

RECHT WIRTSCHAFT STEUERN

HANDBUCH

Martin R. Schulz (Hrsg.)

Compliance Management im Unternehmen

Erfolgsfaktoren und praktische Umsetzung

2. Auflage

RECHT WIRTSCHAFT STEUERN

Compliance Management im Unternehmen

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; Prof. Dr. Benjamin von Bodungen, LL.M. (Auckland); Dietmar Böhlke, MBA (Warwick); Dr. Marcus Böttger; Dr. Konstantin von Busekist; Juliane Dopychai; Armin Fladung; Prof. Dr. Kai Förstl; Melanie Frankenberger; Dr. Katharina Hastenrath; Dr. Antje Heinen, LL.M., MBA; Sven Jacobs; Dr. Joachim Kaetzler; Prof. Dr. Oliver Keßler; Martin T. Knopp; Till Komma; Dr. Michaela Möhlenbeck; Dr. Oliver Mross; Dr. Manfred Rack; Dr. Christian Rau, LL.M. (Georgetown); Hartmut T. Renz; Frank Romeike; Dr. Christian Scherer; Dr. Martin C. Schleper; Prof. Dr. Martin R. Schulz, LL.M. (Yale); Dr. Tobias Schwartz; Prof. Dr. Daniela Seeliger; Prof. Dr. Christopher Stehr; Dr. Anja Stürzl-Friedlein; Dr. Thomas Uhlig; Dr. Benjamin Ullrich, M.Jur. (Oxford); Klaus G. Walter; Dr. Florian Wettner

2., aktualisierte und erweiterte Auflage 2021

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 9 7 8 - 3 - 8 0 0 5 - 1 7 3 8 - 1

dfv Mediengruppe

© 2021 Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft,
Frankfurt am Main

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 2. Auflage

Compliance und Compliance Management zählen zu den zentralen Themen der Unternehmenspraxis. Denn sie betreffen die Organisation regelkonformen und integren Verhaltens und damit elementare Fragen rechtssicherer und werteorientierter Unternehmensführung. Diese Grundfragen sind für alle Unternehmen und Verbände relevant, da mit nahezu jeder unternehmerischen Tätigkeit vielzählige komplexe rechtliche Anforderungen verbunden sind. Obwohl inzwischen viele Unternehmen und Verbände über Compliance-Programme bzw. Compliance-Management-Systeme (CMS) verfügen, belegen zahlreiche aktuelle Fälle von „Non-Compliance“, dass die Etablierung wirksamer Compliance-Maßnahmen für viele Unternehmen nach wie vor eine veritable Herausforderung bzw. eine kaum lösbare Aufgabe darstellt. Dabei bleibt das regulatorische Umfeld weiterhin dynamisch, die ohnehin kaum noch zu überblickende Zahl rechtlicher Pflichten und Gebote nimmt ständig weiter zu. Seit dem Erscheinungsdatum der 1. Auflage seien exemplarisch nur neue Pflichten nach Umsetzung der EU-DSGVO und dem Geschäftsgeheimnisgesetz genannt, ebenso wie erweiterte Pflichten im Zusammenhang mit IT-Compliance und „Cyber Security“. Vor Herausforderungen stellt viele Unternehmen auch die EU-Whistleblower-Richtlinie, die bis zum 17.12.2021 in deutsches Recht umzusetzen ist. Hinzu kommen erweiterte Anforderungen bei der Kartellrechts-Compliance, der Prävention von Korruption und Geldwäsche sowie der Einhaltung exportkontrollrechtlicher Vorgaben. Zu der Vielzahl bestehender und neuer Rechtspflichten treten zudem verstärkt normative Anforderungen der Stakeholder an eine rechtskonforme und integre Unternehmensführung hinzu, auch in Bezug auf die verschärfte Kontrolle der für die Unternehmen relevanten Wertschöpfungsnetzwerke (wie die Diskussion um das „Lieferketten-Gesetz“ nachhaltig verdeutlicht). Wie die massiven Nachteile und Kosten aufgedeckter „Non-Compliance“ belegen, kann es sich kein Unternehmen mehr leisten, die jeweiligen Compliance-Risiken nicht durch angemessene organisatorische Maßnahmen zu adressieren. Zugleich zeigen neuere Entwicklungen in Gesetzgebung und Rechtsprechung, dass die erfolgreiche Implementierung von Compliance-Maßnahmen für Unternehmen und Verbände vielfältige positive Wirkungen (wie insbesondere das Potenzial zur Sanktionsminderung bei Compliance-Verstößen) haben kann. Der aktuell diskutierte Regierungsentwurf für ein „Verbandssanktionengesetz“ verfolgt ausdrücklich das Ziel, Compliance-Maßnahmen in Verbänden und Unternehmen zu fördern und hierfür normative Anreize zu setzen.

Mit der Neuauflage greifen wir aktuelle Entwicklungen in Gesetzgebung, Rechtsprechung und Rechtswissenschaft auf und zeigen am Beispiel zentraler Compliance-Fragen, wie ein erfolgreiches Compliance Management gelingen kann. Mit seinen vielfältigen Perspektiven und Handlungsempfehlungen aus Wissenschaft und Praxis will das jetzt aktualisiert vorgelegte Handbuch dazu

beitragen, Compliance Management als anspruchsvolle Organisations- und Führungsaufgabe in Unternehmen und Verbänden erfolgreich und nachhaltig zu etablieren.

Mein herzlicher Dank gilt allen Co-Autorinnen und Co-Autoren, welche durch ihre umfangreichen Kenntnisse und Erfahrungen im Umgang mit Compliance-Themen diese Neuauflage ermöglicht haben. Ebenso danke ich Frau Dr. Anette Schunder-Hartung (aHa Strategische Geschäftsentwicklung, Frankfurt am Main) für die Koordination der Autorenbeiträge und ihr erfolgreiches Projektmanagement. Ferner bedanke ich mich herzlich bei Frau Nadine Grüttner und Frau Tanja Brücker, die als Lektorinnen der dfv Mediengruppe das Buchprojekt erneut umfassend und umsichtig betreut haben, sowie – last but not least – bei Herrn Martin Knopp und Frau Gabriele Eller für ihre unermüdliche Hilfe bei der Erstellung der Verzeichnisse.

Heilbronn/Frankfurt am Main, im November 2020

Martin R. Schulz

Autorenverzeichnis

Wolfram Bartschka ist 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. 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 leitet den Zentralbereich „Recht, Compliance und Datenschutz“ bei der Wilh. Werhahn KG in Neuss. Von 2017 bis 2020 war er als Partner für Compliance/Corporate Governance sowie als Mitglied im globalen Steuerungskomitee „Compliance & Investigations“ im Düsseldorf Büro der Bird & Bird LLP tätig. Zuvor führte er von 2006 bis 2016 als Chefsyndikus und CCO den Konzernbereich „Recht und Compliance“ der börsennotierten Wüstenrot & Württembergische AG in Stuttgart.

Professor 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. Seit 2011 ist er neben seiner Anwaltstätigkeit Professor für Bürgerliches Recht sowie deutsches und internationales Arbeits- und Wirtschaftsrecht an der German Graduate School of Management and Law (GGS) in Heilbronn. 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 Co-Chair der globalen Praxisgruppe Data, Privacy & Cyber Security sowie der globalen FinTech Task Force. Sie berät deutsche und internationale Internet-, Technologie- und Medienunternehmen, insbesondere in den Bereichen Digitalisierung, E-Commerce, digitale Zahlungsdienstleistungen, Lizensierungen 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.

Professor Dr. Benjamin von Bodungen, LL.M. (Auckland), ist Professor für deutsches und internationales Handels- und Gesellschaftsrecht, Finanz- und Steuerrecht an der German Graduate School of Management and Law (GGs) in Heilbronn. Zudem ist er als Of Counsel im Bereich Banking & Finance der internationalen Anwaltssozietät Bird & Bird LLP in Frankfurt am Main tätig. In den Bereichen Bank- und Finanzrecht sowie Transport-, Verkehrs- und Außenwirtschaftsrecht hat er zahlreiche Fachveröffentlichungen vorgelegt.

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 Anwaltsgerichtshof des Landes Nordrhein-Westfalen. Er veröffentlicht regelmäßig in den Bereichen Wirtschaftsstrafrecht und Compliance.

Dr. Konstantin von Busekist ist Rechtsanwalt, Steuerberater und Partner bei KPMG Law. Er leitet in der KPMG Law Global den Compliance & Investigation Bereich und berät Vorstände und Aufsichtsräte nationaler sowie internationaler Konzerne – auch außerhalb Deutschlands – in Compliance-Fragen sowie in internationalen Monitor-Verfahren. Er ist vielseitig mit Vorträgen und Veröffentlichungen aktiv, Mitglied des Verwaltungsrates der DICO sowie in Fachbeiräten verschiedener Compliance-Zeitschriften vertreten.

Juliane Dopychai ist Richterin im Bezirk des Oberlandesgerichts Hamm. Zuvor war sie als Rechtsanwältin in der internationalen Wirtschaftskanzlei Bird & Bird LLP am Standort Düsseldorf tätig. Als Mitglied in den Teams von Dr. Michael Jünemann und Carsten Beisheim beriet sie industrieübergreifend nationale und internationale Mandanten im Bereich Compliance und Investigations. Sie ist Autorin verschiedener Fachbeiträge auf diesem Gebiet.

Armin Fladung, RA, DSB, C.O., ist Gründer und Geschäftsführer des CAD-Institut für Compliance, Arbeitsrecht und Datenschutz. Er unterstützt seit über 15 Jahren vor allem mittelständische Unternehmen bei der Einführung von Compliance- und Datenschutz-Managementsystemen insbesondere auch hinsichtlich arbeitsrechtlicher Herausforderungen. Zudem gehört er dem BAVC-Kompetenzteam „Digitalisierung“ an und ist Autor zahlreicher Fachveröffentlichungen.

Prof. Dr. Kai Förstl ist seit Oktober 2020 Professor für Supply Chain Management an EBS Universität für Wirtschaft und Recht in Wiesbaden. Er ist erfolgreicher Autor, Gutachter und Associate Editor in akademischen Fachzeitschriften wie dem Journal of Supply Chain Management, dem Journal of Business Logistics und dem International Journal of Operations & Production Management. In den vergangenen Jahren leitete er Forschungsprojekte im Bereich der Automobil-, sowie der Chemie- & Pharmaindustrie. In Forschung und Lehre befasst er sich mit Fragestellungen des nachhaltigen Supply Chain Managements und der Cross-funktionalen Integration von Unternehmensbereichen im Kontext globaler Liefernetzwerke.

Melanie Frankenberger, CCP, ist Compliance Counsel im Bereich Global Markets Compliance, Global Standards Markets Compliance der Commerzbank AG.

Ihr Beitrag stellt ausschließlich die persönliche Meinung der Verfasserin dar und ist nicht zwingend auch die Auffassung des Arbeitgebers.

Dr. Katharina Hastenrath ist Rechtsanwältin und Dozentin für Compliance und Compliance Management an der Züricher Hochschule für Angewandte Wissenschaften (ZHAW). Daneben berät sie in strategischen und rechtlichen Compliance-Fragen. Zuvor war sie für drei Unternehmen als Compliance Counsel bzw. Chief Compliance Officer tätig. Hastenrath ist Vorstand im „Netzwerk Compliance“, Dozentin an mehreren renommierten Hochschulen sowie in mehreren Fachbeiräten als Compliance-Experte engagiert.

Dr. Antje Heinen, LL.M., MBA ist Group Director Audit der Vaillant GmbH, Remscheid. Zuvor war sie als Leiterin Interne Revision und Compliance der DALLI-Werke GmbH & Co. KG tätig, davor als Rechtsanwältin in der Fachgruppe Kartellrecht der Kanzlei Linklaters LLP in Köln, Brüssel und Düsseldorf. Heinen leitet den Arbeitskreis Mittelstand im Berufsverband Deutsches Institut für Interne Revision e.V. (DIIR) und vertritt den Mittelstand im DIIR-Programmausschuss.

Sven Jacobs arbeitet als Corporate Legal Counsel für Cisco Systems im Bereich IT-Lizenzverträge und regulatorische Marktzugangsbedingungen. Es ist darüber hinaus Lehrbeauftragter für Immaterialgüterrecht an der Hector School des Karlsruhe Institute of Technology und Modulverantwortlicher für IT-Recht an der IUBH Bad Honnef. Des Weiteren ist Sven Jacobs Mitautor eines Kommentars zur Unionsmarkenverordnung und Autor diverser Bücher zu den Themen IT-Compliance und Legal Tech.

Dr. Joachim Kaetzler ist Rechtsanwalt und Partner bei CMS in Frankfurt. Seit 2014 ist er globaler Fachbereichsleiter Banking & Finance. Seit 1999 berät er Unternehmen innerhalb und außerhalb des Finanzsektors in Compliancefragen, insbesondere zur Geldwäsche- und Korruptionsprävention. Er begleitet aktuelle rechtliche Entwicklungen seit vielen Jahren durch Publikationen, Vorträge und Lehrtätigkeit an verschiedenen Hochschulen sowie Bildungseinrichtungen.

Professor Dr. Oliver Keßler ist Professor für Wirtschaftsrecht an der Hochschule Karlsruhe Technik und Wirtschaft. Zuvor hat er über 20 Jahre lang als Rechtsanwalt und Partner führender internationaler Wirtschaftskanleien 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. Zudem lehrt er als Visiting Professor Europäisches Gesellschaftsrecht an der EBS Universität für Wirtschaft und Recht.

Martin T. Knopp ist wissenschaftlicher Mitarbeiter am Institut für Compliance und Unternehmensrecht an der German Graduate School of Management & Law (GGS) in Heilbronn. Er studierte u. a. Recht der internationalen Wirtschaft (LL.M.), Staat und Verwaltung in Europa (LL.M.) und Mediation (MM). Er ist ausgebildeter CSR- und Nachhaltigkeitsmanager (SRH) und Wirtschaftsmediator (CVM/MuCDR). Im Rahmen seiner Forschung befasst er sich im Schwerpunkt mit Corporate Responsibility, Corporate Governance, Corporate Compliance, Corporate Crime und Criminal Compliance.

Till Komma ist Rechtsanwalt bei CMS in 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.

Dr. Michaela Möhlenbeck ist Leiterin Hinweismanagement im Bereich Compliance der Deutschen Bahn, Berlin. Zuvor war sie Rechtsanwältin in einer überörtlichen Sozietät in Dresden/Frankfurt. Möhlenbeck ist darüber hinaus als Lehrbeauftragte an verschiedenen Fachhochschulen und kommunalen Einrichtungen tätig. Sie veröffentlicht regelmäßig u. a. zum Thema Hinweismanagement/Whistleblowing-Systeme sowie zu wirtschaftsstrafrechtlichen Themen.

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), begann seine Berufslaufbahn als Rechtsanwalt bei Freshfields. Stationen bei Johnson & Johnson in Brüssel und New Jersey (Ass. General Counsel und Geschäftsführungsmitglied einer internationalen J&J Tochtergesellschaft) schlossen sich an. 2007 übernahm er den globalen Konzernbereich Recht und Compliance beim Dax-30-Unternehmen Linde AG. Seit 2018 leitet Dr. Rau als Chief Compliance Officer EMEA die Corporate Governance Funktion (Compliance und Datenschutz) des japanischen Medizintechnik- und Optikunternehmens Olympus für Europa, den Mittleren Osten und Afrika.

Hartmut T. Renz ist Syndikusrechtsanwalt und verantwortet als Head of Compliance/Managing Director die Compliance Funktion des deutschen Franchise der Citigroup inklusive der Citigroup Global Markets Europe AG und deren europäische Niederlassungen. Sein Beitrag stellt ausschließlich die persönliche Meinung des Verfassers dar und ist nicht zwingend auch die Auffassung des Arbeitgebers.

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.

Dr. Christian Scherer ist Fachanwalt für Vergaberecht und für Verwaltungsrecht sowie Partner bei CMS in 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.

Dr. Martin C. Schleper ist Associate Professor für Supply Chain Management an der University of Sussex Business School in Brighton, UK. Nach seiner Promotion und Projektleitung an EBS Universität für Wirtschaft und Recht in Wiesbaden arbeitete er an der German Graduate School of Management & Law (GGS) in Heilbronn und an der University of Nottingham, UK. Er ist Autor und Gutachter diverser Fachzeitschriften und forscht u.a. zu Fragestellungen im Bereich des nachhaltigen Supply Chain Managements.

Prof. Dr. Martin R. Schulz, LL.M (Yale), ist seit 2009 Professor für deutsches und internationales Privat- und Unternehmensrecht an der German Graduate School of Management and Law (GGS) in Heilbronn. Er leitet dort das Institut für Compliance und Unternehmensrecht und ist akademischer Direktor des berufsbegleitenden Master-Programms „LL.M. in Business Law“. Seine Publikations- und Tätigkeitsschwerpunkte sind Gesellschaftsrecht, Compliance-Ma-

nagement im Unternehmen sowie Wissensmanagement für Juristen. Zu diesen Themen hat Martin Schulz zahlreiche Beiträge in deutscher und englischer Sprache veröffentlicht; seine aktuellen Forschungs- und Tätigkeitsfelder umfassen u. a. die Wirksamkeit von Compliance-Management-Systemen, Rechtsfragen der digitalen Transformation sowie Wissens- und Innovationsmanagement in Kanzleien. Martin Schulz verfügt zudem über langjährige Erfahrung als Rechtsanwalt und ist neben seiner Hochschultätigkeit als Rechtsanwalt und Of Counsel bei CMS in Frankfurt am Main tätig.

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 Bereich Competition/Antitrust 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), Mitglied der Kommission Wettbewerbsrecht 4.0. des Bundesministeriums für Wirtschaft und Energie und seit Dezember 2018 im Vorstand der Studienvereinigung Kartellrecht e. V. vertreten.

Professor Dr. Christopher Stehr studierte Politik- und Wirtschaftswissenschaften an der Universität von München. 2003 gründete er die Unternehmensberatung 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. Seit Oktober 2010 ist Stehr Professor für Internationales Management an der German Graduate School of Management and Law (GGS) in Heilbronn. 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 und Globalisierung von KMU, CSR und Nachhaltigkeit und Interkulturelle Kompetenz.

Dr. Anja Stürzl-Friedlein, LL.M., ist als Rechtsanwältin in der Sozietät Flick Gocke Schaumburg in Bonn tätig. Sie berät und verteidigt Privatpersonen und Unternehmen im Bereich des Wirtschaftsstrafrechts sowie schwerpunktmäßig im Bereich des Steuerstrafrechts. In diesen Themenbereichen hält sie Vorträge und veröffentlicht regelmäßig Fachbeiträge. Zudem ist sie Vorstandsvorsitzende des Vereins JuWiSt e. V.

Dr. Thomas Uhlig ist seit 2010 als Rechtsanwalt bei KPMG Law im Bereich der rechtlichen Complianceberatung tätig. Er hat langjährige Erfahrung bei der Beratung international tätiger Unternehmen in den Schwerpunkten Compliance- und Governance-Organisation, Produkt Compliance sowie Compliance Risk Assessments. In diesen Kontext hat er zahlreiche nationale und internationale Projekte geleitet. Bei KPMG Law verantwortet er den Bereich Produkt Compliance.

Dr. Benjamin Ullrich, M.Jur (Oxford), ist Rechtsanwalt und Partner der Sozietät Schnittker Möllmann Partners (SMP). SMP ist eine Spezialkanzlei für Steuern, Fonds, Transaktionen, Gesellschaftsrecht und Litigation. Er ist spezialisiert auf Corporate Compliance sowie M&A- und Venture-Capital-Transaktionen. Im JUVE-Handbuch Wirtschaftskanzleien wird er als „stark in Transaktionen“ und als einer der 20 führenden Berater in Deutschland im Bereich Venture Capital genannt.

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 & Dannenfeldt tätig. Walter verteidigt und berät seine Mandanten schwerpunktmäßig im Korruptionstrafrecht 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).

Inhaltsverzeichnis

Vorwort.....	V
Abkürzungsverzeichnis.....	XLV

Teil 1

Grundlagen, Erfolgsfaktoren und Handlungsstrategien

1. Kapitel

Compliance Management – Grundlagen, Orientierungshilfen und Erfolgsfaktoren

(Schulz)

I. Grundlagen und Zusammenhänge.....	1
1. Bedeutung von Compliance und positive Wirkung von Compliance Management.....	1
2. Compliance Management als Inbegriff rechtskonformer Verbandsorganisation.....	3
3. Risiken und Nachteile von Regelverletzungen und „Non-Compliance“.....	4
4. Funktionen von Compliance und Compliance Management.....	6
5. Permanente Aufgabe im dynamischen regulatorischen Umfeld... ..	8
6. Erweiterung von Organisationspflichten durch Gerichte.....	11
7. Beachtung von Compliance-Anforderungen anderer Rechtsordnungen.....	12
8. Compliance Management im Kontext aktueller Entwicklungen von Corporate Governance und Corporate Social Responsibility .	12
9. Verbindungslinien zum Reputationsmanagement.....	14
II. Vorgaben und Orientierungshilfen für Compliance Management ...	16
1. Compliance-Organisationspflicht als verbandsübergreifende Ausprägung der Leitungsverantwortung.....	16
2. Individuelle Ausgestaltung des Compliance Managements.....	17
3. Vielfalt an Vorgaben und Orientierungshilfen.....	18
a) Branchenspezifische Sonderregeln als Erkenntnisquelle.....	19
b) Erkenntnisse des Risikomanagements.....	21
aa) Besonderheiten von Compliance-Risiken.....	21
bb) Berücksichtigung integrativer Perspektiven (Beispiel GRC-Ansatz).....	23
c) Anforderungen an Aufsichts- und Überwachungsmaßnahmen.	24
d) Vorgaben der Unternehmensorganisationspflichten und Garantenpflichten.....	24

e) Beispiele von Leitfäden anderer Rechtsordnungen.....	25
aa) UK Bribery Act (Vereinigtes Königreich).....	25
bb) Leitfaden des Department of Justice (USA).....	26
f) Compliance-Standards als Orientierungshilfe (Beispiel IDW PS 980).....	27
III. Erfolgsfaktoren für ein wirksames Compliance Management	28
1. Gestaltungsermessen bei Strukturen, Prozessen und Systemen....	29
2. Konzeption einer individuellen Compliance-Strategie	29
a) Fokussierung auf effektive Compliance-Maßnahmen	30
b) Wahl eines unternehmensspezifischen Organisationsmodells ..	31
c) Ermittlung des besonderen Compliance-Risikoprofils	32
aa) Systematische Identifikation von Compliance-Risiken ...	33
bb) Analyse und Bewertung.....	34
cc) Entwicklung von Risikosteuerungsmaßnahmen.....	34
dd) Berichterstattung zu Compliance-Risiken.....	35
ee) Regelmäßige Compliance-Audits	35
d) Klärung von Zuständigkeiten und Delegationsfragen	36
e) Eigenständige und unabhängige Positionierung der Compliance Officer.....	37
f) Förderung und Incentivierung von Regeltreue (Compliance-Kultur).....	38
aa) Compliance Commitment durch die Unternehmens- und Verbandsleitung	39
bb) Akzeptanz von Compliance-Maßnahmen als Grundlage der Befolgung	40
cc) Kommunikation von Werten für Regelungslücken und „Graubereiche“	42
3. Verfassung von Regeln, Richtlinien und Werten.....	43
4. Compliance als Personalführungs- und Schulungsaufgabe	44
a) Zielgruppenorientierte Schulungs- und Fortbildungs- programme	44
aa) Bedarfsanalyse und Zielgruppenorientierung	44
bb) Positionierung von Compliance als „Business enabler“....	44
cc) Aktualisierung und Anpassung der Fortbildungsformate ...	45
dd) Aktive Einbeziehung der Unternehmensangehörigen.....	45
b) Anreize für Compliance	45
5. Integration von Compliance-Themen in die Geschäftsprozesse ...	46
6. Koordination der Zusammenarbeit mit anderen Unternehmens- funktionen.....	47
7. Einrichtung von wirksamen Kontrollen und Feedback- Prozessen	47
8. Aufklärung von Verstößen und Bedeutung von Hinweisgeber- systemen	48
9. Konsequente Sanktionierung von regelwidrigem Verhalten.....	49

10. „Legal Monitoring“ und regelmäßige Aktualisierung	49
11. Angemessene Dokumentation	50
IV. Vorteile eines effektiven Compliance Managements	50
1. Prävention und Reduzierung der Kostenrisiken und Nachteile von „Non-Compliance“	50
2. Schutz von Unternehmen, Leitungsorganen und Unternehmensangehörigen	50
3. Sicherung der Reputation und Vertrauenserhalt der Stakeholder ..	51
4. Eröffnung und Wahrung rechtlicher Chancen und Gestaltungsoptionen	51
5. Vorteile beim Marketing und im Wettbewerb	52
6. Verteidigungsmöglichkeiten bei „Non-Compliance“	52
7. Verbesserung von Strukturen und Prozessen	52
V. Zusammenfassung und Empfehlungen	53

2. Kapitel

Compliance Management und Strafrecht

(Böttger)

I. Einführung in die Criminal Compliance	57
II. Strafrechtliche Grundlagen der Compliance-Verpflichtung	65
III. Typische strafrechtliche Compliance-Risiken	69
1. Korruption	71
a) Vorteilsgewährung (§ 333 StGB)	75
b) Bestechung (§ 334 StGB)	82
c) Bestechung von Mandatsträgern (§ 108e StGB)	84
d) Bestechung im geschäftlichen Verkehr (§ 299 Abs. 2 StGB) ..	86
e) Bestechlichkeit im geschäftlichen Verkehr (§ 299 Abs. 1 StGB)	91
f) Bestechung im Gesundheitswesen (§ 299b StGB)	91
g) Auslandskorruption	93
h) Korruptionsdelikte im weiteren Sinne	98
2. Untreue (§ 266 StGB)	99
a) Generierung von Bestechungsgeld	100
b) Zahlung von Bestechungsgeld	101
3. Steuerverkürzung (§§ 370 ff. AO)	103
IV. Strafrechtliche Risiken der Non-Compliance für die Verantwortlichen des Unternehmens	105
1. Originäre strafrechtliche Verantwortlichkeit	105
a) Verantwortlichkeit der Geschäftsleitung	107
b) Gremienentscheidungen	107

c) Delegation von Verantwortungsbereichen	108
d) Verantwortlichkeit des Compliance Officers	111
e) Aufsichtsrat	113
2. Innerbetriebliche Anweisungen/Täterschaft kraft Organisations- herrschaft	115
3. Fahrlässigkeitshaftung (sog. Organisationsverschulden)	116
4. Verletzung der Aufsichtspflicht in Betrieben und Unternehmen (§ 130 OWiG)	116
V. Strafrechtliche Risiken der Non-Compliance für das Unternehmen	120
1. (Unternehmens-)Strafrecht	120
a) Überblick	120
b) Verbandssanktionengesetz	121
c) Einziehung	124
c) Das Unternehmen als Nebenbeteiligter im Strafverfahren	126
2. Ordnungswidrigkeitenrecht	127
a) Unternehmensgeldbuße 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 ..	130
1. Blacklisting und Vergabesperren	130
a) Registereintragungen	130
aa) Bundeszentralregister	130
bb) Gewerbezentralregister	131
cc) Vergabe- bzw. Wettbewerbsregister	132
dd) Verbandssanktionenregister	134
ee) Sonstige Register	134
b) Vergaberechtliche Konsequenzen	134
2. Inhabilität (§§ 70 StGB, 6 GmbHG, 76 AktG)	136
3. Aufsichtsrechtliche Konsequenzen	137
VII. Strafrechtliche Risiken innerhalb des Compliance-Prozesses („failed compliance“)	138

3. Kapitel

Compliance Management als Schnittstellenaufgabe – Überlegungen und Anregungen 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	153
5. Betriebsrat	155
6. Finanzfunktion	156
7. Innenrevision	157
8. Wirtschaftsprüfer	159
9. Unternehmenskommunikation	160
10. Andere	162
11. Fallbeispiel	163
III. Fazit	165

4. Kapitel

Einführung eines „Code of Conduct“

(Benkert)

I. Einleitung	169
II. Ausgestaltung	170
1. Erscheinungsformen	170
2. Typische Regelungen	173
III. Einführung eines „Code of Conduct“	175
1. Individualvertragliche Umsetzung	175
a) Weisungsrecht des Arbeitgebers	175
b) Vertragliche Vereinbarung	177
c) Änderungskündigung	179
2. Betriebsvereinbarung	179
IV. Datenschutzrechtliche Implikation	182
V. Mitbestimmungsrecht des Betriebsrats	183

5. Kapitel

Whistleblowing-Systeme – Aufbau und Management

(Möhlenbeck)

I. Einleitung	187
1. Begriffsbestimmung	188
2. Gründe für die Einführung eines Whistleblowing-Systems	189
3. Aktuelle Rechtliche Rahmenbedingungen	190

a) Internationale Anforderungen	190
aa) Sarbanes Oxley Act (SOX) (USA)	190
bb) Dodd-Frank Act (USA)	191
cc) UK Bribery Act (Großbritannien)	192
dd) OECD-Übereinkommen vom 17.12.1997	193
b) Aktuelle Rechtslage in Deutschland	194
aa) Gesellschaftsrechtliche Vorgaben	195
bb) Ordnungswidrigkeitenrechtliche Vorgaben	195
cc) Vorgaben des Deutschen Corporate Governance Kodex.	195
dd) Vorgaben aus der Rechtsprechung.	196
II. Die neuen Vorgaben der EU-Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden	197
1. Ziel der Richtlinie	197
2. Überblick über den Inhalt der Richtlinie	197
3. Sachlicher Anwendungsbereich	198
4. Persönlicher Anwendungsbereich der Richtlinie	199
5. Voraussetzungen für den Schutz von Hinweisgebern.	200
a) Gemeinsame Schutzvoraussetzungen	201
b) Besondere Voraussetzung in Abhängigkeit von dem gewählten Meldeweg	202
aa) Interne Meldungen gemäß Art. 7 WBRL	202
bb) Externe Meldungen gemäß Art. 9 WBRL	203
cc) Offenlegung gemäß Art. 15 WBRL	204
6. Pflicht zur Einrichtung eines internen Hinweismanagement- systems	205
a) Juristische Personen des privaten Sektors	205
b) Juristische Personen des öffentlichen Sektors	205
7. Anforderungen der Richtlinie an ein internes Hinweismanagement- system	206
a) Wahrung der Vertraulichkeit	206
b) Meldewege	206
c) Bearbeitung der eingehenden Meldungen.	207
8. Pflicht zur Einrichtung externer Meldekanäle.	208
9. Vorschriften/Anforderungen an den Umgang mit internen und externen Meldungen	209
10. Schutzmaßnahmen	210
a) Verbot von Repressalien	210
b) Maßnahmen zum Schutz betroffener Personen	212
c) Sanktionen bei Verstößen.	212
11. Umsetzung in nationales Recht durch den deutschen Gesetzgeber.	212
III. Überblick über die mögliche Ausgestaltung von Hinweis- managementsystemen	213
1. Externes Whistleblowing.	213

2. Internes Whistleblowing	214
3. Mögliche Begrenzungen (Hinweisgeber, Empfänger, Themen) ..	214
IV. Aufbau/Einführung eines Hinweismanagementsystems	214
1. Allgemeine rechtliche Anforderungen	214
a) Rechtslage in Deutschland	214
b) Vorgaben auf europäischer Ebene	216
c) Regelungen in den USA und Großbritannien	216
aa) USA	216
bb) Großbritannien	216
2. Datenschutzrechtliche Regelungen	217
3. Entscheidungen hinsichtlich der konkreten Ausgestaltung	218
a) Organisation	218
b) Ausgestaltungsmöglichkeiten	218
aa) Kreis der Hinweisgeber	219
bb) Eingangskanäle	219
cc) Arten der meldbaren Verstöße	221
dd) Regelungen zur Einführung eines Hinweismanagement-	
systems	221
4. Kommunikation	222
V. Die praktische Arbeit mit einem Whistleblowing-System	223
1. Schutz des Hinweisgebers vor Nachteilen	223
2. Schutz des Betroffenen	224
3. Datenschutzkonformer Umgang mit eingegangenen Hinweisen ..	224
VI. Fazit	225

6. Kapitel

Kommunikationsmanagement und Schulungen

(Hastenrath)

I. Einleitung	227
II. Grundzüge zur Kommunikation in der Unternehmenspraxis	227
1. Relevanz der Kommunikation im Unternehmen und bei	
Compliance	227
2. Kommunikationsmodelle	229
a) Modell zu Konfliktarten als Grundlage für die Kommunikation	230
b) Praxisrelevantes Beispiel	232
III. Ausgewählte Instrumente der Compliance-Kommunikation	234
1. Tone-From-The-Top	234
2. Persönlicher Kontakt mit dem Compliance Officer	235
3. Zusammenarbeit des Compliance Officers mit Schlüssel-	
funktionen im Unternehmen	235

4. Schriftliche Informationen an die Mitarbeiter	236
5. Compliance im firmeneigenen Intranet	236
IV. Schulungen	237
1. Persönliche Schulungen durch die Compliance-Funktion	237
2. Schulungen mit klassischem E-Learning	238
3. Digitale Schulungen: Schulungen mit Webinaren, Podcasts, Livestreams oder vertonten Präsentationen	239
4. Unterstützung dezentraler Compliance-Funktionen: das Schulungshandbuch	252
V. Die „Top 5 Stolpersteine“ in der Compliance- Kommunikation und Lösungsvorschläge	254
1. Fehlende, verspätete oder missverständliche Information	254
a) Problemstellung	254
b) Lösungsvorschlag	254
2. Mangelnde Authentizität („Nicht gelebte Hochglanzaussagen“) ..	255
a) Problemstellung	255
b) Lösungsvorschlag	256
3. Fehler im Kommunikationsmanagement: Budget- und Ressourcenmangel	257
a) Problemstellung	257
aa) Unzureichende Übersetzung eines Code of Conduct (CoC)	258
bb) Unzureichendes Schulungsbudget	259
b) Lösungsvorschlag	259
4. Probleme mit der Technik	260
a) Problemstellung	260
b) Lösungsvorschlag	261
5. Fehler im Kommunikationsmanagement von Compliance aufgrund von Kulturunterschieden	262
a) Problemstellung	262
b) Lösungsvorschlag	263
VI. Fazit zur Compliance-Kommunikation	264

7. Kapitel

**Auswirkungen des ISO-Standards 19600 auf die Prüfung von
Compliance-Management-Systemen nach IDW PS 980**

(von Busekist/Uhlig)

I. Einleitung	267
II. Zielsetzung und Zielgruppe	268
1. Ausgangslage	268
2. Zielsetzung des IDW PS 980	268

3. Zielsetzung des ISO 19600:2014	268
4. Vergleich	269
5. Ausblick auf ISO 37301	269
III. Unterschiedliche Regelungstiefe zur Ausgestaltung des CMS	269
1. CMS-bezogene Regelungsinhalte des IDW PS 980	269
2. Regelungsinhalte des ISO 19600:2014	270
IV. ISO 19600 als geeignetes, angemessenes Rahmenkonzept für ein CMS	273
1. Anforderungen des IDW PS 980 an ein Rahmenkonzept	273
2. Vergleich ISO 19600 Guidelines mit IDW PS 980-Grundelementen	274
V. Zwischenergebnis	276
VI. Argumente für eine Ausrichtung des CMS nach ISO 19600	276
1. Basis für Ermessensentscheidung und Compliance-Richtlinie	276
2. Beurteilung der angemessenen Einrichtung eines wirksamen CMS	279
VII. Zusammenfassung	280

8. Kapitel

Management interner Untersuchungen

(Wettner/Walter)

I. Einleitung	281
II. Entscheidung über die Durchführung interner Untersuchungen	282
1. Entscheidungsbefugte Stellen	282
2. Pflicht zur Aufklärung konkreter Verdachtsfälle	283
3. Interne Untersuchung oder externe Ermittlung?	284
a) Bereits laufendes behördliches Verfahren	284
b) (Noch) kein behördliches Verfahren	286
III. Vornahme von Eilmaßnahmen	287
1. Einrichtung einer zentralen Koordinierungsstelle	287
2. Maßnahmen der Daten- und Beweissicherung	288
3. Arbeitsrechtliche Maßnahmen	288
4. Beachtung von Informations- und Berichtspflichten	288
IV. Planung der internen Untersuchung	289
1. Grundlagen der Planung	289
a) Beachtung von Recht- und Verhältnismäßigkeit	290
b) Beachtung von Risiken und Folgen der internen Untersuchung	290
2. Festlegung des Untersuchungsgegenstands	292

3. Bestimmung des Untersuchungsteams und der Verantwortlichkeiten.	292
a) Auswahl von Mitarbeitern und externen Beratern.	293
b) Festlegung von Verantwortlichkeiten und Berichtswegen.	294
4. Bestimmung und Vorbereitung der Informationsquellen.	294
a) Relevante Informationsquellen.	294
aa) Dokumente.	295
bb) Elektronische Daten und E-Mails.	295
cc) (Ehemalige) Mitarbeiter.	295
b) Notwendige Abstimmung der geplanten Untersuchungsmaßnahmen.	296
aa) Beteiligung von Betriebsrat oder Sprecherausschuss.	296
bb) Abstimmung mit Ermittlungs- und Aufsichtsbehörden.	296
c) Einrichtung eines Datenraums oder eines „Projektportals“.	297
5. Sicherung der Vertraulichkeit.	298
a) Zugriffsmöglichkeiten Dritter.	298
aa) Beschlagnahme durch Ermittlungsbehörden.	298
bb) Herausgabe von Unterlagen an Versicherer.	300
b) Begrenzung der E-Mail- und sonstigen schriftlichen Kommunikation.	301
c) Kennzeichnung und Aufbewahrung geschützter Kommunikation.	301
6. Erstellen eines Untersuchungsplans.	302
V. Durchführung der internen Untersuchung.	302
1. Allgemeine Untersuchungsgrundsätze.	302
2. Dokumentation der Untersuchung.	303
3. Erhebung und Auswertung von Dokumenten.	304
4. Erhebung und Auswertung von elektronischen Daten.	305
5. Befragung von Mitarbeitern.	305
6. Auswertung und Aufarbeitung der Untersuchungsergebnisse.	308
VI. Fazit.	309

Teil 2

Übergreifende Themen und Herausforderungen

9. Kapitel

**Risiko- und Chancenmanagement –
Erfolgsfaktoren für eine wirksame Umsetzung**

(Romeike)

I. Corporate Governance und das Management von Chancen und Risiken.	311
--	-----

II. Abgrenzung des Risiko- und Chancenbegriffs	314
III. Nutzen eines wirksamen Chancen- und Risikomanagements	317
IV. Unterscheidung von Ursachen – Risiken – Wirkungen.	318
V. Verknüpfung von Risikomanagement und Strategie	320
VI. Der Risikomanagement-Prozess als Regelkreis	322
VII. Methoden zur Risikoidentifikation und -bewertung	325
VIII. Aggregation von Risiken.	328
IX. Maßnahmen zur Risikosteuerung	329
X. Unterschiedliche Reifegrade im Risikomanagement	331
XI. Fazit und Ausblick	332

10. Kapitel

**Governance, Risk und Compliance im Mittelstand –
Zusammenhänge und Abhängigkeiten**

(Bartuschka)

I. Einleitung – Die Notwendigkeit der Einrichtung von Instrumenten zur Überwachung von Unternehmen	337
II. Das System der Unternehmensüberwachung	339
1. Überblick über das Gesamtsystem	339
2. Externe Komponenten der Unternehmensüberwachung	340
3. Interne Komponenten der Unternehmensüberwachung	341
III. Die Verknüpfung der einzelnen Elemente der Unternehmens- überwachung	342
1. Der GRC-Ansatz	342
2. Das interne Kontrollsystem und die anderen Elemente der Überwachung des Unternehmens.	344
3. Compliance- und Risikomanagement	345
4. Risikomanagement und Controlling	345
5. Interne Revision, Compliance und Risikomanagement	346
6. Fazit	347
IV. Grundkonzept für die Ausgestaltung eines integrierten Systems der Überwachung für mittelständisch geprägte Unternehmen	347
1. Bestimmung der Zielgruppe der Unternehmen	347
2. Zielstellung für die Einführung eines integrierten Systems der Überwachung	348

3. Vorgehensweise	348
a) Risikoanalyse	348
b) Analyse bestehender Strukturen	349
c) Ermittlung des Anpassungsbedarfs	349
d) Umsetzung	350
4. Fazit	352

11. Kapitel

Datenschutz im Compliance Management

(Becker/Böhlke/Fladung)

I. Einleitung	353
II. Der konzeptionelle Schutz personenbezogener Daten	357
1. Gesetzliche Grundlagen	357
a) Datenschutzgrundverordnung	357
b) Bundesdatenschutzgesetz	358
c) Landesdatenschutzgesetz	358
d) Europäische Richtlinien	359
e) Weitere Gesetze mit datenschutzrechtlichen Vorgaben	359
2. Zentrale Grundsätze	361
a) Verbot mit Erlaubnisvorbehalt	361
b) Prinzip der Verhältnismäßigkeit	363
c) Datensparsamkeit	364
d) Transparenz	364
e) Zweckbindung	365
3. Grundbegriffe	365
a) Personenbezogene Daten	365
b) Verantwortliche Stelle	366
c) Umgang mit personenbezogenen Daten	367
aa) Erheben	367
bb) Speichern	368
cc) Verändern	368
dd) Übermitteln	368
d) Auftragsverarbeitung	371
III. Betrieblicher Datenschutz	372
1. Pragmatischer Ansatz: Wo fange ich an?	372
2. Beratungspraxis	376
a) Der betriebliche Datenschutzbeauftragte	379
b) Prozess der Datenschutzberatung	381
c) Praxisrelevante Beispiele	384
3. Implementierung	386
4. Zusammenarbeit mit Behörden	389

IV. Instrumente der datenschutzrechtlichen Compliance	390
1. Tone-from-the-Top	390
2. Interne Richtlinien	391
a) Datenschutzrichtlinie	391
b) IT-Nutzungsrichtlinie	391
c) E-Mail-Policy	392
d) Social-Media und Messaging-Dienste	393
e) IT-Datenschutzmanagement-Richtlinie (Datenschutz- managementkonzept)	393
f) Archivierungs- und Lösungsrichtlinie	394
3. Verzeichnis von Verarbeitungstätigkeiten	395
4. Interne Kommunikation und Awareness	396
a) Der Datenschutz-Newsletter	396
b) Intranet	397
c) Der „Datenschutz-Tag“ und Fachtagungen	397
5. Schulungen	397
a) Persönliche Schulungen	398
b) E-Learning/Webinars	400
c) Unterstützung dezentraler Compliance-Funktionen	400
V. Effektive Datenschutzüberwachung	401
1. Audits und Maßnahmenpläne/Quick Self-Assessment	401
2. IT-Infrastruktur-Reviews und Koordinierung mit IT Security	403
3. Incident- und Regel-Reporting aus den Betrieben	404
4. Der Datenschutzjahresbericht	404
5. Bericht an Aufsichtsrat/Compliance-Bericht/Audit Committee	405
6. Zusammenarbeit mit dem Compliance Officer, IT-Security und Revision	405
VI. Beschäftigtendatenschutz	408
1. Bedeutung des Beschäftigtendatenschutzes für Compliance	408
2. Rechtsgrundlagen für den Umgang mit Mitarbeiterdaten	411
a) Kollektivvereinbarungen zur Nutzung von Mitarbeiterdaten ..	411
b) Rechtfertigende Einwilligung des Mitarbeiters	413
c) Arbeitsvertragliche Regelungsmöglichkeiten	414
d) Gesetzliche Erlaubnistatbestände	416
e) Internationaler Datenverkehr mit Beschäftigtendaten	418
3. Risiken beim Umgang mit Beschäftigtendaten	419
a) Phase 1: Begründung des Arbeitsverhältnisses/ „Boarding-Phase“	419
b) Phase 2: Durchführung des Arbeitsverhältnisses/ „On Board-Phase“	420
c) Phase 3: Beendigung des Arbeitsverhältnisses/ „Off Boarding-Phase“	421
4. Zusammenarbeit mit dem Betriebsrat	422

5. Personalleiter und Betriebsrat als Teil des Datenschutz- und Compliance-Teams	423
6. Hinweise, Muster und Beispielsfall	425
a) Hinweise zur Regelung der Nutzung von Beschäftigtendaten . .	425
b) Hinweise zur Regelung der Nutzung von Internet und E-Mail . .	427
c) Beispielsfall zur Kontrolle bei Verdacht gegen Mitarbeiter	430
d) Beispielsfall zum Auskunftsrecht eines Mitarbeiters bei Untersuchungen von Compliance-Verstößen	432
VII. Fazit	434

12. Kapitel

**IT-Compliance – Software-Lizenzmanagement,
IT-Sicherheit und Blockchain**

(Jacobs)

I. Rechtliche Herausforderungen der fortschreitenden Digitalisierung und Vernetzung	437
II. Software-Lizenzmanagement	438
1. Rechtliche Grundlagen der Nutzung von Computerprogrammen . .	439
2. Besondere Arten von Software, insbesondere Open-Source-Software	440
3. Software-Lizenzmanagement im Rahmen verantwortungsbewusster Unternehmensführung	441
4. Rechtsfolgen einer Unterlizenzierung	442
III. Software-Lizenzmanagement im Rahmen von Cloud- Diensten	442
1. Nutzungshandlungen beim Cloud Computing	442
a) Recht der öffentlichen Zugänglichmachung der Software	443
b) Recht zur Vervielfältigung der Software	444
2. Lizenzmanagement im Zusammenhang mit Cloud Computing-Diensten	444
IV. Rechtsrahmen von Softwarelizenz-Audits	445
1. Rechtliche Grundlagen für einen Softwarelizenz-Audit	446
2. Vertragliche Ausgestaltung eines Softwarelizenz-Audits	447
V. IT-Sicherheit	448
1. Das IT-Sicherheitsgesetz	448
2. Die Vorgaben der EU-Datenschutz-Grundverordnung	449
3. Adressaten der Pflichten zur IT-Sicherheit	451
VI. Blockchain und Smart Contracts	452
1. Was ist die „Blockkette“?	452
2. Rechtliche Herausforderungen und Compliance-Themen	453

VII. Implementierung eines IT-Compliance-Systems	453
1. Risikoanalyse und Grundlagen eines Lizenzmanagement-Systems	453
2. Richtlinie zur IT-Sicherheit	455
3. Der IT-Sicherheitsbeauftragte	455

13. Kapitel

Cybersecurity, IT-Sicherheit und Krisenmanagement

(Bensinger)

I. Analyse	457
1. Ziele der IT-Sicherheit	457
2. Cybercrime im Wandel	458
a) Ideelle Hintergründe	459
b) Materielle Hintergründe	461
3. Entwicklungen bei Schutzmaßnahmen	462
II. Vorbeugende Maßnahmen	462
1. Adressaten	463
a) KRITIS-Betreiber	463
b) Anbieter von Telemediendiensten	465
c) Anbieter von Telekommunikationsdiensten	465
d) Bank- und Finanzwesen	465
e) Energiewirtschaft	466
f) Geschäftsführung von Aktiengesellschaften und GmbHs	466
2. Inhalt der gesetzlichen Verpflichtungen	466
a) BSIG	468
aa) Pflichten der KRITIS-Betreiber	468
bb) Befugnisse des BSI	470
b) DSGVO	471
c) BDSG	477
d) TMG und TKG	477
aa) TMG	477
bb) TKG	478
cc) Verhältnis zur DSGVO	478
e) KWG, ZAG, MaRisk und MaSI	479
aa) MaRisk (Mindestanforderungen an das Risikomanagement)	480
bb) ZAG und MaSI	484
cc) § 27 Abs. 1 ZAG	486
dd) Konkurrenz zum BSIG	486
f) EnWG	486
g) NIS-Richtlinie	487
h) §§ 76, 91, 93 AktG	487
aa) Ausgestaltung des IT-Risikomanagementsystems	489

bb) Anforderungen nach DSGVO	491
cc) Verantwortungsverteilung innerhalb der Geschäftsleitung	492
dd) Dokumentationspflicht	493
3. Unternehmensinterne Vorkehrungen.....	493
a) Interne Vorgaben	493
b) Aktuelle technisch-organisatorische Schutzmaßnahmen.....	494
III. Der Krisenfall	496
1. Hacker-Angriffe erkennen.....	496
2. Rechtliche Konsequenzen und Handlungsoptionen	496
a) Melde- und Informationspflichten	496
aa) DSGVO.....	496
bb) BDSG	502
cc) BSIG	502
dd) Meldepflichten für Energiewirtschaftsunternehmen	504
ee) ZAG.....	504
ff) Meldepflichten für Energiewirtschaftsunternehmen	506
gg) TMG	506
hh) TKG.....	507
ff) Sonstige Informationspflichten	507
b) Werkzeuge zur Abwehr von Cyberangriffen	508
3. Interne und externe Kommunikation.....	509
4. Mittel- und längerfristige Maßnahmen.....	510
IV. Ausblick.....	510

14. Kapitel

**Corporate Social Responsibility und Corporate Compliance –
Die gesellschaftliche und juristische Verantwortung von Unternehmen**

(Stehr/Knopp)

I. Einführung	511
1. „Shareholder Value“ und „Stakeholder Value“ – eine „Mission Impossible“?	511
2. CSR und Unternehmensführung – Auswirkungen auf die Unternehmen?	512
3. CSR und Unternehmensführung – Auswirkungen auf die Compliance?.....	513
II. Grundlagen	515
1. Corporate Social Responsibility.....	515
a) Bedeutungswandel des Begriffsverständnisses	515
b) Konzeptionen und Modelle	515
c) Definitionen	517

2. Corporate Governance	518
a) Begriffsverständnis.....	518
b) Corporate Governance und Corporate Social Responsibility ..	519
c) Gesellschaftsrecht und Deutscher Corporate Governance Kodex	520
3. Corporate Compliance	523
a) Begriffsverständnis.....	523
b) Corporate Compliance und Corporate Governance.....	524
c) Corporate Compliance als Organisationspflicht.....	524
d) Implikationen durch ein „Verbandssanktionengesetz“	525
III. Corporate Social Responsibility und Regulierung.....	526
1. Einführung in die CSR-Regulierung	526
a) Regulierungsebenen.....	526
b) Regulierungsansätze	526
c) Rechtsqualität	527
d) Reputationsmanagement	528
2. Beispiele für CSR-Regulierung.....	528
a) Globale Regulierungsebene	528
aa) OECD-Leitlinien für multinationale Unternehmen	528
bb) GRI-Berichtsstandards.....	529
cc) UN Global Compact	529
dd) ISO 26000.....	530
b) Internationale Regulierungsebene.....	531
c) Supranationale bzw. europäische Regulierungsebene.....	532
d) Nationale bzw. deutsche Regulierungsebene	533
3. CSR-Normenflut als Herausforderung für Unternehmen	534
IV. Corporate Social Responsibility und Corporate Compliance	536
1. Einführung.....	536
2. Allgemeine Relevanz von CSR-Normen für die Corporate Compliance	539
3. Konkrete Relevanz von CSR-Normen sowie sonstiger CSR-Themen für die Corporate Compliance.....	539
a) CSR-Normen und CSR-Themen im Compliance-Risiko- managementprozess.....	540
aa) Schritt 1: Definition der CSR-Compliance-Risiken.....	540
bb) Schritt 2: Identifikation der CSR-Compliance-Risiken....	541
cc) Schritt 3: Analyse und Bewertung der CSR-Compliance-Risiken	541
dd) Schritt 4: Berichterstattung der CSR-Compliance-Risiken	542
ee) Schritt 5: Steuerung der CSR-Compliance-Risiken.....	543
ff) Schritt 6: CSR-Compliance-Risikomonitoring.....	543
b) Verknüpfung von CSR- und Compliance-Risiken	543
V. Zusammenfassung	543

15. Kapitel

CSR-Compliance: Herausforderungen des CSR-Reportings

(Beisheim/Dopychai)

I. Einleitung: Corporate Social Responsibility, Corporate Governance und die (mögliche) Rolle von Compliance	545
1. Zielsetzungen der CSR-Richtlinie und des CSR-Richtlinie-Umsetzungsgesetzes	547
2. Neuausrichtung des Nachhaltigkeitsreportings	549
a) Bereits vor dem CSR-RUG vorhandene, nichtfinanzielle Berichtspflichten im deutschen Bilanzrecht	549
b) Sog. „Soft Law-Ansätze“ als Rahmenwerke für das CSR-Reporting	551
c) Paradigmenwechsel	551
3. Adressaten der CSR-Berichtspflichten	552
a) Der Adressatenkreis im Rahmen der nichtfinanziellen Erklärung	553
b) Die Verpflichteten der Vorgaben zum Diversitätskonzept	555
4. Berichtsanforderungen im Rahmen des CSR-Reportings	556
a) Berichtsvarianten: Die nichtfinanzielle Erklärung und der gesonderte Bericht	556
b) Inhalte, Relevanzmaßstab und Methodik des CSR-Reportings	557
c) Muster: Struktur und Ansätze zur Gestaltung des CSR-Reportings	561
d) Die Möglichkeit der Verwendung von Rahmenwerken	564
5. Ein Spezifikum: Das Diversitätskonzept	565
6. Nichtangaben, unrichtige Angaben und ihre Folgen	566
a) Der „Comply or Explain“-Grundsatz	566
b) Ein Sonderfall: Das (vorübergehende) Weglassen nachteiliger Angaben	568
c) Prüfungen	568
d) Verstöße, Säumnisse und Sanktionen	570
II. Fazit und Ausblick	571

16. Kapitel

Compliance im Kontext nachhaltigen Supply Chain-Managements

(Schleper/Förstl)

I. Einleitung	573
II. Nachhaltiges Lieferantenmanagement	574
1. Lieferantenbewertung	575
2. Lieferantenentwicklung	576
3. Lieferantenauswahl	576

4. Lieferantenmonitoring	577
III. Unterschiede entlang der Supply Chain	577
IV. Konfliktmineralien und Due Diligence – „beyond compliance“	580
V. Praxisrelevanz	582
VI. Fazit	584

17. Kapitel

Das Organisationsrisiko der „kriminogenen Verbandsattitüde“

(Rack)

I. Nützliche Rechtsverstöße zum Vorteil des Unternehmens und zum Nachteil des Mitarbeiters	585
II. Die Theorie der kriminogenen Verbandsattitüde	586
III. Empirische Untersuchungen zur kriminogenen Verbandsattitüde ...	587
IV. Das Milgram-Experiment zur Gehorsamsbereitschaft gegenüber Autorität	588
V. Konsequenzen für die Organisationspflicht der Organe	589
VI. Die schon vorhandene kriminelle Attitüde im Unternehmen und die Legalitätspflicht zu ihrer Abwehr	591
VII. Die präventive Legalitätspflicht durch Vorstände und Geschäftsführer vor dem Rechtsverstoß	591
VIII. Die unternehmensexterne Aufklärung	593
IX. Die unternehmensinterne Aufklärung	593
X. Die Strafbarkeit von Managern als „Täter hinter dem Täter“ durch Organisationsherrschaft	594
XI. Zwischenergebnis	595
XII. Kriminelles Mitarbeiterverhalten zum Vorteil des Unternehmens als vorhersehbares Organisationsrisiko	596
XIII. Die Rechtsgutsferne als Ursache kriminogener Wirkung	598
XIV. Die existenzielle Abhängigkeit vom Unternehmen als Ursache kriminogener Wirkungen	598
XV. Der altruistische selbstlose Straftäter als kriminogene Ursache	600

XVI. Die diffuse Verantwortungslosigkeit durch Arbeitsteilung als kriminogene Ursache und die Vermeidung durch die Delegation von Rechtspflichten.....	601
XVII. Blockierte Informationen als Ursache kriminogener Verbandsattitüden	602
XVIII. Die Auskunftspflicht mit Verwertungsverbot als Konfliktlösung	603
XIX. Fazit	605

Teil 3

Besondere Aufgaben und Anwendungsfelder

18. Kapitel

Compliance in M&A-Transaktionen

(Ullrich)

I. Einleitung	607
II. Prozessuale M&A-Compliance – Einhaltung von Rechtsvorschriften im M&A-Verfahren	608
1. Strukturierung der Transaktion.	608
a) Auktions- und Einzelbieterverfahren	608
b) Transaktionsgegenstand	609
2. Offenlegung von Informationen	610
a) Offenlegungs- und Aufklärungspflichten des Veräußerers	610
b) Rechtliche Grenzen der Offenlegung von Informationen	611
aa) Gesellschaftsrechtliche Zulässigkeit der Offenlegung von Informationen gegenüber Dritten	611
bb) Vertraulichkeitsbestimmungen in Verträgen mit Dritten ...	613
cc) Datenschutzrechtliche Anforderungen für die Offenlegung von personenbezogenen Daten.....	614
3. Kartellrechtliche M&A-Compliance – Vollzugsverbot und Informationsaustausch	616
a) Anmeldepflicht und Vollzugsverbot.	616
b) Informationsaustausch	619
4. Kapitalmarktrechtliche M&A-Compliance	622
a) Informationsweitergabe im Rahmen der Due Diligence	622
b) Ad-hoc-Pflicht	622
c) Übernahmerechtliche M&A-Compliance	624
5. Pflicht zur Durchführung einer rechtlichen Due Diligence	624
a) Regelfall.....	624
b) Besonders gelagerte Fälle.....	625
c) Nachgelagerte Due Diligence (Post-Closing Due Diligence) ...	627

6. (Abbruch der) Vertragsverhandlungen	628
7. Zustimmungserfordernisse.....	630
a) Zustimmung von Aufsichtsgremien und/oder der Gesellschafter	630
b) Zustimmung von Ehegatten oder Lebenspartnern	634
8. Vereinbarung von Wettbewerbsverboten im Unternehmenskaufvertrag	635
III. Materielle M&A-Compliance – Prüfung von/Umgang mit Compliance in der Zielgesellschaft.....	637
1. Due Diligence.....	637
a) Erfordernis einer Compliance-Due Diligence	637
aa) Einführung unter besonderer Beachtung von ESG/CSR... ..	637
bb) Erfordernis der Durchführung einer Compliance-Due Diligence.....	638
cc) (Eigen-)Interesse der Geschäftsleitung (Business Judgement Rule).....	640
dd) Normative Kraft des Faktischen.....	641
b) Vorgehensweise: Abgestufte, risikobasierte Compliance-Due Diligence	641
aa) Rechtlicher Rahmen	641
bb) Ermittlung des Risikoprofils der Zielgesellschaft	642
cc) Risikobewertung und Dokumentation.....	643
dd) Eigentliche Due Diligence.....	643
c) Due Diligence nach Vollzug.....	643
2. Umgang mit bekannten/bekanntgewordenen Compliance-Verstößen/-Risiken.....	644
a) Risikobewertung	644
b) Umgang mit bekannten/entdeckten Compliance-Risiken	645
IV. Zusammenfassung	648

19. Kapitel

Die Compliance-Funktion in einem Kreditinstitut

(Renz/Frankenberger)

I. Einführung: Was ist die Bedeutung des Begriffs Compliance?.....	649
II. Welche Compliance-Funktionen gibt es in einem Kreditinstitut?....	650
1. Kapitalmarkt-Compliance	651
2. Zentrale Stelle/sonstige strafbare Handlungen (inkl. Geldwäscheprävention).....	652
3. MaRisk-Compliance	654
4. Hinweisgebersystem (Whistleblowing).....	656
5. Datenschutz.....	657

6. Auslagerung der Compliance-Funktion oder von einzelnen Compliance-Tätigkeiten	658
III. Inhalt und Aufgabe einer modernen Compliance-Funktion	659
IV. Das Compliance-Management-System (CMS)	660
V. Schnittstellen zu anderen Funktionen	663
1. Fach- und Marktbereiche	664
2. Rechtsabteilung	664
3. Risikocontrolling-Funktion	665
4. Interne Revision	666
VI. Compliance als Teil des IKS eines Kreditinstituts	667
VII. Übertragung der Struktur/des Ansatzes auf andere Industriesäulen – und umgekehrt	672
VIII. Fazit/Ausblick	674

20. Kapitel

Der Geldwäschebeauftragte – Stellung und Aufgaben

(Kaetzler)

I. Der Geldwäschebeauftragte	675
1. Warum eigentlich ein Geldwäschebeauftragter? – Geschichte einer besonderen Funktion	676
2. Verpflichtete Unternehmen	684
a) Qua Gesetz	684
b) Freistellungsmöglichkeit (§ 7 Abs. 2 GwG)	686
c) Anordnung der Behörden	687
3. Anforderungen an den Geldwäschebeauftragten und Bestellung ..	688
4. Kompetenzen und Stellung im Unternehmen	690
5. Aufgaben des Geldwäschebeauftragten	695
a) Risikoanalyse	695
b) Sicherungsmaßnahmen	696
c) Antizipation und Implementierung neuer rechtlicher und verwaltungspraktischer Vorschriften	696
d) Kontinuierliche Überwachung von Geschäftsbeziehungen/ „Monitoring“	697
e) Verdachtsfälle und Verdachtsmeldewesen/ Unstimmigkeitsmeldungen	697
f) Berichtswesen, Bericht an Geschäftsleitung und Aufsichtsorgan	699
g) Mitarbeiterschulungen	700

6. Arbeitsrechtlicher Schutz des Geldwäschebeauftragten und Teilausnahme vom Direktionsrecht des Arbeitgebers.	700
a) Sonderkündigungsschutz	701
b) Benachteiligungsverbot.	701
c) Ausnahme vom Direktionsrecht	702
7. Auslagerung der Funktion	703
8. Haftung	704
9. Der Geldwäschebeauftragte – gefangen zwischen hoheitlicher und unternehmerischer Tätigkeit?	705

21. Kapitel

Geldwäsche-Compliance in Industrie und Handel

(Komma)

I. Einführung in die Geldwäscheprevention	707
1. Begriff und Methoden der Geldwäsche	707
2. Die Geldwäschebekämpfung.	709
a) Geldwäschebekämpfung auf internationaler Ebene: FATF	709
b) Geldwäschebekämpfung in der deutschen Gesetzgebung	710
3. Geldwäscherisiken für Industrie- und Handelsunternehmen	711
II. Industrie- und Handelsunternehmen im GwG:	
Der Begriff des Güterhändlers	713
III. Die Pflichten der Güterhändler im GwG	715
1. Die privilegierte Verpflichtetenstellung von Güterhändlern	715
a) Praktische Umsetzung des Bargeldausschlusses	716
b) Konsequenzen bei Einführung einer Bargeldbeschränkung.	717
2. Risikomanagement	718
a) Risikoanalyse.	719
b) Interne Sicherungsmaßnahmen	720
aa) Richtlinie zur Prävention von Geldwäsche	721
bb) Überprüfung von Geschäftspartnern	722
cc) Überwachung von Zahlungseingängen.	722
c) Gruppenweite Pflichten.	722
3. Kundensorgfaltspflichten	723
a) Auslösetatbestände der Sorgfaltspflichten für Güterhändler ...	724
b) Ausgewählte Aspekte der allgemeinen Sorgfaltspflichten.	725
c) Ausgewählte Aspekte der vereinfachten und verstärkten Sorgfaltspflichten	726
4. Pflicht zur Abgabe von Verdachtsmeldungen	728
a) Verdachtsfall und typische Verdachtsmomente	728
b) Folgen einer Verdachtsmeldung.	729
aa) Strafbefreiende Wirkung	730
bb) Transaktionssperrfrist § 46 GwG	730

cc) Verbot der Informationsweitergabe (Tipping Off-Verbot) . . 730
IV. Fazit 731

22. Kapitel

Produktbezogenes Compliance- und Risikomanagement im Treasury

(Keßler)

I. Einleitung 733
II. Finanz- und Kapitalmarktprodukte; Risiken 734
1. „Einfache“ Produkte 734
2. „Komplexe“ Produkte 735
a) Überblick 735
b) Risiken im Einzelnen 738
III. Rechtliche Anforderungen an das Risikomanagement- und Compliance-System 740
1. Anforderungen an Finanzinstitute 740
a) Aufsichtsrechtliche Anforderungen 740
b) „Best Practice“ und praktische Ausgestaltung 742
aa) Risikomanagement 742
bb) Compliance 745
2. Anforderungen an Unternehmen 746
a) Normativer Rahmen und Übertragbarkeit 746
b) Grenzen 749
IV. Ausgestaltung des Risikomanagement- und Compliance-Systems im Unternehmensbereich 749
1. Finanzproduktbezogenes Risikomanagement und Compliance – Überblick 749
2. Die Ausgestaltung der wichtigsten ICRM-Komponenten im Einzelnen 751
a) Rechtliche Einzelfallprüfung: Covenant-Tool 751
b) Kreditrisiko-Tool 752
c) Marktrisiko-Tool 753
d) Liquiditätsrisiko-Tool 754
3. Delegation des Risikomanagements und Compliance 754
V. Haftungsfragen 756
1. Verstoß gegen die Pflicht zum Risikomanagement 757
2. Verstoß gegen die Pflicht zur Compliance 758
VI. Fazit 758

23. Kapitel

Kartellrechts-Compliance*(Seeliger/Heinen/Mross)*

I. Überblick über die Kartellrechts-Risiken	761
1. Einführung	761
2. Kartellrechts-Risikokategorien	763
a) Das Verbot wettbewerbsbeschränkender Vereinbarungen:	
Absprachen mit anderen Unternehmen	764
aa) Vereinbarung, abgestimmtes Verhalten oder Beschluss ...	764
bb) Bezweckte oder bewirkte Wettbewerbsbeschränkung	765
cc) Sehr hohe Risiken	766
dd) Weniger hohe Risiken	776
b) Machtmissbrauch (einseitige Handlungen)	780
aa) Allgemeine Voraussetzungen	780
bb) Sehr hohe Risiken	783
cc) Weniger hohe Risiken	784
3. Haftungssubjekte (Wer haftet für wen?)	787
a) Unternehmenshaftung	787
b) Persönliche Haftung	787
c) Haftung im Konzern („Wirtschaftliche Einheit“)	788
d) Haftung bei Gemeinschaftsunternehmen	789
e) Haftung für Beauftragte	790
f) Haftung bei Rechtsnachfolge	790
4. Art und Umfang der Haftung	791
a) Strafrechtliche Sanktionen	791
b) Bußgelder	792
aa) EU-Recht	792
bb) Deutsches Recht	794
c) Schadensersatz	795
aa) Individualansprüche	796
bb) Kollektiver Rechtsschutz	797
cc) Schadensausgleich im Innenverhältnis	797
d) Sonstige Nachteile	798
II. Management der Kartellrechtsrisiken in der Praxis	799
1. Risikoanalyse: Identifizierung und Bewertung	799
a) Kartellrechtliches Risikoprofil	800
b) Geschäftstätigkeit und Geschäftsbeziehungen	800
c) Risikokategorisierung und Risikobewertung	801
d) Einführung eines Top-down-Ansatzes	802
2. Präventive Maßnahmen	802
a) Richt- und Leitlinien zum Kartellrecht	803
b) Schulungen (Präsenzs Schulungen und Webinars/E-Learning) ..	805
3. Maßnahmen zur Kontrolle/Aufdeckung	808

III. Behördliche Untersuchungen	809
1. Durchsuchungen der EU-Kommission	810
a) Zuständigkeit	810
b) Befugnisse	811
c) Elektronische Durchsuchung	812
d) Typischer Ablauf	813
2. Durchsuchungen des Bundeskartellamts	814
a) Zuständigkeit	814
b) Befugnisse	815
c) Elektronische Durchsuchung	816
d) Typischer Ablauf	816
3. Verhaltensregeln für die Unternehmen	817
a) Vor der Durchsuchung	817
b) Während der Durchsuchung	818
c) Nach der Durchsuchung	819

24. Kapitel

Compliance-Anforderungen im Wettbewerb um öffentliche Aufträge

(Scherer)

I. Einleitung	821
II. Anforderungen an Unternehmen in Vergabeverfahren	822
III. Ausschlussgründe	824
1. Zwingende Ausschlussgründe	824
a) Straftatbestände	824
b) Steuer- und Abgabentatbestände	825
2. Fakultative Ausschlussgründe	826
a) Verstoß gegen umwelt-, sozial- oder arbeitsrechtliche Verpflichtungen	826
b) Insolvenz und Liquidation	827
c) Schwere Verfehlung im Rahmen beruflicher Tätigkeit	827
d) Wettbewerbsbeschränkende Vereinbarungen oder abgestimmte Verhaltensweisen	828
e) Interessenkonflikt	828
f) Vorbefassung	829
g) Mangelhafte Leistung bei Ausführung früherer Aufträge	830
h) Schwerwiegende Täuschung bei Eignungsprüfung	830
i) Unzulässige Einflussnahme	831
IV. Wettbewerbsregister	831
1. Einrichtung des Wettbewerbsregisters	831
2. Eintragung von Rechtsverstößen	832
3. Einbindung in das Vergabeverfahren	833

4. Löschung von Eintragungen	834
5. Rechtsbehelfe	834
V. Selbstreinigung	834
1. Selbstreinigung im Vergabeverfahren	835
a) Prüfung durch Vergabestelle	835
b) Prüfung durch Wettbewerbsregister	835
2. Kriterien der Selbstreinigung	836
a) Ausgleich des Schadens	836
b) Zusammenarbeit zur Aufklärung	837
c) Technische, organisatorische und personelle Maßnahmen	837
VI. Ausschlussfristen	840
1. Fristenregelung bei zwingenden Ausschlussgründen	840
2. Fristenregelung bei fakultativen Ausschlussgründen	840
3. Ermessensausübung	841

25. Kapitel

Tax Compliance

(Schwartz/Stürzl-Friedlein)

I. Einleitung	843
II. Steuerliche Pflichten	844
1. Allgemeine steuerliche Pflichten	844
2. Spezifische materiell-rechtliche Problemschwerpunkte	849
a) Lohnsteuer und Sozialabgaben	849
b) Umsatzsteuer	850
c) Verdeckte Gewinnausschüttungen	851
d) Anzeigepflicht nach § 153 AO	852
e) Tochtergesellschaften und Betriebstätten im Ausland	853
f) Internationale Verrechnungspreise	854
g) Versagung des Betriebsausgabenabzugs nach § 160 AO	855
h) Betriebsausgabenabzugsverbot nach § 4 Abs. 5 Satz 1 Nr. 10 EStG	856
III. Risiken mangelnder Tax Compliance	857
1. Steuerliche Haftungsrisiken	857
2. Steuerstrafrechtliche und steuerordnungswidrigkeitenrechtliche Risiken	859
a) Sanktionen gegen Organe und Mitarbeiter	859
aa) Steuerhinterziehung und leichtfertige Steuerverkürzung (§§ 370, 378 AO)	859
bb) Verletzung der Aufsichtspflicht (§ 130 OWiG)	866
b) Sanktionen gegen das Unternehmen	867

aa) Verbandsgeldbuße (§ 30 OWiG)	867
bb) Einziehung (§ 29a OWiG).....	869
IV. Tax Compliance-System.....	870
1. Risikoanalyse	870
2. Ausgestaltung eines Tax Compliance-Systems.....	871
a) Zuständigkeit für Tax Compliance	871
b) Zuständigkeit und Verantwortlichkeit bzgl. der steuerlichen Pflichten	871
c) Berichtswege/Berichtspflichten	872
d) Prozessbeschreibung Deklarationswesen	874
e) Kontroll- und Überwachungsmaßnahmen	874
f) Umgang mit Betriebsprüfungen	875
g) Schulungen	876
h) Dokumentation.....	877
V. Zertifizierung des Tax Compliance-Systems durch Dritte	877
VI. Berichtigung von Steuererklärungen	879
1. Korrekturvorschrift	879
2. Selbstanzeige im Unternehmen (§§ 371, 378 Abs. 3 AO).....	880
a) Person des Anzeigerstatters	880
b) Positive Wirksamkeitsvoraussetzungen des § 371 AO	881
c) Negative Wirksamkeitsvoraussetzungen des § 371 AO (Sperrgründe)	883
d) Absehen von Verfolgung nach § 398a AO	886
e) Bußgeldbefreiende Selbstanzeige nach § 378 Abs. 3 AO	887
VII. Verbandssanktionengesetz (VerSanG).....	887
1. Allgemeines	887
2. Wesentliche Inhalte	887
a) Regelungsbereich/Adressaten und Opportunitätsprinzip	887
b) Verschuldensunabhängige Zurechnung: Objektiv vorliegende Aufsichtspflichtverletzung ausreichend	888
c) Sanktionen.....	888
d) Sanktionsmilderung durch Kooperation und Compliance.....	889
VIII. Fazit	889

26. Kapitel

Exportkontrolle und Compliance*(von Bodungen)*

I. Einleitung	891
II. Rechtsgrundlagen der Exportkontrolle in Deutschland	892
1. Supranationale Vorgaben	892
2. Nationale Vorgaben	893
3. Relevanz ausländischen Exportkontrollrechts	894
a) Allgemeines	894
b) Insbesondere: US-Re-Exportkontrolle	894
III. Exportkontrollrechtliche Genehmigungspflichten	895
1. Allgemeines	895
2. Genehmigungspflichten bei Ausfuhren in Länder außerhalb der EU	896
a) Gelistete Güter	896
b) Nicht gelistete Güter	897
3. Genehmigungspflichten bei Verbringungen	897
a) Verbringungen bei Endverbleib in der EU	898
b) Verbringungen mit anschließender Ausfuhr	898
4. Sonstige Genehmigungspflichten	898
a) Handels- und Vermittlungsgeschäfte	898
b) Technische Unterstützung	899
IV. Exportkontrollrechtliches Genehmigungsverfahren	900
1. Zuständigkeit des BAFA	900
2. Ablauf des Genehmigungsverfahrens	901
3. Genehmigungstypen	902
4. Sanktionen bei exportkontrollrechtlichen Verstößen	903
V. Exportkontrollrechtliche Compliance-Strukturen	904
1. Allgemeines	904
2. Der Ausfuhrverantwortliche	905
3. Modell eines innerbetrieblichen Exportkontrollsystems	907
a) Überblick über die relevanten Strukturelemente	907
b) Umsetzung im Einzelfall	910
VI. Zusammenfassung und Ausblick	912
Literaturverzeichnis	915
Sachregister	959

Abkürzungsverzeichnis

a. A./A. A.	andere(r) Ansicht
a. a. O.	am angegebenen Ort
a. F.	alte Fassung
Abb.	Abbildung
ABC-Waffe	atomare, biologische und chemische Waffe
AbgG	Abgeordnetengesetz in der Fassung der Bekanntmachung vom 21.2.1996 (BGBl. I S. 326), zuletzt geändert durch Artikel 1 des Gesetzes vom 11.7.2014 (BGBl. I S. 906)
ABl.	Amtsblatt
Abs.	Absatz
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
AG	Aktiengesellschaft/Die Aktiengesellschaft (Zeitschrift)
AGB	Allgemeine Geschäftsbedingung
AGG	Allgemeines Gleichbehandlungsgesetz in der Fassung vom 14.8.2006 (BGBl. I S. 1897), zuletzt geändert durch Artikel 8 des Gesetzes vom 3.4.2013 (BGBl. I S. 610)
AktG	Aktiengesetz in der Fassung vom 6.9.1965 (BGBl. I S. 1089), geändert durch Gesetz vom 10.5.2016 (BGBl. I S. 1142) m.W. v. 17.6.2016
AktG-E	Aktiengesetz-Entwurf
allg.	allgemein(e)
AMG	Arzneimittelgesetz in der Fassung der Bekanntmachung vom 12.12.2005 (BGBl. I S. 3394), geändert durch Artikel 4 Absatz 11 des Gesetzes vom 18.7.2016 (BGBl. I S. 1666)
ÄndG.	Änderungsgesetz
Anh.	Anhang
Anm.	Anmerkung(en)
AO	Abgabenordnung in der Fassung der Bekanntmachung vom 1.10.2002 (BGBl. I S. 3866; 2003 I S. 61), geändert durch Artikel 3 Absatz 13 des Gesetzes vom 26.7.2016 (BGBl. I S. 1824)
App	Applikation (Anwendungsprogramm, -software)
AR	Aufsichtsrat

Abkürzungsverzeichnis

ArbG	Arbeitsgericht
Art.	Artikel
AstBV (St)	Anweisungen für das Straf- und Bußgeldverfahren (Steuer)
AStG	Gesetz über die Besteuerung bei Auslandsbeziehungen (Außensteuergesetz) vom 8.9.1972 (BGBl. I S. 1713), zuletzt geändert durch Artikel 6 des Gesetzes vom 19.7.2016 (BGBl. I S. 1730)
AT	amtlicher Teil/allgemeiner Teil
AuA	Arbeit und Arbeitsrecht (Zeitschrift)
Aufl.	Auflage
Ausschussdrucks.	Ausschussdrucksache
AW-Prax.	Außenwirtschaftliche Praxis (Zeitschrift)
AWG	Außenwirtschaftsgesetz in der Fassung der Bekanntmachung vom 6.6.2013 (BGBl. I S. 1482), zuletzt geändert durch Artikel 6 des Gesetzes vom 3.12.2015 (BGBl. I S. 2178)
AWV	Außenwirtschaftsverordnung vom 2.8.2013 (BGBl. I S. 2865), zuletzt geändert durch Artikel 1 der Verordnung vom 14.3.2016 (BAnz AT 18.3.2016 V1)
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 5.2.2009 (BGBl. I S. 160), geändert durch Artikel 3 Absatz 3 des Gesetzes vom 18.7.2016 (BGBl. I S. 1666)
BCBS	Basel Committee on Banking Supervision
Bd.	Band
BDI	Bundesverband der Deutschen Industrie e. V.
BDSG	Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14.1.2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 25.2.2015 (BGBl. I S. 162) m.W.v. 1.1.2016
BeckRS	Beck-online Rechtsprechung
Begr.	Begründung
Beil.	Beilage
Bek.	Bekanntmachung
BetrVG	Betriebsverfassungsgesetz in der Fassung der Bekanntmachung vom 25.9.2001 (BGBl. I S. 2518), zuletzt geändert durch Artikel 3 Absatz 4 des Gesetzes vom 20.4.2013 (BGBl. I S. 868)

Beschl.	Beschluss
BFH	Bundesfinanzhof
BFH/NV	Sammlung der Entscheidungen des Bundesfinanzhofs, die nicht veröffentlicht wurden (Zeitschrift)
BGB	Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2.1.2002 (BGBl. I S. 42, 2909; 2003 I S. 738), geändert durch Gesetz vom 24.5.2016 (BGBl. I S. 1190)
BGBI.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungssammlung des Bundesgerichtshofes in Strafsachen
BGHZ	Entscheidungssammlung des Bundesgerichtshofes in Zivilsachen
BHO	Bundeshaushaltsordnung
BImSchG	Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge (Bundes-Immissionsschutzgesetz) in der Fassung der Bekanntmachung vom 17.5.2013 (BGBl. I S. 1274), geändert durch Artikel 3 des Gesetzes vom 26.7.2016 (BGBl. I S. 1839)
BKA	Bundeskriminalamt
BKartA	Bundeskartellamt
BKR	Zeitschrift für Bank- und Kapitalmarktrecht (Zeitschrift)
BMF	Bundesministerium der Finanzen
BMI	Bundesministerium des Inneren
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BOARD	Zeitschrift für Aufsichtsräte in Deutschland (Zeitschrift)
BpO	Betriebsprüfungsordnung
BR-Drucks.	Bundesratsdrucksache
BRAK	Bundesrechtsanwaltskammer
BRAO	Bundesrechtsanwaltsordnung vom 1.8.1959 (BGBl. I S. 565), zuletzt geändert durch Gesetz vom 19.2.2016 (BGBl. I S. 254) m. W. v. 1.4.2016
BremGbl.	Gesetzblatt der Freien Hansestadt Bremen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) vom 14.8.2009 (BGBl. I S. 2821), geändert durch Artikel 3 Absatz 6 des Gesetzes vom 18.7.2016 (BGBl. I S. 1666)
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung) vom 22.4.2016 (BGBl. I S. 958)
bspw.	beispielsweise

Abkürzungsverzeichnis

BStBl.	Bundessteuerblatt
BT	Besonderer Teil
BT-Drucks.	Bundestagsdrucksache
BUrlG	Bundesurlaubsgesetz in der im Bundesgesetzblatt Teil III, Gliederungsnummer 800-4, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 3 Absatz 3 des Gesetzes vom 20.4.2013 (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 21.9.1984 (BGBl. I S. 1229, 1985 I S. 195), zuletzt geändert durch Artikel 2 des Gesetzes vom 11.10.2016 (BGBl. I S. 2226)
bzw.	beziehungsweise
ca.	circa
CB	Compliance-Berater (Zeitschrift)
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
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CR	Computer & Recht (Zeitschrift)
CRi	Computer Law Review International (Zeitschrift)
CSR	Corporate Social Responsibility
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)
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 7.12.2011 (BGBl. I S. 2650)
E-Commerce	Elektronischer Handel/Internethandel
EDV	Elektronische Datenverarbeitung
EFZG	Entgeltfortzahlungsgesetz vom 26.5.1994 (BGBl. I S. 1014, 1065), zuletzt geändert durch Artikel 7 des Gesetzes vom 16.7.2015 (BGBl. I S. 1211)
EG	Europäische Gemeinschaft
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)

Abkürzungsverzeichnis

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 endg.	Europäische Menschenrechtskonvention endgültig
EnergieStG	Energiesteuergesetz vom 15.7.2006 (BGBl. I S. 1534; 2008 I S. 660, 1007), zuletzt geändert durch Artikel 10 des Gesetzes vom 3.12.2015 (BGBl. I S.2178)
EnWG	Energiewirtschaftsgesetz vom 7.7.2005 (BGBl. I S. 1970, 3621), geändert durch Artikel 3 des Gesetzes vom 29.8.2016 (BGBl. I S. 2034)
ErbStG	Erbschaftsteuer- und Schenkungsteuergesetz in der Fassung der Bekanntmachung vom 27.2.1997 (BGBl. I S. 378), zuletzt geändert durch Artikel 8 des Gesetzes vom 31.7.2016 (BGBl. I S. 1914)
ESMA	European Securities and Markets Authority (Europäische Wertpapier- und Marktaufsichtsbehörde)
ESt	Einkommenssteuer
EStG	Einkommensteuergesetz in der Fassung der Bekanntmachung vom 8.10.2009 (BGBl. I S. 3366, 3862), zuletzt geändert durch Artikel 7 des Gesetzes vom 31.7.2016 (BGBl. I S. 1914)
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.	folgende
F&E	Forschung und Entwicklung
FAQ	Frequently Asked Questions

L

ff.	fortfolgende
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 Artikel 8 des Gesetzes vom 11.10.2016 (BGBl. I S. 2222)
FKVO	Verordnung (EG) Nr. 139/2004 des Rates vom 20.1.2004 über die Kontrolle von Unternehmenszusammenschlüssen („EG-Fusionskontrollverordnung“)
Fn.	Fußnote
FS	Festschrift
GA	Goldammer's Archiv für Strafrecht (Zeitschrift)
GbR	Gesellschaft bürgerlichen Rechts
GewO	Gewerbeordnung in der Fassung der Bekanntmachung vom 22.2.1999 (BGBl. I S. 202), zuletzt geändert durch Gesetz vom 31.7.2016 (BGBl. I S. 1914) m. W. v. 6.8.2016
GewSt	Gewerbsteuer
GewStG	Gewerbsteuergesetz in der Fassung der Bekanntmachung vom 15.10.2002 (BGBl. I S. 4167), zuletzt geändert durch Artikel 5 des Gesetzes vom 2.11.2015 (BGBl. I S. 1834)
GF	Geschäftsführer
GG	Grundgesetz für die Bundesrepublik Deutschland in der im BGBl. Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, geändert zuletzt durch Gesetz vom 23.12.2014 (BGBl. I S. 2438) m. W. v. 1.1.2015
ggf./ggfs.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GmbH & Co KG	Gesellschaft mit beschränkter Haftung & Compagnie Kommanditgesellschaft
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbH-Gesetz) in der Fassung vom 20.4.1892 (RGBl. I S. 477), zuletzt geändert durch Gesetz vom 10.5.2016 (BGBl. I S. 1142) m. W. v. 17.6.2016
GmbHR	GmbH-Rundschau (Zeitschrift)
GRC	Governance, Risikomanagement & Compliance
GRI	Global Reporting Initiative
GrESTG	Gründerwerbsteuergesetz in der Fassung der Bekanntmachung vom 26.2.1997 (BGBl. I S. 418, 1804), zuletzt geändert durch Artikel 18 des Gesetzes vom 18.7.2016 (BGBl. I S. 1679)
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)

Abkürzungsverzeichnis

GRUR-RR	Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungs-Report (Zeitschrift)
GSSt	Großer Senat für Strafsachen
GVOBl.	Gesetz- und Verordnungsblatt
GWB	Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bekanntmachung vom 26.6.2013 (BGBl. I S. 1750, 3245), zuletzt geändert durch Artikel 4 Absatz 8 des Gesetzes vom 11.10.2016 (BGBl. I S. 2262)
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz) in der Fassung der Bekanntmachung vom 13.8.2008 (BGBl. I S. 1690), zuletzt geändert durch Artikel 7 des Gesetzes vom 11.4.2016 (BGBl. I S. 720)
GWR	Gesellschafts- und Wirtschaftsrecht (Zeitschrift)
Hdb.	Handbuch
HGB	Handelsgesetzbuch in der Fassung vom 10.5.1897 (RGBl. I S. 219), zuletzt geändert durch Gesetz vom 5.7.2016 (BGBl. I S. 1578 BGBl. I S. 1578)
HGB-E	HGB-Entwurf
h. L.	herrschende Lehre
h. M.	herrschende Meinung
HmbGVBl.	Hamburgisches Gesetz- und Verordnungsblatt
HR	Human Resources
HRRS	Online-Zeitschrift für Höchstgerichtliche 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 5.10.1994 (BGBl. I S. 2866), zuletzt geändert durch Artikel 16 des Gesetzes vom 20.11.2015 (BGBl. I S. 2010)

InstitutsVergV	Verordnung über die aufsichtsrechtlichen Anforderungen an Vergütungssysteme von Instituten (Institutsvergütungsverordnung) in der Fassung vom 6.10.2010 (BGBl. I S. 1374), zuletzt geändert durch Gesetz vom 16.12.2013 (BGBl. I S. 4270)
IntBestG	Gesetz zur Bekämpfung internationaler Bestechung vom 10.9.1998 (BGBl. 1998 II S. 2327), 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 in der Fassung der Bekanntmachung vom 4.7.2013 (BGBl. I S. 1981), zuletzt geändert durch Artikel 6 des Gesetzes vom 30.6.2016 (BGBl. I S. 1514)
Kap.	Kapitel
KG	Kommanditgesellschaft
KMU	kleine und mittlere Unternehmen
Komm.	Kommission der Europäischen Union/Kommentar
KOM (2001) 366 endg.	Kommission der Europäischen Gemeinschaften – GRÜN- BUCH – Europäische Rahmenbedingungen für die soziale Verantwortung der Unternehmen vom 18.7.2001
KOM (2011) 206 endg.	Mitteilung der Europäischen Kommission an das Europäi- sche Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Binnen- marktakte – vom 13.4.2011
KOM (2011) 681 endg.	Mitteilung der Europäischen Kommission an das Europäi- sche 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
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbe- reich 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)

Abkürzungsverzeichnis

KRITIS-Betreiber	Betreiber kritischer Infrastrukturen
KSchG	Kündigungsschutzgesetz in der Fassung der Bekanntmachung vom 25.8.1969 (BGBl. I S. 1317), zuletzt geändert durch Artikel 3 Absatz 2 des Gesetzes vom 20.4.2013 (BGBl. I S. 868)
KSt	Körperschaftsteuer
KStG	Körperschaftsteuergesetz in der Fassung der Bekanntmachung vom 15.10.2002 (BGBl. I S. 4144), zuletzt geändert durch Artikel 4 des Gesetzes vom 19.7.2016 (BGBl. I S. 1730)
KSzW	Kölner Schrift zum Wirtschaftsrecht (Zeitschrift)
KWG	Gesetz über das Kreditwesen (Kreditwesengesetz) in der Fassung vom 9.9.1998 (BGBl. I S. 2776), geändert durch Artikel 3 und 4 des Gesetzes vom 30.6.2016 (BGBl. I S. 1514)
KWKG	Gesetz über die Kontrolle von Kriegswaffen (Kriegswaffenkontrollgesetz) in der Fassung der Bekanntmachung vom 22.11.1990 (BGBl. I S. 2506), zuletzt geändert durch Artikel 30 der Verordnung vom 31.8.2015 (BGBl. I S. 1474)
LAG	Landesarbeitsgericht
LCO	Local Compliance Officer
LG	Landgericht
lit.	littera (Buchstabe)
LK	Leipziger Kommentar
LohnSt	Lohnsteuer
LPartG	Lebenspartnerschaftsgesetz vom 16.2.2001 (BGBl. I S. 266), zuletzt geändert durch Artikel 19 des Gesetzes vom 20.11.2015 (BGBl. I S. 2010)
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)
LIV	

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) in der Fassung vom 11.8.2014 (BGBl. I S. 1348), geändert durch Artikel 2 Absatz 10 des Gesetzes vom 17.2.2016 (BGBl. I S. 203)
Min.	Minute(n)
Mio.	Million(en)
MMR	Multimedia und Recht (Zeitschrift)
Mrd.	Milliarde(n)
M SchrKrim	Monatsschrift für Kriminologie und Strafrechtsreform (Zeitschrift)
MüKo/ MünchKomm.	Münchener Kommentar
m. w. N./ m. w. Nachw.	mit weiteren Nachweisen
m. W. v.	mit Wirkung vom
n. F.	neue Fassung
NGO	Non-Governmental Organization (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	NomosKommentar StGB
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	Rechtssprechungs-Report Arbeitsrecht (Zeitschrift)
NZG	Neue Zeitschrift für Gesellschaftsrecht (Zeitschrift)
NZKart	Neue Zeitschrift für Kartellrecht (Zeitschrift)

Abkürzungsverzeichnis

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)
OHG	Offene Handelsgesellschaft
o. g.	oben genannte(r)
OLG	Oberlandesgericht
OWiG	Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19.2.1987 (BGBl. I S. 602), zuletzt geändert durch Gesetz vom 13.5.2015 (BGBl. I S. 706) m.W. v. 23.5.2015
p. a.	per anno (pro Jahr)
PartG	Gesetz über die politischen Parteien (Parteiengesetz) in der Fassung der Bekanntmachung vom 31.1.1994 (BGBl. I S. 149), zuletzt geändert durch Artikel 1 des Gesetzes vom 22.12.2015 (BGBl. I S. 2563)
PC	Personal Computer
PR	Public Relations (Öffentlichkeitsarbeit)
PSR	Personal Social Responsibility
PStR	Praxis Steuerstrafrecht (Zeitschrift)
PublG	Gesetz über die Rechnungslegung von bestimmten Unternehmen und Konzernen (Publizitätsgesetz) vom 15.8.1969 (BGBl. I S. 1189), zuletzt geändert durch Artikel 4 des Gesetzes vom 24.5.2016 (BGBl. I S. 1190)
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
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 12.11.2009 (BGBl. I S. 3710, 3973; 2011 I S. 363), zuletzt geändert durch Artikel 28 des Gesetzes vom 20.11.2015 (BGBl. I S. 2010)
SGB V	Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20.12.1988, BGBl. I S. 2477, 2482), geändert durch Artikel 2 des Gesetzes vom 11.10.2016 (BGBl. I S. 2233)
SIEM-System	Security, Information and Event-Management-System
SMS	Short Message Service
s. o.	siehe oben
sog.	sogenannt/sogenannte(r/s)
s.u.	siehe unten/siehe unter
Slg.	Sammlung der Rechtsprechung des Gerichtshofs und des Gerichts der Europäischen Union
Stbg	Die Steuerberatung (Zeitschrift)
StGB	Strafgesetzbuch in der Fassung der Bekanntmachung vom 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz vom 3.12.2015 (BGBl. I S. 2177) m. W. v. 10.12.2015
StPO	Strafprozeßordnung in der Fassung der Bekanntmachung vom 7.4.1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Artikel 4 Absatz 5 des Gesetzes vom 11.10.2016 (BGBl. I S. 2226)
StraFo	StrafverteidigerForum (Zeitschrift)
StromStG	Stromsteuergesetz vom 24.3.1999 (BGBl. I S. 378; 2000 I S. 147), zuletzt geändert durch Artikel 11 des Gesetzes vom 3.12.2015 (BGBl. I S. 2178)
st. Rspr.	ständige Rechtsprechung
StV	Strafverteidiger (Zeitschrift)
TK	Telekommunikation
TKG	Telekommunikationsgesetz vom 22.6.2004 (BGBl. I S. 1190), geändert durch Artikel 9 des Gesetzes vom 26.7.2016 (BGBl. I S. 1818)

Abkürzungsverzeichnis

TMG	Telemediengesetz vom 26.2.2007 (BGBl. I S. 179), geändert durch Artikel 1 des Gesetzes vom 21.7.2016 (BGBl. I S. 1766)
Tz.	Textziffer
u.	und
u. a.	unter anderem/und andere
u. a. m.	und andere(s) mehr
Ubg	Die Unternehmensbesteuerung (Zeitschrift)
UmwG	Umwandlungsgesetz vom 28.10.1994 (BGBl. I S. 3210; 1995 I S. 428), zuletzt geändert durch Artikel 22 des Gesetzes vom 24.4.2015 (BGBl. I S. 642)
UN	United Nations (Vereinte Nationen)
UNO	United Nations Organization (Organisation der Vereinten Nationen)
Unterabs.	Unterabsatz
UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz) vom 9.9.1965 (BGBl. I S. 1273), zuletzt geändert durch Artikel 7 des Gesetzes vom 4.4.2016 (BGBl. I S. 558)
Urt.	Urteil
USA	United States of America
USD	US-Dollar
USt	Umsatzsteuer
UStG	Umsatzsteuergesetz in der Fassung der Bekanntmachung vom 21.2.2005 (BGBl. I S. 386), zuletzt geändert durch Artikel 5 des Gesetzes vom 19.7.2016 (BGBl. I S. 1730)
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)
v. H.	von Hundert
verb.	verbunden
VersR	Versicherungsrecht (Zeitschrift)

VersStG	Versicherungsteuergesetz in der Fassung der Bekanntmachung vom 10.1.1996 (BGBl. I S. 22), zuletzt geändert durch Artikel 25 des Gesetzes vom 20.11.2015 (BGBl. I S. 2029)
VG	Verwaltungsgericht
vgl.	vergleiche
VgV	Verordnung über die Vergabe öffentlicher Aufträge (Vergabeverordnung)
VK	Vergabekammer
VO	Verordnung
VOB/A	Vergabe- und Vertragsordnung für Bauleistungen – Teil A
vs.	versus
VVG	Gesetz über den Versicherungsvertrag (Versicherungsvertragsgesetz) vom 23.11.2007 (BGBl. I S. 2631), zuletzt geändert durch Artikel 15 des Gesetzes vom 19.2.2016 (BGBl. I S. 254)
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 20.7.2007 (BGBl. I S. 1432), zuletzt geändert durch Artikel 12 des Gesetzes vom 20.11.2015 (BGBl. I S. 2029)
WpHG	Gesetz über den Wertpapierhandel (Wertpapierhandelsgesetz) in der Fassung vom 9.9.1998 (BGBl. I S. 2708) geändert durch Gesetz vom 30.6.2016 (BGBl. I S. 1514) m.W.v. 2.7.2016
WpHGMaAnzV	Verordnung über den Einsatz von Mitarbeitern in der Anlageberatung, als Vertriebsbeauftragte oder als Compliance-Beauftragte und über die Anzeigepflichten nach § 34d des Wertpapierhandelsgesetzes (WpHG-Mitarbeiteranzeigeverordnung) in der Fassung der Bekanntgabe vom 21.12.2011 (BGBl. I S. 3116), geändert durch Artikel 16 Absatz 5 des Gesetzes vom 30.6.2016 (BGBl. I S. 1514)
WpÜG	Wertpapiererwerbs- und Übernahmegesetz vom 20.12.2001 (BGBl. I S. 3822), geändert durch Artikel 4 Absatz 50 des Gesetzes vom 18.7.2016 (BGBl. I S. 1666)

Abkürzungsverzeichnis

WReg	Gesetz zur Einrichtung und zum Betrieb eines Registers zum Schutz des Wettbewerbs um öffentliche Aufträge und Konzessionen (Wettbewerbsregistergesetz)
WRP	Wettbewerb in Recht und Praxis (Zeitschrift)
WuW	Wirtschaft und Wettbewerb (Zeitschrift)
WuW/E	Wirtschaft und Wettbewerb, Entscheidungssammlung
ZAG	Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdienstenaufsichtsgesetz) vom 25.6.2009 (BGBl. I S. 1506), zuletzt geändert durch Artikel 14 des Gesetzes vom 11.3.2016 (BGBl. I S. 396)
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)
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. Bedeutung von Compliance und positive Wirkung von Compliance Management

Die Bedeutung von Compliance für Unternehmen und Verbände¹ geht über den Wortsinn der reinen Regelbefolgung bzw. Regelkonformität weit hinaus.² Wenn- gleich es an einer einheitlichen Definition fehlt, wird Compliance häufig als Summe derjenigen Maßnahmen verstanden, die der Einhaltung aller an Unter- nehmen gerichteten Gesetze und Regeln dienen.³ Im Mittelpunkt stehen organi- satorische Vorkehrungen zur Verhinderung von Regelverstößen, zur Aufdeckung von „Non-Compliance“, zur angemessenen Reaktion bzw. Sanktionierung, zur Vermeidung von Wiederholungsfällen sowie zur regelmäßigen Aktualisierung dieser Maßnahmen (**Compliance Management**).⁴

Neuere Entwicklungen in Rechtsprechung und Gesetzgebung zeigen, dass Compliance-Maßnahmen für Unternehmen und Verbände positive Wirkungen haben: Wie der Bundesgerichtshof in seinem Urteil vom 9.5.2017 ausdrücklich festge- stellt hat, ist bei Regelverstößen im Rahmen der Bußgeldbemessung von Bedeu- tung, inwieweit ein Unternehmen seiner Pflicht, Rechtsverletzungen aus der Sphäre des Unternehmens zu unterbinden, genügt und ein „effizientes Compli-

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

2 Zur Herkunft und Begriffsentwicklung von Compliance siehe *Klopp*, Der Compliance-Beauftragte, 2012, 21 ff.; *Kutschelis*, Korruptionsprävention und Geschäftsleiterpflichten im nationalen und internationalen Unternehmensverbund, 2014, 90 f.; *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, 2017, 32 ff.; *Balke*, in: Born/Ghassemi-Tabar/Gehle (Hrsg.) MHdBGesRVII, 6. Aufl. 2020, § 104, Rn. 2.

3 *Klopp*, Der Compliance-Beauftragte, 2012, 22 f. m. w. N.; ferner *Lelley*, Compliance im Arbeitsrecht, 2010, 9 ff.; *Schmidt*, Compliance in Kapitalgesellschaften, 2010, 18 ff.; v. *Marnitz*, Compliance-Management für mittelständische Unternehmen, 2011, 1 ff.; *Balke*, in: Born/Ghassemi-Tabar/Gehle (Hrsg.), MHdBGesRVII, 6. Aufl. 2020, § 104, Rn. 2.

4 Vgl. *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, 2017, 34 ff.; *Balke*, in: Born/Ghassemi-Tabar/Gehle (Hrsg.) MHdBGesR VII, 6. Aufl. 2020, § 104, Rn. 2 sowie *Rodewald/Unger*, BB 2006, 113; *Hoffmann/Schieffer*, NZG 2017, 401 so- wie *Schulz*, BB 2017, 1475 m. w. N.

ance-Management“ installiert hat.⁵ Als zentrales Element eines Compliance-Systems gilt dabei „das präventive Bemühen um eine weitgehende Eindämmung von Rechtsverstößen, die aus dem Unternehmen heraus begangen werden“.⁶

- 3 Die positive Wirkung von Compliance Management bei der Beurteilung von Normverletzungen spielt auch eine zentrale Rolle im **Regierungsentwurf eines Gesetzes zur Stärkung der Integrität der Wirtschaft (Verbandssanktionsgesetz – VerSanG-E)**.⁷ Dieser Gesetzentwurf verfolgt ausdrücklich das Ziel, Compliance-Maßnahmen in Verbänden und Unternehmen zu fördern und hierfür normative Anreize zu setzen.⁸ So sollen sich „Vorkehrungen zur Vermeidung und Aufdeckung von Verbandsstraftaten“ (d. h. Compliance-Maßnahmen) unter anderem auf die Höhe der vorgeschlagenen Verbandsgeldsanktion auswirken.⁹ Die Wertschätzung ist dabei sowohl für Maßnahmen vor der Verbandstat, als auch für solche intendiert, die erst nach der Verbandstat getroffen werden.¹⁰ Ferner sieht der Regierungsentwurf die Möglichkeit vor, die geplante Verbandsgeldsanktion unter Vorbehalt zu verhängen und den Vorbehalt mit der Weisung zu verbinden, dass Compliance-Vorkehrungen getroffen und von einer sachkundigen Stelle überprüft werden.¹¹ Die in § 3 VerSanG-E vorgesehene Verantwortlichkeit von Leitungspersonen scheidet im Umkehrschluss aus, wenn die (Verbands-)Straftat durch angemessene Vorkehrungen wesentlich erschwert wurde.¹² Allerdings wird aus der Begründung des VerSanG-E deutlich, dass eine Wertschätzung nur erfolgen kann wenn die Compliance-Maßnahmen wirksam sind und funktionieren. Erweisen sie sich dagegen nur als „Papiertiger“, können sich solche vorgeblichen Compliance-Maßnahmen sogar sanktionsverschärfend aus-

5 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.

6 So ausdrücklich *Raum*, Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten, in: Hastenrath, Compliance-Kommunikation, 2017, S. 31, 33.

7 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>.

8 Vgl. Regierungsentwurf „Entwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft“, 1, 55 f., 95 f. Siehe auch *Böttger*, Kap. 2, Rn. 15 ff., 142 f.

9 Vgl. § 15 Abs. 1 Nr. 2 VerSanG-E.

10 Vgl. Regierungsentwurf „Entwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft“, 55 f., sowie *Ott/Lüneborg*, CCZ 2020, 1361, 1363.

11 Ebenso *Ott/Lüneborg*, CCZ 1361, 1362 f.

12 *Schulz/Block*, CCZ 2020, 49, 50.

wirken.¹³ Damit schafft der Gesetzgeber – im Einklang mit den Grundsätzen in dem oben genannten Urteil des Bundesgerichtshofes vom 9.5.2017 – normative Anreize sowohl für die Einführung von Compliance-Maßnahmen als auch für Verbesserungsmaßnahmen an bereits bestehenden Compliance-Systemen nach Eintritt von Regelverstößen.¹⁴

2. Compliance Management als Inbegriff rechtskonformer Verbandsorganisation

Im Fokus der anhaltenden Diskussion um Compliance und ihre Sicherstellung durch Compliance Management in Form effektiver Strukturen, Prozesse und Systeme stehen folgende Fragen: **4**

- Wie lassen sich die vielfältigen Risiken und Nachteile aus Regelverletzungen („Non-Compliance“) bestmöglich verhindern oder reduzieren.¹⁵
- 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?¹⁶

Diese Grundfragen einer rechtskonformen Unternehmens- und Verbandsorganisation¹⁷ betreffen grundsätzlich alle Unternehmen und Verbände, von der börsennotierten Aktiengesellschaft und der mittelständischen GmbH bis hin zum sog. „Start-up-Unternehmen“.¹⁸ Denn sämtliche Unternehmen und Verbände sowie ihre Leitungsorgane müssen bei ihrer Tätigkeit eine Vielzahl von Normen **5**

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

14 Vgl. § 15 Abs. 3 Nr. 7 VerSanG-E.

15 Vgl. *Merk*, ZIP 2014, 1705, 1706; v. *Marnitz*, Compliance-Management für mittelständische Unternehmen, 2011, 1 ff.; *Jenne*, Zur Überprüfung und Zertifizierung von Compliance-Management-Systemen, 2017, 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.“

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

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

18 Zur Relevanz von Compliance für sog. Start-up-Unternehmen siehe *Nothelfer*, CCZ 2016, 64; zur Relevanz für kleinere und mittelständische Unternehmen siehe u. a. *Merk*, ZIP 2014, 1705 ff. Zur Bedeutung von Compliance für die AG siehe etwa *Harbarth*, ZHR 179 (2015), 136, sowie *Fleischer*, in: *Spindler/Stilz*, AktG, 4. Aufl. 2019, § 91 Rn. 47 ff.

und rechtlichen Vorgaben von Gerichten und Behörden beachten.¹⁹ Zahlreiche aktuelle Fälle von „Non-Compliance“ bei Unternehmen und Verbänden aus ganz unterschiedlichen Branchen, mit unterschiedlichen Geschäftsmodellen und mit unterschiedlicher Größe und Struktur²⁰ zeigen, dass die Beantwortung dieser Fragen offenbar für viele Unternehmen nach wie vor eine Herausforderung bzw. eine kaum lösbare Aufgabe darstellt.²¹ Dies gilt trotz der Tatsache, dass inzwischen viele Verbände und Unternehmen über Compliance-Programme bzw. ein Compliance-Management-System (CMS) verfügen.²²

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

- 6 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

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

20 Zu prominenten Fällen von „Non-Compliance“ und damit verbundener Nachteile und Kosten siehe *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, 2017, 21 ff.; *Gomer*, Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft, 2020, 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-Q52XQE2S6VHQ3JKPGFQKWWMRS4.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“ siehe u. a.: <https://www.rnd.de/wirtschaft/chronologie-des-dieselskandals-das-schmutzigste-kapitel-der-vw-geschichte-PZZDQRN5LRELVGB35C2KDU6K7Y.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.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-at-tacke-fakten-zum-globalen-cyber-angriff-a-1147523.html>. Compliance-Verstöße sind häufig auch Gegenstand von Kartellverfahren der EU-Kommission, siehe etwa: <https://www.spiegel.de/wirtschaft/unternehmen/bmw-daimler-und-vw-unter-kartellverdacht-eu-kommission-verschaerft-ermittlungen-a-1228660.html>; oder: <https://www.spiegel.de/wirtschaft/unternehmen/wilke-wurst-behoerdenbericht-zeigt-zustaeude-nach-fabriksschliessung-a-1293802.html> (alle Quellen zuletzt abgerufen am 24.9.2020).

21 Vgl. etwa *Schulz*, CB 08/2017, I (Editorial); exemplarisch auch folgende Studie: „The Future of Compliance 2018: Herausforderungen und Trends“, https://www.compliance-manager.net/sites/default/files/dateien/the_future_of_compliance_2018.pdf (zuletzt abgerufen am 24.9.2020).

22 Vgl. *Neufang*, IRZ 2017, 249.

und können existenzbedrohende Ausmaße annehmen.²³ Die Nachteile umfassen unter anderem:²⁴

- strafrechtliche Sanktionen gegen die Geschäftsleiter, sonstige Verantwortliche und involvierte Unternehmensangehörige;
- strafrechtliche Sanktionen gegen das Unternehmen bzw. den Verband;²⁵
- Bußgelder gegen das Unternehmen selbst und die Geschäftsleiter;²⁶
- Entzug der Betriebserlaubnis bzw. Lizenz bis hin zur Zwangsliquidation;
- Nachzahlung von Steuern bzw. Strafzuschlägen;²⁷
- Verpflichtung zum Schadensersatz;
- „Vorteilsabschöpfung“ bei rechtswidrigen Geschäften (nach dem „Brutto-Prinzip“);
- Unwirksamkeit von Transaktionen, Nichtigkeit bzw. Anfechtbarkeit von Verträgen und sonstigen Rechtsgeschäften;
- Ausschluss von der Auftragsvergabe;²⁸
- 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.²⁹

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

23 Vgl. etwa *Schockenhoff*, ZHR 180 (2016), 197, 203 f.

24 Zum Spektrum der Compliance-Risiken siehe etwa *Leisch/Lohner*, M&A Review 2009, 133, 134.

25 Zur Ausweitung von Sanktionen durch das geplante Verbandssanktionengesetz siehe *Böttger*, Kap. 2, Rn. 15 sowie *Knauer*, NSTZ 2020, 441, 442 ff.

26 Zu den drastisch gestiegenen Bußgeldern bei Kartellrechtsverstößen sowie anderen Bußgeldern etwa *Schockenhoff*, ZHR 180 (2016), 197, 204 f. mit zahlreichen Beispielen. Zum Risiko drastischer Bußgelder bei Kartellrechtsverstößen siehe *Trüg/Ruppert*, ZWeR 2020, 69 ff. sowie *Seeliger/Heinen/Mross*, Kap. 23, Rn. 2, 87 ff.

27 Beispiele bei *Schockenhoff*, ZHR 180 (2016), 197, 204 f. Zur Tax Compliance siehe *Schwartz/Stürzl-Friedlein*, Kap. 25.

28 Zur Bedeutung von Compliance im Vergabeverfahren siehe *Scherer*, Kap. 24.

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

Unternehmen und Verbänden aus unterschiedlichen Branchen, mit unterschiedlichen Geschäftsmodellen und mit unterschiedlicher Größe und Struktur belegt.³⁰ Dabei beruhen Regelverletzungen einerseits auf vorsätzlichem Fehlverhalten bzw. kriminellen Aktivitäten von Personen (z.B. in Fällen von Korruptionsvergehen oder Kartellrechtsverstößen).³¹ In anderen Fällen ist die Ursache von „Non-Compliance“ fahrlässiges Verhalten durch Verletzung von Sorgfaltspflichten oder aufgrund unzureichender Kenntnis von Regeln und Geboten.³² Normative Vorgaben werden zum Teil nicht richtig eingeschätzt oder ihre dynamische (Weiter-)Entwicklung wird nicht hinreichend beachtet.³³

4. Funktionen von Compliance und Compliance Management

- 8 Die dargestellten Risiken und Nachteile aus „Non-Compliance“ zeigen, dass wirksame Compliance-Maßnahmen zur Vermeidung bzw. Reduzierung für alle Unternehmen und Verbände aktuell und relevant sind.³⁴ Die proaktive Vermeidung bzw. Reduzierung von Regelverstößen ist in allen Unternehmen und Verbänden damit eine wichtige Führungs- und Organisationsaufgabe.³⁵ Compliance Management erfüllt dabei die folgenden Funktionen:³⁶ 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 Leitungsgorga-

30 Vgl. zu aktuellen Fällen die Nachweise in Fn. 20. Zu prominenten Fällen von „Non-Compliance“ in der Vergangenheit etwa die Darstellung von *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, 2017, 21 ff.

31 Zu den diversen Straftatbeständen im Bereich der Korruption vgl. *Böttger*, Kap. 2, Rn. 29 ff. Zum Umgang mit Korruptionsrisiken in M&A-Transaktionen siehe *Ulrich*, Kap. 18, Rn. 77 ff. Zu den diversen Formen kartellrechtswidrigen Verhaltens siehe *Seeliger/Heinen/Mross*, Kap. 23, Rn. 10 ff.

32 Vgl. *Heißner*, Erfolgsfaktor Integrität, 2. Aufl. 2014, 114; *Busmann*, CCZ 2016, 50 ff.; *Preusche/Würz*, Compliance, 3. Aufl. 2020, 30 f.

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

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

35 Siehe dazu unter Rn. 27 ff. Ähnlich *Dittmers*, Werteorientiertes Compliance-Management, 2018, 29 m. w. N.; *Klopp*, Der Compliance-Beauftragte, 2012, 22 f. („Managementfunktion“) m. w. N., sowie *Kutschelis*, Korruptionsprävention und Geschäftsleiterpflichten im nationalen und internationalen Unternehmensverbund, 88 f., 98. Zur Bedeutung des sog. Corporate Reputation Management ausführlich *Seibt*, DB 2015, 171.

36 Zu den Funktionen von Compliance siehe *Hauschka*, Compliance im Gesellschaftsrecht, in: *Hadding/Hopt/Schimansky*, Verbraucherschutz im Kreditgeschäft – Compliance in der Kreditwirtschaft, 2008, 103 ff. sowie ausführlich *Gomer*, Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft, 2020, 73 ff.

ne und der Mitarbeiter.³⁷ Darüber hinaus zielen Compliance-Maßnahmen auch auf den Schutz vor Angriffen auf das Unternehmen sowie den Schutz der Unternehmensposition im Wettbewerb.³⁸ Ferner dient Compliance dem Schutz der Reputation und des Vertrauens der Stakeholder in eine ordnungsgemäße und rechtskonforme Geschäftstätigkeit.³⁹

Neben dieser präventiven **Schutzfunktion** ist auch die **Risikomanagementfunktion** wichtig, denn zwischen Compliance Management und Risikomanagement besteht ein enger Zusammenhang⁴⁰: Das Risikomanagement mit seinen Methoden und Verfahren ist eine wichtige Erkenntnisquelle für die Identifikation und systematische Erfassung von Compliance-Risiken.⁴¹

Das Compliance Management erfüllt ferner eine wichtige **Informations- und Beratungsfunktion**,⁴² welche sowohl die Beratung der Unternehmensleitung zur Steuerung von Compliance-Risiken durch organisatorische Maßnahmen⁴³ als auch die Organisation der Beratung aller Unternehmensangehörigen in allen relevanten Compliance-Fragen umfasst.⁴⁴ Da zu den notwendigen organisatorischen Maßnahmen auch die kontinuierliche Überwachung und Kontrolle relevanter Normen und Regeln zählt,⁴⁵ erfüllt Compliance ferner eine **Monitoring-Funktion**.⁴⁶ 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**.⁴⁷ Indem ein wirksames Compliance Management dazu beiträgt, Normverstöße zu verhindern bzw. zu reduzieren, fördert es die Glaubwürdigkeit

37 Vgl. *Gößwein/Hohmann*, BB 2011, 963, 964 sowie *Gomer*, Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft, 2020, 73.

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

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

40 Vgl. *Schulz/Galster*, in: Bürkle/Hauschka, Der Compliance Officer, § 4 Rn. 12 ff. Zum Zusammenhang zwischen Compliance- und Riskomanagement siehe unter Rn. 39 ff. sowie ausführlich *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019.

41 Vgl. *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 632, 646 ff.

42 Vgl. *Inderst*, in: Inderst/Bannenber/Poppe, S. 136 f.; *Lösler*, NZG 2005, 104, 105; sowie *Gomer*, Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft, 2020, 75 f.

43 Vgl. *Schulz/Renz*, BB 2012, 2511.

44 Vgl. *Klopp*, Der Compliance-Beauftragte, 2012, S. 57.

45 Vgl. *Klopp*, Der Compliance-Beauftragte, 2012, S. 57 f.

46 Vgl. *Lösler*, NZG 2005, 104, 105.

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

des Unternehmens bei seinen Mitarbeitern, Kunden, Geschäftspartnern und sonstigen Stakeholdern und erfüllt damit eine **Marketing-Funktion**.⁴⁸

5. Permanente Aufgabe im dynamischen regulatorischen Umfeld

- 11 Die Flut der rechtlichen Vorgaben und Anforderungen betrifft alle Unternehmensbereiche und speist sich aus allen Quellen des Zivilrechts, des öffentlichen Rechts und des Strafrechts.⁴⁹ Die Sicherstellung rechtskonformer Tätigkeit durch Compliance Management ist anspruchsvoll, denn mit jeder Art der unternehmerischen Tätigkeit 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.⁵⁰ Auch Korruption und Kartellrechtsverstöße zählen für viele Verbände zu den zentralen Compliance-Risiken ihrer Geschäftstätigkeit.⁵¹ Auch in vielen Bereichen der Unternehmensfinanzierung bestehen komplexe Rechts- und Compliance-Risiken.⁵² Hinzu kommen neue bzw. erweiterte Rechtspflichten aus neuen Gesetzen und Regelungsvorhaben. So hat die **Datenschutzgrundverordnung (DSGVO)** von 2018⁵³ das für alle Unternehmen geltende Pflichten- (und Sanktions-)Spektrum in Bezug auf die Beachtung und Umsetzung datenschutzrechtlicher Vorgaben erheblich erweitert.⁵⁴ Über Datenschutzerfordernisse hinausgehend wirft die Digitalisierung weitere Rechtsfragen und damit verbundene besondere Compliance-Risiken auf, etwa im Hinblick auf den rechtssicheren Einsatz sog. „Smart Contracts“ oder der Haftung für autonome Systeme.⁵⁵ Die Gewährleistung einer funktionierenden IT-Sicherheitsstruktur stellt sich im Zeitalter von „Big Data“ als eine komplexe und

48 Vgl. *Lösler*, NZG 2005, 104, 105; *Klopp*, Der Compliance-Beauftragte, 2012, S. 58 f.; *Gomer*, Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft, 2020, 78 f.

49 *Schulz*, Rechtliches Risikomanagement und Compliance im Mittelstand, in: Kessler, Unternehmensfinanzierung Mittelstand, 2014, § 6 Rn. 4. Ferner *Schmidt*, Compliance in Kapitalgesellschaften, 2010, 17 mit dem Hinweis auf Schätzungen, wonach (bereits 2010) durchschnittlich 900 Vorschriften pro Unternehmen zu beachten sein sollten.

50 Vgl. *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 105 ff.

51 Vgl. *Schockenhoff*, ZHR 180 (2016), 197, 204; *Kort*, in: Hirte/Mülbert/Roth, AktG, 5. Aufl. 2015, § 91 Rn. 126; *Trüg/Ruppert*, ZWeR 2020, 69 ff.

52 Vgl. *Schulz*, Rechtliches Risikomanagement und Compliance im Mittelstand, in: Kessler, Unternehmensfinanzierung Mittelstand, 2014, § 6 Rn. 23.

53 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.

54 Siehe hierzu ausführlich *Becker/Böhlke/Fladung*, Kapitel 11.

55 Siehe hierzu weitere Beispiele und Nachweise bei *Schulz*, Digitale Transformation – Herausforderung und Chance für Rechtsanwälte, in: Schulz/Hartung (Hrsg.), Recht 2030 – Legal Management in der Digitalen Transformation, Kap. 2, 29 ff., sowie *Jacobs*, in: Schulz/Hartung (Hrsg.), a. a. O., Kap. 22, Rn. 1 ff.; *von Bodungen*, in: Sassenberg/Faber (Hrsg.), Rechts-handbuch Industrie 4.0 und Internet of Things, 2017, 361 ff.

anspruchsvolle Daueraufgabe des Compliance Managements dar,⁵⁶ insbesondere hinsichtlich der Gewährleistung einer nachhaltigen **Cyber-Security**.⁵⁷ Immer wichtiger wird für Unternehmen und Verbände ferner die Prävention und Kontrolle von Geldwäsche-Risiken (nicht zuletzt im Zusammenhang virtueller Währungen).⁵⁸ Die Erfüllung der damit verbundenen umfangreichen gesetzlichen Compliance-Pflichten reicht inzwischen weit über den Finanzdienstleistungssektor hinaus und erfasst unter anderem sog. Güterhändler.⁵⁹ Zudem sieht ein neuer Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz eine erhebliche **Ausweitung des Geldwäschestrafatbestands** (§ 261 StGB) vor.⁶⁰ Um die Effektivität der Strafverfolgung von Geldwäschedelikten zu erhöhen, sollen zukünftig Vermögenswerte aus sämtlichen Straftaten Gegenstand einer Geldwäsche sein können. Dadurch wird das Risiko einer Geldwäschestrafbarkeit und damit die Bedeutung geeigneter Präventionsmaßnahmen deutlich erhöht.

Herausforderungen bringt für viele Unternehmen auch die **EU-Whistleblower-Richtlinie** mit sich, die bis zum 17.12.2021 in deutsches Recht umzusetzen ist.⁶¹ Danach werden juristische Personen ab bestimmten Schwellenwerten (z. B. Unternehmen ab 50 Arbeitnehmern und Gemeinden ab 10.000 Einwohnern) u. a. verpflichtet sein, Hinweisgebersysteme einzurichten und hierfür interne Meldekanäle vorzuhalten. Diverse Einzelfragen wie etwa der Schutzzumfang für den Hinweisgeber sind noch nicht abschließend geklärt: Dies gilt insbesondere im Hinblick auf (konfligierende) Pflichten zur Vertraulichkeit nach dem **Geschäftsgeheimnisgesetz (GeschGehG)**, da auch Informationen zu etwaigen Rechtsverstößen als Geschäftsgeheimnisse angesehen werden können.⁶² Das Geschäftsgeheimnisgesetz, das am 26.4.2019 in Kraft getreten ist, verpflichtet Unternehmen zu angemessenen Geheimhaltungsmaßnahmen in Bezug auf Geschäftsgeheimnisse (§ 2 Nr. 1 lit. b GeschGehG) und erweitert damit ebenfalls den Katalog erforderlicher Compliance-Maßnahmen.⁶³

56 Schulz, BB 2019, 579. Zur Cyber Security und IT-Compliance siehe etwa *Daghles*, DB 2018, 2289 ff.; *Mehrbrey/Schreibauer*, MMR 2016, 75, sowie *Jacobs*, CB 2017, 299.

57 Zu „Cyber Risks“ als neuem Brennpunkt der Managerhaftung *Schmidt-Versteyl*, NJW 2019, 1637. Zu IT-Compliance und *Cyber-Security* siehe von *Jacobs*, Kap. 12, Rn. 33 ff. und *Bensinger*, Kap. 13.

58 Siehe *Komma*, Kap. 21 sowie *Krais*, Geldwäsche und Compliance, 2018. Zu Stellung und Aufgabe des Geldwäschebeauftragten ausführlich *Kaetzler*, Kap. 20.

59 Siehe *Komma*, Kap. 21.

60 Entwurf eines Gesetzes zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche, www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Geldwaesche_Bekaempfung.html (abgerufen am 23.10.2020).

61 Siehe: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32019L1937> (zuletzt abgerufen am 24.9.2020) und hierzu *Garden/Hiéramente*, BB 2019, 963.

62 Vgl. *Garden/Hiéramente*, BB 2019, 963, 967.

63 Vgl. *Ohly*, GRuR 2019, 441 m. w. N.

- 13 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“).⁶⁴ Dabei gewinnt auch die proaktive Compliance-Kontrolle von Geschäftspartnern, Vertriebsmittlern und sonstigen Intermediären immer größere Bedeutung („Business Partner Compliance“).⁶⁵
- 14 Exportorientierte Unternehmen müssen zahlreiche Vorgaben des Außenwirtschaftsrechts sowie im anwendbaren Umfang auch die Normen anderer Rechtsordnungen beachten.⁶⁶ Zu zahlreichen nationalen Vorgaben und solchen des Unionsrechts kommen darüber hinaus normative Anforderungen anderer Rechtsordnungen bei einem grenzüberschreitenden Bezug der Unternehmens-tätigkeit hinzu.⁶⁷
- 15 Im Rahmen arbeitsteiliger (häufig internationaler) Produktion spielen zudem Compliance-Risiken von Geschäftspartnern (Stichwort: „**Compliance in der Lieferkette**“) eine immer größere Rolle.⁶⁸ Während es in anderen Rechtsordnungen hierzu bereits (zum Teil auch extraterritorial anwendbare) Normen gibt, greift auch der deutsche Gesetzgebers das Thema auf, wie das derzeit von der Bundesregierung geplante „**Lieferketten-Gesetz**“ verdeutlicht.⁶⁹ In Ausführung des „Nationalen Aktionsplans“ (NAP) zur Umsetzung der Leitprinzipien für Wirtschaft und Menschenrechte von 2016 soll für Unternehmen mit mehr als 500 Beschäftigten unter anderem eine sog. „mensenrechtliche Sorgfaltpflicht“ („Human Rights Due Diligence“) eingeführt werden. Danach sollen die betroffenen Unternehmen ihre Lieferketten unter anderem einer fortlaufende Risikoanalyse und Bewertung der Verletzungsrisiken in Bezug auf Menschenrechte unterziehen, angemessene Präventions- bzw. Abhilfemaßnahmen sowie einen Beschwerdemechanismus zugunsten von Betroffenen einführen und bestimmte Dokumentations- und Berichtspflichten einführen. Durch diese neuen Compliance-Pflichten in Bezug auf die Wertschöpfungsnetzwerke werden die Strukturen und Prozesse der Geschäftspartner-Prüfung („Business Partner Screening“) weiter an Bedeutung gewinnen.
- 16 Weitere rechtliche Anforderungen richten sich nach der jeweiligen Branche sowie einzelfallspezifischen Faktoren wie Unternehmensgröße, Unternehmensstruktur, Geschäftsmodell oder internationaler Geschäftstätigkeit.⁷⁰

64 Zum Compliance Management bei M&A-Transaktionen ausführlich *Ullrich*, Kap. 18.

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

66 Siehe dazu unter Rn. 47 ff. Zu Compliance-Fragen im Zusammenhang mit der Export-Kontrolle siehe *von Bodungen*, Kap. 26.

67 Vgl. *Wiedmann/Greubel*, CCZ 2019, 88, 93.

68 Zu Compliance-Fragen im Rahmen des sog. „Supply Chain Management“ aus Management-Sicht siehe *Schleper/Förstl*, Kap. 16, Rn. 5 ff.

69 Siehe zu dem geplanten Lieferketten-Gesetz *Baier*, DB 2020, 1801.

70 Zur Relevanz dieser Kriterien für Compliance und Risikomanagement siehe *Merkt*, ZIP 2014, 1705 ff.

6. Erweiterung von Organisationspflichten durch Gerichte

Auch die Gerichte schaffen bzw. erweitern kontinuierlich ein umfangreiches rechtliches Pflichtenspektrum für Unternehmen und Verbände sowie deren Leitungsorgane.⁷¹ Die Haftung von Geschäftsleitern für Fehlverhalten (sog. Organhaftung) wurde kontinuierlich ausgeweitet,⁷² die Gerichte haben weitreichende Anforderungen auf der Basis sogenannter Unternehmensorganisationspflichten, Verkehrssicherungspflichten und Garantienpflichten entwickelt.⁷³ 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.⁷⁴ Bei juristischen Haftungsfragen in Fällen von „Non-Compliance“ steht häufig die Verletzung rechtlicher Organisationsanforderungen an die Geschäftsleitung im Mittelpunkt.⁷⁵ 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.⁷⁶ Seine Organisationspflicht zur Verhinderung von Rechtsverletzungen erfüllt der Vorstand, „wenn er eine auf Schadensprävention und Risikokontrolle angelegte Compliance-Organisation einrichtet“, die der jeweiligen Gefährdungslage entspricht.⁷⁷ 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.⁷⁸ Dabei orientiert sich das Gericht an den Leitlinien zur Compliance-

71 Siehe die aktuellen Beispiele aus Gesetzgebung und Rechtsprechung bei *Hauschka/Moosmayer/Lösler*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 1 Rn. 28 ff., 33 ff.; ferner *Schulz*, Rechtliches Risikomanagement und Compliance im Mittelstand, in: Kessler, Unternehmensfinanzierung Mittelstand, 2014, § 6 Rn. 4.

72 Vgl. *Lutter*, Entwicklung der Organpflichten und der Organhaftung, in: *Lutter/Krieger*, Handbuch Managerhaftung, 2. Aufl. 2010, 1, 5 ff.

73 Zur Entwicklung von Verkehrssicherungspflichten sowie Unternehmensorganisationspflichten umfassend *Spindler*, Unternehmensorganisationspflichten, 2001; *Matusche-Beckmann*, Organisationsverschulden, 2001, 37 ff. Vgl. ferner *Rack*, CB 2014, 104. Zum Konzept der strafrechtlichen Garantienpflichten siehe *Spindler*, Handbuch des Vorstandsrechts, 2006, § 15 Rn. 68 ff., sowie *Böttger*, Kap. 2, Rn. 121, 132 ff.

74 Vgl. *Schulz*, Rechtliches Risikomanagement und Compliance im Mittelstand, in: Kessler, Unternehmensfinanzierung Mittelstand, 2014, § 6 Rn. 4.

75 Vgl. *Meyer*, DB 2014, 1063.

76 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.

77 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.; *Meyer*, DB 2014, 1063 ff. Der Rechtsstreit endete durch Vergleich, das Urteil enthält jedoch grundlegende Aussagen zu allgemeinen Anforderungen an ein wirksames Compliance Management.

78 *Schulz/Held*, Sicherstellung funktionierender Compliance als Organisationspflicht des Vorstands, juris Praxis Report Compliance 1/2014; *Rack*, CB 2014, 104.

Verantwortung der Unternehmensleitung, welche Wissenschaft und Praxis formuliert haben.⁷⁹

7. Beachtung von Compliance-Anforderungen anderer Rechtsordnungen

- 18 Für international tätige Unternehmen können sich Anforderungen und Vorgaben für das Compliance Management auch aus anderen Rechtsordnungen ergeben. Dies gilt insbesondere für Compliance-Anforderungen des anglo-amerikanischen Rechts, da die extraterritoriale Geltung häufig bereits bei geringfügiger (Geschäfts-)Verbindung mit anderen Rechtsordnungen eintritt.⁸⁰ Die erforderliche Berücksichtigung der Compliance-Anforderungen der jeweils anwendbaren Rechtsordnung erhöht einerseits die Komplexität der Konzeption und Ausgestaltung des Compliance Managements. Andererseits können derartige Vorgaben als wertvolle Orientierungshilfen dienen, wie sich am Beispiel des anglo-amerikanischen Rechts zeigen lässt (siehe dazu unter Rn. 47 ff.).

8. Compliance Management im Kontext aktueller Entwicklungen von Corporate Governance und Corporate Social Responsibility

- 19 Zur wachsenden Bedeutung von Compliance Management tragen auch ein erweitertes Verständnis und höhere Erwartungen der Stakeholder in Bezug auf **verantwortungsvolle Unternehmensführung** bei.⁸¹ Dies zeigen aktuelle Diskussionen zu **Corporate Governance** und **Corporate Social Responsibility (CSR)**.⁸² Unternehmen und Verbände sehen sich immer stärker mit normativen Anforderungen und Erwartungen ihrer Geschäftspartner konfrontiert, ebenso wie mit solchen ihrer Bezugsgruppen bzw. Stakeholder (Mitarbeiter, Kunden, Lieferanten, Investoren etc.) und der Öffentlichkeit im Hinblick auf ein verantwortungsvolles, d. h. integres und ethisch einwandfreies Geschäftsverhalten.⁸³ Die Grenzen zwischen rechtlichen Anforderungen und Anforderungen der Corporate Social Responsibility (CSR) sind teilweise fließend, im Hinblick auf notwendige Maßnahmen der Unternehmen und Verbände für ihren Image- und Reputationsschutz aber in vielen Fällen von vergleichbarer Bedeutung.⁸⁴

79 Vgl. *Fleischer*, in: Spindler/Stilz, AktG, 4. Aufl. 2019, § 91 Rn. 47 ff.; *Hauschka/Moosmayer/Lösler*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 1 Rn. 29 ff.

80 Siehe *Hauschka/Moosmayer/Lösler*, § 1, Rn. 73 ff.; *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, 203 ff.

81 Vgl. etwa *Siedenbiedel*, Corporate Compliance, 2014, 48 f. Zum Zusammenhang zwischen Compliance und CSR siehe *Stehr/Knopp*, Kap. 14.

82 Vgl. *Spießhofer*, Unternehmerische Verantwortung, 2017. Weitere Nachweise bei *Stehr/Knopp*, Kap. 14.

83 Vgl. *Spießhofer*, Unternehmerische Verantwortung, 2017, 25 ff., 34 f.; *Vetter*, ZGR 2018, 338, 360 ff.; *Siedenbiedel*, Corporate Compliance, 2014, 48 f.

84 Zur „Verrechtlichung“ von (vormals freiwilligen) Anforderungen der Corporate Social Responsibility (CSR) siehe *Spießhofer*, Unternehmerische Verantwortung, 2017, 574 ff. Zur Be-

Der **Deutsche Corporate Governance Kodex (DCKG)**⁸⁵ als sog. „Soft Law“²⁰ stellt auf den Zusammenhang mit Compliance und CSR an verschiedenen Stellen ab. So heißt es etwa in Abs. 1 Satz 3 der Präambel, die Prinzipien (der sozialen Marktwirtschaft unter Berücksichtigung der Belange der Aktionäre, der Belegschaft und der sonstigen Stakeholder) verlangen nicht nur Legalität, sondern auch ethisch fundiertes, eigenverantwortliches Verhalten (**Leitbild des Ehrbaren Kaufmanns**). Wenngleich die Aufnahme dieser Formulierung ebenso wie die Orientierung am Leitbild des Ehrbaren Kaufmanns kontrovers diskutiert werden, wird die wachsende Bedeutung von Aspekten der Wirtschaftsethik deutlich.⁸⁶ Die Bedeutung von CSR zeigt auch Abs. 2 Satz 1 der Präambel, wonach sich die Gesellschaft und ihre Organe in ihrem Handeln „der Rolle des Unternehmens in der Gesellschaft und ihrer gesellschaftlichen Verantwortung bewusst zu sein haben“.⁸⁷

Nach der Empfehlung A.2 des DCKG soll der Vorstand für ein an der Risikolage des Unternehmens ausgerichtetes Compliance Management System sorgen und dessen Grundzüge offenlegen. Dabei soll Beschäftigten ebenso wie Dritten die Möglichkeit eingeräumt werden, geschützt Hinweise auf Rechtsverstöße im Unternehmen zu geben.²¹

Die höhere Bedeutung von CSR entspricht dem neueren Begriffsverständnis,⁸⁸ wonach **Corporate Social Responsibility** nicht mehr nur Gegenstand freiwilliger Selbstverpflichtung ist, sondern die Verantwortung von Unternehmen für ihre Auswirkungen auf die Gesellschaft beschreibt: Dabei markiert die Einhaltung des geltenden Rechts (Compliance) nur das Minimum unternehmerischer Verantwortung, Unternehmen sollen darüber hinaus aber auch Auswirkungen auf soziale, ökologische, wirtschaftsethische Belange sowie die Menschenrechte berücksichtigen.⁸⁹ Viele Unternehmen integrieren Fragen nach ihrer gesellschaft-

deutung des sog. Reputationsmanagements näher unten Rn. 23 ff. Zum Zusammenhang von Compliance und CSR siehe *Stehr/Knopp*, Kap. 14.

85 Vgl. Deutscher Corporate Governance Kodex, Fassung vom 16. Dezember 2019 mit Beschlüssen aus der Plenarsitzung vom 16. Dezember, <https://www.dcgk.de/de/kodex/aktuelle-fassung/praeambel.html> (zuletzt abgerufen am 24.9.2020).

86 Vgl. *Illert*, in: *Johannsen-Roth/Illert/Ghassemi-Tabar*, DCGK, 2020, Präambel, Rn. 3, Rn. 6 ff.; vertiefend: *Jüttner/Barnutz*, CCZ 2020, 250 ff.; *Spießhofer*, IWRZ 2019, 65 ff.; *Kort*, NZG 2012, 926 ff.; *Uhrmacher*, BC 2010, 85 ff.; *Wicke*, DNotZ 2020, 448 ff.

87 Vgl. *Illert*, in: *Johannsen-Roth/Illert/Ghassemi-Tabar*, DCGK, 2020, Präambel, Rn. 6; *Walden*, NZG 2020, 50 ff.; *Velte*, NZG 2020, 12 ff.; Begründung des DCGK 2020, 6, https://www.dcgk.de/files/dcgk/usercontent/de/download/kodex/191216_Begrueundung_DCGK.pdf (zuletzt abgerufen am 24.9.2020).

88 Zum Begriffsverständnis und neueren Entwicklungen der Corporate Social Responsibility siehe ausführlich *Spießhofer*, *Unternehmerische Verantwortung*, 2017, 25 ff., sowie *Stehr/Knopp*, Kap. 14, Rn. 11 ff. und *Beisheim/Dopychai*, Kap. 15.

89 *Spießhofer*, in: *Hauschka/Moosmayer/Lösler*, *Corporate Compliance*, 3. Aufl. 2016, § 11 Rn. 5 ff.

lichen Verantwortung in die Erklärung ihrer Unternehmenswerte, z.B. im Rahmen eines **Code of Conduct**.⁹⁰

9. Verbindungslinien zum Reputationsmanagement

- 23** Wie die aktuelle Diskussion um Corporate Social Responsibility zeigt, wird der unternehmerische Verantwortungsbereich durch diverse CSR-Vorgaben und Initiativen für verantwortliches gesellschaftliches Handeln erweitert, ohne dass dabei die Frage nach dem wünschenswerten Umfang unternehmerischer Verantwortung einerseits und dem rechtlich zulässigen Maß der Begrenzung unternehmerischer Aktivität andererseits stets im Einzelnen geklärt wäre.⁹¹ Zu bereits existierenden und oben exemplarisch skizzierten umfangreichen Rechtspflichten tritt ein Trend der „Verrechtlichung“ unterschiedlicher Anforderungen des „Soft Law“ hinzu, wie dies etwa die Pflicht zur CSR-Berichterstattung, die erforderlichen Compliance-Maßnahmen nach der EU-Konfliktmineralien-Verordnung⁹² oder die geplanten menschenrechtliche Sorgfaltspflicht in dem geplanten Lieferketten-Gesetz verdeutlichen.⁹³ Diese Beispiele zeigen: Von Erwartungen an Integrität und verantwortungsvolles Unternehmertum bis hin zu Rechtspflichten und deren Durchsetzung kann es im Kontext neuer Entwicklungen teilweise nur ein kleiner Schritt sein – es entwickelt sich ein neuer Bereich der „CSR-Compliance“.⁹⁴
- 24** Die Beachtung von CSR-Anforderungen kann im Interesse der Sicherung der Unternehmensreputation auch jenseits der Rechtsverbindlichkeit geboten sein. Die Reputation eines Unternehmens gilt als bedeutender immaterieller Vermögensgegenstand.⁹⁵ Die sog. Image- und Reputationsschäden sind häufig schwer zu beziffern, sie können aber zu erheblichen Verlusten und Nachteilen bis hin zu einem Einbruch des Börsenwerts führen.⁹⁶ Der Schutz der Reputation spielt daher eine zentrale Rolle, das positive Image des Unternehmens in der Öffentlichkeit und bei den maßgeblichen Bezugsgruppen (Mitarbeiter, Kunden,

90 Zu Grundlagen und Gestaltung eines *Code of Conduct* siehe ausführlich *Benkert*, Kap. 4.

91 Vgl. *Spießhofer*, in: Hauschka/Moosmayer/Lösler, *Corporate Compliance*, 3. Aufl. 2016, § 11 Rn. 5 ff.

92 Siehe <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32017R0821> (zuletzt abgerufen am 24.9.2020) sowie hierzu *Teicke*, CCZ 2018, 274.

93 Vgl. *Spießhofer*, in: Hauschka/Moosmayer/Lösler, *Corporate Compliance*, 3. Aufl. 2016, § 11 Rn. 43 sowie *dies.*, *Unternehmerische Verantwortung*, 2017, 311 ff., 415 ff. Zur CSR-Berichterstattungspflicht ausführlich *Beisheim/Dopychai*, Kap. 15. Zur Diskussion um das geplante Lieferketten-Gesetz vgl. etwa: *Rünz*, ZVertriebsR 2020, 291 ff.; *Rudkowski*, RdA 2020, 232 ff.; *Mittwoch*, RiW 2020, 397 ff.; *Püschel/Wiedmann*, *Newsdienst Compliance* 2020, 211001; *Redaktion beck-aktuell*, becklink 2017272.

94 So ausdrücklich *Beisheim/Dopychai*, Kap. 15.

95 Vgl. *Kröger*, *Korruptionsschäden, Unternehmensgeldbußen und Imageschäden*, 2013, 261 f.; *Simons*, ZGR 2018, 316; *Spindler*, in: *Goette/Habersack/Kalss*, AktG, 5. Aufl. 2019, Rn. 114.

96 Vgl. *Kröger*, *Korruptionsschäden, Unternehmensgeldbußen und Imageschäden*, 2013, 256 f.

Lieferanten, Investoren etc.) kann durch „Non-Compliance“ nachhaltig beeinträchtigt oder ganz zerstört werden.⁹⁷ Reputationsrisiken und „Reputationsmanagement“ haben sich zu wichtigen Themen für das Compliance- und Risikomanagement entwickelt.⁹⁸ Somit ist die Identifikation und Steuerung von Reputationsrisiken ein wichtiger Bestandteil des Compliance Managements.⁹⁹

Da die Missachtung ethischer Verhaltenserwartungen der Stakeholder ebenso zu Imageschäden und Reputationseinbußen führen kann wie die Missachtung rechtlicher Vorgaben,¹⁰⁰ sollte die Unternehmensleitung im Einzelfall erwägen, zum Schutz vor Reputationsverlusten auf eine Gewinnoptimierung aus ethischen Aspekten zu verzichten.¹⁰¹ Wie die im **Nachhaltigen Aktionsplan (NAP)**¹⁰² formulierten Erwartungen der Regierung an verantwortliches Handeln der Unternehmen und die damit verbundene Diskussion um die Notwendigkeit eines sog. „Lieferkettengesetzes“ exemplarisch zeigen, kann es sich für die jeweilige Unternehmensleitung empfehlen, das eigene Geschäftsmodell und die Unternehmensstrategie nicht allein auf Rechtskonformität, sondern auch auf ethisch einwandfreie Gestaltungen hin zu überprüfen.

Die gezeigten Beispiele umfangreich bestehender Rechtspflichten sowie neuer Anforderungen und weitergehender Trends zur „Verrechtlichung“ vormals freiwilliger Verantwortungsbereiche verdeutlichen, dass Compliance Management für Unternehmen und Verbände sowie deren Leitungsorgane eine dauerhafte und anspruchsvolle Aufgabe ist.¹⁰³ Infolge vielfältiger, komplexer sowie teils unklarer bzw. auslegungsbedürftiger Vorgaben müssen Entscheidungen häufig unter Rechtsunsicherheit getroffen werden.¹⁰⁴

97 Vgl. *Hauschka*, Compliance im Gesellschaftsrecht, in: Hadding/Hopt/Schimansky, Verbraucherschutz im Kreditgeschäft – Compliance in der Kreditwirtschaft 2008, 103, 106.

98 Siehe *Seibt*, DB 2015, 171 ff.; sowie *Seibt*, in: Schmidt/Lutter (Hrsg.), AktG, 4. Aufl. 2020, § 76, Rn. 42 ff. *Spindler*, in: Goette/Habersack/Kalss, AktG, 5. Aufl. 2019, Rn. 114. *Inderst*, Compliance Organisation und praktische Umsetzung, in: Inderst/Bannenberg/Poppe, Compliance, 3. Aufl. 2017, 127, 140 f.; *Seibt*, DB 2015, 171 ff.

99 Vgl. *Schlierenkämper*, in: Bürkle, Compliance in Versicherungsunternehmen, 3. Aufl. 2020, § 11 Rn. 70 ff.

100 *Schmidt*, Compliance in Kapitalgesellschaften, 2010, S. 22 f.

101 Vgl. *Seibt*, Börsenzeitung Nr. 31 v. 14.2.2015, S. 9. Zur Bedeutung ethischer Grundsätze siehe auch *Nietsch*, ZHR 180 (2016), 733, 762. Siehe auch *Simons*, ZGR 2018, 316, 321 f. sowie *Seibt*, in: Schmidt/Lutter (Hrsg.), AktG, 4. Aufl. 2020, § 76, Rn. 42 ff.

102 Vgl. www.auswaertiges-amt.de/aussenpolitik/themen/aussenwirtschaft/Wirtschaft-und-Menschenrechte/nationaler-aktionsplan-wirtschaft-menschenrechte/205208.pdf (abgerufen am 8.10.2020).

103 Ähnlich *Balke*, in: Born/Ghassemi-Tabar/Gehle (Hrsg.) MHD BGesR VII, 6. Aufl. 2020, § 104, Rn. 51 „Die Anforderungen an die Compliance-Organisation oder die erforderlich angesehenen Compliance-Maßnahmen unterliegen dabei einer ständigen Weiterentwicklung.“

104 *Bürkle*, BB 2018, 525, 526.

II. Vorgaben und Orientierungshilfen für Compliance Management

1. Compliance-Organisationspflicht als verbandsübergreifende Ausprägung der Leitungsverantwortung

- 27 Wie ausgeführt, steht im Fokus prominenter Regelverstöße häufig die Frage nach der Verantwortung der Geschäftsleiter für fehlendes oder mangelhaftes Compliance Management.¹⁰⁵ Denn eine der Besonderheiten von Compliance-Fällen liegt in der Pflicht von Geschäftsleitern, nicht nur das eigene, sondern auch das rechtmäßige Verhalten aller Unternehmensangehörigen sicherzustellen (**Legalitäts- bzw. Legalitätskontrollpflicht**).¹⁰⁶ Ursprung, Umfang und Grenzen dieser Pflicht sind seit langem prominenter Gegenstand rechtswissenschaftlicher Diskussion und beschäftigen zunehmend die Gerichte.¹⁰⁷
- 28 Allerdings empfiehlt es sich, hierbei zu differenzieren.¹⁰⁸ Die Compliance-Pflicht im Sinne einer **Organisationspflicht** zur Einhaltung rechtlicher Vorgaben und der Verhinderung regelwidrigen Verhaltens im Unternehmen ist zutreffend als ein allgemeiner, rechtsformübergreifender Grundsatz des Verbandsrechts beschrieben worden,¹⁰⁹ denn sie stellt eine besondere Ausprägung der Leitungsverantwortung dar, wonach jeder Geschäftsleiter im Rahmen seiner sog. Leitungssorgfaltspflicht auf die Normeinhaltung durch den Verband und im Verband zu achten hat.¹¹⁰ Compliance ist eine rechtsform-, struktur- und größen-

105 Siehe oben Rn. 17. Wegweisend ist die Entscheidung des LG München I, Urt. v. 10.12.2013, 5 HK O 1387/10, CB 2014, 167 ff. Dort hat das Gericht in der Einrichtung eines mangelhaften Compliance-Systems bzw. in dessen unzureichender Überwachung eine Pflichtverletzung gesehen, für die der Vorstand als Organ ebenso wie jedes einzelne Vorstandsmitglied haftungsrechtlich verantwortlich ist, vgl. LG München I, Urt. v. 10.12.2013, 5 HK O 1387/10, CB 2014, 167. Obwohl dieser Rechtsstreit später durch Vergleich beendet wurde, bestätigt das Urteil die wachsende Bedeutung der Frage, welche organisatorischen Vorkehrungen und Maßnahmen die Unternehmensleitung treffen muss, um Compliance-Anforderungen zu genügen bzw. Sanktionen aus Regelverletzungen zu vermeiden, vgl. *Fleischer*, NZG 2014, 321 ff.

106 Siehe oben Rn. 1 sowie *Merkt*, ZIP 2014, 1705, 1706. *Grigoleit*, AktG, 2. Aufl. 2020, § 76, Rn. 44.

107 Die Rechtsprechung hat in verschiedenen Entscheidungen Grundsätze zur Haftung für mangelhafte Compliance und zur Bedeutung von Compliance-Maßnahmen entwickelt, siehe insbesondere BGH, Urt. v. 9.5.2017, 1 StR 265/16, CB 2017, 330 sowie LG München I, Urt. v. 10.12.2013, 5 HK O 1387/10, CB 2014, 167 ff., zur Haftung eines Vorstandsmitglieds sowie BGH, Urt. v. 17.7.2009, 5 StR 394/08, NJW 2009, 3173 zur Haftung eines Compliance Officers sowie hierzu *Lackhoff/Schulz*, CCZ 2010, 81 ff.

108 Vgl. *Merkt*, ZIP 2014, 1705 ff.; *Moosmayer*, Compliance, 3. Aufl. 2015, 4 f.

109 *Merkt*, ZIP 2014, 1705 sowie ausführlich *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, 2017, 36 ff., 68 f. Siehe ferner *Balke*, in: Born/Ghassemi-Tabar/Gehle (Hrsg.) MHDGesR VII, 6. Aufl. 2020, § 104, Rn. 6 „Rechtsformübergreifende Pflichtenlage“.

110 So explizit *Merkt*, ZIP 2014, 1705, 1707.

unabhängige Pflichtaufgabe eines jeden Geschäftsleiters,¹¹¹ denn jeder Verband ist so zu organisieren, dass Rechts- und Regelverstöße verhindert werden.¹¹²

Soweit die Geschäftsleiter nicht selbst und höchstpersönlich für die Erfüllung von Rechtspflichten verantwortlich sein sollen (z. B. im Zusammenhang mit steuer- und sozialversicherungsrechtlichen Anforderungen, datenschutzrechtlichen Vorgaben oder Pflichten im Zusammenhang mit einer Insolvenz),¹¹³ müssen sie entsprechende organisatorische Maßnahmen treffen, um rechtskonformes Verhalten der Unternehmensangehörigen sicherzustellen und Regelverletzungen möglichst zu vermeiden.¹¹⁴ Dieser Organisationsauftrag¹¹⁵ der Geschäftsleitung umfasst sowohl die Entscheidung über die Einführung von Compliance-Maßnahmen als auch über die wesentlichen Strategie- und Strukturentscheidungen bezüglich des Compliance Managements.¹¹⁶ Dieses Kernbestands an Organisationsaufgaben kann sich die Unternehmensleitung nicht entäußern bzw. durch Delegation entziehen.¹¹⁷

2. Individuelle Ausgestaltung des Compliance Managements

Dagegen richtet sich die jeweilige Ausgestaltung des Compliance Managements, d. h. Art und Umfang der erforderlichen Compliance-Maßnahmen (einschließlich einer etwaigen „Compliance-Organisation“) stets nach dem individuellen Risikoprofil und den Besonderheiten des jeweiligen Unternehmens oder Verbands. Als relevante Kriterien für die individuelle Ausgestaltung gelten u. a.:¹¹⁸

- 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.¹¹⁹

111 So wörtlich und zutreffend *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, 2017, 68.

112 *Jenne*, vorige Fn., 68 f.; ähnlich *Balke*, in: Born/Ghassemi-Tabar/Gehle (Hrsg.) MHdBGesR VII, 6. Aufl. 2020, § 104, Rn. 6.

113 Vgl. am Beispiel der GmbH *Stephan/Tieves*, in: MünchKomm-GmbHG, 3. Auflage 2019, § 37 Rn. 25 f.

114 Vgl. *Schulz/Galster*, in: Bürkle/Hauschka, Der Compliance Officer, 2015, § 4 Rn. 5; *Kort*, GmbHR 2013, 566 ff.

115 *Haouache*, Unternehmensbeauftragte und Gesellschaftsrecht der AG und GmbH, 2003, 53.

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

117 Vgl. *Groß*, Chief Compliance Officer, 2012, 59 m. w. N.

118 Vgl. *Merkt*, ZIP 2014, 1705 ff.

119 Zu Letzterem explizit *Merkt*, ZIP 2014, 1705, 1708 f.; zur Compliance-Historie bzw. zum Compliance-Risikoprofil siehe etwa *Schulz/Galster*, in: Bürkle/Hauschka, Der Compliance Officer, 2015, § 4 Rn. 27.

- 31** Abgesehen von besonderen gesetzlichen Organisationsvorgaben für bestimmte Branchen¹²⁰ richtet sich der erforderliche Organisationsgrad des Compliance Managements nach der Analyse der oben genannten Kriterien. Diese Analyse beantwortet auch die Frage, ob es einer eigenständigen Compliance-Organisation bedarf oder ob es ausreicht, etwa eine separate Compliance-Funktion bzw. einen Compliance Officer zu bestellen.
- 32** Darüber hinaus enthalten Strafrecht und Zivilrecht für alle Unternehmen bestimmte allgemeine Vorgaben für Aufsichts-, Kontroll- und Untersuchungspflichten, welche die Gerichte fallbezogen konkretisiert haben.¹²¹ Derartige „Leitplanken“ zur Unternehmensorganisation sind Ausgangspunkt und integraler Bestandteil jedes Compliance Managements.

3. Vielfalt an Vorgaben und Orientierungshilfen

- 33** Zwar enthält das deutsche Recht – mit Ausnahme bestimmter branchenspezifischer Normen – bislang keine speziellen Vorschriften für ein Compliance Management.¹²² Allerdings enthalten diverse Rechtsnormen allgemeine Vorgaben und Grundsätze, die bei der Erfüllung der Compliance-Pflicht durch organisatorische Maßnahmen zu berücksichtigen sind.¹²³ Diese Vorgaben sind durch die Gerichte fallbezogen präzisiert sowie durch Rechtswissenschaft und Rechtspraxis kommentiert worden und bilden ein Muster organisatorischer (Mindest-)Anforderungen für eine ordnungsgemäße Unternehmensführung. Für bestimmte Branchen bestehen darüber hinaus (teils selbst geschaffene) Regelwerke und Verhaltenskodizes, in denen zentrale Compliance-Themen behandelt und Handlungsempfehlungen entwickelt werden.¹²⁴ Ferner ist das Thema Compliance seit längerem Regelungsgegenstand verschiedener Standardisierungsorganisationen, zu nennen sind insbesondere der Prüfungsstandard des Instituts der Wirtschaftsprüfer (**IDW PS 980**),¹²⁵ die **ISO 19600** (Compliance-Management-Systemen)

120 Siehe unter Rn. 34 ff.

121 Siehe unter Rn. 45 ff. Zur Relevanz von § 130 OWiG siehe *Böttger*, Kap. 2, Rn. 45 ff., sowie *Moosmayer*, Compliance, 3. Aufl. 2015, 4. Zur Relevanz des Deliktsrecht bzw. der „Unternehmensorganisationspflichten“ für Compliance siehe etwa *Spindler*, WM 2008, 905.

122 Zu den rechtlichen Rahmenbedingungen für Compliance Management siehe unter Rn. 34 ff.

123 Vgl. *Theusinger/Jung*, in: Römermann, Münchener Anwaltshandbuch GmbH-Recht, 4. Aufl. 2018, § 24 Rn. 7 ff.

124 Exemplarisch sind zu nennen der Verhaltenskodex des Gesamtverbandes der Deutschen Versicherungswirtschaft für den Vertrieb von Versicherungsprodukten, <http://www.gdv.de/Human/news/Verhaltenskodex-fuer-den-Vertrieb-11518> (abgerufen am 8.10.2020) sowie der vom Verein „Freiwillige Selbstkontrolle für die Arzneimittelindustrie“ (FSA) veröffentlichte „FSA-Transparenzkodex“ zur Transparenz bei der Zusammenarbeit mit den Angehörigen der Fachkreise und medizinischen Einrichtungen, siehe <http://www.fsa-pharma.de/kodizes/transparenzkodex/inhaltsübersicht> (abgerufen am 8.10.2020).

125 IDW-Prüfungsstandard „Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen“ (IDW PS 980), WPg Supplement 2/2011, 78 ff.; vgl. dazu unten Rn. 50 sowie von *Busekist/Hein*, CCZ 2012, 41 ff.; von *Busekist/Schlitt*, CCZ 2012, 86 ff.

teme)¹²⁶ sowie die **ISO 37001** (Anti-Korruptions-Management-Systeme).¹²⁷ Diese Regelwerke und Standards sind grundsätzlich nicht rechtsverbindlich,¹²⁸ enthalten aber häufig nützliche Empfehlungen und Leitlinien für die Gestaltung eines auf das jeweilige Unternehmen passenden Compliance Managements. Zudem haben Wissenschaft und Praxis einen Katalog an Mindestanforderungen für ein wirksames Compliance Management entwickelt.¹²⁹

a) Branchenspezifische Sonderregeln als Erkenntnisquelle

Besondere (aufsichts-)rechtliche Vorgaben für die Einrichtung einer Compliance-Organisation bestehen für Kredit- und Finanzdienstleistungsunternehmen, für Wertpapierhandelsunternehmen sowie für Versicherungsunternehmen.¹³⁰ 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 insbesondere 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 und einer Internen Revision (§ 25a Abs. 1 Nr. 3 KWG).

Für Wertpapierhandelsunternehmen werden diese Organisationspflichten gemäß § 33 WpHG insbesondere durch die Verpflichtung erweitert, eine dauerhafte und wirksame Compliance-Funktion einzurichten.¹³¹ Diese stellt einen wesentlichen Bestandteil des internen Kontrollsystems des Wertpapierdienstleistungsunternehmens im Sinne des § 25a Abs. 1 Satz 3 Nr. 1 KWG dar.¹³² Damit ist jedes Wertpapierhandelsunternehmen zur Beschäftigung eines Compliance-Beauftragten verpflichtet, nähere Einzelheiten zur Ausgestaltung der Compliance-Funktion ergeben sich aus der Wertpapierdienstleistungs-, Verhaltens- und Organisationsverordnung (WpDVerOV).¹³³ Neben Auslegungshinweisen seitens

126 Zum Vergleich von IDW PS 980 und ISO 19600 ausführlich *Busekist/Uhlig*, Kap. 7.

127 Zur ISO 37001 siehe *Kayser*, CB 2016, 441.

128 Vgl. *Schulz*, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, sowie *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, 2017, 47 f.

129 Ausführliche Darstellung und Nachweise bei *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, 2017, 121 ff.

130 Vgl. *Balke*, in: Born/Ghassemi-Tabar/Gehle (Hrsg.) MHDVGesR VII, 6. Aufl. 2020, § 104, Rn. 9.

131 § 33 Abs. 1 Satz 2 Nr. 1 WpHG, vgl. hierzu *Engelhart*, ZIP 2010, 1832 ff.

132 Zu Funktion und Bedeutung des IKS siehe *Renz/Frankenberger*, Kap. 19, Rn. 49 ff.

133 Siehe § 12 WpDVerOV.

der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zur Konkretisierung der organisatorischen Anforderungen haben kapitalmarktorientierte Unternehmen weitere Vorschriften bzw. aufsichtsbehördliche Empfehlungen zu beachten.¹³⁴

- 36** Versicherungsunternehmen haben die Vorgaben des § 29 VAG zu beachten. 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.
- 37** Bei den genannten Normen handelt es sich allerdings um spezielle Regelungen im Hinblick auf die besonderen Risiken von Finanz- und Versicherungsdienstleistungen, an die der Gesetzgeber besondere (aufsichts-)rechtliche Anforderungen stellt. Daher besteht weitgehend Konsens, dass diese besonderen Anforderungen und Maßstäbe nicht einfach auf das Compliance Management in Unternehmen außerhalb dieser Industriesektoren übertragen werden können.¹³⁵ Ebenso wenig ergibt sich die Verpflichtung zu einer Compliance-Organisation im Wege einer Gesamtanalogie zu diesen (und ausgewählten weiteren) Vorschriften.¹³⁶
- 38** Dem steht es allerdings nicht entgegen, die Vorgaben besonderer Branchen als Anschauungsmaterial für Fragen der Ausgestaltung des Compliance Managements zu nutzen. Denn bei allgemeinen Fragen, wie etwa hinsichtlich der Anforderungen an eine wirksame Compliance-Funktion, können die Branchenregelungen und die hierzu verfügbaren Quellen und Kommentierungen eine wertvolle Erfahrungs- und Erkenntnisquelle sein.¹³⁷ Dies gilt etwa im Hinblick auf die Unabhängigkeit des Compliance Officers, seine Berichtspflichten und für Regelungen zur Vermeidung von Interessenkollisionen.

134 Vgl. *Schulz/Renz*, BB 2013, 2511 ff.

135 So die ganz überwiegende Meinung, vgl. etwa *Meyer*, DB 2014, 1063, 1064; *Seeliger/Mross*, in: *Jaeger/Kokott/Pohlmann/Schroeder*, Frankfurter Kommentar zum Kartellrecht, Stand: 96. Aktualisierung 2020, Teil E. Allg. Teil, Rn. 15 f., jeweils m. w. N.

136 Vgl. etwa *Harbarth*, ZHR 179 (2015), 137, 139; *Seeliger/Mross*, in: *Jaeger/Kokott/Pohlmann/Schroeder*, Frankfurter Kommentar zum Kartellrecht, Stand: 97. Aktualisierung 2020, Teil E., Rn. 15 m. w. N.

137 *Schulz*, Rechtliches Risikomanagement und Compliance im Mittelstand, in: *Keßler*, Unternehmensfinanzierung Mittelstand, 2014, § 6 Rn. 24.

b) Erkenntnisse des Risikomanagements

Wie ausgeführt,¹³⁸ besteht zwischen Compliance Management und Risikomanagement ein enger Zusammenhang. So verpflichtet die Vorschrift des § 91 Abs. 2 AktG den Vorstand einer Aktiengesellschaft nach ihrem Wortlaut dazu, geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten. Demnach hat der Vorstand als Gesamtorgan für eine Organisation zu sorgen, welche die Erkennung von bestandsgefährdenden Entwicklungen sicherstellt.¹³⁹ Bestandsgefährdende Risiken können auch aus „Non-Compliance“ resultieren: Dies gilt etwa bei hohen Geldstrafen bzw. Bußgeldern, z. B. im Zusammenhang mit Kartellrechtsverstößen oder beim Ausschluss von Projekten öffentlicher Auftraggeber.¹⁴⁰ Existenzbedrohend können auch die geplanten Verbandssanktionen nach dem Regierungsentwurf zum Verbandssanktionengesetz sein.¹⁴¹ **39**

Zwar ist die Geltungsreichweite von § 91 Abs. 2 AktG („Ausstrahlungswirkung“) für andere Unternehmens- und Verbandsformen im Einzelnen umstritten,¹⁴² doch ist die Pflicht zur Risikoprävention (ebenso wie die Compliance-Organisationspflicht) eine Ausprägung der Leitungssorgfalt der Verbandsleitung und gilt daher grundsätzlich in jeder Unternehmens- und Verbandsform.¹⁴³ Jedenfalls in dem Umfang, in dem Risiken aus Rechtsverletzungen bestandsgefährdende Ausmaße annehmen, werden sie durch § 91 Abs. 2 AktG (analog) erfasst.¹⁴⁴ Für die Steuerung der sonstigen (nicht bestandsgefährdenden) Compliance-Risiken bestehen zahlreiche Parallelen zum allgemeinen Risikomanagement, da sich auch für Compliance-Risiken die systematische Identifizierung sowie Analyse und Bewertung mit anschließender Einleitung risikosteuernder Maßnahmen empfiehlt.¹⁴⁵ Dabei sind allerdings die Besonderheiten von Compliance-Risiken zu beachten. **40**

aa) Besonderheiten von Compliance-Risiken

Bei der Steuerung von Compliance-Risiken geht es stets um den Umgang mit menschlichem (Fehl-)Verhalten, welches einer juristischen Bewertung bedarf. **41**

138 Siehe oben unter Rn. 9.

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

140 Vgl. *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, 12 ff. Ähnlich *Passarge*, in: Martinek/Semler/Flohr, Handbuch des Vertriebsrechts, 4. Aufl. 2016, § 79 Rn. 93. Zu Bußgeldern wegen Kartellrechtsverstößen ausführlich *Seeliger/Heinen/Mross*, Kap. 23, Rn. 89 ff.

141 Siehe *Böttger*, Kap. 2, Rn. 15.

142 Siehe die Nachw. zum Meinungsstand bei *Merkt*, ZIP 2014, 1705, 1712 f.; *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, 27 ff.

143 *Merkt*, ZIP 2014, 1705, 1713.

144 Vgl. *Liese*, BB-Special Compliance 2008, 17, 19; *Schulz*, Rechtliches Risikomanagement und Compliance im Mittelstand, in: Keßler, Unternehmensfinanzierung Mittelstand, 2014, § 6 Rn. 17; ähnlich *Liese*, BB-Special Compliance 2008, 17, 18.

145 Zum allgemeinen Risikomanagement siehe *Romeike*, Kap. 9. Zum Compliance-Risikomanagement ausführlich *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, 105 ff. sowie *Stork/Ebersoll*, Smart Risk Assessment, 2016, 61 ff.

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.¹⁴⁶

- 42** Eine weitere Besonderheit von Compliance-Risiken folgt ferner aus dem dargelegten 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.¹⁴⁷ Dieses Risiko unzureichender Unternehmensorganisation ist aufgrund des oben dargestellten dynamischen rechtlichen Umfelds hoch, die sog. Legalitätspflicht der Geschäftsleiter hat sich zu einer umfassenden **Legalitätskontrollpflicht** entwickelt.¹⁴⁸ Diese Legalitätskontrollpflicht schließt die Verantwortung für das rechtmäßige Verhalten der Unternehmensangehörigen ein.¹⁴⁹ 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.¹⁵⁰
- 43** Eine wesentliche Besonderheit von Compliance-Risiken und Compliance Management besteht zudem darin, dass der staatliche Rechtsdurchsetzungsanspruch grundsätzlich keine wirtschaftliche Risikoabwägung kennt¹⁵¹ – sog. „nützliche Pflichtverletzungen“ werden rechtlich nicht toleriert und sind regelmäßig Compliance-Verstöße.¹⁵² Wie das oben erwähnte Urteil des Landgerichts München bestätigt hat, können insbesondere regionale Geschäftsgepflogenheiten in anderen Ländern in keinem Fall Bestechungshandlungen rechtfertigen.¹⁵³ Die Leitgedanken dieser Entscheidung – Organisationspflicht zur Vermeidung

146 Vgl. *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, 137.

147 Siehe hierzu die Ausführungen des LG München I, Urt. v. 10.12.2013, 5 HK O 1387/10, CB 2014, 167 ff., sowie *Moosmayer*, Compliance, 3. Aufl. 2015, 1 ff., 5 f.; *Schulz*, Rechtliches Risikomanagement und Compliance im Mittelstand, in: Kessler, Unternehmensfinanzierung Mittelstand, 2014, § 6 Rn. 10; *Nietsch/Hastenrath*, CB 2015, 177, 178.

148 Vgl. *Verse*, ZHR 175 (2011), 401, 403 ff.; *Harbarth*, ZHR 179 (2015), 136, 138; *Grigoleit*, AktG, 2. Aufl. 2020, § 76, Rn. 44 ff.

149 Vgl. *Verse*, ZHR 175 (2011), 401, 403; *Moosmayer*, Compliance, 3. Aufl. 2015, 5; *Grigoleit*, AktG, 2. Aufl. 2020, § 76, Rn. 44 ff.

150 Vgl. *Staub*, CCZ 2009, 121, 129 ff.; *Moosmayer*, in: ders., Compliance-Risikoanalyse, 2014, 5; *Schulz*, Rechtliches Risikomanagement und Compliance im Mittelstand, in: Kessler, Unternehmensfinanzierung Mittelstand, 2014, § 6 Rn. 11; zur Bedeutung von Reputations- und Imageschäden siehe ausführlich *Kröger*, Korruptionsschäden, Unternehmensgeldbußen und Imageschäden, 2013, 255 ff.; zum „Corporate Reputation Management“ siehe *Seibt*, DB 2015, 171.

151 *Preusche/Würz*, Compliance, 3. Aufl. 2020, 46. Ähnlich *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, 105.

152 Vgl. *Kort*, in: Hirte/Mülbert/Roth, AktG, 5. Aufl. 2015, § 91 Rn. 183; *Bosse*, NWB 51/2013, 4056, 4057.

153 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.

von Rechtsverstößen in Abhängigkeit von dem jeweiligen Compliance-Risiko-profil – lassen sich grundsätzlich auf alle Unternehmen und Verbände übertragen.¹⁵⁴ Es empfiehlt sich daher, auf Basis der vielfältigen Organisationsanforderungen der Rechtsordnung¹⁵⁵ eine unternehmensspezifische Risikoinventur als Ausgangspunkt für das Compliance Management zu wählen (siehe unter 57 ff.) und dabei die Besonderheiten von Compliance-Risiken zu beachten.¹⁵⁶

bb) Berücksichtigung integrativer Perspektiven (Beispiel GRC-Ansatz)

Hilfreich für die Konzeption und Weiterentwicklung von Maßnahmen des Compliance-Risiko-Managements kann die Berücksichtigung ganzheitlicher bzw. integrativer Perspektiven sein. So wurde in der Betriebswirtschaftslehre ein integrierter Managementansatz von **Governance, Risk und Compliance** (sog. GRC-Ansatz) entwickelt.¹⁵⁷ Wenngleich nicht alle Unternehmen über eigenständige Kontroll-, Risikomanagement- und Compliance-Funktionen verfügen, erscheint es sinnvoll, über die wirkungsvolle Verknüpfung der durch diese Funktionen institutionalisierten Prozesse nachzudenken. So sollen nach dem Modell der „Three-Lines-of-Defense“¹⁵⁸ in erster Linie bei den operativen Unternehmenseinheiten adressiert, in zweiter Linie durch das Risikomanagement und die Compliance Funktion und in dritter Linie durch die interne Revision verhindert bzw. gesteuert werden.¹⁵⁹ Daraus lässt sich die Notwendigkeit eines differenzierten und abgestuften Prozesses für die Steuerung von Compliance-Risiken ableiten und insbesondere die Notwendigkeit einer Einbettung des Compliance-Risikomanagements in die relevanten Geschäftsprozesse.¹⁶⁰

44

154 Vgl. *Rack*, CB 2014, 104 zur Einordnung der Entscheidung in die Rechtsprechung zum sog. Organisationsverschulden, sowie *Passarge*, in: Martinek/Semler/Flohr, Handbuch des Vertriebsrechts, 4. Aufl. 2016, § 79 Rn. 90 hinsichtlich der Relevanz der Entscheidung für die GmbH.

155 Zur Entwicklung der sog. Unternehmensorganisationspflichten umfassend *Spindler*, Unternehmensorganisationspflichten, 2001; *Matusche-Beckmann*, Organisationsverschulden, 2001; vgl. ferner *Rack*, CB 2014, 104; zum Konzept der strafrechtlichen Garantienpflichten siehe *Spindler*, Handbuch Vorstandshaftung, 2006, sowie *Böttger*, Kap. 2, Rn. 108 ff.

156 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.

157 Siehe hierzu *Bartuschka*, Kap. 10, Rn. 24 ff.; zur Verknüpfung von Internem Kontrollsystem (IKS), Risikomanagementsystem (RMS) und Compliance-Management-System (CMS) siehe auch *Illert*, in: Johannsen-Roth/Illert/Ghassemi-Tabar, DCGK, 2020, Grds. 4, Rn. 19 ff.

158 Siehe hierzu *Renz/Frankenberger*, Kap. 19, Rn. 55 ff. sowie *Illert*, in: Johannsen-Roth/Illert/Ghassemi-Tabar, DCGK, 2020, Grds. 4, Rn. 19.

159 Siehe hierzu *Renz/Frankenberger*, Kap. 19, Rn. 55 ff., sowie *Illert*, in: Johannsen-Roth/Illert/Ghassemi-Tabar, DCGK, 2020, Grds. 4, Rn. 19.

160 Siehe hierzu unter Rn. 83.

c) Anforderungen an Aufsichts- und Überwachungsmaßnahmen

- 45 Auch aus dem Gesetz über Ordnungswidrigkeiten, insbesondere aus § 130 OWiG, lassen sich allgemeine Anforderungen für das Compliance Management ableiten.¹⁶¹ Die Vorschrift gilt rechtsformübergreifend für alle Verbände.¹⁶² Nach § 130 OWiG handelt ordnungswidrig, wer als Inhaber eines Betriebs oder Unternehmens 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. Der Normadressat hat seine Aufsichtspflichten dabei so zu erfüllen, dass grundsätzlich sämtliche betriebsbezogene Pflichten eingehalten werden.¹⁶³ Die Gerichte haben in langjähriger Entscheidungspraxis die relevanten Pflichten nach § 130 OWiG konkretisiert.¹⁶⁴ 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.¹⁶⁵ In den Regelungen zur Haftung des Aufsichtspflichtigen (§§ 130, 9 OWiG) und zur Haftung des Unternehmens bei Fehlverhalten von Aufsichtspflichten (§§ 30, 130, 9 OWiG) wird daher eine zentrale Rechtsgrundlage für Compliance gesehen.¹⁶⁶

d) Vorgaben der Unternehmensorganisationspflichten und Garantenpflichten

- 46 Eine weitere Quelle für die Konkretisierung der Compliance-Pflicht ist die Rechtsprechung zu den sog. Unternehmensorganisationspflichten. Die Gerichte haben auf der Basis deliktsrechtlicher Verkehrssicherungs- und Organisationspflichten sowie strafrechtlicher Garantenpflichten¹⁶⁷ umfangreiche Anforderun-

161 *Bergmoser/Theusinger/Gushurst*, BB-Spezial 2008, 1, 4f.; zu § 130 OWiG siehe ferner *Böttger*, Kap. 2, Rn. 126 ff.

162 Vgl. *Moosmayer*, NJW 2012, 3013; *Koch*, WM 2009, 1013, 1015; *Schmidt*, Compliance in Kapitalgesellschaften, 2010, 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, 2009, 31, 37: „Urmutter“ des Corporate Compliance-Gedankens.

163 *Liese/Schulz*, BB 2011, 1347, 1350.

164 Siehe die Beispiele und Rechtsprechungsnachweise bei *Theusinger/Jung*, Corporate Compliance, in: Römermann, Münchener Anwaltshandbuch GmbH-Recht, 4. Aufl. 2018, § 24 Rn. 29 ff.; *Liese/Schulz*, BB 2011, 1347, 1350.

165 Siehe die Beispiele bei *Theusinger/Jung*, Corporate Compliance, in: Römermann, Münchener Anwaltshandbuch GmbH-Recht, 4. Aufl. 2018, § 24 Rn. 29 ff.

166 Vgl. *Moosmayer*, NJW 2012, 3013; *ders.*, Compliance, 3. Aufl. 2015, 4f.; ähnlich *Rodewald*, CB 2013, 70, 72 („Mutter“ aller Compliance-Vorschriften).

167 Zu den strafrechtlichen Garantenpflichten ausführlich *Böttger*, Kap. 2, Rn. 108 ff., 121 ff., sowie *Beulke/Witzigmann*, in: Moosmayer, Compliance-Risikoanalyse, 2014, 9 ff.

gen entwickelt, für deren Verletzung die Unternehmen (sowie unter bestimmten Umständen auch die Geschäftsleiter persönlich) haften.¹⁶⁸ In einer umfangreichen Kasuistik wurden zahlreiche Organisationspflichten statuiert: Hierzu zählen u. a. Pflichten zu ordnungsgemäßer Betriebsorganisation, Informationsversorgung, Risikosteuerung, Delegation, Instruktion, Überwachung und Kontrolle sowie Dokumentation.¹⁶⁹

e) Beispiele von Leitfäden anderer Rechtsordnungen

Für international tätige Unternehmen können sich weitere Anforderungen und Vorgaben für erforderliche Compliance-Maßnahmen auch aus anderen Rechtsordnungen ergeben.¹⁷⁰ Grenzüberschreitende Geschäftstätigkeit führt insofern zu einer Risiko- und Komplexitätserhöhung in Bezug auf das Compliance Management. So sind häufig besondere Vorgaben zu beachten, etwa beim Export von Gütern¹⁷¹ oder bei jeder Übermittlung personenbezogener Daten.¹⁷² Ein zusätzliches Risiko ist die extraterritoriale Geltung ausländischer Gesetze für inländische Unternehmen, die schon bei einer geringfügigen Geschäftsverbindung mit einer anderen Rechtsordnung eintreten kann.¹⁷³

47

aa) UK Bribery Act (Vereinigtes Königreich)

Ein Beispiel bietet der UK Bribery Act,¹⁷⁴ dessen Strafandrohung für Korruptionsdelikte sich auf alle Unternehmen erstreckt, die im Vereinigten Königreich geschäftstätig sind.¹⁷⁵ Erfasst werden durch seinen weiten Anwendungsbereich auch zahlreiche deutsche Unternehmen mit relevanter Geschäftsbeziehung. Allerdings zeigt das Beispiel des britischen Korruptionsstrafgesetzes, dass Unternehmen und Verbände auch bestimmten Leitlinien und Empfehlungen der Behörden für die Ausgestaltung ihrer Compliance-Maßnahmen nutzen können. So können die betroffenen Unternehmen einer Sanktion nach dem UK Bribery Act dann entgehen, wenn sie die **Umsetzung angemessener Vorkehrungen (ade-**

48

168 Umfassend *Spindler*, Unternehmensorganisationspflichten, 2001, sowie *Matusche-Beckmann*, Das Organisationsverschulden, 2001; zu den diversen Pflichten vgl. ferner *Rack*, CB 2013, 14; *ders.*, CB 2014, 104; *ders.*, CB 2014, 279.

169 Vgl. *Rack*, CB 2014, 104.

170 *Rodewald*, Gesetzestreue als Organisationsproblem – Compliance richtig managen, in: *Maschmann*, Corporate Compliance und Arbeitsrecht, 2009, 31 ff., 41, spricht von einer „Reflexwirkung ausländischer Vorschriften“.

171 Zu Exportkontrolle und Compliance siehe ausführlich *von Bodungen*, Kap. 26.

172 Die Datenübermittlung ins außereuropäische Ausland unterliegt besonders strengen Vorgaben, vgl. *Becker/Böhlke/Fladung*, Kap. 11, Rn. 180 ff.

173 Vgl. *Moosmayer*, Compliance, 3. Aufl. 2015, 10 f. Zur Relevanz des ausländischen Export-Kontrollrechts siehe eingehend *von Bodungen*, Kap. 26.

174 Siehe http://www.legislation.gov.uk/ukpga/2010/23/pdfs/ukpga_20100023_en.pdf (zuletzt abgerufen am 29.1.2020), vgl. dort Sec. 7 (2) sowie *Möhlenbeck*, Kap. 5, Rn. 20 ff. m. w. N.

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

quate procedures) zur **Korruptionsverhinderung** nachweisen.¹⁷⁶ Als angemessene Maßnahmen gelten nach der „Guidance“ des „Ministry of Justice“¹⁷⁷ ein eindeutiges Bekenntnis der Unternehmensleitung zur Korruptionsbekämpfung, die unternehmensweite Einführung von Antikorruptionsmaßnahmen, effektive Risikomanagement-Prozesse sowie die fortlaufende Prüfung des Korruptionsrisikos.¹⁷⁸

bb) Leitfaden des Department of Justice (USA)

- 49 Eine weitere nützliche Orientierungshilfe für die Ausgestaltung des Compliance Managements bietet der **Leitfaden des US-amerikanischen Justizministeriums** (US DOJ) zur Bewertung von Compliance-Programmen (Evaluation of Corporate Compliance Programs), der 2019 in zweiter Auflage veröffentlicht wurde.¹⁷⁹ In den USA gibt es diverse Leitfäden und Empfehlungen zur Evaluierung von Compliance-Maßnahmen; Compliance-Maßnahmen werden von den Behörden bei Regelverstößen regelmäßig im Rahmen der Strafzumessung berücksichtigt.¹⁸⁰ Voraussetzung für eine Sanktionsmilderung ist allerdings stets die Wirksamkeit („effectiveness“) der implementierten Compliance-Strukturen und Maßnahmen.¹⁸¹ Hinsichtlich der Konkretisierung dieses Wirksamkeitsanfordernisses legt der Leitfaden des US-amerikanischen Justizministeriums dabei unter anderem fest, nach welchen Maßstäben vorhandene Compliance-Maßnahmen berücksichtigt werden können.¹⁸² Danach ist anhand von drei zentralen Kernfragen die Wirksamkeit („effectiveness“)¹⁸³ der Compliance-Maßnahmen (sowohl zum Zeitpunkt der Tat als auch zum Zeitpunkt der Sanktionierung) zu bewerten.¹⁸⁴ So ist erstens prüfen, ob das Compliance-System gut konzipiert ist¹⁸⁵ und zweitens, ob es auch ernsthaft und in gutem Glauben umgesetzt wurde. Drittens ist zu prüfen, ob das Compliance-System auch tatsächlich in der Praxis

176 Siehe *Möhlenbeck*, Kap. 5, Rn. 20 ff. m. w. Nachw.

177 Siehe <https://www.justice.gov/downloads/legislation/bribery-act-2010-guidance.pdf> (zuletzt abgerufen am 29.1.2020).

178 Zu diesen Elementen eines adäquaten Compliance-Programms in der Ausführungsregelung durch das britische Justizministerium *Moosmayer*, Compliance, 3. Aufl. 2015, 10 f.; *Teicke/Mohssemi*, BB 2012, 911, 915 ff.; *Timmerbeil/Spachmüller*, DB 2013, 2133, 2135 ff.

179 U.S. Department of Justice Criminal Division, Evaluation of Corporate Compliance Programs. Guidance Document 2019, <https://www.justice.gov/criminal-fraud/page/file/937501/download>, (zuletzt abgerufen am 28.1.2020).

180 Siehe die ausführliche Darstellung des US-Rechts bei *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, 2017, 161 ff. sowie *v. Busekist/Beneke*, WPg 2020, 61, 63 f.

181 US DOJ, S. 13 ff.

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

183 JM § 9-28.8000; US DOJ, S. 1.

184 US DOJ, S. 1.

185 US DOJ, S. 2.

funktioniert.¹⁸⁶ Zur Beantwortung dieser drei Kernfragen zählt der Leitfaden zentrale Elemente eines wirksamen Compliance-Systems sowie jeweils weitere Detailfragen zu diesen Elementen auf, die für die Bewertung relevant sind.¹⁸⁷ Diese Kriterien und Leitfragen sind teilweise etwas redundant, im Hinblick auf die relevanten Maßnahmen aber sehr detailliert formuliert. Das gilt insbesondere für die mit den einzelnen Wirksamkeitsanforderungen verknüpften Umsetzungsprozesse im Unternehmen: So ist in Bezug auf das Compliance-Risikomanagement nach den verwendeten Ressourcen, Methoden und Aktualisierungszyklen zu fragen. Bei der Prüfung der Compliance-Kultur ist das Verhalten der Geschäftsleitung ebenso zu eruieren wie das des oberen und mittleren Managements. Hinsichtlich der Wirksamkeit der Compliance-Abteilung spielen ihr Status, ihre Autonomie und ihre Ausstattung eine wichtige Rolle, auch die Qualifikation der Compliance Officer wird überprüft. Betont werden ferner eine Integration von Know-how aus anderen Unternehmensbereichen sowie das Erfordernis kontinuierlicher Weiterentwicklung und Neubewertung der Compliance-Maßnahmen.¹⁸⁸ Unabhängig von seiner Anwendbarkeit auf deutsche Unternehmen bietet der Leitfaden daher eine Fundgrube für die Optimierung des Compliance Managements.¹⁸⁹

f) 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) verabschiedete Standard „Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen“ (IDW PS 980) stark verbreitet, welcher sog. „Grundelemente“ eines CMS formuliert hat.¹⁹⁰ Dazu zählen zunächst die **Compliance-Kultur** als Grundlage für die Angemessenheit und Wirksamkeit des CMS¹⁹¹ 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

50

186 US DOJ, S. 2.

187 US DOJ, S. 2.

188 US DOJ, S. 13 ff. Vgl. *Jenne*, CB 2019, 327, 328.

189 US DOJ, S. 13 ff.

190 IDW-Prüfungsstandard „Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen“ (IDW PS 980), WPg Supplement 2/2011, 78 ff.; vgl. *von Busekist/Hein*, CCZ 2012, 41 ff.; *von Busekist/Schlitt*, CCZ 2012, 86 ff.; *Makowicz/Maciuca*, WPg 2020, 73; *Balke*, in: *Born/Ghassemi-Tabar/Gehle* (Hrsg.) *MHdBGesR VII*, 6. Aufl. 2020, § 104, Rn. 14 ff. sowie *Jenne*, *Die Überprüfung und Zertifizierung von Compliance-Management-Systemen*, 2017, 131 ff.

191 IDW PS 980, Tz. 23.

die Begrenzung der Compliance-Risiken und die Vermeidung von Compliance-Verstößen ausgerichtet ist.¹⁹² 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.¹⁹³ Diese Grundelemente eines CMS entsprechen weitgehend denjenigen Elementen und „Bausteinen“, die als Kernbestandteile eines wirksamen Compliance Managements gelten.¹⁹⁴

III. Erfolgsfaktoren für ein wirksames Compliance Management

- 51 Zu den Kernelementen und Erfolgsfaktoren, die in Literatur und Rechtsprechung als Anforderungen an ein wirksames Compliance Management erörtert werden,¹⁹⁵ zählen insbesondere die Identifikation und Bestandsaufnahme der relevanten Compliance-Risiken, die Förderung einer nachhaltigen Compliance-Kultur, die kontinuierliche Information und Schulung aller Unternehmensangehörigen, die Kontrolle der Compliance-Maßnahmen sowie die Aufdeckung und Sanktionierung von Regelverletzungen.¹⁹⁶ Diese Kernelemente entsprechen in vielerlei Hinsicht den Grundelementen des IDW PS 980,¹⁹⁷ welche allerdings eine auf die individuellen Besonderheiten des betroffenen Unternehmens abgestimmte Compliance-Strategie nicht ersetzen können.¹⁹⁸ Die Kernelemente wer-

192 IDW PS 980, Tz. 23.

193 IDW PS 980, Tz. 23.

194 Zu den Grundelementen und Mindestanforderungen vgl. *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, 2017, 121 ff.; *Moosmayer*, Compliance, 3. Aufl. 2015, 60 ff.; *Kremer/Klahold*, ZGR 2010, 113, 122 ff.; *Klopp*, Der Compliance-Beauftragte, 2012, 81 ff.; *Schulz/Renz*, BB 2012, 2511, 2512 f., sowie speziell für die GmbH *Theusinger/Jung*, in: Römermann, Münchener Anwaltshandbuch GmbH-Recht, 4. Aufl. 2018, § 24 Rn. 36 ff.

195 Vgl. hierzu die umfangreichen Nachweise bei *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, 2017, 121 ff.

196 Siehe etwa *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, 2017, 121 ff.; *Wilhelm*, Das Ausmaß der erforderlichen Aufsichtsmaßnahmen i. S. d. § 130 OWiG, 2013, 102 ff.; *Kremer/Klahold*, ZGR 2010, 113, 122, 127 ff.; *Moosmayer*, Compliance, 3. Aufl. 2015, 31 ff., 79 ff.; *von Busekist/Hein*, CCZ 2012, 41 ff.; *von Busekist/Schlitt*, CCZ 2012, 86 ff.

197 Der PS 980 nennt als Grundelement eines angemessenen Compliance-Management-Systems u. a. Compliance-Kultur, Compliance-Ziele, Compliance-Organisation, Compliance-Risiken, Compliance-Kommunikation sowie Compliance-Überwachung und -Verbesserung, siehe dazu *von Busekist/Hein*, CCZ 2012, 41 ff., 86 ff.

198 *Schulz*, Prüfung und Bewertung von Compliance-Management-Systemen (insbesondere „IDW PS 980“) für Compliance aus Sicht der Wissenschaft, in: *Bay/Hastenrath*, Compliance-Management-Systeme, 2. Aufl. 2016, 229 ff.

den daher nachfolgend in das Modell einer Strategie für ein wirksames Compliance Management integriert.

1. Gestaltungsermessen bei Strukturen, Prozessen und Systemen

Wie ausgeführt,¹⁹⁹ richten sich die für ein wirksames Compliance Management zielführenden Maßnahmen nach den jeweiligen Besonderheiten des betroffenen Unternehmens und insbesondere nach seinem individuellen **Compliance-Risikoprofil**.²⁰⁰ Die Verbandsleiter haben bei der Ausgestaltung des Compliance Managements ein Handlungsermessen nach den Grundsätzen der sog. „Business Judgment Rule“²⁰¹ hinsichtlich der Einführung geeigneter Strukturen, Prozesse und Systeme.²⁰² Das 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 oder Externe delegiert. In jedem Fall sind einerseits die Zulässigkeit der Delegation sowie andererseits deren Grenzen zu beachten.²⁰³

Die Compliance-Maßnahmen stehen ferner unter dem Vorbehalt der Erforderlichkeit und der Zumutbarkeit, der je nach den Besonderheiten des Unternehmens variiert.²⁰⁴ Während sich ab einer bestimmten Größe die Einrichtung einer Compliance-Organisation empfiehlt, können die Compliance-Aufgaben in kleineren Unternehmen auch durch die Geschäftsleiter (ggf. in Kooperation mit Externen) selbst wahrgenommen werden. Zielführend ist in jedem Fall ein strategischer Ansatz in Abstimmung mit der jeweiligen Unternehmensstrategie.

2. Konzeption einer individuellen Compliance-Strategie

Es sollte das Ziel jeder Unternehmens- und Verbandsleitung sein, geeignete und auf den Verband abgestimmte Rahmenbedingungen für ein regelkonformes und integrires Verhalten der Verbandsangehörigen zu organisieren – dieser Organisationsauftrag ist Bestandteil der Leitungsverantwortung. Hierzu bedarf es unter anderem der systematischen Identifikation und Analyse des individuellen Compliance-Risikoprofils des Verbands, der Entwicklung und Förderung einer Com-

199 Siehe Rn. 30 f.

200 IDW PS 980, Tz. 23.

201 Vgl. *Fleischer*, in: MünchKomm-GmbHG, 3. Aufl. 2019, § 43 Rn. 71 ff.

202 Vgl. *Rodewald*, Gesetzestreue als Organisationsproblem – Compliance richtig managen, in: Maschmann, Corporate Compliance und Arbeitsrecht, 2009, 32, 38; *Hauschka/Moosmayer/Lösler*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 1 Rn. 22 ff., 33; *Balke*, in: Born/Ghassemi-Tabar/Gehle (Hrsg.) MHD BGesR VII, 6. Aufl. 2020, § 104, Rn. 12 f. sowie in Bezug auf die GmbH *Bosse*, NWB 2013, 4056, 4060.

203 Dazu unter Rn. 65 f.

204 Vgl. *Merkt*, 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 2007, 65, 78 f.; *Reichert*, ZIS 2011, 113, 115.

pliance-Kultur²⁰⁵ (siehe unter Rn. 68 ff.) sowie eines Konzepts zur Steuerung der maßgeblichen Compliance-Risiken.²⁰⁶ Ein wichtiger Bestandteil der Compliance-Strategie ist ferner die eindeutige Festlegung von Zuständigkeiten und Verantwortungsbereichen für Compliance-Maßnahmen (siehe unter Rn. 65 f.). Die Compliance-Strategie sollte alle wesentlichen konzeptionellen Fragen und Strukturrentscheidungen adressieren – diese fallen regelmäßig in den Zuständigkeitsbereich der Unternehmensleitung als Gesamtorgan.²⁰⁷

a) Fokussierung auf effektive Compliance-Maßnahmen

- 55** Im Hinblick auf das Ziel einer systematischen Prävention von Regelverletzungen und Fehlverhalten²⁰⁸ reicht die Organisationsaufgabe der Compliance über die bloße Einführung von Regeln und Richtlinien hinaus. Denn wie oben ausgeführt, kommt es nach den Vorgaben aktueller Rechtsprechung und Gesetzgebung entscheidend darauf an, ob die Compliance-Maßnahmen wirksam sind, also tatsächlich funktionieren.²⁰⁹ Zwar führte der Bundesgerichtshof in seiner Entscheidung vom 9.5.2017 als **obiter dictum** 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“.²¹⁰ Allerdings wird diese Anforderung hier nicht näher konkretisiert. Im Zusammenhang der Entscheidungs Begründung und weiteren Stellungnahmen²¹¹ ist denkbar, dass der BGH die Begriffe „effizient“ und „effektiv“ an dieser Stelle nicht näher differenziert hat.²¹² Im Hinblick auf die maßgebliche Anforderung, dass das Compliance Management auf die Vermeidung von Rechtsverstößen ausgelegt sein muss, erscheint folgende Definition empfehlenswert²¹³: Unter Effizienz wird die Beur-

205 Vgl. *Wieland*, Integritäts- und Compliance Management als Corporate Governance – konzeptionelle Grundlagen und Erfolgsfaktoren, in: *Wieland/Steinmeyer/Grüniger*, Handbuch Compliance-Management, 3. Aufl. 2020, 15, 23 ff.; *Grüniger*, Grundlagen einer wertorientierten Compliance, ebenda, 41 ff., 57 ff. Zur Compliance-Strategie ferner *Itzen*, Das Gerüst einer erfolgreichen Compliance-Strategie, BB-Spezial 2008, 12 ff.; *Bergmoser/Theusinger/Gushurst*, Corporate Compliance – Grundlagen und Umsetzung, BB-Spezial 2008, 1, 9 ff.

206 Siehe Rn. 30 ff.

207 Siehe oben Rn. 29, sowie *Karbaum* AG 2013, 863, 870.

208 Vgl. *Raum*, Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten, in: *Hastenrath*, Compliance-Kommunikation, 2017, 31, 48 f.

209 Siehe oben unter Rn. 1 f.

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

211 Vgl. *Raum*, Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten in: *Hastenrath*, Compliance-Kommunikation, 2017, 31, 48 f.

212 *Schulz/Block*, CCZ 2020, 49, 50 f. Im Fall *Siemens/Neubürger*, LG München I, Urt. v. 10.12.2013, 5 HK O 1387/10, 2. Leitsatz, entschied das LG München I, dass die Einrichtung eines *funktionierenden* Compliance-Systems (Hervorhebung durch Verf.) zur Gesamtverantwortung des Vorstands gehöre.

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

teilung der Beziehung zwischen erbrachter Leistung und Ressourceneinsatz verstanden, während **Effektivität** die Beurteilung der Zielerreichung beschreibt, also in welchem Ausmaß die geplanten Ziele auch tatsächlich erreicht worden sind.²¹⁴ Diese Beurteilung, inwieweit die gesetzten Ziele erreichbar sind, dürfte auch für das Compliance Management entscheidend sein, da dessen Zweck in der (bestmöglichen) Vermeidung von Regelverletzungen besteht.²¹⁵ Für eine positive Berücksichtigung von Compliance-Maßnahmen durch Gerichte und Behörden kommt es stets darauf an, dass die Compliance Maßnahmen tatsächlich „gelebt“, also konsequent angewandt und regelmäßig aktualisiert werden.²¹⁶ Nur so kann das Compliance Management seinen primären Zweck einer bestmöglichen Vermeidung von Rechtsverstößen erfüllen und erscheint nicht nur als bloßes Lippenbekenntnis.²¹⁷ Nur ein effektives Compliance Management kann auch die weiteren intendierten Vorteile erreichen, namentlich den Schutz von Unternehmen, Geschäftsleitung und Mitarbeitern, die Sicherung der Reputation des Unternehmens, die rechtssichere Gründung und Gestaltung von Geschäftsmodellen sowie verbesserte Verteidigungsmöglichkeiten in Fällen von „Non-Compliance“.²¹⁸

b) Wahl eines unternehmensspezifischen Organisationsmodells

Entsprechend der Vielfalt unternehmerischer Aktivitäten gibt es für Compliance Management ganz unterschiedliche Organisationsmodelle.²¹⁹ 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),²²⁰ oder die Verantwortlichen beauftragen externe Anbieter (wie Rechtsanwälte oder Wirtschaftsprüfer) mit der Ausführung von Compliance-Aufgaben.²²¹ Dagegen sind in größeren Unternehmen häufig nachgeordnete Unterneh-

214 Vgl. *Thommen/Achleitner/Gilbert/Hachmeister/Jarchow/Kaiser*, Allgemeine Betriebswirtschaftslehre, 9. Aufl. 2020, 47, 48.

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

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

217 *Raum*, Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten, in: *Hastenrath*, Compliance-Kommunikation, 2017, 31, 45, spricht von „Umsetzungsernsthaftigkeit“.

218 Siehe Rn. 97.

219 Siehe ausführlich *Moosmayer*, Compliance, 3. Aufl. 2015, 31 ff., welcher zwischen einer sog. autonomen Compliance-Organisation und einer „Matrix-Organisation“ unterscheidet; *ders.*, in: *Rotsch* (Hrsg.), Criminal Compliance, 2015, 203 ff.; vgl. ferner *Gößwein/Hohmann*, BB 2011, 963 ff.; *Groß*, Chief Compliance Officer, 2012, 61 f.; *Behringer*, in: *Behringer*, Compliance kompakt, 4. 2018, 367 ff.; *Cauers/Haas/Jakob/Kremer/Schartmann/Welp*, DB 2008, 2717 ff.; *Favoccia/Richter*, AG 2010, 137, 138; *Kraft/Winkler*, CCZ 2009, 29, 31.

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

221 Zum „Outsourcing“ von Compliance-Aufgaben auf Externe siehe *Bürkle*, in: *Hauschka/Moosmayer/Lösler*, Corporate Compliance, 3. Aufl. 2016, § 36 Rn. 75 ff.; *Schmidt*, Compliance in Kapitalgesellschaften, 2010, 163 ff.

menseinheiten 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.²²² 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.²²³ Mit Ausnahme spezialgesetzlicher Organisationserfordernisse liegt die Ausgestaltung der organisatorischen Einzelheiten im Handlungsermessen der Geschäftsleiter.²²⁴ Entscheidend ist jeweils die genaue Abstimmung der Compliance-Maßnahmen auf die individuelle Unternehmenssituation und die Anpassung an die jeweils verfolgte Unternehmensstrategie.

c) Ermittlung des besonderen Compliance-Risikoprofils

- 57 Aufgrund des oben beschriebenen Zusammenhangs zwischen Compliance Management und Risikomanagement ist die Entwicklung eines Konzepts zur systematischen Steuerung relevanter Rechts- und Compliance-Risiken ein zentraler Bestandteil der Compliance-Strategie.²²⁵ Die Compliance-Risikostrategie bildet die Basis für die Identifizierung, Bewertung und Überwachung der Compliance-Risiken sowie die Konzeption adäquater Maßnahmen.²²⁶ Sie ist als Bestandteil der Leitungssorgfaltspflicht nicht delegierbar.²²⁷ Das Eingehen von Risiken ist Bestandteil jeder unternehmerischen Aktivität, auch ein umfassendes Compliance Management kann die Risiken der „Non-Compliance“ nicht völlig ausschließen. Aus Sicht eines wirksamen Compliance Managements kommt es jedoch darauf an, die Gefahren aus vorsätzlichem oder fahrlässigem Fehlverhalten

222 Zu diesem mehrstufigen System von Compliance-Beauftragten ausführlich *Bürkle*, in: Hauschka/Moosmayer/Lösler, *Corporate Compliance*, 3. Aufl. 2016, § 8 Rn. 20 ff.; Moosmayer, *Compliance*, 3. Aufl. 2015, 34 f.; *ders.*, in: Rotsch (Hrsg.), *Criminal Compliance*, 2015, 205.

223 Vgl. *Moosmayer*, *Compliance*, 3. Aufl. 2015, 33; *Gößwein/Hohmann*, BB 2011, 963, 966 f.

224 Vgl. *Bürkle*, in: Hauschka/Moosmayer/Lösler, *Corporate Compliance*, 3. Aufl. 2016, § 36 Rn. 12 ff.

225 Vgl. *Kark*, *Compliance-Risikomanagement*, 2. Aufl. 2019, 9: „Das Compliance-Risikomanagement ist der Schlüssel, der den Zugang für ein wirksames Compliance-Programm eröffnet.“ Ähnlich von *Busekist/Schlitt*, CCZ 2012, 86.

226 *Klingenstein*, in: Bay/Hastenrath, *Compliance-Management-Systeme*, 2. Aufl. 2016, 89, 99 f.; *Pauthner/Stephan*, in: Hauschka/Moosmayer/Lösler, *Corporate Compliance*, 3. Aufl. 2016, § 16 Rn. 73 ff.; *Merkt*, ZIP 2014, 1705 ff.; *Balke*, in: Born/Ghassemi-Tabar/Gehle (Hrsg.) *MHdBGesR VII*, 6. Aufl. 2020, § 104, Rn. 17 ff.

227 *Klingenstein*, in: Bay/Hastenrath, *Compliance-Management-Systeme*, 2. Aufl. 2016, 99; *Pauthner/Stephan*, in: Hauschka/Moosmayer/Lösler, *Corporate Compliance*, 3. Aufl. 2016, § 16 Rn. 73 ff.

der Unternehmensangehörigen so weit wie möglich zu reduzieren.²²⁸ Wie ausgeführt,²²⁹ ist dabei die Einbeziehung von Methoden und Verfahren des Risikomanagements hilfreich,²³⁰ die Besonderheiten der Compliance-Risiken sind jedoch stets zu beachten.²³¹ Die Einzelheiten des Compliance-Risikomanagements richten sich nach den unternehmensindividuellen Besonderheiten, Ausgangspunkt ist das jeweils individuelle „Compliance-Risikoprofil“ des Unternehmens.²³²

aa) Systematische Identifikation von Compliance-Risiken

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.²³³ 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 arbeitsrechtlichen, datenschutzrechtlichen und steuerrechtlichen Pflichten, weitere besondere Risiken ergeben sich für viele Unternehmen etwa im Zusammenhang mit dem Wettbewerbs- und Kartellrecht, dem Außenwirtschaftsrecht oder Antikorruptionsvorschriften.²³⁴ 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 Analyse des Umfelds sollte neben Rechts- und Compliance-Risiken ferner besondere länder- und branchenspezifische Risiken einbeziehen.²³⁵

Die Analyse des Umfelds des Unternehmens sollte mit einer sorgfältigen Analyse des individuellen Geschäftsmodells des Unternehmens und seiner Unternehmenseinheiten verknüpft werden.²³⁶ So sind bestimmte Abteilungen wie etwa

228 Vgl. *Raum*, Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten, in: Hastenrath, Compliance-Kommunikation, 2017, 31, 44 ff.

229 Siehe oben unter Rn. 30 f.

230 Siehe hierzu ausführlich *Romeike*, Kap. 9.

231 Vgl. *Staub*, CCZ 2009, 121, 125 ff., sowie *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, 105.

232 Vgl. *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, 105 ff.

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

234 Siehe oben Rn. 11 ff. sowie *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, 163.

235 Vgl. *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, 105.

236 Vgl. *Theusinger/Jung*, in: Römermann, Münchener Anwaltshandbuch GmbH-Recht, 4. Aufl. 2018, § 24 Rn. 36, sowie ausführlich *Staub*, CCZ 2009, 121, 127 mit einem RisikSuchmatrix anhand der „value chain“ des Unternehmens.

Einkauf und Vertrieb besonders anfällig für „Non-Compliance“ durch Korruption oder Verletzungen des Wettbewerbsrechts.²³⁷ Grundsätzlich sollte jede Abteilung und Unternehmensfunktion eine „Risiko-Inventur“ durchführen, unter Zusammenarbeit der jeweiligen Leiter mit dem Compliance Officer, der Rechtsabteilung oder externen Rechtsberatern.

bb) Analyse und Bewertung

- 60** 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.²³⁸ Ein weiterer gravierender Unterschied besteht darin, dass die Geschäftsleitung nicht aus Opportunitätserwägungen heraus Rechtsvorschriften missachten sollte, auch sog. „nützliche Pflichtverletzungen“ sind regelmäßig Compliance-Verstöße.²³⁹ Allerdings besteht Konsens dahingehend, dass Compliance-Maßnahmen unter den Aspekten der Erforderlichkeit und Zumutbarkeit zu beurteilen sind.²⁴⁰ Dementsprechend 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 nicht isoliert erfolgen, sondern Bestandteil eines ganzheitlichen Risikomanagements für das Unternehmen sein. Der Erfassung, Analyse und Steuerung der schwerwiegendsten Risiken sollten umgehend die sonstigen Compliance-Risiken folgen.

cc) Entwicklung von Risikosteuerungsmaßnahmen

- 61** 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.²⁴¹ Andere – weniger radikale – Risikosteuerungsmaßnahmen

237 Vgl. ausführlich *Staub*, CCZ 2009, 121, 127 mit einer Risiko-Suchmatrix anhand der „value chain“ des Unternehmens; ferner *Theusinger/Jung*, in: Römermann, Münchener Anwalts-handbuch GmbH-Recht, 3. Aufl. 2018, § 24 Rn. 36.

238 Siehe oben Rn. 41 sowie *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, 137.

239 Siehe oben Rn. 43 sowie *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, 133.

240 Siehe Rn. 53, sowie *Bachmann*, Compliance – Rechtsgrundlagen und offene Fragen, in: Schriftenreihe der Gesellschaftsrechtlichen Vereinigung (Hrsg.), Gesellschaftsrecht in der Diskussion, 2007, 65, 78 f.

241 Vgl. *Staub*, CCZ 2009, 121, 130. Weitere Beispiele zur Compliance-Risikosteuerung bei *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, 135 ff.

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.²⁴²

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“²⁴³ ihrer Geschäftsabläufe wertvolle Hinweise zur Risikosteuerung geben. Zudem kann durch die aktive Einbeziehung der Geschäftseinheiten die Akzeptanz von Compliance Management erhöht werden, denn zur Vermeidung von Compliance-Risiken ist eine Compliance-Kultur erforderlich, in der ein entsprechendes Risikoverhalten nicht toleriert wird.²⁴⁴ **62**

dd) Berichterstattung zu Compliance-Risiken

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.²⁴⁵ **63**

ee) Regelmäßige Compliance-Audits

Die ständige Veränderung des Umfelds für Unternehmen erfordert eine regelmäßige Überprüfung der Compliance-Maßnahmen sowie die Anpassung des 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.²⁴⁶ 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 **64**

242 Siehe hierzu am Beispiel von Kartellrechtsrisiken *Seeliger/Heinen/Mross*, Kap. 23, Rn. 129 ff.

243 Siehe Rn. 44, 83, sowie *Pauthner-Stephan*, in: Hauschka/Moosmayer/Lösler, *Corporate Compliance*, 3. Aufl. 2016, § 16 Rn. 49 ff.

244 Vgl. *Kark*, *Compliance-Risikomanagement*, 2. Aufl. 2019, 105.

245 Vgl. *Kark*, *Compliance-Risikomanagement*, 2. Aufl. 2019, 132 ff.

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

Wirtschaftsprüfer beanstandet werden können.²⁴⁷ 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.²⁴⁸ 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.²⁴⁹

d) Klärung von Zuständigkeiten und Delegationsfragen

- 65 Wie oben ausgeführt, ist die Compliance-Pflicht eine besondere Ausprägung der Leitungssorgfaltspflicht der Geschäftsleiter.²⁵⁰ Compliance ist „Chefsache“²⁵¹ – dementsprechend verbleibt ein unveräußerlicher Kernbereich der Compliance-Pflicht stets bei der Geschäftsleitung.²⁵² In diesem Rahmen muss sie dafür sorgen, dass eindeutige Zuständigkeiten, Verantwortungsbereiche und Berichtswegen für Compliance-Maßnahmen bestehen.²⁵³ 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**).²⁵⁴ 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**).²⁵⁵
- 66 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 müs-

247 Liese/Schulz, BB 2011, 1347, 1352.

248 Liese/Schulz, BB 2011, 1347, 1352.

249 Zum Datenschutz im Compliance Management vgl. Becker/Böhlke/Fladung, Kap. 11.

250 Siehe oben Rn. 28, sowie Merkt, ZIP 2014, 1705.

251 Siehe Fleischer, CCZ 2008, 1, 3.

252 So ausdrücklich und zutreffend Inderst, Compliance-Programm und praktische Umsetzung, in: Inderst/Bannenber/Poppe, Compliance, 3. Aufl. 2017, 142; siehe ferner Seibt, in: Schmidt/Lutter (Hrsg.), AktG, 4. Aufl. 2020, § 76, Rn. 31 ff. sowie ausführlich Gomer, Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft, 2020, 123 ff., 160 ff.

253 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.) MHD BGesRVII, 6. Aufl. 2020, § 104, Rn. 26 ff.

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

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

sen die übrigen Geschäftsführungsmitglieder die Aufgabenwahrnehmung ihrer Kollegen beobachten und sind verpflichtet, im Fall von Compliance-Verstößen zu intervenieren.²⁵⁶ 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.²⁵⁷

e) Eigenständige und unabhängige Positionierung der Compliance Officer

Angesichts der vielfältigen 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.²⁵⁸ 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,²⁵⁹ 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.²⁶⁰ 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. Evaluierung sowie Bewältigung von Compliance-Risiken.²⁶¹ Eine weitere wichtige Aufgabe besteht in der Steuerung von relevanten Informationsflüssen (**Informations- und Wissensmanagement**).²⁶² Der Compliance Officer fungiert dabei als „Informations-schnittstelle“.²⁶³ Dabei sollte der Compliance Officer einerseits alle relevanten Informationen bzw. entsprechende Informationszugriffsrechte in Bezug auf Compliance-Themen erhalten.²⁶⁴ Ein funktionierendes Informations- und Wis-

67

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

257 Vgl. *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, 105 ff.; *Klopp*, Der Compliance-Beauftragte, 2012, 186 ff. m. w. N.

258 Vgl. *Schulz/Galster*, in: Bürkle/Hauschka, Der Compliance Officer, 2015, § 4 Rn. 11; *Pauthner-Seidel/Stephan*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 27 Rn. 42.

259 Vgl. *Schulz/Galster*, in: Bürkle/Hauschka, Der Compliance Officer, 2015, § 4 Rn. 26 ff.

260 Zur Rolle der Compliance-Funktion in einem Kreditinstitut siehe ausführlich *Renz/Frankenberger*, Kap. 19.

261 Vgl. *Moosmayer*, Compliance, 3. Aufl. 2015, 49 ff.; *Groß*, Chief Compliance Officer, 2012, 75 f. m. w. N.

262 Vgl. *Klopp*, Der Compliance-Beauftragte, 2012, 94 ff.

263 *Schulz/Renz*, BB 2012, 2511, 2514 ff. Ähnlich *Umnuß*, Corporate Compliance Checklisten, 4. Aufl. 2020, 177 „Informations-sammelstelle“.

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

sensmanagement ist auch die Grundlage für die erfolgreiche Kommunikation von Compliance-Themen und entsprechende Schulungsmaßnahmen.²⁶⁵ Zu den Aufgaben der Compliance Officer gehören ferner Überwachungs- und Kontrollpflichten bezüglich Compliance-relevanter Vorgaben sowie Berichts- und Dokumentationspflichten hinsichtlich aller Compliance-Themen.²⁶⁶

f) Förderung und Incentivierung von Regeltreue (Compliance-Kultur)

- 68** Für den Erfolg von Compliance-Maßnahmen und Compliance-Management-Systemen gilt die sog. Compliance-Kultur als wichtiger Erfolgsfaktor.²⁶⁷ Auch der vom Institut der Wirtschaftsprüfer veröffentlichte IDW PS 980²⁶⁸ nennt die Compliance-Kultur als erstes Grundelement für die Bewertung der Angemessenheit und Wirksamkeit eines CMS.²⁶⁹ Die Compliance-Kultur behandelt die Frage, inwieweit Rechtstreue bzw. Regelbefolgung als Wert von allen Organisationsangehörigen akzeptiert, geachtet und getragen wird.²⁷⁰ Sie indiziert die Bereitschaft zu regelkonformem und integrem Verhalten ebenso wie die Toleranz oder Indifferenz gegenüber Regelverstößen.²⁷¹ 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.²⁷² Die Prägung der Unternehmenskultur wird als zentrales Element des sogenannten „normativen Managements“ angesehen und ist Teil der Unternehmensstrategie.²⁷³ Im Hinblick auf die Compliance-Kultur kommt es dement-

265 Vgl. *Klopp*, Der Compliance-Beauftragte, 2012, 87 ff.

266 Vgl. *Klopp*, Der Compliance-Beauftragte, 2012, 92 ff., 211 ff.

267 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.

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

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

270 *Schulz/Muth*, CB 2014, 265; ähnlich *Siedenbiedel*, Corporate Compliance, 2014, 251 ff.; *Bode*, Compliance-Kultur, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, 1 ff., sowie *Wendt*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 49 Rn. 24 ff.

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

272 Zur Unternehmenskultur grundlegend *Schein*, Organisationskultur, 2003; vgl. ferner *Waxenberger*, Integritätsmanagement, 2001, 152 f.; *Dillerup/Stoi*, Unternehmensführung, 5. Aufl. 2016, 132; *Siedenbiedel*, Corporate Compliance, 2014, 252; *Helisch*, CB 2014, 225 ff.

273 Vgl. *Hungenberg*, Strategisches Management in Unternehmen, 8. Aufl. 2014, 23 ff.; *Eichler*, ZCG 2010, 57, 60 ff.

sprechend darauf an, die richtigen Rahmenbedingungen und Anreize für ein regelkonformes Verhalten der Unternehmensangehörigen zu setzen.²⁷⁴

aa) Compliance Commitment durch die Unternehmens- und Verbandsleitung

Es besteht Konsens, dass die Compliance-Kultur maßgeblich durch die Grundeinstellungen und Verhaltensweisen der Mitglieder der Leitungsorgane (Geschäftsleitung und ggf. Aufsichtsorgan) geprägt wird.²⁷⁵ 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“).²⁷⁶ Für die Entwicklung einer Compliance-Kultur ist es sodann 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 Mitarbeiter) vermittelt, aber auch an sonstige Bezugsgruppen (Mitarbeiter, Kunden, Lieferanten, Investoren) eindeutig und unmissverständlich kommuniziert werden („**Tone from the Top**“).²⁷⁷ 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.²⁷⁸ 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.²⁷⁹ Umgekehrt sollte regelkonformes und integrires Verhalten der Unternehmensangehörigen, das sich in Konfliktsituationen bewährt, besonders honoriert werden – die Geschäftsleitung sollte hierfür ein entsprechendes Anreizsystem konzipie-

69

274 Vgl. für kartellrechtliche Compliance-Programme *van Vormizeele*, CCZ 2009, 41, 42, sowie allgemein *Moosmayer*, Compliance, 3. Aufl. 2015, 43 ff.

275 Vgl. *Unger*, Gesellschaftsrecht und Compliance-Organisation, in: Umnuß, Corporate Compliance Checklisten, 4. Aufl. 2020, Rn. 108; *Pauthner-Seidel/Stephan*, in: Hauschka/Moosmayer/Lösler, Corporate, Compliance, 3. Aufl. 2016, § 27 Rn. 59; *Bode*, Compliance-Kultur, in: Bay/Hastenrath, Compliance-Management-Systeme, 2014, 1 ff.

276 Vgl. zum sog. „tone at the top“ etwa *Rieder/Falge*, Grundlagen für Compliance, in: Inderst/Bannenberg/Poppe, Compliance, 3. Aufl. 2017, Rn. 48; *Bode*, Compliance-Kultur, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, 1, 3.

277 Vgl. *Moosmayer*, Compliance, 3. Aufl. 2015, 43 f.; *Hauschka*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 1 Rn. 35.

278 Vgl. *Moosmayer*, Compliance, 3. Aufl. 2015, 43; *Hauschka*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 1 Rn. 35.

279 Vgl. *Volz*, Praxisbericht Compliance, in: Teichmann (Hrsg.), Compliance, 2014, 1, 4 f.

ren.²⁸⁰ Insgesamt sollte deutlich werden, dass im Interesse eines regelkonformen und integren Verhaltens im Zweifelsfall auch wirtschaftliche Einbußen in Kauf genommen werden müssen.²⁸¹

- 70** 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.²⁸² 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.²⁸³

bb) Akzeptanz von Compliance-Maßnahmen als Grundlage der Befolgung

- 71** Die Wirksamkeit von Compliance-Maßnahmen hängt dabei auch von der Bereitschaft der Betroffenen ab, die Regeln und Maßnahmen zu befolgen.²⁸⁴ Nach einer Studie werden die Einstellungen und Werte der Mitarbeiter als kritischer Erfolgsfaktor für Compliance gesehen.²⁸⁵ Diese Erkenntnis stimmt mit empirischen Untersuchungen zur Wirksamkeit von Compliance-Maßnahmen in Unternehmen überein: Diese Untersuchungen haben gezeigt, dass ein integrierter Ansatz von Compliance- und Integritätsmanagement erfolgversprechender ist als ein rein regel- und kontrollbasierter Compliance-Ansatz, der allein auf die Um-

280 Zur Schaffung positiver Anreize für integrires Verhalten vgl. *Heißner*, Erfolgsfaktor Integrität, 2. Aufl. 2014, 137 f.; *Schaupensteiner*, NZA-Beil. 2011, 8, 12; *Bussmann*, CCZ 2016, 50, 55; *Hastenrath/Müller*, CB 2017, 154.

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

282 Vgl. *Dillerup/Stoi*, Unternehmensführung, 5. Aufl. 2016, 158 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, 8. Aufl. 2014, 26 f.

283 Vgl. *Schulz/Muth*, CB 2014, 265; *Bode*, Compliance-Kultur, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, 1 ff.

284 Zu Regelbefolgung und Integrität als Bestandteile der sog. „Compliance-Kultur“ siehe *Wieland*, Wittenberg – Prozess, CSR und Compliance – Die Zukunftsfähigkeit der sozialen Marktwirtschaft, in: *Wieland/Schack*, Soziale Marktwirtschaft: Verantwortungsvoll gestalten, 2011, 14, 17. Ähnlich *Bussmann*, CCZ 2016, 50, 53; *Bonenberger*, Wertemanagement, in: *Jäger/Rödl/Campos Nave*, Praxishandbuch Corporate Compliance, 2009, 419 ff. Vgl. ferner *Schaupensteiner*, NZA-Beilage 2011, 8, 12; *Bussmann*, CCZ 2016, 50, 54 ff. Im Zusammenhang mit der Einführung eines *Code of Conduct* siehe *Benkert*, Kap. 4.

285 Zur Wahrnehmung dieser Thematik in Unternehmen vgl. die Studie von Ernst & Young, Existing Practice in Compliance 2016 – Stand zum Integritäts- und Compliance-Management in Deutschland, Österreich und der Schweiz, unter https://acf.de/wp-content/uploads/0079f20180412_015_studie_2016_Existing-Practice-in-Compliance-2016.pdf (abgerufen am 23.10.2020).

setzung juristischer Vorgaben gerichtet ist.²⁸⁶ 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.²⁸⁷

Regelverletzungen beruhen einerseits auf vorsätzlichem Fehlverhalten bzw. kriminellen Aktivitäten von Personen (z. B. bei Korruptionsvergehen oder Kartellrechtsverstößen),²⁸⁸ in anderen Fällen resultieren sie aus Fahrlässigkeit aufgrund der Verletzung von Sorgfaltspflichten oder auch nur unzureichender Kenntnis von Regeln und Geboten.²⁸⁹ 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.²⁹⁰ Die Beachtung und Einhaltung von Regeln steht in einem engen Zusammenhang mit den Werten, denen sich die Organisationsangehörigen verpflichtet fühlen.²⁹¹ Im Hinblick auf die Verhinderung bzw. Reduzierung abweichenden Verhaltens und der Förderung von Regeltreue empfiehlt sich daher, die Compliance-Maßnahmen durch ein begleitendes Integritätsmanagement zu untermauern.²⁹²

72

-
- 286 Vgl. *Clausen*, Compliance- oder Integrity-Management, 2011, 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, 2. Aufl. 2016, 22 ff.; *Herb*, Von Compliance zu Integrität, 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, 3. Aufl. 2020, 15 ff.
- 287 Siehe *Wieland*, Governancestrukturen des Gemeinwohls – Eine wirtschaftsethische Skizze, in: v. Kempf/Lüderssen/Volk (Hrsg.), Gemeinwohl im Wirtschaftsstrafrecht, 2013, 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, 2017, 161 ff. sowie *Faber*, Anreizbasierte Regulierung von Corporate Compliance 2014, 187 ff.
- 288 Zu den diversen Straftatbeständen im Bereich der Korruption vgl. *Böttger*, Kap. 2, Rn. 29 ff. Zum Umgang mit Korruptionsrisiken in M&A-Transaktionen siehe *Ullrich*, Kap. 18, Rn. 77 ff. Zu den diversen Formen kartellrechtswidrigen Verhaltens siehe *Seeliger/Heinen/Mross*, Kap. 23, Rn. 10 ff.
- 289 Vgl. *Heißner*, Erfolgsfaktor Integrität, 2. Aufl. 2014, 114; *Bussmann*, CCZ 2016, 50 ff.; *Preusche/Würz*, Compliance, 3. Aufl. 2020, 30.
- 290 Vgl. *Moosmayer*, Compliance, 3. Aufl. 2015, 79 ff.; *Siedenbiedel*, Corporate Compliance, 2014, 57.
- 291 Vgl. *Wieland*, Integritäts- und Compliance-Management als Corporate Governance – konzeptionelle Grundlagen und Erfolgsfaktoren, in: *Wieland/Steinmeyer/Grüniger*, Handbuch Compliance-Management, 3. Aufl. 2020, 15 ff.; *Siedenbiedel*, Corporate Compliance, 2014, 251; *Bode*, Compliance-Kultur, in: *Bay/Hastenrath*, Compliance-Management-Systeme, 2. Aufl. 2016, 1 ff.; *Heißner*, Erfolgsfaktor Integrität, 2. Aufl. 2014, 174 f.
- 292 Zur Verknüpfung von Compliance- und Integritätsmanagements siehe *Wieland*, Integritäts- und Compliance-Management als Corporate Governance – konzeptionelle Grundlagen und

cc) *Kommunikation von Werten für Regelungslücken und „Graubereiche“*

- 73 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 Conduct²⁹³ –, sind die Aussagen nicht immer eindeutig oder selbsterklärend oder sie erfassen nicht alle Fallkonstellationen.²⁹⁴ Selbst bei regelmäßiger Erläuterung der Inhalte im Rahmen von Compliance-Schulungen²⁹⁵ können Zweifelsfragen bleiben, die Erfüllung sämtlicher Rechtspflichten im operativen Geschäft ist stets eine Herausforderung.²⁹⁶ 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.²⁹⁷ 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.²⁹⁸ Dies befähigt die Unternehmensangehörigen in solchen Zweifelsfällen entweder zu einer selbstständigen Einschätzung²⁹⁹ oder es fungiert als eine Art Kompass, der in Zweifelsfällen auf eine Klärung der Frage durch den Compliance Officer verweist.
- 74 Die Fundierung der Compliance-Maßnahmen durch ein Integritätsmanagement bietet zugleich die Chance einer höheren Akzeptanz von Compliance-Maßnahmen. Im Hinblick auf den erforderlichen „tone from the top“ lautet die Botschaft an die Unternehmensangehörigen: „Wir vertrauen Ihrem Urteilsvermögen und Ihrer Fähigkeit, sich an diese Regeln zu halten“, zugleich wird versichert: „Werte wie Rechtstreue und Aufrichtigkeit bestimmen das unternehmerische

Erfolgsfaktoren, in: Wieland/Steinmeyer/Grüninger, Handbuch Compliance-Management, 3. Auflage 2020, 15 ff.

293 Zu den Wirksamkeitsvoraussetzungen und typischen Inhalten siehe ausführlich *Benkert*, Kap. 4, Rn. 16 ff.

294 Vgl. *Wieland*, Integritäts- und Compliance-Management als Corporate Governance – konzeptionelle Grundlagen und Erfolgsfaktoren, in: Wieland/Steinmeyer/Grüninger, Handbuch Compliance-Management, 3. Aufl. 2020, 15.

295 Zu den Anforderungen an effektive Compliance-Schulungen ausführlich *Hastenrath*, Kap. 6, sowie im Kontext der Kartellrechts-Compliance *Seeliger/Heinen/Mross*, Kap. 23, Rn. 129 ff.

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

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

298 Vgl. *Göbel*, Unternehmensethik, 5. Aufl. 2017, 263 ff.

299 Zur Orientierungsfunktion ethischer Prinzipien siehe *Waxenberger*, Integritätsmanagement, 2001, 52 ff., 111 ff.; *Göbel*, Unternehmensethik, 5. Aufl. 2017, 263 ff.

und soziale Miteinander im Unternehmen. Darauf kann man sich als Mitarbeitender verlassen.³⁰⁰

Es empfiehlt sich daher, das Compliance Management durch ein Integritäts- und Wertemanagement zu ergänzen bzw. zu fundieren.³⁰¹ So verabschieden beispielsweise viele Unternehmen im Rahmen ihrer Anti-Korruptions-Compliance sog. „Geschenke-Richtlinien“ zur Regelung der Gewährung und Annahme von Vergünstigungen. Die Prävention von Korruptionsrisiken dürfte besser gelingen, wenn gleichzeitig Unbestechlichkeit und faires Wettbewerbsverhalten als Werte durch Unternehmensleitung und 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

3. Verfassung von Regeln, Richtlinien und Werten

Das letztgenannte Beispiel zeigt, dass zusätzlich zu dem eindeutigen Bekenntnis der Unternehmensleitung zu Compliance auch die verständliche und praxisorientierte Formulierung von Compliance-Regeln und Leitwerten eine zentrale Rolle spielt.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 76

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

301 Vgl. *Wieland*, Integritäts- und Compliance-Management als Corporate Governance – konzeptionelle Grundlagen und Erfolgsfaktoren, in: *Wieland/Steinmeyer/Grüninger*, Handbuch Compliance-Management, 3. Aufl. 2020, 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, 2. Aufl. 2014, 113 ff. sowie näher unter Rn. 2 ff.

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*, Handbuch Compliance-Management, 2010, 39 ff., 61 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, 3. Aufl. 2017, 130 ff.

4. Compliance als Personalführungs- und Schulungsaufgabe

- 77 Über die Formulierung und Verabschiedung von Compliance-Regeln und Leitwerten (z. B. in Form von Verhaltenskodizes, Compliance Manuals und Richtlinien³⁰⁶) hinaus bedarf es weiterer Schritte zur dauerhaften Verankerung bei den Unternehmensangehörigen, die Vermittlung von Compliance und Integrität ist eine Personalführungsaufgabe.³⁰⁷

a) Zielgruppenorientierte Schulungs- und Fortbildungsprogramme

aa) Bedarfsanalyse und Zielgruppenorientierung

- 78 Wichtig ist insbesondere ein zielgenaues und fortlaufend aktualisiertes Schulungs- und Fortbildungsprogramm.³⁰⁸ 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-Regel in verständlicher Sprache Werte erläutert und (insbesondere im Falle juristischer Fachterminologie) in gut nachvollziehbare Formulierungen übersetzt werden.³⁰⁹ Hierzu sollten spezielle Aus- und Fortbildungsmaßnahmen entwickelt werden, die genau auf das Geschäftsmodell des Unternehmens und sein spezifisches Compliance-Risiko-Profil abgestimmt sind.³¹⁰ 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.³¹¹

bb) Positionierung von Compliance als „Business enabler“

- 79 Bei Durchführung der 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.³¹² Soweit sie möglich sollte ferner eine positive Vorstellung davon vermittelt werden, unter welchen Bedingungen ein abgelehntes Geschäft

306 Vgl. *Kreßel*, NZG 2018, 841.

307 So wörtlich und zutreffend *Heißner*, Erfolgsfaktor Integrität, 2. Aufl. 2014, 114.

308 Zu den Anforderungen an effektive Compliance-Schulungen ausführlich *Hastenrath*, Kap. 6, sowie im Kontext der Kartellrechts-Compliance *Seeliger/Heinen/Mross*, Kap. 23, Rn. 129 ff.

309 Vgl. *Hastenrath*, Kap. 6.

310 Siehe im Einzelnen hierzu *Hastenrath*, Kap. 6.

311 *Hastenrath*, Kap. 6 m. w. N.

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