch konkrete Vorkehrungen zu unterbinden.⁶²
- 49 Die bisherige Rechtsprechung hatte schon konkrete Maßnahmen herausgearbeitet, die auch in dem Erwägungsgrund Nr. 102 RL 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der RL 2004/18/EG Erwähnung finden. Hierunter sind solche Maßnahmen zu verstehen, die auf ein Verhalten hinwirken, das mit den vergaberechtlichen Vorschriften im Einklang steht.⁶³ Diese Compliance-Maßnahmen umfassen insbesondere Personal- und Organisationsmaßnahmen wie den Abbruch aller Verbindungen zu den an dem Fehlverhalten beteiligten Personen oder Organisationen, geeignete Personalreorganisationsmaßnahmen, die Einführung von Kontroll- und Berichtssystemen, die Schaffung einer internen oder externen Überwachungsstruktur oder auch die Einführung interner Haftungs- und Entschädigungsregelungen. Der Katalog von möglichen Maßnahmen ist dabei nicht abschließend. Vielmehr ist im Einzelfall zu prüfen, welche Maßnahmen in dem konkreten Fall geeignet sind sicherzustellen, dass insbesondere das in Rede stehende Fehlverhalten in der betreffenden Unternehmensstruktur in Zukunft vollumfänglich verhindert wird.
- 50 Insbesondere bei Personengesellschaften und juristischen Personen sind personelle Maßnahmen erforderlich, da nicht das Unternehmen selbst, sondern die für das Unternehmen verantwortlich handelnden Personen die Verstöße begangen haben. Grundsätzlich wird insoweit der Abbruch der Verbindungen zu denjenigen Personen und Organisationen gefordert, die an dem zum Ausschluss führenden Fehlverhalten beteiligt waren.⁶⁴ Wird der Person, die die Straftat oder das Fehlverhalten begangen hat, die tatsächliche und/oder rechtliche Möglichkeit zur Einflussnahme auf die Geschäftsführung belassen, muss sich das Unterneh-

62 LG Berlin, 22.3.2006 – 23 O 118/04.

63 Dreher/Hoffmann, NZBau 2014, 150.

64 Vgl. OLG München, 22.11.2012 – Verg 22/12; OLG Brandenburg, 14.12.2007 – Verg W 21/07; VK Bund, 12.6.2015 – VK 2-31/15; Dreher/Hoffmann, NZBau 2014, 67, 68; Mutschler-Siebert/Dorschfeldt, BB 2015, 642, 645; Schnitzler, BB 2016, 2115, 2119.

men etwaige Verfehlungen i. d. R. auch weiterhin zurechnen lassen.⁶⁵ Dabei können verantwortliche Personen Gesellschafter, Organe und Mitarbeiter des Unternehmens sein. Das Verhalten dieser Personen muss dem Unternehmen zuzurechnen sein bzw. diese müssen einen gewissen Einfluss auf das Unternehmen ausüben können (siehe → Rn. 12). Ein Verbleib der Personen in dem Unternehmen kann daher eine wirksame Selbstreinigung ausschließen,⁶⁶ insbesondere bei vertretungsberechtigten Personen wie Geschäftsführern.⁶⁷ Dies spiegelt sich auch in der neueren Rechtsprechung des OLG Düsseldorf wider, wonach eine personelle Selbstreinigung dann unzureichend erfolgt ist, wenn die Gesellschaft auch nach Durchführung von Selbstreinigungsmaßnahmen noch von dem bisherigen und für das Fehlverhalten verantwortlichen Alleingesellschafter dominiert wird.⁶⁸ Ausreichend sei die Möglichkeit der Einflussnahme der verantwortlichen Person auf das operative Geschäft der Gesellschaft.⁶⁹ Weitere Präventivmaßnahmen seitens des Unternehmens zur Vermeidung zukünftiger Verfehlungen von Mitarbeitern können die Einrichtung einer Clearingstelle, eine externe anwaltliche Prüfung oder die Einführung eines Compliance- oder Wertemanagements mit angemessenen Schulungsmaßnahmen sein. Diese sollten zur effektiven Verhinderung erneuter Verfehlungen parallel zu der Trennung von den verantwortlichen Mitarbeitern ergriffen werden.⁷⁰ Zudem sind Sonderprüfungen der Mitarbeiter, Trennungen von allen Mitarbeitern, die in dem Verdacht der Mitwirkung stehen, oder die Überprüfung und Anpassung aller Handlungsvollmachten, etwa die Einführung des Vier-Augen-Prinzips oder sonstige Mitzeichnungs- oder Kontrollpflichten, geeignete Maßnahmen.⁷¹ Bei Personalmaßnahmen ist immer zu hinterfragen, ob sie arbeitsrechtlich durchsetzbar sind; ansonsten würde deren Umsetzung einen erneuten Rechtsverstoß auslösen. Welche Maßnahmen als ausreichend erachtet werden, ist maßgeblich vom jeweiligen Einzelfall abhängig.

Im gleichen Maße wie Verfehlungen gemäß § 123 Abs. 3 GWB (siehe → Rn. 12) verschiedenen Konzernunternehmen zugerechnet werden können, stellt sich die Frage, inwieweit innerhalb eines Konzerns Maßnahmen i. S. d. § 125 GWB ergriffen werden müssen. Wenn nicht Bußgelder direkt gegen einzelne Konzernunternehmen festgesetzt werden, müssen Selbstreinigungsmaßnahmen bei allen Unternehmen im Konzern in Betracht gezogen werden, denen das Verhalten der Person, die Straftaten oder Verfehlungen begangen hat, zuzurechnen ist. Allerdings ist jedes Unternehmen separat zu betrachten. Sobald ein Unternehmen sich

51

65 OLG Brandenburg, 14.12.2007 – Verg W 21/07; OLG Düsseldorf, 28.7.2005 – Verg 42/05; *Prieß/Stein*, NZBau 2008, 230, 231.

66 VK Bund, 12.6.2015 – VK 2-31/15.

67 VK Bund, 12.6.2015 – VK 2-31/15.

68 OLG Düsseldorf, 18.4.2018 – VII-Verg. 28/17.

69 OLG Düsseldorf, 18.4.2018 – VII-Verg. 28/17.

70 OLG Brandenburg, 14.12.2007 – Verg W 21/07.

71 OLG Düsseldorf, 9.6.2010 – VII Verg 14/10; OLG Düsseldorf, 9.4.2003 – Verg 66/02; LG Berlin, 22.3.2006 – 23 O 118/04; VK Brandenburg, 16.10.2007 – VK 38/07; *Prieß/Stein*, NZBau, 2008, 230, 233.

selbst gereinigt hat, darf es nicht mehr ausgeschlossen werden, selbst wenn ein anderes Unternehmen im Konzern noch nicht selbstgereinigt ist. Eine Selbstreinigung ist gegebenenfalls nicht hinreichend, wenn die betreffende Person beispielsweise zwar als Geschäftsführer abberufen wurde, aber nunmehr über eine andere Position im Konzern eine leitende Funktion i. S. d. § 123 Abs. 3 GWB innehat. Für jedes Unternehmen, das sich an einer Vergabe öffentlicher Aufträge beteiligen will, muss das im Einzelfall genauestens hinterfragt und geprüft werden, auch unter Berücksichtigung der aktuellen Konzernstruktur.

VI. Ausschlussfristen

- 52** Selbst wenn keine Selbstreinigungsmaßnahmen ergriffen wurden, führt das Vorliegen eines Ausschlussgrundes nicht zu einer unbefristeten Auftragssperre. § 126 GWB regelt die Zeiträume, die Unternehmen maximal für Auftragsvergaben gesperrt werden dürfen. Dabei differenziert die Vorschrift bei der Festlegung von Sperrfristen im Hinblick auf die Ausschlussgründe. Die Fristenregelungen unterscheiden sich nicht nur in der Länge der Ausschlussfrist, sondern auch in der Regelung zum Fristbeginn.

1. Fristenregelung bei zwingenden Ausschlussgründen

- 53** Aufgrund eines Ausschlussgrundes nach § 123 GWB darf ein Unternehmen höchstens fünf Jahre ausgeschlossen werden. Nach dem Wortlaut der Bestimmung beginnt die Frist mit „dem Tag der rechtskräftigen Verurteilung“. Ab diesem Tag und damit einschließlich dieses Tags darf für den festgelegten Zeitraum ein Ausschluss erfolgen. Damit ist der Tag der Verurteilung in die Frist mit einbezogen und muss gem. § 187 Abs. 2 BGB bei der Fristberechnung mitberücksichtigt werden. Da die Frist nach Jahren bemessen ist, endet sie gem. § 188 Abs. 2 Var. 2 BGB folglich mit dem Ablauf desjenigen Tages des letzten Monats der Frist, welcher dem Tage vorhergeht, der durch seine Zahl dem Anfangstag der Frist entspricht.

2. Fristenregelung bei fakultativen Ausschlussgründen

- 54** Aufgrund eines Ausschlussgrundes nach § 124 GWB darf ein Unternehmen höchstens drei Jahre ausgeschlossen werden. Nach dem Wortlaut der Bestimmung beginnt die Frist mit „dem betreffenden Ereignis“. Ab diesem Ereignis darf für den festgelegten Zeitraum ein Ausschluss erfolgen. Anders als bei § 126 Nr. 1 GWB wird der Tag, an dem das „Ereignis“ auftritt, nicht vollständig in die Frist mit einbezogen. Der Zeitraum vor Eintritt des Ereignisses ist nicht in die Frist einbezogen. Der Ereignistag muss daher gem. § 187 Abs. 1 BGB bei der Fristberechnung außer Acht gelassen werden. Da die Frist nach Jahren bemessen ist, endet sie gem. § 188 Abs. 2 Var. 1 BGB mit dem Ablauf desjenigen Tages des letzten Monats, welcher durch seine Benennung oder seine Zahl dem Tage entspricht, in den das Ereignis fällt.

Auf welches Ereignis im konkreten Fall abzustellen ist, hängt vom jeweiligen Ausschlussgrund ab.⁷² Problematisch ist dies insbesondere, wenn der Ausschlussgrund an ein Fehlverhalten des Unternehmens anknüpft. Teilweise wurde vertreten, dass bei einem Fehlverhalten auf die betreffende Tathandlung abzustellen sei.⁷³ Der EuGH hat in seinem Urteil vom 24.10.2018⁷⁴ dementsgegen im Hinblick auf den Ausschlussgrund des § 124 Abs. 1 Nr. 4 GWB klargestellt, dass der höchstzulässige Zeitraum des Ausschlusses ab dem Datum, an dem die für die Ahndung des Rechtsverstoßes zuständige Behörde einen Verstoß durch das betreffende Verhalten feststellt, berechnet werden müsse.⁷⁵

3. Ermessensausübung

§ 126 GWB bestimmt sowohl für den Ausschluss aufgrund eines zwingenden Grundes als auch für den Ausschluss wegen eines fakultativen Grundes Höchstfristen. Das bedeutet zum einen, dass diese Fristen nicht überschritten werden dürfen, und zum anderen, dass der öffentliche Auftraggeber diese Fristen unterschreiten kann.⁷⁶ Somit ist ihm ein Ermessen eröffnet, bis zu welchem Zeitpunkt er ein auszuschließendes Unternehmen sperrt.⁷⁷ Dieses Ermessen muss der Auftraggeber pflichtgemäß ausüben und die Entscheidung ist nur eingeschränkt gerichtlich überprüfbar.⁷⁸ Die Sperrfristen dürfen nicht als feststehende Vorgabe angewendet werden. Die Vergabestelle muss ihr Ermessen ausüben. Maßgeblich im Rahmen der Abwägung sind insbesondere die Schwere des Tatvorwurfs im Hinblick auf die Zuverlässigkeit des Unternehmens als zukünftiger Auftragnehmer einerseits und die Intensität des Eingriffs, den eine Auftragssperre für das Unternehmen darstellt, andererseits.⁷⁹

72 Amtliche Begründung, BT-Drs. 18/6281, S. 111.

73 VK Südbayern, 7.3.2017 – Z3-3-3194-1-45-11/16, Rn. 97.

74 EuGH, 24.10.2018 – C-124/17.

75 EuGH, 24.10.2018 – C-124/17, Rn. 41 f.; kritisch hierzu und zum Fristbeginn bei den einzelnen Ausschlussgründen *Scherer*, in: Heuvels/HöB/Kuß/Wagner, Vergaberecht, § 126 Rn. 12 ff.

76 *Radu*, in: Müller-Wrede, GWB, § 126 GWB Rn. 42.

77 Vgl. OLG Karlsruhe, 16.12.2020 – 15 Verg 4/20; *Radu*, in: Müller-Wrede, GWB, § 126 GWB Rn. 45 ff.

78 OLG Karlsruhe, 16.12.2020, Verg 4/20; *Kaufmann*, in: Pünder/Schellenberg, Vergaberecht, § 126 Rn. 29.

79 *Radu*, in: Müller-Wrede, GWB, § 126 GWB Rn. 49.

29. Kapitel Tax Compliance*

I. Einleitung

Tax Compliance ist das Selbstbekenntnis zur **Einhaltung aller steuerrechtlichen Regelungen**, die für das Unternehmen gelten und – über diese sich bereits aus dem Gesetz ergebende Pflicht hinaus – die Sicherstellung der Einhaltung dieser Pflichten durch eine entsprechende **Organisationsstruktur**.¹ Gesetzes-treues Verhalten beinhaltet jedoch auch die zulässige Ausnutzung gesetzgeberischer Spielräume sowie die Auslegung der Steuerrechtsnormen im Rahmen der juristisch zulässigen Möglichkeiten.² Der Steuerpflichtige darf seine steuerlichen Verhältnisse insbesondere so gestalten, dass keine oder möglichst geringe Steuern anfallen, und dabei zivilrechtliche Gestaltungen, die vom Gesetz vorgesehen sind, frei verwenden.³ Tax Compliance darf daher nicht dahingehend missverstanden werden, dass unter Verzicht auf eigene Rechtspositionen der Steuerstreit mit der Finanzverwaltung zu vermeiden sei.

Während Corporate Compliance-Strukturen seit vielen Jahren in Unternehmen implementiert sind, ist Tax Compliance erst im Laufe der letzten zehn Jahre verstärkt in das Bewusstsein der Unternehmensverantwortlichen gerückt.⁴ Grund dafür war nicht zuletzt eine Neuregelung im Anwendungserlass zur AO (AEAO). Die obersten Finanzbehörden des Bundes und der Länder haben den Anwendungserlass im Jahr 2016 um eine Regelung im Rahmen von § 153 AO ergänzt.⁵ Während in fast jedem kleinen und mittelgroßen Unternehmen inzwischen ein Compliance Officer anzutreffen ist, ist ein Tax Compliance Office dagegen selbst in großen Unternehmen aber nach wie vor eine Ausnahmeerscheinung. Die Ursache für den Bedeutungsgewinn der Tax Compliance liegt in dem Spannungsverhältnis, einerseits mitunter komplexe und fehleranfällige steuerrechtliche Sachverhalte ordnungsgemäß erklären zu müssen, während sich andererseits das regulatorische Umfeld, wie bspw. die Erhöhung der Anforderungen an steuerliche Korrekturmöglichkeiten (siehe hierzu → Rn. 101 ff.), als auch die

* Der Autor dankt Frau Dr. *Anja Stürzl*, die in der Voraufgabe an der Bearbeitung dieses Beitrags mitgewirkt hat.

1 *Aichberger/Schwartz*, DStR 2015, 1691, 1692; *Streck/Binnewies*, DStR 2009, 229; *Menner/Bexa*, CCZ 2019, 129.

2 *Streck*, in: *Streck/Mack/Schwedhelm*, Tax Compliance, Rn. 1.16; *Besch/Starck*, in: *Hauschka/Moosmayer/Lösler*, Corporate Compliance, § 33 Rn. 4.

3 BFH, 22.6.2017 – IV R 42/13, DStR 2017, 2653; EuGH, 21.2.2006 – C-255/02, Halifax, BeckRS 2006, 70150.

4 *Aichberger/Schwartz*, DStR 2015, 1691, 1692; *Besch/Starck*, in: *Hauschka/Moosmayer/Lösler*, Corporate Compliance, § 33 Rn. 1.

5 BMF, 23.5.2016 – IV A 3 – S 0324/15/10001; s. a. Nr. 2.6 AEAO zu § 153 AO.

Rechtsprechung des BGH in Steuerstrafsachen⁶ verschärft haben, was damit einhergehend, dass in der gegenwärtigen Verfahrenspraxis der Finanz- und Ermittlungsbehörden die ordnungsgemäße Erfüllung der steuerlichen Pflichten durch Unternehmen zunehmend unter steuerstraft- und steuerordnungswidrigkeitenrechtlichen Gesichtspunkten geprüft wird. Sachverhalte, die früher ausschließlich mit den Veranlagungsbezirken sowie der Betriebsprüfung diskutiert wurden, werden heute tendenziell frühzeitiger an die Straf- und Bußgeldsachenstellen zur Prüfung der Einleitung eines steuerstrafrechtlichen Ermittlungsverfahrens abgegeben. Verschärft wurde diese Entwicklung durch eine Entscheidung des LG Stuttgart. Unterlässt ein Beamter der Finanzbehörde (einschließlich des Außenprüfers) es, den Anfangsverdacht einer Steuerstraftat der innerbehördlich für die Steuerfahndung zuständigen Stelle mitzuteilen, kann er sich danach wegen (versuchter) Strafvereitelung durch Unterlassen (§§ 258 Abs. 1 AO, 13 StGB) strafbar machen.⁷ In der Folge werden nicht selten Ermittlungsverfahren gegen Organe oder Mitarbeiter des Unternehmens eingeleitet. Als originär Verantwortlicher zur Erfüllung der steuerlichen Pflichten des Unternehmens gerät so schnell der Vorstand oder der Geschäftsführer in den Fokus eines steuerstrafrechtlichen Ermittlungsverfahrens. All dies hat den Eindruck einer **Kriminalisierung unternehmerischen Handelns** erweckt.

- 3 Gleichwohl haben nach einer aktuellen Studie bislang acht von zehn Unternehmen noch kein wirksames Tax Compliance-System implementiert. Sechs von zehn Unternehmen investieren nach eigenen Angaben aktuell jedoch in ein Tax Compliance-System. Eine neue Dynamik könnte sich aufgrund des **DAC7-Umsetzungsgesetzes** vom 20.12.2022 ergeben.⁸ Damit hat der Gesetzgeber in Art. 97 § 38 EGAO eine zunächst bis zum Jahr 2029 befristete Erprobungsregelung zur Gewährung von **Prüfungserleichterungen in der Außenprüfung bei vorhandenem Steuerkontrollsystem** eingeführt, die am 1.1.2023 in Kraft getreten ist. Durch diese Neuregelung sollen für den Steuerpflichtigen Anreize zur freiwilligen Installation eines Steuerkontrollsystems geschaffen werden, um dadurch eine verstärkte Kooperation zwischen den Verfahrensbeteiligten und einen beschleunigten Ablauf der Betriebsprüfung zu erzielen.⁹ Hierdurch erfährt das Steuerkontrollsystem (Tax Compliance-System) eine erhebliche gesetzliche Aufwertung, die über seine bisherige Bedeutung im Rahmen der Vermeidung von Haftungsrisiken hinausgeht.
- 4 Durch ein funktionierendes und dokumentiertes Tax Compliance-System können die steuerstraft- und steuerordnungswidrigkeitenrechtlichen Risiken für die

6 Hierfür stehen exemplarisch folgende Entscheidungen: BGH, 2.12.2008 – 1 StR 416/08, NJW 2009, 528 (Millionengrenze); BGH, 20.5.2010 – 1 StR 577/09, DStR 2010, 1133 (Selbstanzeige-Beschluss); BGH, 27.10.2015 – 1 StR 373/15, BeckRS 2016, 02436 (Steuerverkürzung in großem Ausmaß).

7 LG Stuttgart, 24.3.2020 – 61 Ns 142 Js 114222/16, NStZ 2021, 544.

8 BGBl. 2022 I, S. 2730.

9 Kowallik, DB 2023, 804; Hölzemann/Ramadan/Otto/Nordmann, WPg 2023, 1394.

Organe und Mitarbeiter des Unternehmens als auch für das Unternehmen selbst erheblich reduziert werden. Daneben lassen sich steuerliche Haftungsrisiken minimieren. Ungeachtet der Frage, ob eine gesetzliche Pflicht zur Einrichtung eines Tax Compliance-Systems existiert, besteht hierzu jedenfalls eine faktische Notwendigkeit.¹⁰ Dabei ist das grundsätzliche Bedürfnis nach einer Tax Compliance-Struktur unabhängig von der Rechtsform und der Größe eines Unternehmens. Auch in kleineren und mittelgroßen Unternehmen ist ein an den **unternehmensspezifischen Risiken orientiertes Minimum an Tax Compliance dringend zu empfehlen**. Angesichts der Komplexität der Materie und der sich ständig wandelnden Regelungen kommt ein verantwortungsvoll agierender Geschäftsleiter nicht umhin, zumindest ein rudimentär ausgestaltetes System zu implementieren, das Steuerrisiken evaluieren, aufdecken und verhindern soll.¹¹

II. Steuerliche Pflichten

1. Allgemeine steuerliche Pflichten

Die Abgabenordnung sowie die Einzelsteuergesetze legen dem Steuerpflichtigen eine Vielzahl von Pflichten auf. Nachstehend erfolgt ein Überblick über die wesentlichen steuerlichen Pflichten: 5

Nach § 88 AO hat die Finanzverwaltung den der Besteuerung zugrunde liegenden Sachverhalt von Amts wegen zu ermitteln (Untersuchungsgrundsatz). Allerdings ist der Steuerpflichtige nach § 90 Abs. 1 AO zur Mitwirkung bei der Sachverhaltsermittlung verpflichtet. Der **Mitwirkungspflicht** wird insbesondere dadurch nachgekommen, dass die für die Besteuerung erheblichen Tatsachen vollständig und wahrheitsgemäß offengelegt und die bekannten Beweismittel angegeben werden. Der Umfang dieser Pflichten richtet sich nach den Umständen des Einzelfalls. Bei Auslandssachverhalten normiert § 90 Abs. 2 AO gesteigerte Mitwirkungspflichten. Danach hat der Steuerpflichtige den Sachverhalt aufzuklären und die erforderlichen Beweismittel zu beschaffen. Die Verletzung der Mitwirkungspflichten kann zur Begrenzung der Aufklärungs- und Ermittlungspflicht der Finanzverwaltung und zur Schätzung der Besteuerungsgrundlagen (§ 162 AO) führen. Die Schätzungsbefugnis besteht auch, wenn der Steuerpflichtige seiner Mitwirkungspflicht nicht nachkommt, weil gegen ihn ein Strafverfahren anhängig ist und er sich nicht selbst belasten will. 6

¹⁰ Nach der Neufassung der MaRisk durch das BaFin-Rundschreiben 10/2012 (BA) vom 14.12.2012, Gz.: BA 54-FR 2210–2012/0002 ist zumindest für Kreditinstitute und Finanzdienstleistungsinstitute die Einrichtung einer Compliance-Funktion, welche auch die Verpflichtung zur Identifizierung und Vermeidung steuerlicher Risiken umfasst, verbindlich vorgeschrieben. Vgl. auch BaFin, Rundschreiben 09/2017 (Ba) vom 27.10.2017, Gz.: BA 54-FR 2210–2017/0002 zu Mindestanforderungen an das Risikomanagement. Als Folge des Wirecard-Verfahrens wurde in § 91 Abs. 3 AktG für börsennotierte Gesellschaften die Pflicht zur Einrichtung eines wirksamen internen Kontrollsystems und Risikomanagementsystems eingeführt.

¹¹ *Besch/Starck*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 33 Rn. 8.

- 7 § 200 AO regelt die Mitwirkungspflichten des Steuerpflichtigen bei der **Außenprüfung**. Danach hat der Steuerpflichtige bei der Feststellung der Sachverhalte, die für die Besteuerung erheblich sein können, mitzuwirken. Insbesondere hat er Auskünfte zu erteilen, Aufzeichnungen, Bücher, Geschäftspapiere und andere Urkunden zur Einsicht und Prüfung vorzulegen, die zum Verständnis der Aufzeichnungen erforderlichen Erläuterungen zu geben und die Finanzbehörde bei Ausübung ihrer Befugnisse nach § 147 Abs. 6 AO zu unterstützen. Kommt er der Aufforderung zur Erteilung von Auskünften oder zur Vorlage angeforderter Unterlagen im Sinne des § 200 Abs. 1 AO innerhalb einer ihm bestimmten angemessenen Frist nicht nach, kann nach § 146 Abs. 2c AO ein Verzögerungsgeld von 2.500 EUR bis 250.000 EUR festgesetzt werden.
- 8 Zu den Mitwirkungspflichten gehören ferner die **Anzeigepflichten**, die insbesondere in §§ 137–139 AO geregelt sind. Nach § 137 Abs. 1 AO sind dem zuständigen Finanzamt und der für die Erhebung der Realsteuern zuständigen Gemeinde die Gründung, der Erwerb der Rechtsfähigkeit, die Änderung der Rechtsform, die Verlegung der Geschäftsleitung oder des Sitzes und die Auflösung anzuzeigen. Anzeigepflichtig sind nur Steuerpflichtige, die nicht natürliche Personen sind. Die Pflicht zur Anzeige über die Erwerbstätigkeit nach § 138 Abs. 1 AO trifft demgegenüber natürliche wie juristische Personen oder Personenvereinigungen, sofern ein Betrieb eröffnet, verlegt oder aufgegeben wird sowie bei Aufnahme einer freiberuflichen Tätigkeit. Nach § 138 Abs. 1a AO können Unternehmer von der Möglichkeit einer elektronischen Anzeige gegenüber dem für die Umsatzsteuer zuständigen Finanzamt Gebrauch machen. Mit Wirkung zum 1.1.2020 besteht durch die neu gefasste Regelung in § 138 Abs. 1b AO nunmehr eine gesetzliche Pflicht zur Erteilung weiterer Auskünfte, wenn Steuerpflichtige gemäß Abs. 1 Satz 1 bis 3 verpflichtet sind, eine Betriebseröffnung oder Aufnahme einer freiberuflichen Tätigkeit mitzuteilen. Einer gesonderten Aufforderung des Finanzamts hierzu bedarf es nicht mehr. Daneben bestehen nach § 138 Abs. 2 AO Mitteilungspflichten bei der Begründung bestimmter Auslandsengagements (Gründung und Erwerb von Betrieben und Betriebstätten, Beteiligung an ausländischen Personengesellschaften und Beteiligungen an ausländischen Körperschaften, Personenvereinigungen und Vermögensmassen von mindestens 10%, wobei nach Satz 2 unmittelbare und mittelbare Beteiligungen zusammenzurechnen sind, bzw. wenn die Summe der Anschaffungskosten aller Beteiligungen mehr als 150.000 EUR beträgt, in sog. Drittstaaten-Fällen sowie Mitteilung der Art der jeweiligen wirtschaftlichen Tätigkeit im Ausland). Mitteilungen nach den Absätzen 1, 1a und 1b sind innerhalb eines Monats nach dem meldepflichtigen Ereignis zu erstatten (§ 138 Abs. 4 AO). Mitteilungen nach Abs. 2 sind zusammen mit der Einkommensteuer- oder Körperschaftsteuererklärung für den Besteuerungszeitraum, in dem der mitzuteilende Sachverhalt verwirklicht wurde, spätestens jedoch bis zum Ablauf von 14 Monaten nach Ablauf dieses Besteuerungszeitraums, nach amtlich vorgeschriebenem Datensatz über die amtlich bestimmten Schnittstellen zu erstatten (§ 138 Abs. 5 Satz 1 AO). Die Verletzung der Pflicht zur Anzeige von Auslands-

engagements nach § 138 Abs. 2 Satz 1 AO stellt nach § 379 Abs. 2 Nr. 1 AO eine bußgeldbewehrte Steuergefährdung dar. Anzeigepflichten ergeben sich daneben aus den Einzelsteuergesetzen.

Von besonderer Relevanz ist die **Anzeigepflicht nach § 19 GrEStG**. Dabei wird nicht selten übersehen, dass unmittelbare und mittelbare Änderungen des Gesellschafterbstands einer Personengesellschaft, die innerhalb von zehn Jahren zum Übergang von 90 vom Hundert der Anteile am Gesellschaftsvermögen auf neue Gesellschafter geführt haben (§ 19 Abs. 1 Nr. 3a GrEStG), als auch unmittelbare und mittelbare Änderungen des Gesellschafterbstands einer Kapitalgesellschaft, die innerhalb von zehn Jahren zum Übergang von 90 vom Hundert der Anteile der Gesellschaft auf neue Gesellschafter geführt haben (§ 19 Abs. 1 Nr. 3b GrEStG) sowie die Anteilsvereinigung und Anteilsübertragung einer Gesellschaft (§ 19 Abs. 1 Nr. 4–7 GrEStG) die Anzeigepflicht auslösen können, wenn zum Vermögen der Personengesellschaft bzw. der Gesellschaft ein Grundstück gehört. Besonders häufig werden die grunderwerbsteuerlichen Folgen bei internationalen Umstrukturierungen übersehen bei denen der Erwerbsvorgang nach § 1 GrEStG im Ausland ausgelöst wird.¹² Bei Steuersätzen, die je nach Bundesland zwischen 3,5 % und 6,5 % der Bemessungsgrundlage betragen, können bei grunderwerbsteuerlich relevanten Vorgängen schnell hohe Belastungen auf Unternehmen zukommen. Gerade im Konzern, wo es mitunter häufiger zu Umstrukturierungen kommt, sollten die Anteilsbewegungen daher stets genau im Auge behalten werden.¹³

In den letzten Jahren ist zu beobachten, dass es insbesondere im Bereich grenzüberschreitender Steuersachverhalte zu einer Verschärfung von Anzeige- und Dokumentationspflichten gekommen ist, um mehr Transparenz in diesen Fällen zu erreichen.¹⁴ In diesem Zusammenhang wurde im Jahr 2019 eine **Mitteilungspflicht für grenzüberschreitende Steuergestaltungen** eingeführt (§ 138d AO).¹⁵ Hiernach müssen sog. Intermediäre, insbesondere Kreditinstitute, Steuerberater, Rechtsanwälte und Wirtschaftsprüfer, dem Bundeszentralamt für Steuern grenzüberschreitende Steuergestaltungsmodelle mitteilen, die sie konzipiert, organisiert oder verkauft haben.

Zu den für Unternehmen relevanten steuerlichen Pflichten zählen des Weiteren die **Buchführungs- und Aufzeichnungspflichten** (§§ 140–148 AO). Die größte Bedeutung kommt insoweit der Buchführungspflicht für Kaufleute nach §§ 238 ff. HGB zu, die i. V. m. § 140 Abs. 1 AO zu einer steuerrechtlichen Buchführungspflicht wird (sog. derivative Buchführungspflicht). Soweit eine derivative Buchführungspflicht nicht besteht, kann der Steuerpflichtige nach § 141 AO

12 Zur Grunderwerbsteuerhinterziehung durch Anteilsverschiebungen: *Hüschemenger/Zumwinkel*, PStR 2023, 14.

13 *Kamps*, in: Streck/Mack/Schwedhelm, Tax Compliance, Rn. 2.333 ff.

14 *Ditz/Engelen*, DStR 2019, 352.

15 BMF, 29.3.2021 – IV A 3 – S 0304/19/10006 :010; IV B 1 – S 1317/19/10058 :011; DOK 2021/0289747, BStBl. I, 582.

originär buchführungspflichtig sein. Dabei knüpft § 141 AO die Buchführungspflicht für gewerbliche Unternehmen an deren Umsätze und Gewinne. Bücher und Aufzeichnungen sind im Inland zu führen und aufzubewahren (§ 146 Abs. 2 AO). Eine Ausnahme kann nach § 146 Abs. 2a AO auf Antrag bei elektronischer Buchführung bewilligt werden. Ferner enthalten die §§ 140 ff. AO außerdem eine Reihe spezieller Aufzeichnungspflichten. Im engen Zusammenhang mit den Buchführungs- und Aufzeichnungspflichten steht die in § 147 Abs. 1 AO normierte Pflicht zur Aufbewahrung der dort bezeichneten Buchführungsunterlagen (insbesondere Bücher, Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, Handels- und Geschäftsbriefe und Buchungsbelege). Das BMF hat mit Schreiben vom 14.11.2014 seine Auffassung zu den Grundsätzen der ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff zusammengefasst.¹⁶ Das BMF-Schreiben gilt seit dem 1.1.2015 und fordert für jedes Datenverarbeitungssystem eine übersichtlich gegliederte Verfahrensdokumentation, aus der Inhalt, Aufbau, Ablauf und Ergebnisse vollständig und schlüssig ersichtlich sind. Kommt der Steuerpflichtige seinen Buchführungs- und Aufzeichnungspflichten nicht oder nur unvollständig nach, bzw. besteht Anlass zu Zweifeln an der sachlichen Richtigkeit, kann die Finanzverwaltung die Besteuerungsgrundlagen schätzen (§ 162 Abs. 2 Satz 2 AO). Mit Schreiben vom 28.11.2019 hat das BMF eine Neufassung der Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) veröffentlicht, die das bisherige Schreiben ersetzt, allerdings nur punktuelle Änderungen enthält.¹⁷

- 12** Zu den zentralen Pflichten des Steuerpflichtigen gehört ferner die **Pflicht zur Abgabe von Steuererklärungen**. Auch die Steueranmeldung ist eine Steuererklärung, in der aufgrund gesetzlicher Vorschrift die Steuer selbst zu berechnen ist (§ 150 Abs. 1 Satz 3 AO). Die Angaben in Steuererklärungen sind wahrheitsgemäß nach bestem Wissen und Gewissen zu machen (§ 150 Abs. 2 AO). Die Pflicht zur Abgabe von Steuererklärungen bleibt auch dann bestehen, wenn die Finanzverwaltung die Besteuerungsgrundlagen geschätzt hat (§ 149 Abs. 1 Satz 4 AO). Wer zur Abgabe von Steuererklärungen verpflichtet ist, bestimmen die Einzelsteuergesetze (§ 149 Abs. 1 Satz 1 AO). Im Unternehmensbereich sind insbesondere folgende **Steuererklärungspflichten** von Bedeutung:

- Einkommensteuer, § 25 Abs. 3 EStG;
- Einheitliche und gesonderte Gewinnfeststellung, § 181 Abs. 2 AO;
- Körperschaftsteuer, § 31 KStG;
- Gewerbesteuer, § 14a GewStG;
- Umsatzsteuer, § 18 Abs. 1 und 3 UStG;
- Erbschaft- bzw. Schenkungsteuer, § 31 ErbStG;
- Lohnsteuer, § 41a Abs. 1 EStG.

¹⁶ BMF, 14.11.2014 – IV A 4 – S 0316/13/10003, BStBl. I 2014, 1450.

¹⁷ BMF, 28.11.2019 – IV A 4 – S 0316/19/10003, BStBl. I 2019, 1269.

Je nach Branchenzugehörigkeit und Besonderheiten des einzelnen Unternehmens kommen weitere Erklärungsspflichten hinzu (z.B. Anmeldungen nach § 50a EStG, Kapitalertragsteuer-Anmeldungen [§ 45a Abs. 1 EStG], Anmeldungen nach § 48a EStG des Empfängers von Bauleistungen, Versicherungsteuer-Anmeldungen [§ 8 Abs. 1 VersStG], Stromsteuer- und Energiesteuer-Anmeldungen [§ 8 Abs. 1 StromStG, § 8 Abs. 3 EnergieStG]).

Bei der Abgabe von Steuererklärungen und Voranmeldungen sind **gesetzliche Fristen** zu beachten. Steuererklärungen, die sich auf ein Kalenderjahr oder einen gesetzlich bestimmten Zeitpunkt beziehen, sind spätestens sieben Monate nach Ablauf des Kalenderjahres oder sieben Monate nach dem gesetzlich bestimmten Zeitpunkt abzugeben (§ 149 Abs. 2 Satz 1 AO). Bei der Abgabe von Steuererklärungen durch Angehörige der steuerberatenden Berufe sind Steuererklärungen spätestens bis zum letzten Tag des Monats Februar und in den Fällen des Abs. 2 Satz 2 bis zum 31. Juli des zweiten auf den Besteuerungszeitraum folgenden Kalenderjahres abzugeben (§ 149 Abs. 3).¹⁸ Bei Nichtabgabe oder nicht rechtzeitiger Abgabe einer Steuererklärung kann nach § 152 Abs. 1 Satz 1 AO ein Verspätungszuschlag bis zu 25.000 EUR festgesetzt werden. Die Festsetzung liegt grundsätzlich im Ermessen der Finanzbehörde. Allerdings sind seit der Neufassung in Abs. 2 standardisierte Fallgestaltungen geregelt, in denen abweichend von der Grundregelung ein Verspätungszuschlag zwingend festzusetzen ist. Schließlich hat der Steuerpflichtige festgesetzte und fällige Steuern zu zahlen. Die **Fälligkeit** von Ansprüchen aus dem Steuerschuldverhältnis richtet sich nach den Steuergesetzen (§ 220 Abs. 1 AO). Ohne spezielle gesetzliche Regelung über die Fälligkeit wird der Anspruch mit seiner Entstehung fällig, es sei denn, die Finanzbehörde hat eine Zahlungsfrist eingeräumt. Rechtsmittel (Einspruch/Klage) ändern an der Fälligkeit und damit an der Zahlungspflicht nichts. Wird eine festgesetzte Steuer nicht bis zum Ablauf des Fälligkeitstages entrichtet, so ist nach § 240 Abs. 1 Satz 1 AO für jeden angefangenen Monat der Säumnis ein Säumniszuschlag von 1 % des rückständigen Steuerbetrags zu entrichten. Gleiches gilt für zurückzuzahlende Steuervergütungen (§ 240 Abs. 1 Satz 2 AO). Der Säumniszuschlag entsteht kraft gesetzlicher Anordnung mit Ablauf des Fälligkeitstages. Die Vollziehbarkeit eines Steuerbescheids wird nur beseitigt, wenn die Finanzbehörde (auf Antrag) die **Aussetzung der Vollziehung** anordnet (§ 361 AO) oder eine Stundung (§ 222 AO) gewährt. Wird die Aussetzung der Vollziehung angeordnet und die Steuerforderung später nicht aufgehoben, sind Aussetzungszinsen (§ 237 AO) in Höhe von 6 % per anno zu leisten (§ 238 AO). Verfügt der Steuerpflichtige über die zur Begleichung der Steuern erforderliche Liquidität, ist insbesondere in Niedrigzinsphasen häufig empfehlenswert, die streitige Steuer zunächst zu zahlen. Bei einem erfolgreichen Ausgang des

¹⁸ Bedingt durch die Corona-Pandemie wurden die Abgabefristen für Steuererklärungen der VZ 2019 bis 2024 verlängert. Ab VZ 2025 gelten wieder die regulären Fristen. Vgl. hierzu das BMF-Schreiben vom 23.6.2022 (IVA 3 – S 0261/20/10001:018, BStBl. I 2022, 938) aufgrund des Vierten Corona-Steuerhilfegesetzes.

Rechtsbehelfsverfahrens kann der Steuerpflichtige dann selbst einen Zinsanspruch gegenüber dem Fiskus geltend machen (§§ 233a, 236 AO).

- 15 Die Zinssatzhöhe für die **Verzinsung von Steuernachforderungen** nach § 233a AO hat sich in Folge einer Entscheidung des BVerfG¹⁹ geändert. Darin wurde die Verfassungswidrigkeit der bestehenden Regelungen zur Verzinsung von Steuernachzahlungen und -erstattungen (Vollverzinsung, §§ 233a, 238 AO) ab dem Verzinsungszeitraum 2014 festgestellt (bis dahin: 0,5 % pro Monat). Daraufhin hat der Gesetzgeber den Zinssatz für die Verzinsung von Steuernachforderungen nach § 233a AO für die Verzinsungszeiträume ab dem 1.1.2019 auf **0,15 % pro Monat** reduziert (§ 238 Abs. 1a AO). Die Absenkung des Zinssatzes betrifft sowohl Nachzahlungs- als auch Erstattungszinsen nach § 233a AO, nicht aber Stundungs-, Hinterziehungs-, Prozess- oder Aussetzungszinsen (§§ 234 bis 237 AO). Weitergehende Präzisierungen hat das Bundesfinanzministerium in zwei BMF-Schreiben vom 22.7.2022 veröffentlicht.²⁰

2. Spezifische materiell-rechtliche Problemschwerpunkte

a) Lohnsteuer und Sozialabgaben

- 16 Der Arbeitgeber ist zur fristgemäßen **Anmeldung und Abführung der LohnSt** verpflichtet (§ 41a EStG). LohnSt-Anmeldungszeitraum ist grundsätzlich der Kalendermonat. In diesem Fall hat die Anmeldung und Abführung der LohnSt spätestens am zehnten Tag des Folgemonats zu erfolgen. Gleichzeitig ist der Arbeitgeber zur Abführung des Gesamtsozialversicherungsbeitrags verpflichtet. Bei der LohnSt handelt es sich um eine besondere Erhebungsform der ESt des Arbeitnehmers (§ 38 Abs. 1 Satz 1 EStG). Insoweit wird der Arbeitgeber als Dritter in das Besteuerungsverfahren einbezogen, was mit einem umfänglichen Verwaltungsaufwand für den Arbeitgeber verbunden ist. Es ist jedoch davor zu warnen, als Arbeitgeber der LohnSt keine hinreichende Beachtung zu schenken. Einerseits sind gerade in größeren Unternehmen massenhaft Sachverhalte lohnsteuerrechtlich zu würdigen, andererseits ist die LohnSt (insbesondere § 37b EStG) besonders fehleranfällig. Zudem haftet der Arbeitgeber nach § 42d EStG für die einzubehaltende und abzuführende LohnSt, was zu einem erheblichen Kostenfaktor führen kann. Zwar ist in diesem Fall ein Regress bei dem Arbeitnehmer dem Grunde nach möglich, doch ist dieser häufig nicht durchsetzbar. Bei der LohnSt besteht ferner ein latentes Strafbarkeitsrisiko, da bereits die verspätete Abgabe einer LohnSt-Anmeldung eine vollendete Steuerhinterziehung (auf Zeit) begründen kann (siehe hierzu → Rn. 49). Eine funktionierende Fristenkontrolle ist aus diesem Grunde unabdingbar. Hinzu kommt, dass eine fehlerhafte Anmeldung der LohnSt sich regelmäßig in einer fehlerhaften Berechnung der Sozialabgaben fortsetzt.

19 BVerfG, 8.7.2021 – 1 BvR 2237/14, 1 BvR 2422/17, DStR 2021, 1934.

20 BMF, 22.7.2022 – IV A 3 – S 1910/22/10040 :010, DOK 2022/0666774, DStR 2022, 1555; BMF, 22.7.2022 – IV A 3 – S 0338/19/10004 :007, DOK 2022/0668147, DStR 2022, 1614.

Besonders sensible Bereiche sind erfahrungsgemäß Sachbezüge, Spesen, Aus-
hilfen, freie Mitarbeiter und Subunternehmer.²¹ Insbesondere bei der Beauftra-
gung von – vermeintlich selbstständigen – freien Mitarbeitern und Subunterneh-
mern stellt sich häufig die Frage, ob diese nicht in einer Weise in den Betrieb des
Unternehmens eingegliedert sind, dass sie tatsächlich als abhängig beschäftigt
anzusehen sind (**Scheinselbstständigkeit**). Eine Scheinselbstständigkeit führt
regelmäßig zu sozialversicherungsrechtlichen (Nachentrichtung von Sozialver-
sicherungsbeiträgen, ggf. Säumniszuschläge), steuerrechtlichen (Haftungsan-
spruchnahme nach § 42d EStG, Rückerstattung eines etwaigen Vorsteuerabzugs
aus Rechnungen des vermeintlichen Auftragnehmers), arbeitsrechtlichen (Be-
gründung eines Arbeitsverhältnisses mit der Folge der Anwendbarkeit des
KSchG, des BUrlG, des EFZG sowie der einschlägigen Tarifverträge und Be-
triebsvereinbarungen) sowie straf- bzw. bußgeldrechtlichen (§§ 370, 378, 380
AO, § 266a StGB) Konsequenzen. Bisher waren dabei Taten nach § 266a StGB²²
faktisch unverjährbar, weil nach gefestigter Rechtsprechung die Verjährung erst
mit Erlöschen der Beitragspflicht beginnt. Resultat dieser Rechtsprechung war
ein eklatantes Auseinanderfallen der Verjährungsfristen von Taten nach § 266a
StGB und einer regelmäßig mitverwirklichten Steuerhinterziehung. Nunmehr
hat der 1. Strafsenat mit Anfragebeschluss²³ vom 13.11.2019 – unter Aufgabe
seiner bisherigen Rechtsprechung – dargelegt, dass seiner Auffassung nach die
Verjährungsfrist bei Taten gemäß § 266a Abs. 1 und Abs. 2 Nr. 2 StGB mit dem
Verstreichenlassen des Fälligkeitszeitpunktes beginnt. Inzwischen haben sich
sowohl der 3. wie auch der 5. Strafsenat dieser Auffassung angeschlossen.²⁴ Das
Sozialversicherungsrecht bietet die Möglichkeit der Durchführung eines sog.
Statusfeststellungsverfahrens (§ 7a SGB IV), um Rechtssicherheit hinsichtlich
des sozialversicherungsrechtlichen Status zu erlangen.

b) Umsatzsteuer

Neben der LohnSt stellt die USt für Unternehmen regelmäßig den größten steu-
erlichen Risikobereich dar.²⁵ Da sie zusammen mit der LohnSt den überwiegen-
den Teil des Steueraufkommens ausmacht, ist sie Prüfungsschwerpunkt der

21 Siehe zu empfohlenen Melde- und Berichtspflichten an die für die Lohnsteuer zuständige
Abteilung → Rn. 68.

22 Nach neuerer Rechtsprechung des BGH muss der Täter seine Stellung als Arbeitgeber und
die daraus resultierende sozialversicherungsrechtliche Abführungspflicht zumindest für
möglich halten und deren Verletzung billigend in Kauf nehmen. Eine Fehlvorstellung über
die Arbeitgebereigenschaft und die daraus folgende Abführungspflicht sind als Tatbestands-
irrtum im Sinne von § 16 Abs. 1 Satz 1 StGB einzuordnen, BGH, 24.9.2019 – 1 StR 346/18,
NSStZ 2020, 89.

23 BGH, 13.11.2019 – 1 StR 58/19, NSStZ 2020, 159.

24 BGH, 6.2.2020 – 5 ARs 1/20, BeckRS 2020, 2837; BGH, 4.2.2020 – 3 ARs 1/20, BeckRS
2020, 3029.

25 Vertiefend hierzu Gehring, CCZ 2019, 197.

Finanzverwaltung und Gegenstand gesonderter Außenprüfungen (USt-Sonderprüfung). Der Unternehmer hat jährlich USt-Jahreserklärungen abzugeben sowie nach § 18 UStG monatliche oder vierteljährliche Voranmeldungen zu erklären und Vorauszahlungen zu leisten. Die USt-Voranmeldung steht einem Steuerbescheid unter Vorbehalt der Nachprüfung gleich (§ 168 Satz 1 AO). Aufgrund der Vielzahl von Einzelumsätzen sind größere Unternehmen oft nur schwerlich in der Lage, die Voranmeldungen innerhalb der gesetzlichen Frist einzureichen. Um die Umsätze und Vorsteuern zutreffend und fristgemäß erklären zu können, ist daher ein effektiver Informationsfluss im Unternehmen sicherzustellen. Ist dies gleichwohl nicht möglich, ist eine **sachgerechte Schätzung** vorzunehmen. Diese darf jedoch nicht bewusst zu niedrig vorgenommen werden, da eine vorsätzlich zu niedrige Schätzung grundsätzlich den Tatbestand der Steuerhinterziehung erfüllt.

- 19 Ein besonderes Augenmerk sollte zudem auf die steuerliche Behandlung von **Eingangs- und Ausgangsrechnungen** gelegt werden, zumal hierüber üblicherweise nicht in der Steuerabteilung, sondern in der betroffenen Fachabteilung bzw. im Rechnungswesen entschieden wird. Nach § 15 Abs. 1 Satz 1 Nr. 1 Satz 2 UStG setzt die Ausübung des Vorsteuerabzugs voraus, dass das Unternehmen eine nach §§ 14, 14a UStG ausgestellte, ordnungsgemäße Rechnung besitzt. Eingangsrechnungen sind daher sorgfältig auf die Einhaltung der gesetzlichen Rechnungsanforderungen zu prüfen. Nach § 14c UStG schuldet der Unternehmer die unrichtig oder unberechtigt in einer Ausgangsrechnung ausgewiesene USt. Die zutreffende umsatzsteuerrechtliche Behandlung von Rechnungen hängt darüber hinaus von einer Vielzahl materiell-rechtlicher Fragen ab. Insbesondere kann bisweilen die Unternehmereigenschaft des Geschäftspartners nach § 2 Abs. 1 UStG fraglich sein. Bei grenzüberschreitenden Sachverhalten stellt sich ferner häufig die Frage, wo der Ort der Leistung im Sinne der §§ 3 ff. UStG liegt. Besondere Kenntnisse erfordert auch die zutreffende Anwendung des sog. Reverse Charge-Verfahrens nach § 13b USt (Leistungsempfänger als Steuerschuldner). Insoweit ist es ratsam, die Steuerabteilung in den Prozess der Bearbeitung von Eingangs- und Ausgangsrechnungen einzubeziehen, wobei dies aus verfahrensökonomischen Gründen auf Rechnungen ab einem – unternehmensintern festzulegenden – Rechnungsbetrag begrenzt werden kann. Ebenfalls sind Leitfäden über die zutreffende (umsatz-)steuerliche Behandlung von Eingangs- und Ausgangsrechnungen anzuraten.

c) Verdeckte Gewinnausschüttungen

- 20 Bei Kapitalgesellschaften stellen verdeckte Gewinnausschüttungen (§ 8 Abs. 3 Satz 2 KStG) an die Gesellschafter oder diesen nahestehende Personen einen besonderen Problemkreis dar. Eine verdeckte Gewinnausschüttung setzt eine Vermögensminderung oder verhinderte Vermögensmehrung voraus, die durch das Gesellschaftsverhältnis veranlasst ist, nicht auf einer offenen Gewinnausschüttung beruht und sich auf den Unterschiedsbetrag im Sinne des § 4 Abs. 1 Satz 1

EStG i.V.m. § 8 Abs. 1 Satz 1 KStG auswirkt.²⁶ Dabei muss diese Unterschiedsbetragsminderung die objektive Eignung haben, beim Gesellschafter einen sonstigen Bezug im Sinne des § 20 Abs. 1 Nr. 1 Satz 2 EStG auszulösen. Der BFH nimmt eine Veranlassung im Gesellschaftsverhältnis regelmäßig an, wenn die Kapitalgesellschaft ihrem **Gesellschafter einen Vermögensvorteil zuwendet**, den sie bei Anwendung der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters einem Nichtgesellschafter nicht gewährt hätte. Kriterien im Rahmen dieses sog. Fremdvergleichs sind u. a. die Üblichkeit und die Angemessenheit der Zuwendung an den Gesellschafter bzw. die nahestehende Person. Besondere Anforderungen gelten für Verträge mit beherrschenden Gesellschafter-Geschäftsführern. Gegenstand einer verdeckten Gewinnausschüttung kann **jeder geldwerte Vorteil** sein (z.B. Nutzungsüberlassung, Gewährung eines uneinbringlichen Darlehens, Verzicht auf Geltendmachung von Forderungen, Lizenzgebühren, unangemessene Höhe des Geschäftsführergehalts). Aus Compliance-Sicht sind die Gründe zu dokumentieren, die zur Beurteilung der Zuwendung als angemessen geführt haben. Verdeckte Gewinnausschüttungen mindern das Einkommen nicht (§ 8 Abs. 3 Satz 2 KStG), sodass eine – außerbilanzielle – Hinzurechnung zum Einkommen der Körperschaft erfolgt. Bei dem Gesellschafter wird die verdeckte Gewinnausschüttung den Einkünften aus Kapitalvermögen zugerechnet. Ein strafrechtlicher Vorwurf kann daher sowohl auf Hinterziehung von Körperschaftsteuer zugunsten der Gesellschaft als auch auf Hinterziehung von Einkommensteuer zugunsten des Gesellschafters gerichtet sein.²⁷

d) Anzeigepflicht nach § 153 AO

Steuererklärungen von Unternehmen sind aufgrund der Vielschichtigkeit, der Komplexität sowie der schieren Masse der zu betrachtenden Geschäftsvorfälle in hohem Maße fehleranfällig. Daher ist die Anzeige- und Berichtigungspflicht nach § 153 AO von **erheblicher praktischer Relevanz**.²⁸ Erkennt ein Steuerpflichtiger nachträglich vor Ablauf der Festsetzungsfrist, dass eine von ihm oder für ihn abgegebene Erklärung unrichtig oder unvollständig ist und dass es dadurch zu einer Verkürzung von Steuern kommen kann oder bereits gekommen ist, so ist er nach § 153 Abs. 1 Satz 1 AO dazu verpflichtet, dies unverzüglich anzuzeigen und die erforderliche Richtigstellung vorzunehmen.²⁹ Diese Verpflichtung trifft nach § 153 Abs. 1 Satz 2 AO auch die nach §§ 34, 35 AO für den Steuerpflichtigen handelnden Personen, mithin insbesondere den Geschäftsfüh-

21

26 BFH, 5.3.2008 – I R 45/07, DStRE 2008, 1138; BFH, 15.3.2023 – I R 41/19, DStR 2023, 1307.

27 Zu verdeckten Gewinnausschüttungen und Steuerstrafrecht: *Madauß*, ZWH 2019, 44; *Heuel/Matthey*, AO-StB 2018, 54 und 89.

28 In den AEAO wurde durch Schreiben des BMF, 23.5.2016 – IV A 3 – S 0324/15/10001, BStBl. I 2016, 490 erstmals eine Regelung zu § 153 AO eingefügt. Hierzu *Schwartz/Höpfner*, PStR 2016, 210.

29 Vgl. zu § 153 AO: *Wulf*, Stbg 2010, 295; *Schauf/Schwartz*, PStR 2015, 248.

rer einer GmbH oder den Vorstand einer AG. Von § 35 AO kann aber auch ein Prokurist erfasst sein, wenn zu seinem Pflichtenkreis die Wahrnehmung der steuerlichen Pflichten des Geschäftsherrn gehört (z. B. Leiter Steuerabteilung). Die Anzeigepflicht besteht nach § 153 Abs. 2 AO ferner, wenn die Voraussetzungen für eine Steuerbefreiung, eine Steuerermäßigung oder eine sonstige Steuervergünstigung nachträglich ganz oder teilweise wegfallen. Entfällt bspw. durch eine nachträgliche Option (§ 9 UStG) die USt-Befreiung, ist der Steuerpflichtige zur Anzeige verpflichtet. Die Verletzung der Anzeigepflicht kann eine Steuerhinterziehung durch Unterlassen begründen.

- 22 § 153 AO setzt u. a. voraus, dass der Steuerpflichtige die Unrichtigkeit oder Unvollständigkeit der abgegebenen Erklärung positiv erkennt. Ein bloßes Erkennenmüssen oder Erkennenkönnen genügt nicht.³⁰ Eine Pflicht zur ständigen Überwachung der Rechtsprechungs- und Verwaltungsauffassung für in Betracht kommende Rechtsprobleme bis zum Eintritt der Festsetzungsverjährung beinhaltet § 153 AO ebenfalls nicht.³¹ Auch gibt § 153 AO dem Steuerpflichtigen grundsätzlich nicht auf, nach Unrichtigkeiten zu suchen.³² Entscheidet sich ein Unternehmen gleichwohl – etwa um seine Steuerrisiken zu kennen – für eine interne Überprüfung bestimmter Sachverhalte, muss den Verantwortlichen zuvor klar sein, dass die dadurch gewonnenen Erkenntnisse die Anzeigepflicht nach § 153 AO begründen können. Nach der Rechtsprechung des BGH besteht die Anzeigepflicht nach § 153 AO auch dann, wenn der Steuerpflichtige die Unrichtigkeit seiner Angaben bei Abgabe der Steuererklärung nicht gekannt, aber billigend in Kauf genommen hat und später zu der sicheren Erkenntnis gelangt ist, dass die Angaben unrichtig sind.³³ Die Unrichtigkeit oder Unvollständigkeit muss vor Ablauf der Festsetzungsfrist erkannt werden. Wird der Fehler erst danach erkannt, muss demnach keine Anzeige mehr erfolgen. Die **steuerliche Festsetzungsfrist** beträgt regelmäßig vier (§ 169 Abs. 2 Satz 1 Nr. 2 AO), im Fall der leichtfertigen Verkürzung fünf (§ 169 Abs. 2 Satz 2 AO) und im Fall der vorsätzlichen Steuerhinterziehung (Eventualvorsatz ausreichend) zehn Jahre (§ 169 Abs. 2 Satz 2 AO).

- 23 In der Rechtsfolge verpflichtet § 153 AO zunächst zur **unverzüglichen** Anzeige gegenüber der Finanzverwaltung (1. Stufe) und sodann zur Berichtigung der unrichtigen oder unvollständigen Angaben (2. Stufe). Für die Berichtigung sieht das Gesetz keine zeitliche Frist vor. Eine Fristsetzung kann durch die Finanzverwaltung vorgenommen werden. Wird durch die Finanzverwaltung keine Frist gesetzt, hat die Berichtigung in einer angemessenen Zeit zu erfolgen. Die Umstände im Einzelfall sind zu berücksichtigen. Aufgrund des hohen Risikos bei verspäteter Berichtigung ist es empfehlenswert, die benötigte Zeit mit den Be-

30 Rätke, in: Klein, Abgabenordnung, § 153 AO Rn. 10; BGH, 17.3.2009 – 1 StR 479/08, NJW 2009, 1984; BMF, 23.5.2016 – IV A 3 – S 0324/15/10001, BStBl. I 2016, 490.

31 FG Düsseldorf, 26.3.2014 – 7 K 1884/13, BeckRS 2014, 95257.

32 Seer, in: Tipke/Kruse, AO/FGO, Stand: 177. EL, § 153 AO Rn. 16.

33 BGH, 17.3.2009 – 1 StR 479/08, NJW 2009, 1984.

hören abzustimmen, falls der Sachverhalt komplex ist und die benötigte Zeit zur Aufarbeitung nicht genau voraussehbar ist. Rechtsunsicherheiten bestehen aber auch über den genauen Zeitpunkt bzw. die Zeitspanne, die den Verantwortlichen auf der 1. Stufe verbleibt, bis die unverzügliche Anzeige bei der Finanzverwaltung eingehen muss. Nach h. M. stimmt der Unverzüglichkeitsbegriff des § 153 AO mit dem des § 121 Abs. 1 BGB überein und meint, ohne schuldhaftes Zögern, alsbald nach Erkennen des Mangels. Die zur Verfügung stehende Zeitspanne hängt von den Umständen des Einzelfalls ab, namentlich davon, ob eine Korrektur des Fehlers komplizierte Berechnungen erfordert oder ob die einfache Mitteilung einer einzelnen Tatsache dem Zweck der Anzeige genügt. Jedenfalls sollte dem Steuerpflichtigen die Zeit des Abwartens zuzubilligen sein, die zur Verschaffung eines Überblickes über den Sachverhalt sowie einer hinreichenden Klärung der Rechtsfrage – ggf. durch Hinzuziehung externer Berater – in der jeweiligen Situation erforderlich erscheint. In der Praxis werden Zeiträume zwischen zwei und sechs Wochen (abhängig von der Fallgestaltung) in der Regel als unverzüglich angesehen. Die Anzeige ist gegenüber der sachlich und örtlich zuständigen Finanzbehörde zu erstatten. Jedoch ist die Anzeige auch bei der Übermittlung an ein unzuständiges Finanzamt als erstattet anzusehen, sodass auch in diesem Fall die Pflicht des § 153 AO erfüllt ist.³⁴

Durch das DAC7-Umsetzungsgesetz vom 20.12.2022³⁵ wurde **§ 153 Abs. 4 AO** **24 neu** in das Gesetz eingefügt. Die Regelung ist erstmals anwendbar für Steuern und Steuervergütungen, die nach dem 31.12.2024 entstehen sowie für solche, die zwar vor dem 1.1.2025 entstehen, für die aber nach dem 31.12.2024 eine Prüfungsanordnung bekanntgegeben worden ist. Nach § 153 Abs. 4 AO besteht eine Anzeige- und Berichtigungspflicht, wenn **Prüfungsfeststellungen einer Außenprüfung** unanfechtbar in einem Steuerbescheid, einem Feststellungsbescheid nach § 180 Abs. 1 Satz 1 Nr. 2 AO oder einem Teilabschlussbescheid nach § 180 Abs. 1a AO umgesetzt worden sind und die den Prüfungsfeststellungen zugrunde liegenden Sachverhalte auch in einer anderen vom oder für den Steuerpflichtigen abgegebenen Erklärung, die nicht Gegenstand der Außenprüfung war, zu einer Änderung der Besteuerungsgrundlagen führt. Die Vorschrift wird bereits jetzt in der Literatur kontrovers diskutiert, da der Gesetzeswortlaut zu zahlreichen Auslegungsfragen führt.³⁶ Ungeklärt ist die grundlegende Frage, ob der Gesetzgeber durch die Einführung des neuen Absatz 4 eine Spezialregelung für BP-Feststellungen schaffen wollte oder ob Absatz 4 neben die bestehende Anzeige- und Berichtigungspflicht nach Absatz 1 tritt. Während eine vorrangige Anwendbarkeit des Absatz 4 als *lex specialis* für BP-Feststellungen den maßgeblichen Zeitpunkt für das Entstehen der Anzeige- und Berichtigungspflicht auf die Bestandskraft der jeweiligen Bescheide verlagert, kann eine Anzeige- und

34 BFH, 28.2.2008 – VI R 62/06, NJW 2008, 2527; Rätke, in: Klein, Abgabenordnung, § 153 AO Rn. 27.

35 BGBl. 2022 I, S. 2730.

36 Stürzl/Forster, GmbH-Steuerpraxis 1/2024, 8; Wulf/Görlich, PStR 2023, 40; Krumm, Ubg 2023, 284; Beckschäfer/Neuhaus, NZWiSt 2023, 328; Gude, DStR 2023, 2261.

Berichtigungspflicht nach Absatz 1 deutlich früher entstehen. Darüber hinaus ist der Umfang der Anzeige- und Berichtigungspflicht nach Absatz 4 ungeklärt. Unstreitig umfasst sind konkret-individuelle Dauersachverhalte, wie zum Beispiel die Korrektur der anzusetzenden Nutzungsdauer bzgl. der Abschreibung eines Wirtschaftsgutes, wenn diese auch in einer anderen abgegebenen Steuererklärung, die nicht Gegenstand der Außenprüfung war, zu einer Änderung der Besteuerungsgrundlagen führen. Zum Teil wird die Ansicht vertreten, dass § 153 Abs. 4 AO auch gleichgelagerte oder vergleichbare Sachverhalte erfasst. Dies wäre beispielsweise der Fall, wenn von der Betriebsprüfung aufgegriffene Geschäftsmodelle auch mit anderen Vertragspartnern umgesetzt wurden. Aufgrund der bestehenden Rechtsunsicherheiten sollte im Blick gehalten werden, wie sich die Finanzverwaltung und die Rechtsprechung zukünftig zu § 153 Abs. 4 AO positionieren. Ferner erscheint es ratsam, den **Umgang mit § 153 Abs. 4 AO künftig im Rahmen der Schlussbesprechung proaktiv anzusprechen**. Zudem kann angeregt werden, im Prüfbericht zu dokumentieren, dass bzgl. konkreter Prüfungsfeststellungen keine Fortschreibungspflicht für Folgejahre besteht. Ein strafrechtlich relevantes Handeln kann dadurch ausgeschlossen werden. Dies gilt im Grundsatz auch dann, falls die Veranlagungsstelle später zu einer abweichenden Bewertung gelangen sollte.

e) Tochtergesellschaften und Betriebstätten im Ausland

- 25** Bei international operierenden Unternehmen ist der Gründung von Tochtergesellschaften und Betriebstätten im Ausland unter steuerlichen Aspekten besondere Aufmerksamkeit zu widmen, weshalb die Steuerabteilung stets frühzeitig einbezogen werden sollte. Bei der Gründung von **Tochtergesellschaften im Ausland** stellt sich die Frage, wo diese steuerpflichtig sind. Unbeschränkt körperschaftsteuerpflichtig im Inland ist eine Kapitalgesellschaft, die ihre Geschäftsleitung oder ihren Sitz im Inland hat (§ 1 Abs. 1 Nr. 1 KStG). Auch wenn sich der statutarische Sitz (§ 11 AO) der Tochtergesellschaft im Ausland befindet, kann die Gesellschaft gleichwohl allein aufgrund der faktischen Gegebenheiten den Ort ihrer Geschäftsleitung im Sinne des § 10 AO (Mittelpunkt der geschäftlichen Oberleitung) im Inland haben. Wird der maßgebliche Wille der Auslandstochter in der Konzernzentrale in Deutschland gebildet, hat die Gesellschaft hier den Ort ihrer Geschäftsleitung, auch wenn „pro forma“ am Sitz der Gesellschaft ein Geschäftsführer bestellt ist. Ferner ist die steuerliche Anerkennung von Auslandsgesellschaften zu versagen, wenn für ihre Errichtung wirtschaftliche oder sonst beachtliche Gründe fehlen (§ 42 AO), sodass die Einkünfte direkt bei der Muttergesellschaft im Inland zu besteuern sind. Daneben besteht bei sog. funktionsschwachen Gesellschaften mit Sitz im niedrig besteuerten Ausland das Risiko der Hinzurechnungsbesteuerung nach §§ 7ff. AStG.
- 26** **Betriebstätte** ist nach § 12 Satz 1 AO jede feste Geschäftseinrichtung oder Anlage, die der Tätigkeit eines Unternehmens dient (insbesondere Zweigniederlas-

sungen). Es handelt sich somit weder um eine eigenständige Rechtspersönlichkeit noch um ein eigenständiges Steuersubjekt. Das Vorhandensein einer Betriebsstätte im Ausland führt jedoch regelmäßig dazu, dass über die Betriebsstätte erzielte Gewinne im Ausland der Besteuerung unterliegen (vgl. Art. 5 Abs. 1 i. V. m. Art. 7 OECD-Musterabkommen) und im Inland von der Besteuerung ausgenommen sind bzw. eine Anrechnung der ausländischen Steuer auf die deutsche KSt erfolgt.³⁷ Dies macht eine Allokation der Einkünfte entweder zu der Betriebsstätte oder zum Stammhaus erforderlich. Die Betriebsstätten-Gewinnermittlung ist eine äußerst komplexe Materie, die besondere Kenntnisse im internationalen Steuerrecht voraussetzt. Sofern Aufgaben der Betriebsstätten-Gewinnermittlung von Mitarbeitern der Betriebsstätte ausgeführt werden, bestehen besondere Anforderungen an die Aufsichts- und Überwachungspflichten der Gesellschaft, da der Betriebsättengewinn unmittelbare Auswirkung auf das steuerliche Ergebnis der Gesellschaft im Inland hat.

f) Internationale Verrechnungspreise

§ 1 Abs. 3 AStG enthält nähere Vorgaben zur Ermittlung der im Rahmen des Fremdvergleichs (§ 1 Abs. 1 Satz 1 AStG) steuerlich anzusetzenden internationalen Verrechnungspreise. In § 90 Abs. 3 AO sind entsprechende Dokumentationspflichten geregelt. Verstöße gegen diese Pflichten führen dazu, dass nach § 162 Abs. 3 Satz 1 AO widerlegbar vermutet wird, dass der Steuerpflichtige im Inland höhere als die von ihm erklärten Einkünfte hatte. Darüber hinaus sind Zuschläge nach § 162 Abs. 4 AO festzusetzen, sodass der ordnungsgemäßen und fristgemäßen Dokumentation besondere Aufmerksamkeit zu widmen ist. Im Zusammenhang mit unangemessenen Verrechnungspreisen wurden zuletzt vermehrt auch strafrechtliche Ermittlungsverfahren eingeleitet, wobei die besondere Problematik darin besteht, dass es regelmäßig mehrere denkbare Verrechnungspreise gibt.³⁸ Kann der Steuerpflichtige anhand einer ordnungsgemäßen Dokumentation über die Überlegungen zur Ermittlung der Verrechnungspreise eine vertretbare Vorgehensweise darlegen, dürfte es angesichts der Unwägbarkeiten der Verrechnungspreis-Ermittlung regelmäßig am Vorsatz fehlen.

g) Versagung des Betriebsausgabenabzugs nach § 160 AO

Insbesondere für international tätige Unternehmen ist die Regelung des § 160 AO von besonderer Bedeutung. Danach sind Betriebsausgaben steuerlich regelmäßig nicht zu berücksichtigen, wenn der Steuerpflichtige dem Verlangen der Finanzbehörde nicht nachkommt, die **Gläubiger oder Empfänger genau zu benennen**. Die Vorschrift will dafür Vorsorge treffen, dass Ausgaben nur dann bei

³⁷ Die Frage, welche Anforderungen an das Bestehen einer Betriebsstätte im Ausland zu stellen sind, war insbesondere auch bei den Verfahren zu den sog. Goldfinger-Modellen von Bedeutung.

³⁸ Zur Steuerhinterziehung durch unangemessene Verrechnungspreise, *Peters/Pflaum*, wistra 2011, 250.

einem Steuerpflichtigen steuermindernd wirken, wenn die ihnen korrespondierenden Einnahmen bei dessen Geschäftspartner der (deutschen) Besteuerung unterworfen werden. Voraussetzung ist zunächst ein konkretes Benennungsverlangen der Finanzbehörde.³⁹ Dabei ist der wahre Empfänger (d. h. der wirtschaftliche Zahlungsempfänger) zu benennen. Problematisch ist dies bei Geschäftsbeziehungen mit sog. ausländischen Domizil- und Briefkastengesellschaften ohne eigene wirtschaftliche Betätigung. Wird eine solche Domizilgesellschaft oder ein Treuhänder zwischengeschaltet, sind nicht diese der Empfänger im Sinne des § 160 AO, sondern der dahinter stehende Dritte, der eigentlich die Leistung erbracht hat, die bezahlt wurde.⁴⁰ Benannt ist ein Empfänger, wenn er nach Namen und Adresse ohne Schwierigkeiten und eigene Ermittlungen der Finanzbehörde bestimmt und ermittelt werden kann. Erweisen sich die eingeholten Einkünfte als falsch, wirkt dies zulasten des Steuerpflichtigen, sodass er sich Gewissheit über die Richtigkeit der ihm erteilten Angaben verschaffen muss. Dies kann bspw. durch die Anforderung von offiziellen Dokumenten des Geschäftspartners (Registerauszüge, amtliche Bescheinigungen, Ausweiskopien) erfolgen. Ab bestimmten zu definierenden Grenzwerten kann auch der persönliche Besuch in den Geschäftsräumen des Geschäftspartners ein probates Mittel sein. Daneben können über eine Anfrage bei einer deutschen Außenhandelskammer weitere Informationsquellen erlangt werden. Wer dagegen mit seinem Geschäftspartner ausschließlich über Telefon, Fax und E-Mail korrespondiert, hat keine Gewissheit, ob die ihm erteilte Rechnungsanschrift zutrifft.

- 29 Kann der Steuerpflichtige dem Benennungsverlangen nicht entsprechen, wird der **Betriebsausgabenabzug ganz oder teilweise versagt**. Über die Höhe des zu versagenden Ausgabenabzugs hat die Finanzbehörde eine Ermessensentscheidung zu treffen. Da die Sicherung des deutschen Steuersubstrats Zweck des § 160 AO ist, soll nach AEAO zu § 160 Nr. 4 bei Zahlungen an ausländische Empfänger – soweit keine Anhaltspunkte für eine straf- oder bußgeldbewehrte Vorteilszuwendung vorliegen – auf den Empfängernachweis nach § 160 AO verzichtet werden, wenn feststeht, dass die Zahlung im Rahmen eines üblichen Handelsgeschäfts erfolgte, der Geldbetrag ins Ausland abgeflossen ist und der Empfänger nicht der deutschen Steuerpflicht unterliegt. Hierzu ist der Empfänger in dem Umfang zu bezeichnen, dass dessen Steuerpflicht im Inland mit hinreichender Sicherheit ausgeschlossen werden kann. Die bloße Möglichkeit einer im Inland nicht bestehenden Steuerpflicht reicht indes nicht aus.⁴¹

h) Betriebsausgabenabzugsverbot nach § 4 Abs. 5 Satz 1 Nr. 10 EStG

- 30 § 4 Abs. 5 Satz 1 Nr. 10 EStG enthält ein Betriebsausgabenabzugsverbot für Schmier- und Bestechungsgelder.⁴² Im Rahmen der steuerlichen Betriebsprüfun-

39 BFH, 16.5.2013 – X B 131/12, BFH/NV 2013, 1260.

40 BFH, 1.4.2003 – I R 28/02, DStR 2003, 1340.

41 BFH, 13.3.1985 – I R 7/81, BStBl. II 1986, 318.

42 Vgl. hierzu umfassend *Schauf/Idler*, Ubg 2010, 111; *Pelz*, DStR 2014, 449.

gen werden Aufwandskonten regelmäßig auf Anhaltspunkte für Aufwendungen geprüft, die im Zusammenhang mit rechtswidrigen Handlungen von Korruptionstaten stehen. Dabei stellen **Provisions-, Vermittlungs- und Beratungsaufwendungen** erfahrungsgemäß Prüfungsschwerpunkte dar, wobei nicht abzugsfähige Aufwendungen durch vielfältige Möglichkeiten verborgen werden können. Die steuerliche Abzugsfähigkeit von Provisionszahlungen ist nur dann gegeben, wenn tatsächlich eine Leistung erbracht wurde, die durch die Provision angemessen vergütet wurde, der Provisionsempfänger eindeutig benannt werden kann und nachgewiesen wird, dass dieser die Provision tatsächlich erhalten hat. Insoweit ist dringend eine hinreichende Dokumentationslage zu schaffen. Das Abzugsverbot gilt für die Zuwendung von Vorteilen sowie damit zusammenhängende Aufwendungen, wenn die Zuwendung der Vorteile eine rechtswidrige Handlung darstellt, die den Tatbestand eines Strafgesetzes oder eines Gesetzes verwirklicht, das die Ahndung mit einer Geldbuße zulässt. Die lange Zeit umstrittene Frage, ob ein Eingreifen des Abzugsverbots für Bestechungsgelder die Erfüllung sowohl des objektiven als auch des subjektiven Tatbestands des § 299 Abs. 2 StGB voraussetzt, hat der BFH mit Urteil vom 15.4.2021 bejaht.⁴³ Das Betriebsausgabenabzugsverbot kommt demnach nur in Betracht, wenn auch der subjektive Tatbestand des § 299 Abs. 2 StGB erfüllt ist. Das Abzugsverbot gilt nur für Korruptionstatbestände,⁴⁴ wie insbesondere die Bestechung im geschäftlichen Verkehr (§ 299 Abs. 2 StGB) sowie die Vorteilsgewährung und Bestechung (§§ 333, 334 StGB).⁴⁵ Taten wie Untreue (§ 266 StGB) und Betrug (§ 263 StGB) fallen hingegen nicht unter das Abzugsverbot.

Von besonderer Relevanz ist, dass die Finanzbehörden bei einem Anfangsverdacht einer Korruptionstat nach § 4 Abs. 5 Satz 1 Nr. 10 Satz 3 EStG zur **Mitteilung an die Staatsanwaltschaft** verpflichtet sind.⁴⁶ Dies hat dazu geführt, dass Betriebsprüfungen heute eines der wirkungsvollsten Mittel zur Aufdeckung von Korruptionssachverhalten sind. Da die Schwelle für einen solchen Anfangsverdacht in der Praxis sehr gering ist, können z. B. schon bei unklaren Sachverhalten, Dokumentationsmängeln oder auffälligen Zahlungswegen Mitteilungen an die Staatsanwaltschaften ergehen. 31

Um Fehlverhalten in diesem Bereich auszuschließen, ist bereits vor Aufnahme neuer Geschäftsbeziehungen eine **Risikobewertung** (Geschäftspartner-Compliance) vorzunehmen. Risikoindikatoren sind dabei u. a. ungewöhnliche Vertragsgestaltungen (z. B. Hintereinanderschaltung mehrerer Gesellschaften), Auseinanderfallen von Ansässigkeitsstaat und Ort der Bankverbindung, Sitz in Offshore, Zweifel an Qualifikation zur Leistungserbringung, unspezifische Leistungsbeschreibungen, Barzahlungen. Erlangt die Geschäftsführung – etwa durch einen Whistleblower – nachträglich Kenntnis davon, dass Schmier- oder 32

43 BFH, 15.4.2021 – IV R 25/18, DSfR 2021, 1992.

44 Vgl. zu den Korruptionstatbeständen → Böttger, Kap. 2 Rn. 36 ff.

45 In Textziffer H4.14 EStR sind die betroffenen Tatbestände abschließend aufgeführt.

46 Vgl. BFH, 14.7.2008 – VII B 92/08, DSfR 2008, 1734.

Bestechungsgelder gezahlt und als Betriebsausgaben abgezogen wurden, ist dies zur Vermeidung der Verwirklichung des § 370 Abs. 1 Nr. 2 AO zwingend der Finanzverwaltung nach § 153 AO unverzüglich anzuzeigen (siehe hierzu → Rn. 21 ff.).

III. Risiken mangelnder Tax Compliance

1. Steuerliche Haftungsrisiken

- 33** Die Abgabenordnung sieht in den §§ 69 ff. AO Haftungstatbestände für fremde Steuerschulden vor, die insbesondere Organe von Unternehmen treffen. Voraussetzung jeder Haftung ist das Bestehen eines Steueranspruchs. Liegen die Voraussetzungen eines Haftungstatbestands vor, entsteht der Haftungsanspruch kraft Gesetzes. Die Haftungsschuld ist grundsätzlich akzessorisch zur Steuerschuld. Erlischt der Steueranspruch durch Erfüllung, Aufrechnung, Erlass oder Verjährung, teilt der Haftungsanspruch dieses Schicksal. Dies gilt allerdings nicht, wenn die Haftung darauf beruht, dass der Haftende eine Steuerhinterziehung begangen hat (§ 191 Abs. 5 Satz 2 AO). Die Inhaftungnahme erfolgt durch Erlass eines Haftungsbescheids, der im pflichtgemäßen Ermessen der Finanzverwaltung steht. Die Haftung für fremde Steuerschulden ist grundsätzlich unbeschränkt, d. h. der Haftungsschuldner haftet mit seinem gesamten Privatvermögen. Zum Steuerschuldner und weiteren Haftungsschuldnern besteht eine Gesamtschuldnerschaft (§ 44 AO).
- 34** Für die Haftung von Organen ist § 69 Abs. 1 AO der in der Praxis wichtigste Haftungstatbestand. Danach haften die in den §§ 34 und 35 AO genannten Personen (gesetzliche Vertreter oder ihnen Gleichgestellte, insbesondere also Vorstände einer AG und Geschäftsführer einer GmbH sowie sog. faktische Geschäftsführer bzw. faktische Vorstände) unter folgenden Voraussetzungen für Steuerschulden der Gesellschaft:
- Ansprüche aus dem Steuerschuldverhältnis (§ 37 AO) wurden nicht oder nicht rechtzeitig festgesetzt oder erfüllt oder es wurden Steuervergütungen oder Steuererstattungen ohne rechtlichen Grund gezahlt (Schaden);
 - Pflichtverletzung des Haftungsschuldners;
 - Kausalität zwischen Pflichtverletzung und Schaden;
 - Verschulden des Haftungsschuldners (Vorsatz oder grobe Fahrlässigkeit).
- 35** Die Haftungsschuld muss in der Amtszeit des Vorstands oder des Geschäftsführers fällig geworden sein. Eine Haftung für Steuern, die nach Beendigung der Vertretungsbefugnis fällig geworden sind, besteht nicht. Anknüpfungspunkt für die Pflichtverletzung sind alle durch die AO oder die Einzelsteuergesetze auferlegten steuerlichen Pflichten der Gesellschaft. Wird die Erfüllung der steuerlichen Pflicht auf eine Hilfsperson – die Steuerabteilung oder einen externen Steuerberater – delegiert, führt dies nicht per se zu einer Entlastung des Organs. Vielmehr wandelt sich die Erfüllungspflicht in eine Auswahl-, Instruktions- und Überwachungspflicht. Die Erfüllung dieser Pflichten führt regelmäßig jedoch zu

einer Entlastung des Organs. Eine Pflichtverletzung ist für den Haftungsschaden ursächlich, wenn dieser ohne die Pflichtverletzung nicht eingetreten wäre. Vorsätzlich handelt, wer die Pflichten gekannt und ihre Verletzung gewollt bzw. in Kauf genommen hat. Grob fahrlässig handelt, wer die Sorgfalt, zu der er nach seinen persönlichen Kenntnissen und Fähigkeiten verpflichtet und imstande ist, in ungewöhnlich großem Maße verletzt. Eigenes Unvermögen, ungenügende steuerrechtliche Kenntnisse oder Unerfahrenheit können den Schuldvorwurf der groben Fahrlässigkeit nicht ausschließen. Das Organ muss sich mit den handels- und steuerrechtlichen Erfordernissen seines Amtes vertraut machen und im Zweifelsfall Auskunft von sachverständiger Stelle einholen.

Von besonderer Bedeutung ist in diesem Zusammenhang der **Grundsatz der anteiligen Tilgung von Steuerschulden**. Das Organ verletzt seine Pflichten regelmäßig schuldhaft, wenn Steuerschulden schlechter behandelt werden als andere Verbindlichkeiten. Steuerschulden sind in gleichem Umfang zu tilgen wie die Verbindlichkeiten anderer Gläubiger. Auf der anderen Seite bedeutet dies aber auch, dass sich seine Haftung nicht auf den Teil der Steuerschuld erstrecken kann, der auch bei richtiger Anwendung des Grundsatzes der anteiligen Tilgung nicht hätte gezahlt werden können. Nach ständiger Rechtsprechung des BFH gilt der Grundsatz der anteiligen Tilgung nicht bei der LohnSt.⁴⁷ Hier sind die an die Mitarbeiter ausgezahlten Löhne soweit zu kürzen, dass sowohl die Löhne als auch darauf entfallende LohnSt und Sozialabgaben getilgt werden können.

Wer eine Steuerhinterziehung nach § 370 AO begeht oder daran teilnimmt, haftet nach § 71 AO (Haftung des Steuerhinterziehers) für die verkürzten Steuern und die zu Unrecht gewährten Steuervorteile sowie für die Hinterziehungszinsen nach § 235 AO. Eine Haftungsinanspruchnahme nach § 71 AO kann jeden treffen, der an einer Steuerhinterziehung zugunsten des Unternehmens beteiligt ist. Als Haftungsschuldner kommen insoweit also nicht nur Organe des Unternehmens, sondern auch Aufsichtsorgane und Mitarbeiter in Betracht. Voraussetzung für die Haftung ist, dass sowohl der objektive als auch der subjektive Tatbestand des § 370 AO verwirklicht ist. Die Feststellungslast trifft insoweit das Finanzamt, wobei die Haftung nach ständiger Rechtsprechung des BFH nach strafprozessualen Beweisgrundsätzen festzustellen ist. Es gilt der Grundsatz „in dubio pro reo“.⁴⁸

47 BFH, 12.7.1988 – VII R 108–109/87, BFH/NV 1988, 764; vgl. auch *Rüskens*, in: Klein, Abgabenordnung, § 69 AO Rn. 71.

48 BFH, 8.11.2000 – XI B 38/00, BeckRS 2000, 25005273; *Rüskens*, in: Klein, Abgabenordnung, § 71 AO Rn. 20.

2. Steuerstrafrechtliche und steuerordnungswidrigkeitenrechtliche Risiken

- 38 Die Verletzung steuerlicher Pflichten des Unternehmens kann zu strafrechtlichen sowie ordnungswidrigkeitenrechtlichen Konsequenzen für Organe und Mitarbeiter des Unternehmens sowie für das Unternehmen selbst führen.

a) Sanktionen gegen Organe und Mitarbeiter

aa) Steuerhinterziehung und leichtfertige Steuerverkürzung (§§ 370, 378 AO)

- 39 Nach § 370 AO wird bestraft, wer den Finanzbehörden oder anderen Behörden über steuerlich erhebliche Tatsachen unrichtige oder unvollständige Angaben macht, die Finanzbehörden pflichtwidrig über steuerlich erhebliche Tatsachen in Unkenntnis lässt oder pflichtwidrig die Verwendung von Steuerzeichen oder Steuerstemplern unterlässt und dadurch Steuern verkürzt oder für sich oder einen anderen nicht gerechtfertigte Steuervorteile erlangt. Der Bußgeldtatbestand der leichtfertigen Steuerverkürzung nach § 378 AO unterscheidet sich abgesehen von dem enger gezogenen Täterkreis allein im subjektiven Tatbestand von § 370 AO und dient insoweit als Auffangtatbestand, wenn vorsätzliches Handeln nicht nachgewiesen werden kann.

(1) Täter

- 40 Täter einer Steuerhinterziehung durch **aktives Tun** (§ 370 Abs. 1 Nr. 1 AO) kann nicht nur der Steuerschuldner selbst, sondern jeder sein, der die tatbestandlichen Voraussetzungen erfüllt.⁴⁹ Als Täter kommt daher jeder in Betracht, der in der Lage ist, auf die Festsetzung, Erhebung und Vollstreckung der geschuldeten Steuer einzuwirken. Somit kommt nicht nur der gesetzliche Vertreter eines Unternehmens, sondern grundsätzlich **jeder Mitarbeiter** als tauglicher Täter einer Steuerhinterziehung nach § 370 Abs. 1 Nr. 1 AO in Betracht. In diesem Zusammenhang sind vor allem auch die Besonderheiten zu beachten, die sich im Rahmen elektronischer Steuererklärungen ergeben.⁵⁰
- 41 Täter einer Steuerhinterziehung durch **Unterlassen** (§ 370 Abs. 1 Nr. 2 AO) kann dagegen nur derjenige sein, den aus den Einzelsteuergesetzen eine besondere **Pflicht zur Aufklärung** der Finanzbehörden trifft.⁵¹ Eine Zurechnung fremder Pflichtverletzungen über die Grundsätze der Mittäterschaft ist indes ausgeschlossen. Bei juristischen Personen haben nach § 34 Abs. 1 Satz 1 AO die gesetzlichen Vertreter deren steuerliche Pflichten zu erfüllen, sodass diese als Täter einer Steuerhinterziehung durch Unterlassen zugunsten der juristischen Person in Betracht kommen. Bei nicht rechtsfähigen Personenvereinigungen im Sinne des § 34 Abs. 1 Satz 1 AO (wie OHG, KG und GbR) sind die steuerlichen

49 BGH, 6.6.2007 – 5 StR 127/07, NJW 2007, 2864; BGH, 9.4.2013 – 1 StR 586/12, DStR 2013, 1177, 1179.

50 Siehe hierzu vertiefend Heuel/Harink, AO-StB 2020, 49.

51 BGH, 9.4.2013 – 1 StR 586/12, DStR 2013, 1177.

Pflichten durch all jene Personen zu erfüllen, die deren Geschäfte tatsächlich führen und nach außen auftreten. Soweit nicht rechtsfähige Personenvereinigungen auch zivilistische Geschäftsführer haben (wie OHG und KG), haben diese deren steuerliche Pflichten zu erfüllen.⁵² Die steuerlichen Pflichten einer GmbH & Co. KG sind durch den gesetzlichen Vertreter der Komplementär-GmbH zu erfüllen.⁵³ Eine eigene Rechtspflicht zur Aufklärung über steuerlich erhebliche Tatsachen trifft daneben gemäß § 35 AO auch den Verfügungsberechtigten.

Nach § 378 AO kann Täter einer **leichtfertigen Steuerverkürzung** nur sein, wer die Steuerverkürzung „als Steuerpflichtiger“ (§ 33 AO) oder „bei Wahrnehmung der Angelegenheiten eines Steuerpflichtigen“ bewirkt. Zu den Steuerpflichtigen gehören insbesondere auch jene Personen, die nach § 34 Abs. 1 AO die steuerlichen Pflichten juristischer Personen sowie nicht rechtsfähiger Personenvereinigungen zu erfüllen haben. Wird die Erfüllung der steuerlichen Pflichten auf Unternehmensmitarbeiter delegiert, können diese „bei Wahrnehmung der Angelegenheiten eines Steuerpflichtigen“ ebenfalls den Tatbestand des § 378 AO erfüllen. Insoweit ist es unbeachtlich, ob der Mitarbeiter eine leitende Position innehat (wie etwa der Leiter der Steuerabteilung) oder bspw. als Buchhalter nur untergeordnete Arbeiten ausführt. Die Grenze ist dort erreicht, wo Mitarbeiter lediglich Schreib- oder Rechenarbeiten ausführen.⁵⁴ 42

(2) Objektiver Tatbestand

Im Unternehmensbereich sind mögliche steuerliche Verfehlungen äußerst vielfältig. Bei den Ertragsteuern sind häufige Fehlerquellen die unzutreffende Ermittlung von Betriebseinnahmen oder Betriebsausgaben, verdeckte Gewinnausschüttungen und verdeckte Einlagen. Die Grenze zwischen legaler Steuergestaltung, Missbrauch von rechtlichen Gestaltungsmöglichkeiten (§ 42 AO) und Steuerhinterziehung ist in der Praxis mitunter schmal und schwer zu ziehen. Allein die Optimierung der steuerlichen Verhältnisse eines Unternehmens ist nicht strafbar, sondern vielmehr durch die Organe des Unternehmens geschuldet. Die Annahme einer dem Steuerpflichtigen günstigen – und von der Verwaltungsansicht abweichenden – Rechtsansicht ist weder unzulässig noch per se strafbar. Entscheidend ist, dass die Finanzverwaltung über die steuerlich erheblichen Tatsachen – und damit den zugrunde liegenden Sachverhalt – richtig und vollständig unterrichtet wird. Wegen der Formalisierung der Steuererklärungen erschöpfen sich die Angaben gegenüber der Finanzverwaltung zumeist in der Wiedergabe quantifizierter Beträge ohne Sachverhaltsschilderung. Dies ermöglicht der Finanzverwaltung keine rechtliche Prüfung der jeweiligen Sachverhalte. Nach der Rechtsprechung des BGH besteht zumindest eine **Offenbarungspflicht** der Sachverhaltselemente, wenn die von dem Steuerpflichtigen vertretene **Rechtsauffassung** über die Auslegung von Rechtsbegriffen oder die Sub- 43

⁵² *Rüsken*, in: Klein, Abgabenordnung, § 34 AO Rn. 8.

⁵³ *Boeker*, in: Hübschmann/Hepp/Spitaler, AO/FGO, Stand: 274. EL, § 34 AO Rn. 37.

⁵⁴ *Randt*, in: Joecks/Jäger/Randt, Steuerstrafrecht, § 378 AO Rn. 19.

sumtion bestimmter Tatsachen von der Rechtsprechung, Richtlinien der Finanzverwaltung oder der regelmäßigen Veranlagungspraxis abweicht.⁵⁵ Eine Steuerhinterziehung ist demnach ausgeschlossen, wenn der Steuerpflichtige offen oder verdeckt eine ihm günstige (unzutreffende) Rechtsansicht vertritt, aber die steuerlich erheblichen Tatsachen richtig und vollständig vorträgt und der Finanzverwaltung dadurch ermöglicht, die Steuer unter abweichender rechtlicher Beurteilung zutreffend festzusetzen. Durch das BestVerfModG wurde § 93c AO eingeführt, der die in anderen Vorschriften geregelte Pflicht zur elektronischen Übermittlung bestimmter steuerungsrelevanter Daten (z. B. Mitteilungen des Arbeitgebers, der Kranken- oder Rentenversicherung oder der Bundesagentur für Arbeit) eines bei ihm registrierten Steuerpflichtigen harmonisiert. Durch den mit Gesetz vom 18.7.2016 eingeführten § 150 Abs. 7 Satz 2 AO wird fingiert, dass die Daten, die über § 93c AO der Finanzverwaltung übermittelt wurden, als Angaben des Steuerpflichtigen gelten, soweit dieser nicht in einem dafür vorgesehenen Abschnitt oder Datenfeld der Steuererklärung abweichende Angaben tätigt. Neben der hierdurch beabsichtigten Vereinfachung des Besteuerungsverfahrens⁵⁶ ergibt sich für den Steuerpflichtigen der Vorteil, dass er selbst keine unvollständige Erklärung abgibt, wenn er die Daten i. S. d. § 93c AO nicht angibt und ihm selbstverständlich auch falsche Angaben der übermittelnden Stellen nicht zum Nachteil gereichen, wenn er hiervon – wie es regelmäßig der Fall sein wird – keine Kenntnis hat. Umstritten ist in diesem Zusammenhang, ob die Zurechnung über § 150 Abs. 7 Satz 2 AO auch erfolgt, wenn überhaupt keine Steuererklärung (bei bestehender Abgabepflicht) abgegeben wird und welche steuerstrafrechtlichen Auswirkungen hieraus folgen.⁵⁷

- 44 Zur Vermeidung steuerstrafrechtlicher Risiken sollten Steuererklärungen in der Praxis – zumindest in Zweifelsfällen – sehr viel häufiger **Sachverhaltsdarstellungen als Anlage** beigefügt werden.⁵⁸ Dies gilt umso mehr, da die Rechtsprechung annimmt, es sei dem Steuerpflichtigen grundsätzlich zumutbar, bestehende Rechtsfragen nach Aufdeckung des vollständigen und wahren Sachverhalts im Besteuerungsverfahren zu klären.⁵⁹ Die Sachverhaltsdarstellung muss jedoch nicht zwingend in einem Begleitschreiben erfolgen, sondern kann sich auch in den Anlagen zur Steuererklärung wie bspw. dem beigefügten Jahresabschluss und den dortigen Erläuterungen zu bestimmten Bilanzposten befinden.⁶⁰ Zwar mag eine solche Vorgehensweise im Tagesgeschäft nicht immer einfach umzu-

55 BGH, 10.11.1999 – 5 StR 221/99, NStZ 2000, 203, 204; BFH, 22.11.2018 – V R 65/17, DStR 2019, 265; ebenso Jäger, in: Klein, Abgabenordnung, § 370 AO Rn. 44 f.

56 Vgl. BT-Drs. 18/8434, S. 112.

57 Siehe hierzu vertiefend Roth, wistra 2018, 152; Beyer, NZWiSt 2018, 359; Rolletschke, NZWiSt 2018, 185; Grötsch/Stürzl, wistra 2019, 127; Heuel/Harink, AO-StB 2020, 49.

58 Schauß/Schwartz, ZWH 2013, 212, 213.

59 BVerfG, 16.6.2011 – 2 BvR 542/09, wistra 2011, 458, 460; BGH, 8.9.2011 – 1 StR 38/11, NStZ 2012, 160, 161.

60 Schauß/Schwartz, ZWH 2013, 212, 213; Wulf, in: Spatscheck et al., FS Streck, 2011, S. 627, 633.

setzen sein. Um den späteren Vorwurf einer Steuerhinterziehung frühzeitig auszuschließen, ist eine umfassende Sachverhaltsschilderung jedoch unverzichtbar. Auch ist der gegen diese Vorgehensweise häufig vorgebrachte Vorhalt nicht zielführend, dass die Finanzverwaltung hierdurch gerade erst auf die fragliche Thematik hingewiesen werde. Wer fürchtet, die Finanzverwaltung werde bei vollständiger Sachverhaltskenntnis zu einer anderen steuerlichen Würdigung kommen, ist gut beraten, gerade diese Befürchtung zum Anlass einer Sachverhaltsoffenlegung zu nehmen. Es bleibt im Anschluss natürlich die Möglichkeit unbenommen, „mit offenem Visier“ mit der Finanzverwaltung über die zutreffende steuerliche Bewertung zu streiten. Der Ausgang des Steuerstreits (ggf. vor den Finanzgerichten) mag zwar ungewiss sein, doch ist die andernfalls drohende Gefahr der Einleitung eines steuerstrafrechtlichen Ermittlungsverfahrens genannt.

Ferner ist zu berücksichtigen, dass unrichtige oder unvollständige Angaben im Sinne des § 370 Abs. 1 Nr. 1 AO nicht auf Angaben in Steuererklärungen bzw. auf das Steuerfestsetzungsverfahren beschränkt sind. Unrichtige schriftliche oder mündliche Auskünfte im Steuerermittlungsverfahren, in der Außenprüfung, im Rechtsbehelfsverfahren sowie im Erhebungs- und Beitreibungsverfahren unterfallen ebenfalls § 370 Abs. 1 Nr. 1 AO. Ebenso kann den Tatbestand des § 370 AO erfüllen, wer bewusst eine unrichtige oder unvollständige **tatsächliche Verständigung** herbeiführt.⁶¹ **45**

Eine **Steuerhinterziehung durch Unterlassen** (§ 370 Abs. 1 Nr. 2 AO) kann neben der Nichtabgabe von Steuererklärungen und Steueranmeldungen sowie der Nichterfüllung steuerlicher Anzeigepflichten (wie z. B. § 19 GrEStG) insbesondere durch die Verletzung der Anzeigepflicht nach § 153 AO (siehe hierzu → Rn. 21 ff.) begangen werden. Zögert der Steuerpflichtige zu lange, sodass die Anzeige nicht mehr dem Unverzüglichkeitserfordernis des § 153 AO genügt, stellt die verspätete Anzeige zunächst einen Rücktritt vom Versuch nach § 24 StGB dar.⁶² Eine vollendete Steuerhinterziehung durch Unterlassen liegt erst vor, wenn der Zeitpunkt verstrichen ist, zu dem bei ordnungsgemäßer Anzeige ein geänderter Steuerbescheid ergangen wäre. Ab diesem Zeitpunkt kann eine verspätete Anzeige nach § 153 AO jedoch strafbefreiend wirken, wenn sie die Voraussetzungen des § 371 AO (siehe hierzu → Rn. 103 ff.) erfüllt. **46**

§ 370 Abs. 4 AO enthält eine Legaldefinition des **Taterfolgs**. Danach sind Steuern namentlich dann verkürzt, wenn sie nicht, nicht in voller Höhe oder nicht rechtzeitig festgesetzt werden. Dies gilt auch dann, wenn die Steuer vorläufig (§ 165 AO) oder unter Vorbehalt der Nachprüfung (§ 164 AO) festgesetzt wird oder eine Steueranmeldung einer Steuerfestsetzung unter Vorbehalt der Nachprüfung gleichsteht (§ 168 AO). Nicht gerechtfertigte Steuervorteile sind erlangt, soweit sie zu Unrecht gewährt oder belassen werden. Da § 370 AO ein Er- **47**

61 Jäger, in: Klein, Abgabenordnung, § 370 AO Rn. 54.

62 Schauf/Schwartz, PStR 2015, 248, 252.

klärungsdelikt ist und der Taterfolg auf die Steuerfestsetzung abstellt, erfüllt die verspätete oder unterlassene Zahlung der geschuldeten Steuern nicht den Tatbestand des § 370 AO.⁶³ Insoweit unterscheidet sich § 370 AO vom Straftatbestand der gewerbs- oder bandenmäßigen Schädigung des Umsatzsteueraufkommens (§ 26c UStG), der an die Nichtentrichtung von in Rechnungen gemäß § 14 UStG ausgewiesener USt zum Fälligkeitszeitpunkt anknüpft.

- 48 Für die Tatbestandsverwirklichung ist es jedoch unerheblich, ob die Steuer aus anderen Gründen hätte ermäßigt oder der Steuervorteil aus anderen Gründen hätte beansprucht werden können (sog. **Kompensationsverbot**, § 370 Abs. 4 Satz 3 AO). Damit ist gemeint, dass nachträglich geltend gemachte Ermäßigungsgründe, die steuerlich z. B. als neue Tatsachen im Sinne des § 173 Abs. 1 Nr. 2 AO zu berücksichtigen sind, für den Taterfolg außer Betracht bleiben. Hat der Steuerpflichtige vorsätzlich Einkünfte nicht erklärt und zugleich als Betriebsausgaben berücksichtigungsfähigen Aufwand (versehentlich) nicht geltend gemacht, bleibt dieser bei der Bemessung der Steuerverkürzung unberücksichtigt. Eine Ausnahme vom Kompensationsverbot besteht nur dann, wenn die steuermindernden Gründe in einem unmittelbaren wirtschaftlichen Zusammenhang mit dem durch die unrichtigen Angaben herbeigeführten Verkürzungserfolg stehen. Mit Urteil vom 13.9.2018 hat der BGH seine Rspr. zum Kompensationsverbot bei der USt geändert und entschieden, dass Vorsteuern bei der Ermittlung des Verkürzungsumfangs unmittelbar mindernd angesetzt werden können, wenn ein wirtschaftlicher Zusammenhang zwischen Ein- und Ausgangsumsatz besteht und auch die Voraussetzungen des § 15 UStG vorliegen.⁶⁴
- 49 In den letzten Jahren hat im Unternehmensbereich die Anzahl der eingeleiteten Steuerstraßverfahren wegen einer **nicht fristgemäßen Abgabe** einer Steuererklärung deutlich zugenommen. Während bei Veranlagungssteuern nach Fristablauf bis zum Zeitpunkt des allgemeinen Abschlusses der Veranlagungsarbeiten in dem betreffenden Bezirk zunächst nur eine versuchte Steuerhinterziehung vorliegt, liegt bei Fälligkeitssteuer, die als Anmeldeungssteuern ausgestattet sind (wie USt und LohnSt) bei vorsätzlichem Handeln bereits mit Ablauf der Abgabefrist eine vollendete Steuerhinterziehung durch Unterlassen vor. In der Praxis treten Verfehlungen in Form der verspäteten Abgabe von Steuererklärungen insbesondere im Bereich der USt auf. Diese ist mit Ablauf der Abgabefrist verkürzt, da die USt-Erklärung als Steueranmeldung (§ 18 Abs. 3 Satz 1 UStG) einer Steuerfestsetzung unter Vorbehalt der Nachprüfung gleichsteht (§ 168 Satz 1 AO). Dies gilt sowohl für USt-Voranmeldungen (§ 18 Abs. 1 UStG) als auch für USt-Jahreserklärungen (§ 18 Abs. 3 UStG). Gibt der Steuerpflichtige keine Erklärung ab oder reicht er die Erklärung verspätet ein, liegt eine vollendete Steuerhinterziehung mit Fristablauf auch dann vor, wenn die Finanzverwaltung später eine Steuerfestsetzung im Wege der Schätzung nach § 162 AO vornimmt.⁶⁵ Kann

63 BGH, 22.7.2014 – 1 StR 189/14, NSTZ-RR 2014, 310.

64 BGH, 13.9.2018 – 1 StR 642/17, DStR 2018, 2696.

65 Jäger, in: Klein, Abgabenordnung, § 370 AO Rn. 105.

eine Steuererklärung nicht fristgemäß abgegeben werden, sollte daher in jedem Fall ein **Fristverlängerungsantrag** nach § 109 AO gestellt werden. Nr. 132 Abs. 2 AStBV (St) 2023/2024⁶⁶ sieht indes vor, dass bei der USt und der LohnSt berichtigte oder verspätet abgegebene Steuer(vor)anmeldungen nur in begründeten Einzelfällen an die Straf- und Bußgeldsachenstelle weiterzuleiten sind. Insoweit bleibt zu bedenken, dass die AStBV (St) für Staatsanwaltschaften und Gerichte keine Bindungswirkung entfalten und bei der USt und der LohnSt auch geringfügige Terminüberschreitungen den objektiven Tatbestand des § 370 Abs. 1 Nr. 2 AO erfüllen.

(3) Subjektiver Tatbestand

Der subjektive Tatbestand des § 370 AO fordert, dass die Steuerhinterziehung vorsätzlich erfolgt ist, wobei neben sicherem Wissen auch bereits Eventualvorsatz, d. h. ein billigendes Inkaufnehmen der Tatbestandsverwirklichung, ausreichend ist. Hiervon ist grundsätzlich nicht auszugehen, wenn dem Vorstand keine konkreten Anhaltspunkte dafür vorliegen, dass die von der Steuerabteilung oder einem (externen) Steuerberater gefertigte Steuererklärung unvollständige oder unrichtige Angaben enthält. Hat sich ein Unternehmen Organisationsstrukturen gegeben, die im Rahmen des Möglichen und Zumutbaren erkennbar auf die Sicherstellung der Einhaltung der steuerlichen Pflichten des Unternehmens abzielen, schließt dies ein vorwerfbares Handeln regelmäßig aus. Dies hat auch das BMF aufgegriffen und ausgeführt, dass die Einrichtung eines **innerbetrieblichen Kontrollsystems** ein **Indiz gegen das Vorliegen von Vorsatz oder Leichtfertigkeit** darstellen kann.⁶⁷ Dies darf in der Praxis jedoch nicht dahingehend fehlverstanden werden, dass bereits allein das Fehlen eines Tax Compliance-Systems verdachts- und vorsatzbegründend wirkt.⁶⁸ Allein das Gegenteil darf richtig sein. Ist der subjektive Tatbestand des § 370 AO nicht erfüllt, bzw. lässt sich dieser nicht nachweisen, kann eine leichtfertige Steuerverkürzung nach § 378 AO in Betracht kommen. Hierfür reicht es aus, dass der Steuerpflichtige diejenige Sorgfalt außer Acht lässt, zu der er nach den besonderen Umständen des Einzelfalls und seinen persönlichen Kenntnissen und Fähigkeiten verpflichtet und imstande ist, obwohl sich ihm aufdrängen musste, dass dadurch eine Steuerverkürzung eintreten wird.

Hierbei ist zu beachten, dass sich jeder Steuerpflichtige über diejenigen steuerlichen Pflichten unterrichten muss, die ihn im Rahmen seines Lebenskreises treffen. Für Unternehmen gelten nach der Rechtsprechung jedenfalls bei Rechtsgeschäften, die zu ihrer kaufmännischen Tätigkeit gehören, höhere Anforderun-

⁶⁶ BStBl. I 2023, 1798.

⁶⁷ BMF, 23.5.2016 – IVA 3 – S 0324/15/10001, BStBl. I 2016, 490.

⁶⁸ *Schauf/Schwartz*, PStR 2015, 248.

gen an die **Erkundigungspflichten** als bei anderen Steuerpflichtigen.⁶⁹ Unterlässt der Steuerpflichtige die erforderliche Erkundigungspflicht, kann dies (zumindest) leichtfertiges Handeln begründen. Im Umkehrschluss bedeutet dies, dass ein Leichtfertigkeitsevorwurf grundsätzlich ausscheidet, wenn eine qualifizierte Auskunftsperson zu Rate gezogen wurde. Ein etwaiges leichtfertiges Handeln des Steuerberaters kann dem Steuerpflichtigen weder nach straf- oder bußgeldrechtlichen noch nach steuerrechtlichen Gesichtspunkten zugerechnet werden.⁷⁰ Ebenso exkulpiert die Einholung eines **Rechtsgutachtens** regelmäßig den Steuerpflichtigen, sofern dieses nicht durch sachfremde Erwägungen beeinflusst oder besonders zugunsten des Steuerpflichtigen verfasst wurde.⁷¹ Auskünfte, die erkennbar vordergründig und mangelhaft sind oder nach dem Willen des Anfragenden lediglich eine „Feigenblattfunktion“ erfüllen sollen, können hingegen nicht entlasten. Bei der Auskunftserteilung von unternehmenseigenen Anwälten („**Hausjuristen**“) ist Vorsicht geboten. In der Rechtsprechung wird zum Teil die Ansicht vertreten, dass es zur Erfüllung der Sorgfaltspflichten des Verantwortlichen nicht ausreichend sei, den Rat eines Rechtskundigen aus dem eigenen Unternehmen einzuholen, wenn davon auszugehen ist, dass die Auskunft durch eigenes wirtschaftliches Interesse beeinflusst sein könnte.⁷² Vor diesem Hintergrund sollte die Einholung externen Rechtsrats in Zweifelsfällen Baustein eines Tax Compliance-Systems sein. Zum Ausschluss vorwerfbar Handelns bietet sich zudem an, Rechtsfragen im Vorfeld der Realisierung durch eine **verbindliche Auskunft** (§ 89 Abs. 2 AO) abzusichern oder im Anschluss an eine Betriebsprüfung eine verbindliche Zusage (§ 204 AO) einzuholen.

(4) Strafe

- 52** Der Tatbestand des § 370 Abs. 1 AO sieht einen Strafraum von Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe vor. § 370 Abs. 3 AO beinhaltet eine Strafschärfung für besonders schwere Fälle der Steuerhinterziehung. In diesen Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. § 370 Abs. 3 Satz 2 AO enthält sog. Regelbeispiele, deren Erfüllung ein Indiz für das Vorliegen eines besonders schweren Falles darstellt. Im Unternehmensbereich kommt vorwiegend dem Regelbeispiel der Steuerverkürzung bzw. der Erlangung eines nicht gerechtfertigten Steuervorteils **in großem Ausmaß** (§ 370 Abs. 3 Satz 2 Nr. 1 AO) Bedeutung zu. Der BGH nimmt seit seiner Rechtsprechungsänderung im Jahr 2015 ein großes Ausmaß ab einer einheitlichen Wertgrenze von **50.000 EUR je Tat** an.⁷³ Bei Unternehmen wird diese Wertgrenze regelmäßig über-

69 BGH, 8.9.2011 – 1 StR 38/11, NSZ 2012, 160, 161; BFH, 19.2.2009 – II R 49/07, DStRE 2009, 877, 878.

70 BFH, 29.10.2013 – VIII R 27/10, DStR 2013, 2694.

71 FG Düsseldorf, 26.3.2014 – 7 K 1884/13, BB 2014, 2134; zur leichtfertigen Steuerverkürzung nach Einholung eines Rechtsgutachtens, *Schwartz*, PStR 2014, 156.

72 OLG Koblenz, 19.10.1989 – 1 Ss 393/89, LMRR 1989, 53; BGH, 1.12.1981 – KRB 5/79, NJW 1982, 938; kritisch auch *Jäger*, in: Klein, Abgabenordnung, § 370 AO Rn. 183.

73 BGH, 27.10.2015 – 1 StR 373/15, BeckRS 2016, 02436.

schritten. Erschwerend kommt hinzu, dass eine Steuerhinterziehung von 50.000 EUR eine Verfolgungsverjährung von 15 (statt 5) Jahren zur Folge hat (§ 376 Abs. 1 AO). Die Ordnungswidrigkeit des § 378 AO kann mit einer Geldbuße bis zu 50.000 EUR je Tat geahndet werden (§ 378 Abs. 2 AO).

bb) Verletzung der Aufsichtspflicht (§ 130 OWiG)

§ 130 OWiG hat in der jüngeren Vergangenheit gerade im Steuerstrafrecht als Sanktionsmöglichkeit gegen Unternehmensverantwortliche deutlich an Bedeutung gewonnen.⁷⁴ Nach § 130 OWiG kann gegen eine aufsichtspflichtige Person eine Geldbuße festgesetzt werden, wenn sie vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist (sog. Anknüpfungstaten), wenn eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre.⁷⁵ Die §§ 370, 378 AO sind nach h. M. taugliche Anknüpfungstaten im Sinne des § 130 OWiG. Somit können aufsichtspflichtigen Personen (insbesondere Vorstand und Geschäftsführung, über § 9 OWiG bspw. aber auch Ressort- und Abteilungsleitern) Handlungen von Mitarbeitern zugerechnet werden und diese können über den „Umweg“ des § 130 OWiG für eine Steuerhinterziehung oder leichtfertige Steuerverkürzung haftbar gemacht werden, obwohl ihnen persönlich hinsichtlich der betreffenden Taten kein vorsätzliches oder leichtfertiges Handeln zur Last gelegt werden kann. § 130 OWiG bietet damit die Möglichkeit, die **Desorganisation innerhalb eines Unternehmens**, die zu einer Verletzung steuerlicher Pflichten geführt hat, gegenüber der aufsichtspflichtigen Person zu sanktionieren. Allein der Umstand, dass ein Unternehmen keine Compliance-Organisation vorhält, kann für sich genommen indes keine Aufsichtspflichtverletzung nach § 130 OWiG begründen.⁷⁶ Demgegenüber kann eine Entlastung der aufsichtspflichtigen Personen regelmäßig über den Nachweis der gehörigen Aufsicht aufgrund bestehender und funktionierender Tax Compliance-Strukturen erreicht werden.

Ein Verstoß gegen § 130 OWiG kann, wenn die Zuwiderhandlung eine Straftat ist (§ 370 AO), im Höchstmaß mit einer **Geldbuße bis zu 1.000.000 EUR je Tat** geahndet werden (§ 130 Abs. 3 Satz 1 OWiG). Für die fahrlässige Aufsichtspflichtverletzung ist das Höchstmaß in diesen Fällen auf 500.000 EUR begrenzt (§ 17 Abs. 2 OWiG). Handelt es sich bei der Anknüpfungstat dagegen um eine Ordnungswidrigkeit (§ 378 AO), ist das in dieser Vorschrift angedrohte Höchstmaß der Geldbuße entscheidend (§ 130 Abs. 3 Satz 2 OWiG). Im Fall einer leichtfertigen Steuerverkürzung kann ein Verstoß gegen § 130 OWiG demnach

⁷⁴ Zur Aufsichtspflichtverletzung unter Berücksichtigung des Steuerrechts, *Hunsmann*, DStR 2014, 855.

⁷⁵ Zur Anwendbarkeit des § 130 OWiG im Konzern, OLG München, 23.9.2014 – 3 Ws 599, 600/14, BeckRS 2015, 14184.

⁷⁶ *Aichberger/Schwartz*, DStR 2015, 1691, 1696.

lediglich mit einer Geldbuße bis zu 50.000 EUR je Tat geahndet werden (§ 378 Abs. 2 AO).

b) Sanktionen gegen das Unternehmen

aa) Verbandsgeldbuße (§ 30 OWiG)

- 55** Bei der Verletzung steuerlicher Pflichten des Unternehmens machen die Ermittlungsbehörden verstärkt Gebrauch von der sog. Verbandsgeldbuße (Unternehmensgeldbuße) nach § 30 OWiG. Danach kann gegen ein Unternehmen eine Geldbuße verhängt werden, wenn ein vertretungsberechtigtes Organ oder eine sonstige Leitungs- oder Kontrollperson (z. B. Steuerabteilungsleiter) eine Straftat oder Ordnungswidrigkeit (**Anknüpfungstat**) begangen hat, durch die Pflichten des Unternehmens verletzt worden sind oder die zu dessen Bereicherung geführt hat oder jedenfalls führen sollte.⁷⁷ Als Anknüpfungstaten kommen im Zusammenhang mit der Verletzung steuerlicher Pflichten des Unternehmens insbesondere die §§ 370, 378 AO sowie § 130 OWiG in Betracht. Bei vorsätzlicher oder leichtfertiger Steuerverkürzung (§§ 370, 378 AO) oder bei Verletzung von Steuerabzugspflichten (§ 380 AO) ist regelmäßig eine Bereicherung des Unternehmens eingetreten. § 30 OWiG überträgt ein Delikt, das eine natürliche Person begangen hat, auf eine juristische Person, um es bei dieser im Wege der Festsetzung einer Geldbuße sanktionieren zu können. Dabei kann eine Verbandsgeldbuße einerseits neben Sanktionen gegen die verantwortlichen natürlichen Personen verhängt werden, andererseits ist auch eine selbstständige Festsetzung einer „anonymen“ Verbandsgeldbuße möglich, wenn z. B. nicht (mehr) aufgeklärt werden kann, welchem von mehreren Verantwortlichen im Sinne des § 30 Abs. 1 OWiG die Pflichtverletzung zur Last fällt. Kann die Anknüpfungstat wegen einer wirksamen Selbstanzeige (§§ 371, 378 Abs. 3 AO) (siehe hierzu → Rn. 103 ff.) nicht mehr verfolgt werden, ist eine selbstständige Festsetzung einer Verbandsgeldbuße nach § 30 Abs. 4 Satz 3 OWiG ausgeschlossen. Aus diesem Grund ist es wichtig darauf zu achten, dass alle möglichen Täter der Anknüpfungstat im Unternehmen von der Selbstanzeigewirkung erfasst werden. In der Praxis werden hierzu in der Regel Anschlussklärungen aller potenziell Beteiligten eingeholt. Da die Verhängung einer Verbandsgeldbuße aufgrund einer Steuerhinterziehung oder einer leichtfertigen Steuerverkürzung nach einer erfolgreichen Selbstanzeige ausscheidet, kommt es in der Praxis mitunter vor, dass die Strafverfolgungsbehörden versuchen, über den Umweg einer Aufsichtspflichtverletzung nach § 130 OWiG als Anknüpfungstat eine Verbandsgeldbuße zu verhängen. Hiergegen spricht, dass es einen Wertungswiderspruch darstellen würde, wenn in Fällen, in denen der Betriebsinhaber selbst den Tatbestand des § 378 Abs. 1 AO oder § 370 Abs. 1 AO erfüllt hätte, die Selbstanzeige eine Verhängung einer Geldbuße sperren würde, hingegen in Fällen, in denen der Betriebsinhaber lediglich den Auffangtatbestand des § 130 Abs. 1 OWiG verwirklicht hat, eine Verbandsgeldbuße möglich wäre. Dann wäre eine Ahndung des

⁷⁷ Vgl. zu § 30 OWiG im Einzelnen → Böttger, Kap. 2 Rn. 157 ff.

Unternehmens bei der (fahrlässig begangenen) Ordnungswidrigkeit des § 130 OWiG des Betriebsinhabers möglich, hingegen bei der vorsätzlichen Steuerhinterziehung nicht.⁷⁸ Jedoch ist in diesen Fällen weiterhin eine Einziehung nach § 29a OWiG denkbar (siehe hierzu → Rn. 59.).

Im Fall einer vorsätzlichen Straftat (§ 370 AO) kann eine **Geldbuße bis zu 56 10.000.000 EUR** je Tat (Veranlagungszeitraum) festgesetzt werden.⁷⁹ Handelt es sich bei der Anknüpfungstat dagegen um die Ordnungswidrigkeit der leichtfertigen Steuerverkürzung (§ 378 AO), kann eine Geldbuße bis zu 50.000 EUR je Tat festgesetzt werden. Besteht die Anknüpfungstat in § 130 OWiG, ist der Verweis auf § 30 Abs. 2 Satz 3 OWiG zu beachten (§ 130 Abs. 3 Satz 2 OWiG), der für die Zwecke der Verbandsgeldbuße zu einer Verzehnfachung der in § 130 OWiG benannten Geldbuße führt. Von erheblicher praktischer und finanzieller Bedeutung ist ferner, dass das gesetzlich vorgesehene Höchstmaß der Geldbuße zum Zwecke der Gewinnabschöpfung überschritten werden kann (§ 30 Abs. 3, § 17 Abs. 4 OWiG). Mit Wirkung zum 30.6.2013 hat der Gesetzgeber zudem für den Fall einer **Gesamtrechtsnachfolge** oder einer partiellen Gesamtrechtsnachfolge durch Aufspaltung (§ 123 Abs. 1 UmwG) die Möglichkeit der Festsetzung einer Verbandsgeldbuße gegen den Rechtsnachfolger für Anknüpfungstaten von Verantwortlichen des Rechtsvorgängers geschaffen (§ 30 Abs. 2a OWiG). Zuvor konnte gegen den Rechtsnachfolger nur unter engen Voraussetzungen eine Verbandsgeldbuße festgesetzt werden, wenn zwischen der früheren und der neuen Vermögensverbindung nach wirtschaftlicher Betrachtungsweise nahezu Identität bestand.⁸⁰

Bei der Frage der Festsetzung einer Verbandsgeldbuße nach § 30 OWiG kommt **57** der Einrichtung eines **Tax Compliance-Systems** große Bedeutung zu. Führt das Tax Compliance-System nicht schon dazu, dass von einer Verbandsgeldbuße abgesehen ist, so ist es zumindest bei der **Bemessung der Geldbuße** zu berücksichtigen. Dies hat auch der BGH⁸¹ in seinem Urteil vom 9.5.2017 bestätigt, in dem er – soweit ersichtlich – erstmalig die positive Bedeutung von Compliance Bemühungen auch im Rahmen von § 30 OWiG hervorhob und feststellte, dass diese strafmildernd zu berücksichtigen sind:

„Für die Bemessung der Geldbuße ist zudem von Bedeutung, inwieweit die Nebenbeteiligte ihrer Pflicht, Rechtsverletzungen aus der Sphäre des Unternehmens zu unterbinden, genügt und ein effizientes Compliance-Management installiert hat, das auf die Vermeidung von Rechtsverstößen ausgelegt sein muss (vgl. Raum in Hastenrath, Compliance – Kommunikation, 2. Aufl.,

⁷⁸ Siehe hierzu ausführlich *Reichling*, NJW 2013, 2233, 2235.

⁷⁹ Der Bußgeldrahmen wurde für Taten ab dem 30.6.2013 durch die 8. GWB-Novelle auf 10.000.000 EUR erhöht. Für Taten vor dem 30.6.2013 gilt weiterhin der alte Höchstbetrag von 1.000.000 EUR je Tat.

⁸⁰ BGH, 10.8.2011 – KRB 55/10, NJW 2012, 164, 165.

⁸¹ BGH, 9.5.2017 – 1 StR 265/16, ZWH 2017, 290. Vgl. hierzu auch → *Schulz*, Kap. 1. Ebenso BGH, 27.4.2022 – 5 StR 278/21, BeckRS 2022, 13180.

S. 31 f.). Dabei kann auch eine Rolle spielen, ob die Nebenbeteiligte in der Folge dieses Verfahrens entsprechende Regelungen optimiert und ihre betriebsinternen Abläufe so gestaltet hat, dass vergleichbare Normverletzungen zukünftig jedenfalls deutlich erschwert werden.“

- 58 Nach § 4 Abs. 5 Satz 1 Nr. 8 EStG dürfen Geldbußen nach § 30 OWiG **nicht als Betriebsausgabe abgezogen** werden. Dies gilt uneingeschränkt für den Sanktionsteil. Für den Abschöpfungsteil gilt das Abzugsverbot für die Geldbuße nur dann uneingeschränkt, wenn bei der Berechnung des Vermögensvorteils die darauf entfallende ertragsteuerliche Belastung – ggf. im Wege der Schätzung – berücksichtigt worden ist. Andernfalls kann der auf die Abschöpfung entfallende Teil der Geldbuße als Betriebsausgabe abgezogen werden (§ 4 Abs. 5 Satz 1 Nr. 8 Satz 4 EStG). Es sollte daher darauf hingewirkt werden, dass in dem Bußgeldbescheid ausdrücklich angegeben wird, welcher Anteil an der verhängten Geldbuße der Abschöpfung des erlangten wirtschaftlichen Vorteils dient.

bb) Einziehung (§ 29a OWiG)

- 59 Wird – wegen fehlender Verantwortlichkeit, Verfahrenshindernissen oder aus Opportunitätserwägungen – keine Geldbuße nach § 30 OWiG festgesetzt, kann eine selbstständige Einziehungsanordnung nach § 29a OWiG gegen das Unternehmen ergehen.⁸² Diese hat zum Ziel, den aus einer Straftat bzw. einer Ordnungswidrigkeit erlangten Vorteil abzuschöpfen. Die Einziehungsanordnung ist eine verschuldensunabhängige Maßnahme, die allein das Vorliegen einer tatbestandsmäßigen und rechtswidrigen Tatbegehung verlangt. Erfasst werden jedoch nur die unmittelbar aus der Tat erlangten Vorteile. Bei Steuerstraftaten bzw. Steuerordnungswidrigkeiten neigen die Ermittlungsbehörden dazu, den aus der Kapitalnutzung der verkürzten Steuern erlangten Zinsvorteil abzuschöpfen. Dabei geht die Finanzverwaltung nicht selten von einem Zinssatz von 0,5 % pro Monat aus. In Nr. 114 Abs. 1 Satz 5 AStBV (St) 2022 war noch geregelt, dass als Zinssatz mindestens von 0,5 % pro vollen Monat ausgegangen werden soll. Dies erkennt jedoch, dass über § 29a OWiG nicht dem Fiskus ein Nachteil ausgeglichen werden soll, sondern der wirtschaftliche Vorteil abgeschöpft wird. Soweit die – nicht unumstrittene – Möglichkeit der Abschöpfung eines Zinsvorteils angenommen wird, können nach § 29a OWiG demnach allenfalls die tatsächlich gezogenen Nutzungen und nicht ein fiktiver Zinsvorteil abgeschöpft werden, wobei Zinsen nach § 233a AO gegenzurechnen sind.⁸³ Ein abzuschöpfender Zinsvorteil hat sich somit stets an dem tatsächlichen Vorteil im jeweiligen Einzelfall zu orientieren. In der Neufassung der Nr. 114 Abs. 1 AStBV (St) 2023/2024 ist Satz 5 inzwischen ersatzlos gestrichen worden. Eine Einziehungsanordnung nach § 29a OWiG hat den Vorteil, dass kein individuelles Verschulden festzustellen ist, der Einziehungsbescheid gegen das Unternehmen ergeht und damit

82 Vgl. zur Einziehung auch → Böttger, Kap. 2 Rn. 164.

83 Randt, in: Joecks/Jäger/Randt, Steuerstrafrecht, § 377 AO Rn. 35.

die handelnden Personen „aus der Schusslinie“ sind sowie der eingezogene Betrag als Betriebsausgabe steuerlich abzugsfähig ist.

IV. Tax Compliance-System

Bei der Implementierung und Ausgestaltung eines Tax Compliance-Systems⁸⁴ sind im Wesentlichen sechs Kernelemente zu berücksichtigen:⁸⁵ **60**

- Analyse des unternehmensspezifischen Risikos sowie Erstellung eines Risikoprofils (Risikoanalyse);⁸⁶
- Vorbehaltloses und uneingeschränktes Bekenntnis der Unternehmensführung zur Rechtstreue („Commitment“);
- Klare Zuordnung von Zuständigkeiten und Verantwortungsbereichen und deren organisatorische Absicherung (Organisation und Kontrolle);
- Information und Schulung der Mitarbeiter (Kommunikation);
- Vorsorgliche Dokumentation der ergriffenen Maßnahmen (Dokumentation);
- Erfolgen eines systematischen und rollierenden Soll-Ist-Vergleichs (Überwachung und Verbesserung)

1. Risikoanalyse

Vor Einführung eines Tax Compliance-Systems ist eine eingehende Analyse des unternehmensspezifischen Risikos sowie die Erstellung eines Risikoprofils unabdingbar. In die Risikoanalyse sind Tochtergesellschaften und bei international agierenden Unternehmen auch Betriebstätten im Ausland einzubeziehen. Hierbei hat sich eine **zweistufige Herangehensweise** bewährt.⁸⁷ Im ersten Schritt erfolgt zum einen eine Bestandsaufnahme in Form einer formalen Betrachtung der steuerlichen Pflichtenerfüllung in der Vergangenheit (fristgemäßes Erklärungsverhalten, Nachzahlungen nach Außenprüfungen, Festsetzung von finanziellen Sanktionen, Ermittlungsverfahren gegen Verantwortliche des Unternehmens). Zum andern ist die bisherige Organisationsstruktur (z. B. Aufgabenverteilung, Geschäftsaufträge, Berichtswege, Kontrollmaßnahmen, Fortbildungsmaßnahmen) zu überprüfen. Im zweiten Schritt erfolgt die inhaltliche Auseinandersetzung mit den spezifischen materiell-rechtlichen Problemen des jeweiligen Unternehmens. Hierzu gehören neben den im ersten Schritt identifizierten Problemfeldern weitere unternehmensspezifische und branchenspezifische Einzel- **61**

⁸⁴ Zum Teil wird auch die gleichbedeutende Begrifflichkeit „Tax Compliance-Management-System“ verwendet. Eine Orientierungshilfe bei der Ausgestaltung eines Tax Compliance-Systems bietet auch der Prüfungsstandard IDW PS 980. Vgl. auch Hinweise der Bundessteuerberaterkammer für ein steuerliches innerbetriebliches Kontrollsystem – Steuer-IKS. Siehe zur Prüfung und Zertifizierung von Tax Compliance Systemen *Breimann/Schwetzel*, DStR 2017, 2626; *Fila/Püschel*, Newsdienst Compliance 2019, 210017.

⁸⁵ *Aichberger/Schwartz*, DStR 2015, 1758, 1763; *Geuenich/Kiesel*, BB 2012, 155. Zu den Kernelementen eines effektiven CMS siehe auch → *Schulz*, Kap. 1 Rn. 52 ff.

⁸⁶ Siehe vertiefend zur Risikobewertung, *Dahlke*, BB 2019, 619.

⁸⁷ *Aichberger/Schwartz*, DStR 2015, 1758, 1763.

themen (z. B. Grunderwerbsteuer bei Immobilienunternehmen). Ziel der Risikoanalyse ist es, dass sämtliche steuerlichen Pflichten des Unternehmens im In- und Ausland bekannt sind. Deren Einhaltung, Steuerung und Überwachung ist sodann durch geeignete und funktionierende Organisationsstrukturen sicherzustellen.

2. Ausgestaltung eines Tax Compliance-Systems

- 62** Ausgehend von den Ergebnissen der Risikoanalyse ist ein Tax Compliance-System an den jeweiligen Besonderheiten, Gegebenheiten und Bedürfnissen (z. B. Größe, Branche, Unternehmensstruktur) des einzelnen Unternehmens auszurichten. So kann ein Tax Compliance-System eines DAX-Konzerns⁸⁸ hinsichtlich Regelungsumfang und Regeldichte nicht mit dem eines mittelständischen Unternehmens vergleichbar sein. Nachstehend wird auf grundlegende Aspekte eingegangen, die sich in der Organisationsstruktur eines Tax Compliance-Systems wiederfinden lassen sollten.

a) Zuständigkeit für Tax Compliance

- 63** Der Bereich Compliance ist regelmäßig dem Gesamtvorstand unterstellt. Dies dürfte auch dem Urteil des Landgerichts München I vom 10.12.2013 geschuldet sein. So hat das Gericht ausgeführt, dass die Einhaltung des Legalitätsprinzips und demgemäß die Einrichtung eines funktionierenden Compliance-Systems zur Gesamtverantwortung des Vorstands gehört.⁸⁹ Dies gilt in gleicher Weise für die Tax Compliance, die in der Konzernorganisation jedoch zumeist dem Bereich Finanzen oder Steuern zugeordnet ist, der erfahrungsgemäß nicht dem Gesamtvorstand unterstellt ist. Zur Haftungsvermeidung (§ 93 Abs. 2 Satz 1 AktG) ist daher dringend zu empfehlen, die Verantwortlichkeit für Tax Compliance ebenfalls dem **Gesamtvorstand** zu unterstellen, was in der Konzernverfassung bzw. der Konzernorganisation entsprechend dokumentiert sein sollte.

b) Zuständigkeit und Verantwortlichkeit bzgl. der steuerlichen Pflichten

- 64** Unerlässlich sind klare Regelungen über die Zuständigkeiten und Verantwortlichkeiten zur Erfüllung sämtlicher steuerlicher Pflichten des Unternehmens, wozu auch die Meldezuständigkeiten nach §§ 137, 138 AO zählen. Zunächst ist die zulässige Delegation⁹⁰ der Erfüllung der steuerlichen Pflichten vom Vorstand auf die Fachbereiche durch einen eindeutigen **Vorstandsauftrag** (Geschäftsauftrag) zu dokumentieren. Dieser darf nicht auf die Steuerabteilung beschränkt sein, sondern muss sämtliche Bereiche umfassen, die steuerliche Pflichten des Unternehmens erfüllen. Zu denken ist bspw. an die Personalabteilung, sofern

⁸⁸ Siehe vertiefend zu Tax Compliance in Konzernen mit Matrix-Strukturen *Eggert*, DStR 2017, 266; zu Tax Compliance Systemen in der Praxis *Pull*, DStR 2022, 2132.

⁸⁹ LG München I, 10.12.2013 – 5 HK O 1387/10, NZWiSt 2014, 183.

⁹⁰ Siehe hierzu → *Böttger*, Kap. 2 Rn. 119 ff.

diese – wie häufig – die LohnSt zu verantworten hat. Der Geschäftsauftrag sollte zum einen regeln, welche Konzerngesellschaften durch die Steuerabteilung betreut werden und zum andern detailliert beschreiben, welche steuerrelevanten Themen von den einzelnen Bereichen verantwortet werden (sog. Funktionsabgrenzung). Es sollten Zuständigkeitsregelungen u. a. für folgende Themen festgelegt werden:

- Erklärungs- und Meldewesen der im Unternehmen relevanten Steuerarten (ggf. unter Einbeziehung von Tochtergesellschaften);
- Erfüllung der steuergesetzlichen Dokumentationserfordernisse (einschließlich Verrechnungspreisdokumentation);
- Begleitung von Betriebsprüfungen;
- Überwachung und Analyse von Gesetzes- und Rechtsprechungsänderungen sowie von Verwaltungserlassen;
- Bekanntmachung gesetzlicher Neuerungen;
- Ansprechpartner für allgemeine Fragen und Sonderfragen des Steuerrechts.

Daneben sind eindeutige und detaillierte Aufgabenbeschreibungen (**Stellenbeschreibungen**) empfehlenswert, aus denen erkennbar wird, welche Unterabteilung bzw. welche konkreten Mitarbeiter zur Erfüllung der jeweiligen steuerlichen Pflichten verantwortlich sind. Bei der Delegation der Erfüllung der steuerlichen Pflichten sollte größter Wert auf klar strukturierte und dokumentierte Delegationsketten gelegt werden, da durch die Delegation eine Exkulpation der originär Verantwortlichen erreicht werden kann, sofern diese der sich aus der Delegation ergebenden Auswahl-, Instruktions- und Überwachungspflicht nachkommen.⁹¹ **65**

c) Berichtswege/Berichtspflichten

Im Hinblick auf die Entscheidung des Landgerichts München I vom 10.12.2013⁹² sollte die **Tax Compliance-Berichterstattung** an den Gesamtvorstand erfolgen. Denn nur soweit der Gesamtvorstand von wesentlichen Tax Compliance-Sachverhalten Kenntnis erlangt, ist er in der Lage, seine Sorgfaltpflichten zu erfüllen. Ferner sind turnusmäßige (z. B. quartalsweise) Tax Compliance-Berichterstattungen an den Gesamtvorstand zu empfehlen, die eine angemessene schnelle Reaktion auf etwaige Tax Compliance-Fälle ermöglichen. Darüber hinaus sind anlassbezogene Berichte an den Gesamtvorstand notwendig, soweit die Umstände dies erfordern. **66**

Des Weiteren sind eindeutige Regelungen zu den Berichtsstrukturen unabdingbar. So ist zu gewährleisten, dass die für die Erfüllung der steuerlichen Pflichten erforderlichen Tatsachen auch rechtzeitig und vollständig der Steuerabteilung bzw. der zuständigen Fachabteilung mitgeteilt werden. Nicht selten werden in der Praxis objektiv fehlerhafte Steuererklärungen bzw. Steueranmeldungen ab- **67**

⁹¹ Aichberger/Schwartz, DStR 2015, 1758 ff.

⁹² LG München I, 10.12.2013 – 5 HK O 1387/10, NZWiSt 2014, 183.

gegeben, weil die Steuerabteilung nicht hinreichend in die Prüfung des zugrunde liegenden Sachverhalts einbezogen wurde. Es empfiehlt sich daher die Implementierung einer **Unterrichtungspflicht an die Steuerabteilung** in allen steuerrelevanten Sachverhalten bzw. bei steuerlichen Unklarheiten und Zweifelsfällen (z. B. in Form einer sog. Einbindungsrichtlinie). Daneben sind Melde- und Berichtspflichten an die Steuerabteilung bzw. die zuständige Fachabteilung u. a. in folgenden Fallkonstellationen ratsam:

- Vertrieb eines neuen Produkts (zur Prüfung auf etwaige steuerliche Implikationen);
- Wirtschaftlich besonders relevante Geschäftsvorfälle und grundsätzliche Entscheidungen (z. B. Abschluss von Rahmenverträgen);
- Umstrukturierungen (z. B. Umwandlungen, Anwachsungen, Anteilsvereinigungen, Änderungen des Gesellschafterbestands);
- Kauf von Gesellschaften bzw. Erwerb von Anteilen an Gesellschaften;
- Verkauf von Konzerngesellschaften bzw. von Anteilen an Konzerngesellschaften;
- Änderung einer durch die Steuerabteilung freigegebenen Musterklausel (z. B. Umsatzsteuer-Klausel im Kaufvertrag);
- Leistungsvereinbarungen zwischen Konzerngesellschaften;
- Gründung einer Niederlassung, Betriebstätte im Ausland;
- Fachabteilung erkennt nachträglich, dass der Steuerabteilung steuerlich erhebliche Tatsachen nicht mitgeteilt wurden (zur Anzeige nach § 153 AO);
- Verträge mit „ausländischen“ (beschränkt steuerpflichtigen) Vergütungsempfängern zur Steueranmeldung nach § 50a EStG (z. B. Nutzungsüberlassungsverträge mit Lizenzzahlungen, Aufsichtsratsvergütungen).

68 An die für die **LohnSt** zuständige Abteilung sollten u. a. in folgenden Fällen Melde- und Berichtspflichten bestehen:

- Jede Geldzuwendung an Arbeitnehmer (unabhängig von der Höhe der Zuwendung);
- Sachbezüge/geldwerte Vorteile an Arbeitnehmer (z. B. Geschenke mit Ausnahme von Aufmerksamkeiten bis zu einem Wert von 60 EUR, wie Blumen, Genussmittel, Bücher oder Tonträger, die dem Arbeitnehmer oder seinen Angehörigen aus Anlass eines besonderen persönlichen Ereignisses zugewendet werden; Gutscheine; Betriebsveranstaltungen wie etwa Betriebsausflüge, Sommerfeste, Weihnachtsfeiern, Jubiläumsfeiern; Sachprämien; Incentive-Veranstaltungen);
- Drittzusendungen an Arbeitnehmer bei Sachzusammenhang mit dem Arbeitsvertrag (Arbeitslohn von dritter Seite) wie z. B. Geschenke oder Rabatte von Dritten; insoweit ist empfehlenswert, die Rechts- oder Compliance-Abteilung zur Weitergabe entsprechender Compliance-Meldungen zu verpflichten;
- Geldwerte Zuwendungen an Geschäftspartner und deren Arbeitnehmer (zur Pauschalbesteuerung nach § 37b EStG) wie z. B. Sachgeschenke, Einladungen zu sportlichen oder kulturellen Veranstaltungen, Incentive-Reisen;

- Aktienoptionsprogramme für Mitarbeiter.

Im Rahmen von Organschaften sind zur Gewährleistung des Informationsflusses auch die Tochtergesellschaften in die Berichtsstrukturen einzubeziehen (Mutter-Tochter-Dialog). Ein Bericht bzw. eine Anfrage an die für das jeweilige Steuerrechtsgebiet zuständige Abteilung sollte eine vollständige Sachverhaltsdarstellung sowie die relevanten Dokumente enthalten. **69**

d) Prozessbeschreibung Deklarationswesen

Zu den steuerlichen Kernaufgaben – wie dem Deklarationswesen – sollten detaillierte Prozessbeschreibungen existieren. Erfahrungsgemäß bestehen in Unternehmen zumindest Richtlinien zu folgenden Themen: Ertragsteuererklärungen, Umsatzsteuer, Lohnsteuer, Verrechnungspreise, Betriebsprüfung. Die Prozessbeschreibungen sollten nicht nur Regelungen zur Erstellung der Steuererklärungen, sondern auch zur Fristenkontrolle, zur Zahlungsüberwachung sowie zur Prüfung der Steuerbescheide als auch zu Rechtsbehelfen enthalten. Daneben bieten sich folgende Regelungen an: **70**

- Plausibilitätskontrolle und Verprobung gemäß Vier-Augen-Prinzip, Vermerk der Kontrollmaßnahme z. B. auf Review-Sheet;
- Zuständigkeit, Verantwortlichkeit der Daten- und Belegzusammenstellungen sowie der rechtzeitigen Übermittlung bei Beauftragung externer Berater;
- Zuständigkeit, Verantwortlichkeit für die Datenzulieferung aus Konzerngesellschaften;
- Unterzeichnung der Steuererklärungen gem. § 150 Abs. 3 AO i.V.m. Einzelsteuergesetzen (gemäß den gesetzlichen Vorgaben hat der Vorstand die KSt-Erklärungen [§ 31 KStG], die GewSt-Erklärungen [§ 14a Satz 2 GewStG], die USt-Jahreserklärungen [§ 18 Abs. 3 Satz 3 UStG] und die Erklärungen zur gesonderten und einheitlichen Feststellung der Einkünfte [§ 25 Abs. 3 EStG, § 180 AO] zu unterzeichnen);
- Vorstandsinformation (von einem „blinden“ Unterschreiben der Steuererklärungen durch den Vorstand ist dringend abzuraten; empfehlenswert ist ein Vorstandsreport durch den Steuerabteilungsleiter).

e) Kontroll- und Überwachungsmaßnahmen

Eine ordnungsgemäße Pflichtendelegation setzt Kontroll- und Überwachungsmaßnahmen voraus. Deren Umfang lässt sich nicht allgemeingültig definieren. Er richtet sich vielmehr nach der Qualifikation und der Zuverlässigkeit der Mitarbeiter. Allgemein gilt, dass die Nachprüfungspflicht umso größer ist, je mehr Grund zu der Annahme besteht, dass Mitarbeiter unzuverlässig sind oder den fachlichen Anforderungen nicht gewachsen sind. Bei erfahrenen Mitarbeitern fällt der Umfang der Nachprüfungspflicht geringer aus, als bei neu eingestellten Mitarbeitern. So gilt der Grundsatz: Je höher qualifiziert ein Mitarbeiter ist, umso geringer ist die Kontrollpflicht und umgekehrt. Maßgeblich ist ferner, ob und **71**

in welchem Umfang es in der Vergangenheit zu Unrichtigkeiten oder Beanstandungen gekommen ist.

- 72 Eine besondere Problematik stellt sich bei der **steuerlichen Organschaft**.⁹³ Hierbei ist der Organträger zur Erfüllung seiner steuerlichen Erklärungspflichten auf die „Zulieferung“ der Organgesellschaft angewiesen. Die Schwierigkeit als auch die Risiken für den Organträger bestehen demnach darin, dass er zur Erfüllung seiner steuerlichen Erklärungspflichten auf Zahlenmaterial angewiesen ist, das von einer anderen – jedenfalls zivilrechtlich selbstständigen – Gesellschaft ermittelt wurde und für den Organträger kaum zu überprüfen ist. Gleichwohl hat der Organträger dafür Sorge zu tragen, dass die von ihm abgegebenen Steuererklärungen vollständige und richtige Angaben enthalten. Das zugelieferte Zahlenmaterial sollte daher nicht gänzlich ungeprüft übernommen werden. Zumindest Stichproben sind regelmäßig indiziert.
- 73 Neben den Kontroll- und Überwachungsmaßnahmen ist sicherzustellen, dass eine hinreichende **personelle Ausstattung der Steuerabteilung** gegeben ist. Die Steuerabteilung muss der Größe des Unternehmens sowie der ihr übertragenen Aufgaben entsprechend aufgestellt sein (Investitionspflicht). Dabei ist die Anzahl der erforderlichen Mitarbeiter u. a. auch davon abhängig, in welchem Umfang die Erfüllung der steuerlichen Pflichten auf Externe übertragen wird. In der Praxis ist nicht selten eine Unterbesetzung der Steuerabteilungen festzustellen, was bei auftretenden Unregelmäßigkeiten bereits ein Organisationsverschulden begründen kann. Insoweit ist von dem Versuch abzuraten, Unregelmäßigkeiten mit einer Überlastung oder personellen Unterbesetzung der Steuerabteilung zu begründen. Auf Personalmangel und auf erfolglose Bemühungen zur Einstellung weiterer Mitarbeiter kann sich der Betroffene grundsätzlich nicht berufen.⁹⁴

f) Umgang mit Betriebsprüfungen

- 74 Betriebsprüfungen sollten durch Unternehmen professionell vorbereitet und begleitet werden. Hierzu ist eine **Richtlinie empfehlenswert**, die den grundsätzlichen Umgang mit Betriebsprüfungen regelt. Darin sollten insbesondere Regelungen zu folgenden Aspekten getroffen werden:
- Vorbereitung der Betriebsprüfung (z. B. Prüfung von Buchführung, Bilanzen, Vertragsgestaltungen des Prüfungszeitraums, ggf. Anzeige nach § 153 AO, ggf. Prüfung einer Selbstanzeigemöglichkeit nach § 378 Abs. 3 AO, Durchsicht des Berichts der vorhergehenden Betriebsprüfung, Zusammenstellung benötigter Unterlagen);
 - Benennung einer Auskunftsperson nach § 8 BpO (mit dem Ziel eines einheitlichen Auftretens und Argumentierens gegenüber der Betriebsprüfung);

⁹³ Vgl. hierzu *Schauff/Schwartz*, ZWH 2013, 212.

⁹⁴ OLG Nürnberg, 30.3.2022 – 12 U 1520/19, NZG 2022, 1058.

- Instruktion von Mitarbeitern, die möglicherweise Kontakt mit den Betriebsprüfern haben (z. B. keine Beantwortung von Fragen, sondern Verweis an die Auskunftsperson);
- Rechtliche Kontrolle der Prüfungsanordnung;
- Dokumentation von Fristsetzungen der Betriebsprüfung (u. a. zur Vermeidung eines Verzögerungsgeldes nach § 146 Abs. 2b AO);
- Verhaltensregelungen bei Auftreten tatsächlicher Anhaltspunkte für Steuerstraftaten oder Steuerordnungswidrigkeiten während der laufenden Betriebsprüfung;
- Abstimmung der künftigen Handhabe mit der Finanzverwaltung, ggf. Antrag auf verbindliche Zusage nach § 204 AO;
- Verhaltensregelungen und Maßnahmen im Rahmen einer stattfindenden Schlussbesprechung mit der Betriebsprüfung nach § 201 Abs. 1 AO;⁹⁵
- Rechtsbehelfsverfahren gegen Prüfungsfeststellungen.

Im Rahmen der Schlussbesprechung ist darauf zu achten, welche Ergebnisse und ggf. etwaige Hinweise gegeben bzw. festgehalten werden. Dies hat nicht zuletzt Auswirkungen auf ein sich daran anschließendes Rechtsbehelfsverfahren oder eine Berichtigung gem. § 153 Abs. 4 AO. Die sog. Fortschreibungspflicht⁹⁶ nach dem Wortlaut des § 153 Abs. 4 AO gilt generell für sämtliche Zeiträume, sowohl vor als auch nach der jeweiligen relevanten Betriebsprüfung. In der Schlussbesprechung sowie im darauf folgenden Betriebsprüfungsbericht sollte festgehalten werden, für welchen Zeitraum und für welche konkreten Sachverhalte eine etwaige Fortschreibungspflicht besteht. Dadurch minimiert sich für den Steuerpflichtigen das Risiko eines steuerstrafrechtlichen Vorwurfs.⁹⁷ 75

Ein Kernelement einer Richtlinie Betriebsprüfung ist ferner die Anweisung, **jeden Betriebsprüfungsbericht** auf Beanstandungen **auszuwerten** und durch geeignete Maßnahmen sicherzustellen, dass diese künftig unterbunden werden. Die Umsetzung dieser Maßnahmen sollte zwingend kontrolliert werden. Kam es in der Vergangenheit bereits zu Unrichtigkeiten oder Beanstandungen, bestehen insoweit gesteigerte Anforderungen an die Überwachungs- und Kontrollpflicht. Treten in einer späteren Betriebsprüfung die gleichen Beanstandungen erneut auf, wird in der Verfahrenspraxis schnell ein vorsätzliches Handeln (Eventualvorsatz) unterstellt. Dies zeigt beispielhaft der nachstehende Auszug aus einem Durchsuchungsbeschluss: 76

„Den seinerzeit Verantwortlichen der [...] waren die zahlreichen und eklatanten Mängel in der Buchführung auch bekannt, da bereits bei der vorherigen Betriebsprüfung den Verantwortlichen diese Mängel durch die Prüfer mitgeteilt wurden. Da im aktuellen Prüfungszeitraum erneut erhebliche Mängel festgestellt wurden, besteht der Verdacht, dass seitens der Betroffenen auf die

⁹⁵ Dies gilt nicht für den Fall einer abgekürzten Betriebsprüfung, vgl. § 203 Abs. 2 AO.

⁹⁶ Vgl. *Busch*, DB 2023, 1562 ff.

⁹⁷ Siehe hierzu ausführlich bei *Stürzl/Forster*, GmbH-Steuerpraxis 1/2024, 8 ff.

Misstände nicht bzw. jedenfalls nicht im erforderlichen Umfang durch erhöhte oder verbesserte Aufsichtsmaßnahmen und organisatorische Maßnahmen reagiert wurde bzw. die Wirksamkeit evtl. ergriffener Maßnahmen nicht ausreichend kontrolliert wurde.“

- 77 Neben der etwaigen Anpassung der laufenden Deklaration sowie der Steuerrückstellungen ist ebenfalls zu prüfen, ob sich aus dem Betriebsprüfungsbericht im Hinblick auf bereits eingereichte bzw. veranlagte Steuererklärungen Handlungspflichten ergeben (ggf. Anzeige nach § 153 AO, siehe dazu → Rn. 21 ff.).

g) Schulungen

- 78 Die ordnungsgemäße Organisation erfordert die Sicherstellung einer hinreichenden fortlaufenden Schulung der Mitarbeiter. Der (Mindest-)Umfang der jährlichen Schulungen sollte verbindlich festgelegt sein. In Betracht kommen unternehmensinterne oder externe Schulungen. Die Fortbildungsmaßnahmen der einzelnen Mitarbeiter sollten mit Nachweisen jährlich dokumentiert werden. Daneben empfiehlt es sich, dass die Steuerabteilung z. B. im Rahmen von Newslettern oder Rundschreiben über aktuelle steuerliche Fragen und Neuerungen informiert. Ferner kann eine Support-Hotline durch Mitarbeiter der Steuerabteilung sinnvoll sein.

h) Dokumentation

- 79 Von entscheidender Bedeutung ist schließlich eine hinreichende Dokumentation der unternommenen Maßnahmen. Nur so kann möglichen Vorwürfen – insbesondere nach §§ 130, 30 OWiG – effektiv entgegengetreten werden. Das LG München I hat in einer gesellschaftsrechtlichen Entscheidung zudem entschieden, dass der Vorstand einer Aktiengesellschaft nach § 91 Abs. 2 AktG nicht nur verpflichtet wird, ein Frühwarn- und Überwachungssystem einzurichten, sondern darüber hinaus auch eine Rechtspflicht besteht, dieses System zu dokumentieren.⁹⁸ Das Erfordernis der Dokumentation gilt für die allgemeinen Richtlinien und Grundsätze ebenso wie für die auf Grundlage der Richtlinien getroffenen Einzelmaßnahmen. In der Praxis hat sich ein **Organisationshandbuch Steuern** (Tax Compliance Manual) bewährt, das sich sowohl an Mitarbeiter der Steuerabteilung als auch an andere Bereiche richtet, die steuerlich relevante Aufgaben wahrnehmen (z.B. Controlling, Recht, Rechnungswesen, Personalabteilung, Einkauf usw.). Die Dokumente, die die Organisationsstrukturen regeln und beschreiben, sollten zudem jedem Mitarbeiter dauerhaft und leicht zugänglich gemacht werden. Insoweit empfiehlt sich z.B. eine Veröffentlichung der Dokumente im Intranet.

98 LG München I, 5.4.2007 – 5 HKO 15964/06, DStR 2008, 519.

3. Prüfungserleichterungen nach Art. 97 § 38 EGAO

Mit dem DAC7-Umsetzungsgesetz vom 20.12.2022⁹⁹ hat der Gesetzgeber in Art. 97 § 38 EGAO eine zunächst bis zum Jahr 2029 befristete Erprobungsregelung zur Gewährung von **Prüfungserleichterungen in der Außenprüfung** bei vorhandenem Steuerkontrollsystem eingeführt, die am 1.1.2023 in Kraft getreten ist. Durch diese Neuregelung sollen für den Steuerpflichtigen Anreize zur **freiwilligen Installation eines Steuerkontrollsystems** geschaffen werden, um dadurch eine verstärkte Kooperation zwischen den Verfahrensbeteiligten und einen beschleunigten Ablauf der Betriebsprüfung zu erzielen. 80

Als Folge der Neuregelung käme einem Tax CMS neben seiner bisherigen haftungsrechtlichen Dimension auch eine praxisrelevante Dimension im Bereich der Außenprüfung zu. Es bleibt jedoch abzuwarten, wie die Finanzverwaltung die Neuregelung in der Praxis handhabt. Gerade auf der Rechtsfolgenrechtsseite ist aufgrund der unbestimmten Rechtsbegriffe eine Konkretisierung durch die Finanzverwaltung und die Rechtsprechung notwendig, damit der Steuerpflichtige die sich aus § 38 EGAO ergebenden Vorteile der Einrichtung eines Tax CMS erkennt und in der Praxis auch tatsächlich erlangt. 81

a) Tatbestandsvoraussetzungen

§ 38 Abs. 1 Satz 1 EGAO setzt voraus, dass im Rahmen einer Außenprüfung eines Steuerpflichtigen nach den §§ 193 bis 202 AO die Wirksamkeit eines von ihm eingesetzten Steuerkontrollsystems hinsichtlich der erfassten Steuerarten oder Sachverhalte überprüft wurde und kein oder nur ein unbeachtliches steuerliches Risiko für die in § 149 Abs. 3 AO genannten Steuern und gesonderten Feststellungen besteht. 82

Zunächst setzt § 38 Abs. 1 EGAO voraus, dass der Steuerpflichtige ein **Steuerkontrollsystem** einsetzt. Die Anforderungen des Gesetzgebers an ein solches Steuerkontrollsystem werden in § 38 Abs. 2 Satz 1 EGAO näher erläutert. Hiernach muss ein Steuerkontrollsystem alle innerbetrieblichen Maßnahmen umfassen, die gewährleisten, dass die Besteuerungsgrundlagen zutreffend aufgezeichnet und berücksichtigt werden (Nr. 1) und die hierauf entfallenden Steuern fristgerecht und vollständig abgeführt werden (Nr. 2). § 38 Abs. 2 Satz 2 EGAO verlangt, dass das Steuerkontrollsystem die steuerlichen Risiken laufend abbildet. Diese Anforderungen an ein Steuerkontrollsystem decken sich inhaltlich mit den Anforderungen an ein Tax-Compliance-Management-System nach dem IDW-Praxishinweis 1/2016, der zur Konkretisierung des IDW PS 980 entwickelt wurde.¹⁰⁰ 83

Des Weiteren verlangt § 38 Abs. 1 EGAO, dass im Rahmen einer Außenprüfung die Wirksamkeit des Steuerkontrollsystems hinsichtlich der maßgeblichen 84

⁹⁹ BGBl. 2022 I, S. 2730.

¹⁰⁰ Vgl. etwa Tz. 5 und 8 des IDW-Praxisinweises 1/2016; Hölzemann/Ramadan/Otto/Nordmann, WPG 2023, 1394.

Steuerarten und Sachverhalte geprüft wurde (**Wirksamkeitsprüfung**). Hieraus folgt zum einen, dass die Prüfungshandlung im Rahmen einer ersten Außenprüfung zu erfolgen hat, die zeitlich der zweiten Außenprüfung vorangestellt ist, für die der Antragsteller eine Erleichterung nach § 38 Abs. 1 EGAO begehrt.¹⁰¹ Zum anderen macht die Formulierung „im Rahmen der Außenprüfung“ deutlich, dass die Wirksamkeitsprüfung des Steuerkontrollsystems zwingend **durch die Finanzverwaltung** selbst zu erfolgen hat und nicht durch einen externen Steuerberater oder Wirtschaftsprüfer vorgenommen werden kann. Damit wird das unternehmensinterne Tax-Compliance-Management-System zum Gegenstand der Außenprüfung.¹⁰²

- 85** Schwierigkeiten werfen allerdings Fragen nach dem Inhalt und Ablauf der Wirksamkeitsprüfung auf, da § 38 EGAO hierzu keinerlei Regelungen normiert, sondern die **Konkretisierung der Anforderungen der Finanzverwaltung überlässt**. In der Literatur wird teilweise auf die Möglichkeit verwiesen, sich im Rahmen der Wirksamkeitsprüfung an den Anforderungen des IDW-PS 980 bzw. des IDW-Praxishinweises 1/2016 und der darin angelegten Unterscheidung zwischen Angemessenheit und Wirksamkeit zu orientieren.¹⁰³ Zudem empfiehlt es sich, der Finanzverwaltung auch ohne gesetzliche Vorlagepflicht eine dem IDW-Prüfungsstandard entsprechende Testierung des Tax CMS vorzulegen, um so eine reibungslose Prüfung zu ermöglichen.¹⁰⁴
- 86** Zudem darf **kein oder nur ein unbeachtliches steuerliches Risiko** für die in § 149 Abs. 3 AO genannten Steuern und besonderen Feststellungen bestehen. Unter dem Begriff der Steuerrisiken lassen sich grundsätzlich alle Unsicherheiten zusammenfassen, die sich negativ auf Steuerzahlungen auswirken bzw. auswirken können.¹⁰⁵ Bezogen auf § 38 EGAO bedeutet dies, dass steuerliche Risiken sämtliche Umstände bilden, auf Basis derer die zutreffende Aufzeichnung und Berücksichtigung der Besteuerungsgrundlagen und damit die Überprüfbarkeit im Rahmen einer Außenprüfung als gefährdet zu betrachten ist und die eine tatbestandsgetreue Festsetzung und Erhebung von Steuern beeinträchtigen können.¹⁰⁶ Was hingegen unter dem Begriff der „Unbeachtlichkeit“ des steuerlichen Risikos zu verstehen ist, wird im Gesetz nicht näher erläutert, sodass diesbezüglich noch Klärungsbedarf besteht.¹⁰⁷
- 87** Gemäß § 38 Abs. 1 Satz 1 EGAO steht die behördliche Zusage von Ermittlungsbeschränkungen unter der Voraussetzung, dass **keine Änderung der Verhält-**

101 Hölzemann/Ramadan/Otto/Nordmann, WPg 2023, 1394.

102 Seer, IWB 2023, 950.

103 Seer, IWB 2023, 950; Feuerstack/Reimann, StBp 2023, 184; Hölzemann/Ramadan/Otto/Nordmann, WPg 2023, 1394.

104 Feuerstack/Reimann, StBp 2023, 184; Hölzemann/Ramadan/Otto/Nordmann, WPg 2023, 1394.

105 Sradj, DStR 2022, 568.

106 Feuerstack/Reimann, StBp 2023, 184.

107 Feuerstack/Reimann, StBp 2023, 184.

nisse eintritt. Ob damit nur Veränderungen am Steuerkontrollsystem selbst oder auch Veränderungen des zu erhebenden steuerrechtlich relevanten Sachverhalts oder der Rechtslage gemeint sind, lässt sich dem Gesetzeswortlaut nicht eindeutig entnehmen.¹⁰⁸ Zudem muss der Steuerpflichtige nach § 38 Abs. 1 Satz 2 EGAO Veränderungen des Kontrollsystems dokumentieren und sie der Finanzbehörde unverzüglich schriftlich oder elektronisch mitteilen.

Der **Steuerpflichtige** kann die Erleichterungen bei der Außenprüfung nach § 38 Abs. 1 Satz 1 EGAO nur erlangen, wenn er bei den Finanzbehörden einen entsprechenden **Antrag** stellt. Hierbei ist allerdings zu beachten, dass dieses Antragsrecht nach dem Wortlaut des § 38 Abs. 1 Satz 1 EGAO erst nach der zuvor durchgeführten Wirksamkeitsprüfung des Steuerkontrollsystems durch die Finanzverwaltung besteht. Somit stellt sich die Frage, ob der Steuerpflichtige bereits im Vorfeld einen Anspruch auf die Durchführung der Wirksamkeitsprüfung seines Tax CMS durch die Finanzbehörden hat, damit er im Anschluss einen Antrag auf Prüfungserleichterung stellen kann. Aus dem Wortlaut des § 38 EGAO folgt ein solcher Anspruch nicht. Zwar ließe sich in Erwägung ziehen, dass sich der Anspruch aus § 199 Abs. 1 AO ergeben könnte, wonach der Außenprüfer die Besteuerungsgrundlagen zugunsten wie zuungunsten des Steuerpflichtigen zu prüfen hat. Dass sich hieraus aber auch eine umfassende Pflicht der Finanzverwaltung zur vollständigen Prüfung des Kontrollsystems im Sinne des § 38 Abs. 1 EGAO ergibt, erscheint zweifelhaft.¹⁰⁹ Damit hätte der Steuerpflichtige zwar ein Antragsrecht nach durchgeführter behördlicher Wirksamkeitsprüfung, aber keinen Anspruch auf deren Durchführung, wodurch seine Rechtsstellung geschmälert wird und in der Folge die Gefahr besteht, dass die neu eingeführte Regelung des § 38 EGAO in der Praxis ins Leere läuft.¹¹⁰

b) Rechtsfolgen

Liegen die Tatbestandsvoraussetzungen des § 38 EGAO vor, so kann die Finanzverwaltung dem Steuerpflichtigen im Benehmen mit dem Bundeszentralamt für Steuern unter dem Vorbehalt des Widerrufs **für die nächste Außenprüfung Beschränkungen von Art und Umfang der Ermittlungen verbindlich zusagen**.⁸⁹

Die behördliche Zusage führt zu „Beschränkungen von Art und Umfang der Ermittlungen“ in der nächsten Außenprüfung. Allerdings lässt sich dem Normtext nicht entnehmen, welche konkreten Prüfungserleichterungen davon erfasst sind, sodass hier noch Klärungsbedarf besteht. In der Literatur wird zum Teil vorgeschlagen, zur Konkretisierung der Rechtsfolgen des § 38 EGAO eine Parallele zur Gesetzesbegründung der kooperativen Außenprüfung nach § 199 Abs. 2 Satz 3 AO n.F.¹¹¹ zu ziehen. Als mögliche Prüfungserleichterungen kämen demnach

¹⁰⁸ Feuerstack/Reimann, StBp 2023, 184.

¹⁰⁹ Feuerstack/Reimann, StBp 2023, 184.

¹¹⁰ Seer, IWB 2023, 950; Feuerstack/Reimann, StBp 2023, 184.

¹¹¹ BT-Drs. 20/3436, S. 91.

etwa die **Festlegung eines Prüfungsplans** oder die **Aussparung bestimmter Prüfungsfelder** in Betracht.¹¹²

- 91 Aus der Formulierung „kann“ folgt, dass der Behörde auf Rechtsfolgende ein **Ermessen** eingeräumt wurde, sodass dem Steuerpflichtigen auch bei Vorliegen aller Tatbestandsvoraussetzungen kein gebundener Anspruch auf Zusage der Prüfungserleichterungen zusteht.¹¹³ Diese gesetzgeberische Zurückhaltung bei der Ausgestaltung der Rechtsfolge des § 38 EGAO wird auf seinen Charakter als Erprobungsregelung zurückgeführt.¹¹⁴ Um eine zweckmäßige Handhabung des § 38 EGAO zu gewährleisten, wird in der Literatur deshalb vorgeschlagen, bei Erfüllung des Tatbestandes ein intendiertes Ermessen¹¹⁵ oder gar eine Ermessensreduzierung auf Null¹¹⁶ anzunehmen.

V. Zertifizierung des Tax Compliance-Systems durch Dritte

- 92 Kommt es trotz Implementierung eines Tax Compliance-Systems zur Abgabe objektiv unzutreffender bzw. unvollständiger Steuererklärungen, ist damit zu rechnen, dass die hinreichende Ausgestaltung und damit der Vorsatz- bzw. Leichtfertigkeitsschluss durch Ermittlungsbehörden in Zweifel gezogen wird. Insoweit kann durch eine Zertifizierung des Tax Compliance-Systems durch qualifizierte Dritte zusätzliche Rechtssicherheit gewonnen werden.
- 93 Die Bedeutung einer Zertifizierung der Prüfung des Tax Compliance-Systems ist im Hinblick auf eine strafrechtliche Enthaltung m. E. an den Grundsätzen des unvermeidbaren Verbotsirrtums nach § 17 StGB (bzw. § 11 Abs. 2 OWiG) zu bestimmen. Holt sich der Täter Rechtsrat ein, der sich nachträglich als unzutreffend erweist, stellt sich die Frage, ob der Täter im unvermeidbaren Verbotsirrtum und damit ohne Schuld handelte. Hierzu besteht eine umfassende Rechtsprechung. Ähnlich der Einholung von Rechtsrat zielt auch die Beauftragung der Prüfung und Zertifizierung des Tax Compliance-Systems darauf ab, sich rechtskonform zu verhalten und Strafbarkeitsrisiken auszuschließen. Insoweit stellt sich in gleichem Maße die Frage, inwieweit die Inanspruchnahme einer Tax Compliance-Beratung und -Prüfung die Vorwerfbarkeit auszuschließen vermag, wenn entgegen der Zertifizierung kein hinreichendes Tax Compliance-System gegeben sein sollte.
- 94 Wird ein Tax Compliance-System von den Ermittlungsbehörden als nicht hinreichend bewertet, obwohl zuvor eine beanstandungslose Prüfung und Zertifizierung durch qualifizierte Berater erfolgte, fehlt es in der Regel an einem schuldhaften Handeln. Es scheint schwer vorstellbar, einem Unternehmensleiter, der sowohl ein Tax Compliance-System implementiert hat als auch eine Prüfung

112 Kowallik, DB 2023, 804; Hölzemann/Ramadan/Otto/Nordmann, WPg 2023, 1394.

113 Feuerstack/Reimann, StBp 2023, 184.

114 Seer, IWB 2023, 950.

115 Seer, IWB 2023, 950.

116 Feuerstack/Reimann, StBp 2023, 184.

und Zertifizierung durch einen qualifizierten externen Berater vornehmen ließ, ernsthaft vorzuwerfen, nicht alles Erforderliche getan zu haben, um die Abgabe objektiv unzutreffender Steuererklärungen zu vermeiden. Vielmehr wird durch die Prüfung und Zertifizierung des Tax Compliance-Systems einmal mehr der Wille der Unternehmensleitung bezeugt, Rechtsverstößen wirksam vorzubeugen.

Überträgt man die Rechtsprechungsgrundsätze zu § 17 StGB auf die Zertifizierung eines Tax Compliance-Systems kommen als qualifizierte Prüfer grundsätzlich Steuerberater, Wirtschaftsprüfer und Rechtsanwälte mit entsprechender Expertise auf dem Gebiet der Tax Compliance in Betracht. Da es sich bei der Beurteilung von Tax Compliance-Systemen um eine Spezialmaterie handelt, ist die entsprechende Qualifikation des Prüfers bzw. des Prüferteam von besonderer Bedeutung. Neben steuerlichen Kenntnissen setzt dies auch ausreichenden juristischen Sachverstand voraus, da die Normen (§§ 370, 378 AO, §§ 130, 30, 29a OWiG), deren Verwirklichung es zu vermeiden gilt, dem Straf- bzw. Ordnungswidrigkeitenrecht zugehörig sind. Ferner sollte darauf geachtet werden, dass schon der Eindruck vermieden wird, dass der Prüfer die erforderliche Objektivität nicht aufweisen könnte. Die Beauftragung des langjährigen Abschlussprüfers des Unternehmens mit der Zertifizierung sollte daher zuvor äußerst kritisch geprüft werden, da sich aufgrund seiner Vorbefassung mit dem Sachverhalt Zweifel an seiner Unabhängigkeit ergeben können. **95**

Ebenso wie eher zur Absicherung als zur Klärung bestellte Gefälligkeitsgutachten als Grundlage eines unvermeidbaren Verbotsirrtums ausscheiden, vermag auch eine Zertifizierung mit „Feigenblattfunktion“ die straf- und bußgeldrechtliche Vorwerfbarkeit nicht auszuschließen. Ähnlich einem Gutachten sollten der Prüfungsauftrag, die durchgeführten Prüfungshandlungen (Gegenstand, Art und Umfang der Prüfung), die Prüfungsfeststellungen sowie das Prüfungsurteil im Detail schriftlich festgehalten werden. Um dem Maßstab, den der BGH an die Erteilung einer verlässlichen Auskunft stellt (pflichtgemäße Prüfung der Sach- und Rechtslage in verantwortungsbewusster Weise), gerecht zu werden, ist m. E. eine tiefgehende und umfassende Prüfung des Tax Compliance-Systems erforderlich. **96**

Bei der Prüfung eines Tax Compliance-Systems wird zwischen Angemessenheitsprüfungen und Wirksamkeitsprüfungen unterschieden. Die Angemessenheitsprüfung zielt auf die Beurteilung ab, **97**

„ob die in der CMS-Beschreibung enthaltenen Aussagen über die Grundsätze und Maßnahmen des CMS in allen wesentlichen Belangen angemessen dargestellt sind, dass die dargestellten Grundsätze und Maßnahmen in Übereinstimmung mit den angewandten CMS-Grundsätzen geeignet sind, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern und dass die Grundsätze und Maßnahmen zu einem bestimmten Zeitpunkt implementiert waren. Im Kern ist im Rahmen einer Angemessenheitsprüfung des Tax CMS

somit eine Überprüfung der identifizierten Risiken daraufhin vorzunehmen, ob diese vollständig sind und ob diese Risiken durch angemessene Kontrollen auf ein vertretbares Maß reduziert werden.“

- 98 Die Wirksamkeitsprüfung ist umfassender. Über die Angemessenheitsprüfung hinaus wird analysiert, ob die Grundsätze und Maßnahmen während eines bestimmten Zeitraums wirksam waren. Aus diesem Grund kann eine Wirksamkeitsprüfung auch erst dann erfolgen, wenn bereits ein Tax Compliance-System im Unternehmen implementiert ist. Dabei sollte der geprüfte Zeitraum mindestens ein halbes Geschäftsjahr umfassen.
- 99 Aus straf- und ordnungswidrigkeitenrechtlicher Sicht ist eine Wirksamkeitsprüfung zu präferieren, da allein die Implementierung eines Tax Compliance-Systems für eine Exkulpierung nicht ausreichend sein dürfte. Notwendig ist vielmehr, dass das Tax Compliance-System im Unternehmen auch tatsächlich gelebt wird. Schließlich ist zu beachten, dass die Unternehmensleitung auch nach erfolgter Zertifizierung Kontrollmaßnahmen durchzuführen hat. Eine Zertifizierung kann nur eine begrenzte „Lebensdauer“ haben.
- 100 Letztlich ist eine Zertifizierung des Tax Compliance-Systems unter steuerstraft- und steuerordnungswidrigkeitenrechtlichen Gesichtspunkten grundsätzlich empfehlenswert, selbst wenn hierdurch steuerstrafrechtliche und steuerordnungswidrigkeitenrechtliche Vorwürfe nicht mit Sicherheit ausgeschlossen werden können. Gegenüber der „bloßen“ Implementierung eines Tax Compliance-Systems stellt die Zertifizierung durch Dritte zumindest eine zusätzliche Absicherung dar, wodurch Risiken nochmals signifikant reduziert werden.

VI. Berichtigung von Steuererklärungen

1. Korrekturvorschrift

- 101 Besteht in Unternehmen Korrekturbedarf, da eine Steuererklärung objektiv unzutreffend abgegeben worden ist oder den steuerlichen Erklärungs- und Anzeigepflichten objektiv nicht nachgekommen wurde, ist zu entscheiden, welche Rechtsnorm einschlägig ist:
- Anzeige nach § 153 AO (nach objektiv unzutreffend abgegebener Erklärung);
 - § 149 AO i.V.m. Einzelsteuergesetzen (fortbestehende Erklärungspflicht nach unterlassener Abgabe einer Steuererklärung);
 - Selbstanzeige nach § 371 AO (bei vorsätzlicher Steuerhinterziehung) bzw. nach § 378 Abs. 3 AO (bei leichtfertiger Steuerverkürzung).
- 102 Sowohl im Fall der Anzeigepflicht nach § 153 AO (siehe hierzu → Rn. 21 ff.) als auch bei einer Selbstanzeige nach §§ 371, 378 Abs. 3 AO war die Steuererklärung im Zeitpunkt der Abgabe objektiv falsch. Die Abgrenzung der Normen erfolgt allein im subjektiven Bereich. Handelte der Steuerpflichtige im Zeitpunkt der Abgabe der objektiv unrichtigen Steuererklärung mit Hinterziehungsvorsatz, bzw. ist ihm Leichtfertigkeit nachzuweisen, stellt die nachträgliche Korrektur

eine Selbstanzeige nach § 371 AO bzw. nach § 378 Abs. 3 AO dar. Ist die objektive Unrichtigkeit dem Steuerpflichtigen dagegen subjektiv nicht vorwerfbar bzw. nur als „einfache“ Fahrlässigkeit zu qualifizieren, ist der Anwendungsbe-
 reich des § 153 AO eröffnet. Die Abgrenzung ist somit von einer inneren Tatsache abhängig, deren Würdigung durch die Finanzverwaltung im Vorfeld mitunter schwer zu antizipieren ist. Gleichwohl kommt der Abgrenzung, die für Unternehmen im Vorfeld mitunter schwer vorzunehmen ist, erhebliche Bedeutung zu, da sich die Voraussetzungen der §§ 153, 371 AO grundlegend unterscheiden. In **Zweifelsfällen** bleibt Unternehmen im Sinne des sichersten Wegs daher keine andere Wahl, als eine Berichtigung nach § 153 AO – wenn möglich – inhaltlich vorsorglich so auszugestalten, dass sie zugleich die (weitergehenden) Voraussetzungen einer Selbstanzeige nach § 371 AO erfüllt. In der Verwaltungspraxis bestand zuletzt die Tendenz, im Zweifel jedes Korrekturschreiben als Selbstanzeige nach § 371 AO zu werten. Wenngleich das BMF erfreulicherweise bemüht ist, dieser Entwicklung entgegenzuwirken,¹¹⁷ darf nicht verkannt werden, dass die Würdigung einer Korrektur als Selbstanzeige nach § 371 AO aufgrund der verlängerten Festsetzungsfrist (§ 169 Abs. 2 Satz 2 AO), der Hinterziehungszinsen nach § 235 AO sowie insbesondere des Geldbetrags nach § 398a AO aus Sicht der Finanzverwaltung deutlich „lukrativer“ als eine „bloße“ Berichtigung nach § 153 AO ist.

2. Selbstanzeige im Unternehmen (§§ 371, 378 Abs. 3 AO)

Die Änderungen des § 371 AO durch das Schwarzgeldbekämpfungsgesetz im Jahr 2011 sowie durch das Gesetz zur Änderung der Abgabenordnung und des Einführungsgesetzes zur Abgabenordnung vom 22.12.2014 haben dazu geführt, dass Selbstanzeigen in Unternehmen nur noch stark eingeschränkt möglich und durch den regelmäßig einschlägigen § 398a AO mit (erheblichen) zusätzlichen Kosten verbunden sind.

103

a) Person des Anzeigerstatters

Bei der Selbstanzeige handelt es sich um einen persönlichen Strafaufhebungsgrund, sodass nur derjenige Straffreiheit erlangt, in dessen Namen die Offenlegung gegenüber der Finanzverwaltung erfolgt. Da in Unternehmen regelmäßig mehrere Personen als Beteiligte an einer Steuerhinterziehung in Betracht kommen, ist der Personenkreis, für den eine Selbstanzeige abgegeben wird, sorgsam zu prüfen. Auch wenn es bei juristischen Personen nach einer alten BGH-Entscheidung grundsätzlich genügen kann, dass die Selbstanzeige durch einen Bevollmächtigten oder durch einen gesetzlichen Vertreter erstattet wird,¹¹⁸ ist – jedenfalls im Fall des § 371 AO – die namentliche Benennung der betroffenen Personen in der Anzeige aus Gründen der Rechtssicherheit vorzugswürdig (offe-

104

¹¹⁷ BMF, 23.5.2016 – IV A 3 – S – 0324/15/10001, BStBl. I 2016, 490; vgl. auch *Schwartz/Höpfner*, PStR 2016, 210; *Schauff/Schwartz*, PStR 2015, 248.

¹¹⁸ BGH, 24.10.1984 – 3 StR 315/84, wistra 1985, 74.

ne Stellvertretung).¹¹⁹ Dies gilt jedenfalls, wenn ein Geldbetrag nach § 398a AO in Betracht kommt. Neben der namentlichen Nennung des Betroffenen ist es auch ausreichend, wenn dieser für die Finanzverwaltung klar bestimmbar in der Anzeige genannt wird (z.B. Geschäftsführer). Bei der bußgeldbefreienden Selbstanzeige ist hingegen anerkannt, dass diese auch in verdeckter Stellvertretung (also ohne Benennung der einbezogenen Person) wirksam abgegeben werden kann.

b) Positive Wirksamkeitsvoraussetzungen des § 371 AO

- 105** § 371 Abs. 1 AO setzt voraus, dass zu allen Steuerstraftaten einer Steuerart in vollem Umfang die unrichtigen Angaben berichtigt, die unvollständigen Angaben ergänzt oder die unterlassenen Angaben nachgeholt werden (Vollständigkeitsgebot). Dabei müssen Angaben zu allen unverjährten Steuerstraftaten einer Steuerart, mindestens aber zu allen Steuerstraftaten einer Steuerart innerhalb der letzten zehn Kalenderjahre erfolgen (Berichtigungsverbund). Das Vollständigkeitsgebot bezieht sich nur auf vorsätzliche Unrichtigkeiten, die den Tatbestand des § 370 AO erfüllen, etwaige weitere nicht vorsätzliche Fehler sind nicht umfasst. Vor Abgabe einer Selbstanzeige ist stets die strafrechtliche Verfolgungsverjährung zu prüfen. Die Verjährungsfrist beträgt bei einfacher Steuerhinterziehung fünf Jahre (§ 78 Abs. 3 Nr. 4 StGB i.V.m. § 369 Abs. 2 AO). Liegt dagegen eine Steuerhinterziehung im besonders schweren Fall nach § 370 Abs. 3 Satz 2 Nr. 1 bis 6 AO vor, verlängert sich die Verjährungsfrist nach § 376 Abs. 1 AO auf 15 Jahre. § 376 Abs. 1 AO ist stets einschlägig, wenn durch die jeweilige Tat (in der Regel Veranlagungszeitraum) eine Steuerverkürzung von 50.000 EUR verursacht wurde. Im Hinblick auf den Beginn der Verjährungsfrist, das Vorliegen der Unterbrechungs- und Hemmungstatbestände der §§ 78c, 78b StGB oder das tatsächliche Überschreiten der Betragsgrenze von 50.000 EUR kann die Bestimmung der strafrechtlichen Verfolgungsverjährung mit Schwierigkeiten verbunden sein, sodass angesichts des Vollständigkeitsgebots im Zweifelsfall (zunächst) lieber ein Jahr zu viel als ein Jahr zu wenig offengelegt werden sollte. Ungeachtet der Verfolgungsverjährung müssen **mindestens berichtigende Angaben zu allen Steuerstraftaten einer Steuerart innerhalb der letzten zehn Kalenderjahre** gemacht werden. Damit müssen ggf. auch strafrechtlich verjährte einfache Steuerhinterziehungen zwingend angegeben werden, um eine wirksame Selbstanzeige für die nicht verfolgungsverjährten Steuerhinterziehungen zu erreichen.¹²⁰
- 106** In sachlicher Hinsicht bezieht sich das Vollständigkeitsgebot auf die jeweils offenbarte **Steuerart**. Wird bspw. USt hinterzogen, setzt die Wirksamkeit der Selbstanzeige nicht voraus, dass zugleich vorsätzlich falsche Angaben bei der KSt korrigiert werden. Sofern die USt- und die KSt-Hinterziehung auf dem glei-

¹¹⁹ Siehe vertiefend zur (verdeckten) Stellvertretung *Handel*, DStR 2018, 709.

¹²⁰ Vgl. *Schwartz*, PStR 2015, 37, 38; *Schauß*, in: Kohlmann, Steuerstrafrecht, Stand: 71. EL, § 371 AO Rn. 114 ff.

chen Sachverhalt beruhen, sollte dieser jedoch insgesamt zum Gegenstand der Selbstanzeige gemacht werden. Bislang nicht entschieden ist die Frage, ob das Vollständigkeitsgebot dahingehend einzuschränken ist, dass nur dieselbe Steuerart ein und desselben Steuerschuldners umfasst wird.¹²¹ Dies ist insbesondere bei **Beteiligung an gleichartigen Taten Dritter** relevant. So stellt sich die Frage, ob etwa ein Geschäftsführer eines Unternehmens, der eine Selbstanzeige für vorsätzliche Unrichtigkeiten in seinen persönlichen Einkommensteuererklärungen abgibt, zugleich in den Berichtigungszeitraum fallende unzutreffende Lohnsteueranmeldungen im Unternehmen korrigieren muss. Die gleiche Frage stellt sich bei der Teilnahme an der ESt-Hinterziehung anderer Personen im Zusammenhang mit verdeckten Gewinnausschüttungen.

Bei **Personengesellschaften** wird diskutiert, ob bei einer **Korrektur des einheitlichen und gesonderten Gewinnfeststellungsbescheids** zugleich alle übrigen (in den Berichtigungszeitraum fallenden) vorsätzlichen Fehler in den Einkommensteuererklärungen der Gesellschafter offenbart werden müssen. Der Feststellungsbescheid richtet sich nämlich nicht an die Gesellschaft, sondern an die Gesellschafter, da diese Subjekt der ESt sind. Ausgehend davon, dass Gewinnfeststellung und ESt eine Steuerart im Sinne des § 371 Abs. 1 AO sind, muss der vorsätzlich handelnde Feststellungsbeteiligte bei der Berichtigung einer unzutreffenden Feststellungserklärung auch weitere in den Berichtigungsverbund fallende vorsätzliche Unrichtigkeiten seiner Einkommensteuererklärungen korrigieren. Er ist jedoch nicht verpflichtet, auch etwaige Unrichtigkeiten im Rahmen der Einkommensteuererklärungen anderer Feststellungsbeteiligter zu berichtigen. 107

Ein **Verstoß gegen das Vollständigkeitsgebot** hat – sofern nicht eine nur geringfügige Abweichung¹²² vorliegt (Abweichung von nicht mehr als 5 % vom Verkürzungsbetrag im Sinne des § 370 Abs. 4 AO) – grundsätzlich zur Folge, dass die Selbstanzeige insgesamt unwirksam ist (Alles-oder-nichts-Prinzip). Für den Bereich der USt-Voranmeldungen und LohnSt-Anmeldungen hat der Gesetzgeber in § 371 Abs. 2a AO hiervon eine Ausnahme geschaffen. Abweichend von dem Vollständigkeitsgebot tritt Straffreiheit in dem Umfang ein, in dem die unrichtigen Angaben berichtigt, die unvollständigen Angaben ergänzt oder die unterlassenen Angaben nachgeholt werden (**Teilselbstanzeige**). Ferner wird durch § 371 Abs. 2a Satz 2 AO der Sperrgrund der Tatentdeckung ausgeschlossen, wenn die Entdeckung darauf beruht, dass eine USt-Voranmeldung oder LohnSt-Anmeldung nachgeholt oder berichtigt wurde. Hierdurch wird dem Bedürfnis der Praxis, der mehrfachen Korrektur von USt-Voranmeldungen und LohnSt-Anmeldungen, Rechnung getragen. Der Sperrgrund des § 371 Abs. 2 Satz 1 Nr. 3 AO findet in diesem Zusammenhang ausdrücklich ebenfalls keine Anwendung, sodass bei (Teil-)Selbstanzeigen bzgl. USt-Voranmeldungen oder LohnSt- 108

121 Vgl. zum Sach- und Streitstand *Schauf*, in: Kohlmann, Steuerstrafrecht, Stand: 71. EL, § 371 AO Rn. 130 ff.

122 BGH, 25.7.2011 – 1 StR 631/10, NZWiSt 2012, 117, 119.

Anmeldungen unabhängig von der Höhe der verkürzten Steuer kein Geldbetrag nach § 398a AO zu zahlen ist. Die Ausnahmeregelung in § 371 Abs. 2a AO greift nicht für USt-Jahreserklärungen.

- 109 Die Selbstanzeige muss die Finanzverwaltung in die Lage versetzen, ohne größere eigene Ermittlungen die Steuer ordnungsgemäß festsetzen zu können (Grundsatz der Materiallieferung). Jede Selbstanzeige muss daher **zwingend korrigierte Zahlen** enthalten. Nicht erforderlich ist dagegen, dass ausgefüllte Erklärungsvordrucke beigelegt werden. Gleichwohl kann auch in der Abgabe einer Steuererklärung eine Selbstanzeige liegen. Soweit die zu korrigierenden Zahlen aufgrund der Komplexität der in Unternehmen auftretenden Sachverhalte nicht innerhalb der erforderlichen Zeit zu beschaffen sind, können dem Finanzamt in einem ersten Schritt geschätzte Zahlen mitgeteilt werden. Um die Wirksamkeit der Selbstanzeige nicht zu gefährden, sind diese jedoch mit einem hinreichenden Sicherheitszuschlag zu versehen. Nach Auswertung der entsprechenden Unterlagen und der Buchhaltung erfolgt sodann in einem zweiten Schritt die Mitteilung der konkreten Zahlen.
- 110 Nach § 371 Abs. 3 AO setzt die Erlangung der Straffreiheit zudem voraus, dass der an der Tat Beteiligte fristgerecht die zu seinen Gunsten **hinterzogenen Steuern**, die Hinterziehungszinsen nach § 235 AO und die Zinsen nach § 233a AO, soweit sie auf die Hinterziehungszinsen nach § 235 Abs. 4 AO angerechnet werden, **nachentrichtet**. Bei der Korrektur von USt-Voranmeldungen und LohnSt-Anmeldungen hängt die Straffreiheit nur von der fristgerechten Steuernachzahlung ab (§ 371 Abs. 3 Satz 2 AO). Da bei Steuerhinterziehungen in Unternehmen der Steuerpflichtige (Unternehmen) und der Täter (natürliche Person) auseinanderfallen, werden durch den Tatbeteiligten fremde betriebliche Steuern hinterzogen. Die Steuernachzahlung ist jedoch nur dann Wirksamkeitsvoraussetzung, wenn die Steuern zugunsten des an der Tat Beteiligten hinterzogen wurden. Dies setzt den Zufluss eines unmittelbaren wirtschaftlichen Vorteils voraus. Der Gesellschafter-Geschäftsführer einer Ein-Mann-GmbH erlangt einen unmittelbaren wirtschaftlichen Vorteil durch Hinterziehung der Steuern, welche die GmbH schuldet, weil bei wirtschaftlicher Betrachtungsweise das Vermögen der GmbH dem Gesellschafter zusteht. Bei mehreren Gesellschaftern entspricht der unmittelbare Vorteil des handelnden Gesellschafter-Geschäftsführers seinem Gesellschaftsanteil. Ein anteiliger wirtschaftlicher Vorteil des (nur) angestellten Geschäftsführers kann zu bejahen sein, wenn er gewinnabhängige Leistungen erhält. Dagegen erlangt ein Angestellter oder GmbH-Geschäftsführer, dessen Stellung sich nicht von der eines sonstigen abhängigen Angestellten unterscheidet, keinen unmittelbaren Vorteil, wenn er die Hinterziehung zugunsten seines Arbeitgebers begeht, um seinen Arbeitsplatz zu erhalten.

c) Negative Wirksamkeitsvoraussetzungen des § 371 AO (Sperrgründe)

- 111 Straffreiheit tritt nicht ein, wenn einer der Sperrgründe nach § 371 Abs. 2 AO verwirklicht ist:

- Bekanntgabe einer Prüfungsanordnung (§ 371 Abs. 2 Satz 1 Nr. 1a AO);
- Bekanntgabe der Einleitung des Straf- oder Bußgeldverfahrens (§ 371 Abs. 2 Satz 1 Nr. 1b AO);
- Erscheinen eines Amtsträgers der Finanzbehörde zur steuerlichen Prüfung (§ 371 Abs. 2 Satz 1 Nr. 1c AO);
- Erscheinen eines Amtsträgers zur Ermittlung einer Steuerstraftat oder einer Steuerordnungswidrigkeit (§ 371 Abs. 2 Satz 1 Nr. 1d AO);
- Erscheinen eines Amtsträgers der Finanzbehörde zur Nachschau (§ 371 Abs. 2 Satz 1 Nr. 1e AO);
- Tatentdeckung (§ 371 Abs. 2 Satz 1 Nr. 2 AO);
- Verkürzte Steuer von mehr als 25.000 EUR (§ 371 Abs. 2 Satz 1 Nr. 3 AO);
- Besonders schwerer Fall nach § 370 Abs. 3 Satz 2 Nr. 2–6 AO (§ 371 Abs. 2 Satz 1 Nr. 4 AO).

Die Aufzählung ist abschließend, sonstige Sperrgründe gibt es nicht. Im Folgenden kann nur auf die für Unternehmen wesentlichen Regelungen und Konsequenzen eingegangen werden. Liegen die Voraussetzungen eines Sperrgrundes nach § 371 Abs. 2 Satz 1 Nr. 1 oder Nr. 2 AO für (nur) eine zur Selbstanzeige gebrachten Tat vor, sind grundsätzlich alle Taten der betroffenen Steuerart gesperrt (**Infektionswirkung**). In den Fällen des § 371 Abs. 2 Satz 1 Nr. 1a und Nr. 1c AO ist die Sperrwirkung dagegen ausdrücklich auf den sachlichen und zeitlichen Umfang der (**angekündigten**) **Außenprüfung** beschränkt. Für Jahre, die nicht Gegenstand der Prüfungsanordnung sind, kann daher (trotz Betriebsprüfung) grundsätzlich eine strafbefreiende Selbstanzeige abgegeben werden. 112

Die in der Praxis übliche mündliche Ankündigung der Betriebsprüfung sowie eine im Vorfeld erfolgende Terminvereinbarung lösen die Sperrwirkung des § 371 Abs. 2 Satz 1 Nr. 1a AO noch nicht aus, da § 196 AO Schriftform verlangt. Gleiches gilt, wenn mündlich oder auch schriftlich zur Vorbereitung der Prüfung um Übersendung der Buchhaltungsdaten auf einem Datenträger gebeten wird. Die Bekanntgabefiktion des § 122 Abs. 2 Nr. 1 AO dürfte für Zwecke der Selbstanzeige keine Anwendung finden.¹²³ Der sachliche Umfang der Sperrwirkung bestimmt sich nach dem Inhalt der Prüfungsanordnung. Diese führt daher nur hinsichtlich der von ihr umfassten Steuerarten eine Sperrwirkung herbei. Die Bekanntgabe muss gegenüber dem an der Tat Beteiligten (Täter oder Teilnehmer), seinem Vertreter, dem Begünstigten im Sinne des § 370 Abs. 1 AO (Schuldner der hinterzogenen Steuer) oder dessen Vertreter erfolgen. Die Bekanntgabe einer Prüfungsanordnung gegenüber einer Kapitalgesellschaft löst somit auch gegenüber nicht vertretungsberechtigten Mitarbeitern als Täter oder Teilnehmer der im Unternehmen begangenen Steuerhinterziehung Sperrwirkung aus. Dies soll nach der Begründung des Regierungsentwurfs¹²⁴ auch für aus dem Unternehmen ausgeschiedene Mitarbeiter gelten. Die Bekanntgabe einer Prüfungsanordnung an eine Personengesellschaft, die sich auf die gesonderte und 113

¹²³ Jäger, in: Klein, Abgabenordnung, § 371 AO Rn. 113.

¹²⁴ BR-Drs. 431/14, S. 8.

einheitliche Feststellung der Besteuerungsgrundlagen bezieht, dürfte hinsichtlich der ESt der Gesellschafter keine Sperrwirkung herbeiführen. Die Sperrwirkung setzt nur eine wirksame und keine rechtmäßige Prüfungsanordnung voraus. Die Selbstanzeigemöglichkeit lebt nach Abschluss der steuerlichen Prüfung wieder auf. Dies ist nach h.M. der Fall, wenn die Finanzverwaltung die berichtigten Steuerbescheide bekannt gemacht oder das Prüfungsverfahren durch eine Mitteilung nach § 202 Abs. 1 Satz 3 AO abgeschlossen hat.

- 114** Ist der Täter Inhaber mehrerer Betriebe, zwischen denen eine wirtschaftliche Einheit (Identität des Inhabers und enge organisatorische Verzahnung) besteht, so löst das Erscheinen des Prüfers in einem dieser Betriebe die Sperrwirkung des § 371 Abs. 2 Satz 1 Nr. 1c AO für alle Betriebe aus (Gedanke der Sphäreinheit), es sei denn, die Prüfungsanordnung gilt ausdrücklich nur für einen Betrieb. Bei einem **Konzern** sind wegen der rechtlichen Selbstständigkeit der Steuersubjekte die Sphären von Mutter- und Tochterunternehmen bzw. gleichberechtigter Konzerngesellschaften zu trennen. Das Erscheinen des Prüfers in einer der genannten Gesellschaften löst daher noch keine Sperrwirkung gegenüber den anderen aus.¹²⁵
- 115** Nach § 371 Abs. 2 Satz 1 Nr. 3 AO tritt keine Straffreiheit ein, wenn die nach § 370 Abs. 1 AO verkürzte Steuer oder der erlangte nicht gerechtfertigte Steuervorteil einen Betrag von 25.000 EUR je Tat übersteigt. Dieser Grenzwert ist in Unternehmen zumeist erreicht. Dann kommt ein Absehen von der Strafverfolgung nach § 398a AO (siehe hierzu → Rn. 117 ff.) in Betracht, was aufgrund des zusätzlich zu leistenden Geldbetrags mit einer weiteren finanziellen Belastung einhergeht. Die Betragsgrenze von 25.000 EUR bezieht sich auf die jeweilige materiell-rechtliche Tat, bestehend aus Steuerart, Besteuerungszeitraum und Steuerpflichtigem. Eine Addition verkürzter Steuerbeträge mehrerer Jahre oder Steuerarten findet (außer bei Tateinheit) nicht statt.¹²⁶ Bei § 371 Abs. 2 Satz 1 Nr. 3 AO besteht keine Infektionswirkung, sodass das Überschreiten des Grenzbetrages für jede Tat isoliert zu betrachten ist. Für die unter dem Grenzbetrag liegenden Taten bleibt die Selbstanzeige demnach wirksam. Bei der Bestimmung der verkürzten Steuern findet nach dem Gesetzeswortlaut das Kompensationsverbot (siehe hierzu → Rn. 48) Anwendung, sodass Steuerminderungsgründe ohne Berücksichtigung bleiben.
- 116** Bei Steuerhinterziehungen in Verbindung mit Urkundenfälschungen ist stets zu prüfen, ob überhaupt eine wirksame Selbstanzeige abgegeben werden kann. Nach § 371 Abs. 2 Satz 1 Nr. 4 AO ist eine wirksame Selbstanzeige u. a. ausgeschlossen, wenn der Täter unter Verwendung nachgemachter oder verfälschter Belege fortgesetzt Steuern verkürzt oder nicht gerechtfertigte Steuervorteile erlangt (§ 370 Abs. 3 Satz 2 Nr. 4 AO). Hierzu muss er mehrfach unechte Urkunden im Sinne des § 267 Abs. 1 StGB verwendet, d. h. dem Finanzamt eingereicht

¹²⁵ *Schauf*, in: Kohlmann, Steuerstrafrecht, Stand: 71. EL, § 371 AO Rn. 462.

¹²⁶ BGH, 15.12.2011 – 1 StR 579/11, NJW 2012, 1015, 1016; *Schauf*, in: Kohlmann, Steuerstrafrecht, Stand: 73. EL, § 371 AO Rn. 777.

oder einem Prüfer vorgelegt haben. Unter den Voraussetzungen des § 398a AO wird jedoch von der Strafverfolgung abgesehen.

d) Absehen von Verfolgung nach § 398a AO

Ein Absehen von der Strafverfolgung erfolgt unter folgenden Voraussetzungen: **117**

- Vorliegen einer Selbstanzeige nach § 371 AO, deren Wirksamkeit allein an der Verwirklichung des Sperrgrundes des § 371 Abs. 2 Satz 1 Nr. 3 oder Nr. 4 AO scheitert;
- Fristgemäße Zahlung der zugunsten des an der Tat Beteiligten hinterzogenen Steuern, der Hinterziehungszinsen nach § 235 AO und der Zinsen nach § 233a AO, soweit sie auf die Hinterziehungszinsen nach § 235 Abs. 4 AO angerechnet werden;
- Fristgemäße Zahlung des Geldbetrags nach § 398a Abs. 1 Nr. 2 AO.

Die **Bemessung des Geldbetrags** hängt von der Höhe der hinterzogenen Steuer ab und ist wie folgt gestaffelt: **118**

- 10 % der hinterzogenen Steuer, wenn der Hinterziehungsbetrag 25.000 EUR übersteigt und 100.000 EUR nicht übersteigt;
- 15 % der hinterzogenen Steuer, wenn der Hinterziehungsbetrag 100.000 EUR übersteigt und 1.000.000 EUR nicht übersteigt;
- 20 % der hinterzogenen Steuer, wenn der Hinterziehungsbetrag 1.000.000 EUR übersteigt.

Bemessungsgrundlage für die Berechnung des Geldbetrags nach § 398a Abs. 1 Nr. 2 AO ist die jeweilige nicht verfolgungsverjährte materiell-rechtliche Tat, die unter den Anwendungsbereich des § 398a AO fällt. Die Ermittlungsbehörden vertreten regelmäßig die Ansicht, dass der Geldbetrag nach § 398a Abs. 1 Nr. 2 AO **durch jeden Tatbeteiligten** in voller Höhe zu zahlen sei.¹²⁷ Dies trifft Unternehmen in besonderem Maße, da regelmäßig mehrere Personen als Täter oder Teilnehmer in Betracht kommen. Erschwerend kommt hinzu, dass der Geldbetrag auch dann zu zahlen ist, wenn der Täter – wie typischerweise im Unternehmen – nicht zu eigenen Gunsten handelte. Es besteht jedoch keine Rechtspflicht zur Zahlung des Geldbetrags. Vielmehr kann der an der Tat Beteiligte entscheiden, ob er durch die Erfüllung der Voraussetzungen des § 398a AO einseitig die weitere Verfolgbarkeit der Tat abwendet oder ob er sich einem Strafverfahren stellt.¹²⁸ Je nach Fallkonstellation kann es sich anbieten, die „Flucht in das Strafverfahren“ anzutreten, wenn etwa eine Geldauflage bei einer Verfahrenseinstellung nach § 153a StPO geringer ausfällt, als die starre Regelung des § 398a AO. Dies kann bspw. der Fall sein, wenn kein oder nur ein geringer Steuerschaden entstanden ist, aufgrund der Anwendung des Kompensationsverbots jedoch erhebliche Hinterziehungsbeträge im Sinne des § 398a Abs. 1 Nr. 2 AO vorliegen sowie in Fällen der Beihilfe zur Steuerhinterziehung, wenn der Gehilfe nur einen

¹²⁷ Ebenso LG Aachen, 27.8.2014 – 86 Qs 11/14, wistra 2014, 493.

¹²⁸ Jäger, in: Klein, Abgabenordnung, § 398a AO Rn. 3; Schwartz, PStR 2015, 37, 45.

untergeordneten Tatbeitrag geleistet hat. Der Geldbetrag nach § 398a Abs. 1 Nr. 2 AO ist nicht als Betriebsausgabe steuerlich abzugsfähig.

e) Bußgeldbefreiende Selbstanzeige nach § 378 Abs. 3 AO

- 120** In den Fällen leichtfertiger Steuerverkürzung kommt eine bußgeldbefreiende Selbstanzeige nach § 378 Abs. 3 AO in Betracht, die sich wesentlich von den Voraussetzungen des § 371 AO unterscheidet. § 378 Abs. 3 AO kennt kein Vollständigkeitsgebot, sodass auch Teilselbstanzeigen im Umfang der Berichtigung wirksam sind. Im Übrigen existiert einzig der Sperrgrund der Bekanntgabe der Einleitung eines Straf- oder Bußgeldverfahrens. Eine Selbstanzeige ist demnach sowohl nach Bekanntgabe der Prüfungsanordnung als auch während der Betriebsprüfung möglich. Erwähnenswert ist zudem, dass die Höhe der verkürzten Steuer keinen Einfluss auf die Wirksamkeit einer Anzeige nach § 378 Abs. 3 AO hat. Soweit im Unternehmen vorwerfbare steuerliche Unrichtigkeiten zu korrigieren sind, kann es daher lohnenswert sein, mit den Finanzbehörden um die Leichtfertigkeit zu kämpfen.

VII. Fazit

- 121** In einem Umfeld, das von einem komplexen Steuerrecht, ständigen Gesetzesänderungen, einer steigenden Internationalität sowie einer zunehmenden Sensibilisierung der Öffentlichkeit für steuerliches Fehlverhalten von Unternehmen einerseits und einem extensiveren Gebrauch der §§ 130, 30 OWiG durch die Ermittlungsbehörden andererseits geprägt ist, steht das Erfordernis eines Tax Compliance-Systems außer Frage. Orientierungshilfe bei der Ausgestaltung eines Tax Compliance-Systems kann der von dem Institut der Wirtschaftsprüfer (IDW) herausgegebene **Prüfungsstandard IDW PS 980** bieten, der die Grundsätze zur ordnungsmäßigen (freiwilligen) Prüfung von Compliance-Management-Systemen definiert. Ein funktionierendes und immer wieder auf den Prüfstand gestelltes Tax Compliance-System vermag steuerliche-, zivilrechtliche-, aber auch straf- und bußgeldrechtliche Haftungsrisiken erheblich zu reduzieren und schafft daher langfristig einen klaren Mehrwert in Bezug auf Finanzen und Reputation, und zwar nicht nur aus Sicht der Geschäftsleitung und der Aufsichtsorgane, sondern auch für das gesamte Unternehmen und dessen Anteilseigner.¹²⁹

¹²⁹ Besch/Starck, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, § 33 Rn. 150; Aichberger/Schwartz, DStR 2015, 1758, 1764.

Literaturverzeichnis

<i>Ahrend</i>	Cyberangriffe in der Realität, CB 2019, 105
<i>Aichberger/Schwartz</i>	Tax Compliance – Der Vorstand im Fokus?, DStR 2015, 1691 (Teil I), 1758 (Teil II)
<i>Altenburg</i>	Whistleblowing – Korruptionsbekämpfung durch Business Keeper Monitoring System?, Bucerius Law Journal 2008, 3
<i>Altenschiedt/Helling</i>	LkSG, Lieferkettensorgfaltspflichtengesetz, Kurzkommentar, 2022
<i>Altmeppen (Hrsg.)</i>	GmbHG, 11. Aufl. 2023
<i>Andrae/Hellmich/ Schmaltz</i>	Bankaufsichtliches Risikomanagement – Grundlagen und Anwendung, Regulatorischer Anforderungen, 2018
<i>Andras/Szesny</i>	Nicht ohne eine Compliance-Due-Diligence, Deutscher Anwalt Spiegel 20/2015, 3
<i>Andrejewski/Krause/ von Hesberg (Hrsg.)</i>	Praxishandbuch ESG – Grundlagen, Bedeutung und Umsetzung in Unternehmen, 2023
<i>Antoine</i>	Datenzugangsrechte im finalen Data Act – Fortschritt, Rückschritt, neue Fragen?, CR 2024, 1
<i>Arnold</i>	Transnational corporations and the duty to respect basic human rights, Business Ethics Quarterly, 20(3), 371
<i>Arntzen/Abele</i>	Der Umgang mit ESG-Kriterien im Rahmen der Due Diligence bei M&A- und Private Equity-Transaktionen, BB 2023, 2823
<i>Assion/Willecke, Auer-Reinsdorff/ Conrad (Hrsg.)</i>	Der EU Data Act, MMR 2023, 805 Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019
<i>Awaysheh/Klassen</i>	The impact of supply chain structure on the use of supplier socially responsible practices, International Journal of Operations & Production Management, 30(12), 1246
<i>Bachmann</i>	Compliance – Rechtsgrundlagen und offene Fragen, in: Schriftenreihe der Gesellschaftsrechtlichen Vereinigung (Hrsg.), Gesellschaftsrecht in der Diskussion, 2007
<i>Bachmann</i>	CSR-bezogene Vorstands- und Aufsichtsratspflichten und ihre Sanktionierung, ZGR 2018, 231
<i>Badtke</i>	Die Bedeutung des Kartellrechts bei M&A-Transaktionen, KSzW 2011, 418
<i>Bajaj</i>	Fatal fire in Bangladesh highlights the dangers facing garment workers. New York Times (25.11.2012), https://www.nytimes.com/2012/11/26/world/asia/bangladesh-fire-kills-more-than-100-and-injures-many.html (zuletzt abgerufen am 22.2.2024)
<i>Bälz</i>	Ausländische Wirtschaftssanktionen als Leistungshindernis in internationalen Verträgen, NJW 2020, 878
<i>Balzer/Nugel</i>	Das Auslesen von Fahrzeugdaten zur Unfallrekonstruktion im Zivilprozess, NJW 2016, 193

- Bamberger/Roth/Hau/ Poseck* (Hrsg.) Bürgerliches Gesetzbuch: BGB, 5. Aufl. 2022/2023
- Banerjea* Due Diligence beim Erwerb von Aktien über die Börse, ZIP 2003, 1730
- Baranowski/Glaßl* Whistleblowing in Recht und Praxis – und ein bisschen Datenschutz, CB 2018, 271
- Barnitzke* Zur indirekten Nutzung von Software – Komplex, intransparent und unwirksam?, K&R 2018, 455
- Baron/Trebing* Umgang mit Kartellrechtsrisiken in M&A-Transaktionen – aktuelle Fragestellungen und Entwicklungen, BB 2016, 131
- Bartsch* Aktuelle Fragen zur IT-Sicherheit bei Energieversorgungsunternehmen, EnWZ 2023, 69
- Bartz/Schmidt/Lehne* Nationale Gesetze, internationale Lieferketten – zu den Wechselwirkungen verschiedener nationaler Lieferkettenregulierungen am Beispiel von LkSG und UFLPA, CCZ 2024, 25
- Bartz/Schmidt/Weber* Die wichtigsten Entwicklungen im Lieferkettenrecht im ersten Halbjahr 2024, CCZ 2024, 172
- Baumert* Handlungssicherheit in der Compliance-Arbeit an Beispielen, CCZ 2013, 265
- Baums* Risiko und Risikosteuerung, ZGR 2011, 218
- Baumüller/Scheid* Verschärfung der unternehmerischen Sorgfaltspflichten entlang der Lieferkette, DK 2022, 195
- Baur/Holle* Compliance-Defense bei der Bußgeldbemessung und ihre Einpassung in das gesellschaftsrechtliche Pflichtenprogramm, NZG 2018, 14
- Bausch/Voller* Geldwäsche-Compliance für Güterhändler, 2014
- Bay* (Hrsg.) Handbuch Internal Investigations, 2013
- Bay/Hastenrath* (Hrsg.) Compliance-Management-Systeme. Praxiserprobte Elemente, Prozesse und Tools, 3. Aufl. 2022
- Bayerische Rück* Gesellschaft und Unsicherheit, 1987
- Becker/Kingreen* SGB V – Gesetzliche Krankenversicherung, Kommentar, 8. Aufl. 2022
- Beckschäfer/Neuhaus* Die straf- und ordnungswidrigkeitenrechtliche Bedeutung der erweiterten Anzeige- und Berichtigungspflicht gemäß § 153 Abs. 4 AO, NZWiSt 2023, 328
- Bednarski/Roscoe/ Blome/Schleper* Geopolitical disruptions in global supply chains: a state-of-the-art literature review. Production Planning & Control, (im Druck), DOI: <https://doi.org/10.1080/09537287.2023.2286283>
- Behling* Der Zugriff auf dienstliche E-Mail-Postfächer im Lichte der aktuellen Rechtsprechung, CB 2013, 265
- Behling* Die datenschutzrechtliche Compliance-Verantwortung der Geschäftsleitung, ZIP 2017, 697
- Behringer* Compliance kompakt – Best Practice im Compliance Management, 4. Aufl. 2018

- Beisel/Andreas* Beck'sches Mandatshandbuch Due Diligence, 4. Aufl. 2024
- Beisel/Klumpp* Der Unternehmenskauf, 7. Aufl. 2016
- Bello* Improving Anti-Money Laundering Compliance, 2017
- Benne* Whistleblowing – Wenn Wissen Sensibilität erfordert, CCZ 2014, 189
- Bensinger/Kozok* Kampf gegen Cyber Crime und Hacker-Angriffe, CB 2015, 376
- Benz* Compliance-Risiken in Transaktionen, BOARD 2012, 137
- Benz* Der Prozess hinter dem Prozess, ZRFC 2015, 126
- Benz/Klindt* Compliance 2020 – ein Blick in die Zukunft, BB 2010, 2977
- Berg/Kramme* (Hrsg.) Lieferkettensorgfaltspflichtengesetz, Kommentar, 2023
- Bergmoser* Integration von Compliance-Management-Systemen, BB Spezial 4 (zu BB 50/2010), 2
- Bergmoser/Theusinger/Gushurst* Corporate Compliance – Grundlagen und Umsetzung, BB Spezial 2008, 1
- Bernard-Rau* (Hrsg.) Sustainability Stories, The Power of Narratives to understand Global Challenges, 2024
- Bernsmann/Gatzweiler* Verteidigung bei Korruptionsfällen, 2. Aufl. 2014
- Bertke/Sandbrink* Menschenrechts- und Beschwerdebeauftragte nach dem LkSG, NJW 2024, 319
- Besen/Gronemeyer* Informationsaustausch im Rahmen von Unternehmenskäufen – Kartellrechtliche Entwicklungen und Best Practice, CCZ 2013, 137
- Bessis* Risk Management in Banking, 2010
- Bettermann/Hoes* Das Lieferkettensorgfaltspflichtengesetz – Besondere Pflichten für Kreditinstitute?, BKR 2022, 23
- Beyer* Auswirkungen der Erklärungsfiktion des § 150 Abs. 7 S. 2 AO im Steuerstrafrecht bei Mitteilungen Dritter gem. § 93 c AO, NZWiSt 2018, 359
- Bicker/Stoklasa* Business Partner Compliance – Ausgestaltung und Einführung von Prüf- und Kontrollprozessen, BB 2018, 519
- Bierwagen* Iran-Sanktionen der USA und EU-Blocking-Verordnung, RIW 2020, 584
- Bischke/Brack* Neuere Entwicklungen im Kartellrecht, NZG 2018, 696
- Bisges* Urheberrechtliche Aspekte des Cloud Computing – Wirtschaftlicher Vorteil gegenüber herkömmlicher Softwareüberlassung?, MMR 2012, 574
- Blassl* Compliance-Aufgaben des Aufsichtsrats – Ein Beitrag zur akzessorischen Legalitätskontrolle durch den Aufsichtsrat, WM 2017, 992
- Block/Nickel* Einrichtung von Hinweisgebersystemen, ZCG 2024, 11
- Bock* Strafrechtliche Aspekte der Compliance-Diskussion – § 130 OWiG als zentrale Norm der Criminal Compliance, ZIS 2009, 68

- Bock* Criminal Compliance, 2011
- Bock/Borrmann* Vorteilsannahme (§ 331 StGB) und Vorteilsgewährung (§ 333 StGB) durch Kultursponsoring?, ZJS 2009, 625
- Böcking/Groß/Oser/Scheffler/Thormann* Beck'sches Handbuch der Rechnungslegung, Werkstand 70. EL Juli 2023
- Boldt/Büll/Voss* Implementierung einer Compliance-Funktion in einer mittelständischen Bank unter Berücksichtigung der neuen Mindestanforderungen an das Risikomanagement (MaRisk), CCZ 2013, 248
- Bomhard/Merkle* Der Entwurf eines EU Data Acts, RD i 2022, 168
- Bonin, von/Böhmer* Begriff der Insiderinformation bei gestreckten Sachverhalten, EuZW 2012, 694
- Boos/Fischer/Schulte-Mattler* (Hrsg.) Kreditwesengesetz – KWG, 5. Aufl. 2016
- Born/Ghassemi-Tabar/Gehle* Münchener Handbuch des Gesellschaftsrechts Bd. 7: Gesellschaftsrechtliche Streitigkeiten (Corporate Litigation), 6. Aufl. 2020
- Bosse* Compliance und Haftung des GmbH-Geschäftsführers – Management von Compliance-Risiken, NWB 2013, 4056
- Böttcher* Organpflichten beim Unternehmenskauf, NZG 2007, 481
- Böttcher* Verpflichtung des Vorstands einer AG zur Durchführung einer Due Diligence, NZG 2005, 49
- Böttger* (Hrsg.) Wirtschaftsstrafrecht, 3. Aufl. 2023
- Brandenburg/Warasthe/Seuring* Impact pathways: improving supply chain sustainability by due diligence acts? Insights from a German case. International Journal of Operations & Production Management, <https://doi.org/10.1108/IJOPM-03-2023-0200>
- Brauer/Busker* Integration der Anforderungen aus dem LkSG in ein bestehendes CMS, CB, 2022, 472
- Braun/Wybitul* Übermittlung von Arbeitnehmerdaten bei Due Diligence – Rechtliche Anforderungen und Gestaltungsmöglichkeiten, BB 2008, 782
- Breimann/Schwetzel* Prüfung von Tax Compliance Management Systemen nach IDW PS 980: Prüfungsarten, Prüfungsvorgehen und Wirkung des Testats, DStR 2017, 2626
- Brian/Frey/Krais* Umsetzung der Fünften Geldwäsche-Richtlinie in Deutschland, CCZ 2019, 245
- Brink* Empfehlungen zur IuK-Nutzung am Arbeitsplatz, ZD 2015, 295
- Brobeil* Die Auswirkungen der Richtlinie (EU) 2019/1937 auf Arbeitnehmer-Hinweisgeber, 2022
- Brodowski/Eisenmenger* Zugriff auf Cloud-Speicher und Internet-Dienste durch Ermittlungsbehörden. Sachliche und zeitliche Reichweite der „kleinen Online-Durchsuchung“ nach § 110 Abs. 3 StPO, ZD 2014, 119
- Brodowski/Freiling* Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, 2011

- Brouwer* Noch viele offene Rechts- und Auslegungsfragen zum Lieferkettensorgfaltspflichtengesetz – Hinweise zum VCI-Diskussionspapier zur Umsetzung des LkSG, CCZ 2022, 137
- Brühl, von/Sepperer* E-Mail-Überwachung am Arbeitsplatz. Wer bewacht den Wächter, ZD 2015, 415
- Buchert* Der externe Ombudsmann – ein Erfahrungsbericht, Hinweisgeber brauchen Vertrauen und Schutz, CCZ 2008, 148
- Bungenberg/Dutzi/Krebs/Zimmermann* Corporate Compliance und Corporate Social Responsibility, 2014
- Bünnigmann* § 22 IV AWG: Bestandsaufnahme drei Jahre nach Einführung einer dogmatisch diskutierten und praktisch postulierten Vorschrift, CCZ 2016, 60
- Bunte (Hrsg.)* Kartellrecht, Kommentar. Bd. 1: Deutsches Kartellrecht/Bd. 2: Europäisches Kartellrecht, 14. Aufl. 2021
- Burgi/Dreher (Hrsg.)* Beck'scher Vergaberechtskommentar, Bd. 1, 4. Aufl. 2022
- Bürkle* Zur Unionsrechtskonformität zentraler Konzernmeldestellen für Hinweisgeber, CCZ 2022, 335
- Bürkle* Die Bußgeldrelevanz des Compliance-Managements, BB 2018, 525
- Bürkle* Die Compliance-Praxis im Finanzdienstleistungssektor nach Solvency II, CCZ 2008, 50
- Bürkle (Hrsg.)* Compliance in Versicherungsunternehmen, 3. Aufl. 2020
- Bürkle/Hauschka/Schieffer (Hrsg.)* Der Compliance Officer – Ein Handbuch in eigener Sache, 2. Aufl. 2024
- Busch* Darf ich mich noch einigen? Der neue § 153 Abs. 4 AO aus Verrechnungspreissicht, DB 2023, 1562
- Busekist, von/Beneke* Anforderungen an CMS: Compliance-Treiber gestern und heute WPg 2020, 61
- Busekist, von/Schlitt* Der IDW PS 980 und die allgemeinen rechtlichen Mindestanforderungen an ein wirksames Compliance Management System (2) – Risikoeermittlungspflicht, CCZ 2012, 86
- Busekist, von/Timmerbeil* Die Compliance Due Diligence in M&A-Prozessen, CCZ 2013, 225
- Bussche, von dem/Voigt (Hrsg.)* Konzerndatenschutz, Rechtshandbuch, 2. Aufl. 2019
- Busse/Meinlschmidt/Foerstl* Managing information processing needs in global supply chains: A prerequisite to sustainable supply chain management. Journal of Supply Chain Management, 53(1), 2017, 87
- Busse/Schleper/Niu/Wagner* Supplier development for sustainability: contextual barriers in global supply chains, International Journal of Physical Distribution & Logistics Management, 46(5), 442
- Bussmann* Die Zukunft der unternehmerischen Haftung bei Compliance Verstößen, CCZ 2009, 132
- Bussmann* Integrität durch nachhaltiges Compliance Management über Risiken, Werte und Unternehmenskultur, CCZ 2016, 50

Literaturverzeichnis

- Caracas* § 130 OWiG – Das lange Schwert der Korruptionsbekämpfung im privaten Sektor – Teil 1, CCZ 2015, 167
- Carroll* The Pyramid of Corporate Social Responsibility: “Toward the Moral Management of Organizational Stakeholders”, Business Horizons (July-August 1991), 39
- Carroll/Brown/Buchholtz* Business & Society: Ethics, Sustainability & Stakeholder Management, 10. Aufl. 2018
- Carroll/Shabana* The Business Case for Corporate Social Responsibility: “A Review of Concepts, Research and Practice”, International Journal of Management Reviews 2010, 12 (1), 85
- Carter/Rogers* A framework of sustainable supply chain management: moving toward new theory, International Journal of Physical Distribution & Logistics Management, 38(5), 360
- Casper/Terlau* (Hrsg.) Zahlungsdiensteaufsichtsgesetz – Das Aufsichtsrecht des Zahlungsverkehrs und des E-Geldes, Kommentar, 3. Aufl. 2023
- Cauers/Haas/Jakob/Kremer/Schartmann/Welp* Ist der gegenwärtig viel diskutierte Begriff „Compliance“ nur alter Wein in neuen Schläuchen?, DB 2008, 2717
- Claussen* Compliance- oder Integritätsmanagement, 2011
- Cohen/Holland* Fünf Punkte, die ausländische Unternehmen über den United States Foreign Corrupt Practices Act (FCPA) wissen sollten, CCZ 2008, 7
- Colneric/Gerdemann* (Hrsg.) BeckOK HinSchG, 2. Edition, Stand: 15.1.2024
- Committee of the Sponsoring Organizations of the Treadway Commission (COSO)* (Hrsg.) Enterprise Risk Management – Integrated Framework, 2004
- Crane/Matten/Glozer/Spence* Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization, 5. Aufl. 2016
- Crane/McWilliams/Matten/Moon/Siegel* (Hrsg.) The Oxford Handbook of Corporate Social Responsibility, 2009
- Cressey* Other People’s Money – a study in the social psychology of embezzlement, 2. Aufl. 1973
- Daghles* Cybersecurity-Compliance: Pflichten und Haftungsrisiken für Geschäftsleiter in Zeiten fortschreitender Digitalisierung, DB 2018, 2289
- Dahlke* Risikobewertung in einem Tax-Compliance-Management-System, BB 2019, 619
- De Decker/Schaumüller-Bichl* (Hrsg.) Communications and Multimedia Security, 2010
- de Ruijter/Guldenmund* The bowtie method: A review, Safety Science, 88/2016, 211
- Decker* Beurkundungspflicht des Zustimmungsbeschlusses bei der Übertragung des gesamten Vermögens einer GmbH?, NZG 2018, 447

- Deike* Open Source Software: IPR-Fragen und Einordnung ins deutsche Rechtssystem, CR 2003, 9
- Denga* Völkerrechtswidrige Wirtschaftssanktionen im deutschen Vertragsrecht, RIW 2022, 93
- Depping/Walden* (Hrsg.) Lieferkettensorgfaltspflichtengesetz: LkSG, Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in der Lieferkette, 2022
- Di Sano/Gunnella/Lebastard* Deglobalisation: risk or reality?, 2023, <https://www.ecb.europa.eu/press/blog/date/2023/html/ecb.blog230712~085871737a.en.html> (zuletzt abgerufen am 22.2.2024)
- Dieners* (Hrsg.) Handbuch Compliance im Gesundheitswesen, 4. Aufl. 2022
- Dierks/Sandmann/Herre* Das neu überarbeitete COSO-Rahmenwerk für Interne Kontrollsysteme und die Konsequenzen für die deutsche Unternehmenspraxis, CCZ 2013, 164
- Dillerup/Stoi* Unternehmensführung, 6. Aufl. 2020
- Dilling* Die Konzernlösung gemäß § 14 Abs. 1 S. 1 HinSchG im Spannungsfeld zwischen europarechtlichen Vorgaben und den praktischen Bedürfnissen der von der Umsetzung betroffenen Unternehmensverbände, CCZ 2023, 91
- Dittmers* Werteorientiertes Compliance-Management: Die Werte von Compliance-Beauftragten und ihr Einfluss auf die Compliance-Kultur im Unternehmen, 2018
- Dittrich/Dochow/Ippach* (Hrsg.) Rechtshandbuch Cybersicherheit im Gesundheitswesen, 2024
- Dittrich/Heinelt* Der Europäische DORA – neue Sicherheitsvorgaben für den Finanzsektor, RD i 2023, 164
- Ditz/Engelen* Neue Anzeigepflichten für Steuergestaltungen – Überblick und erste Handlungsempfehlungen, DStR 2019, 352
- Dorsch* Zollrecht, 221. Ergänzungslieferung, November 2023
- Dreher/Hoffmann* Die erfolgreiche Selbstreinigung zur Wiedererlangung der kartellvergaberechtlichen Zuverlässigkeit und die vergaberechtliche Compliance – Teil 1, NZBau 2014, 67
- Dreier/Schulze* Urheberrechtsgesetz, Kommentar, 6. Aufl. 2018
- Dzida* Die Mitbestimmungen des Konzernbetriebsrats bei Ethik-Richtlinien, NZA 2008, 1265
- Eberius* Verrechtlichung der ESG-Compliance: Pflichten für Fondsmanager und institutionelle Investoren – Bestehende und zukünftige rechtliche Vorgaben zum Umgang mit Nachhaltigkeitskriterien und -risiken, WM 2019, 2143
- Ebersoll/Stork* Smart Risk Assessment: Mehr Effizienz durch Screening, CCZ 2013, 129
- Ecker* Die Publikationen des BAFA zum LkSG – Anlass für einen „Rückzug vor Befähigung“ statt für eine „Befähigung vor Rückzug“?, CCZ 2023, 69

- Ecker* Die Publikationen des BAFA zur Zusammenarbeit in der Lieferkette und die Frage nach der Umsetzbarkeit, ESG 2023, 254
- Eggers/Haak* Finanzinstitute und Sanktionen, CB 2022, 416
- Eggert* Tax Compliance in Konzernen mit Matrix-Strukturen – Steuerrechtliche Verantwortung der Geschäftsleiter, DStR 2017, 266
- EGMR* Kündigung einer Altenpflegerin nach Strafanzeige gegen Arbeitgeber – Whistleblowing Urteil vom 21.7.2011 – 28274/08, NJW 2011, 3502
- Ehlers/Wolffgang* Recht der Exportkontrolle – Bestandsaufnahme und Perspektiven, 2015
- Ehmann* Der Regierungsentwurf für das Lieferkettengesetz: Erläuterung und erste Hinweise zur Anwendung, ZVertriebsR 2021, 141
- Ehmann/Selmayr* (Hrsg.) Datenschutz-Grundverordnung, Kommentar, 2. Aufl. 2018
- Ehrgott/Reimann/Kaufmann/Carter* Social sustainability in selecting emerging economy suppliers, Journal of Business Ethics, 98(1), 99
- Eichler* Nachhaltige Unternehmenskultur als Grundlage wirksamer Corporate Governance, ZCG 2010, 57
- Eidam* Unternehmen und Strafe: Vorsorge- und Krisenmanagement, 5. Aufl. 2018
- Eisenberg* Beweisrecht der StPO, Spezialkommentar, 10. Aufl. 2017
- Eisenmenger* Ein neuer Rechtsrahmen für Kritische Infrastrukturen (KRITIS) – unter Berücksichtigung der EU-Resilienz-Richtlinie, NVwZ 2023, 1203
- Ellenberger/Bunte* (Hrsg.) Bankrechts-Handbuch, 6. Aufl. 2022
- Engelhardt/Klein* Bitcoins – Geschäfte mit Geld, das keines ist – Technische Grundlagen und zivilrechtliche Betrachtung, MMR 2014, 355
- Erben/Romeike* Allein auf stürmischer See – Risikomanagement für Einsteiger, 3. Aufl. 2016
- Erbs/Kohlhaas* (Hrsg.) Strafrechtliche Nebengesetze, 249. EL 09/2023
- Erdmann/Diehl/Schradin* BeckOK VAG, Stand: 1.9.2023
- Esser/Rübenstahl/Saliger/Tsambikakis* (Hrsg.) Wirtschaftsstrafrecht, 2017
- Eufinger* Kartellrechtliche Compliance im Bankensektor, WM 2014, 1114
- Eufinger* Die neue CSR-Richtlinie – Erhöhung der Unternehmenstransparenz in Sozial- und Umweltbelangen, EuZW 2015, 424
- Eufinger* Der Entwurf zur Einrichtung eines bundesweiten Wettbewerbsregisters – Implikationen für die Compliance, CB 2017, 240
- Eufinger* Zur Kündigung eines Arbeitsverhältnisses wegen Verstößen gegen eine Richtlinie zur Informationssicherheit, CCZ 2022, 411
- Ewelt-Knauer* Proaktive Gestaltung der Compliance-Kultur, WPg 2016, 597
- Faber* Anreizbasierte Regulierung von Corporate Compliance, 2014

- Faust* Compliance und Korruptionsbekämpfung: Beiträge und Übungen zur Organisationsethik (Band 1), 2. Aufl. 2016
- Favoccia/Richter* Rechte, Pflichten und Haftung des Compliance Officers aus zivilrechtlicher Sicht, AG 2010, 137
- Feisel/Makowka* Die neue Nachhaltigkeitsberichterstattung – Welche Anforderungen kommen durch die CSRD auf deutsche Unternehmen zu?, DB 2024, 65
- Feuerstack/Reimann* Tax Compliance Management Systeme in der Betriebsprüfung, StBp 2023, 184
- Fischer* Die Business Judgment Rule als typübergreifendes Institut, 2018
- Fischer* (Hrsg.) Strafgesetzbuch: StGB mit Nebengesetzen, Kommentar, 71. Aufl. 2024
- Fischer/Pellmann/Schoch* (Hrsg.) Kommentar zum Hinweisgeberschutzgesetz, 2023
- Fischer/Schuck* Die Einrichtung von Corporate Governance-Systemen nach dem FISG, NZG 2021, 534
- Fischer/Schulte-Mattler* (Hrsg.) KWG, CRR – Kommentar zu Kreditwesengesetz, VO (EU) Nr. 575/2013 (CRR) und Ausführungsvorschriften, 6. Aufl. 2023
- Fitting/Engels/Schmidt/Trebinge/Linsenmaier* Betriebsverfassungsgesetz: BetrVG, 31. Aufl. 2022
- Fitzer/Gergen* Know your risks: Risiken managen und analysieren nach dem LkSG, CB 2022, 327
- Fladung* Datenschutz-Grundverordnung – neue Compliance-Risiken im Beschäftigtendatenschutz, CB 2015, 364
- Fleischer* Grundstrukturen der lieferkettenrechtlichen Sorgfaltspflichten, CCZ 2022, 205
- Fleischer* Aktienrechtliche Compliance-Pflichten im Praxistest: Das Siemens/Neubürger-Urteil des LG München I, NZG 2014, 321
- Fleischer* Corporate Compliance im aktienrechtlichen Unternehmensverbund, CCZ 2008, 1
- Fleischer/Körber* Due diligence und Gewährleistung beim Unternehmenskauf, BB 2001, 841
- Fleischer/Mankowski* (Hrsg.) Lieferkettensorgfaltspflichtengesetz: LkSG, Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in der Lieferkette, Kommentar, 2023
- Foerstl/Azadegan/Leppelt/Hartmann* Drivers of supplier sustainability: moving beyond compliance to commitment, Journal of Supply Chain Management, 51(1), 67
- Foerstl/Reuter/Hartmann/Blome* Managing supplier sustainability risks in a dynamically changing environment – sustainable supplier management in the chemical industry, Journal of Purchasing and Supply Management, 16(2), 118
- Forgó/Helfrich/Schneider* (Hrsg.) Betrieblicher Datenschutz, 3. Aufl. 2019

Literaturverzeichnis

- Franck* Bring your own device – Rechtliche und tatsächliche Aspekte, RDV 2013, 185
- Frank/Edel/Heine/Heine* Pionierarbeiten in der Lieferkette, Praxisfolgen für das Handels- und Arbeitsrecht (Teil I), BB 2021, 2165
- Freiberg/Lanfermann* (Hrsg.) ESRS Kommentar, Kommentar zu den European Sustainability Reporting Standards, 2023
- Freund* Risikomanagement für Geschäftsführer und Vorstände, NZG 2021, 579
- Freund/Krüger* Das neue Lieferkettensorgfaltspflichtengesetz, NVwZ 2022, 665
- Frey/Pelz* (Hrsg.) BeckOK Geldwäschegesetz, 16. Edition, Stand: 1.12.2023
- Fromm/Nordemann* Urheberrecht, 13. Aufl. 2024
- Fuhlrott* Arbeitnehmerdatenschutz – Aktuelle Entwicklungen, ArbRAktuell 2020, 103
- Funk/Zeifang* Die GNU General Public License, Version 3, CR 2007, 617
- Gabriel/Mertens/Prieß/Stein* (Hrsg.) BeckOK Vergaberecht, 31. Edition, Stand: 1.2.2024
- Gaess* IT-Governance als Basis strategischer IT-Steuerung, Cloud Governance und für ein erfolgreiches Management von Cyber Risiken, 2023
- Gänswein* Gesamtschuldnerausgleich unter Kartellbeteiligten, NZKart 2016, 51
- Garden/Hiéramente* Die neue Whistleblowing-Richtlinie der EU – Handlungsbedarf für Unternehmen und Gesetzgeber, BB 2019, 963
- Gebauer/Kirschhöfer/Repke* (Hrsg.) Compliance-Miszellen, Dieter Eisele zum 80. Geburtstag gewidmet, 2019
- Gehling/Ott* (Hrsg.) LkSG, Kommentar, 2022
- Gehling/Ott/Lüneborg* Das neue Lieferkettensorgfaltspflichtengesetz – Umsetzung in der Unternehmenspraxis, CCZ 2021, 230
- Gehra/Gittfried/Lienke* Prävention von Geldwäsche und Terrorismusfinanzierung, 2. Aufl. 2020
- Gehring* Tax CMS in der Umsatzsteuer – ein Praxisleitfaden, CCZ 2019, 197
- Gehrman/Wengenroth* Geldwäscherechtliche Pflichten für Güterhändler am Beispiel von Immobilienunternehmen, BB 2019, 1035
- Geier/Meringdal/Stille* ESG-Compliance – Taxonomie, Offenlegung, Governance, 2023
- Geminn/Johannes/Miedzianowski* Datenschutz nach Corona – was ist da, was bleibt, was kommt?, ZD-Aktuell 2020, 07073
- Geppert/Schütz* (Hrsg.) Beck'scher Kommentar zum TKG, Telekommunikationsgesetz, Telekommunikation-Telemedien-Datenschutz-Gesetz, 5. Aufl. 2023
- Gerdemann* Revolution des Whistleblowing-Rechts oder Pfeifen im Walde?, RdA 2019, 16

- Gergen/Fitzer* Who is who – Der (unmittelbare) Zulieferer im System des LkSG – Teil 1, CCZ 2024, 98
- Geuenich/Kiesel* Tax Compliance bei Unternehmen – einschlägige Risiken und Folgerungen für die Praxis, BB 2012, 155
- Geyrhalter/Zirngibl/Strehle* Haftungsrisiken aus dem Scheitern von Vertragsverhandlungen bei M&A-Transaktionen, DStR 2006, 1559
- Ghassemi-Tabar* (Hrsg.) Lieferkettensorgfaltspflichtengesetz, Kommentar, 2024
- Ghassemi-Tabar* (Hrsg.) Deutscher Corporate Governance Kodex: DCGK, Kommentar, 2. Aufl. 2023
- Giebichenstein/Schirp* Neues IT-Sicherheitsgesetz (IT-SiG) und Sicherheitskatalog gem. § 11 Abs. 1a EnWG, CB 2015, 66
- Gierschmann/Baumgartner* (Hrsg.) Telekommunikation-Telemedien-Datenschutz-Gesetz: TTDSG, Kommentar, 2023
- Giese/Dachner* Arbeitsrechtliche Folgen des VerSanG: Das Ende des Personalgesprächs bei internen Ermittlungen, ZIP 2020, 498
- Gleißner* Grundlagen des Risikomanagements – Handbuch für ein Management unter Unsicherheit, 2022
- Gleißner* Entscheidungsorientiertes Risikomanagement: Risikoanalyse, risikogerechte Bewertung und wertorientiertes Management, Risiko Manager 01/2019, 28
- Gleißner* Risikomaße und Bewertung, Teil 2: Downside-Risikomaße – Risikomaße, Safety-First-Ansätze und Portfoliooptimierung, Risiko Manager 13/2006, 17
- Gleißner* Risikomaße und Bewertung, Teil 3: Kapitalmarktmodelle – Alternative Risikomaße und Unvollkommenheit des Kapitalmarkts, Risiko Manager 14/2006, 14
- Gleißner/Günther/Walkshäusl* Financial sustainability: measurement and empirical evidence, Journal of Business Economics, Vol. 92, 2022, 467
- Gleißner/Nickert/Romeike* Lücken im IDW-Prüfungsstandard 340. Gesetzliche Anforderungen an das Risikomanagement aus StaRUG gehen weit über KonTraG hinaus, Board 01/2024, 22
- Gleißner/Romeike* Risikomanagement – Umsetzung, Werkzeuge, Risikobewertung, 2005
- Gleißner/Romeike* Entscheidungsorientiertes Risikomanagement nach DIIR RS Nr. 2, Der Aufsichtsrat 4/2020, 55
- Gleißner/Romeike* StaRUG und FISG: Neue Aufgaben für den Aufsichtsrat, Der Aufsichtsrat 01/2022, 2
- Gleißner/Romeike* Financial sustainability and risk management, FIRM Yearbook 2023, 125
- Global Reporting Initiative* Consolidated set of the GRI standards, 2022, <https://www.globalreporting.org/standards/download-the-standards/> (zuletzt abgerufen am 22.2.2024)
- Göbel* Unternehmensethik, 5. Aufl. 2017
- Goette/Habersack/Kalss* (Hrsg.) Münchener Kommentar zum Aktiengesetz, Bd. 2, 6. Aufl. 2023

Literaturverzeichnis

- Göhler* Gesetz über Ordnungswidrigkeiten, Kommentar, 19. Aufl. 2024
- Gola/Heckmann* (Hrsg.) Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO/BDSG, 3. Aufl. 2022
- Gola/Heckmann* (Hrsg.) BDSG, Kommentar, 13. Aufl. 2019
- Gold/Trautrimis/Trodd* Modern slavery challenges to supply chain management. Supply Chain Management, 20(5), 2015, 485
- Gomer* Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft, 2020
- Göpfert* Steuerungsinstrumente für die Personalarbeit – Global HR Policies, NZA 2011, 1259
- Gößwein* Die Führungskräfte im Zentrum eines funktionierenden Compliance Management Systems, CCZ 2017, 43
- Gößwein/Hohmann* Modelle der Compliance-Organisation in Unternehmen – Wider den Chief Compliance Officer als „Überoberverantwortungsnehmer“, BB 2011, 963
- Göthel* Grenzüberschreitende M&A-Transaktionen – Unternehmenskäufe, Umstrukturierungen, Joint Ventures, SE, 5. Aufl. 2020
- Grabitz/Hilf/Nettesheim* Das Recht der Europäischen Union, Kommentar, 82. EL 2024
- Grabosch* (Hrsg.) Das neue Lieferkettensorgfaltspflichtengesetz (LkSG), 2021
- Graf* (Hrsg.) BeckOK OWiG, 42. Edition, Stand: 1.4.2024
- Grainer/Kalle* Betriebliche Mitbestimmung nach § 87 Abs.1 Nr.1 und 6 BetrVG – Konvergenzen und Widersprüche im Digitalisierungskontext, RdA 2021, 76
- Grambow/Cimino* Das Lieferkettensorgfaltspflichtengesetz in der Praxis, AnwaltSpiegel 5/2023, S. 7
- Granetzny/Krause* Was kostet ein gutes Gewissen? – Förderung von Whistleblowing durch Prämien nach US-Vorbild?, CCZ 2020, 29
- Grau/Granetzny* EU-US-Privacy Shield – Wie sieht die Zukunft des transatlantischen Datenverkehrs aus?, NZA 2016, 40
- Grigoleit* (Hrsg.) Aktiengesetz, Kommentar, 2. Aufl. 2020
- Grimm/Windeln* (Hrsg.) Zielvereinbarungen, 2006
- Groening/Kanuri* Investor Reaction to Positive or Negative Corporate Social Events, Journal of Business Research, 66 (10) 2013, 852
- Groß* Chief Compliance Officer, 2012
- Grötsch/Scherer* Die Bedeutung von Compliance-Management-Systemen im Straf- und Ordnungswidrigkeitenrecht sowie im Zivil- und Steuerrecht, wistra 2024, 139
- Grötsch/Stürzl* Die „Unkenntnis“ in § 370 Abs. 1 Nr. 2 AO, wistra 2019, 127
- Grottel/Justenhoven/
Schubert/Störk/Deubert/
Budde/Clemm/Pankow/
Sarx* (Hrsg.) Beck'scher Bilanz-Kommentar – Handels- und Steuerbilanz, 13. Aufl. 2022

- Grottel/Schmidt/
Schubert/Störk/Deubert*
(Hrsg.) Beck'scher Bilanz-Kommentar – Handels- und Steuerbilanz,
12. Aufl. 2019
- Grottel/Schmidt/
Schubert/Winkeljohann*
(Hrsg.) Beck'scher Bilanz-Kommentar – Handels- und Steuerbilanz,
10. Aufl. 2016
- Grühn* Der Umweltgutachter, Berufsrecht und Haftungsrecht im Ver-
gleich zum Wirtschaftsprüfer, 2000
- Grüneberg* Bürgerliches Gesetzbuch, Kommentar, 83. Aufl. 2024
- Grützmaker* Open Source Software und Embedded Systems, ITRB 2009,
184
- Grützmaker* Application Service Providing – Urhebervertragsrechtliche As-
pekte, ITRB 2001, 59
- Grützner/Güngör* Aktuelle Entwicklungen in den USA, CCZ 2019, 189
- Grützner/Jakob* Compliance von A–Z, 2. Aufl. 2015
- Guckelberger* Rechtsfragen kritischer Infrastrukturen, DVBl 2019, 525
- Gude* Let's get dangerous – Zur Reichweite der besonderen Mitwir-
kungspflicht gemäß § 153 Abs. 4 AO und der damit verbunde-
nen steuerstrafrechtlichen Implikationen, DStR 2023, 2261
- Gündel/Feiler* Novelle zum Außenwirtschaftsrecht: Handlungsbedarf für
Compliance-Verantwortliche in grenzüberschreitend tätigen
Unternehmen, CB 2013, 236
- Haag/Drodofsk* ESG-Rechtsvorschriften im internationalen Konzern – Imple-
mentierungsmaßnahmen, CB 2024, 61
- Habersack/Huber/
Spindler* (Hrsg.) Festschrift für Eberhard Stolz, 2014
- Hadding/Hopt/
Schimansky* Verbraucherschutz im Kreditgeschäft – Compliance in der Kre-
ditwirtschaft, 2008
- Haellmigk* Vorsicht beim Datentransfer: Exportrecht gilt für alle Unterneh-
men, CR 2013, 350
- Haellmigk/Vulin* (Cloud-)Datentransfer und Exportkontrolle – Neue Compli-
ance-Herausforderungen für Unternehmen, CCZ 2016, 28
- Häfel* Der Menschenrechtsbeauftragte im Lieferkettensorgfalts-
pflichtengesetz – ein weiterer betrieblicher Beauftragter?, ARP
2021, 299
- Hagel/Wiedmann* Menschenrechtsbeauftragte, Rechte und Pflichten sowie Ar-
beitshilfen für die Praxis, 2024
- Hagel/Wiedmann* Der Menschenrechtsbeauftragte – Das (noch) unbekannte We-
sen der LkSG-Compliance, BB 2023, Heft 19, I
- Hagel/Wiedmann* Konfliktpotenziale bei der LkSG-Compliance, Konfliktdyna-
mik 2023, 266
- Hagel/Wiedmann* Wie muss das LkSG aufgrund der CS3D angepasst werden?,
CCZ 2024, 185

- Hamann/Sigle/Grub* (Hrsg.) Gesellschaftsrecht, Finanzierung und Unternehmensnachfolge – Gestaltung, Finanzierung, Internationalisierung, Mergers & Acquisitions und Nachfolge, 3. Aufl. 2022
- Hammer* Operational Tax – Schnittstelle zwischen Steuerrecht, Produktkenntnis und Prozesswissen bei Finanzdienstleistern, BB 2013, 1175
- Handel* Meldestellenbeauftragte – Rechte, Pflichten und Praxishinweise für Beauftragte nach dem HinweisgeberschutzG, 2023
- Handel* Die Stellvertretung bei der Selbstanzeige, DSr 2018, 709
- Hannemann/Steinbrecher/Weigl* Mindestanforderungen an das Risikomanagement (MaRisk), Kommentar, 6. Aufl. 2022
- Hannich/Apppl/Diemer et al.* Karlsruher Kommentar zur Strafprozessordnung: StPO, 7. Aufl. 2013
- Haouache* Unternehmensbeauftragte und Gesellschaftsrecht der AG und GmbH, 2003
- Haouache* Unternehmensbeauftragte und Gesellschaftsrecht der AG und GmbH, 2003
- Harbarth* Anforderungen an die Compliance-Organisation in börsennotierten Unternehmen, ZHR 2015, 136
- Harbarth/Brechtel* Rechtliche Anforderungen an eine pflichtgemäße Compliance-Organisation im Wandel der Zeit, ZIP 2016, 241
- Hardtke/Kleinfeld* (Hrsg.) Gesellschaftliche Verantwortung von Unternehmen, 2010
- Harings/Jürgens/Thalhammer* Die Rolle des Menschenrechtsbeauftragten im Lieferketten-sorgfaltspflichtengesetz, CB 2022, 93
- Harings/Beermann/Hörnig* BAFA-Handreichung zur Zusammenarbeit in der Lieferkette, CB 2023, 450
- Harings/Jürgens* Das Lieferketten-sorgfaltspflichtengesetz, Umsetzung und Auswirkungen des LkSG in der Praxis, 2022
- Harings/Loets* Auswirkungen personenbezogener Sanktionen auf privatrechtliche Verträge, RdTW, 2015, 321
- Hartl/Jentzen* Der Data Act, Datenzugangsrechte und Art. 6 DS-GVO, ZdiW 2023, 65
- Hartmann/McGuire/Schulte-Nölke* Datenzugang bei smarten Produkten nach dem Entwurf für ein Datengesetz (Data Act), RDi 2023, 49
- Hartmann/Moeller* Chain liability in multitier supply chains? Responsibility attributions for unsustainable supplier behavior, Journal of Operations Management, 2014, 32(5), 281
- Hartmann/Romeike* Business Judgement Rule, FIRM Jahrbuch 2015
- Hartmann-Rüppel/Nagel* Durchsuchungen des Bundeskartellamts. Konvergenzen mit und Unterschiede zum EU-Recht und die behördliche Praxis nach der 10. GWB-Novelle, CB 2022, 230
- Hasselbach/Stepper* Veröffentlichungspflichten bei M&A-Transaktionen und bei Übernahmen börsennotierter Unternehmen, BB 2020, 203

- Hastenrath* E-Learning in der Compliance-Praxis: Anforderungen, Möglichkeiten, Grenzen, Kosten, CCZ 2014, 132
- Hastenrath* Möglichkeit und Grenzen der Pflichtendelegation an den (Chief) Compliance Officer, CB 2016, 6
- Hastenrath* (Hrsg.) Compliance-Kommunikation, Professionell – international – zielgruppengerecht, 2017
- Hastenrath/Müller* Möglichkeiten der Incentivierung von Compliance-gerechtem Verhalten, CB 2017, 154
- Hau/Poseck* (Hrsg.) BeckOK BGB, 68. Edition, Stand: 1.11.2023
- Haus/Erne* Kartellrechtliche Compliance – Anforderungen und Ausgestaltung, ZWH 2016, 162
- Hauschka* Compliance am Beispiel der Korruptionsbekämpfung Eine Erwiderung aus der Praxis auf Uwe H. Schneiders Vorschläge, ZIP 2003, 645, ZIP 2004, 877
- Hauschka* Compliance am Beispiel der Korruptionsbekämpfung – Eine Erwiderung aus der Praxis auf Uwe H. Schneiders Vorschläge, ZIP 2004, 877
- Hauschka* Formularbuch Compliance, 2013
- Hauschka/Galster/Marschlich* Leitlinien für die Tätigkeit in der Compliance-Funktion im Unternehmen (für Compliance Officer außerhalb regulierter Sektoren) – Gemeinsames Positionspapier des Netzwerk Compliance e. V., der Fachgruppe Compliance des Bundesverbandes der Unternehmensjuristen (BUJ), des DICO – Deutsches Institut für Compliance und des Berufsverbandes der Compliance Manager (BCM), CCZ 2014, 243
- Hauschka/Moosmayer/Lösler* (Hrsg.) Corporate Compliance, Handbuch der Haftungsvermeidung im Unternehmen, 3. Aufl. 2016
- Hauser/Bretti-Rainalter/Blumer* Whistleblowing Report 2021
- Heckschen* Keine analoge Anwendung des § 179a AktG auf die GmbH, AG 2019, 420
- Hefendehl* Alle lieben Whistleblowing, in: Böse/Sternberg-Lieben, Festschrift für Amelung, 2009
- Heiermann/Zeiss/Summa* (Hrsg.) jurisPK-Vergaberecht, 5. Aufl. 2016
- Heinmann/Flöter* Neue Herausforderungen für die Mitbestimmung durch ESG (Environmental Social Governance), ESG 2022, 138
- Heißner* Erfolgsfaktor Integrität, 2. Aufl. 2014
- Helisch* Unternehmenskultur, Corporate Identity und Loyalität als wesentliche Bestimmungsgrößen für gelebte Compliance, CB 2014, 225
- Hembach* Praxisleitfaden Lieferkettensorgfaltspflichtengesetz 2022
- Henn/Jahn* (Hrsg.) BeckOK Lieferkettensorgfaltspflichtengesetz, 5. Edition, Stand: 15.3.2024

Literaturverzeichnis

- Hennrichs/Pöschke* Die Pflicht des Aufsichtsrats zur Prüfung des „CSR-Berichts“, NZG 2017, 121
- Henssler/Willemsen/Kalb* Arbeitsrecht, 10. Aufl. 2022
- Herb* Von Compliance zu Integrität, Handelsblatt Journal 2015, 17
- Herold* Whistleblower – Entscheidungsfindung, Meldeverhalten und kriminologische Bewertung, 2016
- Herrlinger/Ahlenstiehl* Durch Selbstreinigung aus dem Wettbewerbsregister, WuW 2022, 396
- Herrmann/Rünz* Praktische Hinweise und Maßnahmen zur Umsetzung des Lieferkettensorgfaltspflichtengesetzes im Unternehmen, DB 2021, 3078
- Herzog/Achtelik* (Hrsg.) Geldwäschegesetz (GwG), 5. Aufl. 2023
- Heuel/Harink* Steuerhinterziehung im Zeitalter elektronischer Steuererklärungen, AO-StB 2020, 49
- Heuel/Matthey* Steuerhinterziehung: Verteidigung gegen verdeckte Gewinnausschüttung (Teil 1), AO-StB 2018, 54
- Heuking/von Coelln* Public Compliance – Maßnahmen zur Regelkonformität im öffentlichen Sektor, DÖV 2012, 827
- Heussen* Rechtliche Verantwortungsebenen und dingliche Verfügungen bei der Überlassung von Open Source Software, MMR 2004, 445
- Heuvels/Höβ/Kuß/Wagner* Vergaberecht. Gesamtkommentar zum Recht der öffentlichen Auftragsvergabe (GWB – 4. Teil, VgV, KonzVgV, SektVO, VSVgV, VO(EG)1370/2007, VOB/A, VOL/A), 2. Aufl. 2021
- Hildebrandt/Koch* Smart Sanctions – Grundlagen und praktische Bedeutung der EU-Sanktionslisten, IWRZ 2016, 152
- Hilgert* Das IT-Sicherheitsgesetz: Neue Anforderungen für alle geschäftsmäßigen Onlinedienste, CR-online.de Blog, <https://www.cr-online.de/blog/2015/08/17/das-it-sicherheitsgesetz-neue-anforderungen-fuer-alle-geschaftsmaessigen-onlinedienste/>
- Hirsch/Trouvain* Das deutsche Hinweisgeberschutzgesetz – Was lange währt, wird endlich gut?, ESG 2023, 9
- Hirte/Mülbert/Roth* (Hrsg.) Aktiengesetz: AktG, Bd. 2/1: §§ 23–40, 5. Aufl. 2015
- Höche/Piekenbrock/Siegmann* (Hrsg.) Bankrecht und Bankpraxis, Loseblattwerk, Stand 3/2024
- Hoejmoose/Brammer/Millington* “Green” supply chain management: The role of trust and top management in B2B and B2C markets, Industrial Marketing Management, 41(4), 609
- Hoeren* Softwareauditierung, CR 2008, 409
- Hoffmann* Das Verbot der Abgabe einer Boykott-Erklärung nach § 7 Außenwirtschaftsverordnung, EuZW 2019, 315

- Hoffmann/Schieffer* Pflichten des Vorstands bei der Ausgestaltung einer ordnungsgemäßen Compliance-Organisation, NZG 2017, 401
- Hofmann/Busse/Bode/Henke* Sustainability-related supply chain risks: conceptualization and management, Business Strategy and the Environment, 23(3), 160
- Hofmann/Schleper/Blome* Conflict minerals and supply chain due diligence: an exploratory study of multi-tier supply chains. Journal of Business Ethics, 147(1), 2018, 115
- Hohmann* Die zentralen Genehmigungspflichten/Verbote des US-Reexportrechts, AW-Prax 2007, 456
- Holle* Kartellrechtliche Bewältigung von Nachhaltigkeitskooperationen, ZHR 188, 98
- Hölters (Hrsg.)* Aktiengesetz, Kommentar, 4. Aufl. 2022
- Hölezemann/Ramadan/Otto/Nordmann* Tax-CMS als Game-Changer in steuerlichen Außenprüfungen?, WPg 2023, 1394
- Hooghoff* Bessere Informationen für öffentliche Auftraggeber: Das Wettbewerbsregister beim. Bundeskartellamt, WuW 2021, 551
- Hopson* Effektive ethische Compliance-Programme im Sinne der United States Federal Sentencing Guidelines, CCZ 2008, 208
- Hornkohl* Kartellrechtliche Kollektivklagen nach dem Verbandsklagenrichtlinienumsetzungsgesetz: (K)ein Meilenstein?, NZKart 2024, 2
- Huber/Huetz* Handbuch Import- und Exportrecht, 2014
- Hübschmann/Hepp/Spitaler* Abgabenordnung-Finanzgerichtsordnung, Kommentar, 277. EL Stand: 12/2023
- Hüffer/Koch (Hrsg.)* Aktiengesetz, Kommentar, 14. Aufl. 2020
- Hugger/Röhrich* Der neue UK Bribery Act und seine Geltung für deutsche Unternehmen, BB 2010, 2643
- Hungenberg* Strategisches Management in Unternehmen, Ziele – Prozesse – Verfahren, 8. Aufl. 2014
- Hunsmann* Die Aufsichtspflichtverletzung (§ 130 OWiG) unter besonderer Berücksichtigung des Steuerrechts, DStR 2014, 855
- Huppertz/Schneider* Software-Lizenzaudits im Unternehmen – Datenschutzrechtliche Aspekte bei der Überprüfung von Softwarenutzung, ZD 2013, 427
- Hüskemenger/Zumwinkel* Mittelbare (ausländische) Anteilsverschiebungen an grundbesitzhaltenden Gesellschaften, PStR 2023, 14
- Huth/Romeike (Hrsg.)* Risikomanagement in der Logistik, 2016
- Ihle* Beweisverwertungsverbote bei heimlicher Überwachung von Arbeitnehmern, BB 2014, 896
- Immenga/Mestmäcker (Begr.)* Wettbewerbsrecht, Band 1, Teil 1, Kommentar zum Europäischen Kartellrecht, 6. Aufl. 2019 ; Band 2, Teil 1, Kommentar zum Deutschen Kartellrecht – GWB, 7. Aufl. 2024

Literaturverzeichnis

- Inderst/Bannenberg/
Poppe* Compliance – Aufbau – Management – Risikobereiche, 3. Aufl. 2017
- Institut der Deutschen
Wirtschaftsprüfer (IDW)* WP-Handbuch, Band 1, 16. Aufl. 2019
- Institut der Deutschen
Wirtschaftsprüfer (IDW)* IDW Prüfungsstandard 261 „Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken“ (IDW PS 261 n. F.), Stand: 13.3.2013
- International Chamber
of Commerce (ICC)* The ICC Antitrust Compliance Toolkit, 2013
- Intveen* Softwarelizenzaudits aus Anwendersicht, ITRB 2012, 208
- Itzen* Richtungswechsel, Bestandsaufnahme, Prävention: Das Gerüst einer erfolgreichen Compliance-Strategie, BB-Special 5/2008, 12
- Jacobs* IT-Compliance – Vorgaben und Handlungsrahmen, CB 2017, 299
- Jaeger* Auswirkungen der EU-Urheberrechtsrichtlinie auf die Regelungen des Urheberrechtsgesetzes für Software, CR 2002, 309
- Jaeger/Kokott/Pohl-
mann/Schroeder/
Seeliger (Hrsg.)* Frankfurter Kommentar zum Kartellrecht, Bd. 2 (EG-Kartellrecht Teil 1), Stand: 5/2024
- Jaeger/Metzger* Open Source Software und deutsches Urheberrecht, GRUR Int. 1999, 839
- Jaeger/Metzger* Open Source Software, 5. Aufl. 2020
- Jäger/Rödl/Campos
Nave* Praxishandbuch Corporate Compliance, 2009
- Jakob/Orth/Stopper* Praxishandbuch Vereins- und Verbandsrecht, 2021
- Jarosch/Schreier* „Quiet Quitting“ im Kontext von Arbeitskräftemangel und den aktuellen arbeitsrechtlichen Rahmenbedingungen, ARP 2023, 262
- Jenne* US-Leitfaden zur Bewertung von Compliance-Systemen – Orientierungshilfe für deutsche Unternehmen, Behörden und Gerichte, CB 2019, 327
- Jenne* Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, 2017
- Joecks/Jäger/Randt* Steuerstrafrecht, 9. Aufl. 2023
- Johann/Sangi (Hrsg.)* Lieferkettensorgfaltspflichtengesetz, Kommentar 2023
- Johannsen-Roth/Illert/
Ghassemi-Tabar;* DCGK: Deutscher Corporate Governance Kodex, 1. Aufl. 2020
- Johnson* Die Regelung zur Beweislastumkehr nach Maßgabe des Richtlinienentwurfs der EU-Kommission zum Schutz von Hinweisgebern – Quell eines institutionellen Rechtsmissbrauchs?, CCZ 2019, 66
- Johnson* LG Dortmund, Urteil vom 10.1.2019 – 7 O 95/15 – Verhaltenskodex mit Lieferanten ist regelmäßig kein Vertrag zugunsten Dritter bzw. mit Schutzwirkung für Dritte, CCZ 2020, 103

- Johnson* CB-Kommentar: OLG Nürnberg: Die unterlassene Implementierung eines Vier-Augen-Prinzips als haftungsrelevante Pflichtverletzung, CB 2022, 502
- Joost* Die Prinzipal-Agenten-Theorien in der Betriebswirtschaftslehre, 2001
- Jungkind/Bormann* Interne Compliance-Programme als Instrument der Exportkontrolle, AW-Prax 2020, 103
- Jungkind/Winkler* Beschränktes Boykottverbot nach § 7 Satz 2 AWV neu – Freie Fahrt für die Geltung ausländischen Sanktionsrechts für deutsche Unternehmen?, AW-Prax 2019, 354
- Kaeser* Gewinne sind nicht das einzige Ziel, Harvard Business Manager 10/2019, 44
- Kahneman* Thinking, Fast and Slow, Farrar, Straus and Giroux, 2011
- Kajüter* Nichtfinanzielle Berichterstattung nach dem CSR-Richtlinie-Umsetzungsgesetz, DB 2017, 617
- Kalls* Wie sollen die Verhaltenspflichten nach der Lieferkettensorgfalts-Richtlinie (CSDDD) erfüllt werden – ein rechtspolitischer Zuruf!, ZfPW 2024, 181
- Kaltenborn /Krajewski/
Rühl/Saage-Maaß
(Hrsg.)* Lieferkettensorgfaltspflichtenrecht, LkSG, GwB, EU-HolzhandelsVO, EU-KonfliktmineralienVO, BetrVG, WRegG, CSR-RL-UmsG, 2023
- Kaltenbrunner/Urnik* Unternehmensführung, State of the art und Entwicklungsperspektiven, 2012
- Karbaum* Kartellrechts-Compliance – Mehr Fragen als Antworten nach einer Dekade intensiver Diskussion der Compliance-Verantwortung des Vorstands?, AG 2013, 863
- Kark* Compliance-Risikomanagement – Gefährdungslagen erkennen und steuern, 2. Aufl. 2019
- Karten* Existenzrisiken der Gesellschaft – Herausforderungen für die Assekuranz, ZVersWiss 3/1988, 343
- Kassing* Softwarepooling im Konzern – Möglichkeiten und Grenzen, 2006
- Kayser* ISO 37001: Ein Standard will mit Korruption aufräumen, CB 2015, 441
- Keller/Schümmer* M&A – Aufklärungspflichten des Verkäufers nach einer Due Diligence, NJW-Spezial 2023, 719
- Kempff/Lüderssen/Volk
(Hrsg.)* Gemeinwohl im Wirtschaftsstrafrecht, 2013
- Kempff/Schilling* Vermögensabschöpfung: Strategien bei (drohendem) Verfall von Grundrechten (Deutsch), 2007
- Kempter/Steinat* Compliance – arbeitsrechtliche Gestaltungsinstrumente und Auswirkungen in der Praxis, NZA 2017, 1505
- Kerner/Rixen* Ist Korruption ein Strafrechtsproblem?, GA 1996, 355

- Kessler* Der Einsatz komplexer Finanzinstrumente im Unternehmen – gesellschaftsrechtliche Anforderungen an das Risikomanagement, BB 2013, 1098
- Kessler* (Hrsg.) Das Strukturrisiko von Finanzderivaten, 2012
- Kessler* (Hrsg.) Unternehmensfinanzierung Mittelstand, 2014
- Kindhäuser/Neumann/Paeffgen/Saliger* (Hrsg.) Strafgesetzbuch: StGB, Kommentar, 6. Aufl. 2023
- Kipker* (Hrsg.) Cybersecurity, Rechtshandbuch, 2. Aufl. 2023
- Kipker/Dittrich* Kritischer Infrastrukturschutz ganz konkret?, ZRP 2023, 230
- Klein, David* Blockchains als Verifikationsinstrument für Transaktionen im IoT, DSRITB 2015, 429
- Klein, Franz* (Hrsg.) Abgabenordnung, Kommentar, 17. Aufl. 2023
- Kleinfeld/Martens* (Hrsg.) CSR und Compliance: Synergien nutzen durch ein integriertes Management, 2018
- Klene* Corporate Social Responsibility – Richtlinie, Umsetzung und Konsequenzen, WM 2018, 308
- Klinger, Michael A./Klinger, Oskar* (Hrsg.) Das Interne Kontrollsystem im Unternehmen, 2. Aufl. 2009
- Klopp* Der Compliance-Beauftragte, Arbeitsrechtliche Stellung und Funktion in der Compliance, 2012
- Knauff* Der Regelungsverbund: Recht und Soft Law im Mehrebenensystem, 2010
- Knierim/Rübenstahl/Tsambikakis* Internal Investigations – Ermittlungen im Unternehmen, 2. Aufl. 2016
- Koch, Frank* Client Access License – Abschied von der Softwarelizenz?, ITRB 2011, 42
- Koch, Frank* Urheber- und kartellrechtliche Aspekte der Nutzung von Open-Source-Software, CR 2000, 273
- Koch, Frank* Urheber- und kartellrechtliche Aspekte der Nutzung von Open-Source-Software (II), CR 2000, 333
- Koch, Jens* Aktiengesetz, 18. Aufl. 2024
- Koch, Jens* Compliance-Pflichten im Unternehmensverbund, WM 2009, 1013
- Köhlbrandt/Gleißner/Günther* Umsetzung gesetzlicher Anforderungen an das Risikomanagement in DAX- und MDAX-Unternehmen. Eine empirische Studie zur Erfüllung der gesetzlichen Anforderungen nach den §§ 91 und 93 AktG, Corporate Finance, Heft Nr. 07-08/2021, 248
- Köhler/Häferer* Mitbestimmungsrechte des Betriebsrats im Zusammenhang mit Compliance-Systeme, GWR 2015, 159
- Köhler/Häferer* Mitbestimmungsrechte des Betriebsrats im Zusammenhang mit Compliance-Systemen, GWR 2015, 159
- Kohlmann* Steuerstrafrecht, Kommentar, 81. EL Stand: 11/2023

- Kohm/Eppelmann* Blick aus der Praxis auf die neue Vertikal-GVO, GRUR-Prax 2022, 458
- Kölbel/Herold* Whistleblowing, Eine kriminologische Analyse aus Anlass der aktuellen kriminalpolitischen Debatte, MschrKrim 2010, 424
- Koll* Koll Vorzeitige Löschung aus dem vergaberechtlichen Wettbewerbsregister wegen Selbstreinigung, NZBau 2023, 491
- Kollmann* Das „Gesetz zur Modernisierung des Außenwirtschaftsrechts“, AW-Prax 2013, 267
- Komma* Der Geldwäscheverdacht als Haftungsfalle ?, CB 2019, 197
- Körner* Beschäftigtendatenschutz in Betriebsvereinbarungen unter Geltung der DS-GVO, NZA 2019, 1389
- Kort* Verhaltensstandardisierung durch Corporate Compliance, NZG 2008, 81
- Kort* Compliance-Pflichten und Haftung von GmbH-Geschäftsführern, GmbHR 2013, 566
- Korte/Romeike* MaRisk VA erfolgreich umsetzen: Praxisleitfaden für das Risikomanagement in Versicherungen, 2. Aufl. 2010
- Kotthoff/Wieczorek* Rechtsrahmen von Softwarelizenzaudits – Zulässigkeit und Grenzen, MMR 2014, 3
- Kowallik* Antrag auf Prüfungserleichterungen nach § 38 EGAO in der nächsten Außenprüfung, DB 2023, 804
- KPMG AG (Hrsg.)* Das wirksame Compliance-Management-System, 2. Aufl. 2016
- Kraft/Winkler* Zur Garantenstellung des Compliance Officers – Unterlassungsstrafbarkeit durch Organisationsmangel, CCZ 2009, 29
- Krais* Geldwäsche und Compliance: Praxisleitfaden für Güterhändler, 2018
- Krais* Geldwäsche-Compliance für Industrie und Handel, 2. Aufl. 2022
- Kramer/Renz/Hartz/Braun* Soll ich Compliance-Beauftragter werden?, BvD – News 1/2015, 12
- Kramer/Schunder* Business Human Rights Due Diligence nach dem Lieferketten-sorgfaltspflichtengesetz – need to know für Unternehmen, BB 2024, 75
- Krause* Strafrechtliche Haftung des Aufsichtsrates, NSTz 2011, 57
- Krause/Prieß* Die bußgeldbefreiende Selbstanzeige bei fahrlässigen Verstößen im neuen Außenwirtschaftsrecht (§ 22 IV AWG n. F.), NSTz 2013, 688
- Kreiß/Siebenbrock* Blenden Wuchern Lamentieren: Wie die Betriebswirtschaftslehre zur Verrohung der Gesellschaft beiträgt, 2019
- Kremer/Bachmann/Favoccia/v. Werder* Deutscher Corporate Governance Kodex, 9. Aufl. 2023
- Kremer/Klahold* Compliance-Programme in Industriekonzernen, ZGR 2010, 113
- Kreutzer* Wirksamkeit der GNU General Public Licence (GLP) nach deutschem Recht, MMR 2004, 693

Literaturverzeichnis

- Krieger/Schneider* Handbuch Managerhaftung, 4. Aufl. 2023
- Krimphove* Die „neue“ MaRisk (BA) 9/2017, BKR 2018, 1
- Krimphove (Hrsg.)* MaComp – Rundschreiben 05/2018 (WA) – Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten, 3. Aufl. 2021
- Krimphove/Kruse (Hrsg.)* MaComp – Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 63 ff. WpHG für Wertpapierdienstleistungsunternehmen“, Kommentar, 2. Aufl. 2019
- Kröger* Korruptionsschäden, Unternehmensgeldbußen und Imageschäden – Haftungs- und schadensrechtliche Fragen der Organmitgliederhaftung, 2013
- Kroke* Ist die Lizenz- und Vergütungspflicht für indirekte Nutzung von Software urheberrechtlich unwirksam?, CR 2019, 73
- Krumm* Die sog. Modernisierung der Außenprüfung, Ubg 2023, 284
- Kubis/Tödtmann (Hrsg.)* Arbeitshandbuch für Vorstandsmitglieder, 3. Aufl. 2022
- Kuhlen* Zum Verhältnis von strafrechtlicher und zivilrechtlicher Haftung für Compliance-Mängel, NZWiSt 2015, 121
- Kühling/Buchner (Hrsg.)* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Kommentar, 4. Aufl. 2024
- Kuhn/Weibler* Ist Ethik ein Erfolgsfaktor? Unternehmensethik im Spannungsfeld von Oxymoron Case, Business Case und Integrity Case, Zeitschrift für Betriebswirtschaft 81, Special Issue 1/2011, 93
- Kuhn/Weibler* Bad Leadership, 2020
- Kümpel/Mülbert/Früh/Seyfried (Hrsg.)* Bankrecht und Kapitalmarktrecht, 6. Aufl. 2022
- Kupczyk* Die Projektantenproblematik im Vergaberecht, NZBau 2010, 21
- Kütting/Busch* Zum Wirrarr der Überwachungsbegriffe, DB 2009, 1361
- Kutschelis* Korruptionsprävention und Geschäftsleiterpflichten im nationalen und internationalen Unternehmensverbund, 2014
- Küttner* Personalbuch 2024, Arbeitsrecht, Lohnsteuerrecht, Sozialversicherungsrecht, 31. Aufl. 2024
- Laasch/Jamali/Freeman/Suddaby (Hrsg.)* The Research Handbook of Responsible Management, 2020
- Lampert/Niejahr/Kübler/Weidenbach* EG-KartellVO, Praxiskommentar, 2004
- Langfermann/Baumüller* Der Anwendungsbereich der Corporate Sustainability Reporting Directive (CSRD): Detailregelungen und Zweifelsfragen, IRZ 2023, 89
- Lanzinner/Wirth* Compliance Challenge Social Media, CCZ 2021, 151
- Laufhütte/R. Rissing-van Saan/K. Tiedemann (Hrsg.)* Strafgesetzbuch, Leipziger Kommentar, 12. Aufl. 2006 ff.
- Laux* Entscheidungstheorie, 3. Aufl. 1995

- Laux/Gillenkirch/
Schenk-Mathes* Entscheidungstheorie, 10. Aufl. 2018
- LeBaron/Lister* The hidden costs of global supply chain solutions. Review of International Political Economy, 29(3), 2021, 669
- Lehmann/Giedke* Urheberrechtliche Fragen des Cloud Computings, CR 2013, 681
- Lelley* Compliance im Arbeitsrecht, 2010
- Leupold/Wiebe/Glossner* Münchener Anwaltshandbuch IT-Recht Recht, Wirtschaft und Technik der digitalen Transformation, 4. Aufl. 2020 (Hrsg.)
- Lexa/Hammer* Social Media Guidelines – Sichere Kommunikation in den sozialen Medien, CCZ 2014, 45
- Leyens* Erfahrungen im Europäischen Gesellschaftsrecht und Entwicklungschancen des Regelungsansatzes, Zeitschrift für Europäisches Privatrecht, ZEuP 2016, 388
- Liese* Compliance in Due-Diligence-Fragelisten, BB Special 4 (zu BB 50/2010), 27
- Liese* Much Ado about Nothing? Oder: Ist der Vorstand einer Aktiengesellschaft verpflichtet, eine Compliance-Organisation zu implementieren?, BB-Special 5 (zu BB 5/2008), 17
- Liese/Schulz* Risikomanagement durch Compliance-Audits – Neue Herausforderungen für die Unternehmensorganisation, BB 2011, 1347
- Link/Scheffler/Flath/
Oehlmann/Dommers* Risikomanagement in deutschen Industrieunternehmen, Controller Magazin, Heft 2/2021, 54
- Linke/Fröhlich* Gestaltungsoptionen für Vertraulichkeitsvereinbarungen bei Unternehmenstransaktionen, GWR 2014, 449
- Lo* Effects of supply chain position on the motivation and practices of firms going green, International Journal of Operations & Production Management, 34(1), 93
- Loewenheim/Meessen/
Riesenkampff/Kersting/
Meyer-Lindemann* Kartellrecht, Kommentar zum Deutschen und Europäischen Recht, 4. Aufl. 2020 (Hrsg.)
- Lorenz/Krülls* Die Lieferketten-Risikoanalyse nach dem LkSG – Ein taugliches Konzept, aber unklare Maßstäbe, CCZ 2023, 100
- Löschhorn/Fuhrmann* „Neubürger“ und die Datenschutz-Grundverordnung: Welche Organisations- und Handlungspflichten treffen die Geschäftsleitung in Bezug auf Datenschutz und Datensicherheit?, NZG 2019, 161
- Lösler* Das moderne Verständnis von Compliance im Finanzmarktrecht, NZG 2005, 104
- Lüdemann* Connected Cars – Das vernetzte Auto nimmt Fahrt auf, der Datenschutz bleibt zurück, ZD 2015, 247
- Lüneborg* Das Hinweisgeberschutzgesetz – die (un)endliche Geschichte, ZIP 2023, 941

Literaturverzeichnis

- Lutter* Die Business Judgment Rule und ihre praktische Anwendung, ZIP 2007, 841
- Lutter* Due diligence des Erwerbers beim Kauf einer Beteiligung, ZIP 1997, 613
- Lutter/Hommelhoff* (Hrsg.) GmbHG, Kommentar, 20. Aufl. 2020
- Lutter/Krieger* Handbuch der Managerhaftung, 3. Aufl. 2017
- Luz/Neus/Schaber/Schneider/Wagner/Weber* KWG mit CRR, Kommentar, 4. Aufl. 2023
- Madauß* Verdeckte Gewinnausschüttung und Steuerstrafrecht – ausgewählte Einzelaspekte, ZWH 2019, 44
- Mäger/von Schreitter* Die kartellrechtliche Bußgeldhaftung nach der 9. GWB Novelle – Überblick und Kritik, NZKart 2017, 264
- Mahnhold* „Global Whistle“ oder „Deutsche Pfeife“ – Whistleblowing-Systeme im Jurisdiktionskonflikt, NZA 2008, 737
- Mai/Scherer* Simulating Copulas (Stochastic Models, Sampling Algorithms and Applications), World Scientific, 2012
- Makowicz* Die Deutschen und deren Compliance, CB 2015, 45
- Makowicz/Wüstemann* Betriebswirtschaftlicher und juristischer Nutzen der Ausgestaltung von Compliance-Management-Systemen nach dem globalen Leitfaden ISO 19600, BB 2015, 1195
- Mallmann/Henke* Anm. zu BGH: Erfüllung von Aufklärungspflichten durch Unterlagen im Datenraum, NJW 2023, 3398
- Mandelbrot* Fraktale und Finanzen – Märkte zwischen Risiko, Rendite und Ruin, 2004
- Mann* Buddenbrooks. Verfall einer Familie, 46. Aufl. 1999
- Mantz* Anmerkung zu LG Hamburg, Urt. v. 14.6.2013 – 308 O 10/13: Pflicht zur Bereithaltung des Quellcodes nach GPLv2, CR 2013, 640
- Marly* Praxishandbuch Softwarerecht, 7. Aufl. 2018
- Marsch-Barner* Corporate Whistleblowing, ZHR 181, 847
- Martinek/Semler/Flohr* (Hrsg.) Handbuch des Vertriebsrechts, 4. Aufl. 2016
- Maschmann* (Hrsg.) Corporate Compliance und Arbeitsrecht, 2009
- Maschmann/Fritz* Matrixorganisationen, Handbuch Gesellschaftsrecht, Arbeitsrecht, Datenschutz, Compliance, 2. Aufl. 2024
- Matusche-Beckmann* Das Organisationsverschulden (Jus Privatum), 2001
- Mehrbrey/Schreibauer* Haftungsverhältnisse bei Cyber-Angriffen – Ansprüche und Haftungsrisiken von Unternehmen und Organen, MMR 2016, 75
- Meier* Nachhaltigkeit – Die drei größten Missverständnisse in Unternehmen, Wirtschaftswoche v. 1.7.2013
- Mengel* Compliance und Arbeitsrecht, 2. Aufl. 2023

- Mengel* Arbeitsrechtliche Besonderheiten der Implementierung von Compliance-Programmen in internationalen Konzernen, CCZ 2008, 85
- Menner/Bexa* Praktische Vorgehensweise bei der Einführung eines Tax Compliance Management Systems im Unternehmen, CCZ 2019, 129
- Merkt* Compliance und Risikofrüherkennung in kleinen und mittleren Unternehmen, ZIP 2014, 1705
- Merkt* Überprüfung des Compliance-Management-Systems zwischen Wirtschaftsprüfern und Juristen Teil 1, DB 2014, 2273
- Metzger/Hoppen* Zur Zulässigkeit von Nutzungsbeschränkungen in Lizenzverträgen bei Verwendung von Drittanbietersoftware, CR 2017, 625
- Metzger/Schweitzer* Shaping Markets: A Critical Evaluation of the Draft Data Act, ZEuP 2023, 42
- Meyer* Compliance-Verantwortlichkeit von Vorstandsmitgliedern – Legalitätsprinzip und Risikomanagement, DB 2014, 1063
- Miceli/Near/Dworkin,* Explaining the Whistle-Blowing Process: Suggestions from Power Theory and Justice Theory, 1993
- Miegel* Nachhaltigkeit – Der Anfang ist gemacht, Frankfurter Allgemeine Feuilleton v. 23.10.2013
- Miemczyk/Johnsen/Macquet* Sustainable purchasing and supply management: a structured literature review of definitions and measures at the dyad, chain and network levels. Supply Chain Management: An International Journal, 17(5), 478
- Minkoff/Sahan/Wittig* (Hrsg.) Konzernstrafrecht: Handbuch für die Unternehmens- und Anwaltspraxis, 2020
- Mitsch* (Hrsg.) Karlsruher Kommentar zum Gesetz über Ordnungswidrigkeiten, 5. Aufl. 2018
- Mock* Berichterstattung über Corporate Social Responsibility nach dem CSR-Richtlinie-Umsetzungsgesetz, ZIP 2017, 1195
- Moll* (Hrsg.) Münchener Anwaltshandbuch Arbeitsrecht, 5. Aufl. 2021
- Möller* Offenlegungen und Aufklärungspflichten beim Unternehmenskauf, NZG 2012, 841
- Molnár-Gábor/Kaldowski/Korbel* Verhaltenskodex für die Omics-Forschung, ZD 2021, 313
- Momsen/Grützner* (Hrsg.) Wirtschaftsstrafrecht: Handbuch für die Unternehmens- und Anwaltspraxis, 2. Aufl. 2020
- Moosmayer* Compliance-Risikoanalyse, 2. Aufl. 2020
- Moosmayer* Compliance – Praxisleitfaden für Unternehmen, 4. Aufl. 2021
- Moosmayer* Modethema oder Pflichtprogramm guter Unternehmensführung? – Zehn Thesen zu Compliance, NJW 2012, 3013
- Moosmayer/Hartwig* (Hrsg.) Interne Untersuchungen, Praxisleitfaden für Unternehmen, 2. Aufl. 2018
- Moosmayer/Lösler* Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen, 4. Aufl. 2024

- Mülbert* Soziale Verantwortung von Unternehmen im Gesellschaftsrecht, AG 2009, 766
- Müller, Elke-Luise* Künstliche Intelligenz (KI) im Arbeitsverhältnis, öAT 2024, 26
- Müller, K. J.* Reichweite der Vertretungsmacht des GmbH-Geschäftsführers bei der Veräußerung des gesamten Gesellschaftsvermögens, NZG 2019, 807
- Müller, K. J.* Gestattung der Due Diligence durch den Vorstand der Aktiengesellschaft, NJW 2000, 3452
- Müller-Glöge/Preis/
Gallner/Schmidt (Hrsg.)* Erfurter Kommentar zum Arbeitsrecht, 24. Aufl. 2024
- Müller-Ibold/Herrmann* Die Entwicklung des Europäischen Außenwirtschaftsrechts (2020–2022), EuZW 2022, 1085
- Müller-Wrede (Hrsg.)* GWB – Vergaberecht einschließlich WRegG, Kommentar, 2. Aufl. 2023
- Münchener Kommentar
zum Aktiengesetz* Herausgegeben von Goette/Habersack, Bd. 2, 6. Aufl. 2023 (zit.: MünchKomm-AktG)
- Münchener Kommentar
zum Bürgerlichen Ge-
setzbuch* Herausgegeben von Säcker/Rixecker/Oetker/Limpberger, Bd. 1: Allgemeiner Teil, 9. Aufl. 2021; Bd. 2: Schuldrecht – Allgemeiner Teil I, 9. Aufl. 2022; Bd. 3: Schuldrecht – Allgemeiner Teil II, 9. Aufl. 2022; Bd. 5: Schuldrecht – Besonderer Teil III, 9. Aufl. 2023 (zit.: MünchKomm-BGB)
- Münchener Kommentar
zum GmbHG* Herausgegeben von Fleischer/Goette, Band 2, 4. Aufl. 2023 (zit.: MünchKomm-GmbHG)
- Münchener Kommentar
zum Strafgesetzbuch* Herausgegeben von Joecks/Miebach, Bd. 5, 4. Aufl. 2020 ff. (zit.: MünchKomm-StGB)
- Münchener Kommentar
zum Wettbewerbsrecht* Herausgegeben von Säcker/Ganske/Knauff, Bd. 3 Vergaberecht I, 4. Aufl. 2022 (zit.: MünchKomm-Wettbewerbsrecht)
- Mutschler-Siebert/
Dorschfeldt* Vergaberechtliche Selbstreinigung und kartellrechtliche Compliance – zwei Seiten einer Medaille, BB 2015, 642
- Nägele/Jacobs* Rechtsfragen des Cloud Computing, ZUM 2010, 281
- Nauheim/Goette* Managerhaftung im Zusammenhang mit Unternehmenskäufem – Anmerkungen zur Business Judgement Rule aus der M&A-Praxis, DStR 2013, 2520
- Neufang* Digital Compliance – Wie digitale Technologien Compliance-Verstöße vorhersehen, IRZ 2017, 249
- Neufeld/Knitter* Mitbestimmung des Betriebsrats bei Compliance-Systemen, BB 2013, 821
- Nguyen/Romeike* Versicherungswirtschaftslehre – Grundlagen für Studium und Praxis, 2013
- Nickert/Nickert* Früherkennungssystem als Instrument zur Krisenfrüherkennung nach dem StaRUG, GmbHR, Heft 8 (April 2021), 401
- Niedernhuber* Smart Sanctions: Der Umgang mit eingefrorenen Vermögenswerten gelisteter Personen in Deutschland, GSZ-Sonderausgabe 2022, 32

- Niemann* Shift der urheberrechtlichen Verwertungsrechte in der arbeits-
teiligen digitalen Welt, CR 2009, 661
- Niestedt/Trennt* Das neue Außenwirtschaftsrecht, BB 2013, 2115
- Nietsch* Compliance-Risikomanagement als Aufgabe der Unterneh-
mensleitung, ZHR 2016, 733
- Nietsch* Geschäftsleiterermessen und Unternehmensorganisation bei der
AG, ZGR 2015, 631
- Nietsch* Nachhaltigkeitsberichterstattung im Unternehmensbereich ante
portas – der Regierungsentwurf des CSR-Richtlinie-Umset-
zungsgesetzes, NZG 2016, 1330
- Nietsch* Compliance-Risikomanagement als Aufgabe der Unterneh-
mensleitung, ZHR 180 (2016), 733
- Nietsch* Nachhaltigkeit als Aufgabe von Compliance? – Grundsatzüber-
legungen zur organisatorischen Zuweisung im Unternehmen,
CCZ 2023, 61
- Nietsch/Hastenrath* Business-Judgement bei Compliance-Entscheidungen – ein
Ausweg aus der Haftungsfalle? – Teil 1, CB 2015, 177
- Nietsch/Hastenrath* Business-Judgement bei Compliance- Entscheidungen – ein
Ausweg aus der Haftungsfalle? – Teil 2, CB 2015, 221
- Nietsch/Munerotto* Der Referentenentwurf zur Umsetzung der CSR-Richtlinie, CB
2016, 177
- Nietsch/Wiedmann* Der Regierungsentwurf eines Gesetzes über die unternehmeri-
schen Sorgfaltspflichten in der Lieferkette, CCZ 2021, 101
- Nimmer* Coexisting with Free and Open Source Software, CRi 2006, 129
- Nothelfer* Die Einführung eines Compliance Management Systems als or-
ganisatorischer Lernprozess, CCZ 2013, 23
- Nothelfer* Herausforderungen für das Compliance Management in Start-
up-Unternehmen, CCZ 2016, 64
- Oberlin* Social Media Nutzung, Marketing und die DS-GVO: Wie soll-
ten Unternehmen mit den neuen Medien und Marketingtechno-
logien umgehen? – Teil 2, CB 2019, 67
- Oberlin/Bossardt* Datenschutz-Compliance: Die Anforderungen der EU-DSGVO
und des VE-DSG der Schweiz, CB 2017, 245
- OLG München* Anwendbarkeit des § 130 OWiG auf Konzernsachverhalte, BB
2015, 2004
- Otto* Das strafrechtliche Risiko der Vertreter und Geldwäschebeauf-
tragten nach dem Geldwäschegesetz, wistra 1995, 323
- Ovie/Berger/Harnisch-
macher (Hrsg.)* Praxishandbuch Transport, Logistik – Versicherung – Zoll – Ex-
portkontrolle – Steuern – VuB, 2. Aufl. 2017
- Paall/Pauly (Hrsg.)* Datenschutz-Grundverordnung Bundesdatenschutzgesetz,
Kommentar, 3. Aufl. 2021
- Pape* Zur Wirksamkeit von Corporate Compliance, CCZ 2009, 233
- Park (Hrsg.)* Kapitalmarktraferecht, 5. Aufl. 2019
- Paschke/Graf/Olbrisch* Hamburger Handbuch des Exportrechts, 2. Aufl. 2014

Literaturverzeichnis

- Passarge* Erfolgreiche Struktur von Hinweisgebersystemen – Praktische Aspekte und das Zusammenspiel mit anderen Gesetzen, CB 2021, 453
- Passarge* Praxiseignung und offene rechtliche Fragen beim LkSG, CB 2023, 171
- Passas/Holtz* Die Gestaltung von LkSG-Compliance-Klauseln in Lieferbeziehungen, BB 2023, 387
- Patzina/Bank/Schimmer/Simon-Widmann* Haftung von Unternehmensorganen, 2010
- Pelz* Aktuelle Rechtsprobleme des § 4 Abs. 5 S. 1 Nr. 10 EStG und seine Folgen, DStR 2014, 449
- Pelz/Hofschneider* Die Selbstanzeige im neuen Außenwirtschaftsrecht, AW-Prax 2013, 173
- Pelz/Hofschneider* Die Selbstanzeige im neuen Außenwirtschaftsrecht – Chance oder Risiko?, wistra 2014, 1
- Pelz/Krais* Lieferketten in der Unternehmenspraxis, Lieferkettensorgfaltspflichtengesetz – Best Practice, 2022
- Peters/Pflaum* Steuerhinterziehung durch unangemessene Verrechnungspreise?, wistra 2011, 250
- Petrushevskaja* Corporate challenges and interventions in practicing compliance and integrity – results from a survey with compliance and integrity experts, CCZ 2023, 241
- Pfeil/Mertgen* (Hrsg.) Compliance im Außenwirtschaftsrecht, 2. Aufl. 2023
- Plath/Struck/ter Haebe* Verkauf von Kundendaten im Asset Deal, CR 2020, 9
- Podszun/Pfeifer* Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission, GRUR 2022, 953
- Pohl* Umweltaudits in der betrieblichen Praxis, BB 1998, 381
- Pohle/Ammann* Über den Wolken ... – Chancen und Risiken des Cloud Computing, CR 2009, 273
- Polley/Seeliger* Anwendung der neuen Gruppenfreistellungsverordnung für Vertikalverträge Nr. 2790/1999 auf Softwareverträge, CR 2001, 1
- Pörnbacher/Mark* Auswirkungen des UK Bribery Act 2010 auf deutsche Unternehmen, NZG 2010, 1375
- Porter/Kramer* Creating Shared Value, Harvard Business Review, Vol. 89, Nr. 1/2, 2
- Porter/Kramer* Strategy and Society: “The Link Between Competitive Advantage and Corporate Social Responsibility”, Harvard Business Review, December 2006, 78
- Powilleit* Compliance im Unternehmen: Rechtliches Risikomanagement als Wertschöpfungsfaktor, GWR 2010, 28
- Preusche/Würz* Compliance, 3. Aufl. 2019

- Preußner* Risikomanagement und Compliance in der aktienrechtlichen Verantwortung des Aufsichtsrats unter Berücksichtigung des Gesetzes zur Modernisierung des Bilanzrechts (BilMoG), NZG 2008, 574
- Prieß/Arend* Absolvo vos, AW-Prax 2013, 71
- Prieß/Stein* Nicht nur sauber, sondern rein: Die Wiederherstellung der Zuverlässigkeit durch Selbstreinigung, NZBau 2008, 230
- Prieß/Thoms* Der Ausführungsverantwortliche im Großunternehmen, AW-Prax 2013, 110
- Prinz/Peters/Perten* Medienrecht, Die zivilrechtlichen Ansprüche, 2. Aufl. 2020
- Pull* Tax Compliance Management Systeme in der Praxis, DStR 2022, 2132
- Pünder/Schellenberg*
(Hrsg.) Vergaberecht, GWB – VgV – VSVgV – SektVO – VOL/A – VOB/A – VOF – Haushaltsrecht – Öffentliches Preisrecht, Handkommentar, 3. Aufl. 2019
- Rack* Lieferketten-Compliance im Digitalen Zwilling – Zum zivilrechtlichen Haftungsrisiko von Vorständen und Geschäftsführern, CB 2022, Heft 6, Sonderbeilage 1, 1
- Rack* Mehr Rechtssicherheit für Vorstände durch die neue DIN ISO 37301, CB 2021, 433
- Rack* Das Risiko der Expertenhaftung beim Zertifizieren von Compliance-Management-Systemen – Teil 1, CB 2016, 284
- Rack* Die häufigsten Fehler der Unternehmensorganisation – Das Unterlassen organisatorischer Maßnahmen, CB 2014, 104
- Rack* Die rechtlichen Voraussetzungen für ein Compliance-Management-System, CB 2014, 279
- Rack* Die Einhaltung von Rechtspflichten im Unternehmen und ihre Aktualisierung als Organisationsproblem, CB 2013, 14
- Rack* Informationsmanagement als Organisationspflicht, CB 2013, 58
- Raith* Mythos CSR: Zur Verwertung von Verantwortung und Beratung, 2013
- Ransiek* Zur Frage der Ernsthaftigkeit solcher Erklärungen, StV2009, 321
- Rat für Nachhaltige Entwicklung* Der Deutsche Nachhaltigkeitskodex, Texte Nr. 47, 2015
- Rath/Ekardt/Schiela* Cybersicherheit in der Energiewende und das deutsche Recht, MMR 2023, 176
- Rauer/Ettig* Rechtskonformer Einsatz von Cookies, ZD 2015, 255
- Raum* Paradigmenwechsel bei Geldbußen gegen Unternehmen – Betrachtungen zur 10. GWB-Novelle und zum Verbandssanktionengesetz, CCZ 2020, 245
- Raus/Lützelner* Berufspflicht des Compliance Officers – zwischen interner Eskalation und externer Anzeige, CCZ 2012, 96

Literaturverzeichnis

- Redeker* „Indirekte Nutzer“ in Softwarenutzungsbedingungen, ITRB 2017, 44
- Rehbahn* Zur Methodenlehre des Unionsrechts – insbesondere im Privatrecht, ZfPW 2016, 281
- Reich* Superkapitalismus. Wie die Wirtschaft unsere Demokratie untergräbt, 2008
- Reichling* Selbstanzeige und Verbandsgeldbuße im Steuerstrafrecht, NJW 2013, 2233
- Reimer/Brack/Schmidt* Kartellschadenprävention als Bestandteil der kartellrechtlichen Compliance, CCZ 2016, 83
- Reimers/Brack/Modest* Kartellrechtliche Compliance in Zeiten der Digitalisierung, NZKart 2018, 453
- Reimers/Hainz* Kartellschadenprävention als Bestandteil der kartellrechtlichen Compliance, CCZ 2016, 188
- Reinhard* Mitbestimmungsrechte des Betriebsrats bei der Implementierung von Unternehmens-, insbesondere Verhaltensrichtlinien, NZA 2016, 1233
- Reinhard/Pohl/Capellaro* IT-Sicherheit und Recht, 2007
- Reischauer/Kleinhans* KWG, EL (09/19), 2020
- Renz* Organisationsmodelle zu Compliance & Datenschutz, BvD-News 2/2014, 26
- Renz/Frankenberger* Aufgaben einer Compliance-Organisation im Rahmen des Internen Kontrollsystems (IKS), CB 2015, 420
- Renz/Frankenberger* Compliance und Datenschutz, ZD 2015, 158
- Renz/Hense/Marbeiter (Hrsg.)* Wertpapier-Compliance in der Praxis, 2. Aufl. 2019
- Renz/Rohde-Liebenau* Die Hinweisgeber-Regelung des § 25a KWG, BB 2014, 692
- Renz/Spallek* Einsatz von ISO-Standards bei Einhaltung von Sorgfaltspflichten nach dem LkSG, Comply 202, 26
- Reuter* Das Hinweisgeberschutzgesetz ist da – Was Unternehmen jetzt tun müssen, BB 2023, 1539
- Reuter* OLG Nürnberg 30.3.2022 – 12 U 1520/19: Organisationspflichten und Geschäftsleiterhaftung am Beispiel des Vier-Augen-Prinzips und anderer Compliance Management-Vorgaben, NZG 2023, 322
- Richardi (Hrsg.)* BetrVG mit Wahlordnung, 17. Aufl. 2022
- Richter* Vereinbarkeit des Entwurfs zum Data Act und der DS-GVO, MMR 2023, 163
- Rieder/Falge* Sieben Thesen zur standardisierten Prüfung von Compliance-Management-Systemen, BB 2013, 778
- Rimmelspacher/Schäfer/Schönberger* Das CSR-Richtlinie-Umsetzungsgesetz: Neue Anforderungen an die nicht finanzielle Berichterstattung und darüber hinaus, KoR 2017, 225

- Ritzenhoff/Sonnenberg/Schulz* Kommunikation als Schlüssel zu erfolgreichem Compliance-Management – Sieben Thesen, CB 2019, 1
- Rivas/Van De Walle De Ghelcke* Concerted practices and Exchange of information: An overview of EU and national case law, e-Competitions, N°43913
- Rodewald* Zwischen Perfektionismus und Pragmatismus – wie viel Anti-Korruptions-Management kann, darf und muss sein?, CB 2013, 70
- Rodewald/Unger* Corporate Compliance – Organisatorische Vorkehrungen zur Vermeidung von Haftungsfällen der Geschäftsleitung, BB 2006, 113
- Rodewald/Unger* Kommunikation und Krisenmanagement im Gefüge der Corporate Compliance-Organisation, BB 2007, 1629
- Roeder/Schlutz/Hille/Havlik/Conte* Compliance (Due Diligence) im Kontext von Transaktionen – Außenwirtschaftsrecht, CCZ 2023, 337, 338
- Roeder/Werthmüller/Havlik* Compliance (Due Diligence) im Kontext von Transaktionen – Die ESG Due Diligence, CCZ 2024, 13
- Rogall* Karlsruher Kommentar zum OWiG, 5. Aufl. 2018
- Röh* Compliance nach der MiFID – zwischen höherer Effizienz und mehr Bürokratie, BB 2008, 398
- Röhrich (Hrsg.)* Methoden der Korruptionsbekämpfung: Risiken erkennen – Schäden vermeiden, 2008
- Rolfs/Giesen/Meißling/Udsching (Hrsg.)* BeckOK Arbeitsrecht, BetrVG, 71. Edition, Stand: 1.3.2024
- Rolletschke* Auswirkungen der elektronischen Datenübermittlung (§ 93c AO) auf die Strafbarkeit nach § 370 Abs. 1 Nr. 2 AO, NZWiSt 2018, 185
- Romeike* Risikomanagement, 2018
- Romeike* Beautiful, Colourful Risk: Benoît B. Mandelbrot – Remembering the Father of Fractals, in: Union Investment Institutional (Hrsg.), The Measurement of Risk, 2015, S. 197
- Romeike* Toolbox – Reifegrade definieren Methoden, GRC aktuell 01/2018, 41
- Romeike* Risikomanagement, 2018
- Romeike* Bow-Tie-Analyse, GRC aktuell 01/2019, 39
- Romeike/Hager* Erfolgsfaktor Risiko-Management 3.0: Methoden, Beispiele, Checklisten Praxishandbuch für Industrie und Handel, 3. Aufl. 2013
- Romeike/Hager* Erfolgsfaktor Risikomanagement 4.0: Methoden, Beispiele, Checklisten – Praxishandbuch für Industrie und Handel, 4. Aufl. 2020
- Romeike/Müller-Reichart* Risikomanagement in Versicherungsunternehmen, 2020
- Romeike/Stallinger* Bandbreiten- bzw. Korridorplanung – Integration von Risikomanagement und Unternehmensplanung, Risk, Compliance & Audit (RC&A), 06/2012, 12

- Romeike/Stallinger* Schwarze Schwäne im Risikomanagement – Zum Umgang mit seltenen Ereignissen, Risiko Manager, 06/2014, 1
- Rörmann* Münchener Anwaltshandbuch GmbH-Recht, 4. Aufl. 2018
- Rönnau* Haftung für unterlassene Aufsicht nach § 130 OWiG und strafrechtlicher (Drittempfänger-)Verfall gemäß § 73 Abs. 3 StGB – zwei bedeutsame Bedrohungsszenarien für Unternehmen, ZGR 2016, 277
- Roos* MonIKA: IT-Sicherheit durch kooperative Ansätze, 2015
- Rosbach* Ethik in einem Wirtschaftsunternehmen – nützlich oder überflüssige Förmerei?, CCZ 2008, 101
- Rosling/Rosling* Factfulness, 2018
- Rönnlund/Rosling*
- Rost/Wigger* Compliance-Lernkurve? Datenschutz-Bußgeldverfahren aus behördlicher Sicht, CB 2023, 333
- Roth* Elektronische Daten im Finanzamt: § 150 Abs. 7 Satz 2 AO n. F. als Totengräber der Steuerhinterziehung?, wistra 2018, 152
- Roth* Aufsichtsrat und interne Kontrolle nach dem Finanzmarktintegritätsstärkungsgesetz (FISG), NZG 2022, 53
- Rothe/Schlombs* Übles von jemandem denken, ZRFC 2018, 266
- Rothermel* Lieferkettensorgfaltspflichtengesetz, Kommentar, 2022
- Rotsch* Wissenschaftliche und praktische Aspekte der nationalen und internationalen Compliance-Diskussion, 2013
- Rotsch (Hrsg.)* Criminal Compliance, Handbuch, 2015
- Rowedder/Schmidt-Leithoff (Hrsg.)* GmbHG, 6. Aufl. 2017
- Röwekamp/Kus/Portz/Prieß (Hrsg.)* Kommentar zum GWB-Vergaberecht, 5. Aufl. 2020
- Roxin* Täterschaft und Tatherrschaft, 11. Aufl. 2022
- Rübenstahl* Der Foreign Corrupt Practices Act (FCPA) der USA, NZWiSt 2012, 401
- Rübenstahl/Hahn/Voet van Vormizeele (Hrsg.)* Kartell Compliance – Prävention – Investigation – Corporate Defense – Remediation, 2020
- Rudkowski/Manzanza Lumingu* Zur eingeschränkten Effektivität des LkSG am Beispiel der Demokratischen Republik Kongo, RdA 2023, 291
- Ruggie* Protect, respect and remedy: A framework for business and human rights. Innovations: Technology, Governance, Globalization, 3(2), 2008, 189
- Ruhmannseder/Behr/Krakow (Hrsg.)* Hinweisgebersysteme – Implementierung in Deutschland, Österreich und der Schweiz, 2. Aufl. 2021
- Ruttloff/Wagner/Hahn/Freihoff* Der Menschenrechtsbeauftragte, CCZ 2022, 20
- Sachs/Krebs* Anforderungen an ein außenwirtschaftsrechtliches Compliance-Programm und seine Ausgestaltung in der Praxis, CCZ 2013, 60

- Sachs/Krebs* Quid pro Quo im Außenhandel: Compliance gegen Verfahrensprivilegien, CCZ 2013, 12
- Sachs/Pelz* Außenwirtschaftsrecht, 3. Aufl. 2024
- Saenger* Gesellschaftsrecht, 6. Aufl. 2023
- Sahut/Peris-Ortiz/Teulon* Coprorate social responsibility and governance, Journal of Management and Governance 23/2019, 901
- Saliger/Gaede* Rückwirkende Ächtung der Auslandskorruption und Untreue als Korruptionsdelikt – Der Fall Siemens als Startschuss in ein entgrenztes internationalisiertes Wirtschaftsstrafrecht?, HRRS 2008, 57
- Saller* Vorgehensweise des Bundeskartellamtes bei der Sicherstellung von IT-Asservaten im Rahmen einer Unternehmensdurchsuchung im Kartellordnungswidrigkeitenverfahren, CCZ 2012, 189
- Salvenmoser/Hauschka* Korruption, Datenschutz und Compliance, NJW 2010, 331
- Sandmann* Die Compliance-Funktion unter Solvency II – Ein Überblick, CCZ 2015, 74
- Sassenberger/Faber* (Hrsg.) Rechtshandbuch Industrie 4.0 und Internet of Things, 2. Aufl. 2020
- Sattler* Einführung in das Sanktionsrecht, JuS 2019, 18
- Schäfer* Die MaComp und das Erfordernis der Unabhängigkeit, Wirksamkeit, Dauerhaftigkeit von Compliance, BKR 2011, 45
- Schäfer* Die MaComp und die Aufgaben von Compliance, BKR 2011, 187
- Schäfer/Schütze* Die CSDDD – eine Verantwortlichkeit und Haftung in Lieferantenketten für die deutsche Wirtschaft, BB 2024, 1091
- Schäfer/Sethe/Lang* Handbuch der Vermögensverwaltung, 3. Aufl. 2022
- Schalast/Raettig* (Hrsg.) Grundlagen des M&A-Geschäftes: Strategie, Recht, Steuern, 2. Aufl. 2019
- Schall/Theusinger/Pour Rafsendjani* (Hrsg.) Lieferkettensorgfaltspflichtengesetz, 2023
- Schau/Idler* Praxiserfahrungen im Zusammenhang mit § 4 Abs. 5 Satz 1 Nr. 10 EStG, Ubg 2010, 111
- Schau/Schwartz* Tax-Compliance im Unternehmen aus steuerstrafrechtlicher Sicht – insbesondere: Risikoverteilung in der Organshaft, ZWH 2013, 212
- Schau/Schwartz* Noch Berichtigung oder schon Selbstanzeige? Der neue Anwendungserlass zu § 153 AO in der Diskussion, PStR 2015, 248
- Schaupensteiner* Rechtstreue im Unternehmen – Compliance und Krisenmanagement, NZA-Beil. 2011, 8
- Schefold* 10 Jahre IDW PS 980, ZRfC 2022, 170
- Schein* Organisationskultur, 2003
- Scherer-Leydecker* Das Wettbewerbsregister: Die bundesweite schwarze Liste für die Vergabe öffentlicher Aufträge, CB 2017, 261

Literaturverzeichnis

- Schettgen-Sarcher/Bachmann/Schettgen* Compliance Officer, Das Augsburger Qualifizierungsmodell, 2014
- Schewe* Unternehmensverfassung: Corporate Governance im Spannungsfeld von Leitung, Kontrolle und Interessensvertretung, 4. Aufl. 2018
- Schiffer/Bruß* Due Diligence beim Unternehmenskauf und vertragliche Vertraulichkeitsvereinbarungen, BB 2012, 847
- Schimansky/Bunte/Lwowski* (Hrsg.) Bankrechts-Handbuch, 5. Aufl. 2017
- Schläpke/Lühmann* Kollektiver Rechtsschutz nach der Umsetzung der EU-Verbandsklagen-RL, NJW 2023, 3385
- Schleper/Blome/Steven-son/Thürer/Tusell* When it's the slaves that pay: In search of a fair due diligence cost distribution in conflict mineral supply chains. Transportation Research Part E: Logistics and Transportation Review 164, 2022, 102801
- Schleper/Blome/Wuttke* The dark side of buyer power: Supplier exploitation and the role of ethical climates. Journal of Business Ethics, 140(1), 2017, 97
- Schleper/Busse* Towards a standardized supplier code of ethics: development of a design concept based on diffusion of innovation theory. Logistics Research, 6(4), 2013, 187
- Schmidt* Compliance in Kapitalgesellschaften, 2010
- Schmidt* Compliance-Funktion nach MaRisk, 2015
- Schmidt/Lutter* (Hrsg.) Aktiengesetz, Kommentar, 4. Aufl. 2020
- Schmidt/Schaltenbrand/Foerstl* The supply chain position paradox: green practices and firm performance. Journal of Supply Chain Management, 53(1), 2017, 3
- Schmidt/Wermelt/Eibelshäuser* ISO 19600 aus der Sicht der Wirtschaftsprüfung, CCZ 2015, 18
- Schmidt-Versteyl* Cyber-Risks – neuer Brennpunkt Managerhaftung?, NJW 2019, 1637
- Schmitz* Smarte Bekämpfung der Pandemie ist datenschutzrechtlich erlaubt, ZD-Aktuell 2020, 04404
- Schmolke* Die neue Whistleblower-Richtlinie ist da! Und nun?, NZG, 2020, 5
- Schmucker* Strafrechtliche Verantwortlichkeit der Unternehmensleitung durch innerbetriebliche Anweisungen, StraFo 2010, 235
- Schneider* Indirekte Softwarenutzung – ein Vertragsrisiko für beide Seiten, ITRB 2017, 286
- Schneider* Compliance als Aufgabe der Unternehmensleistung, ZIP 2003, 645
- Schneider* Die Überlagerung des Konzernrechts durch öffentlich-rechtliche Strukturnormen und Organisationspflichten, ZGR 1996, 225
- Schneider/Conrady/Kapoor* Die Abhilfeklage – Eine ernstzunehmende Konkurrenz für die Abtretungsmodelle?, BB 2023, 2179

- Schneider/Schmidpeter* (Hrsg.) Corporate Social Responsibility: Verantwortungsvolle Unternehmensführung in Theorie und Praxis, 2. Aufl. 2015
- Schnichels/Resch* Das Anwaltsprivileg im europäischen Kontext, EuZW 2011, 47
- Schnitzler* Wettbewerbsrechtliche Compliance – vergaberechtliche Selbstreinigung als Gegenmaßnahme zum Kartellverstoß, BB 2016, 2115
- Schockenhoff* Compliance im Verein, NZG 2019, 281
- Schockenhoff* Haftung und Enthftung von Geschäftsleitern bei Compliance-Verstößen in Konzernen mit Matrix-Strukturen, ZHR 2016, 197
- Scholz* (Hrsg.) Kommentar zum GmbHG mit Anhang Konzernrecht, II. Band, 12. Aufl. 2018/2019
- Schönke/Schröder/Heine/Eisele* (Hrsg.) Strafgesetzbuch: StGB, 30. Aufl. 2019
- Schreiber* Implementierung von Compliance-Richtlinien, NZA-RR 2010, 617
- Schrey/Krupna* Softwarelizenzmanagement – Ein unterschätztes Compliance-Risiko, CCZ 2012, 141
- Schröder* Anforderungen an einen Compliance-/CSR-Prozess im Lieferantenmanagement (Compliance-Risiko: Korruption), CCZ 2013, 74
- Schröder* Die Entwicklung von Compliance-Management-Systemen hinsichtlich Kartellrechtscompliance, CCZ 2015, 63
- Schröder* Der Ausschluss von öffentlichen Aufträgen als Sanktion des neuen LkSG, CB 2023, 15
- Schröder/Schulz* Praxisleitfaden Supply Chain Compliance, 2023
- Schroeder* Darf der Vorstand der Aktiengesellschaft dem Aktienkäufer eine Due Diligence gestatten?, DB 1997, 2161
- Schröter/Klotz/von Wendland* (Hrsg.) Europäisches Wettbewerbsrecht, Kommentar, 3. Aufl. 2024
- Schulte* Handbuch Fusionskontrolle, 3. Aufl. 2020
- Schultze* (Hrsg.) Compliance Handbuch Kartellrecht, 2. Aufl. 2021
- Schultze/Pautke/Wagener* Die Gruppenfreistellungsverordnung für Technologietransfer-Vereinbarungen, Praxiskommentar, 2005
- Schultze/Pautke/Wagener* Vertikal-GVO, Praxiskommentar, 3. Aufl. 2011
- Schultze/Pautke/Wagener* Vertikal-GVO 2022: Erste Erfahrungen – Bewertung aus Praktikersicht – Teil 1, WuW 2023, 646
- Schultze/Pautke/Wagener* Vertikal-GVO 2022: Erste Erfahrungen – Bewertung aus Praktikersicht – Teil 2, WuW 2024, 70
- Schulz, Martin* Compliance-Management im Mittelstand, CB 2015, 309
- Schulz, Martin* Compliance-Management im Unternehmen – Compliance-Strategie als (Dauer-)Aufgabe der Unternehmensleitung, BB 2019, 579

Literaturverzeichnis

- Schulz, Martin* Compliance-Management im Unternehmen – Grundfragen, Herausforderungen und Orientierungshilfen, BB 2017, 1475
- Schulz, Martin* Risikomanagement durch Compliance Audits – Neue Herausforderungen für die Unternehmensorganisation, BB 2011, 1347
- Schulz, Martin/Block* Wirksames Compliance-Management – Anreize und Orientierungshilfen zur Vermeidung von (Verbands-)Sanktionen, CCZ 2020, 49
- Schulz, Martin/Block* Wirksames Compliance-Management – Anreize und Orientierungshilfen zur Vermeidung von (Verbands-)Sanktionen, CCZ 2020, 49
- Schulz, Martin/Hartung (Hrsg.)* Recht 2030 – Legal Management in der digitalen Transformation, 2019
- Schulz, Martin/Held* Sicherstellung funktionierender Compliance als Organisationspflicht des Vorstands, juris Praxis Report Compliance 1/2014
- Schulz, Martin/Muth* Erfolgsfaktor Compliance-Kultur – Grundlagen und Hinweise zur Gestaltung durch die Unternehmensleitung, CB 2014, 265
- Schulz, Martin/Renz* Der erfolgreiche Compliance-Beauftragte – Leitlinien eines branchenübergreifenden Berufsbildes, BB 2012, 2511
- Schulz, Martin/Renz* Zum Berufsbild des Compliance Officers – Entwicklung branchenübergreifender Mindestanforderungen, CB 2013, 294
- Schulz, Mike* Compliance – Internes Whistleblowing, BB 2011, 629
- Schürrie* Compliance-Verantwortung in der AG – Praktische Empfehlungen zur Haftungsbegrenzung an Vorstände und Aufsichtsräte, CCZ 2010, 102
- Schürrie/Fleck* Whistleblowing Unlimited – Der U.S. Dodd-Frank Act und die neuen Regeln der SEC zum Whistleblowing, CCZ 2011, 218
- Schürrie/Olbers* Compliance-Verantwortung in der AG – Praktische Empfehlungen zur Haftungsbegrenzung an Vorstände und Aufsichtsräte, CCZ 2010, 102
- Schuster/Darsow* Einführung von Ethikrichtlinien durch Direktionsrecht, NZA 2005, 273
- Schuster/Reichl* Cloud Computing & SaaS: Was sind die wirklich neuen Fragen?, CR 2010, 38
- Schütz/Beckmann/Röbken* Compliance-Kontrolle in Organisationen: Soziologische, juristische und ökonomische Aspekte, 2018
- Schwark/Zimmer (Hrsg.)* Kapitalmarktsrechts-Kommentar, 5. Aufl. 2020
- Schwartzmann/Jaspers/Thüsing/Kugelman (Hrsg.)* DS-GVO/BDSG, 2. Aufl. 2020
- Schwartz* Keine leichtfertige Steuerverkürzung nach Einholung eines Rechtsgutachtens, PStR 2014, 156
- Schwartz* Praxisfragen zur neuen Selbstanzeigeregelung zum 1. Januar 2015, PStR 2015, 37
- Schwartz/Carroll* Corporate Social Responsibility: A Three-Domain Approach, Business Ethics Quarterly, Volume 13, Issue 4/2003, 503

- Schwartz/Höpfner* AEAO zu § 153 AO neu geregelt, PStR 2016, 2
- Schwarz* Im Fadenkreuz der Regulatoren – worauf strategische und Private-Equity-Investoren bei M&A-Transaktionen achten müssen, BB 2012, 136
Schwarze Soft Law im Recht der Europäischen Union, EuR 2011, 3
- Schweitzer/Metzger* Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?, GRUR-Int. 2023, 337
- Schwendinger/Rehle* Die EU-Blocking-Verordnung zur Abwehr extraterritorialer US-Sanktionen; RdTW 2022, 382
- Schwennicke/Auerbach* Kreditwesengesetz, Kommentar, 4. Aufl. 2021 (Hrsg.)
- Seeliger/Gänswein* E-Raids – IT-Durchsuchungen von Unternehmen durch die Europäische Kommission und das Bundeskartellamt, BB 2014, 1027
- Seeliger/Gürer* ESG und Kartellrecht – neue Chancen für Unternehmen, DB-Beilage 2023, 58
- Seeliger/Mross* Aktuelle Entwicklung in der kartellrechtlichen Compliance, CB 2017, 304
- Seer* Ein zaghafter Schritt zur kooperativen Außenprüfung – Inhalt und Bewertung des Art. 97 § 38 EGAO, IWB 2023, 950
- Seibt* Corporate Reputation Management: Rechtsrahmen für Geschäftsleiterhandeln, DB 2015, 171
- Seibt (Hrsg.)* Beck'sches Formularbuch Mergers & Acquisitions, 3. Aufl. 2018
- Seibt/Vesper-Gräse* Lieferkettensorgfaltspflichtengesetz erweitert Compliance-Pflichten, CB 2021, 357
- Seidel* Datenbanken und Persönlichkeitsrecht, unter besonderer Berücksichtigung der amerikanischen Computer Privacy, 1972
- Semler/v. Schenck/Wilsing* Arbeitshandbuch für Aufsichtsratsmitglieder, 5. Aufl. 2021
- Sester* Open-Source-Software: Vertragsrecht, Haftungsrisiken und IPR-Fragen, CR 2000, 797
- Seuring/Müller* From a literature review to a conceptual framework for sustainable supply chain management. Journal of Cleaner Production, 16(15), 2008, 1699
- Siadat* Markets in Crypto Assets Regulation – erster Einblick mit Schwerpunktsetzung auf Finanzinstrumente, RdF 2021, 12
- Siedenbiedel* Corporate Compliance, 2014
- Siepelt/Pütz* Die Compliance-Verantwortung des Aufsichtsrats, CCZ 2018, 78
- Simitis (Hrsg.)* Bundesdatenschutzgesetz, 8. Aufl. 2014
- Simitis/Hornung/Spiecker gen. Döhmann* Datenschutzrecht – DSGVO mit BDSG, Kommentar, 2019

- Simons* Corporate Social Responsibility und globales Wirtschaftsrecht, Zeitschrift für Unternehmens- und Gesellschaftsrecht 2–3/2018, 316
- Smith* (Hrsg.) The Wealth of Nations, 2010
- Spatscheck/Binnewies/Rakete-Dombek* (Hrsg.) Festschrift für Michael Streck, 2011
- Specht-Riemenschneider* Data Act – Auf dem (Holz-)Weg zu mehr Dateninnovation?, ZRP 2022, 137
- Spehl/Grützner* Resource Guide to the U.S. States Foreign Corrupt Practices Act (FCPA-Guide) – Eine Hilfe für Unternehmen im Umgang mit dem FCPA, CCZ 2013, 198
- Spießhofer* Die neue europäische Richtlinie über die Offenlegung nichtfinanzieller Informationen, NZG 2014, 1281
- Spießhofer* Unternehmerische Verantwortung, 2017
- Spießhofer* Unternehmerische Verantwortung: Zur Entstehung einer globalen Wirtschaftsordnung, 2017
- Spießhofer/Späth* (Hrsg.) Lieferkettensorgfaltspflichtengesetz – unter Berücksichtigung AGB-rechtlicher Besonderheiten, Kommentar, 2024
- Spindler* Compliance in der multinationalen Bankengruppe, WM 2008, 905
- Spindler* Unternehmensorganisationspflichten – Zivilrechtliche und öffentlich-rechtliche Regelungskonzepte, 2001
- Spindler* Handbuch des Vorstandsrechts, 2006
- Spindler* Haftung der Geschäftsführung für IT-Sachverhalte, CR 2017, 715
- Spindler* Verantwortlichkeit und Haftung in Lieferantenketten – das Lieferkettensorgfaltspflichtengesetz aus nationaler und europäischer Perspektive, ZHR 186 (2022), 67
- Spindler/Bille* Rechtsprobleme von Bitcoins als virtuelle Währung, WM 2014, 1357
- Spindler/Schuster* (Hrsg.) Recht der elektronischen Medien, Kommentar, 4. Aufl. 2019
- Spindler/Stilz* (Hrsg.) Kommentar zum Aktiengesetz, 5. Aufl. 2022
- Splittergerber/Rockstroh* Sicher durch die Cloud navigieren – Vertragsgestaltung beim Cloud Computing, BB 2011, 2179
- Sradj* Versicherung von Steuerrisiken, DStR 2022, 568
- Stanitzek* Die Bedeutung von Criminal Compliance für das Strafrecht bei der Bekämpfung von Wirtschaftskorruption, 2013
- Staub* Überlegungen zur Erfassung und Steuerung rechtlicher Risiken im Unternehmen (aus Schweizer Sicht), CCZ 2009, 121
- Stawinoga/Velte* Der Referentenentwurf für ein CSR-Richtlinie-Umsetzungsgesetz, DB 2016, 841
- Steger* Verstoß gegen das Vollzugsverbot der Fusionskontrolle – erhebliches Risiko bei M&A-Transaktionen, DB 2014, 1857

- Stein/Thoms* (Hrsg.) Außenwirtschaftsgesetz, 2. Aufl. 2023
- Steinle/Fuhrer* Details. Kartellrecht im Personalbereich: Das immer noch unterschätzte Risiko, CB 2023, 201
- Steinrötter* Verhältnis von Data Act und DS-GVO, GRUR 2023, 216
- Stemberg* Die drei „Schlüsselkriterien“ des Beschwerdeverfahrens nach § 8 Lieferkettensorgfaltspflichtengesetz, CCZ 2022, 92
- Stober* Compliance in der öffentlichen Verwaltung – Eine Anforderung zwischen moderner Governance und klassischem Verwaltungsethos, DVBl 2012, 391
- Stork* Step-by-step: Die Einführung von Richtlinien im Unternehmen, CB 2013, 89
- Story* Lead paint prompts Mattel to recall 967,000 toys. New York Times (2.8.2007), http://www.nytimes.com/2007/08/02/business/02toy.html?_r=0 (zuletzt abgerufen am 22.2.2024).
- Strauss* Konzeption eines Hinweisgebersystems, ZRFC 2014, 164
- Streck/Binnewies* Tax Compliance, DStR 2009, 229
- Streck/Mack/Schwedhelm* (Hrsg.) Tax Compliance, Risikominimierung durch Pflichtenbefolgung und Rechteverfolgung, 3. Aufl. 2019
- Strittmatter/Harnos* Softwareaudits, CR 2013, 621
- Stürzl/Forster* Die neue Berichtigungspflicht der Steuerpflichtigen nach einer Außenprüfung, GmbH-Steuerpraxis 1/2024, 8
- Summa* Die Entscheidung über die Auftragsvergabe – Ein Ausblick auf das künftige Unionsrecht, NZBau 2012, 729
- Sydow* (Hrsg.) Europäische Datenschutzgrundverordnung, 2. Aufl. 2018
- Szesny* Im Blickpunkt: Internal Investigations Zulässigkeit und Grenzen unternehmensinterner Ermittlungen, BB 45/2011, VI/VII
- Szesny/Kuthe* (Hrsg.) Kapitalmarkt Compliance, 2. Aufl. 2018
- Taeger/Gabel* (Hrsg.) DSGVO – BDSG – TTDSG, 4. Aufl. 2022
- Taeger/Pohle* (Hrsg.) Computerrechts-Handbuch – Informationstechnologie in der Rechts- und Wirtschaftspraxis, 38. Aufl. 2023
- Tamcke/Dembinski* Vorvertragliche Aufklärungspflichten bei Verwendung eines virtuellen Datenraums – Zugleich Anmerkung zu BGH Urt. v. 15.9.2023 – V ZR 77/22, GWR 2023, 338
- Teichmann* (Hrsg.) Compliance, 2014
- Teicke* Gute Unternehmenspraxis für Internal Investigations – Praxistipps zur erfolgreichen Umsetzung unter Berücksichtigung des VerSanG-E, CCZ 2019, 298
- Teicke* CSR meets Compliance – Über die zunehmende Verrechtlichung der Corporate Social Responsibility, CCZ 2018, 274
- Teicke/Mohsseni* Facilitation Payments – Haftungsrisiken für Unternehmen nach deutschem Recht, FCPA und UK Bribery Act, BB 2012, 911
- Thommen/Achleitner/Gilbert/Hachmeister/Jarchow/Kaiser* Allgemeine Betriebswirtschaftslehre, 9. Aufl. 2020

<i>Thüsing</i>	Schwerpunkte HR – Compliance und Datenschutz, CB 10/2015
<i>Thüsing</i>	Datenschutz im Arbeitsverhältnis, NZA 2009, 865
<i>Thüsing</i> (Hrsg.)	Hinweisgeberschutzgesetz, Kommentar, 2024
<i>Thüsing</i> (Hrsg.)	Beschäftigtendatenschutz und Compliance, 3. Aufl. 2021
<i>Thüsing/Rombey</i>	Nachdenken über den Richtlinienvorschlag der EU-Kommission zum Schutz von Whistleblowern, NZG 2018, 1001
<i>Tieben</i>	Das Drei-Säulen-System des Bankenmarktes als regulierungsrechtliche Steuerungsressource, 2012
<i>Timmerbeil/Blome</i>	Steter Tropfen höhlt den Stein – Die „wirtschaftliche Einheit“ im deutschen Kartellrecht nach der 9. GWB-Novelle, BB 2017, 1544
<i>Timmerbeil/Spachmüller</i>	UK Bribery Act – Das Damoklesschwert über deutschen Unternehmen?, DB 2013, 2133
<i>Tipke/Kruse</i>	Abgabenordnung/Finanzgerichtsordnung, Stand: 178. EL, 2023
<i>Tribess/Spitz</i>	Datenschutz im M&A Prozess, GWR 2019, 261
<i>Trittin/Fischer</i>	Datenschutz und Mitbestimmung, NZA 2009, 343
<i>Trüg/Ruppert</i>	Die Bedeutung von Compliance-Management-Systemen für die Kartell- und sonstige Verbandsgeldbuße – zugleich ein Plädoyer für eine rationale Unternehmenssanktion, ZWeR 2020, 69
<i>Ulber</i>	Whistleblowing und der EGMR, NZA 2011, 962
<i>Umnuß</i> (Hrsg.)	Corporate Compliance Checklisten, 5. Aufl. 2022
<i>Union Investment Institutional</i> (Hrsg.)	The Measurement of Risk, 2015
<i>van Vormizeele</i>	Kartellrechtliche Compliance-Programme im Rahmen der Bußgeldbemessung de lege lata und de lege ferenda, CCZ 2009, 41
<i>Velte</i>	Prüfung der nichtfinanziellen Erklärung nach dem CSR-Richtlinie-Umsetzungsgesetz, IRZ 2017, 325
<i>Velte</i>	Prüfung der nichtfinanziellen Erklärung und der Erklärung zur Unternehmensführung durch Aufsichtsrat und Abschlussprüfer, AG 2018, 266
<i>Velte</i>	Regulierung von Corporate Governance-Systemen durch das geplante FISG: Eine kritische Würdigung, WPg, 74. Jg., Heft 6/2021, 387
<i>Velte/Eulerich</i>	Das geplante Finanzmarktintegritätsstärkungsgesetz (FISG). Eine kritische Diskussion aus Sicht der Internen Revision, Zeitschrift Interne Revision (ZIR), 56. Jg., Heft 2/2021, 64
<i>Verse</i>	Compliance im Konzern, ZHR 2011, 401
<i>Vetter</i>	Geschäftsleiterpflichten zwischen Legalität und Legitimität: Muss sich Ethik lohnen?, ZGR 2018, 338
<i>Vitt</i>	Die europäische Corporate Sustainability Due Diligence Directive im Überblick, CB 2024, 365
<i>Vogel</i>	Umfassende IT-Sicherheit: Für Unternehmen ein Muss, CB 2018, 197

- Vogelsang/Nahrstedt/
Fuhrmann* Compliance-Systeme auf Bundes- und Kommunalebene, CCZ 2014, 181
- Vollmer* Der Zugriff auf elektronisch gespeicherte Daten im Kartellordnungswidrigkeitenverfahren, WuW 2006, 235
- von der Linden* Deutscher Corporate Governance Kodex 2022 – Grüner, diverser, kleinteiliger, DStR 2022, 1765
- von Heintschel-Heinegg/
Kudlich (Hrsg.)* BeckOK StGB, 60. Edition, Stand: 1.2.2024
- von Holleben/Menz* IT-Risikomanagement – Pflichten der Geschäftsleitung, CR 2010, 63
- von Marnitz* Compliance-Management für mittelständische Unternehmen, 2011
- Voppel/Osenbrück/
Bubert (Hrsg.)* VgV Kommentar, 4. Aufl. 2018
- Voss* 14. Russland-Sanktionspaket der EU: Erhöhtes Straf- und Bußgeldrisiko bei Sanktionsumgehungen, CCZ 2024, 198
- Votaw/Sethi* The Corporate Dilemma. Traditional Values versus Contemporary Problems, 1973
- Wabnitz/Janovsky/
Schmitt (Hrsg.)* Handbuch Wirtschafts- und Steuerstrafrecht, 5. Aufl. 2020
- Wagner* „Internal Investigations“ und ihre Verankerung im Recht der AG, CCZ 2009, 8
- Wagner/Ruttloff* Das Lieferkettensorgfaltspflichtengesetz – Eine erste Einordnung, NJW 2021, 2145
- Wagner/Ruttloff/
Miederhoff* Product Compliance – Ein wesentlicher Baustein für Compliance Organisationen, CCZ 2020, 1
- Wagner/Ruttloff/Wagner
(Hrsg.)* Das Lieferkettensorgfaltspflichtengesetz in der Unternehmenspraxis, 2022
- Walden/Depping (Hrsg.)* CSR und Recht, Juristische Aspekte nachhaltiger Unternehmensführung erkennen und verstehen, 2015
- Wandtke/Bullinger
(Hrsg.)* Praxiskommentar zum Urheberrecht, 5. Aufl. 2019
- Warneke* Die Garantenstellung von Compliance-Beauftragten, NStZ 2010, 312
- Warren/Brandeis (Hrsg.)* The Right to Privacy, 4 Harvard Law Review, 193, 1890
- Waxenberger (Hrsg.)* Integritätsmanagement, 2001
- Weber-Rey* Compliance – a never ending story, CCZ 2014, 97
- Wecker/Ohl (Hrsg.)* Compliance in der Unternehmenspraxis, 3. Aufl. 2013
- Wegner/Schwenker/
Altdorf* Die neue Vertikal-Gruppenfreistellungsverordnung (EU) 2022/720 nebst Vertikal-Leitlinien – Kontinuität und Umbruch in der Vertriebspraxis, ZWeR 2022, 243
- Weihe* Compliance 2024: Was Verantwortliche im Mittelstand wissen müssen, CCZ 2024, 85

Literaturverzeichnis

- Weise/Brühl* Auswirkungen eines künftigen IT-Sicherheitsgesetzes auf Betreiber Kritischer Infrastrukturen, CR 2015, 290
- Weitbrecht/Mühle* Die Entwicklung des europäischen Kartellrechts 2015, EuZW 2016, 172
- Weller/Lieberknecht/Habrich* Virulente Leistungsstörungen – Auswirkungen der Corona-Krise auf die Vertragsdurchführung, NJW 2020, 1017
- Werder, von/Kost* Vertraulichkeitsvereinbarungen in der M&A-Praxis, BB 2010, 2903
- Werner* Bebußung der Konzernobergesellschaft für ein Fehlverhalten der Tochtergesellschaft nach § 130 OWiG, CB 2016, 167
- Werner* Strafbarkeitsrisiken durch das LkSG?, CB 2024, 245
- Wettner/Mann* Informationsrechte und Informationspflichten bei Internen Untersuchungen, DStR 2014, 655
- Wiedemann (Hrsg.)* Handbuch des Kartellrechts, 4. Aufl. 2020
- Wiedmann/Greubel* Compliance Management Systeme – Ein Beitrag zur effektiven und effizienten Ausgestaltung, CCZ 2019, 88
- Wiedmann/Hoppmann* Whistleblowing im DAX – Auswirkungen von HinSchG, LkSG, CSRD und CS3D-E, CCZ, 2023, 11
- Wiedmann/Seyfert* Richtlinienentwurf der EU-Kommission zum Whistleblowing, CCZ 2019, 12
- Wiedmann/Will* Die Russland-Sanktionen der EU, RIW 2022, 173
- Wieland* Unternehmensethik und Compliance Management – Zwei Seiten einer Medaille, CCZ 2008, 15
- Wieland/Schack* Soziale Marktwirtschaft: Verantwortungsvoll gestalten, 2011
- Wieland/Steinmeyer/Grüninger (Hrsg.)* Handbuch Compliance-Management, 3. Aufl. 2020
- Wiesner/Hömann* Die Kooperationsobliegenheit nach § 8 Abs. 1 Satz 3 WRegG, WuW 2022, 472
- Wimmer* MaRisk: Überblick und Konsequenzen für die Geschäftsleitung, BKR 2006, 146
- Windoffer* Der Lieferantenkodex als Mittel für ein LkSG-konformes und praktikables Miteinander im Geschäftsverkehr, CB 2023, 93
- Withus (Hrsg.)* Betriebswirtschaftliche Grundsätze für Compliance-Management-Systeme, 2014
- Withus/Kunz* Auswirkungen des neuen ISO 19600:2014 zu Compliance-Management-Systemen auf die Prüfung nach IDW PS 980, BB 2015, 685
- Wittig* Reform der Corporate Governance von Finanzinstituten als Reaktion auf die Finanzmarktkrise, WM 2010, 2337
- Wohlschlägl-Aschberger (Hrsg.)* Geldwäscheprävention: Recht, Produkte, Branchen, 2017
- Wolf, Klaus* Der IDW Prüfungsstandard 980 zur ordnungsmäßigen Prüfung von Compliance Management Systemen, DStR 2011, 997

- Wolf, Martin* Der Compliance-Officer – Garant, hoheitlich Beauftragter oder Berater im Unternehmensinteresse zwischen Zivil-, Straf- und Aufsichtsrecht?, BB 2011, 1353
- Wolff/Brink* (Hrsg.) BeckOK Datenschutzrecht, 46. Edition, Stand: 1.8.2023
- Wolff/Schroeren/Martin* Durchführung einer Risikoanalyse gemäß den MaComp und Zusammenspiel mit den Anforderungen an die Compliance-Funktion durch die 4. MaRisk-Novelle, CCZ 2014, 88
- Wolffgang/Witte* Compliance in der Exportkontrolle, CB 2015, 138
- Wright/Siegel/Keasey/Filatotchev* (Hrsg.) The Oxford Handbook of Corporate Governance, 2014
- Wulf* Praxishinweise zur Berichtigungspflicht nach § 153 AO, Stbg 2010, 295
- Wulf/Görlich* Neue Anzeigepflichten zur Umsetzung von Außenprüfungsergebnissen – eine erste Analyse, PStR 2023, 40
- Wurzberger/Nagel* Auswirkungen des „ESG-Tsunamis“ auf das Compliance-Management – Teil 1, ZRFC 2023, 325
- Wurzberger/Nagel* Auswirkungen des „ESG-Tsunamis“ auf das Compliance-Management – Teil 2, ZRFC 2023, 366
- Wüstemann/Büchner* Das Lieferkettensorgfaltspflichtengesetz: Pflichten und Verantwortung von Unternehmen – Eine kritische Würdigung, BB 2024, 579
- Wybitul* „Whistleblowing“ – datenschutzkonformer Einsatz von Hinweisgebersystemen? – Für und Wider zum rechtskonformen Betrieb, ZD 2011, 118
- Wybitul* Compliance und Betriebsrat – typische Konfliktfelder und praktische Lösungen, CB 2015, 77
- Wybitul/Astor* Datenschutzrecht als Grenze für Compliance-Maßnahmen, CB 2014, 260
- Wybitul/Fladung* EU-Datenschutz-Grundverordnung – Überblick und arbeitsrechtliche Betrachtung des Entwurfs, BB 2012, 509
- Zahrte* Die „zweite Stufe“ der PSD-2-Umsetzung, BKR 2019, 484
- Zeidler/Dürr* Greenwashing – Haftungsfallen und ihre Vermeidung, CCZ 2022, 377
- Zentes/Glaab* (Hrsg.) Frankfurter Kommentar zum Geldwäschegesetz, 3. Aufl. 2022
- Zerey* (Hrsg.) Finanzderivate, 5. Aufl. 2023
- Ziekow/Völlink* (Hrsg.) Vergaberecht, 5. Aufl. 2024
- Ziemons/Jaeger/Pöschke* (Hrsg.) BeckOK GmbHG, 40. Edition, Stand: 08/2019
- Zimmer/Seebacher* Whistleblowing – Wichtige Erkenntnisquelle oder gefährliches Pflaster?, CCZ 2013, 31
- Zimmermann* Die straf- und zivilrechtliche Verantwortlichkeit des Compliance-Officers, BB 2011, 634

Literaturverzeichnis

- Zimmermann, von* Whistleblowing und Datenschutz, RDV 2006, 242
- Zimmermann, von* Whistleblowing – Anforderungen des Sarbanes-Oxley-Acts, WM 2007, 1060
- Zöllner/Noack (Hrsg.)* Kölner Kommentar AktG, Bd. 2/1, 3. Aufl. 2009

Sachregister

Fette Zahlen verweisen auf die Kapitel, magere auf die Randnummern.

- Abbruch Geschäftsbeziehung **18 339**
- Abhilfemaßnahmen **18 338**
 - Wirksamkeit **18 340**
- Abwerbeverbot **27 49, 51**
- Ad-hoc-Meldungen **14 145**
- Ad-hoc-Pflicht **26 41 ff.**
 - Selbstbefreiung **26 42 f.**
- Adressaten **16 77**
- Adressenausfallrisiko **21 10, 17, 46**
- Agency-Theorie **11 11**
- AI Act **1 16**
- Akzeptanz
 - als Grundlage der Regelbefolgung **1 71 ff.**
 - der Unternehmensangehörigen **1 70**
 - des Compliance Managements **1 65**
- Amtsträger **2 45 ff.**
 - europäischer **2 88**
- Analyse des individuellen Geschäftsmodells des Unternehmens **1 62**
- Analyse- und Auswertetools **14 16**
- Anbieter digitaler Dienste **14 25 f., 31, 36, 128, 139**
- Anfangsverdacht **2 18; 8 7, 12, 28, 99; 22 96; 29 31**
- Angemessenheitsprinzip **18 323, 324 f.**
- Angriffserkennung **14 16, 36**
- Angriffsprävention **14 35**
- Anlassbezogene Risikoanalyse **18 331 f.**
- Anreizsystem **1 69**
- Arbeitnehmervertretung **16 122**
- Auditoren **10 30 ff., 39 ff.**
 - falsche Zertifikate **10 39 f.**
 - Risiken **10 58 ff.**
 - Widerruf der Zulassung **10 53 ff.**
- Auditverfahren **10 1 ff.**
- Aufklärung
 - Aufklärungspflicht des Aufsichtsrats **3 24**
- Aufsichtsmaßnahmen **1 35**
- Aufsichtspflicht
 - Verletzung der **2 133 ff.; 29 53 f.**
- Aufsichtsrat **2 125 ff.; 3 20 ff.**
- Auftragsdatenverarbeitung **12 65 ff.**
- Ausfuhrliste **25 19 ff.**
- Ausführverantwortlicher **25 35, 43, 45 ff., 51 f., 57 ff.**
- Auslagerungsmanagement (AT 9 Tz. 12 MaRisk) **14 72**
- Ausschreibungen **14 15; 27 19**
- Außenwirtschaftsrecht **1 19**
- Austausch von Informationen und Wissen **14 85**
- Auswahlermessen **1 53**
- Auswahlpflicht **1 57**
- Awareness-Schulung **14 150**
- B3S **14 37**
- BAFA *s. Bundesamt für Wirtschaft und Ausfuhrkontrolle*
 - FAQs **18 345 f.**
 - Handreichungen **18 345 f.**
 - Kontrollbefugnisse **18 347 f.**
 - Zuständigkeiten LkSG **18 345 f.**
- BaFin *s. Bundesanstalt für Finanzdienstleistungsaufsicht*
- BAIT **14 71, 81, 92**
- BDSG *s. Bundesdatenschutzgesetz*
- Bedeutende Institute **14 70**
- Befähigung vor Rückzug **18 339**
- Befragung von Mitarbeitern **8 103 ff.**
- Belastbarkeit **14 51 f.**
- Bemühenspflicht **18 323**
- Benachrichtigungspflicht **14 118, 137**
- Beratung der Geschäftsleitung **1 77**
- Beratungsstelle **1 81**

- Bereitstellung **24** 79 f.
– mittelbare **24** 84 ff.
Bereitstellungsverbot **24** 77 ff.;
25 8
Berichts- und Dokumentationspflichten **1** 4, 77; **29** 66 ff.
Berichtspflicht **18** 344, 346 f.
Berichtsweg **29** 66 ff.
Beschaffungsstrategien **18** 334 f.
Beschäftigtendatenschutz **12** 154 ff.
– Arbeitsvertrag **12** 154, 178 ff., 217
– Boarding-Phase **12** 194
– Einwilligung **12** 194 ff.
– internationaler Datenverkehr **12** 188 ff.
– Off-Boarding-Phase **12** 202 ff.
Beschwerdebeauftragte
– Befangenheit **19** 49
– Ernennung **19** 51
– Haftung **19** 55
– Kündigungsschutz **19** 48, 54
– Qualifikation **19** 46 f.
– Stellung im Unternehmen **19** 52 f.
– Unabhängigkeit **19** 48 f.
– Unparteilichkeit **19** 48
– verfahrensbegleitende Personen **19** 38
– verfahrensleitende Personen **19** 38
– Verschwiegenheit **19** 50
– Weisungsungebundenheit **19** 48, 55
Beschwerdeverfahren
– anonyme Hinweise **19** 41
– Beschwerdebeauftragte **19** 38
– Eingangsbestätigung **19** 42
– Konfliktbelegungsverfahren **19** 38, 44
– LkSG **18** 340 f.
– Rückmeldung **19** 45
– Verfahrensordnung **19** 39
– Wiedergutmachung **19** 43
Besonders wichtige Einrichtungen **14** 23, 26, 89, 93
Best Practice **8** 24, 43 f., 47
Bestandsaufnahme von Vorgaben des rechtlichen Umfelds **1** 61
Bestandsverzeichnis **1** 61
Bestechung **2** 58 ff.
– Abgeordnetenbestechung **2** 63 ff.
– Auslandsbestechung **2** 87 ff.
– Bestechungsgelder **29** 30
– im geschäftlichen Verkehr **2** 69 ff.
– im geschäftlichen Verkehr (Angestellter) **2** 72
– im geschäftlichen Verkehr (Beauftragter) **2** 72
– im Gesundheitswesen **2** 81 ff.
– von Mandatsträgern **2** 63 ff.
Bestpreisklauseln **27** 47
Betreiber von Energieversorgungsnetzen oder Energieanlagen **14** 29, 83
Betriebsausgabenabzug, Versagung **29** 28 f.
Betriebsführung durch Dritte **14** 29
Betriebsinterne Zuständigkeit **18** 326
Betriebsrat **3** 45 ff.; **12** 78, 206 ff.
– Mitbestimmungsrecht **5** 65 ff.
Betriebsstätte **29** 26
Betriebsvereinbarung **12** 31, 166 ff., 216 ff.; **29** 53 ff.
Betriebsvorfall **14** 132 ff.
Betroffenenrechte **12** 60
Beziehungskonflikt **6** 8 ff.
Bezugsgruppen **1** 11, 24, 69, 94 f.
Blacklisting **2** 165 ff.
Blockchain **13** 1 ff., 81 ff.
Bow-Tie-Analyse **9** 52 ff., 79
Boykott **27** 48
Branchenorganisationen **14** 37
Briefkastengesellschaften **29** 28
BSI *s. Bundesamt für IT-Sicherheit*
BSIG *s. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*
BSI-KritisV **14** 19
BSI-Sicherheitskennzeichen **14** 32
Buchführungs- und Aufzeichnungspflichten **29** 11
Budget- und Ressourcenmangel **6** 80 ff.

- Bundesamt für IT-Sicherheit (BSI) **14** 17, 19, 31 ff., 37, 39 ff., 54, 83, 92, 103, 126, 128 f., 131, 138 f., 141, 144, 151
- Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) **25** 30 ff., 35 ff., 45 ff., 58 ff.
- Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) **14** 28, 37, 65, 71, 74 ff., 81, 92, 132 ff.
- Bundesdatenschutzgesetz (BDSG) **12** 8, 13 ff., 82, 109, 196, 214, 216 ff., 229, 236; **14** 2, 52, 58 f., 88, 118, 122, 125; **20** 37
- Bundeskartellamt **27** 153 ff., 169 ff.
- Bundesnetzagentur **14** 27, 29, 62, 83, 138, 142, 151
- Business Continuity Management **14** 16, 35, 81
- Business Judgement Rule **1** 53; **13** 11; **14** 38, 90 f.
- Business Partner Compliance **1** 18
- Business Partner Control **1** 4
- Business Partner Due Diligence **20** 81
- Business Partner Screening **11** 61 f.
- Bußgeld **12** 10; **14** 33, 57, 113; **27** 91 ff.; **29** 55 ff.
- Unternehmensgeldbuße **2** 13, 87, 143, 156 ff.; **29** 55
 - Verbandsgeldbuße **29** 55
- CER-Richtlinie **14** 21
- Chief Compliance Officer (CCO) **1** 55;
s. auch Compliance Officer
- Cloud Computing **13** 17 ff., 21 ff.
- Cloud-Dienste **13** 16 ff.
- CMS *s. Compliance-Management-System*
- Code of Conduct **1** 73, 76; **3** 68 f.; **5** 1 ff.; **12** 107
- Ausgestaltung **5** 8 ff.
 - Betriebsvereinbarung **5** 48 ff.
 - datenschutzrechtliche Implikation **5** 60 ff.
 - Einführung **5** 26 ff.
 - Erscheinungsformen **5** 8 ff.
 - Günstigkeitsprinzip **5** 58
 - individualvertragliche Umsetzung **5** 29 ff.
 - Mitbestimmungsrecht des Betriebsrats **5** 65 ff.
 - typische Regelungen **5** 16 ff.
- Combined Attacks **14** 6
- Combined-Assurance **1** 50
- Commitment zu Compliance und Integrität **1** 69 f.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) **8** 8, 13, 24, 48
- Compliance
- als Auftragsvergabekriterium **30** 1
 - als Dauerpflicht **10** 2, 4
 - in der Lieferkette **1** 2, 17, 26, 84
 - Integration in die Geschäftsprozesse **1** 83 f.
 - Interaktionen mit bestehenden Unternehmensfunktionen **3** 4 ff., 76 ff.
 - junge Unternehmensfunktion **3** 2 ff.
 - Kontrollen **1** 18, 36, 40, 86
 - Koordination weiterer Unternehmensfunktionen **1** 85
 - Organisationsaufgabe **1** 2, 13
- Compliance Commitment **1** 69 f.
- Compliance Management **1** 1 ff.
- Aktualisierung **1** 1, 41, 58, 89, 91
 - Akzeptanz **1** 65, 70 f., 74
 - Auswahlmessen **1** 53
 - Delegation (und deren Grenzen) **1** 53, 56 f.
 - effizientes **1** 59
 - Erforderlichkeit und Zumutbarkeit **1** 58, 63
 - Führungs- und Organisationsaufgabe **1** 13
 - Informations- und Beratungsfunktion **1** 15
 - Kernelemente **1** 9, 51, 102
 - Marketing-Effekte **1** 96
 - Monitoring-Funktion **1** 15

- Organisationsgrad **1 51**
- Organisationsmodelle **1 55**
- Organisationspflicht **1 28, 38 f., 41, 49, 100**
- organisatorische Vorkehrungen **1 1**
- Qualitätssicherungs- und Innovationsfunktion **1 15, 99**
- und Integritätsmanagement **1 71 ff.**
- Vorteile **1 91 ff.**
- Wettbewerbsfähigkeit **1 96**
- Wettbewerbsvorteil **1 96**
- Wirksamkeit **1 44, 51, 58, 67 f., 71, 85, 102**
- Compliance Officer **1 55, 77 ff.;**
3 13 ff., 23, 26; 22 11, 103; s. auch
Chief Compliance Officer (CCO)
- Beratung der Geschäftsleitung **1 15, 77**
- Berichts- und Dokumentationspflichten **1 77**
- Informationsschnittstelle **1 77**
- Informationszugriffsrechte **1 77**
- Steuerung von relevanten Informationen **1 77**
- strafrechtliche Verantwortlichkeit **2 122 ff.**
- Überwachungs- und Kontrollpflichten **1 77**
- Compliance und CSR *s. Corporate Social Responsibility (CSR)*
- Compliance und Integrität **1 69, 71, 78, 83**
- Compliance-Audits **1 67, 89**
- Compliance-Ausschuss **3 21**
- Compliance-Beauftragter **20 6**
- Compliance-Berichterstattung **3 25;**
29 66 ff.
- Compliance-Committee **1 55**
- Compliance-Due Diligence **1 18;**
17 19 ff.; 26 73 ff.
- Stolpersteine **6 68 ff.**
- Vier-Schritte-Dialog **6 14**
- Compliance-Funktion **1 28 ff., 50, 55**
- Auslagerung **20 41 ff.**
- Compliance-Helpline **1 81**
- Compliance-Klauseln **3 38**
- Compliance-Kommunikation **1 51; 8 7,**
21; 20 52
- Compliance-Krise **3 42, 74**
- Compliance-Kultur **1 51 ff., 65, 68 ff.,**
88; 20 34, 47, 52
- Bereitschaft zu regelkonformen Verhalten **1 68**
- Commitment zu Compliance und Integrität **1 69 f.**
- Leitungsorgane **1 69**
- Compliance-Management-System (CMS) **1 10, 40, 46, 51; 3 6; 12 164;**
14 88, 99; 20 1, 48 ff.
- Angemessenheit **8 1, 6, 20, 50 ff., 55**
- Aufsichtsrat **3 22**
- Ausgestaltung **8 7 ff., 15, 55**
- Betriebsrat **3 5 ff.**
- CMS-Prüfung **8 1, 51**
- Compliance-Kommunikation **8 7;**
20 52
- Compliance-Kultur **8 7; 20 52**
- Compliance-Organisation **8 7; 20 1,**
52
- Compliance-Programm **8 7; 20 52**
- Compliance-Risiken **8 7; 20 47, 52,**
56, 61 ff.
- Compliance-Überwachung **8 7**
- Compliance-Verbesserung **20 52**
- Compliance-Verstoß **2 196 ff.; 3 24,**
42; 8 1 ff., 11 ff., 41
- Compliance-Ziele **8 7; 20 52**
- effektives **20 49, 56 f.**
- Einrichtung **3 6 ff.; 8 15**
- Finanzfunktion **3 50 ff.**
- Geschäftsleitung **3 5 ff.**
- Grundelemente **8 7 ff., 20 ff.**
- Implementierung **3 6 ff.; 8 17**
- Innenrevision **3 55 ff.**
- Personalabteilung **3 37 ff.**
- Rahmenkonzept **8 13, 16 ff.**
- Rahmenwerk **8 8, 15**
- Rechtsabteilung **3 28 ff.**
- Unternehmenskommunikation **3 66 ff.**

- Whistleblowing-Management-System **12** 107, 239 f.
- Wirksamkeit **8** 6
- Wirtschaftsprüfer **3** 60 ff.; **8** 15, 37
- Compliance-Maßnahmen **1** 2 ff.
- Akzeptanz **1** 71 ff.
- Marketingeffekte **1** 96
- Prioritätensetzung **1** 58
- Überprüfung **1** 67
- Wirksamkeit **1** 58, 71
- Zuständigkeiten und Verantwortungsbereiche **1** 32, 56
- Compliance-Organisation **1** 51; **8** 7; **20** 1, 37 f., 52
- Compliance-Organisationspflicht **1** 100
- Compliance-Pflicht **1** 26 ff., 36 ff.; **15** 34, 73
 - Ausweitung **1** 101
 - Kernbereich **1** 56
- Compliance-Programm **1** 10, 17, 44, 51; **8** 7; **20** 18, 52
- Compliance-Richtlinie **8** 43 ff.
- Compliance-Risiken **1** 14 ff., 48 f., 51, 60 ff., 83 f.; **8** 7; **20** 26 f., 47, 49, 56, 62 f.; **26** 95 ff.
 - Analyse und Bewertung **1** 63
 - Berichterstattung **1** 66
 - Bestandsaufnahme von Vorgaben des rechtlichen Umfelds **1** 61
 - Bestandsverzeichnis **1** 61
 - Bewertung menschl. Verhaltens **1** 63
 - Eintrittswahrscheinlichkeit **1** 63
 - Konzept zur Identifikation und Steuerung **1** 60, 64
 - Schadensausmaß **1** 63
 - systematische Identifikation **1** 61 f.
- Compliance-Risikoprofil **1** 49, 52 f., 60
- Compliance-Risikostrategie **1** 60, 66
 - Reporting **1** 66
- Compliance-Risiko-Struktur **1** 40, 86
- Compliance-Schulungen **1** 44, 73, 78 ff.
- Compliance-Standards **1** 51
- Compliance-Strategie **1** 54 ff.
- Compliance-Überwachung **1** 51; **8** 7
- Compliance-Verbesserung **1** 51, 99; **20** 52
- Compliance-Verpflichtungen **14** 3
- Compliance-Verstoß **1** 48 f., 51 f., 57, 63; **2** 196 ff.; **3** 24, 42; **8** 1 ff., 11 ff., 41; **14** 94, 96
 - Aufklärung **1** 87
- Compliance-Ziele **1** 51; **8** 7; **20** 52
- Comply or explain **15** 26, 64
- Computerprogramme **13** 6 ff.
- Cookies **12** 19, 93
- Corporate Citizen **15** 5
- Corporate Citizenship **15** 14, 15, 20
- Corporate Governance **15** 18 f.
 - und Corporate Social Responsibility **15** 20 f.
- Corporate Social Responsibility (CSR) **1** 4, 21; **15** 1 ff.; **16** 1 ff.
 - Berichterstattung **1** 23
 - Berichterstattung, nichtfinanzielle **16** 7, 12 ff.
 - Berichtspflichten **15** 50, 61; **16** 13 ff., 21 ff., 30 ff.
 - Compliance **1** 23; **16** 1 ff., 6 ff.
 - „Comply or explain“-Grundsatz **16** 53 ff.
 - Creating Shared Value (CSV) **15** Abb. 1
 - CSR 0.0 bis CSR 3.0 **15** 14
 - CSR 4.0 **15** 15
 - CSR-Richtlinie-Umsetzungsgesetz **15** 61, 63; **16** 7 ff.
 - Definition **15** 11 f., 16 f.; **16** 18
 - Deregulierung **15** 2
 - Deutscher Corporate Governance Kodex **15** 25 f., 64
 - Diversität(-skonzepte) **16** 7, 12, 20, 24, 42, 52, 62, 121
 - ehrbarer Kaufmann **15** 11, 15, 28, 54; **16** 3
 - Erklärung, nicht-finanzielle **15** 50, 61; **16** 22 ff., 30 ff., 41 ff.
 - Four Part Model **15** 13

- Globalisierung **15** 2
- Governance Gap **15** 67
- GRI-Berichtsstandard **15** 49 f.
- Hard Law **15** 43, 74
- Individualethik **15** 15
- Institutionsethik **15** 15; **16** 2
- ISO 26000 **15** 17, 56 f.
- kategorischer Imperativ **15** Abb.1
- Konzept **15** 5 ff., 13 ff.
- Konzernbericht, nichtfinanzieller **15** 61; **16** 24, 31, 38, 59 f.
- Koregulierung **15** 41, 64, 67
- Leistungsindikatoren, nichtfinanzielle **16** 13 ff., 38 f.
- Licence to Operate **15** 8
- OECD-Leitlinien für multinationale Unternehmen **15** 47 f.
- Personal Social Responsibility (PSR) **15** 15
- Prüfungen **16** 58 ff.
- Rahmenwerke **16** 17, 49 ff.
- Regulierung **15** 38 ff.
- Regulierungsmix **15** 61 f., 62 f.
- Reifegradpyramide **15** 14
- Reporting **15** 49 f., 61; **16** 1 ff.
- Reputationsmanagement **15** 7, 46
- Richtlinie **15** 61; **16** 7 ff.
- Risiken **15** 76 ff.; **16** 36 ff.
- Risikomanagement **15** 76, 77 ff.
- Selbstregulierung **15** 41, 65
- Shareholder **15** 1 f., 6, 21 f.; **16** 5
- Social Responsibility **15** 17
- Soft Law **15** 43 ff., 47, 49, 55, 57, 64, 76 ff.
- Stakeholder **15** 1 f., 16, 22, 46, 61 f., 71, 86; **16** 3 f.
- Strategie **15** 16, 62, 88
- UN Global Compact **15** 52 f.
- und Compliance **15** 1 ff., 70 ff.; **16** 1 ff.
- und Unternehmensführung **15** 5 f., 8 f.
- Verstöße, Säumnisse, Sanktionen **16** 63 ff.
- Corporate Sustainability Reporting Directive (CSRD) **15** 5; **15** 37; **16** 66 ff.
- COSO *s. Committee of Sponsoring Organizations of the Treadway Commission*
- COSO ERM **9** 64, 66
- Covenant-Tool **21** 43
- Creating Shared Value (CSV) **15** Abb. 1
- Crime as a Service **14** 5
- Criminal Compliance **2** 1 ff.
- Compliance-Verpflichtung **2** 22
- Kern-Compliance-Risiken **2** 21, 31 ff., 34
- CS3D *s. CSDDD*
- CSDDD **14**, 20; **19** 5
- Aktivitätskette **18** 351
- Anpassung LkSG **19** 5, 59
- Anwendungsbereich **18** 350 f.
- Corporate Sustainability Due Diligence Directive **15** 37; **18** 350 f.
- Sanktionen **18** 351
- Schutzgüter **18** 351
- Zivilrechtliche Haftung **18** 351
- CSR *s. Corporate Social Responsibility*
- CSRD *s. Corporate Sustainability Reporting Directive*
- CSV *s. Creating Shared Value*
- Cyberaktivisten **14** 6
- Cyber-Angriffe **1** 16
- Cyberattacke(n) **14** 10, 146, 148, 150
- Cybercrime **14** 4 f., 31
- Cyberintelligence **14** 16
- Cyber-Security **15**, 16, 101
- Cyberversicherung **14** 92, 145
- Data Act **1** 16; **13** 33 ff.
- Datennutzung **13** 63 ff.
- Datenschutzrecht **13** 61 f.
- Datenverarbeitungsdienste **13** 74 ff.
- Datenweitergabe **13** 41 ff., 63 ff.
- Regelungsinhalt **13** 38 ff.

- Data Leakage **14** 103
- Datengeheimnis **12** 69, 178 f., 207
- Datenportabilität **12** 11
- Datenschutz **5** 101 ff., 111, 161 ff.;
12 1 ff.; **14** 45, 102, 149; **20** 4, 35 ff.;
26 22 ff.
 - Anonymisierung **12** 31
 - Archivierungs- & Lösungsrichtlinie **12** 116 ff.
 - Auftragsdatenverarbeitung **12** 65 ff.
 - Betriebsrat **12** 78, 206 ff.
 - Betriebsvereinbarung **12** 155, 166 ff.
 - Datengeheimnis **12** 69, 178 f., 207
 - Datenschutz-Newsletter **12** 122
 - Datenverarbeitung **12** 15, 31, 68 ff., 135 ff.
 - Dokumentation **12** 77 ff., 135 ff., 178
 - Erlaubnisvorbehalt **12** 29 ff.
 - Funktionsübertragung **12** 67
 - Honeywell-Entscheidung **12** 167
 - HR-Compliance-Review **12** 178 ff.
 - Incidentreporting **12** 142
 - Internetnutzung **12** 222 ff.
 - IT-Datenschutzmanagement-Richtlinie **12** 114 ff.
 - IT-Infrastruktur-Review **12** 140 f.
 - IT-Nutzungsrichtlinie **12** 110 ff.
 - Kommunikation **12** 121
 - Kontrolle **12** 135 ff.
 - Löschmanagement **12** 203, 207
 - Personalleiter **12** 209 ff.
 - personenbezogene Daten **12** 43 ff., 49 ff.
 - Privatnutzung **12** 223, 227
 - Pseudonymisierung **12** 31, 49
 - Quick-Self-Assessment **12** 135 ff.
 - Schrankkontrolle (BAG-Entscheidung) **12** 232, 237
 - Schulung **12** 126 ff.
 - Transparenz **12** 37 ff.
 - Überwachung **12** 135 ff.
 - verantwortliche Stelle **12** 47 f.
 - Verdachtskündigung **12** 232
 - Verfahrensverzeichnis **12** 97, 114
 - Zweckbindung **12** 40
- Datenschutz-Audit **12** 64, 135 ff.
- Datenschutzbehörde **12** 105 ff.
- Datenschutzberatung **12** 87 ff.
- Datenschutz-Compliance **12** 28 ff.
- Datenschutz-Folgenabschätzung **12** 70
- Datenschutz-Grundverordnung (DSGVO) **1** 6, 16, 30; **12** 1, 13 f.;
13 61 f., 66, 73; **14** 2, 17 f., 45 ff., 52,
63, 88, 97, 109 ff., 137, 144; **20** 4,
37 f.
- Datenschutzjahresbericht **12** 140 ff.
- Datenschutzkontrolle **12** 135 ff.
- Datenschutzmanagementsystem **12** 6,
99 ff.
- Datenschutz-Newsletter **12** 122
- Datenschutzrecht **12** 27 ff.
- Datenschutz-Richtlinien **12** 17 ff.,
108 ff.
- Datenschutzverstöße **14** 94 f., 112
- Datenschutzbeauftragter **12** 5, 68 ff.
 - betrieblicher **12** 68 ff., 82 ff.
- Datensicherheit **13** 92
- Datensicherheitsziele **14** 51
- Datensparsamkeit **12** 35 f.
- Datenverordnung **13** 33 ff.
- Daueraufgabe in einem dynamischen
Umfeld **1** 8, 16 ff.
- Dauerhaftigkeit **20** 6
- Dawn Raids **27** 153, 180 ff.
- DCGK *s. Deutscher Corporate Governance Kodex*
- Delegation **2** 119; **8** 8 f.; **29** 64
 - horizontale **1** 53, 56 f.; **8** 8
 - vertikale **1** 56; **8** 9
- Delegation der Verantwortung
 - Geschäftsverteilungsplan **19** 26
 - horizontale **19** 26
 - Ressortverantwortlichkeit **19** 26
 - vertikale **19** 26
- Delegationsfrage **1** 35, 54, 56 f.
- Denial-of-Service-Angriff **14** 5 f., 15
- Desorganisation **29** 53
- Deutscher Corporate Governance Ko-
dex (DCGK) **1** 21, 46; **5** 35 f.;
15 25 f.; **20** 3

- Dezentrale Compliance-Mitarbeiter **6** 64 f.
- Digital Operational Resilience Act (DORA) **1** 6; **14** 81, 89
- Digitale Attacke **14** 108
- Digitale Schulungen: Schulungen mit Webinaren, Podcasts, Livestreams **6** 39 ff.
- Digitalisierung **1** 3, 16, 101
- Diversitätskonzepte **16** 7, 12, 20, 24, 42, 52, 62, 121
- Dodd-Frank Act **5** 18; **17** 16
- Dokumentation **14** 100, 116, 124; **22** 7, 10; **29** 60, 79
 - LkSG **18** 344
- Domizilgesellschaften **29** 28
- DORA *s. Digital Operational Resilience Act*
- Drittstaaten **16** 75
- DSGVO *s. Datenschutz-Grundverordnung*
- Dual-Use-Güter **25** 2, 6, 23 f., 40, 43 ff., 55
- Due Diligence **16** 35, 43 ff.; **17** 19 ff.; **20** 18, 81; **26** 11 ff., 22 ff., 40 ff.
 - Pflicht zur Durchführung **26** 45 ff.
 - Post-Closing Due Diligence **26** 52, 93 ff.
 - Third Party Due Diligence **1** 84
 - Umfang **26** 45 ff.
- Durchfuhr **25** 6, 11, 15
- Durchsuchung **27** 7
- Durchsuchungsbeschluss **27** 169
- Dynamik des rechtlichen Rahmens **1** 3

- EBA-Leitlinien **14** 74, 78, 133
- Effektivität **1** 59
- E-Geldinstitute **14** 28, 80
- E-Health-Gesetz **14** 17
- Ehrbarer Kaufmann **15** 11, 15, 28, 54; **16** 3
- Eigener Geschäftsbereich **18** 315 f.
- Einbeziehung von Führungskräften und Mitarbeitern **1** 65
- Einfrieren **24** 66
- Einfriergebot **24** 90 f.
- Einheitliches Sicherheitsniveau **14** 85
- Einkaufskooperationen **27** 54
- Einkaufspraktiken **18** 334 f.
- Einstweilige Unterlassungsverfügung **14** 147
- Einzelgenehmigung **25** 35 ff., 43
- Einziehung **2** 146, 164 ff.; **29** 58
- Embargo **24** 8 ff.
- Embargoverordnungen **25** 31
- Enabling Function **1** 95
- Energieunternehmen **14** 2
- Energieversorgungsnetz **14** 29, 83, 138
- Energiewirtschaft **14** 29
- Energiewirtschaftsgesetz (EnWG) **14** 2, 29, 83
- Enforcement **11** 18 ff.
- ENISA *s. Europäische Agentur für Netz- und Informationssicherheit*
- Enterprise Risk Management **9** 66, 96
- EnWG *s. Energiewirtschaftsgesetz*
- ePrivacy-Richtlinie **14** 63
- Erforderlichkeit **18** 315
- Erkundigungspflichten **29** 51
- Erlaubnisvorbehalt **12** 29 ff.
- Erleichterungen **16** 108 ff.
- Ermittlungsbefugnisse **27** 7
- Erstbenachrichtigung **14** 115
- ESEF *s. European Single Electronic Format*
- ESG-Compliance **1** 3 f., 17, 101
- ESG-Risiken **14** 66
- ESG-Themen **1** 4
- ESRS *s. European Sustainability Reporting Standards*
- Ethikprogramm **1** 71
- Ethische Standards **20** 1
- EU Cybersecurity Act **14** 32
- EU Forced Labor Prevention Regulation (FLPR) **1** 5
- EU-AML-Verordnung **24** 114
- EU-Blocking-VO **24** 143 f.
- EU-Deforestation Regulation (EUDR) **1** 5

- EUDR *s. EU-Deforestation Regulation*
 EU-Embargoverordnungen **25** 7, 50
 EU-Geldwäscherichtlinien **22** 4, 5, 13, 17, 24, 28, 32, 107
 Europäische Agentur für Netz- und Informationssicherheit (ENISA) **14** 85, 126
 European Single Electronic Format (ESEF) **16** 106, 119
 European Sustainability Reporting Standards (ESRS) **16** 69 ff., 84 ff.
 EU-Sanktionen **24** 26 ff.
 EU-Terrorismusverordnungen **25** 8, 50
 Event Tree Analysis **9** 54, 79
 Expertenhaftung **10** 36
 Exportkontrolle **25** 4 ff., 16, 25, 46 ff., 57 ff.
 Exportkontrollrecht **1** 7, 19
 Externe Ermittlung **3** 61; **8** 14 ff.
 Externe Ermittlungs- oder Aufsichtsbehörden **8** 15
 Externe Meldestelle **5** 105 ff.
 Externer Rechtsrat **29** 51
 Extraterritoriale Geltung ausländischer Gesetze **14** 2

 Fahrlässigkeit **1** 72
 Fahrlässigkeitshaftung **2** 131 ff.
 Failed Compliance **2** 196 ff.
 FATF *s. Financial Action Task Force on Money Laundering*
 Fault Tree Analysis **9** 54, 79
 FCPA *s. Foreign Corrupt Practices Act*
 Fehlverhalten **1** 35, 38, 83
 – menschliches **14** 8, 63
 – vorsätzliches **1** 12, 60, 72
 Financial Action Task Force on Money Laundering (FATF) **23** 9
 Financial Intelligence Unit (FIU) **23** 28
 Finanz- und Kapitalmarktprodukte **21** 1 ff.
 – Adressenausfall-/Kreditrisiko **21** 42
 – Anforderungen, aufsichtsrechtliche **21** 15
 – Asset Backed Securities (ABS) **21** 5
 – Ausstattung, personelle und technische **21** 26
 – Aval/Akkreditiv **21** 3
 – Cash-Pooling und Payment Factory Lösungen **21** 5
 – Covenant-Tool **21** 43
 – Darlehen **21** 3
 – Darlehen mit separater Zinssicherung **21** 5
 – Derivate **21** 3
 – einfache Produkte **21** 3 f.
 – Factoring **21** 3
 – interne Kontrollverfahren **21** 25
 – komplexe Produkte **21** 5 f.
 – Kreditrisiko-Tool **21** 46
 – Liquiditätsrisiko **21** 42
 – Liquiditätsrisiko-Tool **21** 51
 – Marktrisiko **21** 42
 – Marktrisiko-Tool **21** 48
 – Notfallkonzept **21** 27
 – operationelles Risiko **21** 11, 42
 – Rechtsrisiko **21** 11 ff., 42
 – Risiken **21** 10
 – Risikomanagementstrategie **21** 22 ff.
 – Risikotragfähigkeitskonzept **21** 24
 – strukturierte Schuldscheine, Anleihen und Kreditderivate **21** 5
 – Strukturrisiko **21** 13
 – Value-at-Risk-Modelle **21** 14
 – Vergütungssystem, nachhaltiges **21** 28
 – Zahlungsverkehr **21** 3
 Finanzberichterstattung **16** 102 ff.
 Finanzfunktion **3** 50 ff.
 Finanzindustrie
 – Kernverpflichtete **22** 33, 35, 46, 51
 Finanzinstitute **14** 66, 74; **21** 15 ff.
 Finanzmarktintegritätsstärkungsgesetz (FISG) **9** 16, 26
 Finanzsanktionen **24** 51 ff.
 First Line **20** 76 f.

- FISG *s. Finanzmarktintegritätsstärkungsgesetz*
FIU *s. Financial Intelligence Unit*
FLPR *s. EU Forced Labor Prevention Regulation*
Förderung von Regeltreue **1** 68 ff.
Foreign Corrupt Practices Act (FCPA) **2** 81; **20** 19
Fraud Triangle **11** 3
Früherkennung bestandsgefährdender Risiken **13** 3
Funktionsübertragung **12** 67
Fusionskontrolle **26** 26 ff.
- GAiN **14** 39
Garantenpflichten **1** 38, 41
Geeignete Nachweiserbringung **14** 39
Geldbuße **14** 124
Gelder **24** 57 f.
Geldwäsche **20** 4, 16 ff.; **22** 1 ff.; **23** 1 ff.
– Begriff **23** 2
– Funktionsweise **23** 6
– Skandale **23** 19 ff.
Geldwäschebeauftragter **22** 1
– arbeitsrechtlicher Schutz **22** 107
– Aufgaben **22** 1, 77
– Auslagerungsfähigkeit **22** 121
– Ausstattung **22** 60
– Bestellung **22** 13, 48, 129
– Haftung **22** 74, 130
– hoheitliche vs. unternehmerische Tätigkeit **22** 1, 116, 137
– Interessenkonflikte **22** 67
– Kompetenzen **22** 56, 84
– Residenzpflicht **22** 57
– Zuverlässigkeit **22** 48, 53, 127
Geldwäschebekämpfung
– Handel **23** 1, 5, 6
– Industrie **23** 1, 5, 6
– internationale Ebene **23** 9, 21
Geldwäsche-Compliance **23** 3, 9, 85
Geldwäschegesetz **22** 13, 118, 121; **23** 2, 13
– behördliche Anordnungen **22** 44
– Freistellungsmöglichkeiten **22** 38
– Verpflichtetengruppen **22** 4
– Ziele **23** 2, 8
Geldwäsche-Risiken **1** 16
Gesamtrechtsnachfolge **29** 56
Geschäftsführung einer GmbH **14** 3, 17, 30, 87 f.
Geschäftsgeheimnis **1** 6, 30
Geschäftsgeheimnisgesetz (GeschGehG) **1** 6, 30
Geschäftsherrenhaftung **2** 114, 122
Geschäftsleitung **1** 8, 39, 54, 58, 69, 86, 97; **3** 5 ff.
– Organisationsauftrag **1** 8, 37
Geschäftspartner **1** 7
Geschäftspartner-Compliance **29** 32
Gesetz gegen den unlauteren Wettbewerb (UWG) **12** 23, 26
Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) **1** 6; **14** 17 ff., 26 ff., 35 ff., 62, 81 ff., 92, 126 ff., 138 ff.
Gesetz zur Stärkung der Integrität in der Wirtschaft **8** 3
Gesundheitswesen **14** 17, 20
Good Corporate Governance **16** 1 ff.
Good Governance **1** 20
GRC
– Ansatz **1** 50, 83; **11** 24 ff.
– Konzept **11** 24
Grenzüberschreitende Geschäftstätigkeit **1** 7
Grundfragen einer rechtssicheren Unternehmensorganisation **1** 9 ff.
Grundsatzerklärung **18** 332 f.
Grundsatzkatalog **14** 37, 71
Gruppenfreistellungsverordnungen **27** 54
– Forschung und Entwicklung **27** 54
– gemeinsame Produktion bzw. Spezialisierung **27** 54
– gemeinsame Vermarktung **27** 54
– gemeinsamer Einkauf **27** 54

- Güterhändler **23** 22, 58
 - allgemeine Sorgfaltspflichten **23** 58
 - Bargeldtransaktionen **23** 29
 - Drittstaaten **23** 56, 67, 69, 73
 - Politisch exponierte Personen (PEPs) **23** 65, 67
 - Risikomanagement **23** 29, 39
 - Tipping-Off-Verbot **23** 61, 80, 82
 - Verdachtsfall-Meldungen **23** 36, 71
- Hackerangriff(e) **14** 4, 8 f.
- Haftung
 - bei Gemeinschaftsunternehmen **27** 85
 - bei Rechtsnachfolge **27** 87 f.
 - des Aufsichtspflichtigen **1** 35
 - des Steuerhinterziehers **29** 37
 - für Beauftragte **27** 86
 - GmbH-Geschäftsführer **1** 40
 - von Organen **29** 34
- Halten **24** 73 ff.
- Handels- und Vermittlungsgeschäfte **25** 15, 25 ff., 51
- Hardcore-Kartelle **27** 17
- HinschG *s. Hinweisgeberschutzgesetz*
- Hinweisgeberschutzgesetz (HinschG) **1** 87; **5** 26
 - persönlicher Anwendungsbereich **5** 46 ff.
 - sachlicher Anwendungsbereich **5** 43 ff., 110
 - Schutz von Hinweisgebern, Voraussetzungen **5** 51 ff.
 - Ziel **5** 40
- Hinweisgebersystem **1** 87; **20** 4, 28 ff.
 - Ausgestaltung **5** 126 ff.
 - Compliance-System **5** 9 f.
 - Einrichtung im Unternehmen **5** 123 ff.
 - Gesellschaftsrecht **5** 33
 - gesetzliche Anforderungen **5** 78 ff., 105 ff.
 - Gründe für die Einführung **5** 9 ff.
 - interne Richtlinie **5** 153
 - IT-gestützte Hinweisgebersysteme **5** 139
 - Meldewege **5** 11, 83 ff., 135 ff.
 - Ombudsleute **1** 87
 - Ordnungswidrigkeitenrecht **5** 34
 - Organisation **5** 124 f.
 - Spezialgesetze **5** 27 ff.
 - Vertraulichkeit **5** 79 ff., 111
- Honeywell-Entscheidung **12** 167
- Hospitality **2** 55
- HR-Compliance-Review **12** 178
- IDW PS 340 **9** 95
- IDW PS 980 **1** 26, 51, 68; **8** 1 ff., 15, 16 ff., 20 ff., 55; **20** 53 f.
- IKS *s. Internes Kontrollsystem*
- Imageschäden **1** 24 f., 48
- Implementation Guidances **16** 73, 101
- Implementierungskosten **14** 47 f.
- Incidentreporting **12** 142
- Individualethik **15** 15
- Industriespionage **14** 15, 31
- Information Security Management **14** 35
- Informations- und Wissensmanagement **1** 77
- Informationspflichten **14** 109, 145
- Informationsschnittstelle **1** 77
- Informationszugriffsrechte **1** 77
- Inhabilität **2** 186 ff.
- Innenrevision **3** 55 ff.
- Innerbetriebliches Exportkontrollsystem **25** 36, 43 f., 48 ff., 60
- Innerbetriebliches Kontrollsystem **29** 50
- Inside-out-Perspektive **1** 21
- Insider Threats **14** 103
- Insiderrecht **26** 43
- Institutionsethik **12** 78; **15** 15
- Instruktionspflicht **1** 57
- Integrierendes Modell **11** 24
- Integrierter Ansatz **1** 71
- Integrität **15** 88
- Integritätsmanagement **1** 72

- Interessenkonflikt
– Beschwerdebeauftragte **19** 47, 58
– Menschenrechtsbeauftragte **19** 9, 11 f., 18, 26, 28, 58
Internal Investigations **8** 2; **14** 92
Internationale Verrechnungspreise **29** 27
Interne Kontroll- und Risikomanagementsysteme **8** 8; **21** 25
Interne Meldestelle **5** 87 ff.
– Dritte **5** 88, 138
– Konzern **5** 90 ff., 133 ff.
– Unabhängigkeit **5** 89
Interne Revision **11** 21; **20** 9, 24, 61, 68 f.
Interne Richtlinien **3** 38; **14** 92, 101
Interne Untersuchung **8** 1 f.
Internes Kontrollsystem (IKS) **1** 29, 34, 50; **11** 14 f., 21; **20** 5, 9, 26, 56, 70 ff.
Internet-Attacke **14** 147
Internetnutzung **12** 222 ff.
Internetverkäufe **27** 45
Internetzahlungen **14** 74
Interpretationsleitfaden MaRisk **14** 65
Interviews von Mitarbeitern **8** 62, 71 f., 91
Intranetauftritt **6** 27
Intrusion Prevention **14** 103
ISIS 12 **14** 103
ISO 19600 **8** 11, 23, 55; **20** 49 f.
ISO 26000 **15** 17, 43, 56 f.
ISO 27000-Normreihe **14** 47
ISO 31000:2018 **9** 41
ISO 31022 **8** 1 ff., 31 ff.
ISO 37301 **1** 26; **8** 1 ff., 5, 11 ff., 24, 37 ff., 43 ff., 55; **20** 49 f., 53 f.
ISO-Norm **8** 1 ff.
IT-Compliance **1** 5; **13** 1 ff., 89
– rechtliche Herausforderungen **13** 1 ff.
– Risikoanalyse **13** 56 ff.
IT-Compliance-System **13** 88 ff.
IT-Datenschutzmanagement-Richtlinie **12** 114 ff.
IT-Dienstleistungen **14** 22
IT-forensische Analyse **14** 146
IT-Grundschutz Kompendium **14** 91
IT-Infrastruktur **14** 3 f., 28, 52, 53
– Review **12** 140 f.
IT-Landschaft **6** 89
IT-Nutzungsrichtlinie **12** 110 ff.
IT-Risikomanagementsysteme **14** 87
IT-Sicherheit **13** 1 ff., 89; **14** 1 ff., 16 f., 29, 45, 47, 82, 85, 91, 97, 101, 103, 126, 131
– Austausch von Information und Wissen **14** 85
IT-Sicherheitsgesetz **14** 2, 17, 19, 29, 31 ff., 83 ff., 144, 151
IT-Sicherheitskataloge **14** 29
IT-Sicherheitssysteme **14** 16

Kapitalmarkt-Compliance **20** 4, 6 ff., 38
Kartell-Compliance **20** 5, 81
Kartelle **27** 11
Kartellrecht
– Art und Umfang der Haftung **27** 89 ff.
– Ausbeutungsmissbrauch **27** 72 f.
– Ausschließlichkeitsbindungen **27** 77
– Ausschreibungen **27** 19
– Behinderung/Ausgrenzung von Wettbewerbern **27** 68
– Bestpreisklauseln **27** 47
– Boykott **27** 48
– Bundeskartellamt **27** 153 ff., 169
– Compliance **27** 1, 121
– Dawn Raids **27** 153, 181 ff.
– Definition des relevanten Marktes **27** 63
– Diskriminierung abhängiger Unternehmen **27** 78
– Durchsuchung **27** 7
– Einstandspreis **27** 79
– E-Raids (Elektronische Untersuchungen) **27** 162 ff.
– Ermittlungsbefugnisse **27** 7

- Essential Facilities 27 76
- Europäische Kommission 27 153 ff.
- Haftungssubjekte 27 80 ff.
- Hardcore-Kartelle 27 17
- Informationsaustausch 27 24 ff.
- Internetverkäufe 27 45
- Kartellrechts-Risiken 27 1
- kollektiver Rechtsschutz; Sammelklage 27 105 f.
- Kopplung von Angeboten 27 71
- Kosten-Preis-Schere 27 70
- Kundenbindung; Treuerabatte 27 69
- Leitlinien 27 122
- Marktaufteilungen 27 41 ff.
- marktbeherrschende Stellung 27 63
- Missbrauchsverbot 27 60
- Nachprüfungsentscheidung 27 157
- Niedrigpreisstrategien 27 74
- Preisabsprachen 27 11
- Preisbindungen 27 36 ff.
- Preisempfehlungen 27 36 ff.
- Risiken 27 1, 110 ff.
- Risikoanalyse 27 112 ff.
- Verbände 27 35
- Verbandsarbeit 27 31 f.
- Vereinbarungen zwischen Unternehmen 27 8
- Vertriebsbeschränkungen 27 55 ff.
- wettbewerbsbeschränkende Vereinbarungen 27 10
- Wettbewerbsbeschränkung, bewirkte 27 16
- Wettbewerbsbeschränkung, bezweckte 27 15
- Wettbewerbsverbote (Markenzwang); Alleinbezugsverpflichtungen 27 58 f.
- Zufallsfunde 27 174
- Zwangslizenz 27 75
- Kartellrechtsverstöße 1 16
- Kategorien personenbezogener Daten 14 49, 118
- Kategorischer Imperativ 15 Abb. 1
- KI-Compliance 1 16, 101
- Klärung von Zuständigkeiten 1 54, 56 f.
- KMU 16 75, 82 f.
- Know Your Customer- (KYC-)Prinzip 20 17; 23 57
- Kollektiver Rechtsschutz 27 105 f.
- Kommunikations-Management 6 12
- Fehler 6 80 ff.
- Kommunikationsmodelle 6 7
- Kommunikationsstrategie 6 3; 14 145 ff.
- Konfliktarten 6 8
- Beziehungskonflikt 6 8
- Sachkonflikt 6 8
- Konfliktmineralien 17 19 ff.
- Konfliktmineralien-Verordnung 1 5
- Kontroll- und Überwachungspflicht 1 57, 77, 86
- Kontroll- und Überwachungsverantwortung 14 97 f.
- Kontrollen 1 15, 36, 40, 86; 20 77 f.; 24 73 ff.
- Mitarbeiter 1 40
- systematische 1 86
- Kontrollhandlungen 20 27, 62, 76
- Konzernhaftung 27 83 f.
- Konzernprivileg 16 81 f.
- Koordinierungsstelle 8 25 f., 46, 56, 91
- Korruption 1 16; 2 36 ff.; 3 2, 17; 20 18 f., 46
- Auslandsbestechung 2 87 ff.
- Bekämpfung 2 36 ff.; s. auch *Korruptionsbekämpfung*
- Beratervertrag 2 101
- Bestechung 2 58 ff.
- Bestechung im geschäftlichen Verkehr 2 69 ff.
- Bestechung im Gesundheitswesen 2 81 ff.
- Bestechung von Mandatsträgern 2 63 ff.
- Hospitality 2 55
- Korruptionsregister 2 9, 176
- Risiken 20 18

- steuerliche Effekte **2** 107 ff.
- Überblick **2** 36 ff.
- Unrechtsvereinbarung **2** 50, 59
- Vorteilsgewährung **2** 44 ff.
- Korruptionsbekämpfung **2** 36 ff.
- Internationalisierung der **2** 8
- Kosten-Preis-Schere **2** 70
- Kreditinstitut **14** 28, 64, 82; **16** 21, 25, 64 f, 80
- Kreditrisiko **21** 42
- Kreditrisiko-Tool **21** 46
- Kreditunternehmen **14** 2
- Kreditwesengesetz (KWG) **14** 28, 64, 73, 81; **21** 15
- Kriegswaffenkontrollgesetz (KrWaffKontrG) **25** 10, 17
- Krisenfall **14** 106
- Krisenstab **14** 102
- KRITIS-Betreiber **14** 19 ff., 31 f., 35 ff., 126, 129 ff.
- KRITIS-Dachgesetz **14** 21, 44
- KRITIS-Unternehmen **14** 19, 27, 32
- Kronzeugenantrag **27** 186
- KrWaffKontrG *s. Kriegswaffenkontrollgesetz*
- Kulturunterschiede **6** 98
- Kundendaten **14** 24
- KWG *s. Kreditwesengesetz*

- Lagebericht **16** 105 ff.
- Legal Monitoring **1** 89, 103
- Legalitätsthroughsetzungspflicht **1** 36
- Legalitätskontrollpflicht **1** 36, 48
- Legalitätspflicht **1** 36, 39 f.; **3** 28 ff., 31; **14** 87; **20** 64
- Legitimitätsprinzip **20** 64
- Leichtfertige Steuerverkürzung **29** 39 ff.
- Leitungsorgane **1** 2, 69, 93 ff.
- Leitungssorgfaltspflicht **1** 56, 60
- Leitungsverantwortung **1** 36 f.
- Licence to Operate **15** 8
- Lieferant **17** 1 ff.
- Lieferantenauditierung **17** 26
- Lieferantenauswahl **17** 11 ff.
- Lieferantenbewertung **17** 7 ff.
- Lieferantenentwicklung **17** 9 ff.
- Lieferantenmonitoring **17** 13 ff.
- Lieferkette **16** 29, 37, 43
- LkSG **18** 314 f.
- Lieferketten-Compliance **1** 2, 17, 26, 84
- Lieferkettenrichtlinie *s. CSDDD*
- Lieferkettensorgfaltspflichtengesetz (LkSG) **1** 4, 30; **15** 36; **16** 120; **20** 1, 21 f.
- Limit- oder Ampelsysteme **14** 66
- Liquiditätsrisiko **21** 42
- Liquiditätsrisiko-Tool **21** 51
- Listenprinzip **24** 47 ff.
- LkSG *s. Lieferkettensorgfaltspflichtengesetz*
- LkSG-Risikomanagement
- Überwachung **19** 5 ff., 10, 23, 33, 26, 28 f., 58
- Lohnsteuer **29** 16 f.
- Löschmanagement **12** 203, 207

- M&A-Transaktionen **26** 1 ff.
- Abbruch der Verhandlungen **26** 53 ff.
- Asset Deal **26** 6, 98 f.
- Bieterverfahren **26** 5
- Compliance-Risiken **26** 95 ff.
- Datenschutz **26** 22 ff.
- Due Diligence **26** 3, 16, 22 ff., 40
- M&A-Compliance, materielle **26** 3 f., 73 ff.
- M&A-Compliance, prozessuale **26** 5 ff.
- Share Deal **26** 6, 98
- Zustimmungserfordernisse **26** 57 ff.
- MaComp **20** 4, 6; **21** 32 ff.
- Compliance **21** 32 ff.
- Mangelnde Authentizität **6** 76 ff.
- MaRisk **14** 28, 37, 64 ff., 80 ff.; **20** 4, 24 ff.; **21** 15, 29
- BA-Compliance **21** 29
- Compliance **20** 24 ff.

- Marker **27** 186
- Marktaufteilungen **27** 41 ff.
- Marktmacht/Marktbeherrschende Stellung **17** 23; **27** 63
- Marktrisiko **21** 42
 - Tool **21** 48
- MaSI **14** 74, 78, 132
- Maßnahmen
 - restriktive **24** 9 ff.
 - zur Prävention von Fehlverhalten **1** 83
- Matrix-Organisation **1** 55
- Melde- und Beschwerdeverfahren **1** 4
- Meldepflicht **14** 27, 32, 34, 109 ff., 145
- Meldestellenbeauftragte **19** 56
- Meldewesen **22** 8, 95
- Meldungen
 - anonyme Meldungen **5** 149 f.
 - Bearbeitung **5** 94 ff., 111
 - Dokumentation **5** 102 ff.
 - externe Meldungen **5** 63 ff.
 - Folgemaßnahmen **5** 97 f.
 - interne Meldungen **5** 60 ff.
 - Offenlegung **5** 67 ff.
 - Wahlrecht **5** 59
- Menschenrechtliche Risiken **18** 317 f.
- Menschenrechtsbeauftragte **18** 320 f., 326
 - Ernennung **19** 20 f., 23
 - Haftung **19** 34 f.
 - Integration **19** 27, 30
 - Jahresplan **19** 13
 - Konzernmenschenrechtsbeauftragte **19** 32
 - Kündigungsschutz **19** 24, 29
 - Qualifikation **19** 14
 - Unabhängigkeit **19** 17 f.
 - Unparteilichkeit **19** 17 f.
 - Weisungsungebundenheit **19** 17 f., 28
 - Verankerung **19** 27
 - Verschwiegenheit **19** 22
- Menschenrechtsbezogene Pflichten **18** 319 f.
- Menschenrechts-Komitee **19** 6, 18
- Menschenrechtsstrategie **18** 333
- MiCAR **20** 13 f.
- Mission Statement **1** 70
- Mitarbeiterbindung **1** 11
- Mitteilungspflicht **29** 8
- Mittelbare Zulieferer **18** 317
- Multi-Faktor-Authentifizierung **14** 64
- Muster organisatorischer (Mindest-)Anforderungen für ordnungsgemäße Unternehmensführung **1** 26
- MVP-Portal **14** 134
- Nachhaltigkeit **15** 1 ff., 54; **16** 1 ff.; **17** 4 ff.
 - Aktivitäten **17** 15 ff.
 - Deutscher Nachhaltigkeitskodex **16** 50
 - Engagement **17** 17 ff.
 - Investition **17** 18
 - Performance **17** 9 ff.
 - Risiken **17** 14
- Nachhaltigkeitsvereinbarungen **27** 54
- Nachprüfungsentscheidung **27** 157
- NAP *s. Nationaler Aktionsplan*
- Nationaler Aktionsplan (NAP) **18** 313
- Nationales Sanktionsrecht **24** 99 f.
- Near misses **14** 34
- NIS-Richtlinie **1** 6; **14** 17, 20, 31, 84 f., 126, 151
- NIS-2-Richtlinie **14** 34, 81, 86, 93, 127, 151
- NIS2UmsuCG **14** 86, 89, 127
- No Claim Clause **24** 191
- No-hire Agreement **27** 49
- Non-Compliance
- Non-Compliance (Regelverletzung) **1** 1, 8, 11 ff., 24, 62, 75, 76, 87 f., 90, 92, 100; **15** 71
 - Aufdeckung und Sanktionierung **1** 44

- fahrlässiges Verhalten **1 12**
- Nachteile von **1 13**
- proaktives Vermeidung **1 8, 11 ff.**
- Risiken **1 8, 11 ff.**
- Verteidigungsmöglichkeiten **1 97**
- vorsetzliches Fehlverhalten **1 12**
- No-poach Agreement **27 49**
- Notfallkonzept **14 71, 92; 21 27**
- Nullbescheid **25 38**
- Nützliche Pflichtverletzungen **1 49, 63, 104**

- OECD-Übereinkommen **5 25**
- Öffentliche Zugänglichmachung **13 19 f.**
- Ombudspersonen **1 87**
- Open-Source-Software **13 11 f.**
- Ordnungsgemäße Geschäftsorganisation (§25a KWG) **14 65, 76**
- Organhaftung **1 38; 29 34**
- Organisationsauftrag **1 2, 37**
- Organisationsherrschaft **2 129 ff.**
- Organisationsmodelle **1 55**
- Organisationspflicht **1 39, 41, 48, 90, 100**
- zur Verhinderung von Rechtsverletzungen **1 39, 49**
- Organisationspflichtverletzungen **14 75**
- Organisationsverschulden **2 131**
- Organmitglied **14 97 f.**
- OWiG **1 35, 59**

- Personal Social Responsibility (PSR) **15 15**
- Personalabteilung **3 37 ff.**
- Personalprinzip **24 30 ff.**
- Personenbezogene Daten **12 43 ff., 49 ff.**
- Persönliche Haftung **27 81**
- Persönlichkeitsrecht **12 3**
- Pflicht zur Einrichtung eines Hinweisgebersystems **5 71 ff.**
- juristische Personen des öffentlichen Sektors **5 76 f.**
- private Unternehmen **5 72 ff.**
- Pflichten
- Aufsichtspflicht **1 27, 35**
- Auswahlpflicht **1 57**
- Berichts- und Dokumentationspflicht **1 4, 77**
- Compliance-Pflicht **1 4, 6, 16, 23, 26, 27 ff., 36 ff., 38 f., 56**
- Instruktionspflicht **1 56**
- Organisationspflicht **1 28, 38 f., 41, 49, 100**
- Rechtspflicht **1 2, 16, 23, 61, 73, 77**
- Sorgfaltspflicht **1 4, 7, 12, 23, 56**
- Überwachungspflicht **1 57, 86**
- Unternehmensorganisationspflicht **1 38, 41**
- Plan-Do-Check-Act **20 53**
- Plattformen **27 47**
- Plausibilitätskontrolle **29 70**
- Polizei **14 59, 146**
- Prävention **1 4, 13, 16, 48, 58, 74, 77, 83, 92; 3 4, 5; 20 4, 16, 53, 57 f., 68**
- Präventionsmaßnahmen
- LkSG **18 334 ff.**
- Wirksamkeit **18 338**
- Präventive Maßnahmen **27 121**
- Preisabsprachen **27 11**
- Preisbindungen **27 36 ff.**
- Preiseempfehlungen **27 36 ff.**
- Presseöffentlichkeit **2 18**
- Primärsanktionen **24 126 ff.**
- Privatnutzung **12 223, 227**
- Proaktiv präventive Beratung **20 62**
- Probleme mit der Technik **6 88 ff.**
- Process Owner **1 65, 83**
- Produktwarnungen **14 43**
- Prozessbeschreibung **29 70**
- Prozessstandschaft **18 350**
- Prozessunabhängigkeit **20 76, 80**
- Prüfung **16 107, 118**
- Prüfung von Compliance-Management-Systemen (IDW PS 980) **1 51**
- Prüfungsstandard 261 **11 30**
- PSD II **14 64, 74, 81**
- PSR *s. Personal Social Responsibility*

- Qualifizierte Sicherheitsdienstleister **14** 37
- Querschnittsstandards **16** 90
- Ransomware **14** 5, 9 f.
- Reaktion **20** 53, 57
- Rechenschaftspflicht **12** 2
- Rechtsabteilung **3** 28 ff.
- Rechtsbereich **20** 63 ff.
- Rechtsdurchsetzungsanspruch **1** 49
- Rechtsrisiko **21** 11 ff., 42
- Rechtstreue **5** 11 ff.
- Referentenentwurf **16** 111 ff.
- Regelverletzung *s. Non-Compliance*
- Regelverstöße *s. Non-Compliance*
- Reporting **16** 1 ff.
- Reputation **1** 13, 24, 94, 105; **3** 66 ff., 92 ff.; **15** 16; **16** 5, 13 f., 48, 53 94
- Reputational Risk Management **1** 94
- Reputationsmanagement **1** 23 ff.; **15** 7, 46
- Reputationsrisiken **1** 24, 48, 94; **20** 66
- Reputationsschäden **1** 11, 24 f.; **17** 3 ff.
- Resilienzmaßnahmen **14** 44
- Ressourcen
- wirtschaftliche **24** 59 ff.
- Risiko
- geografisches **24** 209
 - kundenbezogenes **24** 206
 - leistungswirtschaftliches **9** 77
 - operationelles **21** 11, 42
 - produktbezogenes **24** 207
 - transaktionsbezogenes **24** 208
 - unzureichender Unternehmensorganisation **1** 48
- Risikoaggregation **9** 87 ff.
- Risikoanalyse **14**; **11** 53 ff.; **13** 89; **14** 44, 46, 66, 90, 103, 118, 123; **18** 327 ff.; **27** 112 ff.; **29** 61
- Risikoappetit **9** 15, 63, 66, 69
- Risikobegrenzung **11** 39
- Risikobewertung **9** 52, 55, 78 ff.
- Risikobewusstsein **20** 75
- Risikocontrolling **11** 39; **20** 8, 24, 66 f., 78
- Risikodeckungspotenzial **9** 20, 69, 87 f.
- Risikoidentifikation **9** 70, 72, 77 ff.
- Risikoinventur **1** 49, 62; **20** 66
- Risikokategorisierung und -bewertung **27** 116 f.
- Risikokultur **9** 56, 66, 96 108,
- Risikomanagement **1** 14, 27, 43, 47 ff., 54 f., 63, 83, 85; **6** 16; **9** 1 ff.; **14** 25, 30, 37, 64 ff., 74, 151; **16** 11, 90; **20** 4, 11, 27, 53, 63, 66, 68, 76; **21** 1 ff.
- Delegation **21** 53
 - LkSG **18** 324
 - Methoden und Verfahren **1** 60
 - Prozess **9** 64 ff.
 - Strategie **21** 22 ff.
 - Wirksamkeit **18** 325 f.
- Risikoprävention **1** 33
- Risikoprofil **1** 52 ff., 60, 65; **22** 114
- Risikosteuerungs- und -controlling-prozesse **14** 69
- Risikosteuerungsmaßnahmen **1** 64 f.
- Risikostrategie **1** 27, 60, 66; **9** 59 ff.
- Risikotragfähigkeit **9** 15, 57, 63, 69, 87 ff.
- Risikotragfähigkeitskonzept **21** 24
- Risikovermeidungsmaßnahmen **1** 64
- Risk based approach **22** 16
- RTS-Standards **14** 64
- Sachkonflikt **6** 8
- Sammelgenehmigung **25** 36, 43, 50
- Sammelklage **27** 105
- Sanction Compliance **1** 3
- Sanktionen **13** 73; **14** 73, 124
- LkSG **18** 348 f.
- Sanktionierung von Regelverletzungen **1** 1, 33, 35, 44, 72, 88, 100, 104
- Sanktionsdurchsetzungsgesetz I **24** 112
- Sanktionsdurchsetzungsgesetz II **24** 113
- Sanktionsrecht **1** 19

- Sanktionsregelungen **17**
 SAR *s. Suspicious Activity Reporting*
 Sarbanes Oxley Act (SOX) **517**
 Schadensersatz **2797 f.**
 Schmiergelder **2930**
 Schnittstellenmanagement **185**
 Schulung **150, 64, 78 ff.; 312, 39;**
 12126 ff.; 27133 ff.; 2979
 – E-Learning **12131; 27133 ff.**
 – persönliche **632 f.**
 – Schulungshandbuch **664 ff.**
 Schulungs- und Fortbildungsmaßnahmen **179 f.**
 Schulungsprogramm **154**
 Schutz von Unternehmen, Leitungsorganen und Unternehmensangehörigen **193**
 Schutzmaßnahmen **1416, 103, 106, 118, 151**
 Schutzmaßnahmen zugunsten von Hinweisgebern **5115 ff.**
 – Beweislastumkehr **5119**
 – Verbot von Repressalien **5116 ff.**
 – Schwarze Kasse **234, 101**
 SDGs *s. Sustainable Development Goals*
 SDN **24139**
 Second Line **205, 26, 63, 76, 78**
 Sektorklassifikation
 1674, 76
 Sekundärsanktionen **24126 ff.**
 Selbstanzeige **29101 ff.**
 Selbstverpflichtung **169**
 Sensitivitätsanalyse **990 f.**
 Share Deal **266, 98**
 Shareholder **151 f., 6, 21 f.; 165**
 Shareholder Value Management
 151 f.
 Shitstorm **146, 104**
 Sicherer IT-Betrieb **1471**
 Sicherheitsaudits **1439**
 Sicherheitsbeauftragter **1462**
 Sicherheitskonzept **1462, 78, 101**
 Sicherheitsprodukte **1442**
 Sicherheitsstandards **1437**
 Sicherheitsvorfall **1436, 55, 92, 118, 120, 123, 125, 127, 132 ff., 139 ff.**
 Sicherung der Reputation des Unternehmens **194**
 Sicherungssysteme **2016**
 Siemens/Neubürger **264, 84**
 Small and Medium-sized Entities
 s. SMEs
 Smart Contracts **1381 ff.**
 Smart Sanction **2413 ff.**
 SMEs
 1675, 82 f.
 Soft Law **123**
 Softwarelizenz-Audit **1326 ff.**
 Software-Lizenzmanagement **131 ff., 4 ff., 13 ff., 16 ff., 23 ff., 90 f.**
 Sonstige strafbare Handlungen (§ 25h KWG) **204**
 Sorgfaltspflichten **14; 2017**
 – LkSG **18320 ff.**
 SOX *s. Sarbanes Oxley Act*
 Sozial- und Umweltfaktoren **121**
 Sozialadäquanz **252**
 Soziale Medien **14104**
 Specially Designated Nationals *s. SDN*
 Spezialisierung **2754**
 Staatsanwaltschaft **14146**
 Stakeholder **113, 82, 94; 151 f., 16, 22, 46, 61 f., 71, 86; 163 f., 5**
 Stakeholder Value Management **154**
 Stand der Technik **1436 f., 44, 47 f., 50, 92, 96, 100, 103**
 Starke Kundenauthentifizierung **1464, 74, 79**
 Start-Up-Unternehmen **110**
 StaRUG **916, 18 ff., 95 f.**
 State Sponsored Attacks **1411**
 Stellenbeschreibungen **337; 2965**
 Steuer- und Abgabentatbestände im Vergaberecht **3015**
 Steuerhinterziehung **2108 ff.; 2939 ff.**
 Steuerliche Haftungsrisiken **2933 ff.**
 Steuerliche Organschaft **2969**
 Steuerliche Pflichten **295 ff.**
 Stichprobenargument **108**

- Stolpersteine **6** 68 ff.
 Strafrechtliche Sanktionen **27** 89;
 30 13
 Strategie- und Strukturentscheidungen
 1 2, 37, 54
 Stresstests **14** 68 f.
 Strukturrisiko **21** 13
 Substantiierte Kenntnis **18** 342 ff.
 Supply Chain **15** 59 f.; **17** 1 ff., 15 ff.,
 23
 – Due Diligence **17** 19 ff., 23
 – Konfliktmineralien **17** 19 ff.
 – Qualifizierungsauditierung **17** 11 ff.
 – Supply Chain Manager **17** 4, 19
 – Supply-Chain-Position **17** 16 ff.
 – Zulieferer **17** 23 f.
 Supply-Chain-Compliance **1** 17, 26
 Suspicious Activity Reporting (SAR)
 22 26
 Sustainable Development Goals
 (SDGs) **15** 52
 Szenarioanalyse **9** 77, 79
- Targeted Attacks **14** 6
 Tax Compliance **29** 1 ff.
 Tax-Compliance-System **29** 50, 57,
 83 ff., 92 ff.
 TDDDG *s. Telekommunikation-
 Digitale-Dienste-Datenschutz-
 Gesetz*
 Technikneutralität **14** 51
 Technische und organisatorische Maß-
 nahmen **14** 16, 36, 45, 52 ff., 57, 103
 Technische Unterstützung **25** 28 f.
 Telekommunikation- Telemedien-
 Datenschutz-Gesetz (TTDSG)
 14 24, 60, 63
 Telekommunikation-Digitale-Dienste-
 Datenschutz-Gesetz (TDDDG)
 12 23 f.
 Telekommunikationsanbieter **14** 13,
 20, 27, 142
 Telekommunikationsgesetz (TKG)
 14 27, 32, 61 ff., 142 ff.
 Telemediendienstanbieter **14** 24
- Telemediengesetz (TMG) **14** 24, 32,
 60, 139
 Territorialprinzip **24** 28 ff.
 Terrorismusfinanzierung **20** 4, 16, 18
 Themenstandards **16** 91 ff.
 Third Line **20** 68, 76, 80
 Three Lines Model
 1 50; **19** 10
 TKG *s. Telekommunikationsgesetz*
 TMG *s. Telemediengesetz*
 Tochtergesellschaften im Ausland
 29 25 f.
 Tone at the Top **1** 69; **3** 11, 37, 70, 93
 100 ff.; **6** 20; **20** 3, 52, 58
 Tone from the Top **1** 69; **6** 20
 Transparenz **12** 37 ff.
 Transparenzkultur **22** 29, 30
 Trickle-Down-Effekt **1** 4
 Trojaner **14** 10, 107
 Trolling **14** 104
 TTDSG *s. Telekommunikation- Tele-
 medien-Datenschutz-Gesetz*
- UAG *s. Umweltauditgesetz*
 Überwachung **1** 15, 22, 29, 35, 41
 – systematische **1** 86
 – von Mitarbeitern **1** 40
 Überwachung von Unternehmen **11** 2
 – (Jahres-)Abschlussprüfung **11** 14 f.
 – Compliance **11** 14
 – Controlling **11** 15, 22
 – Corporate Governance **11** 14
 – Instrumente der Unternehmensüber-
 wachung **11** 12
 – Integriertes System **11** 51
 – interne Revision **11** 21
 – internes Kontrollsystem **11** 14 f., 21
 – internes Überwachungssystem
 11 21
 – mittelständisch geprägte Unterneh-
 men **11** 47 ff.
 – Risikoanalyse **11** 53 ff.
 – Risikomanagement **11** 15
 – Risikomanagement im engeren Sin-
 ne **11** 23

- Risikomanagement im weiteren Sinne **11 20**
- Risk Management **11 14**
- Überwachungs- und Kontrollpflichten **1 77**
- Überwachungspflicht **1 57, 77, 86**
- UBI *s. Unternehmen im besonderen öffentlichen Interesse*
- UK Bribery Act (UKBA) **1 43; 2 81; 5 22 ff.; 20 18**
- UKBA *s. UK Bribery Act*
- Umsatzsteuer **29 18 f.**
- Umstrukturierung **29 67**
- Umweltauditgesetz **10 41 ff.**
- Umweltbezogene Pflichten **18 319 f.**
- Umweltbezogene Risiken **18 318 f.**
- Umweltgutachter **30 ff., 39 ff., 43 ff.**
 - falsche Zertifikate **10 39 f.**
 - Risiken **10 58 ff.**
 - Widerruf der Zulassung **10 53 ff.**
- Umweltgutachterausschusses **10 50 ff.**
- Unabhängigkeit **20 6**
- Unmittelbare Zulieferer **18 316 f.**
- UN-Sanktionen **24 21 ff.**
- Unterlizenzierung **13 5, 14 f., 26**
- Unternehmen im besonderen öffentlichen Interesse (UBI) **14 23**
- Unternehmensethik **16 2**
- Unternehmensführung **16 5, 11, 16 ff., 24, 42, 62**
- Unternehmensgeldbuße **29 55 ff.**
- Unternehmenshaftung **27 80**
- Unternehmenskommunikation **3 66 ff.**
- Unternehmenskultur **1 68**
- Unternehmensleitbild („Mission Statement“) **1 70**
- Unternehmensorganisationspflichten **1 38, 41**
- Unternehmensstabilisierungs- und -restrukturierungsgesetz *s. StaRUG*
- Unternehmensstrafrecht **2 114 ff.**
- Unternehmensstrategie **1 55**
- Unternehmerische Entscheidung **13 11, 88**
- Unterrichtungspflicht an die Steuerabteilung **29 66 ff.**
- Untersuchungsplan **8 34, 90 ff., 94, 96, 108 f.**
- Untersuchungsunterlagen **8 79 ff.**
- Untreue **2 99 ff.**
 - Bildung schwarzer Kassen **2 101**
- Unzuverlässigkeit **14 73**
- UP KRITIS **14 19**
- Ursache-Wirkungs-Diagramm **9 54**
- US-Exportkontrollrecht **25 12 ff., 31**
- US-Re-Exportkontrolle **25 12**
- US-Sanktionen **24 119**
- UWG *s. Gesetz gegen den unlauteren Wettbewerb*
- Value-at-Risk-Modelle **21 14**
- VDS-Richtlinie 3472 **14 103**
- Verantwortliche Stelle **12 31, 47 f.**
- Verantwortlichkeit
 - Aufsichtsrat **2 125 ff.**
 - Compliance Officer **2 122 ff.**
 - Delegation **2 119**
 - Geschäftsleitung **2 116 ff.**
 - Gremienentscheidungen **2 117**
 - Organisationsherrschaft **2 129 ff.**
 - Organisationsverschulden **2 114, 131**
 - strafrechtliche **2 114 ff.; 30 11**
- Verarbeitungsverzeichnis **12 95**
- Verbände **27 35**
- Verbandsgeldbuße **2 13, 157 ff.; 29 55**
- Verbandssanktionengesetz (VerSanG) **1 58; 2 16; 8 2, 105; 15 35**
- Verbesserung von Strukturen und Prozessen **1 99**
- Verbringung **25 22 ff.**
- Verdachtskündigung **12 232**
- Verdachtsmeldungen **23 50, 71**
- Verdeckte Gewinnausschüttungen **29 20**
- Vergabeausschluss **2 172 ff., 181, 185**
- Vergaberecht **30 1 ff.**
 - Insolvenz und Liquidation **30 19 ff.**
 - Interessenkonflikt **30 25**

- mangelhafte Leistung bei Ausführung früherer Aufträge **30 27**
- schwere Verfehlung im Rahmen beruflicher Tätigkeit **30 21**
- schwerwiegende Täuschung bei Eignungsprüfung **30 28**
- unzulässige Einflussnahme **30 30**
- Verstöße gegen Steuer- und Abgabentatbestände **30 15**
- Verstöße gegen umwelt-, sozial- oder arbeitsrechtliche Verpflichtungen **30 18**
- Vorbefassung **30 26**
- Vergabesperre **18 349**
- Vergabeverfahren **30 1 ff.**
 - Anforderungen **30 4 ff.**
 - Ausschlussfristen **30 52 ff.**
 - fakultativer Ausschluss **30 18 ff.**
 - zwingender Ausschluss **30 11 ff.**
 - Selbstreinigung **30 41 ff.**
 - Vergabestelle **30 7 ff., 25, 38, 42, 56**
 - Wettbewerbsregister **30 31 ff.**
- Vergütungssystem, nachhaltiges **21 28**
- Verhältnismäßigkeit **8 36 f.; 12 32 ff., 78**
- Verkehrssicherungspflichten **1 38**
- Verknüpfung von Compliance und Integritätsmanagement **1 72**
- Verletzung rechtlicher Organisationsanforderungen **1 37, 39**
- Verrechtlichung **1 23**
- VerSanG *s. Verbandssanktionengesetz*
- Verschwiegenheit
 - Beschwerdebeauftragte **19 40, 50, 51**
 - Menschenrechtsbeauftragte **19 17, 22, 23**
 - Need-to-know-Basis **19 50**
- Versicherung **8 33; 14 37, 145**
- Versicherungsunternehmen **1 29**
- Verteidigungsunterlagen **8 81, 88**
- Vertragsgestaltung **1 95**
- Vertragsklausel
 - missbräuchliche **13 68 ff.**
- Vertraulichkeit **8 77 ff.; s. auch Verschwiegenheit**
- Vertraulichkeitsvereinbarung **26 14 ff., 39, 43 f.**
- Vertriebsbeschränkungen **27 55 ff.**
- Vertriebsformen **27 57**
 - Alleinbelieferung **27 57**
 - Alleinvertrieb **27 57**
 - Exklusivvertrieb **27 57**
 - Franchising **27 57**
 - selektiver Vertrieb **27 57**
- Vervielfältigung **13 4, 21 f.**
- Vier-Augen-Prinzip **14 66**
- Vier-Schritte-Dialog **6 14**
- Vorstand einer Aktiengesellschaft **14 3, 30, 87, 89**
- Wage Fixing **27 49**
- Wahl eines unternehmensspezifischen Organisationsmodells **1 54 f.**
- Warn- und Meldestruktur des BSI **14 129**
- Warnungen und Empfehlungen **14 42**
- Webinar **6 39; 12 131 ff.**
- Weitergabeklausel **18 336 f.**
- Werte **1 68, 72, 73 ff., 76**
- Werte- und Integritätsmanagement **1 104**
- Wertekultur **20 47**
- Wertpapier-Compliance **20 6**
 - Beauftragter **20 6, 22**
 - interne Revision **20 9**
- Wertpapierhandelsgesetz (WpHG) **21 15**
- Wertpapierhandelsunternehmen **1 28**
- Wertschöpfung **15 14; 16 5; 17 1 ff.**
- Wertschöpfungskette **16 68, 85 f., 90 f., 100 ff.**
- Wertschöpfungsnetzwerk **1 5**
- Wesentlichkeit, doppelte **16 34, 95 ff.**
- Wettbewerbsbeschränkende Vereinbarungen **27 10; 30 23 f.**

- Wettbewerbsbeschränkung
– bewirkte **27** 16
– bezweckte **27** 15
Wettbewerbsregister **2** 172 ff.; **27** 109
Wettbewerbsverbot **27** 58 f.; **26** 71 ff.
Whistleblowing **1** 87; **3** 48, 86, 89
– Begriffsbestimmung **5** 7 f.; **12** 107, 239 f.
Whistleblowing-System *s. Hinweisgebersystem*
Wichtige Einrichtungen **14** 23, 26, 86, 89, 93
Wirksamkeit **20** 6
– des Risikomanagements **18** 325 f.
Wirtschaftliche Einheit **27** 83 f.
Wirtschaftsethik **16** 3
Wirtschaftskriminalität **20** 46
Wirtschaftsprüfer **3** 60 ff.; **8** 15, 55
WpHG *s. Wertpapierhandelsgesetz*
ZAG *s. Zahlungsdiensteaufsichtsgesetz*
Zahlungsdiensteaufsichtsgesetz (ZAG) **14** 64, 74 ff., 130, 137
Zahlungsdienstleister **14** 76 f., 82, 92, 132 ff.
Zahlungsinstitute **14** 28, 80
ZAIT **14** 74, 78, 81 f.
Zeitressourcen **6** 65
Zentrale Stelle **20** 4, 16 ff.
Zertifizierung **29** 92 ff.
Zivilrechtliche Haftung **18** 350
Zulieferer **17** 23 f.
Zweckbindung **12** 40
Zwei-Faktor-Authentifizierung **14** 64