Compliance Management im Unternehmen

Grundlagen, Erfolgsfaktoren und praktische Umsetzung

Herausgegeben von

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

Mit Beiträgen von

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

3., aktualisierte und wesentlich erweiterte Auflage 2025

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

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

Bibliografische Information der Deutschen Nationalbibliothek

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

ISBN 978-3-8005-1931-6

dfv Mediengruppe

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

www.ruw.de

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

Satzkonvertierung: Lichtsatz Michael Glaese GmbH, 69502 Hemsbach

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

Printed in Germany

Vorwort zur 3. Auflage

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

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

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

Frankfurt am Main, im November 2024 *Martin R. Schulz*

Verzeichnis der Autorinnen und Autoren

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Inhaltsverzeichnis

Vorwort V

Verzeichnis der Autorinnen und Autoren VII

Abkürzungsverzeichnis LIII

Teil 1

Grundlagen, Erfolgsfaktoren und Handlungsstrategien

1. Kapitel

Compliance Management – Grundlagen, Orientierungshilfen und Erfolgsfaktoren

(Schulz)

I. Grundlagen und Zusammenhänge 1
1. Anhaltende Bedeutung von Compliance und Compliance Management 1
2. Compliance Management als Inbegriff regelkonformer Unternehmensorganisation 5
3. Risiken und Nachteile von Regelverletzungen und „Non-Compliance“ 7
4. Funktionen von Compliance und Compliance Management 9
5. Compliance Management als Daueraufgabe im dynamischen Umfeld 10
6. Compliance als Basis für „Good Corporate Governance“ 12
7. Compliance und Reputationsmanagement 14

II. Vorgaben und Orientierungshilfen für das Compliance Management 15
1. Grundlagen der Compliance-Pflicht – Regelungsbeispiele 16
2. Compliance-Pflicht als rechtsformübergreifende Ausprägung der Leitungsverantwortung 20
3. Rechtsprechung zur Compliance-Pflicht 21
4. Compliance-Anforderungen anderer Rechtsordnungen 23
a) UK Bribery Act (Vereinigtes Königreich) 24
b) Leitfaden des Department of Justice (USA) 24
5. Deutscher Corporate Governance Kodex 26
6. Erkenntnisse des Risikomanagements 26
a) Besonderheiten von Compliance-Risiken 27
b) Mögliche Berücksichtigung integrativer Perspektiven 28
7. Compliance-Standards als Orientierungshilfe (Beispiel IDW PS 980) 29

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

IV. Vorteile eines effektiven Compliance Managements 51
1. Prävention und Reduzierung der Kostenrisiken und Nachteile von „Non-Compliance“ 52
2. Schutz von Unternehmen, Leitungsorganen und Unternehmensangehörigen 52
3. Sicherung der Reputation und Vertrauenserhalt der Stakeholder 52
4. Eröffnung und Wahrung rechtlicher Chancen und Gestaltungsoptionen 53

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

V. Zusammenfassung und Empfehlungen 55

2. Kapitel

Compliance Management und Strafrecht

(Böttger)

I. Einführung in die Criminal Compliance 59

II. Strafrechtliche Grundlagen der Compliance-Verpflichtung 67

III. Typische strafrechtliche Compliance-Risiken 72
1. Korruption 74
a) Vorteilsgewährung (§ 333 StGB) 77
b) Bestechung (§ 334 StGB) 84
c) Bestechung von Mandatsträgern (§ 108e StGB) 86
d) Bestechung im geschäftlichen Verkehr (§ 299 Abs. 2 StGB) . . 89
e) Bestechlichkeit im geschäftlichen Verkehr (§ 299 Abs. 1 StGB) 93
f) Bestechung im Gesundheitswesen (§ 299b StGB) 94
g) Auslandskorruption 96
h) Korruptionsdelikte im weiteren Sinne 100
2. Untreue (§ 266 StGB) 102
a) Generierung von Bestechungsgeld 103
b) Zahlung von Bestechungsgeld 104
3. Steuerverkürzung (§§ 370 ff. AO) 105

IV. Strafrechtliche Risiken der Non-Compliance für die Verantwortlichen des Unternehmens 109
1. Originäre strafrechtliche Verantwortlichkeit 109
a) Verantwortlichkeit der Geschäftsleitung 110
b) Gremienentscheidungen 111
c) Delegation von Verantwortungsbereichen 112
d) Verantwortlichkeit des Compliance Officers 114
e) Aufsichtsrat 116
2. Innerbetriebliche Anweisungen/Täterschaft kraft Organisationsherrschaft 118
3. Fahrlässigkeitshaftung (sog. Organisationsverschulden) 119
4. Verletzung der Aufsichtspflicht in Betrieben und Unternehmen (§ 130 OWiG) 120

V. Strafrechtliche Risiken der Non-Compliance für das Unternehmen 123
1. (Unternehmens-)Strafrecht 123
a) Überblick 123
b) Einziehung 124
c) Das Unternehmen als Nebenbeteiligter im Strafverfahren . . . 127
2. Ordnungswidrigkeitenrecht 127
a) Verbandsgeldbuße gem. § 30 OWiG 127
b) Das Unternehmen als Nebenbeteiligter im Verfahren wegen § 30 OWiG 130
c) Einziehung (§ 29a OWiG) 130

VI. Sonstige Risiken für das Unternehmen und seine Verantwortlichen 131
1. Blacklisting und Vergabesperren 131
a) Registereintragungen 131
aa) Bundeszentralregister 131
bb) Gewerbezentralregister 131
cc) Vergabe- bzw. Wettbewerbsregister 132
dd) Sonstige Register 134
b) Vergaberechtliche Konsequenzen 135
2. Inhabilität (§§ 70 StGB, 6 GmbHG, 76 AktG) 136
3. Aufsichtsrechtliche Konsequenzen 138

VII. Strafrechtliche Risiken innerhalb des Compliance-Prozesses („Failed Compliance“) 138

3. Kapitel

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

(Rau)

I. Einleitung 143

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

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

III. Fazit 167

4. Kapitel

Einführung eines „Code of Conduct“

(Benkert)

I. Einleitung 171

II. Ausgestaltung 172
1. Erscheinungsformen 172
2. Typische Regelungen 175

III. Einführung eines „Code of Conduct“ 177
1. Individualvertragliche Umsetzung 178
a) Weisungsrecht des Arbeitgebers 178
b) Vertragliche Vereinbarung 180
c) Änderungskündigung 182
2. Betriebsvereinbarung 182

IV. Datenschutzrechtliche Implikation 185

V. Mitbestimmungsrecht des Betriebsrats 186

5. Kapitel

Hinweisgebersysteme – Aufbau und Management

(Block/Sonnenberg)

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

II. Die Vorgaben des deutschen Hinweisgeberschutzgesetzes 202
1. Ziel des Gesetzes 202
2. Überblick über den Inhalt des Hinweisgeberschutzgesetzes 203
3. Sachlicher Anwendungsbereich 203
4. Persönlicher Anwendungsbereich des Hinweisgeberschutzgesetzes 204
5. Voraussetzungen für den Schutz von Hinweisgebern 205
a) Gemeinsame Schutzvoraussetzungen 206
b) Besonderheiten in Abhängigkeit vom Meldeweg 207
aa) Interne Meldungen gemäß § 17 HinSchG 207
bb) Externe Meldungen gemäß § 27 HinSchG 208
cc) Offenlegung gemäß § 32 HinSchG 209
6. Pflicht zur Einrichtung eines internen Hinweisgebersystems.... 210
a) Unternehmen des privaten Sektors 210
b) Juristische Personen des öffentlichen Sektors 211
7. Gesetzliche Anforderungen an ein internes Hinweisgebersystem 211
a) Wahrung der Vertraulichkeit 211
b) Meldewege 212
c) Interne Meldestelle 213
d) Exkurs: Interne Meldestellen im Konzern 214
e) Bearbeitung der eingehenden Meldungen 215
f) Dokumentation und Datenschutz 216
8. Pflicht zur Einrichtung externer Meldestellen 217
9. Schutzmaßnahmen 219
a) Verbot von Repressalien und Schutz von Hinweisgebern 219
b) Sanktionen bei Verstößen 221

III. Aufbau/Einführung eines Hinweisgebersystems im Unternehmen . 221
1. Entscheidungen hinsichtlich der konkreten Ausgestaltung..... 221
a) Organisation 221
b) Ausgestaltungsmöglichkeiten 222
aa) Kreis der Hinweisgeber 222
bb) Zentrale Meldestelle vs. lokale Meldestellen 223
cc) Meldekanäle 224
dd) Arten der meldbaren Verstöße 227
ee) Anonyme Meldungen 227
ff) Regelungen zur Einführung eines Hinweisgebersystems . 228
2. Kommunikation 229
3. Datenschutzrechtliche Regelungen 230

IV. Die praktische Arbeit mit einem Hinweisgebersystem..... 232
1. Schutz des Hinweisgebers vor Nachteilen 232
2. Schutz des Betroffenen..... 233
3. Datenschutzkonformer Umgang mit eingegangenen Hinweisen . 234

V. Fazit 235

6. Kapitel

Kommunikationsmanagement und Schulungen (analog und remote)

(Hastenrath)

I. Einleitung 237

II. Grundzüge zur Kommunikation in der Unternehmenspraxis 238
1. Relevanz der Kommunikation im Unternehmen und bei Compliance 238
2. Kommunikationsmodelle 240
a) Modell zu Konfliktarten als Grundlage für die Kommunikation 240
b) Praxisrelevantes Beispiel 242

III. Ausgewählte Instrumente der Compliance-Kommunikation 245
1. Tone from the Top 245
2. Persönlicher Kontakt mit dem Compliance Officer 246
3. Zusammenarbeit des Compliance Officers mit Schlüsselfunktionen im Unternehmen 246
4. Schriftliche Informationen an die Mitarbeiter 247
5. Compliance im firmeneigenen Intranet 247

IV. Schulungen 248
1. Persönliche Schulungen durch die Compliance-Funktion 248
2. Schulungen mit klassischem E-Learning 249
3. Digitale Schulungen: Schulungen mit Webinaren, Podcasts, Livestreams oder vertonten Präsentationen 250
4. Unterstützung dezentraler Compliance-Funktionen: das Schulungshandbuch 263

V. Die „Top 5 Stolpersteine“ in der Compliance-Kommunikation und Lösungsvorschläge 265
1. Fehlende, verspätete oder missverständliche Information 265
a) Problemstellung 265
b) Lösungsvorschlag 266
2. Mangelnde Authentizität („Nicht gelebte Hochglanzaussagen“). 267
a) Problemstellung 267
b) Lösungsvorschlag 267
3. Fehler im Kommunikationsmanagement: Budget- und Ressourcenmangel 268
a) Problemstellung 268
aa) Unzureichende Übersetzung eines Code of Conduct (CoC) 269
bb) Unzureichendes Schulungsbudget 270
b) Lösungsvorschlag 271

4. Probleme mit der Technik 271
a) Problemstellung 271
b) Lösungsvorschlag 272
5. Fehler im Kommunikationsmanagement von Compliance aufgrund von Kulturunterschieden 274
a) Problemstellung 274
b) Lösungsvorschlag 275

VI. Fazit zur Compliance-Kommunikation 276

7. Kapitel

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

(Uhlig/Federmann)

I. Einleitung 279

II. Zielsetzung und Zielgruppe 280
1. Ausgangslage 280
2. Zielsetzung des IDW PS 980 281
3. Zielsetzung des ISO 37301:2021 281
4. Vergleich 282

III. Unterschiedliche Regelungstiefe zur Ausgestaltung des CMS 282
1. CMS-bezogene Regelungsinhalte des IDW PS 980 282
2. Regelungsinhalte des ISO 37301 283

IV. ISO 37301 als geeignetes, angemessenes Rahmenkonzept für ein CMS 286
1. Anforderungen des IDW PS 980 an ein Rahmenkonzept 286
2. Vergleich ISO 37301 Anforderungen mit IDW PS 980-Grundelementen 287

V. Zwischenergebnis 289

VI. Die Legalitätskontrolle als Bindeglied zwischen Risiko- und Compliance-Management? 289
1. Zielsetzung des ISO 31022 291
2. Regelungsinhalte des ISO 31022 291
3. Vergleich zum Compliance-Risiko/Vergleich zur ISO 37301 292
4. Zwischenergebnis 292

VII. Argumente für eine Ausrichtung des CMS nach ISO 37301 293
1. Basis für Ermessensentscheidung und Compliance-Richtlinie 293
2. Beurteilung der angemessenen Einrichtung eines wirksamen CMS 295

VIII. Zusammenfassung 296

8. Kapitel

Management interner Untersuchungen

(Wettner/Walter)

I. Einleitung 299

II. Entscheidung über die Durchführung interner Untersuchungen 300
1. Entscheidungsbefugte Stellen 301
2. Pflicht zur Aufklärung konkreter Verdachtsfälle 301
3. Interne Untersuchung oder externe Ermittlung? 302
a) Bereits laufendes behördliches Verfahren 303
b) (Noch) kein behördliches Verfahren 304

III. Vornahme von Eilmaßnahmen 305
1. Einrichtung einer zentralen Koordinierungsstelle 306
2. Maßnahmen der Daten- und Beweissicherung 306
3. Arbeitsrechtliche Maßnahmen 307
4. Beachtung von Informations- und Berichtspflichten 307

IV. Planung der internen Untersuchung 308
1. Grundlagen der Planung 308
a) Beachtung von Recht- und Verhältnismäßigkeit 308
b) Beachtung von Risiken und Folgen der internen Untersuchung 309
2. Festlegung des Untersuchungsgegenstands 310
3. Bestimmung des Untersuchungsteams und der Verantwortlichkeiten 311
a) Auswahl von Mitarbeitern und externen Beratern 311
b) Festlegung von Verantwortlichkeiten und Berichtswegen 312
4. Bestimmung und Vorbereitung der Informationsquellen 313
a) Relevante Informationsquellen 313
aa) Dokumente 313
bb) Elektronische Daten und E-Mails 313
cc) (Ehemalige) Mitarbeiter 314
b) Notwendige Abstimmung der geplanten Untersuchungsmaßnahmen 315
aa) Beteiligung von Betriebsrat oder Sprecherausschuss 315
bb) Abstimmung mit Ermittlungs- und Aufsichtsbehörden . . . 315
c) Einrichtung eines Datenraums oder eines „Projektportals“ . . . 316
5. Sicherung der Vertraulichkeit 317
a) Zugriffsmöglichkeiten Dritter 317
aa) Beschlagnahme durch Ermittlungsbehörden 317
bb) Herausgabe von Unterlagen an Versicherer 319
b) Begrenzung der E-Mail- und sonstigen schriftlichen Kommunikation 319

c) Kennzeichnung und Aufbewahrung geschützter Kommunikation 320
6. Erstellen eines Untersuchungsplans 321

V. Durchführung der internen Untersuchung 321
1. Allgemeine Untersuchungsgrundsätze 321
2. Dokumentation der Untersuchung 322
3. Erhebung und Auswertung von Dokumenten 323
4. Erhebung und Auswertung von elektronischen Daten 324
5. Befragung von Mitarbeitern 324
6. Auswertung und Aufarbeitung der Untersuchungsergebnisse . . . 326

VI. Fazit 328

Teil 2

Übergreifende Themen und Herausforderungen

Abschnitt 2.1

Risiko und Governance

9. Kapitel

Risiko- und Chancenmanagement – Erfolgsfaktoren für eine wirksame Umsetzung

(Romeike)

I. Corporate Governance und das Management von Chancen und Risiken 331
1. Grundlagen und Einführung 331
2. Die Odyssee und der Umgang mit Risiken 333
3. Risikomanagement als zentraler Erfolgsfaktor 335
4. Überblick über aktuelle regulatorische Entwicklungen 335
5. Krisenfrüherkennung gemäß Unternehmensstabilisierungs- und -restrukturierungsgesetz (StaRUG) 336
6. FISG fordert Internes Kontrollsystem und Risikomanagement-system 338

II. Abgrenzung des Risiko- und Chancenbegriffs 339

III. Nutzen eines wirksamen Chancen- und Risikomanagements 342

IV. Unterscheidung von Ursachen – Risiken – Wirkungen 344

V. Verknüpfung von Risikomanagement und Strategie 347

VI. Der Risikomanagement-Prozess als Regelkreis 349

VII. Methoden zur Risikoidentifikation und -bewertung 353

VIII. Aggregation von Risiken. 356

IX. Maßnahmen zur Risikosteuerung 357

X. Unterschiedliche Reifegrade im Risikomanagement 360

XI. Fazit und Ausblick 361

10. Kapitel

Auditverfahren: Compliance als Dauerpflicht

(Rack)

I. Einleitung 367

II. Die Dauerpflicht zur Sicherstellung der dauerhaften Wirksamkeit des CMS nach DIN und EMAS 367

III. Die Beweislast für Vorstände und Geschäftsführer 369

IV. Die Unvorhersehbarkeit von Rechtsverstößen als Grund für Compliance als Dauerpflicht 369

V. Zertifikate sind bloße Momentaufnahmen ohne Nachweis dauerhafter Wirksamkeit eines CMS 369

VI. Das Stichprobenargument in Rechtsprechung und Literatur 370

VII. Der erfolglose Entlastungsversuch durch den Hinweis auf Regeln ohne Anwendung 372

VIII. Die Haftung von Vorständen und Geschäftsführern für fehlende und fehlerhafte CMS nach der Rechtsprechung 375

IX. Die Haftung von Auditoren und Umweltgutachtern gegenüber dem zertifizierten Unternehmen nach der Expertenhaftung 375

X. Die Expertenhaftung von Auditoren und Umweltgutachtern gegenüber Dritten 377

XI. Aufsicht und Sanktionen von Behörden gegen Umweltgutachter und Auditoren für falsche Zertifikate nach dem Auditverfahren . . . 378

XII. Der Gesetzeszweck des UAG 378

XIII. Die Zulassung 378

XIV. Die Aufsicht. 379

XV. Die Konkretisierung des UAG durch Richtlinien des Umweltgutachterausschusses 379

XVI. Mehr Risiken durch Anordnungen, Untersagungen und Widerruf der Zulassung für Umweltgutachter und Auditoren durch Hinweise auf Rechtsverstöße nach dem Hinweisgeberschutzgesetz 380

XVII. Mehr Risiken für Umweltgutachter und Auditoren durch den erweiterten Kreis der Hinweisgeber außerhalb der Unternehmensbelegschaft 381

XVIII. Fazit 382

11. Kapitel

Governance, Risk und Compliance im Mittelstand – Zusammenhänge und Abhängigkeiten

(Bartuschka)

I. Einleitung – Die Notwendigkeit der Einrichtung von Instrumenten zur Überwachung von Unternehmen 383

II. Das System der Unternehmensüberwachung 386
1. Überblick über das Gesamtsystem 386
2. Externe Komponenten der Unternehmensüberwachung 386
3. Interne Komponenten der Unternehmensüberwachung 388

III. Die Verknüpfung der einzelnen Elemente der Unternehmensüberwachung 389
1. Der GRC-Ansatz 389
2. Das interne Kontrollsystem und die anderen Elemente der Überwachung des Unternehmens 390
3. Compliance- und Risikomanagement 391
4. Risikomanagement und Controlling 392
5. Interne Revision, Compliance und Risikomanagement 393
6. Fazit 393

IV. Grundkonzept für die Ausgestaltung eines integrierten Systems der Überwachung für mittelständisch geprägte Unternehmen 394
1. Bestimmung der Zielgruppe der Unternehmen 394
2. Zielstellung für die Einführung eines integrierten Systems der Überwachung 394
3. Vorgehensweise 394
a) Risikoanalyse 395
b) Analyse bestehender Strukturen 396
c) Ermittlung des Anpassungsbedarfs 396
d) Umsetzung 397
4. Fazit 399

Abschnitt 2.2

Datenschutz und IT-Security

12. Kapitel

Datenschutz im Compliance Management

(Becker/Böhlke/Fladung)

I. Einleitung 401

II. Der konzeptionelle Schutz personenbezogener Daten 405
1. Gesetzliche Grundlagen 405
a) Datenschutzgrundverordnung 405
b) Bundesdatenschutzgesetze 406
c) Landesdatenschutzgesetz 406
d) Europäische Richtlinien und Verordnungen 407
e) Weitere Gesetze mit datenschutzrechtlichen Vorgaben 408
2. Zentrale Grundsätze 409
a) Verbot mit Erlaubnisvorbehalt 409
b) Prinzip der Verhältnismäßigkeit 412
c) Datensparsamkeit 412
d) Transparenz 413
e) Zweckbindung 413
3. Grundbegriffe 413
a) Personenbezogene Daten 414
b) Verantwortliche Stelle 415
c) Umgang mit personenbezogenen Daten 415
aa) Erheben 416
bb) Speichern 416
cc) Verändern 416
dd) Übermitteln 416
d) Auftragsverarbeitung 419

III. Betrieblicher Datenschutz 420
1. Pragmatischer Ansatz: Wo fange ich an? 420
2. Beratungspraxis 425
a) Der betriebliche Datenschutzbeauftragte 428
b) Prozess der Datenschutzberatung 430
c) Praxisrelevante Beispiele 433
3. Implementierung 435
4. Zusammenarbeit mit Behörden 438

IV. Instrumente der datenschutzrechtlichen Compliance 439
1. Tone from the Top 439
2. Interne Richtlinien 439
a) Datenschutzrichtlinie 440

b) IT-Nutzungsrichtlinie 440
c) E-Mail-Policy 441
d) Social-Media und Messaging-Dienste 442
e) IT-Datenschutzmanagement-Richtlinie (Datenschutzmanagementkonzept) 442
f) Archivierungs- und Löschungsrichtlinie 443
3. Verzeichnis von Verarbeitungstätigkeiten 444
4. Interne Kommunikation und Awareness 445
a) Der Datenschutz-Newsletter 445
b) Intranet 446
c) Der „Datenschutz-Tag“ und Fachtagungen 446
5. Schulungen 446
a) Persönliche Schulungen 447
b) E-Learning/Webinars 448
c) Unterstützung dezentraler Compliance-Funktionen 449

V. Effektive Datenschutzüberwachung 450
1. Audits und Maßnahmenpläne/Quick Self-Assessment 450
2. IT-Infrastruktur-Reviews und Koordinierung mit IT-Security . . . 452
3. Incident- und Regel-Reporting aus den Betrieben 452
4. Der Datenschutzjahresbericht 453
5. Bericht an Aufsichtsrat/Compliance-Bericht/Audit Committee . 453
6. Zusammenarbeit mit dem Compliance Officer, IT-Security und Revision 454

VI. Beschäftigtendatenschutz 457
1. Bedeutung des Beschäftigtendatenschutzes für Compliance 457
2. Rechtsgrundlagen für den Umgang mit Mitarbeiterdaten 461
a) Kollektivvereinbarungen zur Nutzung von Mitarbeiterdaten . 461
b) Rechtfertigende Einwilligung des Mitarbeiters 463
c) Arbeitsvertragliche Regelungsmöglichkeiten 464
d) Gesetzliche Erlaubnistatbestände 466
e) Internationaler Datenverkehr mit Beschäftigtendaten 469
3. Risiken beim Umgang mit Beschäftigtendaten 470
a) Phase 1: Begründung des Arbeitsverhältnisses/ „Boarding-Phase“ 471
b) Phase 2: Durchführung des Arbeitsverhältnisses/ „On Board-Phase“ 471
c) Phase 3: Beendigung des Arbeitsverhältnisses/ „Off Boarding-Phase“ 472
4. Zusammenarbeit mit dem Betriebsrat 473
5. Personalleiter und Betriebsrat als Teil des Datenschutz- und Compliance-Teams 475
6. Hinweise, Muster und Beispielsfall 476
a) Hinweise zur Regelung der Nutzung von Beschäftigtendaten 476

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

VII. Fazit 485

13. Kapitel

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

(Jacobs)

I. Rechtliche Herausforderungen der fortschreitenden Digitalisierung und Vernetzung 487

II. Software-Lizenzmanagement 487
1. Rechtliche Grundlagen der Nutzung von Computerprogrammen 488
2. Besondere Arten von Software, insbesondere Open-Source-Software 489
3. Software-Lizenzmanagement im Rahmen verantwortungsbewusster Unternehmensführung 490
4. Rechtsfolgen einer Unterlizenzierung 491

III. Software-Lizenzmanagement im Rahmen von Cloud-Diensten 491
1. Nutzungshandlungen beim Cloud Computing 491
a) Recht der öffentlichen Zugänglichmachung der Software 492
b) Recht zur Vervielfältigung der Software 493
2. Lizenzmanagement im Zusammenhang mit Cloud Computing-Diensten 493

IV. Rechtsrahmen von Softwarelizenz-Audits 494
1. Rechtliche Grundlagen für einen Softwarelizenz-Audit 495
2. Vertragliche Ausgestaltung eines Softwarelizenz-Audits 496

V. Rechte an und Zugang zu nicht-personenbezogenenen Daten 497
1. Regelungsinhalt und Struktur des Data Act 499
2. Datenweitergabe unter dem Data Act 500
a) Allgemeine Pflichten 501
b) Erfasste Datenkategorien 502
c) Datenzugriffsrechte für Nutzer 502
d) Recht der Nutzer auf Datenweitergabe an Dritte 503
3. Verhältnis zum Datenschutzrecht 504
4. Nutzung durch und Weitergabe von Daten durch den Dateninhaber 504
5. Missbräuchliche Vertragsklauseln 506
6. Sanktionen 506

VI. Wechsel von Datenverarbeitungsdiensten 507

VII. Blockchain und Smart Contracts 508

VIII. Implementierung eines IT-Compliance-Systems 509

14. Kapitel

Cybersecurity, IT-Sicherheit und Krisenmanagement

(Bensinger)

I. Analyse 511
1. Ziele der IT-Sicherheit 511
2. Cybercrime im Wandel 512
a) Ideelle Hintergründe 513
b) Materielle Hintergründe 516
3. Entwicklungen bei Schutzmaßnahmen 516

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

i) §§ 76, 91, 93 AktG 547
aa) Ausgestaltung des IT-Risikomanagementsystems 548
bb) Anforderungen nach DSGVO 551
cc) Verantwortungsverteilung innerhalb der Geschäftsleitung 552
dd) Dokumentationspflicht 553
3. Unternehmensinterne Vorkehrungen 553
a) Interne Vorgaben 553
b) Aktuelle technisch-organisatorische Schutzmaßnahmen 554

III. Der Krisenfall 556
1. Hacker-Angriffe erkennen 556
2. Rechtliche Konsequenzen und Handlungsoptionen 556
a) Melde- und Informationspflichten 556
aa) DSGVO 556
(1) Meldung an die Aufsichtsbehörde (Art. 33 DSGVO) 557
(2) Meldung an die Betroffenen (Art. 34 DSGVO) 559
(3) Sanktionen 562
bb) BDSG 562
cc) BSIG 562
dd) ZAG 564
ee) Meldepflichten für Energiewirtschaftsunternehmen 566
ff) TMG 566
gg) TKG 567
hh) Sonstige Informationspflichten 568
b) Werkzeuge zur Abwehr von Cyberangriffen 568
3. Interne und externe Kommunikation 570
4. Mittel- und längerfristige Maßnahmen 570

IV. Ausblick 571

Abschnitt 2.3

ESG und Governance

15. Kapitel

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

(Stehr/Knopp)

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

II. Grundlagen 577
1. Corporate Social Responsibility 577
a) Bedeutungswandel des Begriffsverständnisses 577
b) Konzeptionen und Modelle 577
c) Definitionen 579
2. Corporate Governance 581
a) Begriffsverständnis 581
b) Corporate Governance und Corporate Social Responsibility . 581
c) Gesellschaftsrecht und Deutscher Corporate Governance Kodex 583
3. Corporate Compliance 585
a) Begriffsverständnis 585
b) Corporate Compliance und Corporate Governance 586
c) Corporate Compliance als Organisationspflicht 587
d) Aktuelle gesetzliche Entwicklungen in Deutschland und der Europäischen Union 588

III. Corporate Social Responsibility und Regulierungsebenen 590
1. Einführung in die CSR-Regulierung 590
a) Regulierungsebenen 590
b) Regulierungsansätze 590
c) Rechtsqualität 591
d) Reputationsmanagement 592
2. Beispiele für CSR-Regulierung 592
a) Globale Regulierungsebene 592
aa) OECD-Leitsätze für multinationale Unternehmen 592
bb) GRI-Berichtsstandards 593
cc) UN Global Compact 594
dd) ISO 26000 595
b) Internationale Regulierungsebene 596
c) Supranationale bzw. europäische Regulierungsebene 597
d) Nationale bzw. deutsche Regulierungsebene 597
3. CSR-Normenflut als Herausforderung für Unternehmen 599

IV. Corporate Social Responsibility und Corporate Compliance 601
1. Einführung 601
2. Allgemeine Relevanz von CSR-Normen für die Corporate Compliance 603
3. Konkrete Relevanz von CSR-Normen sowie sonstiger CSR-Themen für die Corporate Compliance 604
a) CSR-Normen und CSR-Themen im Compliance-Risikomanagementprozess 605
aa) Schritt 1: Definition der Compliance-Risiken 605
bb) Schritt 2: Identifikation der Compliance-Risiken 605

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

V. Zusammenfassung 608

16. Kapitel

„ESG-Compliance“: Herausforderungen des Nachhaltigkeitsreportings

(Beisheim)

I. Einleitung: Nachhaltigkeit, Corporate Governance und die Rolle von Compliance 611

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

III. Die CSRD: Neue Anforderungen im Nachhaltigkeitsreporting 636
1. Adressaten und Konzernprivileg 640

2. Überblick über die ESRS 642
a) Regelungsinhalte des Set 1 der ESRS 643
b) Der Grundsatz der doppelten Wesentlichkeit und weitere Verfahrensvorgaben 647
c) Verortung im Lagebericht und Prüfung 651
d) Erleichterungen im Rahmen der Implementierung des Reportings 652

IV. Der Referentenentwurf zum CSRD-Umsetzungsgesetz und ein weitergehender Ausblick 653

17. Kapitel

Compliance im Kontext nachhaltigen Supply Chain Managements – Die betriebswirtschaftliche Perspektive

(Schleper/Förstl)

I. Einleitung 659

II. Nachhaltiges Lieferantenmanagement 661
1. Lieferantenbewertung 661
2. Lieferantenentwicklung 662
3. Lieferantenauswahl 663
4. Lieferantenmonitoring 663

III. Unterschiede entlang der Lieferkette 664

IV. Menschenrechtsprobleme und Due Diligence – „beyond compliance“ 666

V. Praxisrelevanz 669

VI. Fazit 670

18. Kapitel

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

(Heske)

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

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

(1) Substantiierte Kenntnis (§ 9 Abs. 3 LkSG) 700
(2) Maßnahmen nach Erlangung von substantiierter Kenntnis (§ 9 Abs. 3 LkSG) 701
ii) Dokumentation und Berichterstattung (§ 3 Abs. 1 Nr. 9 LkSG) 702
(1) Dokumentationspflichten (§ 10 Abs. 1 LkSG) 702
(2) Berichtspflicht (§ 10 Abs. 2 LkSG) 702

III. Das BAFA als zuständige Behörde für die Kontrolle und Durchsetzung der Regelungen des LkSG 703
1. FAQs, Handreichungen und sonstige Informationsquellen 703
2. Berichtspflicht und Kontrollen 704
a) Elektronische Berichtspflicht der Unternehmen 704
b) Kontrollbefugnisse des BAFA 705
c) Anordnungen und Maßnahmebefugnisse des BAFA 706

IV. Sanktionen 706
1. Bußgeld und Bemessungsgrundlage 707
2. Ausschluss von der Vergabe öffentlicher Aufträge 707

V. Zivilrechtliche Haftung und Prozessstandschaft 708

VI. Auswirkungen der europäischen Lieferkettenregelung (CSDDD) – Anpassung des LkSG 708

19. Kapitel

Menschenrechtsbeauftragte und Beschwerdebeauftragte nach dem LkSG

(Hagel/Wiedmann)

I. Einleitung 711

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

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

IV. Verhältnis Menschenrechts- zu Beschwerdebeauftragtem 730

V. Fazit 731

Teil 3

Besondere Aufgaben und Anwendungsfelder

20. Kapitel

Die Compliance-Funktion in einem Kreditinstitut

(Renz/Frankenberger)

I. Einleitung: Was ist die Bedeutung des Begriffs Compliance? 733

II. Welche Compliance-Funktionen gibt es in einem Kreditinstitut? 734
1. Kapitalmarkt-Compliance 735
2. Zentrale Stelle/sonstige strafbare Handlungen (inkl. Geldwäscheprävention) sowie Finanzsanktionen und Embargo (Anti-Financial Crime (AFC)) 739
3. MaRisk-Compliance 742
4. Hinweisgebersystem (Whistleblowing) 744
5. Datenschutz 746
6. Auslagerung der Compliance-Funktion oder von einzelnen Compliance-Tätigkeiten 748

III. Inhalt und Aufgabe einer modernen Compliance-Funktion 749

IV. Das Compliance-Management-System (CMS) 750

V. Schnittstellen zu anderen Funktionen 754
1. Fachbereiche 755
2. Rechtsbereich 755
3. Risikocontrolling-Funktion 757
4. Interne Revision 757

VI. Compliance als Teil des IKS eines Kreditinstituts 759

VII. Übertragung der Struktur/des Ansatzes auf andere Industriesäulen – und umgekehrt 764

VIII. Fazit/Ausblick 766

21. Kapitel

Produktbezogenes Compliance- und Risikomanagement im Treasury

(Keßler)

I. Einleitung 767

II. Finanz- und Kapitalmarktprodukte; Risiken 768
1. „Einfache“ Produkte 768
2. „Komplexe“ Produkte 769
a) Überblick 769
b) Risiken im Einzelnen 772

III. Rechtliche Anforderungen an das Risikomanagement- und Compliance-System 774
1. Anforderungen an Finanzinstitute 774
a) Aufsichtsrechtliche Anforderungen 774
b) „Best Practice“ und praktische Ausgestaltung 776
aa) Risikomanagement 776
(1) Risikomanagementstrategie 777
(2) Risikotragfähigkeitskonzept 777
(3) Interne Kontrollverfahren 778
(4) Personelle und technische Ausstattung 778
(5) Notfallkonzept 778
(6) Nachhaltiges Vergütungssystem 778
bb) Compliance 779
(1) MaRisk BA-Compliance 779
(2) MaComp-Compliance 780
2. Anforderungen an Unternehmen 780
a) Normativer Rahmen und Übertragbarkeit 780
b) Grenzen 783

IV. Ausgestaltung des Risikomanagement- und Compliance-Systems im Unternehmensbereich 783
1. Finanzproduktbezogenes Risikomanagement und Compliance – Überblick 783
2. Die Ausgestaltung der wichtigsten ICRM-Komponenten im Einzelnen 785
a) Rechtliche Einzelfallprüfung: Covenant-Tool 785
b) Kreditrisiko-Tool 786

c) Marktrisiko-Tool 787
d) Liquiditätsrisiko-Tool 788
3. Delegation des Risikomanagements und Compliance 788

V. Haftungsfragen 790
1. Verstoß gegen die Pflicht zum Risikomanagement 790
2. Verstoß gegen die Pflicht zur Compliance 792
3. Einsatz von Künstlicher Intelligenz 792

VI. Fazit 793

22. Kapitel

Der Geldwäschebeauftragte – Stellung und Aufgaben

(Kaetzler)

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

23. Kapitel

Geldwäsche-Compliance in Industrie und Handel

(Komma)

I. Einführung in die Geldwäscheprävention 827
1. Begriff und Methoden der Geldwäsche 827
2. Die Geldwäschebekämpfung 829
a) Geldwäschebekämpfung auf internationaler Ebene: FATF ... 829
b) Geldwäschebekämpfung in der deutschen Gesetzgebung 830
3. Geldwäscherisiken für Industrie- und Handelsunternehmen 832

II. Industrie- und Handelsunternehmen im GwG:
Der Begriff des Güterhändlers 834

III. Die Pflichten der Güterhändler im GwG 835
1. Die privilegierte Verpflichtetenstellung von Güterhändlern 836
a) Praktische Umsetzung des Bargeldausschlusses 836
b) Konsequenzen bei Einführung einer Bargeldbeschränkung .. 838
2. Risikomanagement 839
a) Risikoanalyse 839
b) Interne Sicherungsmaßnahmen 841
aa) Richtlinie zur Prävention von Geldwäsche 842
bb) Überprüfung von Geschäftspartnern 842
cc) Überwachung von Zahlungseingängen 842
c) Gruppenweite Pflichten 843
3. Kundensorgfaltspflichten 844
a) Auslösetatbestände der Sorgfaltspflichten für Güterhändler .. 844
b) Ausgewählte Aspekte der allgemeinen Sorgfaltspflichten ... 846
c) Ausgewählte Aspekte der vereinfachten und verstärkten Sorgfaltspflichten 847
4. Pflicht zur Abgabe von Verdachtsmeldungen 848
a) Verdachtsfall und typische Verdachtsmomente 848
b) Folgen einer Verdachtsmeldung 850
aa) Strafbefreiende Wirkung 850
bb) Transaktionssperrfrist § 46 GwG 851
cc) Verbot der Informationsweitergabe (Tipping Off-Verbot) 851

IV. Fazit 852

24. Kapitel

Sanktions-Compliance als Teil eines effektiven Compliance-Management-Systems

(Salathé/Moussaoui)

I. Einleitung 855
1. Terminologien und Begriffsverständnis 856

2. Sanktionen: Historie, Gründe und Ziele 857

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

III. Konsequenzen und Haftung 885
1. Straf- und ordnungswidrigkeitsrechtliche Folgen 885
a) § 17 AWG 885
b) § 18 AWG 885
c) § 19 AWG 886

d) Vermeidung von Verstößen 887
2. Zivilrechtliche Folgen 887
3. Schadenserssatz 889
4. Sonstige Folgen 889

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

V. Checkliste 900

25. Kapitel

Exportkontrolle und Compliance

(v. Bodungen)

I. Einleitung 903

II. Rechtsgrundlagen der Exportkontrolle in Deutschland 904
1. Supranationale Vorgaben 904
2. Nationale Vorgaben 906
3. Relevanz ausländischen Exportkontrollrechts 906
a) Allgemeines 906
b) Insbesondere: US-Re-Exportkontrolle 906

III. Exportkontrollrechtliche Genehmigungspflichten 908
1. Allgemeines 908
2. Genehmigungspflichten bei Ausfuhren in Länder außerhalb der EU 908
a) Gelistete Güter 908
b) Nicht gelistete Güter 909
3. Genehmigungspflichten bei Verbringungen 910
a) Verbringungen bei Endverbleib in der EU 910

b) Verbringungen mit anschließender Ausfuhr 910
4. Sonstige Genehmigungspflichten 911
a) Handels- und Vermittlungsgeschäfte 911
b) Technische Unterstützung 911

IV. Exportkontrollrechtliches Genehmigungsverfahren 912
1. Zuständigkeit des BAFA 912
2. Ablauf des Genehmigungsverfahrens 913
3. Genehmigungstypen 914
4. Sanktionen bei exportkontrollrechtlichen Verstößen 915

V. Exportkontrollrechtliche Compliance-Strukturen 916
1. Allgemeines 916
2. Der Ausfuhrverantwortliche 918
3. Modell eines innerbetrieblichen Exportkontrollsystems 919
a) Überblick über die relevanten Strukturelemente 920
b) Umsetzung im Einzelfall 922

VI. Zusammenfassung und Ausblick 924

26. Kapitel

Compliance in M&A-Transaktionen

(Ullrich)

I. Einleitung 927

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

c) Übernahmerechtliche M&A-Compliance 944
5. Pflicht zur Durchführung einer rechtlichen Due Diligence 945
a) Regelfall. 945
b) Besonders gelagerte Fälle. 946
c) Nachgelagerte Due Diligence (Post-Closing Due Diligence) . 948
6. (Abbruch der) Vertragsverhandlungen 948
7. Zustimmungserfordernisse 950
a) Zustimmung von Aufsichtsgremien und/oder der Gesellschafter 950
b) Zustimmung von Ehegatten oder Lebenspartnern. 954
8. Vereinbarung von Wettbewerbsverboten im Unternehmenskaufvertrag 956

III. Materielle M&A-Compliance – Prüfung von/Umgang mit Compliance in der Zielgesellschaft 957
1. Due Diligence 957
a) Erfordernis einer Compliance-Due Diligence 957
aa) Einführung unter besonderer Beachtung von ESG/CSR . 957
bb) Erfordernis der Durchführung einer Compliance-Due Diligence 959
cc) (Eigen-)Interesse der Geschäftsleitung (Business Judgement Rule). 961
dd) Normative Kraft des Faktischen. 962
b) Vorgehensweise: Abgestufte, risikobasierte Compliance-Due Diligence 962
aa) Rechtlicher Rahmen. 962
bb) Ermittlung des Risikoprofils der Zielgesellschaft 963
cc) Risikobewertung und Dokumentation 964
dd) Eigentliche Due Diligence 964
c) Due Diligence nach Vollzug 964
2. Umgang mit bekannten/bekanntgewordenen Compliance-Verstößen/-Risiken 965
a) Risikobewertung 965
b) Umgang mit bekannten/entdeckten Compliance-Risiken 966

IV. Zusammenfassung 969

27. Kapitel

Kartellrechts-Compliance

(Seeliger/Mross/Seydel)

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

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

4. Art und Umfang der Haftung 1005
a) Strafrechtliche Sanktionen 1005
b) Bußgelder 1006
aa) EU-Recht 1006
bb) Deutsches Recht 1007
c) Schadensersatz 1009
aa) Individualansprüche 1009
bb) Kollektiver Rechtsschutz 1011
cc) Schadensausgleich im Innenverhältnis 1012
d) Sonstige Nachteile 1012

II. Management der Kartellrechtsrisiken in der Praxis 1013
1. Risikoanalyse: Identifizierung und Bewertung 1015
a) Kartellrechtliches Risikoprofil 1015
b) Geschäftstätigkeit und Geschäftsbeziehungen 1015
c) Risikokategorisierung und Risikobewertung 1016
d) Einführung eines Top-down-Ansatzes 1017
2. Präventive Maßnahmen 1017
a) Richt- und Leitlinien zum Kartellrecht 1018
b) Schulungen (Präsenzschulungen und Webinars/E-Learning) . 1021
3. Maßnahmen zur Kontrolle/Aufdeckung 1023

III. Behördliche Untersuchungen 1025
1. Durchsuchungen der EU-Kommission 1026
a) Zuständigkeit 1026
b) Befugnisse 1027
c) Elektronische Durchsuchung 1028
d) Typischer Ablauf 1029
2. Durchsuchungen des Bundeskartellamts 1030
a) Zuständigkeit 1030
b) Befugnisse 1031
c) Elektronische Durchsuchung 1033
d) Typischer Ablauf 1034
3. Verhaltensregeln für die Unternehmen 1034
a) Vor der Durchsuchung 1034
b) Während der Durchsuchung 1035
c) Nach der Durchsuchung 1037

28. Kapitel

Compliance-Anforderungen im Wettbewerb um öffentliche Aufträge

(Scherer)

I. Einleitung 1039

II. Anforderungen an Unternehmen in Vergabeverfahren 1040

III. Ausschlussgründe 1042
1. Zwingende Ausschlussgründe 1042
a) Straftatbestände 1042
b) Steuer- und Abgabentatbestände 1043
2. Fakultative Ausschlussgründe 1044
a) Verstoß gegen umwelt-, sozial- oder arbeitsrechtliche Verpflichtungen 1044
b) Insolvenz und Liquidation 1045
c) Schwere Verfehlung im Rahmen beruflicher Tätigkeit 1045
d) Wettbewerbsbeschränkende Vereinbarungen oder abgestimmte Verhaltensweisen 1046
e) Interessenkonflikt 1047
f) Vorbefassung 1047
g) Mangelhafte Leistung bei Ausführung früherer Aufträge 1048
h) Schwerwiegende Täuschung bei Eignungsprüfung 1048
i) Unzulässige Einflussnahme 1049

IV. Wettbewerbsregister 1050
1. Einrichtung des Wettbewerbsregisters 1050
2. Eintragung von Rechtsverstößen 1050
3. Einbindung in das Vergabeverfahren 1051
4. Löschung von Eintragungen 1052
5. Rechtsbehelfe 1053

V. Selbstreinigung 1053
1. Selbstreinigung im Vergabeverfahren 1053
a) Prüfung durch Vergabestelle 1053
b) Prüfung durch Wettbewerbsregister 1054
2. Kriterien der Selbstreinigung 1054
a) Ausgleich des Schadens 1054
b) Zusammenarbeit zur Aufklärung 1055
c) Technische, organisatorische und personelle Maßnahmen 1056

VI. Ausschlussfristen 1058
1. Fristenregelung bei zwingenden Ausschlussgründen 1058
2. Fristenregelung bei fakultativen Ausschlussgründen 1058
3. Ermessensausübung 1059

29. Kapitel

Tax Compliance

(Schwartz)

I. Einleitung 1061

II. Steuerliche Pflichten 1063

1. Allgemeine steuerliche Pflichten 1063
2. Spezifische materiell-rechtliche Problemschwerpunkte 1068
a) Lohnsteuer und Sozialabgaben 1068
b) Umsatzsteuer 1069
c) Verdeckte Gewinnausschüttungen 1070
d) Anzeigepflicht nach § 153 AO 1071
e) Tochtergesellschaften und Betriebstätten im Ausland 1074
f) Internationale Verrechnungspreise 1075
g) Versagung des Betriebsausgabenabzugs nach § 160 AO 1075
h) Betriebsausgabenabzugsverbot nach § 4 Abs. 5 Satz 1 Nr. 10 EStG 1076

III. Risiken mangelnder Tax Compliance 1078
1. Steuerliche Haftungsrisiken 1078
2. Steuerstrafrechtliche und steuerordnungswidrigkeitenrechtliche Risiken 1080
a) Sanktionen gegen Organe und Mitarbeiter 1080
aa) Steuerhinterziehung und leichtfertige Steuerverkürzung (§§ 370, 378 AO) 1080
(1) Täter 1080
(2) Objektiver Tatbestand 1081
(3) Subjektiver Tatbestand 1085
(4) Strafe 1086
bb) Verletzung der Aufsichtspflicht (§ 130 OWiG) 1087
b) Sanktionen gegen das Unternehmen 1088
aa) Verbandsgeldbuße (§ 30 OWiG) 1088
bb) Einziehung (§ 29a OWiG) 1090

IV. Tax Compliance-System 1091
1. Risikoanalyse 1091
2. Ausgestaltung eines Tax Compliance-Systems 1092
a) Zuständigkeit für Tax Compliance 1092
b) Zuständigkeit und Verantwortlichkeit bzgl. der steuerlichen Pflichten 1092
c) Berichtswege/Berichtspflichten 1093
d) Prozessbeschreibung Deklarationswesen 1095
e) Kontroll- und Überwachungsmaßnahmen 1095
f) Umgang mit Betriebsprüfungen 1096
g) Schulungen 1098
h) Dokumentation 1098
3. Prüfungserleichterungen nach Art. 97 § 38 EGAO 1099
a) Tatbestandsvoraussetzungen 1099
b) Rechtsfolgen 1101

V. Zertifizierung des Tax Compliance-Systems durch Dritte 1102

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

VII. Fazit 1112

Literaturverzeichnis 1113

Sachregister 1157

Teil 1
Grundlagen, Erfolgsfaktoren und Handlungsstrategien

1. Kapitel
Compliance Management – Grundlagen, Orientierungshilfen und Erfolgsfaktoren

I. Grundlagen und Zusammenhänge

1. Anhaltende Bedeutung von Compliance und Compliance Management

Die rechtliche Bedeutung von Compliance für Unternehmen und Verbände[1] geht über den Wortsinn einer Regelbefolgung bzw. Regelkonformität weit hinaus.[2] Wenngleich es nach wie vor an einer einheitlichen Definition fehlt, wird mit Compliance häufig die Summe derjenigen Maßnahmen bezeichnet, die der Einhaltung aller an Unternehmen gerichteten Gesetze und Regeln dienen.[3] Im Mittelpunkt stehen damit **organisatorische Vorkehrungen** zur Verhinderung von Regelverstößen, zur Kontrolle der eingeleiteten Maßnahmen, zur Aufdeckung von „Non-Compliance", zur angemessenen Reaktion bzw. Sanktionierung von Regelverletzungen sowie zur regelmäßigen Aktualisierung der etablierten Strukturen und Maßnahmen (**Compliance Management**).[4] **1**

Primär verantwortlich für das Compliance Management sind die Mitglieder der **Leitungsorgane**, die für normgerechtes Verhalten im Unternehmen und durch das Unternehmen sorgen müssen.[5] Soweit die Geschäftsleiter nicht schon selbst **2**

---

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

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

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

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

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

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

3 Compliance und das damit erforderliche Compliance Management sind durch eine anhaltende **Dynamik des rechtlichen Rahmens** geprägt, die durch vielfältige Aktivitäten des Gesetzgebers und der Gerichte sowie durch neue Entwicklungen in Rechtswissenschaft und Unternehmenspraxis bedingt sind. Dies gilt insbesondere für wachsende Anforderungen im Bereich der sog. „**ESG-Compliance**",[11] für die besonderen Compliance-Herausforderungen im Zuge der **Digitalisierung**[12] sowie für gestiegene Risiken bei dem Verstoß gegen Sanktionsregelungen („**Sanctions Compliance**").

4 Neben den (vormals überwiegend freiwillig zu erfüllenden) Anforderungen der **Corporate Social Responsibility** (**CSR**) werden Unternehmen und ihre Leitungsorgane zunehmend mit neuen Compliance-Pflichten zu **ESG-Themen**, also den Themenfeldern „**Environment**" (u. a. Klimaschutz, nachhaltige Naturnutzung, Tierschutz), „**Social**" (u. a. Schutz von Menschenrechten, Verhinderung von Ausbeutung, faire Arbeitsbedingungen) und „**Governance**" (u. a. gute Unternehmensführung, Korruptionsbekämpfung, Ermöglichung von Melde-

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

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

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

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

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

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

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

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

Neben diesen neuen Sorgfaltspflichten in Lieferketten und **Wertschöpfungsnetzwerken** werden viele Unternehmen (je nach Geschäftsmodell und geschäftlichen Aktivitäten) mit zahlreichen weiteren **ESG-Compliance-Vorgaben** konfrontiert, beispielsweise im Zusammenhang mit der EU-Entwaldungsverord- **5**

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

2. Compliance Management als Inbegriff regelkonformer Unternehmensorganisation

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

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

---

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

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

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

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

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

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

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

10 Diese **Grundfragen einer rechtskonformen Unternehmensorganisation**[36] betreffen grundsätzlich alle Unternehmen, von der börsennotierten Aktiengesellschaft und der mittelständischen GmbH bis hin zum Start-up-Unternehmen.[37] Denn sämtliche Unternehmen und ihre Leitungsorgane müssen bei ihrer Tätigkeit eine Vielzahl von Normen und rechtlichen Vorgaben von Gerichten und Behörden beachten.[38] Zahlreiche aktuelle Fälle von „Non-Compliance" bei Unternehmen und Verbänden aus ganz unterschiedlichen Branchen, mit unterschiedlichen Geschäftsmodellen und mit unterschiedlicher Größe und Struktur[39]

---

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

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

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

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

39 Zu prominenten Fällen von „Non-Compliance" und damit verbundener Nachteile und Kosten siehe. Zu aktuellen Compliance-Fällen → *Stehr/Knopp*, Kap. 15 Rn. 70. Siehe ferner *Jenne*, Die Überprüfung und Zertifizierung von Compliance-Management-Systemen, S. 21 ff.; *Gomer*, Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft, S. 73 ff. Aus der Vielzahl in den Medien gemeldeter (Verdachts-)Fälle von „Non-Compliance" vgl. beispielsweise die Meldungen zum Fall „Wirecard": https://www.rnd.de/wirtschaft/wirecard-skandal-was-passierte-wann-die-chronologie-des-versagens-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" u. a.: https://www.rnd.de/wirtschaft/chronlogie-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-attacke-fakten-zum-globalen-cyberangriff-a-1147523.html. Compliance-Verstöße sind häufig auch Gegenstand von Kartellverfahren der EU-Kommission, siehe etwa: https://www.spiegel.de/wirtschaft/unternehmen/

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

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

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

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

---

bmw-daimler-und-vw-unter-kartellverdacht-eu-kommission-verschaerft-ermittlungen-a-1228660.html; oder: https://www.spiegel.de/wirtschaft/unternehmen/wilke-wurst-behoerden bericht-zeigt-zustaende-nach-fabrikschliessung-a-1293802.html (alle Quellen zuletzt abgerufen am 24.9.2024).

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

4. Funktionen von Compliance und Compliance Management

Die dargestellten Risiken und Nachteile aus „Non-Compliance" zeigen, dass wirksame Compliance-Maßnahmen für alle Unternehmen und Verbände aktuell und relevant sind.[54] Die **proaktive Vermeidung bzw. Reduzierung von Regelverstößen** ist damit nicht nur eine Pflicht der Leitungsorgane, sondern eine wichtige Führungs- und Organisationsaufgabe (siehe dazu unter → Rn. 36 f., 54 ff.).[55] Compliance Management erfüllt dabei die folgenden **Funktionen**:[56] Compliance Management dient sowohl dem **Schutz** des Verbands vor zivilrechtlicher Haftung und strafrechtlichen Sanktionen als auch der Prävention bzw. Reduzierung persönlicher zivil- und strafrechtlicher Haftungsrisiken der Mitglieder der Leitungsorgane und der Mitarbeiter.[57] Darüber hinaus zielen Compliance-Maßnahmen auch auf den Schutz vor Angriffen auf das Unternehmen sowie den Schutz der Unternehmensposition im Wettbewerb.[58] Ferner dient Compliance dem Schutz der **Reputation** und des **Vertrauens der Stakeholder** in eine ordnungsgemäße und rechtskonforme Geschäftstätigkeit.[59] **13**

Neben dieser präventiven **Schutzfunktion** ist auch die **Risikomanagementfunktion** wichtig, denn zwischen Compliance Management und Risikomanagement besteht ein enger Zusammenhang:[60] Das Risikomanagement mit seinen Methoden und Verfahren ist eine wichtige Erkenntnisquelle für die Identifikation und systematische Erfassung von Compliance-Risiken.[61] **14**

---

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

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

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

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

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

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

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

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

15 Das Compliance Management erfüllt ferner eine wichtige **Informations- und Beratungsfunktion**,[62] welche sowohl die Beratung der Unternehmensleitung zur Steuerung von Compliance-Risiken durch organisatorische Maßnahmen[63] als auch die Organisation der Beratung aller Unternehmensangehörigen in allen relevanten Compliance-Fragen umfasst.[64] Da zu den notwendigen organisatorischen Maßnahmen auch die kontinuierliche Überwachung und Kontrolle relevanter Normen und Regeln und deren Durchsetzung zählt,[65] erfüllt Compliance ferner eine **Monitoring-Funktion**.[66] Durch die systematische Erfassung von Rechts- und Compliance-Risiken, die kontinuierliche Beobachtung neuer rechtlicher Entwicklungen und deren Auswirkungen auf das Compliance-System hat das Compliance Management im Unternehmen zudem eine **Qualitätssicherungs- und Innovationsfunktion**.[67] Indem ein wirksames Compliance Management dazu beiträgt, Normverstöße zu verhindern bzw. zu reduzieren, fördert es die Glaubwürdigkeit des Unternehmens bei seinen Mitarbeitern, Kunden, Geschäftspartnern und sonstigen Stakeholdern und erfüllt damit eine **Marketing-Funktion**.[68]

5. Compliance Management als Daueraufgabe im dynamischen Umfeld

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

---

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

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

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

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

66 Vgl. *Lösler*, NZG 2005, 104, 105.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

17 Wie ausgeführt, ergeben sich aus vielfältigen Regelungen unter dem Oberbegriff der „**ESG-Compliance**" zahlreiche neue Pflichten und Haftungsrisiken für Unternehmen und deren Leitungsorgane. Das LkSG als prominentes Beispiel der ESG-Regulierung zeigt exemplarisch, dass bestehende Compliance-Programme um einen Bereich der **Supply-Chain-Compliance** (insbesondere in Bezug auf Menschenrechte und Umweltbelange) erweitert werden müssen.[81]

18 Rechts- und Compliance-Risiken sind ferner bei Wachstumsstrategien, etwa beim Erwerb von Unternehmen und Restrukturierungsmaßnahmen oder beim Eintritt in Joint Ventures zu beachten („**Compliance Due Diligence**").[82] Wie die zunehmende Regulierung von Lieferketten und Wertschöpfungsnetzwerken zeigt, gewinnt dabei die proaktive Compliance-Kontrolle von Geschäftspartnern, Vertriebsmittlern und sonstigen Intermediären immer größere Bedeutung („**Business Partner Compliance**").[83]

19 Exportorientierte Unternehmen müssen bei Einritt in neue Märkte zudem neue Vorgaben des **Exportkontrollrecht**s und des **Außenwirtschaftsrecht**s sowie im anwendbaren Umfang auch die Normen anderer Rechtsordnungen beachten.[84] Hinzu kommen neue Embargo-Bestimmungen und sonstige **Sanktionsrecht**sregelungen.[85]

6. Compliance als Basis für „Good Corporate Governance"

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

---

80 Siehe → *Komma*, Kap. 23.

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

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

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

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

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

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

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

21 Die Diskussion um verantwortungsvolle Unternehmensführung, Corporate Social Responsibility und „Good Corporate Citizenship" mit einem Fokus auf Umwelt und Sozialbelange zeigt sich auch in der neuen Fassung des **Deutschen Corporate Governance Kodex (DCGK)** von 2022:[90] So wurde in der Präambel die Bedeutung von Sozial- und Umweltfaktoren für den Unternehmenserfolg um den Zusatz erweitert, dass die Tätigkeiten des Unternehmens Auswirkungen auf Mensch und Umwelt haben.[91] Damit geht es nicht mehr allein um die Auswirkungen von Sozial- und Umweltbelangen auf den Unternehmenserfolg („Outside-in-Perspektive"), vielmehr sind nunmehr auch die Auswirkungen der Unternehmenstätigkeit auf Menschen und Umwelt zu berücksichtigen („**Inside-out-Perspektive**").[92] Vorstand und Aufsichtsrat müssen **Sozial- und Umweltfaktoren** bei der Führung des Unternehmens bzw. Überwachung der Unternehmenstätigkeit im Rahmen des Unternehmensinteresses berücksichtigen.[93]

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

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

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

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

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

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

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

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

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

7. Compliance und Reputationsmanagement

23 Wie die aktuelle Diskussion zum Zusammenhang zwischen Compliance, Governance und ESG zeigt, wird der unternehmerische Verantwortungsbereich durch zahlreiche Normen und Vorgaben für verantwortliches gesellschaftliches Handeln immer mehr erweitert.[95] Zu bereits existierenden und oben exemplarisch skizzierten umfangreichen Rechtspflichten tritt ein genereller Trend der „**Verrechtlichung**" unterschiedlicher Anforderungen des „**Soft Law**" hinzu, wie dies insbesondere die neuen Sorgfaltspflichten in der Lieferkette,[96] die Pflicht zur CSR-Berichterstattung,[97] besondere Compliance-Maßnahmen nach der EU-Konfliktmineralien-Verordnung[98] und weitere neue Compliance-Pflichten zeigen.[99] So hat sich inzwischen ein neuer Bereich der „CSR-Compliance" bzw. „ESG-Compliance" entwickelt.[100]

24 Die Erfüllung neuer Sorgfaltspflichten und Anforderungen der ESG-Compliance dienen auch der Sicherung der Unternehmensreputation, die als bedeutender immaterieller Vermögensgegenstand gilt.[101] Die sog. **Image- und Reputationsschäden** sind häufig schwer zu beziffern, sie können aber zu erheblichen Verlusten und Nachteilen und bei börsennotierten Unternehmen bis hin zu einem Einbruch des Börsenwerts führen.[102] Der Schutz der Reputation durch ein wirksames Compliance Management spielt daher eine zentrale Rolle, das positive Image des Unternehmens in der Öffentlichkeit und bei den maßgeblichen Bezugsgruppen (Mitarbeiter, Kunden, Lieferanten, Investoren etc.) kann durch „Non-Compliance" nachhaltig beeinträchtigt oder ganz zerstört werden.[103] Reputationsrisiken und „**Reputationsmanagement**" haben sich daher zu wichtigen Themen für das Compliance- und Risikomanagement entwickelt.[104]

---

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

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

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

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

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

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

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

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

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

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

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