

Christoph Becker
Carina Metscher
Hanspeter Vietz *Hrsg.*

Compliance Officer

Das Augsburger Qualifizierungsmodell

2. Auflage



Springer Gabler

Compliance Officer

Christoph Becker • Carina Metscher •
Hanspeter Vietz
Hrsg.

Compliance Officer

Das Augsburger Qualifizierungsmodell

2. Auflage

Hrsg.

Christoph Becker
Juristische Fakultät
Universität Augsburg
Augsburg, Deutschland

Carina Metscher
Zentrum für Weiterbildung und Wissenstransfer
Universität Augsburg
Augsburg, Deutschland

Hanspeter Vietz
Zentrum für Weiterbildung und Wissenstransfer
Universität Augsburg
Augsburg, Deutschland

ISBN 978-3-658-42420-6 ISBN 978-3-658-42421-3 (eBook)
<https://doi.org/10.1007/978-3-658-42421-3>

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

© Der/die Herausgeber bzw. der/die Autor(en), exklusiv lizenziert an Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2014, 2025

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jede Person benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des/der jeweiligen Zeicheninhaber*in sind zu beachten.

Der Verlag, die Autor*innen und die Herausgeber*innen gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autor*innen oder die Herausgeber*innen übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung/Lektorat: Guido Notthoff

Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Wenn Sie dieses Produkt entsorgen, geben Sie das Papier bitte zum Recycling.

Geleitwort von Dr. Gisa Ortwein

Compliance ist längst keine neue Disziplin mehr, sondern hat sich zu einer fest verankerten Säule erfolgreicher Unternehmen und Organisationen entwickelt. Ihre Bedeutung bleibt dennoch ungebrochen hoch, und zwar aus einem einfachen Grund: Die Geschäftswelt hat sich drastisch verändert, und mit ihr auch die Anforderungen an Compliance.

Während mit dem Begriff „Compliance“ in der Vergangenheit primär Regel- und gesetzeskonformes Verhalten gemeint war – und obwohl diese Grundprinzipien immer noch von zentraler Bedeutung sind – muss „Compliance“ heute einer deutlich höheren Komplexität Rechnung tragen. Unternehmensumfelder sind globaler und vernetzter geworden, wodurch sich die Vielfalt und Anzahl der relevanten Vorschriften erhöht hat. Die Digitalisierung hat neue Technologien und Datenströme hervorgebracht, die spezifische Compliance-Anforderungen und -Risiken mit sich bringen. Ethische Standards und soziale Verantwortung haben einen Stellenwert erlangt, der der Einhaltung von Gesetzen nichts nachsteht: Unternehmen und Organisationen müssen nicht nur juristisch korrekt handeln, sondern auch ethisch und verantwortungsbewusst agieren, um das Vertrauen ihrer Stakeholder zu gewinnen und zu erhalten.

Entsprechend hat sich auch die Rolle des Compliance Officer gewandelt. Compliance Officer sind längst nicht mehr reine Regelwächter, sondern auch Berater, die Unternehmen bei der Gestaltung ethischer und rechtskonformer Geschäftspraktiken unterstützen. Sie müssen nicht nur Gesetze verstehen, sondern auch in der Lage sein, Risiken zu identifizieren, zu bewerten und proaktiv darauf zu reagieren. Sie brauchen solides Handwerkzeug und umfassendes Grundlagenwissen. Und gleichzeitig brauchen Sie die notwendige Flexibilität und den Willen zur kontinuierlichen Weiterbildung, um in der Lage zu sein, schnell und proaktiv auf neue Entwicklungen reagieren zu können. Professionalisierung und Agilität sind damit zu zentralen Leitbildern des Berufsstandes der Compliance Officer geworden.

Dieses Buch, das gleichzeitig Begleitband zum Zertifikatsstudium „Compliance Officer“ des Zentrums für Weiterbildung und Wissenstransfer (ZWW) der Universität Augsburg ist, vermittelt die essentiellen Kenntnisse zur Compliance und beleuchtet deren vielschichtige Facetten. Es bildet wesentliche Grundlagen der Compliance ab und wird damit

ein unverzichtbarer Begleiter und leistungsstarker Kompass für Compliance Professionals und all jene, die sich zukünftig in dieser wichtigen Disziplin engagieren wollen.

Dr. Gisa Ortwein
Director Integrity der NORMA Group SE
Präsidentin des Berufsverbandes der Compliance Manager (BCM) e.V.

Geleitwort von Dr. Marcus Gebert und Christina Braun

In Unternehmen galt – überspitzt ausgedrückt – Compliance lange Zeit als unbewegliche, geschäfts fremde Materie, die mit überzogener Bürokratie Geschäfte und Business- Opportunitäten verhindere.

Dieses Bild hat sich grundlegend geändert und der Mehrwert, den eine an klaren Compliance-Maßstäben ausgerichtete Unternehmensführung bietet, wird allgemein anerkannt. Denn Fakt ist:

- Compliance schafft eine Unternehmenskultur, die von Ehrlichkeit, Verantwortungsbewusstsein und Vertrauen geprägt ist;
- Compliance sichert den Erfolg des Unternehmens ab, schützt es vor finanziellen Schäden und ist damit ein wesentlicher Business-Faktor;
- Gute Compliance stärkt das positive Image eines Unternehmens nach innen und nach außen;
- Compliance schafft eine Arbeitsatmosphäre, in der Mitarbeitende sich wohlfühlen und so aktiv zum Unternehmenserfolg beitragen.

Die Akzeptanz von Compliance wird maßgeblich davon bestimmt, dass man Mitarbeitende mitnimmt, schult und Verständnis für die Bedeutung von regelkonformem und werteorientiertem Miteinander schafft.

Dabei gilt, dass Compliance verständliche und klare Regelungen vorgeben muss, die Mitarbeitende nachvollziehen und verinnerlichen können. Compliance kann so Bestandteil einer gesunden Unternehmenskultur werden.

Andererseits muss eine Compliance-Organisation auch so aufgestellt sein, dass Verdachtsfälle zügig untersucht und begangene Verstöße angemessen sanktioniert werden. Auch dies trägt zur Akzeptanz von Compliance bei.

Aufgrund dieser Komplexität ist zeitgemäße Weiterbildung wichtig. Genau das bietet das Augsburger Zertifizierungsmodell. Das Zertifikatsstudium zum „Compliance Officer“ zeigt praxisnah auf, wie ein Compliance-Management-System in verschiedenen Detaillierungen stufenweise eingeführt werden kann, das nicht nur inhaltlich einwandfrei ist, sondern auch dem Unternehmen entsprechend gestaltet ist. Aber es geht noch einen Schritt

weiter und vermittelt genau das Wissen, das man als Compliance-Expert:In braucht, um etwaige Schieflagen rechtzeitig zu erkennen, Red Flags zu identifizieren und professionell entgegenzusteuern.

Dieser Ansatz ist wegweisend, denn natürlich braucht es Kompetenz und Wissen, um eine Compliance-Funktion sicher und wertschöpfend auszufüllen. Aber genauso bedarf es des vermittelnden Verständnisses, dass kein Unternehmen compliant sein kann, wenn wir nicht alle Menschen erreichen, sowohl unsere Führungskräfte und Mitarbeitenden in allen Bereichen von Blue Collar bis White Collar, als auch unsere Lieferanten und diejenigen, die in unserer Lieferkette beschäftigt sind.

Das heißt, dass wir mit den Fachabteilungen Hand in Hand arbeiten, um bestmögliche Lösungen zu finden. Und, ja – um ein Veto einzulegen, wenn die Compliance in Gefahr ist. Denn auch diese Grenze müssen wir weiterhin mit aller Bestimmtheit ziehen.

Dr. Marcus Gebert
Chefsyndikus/General Counsel

Christina Braun
Compliance Manager
KUKA AG

Vorwort zur 2. Auflage

Zum Werk Becker/Metscher/Vietz (Herausgeber), Compliance Officer – Das Augsburger Qualifizierungsmodell

Die zweite Auflage des Buches beruht auf dem interdisziplinären Compliance-Modell und dem damit verbundenen Qualifizierungskonzept, die unter Mitwirkung von Dr. Walburga Schettgen-Sarcher, Sebastian Bachmann und Professor Dr. Peter Schettgen an der Universität Augsburg entwickelt und von ihnen als Herausgebern erstmalig veröffentlicht wurden. In die Neuauflage flossen sowohl Änderungen rechtlicher Rahmenbedingungen und wissenschaftlicher Lösungsansätze der beteiligten Disziplinen ein als auch praktische Erfahrungen in der Wahrnehmung von Compliance im Wirtschaftsleben sowie Beobachtungen aus der Vermittlung von Compliance in der Weiterbildung. Wie schon die Erstauflage soll auch die zweite Auflage die Weiterbildung an der Universität Augsburg begleiten und sich womöglich weitere Leserkreise erschließen.

Die Beiträge stammen zumeist noch aus dem Autorenkreis der ersten Auflage. Doch machen sich Wandel inhaltlicher Schwerpunkte in der Augsburger Weiterbildung zum „Compliance Officer“ in Veränderungen der Autorenschaft ebenso bemerkbar wie in Themenzuschnitten und Ausführungen im Einzelnen. Der einführende Beitrag dokumentiert diese Entwicklung: Er ist der ersten Auflage entnommen und zeigt die Sicht der Verfasser Bachmann und Fechner auf Grundlinien und Möglichkeiten der Vermittlung von Compliance zu Beginn der Weiterbildung im Augsburger Modell, den damaligen Stand von Praxis und Wissenschaft abbildend. Doch haben die Mitherausgeber Carina Metscher und Hanspeter Vietz ihn überarbeitet und Ergänzungen angebracht, die die erreichte gegenwärtige Struktur des Augsburger Qualifizierungsmodells widerspiegeln.

Der Aufbau des Buches konnte bei allen Detailänderungen im Wesentlichen gleichbleiben. Auf Einführung und Kennzeichnung der Interdisziplinarität von Pflichterfüllung (Teil 1) folgen exemplarische Risiko-Analysen (Teil 2). Weitere Beiträge setzen sich mit Möglichkeiten und Grenzen des Einsatzes von Kontrollmechanismen (Teil 3) und der Integration von Compliance in den Betriebsalltag (Teil 4) auseinander. Ethische Fragen und die Identifikation von Compliance als Führungsaufgabe (Teil 5) beschließen das Buch.

Die Wahl des orthographischen Regelwerks blieb den Mitwirkenden freigestellt. Im Bildungswesen wird überdies häufig nach gleicher Berücksichtigung der Geschlechter in theoretischer Darstellung und praktischer Anwendung gefragt. Wie zur ersten Auflage gab es auch zur vorliegenden zweiten Auflage keine Vorgabe an die Autoren, auf welche Weise alle Geschlechter anzusprechen seien. Die Beiträge zeigen unterschiedliche Lösungen. Doch sind in diesem Buch auch dort, wo nur die maskuline Form verwendet ist, alle Geschlechtsidentitäten gemeint. Das generische Maskulinum entspricht der Sprache des Gesetzes, welches Grundbedingungen für Compliance formuliert. Die Vereinbarkeit von Erörterungen zur Pflichterfüllung mit der Sprache des Gesetzes hilft, Missverständnisse zu vermeiden. Die Gesetzessprache steht in der Tradition des römischen Rechts, welches die Wurzel der modernen europäischen Rechtsordnungen darstellt. Im sechsten Jahrhundert nach Christus ließ der oströmische Kaiser Justinian von Auszügen aus den Werken römischer Rechtswissenschaft der vorangegangenen Jahrhunderte eine Zusammenstellung anfertigen. Diese Zusammenstellung erhielt die Bezeichnung „Digesten“ (Zerlegtes, Verarbeitetes) oder „Pandekten“ (Allumfassendes), und Justinian führte sie im Jahre 533 als Gesetz ein. Die justinianischen Digesten enthalten an verschiedenen Stellen Klarstellungen zur geschlechtsneutralen Begriffsverwendung, entnommen den Schriften der Juristen Gaius (Mitte des 2. Jahrhunderts) und Ulpianus (um 200). Man liest: „qui‘ sic accipendum est ,quaeve‘ – ,derjenige‘ muss man so auffassen, als ob auch ,oder diejenige‘ dort stünde“ (Digesten 13.5.1.1 nach Ulpianus); „Verbum hoc ,si quis‘ tam masculos quam feminas complectitur“ – Der Ausdruck „wenn einer“ umfasst Männer ebenso wie Frauen (Digesten 50.16.1 nach Ulpianus); „Patroni“ appellatione et patrona continetur – In der Bezeichnung „Schutzherr“ ist auch die Schutzherrin enthalten (Digesten 50.16.52 nach Ulpian); „Hominis appellatione tam feminam quam masculum contineri non dubitatur“ – Zweifellos umfasst die Bezeichnung „Mann“ [im römischen Recht Ausdruck für Sklave] das weibliche wie das männliche Geschlecht (Digesten 50.16.152 nach Gaius); „Liberti appellatione etiam libertam contineri placuit“ – Man hat sich darauf verständigt, dass die Bezeichnung „Freigelassener“ auch die Freigelassene enthält (Digesten 50.16.172 nach Ulpian).

Herrn Guido Nothoff vom Springer Gabler Verlag möchten wir ganz herzlich danken für die erneut ausgezeichnete, zuvorkommende und geduldige Betreuung zur Realisierung der Neuauflage des vorliegenden Kompendiums.

Augsburg, Deutschland
Dezember 2024

Christoph Becker
Carina Metscher
Hanspeter Vietz

Vorwort der Herausgeber der 1. Auflage

Compliance, das heißt regelkonformes und gesetzestreues Handeln und Verhalten in Unternehmen, ist durch Kartellrechtsfälle, Geldwäsche- und Korruptionsskandale mittlerer und großer Unternehmen, die wiederholt in den Schlagzeilen auftauchten, nicht nur beim Fachpublikum, sondern auch in der allgemeinen Öffentlichkeit zu einem gängigen Begriff geworden. Durch zahlreiche Richtlinien, wie zum Beispiel dem Corporate Governance Codex, dem KonTraG und MaComp im Banken- und Versicherungsbereich, wurden Unternehmen verpflichtet, für die Einhaltung von Gesetzen im Unternehmen zu sorgen. Dafür sind entsprechende Compliance-Strukturen zu schaffen und Programme zu deren Funktionieren zu implementieren. Allein der Blick auf Recht und Struktur wird jedoch dem Themenkomplex „Compliance“ nicht gerecht. Auch betriebswirtschaftliche Implikationen, die ein unternehmerisches Handeln unter Compliance-Gesichtspunkten ermöglichen, und nicht zuletzt der „menschliche Faktor“ spielen bei der Etablierung und dem Gelebtwerden von Compliance neben den rechtlichen und organisatorischen Aspekten eine erhebliche Rolle.

Ziel und Anliegen des Buches ist es, das Thema Compliance in seinen vielfältigen Facetten darzustellen und diese in einen ganzheitlichen Ansatz zu integrieren. Im vorliegenden Handbuch drückt sich diese Integration in einem Vierklang aus, der das Thema Compliance in seiner rechtlichen, betriebswirtschaftlichen, psychologischen und ethischen Dimension reflektiert. Das Handbuch selbst soll nicht nur Einblicke in die Compliance gewähren und Hintergründe aufzeigen, sondern auch praxisorientiert auf die relevanten Fragestellungen hinweisen und Unterstützung bei der praktischen Umsetzung leisten. Darüber hinaus fungiert das Handbuch als Begleitlektüre zum Zertifikatskurs Compliance Officer (Univ.), der am Zentrum für Weiterbildung und Wissenstransfer (ZWW) der Universität Augsburg konzipiert wurde und seit 2011 kontinuierlich mit Erfolg durchgeführt wird.

Inhaltlich spiegelt das Compliance-Handbuch – Das Augsburger Qualifizierungsmodell – die Lerninhalte des Zertifikatskurses und dessen Modulstruktur wider: Nach Be trachtung der rechtlichen Rahmenbedingungen, der betriebswirtschaftlichen Grundlagen und des Risikomanagement-Systems wird Compliance als Führungsaufgabe beleuchtet. Dabei stehen die ethische Verantwortung des Unternehmens, der Führungskräfte und

Mitarbeiter ebenso im Vordergrund wie die persönlichen Anforderungen an den Compliance Officer bei der Einführung und Organisation von Compliance im Unternehmen. Die Themen Korruption, Kapitalmarkt und Kartelle sowie die Bereitschaft eines Unternehmens, sich präventiv für interne oder externe Untersuchungen zu wappnen („investigation readiness“), bilden den dritten Schwerpunkt in Kurs und Buch. Wie Unternehmen versuchen, mit Hilfe von Codes of Conduct und Ethik-Standards regelkonformes Verhalten zu gewährleisten und durchzusetzen, vertieft das Kap. „Compliance in der Unternehmensentwicklung“. Dabei ist jedoch die arbeitsrechtliche Implementierung ein wesentlicher Faktor, der sämtliche Bereiche der Compliance-Organisation betrifft und maßgeblich beeinflusst. Hinweisgebersysteme, Whistleblowing, Datenschutz und Informationssicherheit bilden mit dem Kap. „Compliance und IT“ einen weiteren Schwerpunkt, der aufgrund aktueller weltpolitischer Ereignisse zunehmend an Aufmerksamkeit gewonnen hat.

Wir danken ausdrücklich den Autoren und Referenten des Zertifikatkurses, die mit ihren Beiträgen der Philosophie des ZWW an der Universität Augsburg gefolgt sind: nämlich vor einem wissenschaftlich fundierten Hintergrund die Compliance-Fragestellungen konsequent in ihrem Bezug zur Praxis weiter zu entwickeln und Compliance somit einem an der Anwendung interessierten Publikum leichter zugänglich zu machen. Als Herausgeber haben wir den Autoren keine Vorgaben gemacht, wie sie mit der Verwendung der männlichen versus weiblichen Schreibweise in ihren Texten umgehen sollen, so dass in den Beiträgen unterschiedliche Varianten auftreten. Unser Anliegen war es, an dieser Stelle Vielfalt zuzulassen und die Möglichkeiten der Autoren nicht von vornherein zu beschränken. Wir möchten von unserer Seite aber betonen, dass selbstverständlich auch das weibliche Geschlecht gemeint ist, falls nur die männliche Schreibweise gewählt wurde.

Guido Notthoff vom Gabler-Springer Verlag gebührt unser herzlicher Dank für seine aus-gezeichnete Betreuung und belastbare Geduld bei der Realisierung des Buchprojekts. Ein ganz besonderer Dank gilt abschließend Stephanie Kirsten am ZWW für die formale Überarbeitung und Gestaltung der Beiträge, ihre vielfältigen Recherchetätigkeiten, die mit großer Mühe und Ausdauer erstellten Korrekturleistungen sowie ihre wertvolle Unterstützung bei der Koordination des gesamten Buchprojektes.

Augsburg, Deutschland
Dezember 2013

Dr. Walburga Schettgen-Sarcher
Sebastian Bachmann
Professor Dr. Peter Schettgen

Inhaltsverzeichnis

Teil I Compliance als mehrdimensionales Anforderungssystem

1	Compliance als interdisziplinäre Herausforderung – Das Augsburger Qualifizierungsmodell	3
	Carina Metscher und Hanspeter Vietz	
	Literatur	15
2	Compliance: Grundlagen – Betriebswirtschaftliche Aspekte	19
	Thomas Berndt	
2.1	Einleitung	19
2.2	Nichtfinanzielle Erklärung	20
2.3	Nachhaltigkeitsberichterstattung	22
2.4	„Lieferkettengesetz“ und CSDDD	24
2.5	Prüfung	26
2.6	Risikomanagement und IKS	28
2.7	Corporate Governance und „Three Lines“	31
2.8	Fraud	33
2.9	Kultur	35
2.10	Schluss	36

Teil II Compliance-Risiken

3	Anti-Korruption	41
	Christian Pelz	
3.1	Einleitung	42
3.2	Rechtslage in Deutschland	44
3.2.1	Übersicht	44
3.2.2	Wesentliche Merkmale von Korruptionsdelikten	46
3.2.2.1	Vorteil	46
3.2.2.1.1	Materielle und immaterielle Vorteile	46
3.2.2.1.2	Drittvorteile	47

3.2.2.2	Unrechtsvereinbarung	47
3.2.2.2.1	Amtsträgerkorruption	48
3.2.2.2.2	Korruption im privaten Sektor	51
3.2.2.2.3	Bestechung und Bestechlichkeit im Gesundheitswesen	53
3.2.2.2.4	Mandatsträgerkorruption	53
3.2.2.2.5	Arbeitnehmervertreter	54
3.2.2.2.6	Sozialadäquate Zuwendungen	54
3.2.2.3	Tathandlung	54
3.2.3	Korruptionsstraftaten im Ausland	55
3.2.3.1	Amtsträgerkorruption	56
3.2.3.2	Mandatsträgerkorruption	57
3.2.3.3	Angestellte und Beauftragte im privaten Sektor bzw. von Heilberufen	57
3.3	Ausländische Rechtsvorschriften	57
3.3.1	Überblick	57
3.3.2	UK Bribery Act 2010	58
3.3.3	Der Foreign Corrupt Practices Act der USA	59
3.3.4	Sonstige ausländische Rechtsvorschriften	60
3.4	Anforderungen an Compliance	61
3.4.1	Notwendigkeit eines Compliance-Systems	61
3.4.2	Risikoanalyse	62
3.4.3	Richtlinien und Policies	63
3.4.3.1	Inhalt von Richtlinien	63
3.4.3.2	Branchenregelungen oder Richtlinien	64
3.4.3.3	Wesentliche Policies	64
3.4.3.3.1	Geschenke und Einladungen	64
3.4.3.3.2	Spenden und Sponsoring	67
3.4.3.3.3	Berater und Vermittler	68
3.4.4	Geschäftspartner, Joint Venture und M&A Due Diligence	69
3.4.5	Schulungen und Trainings	70
3.4.6	Hinweisgebersysteme	71
3.4.7	Audits und interne Untersuchungen	71
3.4.8	Reaktion auf entdecktes Fehlverhalten	72
3.4.9	Strafanzeige und Offenbarung gegenüber Ermittlungsbehörden	72
Literatur	73	
4	Competition Compliance	75
Christian Heinichen		
4.1	Einleitung	76
4.2	Kartellrechtliche Risiken	76
4.2.1	Kontakte zu Wettbewerbern	76
4.2.2	Beziehungen zu Lieferanten und Händlern	78

4.2.3	Missbrauch von Marktmacht	79
4.2.4	Risiken bei M&A-Transaktionen	80
4.3	Folgen von Kartellverstößen	81
4.3.1	Geldbußen	81
4.3.2	Schadenersatz	82
4.3.3	Persönliche Verantwortung	83
4.3.4	Vergaberechtliche Folgen	84
4.3.5	Weitere Folgen	84
4.4	Nachhaltige Wertschöpfung durch effektive Competition Compliance ...	85
4.5	Kartellverfahren	85
4.5.1	Wettbewerbsbehörden	85
4.5.2	Kartellbußgeldverfahren	86
4.5.3	Kartellschadenersatzverfahren	87
4.6	Kartellrechtliche Compliance-Maßnahmen	88
4.6.1	Überblick	88
4.6.2	Risikoanalyse	89
4.6.3	Empirische Screenings	91
4.6.4	Mock Dawn Raids	92
4.7	Fazit	93
	Literatur	94
5	Geldwäsche-Compliance bei Industrie- und Handelsunternehmen	
	(Güterhändler)	95
	Jürgen Krais	
5.1	Einführung	96
5.2	Geldwäsche	96
5.3	Terrorismusfinanzierung	98
5.4	Güterhandel: die internationale Perspektive	99
5.5	Güterhandel: Rechtslage in Deutschland	99
5.6	Güterhandel: Unternehmensgruppen	100
5.7	Privilegierte Güterhändler	101
5.8	Verdachtsmeldepflichten	103
5.8.1	Meldepflichtige Verdachtsfälle	103
5.8.2	Niedrige Verdachtsmeldeschwelle	103
5.8.3	Geldwäsche-Verdachtmeldung	105
5.8.4	Verbot des „Tipping-Off“	106
5.8.5	Wartefrist nach Verdachtmeldung	106
5.9	Kundensorgfaltspflichten im Verdachtsfall	107
5.9.1	Allgemeine Sorgfaltspflichten	107
5.9.2	Verstärkte Sorgfaltspflichten	108
5.9.3	Mitwirkungspflichten und Tipping-Off	108
5.10	Verdachtsfälle und Risiko der Strafbarkeit	109
5.11	Ausblick: EU-Verordnung zur Verhinderung von Geldwäsche	110
	Literatur	111

6 Tax Compliance	113
Christian Sering	
6.1 Definition der Tax Compliance	113
6.2 Aufgabenfelder der Tax Compliance	114
6.3 Gesetzliche Vorgaben, Rechtsprechung und Finanzverwaltung zur Tax Compliance	116
6.4 Interpretation des IKS durch den IDWPS 980	118
6.4.1 Compliance-Kultur	119
6.4.2 Compliance-Ziele	119
6.4.3 Compliance-Risikomanagement	121
6.4.4 Compliance-Programm	122
6.4.5 Compliance-Organisation	123
6.4.6 Compliance Kommunikation	123
6.4.7 Compliance-Überwachung	124
7 Bank- und Kapitalmarkt-Compliance	125
Axel-Dirk Blumenberg	
7.1 Grundlagen des Bank- und Kapitalmarktrechts	126
7.1.1 Einführung	126
7.1.2 Funktionsweise des Kapitalmarkts	127
7.1.3 Aufsichtsbehörde	128
7.2 Prävention und Detektion von Marktmissbrauch	129
7.2.1 Insiderhandel	129
7.2.2 Organisatorische Maßnahmen	130
7.2.3 Marktmanipulation	132
7.2.3.1 Das Verbot der Marktmanipulation	132
7.2.3.2 Safe Harbours	135
7.2.4 Anzeigepflichten	135
7.2.5 Reg-Tech	135
7.3 Ad-hoc-Publizität	136
7.4 Director's Dealings	137
7.5 Organisationspflichten nach § 80 Abs. 1 WpHG, Art. 22 DV und 26 Abs. 7 DV und 26 Abs. 7 DV	138
7.5.1 Stellung der Compliance	139
7.5.1.1 Unabhängigkeit	140
7.5.1.2 Dauerhaftigkeit der Compliance	140
7.5.2 Aufgaben der Compliance	141
7.5.2.1 Beratungs- und Unterstützungsfunction	141
7.5.2.2 Überwachung	141
7.5.2.3 Berichtspflichten	141
7.6 Organisationspflichten nach § 25a KWG	142
Literatur	143

Teil III Kontrollmechanismen – Compliance bei Ausübung von Compliance

8 Compliant Compliance – Ausgewählte Grenzen maximaler Kontrolle	147
Michael Schmidl	
8.1 Einleitung und aktuelle Entwicklung	149
8.1.1 Übererfüllung von Compliance-Bemühungen	149
8.1.2 Arbeitnehmer- und Dritte Rechte als Schranken	149
8.1.3 Eignung einer Maßnahme	152
8.2 E-Mail-Filterung im Lichte von §§ 206, 303 a StGB	152
8.2.1 Auswirkungen von § 206 StGB im Bereich der E-Mail-Filterung	152
8.2.1.1 Geschütztes Rechtsgut	152
8.2.1.2 Reichweite des Schutzes	153
8.2.1.3 Eingriff in den Normalverlauf der Telekommunikation	153
8.2.1.4 Taugliche Täter	154
8.2.1.5 E-Mail als taugliches Tatobjekt	155
8.2.1.6 Ausfiltern und Verzögern als Tathandlung	155
8.2.1.7 Zeitliche Grenze der Tatbestandsverwirklichung	156
8.2.1.8 Zur Übermittlung anvertraut	164
8.2.1.9 Rechtswidrigkeit	165
8.2.2 Regelungsgehalt und Auswirkungen von § 303 a StGB	165
8.2.3 Lösungsansätze	166
8.3 Whistleblowing im Lichte des Datenschutzrechts	167
8.3.1 Hinweisgeberschutzgesetz	167
8.3.1.1 Meldestellen	168
8.3.1.2 Vertraulichkeit	168
8.3.2 Zentrale Anforderungen des Datenschutzrechts	169
8.3.2.1 Schutzziel des Datenschutzrechts	169
8.3.2.2 Datenminimierung	170
8.3.2.3 Information der Betroffenen	170
8.3.2.4 Kein Konzernprivileg	172
8.3.2.5 Anforderungen an internationale Übermittlungen	173
8.3.3 Lösungsansätze	174
8.4 Screening von E-Mail und Internetverkehrsdaten	175
8.4.1 Screening von E-Mail	175
8.4.1.1 Interessenlage	175
8.4.1.2 Anwendung von § 206 StGB	176
8.4.1.3 Anwendung des Datenschutzrechts	177
8.4.2 Screening von Internetverkehrsdaten	178
8.4.2.1 Anwendbarkeit des TDDDG	178
8.4.2.2 Mögliche Erlaubnistratbestände	179

8.5	Totalüberwachung im Lichte von Art. 1 GG und sonstige Grenzen	180
8.5.1	Grenzen der Überwachung aus Art. 1 GG	180
8.5.1.1	Verbot der Totalüberwachung	180
8.5.1.2	Datenschutzrechtliche Absicherung	181
8.5.1.3	Bezugspunkt der Totalüberwachung	181
8.5.2	Auswirkungen auf typische Maßnahmen	182
8.5.2.1	Mitlesen von Bildschirmen	182
8.5.2.2	Einsatz von Keylogger-Software	182
8.5.2.3	Lückenlose Browser-Überwachung	182
8.5.3	Zusätzlicher Schutz bei Telefon- und Videoüberwachung	183
8.5.3.1	Schutz durch § 201 StGB	183
8.5.3.2	Schutz gemäß § 201 a StGB	184
8.6	Kontrollmaßnahmen im Lichte des IT-Grundrechts	186
8.6.1	Schutzbereich des IT-Grundrechts	186
8.6.1.1	Herleitung und Schutzbereich	186
8.6.1.2	Übertragbarkeit auf Verhältnisse am Arbeitsplatz	187
8.6.2	Auswirkungen auf Kontrollmaßnahmen	189
8.7	Sonstige Folgen unzulässiger Kontrollmaßnahmen	190
8.7.1	Beweisrechtliche Folgen	190
8.7.2	Reputationsverlust	193
8.7.3	Maßnahmen von Aufsichtsbehörden	193
8.7.4	Sonstige Ansprüche und Rechte der Betroffenen	193
8.7.5	Strafrechtliche und ordnungswidrigkeitenrechtliche Folgen	194
9	Hinweisgebersysteme als Bestandteil eines effektiven Compliance-Managements	195
	Carolin Püschel und Sascha Süße	
9.1	Begriffsdefinitionen	196
9.1.1	Whistleblowing	196
9.1.2	Hinweisgeber (Whistleblower)	198
9.1.3	Internes und externes Whistleblowing	198
9.1.4	Compliance-Management-Systeme und Hinweisgeberschutz	200
9.2	Rechtliche Grundlagen	201
9.2.1	Zu den Regelungen des Sarbanes-Oxley Act	202
9.2.2	Weitere internationale Regelungen	203
9.2.3	Europäische Rechtsprechung	204
9.2.4	Einzelgesetzliche Regelungen des Hinweisgeberschutzes in Deutschland	205
9.2.4.1	Zum Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)	206
9.2.4.2	Zum Lieferkettensorgfaltspflichtengesetz (LkSG)	207
9.2.5	(Gescheiterte) Vorhaben zur Etablierung eines gesetzlichen, flächendeckenden Hinweisgeberschutzes in Deutschland	208

9.2.6	Zur Hinweisgeberschutzrichtlinie der EU	210
9.2.6.1	Zum Ziel und Regelungsgehalt der Richtlinie	210
9.2.6.2	Zum Vertragsverletzungsverfahren der EU-Kommission gegen Deutschland	212
9.2.7	Das Hinweisgeberschutzgesetz	213
9.2.7.1	Ziel: Schutz von Hinweisgebern	214
9.2.7.2	Gesetzgebungsprozess	214
9.2.7.3	Systematik und Regelungsgehalt	215
9.2.7.3.1	Aufbau, Anwendungsbereich und vorgesehene Sanktionen	215
9.2.7.3.2	Verhältnis der internen und externe Meldestelle(n) nach dem HinSchG	217
9.3	Einführung eines Hinweisgeberschutzgesetzes im Unternehmen	218
9.3.1	Gründe für die Einführung eines Hinweisgebersystems	218
9.3.2	Arten von Hinweisgebersystemen	219
9.3.2.1	Telefon-Hotline	219
9.3.2.2	Internetbasiertes Hinweisgebersystem	219
9.3.2.3	Ombudsmann/-frau bzw. Vertrauensanwalt/-anwältin ..	220
9.3.3	Anforderungen des HinSchG an die interne Meldestelle	221
9.3.3.1	Pflicht zur Einrichtung einer internen Meldestelle	221
9.3.3.2	Organisation und Aufgaben der internen Meldestelle ..	222
9.3.3.3	Einrichtung von Meldekanälen	224
9.3.3.4	Verfahren bei internen Meldungen und Folgemaßnahmen	225
9.3.4	Implementierung der internen Meldestelle im Unternehmen	225
9.3.4.1	Besetzung und Auswahl der Meldestelle	225
9.3.4.2	Meldestellen im Konzern	226
9.3.4.3	Auswahl der Meldekanäle	228
9.3.4.4	Abwägung der Vor- und Nachteile der verschiedenen Meldekanäle	228
9.3.4.5	Konkrete Auswahl	231
9.3.4.6	Interne Richtlinien und Kommunikation	232
9.3.4.7	Kommunikation und Integration	232
9.4	Rechtliche Einzelfragen	233
9.4.1	Arbeitsrechtliche Fragestellungen	233
9.4.2	Datenschutzrechtliche Fragestellungen	234
9.4.2.1	Grundsätzliches	235
9.4.2.2	Pflicht zur Benennung eines Datenschutzbeauftragten ..	236
9.4.3	Strafrechtliche Fragestellungen	237
9.5	Zusammenfassung	239
	Literatur	240

Teil IV Compliance in der Unternehmensentwicklung

10 Organisationspsychologische Aspekte der Compliance	247
Silja Kennecke	
10.1 Einführung	248
10.1.1 Der Compliance-Begriff in der Psychologie und verwandten Disziplinen	249
10.1.2 Non-Compliance im Organisationskontext	249
10.2 Gründe für Non-Compliance	252
10.2.1 Allgemeine Erklärungsmodelle für organisationales Fehlverhalten	252
10.2.1.1 Die Theorie der rationalen Entscheidung	252
10.2.1.2 Lerntheorien	253
10.2.1.3 Die Theorie des geplanten Verhaltens	253
10.2.1.4 Die Theorie der kognitiven Dissonanz	254
10.2.1.5 Das Reziprozitätsprinzip	254
10.2.2 Bedingungen auf Personenebene	255
10.2.2.1 Negative Affektivität und Attributionsstil	255
10.2.2.2 Integrität, Gewissenhaftigkeit, Verträglichkeit und emotionale Stabilität	256
10.2.2.3 Dunkle Triade: Narzissmus, Psychopathie und Machiavellismus	256
10.2.2.4 Selbstwertgefühl und Vertrauen in eigene Fähigkeiten	257
10.2.2.5 Selbstkontrolle	257
10.2.2.6 Moralbewusstsein	258
10.2.2.7 Loyalität und Angst vor Exklusion	258
10.2.3 Persönliche Umstände	258
10.2.3.1 Arbeitsbedingungen	258
10.2.3.2 Wettbewerbsdruck, überhöhte Zielvorgaben und Orientierung an kurzfristigen Erfolgsparametern ..	259
10.2.3.3 Probleme im Kontrollsysteem	259
10.2.3.4 Führung und Unternehmenskultur	260
10.2.4 Spezifische Erklärungsmodelle für organisationales Fehlverhalten	261
10.2.4.1 Modell der kausalen Schlussfolgerung	261
10.2.4.2 Stressor-Emotion Modell	261
10.2.4.3 Motivationales Rahmenmodell	262
10.3 Bedingungen für regelkonformes Verhalten	263
10.3.1 Gruppendruck	263
10.3.2 Schutzmotivation	264
10.3.3 Verantwortlichkeit	265

10.3.4	Maßnahmen zur Förderung von Compliance	267
10.3.4.1	Personenbezogene Maßnahmen	267
10.3.4.1.1	Personalmarketing	267
10.3.4.1.2	Personalauswahl	268
10.3.4.1.3	Personalentwicklung	269
10.3.4.2	Umfeldbezogene Maßnahmen	270
10.3.4.2.1	Compliance-Management-Systeme (CMS)	270
10.3.4.2.2	Entwicklung einer Integritätskultur	272
10.3.5	„Unternehmen brauchen einen Kompass, kein Navigationssystem“	274
	Literatur	276
11	Arbeitsrechtliche Implementierung von Compliance in Unternehmen	281
	Andreas Katzer	
11.1	Grundlagen	282
11.1.1	Arbeitsrecht und Compliance	282
11.1.2	Pflichten von Arbeitgebern	283
11.1.3	Compliance-Management-System (CMS)	284
11.2	Implementierung	285
11.2.1	Compliance-Pflichten als arbeitsvertragliche Nebenpflichten	285
11.2.2	Gestaltungsinstrumente	286
11.2.2.1	Direktionsrecht	286
11.2.2.1.1	Inhalt und Umfang des Direktionsrechts	286
11.2.2.1.2	Rechtliche Anforderungen	286
11.2.2.1.3	Vor- und Nachteile	287
11.2.2.2	Arbeitsvertrag	287
11.2.2.2.1	Rechtliche Anforderungen	287
11.2.2.2.2	Vor- und Nachteile	288
11.2.2.2.3	Änderungskündigung	289
11.2.2.3	Betriebsvereinbarung	289
11.2.2.3.1	Allgemeines	289
11.2.2.3.2	Vor- und Nachteile	290
11.2.2.4	Regelungsabrede und Tarifvertrag	291
11.2.2.5	Unternehmensstrategie	292
11.2.3	Mitbestimmung des Betriebsrats bei der Implementierung	293
11.2.4	Dokumentation und Kommunikation	294
11.3	Allgemeines Gleichbehandlungsgesetz (AGG)	295
11.3.1	Grundsätze	295
11.3.2	Pflichten von Arbeitgebern	297
11.3.3	Rechte von Arbeitnehmern	297

11.4	Überwachung und Sanktionierung	298
11.4.1	Allgemeines	298
11.4.2	Überwachung des Arbeitnehmers durch den Arbeitnehmer	298
11.4.3	Interne Ermittlungen im Verdachtsfall	299
11.4.4	Whistleblowing	300
11.4.5	Compliance-Beauftragter	300
11.4.6	Maßnahmen bei Verstößen von Arbeitnehmern und Arbeitgebern	301
11.4.7	Verwertung vor Gericht	302
11.5	Exkurs: Gesetz zum Schutz von Geschäftsgeheimnissen	302
11.6	Mitarbeiterdatenschutz	304
11.6.1	Grundsätze	304
11.6.2	Erlaubte Datenverarbeitungen im Arbeitsverhältnis	305
11.6.2.1	Erfüllung eines Vertrags, Art. 6 Abs. 1 lit. b DSGVO	305
11.6.2.2	Wahrung berechtigter Interessen, Art. 6 Abs. 1 lit. f DSGVO	305
11.6.2.3	Aufdeckung von Straftaten, § 26 Abs. 1 S. 2 BDSG	306
11.6.2.4	Einwilligung als Rechtsgrundlage für Datenverarbeitungen regelmäßig untauglich	307
11.6.2.5	Kollektivvereinbarungen, § 26 Abs. 4 BDSG	307
11.6.2.6	Zweckänderung	307
11.6.2.7	Umgang mit besonderen Kategorien personenbezogener Daten	308
11.6.2.8	Pflichten von Arbeitgebern vor und bei der Durchführung von Überwachungsmaßnahmen	309
11.6.3	Rechte und Pflichten des Betriebsrats	310
11.6.4	Besondere Fallkonstellation: Datenschutz im Home-Office	311
11.6.5	Haftung und Sanktionen bei Verstößen	312
Literatur	313	
12	Compliance, Kundenschutz und Product Governance	315
	Daniel Sandmann	
12.1	Einleitung	315
12.2	Fallbeispiele und Unternehmens(fehl)entwicklung	317
12.2.1	Kreditversicherungen in Großbritannien	318
12.2.2	T-Mobile US – rural calls – Falsche Klingeltöne in den U.S.A.	320
12.3	Unternehmensentwicklung	321
12.3.1	Von der rechtsgebietsbezogenen Compliance zur prozessbezogenen Compliance	323

12.3.2	Kundenschutz und Produkt-Compliance in Abgrenzung zu Qualitätssicherung und Produkthaftung	323
12.3.3	Erkenntnisquellen, Risikobewertung und Unternehmenssteuerung	324
12.4	Produkt-Compliance – Prozesse am Beispiel Finanzindustrie	326
12.5	Fazit und Ausblick	327
	Literatur	327
Teil V Compliance als Bestandteil der Unternehmenskultur		
13	Compliance als Führungsaufgabe – Ethische Verantwortung im Bereich Compliance	331
	Thomas Schwartz, Nikolaus Seitz und Twain Stolz	
13.1	Ethische Aspekte des Compliance-Managements	331
13.2	Compliance als moderne Managementaufgabe?	332
13.2.1	Good Governance und der Begriff der „Compliance“	332
13.2.2	Rolle und Selbstverständnis des Compliance Officers aus ethischer Sicht	335
13.2.3	Die fachliche Expertise des Compliance Officers in ethischer Perspektive	336
13.3	Compliance als Führungsaufgabe	338
13.4	Compliance-Management als Wertemanagement	340
13.5	Ausblick und Herausforderungen	342
	Literatur	343
14	Compliance als Führungsaufgabe	347
	Gerald Marimón	
14.1	Prolog zur Compliance	348
14.2	Eine Arbeitsplatzbeschreibung	349
14.2.1	Ist Compliance Ihre Aufgabe?	349
14.2.2	Einer für alle oder alle für einen?	350
14.2.3	Compliance-Kommunikation	351
14.3	Typen, Ziele, Abenteuer	353
14.3.1	Haben Sie Ziele?	353
14.3.2	Karriere mit Compliance	355
14.3.3	Eine Typenschule	355
14.4	Ein Haus der Compliance bauen	357
14.4.1	Statik und Mechanik	357
14.4.2	Negative Zonen und Blind Spots	358
14.4.3	Sensoren und Aktoren – Die Haustechnik	360

14.5 Compliance wird bei uns gemanagt	362
14.5.1 Die vier Gebote der Compliance	362
14.5.2 Wertbeitrag der Compliance	363
Literatur	364
Autorin des Stichwortverzeichnisses	367
Stichwortverzeichnis.....	369

Über die Herausgeber



Prof. Dr. Christoph Becker Professor Dr. iur. utr. Christoph Becker, geboren 1960 in Düsseldorf, aufgewachsen in Neuss. Abitur am Quirinus-Gymnasium Neuss, darauf Grundwehrdienst und anschließend Studium der Rechtswissenschaft an der Universität zu Köln. Nach dessen Abschluß Graduiertenstipendium des Landes Nordrhein-Westfalen (Betreuer: Professor Dr. iur. Heinz Hübner, Köln) und Juristischer Vorbereitungsdienst im Bezirk des Landgerichts Köln. Während des Vorbereitungsdienstes Beginn langjähriger Lehrtätigkeit in der berufsbegleitenden Weiterbildung (Verwaltungs- und Wirtschafts-Akademie Köln, später Verwaltungs- und Wirtschafts-Akademie Schwaben sowie Kulturbüro Rheinland-Pfalz). Nach dem Assessorexamen wissenschaftlicher Mitarbeiter an der Universität zu Köln und Habilitation dort (Betreuer: Professor Dr. iur. Klaus Luig). Auf Lehrstuhlvertretungen an der Johann-Wolfgang-Goethe-Universität Frankfurt am Main und an der Universität zu Köln folgte im Jahre 1999 Ernennung auf den Lehrstuhl für Bürgerliches Recht und Zivilverfahrensrecht, Römisches Recht und Europäische Rechtsgeschichte der Universität Augsburg. Dekan der Juristischen Fakultät der Universität Augsburg 2007–2009. Mitglied des Leitungsgremiums des Zentrums für Weiterbildung und Wissenstransfer der Universität Augsburg.



Carina Metscher Rechtsanwältin Carina Metscher, geboren 1984 in Augsburg. Studium der Rechtswissenschaften und Referendariat in Augsburg. Nach dem Assessorexamen Tätigkeit als Rechtsanwältin einer mittelständischen Anwaltskanzlei in Augsburg. Seit 2016 Produktmanagerin der Juristischen Weiterbildung am Zentrum für Weiterbildung und Wissenstransfer der Universität Augsburg.



Hanspeter Vietz Diplom-Kaufmann und MBA, geboren 1963 in Pfronten/Allgäu. Abitur in Wiesbaden und Studium der Wirtschaftswissenschaften an der Universität Augsburg. Berufliche Engagements im Bereich Marketing, Strategie und Unternehmensführung. Experte für Gesprächs- und Verhandlungsführung. Konzeption und Aufbau des berufsbegleitenden MBA-Studiengangs „Unternehmensführung“ an der Universität Augsburg; Vorstandsmitglied des MBAalumni e.V.; Mitglied des Sprecherrats der DGWF-Bayern (Deutsche Gesellschaft für Weiterbildung und Fernstudien). Preisträger der Kurt und Felicitas Viermetz Stiftung. Ab 2010 stellvertretender Geschäftsführer des ZWW und seit 2019 Geschäftsführer des ZWW und Mitglied des Leitungsgremiums des ZWW (Zentrum für Weiterbildung und Wissenstransfer).

Abkürzungsverzeichnis

a. o.	außerordentlich
aaO.	am angegebenen Ort
Abb.	Abbildung
Abs.	Absatz
ACA-HSG	Institut für Accounting, Controlling und Auditing – Hochschule St. Gallen
ACFE	Association of Certified Fraud Examiner
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Aktiengesellschaft, Amtsgericht, Arbeitgeber, Ausführungsgesetz
AG	Die Aktiengesellschaft (Fachzeitschrift)
AGB	Allgemeine Geschäftsbedingungen
AGG	Allgemeines Gleichbehandlungsgesetz
AHB	Allgemeine Versicherungsbedingungen für die Haftpflichtversicherung
AI	Artificial Intelligence
AktG	Aktiengesetz
Anm.	Anmerkung
AO	Abgabenordnung
ArbGG	Arbeitsgerichtsgesetz
Art	Artikel
AT	Allgemeiner Teil
AT MaRisk	Modul Allgemeiner Teil – Mindestanforderungen an das Risikomanagement
AVB-AVG	Allgemeine Versicherungsbedingungen – Angestelltenversicherungsgesetz
Az.	Aktenzeichen
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAG	Bundesarbeitsgericht
BB	Betriebs-Berater (Zeitschrift für Recht, Steuern und Wirtschaft)
BB	Bundesbank

BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGHSt	Entscheidungssammlung des Bundesgerichtshof in Strafsachen
BIImSchG	Bundes-Immissionsschutzgesetz
BKR	Zeitschrift für Bank- und Kapitalmarktrecht
BörsG	Börsengesetz
BRAO	Bundesrechtsanwaltsordnung
bspw.	beispielsweise
BT	Bundestag
BT-Drs.	Bundestagsdrucksache
BTO	Besonderer Teil Organisation (zu MaRisk)
BTR	Besonderer Teil Risiken (zu MaRisk)
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
CCZ	Corporate Compliance Zeitschrift
CEBS	Committee of European Banking Supervisors
CESR	Committee of European Securities Regulators (Ausschuss der Europäischen Aufsichtsbehörden für das Wertpapierwesen)
COSO	Committee of Sponsoring Organizations
CSDDD	Corporate Sustainability Due Diligence Directive
CSR	Corporate Social Responsibility
CSRD	Corporate Sustainability Reporting Directive
d. h.	das heißt
DB	Der Betrieb (Zeitschrift)
DCGK	Deutsche Corporate Governance Kodex
DIHK	Deutsche Industrie- und Handelskammer
DStR	Deutsches Steuerrecht
DuD	Datenschutz und Datensicherung
EBA	Europäische Bankenaufsichtsbehörde
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EGMR	Europäischer Menschenrechtsgerichtshof
EMRK	Europäische Menschenrechtskonvention
ESG	Environmental, Social and Corporate Governance
ESMA	European Securities and Markets Authority (Europäische Wertpapier- und Marktaufsichtsbehörde)
ESRS	European Sustainability Reporting Standards
EStG	Einkommensteuergesetz
EU	Europäische Union

EU-BestG	Europäisches Bestechungsgesetz
EU-DSGVO	Europäische Datenschutz-Grundverordnung
EuGH	Europäischer Gerichtshof
f.	folgend
FCPA	Foreign Corrupt Practices Act
ff.	folgende
FIU	Financial Intelligence Unit
GDV	Gesamtverbands der Deutschen Versicherungswirtschaft
GenG	Genossenschaftsgesetz
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
GewO	Gewerbeordnung
GG	Grundgesetz
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	Gesetz über die GmbH
GRECO	Group of States against corruption (Groupe d'Etats contre la Corruption)
GRI	Global Reporting Initiative
GWB	Gesetz gegen Wettbewerbsbeschränkungen
GwG	Geldwäschegesetz (Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten)
HdB	Handbuch
HinwGebSchG	Hinweisgeberschutzgesetz
i. S. d.	im Sinne des
i. S.	im Sinne
ICAEW	Institute of Chartered Accountants in England and Wales
ICC	International Chamber of Commerce
ICSA	Institute of Chartered Secretaries and Administrators
IDW PS	Institut der Wirtschaftsprüfer Prüfungsstandards
IIA	Institute of Internal Auditors
IKS	Internes Kontrollsyste
InsO	Insolvenzordnung
IntBestG	Gesetz zur Bekämpfung internationaler Bestechung
ISAE	International Standard on Assurance Engagements
ISO	International Organization for Standardization
ISSA	International Standard on Sustainability Assurance
IT	Informationstechnik
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KPMG	Klynveld, Peat, Marwick, Goerdeler
KSchG	Kündigungsschutzgesetz
KSzW	Kölner Schrift zum Wirtschaftsrecht
KWG	Kreditwesengesetz
KYC	Know Your Customer

LAG	Landesarbeitsgericht
lit.	Litera
LkSG	Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten
LLP	Limited Liability Partnership
M&A	Merger & Acquisitions
MaComp	Mindestanforderungen an die Compliance
MaKonV	Marktmanipulations-Konkretisierungsverordnung
MaRisk	Mindestanforderungen an das Risikomanagement
MdEP	Mitglied des Europäischen Parlaments
MiFID	Markets in Financial Instruments Directive, deutsch: Richtlinie über Märkte für Finanzinstrumente
MMR	Multimedia und Recht
mwN. oder m. w. N.	mit weiteren Nachweisen
NFRD	Non-Financial Disclosure Directive
NGOs	Non Governance Organizations
NJW	Neue juristische Wochenschrift (Zeitschrift)
NSiZ	Neue Zeitschrift für Strafrecht
NZWiSt	Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht
o. g.	oben genannt
o.r.	oben rechts
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OLG	Oberlandesgericht
OWiG	Ordnungswidrigkeitengesetz
RIW	Recht der internationalen Wirtschaft (Zeitschrift)
Rn.	Randnummer
S.	Seite
s. o.	siehe oben
SchVG	Schuldverschreibungsgesetz
SEC	United States Securities and Exchange Commission
SFDR	Sustainable Finance Disclosure Regulation
SK-StGB	Systematischer Kommentar zum Strafgesetzbuch
sog.	sogenannt
SOX	Sarbanes-Oxley Act
st. Rspr.	ständige Rechtsprechung
StBerG	Steuerberatungsgesetz
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
Str.	Aktenzeichen für Revision in Strafsachen am Bundesgerichtshof
StV	Strafverteidiger (Zeitschrift)

TKG	Telekommunikationsgesetz
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
TVG	Tarifvertragsgesetz
u. a.	unter anderem; und andere
U.S.C.	United States Code
USSG	U.S. Sentencing Guidelines
VAG	Versicherungsaufsichtsgesetz
vgl.	vergleiche
VO	Verordnung
VOB/A	Verdingungsordnung für Bauleistungen/Teil A
VOL/A	Vergabe- und Vertragsordnung für Leistungen (VOL) – Teil A – Allgemeine Bestimmungen für die Vergabe von Leistungen
VStGB	Völkerstrafgesetzbuch
VVG	Versicherungsvertragsgesetz
wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht
WM	Wertpapier-Mitteilungen (Zeitschrift für Wirtschafts- und Bankrecht)
WpAIV	Wertpapierhandelsanzeige- und Insiderverzeichnisverordnung
WpDVerOV	Verordnung zur Konkretisierung der Verhaltensregeln und Organisationsanforderungen für Wertpapierdienstleistungsunternehmen
WpHG	Wertpapierhandelsgesetz
WpPG	Wertpapierprospektgesetz
WRP	Wettbewerb in Recht und Praxis
WuW	Wirtschaft und Wettbewerb (Zeitschrift für Deutsches und Europäisches Wettbewerbsrecht)
z. B.	zum Beispiel
ZCG	Zeitschrift für Corporate Governance
Ziff.	Ziffer
ZIP	Zeitschrift für Wirtschaftsrecht
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
ZJS	Zeitschrift für das Juristische Studium
ZPO	Civilprozessordnung
ZRP	Zeitschrift für Rechtspolitik
ZWeR	Zeitschrift für Wettbewerbsrecht
ZWW	Zentrum für Weiterbildung und Wissenstransfer

Abbildungsverzeichnis

Abb. 1.1	Risiken von Compliance-Verstößen	6
Abb. 1.2	Strukturmodell des Compliance Officer (Univ.) am ZWW der Universität Augsburg	13
Abb. 1.3	Wertschöpfung durch Compliance	14
Abb. 2.1	European Sustainability Reporting Standards	23
Abb. 2.2	COSO-Rahmenkonzept	29
Abb. 2.3	Prinzipienorientierung 2013	30
Abb. 2.4	Das IIA Drei-Linien-Modell	32
Abb. 3.1	Entwicklung der Verfahrenszahlen 2018–2022 (Bundeskriminalamt Bundeslagebild Korruption 2022, 4)	43
Abb. 4.1	Elemente eines kartellrechtlichen Compliance-Programms	88
Abb. 10.1	Begriffsbestimmung: Compliance und Non-Compliance	250
Abb. 10.2	Eine Typologie kontraproduktiven Arbeitsverhaltens. (Nach Robinson & Bennett, 1995; © Adademy of Management (NY) 1995)	251
Abb. 10.3	Bedingungen für Non-Compliance	255
Abb. 10.4	Integratives Rahmenmodell zur Erklärung organisationalen Fehlverhaltens. (In Anlehnung an Vardi & Wiener, (1996); © Institute for Operations Research and the Management Sciences, (1996))	263
Abb. 10.5	Dreiecksmodell der Verantwortung. (In Anlehnung an Schlenker, Britt, Pennington, Murphy & Doherty, (1994); © American Psychological Association, Inc., (1994))	265
Abb. 10.6	Typische Elemente im Aufbau eines Compliance-Systems	271
Abb. 10.7	Markenzeichen einer effektiven Integritätsstrategie nach Paine (1994)	272

Abb. 10.8	Die Performance-Value Matrix nach Jack Welch	273
Abb. 10.9	Das Konzept ethikorientierter Führung nach Frey, Streicher & Aydin (2012)	275
Abb. 14.1	Modell „Einer für alle“	351
Abb. 14.2	Servant Leadership Ansatz für die Compliance	361

Tabellenverzeichnis

Tab. 3.1	Geldbußen wegen Korruptionsdelikten in Deutschland	43
Tab. 3.2	Geberseite vs. Nehmerseite	45
Tab. 3.3	Auslandsbestechung	45
Tab. 4.1	Geldbußen	81

Teil I

Compliance als mehrdimensionales Anforderungssystem



Compliance als interdisziplinäre Herausforderung – Das Augsburger Qualifizierungsmodell

Carina Metscher und Hanspeter Vietz

Inhaltsverzeichnis

Literatur	15
-----------------	----

Zehn Jahre nach Erscheinen der Erstauflage des vorliegenden Begleitbandes zum Augsburger Zertifikatsstudium zum „Compliance Officer (Univ.)“ lässt sich Compliance aus der Unternehmenswelt nicht mehr wegdenken. Im Kontext verstärkter regulatorischer Entwicklungen, zunehmender Beschleunigung technologischer Neuerungen und einem gesteigerten Bewusstsein ethisch-sozialer Verantwortung, ist Compliance in Unternehmen und Organisationen fest verankert. Einhergehend mit dem Bedeutungszuwachs, auch als Managementkomponente und unternehmerischer Erfolgsfaktor, erfährt der Berufsstand eine stetige Professionalisierung.

Für den Compliance-Begriff haben sich unterschiedliche Definitionen mit verschiedenen Schwerpunkten herausgebildet.

Im Allgemeinen wird Compliance verstanden als Handeln in Übereinstimmung mit allen anwendbaren bzw. anzuwendenden Regeln. Folgt man dieser Definition, besitzt die Thematik Compliance als Untersuchungsgegenstand vor allem zwei Dimensionen: Zum einen umfasst sie die Summe der organisatorischen Maßnahmen im Unternehmen, die

In Fortführung des Beitrages von Herrn Dr. Sebastian Bachmann und Simon Fechner, Erstauflage des vorliegenden Bandes.

C. Metscher (✉) · H. Vietz

Zentrum für Weiterbildung und Wissenstransfer (ZWW), Universität Augsburg,
Augsburg, Deutschland

E-Mail: carina.metscher@zww.uni-augsburg.de; hanspeter.vietz@zww.uni-augsburg.de

gewährleisten, dass sich Organe und Mitarbeiter des Unternehmens rechtmäßig verhalten (auch Corporate Compliance).¹ Zum anderen schließt der Begriff Compliance aber auch die Perspektive auf das individuelle gesetzestreue Verhalten ein. Im Folgenden wird Compliance somit zielorientiert und konturenstärker als institutionalisierte und intuitive Normloyalität im Unternehmen begriffen.

Der Fokus liegt im Weiteren dabei vor allem auf der Entwicklung des Themas in Wissenschaft und Praxis und der daraus resultierenden qualifikatorischen, aber auch praxisrelevanten Aufgaben.

Von Compliance als neuer Herausforderung – so 2014 noch bei Erscheinen in der Erstauflage beschrieben – kann aufgrund der weiteren Entwicklungen kaum mehr gesprochen werden. Vielmehr hat sich Compliance nicht nur als eigenständige Unternehmensaufgabe, sondern als strategische Komponente zur Sicherung eines nachhaltigen Unternehmenserfolges etabliert. Dieser Prozess wurde sowohl von betriebswirtschaftlichen als auch von juristischen Einflüssen getrieben. Befeuert wurde die grundsätzlich kontinuierliche Entwicklung durch einzelne besonders öffentlichkeitswirksame Fälle.

Die ersten Ansätze von Compliance-Programmen, wie wir sie heute kennen, zeigten sich bereits in den 1950er-Jahren in US-amerikanischen Unternehmen. Ihre Einführung folgte damals keiner unmittelbaren rechtlichen Pflicht, sondern der betriebswirtschaftlichen Idee, sich als integres Unternehmen zu positionieren.²

In den 1960er-Jahren folgten umfangreichere und ausgereiftere Compliance-Programme, sowie erste wissenschaftliche Abhandlungen. Zu diesem Zeitpunkt stand vorwiegend das Kartellrecht im Zentrum der Betrachtungen.³ Auch wenn sich in der Folge noch keine dynamische Ausbreitung des Themas Compliance identifizieren lässt, so gab es doch entscheidende Entwicklungen in den Risikobereichen. Besonders hervorzuheben sind hierbei die zahlreichen Verfahren der amerikanischen Börsenaufsicht SEC Anfang und Mitte der 1970er-Jahre und das Inkrafttreten des FCPA (1977), der neben einer Erweiterung der Korruptionsverbote auch die Begründung von Transparencystrukturen vorsah.⁴ Der Gedanke einer expliziten Compliance-Organisation wurde anschließend vor allem durch das Bankrecht aufgegriffen.⁵ Die erste branchenübergreifende Kodifikation fand sich in den U.S. Sentencing Guidelines (USSG) von 1991, einer Art Richtlinie zur Strafbemessung, die eine Strafreduktion für Unternehmen vorsahen, wenn ein effektives Programm zur Vermeidung und Aufdeckung von Rechtsverstößen eingerichtet war.⁶ Die Definition eines solchen Programms war bereits relativ breit und interdisziplinär angelegt.⁷

¹ Hauschka/Moosmayer/Lösler (2016), S. 5, Vetter (2009), S. 33.

² Jäger/Rödl/Campos Nave (2009), S. 33.

³ Eufinger (2012), S. 22, m. w. N.

⁴ Bartz/Weidig (2020), S. 359 ff.

⁵ Lösler (2003), S. 119 f.

⁶ U.S.S.G. § 8C2.5(f).

⁷ U.S.S.G. § 8A1.2, comment. (n. 3(k)).

Die Thematik Compliance fand über das Bank- und Kapitalmarktrecht schließlich auch den Weg nach Europa.⁸ Grundlegende rechtliche Voraussetzungen lagen mit § 30, 130 OWiG zwar schon vor,⁹ durch das KonTraG¹⁰ von 1998, beziehungsweise den neu eingeführten § 91 Abs. 2 AktG wurden die Vertreter der Aktiengesellschaften jedoch erstmals zur Einrichtung von Maßnahmen des Risikomanagements und somit – zumindest indirekt – zu ersten Schritten in Richtung eines Compliance-Programms verpflichtet.¹¹ Eine regelrechte Dynamik nahm die Thematik dann auf beiden Seiten des Atlantiks durch die großen Rechnungslegungsskandale von Enron¹² und Worldcom¹³ kurz nach der Jahrtausendwende auf. Mit einem Schlag war die Frage der verantwortungsvollen Unternehmensführung omnipräsent. Schlagwörter wie Corporate Governance,¹⁴ Corporate Social Responsibility, Wertemanagement und Wirtschaftsethik wurden auch außerhalb der Fachöffentlichkeit kontrovers diskutiert. Im US-amerikanischen Recht wurde mit dem SOX¹⁵ eine unmittelbare Verpflichtung für börsennotierte Unternehmen geschaffen, Elemente eines Compliance-Programms einzuführen, etwa einen Code of Ethics zu formulieren oder eine Whistleblower-Hotline einzurichten.¹⁶ Etwa gleichzeitig wurde in Deutschland der Deutsche Corporate Governance Kodex (DCGK) veröffentlicht, der über § 161 Abs. 1 AktG den Weg in das positive Recht findet. Der DCGK ist sowohl wegen seines Charakters als „Soft-Law“, als auch wegen seines Regelungsgehalts ein Novum im deutschen Recht. Auch wenn der Begriff Compliance erst 2007 eingefügt wurde,¹⁷ so war bereits zu Beginn die Pflicht des Vorstandes enthalten, für die Gesetzestreue in seinem Unternehmen zu sorgen.¹⁸ In Aktiengesellschaften war das Thema Compliance somit angekommen.

Die Wissenschaft nahm sich ebenfalls verstärkt dem Thema an, was sich auch in steigenden Veröffentlichungszahlen zum Thema Compliance in den folgenden Jahren zeigte¹⁹ – weiterhin allerdings mit dem Kartellrecht als inhaltlichem und der Bank- und Versicherungswirtschaft als Branchenschwerpunkt.²⁰ Im Jahr 2006 wurde mit der Siemens-

⁸ Fleischer (2004), (1129, 1131); Hauschka (2006), S. 258; Eisele (1993).

⁹ Rogall (2006), Rn. 22; Rogall (2006), Rn. 7.

¹⁰ Gesetz zur Kontrolle und Transparenz im Unternehmensbereich von 27.4.1998 (BGBl. I, S. 786).

¹¹ Obermayr (2010), Rn. 7 f.

¹² Vgl. Powers, JR./Troubh/Winokur, JR. (2002).

¹³ Vgl. Tanski (2002).

¹⁴ Hauschka/Moosmayer/Lösler (2016), Rn. 1 ff.

¹⁵ Sarbanes-Oxley Act vom 30.7.2002.

¹⁶ Sec. 406, 806 SOX; Grummer/Seeburg (2010); Block (2003).

¹⁷ Zusammen mit der Erweiterung der Vorstandspflichten auch auf die Einhaltung der unternehmensinternen Richtlinien hinzuwirken, 4.1.3 DCGK 2007 (Änderung vom 14.7.2007).

¹⁸ 4.1.3 DCGK (2002).

¹⁹ Siehe bspw. Schneider (2003); Scherp (2003); Fleischer (2003); Hauschka (2004a); Hauschka (2004b); Bürkle (2004b).

²⁰ Siehe bspw. Lamper (2002); Dreher (2004); Hauschka (2004c); Bürkle (2004a); Lösler (2003); Lösler (2005).

Korruptionsaffäre der wohl öffentlichkeitswirksamste Korruptionsskandal in Deutschland aufgedeckt.²¹ Dies lag zum einen an der erschreckend tiefen Verwurzelung von illegalen Handlungen in etablierten Unternehmensprozessen und zum anderen daran, dass hochrangige Manager, auch durch ihr eigenes Unternehmen, zur Verantwortung gezogen wurden. Der Imageschaden für Siemens war immens, wenn auch nicht existenzgefährdend. Es zeigte sich aber, dass die Gefahr eines Reputationsverlustes ein dominierender Treiber für die Einführung von Compliance-Programmen sein kann. Noch mehr als im Mischkonzern Siemens gilt dies für die Sektoren, in denen Vertrauen eine besondere Rolle spielt, wie in der Finanzmarktbranche. Für diese wurde daher in unmittelbarem zeitlichem Zusammenhang zum Siemens-Fall durch den europäischen Gesetzgeber eine erste direkte Pflicht zur Implementierung von Compliance-Programmen begründet. Mit der Umsetzung der europäischen Finanzmarktrichtlinie MiFID²² wurde im Wertpapierhandelsgesetz die Einführung einer unabhängigen Compliance-Funktion vorgeschrieben (Abb. 1.1).²³



Abb. 1.1 Risiken von Compliance-Verstößen

²¹ Eine Chronologie des Siemens-Korruptionsskandals findet sich unter: <https://www.br.de/nachricht/spezial/zeitstrahl-siemens-skandale100.html> (aufgerufen am 29.1.2024).

²² Umsetzung der Markets in Financial Instruments Directive vom 21.4.2004 (MiFID), RL 2004/39/EG, ABl. EU L 145/1, durch das deutsche Gesetz zur Umsetzung der Richtlinie über Märkte für Finanzinstrumente und der Durchführungsrichtlinie der Kommission vom 16.7.2007 (FRUG), BGBl. I S. 1330.

²³ § 33 I 1 Nr. 1 WpHG, sowie § 25a KWG für das Risikomanagement.

Compliance war nun das wirtschaftsrechtliche Thema Nummer eins.²⁴ In der Folgezeit diffundierte das Thema ausgehend von seinen Kernbereichen immer weiter in alle betrieblichen und rechtlichen Bereiche. Es entstanden neue Fachmedien und wissenschaftliche Gesamtdarstellungen.²⁵ Mit den MaComp,²⁶ einer norminterpretierenden Verwaltungsvorschrift, wurden im Jahr 2010 neue Anforderungen an eine Compliance-Organisation formuliert, die für den Finanzsektor einen hohen Bindungsgrad aufweisen. Noch im selben Jahr wurde von Wirtschaftsprüferseite erstmals der Entwurf eines Prüfungsstandards veröffentlicht, der in Form von sieben Grundelementen ein effektives Compliance-Management-System beschreibt.²⁷ Der IDW PS 980 hat sich im Laufe der Jahre zum vorherrschenden Standard zur Strukturierung und Prüfung von CMS entwickelt.²⁸ Mittlerweile aufgrund der geänderten Rahmenbedingungen und gestiegenen Anforderungen umfassend überarbeitet, enthält der IDW PS 980 n. F. insbesondere Fortentwicklungen bei Errichtung eines CMS und die zwischenzeitliche Rechtsprechung im Bereich Compliance.²⁹ Weitere Standards haben im Folgenden die Einrichtung von Compliance-Management-Systemen aufgegriffen, etwa die 2014 von der International Organization for Standardization (ISO) veröffentlichte ISO 19600,³⁰ später abgelöst von der ISO 37001 mit klaren Leitlinien und Praxisempfehlungen.³¹

Gesetzliche Regelungen wiederum finden sich für die Compliance gegenwärtig insbesondere im Zusammenhang mit Organisationspflichten im Finanzwesen: Die Verpflichtung etwa zur Errichtung eines internen Kontrollsystems (IKS) für Kredit- und Finanzdienstleistungsinstitute findet sich in § 25a Abs. 1 KWG.³² Von zentraler Bedeutung darüber hinaus sind die EU-Geldwäscherichtlinien und das Geldwäschegegesetz im Hinblick auf die Prüfung von Geschäftspartnern.³³

²⁴ Dieners/Besen (2010), Kap. 7 Rn. 1 m. w. N.

²⁵ Bspw. die Zeitschriften Compliance-Berater (2012), die Corporate Compliance Zeitschrift (CCZ); Corporate Compliance (2010).

²⁶ BaFin Rundschreiben 4/2010 (WA) – Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 31 ff. WpHG für Wertpapierdienstleistungsunternehmen (MaComp).

²⁷ IDW PS 980 vom 11.3.2013.

²⁸ Schulz (2016), S. 230.

²⁹ Zur Überarbeitung des IDW PS 980n. F. (9.2022) durch den Hauptfachausschuss (HFA) des IW: <https://www.idw.de/idw/aktuell/idw-ps-980-n-f-09-2022-zur-pruefung-von-compliance--management-systemen-verab-schiedet.html> (aufgerufen am 1.2.2024).

³⁰ Fila/Püsche, Newsdienst Compliance, 2019, 210017.

³¹ Hoffmann, CCZ 2023, S. 299 ff.

³² Für Versicherungsunternehmen wiederum ist hier entsprechend § 29 Abs. 1 VAG und für Wertpapierdienstleistungsunternehmen § 80 Abs. 1 WpHG anzuführen.

³³ Veit, V./Bornefeld, D.: Geldwäsche-Problematik in Deutschland: Eine Handreichung für Güterhändler, in CCZ 2023, S. 276 ff.; Krais, J., Geldwäsche-Compliance für Industrie und Handel, Praxishandbuch für Güterhändler, Verlag C.H. Beck, 2. Auflage 2022, § 10.

Im Zuge der fortschreitenden Globalisierung und der damit verbundenen Erschließung neuer Märkte und informationstechnologischen Entwicklungen, sind für Compliance Officer in den letzten Jahren weitere Themen in den Fokus gerückt:

Als präsenes Beispiel mag hier insbesondere die Einführung der EU-DSGVO,³⁴ verpflichtend seit dem 25. Mai 2018, angeführt werden. Der Schutz personenbezogener Daten ist selbstredend zentraler Bestandteil der Compliance in Unternehmen und Organisationen. Er rückte durch die Vereinheitlichung auf europäischer Ebene und der damit niedergelegten umfangreichen, bußgeldbewehrten Vorschriften noch mehr in den Fokus der Compliance Officer.

Ein Spannungsfeld kann sich in diesem Kontext durch die Einführung des Hinweisgeberschutzgesetzes ergeben: Am 2. Juli 2023 nach langwierigen Verhandlungen in Kraft getreten zur nationalen Umsetzung der Hinweisgeberrichtlinie,³⁵ regelt das Gesetz nun den Schutz hinweisgebender Personen und dieser sie unterstützenden oder von der Meldung betroffenen Personen: Die Meldung eines Hinweisgebers über Gesetzesverstöße löst schließlich eine Reihe von Handlungspflichten für das Unternehmen aus, auf der anderen Seite sind jedoch die Rechte der betroffenen Personen effektiv zu schützen. Die über das Hinweisgebersystem erhobenen und verarbeiteten – in der Regel personenbezogenen – Daten sind in Einklang mit den Betroffenenrechten zu bringen. Die Sicherstellung der Einhaltung aller hier relevanten Vorschriften liegt in den meisten Organisationen sicherlich wiederum im Compliance-Bereich.³⁶

Als gegenwärtig in ihrer Dimension noch nicht greifbar, aber voraussichtlich eine relevante Rolle im Kontext des Datenschutzrechts spielend, kann darüber hinaus der zunehmende Einsatz von generativer KI angesehen werden. Der AI Act, der die Entwicklung und Nutzung von Systemen der künstlichen Intelligenz (AI)³⁷ innerhalb der EU regeln soll, wurde nun am 21. Mai 2024 durch den Rat der EU-Mitgliedstaaten verabschiedet. Wie sich die neue Verordnung auf die Compliance Arbeit auswirken wird, ist momentan noch nicht abzusehen.³⁸

Das Aufgabenfeld der Compliance Officer wird sich künftig insbesondere auch durch die sich stetig ausdifferenzierenden Umwelt- Sozial- und Governance-Vorschriften (ESG) noch mehr erweitern:

³⁴Verordnung (EU) 2016/679 vom 27.4.2016 (EU-Datenschutz-Grundverordnung), S. L 119/1.

³⁵Richtlinie (EU) 2019/1937 (Hinweisgeberrichtlinie), S. L 305/17.

³⁶Lang, M: Datenschutzrechtliche Implikationen des Hinweisgeberschutzgesetzes, in: ZD 2024, S. 17 ff.

³⁷Verordnung (EU) 2024/1689 vom 13.6.2024 (Verordnung über künstliche Intelligenz), Abl. L 2024/1689.

³⁸Hacker, P./Berz, A.: Der AI-Act der Europäischen Union – Überblick, Kritik und Ausblick, in: ZRP 2023, S. 226 ff.

Als prominente Neuregelung lässt sich hier etwa das am 11. Juli 2021 verabschiedete Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten (Lieferkettensorgfaltspflichtengesetz)³⁹ nennen. Seit dem 1. Januar 2024 ist der Einflussbereich des Gesetzes nun auf Unternehmen mit mehr als 1000 Mitarbeitenden ausgedehnt – was die gestiegene Bedeutung des Lieferkettenmanagements betont. Durch die Anforderungen des Gesetzes sind die betroffenen Unternehmen nun zur Einhaltung und Umsetzung umfangreicher Maßnahmen angehalten, angefangen bei der Implementierung eines hinreichenden Risikomanagements und Durchführung von Risikoanalysen bis hin zur Einrichtung eines Beschwerdeverfahrens und Präventivmaßnahmen. Herausfordernd mag sicher künftig sein, dass damit nicht nur die direkten, sondern auch indirekten Lieferketten nach dem Willen des Gesetzgebers einer Kontrolle unterworfen werden sollen. Das Lieferkettensorgfaltspflichtengesetz setzt damit ein klares Signal gegen Menschenrechtsverletzungen und der Missachtung von Umweltschutzstandards.

Im ESG Bereich sind indes mittlerweile noch weitere Regularien relevant, die in der Compliance Arbeit bereits eine Rolle spielen bzw. künftig verstärkt spielen werden: Exemplarisch seien hier die EU-Taxonomie⁴⁰ als Klassifizierungssystem für ökologisch nachhaltige Wirtschaftstätigkeiten, die Corporate Sustainability Reporting Directive (CSRD)⁴¹ zur Wahrung von Transparenz im Rahmen der nicht-finanziellen Berichterstattung mithilfe von Nachhaltigkeitsindikatoren oder auch die Sustainable Finance Disclosure Regulation (SFDR)⁴² genannt, durch deren Anforderungen die Finanzbranche Marktteilnehmern gegenüber im ESG-Bereich für mehr Transparenz zu sorgen hat. Sicherlich werden sich die Vorschriften in diesem Bereich nicht nur fortentwickeln, sondern auch neue Regularien hinzukommen, sodass sich das Aufgabenfeld von Compliance Officers noch weiter ausdifferenzieren wird.⁴³

Die gestiegene Bedeutung der Compliance lässt sich auch an der Rechtsprechung festmachen:

In einem Obiter Dictum nahm der BGH 2009 noch lediglich die Annahme einer Garantenpflicht des Compliance Officers an. Die Rechtsprechung honoriert mittlerweile klar die die Einführung umfassender Compliance-Maßnahmen: Als wegweisend für eine Compliance Kultur mag das auf dem Siemens-Korruptionsskandal basierende Siemens/

³⁹ Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten (LkSG), BGBL I 2021, S. 2959.

⁴⁰ Verordnung (EU) 2020/852 des Europäischen Parlaments und des Rates vom 18. Juni 2020 über die Einrichtung eines Rahmens zur Erleichterung nachhaltiger Investitionen und zur Änderung der Verordnung (EU) 2019/2088, S. L198/13.

⁴¹ Richtlinie (EU) 2022/2464 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 zur Änderung der Verordnung (EU) Nr. 537/2014 und der Richtlinien 2004/109/EG, 2006/43/EG und 2013/34/EU hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen, S. L 322/15.

⁴² Verordnung (EU) 2019/2088 des Europäischen Parlaments und des Rates vom 27. November 2019 über nachhaltigkeitsbezogene Offenlegungspflichten im Finanzdienstleistungssektor, S. L 317/1.

⁴³ Weinrauer, M: Corporate Sustainability – Compliance, Unternehmensstrategien und Risiken (Teil I und Teil II), in GWR 2023, S. 221 ff. und S. 239 ff.

Neubürger Urteil des LG München I vom 10. Dezember 2013⁴⁴ gelten, in welchem das Gericht die wesentlichen Compliance-Pflichten und Gesamtverantwortlichkeit des Vorstands niederlegte. In seinem Urteil vom 9. Mai 2017 positionierte sich der BGH sodann konkret dazu, dass für die Bemessung der Geldbuße gegen eine Leitungsperson die Errichtung eines effizienten Compliance-Management-System zu berücksichtigen sei.⁴⁵ Existiert mittlerweile zwar noch keine allgemeine Pflicht zur Einführung eines solchen Systems, wird mittlerweile etwa auch aus der zivilrechtlichen Rechtsprechung deutlich, dass keine Frage nach dem „Ob“ hinsichtlich der Errichtung eines Compliance-Management-Systems zu stellen ist, sondern nach der konkreten Ausgestaltung.⁴⁶

Insgesamt zeigt sich mithin weiterhin, dass es kaum ein unternehmerisch relevantes Thema gibt, das trotz seiner bereits großen Bedeutung auch aktuell und weiterhin noch eine solche Dynamik besitzt, wie Compliance. Ein maßgeblicher Faktor für diese Stellung des Themas und grundlegendes Merkmal der Unternehmensherausforderung stellt seine Interdisziplinarität dar.

Es ist unmöglich eine umfassende Betrachtung der Thematik Compliance vorzunehmen, ohne die Schnittmenge zwischen juristischen Regelungen, betriebswirtschaftlichen Vorgängen, ethischen Werten und psychologischen Strukturen zu erkennen. Erst das Verständnis für diesen Vierklang ermöglicht es dem Compliance Officer, Unternehmensvorgänge richtig einzuordnen und mit geeigneten Maßnahmen auf erkannte Risiken und Phänomene zu reagieren.⁴⁷

Trotz dieses weiten Verständnisses der Betätigungsfelder von Compliance liegt der historische Nukleus des deutschen Bewusstseins im Bank- und Kapitalmarktrecht.⁴⁸ Aus diesem Bereich hat sich eine „bemerkenswerte juristische Karriere“⁴⁹ der Thematik entwickelt, was soweit führt, dass in der Rechtswissenschaft sogar das Potenzial für Compliance als eigenständiges Rechtsgebiet gesehen wird.⁵⁰ Dieses muss sich als Querschnittsmaterie mit Fragestellungen diverser rechtlicher Fachdisziplinen auseinandersetzen. Das Bestreben, die zivil- und strafrechtliche Haftung des Unternehmens, seiner Organe und der einzelnen Mitarbeiter zu minimieren, muss als Kerndefinition des Begriffs Compliance aus rechtlicher Sicht erkannt werden.⁵¹ Zur Erfüllung dieser Aufgabe ist es für den Compliance Officer häufig unumgänglich neben Kenntnissen der eigenen nationalen Rechtslage auch solche der gesetzlichen Regelungen der Länder zu besitzen, in denen das Unternehmen in jeglicher Weise geschäftlich aktiv ist. Während das deutsche Recht

⁴⁴ LG München I, Urteil vom 10.12.2013, Az. 5 HK O 1387/10, NZWiSt 2014, 183.

⁴⁵ BGH, Urteil vom 9.5.2017, Az. 1 StR 265/16, NZWiSt 2018, 379, fortgeführt durch BGH, Urteil vom 27.4.2022, Az. 5 StR 278/21, NZWiSt 2022, 410.

⁴⁶ OLG Nürnberg, Endurteil von 30.3.2022, Az. 12 U 1520/19, BeckRS 2022, 9637.

⁴⁷ Rotsch (2012), S. VI.

⁴⁸ Hauschka (2008), S. VII.

⁴⁹ Fleischer (2008), S. 1.

⁵⁰ Rotsch (2012), S. VII.

⁵¹ Steinmeyer/Späth (2020), S. 185 ff.

weiterhin keine Strafbarkeit von Unternehmen gemäß einem eigenständigen Verbandsstrafrecht vorsieht, kann eine solche in anderen Jurisdiktionen zu erheblichen finanziellen Risiken führen.⁵² Daneben stehen den Mitbewerbern bei entsprechenden Verstößen zivilrechtliche Schadenersatzansprüche gegen das betreffende Unternehmen zu. Als mittelbare Folge droht daneben zudem ein zumindest zeitweiser Ausschluss von öffentlichen Ausschreibungen (sogenannte Blacklisting). Darüber hinaus haben sich der Compliance Officer und weitere Führungskräfte im Falle eigener Untätigkeit trotz Kenntnis von Compliance-Verstößen nach Ansicht des Bundesgerichtshofs strafrechtlich zu verantworten.⁵³ Zur Haftung des Unternehmens tritt somit auch die rechtliche Betroffenheit der – gegebenenfalls auch nur mittelbar – beteiligten Einzelpersonen.

Zeitgleich mit der steigenden Brisanz in der Rechtswissenschaft entwickelte sich die Thematik Compliance auch zu einem wichtigen Feld der Wirtschaftswissenschaften.⁵⁴ Dies ist vor allem der Tatsache geschuldet, dass sich ein Großteil der rechtlichen Risiken überhaupt erst dadurch erkennen und verhindern lässt, indem der Compliance Officer die zugrunde liegenden betriebswirtschaftlichen Prozesse versteht und wenn nötig verändert. Durch eine Analyse des „Ist-Zustandes“ der wirtschaftlichen Vorgänge eines Unternehmens muss in einem ersten Schritt ermittelt werden, in welchen Bereichen Compliance-Risiken vorliegen. Anhand dieser Prüfungsergebnisse werden in der Folge kurz-, mittel- oder langfristige Maßnahmen ergriffen, um der zukünftigen Realisierung der erkannten Gefahren entgegenzutreten. Im Streben nach einer „best practice“ muss die stetige Optimierung des Compliance-Managements im Unternehmen daher das ausgesprochene Ziel der Geschäftsführung sein.⁵⁵

Weiterhin kann nur ein gemeinsames, sinnvolles Werteverständnis Garant für die Funktionsfähigkeit des Compliance-Systems im Unternehmen sein.⁵⁶ Es würde dem weiten Feld der Compliance daher nicht gerecht werden, wenn unternehmensspezifische Vorgaben als reine Komposition rechtlicher Regelungen mit wirtschaftlicher Motivation angesehen würden. Tatsächlich spiegeln die maßgeschneiderten Verhaltenskodizes eines Unternehmens zu erheblichen Teilen auch dessen individuell-ethische Grundsätze wider.⁵⁷ Compliance muss als Integritätsforderung an jeden einzelnen Mitarbeitenden verstanden werden, die er eo ipso erfüllt. Nur wenn das legale Handeln als legitim anerkannt wird und die vorgegebenen Regeln moralisch akzeptiert werden, ist die notwendige Basis einer erfolgreichen Compliance-Struktur gegeben.⁵⁸

Aus psychologischer Sicht bedeutet dies, dass eine solche Struktur jedem Mitarbeitenden auch in schwierigen Situationen Sicherheit in seinem Handeln gibt.⁵⁹ Das

⁵² Eufinger, CCZ 2016, S. 209 ff.

⁵³ BGH, Urteil vom 17.7.2009, Az. 5 Str. 394/08, WM 2009 Heft 40, 1882.

⁵⁴ Rotsch (2012), S. V.

⁵⁵ Vertiefend Bernd, Compliance Grundlagen – Betriebswirtschaftliche Aspekte, vgl. Seite 26 ff.

⁵⁶ Vertiefend Schwartz/Seitz, Compliance als Führungsaufgabe, vgl. Seite 337 ff.

⁵⁷ Poppe (2017), S. 1 ff.

⁵⁸ Vertiefend Schwartz/Seitz, Compliance als Führungsaufgabe, vgl. Seite 337 ff.

⁵⁹ Vgl. zur empirischen Evidenz KPMG LLP, 2008–2009 Integrity Survey, S. 17 ff.

hierzu notwendige Vertrauen und die Glaubwürdigkeit in das eigene Unternehmen zu gewährleisten und zu stärken, ist eine der zentralen Aufgaben der Compliance-Abteilung.⁶⁰ Alleine mit der Organisation von Prozessen, Delegation von Aufgaben und der entsprechenden Kontrolle wird ein nachhaltiges Compliance-System nicht etabliert werden können. Nur durch das Vorleben der angestrebten Werte und das Einhalten der vorformulierten Regeln auch und insbesondere durch die Vorgesetzten („tone from the top“) kann ein ganzes Unternehmen dieser Herausforderung gerecht werden. Hieraus ergibt sich, dass Compliance immer und unbedingt Führungsaufgabe ist. Die entwickelten Regelungen müssen ausnahmslos für alle gelten. Es muss zum Selbstverständnis werden, in Übereinstimmung mit allen anwendbaren – auch ethischen – Normen zu handeln.

Bereits im Jahr 2008 wurde an der Juristischen Fakultät der Universität Augsburg eine Forschungsstelle zum Thema Compliance eingerichtet. Diese widmete sich den rechtswissenschaftlichen Auswirkungen der großen Compliance-Skandale der vorangegangenen Jahre.⁶¹ In der Folge setzte die Forschungsstelle einen Schwerpunkt auf die strafrechtlichen Aspekte und gründete das „Center for Criminal Compliance“. Neben drei Professoren waren an ihr zahlreiche Praktiker beteiligt.⁶²

Schon früh wurde auch an der Wirtschaftswissenschaftlichen Fakultät der Universität Augsburg erkannt, dass bei der „Corporate Governance“-Forschung die Thematik Compliance eine bedeutende Rolle spielt. Die beteiligten Wissenschaftler⁶³ setzten sich insbesondere mit der Frage auseinander, welche Vor- und Nachteile die Implementierung einer Compliance-Struktur in die „Corporate Governance“ aus ökonomischer Sicht bietet.

Als Schnittstelle zwischen Wissenschaft und Praxis reagierte das Zentrum für Weiterbildung und Wissenstransfer (ZWW) der Universität Augsburg auf die parallel zu diesen Entwicklungen aufkeimenden Bedürfnisse der Praxis und füllte die Lücke im Qualifizierungsangebot durch das Zertifikatsstudium „Compliance Officer (Univ.)“. Hierdurch generierte das ZWW bundesweit einen neuen Standard in diesem Bereich der universitären Weiterbildung. Seit nunmehr über 10 Jahren bildet das Zertifikatsstudium in einem zweimaligen Durchlauf pro Jahr einen festen Bestandteil in der Compliance-Weiterbildungslandschaft der DACH-Region. Mehr als 500 Absolventinnen und Absolventen des ZWW der Universität Augsburg haben sich durch die universitätszertifizierte Weiterbildung nicht nur das nötige professionelle Know-How zur Tätigkeit als Compliance Officer aneignen vertraut, sondern sind damit auch Teil eines umfassenden compliance-spezifischen Netzwerkes geworden.

Um dem hochprofessionellen Compliance-Ansatz gerecht zu werden, vereinigt und verknüpft das Kurskonzept des ZWW die vier Fachdisziplinen Recht, Betriebswirtschaft, Ethik und Psychologie und formuliert damit in seinem Curriculum einen umfassend ganzheitlichen, integrierten Ansatz (Abb. 1.2):

⁶⁰Vertiefend Schwartz/Seitz, Compliance als Führungsaufgabe, vgl. Seite 337 ff.

⁶¹Vgl. Seite 85.

⁶²Prof. Dr. Michael Kort: Arbeitsrecht, Gesellschaftsrecht; Prof. Dr. Thomas M.J. Möllers: Kapitalmarktrecht; Prof. Dr. Thomas Rotsch: Strafrecht; Prof. Dr. Michael Schmidl, Dr. Christian Heinichen, Dr. Christian Pelz.

⁶³Federführend Prof. Dr. Erik E. Lehmann.



Abb. 1.2 Strukturmodell des Compliance Officer (Univ.) am ZWW der Universität Augsburg

Das hieraus zu erkennende breite Spektrum decken Dozierende ab, die seit Jahren praktisch und theoretisch mit der jeweiligen Materie befasst sind. Gerade bei einem solch dynamischen Thema ist die Rückkopplung mit der Praxis wichtig, um aktuelle angewandte Problemstellungen aufzunehmen. Die wissenschaftliche Fundierung dient der Bildung eines Hintergrundverständnisses, das wiederum beim Aufbau von nachhaltigen Strukturen unabdingbar ist. Nach einem grundlegenden rechtlichen und betriebswirtschaftlichen Überblick folgen die einzelnen Spezialisierungen, stets unter Berücksichtigung gesetzlicher Neuregelungen, bevor diese zum Abschluss des Zertifikatsstudiums in einer praxisnahen Fallstudie wieder zusammengeführt werden. Dabei spiegelt sich die Vielfältigkeit der behandelten Themen in den unterschiedlichen methodischen Konzepten wider.

Der Kurs baut dabei auf der Compliance-Definition der institutionalisierten und intuitiven Normloyalität auf und orientiert sich an den Bedürfnissen der Praxis. Institutionalisierte von Compliance-Strukturen erfolgen im Unternehmen entlang der Funktionskette Prävention – Aufdeckung – Reaktion.⁶⁴ Den präventiven Ausgangspunkt stellt die Risikoanalyse dar. Auf diese baut ein unternehmensspezifischer Code of Conduct auf, der wiederum selbst die Grundlage für einzelne, konkrete Richtlinien darstellt. Schulungen und die Bereitstellung eines Helpdesks sichern die Einhaltung dieser Regularien. Insbesondere ein solcher Helpdesk als Anlaufstelle zur Beantwortung von compliancespezifischen Fragen kann darüber hinaus auch anlassbezogen das Erkennen von Compliance-Verstößen erleichtern. Externe Ombudsleute und das – seit Einführung des Hinweisgeberschutzgesetzes für Unternehmen mit mehr als 50 Beschäftigten zwingend zu errichtende – Hinweisgebersystem mögen diesbezüglich jedoch die praktisch größere Bedeutung aufweisen. Regelmäßige Überprüfungen und Berichtspflichten sorgen für Transparenz und damit für

⁶⁴ Moosmayer (2021), § 1, Rn. 4.

die kontinuierliche Grundlage der Aufdeckung. Personen- und sachbezogenen Warnsignalen („Red Flags“) kommt dabei eine zentrale Rolle zu. Durch Internal Investigations, Regress bei Managerinnen und Managern und arbeitsrechtlichen Konsequenzen kann schließlich auf Compliance-Verstöße individuell und dem Einzelfall angepasst reagiert werden. Freilich kann dies stets nur im Rahmen der gesetzlichen Vorgaben insbesondere des Arbeits- und Datenschutzrechts erfolgen.

Im Hinblick auf die intuitive Normloyalität sollte dabei Ziel sein, dass Compliance ein Automatismus im Handeln jedes einzelnen Mitarbeitenden wird. Dies muss unabhängig von seiner Position im Unternehmen erfolgen. Erst durch den notwendigen „tone from the top“ kann ein „echtes“ Verständnis von Compliance vermittelt werden. Es muss für den Mitarbeitenden zum Selbstverständnis werden, sich an die unternehmens-individuellen Regeln zu halten. Dabei obliegt es dem Compliance Officer, diese Denkweise bei seinen Kolleginnen und Kollegen zu aktivieren. Seine Aufgabe ist es, über die Unternehmenshierarchien hinweg Akzeptanz für die Thematik Compliance zu schaffen. Hierdurch wird es erst möglich, dass Compliance intuitiv gelebt wird.

Mit der erfolgreichen Implementierung eines Compliance-Systems wird eine positive Unternehmenskultur verstärkt oder aufgebaut. Dies fördert die Identifikation und damit auch die Motivation jedes einzelnen Mitarbeitenden, sich für das Kollektiv einzubringen. Damit ist eine Effektivitätssteigerung im Arbeitsalltag verbunden, da fortwährend gesteigertes Wissen und Verständnis für Unternehmensprozesse geschaffen werden. Die Compliance-Strukturen fügen sich nahtlos in bestehende Qualitätssicherungssysteme ein und sichern damit den Unternehmenserfolg und die Kundenzufriedenheit ab (Abb. 1.3).

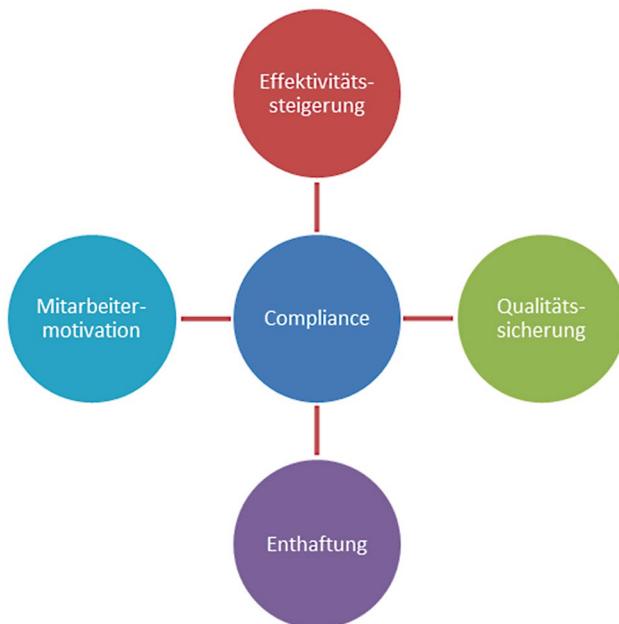


Abb. 1.3 Wertschöpfung durch Compliance

Bereits bei Erscheinen der Erstauflage war der Compliance nicht nur für Großunternehmen eine bedeutsame Rolle zu attestieren. Die Relevanz von Compliance hat sich seitdem insbesondere auch für mittelständische und kleine Unternehmen jeder Branche weiter maßgeblich etabliert. Nicht nur, um die Einhaltung der gesetzlichen Vorschriften zu gewährleisten, sondern insbesondere auch, um die Wettbewerbsfähigkeit durch Risikominimierung, Verbesserung von Effizienz und internen Kontrollen und die Unternehmensreputation sicherzustellen.⁶⁵

Insgesamt wird Compliance, nicht nur im Kontext von Entwicklungen im regulatorischen Bereich, für erfolgreiche Organisationen und Unternehmen immer noch bedeutsamer! Gleichzeitig haben sich das Aufgabenportfolio, wie auch die Ansprüche an die professionelle Rolle der Compliance Officer quantitativ wie qualitativ enorm ausgeweitet und gesteigert – was sich auch im Ausblick auf die kommenden Jahre noch intensivieren wird.

Nach der mittlerweile erfolgten Etablierung der Profession „Compliance“ ist gegenwärtig der Trend, wohl auch die Notwendigkeit erkennbar, sich von der Rolle des Compliance Officer als Generalist fachlich hin zum Compliance Officer als Spezialist zu entwickeln.

Dass der Trend zur Compliance-Spezialisierung, für große Unternehmen, aber insbesondere auch für KMU, eine Herausforderung darstellt, ist offensichtlich. Umso wichtiger ist es, frühzeitig und umfassend mit der Qualifizierung geeigneter Mitarbeiterinnen und Mitarbeiter zu beginnen, diese zu fördern und zu qualifizieren, den notwendigen Know-how Aufbau sicherzustellen und das eigene Unternehmen compliance-zukunfts-trächtig aufzustellen. Dies ist der wichtigste Hebel, um mit wenig Investition äußerst wirkungsvoll hohe Risiken zu minimieren.

Mit dem Zertifikatsstudium zum Compliance Officer, mit den zusätzlichen, spezialisierten Compliance-Seminaren und auch mit diesem Begleitbuch möchten wir als ZWW/ Universität Augsburg für unsere Teilnehmenden und deren Unternehmen als Partner einen Beitrag dazu leisten der komplexen, gleichzeitig überaus herausfordernden und verantwortungsvollen Aufgabe „Compliance“ professionell gerecht werden zu können.

Literatur

- BEHRINGER, S. (2010) 2018: Compliance – Modeerscheinung oder Prüfstein für gute Unternehmensführung?, in: BEHRINGER, S. (Hrsg.), Compliance kompakt: Best Practice im Compliance Management, S. 25 ff, Berlin.
- BLOCK, U. (2003): Neue Regelungen zur Corporate Governance gemäß Sarbanes-Oxley Act, in: BKR (2003) S. 774 ff.
- BÜRKLE, J. (2004): Compliance in Versicherungsunternehmen: Ja, aber wie?, in: VW (2004a) S. 830 ff.
- BÜRKLE, J. (2004): Weitergabe von Informationen über Fehlverhalten in Unternehmen (Whistleblowing) und Steuerung auftretender Probleme durch ein Compliance-System, in: DB (2004b) S. 2158 ff.
- DIENERS, P./BESEN, M. (2010): Handbuch Compliance im Gesundheitswesen: Kooperation von Ärzten, Industrie und Patienten, 3. Aufl., München.

⁶⁵Vertiefend Moosmayer (2021), § 1 Rn. 7: Zum Verständnis der Compliance als „Reputationsmanagement“ für Organisationen.

- DREHER, M. (2004): Kartellrechtscompliance, in: ZWeR (2004) S. 75 ff.
- EISELE, D. (1993): Insiderrecht und Compliance, in: WM (1993) S. 1021 ff.
- EUFINGER, A. (2012): Zu den historischen Ursprüngen der Compliance, in: CCZ (2012) S. 21 f.
- FLEISCHER, H. (2003): Vorstandsverantwortlichkeit und Fehlverhalten von Unternehmensangehörigen: Von der Einzelüberwachung zur Errichtung einer Compliance-Organisation, in: AG (2003) S. 291 ff.
- FLEISCHER, H. (2004): Legal Transplants im deutschen Aktienrecht, in: NZG (2004) S. 1129 ff.
- FLEISCHER, H. (2008): Corporate Compliance im aktienrechtlichen Unternehmensverbund, in: CCZ (2008) S. 1.
- GRUMMER, J.-M./SEEBURG, J. (2010): SOX Compliance, in: BEHRINGER, S. (Hrsg.), Compliance kompakt: Best Practice im Compliance Management, S. 211 ff, Berlin.
- HAUSCHKA, C. E. (2004): Compliance, Compliance-Manager, Compliance-Programme: Eine geeignete Reaktion auf gestiegene Haftungsrisiken für Unternehmen und Management?, in: NJW (2004a) S. 257 ff.
- HAUSCHKA, C. E. (2004): Corporate Compliance – Unternehmensorganisatorische Ansätze zur Erfüllung der Pflichten von Vorständen und Geschäftsführern, in: AG (2004b) S. 461 ff.
- HAUSCHKA, C. E. (2004): Der Compliance-Beauftragte im Kartellrecht, in: BB (2004c) S. 1178 ff.
- HAUSCHKA, C. E. (2006): Von Compliance zu Best Practice, in: ZRP (2006) S. 258 ff.
- HAUSCHKA, C. E. (2008): Einleitung, in: Umnuß, K. (Hrsg.), Corporate Compliance Checklisten: Rechtliche Risiken im Unternehmen erkennen und vermeiden, S. XII ff, München.
- HAUSCHKA, C. E./MOOSMAYER, K./LÖSLER, T. (2016): Corporate Compliance: Handbuch der Haftungsvermeidung in Unternehmen, München
- JÄGER, A./RÖDL, C./CAMPOS NAVÉ, J. (2009): Praxishandbuch Corporate Compliance: Grundlagen – Checklisten – Implementierung, 1. Aufl., Weinheim.
- KLINDT, T. (2006): Nicht-börsliches Compliance-Management als zukünftige Aufgabe der Inhouse-Juristen, in: NJW (2006) S. 3399 f.
- KLINDT, T./PELZ, C./THEUSINGER, I. (2010): Compliance im Spiegel der Rechtsprechung, in: NJW (2010) S. 2385 ff.
- LAMPER, T. (2002): Gestiegenes Unternehmensrisiko Kartellrecht – Risikoreduzierung durch Competition-Compliance-Programme, in: BB (2002) S. 2237 ff.
- LÖSLER, T. (2003): Compliance im Wertpapierdienstleistungskonzern, Berlin, Würzburg.
- LÖSLER, T. (2005): Das moderne Verständnis von Compliance im Finanzmarktrecht, in: NZG (2005) S. 104 ff.
- MOOSMAYER, K. (2021): Compliance – Praxisleitfaden für Unternehmen, München.
- OBERMAYR, G. (2010): § 17 Revision, in: HAUSCHKA, C. E. (Hrsg.), Corporate Compliance: Handbuch der Haftungsvermeidung im Unternehmen, S. 424 ff, München.
- POPPE, S. (2017): Begriffsbestimmung Compliance: Bedeutung und Notwendigkeit, in: INDERST, C./BANNENBERG, B./POPPE, S. (Hrsg.), Compliance: Aufbau – Management – Risikobereiche, Heidelberg, 3. Aufl. 2017, (= Wirtschaftsrecht), S. 1 ff.
- POWERS, W. C., JR./TROUBH, R. S./WINOKUR, H. S., JR. (2002): Report of Investigation by the Special Investigative Committee of the Board of Directors of Enron Corp., <<http://i.cnn.net/cnn/2002/LAW/02/02/enron.report/powers.report.pdf>>.
- ROGALL, K. (2006): § 130, Karlsruher Kommentar zum Gesetz über Ordnungswidrigkeiten, 3. Aufl., München.
- ROGALL, K. (2006): § 30, Karlsruher Kommentar zum Gesetz über Ordnungswidrigkeiten, 3. Aufl., München.
- ROTSCH, T. (2012): Wissenschaftliche und praktische Aspekte der nationalen und internationalen Compliance-Diskussion, Baden-Baden 2012 (= Schriften zu Compliance, Bd. 2).
- SCHERP, D. (2003): Compliance, in: Kriminalistik (2003) S. 486 ff.
- SCHNEIDER, U. H. (2003): Compliance als Aufgabe der Unternehmensleitung, in: ZIP (2003) S. 645 ff.

- STEINMEYER, R./SPÄTH, P. (2020): Bedeutung des Rechts für Unternehmen und die Erwartungshaltung der Rechtsordnung gegenüber Unternehmen: Corporate Compliance, in: WIELAND, J./STEINMEYER, R./GRÜNINGER, S. (Hrsg.), Handbuch Compliance-Management, Berlin, 3. Auflage, 2020, S. 185ff.
- TANSKI, J. S. (2002): WorldCom: Eine Erläuterung zu Rechnungslegung und Corporate Governance, in: DStR (2002) S. 2003 ff.
- VETTER, E. (2009): Compliance in der Unternehmenspraxis, in: WECKER, G./van LAAK, H. (Hrsg.), Compliance in der Unternehmenspraxis, S. 33 ff, Wiesbaden.
- BATZ, S./WEIDIG, J.: Aktuelle Entwicklungen in den USA – Zweite Auflage des FCPA-Guide, in: CCZ (2020), S. 359 ff.
- SCHULZ, M.: Prüfung und Bewertung von Compliance-Management-Systemen (insbesondere „IDW PS 980“) für Compliance aus Sicht der Wissenschaft, in: BAY, K.-C., HASTENRATH, K.: Compliance-Management-Systeme: Praxiserprobte Elemente, Prozesse und Tools, 2. Aufl., München, 2016, S. 229 ff.
- FILA, D./PÜSCHEL, C.: Wie misst man Compliance? – Ein aktueller Überblick zu den Möglichkeiten der Zertifizierung von Compliance-Management-Systemen und Compliance-Verantwortlichen, in: Newsdienst Compliance (2019), 210017 ff.
- HOFMANN, R.: Die Messung von Compliance aus Sicht eines internationalen Konzernes, in CCZ 2023, S. 299 ff.



Carina Metscher Rechtsanwältin, geboren 1984 in Augsburg. Studium der Rechtswissenschaften und Referendariat in Augsburg. Nach dem Assessorexamen Tätigkeit als Rechtsanwältin einer mittelständischen Anwaltskanzlei in Augsburg. Seit 2016 Produktmanagerin der Juristischen Weiterbildung am Zentrum für Weiterbildung und Wissenstransfer der Universität Augsburg.



Hanspeter Vietz Diplom-Kaufmann und MBA, geboren 1963 in Pfronten/Allgäu. Abitur in Wiesbaden und Studium der Wirtschaftswissenschaften an der Universität Augsburg. Berufliche Engagements im Bereich Marketing, Strategie und Unternehmensführung. Experte für Gesprächs- und Verhandlungsführung. Konzeption und Aufbau des berufsbegleitenden MBA-Studiengangs „Unternehmensführung“ an der Universität Augsburg; Vorstandsmitglied des MBA-lumni e. V.; Mitglied des Sprecherrats der DGWF-Bayern (Deutsche Gesellschaft für Weiterbildung und Fernstudien). Preisträger der Kurt und Felicitas Viermetz Stiftung. Ab 2010 stellvertretender Geschäftsführer des ZWW und seit 2019 Geschäftsführer des ZWW und Mitglied des Leitungsgremiums des ZWW (Zentrum für Weiterbildung und Wissenstransfer).



Compliance: Grundlagen – Betriebswirtschaftliche Aspekte

2

Thomas Berndt

Inhaltsverzeichnis

2.1 Einleitung	19
2.2 Nichtfinanzielle Erklärung	20
2.3 Nachhaltigkeitsberichterstattung	22
2.4 „Lieferkettengesetz“ und CSDDD	24
2.5 Prüfung	26
2.6 Risikomanagement und IKS	28
2.7 Corporate Governance und „Three Lines“	31
2.8 Fraud	33
2.9 Kultur	35
2.10 Schluss	36

2.1 Einleitung

Beispiel zur Korruption

„Petrus will die Himmelspforte renovieren und holt dafür drei Angebote ein: Der Albaner verlangt € 600 (€ 200 für die Farbe, € 400 für die Arbeit). Der deutsche Handwerker will € 1000 (€ 300 für die Qualitätsfarbe, € 300 für die Arbeit und € 400 für Steuer und Versicherung). Der Grieche will € 3000! Er erklärt dem geschockten

T. Berndt (✉)

Institut für Law and Economics, Universität St. Gallen, St. Gallen, Schweiz

Petrus: € 1000 für mich, € 1000 für Dich, € 200 für die Farbe, € 500, damit der Deutsche sein Angebot zurückzieht, und € 300 für den Albaner – irgendwer muss die Arbeit ja machen.“¹ ◀

Nicht unbedingt vor Petrus aber dennoch in einer ähnlichen Situation mag manches Unternehmen, das Leistungen am Markt nachfragt oder anbietet, schon einmal gewesen sein. Diese Anekdote zeigt anschaulich, dass Compliance auch und vor allem betriebswirtschaftliche Aspekte umfasst: Unternehmen haben das Ziel der betrieblichen Leistungserstellung. Aus ökonomischer Sicht stellt daher das Einhalten rechtlicher (oder sonstiger) Regelungen lediglich eine Nebenbedingung dar. Damit ist freilich ein typischer Grundkonflikt in der praktischen Tätigkeit schon vorprogrammiert: Denn aus juristischer Sicht stellt die Sicherstellung regelkonformen Verhaltens – im jeweiligen unternehmerischen Kontext – die zentrale Hauptleistung dar. Nicht selten empfinden daher juristische Compliance-Vertreter zum Beispiel Vertriebsmitarbeiter als wenig einsichtig und beratungsresistent, wenn es um die Einhaltung von rechtlichen Vorgaben geht. Und umgekehrt fühlen sich etwa Vertriebsmitarbeiter durch Compliance-Vorgaben gegängelt, in ihrer Kreativität, zum Wohl des Unternehmens (oder manchmal auch nur zu ihrem eigenen Wohle) zu handeln. Oftmals wäre den Unternehmen schon viel geholfen, wenn eine deutlichere, offenere Kommunikation zwischen den verschiedenen Gruppen stattfinden könnte, um gegenseitig Verständnis für die eigenen Aufgaben und Anforderungen aufbringen zu können.

In diesem Beitrag werden einige wenige ausgewählte Aspekte und Schnittpunktthemen der Compliance aus betriebswirtschaftlicher Sicht angesprochen. Die Anknüpfungspunkte zwischen Compliance und Betriebswirtschaft sind dabei vielfältig: Corporate Governance, Audit Committee, Interne Kontrollsysteme, Internal Audit, Risikomanagement, Rechnungslegung, Finanzielle und nichtfinanzielle Berichterstattung, Unternehmenskultur, Reputation, Fraud, Hinweisgebersysteme, Compliance Management-Systeme, Drittparteienmanagement-Systeme, Abschlussprüfung, Zertifizierung. Und mit dem Thema der „Nachhaltigkeit“ im weitesten Sinne („ESG“, Corporate Social Responsibility etc.) hat sich in den letzten Jahren ein weiteres zentrales Anwendungsfeld der Compliance an der Schnittstelle von Recht und Betriebswirtschaft ergeben. Es zeigt sich einmal mehr, dass eine gute Corporate Compliance letztlich nur durch interdisziplinäres Zusammenwirken von juristischen und ökonomischen Vertretern aufgebaut und effektiv gelebt werden kann.

2.2 Nichtfinanzielle Erklärung

In das Bewusstsein vieler Betriebswirte ist das Thema der Compliance in den letzten Jahren nicht zuletzt aufgrund der Nachhaltigkeitsthematik gerückt. Aus einem eher unverbindlichen, nicht selten dem Marketingbereich zuzuordnendem Versprechen, ein Unternehmen

¹Vgl. FAZ vom 2. Oktober 2011. Griechischer Witz erzählt von Raimund Wünsche.

produziere und vertreibe „grüne“, „nachhaltige“ Produkte, ist eine gesetzliche Verpflichtung geworden, über eine Vielzahl nichtfinanzialer Aspekte Rechenschaft abzulegen. Die EU-Richtlinie 2014/95, die so genannte „Non-Financial Disclosure Directive“ (NFRD), verpflichtet Unternehmen von öffentlichem Interesse, die mehr als 500 Mitarbeiter beschäftigen, für ab dem 1. Januar 2017 beginnende Geschäftsjahre, zur Angabe von nichtfinanziellen und die Diversität betreffenden Informationen. Im Kern verlangt die Richtlinie, die über das Gesetz zur Stärkung der nichtfinanziellen Berichterstattung der Unternehmen in ihren Lage- und Konzernlageberichten („CSR-Richtlinie-Umsetzungsgesetz“) 2017 in das deutsche Recht umgesetzt wurde, dass die betroffenen Unternehmen eine Erklärung zu Umwelt-, Sozial- und Arbeitnehmerbelangen, die Achtung der Menschenrechte und die Bekämpfung der Korruption machen müssen. Zu diesen Aspekten muss die Beschreibung des Geschäftsmodells erfolgen, der verfolgten Konzepte und deren Ergebnisse, die angewandten Due-Diligence-Prozesse, die damit verbundenen wesentlichen Risiken und deren Verknüpfung und Auswirkung auf die Geschäftstätigkeit sowie die mit der Geschäftstätigkeit verbundenen wichtigsten nichtfinanziellen Leistungsindikatoren.²

Die betriebswirtschaftlichen Aspekte der Compliance in Zusammenhang mit der Nichtfinanziellen Erklärung sind ebenso offenkundig wie vielfältig, wobei nachfolgend nur zwei Aspekte hervorgehoben werden sollen: Zum einen betrifft dies das Identifizieren der wesentlichen Risiken aus der eigenen Geschäftstätigkeit wie auch der wesentlichen Risiken aus Geschäftsbeziehungen, Produkten und Dienstleistungen. Die nichtfinanziellen Aspekte sind insofern zwingend in das Risikomanagement der Unternehmen explizit zu berücksichtigen, um deren (Nicht-)Wesentlichkeit in einem geordneten Verfahren überhaupt bestimmen zu können. Zum anderen betrifft dies die Kommunikation der wichtigsten nichtfinanziellen Leistungsindikatoren. Hierzu hat die Europäische Kommission 2017 Leitlinien zur Orientierung erlassen.³ Während die Leistungsindikatoren bezüglich Umweltbelange eher technischer Natur sind (etwa Treibhausgasemissionen oder Energieverbrauch), sind Indikatoren zur Bekämpfung von Korruption und Bestechung oder zur Achtung der Menschenrechte unmittelbar mit dem Compliance-Management-System der Unternehmen verbunden, beispielsweise wenn es um die zur Korruptionsbekämpfung eingesetzten Konzepte, Verfahren und Standards geht, die Kriterien zur Bewertung von Korruptionsrisiken, die zum Thema Bekämpfung von Korruption und Bestechung geschulten Mitarbeiter oder auch die Anzahl wegen wettbewerbswidrigen Verhaltens anhängiger oder abgeschlossener Klagen. Die überwiegende Mehrheit der Unternehmen nimmt dies zum Anlass, in der Nichtfinanziellen Erklärung ihr Compliance-Management-System zu beschreiben, weswegen der Compliance-Abteilung eine wichtige Funktion in der fristgemäßen, zweckmäßigen und angemessenen Bereitstellung relevanter Informationen für die Berichterstellung der Unternehmen zukommt.

²Vgl. zu Details Berndt/Jablowski: Die Umsetzung der CSR-Richtlinie in Deutschland, in: ZCG 2019, S. 86 ff.

³Vgl. <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52017XC0705%2801%29> (aufgerufen am 15.2.2024).

Hervorzuheben ist, dass die Nichtfinanzielle Erklärung letztlich „nur“ eine spezifische Berichterstattungspflicht ist, die sich etwa bereits unter Rückgriff auf ein anerkanntes internationales Rahmenwerk wie das der Global Reporting Initiative (GRI) erfüllen lässt.⁴ Unternehmen, die zuvor freiwillig einen Nachhaltigkeitsbericht erstellt hatten – und das ist bei den kapitalmarktorientierten die überwiegende Mehrheit – stellte die Erfüllung der neuen Vorgaben vor keine wesentlichen neuen Anforderungen. Teilweise umstritten waren eher pragmatisch-organisatorische Aspekte, so etwa die Frage, ob bei der Darstellung von Risiken der eigenen Geschäftstätigkeit von einer Bruttobetrachtung oder einer Netto betrachtung auszugehen sei. Letztere würde den Umfang der erläuternden Angaben teils deutlich reduzieren, erstere wäre jedoch aus Adressatensicht wesentlich aussagekräftiger. Das Institut der Wirtschaftsprüfer (IdW) hat in einem Positionspapier zutreffend die Bruttobetrachtung empfohlen.⁵ Zu den pragmatisch-organisatorischen Aspekten gehört auch die Frage, nach der Einbindung der Nichtfinanziellen Erklärung in die Governance-Struktur der Unternehmen: Nach § 171 Abs. 1 Satz 4 AktG erstreckt sich die Prüfungspflicht des Aufsichtsrates auch auf die Nichtfinanzielle Erklärung, wobei Art und Umfang der Prüfungshandlungen letztlich im Ermessen des Aufsichtsrats liegen und von reinen Plausibilitätsprüfungen bis zur freiwilligen Beauftragung externer Prüfungen mit begrenzter oder hinreichender Sicherheit reichen können.⁶

2.3 Nachhaltigkeitsberichterstattung

Die Europäische Union hat bereits kurz nach dem Inkrafttreten der Nichtfinanziellen Erklärung erheblichen Änderungsbedarf gesehen und schon in 2021 den Vorschlag einer Corporate Sustainability Reporting Directive (CSRD) veröffentlicht. Die im Januar 2023 verabschiedete CSRD fügt sich in die „Green Deal Policy“ der EU ein und erhebt erklärtermaßen Nachhaltigkeitsinformationen in den gleichen Rang wie die tradierten Finanzinformationen.⁷ Im Kern lassen sich fünf wesentliche Neuerungen gegenüber der Nichtfinanziellen Erklärung identifizieren: Erstens wird der Anwendungsbereich deutlich ausgeweitet: Während zunächst für ab dem 1. Januar 2024 beginnende Geschäftsjahre nur diejenigen Unternehmen verpflichtend einen Nachhaltigkeitsbericht erstellen müssen, die zuvor in den Anwendungsbereich der NFRD fielen (also die Unternehmen von öffentlichem Interesse mit über 500 Mitarbeitern), wird für zum 1. Januar 2025 beginnende Geschäftsjahre die Berichtspflicht auf sämtliche großen Unternehmen ausgeweitet. Als groß gelten Unternehmen, wenn sie zwei der drei nachfolgenden Kriterien überschreiten: Bilanzsumme grösser € 20. Mio., Nettoumsatzerlöse grösser € 40 Mio. und Arbeitnehmerzahl über 250. Es wird erwartet, dass statt bisher rund 11.000 Unternehmen in der EU nunmehr über 50.000 Unternehmen die neuen Berichterstattungspflichten erfüllen müssen.

⁴Vgl. <https://www.globalreporting.org/> (aufgerufen am 7.2.2024).

⁵IdW (2017): Pflichten und Zweifelsfragen zur nichtfinanziellen Erklärung als Bestandteil der Unternehmensführung.

⁶Vgl. Gundel, A. (2018). Prüfung der CSR-Berichterstattung durch den Aufsichtsrat. Wie intensiv muss der Aufsichtsrat die Rechtmäßigkeit prüfen?, in WPg 02/2018.

⁷<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2464> (aufgerufen am 7.2.2024).

Für die Zukunft ist darüber hinaus vorgesehen, auch KMU zu einer vereinfachten Nachhaltigkeitsberichterstattung zu verpflichten.

Zweitens werden die Anforderungen an die Inhalte des Nachhaltigkeitsberichts normiert und präzisiert. Dazu hat die EU eigene Standards veröffentlicht, die European Sustainability Reporting Standards (ESRS).⁸ Während ESRS 1 und 2 bereichsübergreifende Regelungen enthalten, finden sich in den weiteren ESRS themenspezifische Regelungen. Später sollen noch industriespezifische Standards folgen (vgl. Abb. 2.1). Die EU hat in den ESRS u. a. auch das in der Praxis zuvor unterschiedlich ausgelegte Wesentlichkeitsprinzip definiert. Danach gilt die so genannte „Doppelte Wesentlichkeit“ (oder „Doppelte Materialität“). Nachhaltigkeitsinformationen gelten dann als wesentlich, wenn sie entweder aus einer Inside-Out-Perspektive oder einer Outside-In-Perspektive wesentlich sind. Erstere wird auch als



Abb. 2.1 European Sustainability Reporting Standards

⁸Wichtige Materialien für das Verständnis und zur Einordnung der ESRS finden sich unter <https://www.efrag.org/lab6> (aufgerufen am 7.2.2024).

Impact Materiality bezeichnet, meint also die Auswirkungen, die Unternehmenstätigkeiten auf nachhaltigkeitsrelevante Themen hat. Letztere bezeichnet man auch als Financial Materiality und gibt damit die Chancen und Risiken von Nachhaltigkeitsaspekten auf die finanzielle Lage und Zukunftsfähigkeit des Unternehmens an.

Drittens sieht die CSRD vor, dass der Nachhaltigkeitsbericht nur noch als Teil des Lageberichts veröffentlicht werden darf. Irgendwelche gesonderten Formate sind damit nicht mehr zulässig.

Viertens wird eine digitale Berichterstattung mit digitalem Tagging verpflichtend, um eine höhere Vergleichbarkeit, Auswertbarkeit bzw. Analyse und Nutzung von Nachhaltigkeitsinformationen für alle Adressaten zu ermöglichen.

Und schließlich wird für die Nachhaltigkeitsberichterstattung eine Prüfung mit begrenzter Prüfungssicherheit verpflichtend, um die Verlässlichkeit der Informationen sicherzustellen. Bei der begrenzten Sicherheit wird der Umfang der durchgeführten Prüfungshandlungen gegenüber der hinreichenden Sicherheit reduziert. Das Prüfungsurteil formuliert, dass im Rahmen der Prüfungshandlungen keine Kenntnisse erlangt wurden, die darauf schließen ließen, dass der Bericht nicht in Übereinstimmung mit den anwendbaren Regelungen steht.

Es wird deutlich, dass der Compliance eine enorme Bedeutung im Zusammenhang mit der CSRD zukommt. Das gilt zum einen in formeller Hinsicht bezüglich der Einhaltung der neuen gesetzlichen Anforderungen. Es gilt aber viel mehr noch in materieller Hinsicht; denn die themenspezifischen Berichtserfordernisse verlangen die Bereitstellung umfangreicher Informationen, die nunmehr auch prüfungspflichtig sind, also strengeren Qualitätsansprüchen genügen müssen, als lediglich freiwillige oder nur für interne Zwecke verwendete Informationen. Unternehmen mögen sich nicht zu Unrecht fragen, ob mit den neuen Nachhaltigkeitsberichten nicht auch vermehrt Anknüpfungspunkte für juristische Auseinandersetzungen gegeben sind.

2.4 „Lieferkettengesetz“ und CSDDD

2018 wurde der OECD-Leitfaden für die Erfüllung der Sorgfaltspflicht für verantwortungsvolles unternehmerisches Handeln gebilligt, der ein gemeinsames Verständnis von Due Diligence in der Lieferkette schaffen sollte.⁹ Der deutsche Gesetzgeber hat diese Vorgaben in dem Lieferkettensorgfaltspflichtengesetz (LkSG) 2021 umgesetzt.¹⁰ Direkt davon

⁹Vgl. <https://mneguidelines.oecd.org/OECD-leitfaden-für-die-erfüllung-der-sorgfaltspflicht-für-verantwortungsvolles-unternehmerisches-handeln.pdf> (aufgerufen am 7.2.2024).

¹⁰Zu ausführlichen Details siehe zum Beispiel Wagner/Rutloff/Wagner: Das Lieferkettensorgfaltspflichtengesetz in der Unternehmenspraxis, München 2022.

betroffen sind seit dem 01.01.2024 Unternehmen mit mehr als 1000 Arbeitnehmern, die entweder ihren Sitz in Deutschland oder hier eine Zweigniederlassung haben. Indirekt hingegen noch viel mehr Unternehmen, da es ja gerade Sinn des LkSG ist, die Angemessenheit von Menschen- und Arbeitnehmerrechten sowie Umweltbelangen in der Lieferkette, also bei vorgelagerten Unternehmen sicherzustellen. Auch KMU und ausländische Unternehmen, zu denen eine (direkte) Vertragsbeziehung besteht, müssen insofern den Sorgfaltsmassstab der direkt betroffenen Unternehmen erfüllen. Das LkSG verdeutlicht die enge Verzahnung von Compliance und Betriebswirtschaft: Wiederum ist das Risk-management von entscheidender Bedeutung; denn die Angemessenheit bestimmt sich aus der Art der Geschäftstätigkeit (dem „Kontrollumfeld“), der Risikowahrscheinlichkeit, der Schwere des möglichen Schadens sowie den Einwirkungsmöglichkeiten des Unternehmens. Ohne Transparenz in der Lieferkette, ohne Integration in bestehende Managementsysteme, ohne Einbezug von Stakeholdern und ohne Integration in die Nachhaltigkeitsberichterstattung sind die gesetzlichen Anforderungen kaum zu erfüllen.

Als unbefriedigend erkannt ist die Situation, in der zahlreiche Länder jeweils eigene Sorgfaltspflichtengesetze mit teilweise unterschiedlichen Anwendungsbereichen und Reichweiten erlassen. Mit der Corporate Sustainability Due Diligence Directive (CSDDD) – oder auch „EU-Lieferkettengesetz“ liegt ein Mitte 2023 vom EU-Parlament nochmals verschärfter Richtlinienentwurf vor, der diese Situation, zumindest innerhalb der EU, verhindern soll. Im Sommer 2024 ist die CSDDD endgültig von der EU verabschiedet worden und muss nun in das nationale Recht transformiert werden. Nach dem derzeitigen Stand müssen bis 2029 alle EU-Gesellschaften von erheblicher Größe und Wirtschaftskraft (mit mindestens 1000 Beschäftigten und einem Nettoumsatz von mindestens 450 Mio. € weltweit) die Anforderungen erfüllen, für ausländische Unternehmen gilt ein Schwellenwert von 450 Mio. € Nettoumsatz in der EU. Es gelten allerdings mehrjährige Übergangsfristen, so dass zunächst nur besonders grosse Unternehmen die Anforderungen der CSDDD ab 2027 erfüllen müssen (5000 Mitarbeiter und 1,5 Mrd. € Nettoumsatz). In der EU würden damit ca. 5400 Unternehmen in den direkten Anwendungsbereich der CSDDD fallen. Über die Lieferkettenverknüpfung mit Zulieferern und Abnehmern ist die indirekte, faktische Auswirkung aber um ein Vielfaches grösser.

Als maßgeblich zu erfassende Themenkreise gelten die tatsächlichen oder potenziellen negativen Auswirkungen auf die Menschenrechte und die Umwelt. Diese sind zu integralen Bestandteilen der Tätigkeiten der Unternehmensleitung zu machen, schlagen sich also auf die Corporate Governance-Anforderungen der Unternehmen nieder. Explizit wird hervorgehoben, dass nicht nur eine Bewertung entsprechender Risiken vorzunehmen ist, sondern es sind wirksame Maßnahmen zu ergreifen, die Auswirkungen abzustellen oder auf ein Minimum zu reduzieren. Hinzu kommt die Einrichtung einer Beschwerdestelle und auf Länderebene die Einrichtung einer Aufsichtsbehörde.

2.5 Prüfung

Der betriebswirtschaftliche Zusammenhang zur Compliance wird im Anwendungsfall der „Prüfung“ besonders deutlich. Zwei Aspekte sollen nachfolgend angesprochen werden: Zum einen die Prüfung von Compliance-Management-Systemen an sich. Zum anderen die bereits oben angesprochene Prüfung von Nachhaltigkeitsberichten bzw. ESG-relevanten Informationen.

Mit der Verabschiedung des IdW Prüfungsstandards PS 980 „Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen“ im März 2011 hat das Thema der Zertifizierung einen großen Aufschwung genommen. Nachdem viele Konzerne große Anstrengungen in den Aufbau ihrer Compliance-Systeme unternommen hatten, war es ihnen ein Anliegen, darüber ein verlässliches, sachverständiges, unabhängiges Urteil zu erlangen. Zu betonen ist zunächst, dass es auch derzeit weiterhin keine Prüfungspflicht für Compliance Management-Systeme gibt und IdW PS 980 insofern nur den Inhalt freiwilliger Prüfungen durch den Berufsstand der Wirtschaftsprüfer regelt. Er verfolgt das Ziel, einen standardisierten Rahmen für Compliance-Systeme unter gleichzeitiger Wahrung individueller Spielräume für Unternehmen zu bieten. Entsprechend können die Unternehmen den Anwendungsbereich selbst auf einzelne Rechtsgebiete (zum Beispiel Wettbewerbs-, und Kartellrecht, Börsenrecht, Außensteuerrecht etc.), einzelne Geschäftsbereiche und/oder operative Prozesse beschränken. Ein spezifisches Rahmenkonzept für Compliance-Systeme formuliert der Standard nicht, sondern verweist auf den Entscheidungsspielraum des Managements, sich zum Beispiel an die Guidelines von Transparency, der OECD, der DIHK etc. zu orientieren. Der Prüfer soll dann mit hinreichender Sicherheit eine Aussage treffen bezüglich:

1. Konzeptionsprüfung und Dokumentation des CMS (Auftragstyp 1);
2. Angemessenheitsprüfung und Implementierung (Auftragstyp 2);
3. Wirksamkeitsprüfung (Auftragstyp 3).

Hinsichtlich der Grundelemente eines Compliance Management-Systems orientiert sich IdW PS 980 an dem oben COSO-Framework.

Hinzu kommen die für die Praxis wichtigen Zertifizierungsmöglichkeiten gemäß den ISO-Normen, etwa ISO 37301 für „Compliance-Management-Systeme“, ISO 37002 für „Whistleblowing“ und ISO 37001 für „Anti-Korruptions-Management-Systeme“. ISO 37301 behält die Kernelemente des alten, bekannten ISO 19600 bei, gab jedoch nur Empfehlungen, wohingegen die neuen Regelungen tatsächlich Zertifizierungsnormen darstellen.¹¹

Der Nutzen solcher Prüfungen bzw. Zertifizierung wird vielfach als hoch eingeschätzt: Der Zertifizierungsprozess soll die Compliance-Kultur fördern, das Kontrollbewusstsein

¹¹Vgl. zum Beispiel Makowicz/Maciuca, in WPg 2020, S. 73 ff. und Wittmann/Jablowski/Berndt: CMS in Schweizer Unternehmen, Expert Focus 2021.

der Mitarbeiter stärken und die Strukturierung/Dokumentation der Elemente des vorhandene Compliance Management-Systems vorantreiben. Insofern steht durchaus zunächst auch die Selbstinformation zum unternehmensindividuellen Stand des Systems im Vordergrund. Extern erhofft man sich neben Reputationsgewinnen („Tue Gutes und rede darüber“), einem erhöhten Vertrauen der Stakeholder des Unternehmens aber vor allem auch eine Reduzierung von Haftungsrisiken.

Auf der anderen Seite dürfen zahlreiche Herausforderungen bei der Zertifizierung nicht übersehen werden. Unklar ist etwa, ob die enthaftende Wirkung der Zertifizierung so weit reicht, wie von den Unternehmen erhofft. Hervorzuheben ist auch, dass IdW PS 980-Prüfungen nicht darauf ausgerichtet sind, Prüfungssicherheit über die tatsächliche Einhaltung von Regeln zu erlangen. In den Prüfungsbereich fällt also – quasi als ökonomische Kernkompetenz – die Prozessprüfung, nicht jedoch die juristische Würdigung eines einzelnen konkreten Sachverhaltes. Daher bietet der Standard inhaltlich auch wenig Neues; denn praktisch alle Compliance relevanten Detailbereiche wie etwa Kartellrecht, Steuerrecht, Börsenrecht, Antikorruption, Datenschutz, Exportkontrolle, Geldwäscherei, IT-Recht, Immaterialgüterrecht etc. sind nicht weiter konkretisiert. Unzweifelhaft zeigt IdW PS 980 im Ergebnis auf, dass Zertifizierung ernstgenommen einen interdisziplinären Ansatz unter Bezug von Juristen und IT-Spezialisten voraussetzt.

Große Bedeutung erlangt das Thema „Prüfung“ für die Nachhaltigkeitsberichte. Bisher hatten zahlreiche Unternehmen einzelne Kennzahlen, bestimmte Themen oder auch ganze Berichte extern prüfen lassen – dies aber nur freiwillig. Damit sollte u. a. die Verlässlichkeit in die Aussagen gesteigert und etwaigen Vorwürfen von „Greenwashing“ vorgebeugt werden. Die CSRD verlangt, wie zuvor beschrieben, neu eine Prüfungspflicht, zunächst eine so genannte „limited assurance“, später eventuell sogar eine „reasonable assurance“. Die bisher freiwillig durchgeführten Prüfungen basieren vor allem auf dem International Standard on Assurance Engagements (ISAE) 3000, der allerdings allgemein für betriebswirtschaftliche Prüfungen ausgelegt ist. Derzeit erarbeitet der Berufsstand auf internationaler Ebene einen International Standard on Sustainability Assurance (ISSA) 5000 „General Requirements for Sustainability Assurance Engagements“, dessen Entwurf bereits vorliegt. Dieser Prüfungsstandard wird künftig die Grundlage für die Prüfung von Nachhaltigkeitsberichten.

Aus Governance- und Compliance-Sicht ist zu raten, sich mit den dortigen – nach „limited“ und „reasonable“ assurance unterscheidenden – Anforderungen vertraut zu machen und vor allem auf die rechtzeitige Bereitstellung prüfbarer Informationen im Unternehmen zu drängen. Es erscheint nicht unrealistisch, dass zahlreichen Unternehmen die Einschränkung oder das Versagen des entsprechenden Prüfungsurteils versagt bleibt, nicht, weil die Unternehmen gar keinen Nachhaltigkeitsbericht erstellt hätten, sondern weil schlicht nicht hinreichend prüfbare Angaben vorliegen. Darüber hinaus finden sich in ISSA 5000 auch zahlreiche Formulierungsbeispiele, etwas welche qualitativen Beschreibungen vom Prüfer zurückzuweisen und insofern von den Unternehmen zu vermeiden wären.

2.6 Risikomanagement und IKS

Die Einhaltung von Regeln (gesetzlich vorgeschrieben oder freiwillig bestimmt, „hard law“ oder „soft law“) erscheint zunächst eine Selbstverständlichkeit: Das Befolgen von Gesetzesnormen ist schlicht Ausdruck des Rechtsstaatsprinzips. Das Einhalten von Fachnormen oder freiwillig gesetzten Unternehmensleitlinien ist Ausdruck unternehmerischer Entscheidung und insofern auch konsequent zu beachten und umzusetzen. Hier zeigt sich die enge Verbindung zur Corporate Governance. Aus ökonomischer Sicht wird Compliance allerdings teilweise missverstanden als genereller Ansatz zur Verhinderung fehlerhafter Unternehmensentscheidungen. Dies kann – und soll – Compliance selbstverständlich nicht leisten. Vielmehr geht es um die Einbindung der Compliance in das allgemeine Risikomanagementsystem des Unternehmens.

Für Ökonomen wie Juristen gleichermaßen bedeutsam ist ein weiterer Aspekt der Compliance: Es geht sowohl um die Verantwortung des Gesamtunternehmens (Stichwort Unternehmensstrafrecht, Organisationsversagen), als auch die Verantwortung jedes einzelnen Mitarbeiters. Dies ist auch der Grund, weshalb oft von einer **Compliance-Kultur** als Ausdruck einer spezifischen Unternehmenskultur gesprochen wird. Diese Kultur soll zugleich dazu beitragen, den Fokus stärker auf die Prävention zu legen und so Lähmungen der Geschäftsprozesse durch allfällige externe oder interne Untersuchungen oder Reputationsverluste zu vermeiden. Gerade in den vielfältigen tatsächlichen (oder auch nur angeblichen) Unternehmensskandalen hat sich gezeigt, dass weniger fehlende Regelungen oder Ressourcen zur Überwachung das Problem darstellten, sondern eine falsche (oder von einzelnen Personen falsch verstandene) Unternehmenskultur einhergehend mit ineffektiven Kontrollprozessen.

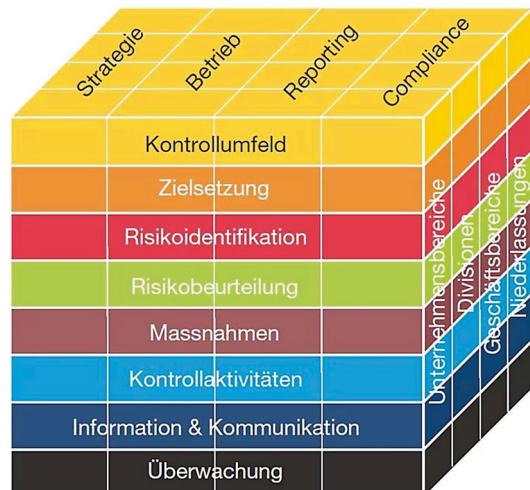
Umstritten aus rechtlicher wie ökonomischer Sicht ist die **Reichweite der Compliance-Risiken** und damit die Frage der Verantwortlichkeit: Selbstverständlich sind die Compliance-Risiken innerhalb einer Gesellschaft in den verschiedenen Abteilungen zwar unterschiedlich (etwa Einkauf, Vertrieb, Rechnungslegung, IT, ESG etc.) aber sämtliche in der Verantwortung des Unternehmens. Das gleiche, wenngleich schwerer zu implementieren, gilt grundsätzlich auch für Konzernstrukturen. Unter Compliance-Gesichtspunkten kann es keinen Unterschied machen, ob etwa eine unselbstständige Vertriebsabteilung besteht oder mehrere rechtlich selbstständige aber aufgrund der Konzernzugehörigkeit eben wirtschaftlich abhängige Vertriebsgesellschaften. Allerdings steigen die betriebswirtschaftlichen Herausforderungen etwa der Datenbeschaffung, Datenqualität, Zugriffsmöglichkeiten auf IT-Systeme und Weisungsbefugnisse gegenüber Mitarbeiter etc. in solchen (komplexen) Konzernstrukturen nicht unerheblich. Die Reichweite der Compliance-Risiken geht in der Praxis, wie LkSG bzw. CSDDD zeigen – aber tatsächlich noch viel weiter und erstreckt sich auch über Konzerngrenzen hinweg auf die (gesamte) Lieferanten- oder Wertschöpfungskette. Damit werden häufig die Compliance-Anforderungen multinationaler

Großkonzerne auch auf kleine und mittelständische Zulieferbetriebe überwälzt, umgekehrt die Compliance-Risiken von KMU zu denen der Konzerne.

Eine besondere Bedeutung bei der Sicherstellung der Compliance kommt der **Rechnungslegung** zu; denn Zahlungen zur Auftragserlangung oder für betrügerische Handlungen führen regelmäßig zur Verfälschung der Buchführung und gegebenenfalls zur unrichtigen Darstellung der Vermögens-, Finanz- und Ertragslage einer Gesellschaft. „Schwarze Kassen“ – selbst wenn sie „nur“ für Zwecke des Unternehmens und nicht für private Zwecke einzelner Mitarbeiter eingesetzt werden – entziehen regelmäßig dem Unternehmen den Zugriff auf eben dieses Vermögen, sind nicht ordentlich verbucht, nicht in den Konsolidierungssystemen ordnungsgemäß erfasst und führen damit (mindestens indirekt) zu einem Schaden der Gesellschaft. Viele Compliance-Verstöße ziehen daher bilanz- und/oder steuerrechtliche Verstöße nach sich. Es ist zwingende Aufgabe des Aufsichtsrates, die ordnungsmäßige Überwachung der Einhaltung von Compliance-Verstößen sicherzustellen, weswegen ein mangelhaftes Compliance Management-System oder ein mangelhaftes Internes Kontrollsyste (IKS) eine Verletzung der Sorgfaltspflichten des Aufsichtsrates darstellen kann. Kurz gesagt: Das bloße Vorhandensein eines irgendwie ausgestalteten Compliance-Systems reicht zur Enthaltung im Einzelfall nicht aus, es muss auch effektiv (und effizient) funktionieren. Und da in der Konzernwirklichkeit typischerweise über 99 % sämtlicher Informationen elektronisch vorliegen, setzt ein insgesamt funktionierendes Compliance-System immer auch eine funktionierende IT-Compliance voraus.

Die enge Verknüpfung der Compliance zur Rechnungslegung, dem Risikomanagement und dem Internen Kontrollsyste zeigt sich besonders gut am weit verbreiteten so genannten COSO-Würfel oder **COSO-Rahmenkonzept** (Abb. 2.2):

Abb. 2.2 COSO-Rahmenkonzept



Das US-amerikanische Committee of Sponsoring Organizations (COSO) definiert interne Kontrolle als ein vom Aufsichtsrat, dem Management und anderem Personal ausgeübten Prozess, welcher so ausgestaltet ist, dass er angemessene Sicherheit bezüglich der Erreichung der Ziele in den Bereichen Wirtschaftlichkeit und Effizienz des Betriebes, Zuverlässigkeit der Finanzberichterstattung sowie Einhaltung von anwendbaren Recht und Vorschriften bietet. Standen nach den Bilanzskandalen wie Enron, Worldcom, Xerox etc. und der darauf folgenden Regulierungswelle (zum Beispiel Sarbanes-Oxley Act) zunächst die Anstrengungen zur Verbesserung der Finanzberichterstattung im Vordergrund, gewinnt das Rahmenkonzept jetzt mehr und mehr an Bedeutung für die Implementierung von Compliance-Systemen, wie auch der zuvor erwähnte IDW PS 980 zeigt. Letztlich finden sich – so, oder so ähnlich – die Elemente „Kontrollumfeld“, „Risikobeurteilung“, „Kontrollaktivitäten“, „Information & Kommunikation“ sowie „Überwachung“ auch bei jedem Compliance Management-System wieder. In Zukunft wird diese Struktur auch bei der Implementierung der Nachhaltigkeitsthematik von großer Bedeutung sein.

Das Risikomanagementsystem nach dem COSO-Würfel ist in der Folgezeit weiterentwickelt worden, in den Kernbestandteilen jedoch identisch geblieben. Wichtig war insbesondere der Schritt hin zu einer Prinzipienorientierung 2013 (Abb. 2.3):¹²

Während zuvor insbesondere die Bedeutung des Risk Assessment-Prozesses hervorgehoben wurde, und dort vor allem die Bestimmung von Eintretenswahrscheinlichkeit und Schadensausmaß des Risikos, wird nunmehr das Kontrollumfeld besonders betont und damit der „Ton-of-the-Top“. Wichtig ist sich klarzumachen, dass letztlich die Unternehmenskultur die Vorgaben und Verantwortlichkeiten der Unternehmensleitung, deren

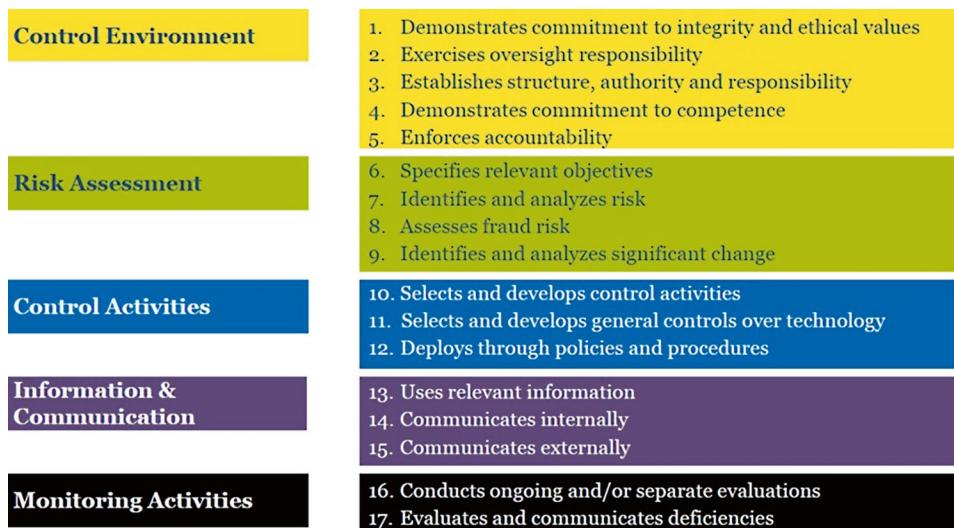


Abb. 2.3 Prinzipienorientierung 2013

¹²Vgl. COSO 2013 – Internal Control – Integrated Framework.

eigene Risikoneigung die weitere Ausgestaltung des Risikomanagementsystems prägen. Und letztlich bestimmt damit die Qualität des Risikomanagementsystems auch die Qualität des Compliance-Management-Systems.

Ein zentraler ökonomischer Aspekt der Compliance in Zusammenhang mit dem Riskmanagement ist auch die Frage nach der Effektivität, der Wirksamkeit und damit nach der **Qualität**. Im Rahmen des Internal Audits sind dazu Methoden entwickelt worden, digital erfasste Prozesse mittels Massendatenanalyse zu prüfen und zu bewerten. Dies ermöglicht ein konzernweites Screening, sofern freilich zunächst geeignete Indikatoren ermittelt wurden. Entscheidend ist, dass die Compliance relevanten Indikatoren regelmäßig erhoben werden können, das spezifische Compliance-Risiko auch abbilden und auch die Tauglichkeit möglicher Maßnahmen wiederum erfasst und gemessen werden kann. Für eine Vielzahl von Einkaufs- und Absatzaktivitäten ist dies möglich, sofern diese Transaktionen etwa im SAP- oder Oracle-Umfeld erfasst werden. Will man klassische Umsatzgeschäfte auf ihre Compliance-Risiken hin analysieren, so bieten sich als geeignete Indikatoren zum Beispiel die Bartransaktionen an, das manuelle Auslösen von Zahlungen, das Buchen von Zahlungen über ein CpD-Konto, die Auszahlung ohne korrespondierende ordnungsmäßige Bestellung etc. Aus dieser Analyse lassen sich dann konzernintern Vergleichszahlen etwa über verschiedene Perioden oder Regionen oder Geschäftsbereiche generieren.

2.7 Corporate Governance und „Three Lines“

Effektive Corporate Governance bedingt das koordinierte Zusammenarbeiten verschiedener Überwachungs- und Kontrollfunktion im Unternehmen. Aus Sicht der Compliance gilt es insbesondere der Gefahr einer „Eigendynamik“ einzelner Organisationseinheiten (Tochtergesellschaften, Bereiche, Regionen, Business Units etc.) entgegenzuwirken, die sich voneinander abgrenzen, deren Handeln wenig koordiniert und nicht aufeinander abgestimmt ist. Es drohen dann isolierte „Insellösungen“, die einem einheitlichen Compliance Risk-management System zuwiderlaufen und entweder zu Doppelpurigkeiten führen, weil verschiedene Organisationseinheiten jeweils eigene Lösung entwickeln, was offenkundig ineffizient ist. Oder, schlimmer, es drohen Kontrolllücken, weil entweder der Gesamtüberblick über getroffene Maßnahmen verloren gegangen ist oder weil manche Organisationseinheiten sich unrichtigerweise darauf verlassen, dass andere (übergeordnete) Einheiten bestimmte Aktivitäten schon vornehmen werden („Lean-Back-Syndrom“). In diesem Falle ist das System dann vor allem ineffektiv, also letztlich nicht im angemessenen Maße wirksam.

Das ursprünglich so genannte und maßgeblich vom Institute of Internal Auditors (IIA) mit entwickelte „Three Lines of Defense“-Modell hat die organisatorische Struktur des Risikomanagements innerhalb der Unternehmen entscheidend geprägt. Um das nicht akzeptable inhärente Risiko, also das Risiko, dass ohne Berücksichtigung irgendwelcher inneren Kontrollen Geschäftsvorfälle, Sachverhalte etc. fehlerbehaftet sind, auf ein gemessen am Risikoappetit akzeptables, vertretbares, managebares Risiko zu verringern, sind drei „Verteidigungslinien“ definiert worden. Die Verteidigungslinien erfüllen quasi eine „Filterfunktion“, wobei jeder Linie eine klare Verantwortlichkeit zugemessen wird und die einzelnen Risiko- und Kontrolleinheiten in ein einheitliches Governance-System eingebettet sind.

Die 1. Verteidigungslinie umfasst die „Business Operations“. Das operative Management ist verantwortlich für die Beurteilung, Kontrolle und Risikoreduzierung der sich aus dem operativen Geschäft ergebenen Risiken. Die 2. Verteidigungslinie beinhaltet Unterstütztätigkeit zur Steuerung und Überwachung des operativen Geschäfts. Typischerweise zählen hierzu etwa die Legal- und Compliance-Abteilung, das Reporting, Qualitätssicherung oder auch Risikomanagementabteilungen, die die Methoden und Verfahren für das Risikomanagement festlegen. Die Interne Revision („Internal Audit“) ist die 3. Verteidigungslinie und die erste Linie, die prozessunabhängig ist. Sie überprüft die Tätigkeiten der beiden ersten Linien insbesondere hinsichtlich der Angemessenheit und Effektivität der internen Kontrollen und Prozesse und gibt ihre unabhängige Einschätzung – je nach Unternehmensorganisation – an die Geschäftsleitung und/oder das Überwachungsorgan (Aufsichtsrat oder Verwaltungsrat). Insgesamt soll so sichergestellt werden, dass die Risiken entsprechend der vorgegebenen Ziele effektiv und effizient identifiziert, beurteilt und gemanagt werden.

Das zuvor skizzierte „Three Lines of Defense“-Modell ist 2020 zu einem eher prinzipienorientierten „Three Lines“-Modell weiterentwickelt worden (Abb. 2.4):¹³

Das IIA Drei- Linien-Modell

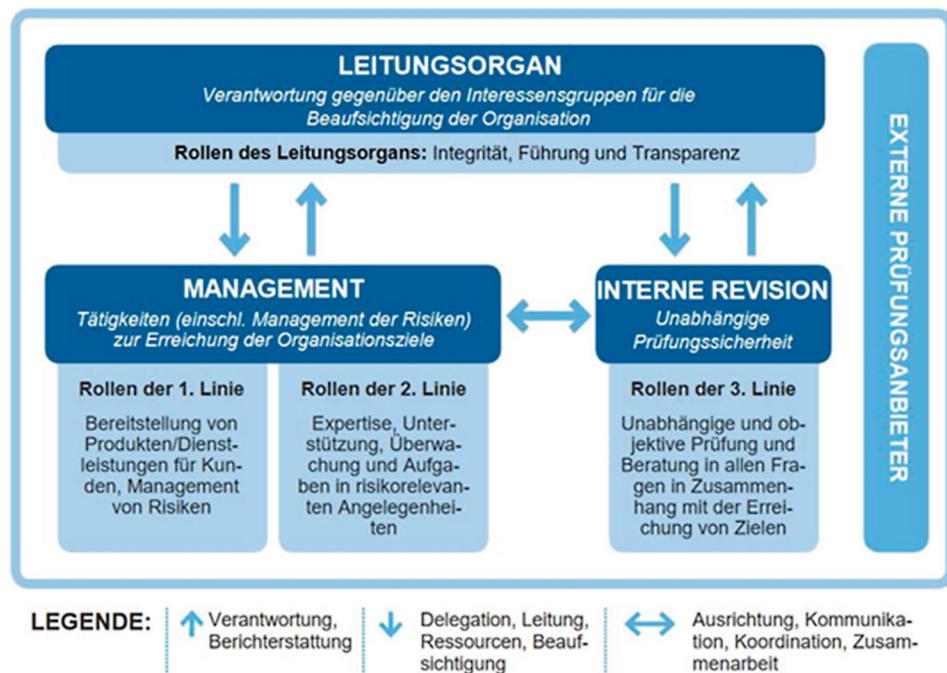


Abb. 2.4 Das IIA Drei-Linien-Modell

¹³Vgl. <https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf> (aufgerufen am 7.2.2024).

Es handelt sich dabei nicht um eine grundlegende Änderung des Modells, sondern vor allem um eine Klarstellung: Die „Linien“ sollen nicht als starre, formale Organisationselemente missverstanden werden, sondern vielmehr „Rollenbilder“ definieren; die Linien unterscheiden sich also primär in den unterschiedlichen Rollen, die ihnen in der gesamten Governance-Struktur zukommen.

2.8 Fraud

Nach der Definition der Association of Certified Fraud Examiner (ACFE) umfasst der Begriff „Fraud“ die Bereiche Korruption, Vermögensschäden und betrügerische Unternehmensberichterstattung. Die **Betrugshandlungen** können dabei entweder zum Nutzen der Gesellschaft durchgeführt werden (etwa Bestechung zum Zwecke der Auftragserlangung, Kreditbetrug) oder zu Lasten des Unternehmens (zum Beispiel Veruntreuung von Geldern). Angesichts der hohen Dunkelziffer liegt es auf der Hand, dass nur schwer verlässliche Zahlen über die tatsächlichen Kosten von Betrugshandlungen ermittelt werden können. Einige Anhaltspunkte liefern die zahlreichen Befragungen, wie sie etwa von den großen Wirtschaftsprüfungsgesellschaften durchgeführt werden (zum Beispiel PwC Economic Crime Survey, EY Fraud Survey). Allen diesen Umfragen ist gemein, dass es erhebliche Unterschiede in den Schadensursachen, den Schadensausmaßen, den Regionen, in denen die Schäden primär entstehen, den Gründen für die Aufdeckung dieser kriminellen Handlungen, den Strafzahlungen etc. gibt. Trotz dieses heterogenen Bildes können die vorhandenen Erkenntnisse für die praktische Ausgestaltung des Compliance Management-Systems genutzt werden: Sie erhellen durchaus das Kontrollumfeld, in dem das Unternehmen tätig ist und erleichtern die Beurteilung von Compliance-Risiken. Das gilt etwa, wenn zu beurteilen ist, ob in bestimmten Regionen, in denen das Unternehmen tätig ist, ein besonderes Korruptionsrisiko besteht, ob bestimmte Vertriebsaktivitäten (etwa durch Hinzuziehen von Business Consultants) risikobehafteter sind, spezifische Geschäftsmodelle (Forschung, IT, Pharmazie, Finanzdienstleistungen etc.) spezifische Compliance-Risiken nach sich ziehen oder in bestimmten Regionen erhöhte Risiken von Kinderarbeit in der Lieferkette drohen.

In Zusammenhang mit den wirtschaftskriminellen Handlungen rücken immer mehr auch die **Folgeschäden** in den Mittelpunkt des Interesses: Neben die eigentlichen Vermögensschäden und Strafzahlungen treten etwa die Kündigung langfristiger Geschäftsbeziehungen oder das Ausscheiden wichtiger Mitarbeiter als bedeutsame Schäden. Die Unternehmensreputation leidet, neue Mitarbeiter können schwerer gewonnen werden, die Zusammenarbeit mit Regulatoren und Aufsichtsbehörden gestaltet sich schwieriger. Die institutionellen Investoren üben einen aktiveren Einfluss auf das Unternehmen aus. Teilweise werden Unternehmen von öffentlichen Aufträgen ausgeschlossen.

Vor dem Hintergrund der direkten und indirekten Schäden ist der Aspekt der Prävention zentral. Dies versucht man auf der einen Seite durch entsprechende Überwachungsprozesse und technische Maßnahmen zu erreichen, andererseits durch die Auswahl des entsprechenden Personals. Daher hat man das Verhalten von Wirtschaftskriminellen

analysiert, um die Ursachen ihrer Handlungen besser zu verstehen. Nach dem weit verbreiteten „**Fraud Triangle**“ von Cressey sind es letztlich immer drei Faktoren, die das Verhalten von Missetätern bestimmen:¹⁴ Die Möglichkeit, überhaupt solche wirtschaftskriminellen Handlungen durchführen zu können. Der Druck, dem die Täter sich ausgesetzt sahen. Und schließlich die innere Einstellung, in dem das eigene Handeln vor sich selbst gerechtfertigt wurde. Auch in empirischen Studien zeigt sich, dass etwa der Druck bzw. die Angst, den Arbeitsplatz zu verlieren oder (völlig) unrealistische Planzahlen erreichen zu müssen, vielfach Ursache betrügerischer Handlungen ist. Und Möglichkeiten, die sich etwa aus schwachen Überwachungssystemen oder veränderten Rahmenbedingungen ergeben, gewähren mehr Gelegenheiten zu solchen Handlungen. Allerdings zeigen die Studien auch, dass letztlich praktisch jeder Mitarbeiter auch ein potenzieller Täter werden kann, wenn nur das subjektive Umfeld und der unternehmerische Rahmen entsprechend sind.

Auch wenn es banal erscheinen mag: Eine gute Unternehmenskultur, hohe Loyalität der Mitarbeiter zum eigenen Unternehmen und effektive Kontrollprozesse sind immer noch die beste **Prävention**. Befragt man Unternehmen, die Opfer von Betrugshandlungen geworden sind, so wird man regelmäßig das Ergebnis erhalten, dass bei entsprechender Sensibilisierung der Mitarbeiter solche Handlungen hätten verhindert oder früher aufgedeckt werden können. Dies gilt jedenfalls für die Vielzahl „typischer“ Betrugshandlungen, für die es mittlerweile ganze Kataloge oder Checklisten von „**Red Flags**“ gibt. Red Flags sind Anomalien/Auffälligkeiten und man kann drei verschiedene Bereiche unterscheiden: Verhaltensanomalien, etwa wenn einzelne Mitarbeiter durch bestimmte ungewöhnliche Aktivitäten auffallen. Analytische Anomalien, wie sie sich aus zunächst nicht erklärbaren Abweichungen zu spezifischen Kennzahlen oder aus ungewöhnlichen Zahlenmustern ergeben. Und schließlich organisatorische Anomalien. Kennzeichen hierfür sind zum Beispiel fehlende Transparenz, häufige Beschwerden, hohe Mitarbeiterrotation, schlechtes Arbeitsklima, mangelnde Ressourcenausstattung für Überwachungsprozesse.

Nachfolgend sind einige typische Red Flags aus dem **Beschaffungsbereich** aufgeführt:

- Einkaufspreise steigen höher als die Inflationskosten;
- Lieferanten, die nicht auf der zugelassenen Lieferantenliste stehen;
- Unbekannte Lieferanten – niemand in der gleichen Industrie kennt diese;
- Lieferanten mit einer „Postfach“ Adresse;
- Verdächtige Lieferantenrechnungen ohne entsprechende Angaben;
- Einkäufe ohne Auftragsbestätigung;
- Favorisierung eines bestimmten Lieferanten ohne erkennbaren Grund;

¹⁴Vgl. Donald Cressey, Other People's Money, Patterson Smith, New Jersey, 1973.

- Wirtschaftlicher Nutzen für den Einsatz des Lieferanten ist unklar;
- Person, die bestellt, bestätigt auch zugleich die Lieferantenrechnung;
- Kontinuierliche Akzeptanz von „high-price low-quality“ Waren/Dienstleistungen.

Aus der Erfahrung des Unternehmens lassen sich so in praktisch allen Unternehmensbereichen und für spezifische Unternehmenssituationen (etwa M & A-Transaktionen) entsprechende Red Flags identifizieren und geeignete Richtlinien und Kontrollprozesse implementieren. Für den zuvor angesprochenen Beschaffungsbereich könnte dies zum Beispiel bedeuten:

- Alle neuen Lieferanten müssen bewilligt werden.
- Es gibt eine klare Pflichten- und Aufgabentrennung.
- Der Zugang und die Erlaubnis, um neue Lieferanten im IT-System anlegen zu können oder bestehende zu modifizieren, ist limitiert.
- Es sind klare Einkaufsvorschriften etabliert.
- Die Einkäufer sollte alle x Jahre gewechselt oder die Lieferverträge wieder neu ausgeschrieben werden.
- Lieferanten sind davon in Kenntnis zu setzen, dass Geschenke an das Einkaufspersonal verboten sind und an Wohltätigkeitsorganisationen gegeben werden.
- Whistleblowing-Hotlines existieren und auch jeder Lieferant und sämtliche Mitarbeiter haben Zugang dazu.
- Es ist sicherzustellen, dass alle Verträge von min. zwei Personen unterschrieben sind (Vier-Augen-Prinzip).
- Es existiert ein Trainingsprogramm zur Deliktsprävention.

Man erkennt, dass ein gutes, effizientes Compliance Management-System zwingend das Verständnis von den unternehmerischen Abläufen und Prozessen voraussetzt und daher nur im interdisziplinären Zusammenspiel von Juristen, Ökonomen und – entscheiden für die Implementierung – IT-Spezialisten umgesetzt werden kann.

2.9 Kultur

Die Unternehmenskultur als wichtiger betriebswirtschaftlicher Aspekt spielt insbesondere in der Abgrenzung von „klassischen“, regelorientierten Compliance Management-Systemen und wert- bzw. kulturorientierten Integrity Management-Systemen eine zentrale Rolle. Während ersteres insbesondere durch gesetzliche Vorgaben getrieben und auf die Vermeidung von Gesetzesverstößen gerichtet ist, will letzteres durch intrinsische Motivation der Mitarbeiter deren moralisches Handeln fördern. Beide Ansätze schließen sich selbstverständlich nicht aus und ein etabliertes Compliance Management-System ist schon allein aufgrund der vielfachen gesetzlichen Anforderungen (Dokumentationsnachweise

etc.) zwingend erforderlich. Jedoch hängt dessen Effizienz und Effektivität nicht zuletzt von der gelebten Praxis der Mitarbeiter ab, die wiederum maßgeblich durch gemeinsame und gelebte Werte bestimmt wird. Ein glaubwürdiges Auftreten gegenüber Geschäftspartnern nach außen oder eine „speak-up-policy“ nach innen lassen sich durch eine einheitlich gelebte integre Unternehmenskultur regelmäßig besser realisieren, als etwa durch Regelbefolgung aufgrund der bloßen Tatsache, dass Compliance vielleicht Bestandteil der Bonusvereinbarung ist.

Allgemein lassen sich (mindestens) vier Dimensionen identifizieren, die eine Unternehmenskultur prägen: Zum einen ist dies das Geschäftsmodell und damit das ökonomische Umfeld. Zum anderen prägt auch das regulatorische Umfeld (Gesetze, Aufsichts- und Regulierungsbehörden etc.) die Kultur. Drittens sind das individuelle Denken, Handeln und Verhalten prägend. Und schließlich, viertens, wirken natürlich die allgemein akzeptierten Werte und die „Ethik“ auf die Kultur. Es ist offensichtlich, dass insbesondere in internationalen Konzernstrukturen oder bei internationalen Geschäftspartnern und Lieferketten die jeweiligen Dimensionen gänzlich anders ausgeprägt sein können und jeweils differenzierte Compliance-Strukturen erfordern. Für die Ausgestaltung eines Compliance-Riskmanagement-Systems ist es von entscheidender Bedeutung, ob der Compliance-Officer auf ein Umfeld trifft, dass für die Abwägung, ob Korruptionshandlungen zur Auftragserlangung ergriffen werden sollten oder nicht, kurzfristige, ökonomische Kosten-Nutzen-Überlegungen für maßgeblich hält. Oder aber auf ein Umfeld, dass korruptive Handlungen als Geschäftspraxis aufgrund allgemein akzeptierter moralischer, ethischer Werte generell ablehnt und daher auch in den jeweiligen konkreten Einzelfällen stets zum Ergebnis käme, dass solche Handlungen nicht zu tolerieren sind.

2.10 Schluss

Ohne Zweifel: Die Komplexität Compliance-relevanter Regulierung hat in den letzten Jahren unglaublich zugenommen und wird dies unter dem Stichwort „ESG“ auch in Zukunft. Da diese Regelungen an tatsächliche unternehmerische Abläufe und Gegebenheiten anknüpfen bzw. in diese einzubinden sind (Informationserhebung, Bewertungen, Risikomanagement, Lieferketten, Sorgfaltspflichten etc.) ist ein gewisses betriebswirtschaftliches Verständnis des Compliance Officers für seine Akzeptanz von großer Bedeutung. Denn faktisch kann es auf die Fragestellung, ob sich Unternehmen entweder regelkonform verhalten **oder** nicht doch lieber Geschäfte machen sollen, nur eine Antwort geben: Sie müssen sich regelkonform verhalten **und** Geschäfte machen. Compliance wird zu einem zentralen Wettbewerbsfaktor werden, zu einem „Business Enabler“ – und ESG-Compliance eines der großen Zukunftsfelder für die Tätigkeit der Compliance-Officer.



Professor Dr. Thomas Berndt ist ordentlicher Professor für Rechnungslegung an der Universität St. Gallen und Direktor am dortigen Institut für Law & Economics (ILE-HSG). Im Rahmen der universitären und außeruniversitären Aus- und Weiterbildung lehrt und forscht er in verschiedenen Bereichen der finanziellen Führung von Unternehmen, insbesondere der nationalen und internationalen Rechnungslegung sowie der Konzernrechnungslegung, der Unternehmensbewertung, der finanziellen und nichtfinanziellen Berichterstattung sowie der Corporate Governance und der Corporate Compliance. Er ist u. a. Mitglied der European Accounting Association (EAA), der American Accounting Association (AAA) und der Schmalenbach-Gesellschaft für Betriebswirtschaft e. V. Darüber hinaus ist er Mitglied des Fachbeirats der „Zeitschrift für Corporate Governance“ (ZCG), des „Betriebs-Berater – Zeitschrift für Recht und Wirtschaft“ (BB) und des Center for Corporate Reporting (CCR). 2014 wurde er zum Mitglied der Prüfungskommission für Wirtschaftsprüfer bestellt. Thomas Berndt ist Verwaltungsratsmitglied der equia AG, Schweiz und als Fachgutachter tätig.

Teil II

Compliance-Risiken



Anti-Korruption

3

Christian Pelz

Inhaltsverzeichnis

3.1 Einleitung	42
3.2 Rechtslage in Deutschland	44
3.2.1 Übersicht	44
3.2.2 Wesentliche Merkmale von Korruptionsdelikten	46
3.2.2.1 Vorteil	46
3.2.2.1.1 Materielle und immaterielle Vorteile	46
3.2.2.1.2 Drittvorteile	47
3.2.2.2 Unrechtsvereinbarung	47
3.2.2.2.1 Amtsträgerkorruption	48
3.2.2.2.2 Korruption im privaten Sektor	51
3.2.2.2.3 Bestechung und Bestechlichkeit im Gesundheitswesen	53
3.2.2.2.4 Mandatsträgerkorruption	53
3.2.2.2.5 Arbeitnehmervertreter	54
3.2.2.2.6 Sozialadäquate Zuwendungen	54
3.2.2.3 Tathandlung	54
3.2.3 Korruptionsstraftaten im Ausland	55
3.2.3.1 Amtsträgerkorruption	56
3.2.3.2 Mandatsträgerkorruption	57
3.2.3.3 Angestellte und Beauftragte im privaten Sektor bzw. von Heilberufen	57
3.3 Ausländische Rechtsvorschriften	57
3.3.1 Überblick	57
3.3.2 UK Bribery Act 2010	58
3.3.3 Der Foreign Corrupt Practices Act der USA	59
3.3.4 Sonstige ausländische Rechtsvorschriften	60

C. Pelz (✉)

Noerr, München, Deutschland

E-Mail: christian.pelz@noerr.com

3.4 Anforderungen an Compliance	61
3.4.1 Notwendigkeit eines Compliance-Systems	61
3.4.2 Risikoanalyse	62
3.4.3 Richtlinien und Policies	63
3.4.3.1 Inhalt von Richtlinien	63
3.4.3.2 Branchenregelungen oder Richtlinien	64
3.4.3.3 Wesentliche Policies	64
3.4.3.3.1 Geschenke und Einladungen	64
3.4.3.3.2 Spenden und Sponsoring	67
3.4.3.3.3 Berater und Vermittler	68
3.4.4 Geschäftspartner, Joint Venture und M&A Due Diligence	69
3.4.5 Schulungen und Trainings	70
3.4.6 Hinweisgebersysteme	71
3.4.7 Audits und interne Untersuchungen	71
3.4.8 Reaktion auf entdecktes Fehlverhalten	72
3.4.9 Strafanzeige und Offenbarung gegenüber Ermittlungsbehörden	72
Literatur	73

3.1 Einleitung

Über viele Jahrzehnte wurde Korruption, zumindest wenn sie im Ausland begangen wurde, als ein legitimes Mittel angesehen, um wirtschaftlich erfolgreich tätig sein zu können.¹ Schmiergelder konnten zudem steuerlich als Betriebsausgaben abgesetzt werden. Doch die Zeiten haben sich geändert. Korruption gehört heute zu den weltweit verpönten Geschäftspraktiken. Internationale Übereinkommen der Vereinten Nationen,² der OECD,³ des Europarats⁴ oder anderer internationaler Institutionen⁵ fordern eine konsequente Verfolgung von Korruptionsdelikten. Fortschritte der Staaten im Kampf gegen Korruption werden sowohl von der EU, den Vereinten Nationen, GRECO⁶ oder anderen internationalen und zwischenstaatlichen Organisationen als auch durch NGOs, an vorderster Stelle Transparency International, überwacht.

¹ BGH NJW 1964, 966; 1985, 2405.

² Übereinkommen der Vereinten Nationen gegen Korruption vom 31.10.2003, http://www.unodc.org/pdf/crime/convention_corruption/signing/Convention-e.pdf (aufgerufen am 23.8.2024).

³ OECD-Übereinkommen über die Bekämpfung der Bestechung ausländischer Amtsträger im internationalen Geschäftsverkehr vom 17.12.1997, <https://www.oecd.org/en/topics/fighting-foreign-bribery.html> (aufgerufen am 23.8.2024).

⁴ Strafrechtsübereinkommen über Korruption vom 17.12.1997, <http://conventions.coe.int/Treaty/GER/Treaties/Html/173.htm> (aufgerufen am 23.8.2024); Zivilrechtsübereinkommen über Korruption vom 4.11.1999, <http://conventions.coe.int/Treaty/GER/Treaties/Html/174.htm> (aufgerufen am 23.8.2024).

⁵ Vgl. Androulakis, Die Globalisierung der Korruptionsbekämpfung, S. 118 ff.

⁶ <http://www.coe.int/t/dghl/monitoring/greco/> (aufgerufen am 23.8.2024).

Als Folge dieser internationalen Entwicklung sind seit dem Jahr 1999 auch in Deutschland die Strafvorschriften zur Korruptionsbekämpfung immer mehr erweitert worden. Neben der Bestechung deutscher Amtsträger ist auch diejenige ausländischer Amtsträger, ebenso die Bestechung im privaten Sektor im Ausland unter Strafe gestellt. Daneben wurden Strafvorschriften über die Bestechung im Gesundheitssektor eingeführt sowie diejenigen über die Bestechung von Mandatsträgern erheblich erweitert. Schmiergelder sind seit dem Jahr 1999 nicht mehr steuerlich abzugsfähig (§ 4 Abs. 5 Satz 1 Nr. 10 EStG).

Neben kartellrechtlichen Verstößen gehören Korruptionshandlungen zu den Rechtsverletzungen, bei denen die höchsten Sanktionen gegen Unternehmen verhängt werden. Verbundsgeldebußen können schnell dreistellige Millionenbeträge erreichen (Tab. 3.1).

Die Verfolgung von Korruptionsdelikten ist bereits seit einigen Jahren ein Schwerpunkt der Finanz- und Ermittlungsbehörden, nicht zuletzt aufgrund fiskalischer Erwägungen, da bei Versagung des Betriebsausgabenabzugs und infolge der hohen Unternehmensgeldebußen der Ermittlungsaufwand besonders lohnend ist. Das Bundeslagebild Korruption des Bundeskriminalamts für das Jahr 2022 zeigt, dass ungeachtet der verschiedenen Korruptionsskandale weiterhin eine hohe Anzahl an Ermittlungsverfahren zu verzeichnen ist (Abb. 3.1).

Tab. 3.1 Geldebußen wegen Korruptionsdelikten in Deutschland

Geldbußen wegen Korruptionsdelikten in Deutschland	
Siemens (2007)	201 Mio. €
Siemens (2008)	395 Mio. €
MAN (2009)	150,6 Mio. €
Ferrostaal (2011)	149 Mio. €
Linde (2011)	35 Mio. €
Rheinmetall (2014)	37,07 Mio. €
Atlas Elektronik (2017)	48 Mio. €

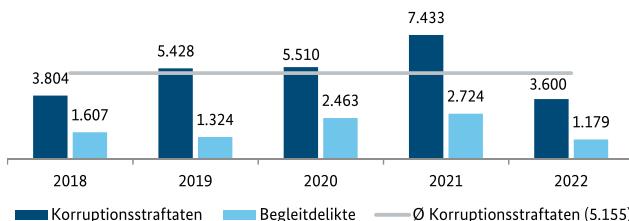


Abb. 3.1 Entwicklung der Verfahrenszahlen 2018–2022 (Bundeskriminalamt Bundeslagebild Korruption 2022, 4)

Aus diesen Gründen überrascht es nicht, dass Korruption eines der Topthemen ist, mit denen sich eine Compliance-Organisation, insbesondere bei international tätigen Unternehmen, nahezu zwingend befassen muss. Die Verwicklung eines Unternehmens in Korruption hat meist einen erheblichen Reputationsverlust gegenüber der Öffentlichkeit, bei Investoren und Anteilseignern, aber auch gegenüber Geschäftspartnern und Mitarbeitern zur Folge, der gravierende Auswirkungen auf die wirtschaftliche Entwicklung nehmen kann. Angesichts des Umstands, dass bei Korruptionsdelikten nicht nur Unternehmensgeldbußen oder Unternehmensstrafen und die Abschöpfung erlangter Vorteile drohen, sondern darüber hinaus Korruptionsdelikte auch zum Ausschluss von öffentlichen Auftragsvergaben oder zum Blacklisting bei internationalen Organisationen führen können, mit entsprechend weitreichenden Folgen, ist es verständlich, dass ein effektives Compliance-Management in diesem Bereich für alle Unternehmen ein Muss ist.

3.2 Rechtslage in Deutschland

3.2.1 Übersicht

In Deutschland gibt es eine Vielzahl von Strafvorschriften, die Korruption oder korruptionsähnliche Verhaltensweisen verbieten. Im Kernbereich der Korruptionsdelikte wird nach der Funktion des Empfängers differenziert: So gibt es Strafvorschriften in Bezug auf Korruption gegenüber Amtsträgern, Mandatsträgern, Angestellten und Beauftragten im privaten Bereich, im Gesundheitssektor sowie von Arbeitnehmervertretern. Daneben existiert noch eine Vielzahl weiterer Bestimmungen, die korruptive Handlungen mit Geldbuße bedrohen.⁷ In aller Regel begeht sowohl der Geber als auch der Nehmer eine Rechtsverletzung, sodass es fast immer zu einer spiegelbildlichen Strafbarkeit bzw. Ahndbarkeit kommt. Die wesentlichen Strafvorschriften sind im umseitig abgedruckten Schaubild dargestellt (Tab. 3.2, nächste Seite):

Die Auslandsbestechung ist in vielen, aber nicht in allen Fällen⁸ auch nach deutschem Recht mit Strafe bedroht.⁹ Voraussetzung ist hierbei aber meist, dass die Tathandlung entweder ganz oder teilweise in Deutschland vorgenommen wurde, der Taterfolg in Deutschland eingetreten oder aber der Täter Deutscher ist.¹⁰ In Ausnahmefällen ist bei reinen Auslandstaten auch nach § 7 Abs. 2 Nr. 2 StGB eine Strafverfolgung von Ausländern möglich (Tab. 3.3, nächste Seite).

⁷Zum Beispiel § 81 Abs. 3 Nr. 2 i. V. m. § 21 Abs. 2 GWB, § 405 Abs. 3 Nr. 2, 6, 7 AktG, § 152 Abs. 1 GenG, § 23 Abs. 1 Nr. 3, 4 SchVG.

⁸So ist bspw. die Vorteilsgewährung (§ 333 StGB) an ausländische Amtsträger weitgehend nicht strafbar. Eine Strafbarkeit der Nehmerseite bei Vorteilsannahme besteht lediglich in Bezug auf Richter ausländischer oder internationaler Gerichte.

⁹Unabhängig davon besteht in den meisten Fällen auch eine Strafbarkeit nach dem jeweils anwendbaren ausländischen Recht.

¹⁰Pelz, Die Bekämpfung der Korruption im Auslandsgeschäft, StraFo 2000, 300.

Tab. 3.2 Geberseite vs. Nehmerseite

Geberseite	Nehmerseite
Amtsträger	
Vorteilsgewährung, § 333 StGB	Vorteilsannahme, § 331 StGB
Bestechung, § 334 StGB	Bestechlichkeit, § 332 StGB
Mandatsträger	
Mandatsträgerbestechung, § 108e Abs. 2 StGB; Unzulässige Interessenwahrnehmung, § 108f Abs. 2 StGB	Mandatsträgerbestechlichkeit, § 108e Abs. 1 StGB; Unzulässige Interessenwahrnehmung, § 108f Abs. 1 StGB
Angestellte und Beauftragte	
Bestechung im geschäftlichen Verkehr, § 299 Abs. 2 StGB	Bestechlichkeit im geschäftlichen Verkehr, § 299 Abs. 1 StGB
Bestechung im Gesundheitswesen, § 299b StGB	Bestechlichkeit im Gesundheitswesen, § 299a StGB
Arbeitnehmervertreter	
Straftaten gegen Betriebsverfassungsorgane und ihre Mitglieder, § 119 Abs. 1 Nr. 3 BetrVG	n. a.

Tab. 3.3 Auslandsbestechung

Auslandsbestechung	
Geberseite	Nehmerseite
Amtsträger	
Bestechung ausländischer oder internationaler Bediensteter, § 335a Abs. 1 StGB	Bestechlichkeit ausländischer oder internationaler Bediensteter, § 335a Abs. 2, 3 StGB
Vorteilsgewährung an ausländische oder internationale Bedienstete, § 335a Abs. 1–3 StGB	Vorteilsannahme von ausländischen oder internationalen Richtern, § 335a Abs. 1 StGB
Mandatsträger	
Mandatsträgerbestechung § 108e Abs. 2, 3 Nr. 4–6 StGB; Unzulässige Interessenwahrnehmung, § 108f Abs. 2 StGB	Mandatsträgerbestechlichkeit § 108e Abs. 1, 3 Nr. 4–6 StGB; Unzulässige Interessenwahrnehmung, § 108f Abs. 1 StGB
Angestellte und Beauftragte	
Bestechung im geschäftlichen Verkehr, § 299 Abs. 2 StGB	Bestechlichkeit im geschäftlichen Verkehr, § 299 Abs. 1 StGB
Bestechung im Gesundheitswesen, § 299a StGB	Bestechlichkeit im Gesundheitswesen, § 299b StGB

Ein typisches Begleitdelikt bei Korruptionsdelikten ist die Steuerhinterziehung nach § 370 AO, da Schmiergelder und vergleichbare Aufwendungen nach § 4 Abs. 5 Satz 1 Nr. 10 EStG vom Betriebsausgabenabzug ausgeschlossen sind, Schmiergeldzahlungen aber häufig als Provisionen, Beraterhonorare, Marketingaufwendungen o. ä. getarnt und verbucht werden.¹¹

¹¹ Pelz, Steuerliche und strafrechtliche Schritte zur Bekämpfung der Korruption im Auslandsgeschäft, WM 2000, 1566, 1567 f.; Sahan, Korruption als steuerstrafrechtliches Risiko, Festschrift für Erich Samson, 2010, S. 399 ff.

Darüber hinaus wird bei Schmiergeldzahlungen oder dem Unterhalten schwarzer Kas-¹²sen eine Untreuestrafbarkeit nach § 266 StGB in Betracht kommen,¹³ ebenso ggf. eine solche wegen Betrugs oder Geldwäsche.

3.2.2 Wesentliche Merkmale von Korruptionsdelikten

Wesentliches Merkmal aller Korruptionsdelikte ist das Anbieten oder Zuwenden eines Vorteils an einen Entscheidungsträger oder eine andere Person, damit dieser eine bestimmte Handlung oder Tätigkeit vornimmt oder die Entscheidungsfindung bzw. das Entscheidungsergebnis beeinflusst. Der Zusammenhang zwischen dem Vorteil einerseits und der damit erwarteten Gegenleistung andererseits wird im deutschen Recht als Unrechtsvereinbarung bezeichnet. Alle Korruptionsdelikte in Deutschland (und auch die meisten ausländischen) weisen im Wesentlichen dieselbe Grundstruktur auf und unterscheiden lediglich im Hinblick auf den Inhalt der Unrechtsvereinbarung.

3.2.2.1 Vorteil

Ein notwendiges Element aller Korruptionsdelikte besteht zunächst in der Inaussichtstellung oder Gewährung einer Zuwendung (Vorteil) durch den Geber an den Nehmer (für eine Strafbarkeit genügt allerdings alleine das Vorhandensein eines Vorteils nicht, vielmehr muss noch eine sog. Unrechtsvereinbarung hinzutreten).

3.2.2.1.1 Materielle und immaterielle Vorteile

Als Vorteil wird alles angesehen, was den Empfänger materiell oder immateriell in seiner wirtschaftlichen, rechtlichen oder persönlichen Lage objektiv besserstellt und worauf dieser keinen rechtlich begründeten Anspruch hat.¹⁴ Hierunter fallen alle Leistungen materieller Art, beispielsweise Geld, Darlehen, Geschenke, Rabatte, Einladungen zu Veranstaltungen und Kongressen, Hotelaufenthalte, Urlaubsreisen, Restaurant- und Bordellbesuche, Freikarten, Überlassung von Fahrzeugen und Geräten etc.¹⁵

Aber auch Honorar- oder Gehaltszahlungen auf Grundlage eines Vertrages können als Vorteil angesehen werden; dies auch dann, wenn die Leistung tatsächlich erbracht wurde und das Entgelt angemessen und marktüblich ist. Einen Vorteil kann nämlich bereits die Einräumung der Möglichkeit zum Abschluss eines (Berater-)Vertrages oder einer sonstigen

¹² BGH NStZ 2007, 583; 2009, 95.

¹³ Pelz, Korruption als strafbare Untreue, in: Lewisch (Hrsg.), Wirtschaftsstrafrecht und Organverantwortlichkeit, Jahrbuch 2011, S. 101 ff.; Nestler, Korruption, in Knierim/Rübenstahl/Tsambikakis, Internal Investigations, Kap. 24 Rn. 350 ff.

¹⁴ BGHSt 47, 295, 304; NStZ 2008, 216, 217.

¹⁵ Vgl. Fischer, StGB, § 331 Rn. 11c f.

Nebenbeschäftigung darstellen.¹⁶ Hiervon abzugrenzen sind freilich legale Nebentätigkeiten aufgrund besonderer Kenntnisse und Fähigkeiten des Amtsträgers.¹⁷

Feste Wertgrenzen, unterhalb derer man nicht von einem Vorteil sprechen kann, hat die Rechtsprechung stets abgelehnt und auch lediglich geringwertige Zuwendungen als Vorteil anerkannt. Als Faustformel kann dabei davon ausgegangen werden, dass Zuwendungen von mehr als 25,00 bis 30,00 € bei Amtsträgern¹⁸ bzw. 50,00 € im privaten Geschäftsverkehr als Vorteil angesehen werden müssen.¹⁹

Vorteile können auch immaterieller Natur sein, sofern sie einen objektiv messbaren Inhalt haben und den Empfänger in irgendeiner Weise tatsächlich besserstellen.²⁰ Dies kann beispielsweise bei Ehrungen, Unterstützung bei Wahlen, Verbesserung von Beförderungs- oder Karrierechancen der Fall sein.

3.2.2.1.2 Drittvochteile

Unerheblich ist es dabei, ob der Vorteil dem Bestochenen selbst oder einem Dritten zugesendet wird. Dritte können neben Angehörigen des Bestochenen (z. B. Ehefrau, Kinder, Verwandte) auch Vereine, Parteien oder sonstige Institutionen sein. Zu beachten ist, dass insbesondere auch Behörden, die Anstellungskörperschaft des Amtsträgers²¹ oder der Arbeitgeber bzw. Auftraggebers eines Angestellten oder Beauftragten²² Dritte in diesem Sinne sein können.²³ Dass der Bestochene persönlich weder unmittelbar noch mittelbar bereichert ist oder ihm der Vorteil zugutekommt, schließt Korruption daher nicht von vornherein aus. Gerade bei Zuwendungen an die Anstellungskörperschaft bzw. an den Arbeitgeber oder Auftraggeber ist die Abgrenzung legalen und korruptiven Verhaltens besonders schwierig und es bedarf besonders kritischer Prüfung, ob tatsächlich eine Unrechtsvereinbarung vorliegt.

3.2.2.2 Unrechtsvereinbarung

Maßgebend für die Bestimmung der Strafbarkeit ist das Vorliegen eines Gegenseitigkeitsverhältnisses zwischen der Zuwendung einerseits und der hierfür zu erbringenden Gegenleistung andererseits. Der Inhalt der zur Strafbarkeit führenden Unrechtsvereinbarung unterscheidet sich danach, ob es sich in der Person des Empfängers um einen Amtsträger, einen Abgeordneten, einen Angestellten oder Beauftragten oder ein Mitglied einer Arbeitnehmerver-

¹⁶ BGHSt 31, 264, 279; NStZ 2008, 216, 217.

¹⁷ BGH NStZ-RR 2003, 171; 2007, 309.

¹⁸ Vgl. Heine/Eisele in Schönke/Schröder, StGB, § 331 Rn. 40.

¹⁹ Wobei kein Automatismus besteht, dass eine Zuwendung unterhalb dessen nicht als Vorteil einzustufen ist, Heine/Eisele in Schönke/Schröder, StGB, § 331 Rn. 40.

²⁰ BGHSt 47, 295, 304.

²¹ OLG Karlsruhe NJW 2001, 907, 908; OLG Celle NJW 2008, 164.

²² Fischer, StGB, § 299 Rn. 11; Eisele in Schönke/Schröder, StGB, § 299 Rn. 19; a.A. Nepomuck/Gross, Zuwendungen an den Anstellungsbetrieb als Drittvochteile im Sinne des § 299 StGB?, wistra 2012, 132, 135.

²³ Fischer, StGB, § 331 Rn. 14a; Heine/Eisele in Schönke/Schröder, StGB, § 331 Rn. 22.

tretung handelt. Überspitzt gesagt zeichnet sich Korruption durch den Kauf einer Entscheidung oder zumindest deren Beeinflussung aus. Hierdurch unterscheidet sich Korruption auch von freigiebigen Zuwendungen, bei denen gerade keine Gegenleistung erwartet wird.

Korruption liegt schon dann vor, wenn eine Unrechtsvereinbarung erstrebt wird, d. h. der Zuwendende mit der Vorteilsgewährung eine Entscheidung beeinflussen will. Unerheblich ist, ob es tatsächlich zum Abschluss einer solchen Unrechtsvereinbarung kommt. Auch wenn der Empfänger einer Zuwendung die wahren Absichten des Geberts nicht erkennt, ändert dies am Verbotenen des Verhaltens des Geberts daher nichts.

3.2.2.2.1 Amtsträgerkorruption

3.2.2.2.1.1 Amtsträger

Die §§ 333, 334 StGB umfassen Korruptionsdelikte gegenüber deutschen Amtsträgern, für den öffentlichen Dienst besonders Verpflichteten, Soldaten der Bundeswehr, Richtern oder Schiedsrichtern. Amtsträger ist nach § 11 Abs. 1 Nr. 2 StGB zunächst jeder, der statusrechtlich in einem deutschen Beamtenverhältnis steht, also Bundes-, Landes- oder Kommunalbeamter ist. Nicht erfasst sind Ruhestandsbeamte (§ 30 Nr. 4 BBG) oder solche Beamte, die zum Zwecke des Abschlusses eines privatrechtlichen Dienstverhältnisses beurlaubt wurden.²⁴ Als Amtsträger gelten auch Personen, die in einem öffentlich-rechtlichen Amtsverhältnis stehen. Hierzu zählen Minister von Bundes- oder Landesregierungen, parlamentarische Staatssekretäre, Vorstände kommunaler Zweckverbände, Notare, nicht jedoch Kirchenbeamte.²⁵

Daneben gelten als Amtsträger auch Personen, die sonst zur Wahrnehmung öffentlicher Aufgaben bei einer Behörde oder sonstigen Stelle oder in deren Auftrag bestellt sind. Hierunter fallen insbesondere Personen, die bei Körperschaften oder Anstalten des Öffentlichen Rechts, in kommunalen Krankenhäusern sowie bei öffentlich-rechtlichen Rundfunkanstalten oder in kommunalen Eigenbetrieben beschäftigt sind. Sofern die öffentliche Hand Aufgaben durch juristische Personen des Privatrechts, durch gemischte staatlich-private Unternehmen oder durch Public Private Partnerships²⁶ wahrt, können auch deren Beschäftigte Amtsträger sein, sofern es sich bei der Geschäftstätigkeit um Aufgaben der öffentlichen Verwaltung handelt, das private Unternehmen durch die öffentliche Hand (mehrheitlich) gesteuert wird und es bei einer Gesamtbetrachtung als verlängerter Arm des Staates erscheint.²⁷ Öffentliche Aufgaben sind dabei entweder hoheitliche oder solche, die der Daseinsvorsorge dienen, beispielsweise Müllabfuhr, Wasserversorgung, ÖPNV

²⁴ BGHSt 49, 214; diese sind dann wie Angestellte zu behandeln.

²⁵ BGHSt 37, 191, 193.

²⁶ Zu Strafbarkeitsrisiken hierzu vgl. Bernsmann, Public Private Partnership (PPP) – Ein Thema für das Strafrecht?, StV 2005, 685; Saliger, Kick-Back, PPP, Verfall – Korruptionsbekämpfung im Kölner Müllfall, NJW 2006, 3377.

²⁷ BGHSt 43, 370, 377; 50, 299, 303.

etc. Hierzu besteht eine umfangreiche, nicht immer widerspruchsfreie Kasuistik.²⁸ In Zeiten zunehmender Aufgabenprivatisierung und angesichts des Umstands, dass heutzutage für nahezu jede Tätigkeit auch private Wettbewerber auf dem Markt agieren, ist die Abgrenzung von öffentlichen und privaten Aufgaben schwierig²⁹ und einem stetigen Wandel unterworfen.

Für präventive Compliance-Zwecke ist die Abgrenzung im Einzelnen auch nicht entscheidend, da Personen, die nicht als Amtsträger gelten, zumeist Angestellte oder Beauftragte im Sinne von § 299 StGB sein werden und auch deren Bestechung in zwar nicht identischer, aber doch vergleichbarer Weise strafbar ist.

3.2.2.2.1.2 Unrechtsvereinbarung

Die Unrechtsvereinbarung bei Amtsträgern besteht darin, dass die Zuwendung eines Vorteils entweder für die Dienstausübung erfolgt (Vorteilsgewährung) oder als Gegenleistung für eine vergangene oder künftige Diensthandlung, bei der der Amtsträger seine Dienstpflichten verletzt hat oder verletzen wird (Bestechung).

Im Inland unzulässig ist damit jede Zuwendung, die im Zusammenhang mit der Dienstausübung durch einen Amtsträger steht. Eine solche liegt schon dann vor, wenn ein Amtsträger irgendeine in seinen dienstlichen Aufgabenbereich fallende Handlung vornehmen soll. Dies unabhängig davon, ob er durch die erwartete Tätigkeit Dienstpflichten verletzen wird oder nicht. Auch Zuwendungen für an sich rechtmäßige Diensthandlungen, die der Amtsträger ohnehin so hätte vornehmen müssen, sind untersagt. Nicht erforderlich ist, dass die vom Amtsträger vorzunehmende Diensthandlung schon in irgendeiner Weise konkret bestimmt ist. Auch Zuwendungen zur Sicherung der allgemeinen Geneigtheit, zur Klimapflege oder Stimmungspflege sind verboten.³⁰ Verhindert werden soll nämlich bereits der böse Schein der Käuflichkeit behördlicher Entscheidungen.³¹

Die Unrechtsvereinbarung bei der Bestechung liegt darin, dass sich der Amtsträger im Gegenzug für die Zuwendung bereit gezeigt hat, seine Dienstpflichten zu verletzen, also gegen gesetzliche Regelungen oder Dienstvorschriften zu verstößen. Dies betrifft die Fälle, in denen der Amtsträger bei gebundenen Entscheidungen eine unrechtmäßige Entscheidung trifft. Bei Planungs- oder Ermessensentscheidungen liegt eine Pflichtwidrigkeit zum einen dann vor, wenn die Entscheidung selbst die Grenzen des dem Amtsträger eingeräumten Ermessens überschritten hat, also ein Fall eines Ermessensfehlgebrauchs vorliegt. Darüber hinaus bestimmen §§ 332 Abs. 3, 334 Abs. 3 StGB, dass es für eine Pflichtwidrigkeit schon ausreicht, wenn durch die Zuwendung Einfluss auf die Ermessensentscheidung ausgeübt werden soll, mag die getroffene Entscheidung dann inhaltlich auch nicht zu beanstanden sein.

²⁸Vgl. Fischer, StGB, § 11 Rn. 22 ff.; Hecker in Schönke/Schröder, StGB § 11 Rn. 20 ff.

²⁹Zur Einordnung von Angestellten einer Sparkasse je nach Art der Tätigkeit BGH NStZ 2020, 271.

³⁰BGHSt 49, 275, 281; Heine/Eisele in Schönke/Schröder, StGB, § 331 Rn. 30.

³¹BGHSt 49, 275, 281; NStZ 2005, 334, 335.

Keine Unrechtsvereinbarung besteht jedoch dann, wenn der Amtsträger Handlungen vornehmen soll, zu deren Erfüllung er berufen ist. So ist der Abschluss von Kaufgeschäften, Dienst-, Werk-, Miet- oder anderen Verträgen für die Behörde bzw. Anstellungskörperschaft oder der Vergleichsschluss bei Streitigkeiten grundsätzlich zulässig. Dies jedenfalls dann, wenn die (verwaltungs-)rechtlichen Form- und Verfahrensvorschriften eingehalten werden.³² An einer Unrechtsvereinbarung wird es regelmäßig auch dann fehlen, wenn die Zuwendung dem Amtsträger erst die Vornahme der Diensthaltung ermöglichen soll.³³ Als zulässig angesehen wurden daher bspw. auch die Bewirtung eines Vorsitzenden einer Sparkasse anlässlich geschäftlicher Besprechungen³⁴ oder Einladungen hochrangiger Amtsträger zu Repräsentationszwecken.³⁵ Unzulässig sind aber solche Geschäfte oder Handlungen, bei denen es an einer entsprechenden rechtlichen Grundlage fehlt, sei es, dass keine Ermächtigung zum Abschluss bestimmter Geschäfte besteht,³⁶ sei es, dass es sich um eine unzulässige Koppelung unabhängiger Geschäfte handelt.³⁷ Auch der Verstoß gegen bindende gesetzliche Verfahrensvorschriften kann zu einer Strafbarkeit führen, mag das Geschäft auch inhaltlich nicht zu beanstanden sein.³⁸

§ 333 Abs. 3 StGB sieht die Möglichkeit einer Genehmigung für Zuwendungen an Amtsträger vor. Eine solche Genehmigung ist nicht zwingend notwendig, sie kann aber im Falle von Unsicherheiten dazu führen, dass etwaige Strafbarkeitsrisiken beseitigt werden. Zuwendungen an Amtsträger sind nämlich dann zulässig, wenn die zuständige Behörde im Rahmen ihre Befugnisse diese entweder vor Annahme des Vorteils genehmigt (§ 71 Abs. 1 BBG) oder dies unverzüglich danach geschieht. Liegt eine Genehmigung vor, kann dies nicht den Anschein der Käuflichkeit von Behördenentscheidungen wecken. Zuständige Behörde ist dabei die für den Amtsträger vorgesetzte Dienstbehörde, bei Angestellten der öffentliche Arbeitgeber. Voraussetzung einer solchen Genehmigung ist jedoch, dass sämtliche getroffenen Abreden offengelegt werden. Hat der Amtsträger einen Vorteil gefordert, ist dies nicht genehmigungsfähig. In Anti-Korruptionsrichtlinien der Verwaltung wird oftmals eine generelle Zustimmung für bestimmte, typischerweise unkritische Sachverhalte erklärt (sog. Allgemeingenehmigung), wobei vielfach Bagatellgrenzen definiert sind.³⁹

³² BGH NStZ 2002, 648, 650; StV 2012, 19, 20 f.

³³ OLG Zweibrücken NStZ 1982, 204; Korte in Münchener Kommentar StGB, § 331 Rn. 117.

³⁴ BGHSt 31, 264, 279.

³⁵ BGHSt 53, 6, 18; Korte in Münchener Kommentar StGB, § 331 Rn. 128.

³⁶ BGH StV 2012, 19, 21 („Schulfoto“).

³⁷ LG Stade, Beschluss vom 28.1.2005 – 12 Qs 153/04 (abrufbar unter juris).

³⁸ BGH NStZ 2003, 158, 159.

³⁹ Bundesministerium des Inneren, Rundschreiben zum Verbot der Annahme von Belohnungen oder Geschenken in der Bundesverwaltung vom 8. November 2004.

3.2.2.2.2 Korruption im privaten Sektor

3.2.2.2.2.1 Angestellte und Beauftragte

Nach § 299 Abs. 1, 2 StGB strafbar ist lediglich die Korruption von Angestellten und Beauftragten eines geschäftlichen Betriebes. Als geschäftlicher Betrieb gelten alle Stellen, die als Anbieter oder Nachfrager von Waren oder Leistungen am Wirtschaftsleben teilnehmen mit Ausnahme von privaten Endverbrauchern. Umfasst sind daher auch Beschaffungsstellen öffentlicher Einrichtungen und Kirchen, aber auch Freiberufler.

Arbeitnehmer sind all die Personen, die in einem tatsächlichen oder jedenfalls faktischen Arbeitsverhältnis mit einem Unternehmen stehen, also insbesondere Arbeitnehmer oder Geschäftsführer einer GmbH.

Als Beauftragter gilt, wer, ohne Angestellter zu sein, aufgrund seiner Stellung berechtigt und verpflichtet ist, auf geschäftliche Entscheidungen eines Betriebes Einfluss zu nehmen.⁴⁰ Dies trifft beispielsweise für Vorstandsmitglieder einer AG, Testamentsvollstrecker, aber auch außenstehende Personen wie beispielsweise Unternehmensberater,⁴¹ andere externe Berater⁴² oder Architekten zu, welche nur aufgrund eines einzelnen Vertrages vorübergehend für ihren Auftraggeber tätig werden.

Vom Korruptionsverbot nicht erfasst sind daher Zuwendungen an private Endkunden oder an Geschäftsinhaber. Als solche gelten die Inhaber einzelkaufmännischer Unternehmen, nach überwiegender Meinung aber auch der Alleingesellschafter-Geschäftsführer einer GmbH,⁴³ alle Gesellschafter einer juristischen Person oder Personengesellschaft.⁴⁴ Strittig ist, ob der Komplementär einer Kommanditgesellschaft als Geschäftsinhaber anzusehen ist.⁴⁵ Geschäftsinhabern dürfen daher Vorteile für die Beeinflussung geschäftlicher Entscheidungen straflos zugewendet werden. Nach einer umstrittenen Entscheidung sollen daher auch Zuwendungen an Angestellte von Unternehmen zulässig sein, wenn dies mit Einverständnis aller Anteilseigner (und nicht nur der vertretungsberechtigten Geschäftsführer bzw. Gesellschafter) geschieht.⁴⁶

3.2.2.2.2.2 Unrechtsvereinbarung

Bei der Bestechung im geschäftlichen Verkehr muss ein Vorteil als Gegenleistung für eine künftige unlautere Bevorzugung beim Bezug von Waren oder Leistungen versprochen

⁴⁰ Fischer, StGB, § 299 Rn. 15.

⁴¹ OLG Karlsruhe BB 2000, 636.

⁴² Schmidl, Der Fluch der bösen Tat – Finder's Fees und die Bestechlichkeit von Beratern, wistra 2006, 286, 288.

⁴³ Dannecker/Schröder in Kindhäuser/Neumann/Paeffgen/Saliger, StGB, § 299 Rn. 41.

⁴⁴ Korte in Münchener Kommentar StGB, § 299 Rn. 42.

⁴⁵ Bejahend Bürger, § 299 StGB – Eine Straftat gegen den Wettbewerb?, wistra 2003, 130, 132; Eisele in Schönke/Schröder, StGB § 299 Rn. 11; verneinend Korte in Münchener Kommentar StGB, § 299 Rn. 42.

⁴⁶ BGH NStZ 2022, 413.

oder gewährt werden. Daher ist die bloße Belohnung für in der Vergangenheit liegende Ereignisse nicht strafbar, außer die Belohnung wäre bereits zuvor in Aussicht gestellt worden. Bestechung im geschäftlichen Verkehr setzt zunächst einmal das Bestehen eines tatsächlichen oder zumindest potenziellen Wettbewerbsverhältnisses voraus. Strafgrund ist nämlich eine Beeinträchtigung der Wettbewerbslage durch eine Besserstellung gegenüber bestehenden Wettbewerbern oder durch Vermeidung künftigen Wettbewerbs. Die Voraussetzungen hierfür sind nicht hoch. Weder muss ein bestimmter Wettbewerber feststellbar sein noch bedarf es einer konkreten Konkurrenzsituation. Es reicht aus, wenn die bloße Möglichkeit besteht, dass sich Wettbewerber um einen Auftrag bemühen oder der Auftraggeber bei anderen Lieferanten nachfragen könnte. Ein Wettbewerbsverhältnis soll auch dann schon vorliegen, wenn sich die Zuwendung auf ein internes Qualifizierungs- oder Zulassungsverfahren bezieht, das Voraussetzung für die künftige Teilnahme an Vergabeverfahren ist⁴⁷ oder auf die Platzierung auf einer Shortlist, selbst wenn damit noch keine unmittelbare Beauftragung verbunden ist.

Eine Bestechung liegt vor, wenn Angestellte oder Beauftragte beispielsweise Provisio nen für die Erteilung von Aufträgen oder für die Nichtgeltendmachung von Gewährleistungsansprüchen erhalten. Für die Strafbarkeit ist nicht erforderlich, dass der Arbeitgeber oder Auftraggeber einen Schaden erleidet oder ein Verhalten vor diesem verheimlicht wurde. Nach der Korkengeld-Entscheidung⁴⁸ ist die Gewährung von Verkaufsprämien an Angestellte eines Unternehmens auch bei Zustimmung des Arbeitgebers unzulässig. Verkaufsprämien an das Kundenunternehmen hingegen sind jedoch ebenso erlaubt wie deren Weiterleitung durch das Unternehmen an seine Angestellten.⁴⁹

Schwieriger ist die Abgrenzung von strafbarem und straflosem Verhalten in den Fällen, in denen der Arbeitnehmer oder Beauftragte für den Arbeitgeber bzw. Auftraggeber handelt und nur dieser wirtschaftlich von der Bevorzugung profitiert. Teilweise wird angenommen, dass in diesen Fällen nie eine unlautere Bevorzugung vorliegen könne, da Arbeitnehmer und Beauftragte von Gesetzes wegen gehalten seien, zugunsten des Arbeitgebers bzw. Auftraggebers zu handeln. Die überwiegende Meinung nimmt an, eine Zuwendung sei auch in diesen Konstellationen dann unlauter, wenn sie darauf abzielt, eine geschäftliche Entscheidung unter Umgehung der Regeln des Wettbewerbs durch sachfremde Erwägungen zu beeinflussen, die sich nicht mehr nach den Kriterien von Preis und Leistung und den Prinzipien des freien Wettbewerbs bestimmen.⁵⁰ Die Abgrenzung zulässigen und verbotenen Verhaltens kann vor dem Hintergrund des weiten Vorteilsbegriffs schwierig sein. So stellt grundsätzlich auch ein Mengenrabatt einen Vorteil dar, der jedoch straflos ist, solange er die Grenze des Üblichen nicht überschreitet⁵¹ und nicht dazu dient, Wettbewerber vollständig aus dem Markt zu verdrängen. Je nach Ausgestaltung können auch sog. „Eintrittsgelder“,

⁴⁷ BGHSt 49, 214, 228.

⁴⁸ RGSt 48, 291.

⁴⁹ Wackernagel/Gschlossmann, NZWiSt 2021, 51, 55. Zu Kundenbindungs- und Bonusprogrammen Grützner/Behr in Momsen/Grützner, Wirtschafts- und Steuerstrafrecht, 2. Aufl. 2020, § 30 Rn. 265 ff.

⁵⁰ Dannecker/Schröder in Kindhäuser/Neumann/Paeffgen/Saliger, StGB, § 299 Rn. 93.

⁵¹ Dannecker/Schröder in Kindhäuser/Neumann/Paeffgen/Saliger, StGB, § 299 Rn. 68; Krick in Münchener Kommentar StGB, § 299 Rn. 184.

„Listungsentgelte“ oder „Quick-Savings“ risikobehaftet sein,⁵² wenn es sich nicht um reine Preisbestandteile oder vorgezogene Mengenrabatte handelt.

3.2.2.2.3 Bestechung und Bestechlichkeit im Gesundheitswesen

Durch §§ 299a und 299b StGB wurde ein eigenständiger Straftatbestand zur Bestechung bzw. Bestechlichkeit im Gesundheitswesen geschaffen. Danach sind Zuwendungen an Angehörige eines Heilberufs strafbar, wenn dies als Gegenleistung für die Verordnung oder der unmittelbaren Anwendung von Arznei-, Heil- und Hilfsmitteln oder Medizinprodukten oder für die Zuführung von Patienten oder Untersuchungsmaterial geschieht. Durch diese Vorschriften sollen Strafbarkeitslücken geschlossen werden, die sich daraus ergeben, dass insbesondere niedergelassene Ärzte nicht als Angestellte oder Beauftragte i.S.v. § 299 StGB anzusehen sind. Kooperationsvereinbarungen mit Krankenkassen, Versorgungsträgern oder anderen Angehörigen von Heilberufen, die sich innerhalb gesetzlicher Vorgaben bewegen, sind jedoch weiterhin möglich.⁵³

3.2.2.2.4 Mandatsträgerkorruption

Nach § 108e Abs. 2 StGB ist es verboten, einem Abgeordneten oder sonstigen Mandatsträger einen Vorteil dafür anzubieten oder zu gewähren, dass er bei Wahrnehmung seines Mandats im Auftrag oder auf Weisung bestimmte Tätigkeiten vornimmt oder unterlässt. Mandatsträger sind nach § 108e Abs. 2, 3 StGB Mitglieder von Bundestag, Landtagen, sowie Kommunalparlamenten oder Gremien kommunaler Gebietskörperschaften, des Europäischen Parlaments oder parlamentarischer Versammlungen internationaler Organisationen. Die Zuwendung muss im Zusammenhang mit der Wahrnehmung eines Mandats stehen und damit einen unmittelbaren Bezug zur parlamentarischen Tätigkeit des Mandatsträgers in Parlaments- und Fraktionsgremien, insbesondere der Tätigkeit im Plenum, in Ausschüssen, Arbeitskreisen oder Arbeitsgruppen sowie in parlamentarischen Gremien haben.⁵⁴ Nicht hierunter fällt jedoch die Tätigkeit in ausschließlich parteiinternen Gremien oder bei außerparlamentarischen Tätigkeiten, selbst wenn der Mandatsträger hierbei seinen Status oder besondere Zugangsmöglichkeiten ausnutzt.⁵⁵ Hierbei handelt es sich lediglich um Tätigkeiten während des Mandats, die nunmehr aber von § 108f Abs. 2 StGB erfasst werden. Demnach macht sich strafbar, wer einen Vorteil anbietet oder gewährt für die Wahrnehmung von Interessen des Vorteilsgebers (oder eines Dritten) während des Mandats. Die Vorschrift erstreckt sich anders als § 108e Abs. 2 nur auf Vermögensvorteile und setzt zusätzlich voraus, dass die Interessenwahrnehmung parlamentsrechtlich verboten ist (Abs. 2 S. 2), außerdem gilt sie nur in Bezug auf Mitglieder von Bundestag, Landtagen, Europäischem Parlament und parlamentarischen Versammlungen internationaler Organisationen. Nach §§ 108e Abs. 4, 108f Abs. 3 StGB handelt es sich nicht um einen korruptionsrechtlich relevanten Vorteil, wenn Zuwendungen an Mandatsträger im Einklang mit den für ihn maßgeblichen Vorschriften (insbesondere Wohlverhaltensregeln oder vergleichbaren

⁵² Ballo/Skopul, „Quick Savings“ – ein Problem des Korruptionsstrafrechts?, NJW 2019, 1174 ff.

⁵³ Gaede in Leitner/Rosenau, Wirtschafts- und Steuerstrafrecht, 2. Aufl. 2022, § 299a StGB Rn. 85 ff.

⁵⁴ BGHSt 67, 107, 122 ff.

⁵⁵ BGHSt 67, 107, 129.

Regelungen der Parlamente) stehen oder es sich um eine zulässige Parteispende handelt. Einflussspenden, mit denen der Spender bestimmte politische Entscheidungen beeinflussen möchte, sind aber stets unzulässig. Zuwendungen zur Klimapflege, mit allgemeinem Bezug auf die Abgeordnetentätigkeit, Lobbying-Zwecken⁵⁶ oder zur Unterstützung allgemeiner politischer Ansichten sind hingegen zulässig.

Mitglieder von Kommunalparlamenten (Gemeinde-, Stadträte, Kreistage) üben sowohl gesetzgeberische Tätigkeit als auch Verwaltungsaufgaben in der jeweiligen Gebietskörperschaft aus. Sie sind bei Ausübung ihres Wahlmandats grundsätzlich Volksvertreter im Sinne des § 108e Abs. 2 StGB. Soweit sie jedoch konkrete Verwaltungstätigkeiten durchführen, beispielsweise als Mitglieder eines Verwaltungsausschusses bei Auftragsvergaben oder als Aufsichtsrat kommunaler Unternehmen, gelten sie als Amtsträger.⁵⁷

3.2.2.2.5 Arbeitnehmervertreter

§ 119 Abs. 1 Nr. 3 BetrVG untersagt es dem Arbeitgeber, einen Betriebsrat oder ein Mitglied einer gleichgestellten Stelle gegenüber anderen Mitarbeitern zu bevorzugen. Ob dies der Fall ist, wird dadurch ermittelt, dass die einem Betriebsratsmitglied gewährten Zuwendungen mit der Situation verglichen wird, die sich ergäbe, wenn dieselbe Person nicht Betriebsratsmitglied wäre.⁵⁸ Insbesondere dürfen einem Betriebsratsmitglied keine höheren Gelder oder Sachleistungen gewährt werden, als es sie bei einer sonstigen Beschäftigungstätigkeit unter Berücksichtigung üblicher und zu erwartender Karriereentwicklung erhalten würde, einschließlich etwaiger Nebenleistungen wie Firmenfahrzeug etc.

3.2.2.2.6 Sozialadäquate Zuwendungen

Eine Unrechtsvereinbarung fehlt in Fällen sozial adäquater Zuwendungen. Sozial adäquat sind Leistungen, die von der Allgemeinheit gebilligt und als sozial üblich angesehen werden bzw. der Sitte und Höflichkeit entsprechen. Branchenüblichkeit kann auf Sozialadäquanz hindeuten, kann aber auch Ausfluss branchenweiter Missstände sein. Als sozial adäquat angesehen werden übliche, geringwertige Aufmerksamkeiten anlässlich von Weihnachten, Geburtstagen, Jubiläen oder persönlichen Feiertagen, geringfügige Trinkgelder oder Dienstleistungen, die der Höflichkeit entsprechen (zum Beispiel Fahrten zum Bahnhof).⁵⁹ Richtlinien von Behörden und Unternehmen zur Korruptionsprävention, die Aussagen über die Zulässigkeit der Annahme von Zuwendungen treffen, können für die nähere Bestimmung der Sozialadäquanz Bedeutung haben.

3.2.2.3 Tathandlung

Die Tathandlung liegt im Falle aktiver Korruption im Anbieten, Versprechen oder Gewähren eines Vorteils bzw. aus der Nehmerperspektive im Fordern, Sich-Versprechen-Lassen oder Annehmen. Das Anbieten liegt bereits beim bloßen In-AussichtStellen einer

⁵⁶ Dieners in Dölling, Handbuch der Korruptionsprävention, 4. Kapitel Rn. 106 ff.

⁵⁷ BGHSt 51, 44, 49.

⁵⁸ Zimmer/Dörr, Die Betriebsratsbegünstigung – Ab wann ist sie kriminell? NZWiSt 2021, 176; Baader/Reiserer, Die Betriebsratsvergütung als Compliance-Risiko, DStR 2022, 155.

⁵⁹ Heine/Eisele in Schönke/Schröder, StGB, § 331 Rn. 40.

Vorteilszuwendung vor, unabhängig davon, ob der Empfänger sich hierzu bereit zeigt oder nicht. Das Versprechen setzt eine tatsächliche Übereinkunft zwischen Geber und Nehmer voraus. Das Gewähren liegt in der tatsächlichen Zuwendung des Vorteils an den Empfänger oder einen Dritten. Spiegelbildliches gilt für die Nehmerperspektive.

Darüber hinaus ist wegen Beihilfe oder Mittäterschaft derjenige strafbar, der bei einer der Tathandlungen mitwirkt, was nicht nur bei der unmittelbaren Tatdurchführung der Fall ist. Es reicht auch aus, wenn die Vornahme von Bestechungshandlungen gebilligt und in irgendeiner Art und Weise unterstützt wird, beispielsweise durch die Mitwirkung am Abschluss von Verschleierungsverträgen, der Freigabe und der Abwicklung von Zahlungen etc. Die Unternehmensleitung bzw. im Fall der Aufgabendelegation die Leiter entsprechender Unternehmensbereiche sind dafür verantwortlich, gegen Korruptionshandlungen von Mitarbeitern einzuschreiten und diese zu verhindern. Sie trifft insoweit eine Garantenstellung.⁶⁰ Bleiben sie untätig, können sie sich wegen Anstiftung oder Beihilfe durch Unterlassen strafbar machen.

Zudem sind die Mitglieder der Unternehmensleitung sowie die zur Leitung einzelner Unternehmensbereiche beauftragten Personen nach § 130 OWiG verpflichtet, diejenigen organisatorischen Vorkehrungen, Maßnahmen und Kontrollen vorzunehmen, die erforderlich sind, um betriebsbezogene Straftaten – und dazu gehört insbesondere die Korruption – durch Mitarbeiter zu verhindern oder wesentlich zu erschweren. Insbesondere wird neben einer hinreichenden Organisation eine sorgfältige Auswahl der beauftragten Mitarbeiter, hinreichende Instruktion und Schulung sowie eine gehörige Kontrolle und Überwachung gefordert.⁶¹ Allein eine nur fahrlässige Verletzung dieser Organisations- und Kontrollpflichten kann Bußgelder bis zu 10 Mio. € zur Folge haben.

Ob der Compliance-Officer eine umfassende Pflicht zur Verhinderung von Korruptionsdelikten hat,⁶² lässt sich nicht allgemein bestimmen. Dies hängt entscheidend von den dem Compliance-Officer konkret übertragenen Aufgaben ab. Regelmäßig wird es ausreichen, wenn der Compliance-Officer die ihm bekanntgewordenen Verdachtsmomente an die zuständigen Stellen im Unternehmen berichtet (Eskalationspflicht), wobei Einzelheiten und Grenzen der Meldepflicht streitig sind.

3.2.3 Korruptionsstrafaten im Ausland

Durch eine Reihe von Strafvorschriften können auch Korruptionshandlungen im Ausland nach deutschem Recht bestraft werden. Dies gilt jedenfalls dann, wenn die Tathandlung ganz oder teilweise in Deutschland begangen wurde bzw. der Taterfolg in Deutschland

⁶⁰ Mitteldorf, Zur Reichweite individueller strafrechtlicher Verantwortung im Unternehmen für Fehlverhalten von unterstellten Mitarbeitern, ZIS 2011, 123, 125 ff.; Dannecker, Die Folgen der strafrechtlichen Geschäftsherrenhaftung der Unternehmensleitung für die Haftungsverfassung juristischer Personen, NZWiSt 2012, 441, 444 ff.

⁶¹ Grützner/Leisch, §§ 130, 30 OWiG – Probleme für Unternehmen, Geschäftsleitung und Compliance-Organisation, DB 2012, 787; Bock, Criminal Compliance, S. 364 ff.

⁶² So der BGH in einem obiter dictum in NJW 2009, 3173, 3175.

eingetreten ist (§§ 3, 9 StGB) oder der Täter deutscher Staatsangehöriger ist (§ 7 Abs. 2 StGB).

3.2.3.1 Amtsträgerkorruption

Besonderen Schutz genießen Europäische Amtsträger i.S.v. § 11 Abs. 1 Nr. 2a StGB. Diese sind in vollem Umfang deutschen Amtsträgern gleichgestellt. Damit ist sowohl die Vorteilsgewährung als auch die Bestechung strafbar, ebenso die Vorteilsannahme und die Bestechlichkeit. Als Europäische Amtsträger gelten Mitglieder der Europäischen Kommission, der Europäischen Zentralbank, des Rechnungshofs oder eines Gerichts der Europäischen Union sowie Bedienstete von Einrichtungen der EU sowie mit der Wahrnehmung von Aufgaben im Einzelfall betraute Personen.

Gleiches gilt im Ergebnis auch in Bezug auf Richter und Bedienstete des Internationalen Strafgerichtshofs sowie auf in Deutschland stationierte Soldaten oder Bedienstete von NATO-Truppen. Insoweit ist gemäß § 335a Abs. 2 und 3 StGB auch die Vorteilsgewährung (§ 333 Abs. 1 StGB) bzw. die Vorteilsannahme (§ 331 Abs. 1 und 3 StGB) strafbar.

Im Hinblick auf sonstige Bedienstete ausländischer Staaten oder Organisationen findet deutsches Strafrecht nur teilweise Anwendung. § 335a Abs. 1 StGB erweitert den Anwendungsbereich des Tatbestands der aktiven Bestechung (§ 334 StGB) und der Bestechlichkeit (§ 332 StGB) auf ausländische oder internationale Richter, Bedienstete eines ausländischen Staates, einer internationalen Organisation sowie Personen, die öffentliche Aufgaben für einen ausländischen Staat oder eine internationale Organisation wahrnehmen und Soldaten eines ausländischen Staates. Voraussetzung ist in allen Fällen, dass der ausländische Amtsträger für den Vorteil eine künftige Diensthandlung vornehmen soll, bei welcher er seine Dienstpflichten verletzt. Die bloße Belohnung für in der Vergangenheit erbrachte Diensthandlungen ist daher straflos, sofern die Belohnung nicht im Voraus versprochen worden war. Das Gleiche gilt für Zuwendungen für die Vornahme rechtmäßiger Diensthandlungen; daher sind auch sog. Facilitation Payments nach deutschem Recht straflos. Zu beachten ist aber, dass die Beeinflussung von Ermessensentscheidungen – was bei nahezu allen Beschaffungsentscheidungen der Fall sein wird – nach § 332 Abs. 3 Nr. 2 StGB zu einer Qualifikation als pflichtwidrig führt. Wer Bediensteter eines ausländischen Staates ist, bestimmt sich nicht nach dem Recht des ausländischen Staates, sondern ist entsprechend der Zielsetzung des OECD-Abkommens zur Bekämpfung der internationalen Bestechung anderer internationaler Übereinkommen auszulegen.⁶³ Bedienstete ausländischer Staaten können auch Mitarbeiter ausländischer öffentlicher Unternehmen sein. Hierunter können Unternehmen fallen, an dem die öffentliche Hand mehrheitlich beteiligt ist oder sonst die Führungs- oder Verwaltungsfunktion bestimmen kann oder die gegenüber Privaten mit Sondervorteilen ausgestattet sind. In allen Fällen ist Voraussetzung, dass öffentliche Aufgaben wahrgenommen werden, das heißt solche, die der öffentlichen Hand vorbehalten sind und nicht vollständig dem privaten Wettbewerb unterliegen.

⁶³ Gaede in Leitner/Rosenau, Wirtschafts- und Steuerstrafrecht, 2. Aufl. 2022, § 335a StGB Rn. 12.

3.2.3.2 Mandatsträgerkorruption

Die Strafvorschrift der Bestechlichkeit und Bestechung von Mandatsträgern findet gemäß § 108e Abs. 3 Nr. 4 und 6 StGB auch auf Mitglieder des Europäischen Parlaments sowie von Gesetzgebungsorganen eines ausländischen Staates Anwendung. Parlamentsmitglieder ausländischer Staaten, die nicht frei gewählt, sondern von der Parteispitze bestimmt werden, fallen hingegen nicht unter § 108e StGB. Ebenso findet § 108f Abs. 2 StGB auf Mitglieder des Europäischen Parlaments Anwendung, nicht jedoch auf Mitglieder von Gesetzgebungsorganen ausländischer Staaten.⁶⁴

3.2.3.3 Angestellte und Beauftragte im privaten Sektor bzw. von Heilberufen

In § 299 Abs. 1 und 2 StGB sowie in §§ 299a und 299b StGB ist jeweils klargestellt, dass Bestechung und Bestechlichkeit nicht nur bei Angestellten und Beauftragten von Unternehmen bzw. Angehörigen von Heilberufen im Inland, sondern auch im Ausland unter Strafe gestellt ist. Insoweit ist der Schutzmfang im Inland und im Ausland identisch.

3.3 Ausländische Rechtsvorschriften

3.3.1 Überblick

In allen Staaten der Welt ist die Vornahme von Bestechungshandlungen gegenüber inländischen Amtsträgern strafbar. Es mögen sich Unterschiede im Detail ergeben und auch im Verständnis dessen, welche Zuwendungen noch als geringfügig und damit sozialadäquat angesehen werden.⁶⁵ Im Hinblick auf die Strafbarkeit nationaler Amtsträger ist die Rechtslage nach den jeweiligen ausländischen Rechtsordnungen im Wesentlichen mit der deutschen Rechtslage vergleichbar.

Erhebliche Unterschiede gibt es hingegen bei Zuwendungen an Politiker, die in vielen Fällen wie Amtsträger angesehen werden, oder bei der Bestechung im privaten Sektor. Letztere ist in manchen Staaten nicht strafbar,⁶⁶ während die Länder, die entsprechende Strafvorschriften kennen, unterschiedliche Regelungsmodelle verfolgen.⁶⁷ Nach dem Wettbewerbsschutzkonzept führt die unlautere Einflussnahme auf geschäftliche Entscheidungen durch Zuwendungen an Beschäftigte zu einer Strafbarkeit, ähnlich der deutschen Regelung.⁶⁸ Andere Jurisdiktionen verfolgen ein Agent-Principal-Konzept, dem zu-

⁶⁴ Kargl in Kindhäuser/Neumann/Paeffgen/Saliger, StGB, § 108e Rn. 14.

⁶⁵ Auch in Ländern mit endemischer Korruption werden Zuwendungen zur Erlangung von Amtshandlungen von der Bevölkerung meist nicht als üblich und sozialadäquat, sondern notgedrungen als Übel angesehen, sodass derartige Zuwendungen strafbar bleiben.

⁶⁶ Auch wenn keine Strafbarkeit wegen Korruptionsdelikten besteht, kann im Einzelfall dennoch eine Strafbarkeit unter anderen Gesichtspunkten gegeben sein, z. B. wegen Betrugs, Untreue o.ä.

⁶⁷ Androulakis, Die Globalisierung der Korruptionsbekämpfung, S. 97 ff.

⁶⁸ Z. B. Österreich, Schweden, Dänemark, Norwegen.

folge der Strafgrund in dem Herbeiführen einer Pflichtverletzung des Beschäftigten gegenüber seinem Arbeitgeber oder Auftraggeber oder der Verletzung zwingender gesetzlicher Vorschriften liegt.⁶⁹ Bei dieser Konzeption führt die Zustimmung des Arbeitgebers oder Auftraggebers oftmals zu einem Wegfall von Strafbarkeitsrisiken. In manchen Ländern ist auch nur die Bestechung von Angestellten mit Managementfunktionen strafbar.⁷⁰

Einige Rechtsordnungen kennen Straftatbestände, die kein deutsches Pendant besitzen, zum Beispiel das Verbot des Trading in Influence bzw. Influence Peddling. Danach ist auch das Versprechen oder Gewähren eines Vorteils an eine dritte Person strafbar, die vorgibt, Einfluss auf einen Amtsträger oder die Entscheidungsfindung nehmen zu können. Insofern kann die Abgrenzung zwischen Beratungs- und Lobbytätigkeit einerseits und strafbarem Verhalten im Einzelfall schwierig sein.

Da für deutsche Unternehmen ohnehin nach §§ 3, 9 StGB stets deutsches Strafrecht zur Anwendung kommt, ist ein Verhalten nur dann konform, wenn dieses sowohl mit dem deutschen als auch dem ausländischen Recht in Einklang steht.

3.3.2 UK Bribery Act 2010

Großbritannien hat mit Wirkung vom 1. Juli 2011 das Korruptionsstrafrecht modernisiert und in dem Bribery Act 2010⁷¹ konsolidiert.⁷² Das Gesetz verwendet eine Vielzahl von sehr unbestimmten und auslegungsfähigen Begriffen, sodass sich das Justizministerium gehalten gesehen hat, eine Guidance zu veröffentlichen,⁷³ die eine – für die Gerichte allerdings unverbindliche – Interpretationshilfe darstellt.

In Section 1 und 2 stellt der Bribery Act 2010 das Anbieten, Versprechen oder Gewähren sowie das Fordern, Sich-Versprechen-Lassen oder Annehmen eines finanziellen oder anderen Vorteils unter Strafe, wenn dies in der Absicht geschieht, den Empfänger oder einen Dritten zu einer unangemessenen Ausübung einer Funktion oder Aufgabe zu veranlassen oder zu belohnen oder wenn die Entgegennahme des Vorteils selbst schon eine derartige unangemessene Handlung wäre. Dies gilt für Amtsträger wie für den geschäftlichen Bereich gleichermaßen. Wann eine Handlung unangemessen ist, bestimmt sich in Section 5(1) Bribery Act 2010 nach dem sogenannten „**expectation test**“. Maßgebend für die Beurteilung ist, ob der Anschein erweckt wird, der Begünstigte werde nicht mehr in gutem Glauben, unabhängig oder im Einklang mit seiner Vertrauensstellung handeln.⁷⁴

⁶⁹ Z. B. Frankreich, Großbritannien.

⁷⁰ Z. B. Russland, Ukraine.

⁷¹ <http://www.justice.gov.uk/legislation/bills-and-acts/acts/bribery-act-2010> (aufgerufen am 23.8.2024).

⁷² Zum Überblick Petsche 10 Jahre UK Bribery Act – Eine Bestandsaufnahme der Bedeutung des britischen Korruptionsstrafrechts für Unternehmen weltweit, wistra 2021, 135.

⁷³ <https://www.gov.uk/government/publications/bribery-act-2010-guidance> (aufgerufen am 23.8.2024).

⁷⁴ Textziffer 20 Bribery Act 2010 Guidance.

Die bedeutendste Vorschrift des Bribery Acts 2010 ist Section 7 („**failure of commercial organisations to prevent bribery**“), die eine echte Kriminalstrafbarkeit von Unternehmen begründet, wenn irgendeine mit dem Unternehmen in direktem oder indirektem Zusammenhang stehende Person eine Korruptionshandlung begeht, um ein Geschäft oder einen anderen Vorteil für das Unternehmen zu erhalten oder zu sichern. Vom Anwendungsbereich dieser Vorschrift werden nicht nur britische Unternehmen erfasst, sondern auch ausländische, die eine Geschäftstätigkeit oder einen Teil ihrer Geschäftstätigkeit in Großbritannien ausführen („.... **carries on a business, or part of a business, in any part of the United Kingdom ...**“). Diese Unternehmensstrafbarkeit tritt verschuldensunabhängig ein. Die einzige Verteidigungsmöglichkeit ist der durch das Unternehmen zu erbringende Nachweis, dass hinreichende Compliance-Prozesse zur Verhinderung von Korruption implementiert waren („.... **had in place adequate procedures designed to prevent [bribery] ...**“). Was angemessene Prozesse sind, ist im Gesetz nicht näher erläutert, jedoch enthält die Guidance Anhaltspunkte dafür, welche Prinzipien in einem Unternehmen implementiert sein müssen.

3.3.3 Der Foreign Corrupt Practices Act der USA

Der Foreign Corrupt Practices Act (FCPA)⁷⁵ enthält Regelungen zum Verbot aktiver Bestechung von ausländischen Amtsträgern (wobei Partefunktionäre und Kandidaten für politische Ämter ebenfalls als Amtsträger gelten) sowie Buchführungs- und Rechnungslegungsvorschriften.⁷⁶ Das Department of Justice und die Securities and Exchange Commission haben eine umfangreiche Guidance zum FCPA veröffentlicht.⁷⁷ Die Vorschriften des FCPA gelten für amerikanische Unternehmen und amerikanische Staatsangehörige sowie für ausländische Unternehmen, deren Aktien, Wertpapiere oder Schuldtitel an einer US-Börse gelistet sind („**U.S. issuer**“) für die gesamten weltweiten Aktivitäten. In diesem Fall findet der FCPA auch auf Konzerngesellschaften und Joint Ventures Anwendung. Darüber hinaus gilt der FCPA für jede in den USA begangene Bestechungshandlung sowie für alle Aktivitäten, bei denen „.... **instrumentality or means of interstate commerce ...**“ benutzt werden, beispielsweise Geldtransfers über US-Banken, Post-, Telefon- oder E-Mail-Verkehr über US-Gesellschaften oder US-Server o. a. Anders als nach deutschem Recht oder dem UK Bribery Act 2010 lässt der FCPA facilitation payments, d. h. kleinere Zahlungen zur Beschleunigung bei rechtmäßigen Diensthandlungen zu.⁷⁸

⁷⁵ <http://www.justice.gov/criminal/fraud/fcpa/> (aufgerufen am 23.8.2024).

⁷⁶ Ausführlich Partsch, The Foreign Corrupt Practices Act (FCPA) der USA, 2007; Rübenstahl, Dr Foreign Corrupt Practices Act (FCPA) der USA, NZWiSt 2012, 401; Kappel/Ehling, Wie viel Strafe ist genug? Deutsche Unternehmen zwischen UK Bribery Act, FCPA und StGB, BB 2011, 2115; Zimmer, Länderreport USA: Der Foreign Corrupt Practices Act, CB 2014, 272.

⁷⁷ <https://www.justice.gov/criminal-fraud/file/1292051/download> (aufgerufen am 23.8.2024).

⁷⁸ Walther/Zimmer, Haftung deutscher Unternehmen nach dem UK Bribery Act, RIW 2011, 199; Kappel/Ehling, Wie viel Strafe ist genug? Deutsche Unternehmen zwischen UK Bribery Act, FCPA und StGB, BB 2011, 2115.

U.S. issuer und mittelbar auch deren ausländische Tochterunternehmen haben nach 15 U.S.C. § 78m(b)(2)(B) auch für ein hinreichendes internes Kontrollsyste m zu sorgen, um die Einhaltung der Rechnungslegungsvorschriften gewährleisten zu können. Strafbar ist es daher, wenn in Büchern oder Aufzeichnungen Transaktionen oder Dispositionen über Vermögensgegenstände nicht in angemessener Detailiertheit, genau und fair dargelegt sind,⁷⁹ insbesondere wenn Zahlungen oder deren Zweck und Hintergrund in den Büchern verschleiert werden.

3.3.4 Sonstige ausländische Rechtsvorschriften

Frankreich hat durch das loi Sapin-II⁸⁰ Unternehmen in Frankreich mit mehr als 500 Mitarbeitern und einem Jahresumsatz von mindestens 100 Mio. € zur Einführung von Anti-Korruption-Compliance-Programmen verpflichtet, welche eine Risikoanalyse, die Einführung konkreter Verhaltenskodizes, Schulungen von Mitarbeitern, Einrichtung von Hinweisgebersystemen und interne und externe Kontrollen enthalten müssen. Die französische Antikorruptionsbehörde hat hierfür Guidelines veröffentlicht.

Eine Vielzahl ausländischer Strafrechtsordnungen kennt ebenfalls eine Unternehmensstrafe für den Fall, dass aus oder für das Unternehmen heraus Straftaten, insbesondere Korruptionsstraftaten, verübt werden. Insbesondere das italienische Strafrecht sieht in Artikel 6 d. lgs. 231/2011 eine Unternehmensstrafe für u. a. Korruptionshandlungen vor, sofern das Unternehmen nicht nachweist, dass ein effektives Compliance-System vorhanden ist.⁸¹

Auch das spanische Strafrecht sieht in Artikel 31 des spanischen Strafgesetzbuches eine Unternehmensstrafe vor, die an ein Organisationsverschulden des Unternehmens anknüpft.⁸² Sofern ein hinreichendes Compliance-System vorhanden war, entfällt eine Strafbarkeit des Unternehmens. Wird ein Compliance-System erst nachträglich implementiert, kann dies immer noch bei der Strafzumessung mildernd berücksichtigt werden.⁸³

⁷⁹ Grau/Mesholam/Blechschmidt, Der „lange Arm“ des US-Foreign Corrupt Practices Act: Unerkannte Strafbarkeitsrisiken auch jenseits der eigentlichen Korruptionsdelikte, BB 2010, 652; Rübenstahl, Der Foreign Corrupt Practices Act (FCPA) der USA, NZWiSt 2013, 6.

⁸⁰ Schumacher/Saby, „loi Sapin-II“: Die Revolution im französischen Anti-Korruptionsrecht, CCZ 2017, 68; Querenet-Hahn/Kettenberger, Länderreport Frankreich: Das Gesetz zur Transparenz, zum Kampf gegen die Korruption und zur Modernisierung der Wirtschaft vom 9.12.2006 (loi Sapin-II) CB 2017, 8.

⁸¹ Rübenstahl, Strafrechtlichen Unternehmenshaftung in Italien – das Legislativdekret Nr. 231 vom 8.6.2011, RIW 2012, 505, 509 f.; Prudentino, Länderreport Italien: Compliance in Italien nach den Reformen, CB 2013, 9.

⁸² Zapatero, Die strafrechtliche Verantwortlichkeit der juristischen Personen in Spanien, Festschrift für Imme Roxin, 2012, S. 713 f.

⁸³ Zapatero, Die strafrechtliche Verantwortlichkeit der juristischen Personen in Spanien, Festschrift für Imme Roxin, 2012, S. 716 f.

3.4 Anforderungen an Compliance

3.4.1 Notwendigkeit eines Compliance-Systems

Anti-Korruption muss heute zwingender Bestandteil eines Compliance-Systems sein. Dies folgt nicht nur aus Section 7 UK Bribery Act 2010 bzw. Artikel 6 d. lgs. 231/2011, wonach Unternehmen verschuldensunabhängig für in ihrem Interesse begangene Korruptionshandlungen bestraft werden können und die einzige Verteidigungsmöglichkeit der Nachweis eines effektiven Compliance-Systems ist. Auch nach deutschem Recht sind Unternehmen verpflichtet, bei Vorliegen von Korruptionsrisiken hinreichende Prozesse und Kontrollen zu implementieren, um die Begehung von Korruptionshandlungen auszuschließen oder erheblich zu erschweren. Diese Verpflichtung ergibt sich zivilrechtlich aus der Legalitätskontrollpflicht der Geschäftsleitung. Danach müssen Geschäftsleiter ihr Unternehmen so organisieren, dass Verstöße von Mitarbeitern gegen gesetzliche Verpflichtungen verhindert werden. Der Verstoß gegen Compliance-Pflichten löst eine zivilrechtliche Haftung der Geschäftsleitung aus.⁸⁴ Auch strafrechtlich lässt sich eine Compliance-Pflicht aus der Organisations- und Überwachungspflicht der §§ 130, 30 OWiG ableiten. Danach hat der Betriebsinhaber diejenigen Aufsichtsmaßnahmen zu ergreifen, die erforderlich sind, um betriebsbezogene Zu widerhandlungen zu verhindern oder wesentlich zu erschweren. Das Ausmaß dessen, was zur Korruptionsprophylaxe erforderlich ist, lässt sich jedoch nicht einheitlich bestimmen, sondern hängt von der spezifischen Größe, Situation und dem Risikoprofil jedes einzelnen Unternehmens ab.⁸⁵

Die Anti-Korruptions-Compliance ist aber nicht nur deshalb erforderlich, um die Vornahme von Korruptionshandlungen aus dem eigenen Unternehmen heraus zu verhindern, auch wenn viele Unternehmen hierauf einen Schwerpunkt legen. Von zumindest gleicher Bedeutung ist es, Vorgaben und Prozesse zu definieren, durch die die Gefahr der Korrumperung der eigenen Mitarbeiter gemindert wird. Die Bestechlichkeit eigener Mitarbeiter kann für das Unternehmen zu erheblichen finanziellen Risiken führen. Nicht nur werden Schmiergelder und ähnliche Leistungen in die vom Unternehmen zu zahlenden Preise einkalkuliert, vielmehr kann Bestechlichkeit auch dazu führen, dass qualitativ minderwertige oder quantitativ unnötige oder unnütze Waren oder Leistungen bezogen, bestehende Ansprüche nicht geltend gemacht oder sonst nachteilige Handlungen vorgenommen werden und das Unternehmen erheblichen finanziellen Schaden erleidet.

Empfehlungen und Materialien zu Anti-Korruptions-Compliance-Programmen sind von verschiedenen internationalen Institutionen veröffentlicht worden, namentlich der

⁸⁴ LG München I NZG 2014, 345 (Siemens/Neubürger); Hoffmann/Schieffer, Pflichten des Vorstands bei der Ausgestaltung einer ordnungsgemäßen Compliance-Organisation, NZG 2017, 401.

⁸⁵ Hauschka/Greeve, Compliance in der Korruptionsprävention – Was müssen, was sollen, was können die Unternehmen tun? BB 2007, 165, 166; Spindler in Münchener Kommentar zum AktG, 6. Aufl. 2023, § 91 Rn. 80; Hölters/Hölters in Hölters/Weber, AktG, 4. Aufl. 2022, § 93 Rn. 92.

OECD,⁸⁶ der ICC,⁸⁷ aber auch von Aufsichtsbehörden wie der Agence Française Anticorruption⁸⁸ oder dem U.S. Department of Justice.⁸⁹ Diese Guidelines geben international geltende Grundprinzipien für Compliance-Programme wieder, die auch auf die deutsche Rechtslage übertragbar sind.

3.4.2 Risikoanalyse

Grundvoraussetzung einer effektiven Korruptionsprophylaxe ist eine sorgfältige Analyse der Korruptionsrisiken,⁹⁰ mit dem sich ein Unternehmen im geschäftlichen Umfeld konfrontiert sieht. Am Anfang steht daher zunächst eine Risikobewertung, in die unter anderem folgende Gesichtspunkte einfließen:

- Länderrisiko Unternehmensstandorte
- Länderrisiko Zielmärkte
- Industrie- und Branchenrisiko
- Produkt- und Leistungsrisiko
- Kundenstruktur
- Geschäfts- und Vertriebsmodell.

Korruptionsrisiken sind unterschiedlich hoch, je nachdem, ob es sich um Massengeschäfte oder Projekttätigkeiten handelt, ob vornehmlich staatliche oder private Kunden beliefert werden, ob der Vertrieb an Unternehmens- oder Privatkunden erfolgt, dies über eigene Niederlassungen, Tochtergesellschaften oder ausgewählte Vertragshändler erfolgt, dies mithilfe von Handelsvertretern, Beratern oder Vermittlern geschieht, in welchen Staaten das Unternehmen tätig ist, wie sehr sich von Waren oder Leistungen gegenüber denjenigen von Wettbewerbern anders als durch den Preis unterscheiden etc. Eine derartige Risikoanalyse ist für jeden Unternehmensbereich, gegebenenfalls innerhalb eines Unternehmensbereichs für verschiedene Produktgruppen getrennt durchzuführen, da sich die Risikolage zum Teil signifikant unterscheiden kann.

Bei der Risikobewertung dürfen aber nicht nur Risiken aus Geber-Perspektive berücksichtigt werden, sondern es ist in gleichem Maße zu ermitteln, inwieweit Abteilungen im eigenen Unternehmen besonderen Korruptionsgefahren ausgesetzt sind. Derartige Gefahren bestehen insbesondere verstärkt im Bereich Einkauf oder bei der Auftragsvergabe.

⁸⁶ <https://www.oecd.org/corruption/anti-bribery/> (aufgerufen am 23.8.2024).

⁸⁷ <https://www.iccgermany.de/standards-incoterms/verhaltensrichtlinien/korruptionsprävention-und-bekämpfung> (aufgerufen am 23.8.2024).

⁸⁸ <https://www.agence-française-anticorruption.gouv.fr/fr/recommandations> (aufgerufen am 23.8.2024).

⁸⁹ <https://www.justice.gov/criminal-fraud/compliance> (aufgerufen am 23.8.2024).

⁹⁰ Hostenrath, Durchführung einer Risikoanalyse am Beispiel der Antikorruption, CB 2021, 377.

Einfließen sollten hierbei insbesondere die allgemeine Korruptionsgefahr in denjenigen Staaten, in denen das Unternehmen tätig ist, die Korruptionsneigung in bestimmten Branchen oder Vertriebsmodellen, Compliance-Vorfälle, aber auch bestehende Kontrollen und Kontrolldefizite. Die Risikoanalyse sollte in regelmäßigen Abständen aktualisiert werden, insbesondere bei einer Änderung von Geschäfts- und Vertriebsmodellen.

3.4.3 Richtlinien und Policies

3.4.3.1 Inhalt von Richtlinien

Eine wesentliche Voraussetzung, um Korruptionsgefahren in Unternehmen wirksam einzudämmen, ist neben dem „Tone from the top“ die klare Selbstverpflichtung des Unternehmens, korruptive Praktiken nicht zu dulden. Ein Verbot von Korruptionshandlungen wird typischerweise im Code of Conduct niedergelegt. In vielen Fällen dürfte ein derartiges, meist allgemein gehaltenes Verbot für eine effektive Compliance nicht ausreichen, da aufgrund des notwendigen Abstraktionsgrades des Code of Conduct für die Mitarbeiter des Unternehmens kaum klar ersichtlich ist, welche Verhaltensweisen konkret verboten sind. Sinnvoll ist es daher, das grundsätzliche Verbot näher zu konkretisieren. Richtlinien und Policies sollen die Mitarbeiter über die Rechtslage aufklären und ihnen konkrete Handreichungen geben, wie sie sich in bestimmten, für sie typischen Situationen zu verhalten haben. Der Inhalt und Detaillierungsgrad derartiger Richtlinien und Policies hängt von der jeweiligen Risikosituation im Unternehmen ab. Je höher das Risiko und je stärker die Mitarbeiter typischerweise Korruptionsgefahren ausgesetzt sind, desto detaillierter werden die Anweisungen gehalten sein müssen. Je nach Situation können in einer Anti-Korruptionsrichtlinie allgemeine Verhaltensanweisungen gegeben und in spezifischen Policies Regelungen und Prozesse für besondere Situationen und Gestaltungen getroffen werden.

In der allgemeinen Richtlinie wird auch festzulegen sein, in welchem Umfang die Richtlinie konzernweit verbindlich ist und inwieweit einzelne Konzern- oder Landesgesellschaften die Möglichkeit haben sollen, davon abzuweichen und (landes-)spezifische Regelungen zu treffen, die weniger weit gehen oder strenger sind als die Konzernrichtlinie.⁹¹ Insbesondere wird zu klären sein, inwieweit ein Unternehmen aus ethischen Gründen bestimmte korruptionsnahe Handlungen auch dann verbieten will, wenn diese nicht gegen geltendes Recht verstößen, gleichwohl sittlich anstößig oder bedenklich sein könnten. Unternehmen haben insoweit einen großen Spielraum, sie dürfen nur hinter der zwingenden gesetzlichen Rechtslage nicht zurück bleiben.

Im internationalen Kontext ist dabei zu beachten, dass mehrere Rechtsordnungen zur Anwendung kommen können, nämlich die Rechtsordnung am Sitz des Unternehmens bzw. der Unternehmensteile, derjenigen Länder, deren Staatsangehörigkeit die beteiligten Personen besitzen sowie des Landes, in welchem Handlungen oder Geschäfte vor-

⁹¹ Ist die Rechtslage in einem Land strenger als in dem Land, auf deren Rechtslage die Richtlinie basiert, so müssen selbstverständlich strengere nationale Gesetze beachtet werden.

genommen werden. Aufgrund dieser Komplexität werden Richtlinien und Policies selten in der Lage sein, strafrechtliche Gefahren ganz auszuschließen, sie können aber für die wesentlichen Gefahren auf ein absolutes Minimum reduziert werden.

3.4.3.2 Branchenregelungen oder Richtlinien

In verschiedenen Bereichen haben Branchenverbände oder Interessenvereinigungen Regelwerke oder Handreichungen entworfen, die Korruptionsrisiken minimieren sollen.⁹²

Oftmals dienen diese Regelungen dazu, eine „Best Practice“ zu entwickeln. Obgleich diese privaten Regelwerke unverbindlich sind, werden sie doch zunehmend einen Mindeststandard bilden, von dem erwartet wird, dass branchenangehörige Unternehmen ihn beachten. Umgekehrt gilt dies allerdings nicht: Die Beachtung einer Branchenregelung führt nicht automatisch dazu, dass damit das Vorliegen hinreichender organisatorischer Voraussetzungen bejaht werden kann. Jedenfalls aber können diese Richtlinien einen Steinbruch an Ideen und Anregungen zur Ausgestaltung der auf die Bedürfnisse ihres jeweiligen Unternehmens zugeschnittenen Richtlinien und Policies bieten.

3.4.3.3 Wesentliche Policies

Welche Richtlinien und Policies in einem Unternehmen umgesetzt werden sollen, hängt entscheidend von der konkreten Risikosituation sowie der Größe des Unternehmens ab. Je häufiger Mitarbeiter typischerweise mit den nachstehend genannten Konstellationen in Berührung kommen und je dezentralisierter dies geschieht, desto mehr wird sich die Erstellung einer Richtlinie oder Policy aufdrängen.

3.4.3.3.1 Geschenke und Einladungen

Geschenke haben regelmäßig einen Vermögenswert und stellen daher korruptionsrelevante Vorteile dar. Gleichermaßen gilt für Einladungen zu Kultur- und Sportveranstaltungen, Messen, Hotelaufenthalte, Reisen oder ähnliches.

Rechtlich nicht zu beanstanden sind Geschenke, die nicht über bloße Anstands- und Höflichkeitsgeschenke, übliche Werbe-, Gast- und Repräsentationsgeschenke hinaus-

⁹² Kodex zur Abgrenzung von legaler Kundenpflege und Korruption, https://absatzwirtschaft.de/wp-content/uploads/archiv-pdf/Compliance_Kodex_Arbeitskreis_Corporate_Compliance_2010.pdf (aufgerufen am 23.8.2024); Leitfaden Hospitality und Strafrecht, <https://vsa-ev.de/wp-content/uploads/2018/02/Hospitality-und-Strafrecht-ein-Leitfaden.pdf> (aufgerufen am 23.8.2024); Gemeinsamer Standpunkt zur strafrechtlichen Bewertung der Zusammenarbeit zwischen Industrie, medizinischen Einrichtungen und deren Mitarbeitern, <https://www.bvmed.de/download/gemeinsamer-standpunkt.pdf> (aufgerufen am 23.8.2024); FSA-Kodex für die Zusammenarbeit der pharmazeutischen Industrie mit Ärzten, Apothekern und anderen Angehörigen medizinischer Fachkreise, <https://www.fsa-pharma.de/der-fsa/ueber-uns/kodizes-auf-einen-blick/> (aufgerufen am 23.8.2024); BME-Verhaltensrichtlinie, <https://www.bme.de/services/zertifizierungen/bme-code-of-conduct/> (aufgerufen am 23.8.2024); ICC Rules on Combating Corruption, <https://www.iccgermany.de/standards-incoterms-verhaltensrichtlinien/korruptionspraevention-und-bekaempfung/> (aufgerufen am 23.8.2024).

gehen.⁹³ Hingegen sind Zuwendungen, die nicht mehr als geringwertig anzusehen sind, mit Risiken verbunden. Was noch als geringwertig und üblich angesehen wird, mag von Land zu Land variieren und hängt oftmals von den Umständen und dem Anlass einer Zuwendung und insbesondere von den Lebensverhältnissen des Empfängers ab. In Deutschland dürften Geschenke mit einem Wert über 25 € bei Amtsträgern bzw. 50 € im geschäftlichen Bereich im Regelfall kaum noch als geringwertig anzusehen sein. Sind in bestimmten Bereichen, insbesondere bei Amtsträgern, durch dienstliche Vorschriften bestimmte Grenzwerte festgesetzt, bestimmen diese wesentlich die Sozialadäquanz mit. Auch in Ländern mit einer ausgesprochenen Geschenkkultur ist zu beachten, dass dort feine Differenzierungen zwischen dem, was Sitte und Anstand gebieten und dem gemacht werden, was schon korruptiven Charakter hat. Vor einem zu leichtfertigen Umgang mit Geschenken im Ausland ist zu warnen, denn meist werden deutsche Ermittlungsbehörden über die Angemessenheit urteilen und ihre eigenen Anschauungen zugrunde legen.

Die Vorgabe von Wertgrenzen⁹⁴ für Geschenke ist ein sinnvolles Mittel zu Steuerung von Zuständigkeits- und Genehmigungsprozessen, auch wenn absolute Wertgrenzen angesichts unterschiedlicher Kaufkraft und Einkommensverhältnisse der Empfänger nur bedingt Rückschluss auf die Eignung zur Beeinflussung von Entscheidungen zulassen.

In manchen Situationen kann die Zurückweisung eines meist höherwertigen Geschenkes nachteilige Auswirkungen auf die Geschäftsbeziehung haben. Lassen sich diese nicht schon dadurch abfedern, dass der Geschäftspartner im Voraus über die eigene Geschenkerichtlinie informiert und gebeten wird, keine Zuwendung über die dort zugelassenen Fälle hinaus zu machen, bietet es sich an, das Geschenk dem eigenen Unternehmen zur Verfügung zu stellen und den Schenker nachträglich unter Hinweis auf die internen Compliance Vorschriften hierüber schriftlich zu informieren.⁹⁵

Vergleichbares gilt für Einladungen zu Veranstaltungen, die nicht ausschließlich geschäftlichen Charakter besitzen, sondern ganz oder teilweise Freizeit- oder Eventcharakter tragen.⁹⁶ Auch wenn die Durchführung von Freizeitaktivitäten grundsätzlich nicht zu beanstanden ist, beispielsweise Unternehmungen mit Besuchern am Abend oder die Unter-

⁹³ Bömer, Anti-Korruption-Compliance – Einladungen, Geschenke oder „kulante“ Zugeständnisse an öffentliche Amtsträger als Problem, GWR 2011, 28; Reiff, Von kleinen Aufmerksamkeiten und großen Geschenken – was ist erlaubt? „Eine Tasse Kaffee? Nein danke!“ – Wo fängt Korruption an?, CCZ 2018, 194; Reiff, Dienst- und strafrechtliche Risiken bei Einladungen oder der Überlassung von Freikarten für hochrangige Amtsträger, CCZ 2020, 142.

⁹⁴ Marschlich, Praxis der Compliance-Organisation: Geschenke und Einladungen, CCZ 2010, 110.

⁹⁵ Bereits die Annahme eines Vorteils kann zu einer strafbaren Bestechungshandlung führen. Das Schreiben an den Zuwender dient der Dokumentation, dass der Empfänger zu keinem Zeitpunkt eine Unrechtsvereinbarung erstrebt hat.

⁹⁶ Acker/Ehling, Einladung in die Business-Lounge? – Strafbarkeitsrisiko bei Vergabe oder Annahme von Einladungen im geschäftlichen Verkehr, BB 2012, 2517; Eckstein/Püsche, O’zapft is! – Compliance-Risiken bei Einladungen zu Veranstaltungen, Newsdienst Compliance, 2515, 71003.

haltung einer Delegation über das Wochenende, sind Korruptionsrisiken umso höher, je geringer die nachvollziehbaren geschäftlichen Elemente sind.

Gerade bei Geschenken und Einladungen ist im Einzelfall nur sehr schwer zu entscheiden, ob diese zulässig oder korruptionsrelevant sind. Nach der Rechtsprechung⁹⁷ ist anhand einer Gesamtschau aller Umstände zu beurteilen, ob eine Zuwendung oder Einladung zulässig ist. Indizien sind unter anderem:

- Plausibilität einer legalen Zielsetzung (!)
- Stellung des Empfängers
- Dienstliche oder geschäftliche Beziehung des Empfängers zum Zuwendenden
- Art der Zuwendung
- Wert der Zuwendung
- Häufigkeit der Zuwendung
- Zeitliche Nähe zu geschäftlichen oder dienstlichen Entscheidungen
- Vorgehensweise bei der Zuwendung.

Weitere Kriterien können sein, ob die Zuwendung oder Einladung jedem Kunden oder nur ausgewählten Kunden gewährt werden, ob der Empfänger aufgrund seiner Stellung Repräsentationsaufgaben wahrnimmt, ob die Auswahl des Empfängers durch den Zuwendenden oder die Dienststelle bzw. das Kundenunternehmen erfolgt ist etc.⁹⁸ Für eine Risikobewertung werden oftmals Ampelmodelle⁹⁹ verwendet.

Je nach Risikosituation kann es zudem sinnvoll sein, ein Verzeichnis der an die jeweiligen Empfänger gewährten Zuwendungen und ausgesprochenen Einladungen zu führen.

Auch kann in der Policy geregelt werden, auf welche Art und Weise die Zuwendung eines Geschenks oder einer Einladung zu erfolgen hat. Mit zunehmendem Wert einer Zuwendung ist nämlich der Empfänger seinerseits erheblichen Risiken ausgesetzt. So kann die Annahme einer Einladung in eine VIP-Arena zu einem Fußballspiel ohne Wissen des Arbeitgebers eine fristlose Kündigung rechtfertigen.¹⁰⁰

Bei Ausgestaltung einer Geschenke- und Einladungsrichtlinie ist auch darauf zu achten, dass die Gewährung oder Annahme steuerliche Folgen nach sich zieht, sowohl was die

⁹⁷ BGH NStZ 2008, 688, 691 f.; Pelz, Sponsoring – zwischen Marketing und Korruption, LMUR 2009, 50.

⁹⁸ Reiff, Dienst- und strafrechtliche Risiken bei Einladungen oder der Überlassung von Freikarten für hochrangige Amtsträger, CCZ 2020, 142.

⁹⁹ Jakob, Das Ganze ist mehr als die Summe seiner Teile – eine praxisorientierte Anwendung des „Ampel-Kodex“ im Kontext von Einladungen und Geschenken, CCZ 2010, 61; Kodex zur Abgrenzung von legaler Kundenpflege und Korruption, Seite 5 ff.

¹⁰⁰ LAG Rheinland-Pfalz, Beck RS 2009, 56479; Pelz, Compliance-Risiko: VIP-Lounges, CCZ 2010, 73.

Zulässigkeit des Betriebsausgabenabzugs der Aufwendungen als auch die Lohnsteuerpflicht als geldwerter Drittvoteil auf Seiten des Empfängers betrifft. Es ist daher sicherzustellen, dass die Steuerabteilung von den steuerlich relevanten Informationen Kenntnis erlangt.

3.4.3.3.2 Spenden und Sponsoring

Spenden sind unentgeltliche Zuwendungen, die ohne Erwartung einer bestimmten Gegenleistung gegeben werden. Da auch die Zuwendung an einen Dritten einen Vorteil im Sinne der Korruptionstatbestände darstellen kann, können auch Spenden Korruptionsrisiken in sich bergen, wenn Gegenstand einer ausdrücklichen oder stillschweigenden Absprache mit einem Amtsträger, Abgeordneten oder Angestellten ist, dass eine Spende an einen (gemeinnützigen) Verein oder eine sonstige Institution geleistet werden soll. Auch Partei- oder Wahlkampfspenden können strafrechtlich relevant sein, denn es kann sich dabei um einen unzulässigen Drittvoteil handeln, wenn nicht nur die politische Willensbildung an sich unterstützt werden soll, sondern Hintergrund die Erwartung künftiger Sondervorteile für den Spendenden sind.¹⁰¹ Selbst wenn (Partei-)Spenden strafrechtlich nicht zu bestanden sind, können sie im Einzelfall doch Reputationsgefahren nach sich ziehen.

Im Gegensatz zu Spenden findet bei Sponsoring-Aktivitäten ein Leistungsaustausch statt. Für die finanzielle Unterstützung erhält der Sponsor die Gelegenheit zur Werbung, beispielsweise durch die Möglichkeit, sich zu präsentieren, einen Informationsstand zu betreiben, Abdruck von Logos auf Plakaten, Publikationen oder Ähnlichem, oftmals auch ein Paket von Eintrittskarten mit der Möglichkeit, Gäste zur Veranstaltung einzuladen. Der Abschluss einer Sponsoring-Vereinbarung selbst kann als Drittvoteil Gegenstand einer Unrechtsvereinbarung sein, insbesondere wenn die Spende oder Sponsoringleistung Voraussetzung für andere Geschäfte sein soll. Größere Risiken als bei der Ein gehung eines Sponsorings bestehen bei der Einladung von Geschäftspartnern zu gesponserten Veranstaltungen.

Auch die Entscheidung, ob und in welchem Umfang Spenden oder Sponsoring getätigkt werden, kann Gegenstand einer Regelung sein. Zwar haben Unternehmen einen weiten Entscheidungsspielraum, ob und in welchem Umfang sie Spenden- und Sponsoringleistungen erbringen wollen. Diese dürfen aber nicht völlig außer Verhältnis zur Vermögens- und Ertragslage des Unternehmens stehen, müssen einen Zusammenhang mit der unternehmerischen Tätigkeit bzw. einem betrieblichen Zweck haben, die Auswahl der Empfänger muss frei von individuellen Eigeninteressen der Geschäftsleitung sein und die Entscheidung muss transparent erfolgen unter Einbindung der ggf. zuständigen Stellen.¹⁰²

¹⁰¹ BGHSt 49, 275, 294; 56, 203; Fischer, StGB, § 331 Rn. 28 f.

¹⁰² BGH NJW 2002, 1582, 1587.

3.4.3.3 Berater und Vermittler

In vielen Regionen der Welt wird es erforderlich sein, mit Beratern oder Vermittlern zusammenzuarbeiten, insbesondere dann, wenn Unternehmen neue Märkte erschließen oder über keine hinreichenden eigenen Landesgesellschaften dort verfügen. Sofern nicht im Einzelfall, in manchen Staaten bei Geschäften mit Regierungsstellen, der Einsatz von Beratern oder Vermittlern untersagt oder Beschränkungen unterworfen ist, bestehen hiergegen auch aus Compliance-Sicht keine Bedenken. Allerdings bestehen dennoch Gefahren, waren solche Intermediäre doch in vielen Korruptionsfällen die Drehscheibe zur Verschleierung oder Durchführung von Schmiergeldzahlungen. Zudem drohen nicht unerhebliche steuerliche Risiken, wenn die Leistungserbringung nicht darlegt oder der hinter der ausländischen Person stehende wirtschaftlich Berechtigte nicht benannt werden kann.¹⁰³ Unternehmen haben daher sicherzustellen, dass sie nur mit seriösen Beratern und Vermittlern zusammenarbeiten, die tatsächlich die vertraglich geschuldete Leistung erbringen. Auch wenn Korruptionshandlungen durch Berater oder Vermittler nie sicher ausgeschlossen werden können, muss die Wahrscheinlichkeit doch auf ein Minimum reduziert werden. Dies erfordert einen strukturierten Auswahlprozess¹⁰⁴ (Geschäftspartner Due Diligence) mit entsprechender Dokumentation. Zunächst sollte derjenige, der auf Berater und Vermittler zurückgreifen möchte, erläutern, aus welchen Gründen auf die Dienste eines Beraters und Vermittlers zurückgegriffen werden soll und warum der in Betracht gezogene Geschäftspartner hierfür geeignet ist. Typischerweise werden wesentliche Informationen über den Geschäftspartner im Wege einer Selbstauskunft eingeholt, namentlich:

- Firmierung, Anschrift, Rechtsform, gesetzliche Vertreter
- Gesellschafter
- Unternehmensgröße (z. B. Mitarbeiterzahl, Umsatz, Tätigkeitsgebiet)
- Beschreibung des Unternehmens
- Kunden, Referenzen
- Beziehung zu potenziellen Kunden
- Handelsregistereintragungen, Gewerbeanmeldungen, erforderliche Genehmigungen und Lizenzen

¹⁰³ In diesen Fällen kann schon wegen eines nicht ersichtlichen geschäftlichen Bezugs die Betriebsausgabeneigenschaft angezweifelt oder aber nach § 160 AO der Betriebsausgabenabzug ganz oder teilweise versagt werden. U.U. muss auch damit gerechnet werden, dass die Finanzbehörden im Wegen von Spontanauskünften Meldungen über Zahlungen an ausländische Finanzbehörden machen; vgl. dazu Pelz, „Grenzenlose“ Spontanauskünfte – Eine Gefahr für international tätige Unternehmen?, RIW 2007, 467.

¹⁰⁴ Rieder in Inderst/Bannenberg/Poppe, Compliance, Kap. 5 Rn. 323 ff.; Trossbach, Geschäftspartner-Compliance- Wichtig wie nie zuvor, aber wie etabliert mein Unternehmen einen angemessenen Prozess? CCZ 2017, 216; Frank-Fahle/Schuldt, Geschäftspartner-Compliance und Korruptionsprävention im internationalen Anlagenbau: Rechtliche Rahmenbedingungen, Auswirkungen von Compliance-Verstößen und Schutzmaßnahmen, ZfBR 2018, 419; Mössner/Kerner, Praxisbeitrag: Einführung konzernweiter Standards für die Geschäftspartner-Prüfung, CCZ 2011, 182.

- Referenzen
- Compliance Informationen.

Die in der Selbstauskunft genannten Informationen sollten der Intensität nach abgestuft je nach Risikobewertung des Geschäftspartners und der beabsichtigten Zusammenarbeit anhand öffentlich zugänglicher Quellen, insbesondere anhand von Compliance-Datenbanken, überprüft werden. Je nach Risikolage ist darüber hinaus eine intensive Due Diligence der Berater und Vermittler angezeigt. Die Geschäftspartnerprüfung sollte in regelmäßigen Abständen wiederholt werden, um zu gewährleisten, dass der Geschäftspartner auch weiterhin als integer anzusehen ist.

Auch der Inhalt von Verträgen mit Beratern und Vermittlern sollte standardisiert sein. In der Vertragsdurchführung ist auf folgende Punkte zu achten:

- klare Leistungsbeschreibung
- angemessene Vergütungshöhe
- nachvollziehbare Zahlungskonditionen
- plausibler Zahlungsweg
- Dokumentation der Leistungserbringung
- Compliance-Klauseln¹⁰⁵ (Verpflichtung zur Einhaltung aller Gesetze und Compliance-Vorgaben des Auftraggebers, ggf. auch Auditrechte)
- Informations- und Kündigungsrechte.

Besonders ist bei der Einrichtung des Prozesses darauf zu achten, dass Regeln vorhanden sind, die sich mit der ausreichenden Dokumentation der tatsächlichen Leistungserbringung durch den Berater oder Vermittler sowie mit der Aufbewahrung und Speicherung dieser Nachweise befassen. Bei der Durchführung von Due Diligence Prüfungen sind auch die Prüfungsergebnisse zu dokumentieren.

3.4.4 Geschäftspartner, Joint Venture und M&A Due Diligence

Eine Due Diligence von Geschäftspartnern,¹⁰⁶ Joint-Venture-Partnern und bei M&A-Transaktionen, auch auf Compliance-Risiken hin, ist besonders bei Geschäftstätigkeit in kritischen Regionen eine Notwendigkeit. Vielfach wird das Handeln von Geschäftspartnern zivil- oder strafrechtlich unmittelbar dem Unternehmen zugerechnet,¹⁰⁷ mit entsprechenden Strafbarkeits- und Haftungsrisiken. Oftmals genügen schon geringe Prüfungsschritte zur

¹⁰⁵ Gilch/Pelz, Compliance-Klauseln – Gutgemeint, aber unwirksam?, CCZ 2008, 131.

¹⁰⁶ Eine Empfehlung zur Prüfung hat u. a. die Internationale Handelskammer, Paris, herausgegeben, <http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2010/ICC-Guidelines-on-Agents,-Intermediaries-and-Other-Third-Parties/> (aufgerufen am 7.2.2024).

¹⁰⁷ Section 7 UK Bribery Act 2010.

Enttarnung von Schein- und Briefkastenfirmen oder zur Untermauerung einer tatsächlichen operativen und nachhaltigen Geschäftstätigkeit in den entsprechenden Märkten.

Besondere wirtschaftliche Bedeutung kommt der Due Diligence von Joint-Venture-Partnern und bei M&A-Geschäften zu, um Compliance-Risiken bei der Eingehung von Beteiligungen und bei Erwerben zu minimieren. Eine Unternehmensbeteiligung kann schnell deutlich an Wert verlieren oder gar wertlos sein, wenn später gegen das Target oder das Joint Venture Unternehmensstrafen oder Finanzsanktionen wegen Straftaten oder sonstigen Rechtsverstößen verhängt werden. Zudem besteht die Gefahr, dass bei kriminellen Geschäften die Dividendenausschüttung oder die Unternehmensbeteiligung selbst als Objekt einer Geldwäsche gelten könnte und damit kaum mehr verkehrsfähig ist.

Bei einer Compliance Due Diligence wird es aufgrund der Kürze der zur Verfügung stehenden Zeit und der Abhängigkeit von den zur Verfügung gestellten Unterlagen und Informationsmöglichkeiten kaum möglich sein, eine vollständige Untersuchung vorzunehmen. Oftmals bleibt nur die Möglichkeit, eine vorläufige Risikobewertung vorzunehmen oder zu eruieren, ob Umstände vorliegen, die den Deal vollständig scheitern lassen. Eine hinreichend aussagekräftige Beurteilung wird alleine anhand von Dokumenten kaum möglich sein, vielmehr wird es notwendig sein, Hintergrundinformationen zu sammeln und Informationsgespräche mit Verantwortlichen des Zielunternehmens zu führen.

Im Rahmen einer Due Diligence¹⁰⁸ werden zusätzlich zu den Hintergrundinformationen zur Gesellschaft, ihren Gesellschaftern und Organen insbesondere u. a. noch folgende Felder geprüft:

- Länderrisiken im Tätigkeitsgebiet
- Industrie- und branchenspezifische Risiken
- produktbezogene Risiken
- Risiken des Geschäftsmodells
- vertriebsbezogene Risiken (Vertriebsstruktur, Vertriebspartner, Berater, Vermittler)
- Compliance-Programm und Compliance-Organisation
- Ermittlungen und Untersuchungen.

3.4.5 Schulungen und Trainings

Alleine die Erstellung eines Code of Conducts, von Richtlinien und Policies genügt zur Erlangung einer hinreichenden Compliance nicht. Den Mitarbeitern müssen die geltenden unternehmensinternen Regelungen auch nahegebracht und es muss sichergestellt werden, dass sie von den Mitarbeitern auch verstanden werden. Oftmals ist nämlich bereits die Existenz derartiger Regelwerke im Unternehmen weitgehend unbekannt. Schulungen und Trainings können in unterschiedlichster Form angeboten werden, Präsenzschulungen durch interne oder externe Trainer, webbasierte Trainings (E-Learnings) u. a. Empfehlenswert ist ein Mix verschiedener Schulungsarten. Allen Mitarbeiter sollten die Grundzüge

¹⁰⁸ Rieder in Inderst/Bannenberg/Poppe, Compliance, Kap. 5 Rn. 262 ff.

der Anti-Korruptions-Compliance nahegebracht werden. Intensivere Trainings sind notwendig für Mitarbeiter, die in korruptionsgefährdeten Bereichen tätig sind oder Führungsverantwortung ausüben. Ziel der Trainings ist, die Mitarbeiter hinreichend für Gefahren zu sensibilisieren und sie zu motivieren, rechtzeitig um Rat zu fragen. Empfehlenswert ist es, Schulungs- und Trainingsinhalte zu dokumentieren. Sichergestellt werden muss, dass alle Mitarbeiter, die mit Korruptionsrisiken in Berührung kommen, geschult werden. Es ist daher nachzuhalten, dass alle Mitarbeiter an derartigen Schulungen teilgenommen haben. Die Dokumentation von Teilnehmerlisten ist sinnvoll.

3.4.6 Hinweisgebersysteme

Eine wesentliche Rolle bei der Aufdeckung von Korruption oder anderen strafbaren Handlungen spielen Hinweisgebersysteme. Deren Einführung ist ohnehin aufgrund der EU-Whistleblower-Richtlinie und nach § 12 Abs. 1 HinSchG für Unternehmen mit mehr als 49 Mitarbeitern verpflichtend. Korruption spielt sich in Unternehmen selten im Geheimen ab, weil alleine aufgrund unterschiedlicher Zuständigkeits- und Genehmigungsprozesse meist eine Mehrzahl von Personen direkt oder indirekt involviert sind. Mitarbeiter sind daher eine wertvolle Quelle, um frühzeitig Informationen zu Fehlentwicklungen und Missständen zu erhalten.

3.4.7 Audits und interne Untersuchungen

Für eine wirksame Anti-Korruptions-Compliance reicht es nicht aus, Richtlinien und Prozesse zu entwerfen, an die sich Mitarbeiter zu halten haben. Erforderlich ist auch, die tatsächliche Einhaltung der Prozesse zu überprüfen und zu überwachen. Dies hat grundsätzlich zumindest stichprobenweise und anlassunabhängig zu erfolgen (sog. Compliance Audits),¹⁰⁹ nicht erst dann, wenn Verdachtsfälle bekannt geworden sind. Weites Ermessen haben Unternehmen darin, festzulegen, welche Art von Prüfungen durchgeführt werden sollen und wie die Verantwortung für Prüfungen auf operative Einheiten, Compliance-Organisation, interne Revision oder andere interne oder externe Stellen verteilt werden sollen. Bei besonders hohen Compliance-Risiken ist eine Prüfung durch die Compliance-Organisation oder in deren Auftrag sinnvoll.

Werden Verdachtsfälle auf Korruptionshandlungen bekannt, ist eine Aufklärung (sog. internal investigation¹¹⁰) erforderlich, insbesondere um sicherzustellen, dass keine wiederholten oder gar systematischen Rechtsverletzungen erfolgt sind.¹¹¹ Ob diese Untersuchungen durch interne Stellen (z. B. Revision, Compliance-Abteilung), durch externe

¹⁰⁹ Liese/Schulz, Risikomanagement durch Compliance-Audits, BB 2011, 1347.

¹¹⁰ Vgl. hierzu ausführlich Knierim/Rübenstahl/Tsambikakis, Internal Investigations.

¹¹¹ Fuhrmann, Internal Investigations: Was dürfen und was müssen Organe beim Verdacht von Compliance Verstößen tun?, NZG 2016, 881.

Ermittler oder in einer Kombination zwischen beiden durchgeführt werden, hängt von der Situation ab. Eine externe Untersuchung hat oftmals den Vorteil größerer Unabhängigkeit und höherer Glaubwürdigkeit, insbesondere wenn die Untersuchungsergebnisse zur Grundlage der Rechtsverfolgung (z. B. Geltendmachung von Schadensersatzansprüchen etc.) oder der Offenlegung gegenüber Ermittlungsbehörden dienen sollen. Zudem verfügen externe Ermittler oftmals über größere Expertise und Erfahrung in der Durchführung derartiger Ermittlungen. In vielen Fällen werden interne Untersuchungen zu keiner vollständigen Aufklärung des Sachverhalts führen, sondern nur mehr oder weniger umfangreiche Verdachtsmomente zutage fördern. Eine weitergehende Aufklärung wird oftmals allenfalls durch Amnestiezusagen an beteiligte Mitarbeiter¹¹² oder nur durch die den Ermittlungsbehörden zustehenden Zwangsmaßnahmen möglich sein, was dann eine Strafanzeige voraussetzt.

3.4.8 Reaktion auf entdecktes Fehlverhalten

Werden bei Untersuchungen Verstöße gegen interne Richtlinien oder gar strafrechtlich relevantes Verhalten entdeckt, ist es notwendig, alle Maßnahmen zu ergreifen, um eine Wiederholung für die Zukunft auszuschließen. Dies dürfte es regelmäßig erfordern, auf erkanntes Fehlverhalten zu reagieren („zero tolerance“).¹¹³ Dies bedeutet nicht, dass jeder Verstoß zwangsläufig eine Kündigung nach sich ziehen muss. Jedoch darf eine Regelverletzung nicht folgenlos bleiben, da anderenfalls der Eindruck erweckt wird, das Unternehmen billige stillschweigend korrupte Praktiken.¹¹⁴ Je nach Schwere des Verstoßes und den jeweiligen Umständen ist eine angemessene Reaktion erforderlich, die von einer Compliance-Nachschulung über eine Abmahnung, eine Versetzung oder eine Beendigungskündigung reichen kann.

3.4.9 Strafanzeige und Offenbarung gegenüber Ermittlungsbehörden

Eine Verpflichtung, Gesetzesverstöße den Ermittlungsbehörden zu melden, besteht nach deutschem Recht grundsätzlich nicht.¹¹⁵ Allerdings können manche ausländische Rechtsordnungen entsprechende Meldepflichten beim Verdacht von Korruptionsfällen oder aber die Möglichkeit zur Erlangung von Straffreiheit bei einer Selbstanzeige vor einer Tatentdeckung durch Ermittlungsbehörden vorsehen. Eine Anzeigepflicht kann sich auch aus steuerlichen Vorschriften, namentlich § 153 AO ergeben, wenn nachträglich erkannt wird, dass in der Vergangenheit Zahlungen geleistet wurden, denen entweder kein Betriebsaus-

¹¹² Annuss/Pelz, Amnestieprogramme – Fluch oder Segen?, BB Special 4 – 2010, 21 ff.

¹¹³ Kark, Die Zero-Tolerance-Regel, CCZ 2012, 180.

¹¹⁴ Reichert, Reaktionspflichten und Reaktionsmöglichkeiten der Organe auf (möglicherweise) strafrechtsrelevantes Verhalten innerhalb des Unternehmens, ZIS 2011, 113, 119.

¹¹⁵ § 138 StGB enthält eine Verpflichtung zur Mitteilung bei bestimmten schweren bevorstehenden Straftaten. Korruptionsdelikte gehören jedoch nicht hierzu.

gabentypus zukommt oder bei denen ein Betriebsausgabenabzugsverbot besteht, wie nach § 4 Abs. 5 Satz 1 Nr. 10 EStG bei Schmiergeldzahlungen. In diesem Fall kann sich mittelbar die Notwendigkeit einer Meldung auch an die Ermittlungsbehörden ergeben, da die Finanzbehörden bei Vorliegen von Verdachtsmomenten ohnehin zu einer Information der Strafverfolgungsbehörden verpflichtet sind. Auch im Hinblick auf sonst mögliche faktitative oder zwingende Vergabesperren kann eine Mitteilung an die Ermittlungsbehörden sinnvoll sein, um eine hinreichende Selbstreinigung zur Wiederherstellung der Zuverlässigkeit nachzuweisen.

Im Übrigen bedarf es einer sorgfältigen Abwägung, ob und wann eine freiwillige Meldung an die Ermittlungsbehörden Sinn macht.¹¹⁶ In der öffentlichen Wahrnehmung ist eine freiwillige Offenbarung erkannter Sachverhalte an die Ermittlungsbehörden ein Umstand, der positiv wahrgenommen wird und den negativen Umstand des Korruptionsverdachts sogar überlagern kann. Bei einer freiwilligen Meldung können regelmäßig auch Zwangsmaßnahmen wie Durchsuchungen vermieden werden. Zudem wird sich eine Kooperation positiv in der Bemessung der Unternehmensgeldbuße niederschlagen. Allerdings wird eine freiwillige Offenbarung nahezu zwangsläufig die Verhängung einer Unternehmensgeldbuße und jedenfalls die Abschöpfung des wirtschaftlichen Vorteils, d. h. mindestens des Gewinns aus einem korruptiv erlangten Auftrag,¹¹⁷ ggf. auch sonstiger mittelbarer Vorteile wie z. B. Service- und Dienstleistungsverträge, verbesserte Wettbewerbsposition o. ä., nach sich ziehen, sodass die Offenbarung möglicherweise einen sehr hohen finanziellen Schaden mit sich bringt. In Fällen mit Auslandsberührungen ist darüber hinaus in Betracht zu ziehen, welche Auswirkungen dies auf die Strafverfolgung in anderen Staaten haben kann, insbesondere bei zweifelhafter Rechtsstaatlichkeit bzw. bei sonst drohenden exorbitanten Sanktionen.

Literatur

- ANDROULAKIS, IOANNIS, Die Globalisierung der Korruptionsbekämpfung, 2006
BOCK, DENNIS, Criminal Compliance, 2011
BOCK, DENNIS/BORRMANN, LISA, Vorteilsnahme (§ 331 StGB) und Vorteilsgewährung (§ 333 StGB) durch Kultursponsoring?, ZJS 2009, 625
DANNECKER, CHRISTOPH, Die Folgen der strafrechtlichen Geschäftsherrenhaftung der Unternehmensleitung für die Haftungsverfassung juristischer Personen, NZWiSt 2012, 441
DÖLLING, DIETER (Hrsg.), Handbuch der Korruptionsprävention, 2007
FISCHER, THOMAS, Strafgesetzbuch, 71. Aufl. 2024
GILCH, ANDREAS/PELZ, CHRISTIAN, Compliance-Klauseln – Gut gemeint aber unwirksam?, CCZ 2008, 131
INDERST, CORNELIA/BANNENBERG, BRITTA/POPPE, SINA (Hrsg.), Compliance, 3. Aufl. 2017
HAAG, OLIVER/CURIC, LEJLA, Business Partner Compliance – Vorgehensweise und Prozessschritte, CB 2022, 381

¹¹⁶ Reichert, Reaktionspflichten und Reaktionsmöglichkeiten der Organe auf (möglicherweise) strafrechtsrelevantes Verhalten innerhalb des Unternehmens, ZIS 2011, 113, 121.

¹¹⁷ Köhler, Die Reform der strafrechtlichen Vermögensabschöpfung, NStZ 2017, 497, 507; BGHSt 50, 299, 309; NStZ 2012, 381 [zum alten Einziehungsrecht].

- HAUSCHKA, CHRISTOPH/MOOSMAYER, KLAUS/LÖSLER, Thomas (Hrsg.), Corporate Compliance, 3. Aufl. 2016
- HAUSCHKA, CHRISTOPH, Compliance am Beispiel der Korruptionsbekämpfung, ZIP 2004, 877
- HAUSCHKA, CHRISTOPH/GREEVE, GINA, Compliance in der Korruptionsprävention – Was müssen, was sollen, was können die Unternehmen tun?, BB 2007, 165
- ERB, VOLKER/SCHÄFER, JÜRGEN (Hrsg.), Münchener Kommentar Strafgesetzbuch, 4. Aufl. 2020 ff.
- KINDHÄUSER, URS/NEUMANN, ULFRIED/PAEFFGEN, ULLRICH/SALIGER, FRANK (Hrsg.), Strafgesetzbuch, 6. Aufl. 2023
- KNIERIM/RÜBENSTAHL/TSAMBIKAKIS (Hrsg.), Internal Investigations, 2. Aufl. 2016
- KRÄMER, THOMAS/KLARHOLD, CHRISTOPH, Compliance-Programme in Industriekonzernen, ZGR 2010, 1113
- LIESE, JENS/SCHULZ, MARTIN, Risikomanagement durch Compliance-Audits, BB 2011, 1347
- MITTELSDORF, KATHLEEN, Zur Reichweite individueller strafrechtlicher Verantwortung im Unternehmen für Fehlverhalten von unterstellten Mitarbeitern, ZIS 2011, 123
- MOOSMAYER, KLAUS, Compliance-Risikoanalyse, 2. Aufl. 2020
- NEPOMUCK, LUTZ/GROSS, BERND, Zuwendungen an den Anstellungsbetrieb als Drittvoorteile im Sinne des § 299 StGB?, wistra 2012, 132
- PELZ, CHRISTIAN, Steuerliche und strafrechtliche Schritte zur Bekämpfung der Korruption im Auslandsgeschäft, WM 2000, 1566
- PELZ, CHRISTIAN, Die Bekämpfung der Korruption im Auslandsgeschäft, StraFo 2000, 300
- PELZ, CHRISTIAN, Compliance-Risiko: VIP-Lounges, CCZ 2010, 73
- PEDROVIC, MARTIN, Geschäftspartnerprüfungen als Maßnahme zur Korruptionsprävention, 2017
- REICHERT, JOCHEM, Reaktionspflichten und Reaktionsmöglichkeiten der Organe auf (möglichweise) strafrechtsrelevantes Verhalten innerhalb des Unternehmens, ZIS 2011, 113
- SATZGER, HELMUT, Bestechungsdelikte und Sponsoring, ZStW 115 (2003), 469
- SCHÖNKE/SCHRÖDER (Hrsg.), Strafgesetzbuch, 30. Aufl. 2019
- SCHORN, MARTIN, Neuere Entwicklungen in der europäischen Korruptionsbekämpfung gegenüber Unternehmen, WM 2011, 1689
- UMNUß, KARSTEN, Corporate-Compliance Checklisten, 5. Auflage 2022



Professor Dr. Christian Pelz ist Rechtsanwalt, Fachanwalt für Strafrecht und Fachanwalt für Steuerrecht und leitet den Bereich Wirtschafts- und Steuerstrafrecht der internationalen Sozietät Noerr Partnerschaftsgesellschaft mbB. Sein Tätigkeitsbereich umfasst die Vertretung und Verteidigung von Unternehmen und Unternehmensleiter in wirtschafts- und steuerstrafrechtlichen Ermittlungsverfahren, die Beratung von Unternehmen bei der Implementierung und der Durchführung von Compliance-Management-Systemen sowie die Durchführung von Compliance Audits und Internal Investigations. Professor Dr. Christian Pelz veröffentlicht regelmäßig zu wirtschafts- und steuerstrafrechtlichen Themen sowie zu Compliance Fragen und ist Referent auf vielen Veranstaltungen. Professor Dr. Christian Pelz ist Honorarprofessor für Strafrecht an der Universität Augsburg.



Competition Compliance

4

Christian Heinichen

Inhaltsverzeichnis

4.1	Einleitung	76
4.2	Kartellrechtliche Risiken	76
4.2.1	Kontakte zu Wettbewerbern	76
4.2.2	Beziehungen zu Lieferanten und Händlern	78
4.2.3	Missbrauch von Marktmacht	79
4.2.4	Risiken bei M&A-Transaktionen	80
4.3	Folgen von Kartellverstößen	81
4.3.1	Geldbußen	81
4.3.2	Schadenersatz	82
4.3.3	Persönliche Verantwortung	83
4.3.4	Vergaberechtliche Folgen	84
4.3.5	Weitere Folgen	84
4.4	Nachhaltige Wertschöpfung durch effektive Competition Compliance	85
4.5	Kartellverfahren	85
4.5.1	Wettbewerbsbehörden	85
4.5.2	Kartellbußgeldverfahren	86
4.5.3	Kartellschadenersatzverfahren	87
4.6	Kartellrechtliche Compliance-Maßnahmen	88
4.6.1	Überblick	88
4.6.2	Risikoanalyse	89
4.6.3	Empirische Screenings	91
4.6.4	Mock Dawn Raids	92
4.7	Fazit	93
	Literatur	94

C. Heinichen (✉)

Advant Beiten, München, Deutschland

E-Mail: Christian.Heinichen@advant-beiten.com

4.1 Einleitung

Stern, April 2023: „Bundesregierung bringt Verschärfung des Kartellrechts auf den Weg“; SZ, September 2022: „Schienenkartell: Nahverkehrsfirmen pochen auf Schadensersatz“; FAZ, Juni 2022: „Kartellrecht: Brüssel droht mit Razzien“; Handelsblatt, Mai 2021: „LKW-Kartell: Richter machen Weg frei für Milliardenklagen“; FAZ, Juni 2021: „Absprachen bei Abgasreinigung: Deutsche Autobauer müssen 875 Mio. € zahlen“; Handelsblatt, Mai 2021: „EU-Kommission verhängt 371 Mio. € Strafe gegen Bankenkartell“; FAZ, Mai 2020: „Lastwagen-Kartell: Bahn und Bundeswehr klagen“ (385 Mio. €).

Allein dieser kleine Auszug aus den Pressemeldungen der letzten drei Jahre belegt eindrucksvoll die unveränderte Bedeutung kartellrechtlicher Compliance. Ihre Aufgabe ist es, im Unternehmen einen organisatorischen Rahmen zu schaffen, der einerseits – und vorrangig – das Risiko von Kartellverstößen und der mit ihnen verbundenen negativen Folgen für das Unternehmen reduziert, andererseits aber auch einen eigenständigen Beitrag zur unternehmerischen Wertschöpfung leistet.

4.2 Kartellrechtliche Risiken

4.2.1 Kontakte zu Wettbewerbern

Kartellrechtliche Risiken ergeben sich für ein Unternehmen insbesondere aus seinen Kontakten zu Wettbewerbern (Art. 101 AEUV, § 1 GWB). Dies betrifft zum einen die so genannten Hardcore-Absprachen, das heißt besonders schwerwiegende Verstöße gegen das Kartellverbot, die intensiv verfolgt und regelmäßig mit hohen Geldbußen geahndet werden. Zu ihnen gehören insbesondere Absprachen mit Wettbewerbern über

- Preise, zu denen miteinander konkurrierende Waren oder Dienstleistungen an Dritte verkauft werden (**Preiskartelle**). Vom Kartellverbot werden dabei nicht nur Absprachen über Festpreise erfasst, sondern auch solche über Mindestpreise, Richtpreise, Preisrahmen und Kalkulationsschemata. Überdies erstreckt sich das Kartellverbot auf sämtliche Preisbestandteile und -elemente, wie beispielsweise Preisnachlässe, Rabatte, Transportkosten, Währungsaufschläge und Zahlungsziele. Derartige Preisabsprachen lassen sich auch nicht durch den Hinweis auf einen „ruinösen Preiswettbewerb“, auf „Dumping“-Preise, stark angestiegene Rohstoffkosten oder Überkapazitäten rechtfertigen.
- Produktions- oder Absatzquoten (**Quotenkartelle**). Hierzu gehören Vereinbarungen über feste Quoten, durch Ober- und Untergrenzen bestimmte Bandbreiten von Quoten oder Höchstquoten, die nicht überschritten werden dürfen. Auch sogenannte Status quo-Absprachen, bei denen sich die beteiligten Unternehmen verpflichten, ihren Marktanteil nicht über denjenigen eines bestimmten Referenzjahres hinaus auszudehnen, werden vom Kartellverbot erfasst.

- die Aufteilung von geografischen Märkten (**Gebietskartelle**). Dies betrifft sowohl neue als auch bestehende Märkte. Das Kartellverbot erstreckt sich ebenso auf sogenannte Heimatschutzbreden, bei denen sich die beteiligten Unternehmen verpflichten, jeweils nur in „ihrem“ Liefergebiet tätig zu werden und in den Gebieten der jeweils anderen Abspracheteiligen keine Produktionstätigkeit zu beginnen, keine Waren oder Dienstleistungen anzubieten und keine Kunden zu werben (Nichtangriffspakt).
- die Aufteilung von Kunden oder Kundengruppen (**Kundenschutzkartelle**). Dies kann durch Kategorisierung und Zuweisung von neuen und/oder alten Kunden geschehen, aber auch durch eine Vereinbarung diejenigen Kunden, die bereits von einem anderen Abspracheteiligen beliefert werden, nicht abzuwerben und auf Lieferanfragen dieser Kunden mit einem überhöhten Schutzpreis zu reagieren (Bestandskundenschutz).

Kartellrechtlich besonders kritisch, da auch strafrechtlich relevant, sind Submissionsabsprachen. Bei ihnen handelt es sich um wettbewerbsbeschränkende Absprachen bei Ausschreibungen, die darauf abzielen, dem Veranstalter der Ausschreibung zur Annahme eines bestimmten Angebots zu veranlassen (§ 298 Abs. 1 StGB). Vom Straftatbestand werden neben öffentlichen auch privaten Ausschreibungen erfasst, sofern das Vergabeverfahren den §§ 97 ff. GWB oder den für öffentliche Veranstalter relevanten Vergabenormen ähnlich ausgestaltet ist. Gleiches gilt für die freihändige Auftragsvergabe, wenn ein Teilnahmewettbewerb vorausgegangen ist (§ 298 Abs. 2 StGB). Gelingt der Schadensnachweis, kann die Submissionsabsprache darüber hinaus auch als Submissionsbetrug (§ 263 StGB) bestraft werden.

In den letzten Jahren ist zunehmend der Informationsaustausch zwischen Wettbewerbern in den Fokus der Kartellbehörden gerückt. Dies gilt nicht mehr nur für dessen kartellstabilisierende Form, in der ein Austausch von Preis- oder Absatzdaten zur Überwachung einer Preis- oder Quotenabsprache erfolgt. Auch der selbstständige Austausch strategisch relevanter Informationen – sei es formal in Marktinformationsverfahren oder durch Benchmarking, sei es in informellen Gesprächsrunden – kann zu einer Beschränkung des Wettbewerbs führen. Dies ist der Fall, wenn durch den Informationsaustausch die Transparenz auf dem Markt künstlich erhöht und so die Ungewissheit über das zukünftige Marktverhalten der anderen Marktteilnehmer reduziert wird. Ein Austausch unternehmensspezifischer Daten über geplantes zukünftiges Preis- oder Mengenverhalten wird von der EU-Kommission als bezweckte Wettbewerbsbeschränkung angesehen, für die sich im Regelfall keine Rechtfertigung findet. Jenseits dieses Bereichs sind die voraussichtlichen Auswirkungen eines Informationsaustauschs auf den Wettbewerb im konkreten Einzelfall zu prüfen.¹ Das Ergebnis dieser Prüfung hängt von einer Reihe fallspezifischer Faktoren ab. Zu ihnen gehören insbesondere die Merkmale des vom Austausch betroffenen Markts und die Ausgestaltung des Informationsaustauschs. Je transparenter, konzentrierter und weniger komplex ein Markt ist, je stabiler seine Angebots- und Nachfragebedingungen und je symmetrischer seine Strukturen sind, desto eher birgt ein

¹Vgl. EU-Kommission (2011), Rn. 55 ff.

Informationsaustausch das Risiko einer Wettbewerbsbeschränkung in sich. Tauschen Wettbewerber strategische Daten (zum Beispiel Preise, Produktionskosten, Mengen, Umsätze, Verkaufszahlen, Kapazitäten, Marketingpläne, Investitionen, Technologien) aus, so bewirkt dies eher eine Wettbewerbsbeschränkung als der Austausch nicht strategischer Daten. Ob Daten strategisch relevant sind, hängt darüber hinaus von ihrem Aggregationsgrad, ihrem Alter, dem Marktkontext und der Häufigkeit des Informationsaustauschs ab. So ist der Austausch echter aggregierter Daten, die nur mit hinreichender Schwierigkeit Rückschlüsse auf individuelle unternehmensspezifische Daten zulassen, kartellrechtlich weniger riskant als der Austausch unternehmensspezifischer Daten. Je älter die ausgetauschten Daten sind, desto weniger ist es wahrscheinlich, dass sich aus ihnen kartellrechtlich problematische Schlussfolgerungen auf ein zukünftiges Marktverhalten ziehen lassen.

Aushilfslieferungen zwischen Wettbewerbern (Kollegenlieferungen) bergen insbesondere dann ein kartellrechtliches Risiko in sich, wenn sie gegenseitig und langfristig vereinbart werden. Durch sie verzichtet ein beteiligtes Unternehmen darauf, etwaige Produktionsunterbrechungen eines anderen Beteiligten dazu zu nutzen, die eigenen Direktverkäufe an dessen Kunden zu steigern. Aushilfslieferungen sind dagegen in der Regel unbedenklich, wenn sie nur gelegentlich, kurzfristig und zur Überbrückung von Engpässen erfolgen. Einkaufsgemeinschaften von Wettbewerbern, deren Mitglieder sich wechselseitig verpflichten ihren Bedarf an bestimmten Gütern oder Dienstleistungen ausschließlich über die Einkaufsgemeinschaft zu decken, beschränken durch die Koordination des Nachfrageverhaltens und die Nachfragebündelung regelmäßig den Nachfragewettbewerb. Ungeachtet dessen können derartige Einkaufsgemeinschaften kartellrechtlich zulässig sein, etwa wenn sie es kleinen und mittleren Unternehmen ermöglichen, durch den gemeinsamen Einkauf vergleichbare Größenvorteile wie ihre marktstärkeren Mitbewerber zu erzielen.

Kartellrechtlich unzulässig ist auch ein „Abkauf von Wettbewerb“. Er zeichnet sich dadurch aus, dass einem konkurrierenden Unternehmen für sein Ausscheiden aus dem Markt eine Prämie („Sterbegeld“) gezahlt wird, ohne dass als Gegenleistung der wirtschaftliche Wert dieses Unternehmens auf den Prämienzahler übergeht oder vom Prämienzahler später tatsächlich genutzt wird. Das Bundeskartellamt hat bereits eine erhebliche Differenz zwischen dem Kaufpreis und dem Wert der übernommenen Vermögenswerte als Indiz für einen rechtswidrigen Abkauf von Wettbewerb angesehen.

4.2.2 Beziehungen zu Lieferanten und Händlern

Kartellrechtliche Risiken ergeben sich nicht nur aus den Kontakten eines Unternehmens zu seinen Wettbewerbern, sondern auch aus seinen Beziehungen zu den Akteuren auf vor- und nachgelagerten Marktstufen (Art. 101 AEUV, § 1 GWB). Vertikale Vereinbarungen zwischen nicht miteinander im Wettbewerb stehenden Unternehmen sind zwar in einer Vielzahl von Fällen wettbewerbsfördernd, da sie die wirtschaftliche Effizienz innerhalb

einer Produktions- oder Lieferkette erhöhen, indem sie dazu beitragen, Transaktions- und Vertriebskosten zu verringern. Sie können jedoch auch schwerwiegende Wettbewerbsbeschränkungen beinhalten, zu denen unter anderem gehören

- die Festsetzung von Mindest- oder Festpreisen für den Weiterverkauf von Waren (**Preisbindung der zweiten Hand**). Schwierig und in ihren Grenzbereichen nicht geklärt ist dabei die Abgrenzung zwischen der kartellrechtlich zulässigen unverbindlichen Preisempfehlung und der verbotenen Preisbindung durch wiederholte Kontaktaufnahme nach Übersendung einer unverbindlichen Preisempfehlung an den Händler oder durch Einsatz von Druck- oder Lockmitteln.²
- die Beschränkung des passiven Verkaufs in Gebiete, die der Anbieter sich selbst vorbehalten oder anderen Abnehmern exklusiv zugewiesen hat (**absoluter Gebietsschutz**).
- die Verhinderung der wirksamen Nutzung des Internets als Vertriebskanal (**Verbot des Onlinevertriebs**).

4.2.3 Missbrauch von Marktmacht

Ist ein Unternehmen marktbeherrschend, relativ marktstark oder von überragender marktübergreifender Bedeutung für den Wettbewerb, unterliegt es strenger kartellrechtlichen Verhaltensanforderungen. Sie ergeben sich aus den besonderen gesetzlichen Regelungen über den Missbrauch einer marktbeherrschenden, marktstarken oder überragenden marktübergreifenden Stellung (Art. 102 AEUV, §§ 18 ff. GWB).

Marktbeherrschung setzt voraus, dass ein Unternehmen über nicht mehr hinreichend vom Wettbewerb oder von der Marktgegenseite kontrollierte Verhaltensspielräume verfügt. Ihre Prüfung erfordert die häufig schwierige Abgrenzung des sachlich und räumlich relevanten Markts, in deren Mittelpunkt die Austauschbarkeit eines Produkts oder eines Marktteilnehmers aus Sicht der Marktgegenseite steht. Ein wesentlicher Indikator für die marktbeherrschende Stellung eines Unternehmens ist sein Marktanteil. § 18 Abs. 4 GWB vermutet die Einzelmarktbeherrschung bei einem Marktanteil von mindestens 40 %. Dagegen ist ein Unternehmen relativ marktstark, wenn Unternehmen von ihm als Anbieter oder Nachfrager dergestalt abhängig sind, dass für sie ausreichende und zumutbare Möglichkeiten, auf andere Unternehmen auszuweichen, nicht bestehen (§ 20 Abs. 1 GWB). Überragende marktübergreifende Bedeutung können Unternehmen als sogenannte Gatekeeper auf Plattform- oder Netzwerkmärkten haben, wenn sie über Ressourcen oder eine strategische Positionierung verfügen, die es ihnen ermöglichen, erheblichen Einfluss auf die Geschäftstätigkeit Dritter zu nehmen oder die eigene Geschäftstätigkeit in immer neue Märkte auszudehnen.

Marktbeherrschende und relativ marktstarke Unternehmen sowie Unternehmen mit kartellbehördlich festgestellter überragender marktübergreifender Bedeutung unterliegen

²Vgl. Bundeskartellamt (2017).

einem besonderen kartellrechtlichen Missbrauchsverbot (Art. 102 AEUV, §§ 19 ff. GWB). Es untersagt sowohl missbräuchliche Verhaltensweisen, die sich gegen verbliebene Konkurrenten richten (Behinderungsmissbrauch), als auch solche, die zu einer Ausbeutung der Marktgegenseite führen (Ausbeutungsmissbrauch). Beispiele für den Missbrauch einer marktbeherrschenden oder relativ marktstarken Stellung sind unter anderem

- das Fordern missbräuchlich überhöhter Preise.
- die Festsetzung unangemessen niedriger Kampfpreise, um kleinere Mitbewerber vom Markt zu drängen.
- die Diskriminierung von Handelspartnern.
- das Gewähren von Treuerabatten für Kunden, die ausschließlich oder weit überwiegend beim marktbeherrschenden Unternehmen beziehen.
- die Verweigerung des Zugangs zu Daten, Netzen oder Infrastruktureinrichtungen.

Für marktbeherrschende und relativ marktstarke Unternehmen gilt zudem ein allgemeines Diskriminierungs- und Behinderungsverbot (§ 20 Abs. 1 GWB). Unternehmen mit kartellbehördlich festgestellter überragender marktübergreifender Bedeutung dürfen beim Vermitteln des Zugangs zu Beschaffungs- und Absatzmärkten die eigenen Angebote gegenüber denen von Wettbewerbern nicht bevorzugt behandeln oder Maßnahmen zu ergreifen, die andere Unternehmen in ihrer Geschäftstätigkeit auf Beschaffungs- oder Absatzmärkten behindern, wenn die Tätigkeit des Unternehmens für den Zugang zu diesen Märkten Bedeutung hat (§ 19a Abs. 2 GWB).

4.2.4 Risiken bei M&A-Transaktionen

Auch M&A-Transaktionen können kartellrechtliche Risiken in sich bergen. Dies gilt zum einen für fusionskontrollrechtlich anmeldepflichtige Zusammenschlüsse, die nicht angemeldet oder bereits vor der kartellbehördlichen Freigabe vollzogen werden. Weitere kartellrechtliche Risiken bringt der Informationsaustausch mit sich. Er ist bei Unternehmenskäufen regelmäßig erforderlich, um den Unternehmenswert und damit den Kaufpreis bestimmen zu können. Im Falle des Fehlschlagens einer Transaktion zwischen Wettbewerbern kann er dazu führen, dass die an sich bestehende Ungewissheit über das zukünftige Marktverhalten des Transaktionsobjekts verringert und hierdurch der Wettbewerb beschränkt wird.³ War das Unternehmen, das Gegenstand der M&A-Transaktion ist, an einem Kartellverstoß beteiligt, stellt sich zudem – für den Erwerber häufig unerwartet – die Frage, ob der Veräußerer oder der Erwerber hierfür bußgeldrechtlich einzustehen hat. Im EU-Kartellrecht gelten insoweit die sogenannten Anic-Regeln, die zur gefestigten Entscheidungspraxis der Unionsorgane gehören. Ihnen zufolge haftet bußgeldrechtlich grundsätzlich derjenige Unternehmensträger, der im Zeitpunkt der Zuwiderhandlung für den Betrieb des kartellbeteiligten Unternehmens verantwortlich war. Lediglich in den Fällen, in denen dieser Unternehmens-

³Vgl. Besen/Gronemeyer (2009), S. 67 ff.

träger transaktionsbedingt – z. B. infolge einer Verschmelzung oder Aufspaltung – rechtlich nicht mehr existiert, kann der erwerbende Unternehmensträger bußgeldrechtlich in Anspruch genommen werden, um sicherzustellen, dass sich ein Unternehmen nicht durch eine gezielte Umstrukturierung seiner bußgeldrechtlichen Verantwortung entziehen kann. Darüber hinaus gibt es zahlreiche weitere „Ausnahmen“, die das Risiko einer bußgeldrechtlichen Inanspruchnahme des Erwerbers erhöhen. Sie kommen regelmäßig dann zur Anwendung, wenn der ursprüngliche Unternehmensträger zwar rechtlich noch fortbesteht, mangels finanzieller Ausstattung oder aus sonstigen Gründen jedoch nicht mehr in der Lage wäre, ein gegen ihn festgesetztes Bußgeld zu bezahlen.⁴ Im deutschen Kartellrecht war die Rechtsnachfolge in die bußgeldrechtliche Verantwortung lange Zeit gesetzlich nicht geregelt. Dies führte zu einer Sanktionslücke, die es Unternehmen in einem bestimmten Rahmen ermöglichte, sich durch eine Umstrukturierung der drohenden Geldbuße zu entziehen.⁵ Im Zuge der 8. und 9. GWB-Novelle wurde diese Sanktionslücke durch die Einführung von § 30 Abs. 2a OWiG und § 81a GWB geschlossen. Beide Normen ermächtigen zur Erstreckung der bußgeldrechtlichen Verantwortung auf Konzernobergesellschaften sowie Gesamt- und Einzelrechtsnachfolger der bußgeldrechtlich an sich verantwortlichen Gesellschaft.

4.3 Folgen von Kartellverstößen

4.3.1 Geldbußen

Schuldhafte Verstöße gegen das Kartellverbot (Art. 101 AEUV, § 1 GWB) oder das Verbot des Missbrauchs einer marktstarken Stellung (Art. 102 AEUV, §§ 18 ff. GWB) können gravierende bußgeldrechtliche Folgen haben. Art. 23 Abs. 2 VO 1/2003 ermächtigt die EU-Kommission, gegen jedes an der Zu widerhandlung beteiligte Unternehmen eine Geldbuße von bis zu zehn Prozent seines weltweiten Gesamtumsatzes festzusetzen. Vergleichbares gilt für das deutsche Kartellrecht. Gemäß § 81c Abs. 2 GWB können Kartellverstöße mit Geldbußen von bis zu zehn Prozent des Gesamtumsatzes des an der Zu widerhandlung beteiligten Unternehmens geahndet werden, wobei als Gesamtumsatz der weltweite Umsatz aller als wirtschaftliche Einheit operierenden Gesellschaften (Konzernumsatz) zugrunde zu legen ist. In den vergangenen Jahren haben die Geldbußen, die wegen eines Verstoßes gegen das Kartellverbot verhängt wurden, extreme Höhen erreicht, was nachfolgende Tabelle verdeutlicht (Tab. 4.1):

Tab. 4.1 Geldbußen

Zeitraum	EU-Kommission	Bundeskartellamt
2000–2009	12.906 Mio. €	2035 Mio. €
2010–2019	14.450 Mio. €	3747 Mio. €
2020–2021	2034 Mio. €	454 Mio. €
2000–2021	29.390 Mio. €	6236 Mio. €

⁴Vgl. Heinichen (2011), S. 163 ff.

⁵Vgl. Heinichen (2015), S. 862 ff.

Die höchste Bußgeldsumme von insgesamt 3,8 Mrd. € wurde 2016/2017 von der EU-Kommission gegen die Beteiligten des LKW-Kartells verhängt. Die höchste Einzelgeldbuße von einer Milliarde Euro wegen eines Verstoßes gegen das Kartellverbot richtete sich 2016 gegen den LKW-Hersteller Daimler.

Das Kartellbußgeldrecht kennt überdies keinen generellen „Mittelstandsbonus“. Auch gegen mittelständische Unternehmen wurden und werden bei schwerwiegenden Kartellverstößen erhebliche Sanktionen verhängt, wie die Geldbußen gegen die Papierfabrik Köhler (33 Mio. €, 2001), den Kurzwarenproduzenten Prym (40,5 Mio. €, 2007) oder den Keramikhersteller Villeroy & Boch (71 Mio. €, 2007) zeigen.

Zuwiderhandlungen gegen das Kartell- oder das Missbrauchsverbot verjähren sowohl im europäischen als auch im deutschen Kartellrecht nach fünf Jahren (Art. 25 VO 1/2003, § 81g Abs. 1 GWB). Bei dauernden oder fortgesetzten Zuwiderhandlungen beginnt die Verjährungsfrist erst mit dem Tag, an dem die Zuwiderhandlung tatsächlich beendet ist. Dies kann bei Kartellabsprachen von besonderer Bedeutung sein, wenn diese – wie häufig – in die Zukunft wirken. Solange eine solche Absprache wettbewerbsbeschränkende Wirkungen zeitigt, ist sie nicht beendet, sodass die Verjährungsfrist nicht zu laufen beginnt.

4.3.2 Schadenersatz

Kartellverstöße sind auch zivilrechtlich sanktioniert. Nach den Grundsatzentscheidungen **Courage** und **Manfredi** des EuGH kann bei einem schuldhaften Verstoß gegen die Art. 101, 102 AEUV „jedermann“ Ersatz des ihm aus einem Kartellverstoß entstandenen Schadens verlangen. § 33a Abs. 1 GWB stellt einen solchen Schadenersatzanspruch für Verstöße gegen europäisches und deutsches Kartellrecht zur Verfügung. Organe potenziell kartellgeschädigter Unternehmen sind dazu verpflichtet, zur Wahrung der Interessen ihrer Eigentümer die Erfolgsaussichten kartellrechtlicher Schadenersatzansprüche zumindest zu prüfen (vergleiche § 93 Abs. 1 AktG, § 43 Abs. 1 GmbHG).

Im Jahr 2011 hat der BGH entschieden, dass nicht nur die unmittelbaren Kunden des Kartells, sondern auch mittelbare Abnehmer nachgelagerter Marktstufen einen Schaden geltend machen können, der ihnen durch das Kartell entstanden ist. Um seine mehrfache Inanspruchnahme und eine ungerechtfertigte Bereicherung des Anspruchstellers zu vermeiden, kann ein Kartellbeteiligter allerdings einwenden, der Anspruchsteller habe die kartellbedingte Preisüberhöhung an seine eigenen Kunden weitergegeben (**Passing-on-Einwand**). Die Darlegungs- und Beweislast für eine solche Schadensweiterwälzung liegt jedoch beim beklagten Kartellanten. Er muss nachweisen, dass der kartellbedingte Preisaufschlag an die nachgelagerte Marktstufe weitergereicht wurde, dass dem Anspruchsteller kein weiterer Nachteil, etwa in Form eines Nachfragerückgangs, entstanden ist und

dass die Weitergabe des Preisaufschlags nicht auf einem eigenen Wertschöpfungsbeitrag des Anspruchstellers beruht.

Für durch ein Kartell verursachte Schäden haften alle Kartellbeteiligten als Gesamtschuldner (§ 33d GWB), das heißt, geschädigte Abnehmer können ihren gesamten Schaden von einem einzigen Kartellteilnehmer ersetzt verlangen, selbst wenn sie nur einen Teil der kartellbetroffenen Waren bei ihm bezogen haben. Der gesamtschuldnerisch in Anspruch genommene Kartellant muss sich dann im Innenverhältnis gegenüber den anderen Kartellbeteiligten um einen Ausgleich bemühen. Etwaige Kronzeugen sind schadenersatzrechtlich eingeschränkt privilegiert (§ 33e GWB).

4.3.3 Persönliche Verantwortung

Kartellverstöße können nicht nur für Unternehmen, sondern auch für deren handelnde Organe und Repräsentanten negative persönliche Folgen haben. Das Bundeskartellamt ist befugt, Geldbußen von bis zu 1 Mio. € gegen Mitarbeiter des kartellierten Unternehmens festsetzen, wenn sie eine Leitungsfunktion wahrgenommen haben (§ 9 OWiG) und selbst am Kartellverstoß beteiligt waren oder eine ihnen obliegende Aufsichtspflicht verletzt haben (§ 130 OWiG). Beteiligte an einer Submissionsabsprache sehen sich sogar mit einer Strafdrohung von bis zu fünf Jahren Freiheitsstrafe konfrontiert (§ 298 StGB). Formal scheinbar nebensächlich, für den Einzelnen aber von erheblicher Bedeutung ist der Eintrag ins Gewerbezentralregister (§ 149 Abs. 2 GewO), womit diese Person als nicht mehr zuverlässig im gewerberechtlichen Sinne gilt. Darüber hinaus werden durch die Beteiligung an einem Kartellverstoß regelmäßig vertragliche Pflichten verletzt, die sich aus dem Anstellungs- oder Arbeitsvertrag ergeben. Diese Pflichtverletzung kann zu Schadenersatzansprüchen berechtigen, die es den betroffenen Unternehmen ermöglichen, jedenfalls einen Teil des ihnen – durch Bußgeld- und etwaige Schadenersatzverfahren – entstandenen Schadens von den kartellbeteiligten Personen ersetzt zu bekommen. Sie eröffnet zudem das gesamte arbeitsrechtliche Instrumentarium von der Verwarnung über die Abmahnung bis hin zur Versetzung oder Kündigung.

Auch der Compliance-Beauftragte kann Aufsichtspflichtiger im Sinne des § 130 OWiG sein, wenn er aufgrund einer herausgehobenen und klar abgegrenzten Tätigkeit in eigener Verantwortung Aufgaben für den Betriebsinhaber übernimmt (§ 9 Abs. 2 Nr. 2 OWiG). Organisiert er seinen Arbeitsbereich nur unzureichend oder unterlässt er gebotene Aufsichtsmaßnahmen, so hat er persönlich für sämtliche betriebsbezogene Kartellordnungswidrigkeiten bußgeldrechtlich einzustehen, selbst wenn er von diesen keine Kenntnis hat.⁶

⁶Vgl. Raum (2012), S. 197 f.

4.3.4 Vergaberechtliche Folgen

Kartellverstöße, deren Sanktionierung ins Wettbewerbsregister eingetragen wird, können schließlich zur Folge haben, dass die kartellbeteiligten Unternehmen von der Vergabe öffentlicher Aufträge ausgeschlossen werden. Ein zwingender Ausschlussgrund liegt zwar lediglich im Falle des Submissionsbetrugs (§ 263 StGB) und auch nur dann vor, wenn sich die Straftat gegen den EU-Haushalt oder gegen einen von der EU verwalteten Haushalt richtet (§ 123 Abs. 1 Nr. 4 GWB). Darüber hinaus bilden jedoch schwere Verfehlungen einen fakultativen Ausschlussgrund, soweit durch sie die Zuverlässigkeit des Bieters in Frage gestellt wird (§ 124 Abs. 1 Nr. 4 GWB, § 6 Abs. 5 lit. c VOL/A, § 6a Abs. 2 Nr. 7 VOB/A). Diese Beurteilung liegt grundsätzlich im Ermessen der Vergabestelle. Indes qualifizieren mehrere Bundesländer Kartellverstöße in Sonderregelungen unterschiedslos als schwere Verfehlungen. Liegt eine solche schwere Verfehlung vor, kann der Vergabeausschluss nur abgewendet werden, wenn es dem Bieter gelingt darzulegen, dass er hinreichende Selbstreinigungsmaßnahmen ergriffen hat. Zu einer solchen Selbstreinigung gehören eine umfassende Aufklärung des Sachverhalts, die Wiedergutmachung eines etwaigen Schadens sowie personelle und Compliance-Maßnahmen.⁷

4.3.5 Weitere Folgen

Neben den genannten Folgen können Kartellverstöße noch eine Reihe weiterer negativer Konsequenzen mit sich bringen:

- Kartellrechtswidrige Vereinbarungen sind nichtig. Sie müssen neu verhandelt werden. Überdies ergeben sich häufig Abwicklungsprobleme für den Zeitraum, in dem eine solche nichtige Vereinbarung gelebt wurde.
- Kartellbußgeldverfahren werden regelmäßig von einem großen Presseecho begleitet. Geschäftspartner und Kunden erlangen hierdurch Kenntnis vom Verfahren. Die Reputation des betroffenen Unternehmens wird beschädigt.
- Kartellverfahren können die Kreditwürdigkeit eines Unternehmens erheblich beeinträchtigen. Ratings verschlechtern sich, die Kapitalbeschaffung wird teurer.
- Kartellverfahren erstrecken sich häufig über mehrere Jahre. Sie verursachen erhebliche Verfahrenskosten und binden Mitarbeiter des Unternehmens, die zur Beschaffung der verfahrensrelevanten Informationen benötigt werden.

⁷Vgl. Hövelberndt (2017), S. 464 ff.

4.4 Nachhaltige Wertschöpfung durch effektive Competition Compliance

Vordergründiges Ziel kartellrechtlicher Compliance-Maßnahmen ist es, das Eintrittsrisiko der beschriebenen negativen, unter Umständen sogar existenzbedrohenden Folgen von Kartellverstößen zu minimieren. Effektive Competition Compliance leistet indes auch einen wichtigen Beitrag zur unternehmerischen Wertschöpfung. Sie schafft ein Wertesystem, das den Wettbewerbsgedanken zu einem Leitbild der Unternehmenskultur erhebt. Durch sie wird ein organisatorischer Handlungsrahmen geschaffen, innerhalb dessen die Mitarbeiter eines Unternehmens sicher und selbstständig handeln können. Risikoanalysen machen sichtbar, welche Unternehmensbereiche kartellrechtlich sensibel und welche unkritisch sind. Handbücher verschaffen einen Überblick, was erlaubt und was verboten ist. Schulungen und Workshops ermöglichen es, Unsicherheiten über die Grenzen des kartellrechtlich Erlaubten zu beseitigen. Kartellrechtlich derart sensibilisierte und informierte Mitarbeiter agieren regelmäßig sicherer und selbstständiger. Sie können sich auf ihre eigentliche Aufgabe konzentrieren – einen Beitrag zur Wertschöpfung des Unternehmens zu leisten.

Effektive Competition Compliance kann darüber hinaus auch die Wahrnehmung eines Unternehmens in der Öffentlichkeit positiv beeinflussen. Das Vertrauen von Kunden und Geschäftspartnern wird gestärkt. Immer häufiger wird die Erteilung eines Auftrags oder die Aufnahme von Geschäftsbeziehungen davon abhängig gemacht, dass ein Unternehmen über funktionierende Mechanismen zur Abwehr kartellrechtlicher Risiken verfügt. Auch die Kreditwürdigkeit eines Unternehmens steigt, wenn es nachvollziehbar darlegen kann, dass es effektive und nachhaltige Maßnahmen ergriffen hat, um Kartellverstöße und die mit ihnen verbundenen finanziellen Folgen zu vermeiden.

4.5 Kartellverfahren

4.5.1 Wettbewerbsbehörden

Europäische Wettbewerbsbehörde ist die EU-Kommission mit Sitz in Brüssel, insbesondere deren Generaldirektion Wettbewerb. Die Zuständigkeit der EU-Kommission erstreckt sich auf die Anwendung des primär in den Art. 101, 102 AEUV normierten europäischen Kartellrechts. Es findet Anwendung, wenn sich der zu beurteilende Sachverhalt auf den Binnenmarkt auswirkt und überdies einen zwischenstaatlichen Bezug aufweist, das heißt geeignet ist, den Handel zwischen den Mitgliedstaaten zu beeinträchtigen.

Deutsche Wettbewerbsbehörde mit Sitz in Bonn ist das Bundeskartellamt. In seine Zuständigkeit fällt die Anwendung deutschen und europäischen Kartellrechts. Leitet jedoch die EU-Kommission ein Verfahren zur Feststellung einer Zu widerhandlung gegen europäisches Kartellrecht ein, so entfällt die Zuständigkeit der mitgliedstaatlichen Wettbewerbsbehörden und damit des Bundeskartellamts. Neben dem Bundeskartellamt exis-

tieren auch Landeskartellbehörden. Ihre Zuständigkeit ist indes auf Sachverhalte beschränkt, deren Auswirkungen die Grenzen des jeweiligen Bundeslands nicht überschreiten.

4.5.2 Kartellbußgeldverfahren

Bei Vorliegen eines Anfangsverdachts können Wettbewerbsbehörden ein Ermittlungsverfahren gegen die betroffenen Unternehmen einleiten. Auslöser für ein solches Ermittlungsverfahren sind häufig Bonusanträge kartellbeteiligter Unternehmen im Rahmen der kartellrechtlichen Kronzeugenregelungen (Selbstanzeigen). Derartige Kronzeugenregelungen existieren sowohl im europäischen als auch im deutschen Kartellrecht. Vereinfacht gesprochen, gewähren sie dem ersten Unternehmen, das die Wettbewerbsbehörde über ein Kartell informiert und entsprechende Beweise vorlegt, einen vollständigen Erlass der Geldbuße. Allen weiteren kooperierenden Unternehmen wird – abhängig von der Reihenfolge ihrer Bonusanträge und dem Mehrwert ihres Kooperationsbeitrags – eine Bußgeldreduktion von bis zu 50 % in Aussicht gestellt. Diese kartellrechtlichen Kronzeugenregelungen haben sich in den vergangenen Jahrzehnten als äußerst wirksames Instrument zur Aufdeckung von Kartellabsprachen herausgestellt. Anlass für die Einleitung eines Ermittlungsverfahrens können aber auch förmliche Beschwerden, Sektoruntersuchungen oder informelle Erkenntnisse sein, die beispielsweise von ausscheidenden Mitarbeitern, Kunden oder anderen Geschäftspartnern oder durch Presseveröffentlichungen erlangt werden.

Das Ermittlungsverfahren ist sodann regelmäßig von Nachprüfungen,⁸ Auskunftsersuchen und Zeugenbefragungen geprägt. Nachprüfungen (**Dawn Raids**) der EU-Kommission liegt regelmäßig eine Nachprüfungsentscheidung (Art. 20 Abs. 4 VO 1/2003) zu grunde. Sie muss konkrete Angaben zum Nachprüfungsgegenstand enthalten – mit der Folge des Verbots von Fishing Expeditions – und verpflichtet das durchsuchte Unternehmen zur Duldsung sowie eingeschränkt zur Mitwirkung. Die Nachprüfungsbefugnisse der EU-Kommission umfassen das Recht zum Betreten von Unternehmens- und Privaträumlichkeiten, zur Prüfung von (auch elektronischen) Geschäftsunterlagen vor Ort, zur Versiegelung, zum Anfertigen von Kopien und in einem beschränkten Umfang auch zur Befragung von Mitarbeitern. Wird die Nachprüfung schulhaft behindert, kann dies erhebliche Geldbußen zur Folge haben. Ein Siegelbruch kostete E.ON unlängst 38 Mio. €. Bei Auskunftsersuchen der EU-Kommission ist zwischen dem einfachen Auskunftsverlangen, dessen Beantwortung freiwillig erfolgt, und der Auskunftsentscheidung (Art. 18 Abs. 3 VO 1/2003), die zur Antwort verpflichtet, zu differenzieren. Durchsuchungen des Bundeskartellamts sind seit der 10. GWB-Novelle 2021 weitgehend mit denen der EU-Kommission vergleichbar. Im Gegensatz zu staatsanwaltschaftlichen Durchsuchungen gehen Durchsuchungen durch das Bundeskartellamt nicht nur mit Duldsungs-, sondern mit Mitwirkungspflichten einher. Unterlagen können vom Bundeskartell-

⁸Vgl. de Crozals (2009), S. 92 ff.

amt beschlagnahmt und Zeugen vernommen werden. Wichtige Verfahrensrechte sind ein Geständnisverweigerungsrecht, das sowohl im EU- als auch im deutschen Kartellbußgeldverfahren besteht, und ein Beschlagnahmeverbot, das sich aus dem Anwaltsprivileg (**Legal Privilege**) ergibt. Es erstreckt sich auf die Korrespondenz mit externen Anwälten in Ausübung des Verteidigungsrechts.

Bestätigt sich der Anfangsverdacht, werden den betroffenen Unternehmen durch die EU-Kommission zunächst die Beschwerdepunkte mitgeteilt, um rechtliches Gehör zu ermöglichen. Darüber hinaus kann eine mündliche Anhörung beantragt werden. Das förmliche Ermittlungsverfahren kann mit dessen Einstellung, mit der Entgegennahme verbindlicher Verpflichtungszusagen oder mit der Feststellung einer Zu widerhandlung, der Anordnung ihrer Abstellung und der Festsetzung von Geldbußen (auch im Wege eines **Settlements**) enden. Gegen belastende Entscheidungen der EU-Kommission wird Rechtsschutz vor dem Gerichtshof der Europäischen Union gewährt. Das deutsche kartellbehördliche Bußgeldverfahren endet ebenfalls mit seiner Einstellung oder dem Erlass einer Bußgeldentscheidung. Gegen den Bußgeldbescheid kann Einspruch beim OLG Düsseldorf eingelegt werden. Desse n erstinstanzliches Urteil lässt sich durch eine Rechtsbeschwerde zum BGH überprüfen.⁹

4.5.3 Kartellschadenersatzverfahren

Unabhängig von der Höhe des Streitwerts sind in Deutschland erstinstanzlich ausschließlich die Landgerichte für kartellrechtliche Schadenersatzklagen zuständig (§ 87 GWB). Das Bundeskartellamt wird durch das Gericht von derartigen Klagen informiert und kann im Verfahren als amicus curiae auftreten. § 89a GWB ermöglicht es dem Gericht, auf Antrag den Streitwert einseitig herabzusetzen, wenn die Belastung mit den Prozesskosten bei vollem Streitwert die wirtschaftliche Lage der beantragenden Partei erheblich gefährden würde.

Kartellschadenersatzklagen können und werden häufig als **Follow-on-Klagen** erhoben. Sie folgen dann einer bestandskräftigen kartellbehördlichen oder rechtskräftigen kartellgerichtlichen Entscheidung, etwa einer Bußgeldentscheidung, die eine sogenannte Tatbestandswirkung dahingehend entfaltet, dass das Zivilgericht an die Feststellung des Kartellverstoßes gebunden ist (§ 33b GWB). Schwierigkeiten bereitet jedoch regelmäßig der Nachweis eines kausalen Schadens und dessen Höhe. Beides ist grundsätzlich vom Geschädigten zu beweisen. Es existieren jedoch Beweiserleichterungen. § 33a Abs. 2 GWB vermutet, dass ein Kartell einen Schaden verursacht hat. Die Schadenshöhe kann vom Gericht gemäß § 287 ZPO geschätzt werden. § 33a Abs. 4 GWB sieht vor, dass ein Kartellschadenersatzanspruch nicht erst mit Rechtshängigkeit der Schadenersatzklage, sondern bereits ab Schadenseintritt zu verzinsen ist. Bei einem langwierigen Kartellbußgeldverfahren und Follow-on-Klagen kann der geschuldete Zins zu einer erheblichen Zusatzbelastung des Schadenersatzschuldners führen.

⁹Vgl. Wissmann/Dreyer/Witting (2008), S. 86 ff.

Kartellschadenersatzansprüche verjähren grundsätzlich nach fünf Jahren (§ 33h Abs. 1 GWB). Die Frist beginnt mit Schluss des Jahres, in dem der Anspruch entstanden ist und der Gläubiger von den anspruchsgrundlegenden Tatsachen sowie der Person des Schuldners Kenntnis erlangt hat oder ohne grobe Fahrlässigkeit hätte erlangen müssen, soweit das Kartell zu diesem Zeitpunkt beendet ist (§ 33h Abs. 2 GWB). Die Verjährung wird für die Dauer des Kartellbußgeldverfahrens gehemmt. Die Hemmung endet ein Jahr nach Abschluss des Behördenverfahrens oder – wenn die Behördenentscheidung gerichtlich überprüft wird – ein Jahr nach der rechtskräftigen gerichtlichen Entscheidung (§ 33h Abs. 6 GWB).

Im Falle eines Bußgeldverfahrens haben Geschädigte zwar ein Recht auf Akteneinsicht (§ 406e Abs. 1 StPO). Um die Wirksamkeit der kartellrechtlichen Kronzeugenregelung zu wahren, erstreckt sich dieses Akteneinsichtsrecht allerdings nur auf den geschwärzten Bußgeldbescheid (§ 89c Abs. 5 GWB). Dies gilt auch für die Einsichtnahme in die staatsanwaltschaftliche Akte eines Kartellstrafverfahrens (§ 89c Abs. 6 GWB). Daneben verfügt der Geschädigte über einen materiellrechtlichen Auskunfts- und Herausgabeanspruch nach § 33g GWB. Er richtet sich auf die Erteilung von Auskünften und die Herausgabe von Beweismitteln, die für die Erhebung eines Kartellschadensersatzanspruchs erforderlich sind.

4.6 Kartellrechtliche Compliance-Maßnahmen

4.6.1 Überblick

Compliance-Maßnahmen umfassen regelmäßig die Identifikation, Auswertung und Steuerung (Reduzierung) der Risiken eines Unternehmens sowie die Überprüfung ihrer eigenen Effektivität. Dies gilt auch für kartellrechtliche Compliance-Programme, deren einzelne Elemente deshalb deutliche Parallelen zu anderen Bereichen der Compliance aufweisen (Abb. 4.1).

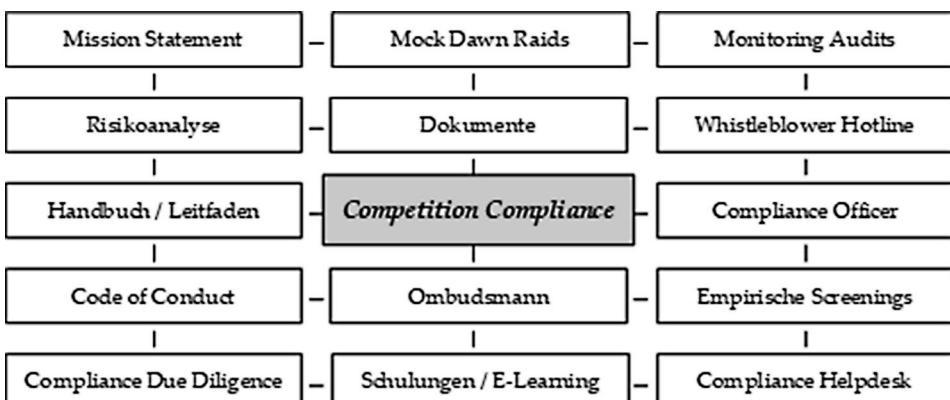


Abb. 4.1 Elemente eines kartellrechtlichen Compliance-Programms

Die Frage, welche Elemente für ein effektives kartellrechtliches Compliance-Programm im konkreten Einzelfall erforderlich sind, lässt sich in allgemeingültiger Weise kaum beantworten. Die Antwort hängt vielmehr von der Struktur des Unternehmens, seinem Tätigkeitsbereich, seiner kartellrechtlichen „Vergangenheit“ und vom wettbewerblichen Umfeld ab, in dem es sich bewegt. So benötigt ein weltweit tätiger Großkonzern mit einem diversifizierten Produktpotfolio, der bereits an sanktionierten Kartellverstößen beteiligt war, ersichtlich ein anderes kartellrechtliches Compliance-Programm als ein mittelständisches Einproduktunternehmen, das lediglich national agiert und kartell(bußgeld) rechtlich bislang nicht in Erscheinung getreten ist. Nachfolgend sollen die kartellrechtlichen Besonderheiten einiger ausgewählter Compliance-Maßnahmen detaillierter dargestellt werden.

4.6.2 Risikoanalyse

Unternehmerisches Handeln ist stets auch mit kartellrechtlichen Risiken verbunden. Selbst effektive Competition-Compliance-Programme vermögen derartige Risiken nicht vollständig auszuschließen. Ihr Ziel ist vielmehr, schwerwiegende Kartellverstöße (Hardcore-Verstöße) zu verhindern und systematischen kartellrechtlichen Fehlentwicklungen durch Etablierung eines organisatorischen Rahmens und einer entsprechenden Werteverordnung entgegenzuwirken. Kartellrechtliche Risiken kann ein Compliance-Programm allerdings nur dann steuern und reduzieren, wenn sie bekannt sind. Hierzu bedarf es einer umfassenden Risikoanalyse. Competition Compliance ohne eine solche Risikoanalyse ist „blind“. Erst die Risikoanalyse schafft das Fundament, auf dem weitere Compliance-Maßnahmen errichtet werden können. Sie ermöglicht eine systematische Erfassung, Auswertung und Operationalisierung der kartellrechtlichen Risiken eines Unternehmens. Schließlich gibt sie Anhaltspunkte, ob und auf welchem Weg eine Organisation – notfalls unter Inanspruchnahme kartellrechtlicher Kronzeugenregelungen – von etwaigen „Altlasten“ zu bereinigen ist, deren Existenz jedes zukünftige Bemühen um Compliance konterkarieren würde.

Am Anfang einer kartellrechtlichen Risikoanalyse steht die systematische Risikoverfassung. Ihre Informationsquellen sind vielfältig. Da schwerwiegende und damit besonders bußgeldträchtige Kartellverstöße heute regelmäßig nicht mehr schriftlich festgehalten werden, gehören die Mitarbeiter eines Unternehmens zu den wichtigsten Trägern kartellrechtlich relevanter Informationen. Ihre Befragung gilt es sorgfältig vorzubereiten. Zunächst bedarf es einer Auswahl der zu befragenden Mitarbeiter, die sich aus kartellrechtlicher Sicht entweder abstrakt auf deren Funktion in der Unternehmensorganisation und ihre Stellenbeschreibung und/oder konkret auf eine Einschätzung des jeweils verantwortlichen Bereichsleiters stützen kann. Die Befragung kann persönlich, mittels eines Fragebogens oder unter Nutzung des Intranets erfolgen. Vor ihrem Beginn ist ein etwaiges

Mitbestimmungsrecht des Betriebsrats abzuklären. Arbeitsvertragliche Treuepflichten verpflichten den Arbeitnehmer grundsätzlich zur wahrheitsgemäßen Auskunft über Geschehnisse innerhalb seines Arbeitsbereichs. Ein Auskunftsverweigerungsrecht kann jedoch bestehen, wenn die Beantwortung einer Frage unzumutbar ist, etwa weil sich der Arbeitnehmer hierdurch der Gefahr einer Strafverfolgung aussetzt. Häufig fürchten die Befragten auch um haftungs- und arbeitsrechtliche Konsequenzen, wenn sie kartellrechtlich bedeutsame Verhaltensweisen offenbaren. Hier kann es aus Sicht eines Unternehmens sinnvoll sein, im Einzelfall einen Haftungs- und/oder Kündigungsverzicht zu erklären, wenn der betreffende Mitarbeiter einen Aufklärungsbeitrag leistet. Parallel zur Befragung bietet es sich an, potenziell wettbewerbsrelevante Dokumente aus dem Arbeitsbereich des befragten Mitarbeiters zu überprüfen. Dies gilt auch für seine E-Mails, wobei sorgfältig zwischen dienstlichen und privaten E-Mails zu unterscheiden ist, wenn der Mitarbeiter seinen E-Mail-Account auch zu privaten Zwecken nutzen darf. Eine weitere Informationsquelle findet sich schließlich in den Marktdaten, deren Auswertung durch empirische Screenings erfolgen kann, die nachfolgend näher erläutert werden.

Die erfassten kartellrechtlichen Risiken sollten systematisch ausgewertet und die Ergebnisse dieser Auswertung in ein Risikoinventar eingefügt werden. Eine Möglichkeit besteht darin, ausgehend von einem Organigramm der Unternehmens- oder Konzernstruktur die erfassten kartellrechtlichen Risiken einzelner Unternehmensbereiche in ein (erweitertes) Ampel-System einzufügen, indem sie quantifiziert und in vier Risikostufen gering (grün), moderat (gelb), hoch (orange) sowie sehr hoch (rot) eingeordnet werden.¹⁰ Eine solche Inventarisierung dient vor allem der Operationalisierung kartellrechtlicher Risiken. Sie reduziert die Komplexität, mit der sich eine Compliance-Organisation insbesondere in unübersichtlichen Konzernstrukturen regelmäßig konfrontiert sieht.

Die erfassten kartellrechtlichen Risiken sollten überdies systematisch dokumentiert werden. Eine solche Dokumentation dient

- als Grundlage einer sich anschließenden Implementierung neuer oder Neuausrichtung bereits bestehender Compliance-Maßnahmen. Sind kartellrechtliche Risiken eines Unternehmensbereichs bekannt, kann ihnen gezielt entgegengewirkt werden. Auch in der Außendarstellung – etwa gegenüber Kartellbehörden, Geschäftspartnern oder der Öffentlichkeit – stärken „vorzeigbare“ Compliance-Bemühen den positiven Eindruck.
- einer Objektivierung der Risikobewertung. Eine Dokumentation zwingt zur Begründung. Die Risikobewertung wird so teilweise von der Person des Bewertenden entkoppelt und damit objektiviert.
- der Selbstkontrolle kartellrechtlicher Compliance-Programme. Im Idealfall sollte zu jedem dokumentierten Risiko eine korrespondierende Compliance-Maßnahme belegt sein. Fehlt es daran, offenbart bereits die Dokumentation eine Lücke im Compliance-Programm, die es zu schließen gilt.

¹⁰Ein Beispiel aus dem Bereich der Antikorruption findet sich bei Jakob (2010), S. 61 ff.

- der Nachhaltigkeit kartellrechtlicher Compliance-Bemühungen. Da kartellrechtliche Risikoanalysen nicht nur ein einziges Mal, vor der Implementierung eines kartellrechtlichen Compliance-Programms, sondern zeitlich nachfolgend in regelmäßigen Abständen durchgeführt werden sollten, ermöglicht ihre Dokumentation, die Entwicklung des kartellrechtlichen Risikos im Zeitablauf nachzuvollziehen und damit auch eine Beurteilung der Wirksamkeit durchgeföhrter Compliance-Maßnahmen.

Indes gilt es zu beachten, dass eine unternehmensintern erstellte und/oder aufbewahrte Dokumentation ermittelner und bewerteter kartellrechtlicher Risiken im Falle einer kartellbehördlichen Durchsuchung mangels Beschlagnahmefestigkeit zur Folge haben kann, dass der Kartellverstoß auf dem „Silbertablett“ präsentiert wird. Dieses Dilemma kann vermieden werden, indem ein externer Rechtsanwalt mit der Erfassung, Bewertung und Dokumentation bestehender kartellrechtlicher Risiken beauftragt wird, der alle entstehenden Dokumente im eigenen Gewahrsam aufbewahrt und sie dem mandatierenden Unternehmen (etwa per Onlinezugriff) zur Verfügung stellt, ohne dass Vertreter dieses Unternehmens Mitgewahrsam an den betreffenden Dokumenten erhalten.

4.6.3 Empirische Screenings

Konventionelle kartellrechtliche Compliance-Maßnahmen können durch ökonomische Screening-Analysen ergänzt werden, die einerseits einen Beitrag zur Identifizierung von Risikomärkten leisten und andererseits geeignet sind, ungewöhnliche und damit erkläungsbedürftige Marktverhaltensweisen aufzuspüren.¹¹ Mittels ökonomischer Analysen lässt sich die Struktur von Märkten untersuchen, auf denen ein Unternehmen tätig ist. Dies kann auf der Grundlage folgender Risikoindikatoren geschehen:

- Konzentrationsgrad des Marktes, gemessen beispielsweise durch dessen absolute und relative Konzentration, die Konzentrationsrate (CR), den Herfindahl-Hirschmann-Index (HHI) oder den Linda-Index (L). Je konzentrierter ein Markt und je geringer die Anzahl der Marktteilnehmer ist, desto leichter lässt sich eine wettbewerbsbeschränkende Absprache realisieren.
- Transparenzgrad des Marktes, gemessen durch marktspezifische Indikatoren, beispielsweise die Anbieter- und Nachfragezahl sowie die Art der marktypischen Transaktionen (von öffentlichen Transaktionen bis zu vertraulichen bilateralen Verhandlungen zwischen Käufern und Verkäufern). Je transparenter ein Markt aus Sicht der Wettbewerber und je intransparenter er für deren Marktgegenseite ist, desto leichter lässt sich eine wettbewerbsbeschränkende Absprache realisieren.
- Marktzutrittsschranken, gemessen beispielsweise durch Aufwandsanalysen. Je geringer der Aufwand und die benötigte Zeitspanne sind, um in einen Markt neu einzutreten,

¹¹Vgl. Nothelfer (2012), S. 186 ff.

desto größer sind die Schwierigkeiten, eine wettbewerbsbeschränkende Absprache zu treffen und aufrechtzuerhalten.

- Stabilität der Angebots- und Nachfragebedingungen, gemessen durch eine Analyse von Nachfrageschwankungen, des inneren Unternehmenswachstums, der Häufigkeit von Marktzutritten. Eine stark schwankende Nachfrage, ein starkes inneres Wachstum einiger Unternehmen am Markt oder häufige Marktzutritte neuer Unternehmen erhöhen die Instabilität der Marktstruktur und damit auch die Schwierigkeiten, eine wettbewerbsbeschränkende Absprache zu treffen und aufrechtzuerhalten.

Mittels ökonomischer und ökonometrischer Analysen lässt sich zudem das Marktverhalten von Unternehmen daraufhin untersuchen, ob es vom gewöhnlichen Marktverhalten abweicht, das unter Wettbewerbsbedingungen zu erwarten wäre. Dies kann geschehen durch

- eine Analyse des Preissetzungsverhaltens. Zeigen sich Entwicklungsanomalien (Preissprünge, gegenläufige Preistrends) oder lässt sich das Preissetzungsverhalten vollständig durch wettbewerbliche Marktfaktoren (Entwicklung der Produktkosten, der Nachfrage) erklären?
- Varianzanalysen, beispielsweise eine Analyse der Varianz der Verkaufspreise oder der Handelsspannen. Wettbewerbsbeschränkende Absprachen führen regelmäßig zu einer Beruhigung des Markts, die häufig (nicht immer) eine Verringerung der Varianz der Verkaufspreise oder Handelsspannen im Vergleich zur Wettbewerbssituation zur Folge hat. Varianzanalysen untersuchen die Stärke der Schwankung um einen Mittelwert.
- Margenanalysen. Wettbewerbsbeschränkende Absprachen haben regelmäßig (nicht immer) eine Änderung des Preis-Kosten-Verhältnisses zur Folge. Margenanalysen decken auf, wenn es im Zeitablauf zu signifikanten Veränderungen des Preis-Kosten-Verhältnisses gekommen ist, was auf den Anfang oder das Ende einer wettbewerbsbeschränkenden Absprache hinweisen kann.

Derartige empirische Screenings können konventionelle kartellrechtliche Compliance-Maßnahmen nicht ersetzen, da ihre Ergebnisse häufig ambivalent und damit interpretationsbedürftig sind. Angepasst an die individuelle Unternehmenssituation bilden sie jedoch eine sinnvolle Ergänzung. Darüber hinaus mag die Kenntnis davon, dass sein Markerverhalten auch einer empirischen Analyse unterzogen wird, den einen oder anderen Mitarbeiter zusätzlich davon abhalten, insgeheim doch einmal eine wettbewerbsbeschränkende Absprache „auszuprobieren“.

4.6.4 Mock Dawn Raids

Mock Dawn Raids sind Scheindurchsuchungen. Sie werden zumeist von unternehmensexternen Beratern durchgeführt, um Regelungsabläufe für den Ernstfall einer kartell-

behördlichen Durchsuchung zu erproben. *Mock Dawn Raids* können aufgrund des mit ihnen verbundenen Überraschungseffekts und der scheinbaren Autorität der vermeintlichen Ermittlungsbeamten bei einer sich anschließenden detaillierten Fehleranalyse überaus effektiv sein und einen nachhaltigen Lerneffekt zur Folge haben. Dennoch sind sie nicht unumstritten. Abhängig vom Führungsstil und von der etablierten Unternehmenskultur können sie das Vertrauensverhältnis zwischen der Unternehmensführung und den Mitarbeitern erheblich stören. Sie bergen überdies das Risiko in sich, dass

- misstrauische Mitarbeiter reale Wettbewerbsbehörden anrufen, um sich von der „Echtheit“ der Durchsuchung zu überzeugen.
- Wettbewerber telefonisch vor der vermeintlichen Durchsuchung gewarnt werden, was diese ihrerseits dazu veranlasst, einen Bonusantrag zu stellen.
- Dokumente vernichtet werden, die für einen eigenen Bonusantrag notwendig oder zumindest hilfreich sind.
- sensible Mitarbeiter überreagieren und gesundheitlichen Schaden nehmen.

Darüber hinaus darf das Bemühen, eine *Mock Dawn Raid* möglichst echt aussehen zu lassen, nicht übertrieben werden. Andernfalls droht eine Strafbarkeit wegen Urkundendelikten (Fälschung des Durchsuchungsbeschlusses, der Dienstausweise), Amtsanmaßung (der vermeintlichen Ermittlungsbeamten), Verletzung persönlicher Geheimbereiche, Sachbeschädigung oder KörpERVERLETZUNG.

4.7 Fazit

Drohende Geldbußen und Schadenersatzansprüche jeweils in vielfacher Millionenhöhe, ein Verlust an Reputation und Kreditwürdigkeit, Vergabesperren und das Risiko einer persönlichen bußgeld- und schadenersatzrechtlichen Inanspruchnahme haben dazu geführt, dass kartellrechtliche Compliance-Maßnahmen heute zu den notwendigen Elementen eines effektiven Compliance-Programms gehören. Dies gilt nicht nur für Großkonzerne, sondern auch für mittelständische Unternehmen, die von den negativen Folgen eines Kartellverstoßes häufig in einem besonderen Maße betroffen sind. Grundlegende Elemente eines effektiven kartellrechtlichen Compliance-Programms sind: tone from the top, Risikoanalyse, Compliance Officer, Kartellrechtsschulungen, Kontrollaudits. Werden diese Elemente an die individuellen kartellrechtlichen Risiken des sie implementierenden Unternehmens angepasst und anschließend als Teil der Unternehmenskultur ehrlich gelebt, besteht eine gute Chance, von den einleitend genannten Pressemeldungen verschont zu bleiben.

Literatur

- BESEN, M./GRONEMEYER, A. (2009): Kartellrechtliche Risiken bei Unternehmenskäufen und Clean Team, aus: CCZ, Heft 1/2009.
- BUNDESKARTELLAMT (2017): Hinweispapier zum Preisbindungsverbot im Bereich des statio-nären Lebensmitteleinzelhandels.
- DE CROZALS, J. (2009): Dawn Raids durch die Kartellbehörden – Ablauf, Grenzen und Hand-lungsoptionen, aus: CCZ, Heft 3/2009.
- EU-Kommission (2011): Leitlinien zur Anwendbarkeit von Artikel 101 des Vertrags über die Arbeitsweise der Europäischen Union auf Vereinbarungen über horizontale Zusammenarbeit, ABI. EU 2011, Nr. C 11, S. 1 ff.
- HEINICHEN, C. (2011): Unternehmensbegriff und Haftungsnachfolge im Europäischen Kartell-recht, Baden-Baden.
- HEINICHEN, C. (2015): Grenzen der kartellrechtlichen Rechtsnachfolgehaftung, aus: WuW, Heft 8/2015.
- HÖVELBERNDT, A. (2017): Erfolgreiche Selbsteinigung bei Verstößen gegen das Kartell- und Wettbewerbsrecht, aus: NZBau, Heft 8/2017.
- JAKOB, A. (2010): Das Ganze ist mehr als die Summe seiner Teile – Eine praxisorientierte An-wendung des „Ampel-Kodex“, aus: CCZ, Heft 2/2010.
- NOTHELFER, W. (2012): Empirische Screening als innovative Methode im Rahmen der Anti-trust-Compliance, aus: CCZ, Heft 5/2012.
- RAUM, R. (2012): Strafrechtliche Pflichten von Compliance-Beauftragten – Zum Urteil des Bundes-gerichtshofs vom 17.7.2009, aus: CCZ, Heft 5/2012.
- WISSMANN, M./DREYER, J./WITTING, J. (2008): Kartell- und regulierungsbehördliche Er-mittlungen im Unternehmen und Risikomanagement, München.



Christian Heinichen ist Rechtsanwalt im Münchener Büro von ADVANT Beiten. Er berät seine Mandanten zu allen Aspekten des europäischen und deutschen Kartellrechts mit einer Spezialisierung auf Kartellbußgeld- und -schadenersatzverfahren. Einen seiner Tätig-keitsschwerpunkte bildet die kartellrechtliche Compliance, ins-besondere für mittelständische Unternehmen. Christian Heinichen ist Autor zahlreicher kartellrechtlicher Publikationen und regelmäßig Referent bei kartellrechtlichen Fachveranstaltungen. Er lehrt zudem als Lehrbeauftragter für Kartellrecht an der Universität Augsburg.



Geldwäsche-Compliance bei Industrie- und Handelsunternehmen (Güterhändler)

5

Jürgen Krais

Inhaltsverzeichnis

5.1	Einführung.....	96
5.2	Geldwäsche.....	96
5.3	Terrorismusfinanzierung.....	98
5.4	Güterhandel: die internationale Perspektive.....	99
5.5	Güterhandel: Rechtslage in Deutschland.....	99
5.6	Güterhandel: Unternehmensgruppen.....	100
5.7	Privilegierte Güterhändler.....	101
5.8	Verdachtsmeldepflichten.....	103
5.8.1	Meldepflichtige Verdachtsfälle.....	103
5.8.2	Niedrige Verdachtsmeldeschwelle.....	103
5.8.3	Geldwäsche-Verdachtsmeldung.....	105
5.8.4	Verbot des „Tipping-Off“.....	106
5.8.5	Wartefrist nach Verdachtsmeldung.....	106
5.9	Kundensorgfaltspflichten im Verdachtfall.....	107
5.9.1	Allgemeine Sorgfaltspflichten.....	107
5.9.2	Verstärkte Sorgfaltspflichten.....	108
5.9.3	Mitwirkungspflichten und Tipping-Off.....	108
5.10	Verdachtsfälle und Risiko der Strafbarkeit.....	109
5.11	Ausblick: EU-Verordnung zur Verhinderung von Geldwäsche.....	110
	Literatur.....	111

J. Krais (✉)
Siemens AG, München, Deutschland

5.1 Einführung

Industrie- und Handelsunternehmen haben in den vergangenen Jahren erhebliche Anstrengungen bei der Implementierung effektiver Compliance-Programme unternommen. Dabei lag der Schwerpunkt in der Regel auf der Verhinderung von Korruptions- oder Kartellstraftaten. Geldwäsche-Compliance spielt dagegen noch immer kaum eine Rolle. Vielfach geht man davon aus, dass Industrie und Handel „*keine Geldwäsche betreiben und daher keine Anti-Geldwäsche brauchen*“.¹ Dabei ist Geldwäsche-Prävention längst mehr als der Versuch, das organisierte Verbrechen daran zu hindern, Gelder aus Drogenkriminalität, Waffenschmuggel oder Menschenhandel auf Bankkonten einzuzahlen. Die Globalisierung der internationalen Handelsströme bietet vielfältige Möglichkeiten im Rahmen von Handelsbeziehungen illegales Vermögen zu generieren, seine Herkunft zu verschleiern, es gewinnbringend anzulegen oder mit legalem Geld zu vermischen und auf diese Weise zu „waschen“ („*trade based money laundering*“). Im Folgenden soll dem Leser ein Überblick über die für Industrie- und Handelsunternehmen („*Güterhändler*“) geltenden Bestimmungen des Geldwäschegesetzes (GwG) gegeben werden. Besonderer Fokus liegt dabei auf der Praxis von Unternehmen in nicht bargeldintensiven Branchen.

5.2 Geldwäsche

§ 1 Abs. 1 GwG definiert Geldwäsche unter Verweis auf den Tatbestand der strafrechtlichen Geldwäsche (§ 261 StGB). Der Begriff Geldwäsche stammt aus der Zeit der Prohibition in den USA. Er wird häufig in Verbindung mit „Al“ Capone gebracht, dem berüchtigten Gangsterboss aus dem Chicago der 1920er-Jahre. Er soll die Herkunft von Bargeld aus illegalen Geschäften mit Hilfe damals weit verbreiteter Waschsalons verschleiert haben (engl. „*Laundromats*“).² 1986 wurde in den USA die weltweit erste Strafnorm gegen Geldwäsche eingeführt. Ziel war, die Verkehrsfähigkeit von Gewinnen aus Drogengeschäften und so indirekt den illegalen Handel mit Drogen einzuschränken („*war on drugs*“).³ 1989 wurde im Rahmen der OECD eine Arbeitsgruppe zur Bekämpfung von Geldwäsche gegründet, die Financial Action Task Force (FATF). Sie hat 40 Empfehlungen zur Verhinderung von Geldwäsche veröffentlicht, die sich an die Staatengemeinschaft richten. Sie bilden die regulatorische Basis der Geldwäsche-Gesetze in fast 190 Ländern der Erde, auch der aktuell 5. EU-Geldwäsche-Richtlinie (EU-GWRL)⁴ und des deutschen Geldwäschegesetzes („GwG“).⁵

¹ Bülte NZWist 2017, 276, 276.

² Ausführlicher dazu Krais, Geldwäsche-Compliance für Industrie und Handel, Praxishandbuch für Güterhändler, Beck, 2. Auflage 2022, § 1 Rn. 4.

³ https://en.wikipedia.org/wiki/Money_Laundering_Control_Act (aufgerufen am 15.4.2023).

⁴ Richtlinie (Eu) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015.

⁵ Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (GeldwäscheG – GwG) – BGBl I 2017, 1822 ff.

Wie Geldwäsche aus kriminalistischer Sicht funktioniert, wird meist mit Hilfe des von US-Zollbehörden in den 1990er-Jahren entwickelten Drei-Phasenmodells erklärt.⁶ Auch wenn das Dreiphasenmodell nicht anhand von Geldwäsche im Kontext internationaler Handelsströme entwickelt wurde, ist es doch ein guter Einstieg zum Verständnis der Materie. Nach diesem Modell werden in einem ersten Schritt Vermögenswerte, die aus einer Straftat stammen, in den legalen Wirtschaftskreislauf eingespeist (Placement). Durch verschiedene Transaktionen wird anschließend die Herkunft aus der Straftat verschleiert (Layering). Dabei kann es sich um einfache Vorgänge handeln, wie z. B. den Kauf eines Fahrzeugs mit der Beute aus einem gewerbsmäßigen Betrug und der rasche Wiederverkauf, um so aus einem vermeintlich legalen Geschäft unverdächtige Erträge zu generieren. Häufig findet aber ein komplexer, internationaler (grenzüberschreitender) Mechanismus Anwendung.⁷ Am Ende steht die Verwendung der gewaschenen Vermögenswerte für legale, unverdächtige Projekte und Investitionen bzw. den Konsum durch die Täter und Beteiligten (Integration). In der Praxis müssen nicht jedes Mal alle Phasen dieses Modells durchlaufen werden. Für die Strafbarkeit der Geldwäsche und den Umfang geldwäscherichtlicher Pflichten des GwG spielt es keine Rolle, in welcher Phase man sich gerade befindet.

Gegenstand strafbarer Geldwäsche i. S. d. § 261 StGB kann, anders als der Begriff vermuten lässt, jeder Vermögensgegenstand sein, nicht nur Geld, insbesondere nicht nur Bargeld. Besonders gut geeignet für Zwecke der Geldwäsche sind hochpreisige bzw. werthaltige, leicht transportierbare und leicht wiederverkaufbare Gegenstände wie z. B. Edelmetalle oder Edelsteine, hochpreisige Fahrzeuge, sowie Kunstgegenstände und Antiquitäten („*hochwertige Güter*“⁸). Für Geldwäsche kommt aber auch jeder andere Vermögensgegenstand in Frage, wie z. B. Immobilien, Unternehmen oder Beteiligungen daran sowie immaterielle Vermögensgegenstände wie Forderungen und Rechte. Der Vermögensgegenstand muss aus einer vorausgehenden Straftat (der Vortat) stammen („*daraus herriühren*“). Seit der Reform des § 261 StGB im März 2021 kann jede Straftat des Kern- und Nebenstrafrechts und auch Auslandsstrafaten Vortat der strafbaren Geldwäsche sein („*all crimes approach*“).⁹ Entscheidend ist dabei nicht, dass ein Vermögensgegenstand unmittelbar aus einer Straftat stammt, wie z. B. die Beute aus dem Bankraub. Geldwäschefähig ist auch jeder Vermögensgegenstand, der durch einen oder mehrere Austauschvorgänge oder Umwandlungsvorgänge an die Stelle des ursprünglich aus der Vortat stammenden Gegenstands tritt („*Surrogate*“), z. B. ein Schmuckstück, das mit Geld aus

⁶Herzog, Herzog/Achtelik, GwG, 4. Auflage 2020, Einleitung, Rn. 7–11.

⁷Siehe z. B. der Russian Laundromat, https://de.wikipedia.org/wiki/Russischer_Waschsalon (aufgerufen am 15.4.2023).

⁸Die Definition: „hochwertiger Güter“ in § 1 X GwG greift nicht alle genannten Kriterien auf und ist daher weiter.

⁹Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche vom 9.3.2021, BGBl. I 2021, 327 ff.

einem Betrug gekauft wird.¹⁰ Der „Makel“ der Straftat setzt sich darüber hinaus bei der Vermischung legalen und illegalen Vermögens am Gesamtvermögen fort, beispielsweise wenn illegal erlangtes Geld auf ein Bankkonto eingezahlt wird, auf dem sich Beträge aus legaler Tätigkeit befinden („*Gesamtkontamination*“).¹¹ Wird derart aus einer Straftat herrührendes Vermögen verwahrt oder versteckt, dem Zugriff der Behörden und Berechtigten entzogen oder unter Verschleierung seiner Herkunft verwendet, droht Strafbarkeit wegen Geldwäsche nach § 261 StGB. Auf die juristischen Einzelheiten der Strafbarkeit soll hier nicht eingegangen werden, da diese – anders als der Verweis in § 1 Abs. 1 GwG vermuten lässt – für die Geldwäsche-Prävention keine wesentliche Rolle spielen. Aus der Perspektive der Unternehmens-Compliance ist zu beachten, dass die Einbeziehung nur indirekt aus einer Straftat herrührender Vermögensgegenstände ein erhebliches Risiko birgt, in Geldwäsche-Aktivitäten Dritter einzbezogen zu werden.

5.3 Terrorismusfinanzierung

Nach den terroristischen Anschlägen vom 11. September 2001 auf die USA wurde das Mandat der FATF auf die Bekämpfung der Terrorismusfinanzierung ausgedehnt („*war on terror*“). Entsprechend reflektieren die Geldwäschegesetze praktisch weltweit sowohl den Kampf gegen Geldwäsche als auch den gegen Terrorismus. Konsequent ist dies insofern, als sich Geldwäscher wie Terroristen und deren Unterstützer ähnlicher Mechanismen bedienen, um ihre illegalen Aktivitäten zu verschleiern. Strukturell besteht allerdings ein wichtiger Unterschied zwischen Geldwäsche und Terrorismusfinanzierung: Geldwäsche dient dazu, die Herkunft von Vermögenswerten aus Straftaten zu verschleiern; dagegen kommt es bei der Terrorismusfinanzierung darauf an, Geld für Terrorismus und begleitende Straftaten zu gewinnen oder zu verwenden. Es bedarf dabei keiner Vortat. Vermögen, das der Terrorismusfinanzierung dient, kann gleichermaßen aus legaler wie illegaler Quelle stammen. Anders als der Begriff Geldwäsche ist Terrorismusfinanzierung in § 1 Abs 2 GwG nicht unter Rückgriff auf (allein) die Vorschrift strafbarer Terrorismusfinanzierung (§ 89c StGB) definiert. Vielmehr umfasst der Begriff auch das Sammeln oder Bereitstellen von Vermögenswerten zur Bildung einer terroristischen Vereinigung im In- oder Ausland, §§ 129 a, b StGB und weit darüber hinaus für eine Vielzahl allgemeiner Strafarten im Sinne des EU-Rahmenbeschlusses zur Bekämpfung des Terrorismus von 2017, wenn diese einen terroristischen Hintergrund oder Zweck haben. Dabei spielt es keine Rolle, ob Täterschaft oder Beihilfe vorliegt (§ 1 Abs. 2 Nr. 3 GwG). Spezifische Pflichten zur Verhinderung der Terrorismusfinanzierung enthält das GwG dagegen nicht. Tatsächlich unterscheiden sich die gesetzlich normierten Anforderungen des GwG an die Verhinderung von Terrorismusfinanzierung nicht von denen der Geldwäsche-Prävention. Soweit im Folgen-

¹⁰ BGH NStZ-RR 2019, 145, 145 f.

¹¹ BGH NZWiSt 2016, 149, 160.

den vereinfachend von Geldwäsche die Rede ist, ist daher die Verhinderung der Terrorismusfinanzierung („*Combat Terrorism Financing*“, CTF) stets mit umfasst.¹²

5.4 Güterhandel: die internationale Perspektive

Nach den Empfehlungen der FATF, wie nach den Vorgaben der EU-GWRL, gelten Anforderungen zur Geldwäsche-Prävention auch im Bereich des Warenhandels (*Güterhandel*). Der Fokus liegt dabei auf dem Handel von Waren gegen Bargeld oberhalb bestimmter Schwellenwerte (bargeldintensive Branchen). So sehen die FATF Empfehlungen die Einziehung von Güterhändlern vor, sofern sie Edelmetalle (z. B. Gold, Silber, Platin) oder Edelsteine bzw. Schmuck ab einer zu definierenden Bargeldschwelle handeln.¹³ Dagegen sieht die EU-GWRL die Einbeziehung aller Güterhändler in den Kreis der Verpflichteten vor, sofern sie im Einzelfall Güter gegen Bargeld in Höhe von mehr als 10.000 € erwerben oder vertreiben. Welche Güter sie erwerben oder vertreiben, spielt dabei keine Rolle.¹⁴ In manchen Ländern wird der Fokus auf weitere, als hochwertig bzw. attraktiv für Geldwäsche angesehene Güter gelegt wie z. B. Luxuswaren (Pelze). Die Mehrzahl der Güterhändler unterliegt jedoch in der EU, wie weltweit, keinen geldwäscherechtlichen Pflichten.

5.5 Güterhandel: Rechtslage in Deutschland

Der deutsche Gesetzgeber folgt der internationalen Systematik im Bereich Güterhandel nicht. Vielmehr sind alle Güterhändler in Deutschland Verpflichtete i. S. d. § 2 Abs. 1 Nr. 16 GwG. Dies gilt ohne Einschränkung auf bestimmte Branchen oder Güter, Unternehmen einer bestimmten Größe oder darauf, ob sie Bargeldgeschäfte vornehmen und ggf. in welchem Umfang. Als Güterhändler gilt in Deutschland jede Person ungeachtet ihrer Rechtsform, die gewerblich Güter vertreibt (§ 1 Abs. 9 GwG), Einzelkaufleute genauso wie größere Unternehmen. Damit geht die Rechtslage in Deutschland weit über die Vorgaben der EU-GWRL hinaus („*überschießende Tendenz*“). Hinzu kommt, dass der Begriff des Güterhändlers weit ausgelegt wird. Er umfasst nicht nur klassische An- und Verkäufer von Waren (Händler), sondern auch das produzierende Gewerbe (Industriebetriebe)¹⁵ und Versorgungs-

¹² Krais, Geldwäsche-Compliance für Industrie und Handel, Praxishandbuch für Güterhändler, Beck, 2. Auflage 2022, § 1 Rn. 5 f.

¹³ Siehe Empfehlung 22 c) der FATF, <https://www.fatf-gafi.org/content/dam/recommandations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf>, (aufgerufen am 15.4.2023).

¹⁴ Art. 2 (1) e) EU-GWRL.

¹⁵ Krais, Geldwäsche-Compliance für Industrie und Handel, Praxishandbuch für Güterhändler, Beck, 2. Auflage 2022, § 3 Rn. 14.

betriebe.¹⁶ Güterhandel setzt nicht voraus, dass Güter in eigenem Namen und auf eigene Rechnung vertrieben werden; daher sind z. B. auch Auktionäre, Kommissionäre und Handelsvertreter Güterhändler, selbst wenn sie zivilrechtlich betrachtet nicht Partei eines Kauf- oder Verkaufsvertrags werden (§ 1 Abs. 9 GwG). Allein der Einkauf von Gütern, wie z. B. der Kauf von Reinigungsmitteln für eine Reinigungsfirma oder von Büchern für eine Rechtsanwaltskanzlei, macht diese dagegen nicht zum Güterhändler.¹⁷ Entscheidend für die Einstufung als Güterhändler ist stets, dass die prägende Tätigkeit des Unternehmens im An- und Verkauf von Gütern besteht.¹⁸ Ungeachtet dessen können sich einzelne geldwäsche-rechtliche Pflichten auf Vorgänge im Einkauf eines Güterhändlers beziehen, wie sich insbesondere aus §§ 4 Abs. 5, 10 Abs. 6a GwG ergibt.

Als Güter gelten heute alle Vermögensgegenstände, die Gegenstand von Handelsgeschäften sein können. Umfasst ist daher nicht nur der Vertrieb beweglicher Sachen, sondern auch der von Immobilien. Der Begriff umfasst des Weiteren nicht nur materielle, sondern auch immaterielle Vermögensgegenstände, wie z. B. Rechte und Forderungen, Unternehmensbeteiligungen oder Schutzrechte, wie Marken, Patente oder Lizenzen bzw. Software. Es spielt keine Rolle, ob Güter für den privaten oder industriellen Bedarf bestimmt sind und ob diese in Deutschland oder international vertrieben werden. Auch der Wert der Güter ist unerheblich. Der Zeitungskiosk an der Ecke ist im Grunde genauso Güterhändler, wie der Großhändler oder ein international tätiger Maschinen- und Anlagenbauer, auch wenn ihr konkretes Geldwäsche-Risiko sehr unterschiedlich sein wird.¹⁹ Ausgenommen vom Begriff des Güterhändlers sind nur Dienstleister (z. B. Zeitarbeitsfirmen, Internet-Plattform und Social-Media-Unternehmen), landwirtschaftliche Betriebe und Bergbau.

5.6 Güterhandel: Unternehmensgruppen

Die Definition des Güterhändlers in § 1 Abs. 9 GwG stellt auf einzelne Personen ab („*wer*“), nicht auf Firmengruppen oder Unternehmen. Dabei spielt keine Rolle, ob es sich um eine natürliche Person („*Einzelkaufmann*“) oder um eine Gesellschaft oder andere privatrechtliche Vereinigung (§ 20 GwG) handelt. Güterhändler iSd. GwG ist daher stets eine natürliche oder juristische Person oder Vereinigung, nicht eine wirtschaftliche Einheit (Betrieb, Unternehmen oder Unternehmensgruppe). Daran ändert auch § 9 GwG

¹⁶ BMF, Auslegung des Begriffs „Güterhändler“ gemäß § 2 Abs. 1 Nr. 12 GwG (a. F.) vom 24.4.2012 – VII A 3 – WK 5023/11/10021.

¹⁷ Krais, Geldwäsche-Compliance für Industrie und Handel, Praxishandbuch für Güterhändler, Beck, 2. Auflage 2022, § 3 Rn. 18.

¹⁸ Gemeinsame Anwendungs- und Auslegungshinweise der Länder (AuA Nichtfinanzsektor) vom März 2021, S. 2, Ziffer 1.2.

¹⁹ Krais, Geldwäsche-Compliance für Industrie und Handel, Praxishandbuch für Güterhändler, Beck, 2. Auflage 2022, § 3 Rn. 12.

(„*gruppenweite Pflichten*“) nichts. Die Vorschrift definiert nicht die Verpflichteten-Eigenschaft von Unternehmen. Sie richtet sich an die Muttergesellschaft einer Gruppe und setzt deren Eigenschaft als Verpflichtete i. S. d. § 2 Abs. 1 GwG voraus. Vor diesem Hintergrund ist es notwendig (und zulässig) jede rechtliche Einheit einer Unternehmensgruppe gemäß § 2 Abs. 1 GwG auf Ihre Eigenschaft als Güterhändler oder anderweitig GwG-Verpflichtete zu überprüfen. Der Umfang geldwäscherechtlicher Pflichten einzelner Gesellschaften in einer Gruppe kann folglich variieren. Während eine Gesellschaft als Kreditinstitut gilt (§ 2 Abs. 1 Nr. 1 GwG), ist eine andere möglicherweise Immobilienmakler (§ 2 Abs. 1 Nr. 14 GwG) und eine dritte Güterhändler (§ 2 Abs. 1 Nr. 16 GwG). Denkbar ist auch, dass einzelnen Mitgliedern der Unternehmensgruppe keine geldwäscherechtlichen Pflichten obliegen, während andere in vollem Umfang Verpflichtete sind. Es gibt im GwG keine Grundlage für die Annahme, dass die Gesellschaft, die die umfangreichsten geldwäscherechtlichen Pflichten hat, stets den Rest der Gruppe „infiziert“. Nur im Geltungsbereich des § 9 GwG muss die Muttergesellschaft, die selbst Verpflichtete ist, gleiche Standards der Geldwäsche-Bekämpfung in der Gruppe schaffen. Auch das bedeutet nicht, dass alle Gruppenmitglieder dieselben geldwäscherechtlichen Pflichten haben. Die vom GwG für einzelne Verpflichtete geschaffenen Privilegierungen werden durch § 9 GwG nicht abgeschafft.

In Bezug auf Holding-Gesellschaften in der Industrie und im Handel, die zumeist nicht oder nur in geringem Umfang operative Geschäfte tätigen, gilt zwar, dass ihr Hauptzweck formal betrachtet im Halten und Verwalten von Beteiligungen besteht. Sie gelten aufgrund der Ausnahmeverordnung in § 1 Abs. 24 Satz 2 GwG nicht als Finanzunternehmen (§ 2 Abs. 1 Nr. 6 GwG) und daher nicht als GwG-Verpflichtete. Andere Gesellschaften, die z. B. strategische Investments in Start-Ups vornehmen („*Venture-Capital-Gesellschaften*“) oder Betriebsteile in Gesellschaften verwalten, die ausgegliedert werden („*De-Investments*“), können dagegen als Finanzunternehmen GwG-Verpflichtete sein (§ 1 Abs. 24 Satz 1 GwG).

5.7 Privilegierte Güterhändler

Zu den geldwäscherechtlichen Kernpflichten der GwG-Verpflichteten gehören das Risikomanagement (§§ 4–9 GwG), die kundenbezogenen Sorgfaltspflichten (§§ 10–15 GwG) und die Pflichten im Zusammenhang mit der Meldung von Verdachtsfällen (§§ 43 ff GwG). Der Umfang geldwäscherechtlicher Pflichten hängt bei Güterhändlern davon ab, ob und in welcher Höhe sie Bargeldgeschäfte tätigen. Konkret sind Güterhändler von den Risikomanagementpflichten des GwG befreit, sofern sie keine Bargeldgeschäfte über Güter ab 10.000 € tätigen (§ 4 Abs. 5 Nr. 1c GwG; „*privilegierte Güterhändler*“). Dabei ist der Begriff „*Privilegierung*“ missverständlich. Zwar handelt es sich um Ausnahmen gegenüber den in Deutschland für alle anderen Verpflichteten geltenden Vorschriften. Ihren Grund haben sie aber in der gegenüber den Vorgaben der FATF und EU-GWRL überschreitenden Tendenz des GwG im Bereich Güterhandel (siehe oben Abschn. 5.5). Sie dienen der (teilweisen)

Korrektur dieses Umstands, mithin der Beseitigung von Nachteilen gegenüber ausländischen Wettbewerbern, nicht der Privilegierung von Güterhändlern im engeren Sinne.²⁰ Die genannten Schwellenwerte gelten gleichermaßen beim Ankauf, wie beim Verkauf von Gütern und stellen auf jeden Einzelfall einer Bargeldtransaktion ab. Umgehungsversuche durch Aufsplitten zusammengehöriger Zahlungen in mehrere Transaktionen („*Smurfing*“) ändern an der Rechtsfolge nichts (siehe dazu auch die umfassende Definition der „Transaktion“ in § 1 Abs 5 GwG). Für bestimmte hochwertige Güter i. S. d. § 1 Abs. 10 Satz 2 Nr. 1 GwG (Edelmetalle) gilt abweichend eine niedrigere Bargeldgrenze von nur 2000 €. Für alle anderen hochwertigen Güter iSD. § 1 Abs. 10 GwG bleibt es bei der Bargeldgrenze von 10.000 Euro. Für gewerbsmäßige Transaktionen über Kunstgegenstände gilt eine allgemeine Grenze von 10.000 €, unabhängig ob bar oder unbar (§ 4 Abs. 5 Nr. 1a GwG). Durch die genannte Vorschrift privilegierte Güterhändler sind in Deutschland zwar GwG-Verpflichtete, aber von der Pflicht zur Erstellung einer Risikoanalyse (§ 5 GwG) und der Durchführung der umfassenden Sicherungsmaßnahmen (§ 6), sowie der Bestellung eines Geldwäschebeauftragten (§ 7 Abs. 3 GwG) und der gruppenweiten Pflichten (§ 9 GwG) befreit. Für sie gilt der 2. Abschnitt des GwG nicht.²¹ Im Hinblick auf die Verhältnismäßigkeit fragwürdig ist allerdings die Auslegung, wonach schon ein einmaliges Überschreiten der Grenzwerte („*Ausreißer*“) die Privilegierung entfallen lässt und die umfassenden Rechtsfolgen der Vorschriften für alle weiteren Geschäfte auslöst.²²

Identische Schwellenwerte definiert § 10 Abs. 6a GwG für die Pflicht zur Durchführung allgemeiner Sorgfaltspflichten (§§ 10–13 GwG) durch Güterhändler, auch als Know-Your-Customer-Prüfung (KYC) bekannt. Güterhändler sind demnach nicht verpflichtet vor Eingehen jeder Geschäftsbeziehung eine KYC -Prüfung durchzuführen. § 10 Abs. 6a GwG verdrängt die allgemeineren Regelungen des § 10 Abs. 3 GwG („lex specialis“). Da sich die Sorgfaltspflichten stets auf den individuellen Geschäftspartner oder Partner einer Transaktion beziehen, ist die Rechtsfolge bei Ausreißern nicht so gravierend wie beim Risikomanagement: Es entsteht dann nur die Pflicht in Bezug auf den konkreten Geschäfts- oder Transaktionspartner allgemeine Sorgfaltspflichten durchzuführen. Dabei darf der Verweis auf (nur) die allgemeinen Sorgfaltspflichten nicht missverstanden werden: Güterhändler sind nicht nur von den allgemeinen Sorgfaltspflichten vor Eingehung einer Geschäftsbeziehung befreit, sondern von jeder Art der kundenbezogenen Prüf- und Dokumentationspflicht des GwG, insbesondere auch den verstärkten Sorgfaltspflichten des § 15 GwG. Denn letztere kommen, wie sich aus § 15 Abs. 1 GwG („zusätzlich“) ergibt, nur in Betracht, wenn bereits eine Pflicht zu allgemeinen Sorgfaltspflichten besteht. Solange sie die Voraussetzungen und Schwellenwerte des § 10 Abs. 6a GwG nicht erreichen, sind Güterhändler daher auch bei Vorliegen (nur) der spezifischen Voraussetzungen des § 15 GwG nicht zu verstärkten Sorgfaltspflichten verpflichtet.²³ Auf die Rechtsfolgen des

²⁰ Krais, Geldwäsche-Compliance für Industrie und Handel, Praxishandbuch für Güterhändler, Beck, 2. Auflage 2022, § 3 Rn. 25.

²¹ BT-Drs. 18/11555, S. 109 noch zu § 4 Abs. 5 GwG a. F.

²² Krais, Geldwäsche-Compliance für Industrie und Handel, Praxishandbuch für Güterhändler, Beck, 2. Auflage 2022, § 4 Rn. 21 f.

²³ Krais, Geldwäsche-Compliance für Industrie und Handel, Praxishandbuch für Güterhändler, Beck, 2. Auflage 2022, § 6 Rn. 9 ff.

§ 10 Abs. 3 Nr. 3 GwG (allgemeine Sorgfaltspflichten im Verdachtsfall) wird im Zusammenhang mit den Verdachtmeldepflichten eingegangen.

5.8 Verdachtmeldepflichten

5.8.1 Meldepflichtige Verdachtsfälle

Kernpflicht aller GwG-Verpflichteten inklusive Güterhändlern ist die Pflicht zur Meldung von Verdachtsfällen (§ 43 Abs 1 GwG). Meldepflichtig ist zum einen der Verdacht der Geldwäsche (§ 43 Abs. 1 Nr. 1 GwG), zum anderen der Verdacht der Terrorismusfinanzierung (§ 43 Abs. 1 Nr. 2 GwG). In der Praxis haben Meldungen wegen des Verdachts der Terrorismusfinanzierung eine nur untergeordnete Rolle, weshalb hier weiterhin nur vom Verdacht der Geldwäsche die Rede sein wird. Eine Privilegierung wie beim Risikomanagement oder bei den Sorgfaltspflichten (siehe Abschn. 5.7) besteht insoweit nicht. Güterhändler sind wie alle anderen Verpflichteten auch, ausnahmslos verpflichtet, bei Vorliegen der Voraussetzungen des § 43 Abs 1 GwG Verdachtmeldung zu erstatten.

5.8.2 Niedrige Verdachtmeldeschwelle

Entgegen dem Eindruck, den § 1 Abs. 1 GwG erweckt, löst sich die Definition des meldepflichtigen Geldwäsche-Verdachts in § 43 Abs. 1 Nr. 1 GwG und seine Auslegung in mehrfacher Hinsicht vom Straftatbestand bzw. den strafprozessualen Voraussetzungen des Geldwäsche-Verdachts. Ein meldepflichtiger Geldwäsche-Verdacht liegt daher nicht erst vor bei Hinweisen auf tatbestandliche Geldwäsche i. S. d. § 261 StGB. Die Meldepflicht besteht vielmehr bereits, wenn „*Tatsachen darauf hindeuten, dass ein Vermögensgegenstand aus einer Straftat stammt, die Vortat der Geldwäsche sein könnte*“ (§ 43 Abs. 1 Nr. 1 GwG). Die Meldepflicht des GwG ist daher „vortatbezogen“ und setzt keinen Hinweis gerade auf die spezifischen Tathandlungen des § 261 StGB voraus. Anders als im Strafprozessrecht ist auch kein doppelter Verdacht nötig, der Elemente der Vortat und geldwäscherechtlicher Handlungen gleichzeitig erfordert.²⁴ Der „*all crimes approach*“ hat seit 18.03.2021 alle Straftaten zur potenziellen Vortat der Geldwäsche gemacht, auch Auslandstaten. Das führt dazu, dass nach § 43 Abs. 1 Nr. 1 GwG Hinweise auf Vermögensgegenstände, die mit irgendeiner Straftat in Verbindung stehen, praktisch stets als Geldwäsche-Verdacht meldepflichtig sein können.

In der Natur des Verdachts liegt es, dass keine Gewissheit erforderlich ist, dass tatsächlich Geldwäsche oder eine andere Straftat vorliegt. Die Aufsichtsbehörden verlangen von den Verpflichteten nicht die formal-juristische Subsumption von verdächtigen Umständen unter die Tatbestandsmerkmale des § 261 StGB oder einer anderen Strafnorm. Es ist unerheblich, ob eine mögliche Straftat bereits vollendet oder beendet wurde, noch im Ver-

²⁴ Zum doppelten Anfangsverdacht z. B. BVerfG, 31.1.2020, NJW 2001, 1351 ff.

suchsstadium ist oder erst im Bereich der Planung und Vorbereitung. Die Aufsichtsbehörden beladen den Verpflichteten auch nicht die Abwägung auf, ob ein Verdacht im Sinne strafprozessualer Vorschriften vorliegt. Unter Berufung auf den Begriff „*hindeuten*“ in § 43 Abs. 1 GwG wird die Verdachtsmeldeschwelle vielmehr deutlich unterhalb der – ohnehin nicht sehr hohen – Schwelle des Anfangsverdachts des § 152 Abs. 2 StPO gesehen.²⁵ Um die Verdachtsmeldeschwelle noch weiter zu konkretisieren, werden von der Meldebehörde, der Zentralstelle für Finanztransaktionsuntersuchungen (FIU, § 27 Abs. 1 GwG), in unregelmäßigen Abständen sogenannte Anhaltspunktepapiere („*Typologien*“) zur Geldwäsche und Terrorismusfinanzierung veröffentlicht.²⁶ Sie enthalten Beispiele für Risikosachverhalte bzw. auffällige Verhaltensweisen oder Muster. Diese stellen in der Mehrzahl keine objektiven Hinweise auf Geldwäsche oder andere Straftaten dar. In der Regel lässt sich nur sich nicht sicher ausschließen, dass das Verhalten oder Muster der Geldwäsche oder anderen Straftaten dient.

Dennoch besteht auch bei Vorliegen von Anhaltspunkten der FIU-Typologien nicht automatisch eine Meldepflicht. Letztlich kommt es stets auf eine individuelle Bewertung des Sachverhalts durch den Verpflichteten an. Das bei ihm vorhandene Branchenwissen räumt ihm einen, wenn auch geringen, subjektiven Beurteilungsspielraum ein, ob ein im Sinne der FIU-Typologien auffälliger Vorgang schon als Verdacht einzustufen und daher zu melden ist. Der subjektive Beurteilungsspielraum bedeutet aber nicht, dass der Verpflichtete Ermessen hat. Im Verdachtsfall besteht eine Rechtpflicht zur Meldung. Die Entscheidung des Verpflichteten kann von der Aufsichtsbehörde überprüft werden, soweit es die Frage betrifft, ob alle wesentlichen Umstände in die Bewertung einbezogen und richtig gewichtet wurden und ob allgemeine und spezielle Erfahrungssätze richtig angewandt wurden. Sieht der Verpflichtete von einer Meldung ab, muss er dies außerdem umfangreich dokumentieren (§ 8 Abs. 1 Nr. 4 GwG). Angesichts der möglichen Rechtsfolgen einer falschen Entscheidung (Bußgeld im Fall nicht ordnungsgemäßer Verdachtsmeldung, § 56 Nr. 69 GwG; ggf. eigene Strafbarkeit nach § 261 Abs. 6 StGB – leichtfertige Geldwäsche und einhergehenden Reputationsrisiken) tendieren Verpflichtete im aufsichtsrechtlich stärker durchdrungenen Finanzsektor bei Vorliegen von Anhaltspunkten iSd. FIU-Typologien zu einer Meldung, sofern Geldwäsche oder andere Straftaten nicht sicher ausgeschlossen werden können. Die FIU-Typologien bewirken daher faktisch eine widerlegbare Vermutung und Beweislastumkehr zugunsten der Meldepflicht. Damit wird der Geldwäsche-Verdacht i. S. d. GwG fast völlig von den strafrechtlichen und strafprozessualen Voraussetzungen insbesondere der Geldwäsche i. S. d. § 261 StGB gelöst. Die Meldepflicht des § 43 Abs. 1 GwG beruht auf einem rein kriminalistisch begründeten Verdachtsbegriff weit unterhalb strafprozessualer Mindestanforderungen.²⁷ Güterhändlern ist in jedem Fall anzuraten eine Meldung desto eher in Betracht zu ziehen, je mehr An-

²⁵ BT-Drs. 18/11555, 156, zu § 43 Abs. 1 GwG.

²⁶ Die Veröffentlichung erfolgt im zugangsbeschränkten Bereich der FIU-Homepage; die Zugangsdaten werden nur an Verpflichtete übermittelt, die sich unter www.goAML.de im Meldetool der FIU registriert haben.

²⁷ Krais, Geldwäsche-Compliance für Industrie und Handel, Praxishandbuch für Güterhändler, Beck, 2. Auflage 2022, § 7 Rn. 61.

haltpunkte im Sinne der FIU-Typologiepapiere in Bezug auf einen Sachverhalt vorliegen bzw. je ungewöhnlicher auf auffälliger ein Sachverhalt ist.

5.8.3 Geldwäsche-Verdachtsmeldung

Die Pflicht zur Verdachtsmeldung gilt unabhängig von der Höhe oder Art der betroffenen Transaktion bzw. Geschäftsbeziehung (§ 43 Abs. 1 GwG). Es gilt keine Privilegierung für Güterhändler. Vielmehr müssen auch Güterhändler ohne Rücksicht auf Wertgrenzen einer Transaktion oder Geschäftsbeziehung Verdachtsmeldung erstatten, wenn die Voraussetzungen vorliegen. Dies gilt selbst dann, wenn gar keine Finanztransaktion durchgeführt wurde oder wenn ein Geschäft oder eine Transaktion noch in der Anbahnung ist, weil z. B. schon während der Angebots- oder Verhandlungsphase Anhaltspunkte i. S. d. FIU-Typologien bestehen. Die Verdachtserfassung bezieht sich gleichermaßen auf geplante wie aktuelle oder bereits durchgeführte und selbst auf abgelehnte Geschäftsvorgänge oder Transaktionen, wenn sich der Verdacht erst nachträglich ergibt. Die Ablehnung einer als problematisch oder verdächtig erkannten Transaktion oder Geschäftsbeziehung entbindet daher nicht von der Meldepflicht.²⁸

Verdachtsmeldungen müssen elektronisch an die FIU erfolgen (§ 45 Abs. 1 GwG). Dafür ist eine vorherige Registrierung und Legitimierung über das Meldetool der FIU („goAML“)²⁹ erforderlich. Die FIU nimmt die Meldungen entgegen, führt diverse Analysen durch und gibt die aus ihrer Sicht relevanten Meldungen an die Ermittlungsbehörden weiter (§ 28 GwG). Sie bestätigt den Verpflichteten den Eingang der Meldung und gibt ihnen binnen angemessener Zeit Rückmeldung zur Relevanz der Meldung (§ 41 GwG). Eine Haftung für den Fall, dass sich die Verdachtsmeldung als nicht begründet erweist, besteht allenfalls bei einer vorsätzlich oder grob fahrlässig falschen Meldung (§ 48 GwG). Vor dem Verlust von Aufträgen oder Auswirkungen auf die Kundenbeziehung schützt die Gesetzesvorschrift allerdings nicht. Die Pflicht zur Registrierung bei der FIU gilt seit dem 1.1.2024 unabhängig davon, ob tatsächlich Verdachtsmeldungen anfallen, § 45 Abs. 1 Satz 2 GwG. § 59 Abs. 6 Satz 3 GwG schränkt dies allerdings ein auf Güterhändler, die mit Kunstgegenständen, Schmuck, Uhren, Edelmetallen, Edelsteinen, Kraftfahrzeugen, Schiffen oder Motorbooten oder Luftfahrzeugen handeln. Allen anderen Güterhändlern gewährt die Vorschrift Zeit bis zum 1.1.2027, sofern sie nicht vorher in mindestens einem Fall Verdachtsmeldung erstatten müssen.

Verdachtfälle i. S. d. § 43 Abs. 1 GwG müssen unverzüglich („ohne schuldhaftes Zögern“, im Finanzsektor sind 24–48 Stunden üblich) an die FIU gemeldet werden. Eine verspätete oder nicht ordnungsgemäße Verdachtsmeldung kann mit Bußgeld geahndet werden (§ 56 Satz 1 Nr. 69 und Satz 2 GwG). Vor diesem Hintergrund besteht faktisch die (indirekte) Organisationspflicht, zur Schaffung eines internen Verdachtserfassungswesens, also von Anweisungen, Prozessen und Instrumenten, die es den Mitarbeitern erlauben, einen möglichen Verdachtsfall zu erkennen und zur weiteren Prüfung (intern) rasch an die zuständige Stelle zu melden. Dies kann die Rechtsabteilung, die Compliance oder eine spezielle Geld-

²⁸ BMF, Auslegungshinweise zur Handhabung des Verdachtserfassungswesens (§ 11 GwG a. F.) vom 6.11.2014, WK 5023/10/10011, Seite 2.

²⁹ Siehe unter www.goaml.de, (aufgerufen am 15.4.2023).

wäsche-Stelle sein. Jahr für Jahr werden zuletzt rund 300.0000 Verdachtsmeldungen erstattet, der weit überwiegende Teil allerdings von Verpflichteten aus dem Finanzsektor.³⁰ Der sogenannte Nicht-Finanzsektor inklusive Güterhändler trägt nur zu einem geringen Teil des Meldeaufkommens bei. Fakt bleibt aber, dass nicht mehr als ein überschaubarer Anteil der Meldungen zu Ermittlungs- oder Strafverfahren führt, häufig nicht wegen Geldwäsche, sondern wegen anderer Delikte. Verurteilungen wegen Geldwäsche sind noch seltener. Die weit überwiegende Zahl der Verdachtsmeldungen wird genutzt, um bei der FIU einen sogenannten Informationspool aufzubauen, d. h. eine Datensammlung, die nicht unmittelbar der Strafverfolgung dient, sondern eher präventiven bzw. nachrichtendienstlichen Zwecken.

5.8.4 Verbot des „Tipping-Off“

Über den Umstand, dass eine Verdachtsmeldung erfolgt oder in Erwägung gezogen wird, dürfen Dritte nicht informiert werden (§ 47 Abs. 1 GwG, „*Tipping-Off-Verbot*“). Das betrifft in erster Linie den Geschäfts- oder Transaktionspartner, der Gegenstand der Verdachtsmeldung ist. Ob Unternehmen der eigenen Unternehmensgruppe als Dritte gelten oder nur Außenstehende, Fremde ist ungeklärt. In jedem Fall sollte der Kreis der Personen, die innerhalb eines Unternehmens von dem Verdacht bzw. einer Meldung Kenntnis haben, so gering wie nötig gehalten werden („*need to know*“). Im Übrigen sollte nur allgemein und ohne expliziten Bezug zu der Verdachtsmeldung kommuniziert werden, z. B. über das Erfordernis vor Aufnahme von Geschäften an bestimmter Stelle im Unternehmen eine detaillierte Geschäftspartner-Prüfung (§ 10 Abs. 3 Nr. 3 GwG) durchzuführen, ohne die Verdachtsmeldung zu erwähnen.

5.8.5 Wartefrist nach Verdachtsmeldung

Rechtsfolge der Verdachtsmeldung ist zunächst ein zeitlich begrenztes Transaktionsverbot bis zum Ablauf von drei vollen Werktagen ab Verdachtsmeldung (§ 46 Abs. 1 GwG, „*Wartefrist*“). Samstage gelten für Zwecke der Wartefrist nicht als Werktag. Vor Ablauf der kurzen Wartefrist darf eine Transaktion, die Gegenstand einer Verdachtsmeldung ist, nur durchgeführt werden, wenn die Staatsanwaltschaft ihre Zustimmung erteilt. Eine Ausnahme gilt nach dem Wortlaut des Gesetzes, wenn eine Transaktion nicht aufschiebbar ist (§ 46 Abs. 2 GwG). Ob vertragliche Verpflichtungen oder drohende Pönale wegen Verzugs in diesem Sinne dringlich sind, wird man eher bezweifeln müssen. Nach Ablauf der Wartefrist besteht keine Erlaubnis, die Transaktion durchzuführen. Es entfällt nur das zeitlich begrenzte Transaktionshindernis. Güterhändler sollten in diesem Fall das Risiko der eigenen Strafbarkeit nach § 261 Abs. 6 StGB (Leichtfertige Geldwäsche) bedenken, das sich schon daraus ergibt, dass der Güterhändler selbst den Vorgang als verdächtig gemeldet hat. Hier ist stets eine sorgfältige Abwägung aller Umstände des Einzelfalls erforderlich. Dabei sprechen zwei Punkte zugunsten des Güterhändlers: Zum einen führt eine Verdachts-

³⁰ Siehe dazu die Jahresberichte der FIU.

meldung nur in wenigen Fällen zu Ermittlungs- oder gar Strafverfahren. In der weit überwiegenden Zahl der Fälle werden die Meldungen mangels Erreichens der strafprozessualen Verdachtsschwelle nicht mal an die Strafverfolgungsbehörden weitergeleitet. Zum anderen sieht das GwG selbst implizit vor, dass eine Geschäftsbeziehung auch im Verdachtsfall fortbestehen bzw. Transaktionen durchgeführt werden können. Voraussetzung ist allerdings, dass zuvor allgemeine und ggf. verstärkte Sorgfaltspflichten durchgeführt werden, §§ 10 Abs. 9, 15 Abs. 9 GwG (siehe Abschn. 5.9.1).

5.9 Kundensorgfaltspflichten im Verdachtsfall

5.9.1 Allgemeine Sorgfaltspflichten

Wie zuvor erwähnt (siehe Abschn. 5.7) sind Güterhändler gemäß § 10 Abs. 6a GwG grundsätzlich nicht verpflichtet vor Aufnahme einer Geschäftsbeziehung kundenbezogene Sorgfaltspflichten durchzuführen. Im Verdachtsfall folgt allerdings aus § 10 Abs. 3 Nr. 3 GwG die Pflicht, allgemeine Sorgfaltspflichten durchzuführen, und zwar „*ungeachtet etwaiger nach diesem Gesetz oder anderen Gesetzen bestehenden Ausnahmeregelungen, Befreiungen oder Schwellenwerte.*“ Mit dem Verdachtsfall in § 10 Abs. 3 Nr. 3 GwG ist nichts anders gemeint als der meldepflichtige Verdacht des § 43 Abs. 1 GwG.³¹ Zwar gilt insoweit kein Gebot unverzüglich zu handeln, allerdings bleibt die Aufnahme oder Fortsetzung einer Geschäftsbeziehung oder die Durchführung einer Transaktion, die verdächtig ist, so lange untersagt, bis die Sorgfaltspflichten erfüllt sind. Wo dies nicht möglich ist, muss die Geschäftsbeziehung durch Kündigung oder andere Art beendet werden (§§ 10 Abs. 9, 15 Abs. 9 GwG). Der Umfang der allgemeinen Sorgfaltspflichten im Verdachtsfall unterscheidet sich nicht von den Sorgfaltspflichten, die z. B. im Fall einer Bargeldzahlung ab den einschlägigen Schwellenwerten des § 10 Abs. 6a GwG durchzuführen wäre. Insbesondere ist der Vertragspartner, die ggf. für ihn auftretende Person, deren Vertretungsbefugnis und der wirtschaftlich Berechtigte des Vertragspartners strikt nach den Vorgaben des GwG zu identifizieren bzw. festzustellen, § 10 Abs. 1 i. V. m §§ 11–13 GwG.

Besondere Sorgfalt sollte im Fall eines KYC wegen Verdacht der Geldwäsche auf die Feststellung des wirtschaftlich Berechtigten (§ 3 GwG) gelegt werden („*ultimate beneficial owner*“, *UBO*). Gerade in strafrechtlicher Hinsicht kommt es entscheidend darauf an, wer „*hinter*“ einer Transaktion oder einem Geschäft steht und ob Geld oder anders Vermögen aus einer legalen Quelle letztlich stammt. Zu beachten ist, dass der wirtschaftlich Berechtigte iSd. GwG stets eine (oder mehrere) natürliche Person ist, anders als z. B. im Steuerrecht. Zentrales Grundprinzip für die Festlegung wer, direkt oder indirekt wirtschaftlich Berechtigter ist, ist das der „*Kontrolle*.“ Kontrolle wir dabei verstanden als beherrschender Einfluss i. S. d. § 290 Abs. 2–4 HGB. Das setzt in der Regel eine Mehr-

³¹ Krais, Geldwäsche-Compliance für Industrie und Handel, Praxishandbuch für Güterhändler, Beck, 2. Auflage 2022, § 5 Rn. 8 ff.

heitsbeteiligung (> 50 %), die Mehrheit der Stimmrechte (> 50 %) oder sonst vergleichbaren Einfluss voraus. Nur bei *direkter* Beteiligung an einer Gesellschaft (also auf Ebene der unmittelbaren Gesellschafter bzw. Aktionäre) reicht bereits ein Anteil von mehr als 25 % am Stammkapital oder den Stimmrechten, um wirtschaftliche Berechtigung iSd. GwG zu begründen. Die Feststellung, wer wirtschaftlich Berechtigter ist, sollte durch die Einrichtung sogenannter Register der wirtschaftlich Berechtigten („*Transparenzregister*“) in der EU erleichtert werden (§§ 19 ff. GwG). Im Rahmen der geldwäscherechtlichen Sorgfaltspflichten wird von den Verpflichteten jedoch erwartet, dass sie zunächst beim Geschäftspartner Auskunft über den wirtschaftlich Berechtigten einholen und die Angaben im zweiten Schritt mit Hilfe des Transparenzregisters überprüfen, §§ 11 Abs. 5, 12 Abs. 3 GwG.

5.9.2 Verstärkte Sorgfaltspflichten

Wie schon erwähnt (siehe Abschn. 5.7), folgt aus § 15 Abs. 1 GwG, dass zusätzlich zu den allgemeinen Sorgfaltspflichten verstärkte Sorgfaltspflichten durchzuführen sind, sofern ein erhöhtes Risiko besteht. Die Pflicht zu allgemeinen Sorgfaltspflichten im Verdachtsfall (§ 10 Abs. 3 Nr. 3 GwG) begründet daher stets die Notwendigkeit zu prüfen, ob ein Anwendungsfall des § 15 GwG vorliegt. Beispielhaft für erhöhte Risiken nennt die Vorschrift das PEP-Risiko (§ 15 Abs. 3 Nr. 1 GwG) in Bezug auf den Geschäftspartner oder seinen wirtschaftlich Berechtigten sowie den Umstand, dass der Geschäftspartner enge Beziehungen zu einem Hochrisikostaat der EU-Liste (§ 15 Abs. 3 Nr. 2 GwG) aufweist. Die im Gesetz genannten erhöhten Risiken sind jedoch nur beispielhaft. Daher können z. B. auch enge Beziehungen zu (nur) von der FATF gelisteten Staaten verstärkte Sorgfaltspflichten auslösen. Dasselbe gilt für das Risiko, das einer Verdachtsmeldung innewohnt: Güterhändler sollten die Meldung eines verdächtigen Sachverhalts prinzipiell als erhöhtes Risiko im Einzelfall auffassen (§ 15 Abs. 1 GwG) und nach einer Verdachtsmeldung nicht nur allgemeine, sondern zusätzlich mindestens die verstärkten Sorgfaltspflichten des § 15 Abs. 4 GwG durchführen. Dazu gehört insbesondere die sorgfältige Klärung der Herkunft von Vermögenswerten, die im Rahmen einer Geschäftsbeziehung oder Transaktion eingesetzt werden („*source of funds*“), § 15 Abs. 4 Nr 2 GwG. Dies gilt umso mehr, wenn sie planen, eine Geschäftsbeziehung trotz des Verdachts fortzusetzen oder eine verdächtige Transaktion nach Ablauf der Wartefrist des § 46 GwG auszuführen. Vereinfachte Sorgfaltspflichten (§ 14 GwG) werden unter diesen Voraussetzungen nicht in Betracht kommen.

5.9.3 Mitwirkungspflichten und Tipping-Off

Ohne Mitwirkung des Geschäfts- bzw. Transaktionspartners ist die Durchführung allgemeiner und ggf. verstärkter Sorgfaltspflichten in der Regel nicht möglich. Der Gesetzgeber verpflichtet Geschäftspartner daher umfassend zur Mitwirkung an der Durchführung

der Kundensorgfaltspflichten (§ 11 Abs. 6 GwG). Sie müssen den Verpflichteten alle erforderlichen Angaben erteilen und Dokumente zur Verfügung stellen, um diese zu belegen. Verweigert der Geschäftspartner die Mitwirkung, liegt eine Verdachtsmeldung nahe; verweigert er die Offenlegung des wirtschaftlich Berechtigten, ist sie zwingend (§ 43 Abs. 1 Nr. 3 GwG). Dabei steht die Pflicht zur Durchführung von Sorgfaltspflichten im Verdachtsfall im Spannungsfeld zum „*Tipping-Off-Verbot*“ des § 47 GwG. Allein in der Anforderung von Informationen zur Erfüllung der gesetzlichen Sorgfaltspflichten kann man jedoch keinen Verstoß sehen. Allerdings muss im Kontakt mit dem Geschäftspartner jeder Hinweis vermieden werden, dass Anlass der Prüfung ein Geldwäsche-Verdacht ist. Dass sich der Betroffene dies mit etwas Rechtskenntnis denken kann, begründet keinen Verstoß des Verpflichteten gegen das GwG, sondern ist (unerwünschte) Rechtsfolge eines im Detail nicht durchdachten Gesetzes.

5.10 Verdachtsfälle und Risiko der Strafbarkeit

Ähnlich wie z. B. die Gewerbeordnung (GewO) oder andere wirtschaftsverwaltungsrechtliche Vorschriften stellt das GwG Anforderungen an Unternehmen und deren Vertreter, wie sie ihre Geschäfte zu führen haben. Verstöße gegen das GwG stellen Ordnungswidrigkeiten dar und führen ggf. zu Bußgeldern, deren Höhe danach variiert, ob es sich um einen Einzelfall handelt oder um systematische, wiederholte bzw. schwerwiegende Verstöße (§ 56 GwG). Ein Verstoß gegen Anforderungen des GwG begründet als solches keine strafrechtliche Verantwortung für Geldwäsche i. S. d. § 261 StGB.

Anders kann dies sein, wenn ein Verdachtsfall vorliegt. Unter diesen Umständen ist stets eine sorgfältige Bewertung strafrechtlicher Risiken erforderlich. Denn die Geldwäsche-Verdachtsmeldung befreit nicht automatisch von jeder strafrechtlichen Verantwortlichkeit, weder rückwirkend noch in die Zukunft gerichtet. Straftaten, die vor einer Verdachtsmeldung vollendet bzw. beendet wurden, werden durch die Meldung nicht ungeschehen oder automatisch frei von Strafe. Sofern ein strafbefreiender Rücktritt (§ 24 StGB) von einer noch nicht vollendeten Tat möglich ist oder wie z. B. bei Geldwäsche eine strafbefreiende Selbstanzeige („*tärtige Reue*“) in Frage kommt (§ 261 Abs. 8 StGB), tritt diese Rechtsfolge nur unter den spezifischen Voraussetzungen der jeweiligen Vorschrift ein. Immerhin hindert die pflichtgemäße Erstattung der Verdachtsmeldung die Inanspruchnahme der Strafbefreiung durch Selbstanzeige nach § 261 Abs. 8 StGB nicht (§ 43 Abs. 4 Satz 2 GwG). In dem eher theoretischen Fall, dass eine Verdachtsmeldung ausnahmslos alle Angaben einer Selbstanzeige nach § 261 Abs. 8 StGB enthält, gilt die Verdachtsmeldung zugleich als Selbstanzeige (§ 43 Abs. 4 Satz 1 GwG).

Mit Blick auf die Fortführung von Geschäftsbeziehungen mit Personen, die Gegenstand einer Verdachtsmeldung sind, bestehen Strafbarkeitsrisiken unter dem Gesichtspunkt der leichtfertigen Geldwäsche (§ 261 Abs. 6 StGB). Danach macht sich strafbar wer leichtfertig (in etwa „*grob fahrlässig*“) verkennt, dass Vermögensgegenstände aus einer Straftat stammen bzw. Geldwäsche betrieben wird. Die Rechtsprechung stellt formal hohe Anforderungen

an die Feststellung der Leichtfertigkeit. Sie setzt voraus, dass sich die Herkunft eines Vermögensgegenstands aus einer Straftat geradezu aufdrängt oder die Vortat (bei näherem Hinsehen) in Grundzügen hätte erkannt werden können. Der Täter muss insoweit gleichgültig oder grob unachtsam handeln.³² Nicht jeder Fehler im Umgang mit einem Geldwäsche-Verdachtsfall führt daher direkt zur Strafbarkeit wegen leichtfertiger Geldwäsche. Verurteilungen wegen leichtfertiger Geldwäsche machen allerdings einen Anteil von weit über 50 % der Geldwäsche-Urteile in Deutschland aus. Sie sind kein theoretischer Ausnahmefall, sondern der praktische Regelatbestand der Geldwäsche im Strafrecht. Typisch sind Sachverhalte bei denen eine Person Dritten ihr Bankkonto zur Verfügung stellt, damit diese Geldtransfers durchführen kann („*sog. Finanzagenten*“).³³ Unternehmen, die keine ausreichenden Maßnahmen treffen, um geldwäscherechtliche Anforderungen des GwG einzuhalten, insbesondere um Verdachtsfälle zu entdecken und zu melden oder die nach einer Meldung ohne Durchführung zumindest der allgemeinen Sorgfaltspflichten Transaktionen durchführen, setzen sich möglicherweise dem Vorwurf der Leichtfertigkeit aus, wenn es in diesem Zusammenhang zu Geldwäsche kommt. Die Gefahr besteht im internationalen geschäftlichen Umfeld ganz allgemein, wenn ein Unternehmen unbedarf Briefkastengesellschaften als Geschäftspartner akzeptiert, Geschäfte ohne erkennbaren Anlass über Steueroasen abwickelt, eingehende Zahlungen unbekannter akzeptiert oder sonst an auffälligen, unnötig komplexen oder sonst auffälligen Handlungen Dritter mitwirkt, nach dem Motto: „Dafür bin ich nicht verantwortlich“.³⁴ Wegen der Strafbarkeit bei leichtfertiger Geldwäsche ist der Sorgfaltmaßstab im Unternehmensalltag deutlich abgesenkt gegenüber z. B. Korruptionsstraftaten, wo fahrlässiges Handeln allenfalls im Rahmen der Aufsichtspflichten eine Rolle spielt. Ein Unternehmen, das seine geldwäscherechtlichen Pflichten erfüllt, hat zwar keine Garantie, das nicht im Einzelfall leichtfertig gehandelt wird. Die korrekte Bearbeitung von Risiken und Verdachtsfällen unterstellt wird es jedoch deutlich schwieriger werden, ein nicht sorgfältiges, leichtfertiges Verhalten anzunehmen und dieses nach den Vorschriften der §§ 9, 30, 130 OWiG der Geschäftsleitung bzw. dem Unternehmen anzulasten.

5.11 Ausblick: EU-Verordnung zur Verhinderung von Geldwäsche

Am 19.6.2024 wurde die EU-Geldwäsche-Verordnung veröffentlicht.³⁵ Die Verordnung stellt unmittelbar anwendbares europäisches Recht dar. Sie wird ab dem 1.7.2027 anwendbar sein. Sie ersetzt die bisherige 5. EU-Geldwäscherichtlinie (EU-GWRL) und mit ihr

³² BGH NStZ-RR 2015, 14 (14).

³³ Krais, Geldwäsche-Compliance für Industrie und Handel, Praxishandbuch für Güterhändler, Beck, 2. Auflage 2022, § 2 Rn. 31.

³⁴ Ausführlich zu möglichen Verdachtsfällen im internationalen, industriellen Umfeld bei Krais, Geldwäsche-Compliance für Industrie und Handel, Praxishandbuch für Güterhändler, Beck, 2. Auflage 2022, § 7 Rn 1 ff.

³⁵ Verordnung 2024/1624 des Europäischen Parlaments und des Rates vom 31.5.2024 zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung, ABL 2024, 111 ff.

das auf ihrer Basis erlassene Geldwäschegesetz (GwG). Die Verordnung begründet eine verbindliche, transaktionsbezogene Bargeldobergrenze von 10.000 Euro beim Kauf und Verkauf von Gütern und Dienstleistungen. Damit entfallen die Transaktionen, die bisher gemäß EU-GWRL die Verpflichteten-Eigenschaft von Güterhändlern begründen. Nach der Verordnung werden Güterhändler nur noch dann Verpflichtete sein, wenn sie Edelmetalle, Edelsteine oder hochwertige Güter handeln, unabhängig vom Schwellenwert oder ob dies gegen Barzahlungen von weniger als 10.000 Euro erfolgt. Die Definition der hochwertigen Güter in der Verordnung umfasst dabei ausschließlich Schmuck, Gold- und Silberwaren sowie Uhren ab einem Wert von 10.000 Euro, Fahrzeuge ab einem Wert von 250.000 Euro, sowie Luftfahrzeuge und Schiffe ab einem Wert von 7.500.000 Euro. Die EU-Verordnung verbietet es dem deutschen Gesetzgeber allerdings nicht, in Deutschland ansässige Güterhändler wie bisher über diesen Umfang hinaus den Vorschriften der EU-Verordnung zu unterwerfen (überschießende Tendenz, siehe Abschn. 5.4). Es bleibt daher abzuwarten, welche begleitenden Regelungen der deutsche Gesetzgeber bis zum Zeitpunkt der Anwendung der EU-Verordnung erlassen haben wird.

Literatur

Aufsätze

BÜLTE, JENS, BÜLTE: Zu den Gefahren der Geldwäschebekämpfung für Unternehmen, die Rechtsstaatlichkeit und die Effektivität der Strafverfolgung, NZWist 2017, 276, 276

Monografien und Kommentare

HERZOG, FELIX, Geldwäschegesetz, Kommentar, 4. Auflage 2022

KRAIS, JÜRGEN, Geldwäsche-Compliance für Industrie und Handel, Praxishandbuch für Güterhändler, Verlag C.H. Beck, 2. Auflage 2022



Jürgen Krais ist Rechtsanwalt in Augsburg und Syndikusrechtsanwalt bei einem DAX-Unternehmen in München. Dort ist er als Senior Legal Counsel Compliance vor allem im Bereich interner Compliance Untersuchungen tätig. Er beschäftigt sich darüber hinaus seit 2012 mit Fragen des Geldwäscherechts im Nichtfinanzsektor, Schwerpunkt Industrie und Handel. Er publiziert regelmäßig zum Thema Geldwäsche-Prävention. Am ZWW hält er seit 2016 Vorlesungen zum Thema Geldwäsche im Rahmen der Ausbildung zum Compliance Officer.



Tax Compliance

6

Christian Sering

Inhaltsverzeichnis

6.1	Definition der Tax Compliance.....	113
6.2	Aufgabenfelder der Tax Compliance.....	114
6.3	Gesetzliche Vorgaben, Rechtsprechung und Finanzverwaltung zur Tax Compliance.....	116
6.4	Interpretation des IKS durch den IDWPS 980.....	118
6.4.1	Compliance-Kultur.....	119
6.4.2	Compliance-Ziele.....	119
6.4.3	Compliance-Risikomanagement.....	121
6.4.4	Compliance-Programm.....	122
6.4.5	Compliance-Organisation.....	123
6.4.6	Compliance Kommunikation.....	123
6.4.7	Compliance-Überwachung.....	124

6.1 Definition der Tax Compliance

Unter Compliance wird die generelle Einhaltung von geltenden Gesetzen und freiwilligen Standards (Codices) verstanden.¹ Das darauf ausgerichtete Compliance-Management-System ist auf die Vermeidung von Rechtsverstößen und potenziellen Haftungsfällen gerichtet und soll die Unternehmensleitung in die Lage versetzen, bei Verdachtsmomenten bezüglich des Vorliegens von Regelverstößen rechtzeitig eingreifen zu können. Letztlich

¹ Streck Mack Schwedhelm Tax Compliance Kap. 1 Rz 1.1.

C. Sering (✉)
Scheidle und Partner, Augsburg, Deutschland

dient Compliance im Unternehmen damit der Verminderung der Haftungsrisiken für die Gesellschaft und deren Geschäftsleitung.²

Tax Compliance ist regelmäßig als Bestandteil einer übergeordneten Gesamt-Compliance zu verstehen und stellt insoweit einen Baustein im Rahmen der Compliance des Unternehmens dar. Tax Compliance bedeutet die Einhaltung der maßgeblichen *steuerlichen* Regelungen und Richtlinien der Finanzverwaltung sowie der freiwilligen Anforderungen des Unternehmens für die ordnungsgemäße Besteuerung; der Bereich Steuern umfasst dabei auch die Zölle.

Tax Compliance ist abzugrenzen von Tax Risk Management.³ Dieses befasst sich mit der Gesamtsteuerstrategie des Unternehmens. Im Kern geht es dabei um die Frage, wieviel legalen und legitimen Steuerstreit sich das Unternehmen als Steuersubjekt leisten kann und will. Bei der Abgabe von Steuererklärungen, die nach der Bearbeitung durch die Finanzverwaltung in Steuerbescheiden münden, ist stets auf die Balance zwischen legaler und zulässiger Steueroptimierung auf der einen Seite und steuerlichem Missbrauch bis hin zur Steuerverkürzung auf der anderen Seite zu achten. Das Ausloten und Ausnutzen legaler steuerlicher Gestaltungsmodelle und das Streiten um deren steuerliche Relevanz ist von der Rechtsschutzgarantie des Staates abgedeckt; das Risiko des Unternehmens als Steuersubjekt besteht insoweit lediglich im steuerlichen Unterliegen mit der Folge einer höheren Steuerlast und der Erwirtschaftung betriebsmindernden Aufwands durch erhöhte Berater- und Rechtsverfolgungskosten, es ist aber steuerstrafrechtlich neutral. Inhalt und Ausgestaltung des Tax Risk Managements hängen wesentlich vom Geschäftsfeld des Unternehmens und dessen steuerlichen Risikoappetit ab.

Beispiel

Die Verlagerung der Produktion in ein Niedrigsteuerland unter Beibehaltung des Betriebs- und Verwaltungssitzes in Deutschland bietet steuerlich erheblich mehr Risikopotenzial als die rein nationale Vertriebstätigkeit mit fest angestellten Mitarbeitern. ◀

6.2 Aufgabenfelder der Tax Compliance

Ein wesentliches Aufgabenfeld der Tax Compliance stellt die Sicherstellung und Überwachung der fristgerechten und vollständigen Abgabe der vom Unternehmen als Steuersubjekt geforderten Steuererklärungen (im Unternehmen namentlich: Umsatzsteuervoranmeldung, Umsatzsteuerjahreserklärung, Körperschafts- und Gewerbesteuererklärung) dar. Dabei hat Tax Compliance die lückenlose Bearbeitung des Steuerfalls – technisch gesehen: die rechtzeitige und vollständige Kommunikation der Bemessungsgrundlagen für die Besteuerung an die Finanzverwaltung – im Unternehmen sicherzustellen und eine Fehlerquellenanalyse zu implementieren.

² Schulze NJW 2914, 3484.

³ Aichberger/Schwartz DStR 2015, 1691.

Warum ist das so? Ein für die Compliance relevanter Konfliktfall tritt bei einer Steuerhinterziehung gemäß § 370 AO oder einer leichtfertigen Steuerverkürzung gemäß § 378 AO ein; letztere hat der Gesetzgeber als Bußgeldtatbestand bewertet.

Nach § 370 Absatz 1 AO macht sich strafbar, wer den Finanzbehörden über steuerlich erhebliche Tatsachen gegenüber unrichtige oder unvollständige Angaben macht oder die Finanzbehörden pflichtwidrig über steuerlich erhebliche Tatsachen in Unkenntnis lässt und dadurch Steuern verkürzt oder ungerechtfertigte Steuervorteile erlangt; erfolgt die Wahrnehmung der Angelegenheiten eines Steuerpflichtigen bei der Abgabe der Steuererklärung leichtfertig unrichtig oder unvollständig und werden dadurch Steuern verkürzt, liegt eine Steuerverkürzung nach § 378 Abs. 1 AO vor.

Kurzum: es besteht steuerstrafrechtliches Konfliktpotenzial, wenn der Steuerpflichtige die Bemessungsgrundlagen für die jeweiligen Steuern zu niedrig, lückenhaft oder außerhalb der dafür vorgesehenen Frist erklärt, die Finanzverwaltung weniger Steuern als gesetzlich geschuldet festsetzt und dadurch ein steuerlicher Verkürzungserfolg eintritt. Die §§ 370, 378 AO sind also als Erklärungsdelikte und im Grundsatz nicht als Nichtzahlungsdelikte ausgestaltet.⁴ Eine Steuerhinterziehung steht daher im Raum, wenn die Erklärung des Steuerpflichtigen – aus welchen Gründen auch immer – hinter den steuerrechtlich nötigen Angaben zurückbleibt und dadurch die zu zahlende Steuer verkürzt wird.

Einer der Gründe dieses Zurückbleibens des notwendigen Erklärungsinhalts kann nun etwas mit fehlender oder unvollständiger Kommunikation der Bemessungsgrundlagen für die Besteuerung (beim Unternehmen i. d. R. also die Umsätze, die Betriebskosten und der Gewinn) zu tun haben. Deshalb ist der lückenlose Transfer der steuerlich relevanten Daten im Unternehmen, aber auch eine funktionierende Datenschnittstelle zum Transfer an die Finanzverwaltung von überragender Bedeutung, um rechtzeitige und vollständige Steuererklärungen zu gewährleisten.

Ob die Verantwortlichen bei fehlerhaften steuerlichen Erklärungen tatsächlich eine Steuerhinterziehung gemäß § 370 AO oder eine Steuerverkürzung gemäß § 378 AO begangen haben, hängt maßgeblich von der Frage ab, welche Erkenntnisse der Erklärende subjektiv bei Abgabe der Steuererklärung hatte, mit anderen Worten also, ob er wusste oder es sich ihm aufdrängen musste, dass seine Erklärung bezüglich der konkret erklärten Steuer unvollständig oder falsch war. Diese Frage ist anhand verschiedener Kriterien zu prüfen; sie ändert indessen nichts daran, dass der Compliance-Fall im Unternehmen bereits dann eingetreten ist, wenn der bloße Verdacht einer Steuerhinterziehung besteht und die Finanzverwaltung deshalb ein behördliches Verfahren einleitet. Weil es naturgemäß schon dieses zu verhindern gilt, ist es Teil des Aufgabenfeldes von Tax Compliance, den Besteuerungsvorgang im Hinblick auf die vorgenannten Erklärungsrisiken zu überwachen.

Von untergeordneter Bedeutung ist, ob die steuerliche Überwachung im Hinblick auf die Richtigkeit und Vollständigkeit der steuerlichen Angaben von der Steuerabteilung des Unternehmens als Teil der Compliance mit übernommen wird, was in der Praxis in aller Regel der Fälle zutreffen dürfte oder ob hierfür ein eigener Stab Tax Compliance eingesetzt wird.

⁴MüKo Schmitz/Wulf § 370 AO Rn. 53.

Aufgabenfeld der Tax Compliance ist aber auch die Überwachung des formellen Steuerrechts, weil auch die (bloß) verspätete Steuererklärung den Tatbestand der §§ 370, 378 AO erfüllen kann, vgl. § 370 Absatz 4 AO. Bestenfalls kassiert das Unternehmen für das entsprechende Defizit nur Säumniszuschläge und Zinsen; ebenso denkbar ist jedoch, dass die Finanzverwaltung wegen der Verspätung ein Bußgeld- oder sogar ein Steuerstrafverfahren einzuleitet. Anders formuliert: organisatorische Mängel im Bereich der Steueradministration im Unternehmen können nicht nur zu einem finanziellen Nachteil werden, sondern behördliche Ermittlungen nach sich ziehen.

(Tax-)Compliance kann dabei keine 100 %ige Sicherheit zur Einhaltung aller Regeln schaffen, sondern sie kennzeichnet das ernsthafte Bemühen, nach vernünftiger Analyse aller Risikofaktoren individuell zugeschnittene Maßnahmen zu ergreifen, die auf die Minimierung von Fehlern zwecks Einhaltung aller Regeln ausgerichtet ist. Welches Restrisiko des (steuerlichen) Regelbruchs dann vom Unternehmen noch einkalkuliert und akzeptiert wird, entscheidet zuletzt der „Risikoappetit“ des Unternehmens als Steuersubjekt.

6.3 Gesetzliche Vorgaben, Rechtsprechung und Finanzverwaltung zur Tax Compliance

Die Verpflichtung des Unternehmens, ein geeignetes Compliance-Management-System zu installieren, ergibt sich bereits aus dem Gesetz. Die Betriebsinhaberhaftung nach § 130 OWiG sanktioniert das Organisationsverschulden des Betriebsinhabers, der Aufsichtsmaßnahmen im Unternehmen unterlässt und es deshalb zu Regelverstößen – so auch die Verfehlung der steuerlichen Pflichten – kommt. Zur Vermeidung eines Konflikts muss das Unternehmen deshalb einen Mindeststandard an Organisation bereithalten,⁵ was der Sache nach nichts anderes als ein Compliance-Management-System darstellt. Ebenso ist in § 30 OWiG (die sogenannte Verbandsgeldbuße) die gesetzliche Verpflichtung zur Compliance verortet. Darin wird das Unternehmen bußgeldrechtlich haftbar gemacht, wenn eine sogenannte Bezugstat, also die Verfehlung eines Mitarbeiters, durch die Pflichten verletzt werden, die dem Unternehmen obliegen, vorliegt. Auch hieraus wird eine Pflicht zu einer hinreichenden Unternehmensorganisation und für die steuerliche Praxis die Notwendigkeit der Implementierung eines Tax- Compliance-Management-Systems abgeleitet.⁶

Der Bundesgerichtshof hat bereits im Jahre 2017 im sog. Panzerhaubitzenfall⁷ entschieden, dass sich die Höhe der Ahndung einer Verbandsgeldbuße im Grundsatz an der Bewertung der von dem Organ begangenen Tat zu orientieren hat. Denn neben den allgemeinen Strafzumessungskriterien soll für den Verband eine zumindest sinngemäß Übertragung der Grundsätze von § 17 Abs. 3 OWiG gelten – das ist vor allem der individuelle Vorwurf, der den Täter trifft, bzw. allgemeine Zumessungsgrundsätze maßgeblich

⁵ KK-OWiG/Rogall § 130 Rn 29.

⁶ Breimann/Schwetzel DStR 2017, 2626.

⁷ BGH, Urteil vom 9.5.2017 – 1 StR 265/16.

sein. Entscheidend ist danach, inwieweit das Unternehmen seiner Pflicht, Rechtsverletzungen aus der Sphäre des Unternehmens zu unterbinden, genügt und ein effizientes Compliance-Management-System installiert hat, das auf die Vermeidung von Rechtsverstößen ausgelegt sein muss. Dabei wird bereits strafmildernd berücksichtigt, wenn das Unternehmen erst dann, wenn bereits Rechtsverstöße bekannt und Ermittlungen durch Behörden eingeleitet wurden, entsprechende Regelungen optimiert und seine betriebsinternen Abläufe so gestaltet hat, dass vergleichbare Normverletzungen zukünftig jedenfalls deutlich erschwert werden. Spätestens hiermit erkennt also der Bundesgerichtshof den Einfluss eines Compliance-Management-Systems auf die Höhe einer möglichen Verbundsgeldbuße ausdrücklich an.

Die Finanzverwaltung hat ihre Auffassung zur Tax Compliance in dem Anwendungserlass zu § 153 AO vom 23. Mai 2016 niedergelegt. Sie stellt für die Beantwortung der Ermessensfrage, wie mit einem steuerlichen Konfliktfall umzugehen ist, auf die Binnenorganisation des Unternehmens ab: So heißt es in Ziffer 2. 6 des Anwendungserlasses:

„Hat der Steuerpflichtige ein innerbetriebliches Kontrollsysteem (IKS) eingerichtet, das der Erfüllung der steuerlichen Verpflichtungen dient, kann dies gegebenenfalls ein Indiz darstellen, das gegen das Vorliegen eines Vorsatzes oder der Leichtfertigkeit sprechen kann, jedoch befreit dies nicht von der Prüfung des Einzelfalles“.

Zur dogmatischen Einordnung an dieser Stelle nur so viel: § 153 AO befasst sich mit der nachträglichen Berichtigung steuerlicher Erklärungen. Sie ist im Grundsatz nur für denjenigen Steuerpflichtigen anwendbar, der die Unrichtigkeit oder Unvollständigkeit der Erklärung erst nach Abgabe der Steuererklärung erkennt. Sodann muss er unverzüglich tätig werden und die Angaben korrigieren; kommt er dieser Pflicht nicht nach, so kann er sich dann dem Vorwurf der Steuerhinterziehung durch Unterlassen aussetzen.⁸ Demgegenüber hat derjenige, der die steuerliche Erklärung bereits bei deren Abgabe vorsätzlich oder leichtfertig unrichtig oder unvollständig erledigte, nur die Möglichkeit, unter den (deutlich schärferen) Voraussetzungen der strafbefreienden Selbstanzeige nach § 371 AO zur steuerlichen Legalität zurück zu gelangen. Der Anwendungserlass vom 23.05.2016 setzt sich demnach mit der Frage auseinander, unter welchen Voraussetzungen unterstellt werden kann, dass der Steuerpflichtige bei der Abgabe einer falschen oder unvollständigen Steuererklärung nicht vorsätzlich oder leichtfertig gehandelt hat. Dabei stellt die Finanzverwaltung maßgeblich auf die Existenz eines internen Kontrollsystems (IKS) ab, wobei es dazu keine inhaltlichen Vorgaben präsentiert. Dessen Zweck liegt aber auf der Hand: genügt das steuerpflichtige Unternehmen den – wie auch immer gearteten – Kriterien der Finanzverwaltung an ein IKS, hat es alles Erforderliche getan, um das Risiko steuerlicher Regelverletzungen auf ein Minimum zu beschränken. Es kann dann im steuerlichen Konfliktfall argumentieren, jedenfalls nicht schuldhaft gehandelt zu haben, d. h. allenfalls einfach fahrlässig eine falsche Steuererklärung abgegeben zu haben, womit der Weg einer Haftung nach §§ 370, 378 AO verschlossen bleibt. Denn nach dem

⁸ Wabnitz/Janovsky/Schmitt 21. Kapitel Rn. 56.

Erlass kann das IKS nach Prüfung des jeweiligen Einzelfalls ein Indiz zur Verneinung von Vorsatz oder Leichtfertigkeit sein. Damit ergibt sich zumindest faktisch aus dem Anwendungserlass zu § 153 AO die Pflicht zur Tax-Compliance.⁹

6.4 Interpretation des IKS durch den IDWPS 980

Das Institut der Wirtschaftsprüfer (IDW) hat in Form des IDW PS 980 einen Prüfungsstandard erstellt, welche Voraussetzungen für ein wirksames Compliance-Management-System geschaffen und unterhalten werden müssen. Nach dem IDW PS 980 ist ein Compliance-Management-System angemessen, wenn es geeignet ist, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern. Zu einem angemessenen CMS gehört es danach auch, dass bereits eingetretene Regelverstöße zeitnah an die zuständige Stelle im Unternehmen gerichtet werden, damit die notwendigen Konsequenzen für eine Verbesserung des CMS getroffen werden können.

Der IDW PS 980 entfaltet – wie auch der Anwendungserlass der Finanzverwaltung – keine Gesetzeskraft, bietet dafür aber den enormen Vorteil einer starken Orientierung an der Praxis. Denn etwa 80 % der in Deutschland zugelassenen Wirtschaftsprüfer sind im IDW vereinigt. Prüft einer dieser so organisierten Wirtschaftsprüfer das CMS und testiert es im Anschluss daran, so bietet das Testat eine gute Grundlage für eine Bewertung als im Sinne der Finanzverwaltung ausreichendes Compliance-Management-System. Naturgemäß ist auch nach dem Anwendungserlass immer der Einzelfall zu prüfen. Es ist aber aus Sicht der Finanzverwaltung ein gutes Zeichen im Sinne einer vertrauensbildenden Maßnahme, wenn zur Gewährleistung der regelkonformen Besteuerung differenzierte Sicherungsmaßnahmen im Unternehmen eingerichtet werden.

Nach dem IDW PS 980 (neueste Fassung derzeit von 09/2022, sh. Heft 12 IDW Life) hängt die konkrete Ausgestaltung des CMS maßgeblich von der Größe des Unternehmens, seiner sowie Art und Umfang der Geschäftstätigkeiten ab.

Der IDW PS 980 hat folgende sieben Grundelemente herausgebildet:

1. Kultur
2. Ziele
3. Risiken
4. Programm
5. Organisation
6. Kommunikation
7. Überwachung

Hierzu sollen in Kürze die Besonderheiten im Hinblick auf Tax Compliance herausgestellt werden:

⁹Beyer, NZWiSt 2016, 234.

6.4.1 Compliance-Kultur

Die Implementierung und das Leben einer Compliance Kultur für den Bereich Steuern ist doppelt schwierig, weil das Thema hoch ambivalent besetzt ist. Kleinere Steuerhinterziehungen werden immer noch als Kavaliersdelikt angesehen und es gibt viele – zum Teil durchaus nachvollziehbare – Gründe für Steuerunehrlichkeit. Das deutsche und auch zunehmend europäische Steuersystem ist sehr unübersichtlich und komplex und wird vielfach als ungerecht empfunden.¹⁰ Der Vorbildcharakter des Managements ist deshalb extrem wichtig. Daneben ist aber nicht nur der „tone from the top“, sondern auch der „tone from the middle“ von großer Bedeutung: Deutliche Eindruckskraft hinterlässt, wenn auch der Einkaufsleiter bei den dienstlichen und privaten Anlässen der Bewirtung strikt trennt und das auch konsequent kommuniziert. Denn nur so wird ein flächendeckendes steuerliches Werteverständnis erzeugt.

6.4.2 Compliance-Ziele

Nächstes Target des IDW PS 980 sind die Compliance-Ziele. Die Organe des Unternehmens legen dabei auf Grundlage der für das Unternehmen bedeutsamen Regeln diejenigen Ziele fest, die mit dem Compliance Management-System erreicht werden sollen.¹¹ Die Ziele stellen die Grundlage für die Beurteilung von Compliance-Risiken dar, sodass auch die speziellen Tax-Compliance Ziele in die allgemeinen Compliance-Ziele zu integrieren sind. Die Ziele müssen messbar formuliert sein, damit sie Wirkung erzeugen. Messbar ist die Verpflichtung zur Steuerehrlichkeit z. B. dann, wenn in Konkretisierung des Bekenntnisses zur Steuerkonformität das interne Kontrollsysteem so beschrieben wird, dass es eine effiziente Organisation vorhält, die für rechtzeitige und vollständige Steuererklärungen sorgt. Das Ziel ist also in aller erster Linie der Aufbau eines auf das Unternehmen und dessen Geschäftsfeld und Risiken konkret zugeschnittenes Compliance-Management-System im Sinne eines internen Kontrollsystems. Dabei unterscheidet man zwischen einer Aufbau- und einer Ablauforganisation, die an den spezifischen Bedarf des Unternehmens anzupassen sind.

In der Aufbauorganisation wird zunächst festgelegt, mit welchen Rahmenbedingungen (Human Resources, EDV, Sachausstattung) die für die Unternehmensbesteuerung notwendigen Aufgaben erledigt werden. Für den Bereich der Steuern besteht die die Aufgabe darin, eine möglichst lückenlose Organisation des steuerlichen Bearbeitungsvorgangs zu ermöglichen.

Exemplarisch könnte eine derartige Aufbaumatrix wie folgt aussehen:

Die Unternehmungsleitungsebene verantwortet die Steuerstrategie, den Verhaltenskodex und die Bereitstellung personeller und sachlicher Ressourcen.

¹⁰Vgl. zum Ganzen: Bussmann, CCZ 2016, 50 ff.

¹¹IDW Praxishinweis 1/2016 (IDW Life 2017, 837 ff.); Handel DStR 2017, 1945.

Die Steuerabteilung verantwortet die Steuerrichtlinie, die fristgerechte Erstellung der Steuererklärungen, die Überwachung der externen steuerlichen Helfer und das steuerliche Wissensmanagement inklusiv Inhouse-Schulungen. In kleineren Unternehmen, wo es eine Steuerabteilung nicht gibt, liegt im Zweifel die Verantwortlichkeit bei der Leitungsebene, idealerweise bei einem Ressortverantwortlichen.

Die Fachabteilung (auch Rechnungswesen, Einkauf, etc.) verantwortet die Pflege der Stammdaten und die Meldung aller außerordentlichen Steuerfälle. Das bedeutet: auch bei Unklarheiten über die Steuererheblichkeit des Vorgangs, Richtigkeit einer Eingangsrechnung oder der Berechnung des Vorsteuerabzugs wird eine Eskalationspflicht mit klaren Vorgaben geregelt. In der Regel sollten Berichtslinien nicht nur mit Funktionsbeschreibungen, sondern mit konkreten Namen versehen werden.

Wenn die steuerliche Aufbauorganisation steht, dann wird schließlich eine Ablaufmatrix, also gewissermaßen der operative Teil des internen Kontrollsystems, benötigt. Sie regelt das Prozessmanagement, in dem die systematischen Abläufe des Compliance-Programms stattfinden. Hierzu einige Beispiele, wie eine derartige Ablauforganisationsstruktur nach dem IDW PS 980 aussehen könnte: Die Ablaufmatrix kann und sollte z. B. enthalten:

- Die Installation einer klaren Berichtsstruktur und den entsprechenden Berichtslinien
- Die Installation regelmäßiger Zielvereinbarungs- und Statusgespräche mit Mitarbeitern,
- Die Einrichtung von Meldepflichten und Eskalationsverfahren für besonders risiko-reiche steuerliche Konstellationen
- Die systematische Installation eines regelmäßigen Kontakts unter Mitarbeitenden auch in den verschiedenen Hierarchiebenen in Jour-Fixes; diese eröffnen im Übrigen den Blick für bottlenecks und Probleme – vielfach hilft es, „einfach“ einmal zu sprechen.
- Die Installation von Vertretungs- und Urlaubsregelungen, damit kein Vakuum bei der Bearbeitung entsteht.
- Das Prozessmanagement sollte auch eindeutige Regelungen für Unterschriftenkompetenzen, die Absendung von Steuererklärungen über Elster und für die Korrespondenz für Behörden und externen Beratern beinhalten.
- In der Ablaufmatrix sollten auch Datenzugriffsrechte definiert und festgelegt werden.

Die Installation und Integration von Schulungsmaßnahmen und Wissensmanagement in die Ablaufmatrix hat schließlich herausragende Wichtigkeit wegen der großen Komplexität und Volatilität des Steuerrechts und seiner Anwendung; hier kann sich auch die Installation eines regelmäßigen Jour-Fixes mit einem steuerlichen Berater anbieten.

Die Ablaufmatrix sollte zuletzt die Überwachung von Zahlungs- und Rechtsbehelfsfristen systematisieren – so kann man uU auch einmal Säumniszuschlägen, die schnell verwirkt sind, entgegentreten; Versäumte Rechtsmittelfristen sind im Übrigen nur schwer heilbar.

Für den „Ernstfall“ sorgen immer mehr Unternehmen vor, indem sie ein Betriebspflichtigungsmanagement/Fahndungsprüfungsmanagement installieren, für den Fall, dass es zu einer unerwarteten Betriebs- oder gar strafrechtlichen Fahndungsprüfung kommt.

Schritt 2 bei der Strukturierung der Ablauforganisation ist dann die Ermittlung des Fahrplans zur Umsetzung, indem eine Matrix vorgegeben wird, innerhalb welchen Zeitraums und mit welcher Priorität die einzelnen Schritte der Ablauforganisation umgesetzt werden.

Am Ende der Erstellung der Aufbau- und Ablauforganisation steht im Prinzip ein End-to-End-Prozess, der den kompletten Geschäftsablauf beinhaltet, in steuerlicher Hinsicht also bei der Prüfung des Vertragspartners (KYC) beginnt, sich über die steuerlich regelkonforme Abwicklung des Geschäftsvorfalls fortsetzt und bei der Kommunikation mit der Finanzverwaltung inclusive der Installation eines Rechtsbehelfsmanagements und Behördenkommunikation endet.

6.4.3 Compliance-Risikomanagement

Nächstes Topic auf der Agenda des IDW PS 980 ist das Risikomanagement.

Zentral für das Compliance-Management-System ist die Implementierung eines Verfahrens zur systematischen Früherkennung von Risiken. Hierzu sind Risikoklassen zu bilden und deren Eintrittswahrscheinlichkeit anhand des konkreten Unternehmensprofils und Geschäftsmodells zu identifizieren.¹² Für den Bereich der Tax Compliance bedeutet dies speziell, dass die steuerlichen Risiken bezogen auf die jeweilige Steuerart und die damit verbundenen Prozesse für die typischen Geschäftsvorfälle des Unternehmens analysiert werden müssen.

Die Einteilung der steuerlichen Risiken empfiehlt sich dabei nach einem zeitlichem/inhaltlichem Cluster.

Nach dem zeitlichen Cluster ist zum Beispiel zu prüfen, ob es durch frühere Geschäftsführer „Sünden“ der Vergangenheit gibt, die es nach § 153 AO zu berücksichtigen gilt. Inhaltlich spielen für die Risikoanalyse immer wieder die typischen operativen Risiken durch Fehler/Unzulänglichkeiten in der jeweiligen Fachabteilung eine Rolle, also z. B. Fehler bei der Rechnungseingangskontrolle („Klassiker“: die falsche Klassifikation des Umsatzsteuersatzes in der FiBu, fehlerhafte Rechnungsangaben). Relevant sein können auch Irrtümer über die Steuerrelevanz (gerade bei Geschäften zwischen Gesellschaft und Gesellschaftern, Stichwort und Themen: Fremdvergleich, Sonderbetriebsvermögen durch Ausgliederung von Produktionsmitteln etc., verdeckte Gewinnausschüttung); bisweilen sind es aber auch die simplen Erklärungsrisiken durch schleppende oder unzureichende Bearbeitung der Geschäftsvorfälle. Es empfiehlt sich, Checklisten für die Klassifizierung von Risiken zu erstellen.

Zur Methodik der Risikoermittlung an dieser Stelle nur so viel: zunächst ist das Brutto-Risiko zu ermitteln. Im Zweifel gilt hier ein Maximalansatz. Für die Ermittlung des Brutto-Risikos zentral ist die komplette Analyse des Geschäftsvorfalls, also vom Anlegen der Stammdaten, dem Eingang der Fremd-Rechnung bis hin zum Erhalt des Steuerbescheids;

¹² IDW Praxishinweis 1/2016 (IDW Life 2017, 837 ff.).

am Reißbrett wird durchgemustert, welche Fehler auftreten könnten. Der Ermittlung des Bruttonrisikos dienen dazu geeignete Software-Tools des Datenverarbeitungsprogramms. Diese operieren zunehmend auch unter Einsatz von KI und zeigen mögliche Fehlerschnittstellen im Sinne potenzieller Risiken auf und benennen die notwendigen Verarbeitungsschritte zur Fehlereliminierung.

Die Qualität der Maßnahmen zur Risikobegrenzung hat entscheidende Auswirkung auf den Weg vom Bruttonrisiko zum verringerten Netto-Risiko. Nach Implementierung der Risikomanagementmaßnahmen wird das verbleibende Netto-Risiko ermittelt. Je nachdem welche Maßnahmen das Unternehmen bei seinem Prozessmanagement ergriffen hat, hat es einen Teil der Risiken herausgefiltert, wobei es noch einmal zu sagen gilt, dass es keine geeignete Strategie geben wird, das Risiko auf null zu bringen, denn das würde im Zweifel dazu führen, dass das Unternehmen aus Sorge vor Risiken gänzlich paralysiert wird; es geht bei einem effizienten Risikomanagement allein darum, die Risiken auf ein vertretbares Maß zu beschränken.

Nächster Schritt ist sodann die Einrichtung einer Risikomatrix, damit Risiken gewichtet und deren Minimierung priorisiert werden können. Eckpfeiler hierfür sind der Grad der Eintrittswahrscheinlichkeit des Risikos mit den Kriterien: selten, unwahrscheinlich, möglich, wahrscheinlich und hoch und der Gewichtung des Risikos in sehr niedrig, niedrig, mittel, hoch und sehr hoch. Hierzu wird idealerweise ein Ampelsystem erstellt: „Rot“ bedeutet: es besteht inakzeptables Risiko, es sind Maßnahmen zu ergreifen. Steht die Ampel auf „gelb“, bedeutet das: es besteht Risiko oberhalb des Nettonrisikos, das Unternehmen braucht ein Monitorship und eventuell sind noch zusätzliche Maßnahmen erforderlich. „Grün“ im Sinne freier Fahrt heißt, dass ein vertretbares Risiko besteht und keine weiteren Maßnahmen erforderlich sind. Auch dieses Ampel-System kann in eine Matrix integriert werden.

6.4.4 Compliance-Programm

Topic 4 des IDW PS 980 beinhaltet das Programm des Compliance-Management-Systems.

Hier werden im Wesentlichen – in größeren Unternehmen häufig in einem (Tax-)Manual – alle Maßnahmen beschrieben, die den erkannten Compliance-Risiken entgegenwirken sollen. Dort wird aber auch beschrieben, welche Maßnahmen ergriffen werden und wie Regelverstöße im Unternehmen sanktioniert werden.¹³ Man unterscheidet präventive Maßnahmen wie z. B. die Erstellung von Richtlinien, Checklisten, Schulungen, Dokumentationsanweisungen und prozessintegrierte Kontrollen wie das Vier-Augen-Prinzip und detektive Maßnahmen wie manuell-analoge, aber auch automatisierte Qualitätskontrollen. Zunehmend wird auch dieser Bereich von intelligenter EDV und KI beherrscht, z. B. das COBIT 2019 (Control Objectives for Information and Related Technology) oder sonstige IT-Kontrollsysteme als sogenannte Corporate Governance Frameworks. Im Kern basieren diese digitalisierten Frameworks darauf, dem Anwender bei einer besseren Verwaltung

¹³ IDW Praxishinweis 1/2016 (IDW Life 2017, 837 f.).

von Informationen und Technologien zu verhelfen. Letztlich ist das aber das Ergebnis künstlicher Intelligenz und verantwortlich bleibt immer der Mensch.

6.4.5 Compliance-Organisation

Zur Organisation des internen Kontrollsystems als nächstem Target nach dem IDW PS 980 ist in erster Linie eine ordnungsgemäße Dokumentation erforderlich: für den Bereich der Besteuerung ergibt sich die Pflicht zur Dokumentation ohnehin aus den GOBD (Grundsätze zur ordnungsgemäßen Führung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form),¹⁴ die eine gute Hilfestellung für die Anforderung stellen, eine lückenlose Dokumentation des „Lebenszyklus“ des Geschäftsvorfalls von seiner Entstehung, Erfassung, Bearbeitung hin bis zur Aufbewahrung und Archivierung von Belegen zu gewährleisten. Aber auch ansonsten gilt, dass sämtliche Compliance-Management-Maßnahmen schriftlich und für alle Mitarbeiter verfügbar sein sollen und die Zuweisung von Verantwortlichkeiten und Themengebieten bereithalten. Eine fehlende Dokumentation entwertet ein internes Kontrollsysteem nicht unerheblich, denn die Finanzverwaltung wird im Ernstfall dem Unternehmen nicht glauben, welche effiziente Struktur man zur Vermeidung von Regelverstößen aufgesetzt hat – natürlich kann man die Dokumentation auch mündlich bewerkstelligen, es fehlt dann aber eben an der Beweissicherheit. Zuletzt sollte auch dokumentiert werden, wie mit Regelverstößen im Unternehmen umgegangen wird, insbesondere bei Steuerverfehlungen, denn damit wird das Vertrauen der Finanzverwaltung in das IKS gestärkt.

6.4.6 Compliance Kommunikation

Die Compliance-Kommunikation umfasst die Mitteilung der Compliance-Regelungen und des Compliance-Programms an die betroffenen Mitarbeiter, aber auch an Dritte.¹⁵ Für den Bereich der Tax Compliance gilt, dass es naturgemäß nicht ausreicht, dass die steuerlichen Anforderungen innerhalb der Steuerabteilung bekannt sind, sondern man sollte einen interdisziplinären Ansatz wählen, damit die steuerliche Regelkonformität in allen Abteilungen des Unternehmens bekannt wird. Der Inhalt der Kommunikation wird für den Bereich Steuern häufig in einem Tax Manual, wenigstens aber in schriftlichen Arbeitsanweisungen niedergelegt. Dort werden auch die konkreten Verantwortlichkeiten festgelegt. Ohne ausreichende Informationen wissen die entsprechenden Mitarbeiter sonst nicht, was sie tun sollen und ohne dieses Wissen ist auch eine wirksame Delegation durch die Geschäftsleitung nicht möglich. Zur Form der Kommunikation gilt zu sagen: alles, was nicht nur einmalig, sondern regelmäßig wiederkehrend ist, schärft die Sinne und die

¹⁴Vgl. hierzu auch § 146 AO.

¹⁵IDW Praxishinweis 1/2016 (IDW Life 2017, 837 ff.).

Sensibilität, weshalb regelmäßige Rundschreiben und ebenso regelmäßige Jour-Fixes förderlich sind. Letztlich prägt gute Kommunikation auch eine positive Unternehmenskultur, weil man den Mitarbeitern keine Fesseln anlegt, sondern Navigationssysteme an die Hand gibt.

6.4.7 Compliance-Überwachung

Die Angemessenheit und Wirksamkeit des Compliance-Management-Systems muss in geeigneter Weise durch die Geschäftsleitung überwacht werden. Hierfür ist wiederum die Dokumentation zentrale Voraussetzung. Werden im Rahmen der Überwachung nach erfolgter Ursachenanalyse Schwachstellen im Compliance-Management-System oder sogar Regelverstöße festgestellt, muss eine klare Berichtslinie an die Compliance-Abteilung oder die Geschäftsleitung installiert und eingehalten werden.¹⁶ Diese Stabstellen sind im Unternehmen letztlich auch dafür verantwortlich, das Compliance-Management-System durchzusetzen, etwaige Mängel zu beseitigen, um es zu verbessern. Für die Überwachung bietet sich folgende Matrix-Struktur an:

- die Festlegung der Zuständigkeit für die Compliance-Überwachung
- die Entwicklung eines Überwachungsplans
- die Bereitstellung von ausreichend erfahrenen Ressourcen für die Durchführung der Überwachungsmaßnahmen
- die Bestimmung der Berichtslinie für die Ergebnisse der Überwachungsmaßnahmen und Auswertung der Berichte durch die zuständige Stelle. Verfügt das Unternehmen über einen Aufsichtsrat, so ist auch er zur Erfüllung seiner eigenen Überwachungsfunktion (vgl. § 107 Abs. 3 AktG) zu informieren.



Dr. Christian Sering, RA, FA Str, seit 1999 als RA zugelassen, seit 2002 als FA StR, überwiegend in den Bereichen Wirtschafts- und Steuerstrafrecht und Compliance in der Kanzlei Scheidle & Partner Rechtsanwälte mbB, Augsburg, tätig; seit 2020 Compliance Officer und Lehrbeauftragter für Tax Compliance beim ZWW; regelmäßige Veröffentlichungen.

¹⁶ IDW Praxishinweis 1/2016 (IDW Life 207, 837 ff.).



Bank- und Kapitalmarkt-Compliance

7

Axel-Dirk Blumenberg

Inhaltsverzeichnis

7.1	Grundlagen des Bank- und Kapitalmarktrechts	126
7.1.1	Einführung	126
7.1.2	Funktionsweise des Kapitalmarkts	127
7.1.3	Aufsichtsbehörde	128
7.2	Prävention und Detektion von Marktmissbrauch	129
7.2.1	Insiderhandel	129
7.2.2	Organisatorische Maßnahmen	130
7.2.3	Marktmanipulation	132
7.2.3.1	Das Verbot der Marktmanipulation	132
7.2.3.2	Safe Harbours	135
7.2.4	Anzeigepflichten	135
7.2.5	Reg-Tech	135
7.3	Ad-hoc-Publizität	136
7.4	Director's Dealings	137
7.5	Organisationspflichten nach § 80 Abs. 1 WpHG, Art. 22 DV und 26 Abs. 7 DV und 26 Abs. 7 DV	138
7.5.1	Stellung der Compliance	139
7.5.1.1	Unabhängigkeit	140
7.5.1.2	Dauerhaftigkeit der Compliance	140
7.5.2	Aufgaben der Compliance	141
7.5.2.1	Beratungs- und Unterstützungsfunction	141
7.5.2.2	Überwachung	141
7.5.2.3	Berichtspflichten	141
7.6	Organisationspflichten nach § 25a KWG	142
	Literatur	143

A.-D. Blumenberg (✉)
Rechtsanwalt Axel-Dirk Blumenberg, Passau, Deutschland

7.1 Grundlagen des Bank- und Kapitalmarktrechts

7.1.1 Einführung

Im Vergleich zur Erstausgabe dieses Buches haben sich nicht unerhebliche Änderungen sowohl auf rechtlicher Ebene als auch im Bereich der Finanzmärkte ergeben. So waren zum damaligen Zeitpunkt etwa Bitcoin und Kryptowährungen kaum von Bedeutung. Prominente Strafverfahren, wie etwa gegen den damaligen Vorstand der Porsche AG wegen des Vorwurfs der Marktmanipulation,¹ haben die Thematik dieses Beitrags in ein neues Licht gerückt und nicht zuletzt sind die Europäisierung und Internationalisierung dieses Rechtsgebiets noch weiter vorangeschritten.

Aus dem Blickwinkel der Compliance ergibt sich ein komplexes Normgefüge aus europäischen Richtlinien, (Delegierten) EU-Verordnungen, nationalen Gesetzen, Rundschreiben und Empfehlungen der Aufsichtsbehörden, etc., die alle in die Unternehmenspraxis integriert werden müssen. Dadurch entstehen lange und unübersichtliche Verweisungsketten, die es insbesondere für juristische Laien sehr schwierig machen können, sich im „Paragrafen-Dschungel“ zu orientieren und zu verstehen, was der jeweilige Normgeber eigentlich vom Rechtsanwender möchte.

Erschwerend hinzu kommen zahlreiche Technizismen (z. B. „OTC-Geschäft“ oder „Schatzanweisungen, Einlagenzertifikate, Commercial Papers und sonstige Instrumente mit im Wesentlichen den gleichen Merkmalen“), die eine vertiefte Sachkenntnis der operativen Geschäftsabläufe nötig machen, um so durch eine Zusammenschau der rechtlichen und operativen Aspekte die tatsächlichen Compliance-Risiken des Unternehmens realistisch einschätzen und auf diese Weise vermeiden bzw. minimieren zu können.

In der Praxis können sich zudem unerwartete Sanktionsrisiken für Unternehmen aufgrund ihrer internationalen Tätigkeit ergeben, etwa wenn Mitarbeiter aus Bequemlichkeit oder falsch verstandener Kundennähe auf unzulässige Kommunikationsmittel wie WhatsApp zurückgreifen. Eine solche Kommunikation sowohl mit Kunden als auch innerhalb des Unternehmens hat zu erheblichen Sanktionen gegen in den USA tätige Finanzdienstleister (auch aus Deutschland) geführt, da sich diese Kommunikationsformen nicht in angemessener Weise nachverfolgen und rechtskonform dokumentieren lassen.²

Das Bank- und Kapitalmarktrecht zählt – neben der Geldwäschebekämpfung – zu den Bereichen, in denen der Staat Unternehmen gezielt in seine Strategie zur Prävention und Detektion von Gesetzesverstößen einbezieht. Diese staatliche Inpflichtnahme der Privatwirtschaft zur Einhaltung der gesetzlichen Vorgaben im Bank- und Kapitalmarktrecht führt zu einem erheblichen Organisations- und Verwaltungsaufwand. Ein Banker hat dies einmal

¹Vgl. dazu Momsen/Laudien, ZIS 2016, 646 – 653.

²Siehe hierzu etwa den Beitrag der FAZ – „Banken drohen hohe Strafen wegen Whatsapp-Nutzung“, <https://www.faz.net/aktuell/finanzen/whatsapp-nutzung-banken-in-den-usa-drohen-hohe-strafen-18261449.html> (aufgerufen am 7.2.2024).

am Rande einer Veranstaltung etwas überspitzt so auf den Punkt gebracht: „*Der Compliance-Aufwand in unserer Branche ist mittlerweile so hoch, dass an einem normalen Tag auf eine Stunde operatives Geschäft fast sieben Stunden Compliance entfallen.*“

Dies macht die Compliance-Arbeit im Bank- und Kapitalmarktrecht spannend, aber auch sehr anspruchsvoll. Die Compliance-Abteilung steht nämlich vor der Aufgabe, die komplexen rechtlichen und fachlichen Anforderungen in verständliche Handlungsanweisungen zu übersetzen, um ein rechtskonformes Verhalten sicherzustellen. Gleichzeitig geht es darum, den Mittelweg zu finden und die wirtschaftlichen Interessen des Unternehmens im Blick zu behalten. So werden im Idealfall die Compliance-Anforderungen sowohl effektiv als auch organisatorisch und wirtschaftlich sinnvoll gestaltet und umgesetzt.

Ein klares Normverständnis und entsprechendes Risikobewusstsein sind Voraussetzung, um mögliche Rechtsverstöße erkennen zu können. Hier ein Beispiel: Ein Kunde, der bisher sein gesamtes Vermögen auf einem Sparkonto und in fest verzinsten Anlagen investiert hatte, gibt plötzlich den Auftrag, sein gesamtes Kapital „*schnellstmöglich*“ in (hochriskante) Aktienoptionen zu stecken, weil er einen „*Geheimtipp aus vertraulicher Quelle innerhalb des Top-Managements*“ bekommen hätte und deshalb davon ausgeht, dass die Aktien dieses Unternehmens stark steigen werden. Dieses Verhalten legt nahe, dass womöglich ein Fall verbotenen Insiderhandels (was zu entsprechenden Meldepflichten führen würde) vorliegt und lässt die „*roten Compliance-Lämpchen*“ aufleuchten.

Neben diesen gesetzlichen Vorgaben bestehen auch zahlreiche weitere Anforderungen, die die Organisation der Compliance-Abteilung selbst betreffen. Aus diesem Grund kann der Blick ins Bank- und Kapitalmarktrecht auch für das allgemeine Compliance-Verständnis äußerst gewinnbringend sein.

7.1.2 Funktionsweise des Kapitalmarkts

Der Kapitalmarkt dient Unternehmen als Finanzierungsquelle und bietet Anlegern die Möglichkeit, ihre Finanzmittel anzulegen. Für die Integrität der Finanzmärkte und damit auch den Schutz des Anlegervertrauens ist das Zusammenspiel von verfügbaren Informationen und Börsenpreisbildung entscheidend. Je mehr und je besser die Information ist, die dem Markt zur Verfügung steht, desto effektiver gestaltet sich die Börsenpreisbildung. Dies gilt auch für Handelsformen, wie den computergestützten Handel, das sogenannte **Algo-Trading** oder den **High-Frequency-Handel** (vgl. dazu Art. 18 f. Delegierte Verordnung (EU) 2017/565).

Der Kapitalmarkt selbst lässt sich in den **Primärmarkt** und den **Sekundärmarkt** unterteilen. Der Primärmarkt ist der Emissionsmarkt, dort wird ein Wertpapier erstmals platziert (§§ 32 ff. Börsengesetz i. V. m. Wertpapierprospektgesetz). Der Sekundärmarkt ist der Markt, auf dem bereits platzierte Wertpapiere gehandelt werden (WpHG). Daneben wird zwischen dem organisierten (§ 2 Abs. 11 WpHG) und nichtorganisierten Markt – etwa dem Freiverkehr (§ 48 BörsG), der auch den KMU-Wachstumsmarkt (§ 48a) umfasst – unterschieden.

Hinzukommen Finanzanlagen, die sich bewusst weitgehend staatlicher Regulierung entziehen und stattdessen auf Unabhängigkeit und Selbstregulierung setzen, wie etwa Kryptowährungen. Ob dies zu einer „Immunität“ gegenüber Marktmanipulation und anderen unerwünschten Handlungsweisen führt, die in geregelten Märkten durch gesetzliche Rahmenbedingungen und staatliche Aufsichtsbehörden verhindert werden sollen, bleibt abzuwarten.

Das Kapitalmarktrecht gilt dabei für Finanzinstrumente (§ 2 Absatz 4 WpHG), darunter fallen Wertpapiere, Geldmarktinstrumente und Derivate. Derivate sind Finanzinstrumente, die sich durch eine Hebelwirkung auszeichnen, also eine Kursbewegung des Basiswerts – etwa einer bestimmten Aktie – überproportional nachvollziehen können und deshalb für den Bereich des Marktmisbrauchs relevant werden. Das Kapitalmarktrecht findet darüber hinaus Anwendung auf Emittenten (§ 2 Absatz 13–16 WpHG) sowie auf Wertpapierdienstleistungsunternehmen, die insbesondere die Organisationspflichten nach § 80 Abs. 1 WpHG, Art. 22 DV und 26 Abs. 7 DV und 26 Abs. 7 DV treffen.

7.1.3 Aufsichtsbehörde

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) übt die Aufsicht über die Einhaltung der Vorgaben des WpHG (vgl. § 6 WpHG), sowie des Kreditwesengesetzes (§ 6 Abs. 2 KWG) aus. Die BaFin konkretisiert die gesetzlichen Anforderungen des Bank- und Kapitalmarktrechts, etwa im Emittenten-Leitfaden,³ sowie in zahlreichen weiteren Informationen. Auch ist die BaFin im Bereich des Verbraucherschutzes tätig, etwa in dem sie Informationen im Hinblick auf Kryptowerte und die damit verbundenen Risiken herausgibt.⁴ Aus Sicht der Compliance-Praxis ist weiter zu berücksichtigen, dass die Kompetenzen der BaFin im Zuge des neuen Finanzmarktintegritätsstärkungsgesetzes erweitert wurden. Zu den Kompetenzen der Finanzaufsichtsbehörde zählt etwa die Möglichkeit, bei Verdacht auf kapitalmarktrechtliches Fehlverhalten eine Warnung zu veröffentlichen oder den Handel auszusetzen (§ 6 Abs. 2 WpHG).

Gerade die Veröffentlichung auf der **Warnliste** ist ein scharfes Schwert, da sie die Reputation eines Unternehmens empfindlich treffen kann. Darüber hinaus stehen zahlreiche weitere Möglichkeiten auf der präventiven bzw. repressiven Ebene zur Verfügung, ganz zu schweigen von einer Weiterleitung von Verdachtsfällen an die Staatsanwaltschaft. Die BaFin verfügt i. Ü. auch über eine Hinweisgeberstelle für die Mitteilung möglicher Rechtsverstöße.⁵

³Abrufbar unter <https://www.bafin.de/dok/11407966> (aufgerufen am 7.2.2024).

⁴Näher <https://www.bafin.de/dok/17339832> (aufgerufen am 7.2.2024).

⁵Nähere Informationen zur Hinweisgeberstelle der BaFin finden sich unter <https://www.bafin.de/dok/8031504> (aufgerufen am 7.2.2024).

7.2 Prävention und Detektion von Marktmissbrauch

7.2.1 Insiderhandel

Strafbarer Insiderhandel fällt zusammen mit Marktmanipulation unter den Oberbegriff „**Marktmissbrauch**“. Die Verbotstatbestände ergeben sich aus einer Zusammenschau der Straf- und Bußgeldvorschriften des WpHG (Abschnitt 17 – §§ 119 bis 126), sowie den einschlägigen europäischen Vorgaben.⁶

► **Wichtig** Das Wertpapierhandelsrecht verbietet im Einzelnen:

- Entgegen Art. 14 a der Marktmissbrauchsverordnung ein Insidergeschäft zu tätigen (§ 119 Abs. 3 Nr. 1 WpHG)
- Insidergeschäfte zu empfehlen oder Dritte dazu zu verleiten (§ 119 Abs. 3 Nr. 2 WpHG, Art. 14 b der Marktmissbrauchsverordnung)
- Insiderinformation unbefugterweise offenzulegen (§ 119 Abs. 3 Nr. 3 WpHG, Art. 14 c der Marktmissbrauchsverordnung).

Was genau unter den Begriff „**Insiderinformationen**“ fällt, definiert die Marktmissbrauchsverordnung in Art. 7 (1) a: Es handelt sich dabei um **nicht öffentlich bekannte präzise Informationen**, die direkt oder indirekt einen oder mehrere Emittenten oder ein oder mehrere Finanzinstrumente betreffen und die, wenn sie öffentlich bekannt würden, **geeignet** wären, den **Kurs** dieser Finanzinstrumente oder den Kurs damit verbundener derivativer Finanzinstrumente **erheblich zu beeinflussen**. Die Verordnung macht zudem Ausführungen im Hinblick auf Warenderivate, Emissionszertifikate und die Mitteilung von Insiderinformation durch Kunden, Art. 7 (1) b–d.

Bei einer Insiderinformation handelt es sich um eine **nicht öffentlich bekannte Tat-sache**. Das bedeutet, dass sie keinem breiten Anlegerpublikum zugänglich gemacht wurde.

Beispiel

Fallbeispiel: Einem Pharmakonzern ist ein entscheidender Durchbruch bei der Entwicklung eines neuartigen Impfstoffs gelungen. Da dieser Impfstoff einen sehr viel effektiveren Schutz vor einer hochansteckenden Infektionskrankheit bietet, ist damit zu rechnen, dass das Bekanntwerden dieser Nachricht den Börsenkurs des Unternehmens beflügeln wird. ◀

⁶Verordnung (EU) Nr. 596/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über Marktmissbrauch (Marktmissbrauchsverordnung) und zur Aufhebung der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates und der Richtlinien 2003/124/EG, 2003/125/EG und 2004/72/EG der Kommission (ABl. L 173 vom 12.6.2014, S. 1; L 287 vom 21.10.2016, S. 320; L 306 vom 15.11.2016, S. 43; L 348 vom 21.12.2016, S. 83), die zuletzt durch die Verordnung (EU) 2016/1033 (ABl. L 175 vom 30.6.2016, S. 1) geändert worden ist.

Des Weiteren ist es **verboden, diese Information unbefugt Dritten mitzuteilen oder zugänglich zu machen**. Auch ist es verboten, auf der Grundlage von Insiderinformationen, den Erwerb oder die Veräußerung von Insiderpapieren zu empfehlen oder andere auf sonstige Weise dazu zu verleiten.

Beispiel

Fallbeispiel: Um das Verbot des Insiderhandels zu umgehen, werden Geschäfte nicht etwa persönlich, sondern etwa über Dritte, z. B. den Lebenspartner oder eine gute Bekannte, getätigt. ◀

Zu beachten sind auch die im WpHG vorgesehenen **Schadensersatzpflichten**: Wird die unverzügliche Veröffentlichung von Insiderinformationen unterlassen, löst dies eine Haftung nach § 97 WpHG aus. § 98 WpHG sieht zudem eine Schadensersatzpflicht für die Veröffentlichung falscher Insiderinformationen vor.

7.2.2 Organisatorische Maßnahmen

Ziel des Insiderhandelsverbots ist es, den Zugriff auf und die Verwendung kritischer Informationen zu kontrollieren, um Missbrauch bzw. die Ausnutzung dieses Wissensvorsprungs zum Zwecke der persönlichen Bereicherung zu verhindern. Ein wichtiger Schritt dafür ist es, einen Überblick darüber zu haben, wer innerhalb des Unternehmens Zugang zu solcher Information haben könnte.

Aus diesem Grund verpflichtet der Gesetzgeber Unternehmen dazu, eine **Insiderliste** (früher Insiderverzeichnis) zu führen (Art. 18 Marktmisbrauchsverordnung). In der Insiderliste sind Personen zu führen, die bestimmungsgemäß Zugang zu Insiderinformationen haben. In dieser – unverzüglich zu aktualisierenden Liste (Art. 4) – ist aufzuführen, von welchem Zeitpunkt an und bis zu welchem Zeitpunkt die einzelne Person Zugang zu Insiderinformationen hatte.

Dies dient der Individual- und Generalprävention von Straftaten, da die namentliche Nennung in einer solchen Liste im Idealfall von einer möglichen Tatbegehung abschreckt. Zum anderen wird damit der Tatnachweis erleichtert, denn so lässt sich problemlos überprüfen, ob eine Person zum Tatzeitpunkt bereits als Insider geführt wurde und mithin als geeigneter Täter bzw. Täterin in Betracht kommt.

► **Wichtig** Die **Insiderliste** muss deshalb mindestens **folgende Informationen** enthalten, Art. 18 (3) Marktmisbrauchsverordnung:

- die Identität aller Personen, die Zugang zu Insiderinformationen haben (a),
- den Grund der Aufnahme in die Insiderliste (b),
- das Datum, an dem diese Person Zugang zu Insiderinformationen erlangt hat sowie die entsprechende Uhrzeit und (c)
- das Datum der Erstellung der Insiderliste (d).

Der Emittent hat die in der Insiderliste geführten Personen über die rechtlichen Pflichten als Insider sowie über die Folgen von Verstößen gegen Insidervorschriften aufzuklären. Diese Verhaltenspflichten werden zusätzlich über schriftliche Handlungsanweisungen abgesichert und oftmals auch ausdrücklich im Arbeitsvertrag festgehalten.

Weitere organisatorische Maßnahmen der Insiderüberwachung sind die Schaffung von Vertraulichkeitsbereichen, sogenannten **Chinese Walls**. Dabei handelt es sich um Informationsbarrieren, um etwa in einem Finanzdienstleistungsinstitut die Bereiche, in denen Insiderinformation vorhanden ist, von anderen Bereichen zu trennen, um so die unbefugte Weitergabe bzw. Kenntnisnahme solcher Informationen bestmöglich zu vermeiden.⁷ Diese Informationsbarrieren können physischer Natur sein, etwa die Unterbringung in getrennten Gebäudekomplexen oder eben auch IT-Systeme betreffen.

Beispiel

Praxisbeispiele: Zu solchen Maßnahmen gehört etwa die „**clear desk policy**“, nach der Personen, die mit kritischer Information zu tun haben, nach Arbeitsende alle kritischen Unterlagen sicher zu verwahren und nicht sichtbar auf dem Schreibtisch liegen zu lassen haben. Somit können Dritte, die Zugang zum Gebäude haben, etwa zum Zweck der Raumpflege oder für Reparaturarbeiten, keine Insider-Informationen einsehen, sodass Dritte, die Zugang zum Gebäude haben, etwa zum Zweck der Raumpflege oder für Reparaturarbeiten, keine Insider-Informationen einsehen können. Auch ist es z. B. wichtig, den Speicher digitaler Kopiergeräte vor Wartungsarbeiten oder Geräte-Erneuerung zu löschen, um zu vermeiden, dass kritische Informationen das Unternehmen unkontrolliert verlassen. Hinzu kommen Handlungsanweisungen, etwa für den Fall, dass ein wichtiger Firmenlaptop gestohlen oder im Taxi vergessen wird, etc. ◀

Es gibt auch die Möglichkeit eines bereichsüberschreitenden Informationsflusses (**Wall crossing**), allerdings ist dabei zu beachten, dass dieser als geordneter Prozess durchzuführen und ordnungsgemäß zu dokumentieren ist.⁸

Dabei zeigt sich die Wichtigkeit, die unternehmensinternen Informationsflüsse so zu gestalten, dass entscheidende Informationen zeitnah weitergeleitet werden und eine umfassende Bewertung dieser Umstände vorgenommen werden kann.

In der Compliance-Praxis ist es ebenfalls wichtig, effektive Schulungen durchzuführen, damit sich Mitarbeiter und Führungskräfte zum einen über ihre detaillierten Pflichten im Klaren sind, zum anderen aber auch weitere Risiken, wie etwa „Informationslecks“, vermieden werden können.

⁷Vgl. dazu die Vorgaben der BaFin <https://www.bafin.de/dok/13483074> (aufgerufen am 7.2.2024).

⁸BaFin a. a. O.

7.2.3 Marktmanipulation

7.2.3.1 Das Verbot der Marktmanipulation

Während das Verbot des Insiderhandels in erster Linie auf die Kontrolle der Informationen an sich abzielt, soll das Verbot der Marktmanipulation sicherstellen, dass die weiteren Spielregeln des Kapitalmarkts von allen Beteiligten eingehalten werden und niemand den Börsenpreis (heimlich) manipuliert.

Dabei ist es so ähnlich wie bei Sportwetten: Das Wetten an sich ist – innerhalb der gesetzlichen Vorgaben-erlaubt. Allerdings ist es verboten, das Wettergebnis zu manipulieren. So haben sich in der Praxis Wettmanipulationen zugetragen, bei denen der Ausgang eines Fußballmatches durch Bestechungszahlungen an Spieler oder Schiedsrichter bereits vor dem Spiel ausgemacht wurde. Im Anschluss wurden mitunter hohe Beträge auf das „abgekartete“ Ergebnis gesetzt, was zu einer unrechtmäßigen Gewinnauszahlung führte.⁹

Die Überwachung der Einhaltung der kapitalmarktrechtlichen Spielregeln ist dabei um einiges komplexer. Das hat damit nicht nur mit der schieren Anzahl der täglich und oftmals in Sekundenbruchteilen getätigten Transaktionen zu tun, sondern auch mit den Schwierigkeiten, nachzuweisen, dass eine bestimmte Handlung tatsächlich kausal für die Preisbeeinflussung war.

Das Verbot der Marktmanipulation nach § 119 Abs. 1 Nr. 1–4 i. V. m. § 120 Abs. 2, Abs. 15 Nr. 3, Verordnung (EU) Nr. 596/2014 WpHG umfasst das **Verbot der Preisbeeinflussung** bei:

- Einem inländischen **Börsen- oder Marktpreis** eines Finanzinstruments, eines damit verbundenen Waren-Spot-Kontrakts, einer Ware im Sinne des § 2 Absatz 5 oder eines ausländischen Zahlungsmittels im Sinne des § 51 des Börsengesetzes,
- einem **Finanzinstrument** oder eines damit verbundenen Waren-Spot-Kontrakts an einem organisierten Markt, einem multilateralen oder organisierten Handelssystem in einem anderen Mitgliedstaat oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum,
- einer **Ware** im Sinne des § 2 Absatz 5 oder eines ausländischen Zahlungsmittels im Sinne des § 51 des Börsengesetzes an einem mit einer inländischen Börse vergleichbaren Markt in einem anderen Mitgliedstaat oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder
- der **Berechnung eines Referenzwertes** im Inland oder in einem anderen Mitgliedstaat oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum.

⁹Dies hat zu einer umfassenden strafrechtlichen Debatte und einer Reform des Strafrechts geführt, im Zuge derer Sportwettbetrug und die Manipulation berufssportlicher Wettbewerbe in § 265 c, d, e StGB unter Strafe gestellt wurden.

Nach § 119 Abs. 1, § 120 Abs. 2 Nr. 3 WpHG wird eine Marktmanipulation danach „entgegen § 25 WpHG in Verbindung mit Artikel 15 der Verordnung (EU) Nr. 596/2014“ begangen. Der Kern des Marktmanipulationsverbots liegt mithin in der Marktmisbrauchsverordnung.

Grundsätzlich gibt es drei verschiedene Formen der Marktmanipulation:

- Informationsgestützte,
- handelsgestützte und
- handlungsgestützte Taten.¹⁰

Nach diesen Vorgaben ist es verboten, unrichtige oder irreführende Angaben über Umstände zu machen, die für die Bewertung eines Finanzinstruments erheblich sind, oder solche Umstände entgegen bestehenden Rechtsvorschriften zu verschweigen, wenn die Angaben oder das Verschweigen geeignet sind, auf den inländischen Börsen- oder Marktpreis eines Finanzinstruments einzuwirken. Dabei handelt es sich um das Verbot **informationsgestützter** Marktmanipulation, das beispielsweise für die Verbreitung falscher Informationen in Internetforen oder die Verletzung kapitalmarktrechtlicher Informations- und Publizitätspflichten zum Zwecke der Marktmanipulation gilt.

Beispiel

Fallbeispiel 1: Der Zusammenhang von Information und Preisentwicklung lässt sich sehr gut am Beispiel des Börsenkurses von Twitter/X im Zuge der Übernahme durch Elon Musk erkennen. So genügte etwa die Behauptung des Tech-Moguls, dass die Anzahl von Spam- und Bot-Accounts höher sei, als von Twitter/X behauptet und er deshalb die Übernahme aussetze, um einen erheblichen Kurssturz der Twitter/X-Aktie auszulösen.¹¹ Die US-amerikanische Finanzaufsicht SEC ermittelt aus diesem Grund erneut wegen Marktmanipulation, zudem werden Sammelklagen von Anlegern zur Geltendmachung von Schadensersatzansprüchen vorbereitet.¹²

Fallbeispiel 2: Der Vorstand eines Unternehmens gibt eine Ad-hoc-Mitteilung heraus, in der er wider besseres Wissen die gravierende finanzielle Schieflage einer wichtigen Unternehmenssparte dementiert. Ziel dieser Maßnahme ist es, den Markt zu beruhigen und den Kurs des Unternehmens künstlich stabil zu halten. Dem Vorstand ist bewusst, dass bei einem Bekanntwerden der tatsächlichen, katastrophalen Lage des Unternehmens der Börsenpreis stark einbrechen wird. ◀

¹⁰Diese Tatvariante kommt in der Praxis nur sehr selten vor. Als Beispiel wäre ein Anschlag auf ein Passagierflugzeug zu nennen, um aus dem vorhersehbaren Kurssturz der Fluggesellschaft Gewinne zu erzielen.

¹¹Vgl. dazu den Beitrag der Süddeutschen Zeitung “SEC-Prüfung, Klagen: Musk wegen Twitter-Einstieg unter Druck”, abrufbar unter <https://www.sueddeutsche.de/wirtschaft/internet-sec-pruefung-klagen-musk-wegen-twitter-einstieg-unter-druck-dpa.urn-newsml-dpa-com-20090101-220527-99-450965> (aufgerufen am 7.2.2024).

¹²A. a. O.

Allerdings ist es auch möglich, den Preis eines Wertpapiers nicht nur durch Information, sondern auch durch Handel an den Wertpapiermärkten – also eine auf den ersten Blick legitime Tätigkeit – zu beeinflussen.

§ 119 Absatz 1, § 120 Abs. 2 Nr. 3 oder Abs. 15 Nr. 2, § 25 WpHG i. V. m. Artikel 15 der Verordnung (EU) Nr. 596/2014 verbietet es, **Geschäfte** vorzunehmen oder **Kauf- bzw. Verkaufsaufträge** zu erteilen, die geeignet sind, falsche oder irreführende Signale für das Angebot, die Nachfrage oder den Börsen- oder Marktpreis von Finanzinstrumenten zu geben oder ein **künstliches Preisniveau** herbeizuführen.

Beispiel

Fallbeispiel „Circular Trading“: Zwei Unternehmen, die zur selben Unternehmensgruppe gehören, verkaufen untereinander Aktien der Holding. Dabei sprechen Sie ab, dass die Transaktion zu einem deutlich über dem Markt liegenden Preis erfolgen soll. Dieser auf den ersten Blick wirtschaftlich unsinnige Hin- und Herverkauf „im Kreis“ (daher der Name), führt jedoch dazu, dass der Marktpreis von Anteilen der Holding in die Höhe getrieben wird. Gerade an diesem höheren Marktpreis kann jedoch sehr wohl ein erhebliches wirtschaftliches Interesse bestehen, etwa wenn der Eintritt einer gewinnbringenden Vertragsklausel an den Börsenpreis geknüpft ist, oder eine positive Unternehmensbewertung angestrebt wird. ◀

Eine weitere Tatvariante ist die absichtliche Verbreitung von **Falschinformationen**, mit dem Ziel der Preisbeeinflussung. Ob Marktmanipulation auch dann in Betracht kommt, wenn Absichten, etwa im Hinblick auf die Übernahme eines anderen Unternehmens, nicht offengelegt werden, war eine Frage, mit der sich die Justiz im folgenden Beispiel auseinandersetzen musste.

Beispiel

Fallbeispiel: Die Vorstandsmitglieder der Porsche SE mussten sich hinsichtlich der Vorwürfe der Beihilfe zur Marktmanipulation im Zusammenhang mit der seinerzeit versuchten Übernahme der deutlich größeren Volkswagen AG verantworten. Ihnen wurde vorgeworfen, Anleger gezielt über ihre Übernahmeabsichten im Unklaren gelassen zu haben. Viele Anleger erlitten, als Porsche im Herbst 2008 die tatsächlichen Übernahmeabsichten offenlegte, zum Teil horrende Verluste, da der Kurs der Volkswagen AG kurzfristig über 1000 € stieg und so zum teuersten Unternehmen des DAX wurde, sie jedoch auf eine gegenteilige Kursentwicklung spekuliert hatten. Im Zuge des anschließenden Strafverfahrens wurden die Vorstandsmitglieder allerdings freigesprochen (LG Stuttgart, 18. März 2016 – 13 KLs 159 Js 69207/09).¹³ ◀

¹³ Besprechung Momsen/Laudien ZIS 9/2016, S. 646 ff., abrufbar unter https://www.zis-online.com/dat/artikel/2016_9_1050.pdf (aufgerufen am 7.2.2024).

7.2.3.2 Safe Harbours

Tatbestandliche Ausnahmen vom Verbot der Marktmanipulation – **safe harbours** – bestehen für Rückkaufprogramme oder erlaubte Stabilisierungsmaßnahmen (Art. 5 Abs. 1 und 4 MAR WpHG).¹⁴ Für Emittenten ist es wichtig, die Grenzen dieser Ausnahme-regelungen genauestens einzuhalten, um strafrechtliche Haftungsrisiken bzw. Ordnungswidrigkeiten wegen Marktmanipulation zu vermeiden.

7.2.4 Anzeigepflichten

Ebenso wie im Bereich der Geldwäsche gilt auch im Bereich der Prävention von Insiderhandel und Marktmanipulation das Prinzip der Inpflichtnahme privater Unternehmen zur Durchsetzung der Rechtseinhaltung, wie bereits in der Einleitung zu diesem Beitrag erwähnt wurde.

Ein weiterer Teilbereich der Compliance im Bank- und Kapitalmarktrecht ist mithin die Erfüllung von Anzeigepflichten nach § 23 WpHG i. V. m. 12, 13 oder 14 der Verordnung (EU) Nr. 236/2012 durch Wertpapierdienstleistungsunternehmen. Diese sind nach dem Wertpapierhandelsgesetz verpflichtet, verdächtige Transaktionen – etwa bei Indizien für Insiderhandel oder Marktmanipulation – an die BaFin zu melden. Dabei handelt es sich um eine rechtssystematische Ausnahme, da Anzeigepflichten in der Rechtsordnung nur in äußerst seltenen Fällen vorgesehen werden (vgl. etwa § 138 StGB). Allerdings überwiegt in diesem Fall das Interesse, die Integrität der Finanzmärkte und das Anlegervertrauen zu schützen.

Eine Meldung darf insbesondere nicht dem betroffenen Kunden mitgeteilt werden. Die BaFin kann bzw. muss ihrerseits den Sachverhalt an die zuständige Staatsanwaltschaft übermitteln (§ 11 WpHG), was zur Einleitung eines strafrechtlichen Ermittlungsverfahrens führen kann. Aus Sicht der Compliance-Praxis ist zudem die Bußgeldbewehrung der Anzeigepflicht zu beachten, § 120 WpHG Abs. 15 a i. V. m. Verordnung (EU) 2019/1238.

7.2.5 Reg-Tech

Für die Einhaltung der Anzeigepflicht nach § 23 WpHG verwenden Wertpapierdienstleistungsunternehmen entsprechende IT-Systeme, die Transaktionen automatisch auf Anomalien untersuchen. Diese Anomalien können sich auf ein außergewöhnliches Handelsvolumen oder einen außergewöhnlichen Handelszeitpunkt beziehen. Solche IT-Systeme

¹⁴ Für Einzelheiten vgl. den Emittentenleitfaden der BaFin, Modul C – Regelungen aufgrund der Marktmisbrauchsverordnung (MAR) – Ausnahmen für Rückkaufprogramme und Kursstabilisierungsmaßnahmen von dem Marktmisbrauchsverbot (sog. „Safe Harbour“), <https://www.bafin.de/dok/13484918> (aufgerufen am 7.2.2024).

kommen in ähnlicher Weise auch zur Prävention und Detektion von Geldwäscherisiken zum Einsatz. Sie gleichen Transaktionen nach bestimmten Indikatoren ab. Werden entsprechende Auffälligkeiten entdeckt, so werden diese zunächst an die Compliance-Abteilung gemeldet, die dann über eine Anzeige nach § 23 WpHG entscheidet.

Da die Erfüllung der rechtlichen Pflichten mittlerweile eine ungeahnte Komplexität erreicht hat, haben sich daraus lukrative Geschäftsmodelle für die IT-Branche entwickelt, die unter dem Stichwort **Regulation Technologie** firmieren. Da immer komplexere und kleinteilige rechtliche Anforderungen die Unternehmen vor einen erheblichen Organisations- und Verwaltungsaufwand stellen, ist dies oftmals nur noch mit Software-Unterstützung möglich.

Ein Bankmitarbeiter hat dies einmal etwas überspitzt folgendermaßen formuliert: „*Mittlerweile ist es fast so, dass an einem normalen Arbeitstag auf eine Stunde Bankgeschäft, gefühlt 7 h Compliance entfallen.*“ Auch dieser Aufwand ist unter Compliance-Gesichtspunkten zu berücksichtigen. Denn die Compliance-Kosten haben ganz reale Auswirkungen: So kann es für Banken schlichtweg nicht mehr rentabel sein, einzelne Filialen zu betreiben oder sogar die Betreuung bestimmter Kundengruppen auf den wirtschaftlichen Prüfstand stellen zu müssen.

7.3 Ad-hoc-Publizität

Im Zusammenhang mit den umfangreichen kapitalmarktrechtlichen Informations- und Publizitätspflichten ist im Bereich der Emittenten-Compliance vor allem die Ad-hoc-Publizität von Bedeutung. Die **Ad-hoc-Publizitätspflicht** dient dazu, einen gleichmäßigen Informationsstand aller Marktteilnehmer zu gewährleisten, weshalb sie schnellstmöglich (= ad-hoc) erfolgen muss.

Aus diesem Grund müssen **Insiderinformationen**, also Informationen, die geeignet sind, den Preis eines Finanzinstruments zu beeinflussen, grundsätzlich unverzüglich veröffentlicht werden (Art. 17 Abs. 1 Marktmissbrauchsverordnung). Beispiele sind Erwerb oder Veräußerung von wesentlichen Beteiligungen, Übernahme und Abfindungs- bzw. Kaufangebote, Kapitalmaßnahmen, wesentliche Änderungen von Geschäftsergebnissen, überraschende Veränderungen von Schlüsselpositionen in Unternehmen. Der Emittentenleitfaden der BaFin bietet weitere nützliche Anhaltspunkte.¹⁵

Die Bewertung der Erheblichkeit stellt nicht nur unter Gesichtspunkten des **Bestimmt-heitsgebots** eine Herausforderung dar. Auch für den Rechtsanwender stellen sich erhebliche Unsicherheiten ein, wenn es darum geht, die Auswirkungen auf den Börsenpreis zu bestimmen, da für die korrekte Bestimmung der Kursentwicklung eine Vielzahl von Faktoren relevant werden.

¹⁵ Abrufbar unter www.bafin.de (aufgerufen am 7.2.2024).

Von der Ad-hoc-Publizität kann abgesehen werden, wenn **berechtigte Interessen des Emittenten** bestehen, Art. 17 Abs. 4, 5 Marktmisbrauchsverordnung. Dies kann etwa der Fall sein, wenn ein öffentliches Interesse daran besteht, mit der Veröffentlichung abzuwarten.

7.4 Director's Dealings

Transaktionen bestimmter **Führungs Personen** von Emittenten (sog. **Eigengeschäfte**) müssen offengelegt werden, Art. 19 Marktmisbrauchsverordnung. Dies gilt für Personen mit Führungsaufgaben, wie etwa Vorstände, Mitglieder des Verwaltungs- und/oder Aufsichtsorgans, persönlich haftende Gesellschafter oder ihnen gleichgestellte Personen, um eine Umgehung dieser Offenlegungspflichten zu vermeiden. Aber auch Führungskräften nahestehende Personen müssen Eigengeschäfte offenlegen.

Diese Vorschrift zählt auf den Anlegerschutz ab, da Eigengeschäfte wichtige Rückschlüsse auf die Wirtschaftslage des Unternehmens zulassen. Verkaufen Führungskräfte etwa Anteile des eigenen Unternehmens in größerer Menge, lässt vermuten, dass sie mit einer deutlichen Verschlechterung der Geschäftsaussichten rechnen. Auch führt eine Offenlegungspflicht zu einer erhöhten Prävention im Hinblick auf verbotene Insidergeschäfte oder Marktmanipulation, da durch die Bekanntmachung für zusätzliche Transparenz auf dem Markt gesorgt wird.

Aus diesem Grund liegt die Marktmisbrauchsverordnung in Art. 19 Abs. 1 S. 2 fest, dass die Mitteilung solcher Transaktionen unverzüglich, spätestens jedoch innerhalb von drei Tagen, erfolgen muss. Die Marktmisbrauchsverordnung lässt den nationalen Aufsichtsbehörden, wie in unserem Fall der BaFin, Spielraum, um Schwellenwerte bis zu einer Höhe von 20.000 € festzulegen. Von dieser Möglichkeit hat die BaFin Gebrauch gemacht.¹⁶

Im Einzelnen müssen folgende Informationen mitgeteilt werden, vgl. Art. 19 Abs. 6 Marktmisbrauchsverordnung:

- a. Name der Person;
- b. Grund der Meldung;
- c. Bezeichnung des betreffenden Emittenten oder Teilnehmers am Markt für Emissionszertifikate;
- d. Beschreibung und Kennung des Finanzinstruments;
- e. Art des Geschäfts bzw. der Geschäfte;
- f. Datum und Ort des Geschäfts bzw. der Geschäfte und
- g. Kurs und Volumen des Geschäfts bzw. der Geschäfte.

¹⁶Näher <https://www.bafin.de/dok/7846232> (aufgerufen am 7.2.2024).

7.5 Organisationspflichten nach § 80 Abs. 1 WpHG, Art. 22 DV und 26 Abs. 7 DV und 26 Abs. 7 DV

§ 80 Abs. 1 WpHG, Art. 22 DV und 26 Abs. 7 DV und 26 Abs. 7 DV definieren die **Organisationspflichten** eines Wertpapierdienstleistungsunternehmens über die organisatorischen Pflichten nach § 25a Abs. 1 und 4 KWG hinaus. Wie die Umsetzung dieser Vorgaben im Einzelnen zu erfolgen hat, definiert die BaFin.

§ 87 Abs. 5 WpHG erfordert, dass der Compliance-Beauftragte über zwei Schlüsselkompetenzen verfügt: **Sachkenntnis¹⁷** und **Zuverlässigkeit**. Auch ist es erforderlich, der BaFin diese Personalentscheidung mitzuteilen, bevor die entsprechende Person ihre Tätigkeit aufnimmt. Die Aufsichtsbehörde kann ggf. die Aufnahme der Tätigkeit untersagen.

Art. 22 Delegierte VO (EU) 2017/565 erfordert im Hinblick auf die Organisationspflichten, dass:

Rechtliche Anforderungen an die Compliance-Organisation und die Präventionsstrategie bei Wertpapierfirmen nach EU-Recht

„(1) Die Wertpapierfirmen legen angemessene Strategien und Verfahren fest, die darauf ausgelegt sind, jedes **Risiko** einer etwaigen Missachtung der in der Richtlinie 2014/65/EU festgelegten Pflichten durch die Wertpapierfirma sowie die damit verbundenen Risiken **aufzudecken**, und setzen diese **auf Dauer** um, und sie führen **angemessene Maßnahmen und Verfahren** ein, um dieses **Risiko auf ein Mindestmaß** zu beschränken und die zuständigen Behörden in die Lage zu versetzen, ihre Befugnisse im Rahmen dieser Richtlinie wirksam auszuüben. (...)

(2) Die Wertpapierfirmen richten eine **permanente und wirksame, unabhängig arbeitende Compliance-Funktion** ein, erhalten diese aufrecht und betrauen sie mit den folgenden Aufgaben:

- a) ständige **Überwachung** und regelmäßige **Bewertung** der Angemessenheit und Wirksamkeit der (...) eingeführten Maßnahmen, Strategien und Verfahren (...);
- b) **Beratung und Unterstützung** der für Wertpapierdienstleistungen und Anlagetätigkeiten zuständigen relevanten Personen (...)
- c) mindestens einmal jährlich Berichterstattung an das Leitungsorgan über die **Umsetzung und Wirksamkeit des gesamten Kontrollumfelds** für Wertpapierdienstleistungen und Anlagetätigkeiten (...).
- d) Überwachung der Prozessabläufe für die Abwicklung von Beschwerden und Berücksichtigung von Beschwerden (...).“

¹⁷Vgl. zu den Anforderungen an die Sachkunde der Compliance-Mitarbeiter die Vorgaben der Ma-Comp – BT 1.3.1.3. Dazu zählen neben Kenntnissen der einschlägigen Rechts- und Verwaltungsvorschriften umfangreiches Wissen zur Ablauforganisation des Unternehmens, Finanzinstrumenten usw. Auch wird auf die Notwendigkeit regelmäßiger Schulungen hingewiesen.

Art. 22 (3) definiert, welche Bedingungen erfüllt sein müssen, damit die gerade genannte **Compliance-Funktion** ihre **Aufgaben ordnungsgemäß und unabhängig** wahrnehmen kann¹⁸:

- „a) dass die Compliance-Funktion über die notwendigen **Befugnisse, Ressourcen** und **Fachkenntnisse** verfügt und **Zugang** zu allen einschlägigen Informationen hat;
- b) das Leitungsorgan ernennt einen **Compliance-Beauftragten** (...);
- c) die Compliance-Funktion **informiert ad hoc** (...), wenn sie ein erhebliches Risiko feststellt, dass die Wertpapierfirma ihre Pflichten gemäß der Richtlinie 2014/65/EU nicht erfüllt;
- d) relevante Personen, die in die **Compliance-Funktion** eingebunden sind, *sind nicht an der Erbringung der von ihnen überwachten Dienstleistungen oder Tätigkeiten beteiligt*;
- e) das Verfahren, nach dem die **Vergütung** der in die Compliance-Funktion eingebundenen relevanten Personen bestimmt wird, beeinträchtigt weder deren Objektivität noch lässt sie eine solche Beeinträchtigung wahrscheinlich erscheinen.“

Im Zuge der Überarbeitung der Vorgaben der europäischen Wertpapieraufsicht ESMA hat die BAFIN auch die Anforderung der Compliance in der MaComp aktualisiert. Diese Änderungen betreffen insbesondere die Anforderungen an die Überwachungshandlungen, die Beratungsaufgaben und die Beteiligung der Compliance-Funktion an Prozessen, sowie die Vorgaben an den jährlichen Compliance-Bericht.

Die folgenden aufgeführten Anforderungen ergeben sich aus den § 80 Abs. 1 WpHG, Art. 22 DV und 26 Abs. 7 DV und 26 Abs. 7 DV, die seitens der BaFin durch das Rundschreiben 05/2018 (WA) – Mindestanforderungen an die Compliance-Funktion und weiteren Verhaltens-, Organisations- und Transparenzpflichten (MaComp) – im Einzelnen dargelegt werden.

Da die MaComp sehr umfassende und detaillierte Vorgaben enthält, soll im Nachfolgenden nur auf besonders relevante Aspekte eingegangen werden, die auch für die allgemeine Compliance-Diskussion von Interesse sein können.

7.5.1 Stellung der Compliance

Die Compliance-Funktion ist **angemessen, dauerhaft** und **wirksam** einzurichten und auszustatten, wofür die Geschäftsleitung die Gesamtverantwortung trägt (BT 1.1). Die Bedeutung der Compliance-Funktion soll ihrer Stellung in der Unternehmensorganisation

¹⁸ Für eine bessere Verständlichkeit wurde der Gesetzestext nicht im Wortlaut wiedergegeben, sondern leicht modifiziert.

gerecht werden. Die BaFin hebt außerdem die Bedeutung der **Compliance-Kultur** innerhalb des Unternehmens hervor, um die Rahmenbedingungen für die Förderungen des Anlegerschutzes und die Integrität der Finanzmärkte zu schaffen. Auch wird betont, dass der Compliance-Officer über eine besonders **integre und rechtschaffene Persönlichkeit** verfügen sollte, also die genannten Werte vorleben und verkörpern müsse.

7.5.1.1 Unabhängigkeit

Die Compliance Funktion sollte über die notwendige Unabhängigkeit innerhalb der Unternehmensorganisation verfügen. Das bedeutet, dass es sich grundsätzlich um eine **eigenständige Unternehmensabteilung** handeln sollte, auch wenn die Möglichkeit besteht, die Compliance Funktion mit anderen Unternehmensabteilungen, wie etwa der Rechtsabteilung, zusammenzulegen.

Die Unabhängigkeit des Compliance-Beauftragten (BT 1.3.3) wird dadurch sichergestellt, dass andere Geschäftsbereiche **kein Weisungsrecht** gegenüber der Compliance-Funktion besitzen. Der Compliance-Beauftragte darf nicht an Wertpapierdienstleistungen beteiligt sein, außer wenn eine Funktionstrennung etwa im Hinblick auf die Größe des Unternehmens unverhältnismäßig wäre (BT 1.3.3.1, 2). Eine aus dem Blickwinkel der allgemeinen Compliance-Organisation interessante Frage ist die Kombination der Compliance-Funktion mit der Rechtsabteilung (BT 1.3.3.3).¹⁹ Die BaFin hält eine Kombination beider Funktionen nur bei kleineren Wertpapierdienstleistungsunternehmen für zulässig. Bei größeren Wertpapierdienstleistungsunternehmen oder solchen mit komplexeren Aktivitäten ist die Kombination nicht statthaft, wenn die Unabhängigkeit der Compliance-Funktion gefährdet wird.

Die Unabhängigkeit des Compliance-Beauftragten ist durch besondere arbeitsvertragliche Regelungen, wie etwa eine Ernennung für mindestens 24 Monate oder die Vereinbarung einer 12-monatigen Kündigungsfrist seitens des Arbeitgebers zu schützen (BT 1.3.3.4 Nr. 4) und muss sich im Vergütungssystem widerspiegeln (BT 1.3.3.4 Nr. 6). Die BaFin betont, dass die **Vergütung** der Mitarbeiter der Compliance-Abteilung nicht von der Tätigkeit der zu überwachenden Mitarbeiter abhängen dürfe. Diese Vorgaben – die im Übrigen auch für allgemeine Compliance-Programme zu gelten haben – schließen eine erfolgsbezogene Vergütung dabei nicht grundsätzlich aus, es muss jedoch sichergestellt werden, dass mögliche Interessenkonflikte vermieden werden. Die Einzelheiten regelt Art. 22 Abs. 4 i. V. m. Abs. 3 e) DV.

7.5.1.2 Dauerhaftigkeit der Compliance

Die BaFin verlangt, dass die Compliance-Funktion dauerhaft eingerichtet sein müsse (BT 1.3.2). Aus diesem Grund müssen Überwachungshandlungen nicht nur anlassbezogen, sondern auf der Grundlage eines **Überwachungsplans** und regelmäßig durchgeführt werden.

¹⁹Vgl. Moosmayer, NJW 2012, 2013, 3014 ff.

BT 1.3.2 Dauerhaftigkeit:

Dem Compliance-Beauftragten ist ein **Vertreter** zuzuordnen. Dieser muss ausreichend qualifiziert sein, um die Aufgaben des Compliance-Beauftragten während seiner Abwesenheit auszuführen. Im Übrigen stellen die Organisations- und Arbeitsanweisungen die hinreichende Aufgabenerfüllung während der Abwesenheit des Compliance-Beauftragten insbesondere durch eine entsprechende **Vertretungsregelung** sicher. Des Weiteren sind die Aufgaben und die Kompetenzen der Compliance-Funktion, Überwachungsplan, Berichtspflichten der Compliance-Funktion, sowie eine Beschreibung des risikobasierten Überwachungsansatzes, insbesondere der Risikoanalyse, festzuhalten.

7.5.2 Aufgaben der Compliance

7.5.2.1 Beratungs- und Unterstützungsfunction

Die BaFin hebt auch die Beratungs- und Unterstützungsfunction der Compliance hervor. Darunter fallen regelmäßige oder anlassbezogene **Schulungsmaßnahmen**, insbesondere bei einer Änderung des rechtlichen Rahmens oder der Unternehmensorganisation (BT 1.2.3).

7.5.2.2 Überwachung

Eine weitere, wichtige Aufgabe der Compliance ist die Überwachung (BT 1.2.1.2). Dabei ist zu prüfen, ob die unternehmensinternen Handlungsvorgaben auf dem neuesten Stand sind oder ob es einer Korrektur bedarf. Als **Prüfungsmaßnahmen** liegt die BaFin aggregierte Risikomessungen, aber auch Vor-Ort-Prüfungen, nahe. Dies gilt auch für die allgemeine Compliance, denn oftmals zeigen sich durch solche **Kontrollmaßnahmen**, inwieweit die internen Handlungsanweisungen tatsächlich umgesetzt werden, oder ob sie „nur auf dem Papier“ eingehalten werden.

Auch sehr wichtig ist es, dass die Mitarbeiter, die Wertpapierdienstleistungen erbringen, das nötige **Bewusstsein für Compliance-Risiken** mitbringen. Dieses Bewusstsein steht in engem Zusammenhang mit der schon oben genannten Compliance-Kultur des Unternehmens, die für die Einhaltung der rechtlichen Vorgaben und des Anlegerschutzes so bedeutsam ist. Zu den Überwachungsaufgaben der Compliance gehört es zudem, die unzulässige Weitergabe von Compliance-relevanten Informationen zu verhindern.

7.5.2.3 Berichtspflichten

Die Geschäftsleitung kann Ihrer Verantwortung für den Bereich Compliance nur dann erfolgreich gerecht werden, wenn sie über **ausreichend Informationen zeitnah und präzise** verfügen kann. Deshalb ist die Übermittlung regelmäßiger Compliance-Berichte an die Geschäftsleitung unverzichtbar.

Die **Berichte** haben laut der Vorgaben der BaFin eine Beschreibung der Umsetzung und Wirksamkeit des gesamten Kontrollwesens hinsichtlich der Wertpapierdienstleistungen sowie eine Zusammenfassung der identifizierten Risiken und der durch-

geführten bzw. durchzuführenden Maßnahmen zur Behebung bzw. Beseitigung von Defiziten und Mängeln sowie zur Risikoreduzierung zu enthalten. Auch verlangt die BaFin, dass die Berichte in angemessenen Zeitabständen, zumindest einmal jährlich, erstellt werden müssen.

Sollten es die Umstände erfordern, so sind auch **ad-hoc-Berichte** unverzüglich zu erstellen, sodass die Geschäftsleitung jederzeit über akute Compliance-Risiken im Bilde ist.

Übersicht

Die **Compliance-Berichte** müssen, soweit einschlägig, zumindest die folgenden Angaben enthalten:

- **Allgemeine Informationen**, wie etwa ein Überblick über die Struktur der Compliance-Funktion oder Angaben zur Angemessenheit der Personal- und Sachausstattung der Compliance-Funktion, oder eine Beschreibung der Risiken, die in dem von der Compliance-Funktion überwachten Bereich identifiziert wurden, sowie weitere Informationen.
- Art und Weise der **Überwachung und Prüfung**, mit Einzelheiten wie etwa einer Zusammenfassung durchgeföhrter Prüfungen (insbesondere Vor-Ort-Prüfungen und Aktenprüfungen).
- Feststellungen von **Risiken, Verstößen und Mängel** in den jeweiligen Compliance-Prozessen, sowie entsprechende Maßnahmen zur Beseitigung bzw. Risikominimierung.
- **Sonstiges**, etwa eine Erklärung darüber, wo und wie die Geschäftsleitung von wichtigen Empfehlungen oder Einschätzungen der Compliance-Funktion abgewichen ist.

7.6 Organisationspflichten nach § 25a KWG

Nicht nur das WpHG, sondern auch das Kreditwesengesetz (KWG) macht – in Verbindung mit den einschlägigen europäischen Vorgaben – zahlreiche Organisationsvorgaben, die der Normeinhaltung dienen, § 25a Abs. 1 KWG. Ein Institut muss nach Satz 3 dieser Vorschrift zudem über ein angemessenes **Risikomanagement** verfügen:

1. die Festlegung von Strategien, insbesondere die Festlegung einer auf die nachhaltige Entwicklung des Instituts gerichteten Geschäftsstrategie und einer damit **konsistenten Risikostrategie**, sowie die Einrichtung von Prozessen zur Planung, Umsetzung, Beurteilung und Anpassung der Strategien;

2. Verfahren zur **Ermittlung und Sicherstellung der Risikotragfähigkeit**, wobei eine vorsichtige Ermittlung der Risiken, der potenziellen Verluste, die sich auf Grund von Stressszenarien ergeben (...);
3. die **Einrichtung interner Kontrollverfahren mit einem internen Kontrollsyste**m und einer **Internen Revision**, wobei das interne Kontrollsyste insbesondere
 - a. **aufbau- und ablauforganisatorische Regelungen** mit klarer Abgrenzung der Verantwortungsbereiche,
 - b. Prozesse zur **Identifizierung, Beurteilung, Steuerung** sowie **Überwachung** und **Kommunikation** der Risiken (...) und
 - c. eine **Risikocontrolling-Funktion** und eine **Compliance-Funktion** umfasst;
4. eine **angemessene** personelle und technisch organisatorische **Ausstattung** des Instituts;
5. Die Festlegung eines angemessenen **Notfallmanagements**, insbesondere für IT-Systeme, und
6. angemessene, transparente und auf eine nachhaltige Entwicklung des Instituts ausgerichtete **Vergütungssysteme** für Geschäftsleiter und Mitarbeiter (...).

Besonders relevant für die Prävention und Detektion von Marktmisbrauch ist die Verpflichtung zur Einrichtung eines Hinweisgebersystems (§ 25a Abs. 1 KWG S. 4 Nr. 3) zur Meldung von Verstößen gegen die Marktmisbrauchsverordnung, sowie „gegen weitere gesetzliche Vorgaben, wie das WpHG, sowie etwaige strafbare Handlungen innerhalb des Unternehmens“.

Auf diese Weise wird ein zusätzliches Instrument geschaffen, um die Integrität der Finanzmärkte und eine umfassende Compliance im Bank- und Kapitalmarktrecht sicherzustellen.

Literatur

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) – Emittentenleitfaden der Bundesanstalt für Finanzdienstleistungsaufsicht, 5., neu gefasste Auflage, Modul A (Stand 9.8.2018), Modul B (Stand 30.10.2018) und Modul C (Stand 25.3.2020) digital verfügbar unter: BaFin – Emittentenleitfaden – Einleitung zum Emittentenleitfaden der BaFin (aufgerufen am 2.3.2024).

FAZ – „Banken drohen hohe Strafen wegen Whatsapp-Nutzung“, abrufbar unter <https://www.faz.net/aktuell/finanzen/whatsapp-nutzung-banken-in-den-usa-drohen-hohe-strafen-18261449.html>, aufgerufen am 26.2.2024.

MOMSEN/LAUDIEN, Der Tatbestand der Marktmanipulation zwischen Porsche-Verfahren und 1. Finanzmarktnovellierungsgesetz (1. FiMaNoG), ZIS 2016, 646–653.

MOOSMAYER, Modethema oder Pflichtprogramm guter Unternehmensführung? – Zehn Thesen zu Compliance, NJW 2012, 2013, 3014 ff.

Süddeutsche Zeitung – „SEC-Prüfung, Klagen: Musk wegen Twitter-Einstieg unter Druck“, abrufbar unter <https://www.sueddeutsche.de/wirtschaft/internet-sec-pruefung-klagen-musk-wegen-twitter-einstieg-unter-druck-dpa.urn-newsml-dpa-com-20090101-220527-99-450965>, aufgerufen am 26.2.2024.

Vertiefend zum Bank- Kapitalmarktrecht

ASSIES, PAUL H./BEULE, DIRK/HEISE, JULIA, Handbuch Bank- und Kapitalmarktrecht, 6. Aufl., Wolters Kluwer, 2024 (im Erscheinen).

BUCK-HEEB, PETRA, Kapitalmarktrecht, 13. Aufl. C.F. Müller, Heidelberg, 2023.

EINSELE, DOROTHEE, Bank- und Kapitalmarktrecht, Nationale und internationale Bankgeschäfte, 5. Auflage, Mohr Siebeck, 2022.

ERNE, ROLAND (Hrsg.) u.a., Bank- und Kapitalmarktrecht Taschenbuch 6. Aufl., C.H.Beck, 2023

LEHMANN, MATTHIAS, Grundriss des Bank- und Kapitalmarktrechts, C.F. Müller, Heidelberg, 2. Aufl., 2023



Dr. Axel-Dirk Blumenberg ist als Anwalt und Dozent u. a. auf Wirtschaftsstrafrecht und Compliance spezialisiert. Studium der Rechtswissenschaften an der Universität Passau und der Universität Castilla-La Mancha (Spanien). Master in Unternehmensführung an der Universität Castilla-La Mancha. Nach seinem Studium war Axel-Dirk Blumenberg als wissenschaftlicher Mitarbeiter am Institut für Europäisches und Internationales Strafrecht der Universität von Castilla-La Mancha tätig. Als Anwalt war er u. A. für die Kanzlei Roxin (München), eine spanische Großkanzlei (Madrid/Barcelona) und eine auf Wirtschafts- und Unternehmensstrafrecht spezialisierte Kanzlei (Madrid/Barcelona), bei der er zum Teil IBEX-35 notierte Unternehmen im Hinblick auf das spanische Unternehmensstrafrecht beriet, tätig. Axel-Dirk Blumenberg promovierte rechtsvergleichend über das Thema „Marktmanipulation und Compliance“ und veröffentlichte zahlreiche Beiträge zu Wirtschaftsstrafrecht und Compliance, sowie Fachübersetzungen.

Teil III

Kontrollmechanismen – Compliance bei Ausübung von Compliance



Compliant Compliance – Ausgewählte Grenzen maximaler Kontrolle

8

Michael Schmidl

Inhaltsverzeichnis

8.1	Einleitung und aktuelle Entwicklung	149
8.1.1	Überfüllung von Compliance-Bemühungen	149
8.1.2	Arbeitnehmer- und Drittrechte als Schranken	149
8.1.3	Eignung einer Maßnahme	152
8.2	E-Mail-Filterung im Lichte von §§ 206, 303 a StGB	152
8.2.1	Auswirkungen von § 206 StGB im Bereich der E-Mail-Filterung	152
8.2.1.1	Geschütztes Rechtsgut	152
8.2.1.2	Reichweite des Schutzes	153
8.2.1.3	Eingriff in den Normalverlauf der Telekommunikation	153
8.2.1.4	Taugliche Täter	154
8.2.1.5	E-Mail als taugliches Tatobjekt	155
8.2.1.6	Ausfiltern und Verzögern als Tathandlung	155
8.2.1.7	Zeitliche Grenze der Tatbestandsverwirklichung	156
8.2.1.8	Zur Übermittlung anvertraut	164
8.2.1.9	Rechtswidrigkeit	165

Geringfügig modifizierter Zweitabdruck des Beitrags „Compliant Compliance – Ausgewählte Grenzen maximaler Kontrolle“ mit Genehmigung des Verlages C.H. Beck oHG, Wilhelmstraße 9, München, aus dem Werk „Wirtschaftsstrafrecht – Handbuch für die Unternehmens- und Anwaltspraxis – Momsen/Grützner, 2013“

M. Schmidl (✉)

Baker McKenzie, München, Deutschland

E-Mail: Michael.Schmidl@bakermckenzie.com

8.2.2	Regelungsgehalt und Auswirkungen von § 303 a StGB	165
8.2.3	Lösungsansätze	166
8.3	Whistleblowing im Lichte des Datenschutzrechts	167
8.3.1	Hinweisgeberschutzgesetz	167
8.3.1.1	Meldestellen	168
8.3.1.2	Vertraulichkeit	168
8.3.2	Zentrale Anforderungen des Datenschutzrechts	169
8.3.2.1	Schutzziel des Datenschutzrechts	169
8.3.2.2	Datenminimierung	170
8.3.2.3	Information der Betroffenen	170
8.3.2.4	Kein Konzernprivileg	172
8.3.2.5	Anforderungen an internationale Übermittlungen	173
8.3.3	Lösungsansätze	174
8.4	Screening von E-Mail und Internetverkehrsdaten	175
8.4.1	Screening von E-Mail	175
8.4.1.1	Interessenlage	175
8.4.1.2	Anwendung von § 206 StGB	176
8.4.1.3	Anwendung des Datenschutzrechts	177
8.4.2	Screening von Internetverkehrsdaten	178
8.4.2.1	Anwendbarkeit des TDDDG	178
8.4.2.2	Mögliche Erlaubnistatbestände	179
8.5	Totalüberwachung im Lichte von Art. 1 GG und sonstige Grenzen	180
8.5.1	Grenzen der Überwachung aus Art. 1 GG	180
8.5.1.1	Verbot der Totalüberwachung	180
8.5.1.2	Datenschutzrechtliche Absicherung	181
8.5.1.3	Bezugspunkt der Totalüberwachung	181
8.5.2	Auswirkungen auf typische Maßnahmen	182
8.5.2.1	Mitlesen von Bildschirmen	182
8.5.2.2	Einsatz von Keylogger-Software	182
8.5.2.3	Lückenlose Browser-Überwachung	182
8.5.3	Zusätzlicher Schutz bei Telefon- und Videoüberwachung	183
8.5.3.1	Schutz durch § 201 StGB	183
8.5.3.2	Schutz gemäß § 201 a StGB	184
8.6	Kontrollmaßnahmen im Lichte des IT-Grundrechts	186
8.6.1	Schutzbereich des IT-Grundrechts	186
8.6.1.1	Herleitung und Schutzbereich	186
8.6.1.2	Übertragbarkeit auf Verhältnisse am Arbeitsplatz	187
8.6.2	Auswirkungen auf Kontrollmaßnahmen	189
8.7	Sonstige Folgen unzulässiger Kontrollmaßnahmen	190
8.7.1	Beweisrechtliche Folgen	190
8.7.2	Reputationsverlust	193
8.7.3	Maßnahmen von Aufsichtsbehörden	193
8.7.4	Sonstige Ansprüche und Rechte der Betroffenen	193
8.7.5	Strafrechtliche und ordnungswidrigkeitenrechtliche Folgen	194

8.1 Einleitung und aktuelle Entwicklung

8.1.1 Übererfüllung von Compliance-Bemühungen

Die zahlreichen und komplizierten rechtlichen Vorgaben zum ordnungsgemäßen Handeln von Geschäftsleitern und die mit ihrer Verletzung einhergehenden Risiken, auch einer persönlichen Haftung, bringen es mit sich, dass in einigen Fällen die im Unternehmen Verantwortlichen, möglicherweise aufgrund der Sorge, unzureichende Maßnahmen zu ergreifen, zur Übererfüllung des Ziels der Herstellung und Wahrung von Compliance im Unternehmen neigen. Übererfüllung im vorgenannten Sinne bezeichnet die ausschließliche Fokussierung auf das Ziel absoluter Compliance (häufig mit dem Fokus auf wenige besonders wichtige Themen, wie die Aufdeckung und Verhinderung von Korruption oder des Verrats von Geschäftsgeheimnissen), ohne bei der Auswahl der dazu erforderlichen Maßnahmen die möglichen Kollateralschäden in Form der Verletzung von Rechten Dritter zu berücksichtigen.

Das Phänomen der Übererfüllung wird durch die rasante technische Entwicklung begünstigt. Die lückenlose Überwachung verschiedener Bereiche des Unternehmens durch Videoaufnahmen oder spezielle Software zur Ausspähung der Tastenanschläge eines Mitarbeiters oder der aufgerufenen Internetseiten lässt sich ohne größeren finanziellen Aufwand realisieren. Im Ergebnis fordert der Gesetzgeber aber keine Compliance um jeden Preis. Vielmehr sind bei jeder Überwachungsmaßnahme die Interessen des Unternehmens gegen die Individualinteressen der betroffenen Arbeitnehmer abzuwägen. Der normative Rahmen dieser Abwägung ist im jeweiligen Einzelfall konkret zu bestimmen und hängt von der Art der Überwachungsmaßnahme, deren Intensität und den auf beiden Seiten betroffenen Rechtsgütern ab.¹

8.1.2 Arbeitnehmer- und Drittrechte als Schranken

Eine große Gruppe, der von einer Übererfüllung von Compliance Standards potenziell Betroffenen, sind die Mitarbeiter des Unternehmens, in dem die entsprechenden Maßnahmen ergriffen werden. Zugleich lassen sich Rechtsverletzungen bei Kunden denken. Auch sonstige Personen außerhalb des Unternehmens, etwa der unternehmensexterne Kommunikationspartner eines E-Mail-Austauschs, kommen in Betracht. Die Grenzen der Maßnahmen zur Herstellung und Wahrung von (bereichsspezifischer) Compliance im Unternehmen werden grundsätzlich durch die Rechte aller potenziell Betroffenen gebildet. Im Grunde müsste sich für die Beurteilung der Rechtmäßigkeit einer Maßnahme eine Differenzierung danach anschließen, mit welcher Intensität in die Rechte der jeweils

¹Vgl. zur Videoüberwachung im Unternehmen bspw. EGMR NZA 2019, 1697 oder BAG NJW 2017, 1193.

Betroffenen eingegriffen wird. Dies wird am Beispiel einer Vollüberwachung der E-Mail-Kommunikation eines Mitarbeiters deutlich.² Aus Sicht des von der Vollüberwachung betroffenen Mitarbeiters ist der Eingriff intensiv und in Abhängigkeit davon, ob die Maßnahme letztlich auf die Totalüberwachung des Mitarbeiters hinausläuft, beispielsweise, weil dieser seine gesamte Arbeitszeit mit der betrieblichen E-Mail-Kommunikation verbringen muss, möglicherweise (als Verletzung seiner Menschenwürde) sogar rechtswidrig. Aus Sicht des unternehmensexternen Kommunikationspartners liegt unter Umständen gar kein oder allenfalls ein sehr geringer Eingriff vor. Der unternehmensexterne Kommunikationspartner dürfte in aller Regel schon nicht unter dem Gesichtspunkt der Totalüberwachung betroffen sein, weil ihn die Vollüberwachung der E-Mail-Kommunikation nur in Form des Ausschnitts, der von ihm versendeten und an ihn gerichteten E-Mails betrifft.

In der Praxis ist der Grad der Berücksichtigung (falls diese überhaupt stattfindet) der grundsätzlich betroffenen Rechte allerdings weitestgehend durch die Frage geprägt, mit welcher Wahrscheinlichkeit der jeweilige Betroffene rechtliche Schritte (z. B. Anzeige, Klage etc.) gegen eine Maßnahme einleiten wird. Dieser Pragmatismus lässt sich beispielhaft an den in vielen Unternehmen eingeführten Lösungen zur E-Mail-Filterung verdeutlichen, die den rechtlichen Schutz des Absenders (als unwahrscheinliche Quelle rechtlicher Schritte gegen die E-Mail-Filterung) in der Regel ausblenden, obwohl beispielsweise das gemäß § 206 II Nr. 2 StGB geschützte Rechtsgut der Integrität des Telekommunikationsverkehrs auch die Interessen der Absender umfasst.

Im Folgenden sollen nicht alle denkbaren Drittrechte in ihrer Wirkung als Schranken der Compliance-Aktivitäten eines Unternehmens analysiert werden. Vielmehr sollen Schranken aufgezeigt und anhand häufiger Compliance-Maßnahmen illustriert werden, die sich aus ausgewählten Straftatbeständen und den Grundrechten der Mitarbeiter (z. B. deren Grundrechten aus den Art. 1, 2 und 10 GG) ergeben können. Auch wenn diese primär als Abwehrrechte gegen den Staat wirken, leiten Rechtsprechung und Lehre aus den Grundrechten einhellig auch eine Schutzwirkung für den zivilrechtlichen Verkehr ab.³ So mag die Totalüberwachung eines Mitarbeiters zwar der Optimierung der Prävention gegen Unterschlagung dienen, sie ist aber ein Verstoß gegen die Menschenwürde⁴ des Betroffenen und daher als Verletzung von Art. 1 GG unzulässig.⁵ Eine Schranke für Compli-

²Aktuell zu dem rechtswidrigen Versuch einer „Totalüberwachung“ mittels Keylogger BAG NZA 2017, 1327 m. Anm. Fuhlrott NZA 2017, 1308; siehe auch Vorinstanz LAG Hamm ZD 2017, 140; zur Überwachung von E-Mails beim Verbot der Privatnutzung EGMR CCZ 2016, 285; vgl. zu den Grenzen der Rundumüberwachung außerhalb des betrieblichen Arbeitsplatzes Kort RdA 2018, 24 (30 ff.).

³„Mittelbare Drittewirkung“ von Grundrechten, jedenfalls anerkannt seit BVerfGE 7, 198 (204) – Lüth-Urteil.

⁴BVerfG NJW 1984, 419 – Volkszählungsurteil – mit der Einführung des „Grundrechts auf informationelle Selbstbestimmung“; vgl. dazu als Vorläufer auch bereits BVerfGE 27, 1 (6) – Mikrozensus: Die zwangswise Registrierung und Katalogisierung von Menschen ist unzulässig; aktuelle Bedeutung v. a. im Arbeitsrecht und im Datenschutzrecht.

⁵Dazu im Einzelnen Rn. 87 ff.

ance Maßnahmen der IT-Sicherheit bildet **auch** das vom **BVerfG** in seinem Urteil vom 27. Februar 2008 entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (häufig „IT-Grundrecht“ genannt).⁶

Als Schranke ist **auch** das Datenschutzrecht zu nennen, das die durch die DS-GVO⁷ und – im Rahmen in dieser enthaltener „Öffnungsklauseln“ – einfachgesetzliche Ausgestaltung des Rechtsregimes zum Schutz des Rechts „auf Schutz personenbezogener Daten“ (siehe Art. 1 II DS-GVO) beziehungsweise auf informationelle Selbstbestimmung darstellt. Es bildet häufig den Gegenpol zur optimalen Compliance und wirkt als Begrenzung technisch wünschenswerter Maßnahmen. Die DS-GVO (Art. 6 I DS-GVO) lässt die Verarbeitung (Art. 4 Nr. 2 DS-GVO) personenbezogener Daten (Art. 4 Nr. 1 DS-GVO), gleich zu welchen Zwecken, nur zu, wenn sich ein Erlaubnistatbestand⁸ finden lässt. Art. 83 DS-GVO sowie §§ 41, 43 BDSG enthalten Sanktionsvorschriften für den Fall der rechtswidrigen Verarbeitung personenbezogener Daten.

Beschränkend auf Compliance-Maßnahmen wirken auch die Regelungen des Strafrechts, wie z. B. die §§ 201 ff. StGB, insbesondere § 206 StGB, über den Schutz der privaten Kommunikation gegen die unzulässige Mitteilung sowie das arbeitgeberseitige Löschen oder Unterdrücken von privaten E-Mails,⁹ die Regelungen des Telekommunikationsrechts, wie den Schutz des Fernmeldegeheimnisses gemäß § 3 TDDDG,¹⁰ ergänzen.

Ungeachtet der ihn schützenden Rechte darf der Arbeitnehmer die Überwachung, insbesondere wenn ihm das Installieren privater Software auf seinem Computer verboten ist, nicht mittels „Abwehrprogrammen“ unterbinden, weil dies seinerseits ein Vertragsverstoß wäre. Nicht abschließend geklärt ist, ob hier zugunsten des Arbeitnehmers eine Rechtfertigung unter dem Gesichtspunkt der „Notwehr“¹¹ oder der Selbsthilfe eingreifen kann.

⁶ BVerfG NJW 2008, 822. Für Ausführungen zum IT-Grundrecht vgl. unter Rn. 295 ff.

⁷ EU-Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG („DS-GVO“).

⁸ Vgl. Kühling/Buchner/Buchner/Petri DS-GVO Art. 6 Rn. 22 ff.

⁹ Die §§ 201 ff. StGB, insbesondere § 206 StGB, bleiben auch unter Geltung der DS-GVO anwendbar, weil es sich bei den betreffenden Vorschriften um Sanktionsnormen iSd Art. 84 DS-GVO handelt, wobei das Tatbestandsmerkmal „unbefugt“ aus § 26 Abs. 1 StGB im Lichte der DS-GVO ausgelegt werden muss (vgl. Koreng/Lachenmann/Bergt DatenschutzR-FormHdB D. III. 1; Kühling/Buchner/Bergt DS-GVO Art. 84, Rn. 26).

¹⁰ Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (im Folgenden TTDSG). Das Inkrafttreten der geplanten ePrivacy Verordnung (siehe dazu Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) kann (den Anwendungsbereich von) § 3 TTDSG betreffen (oder einschränken).

¹¹ Vgl. dazu Ronellenfitsch, DuD 2008, 110 (112).

Die Installation eines Anonymisierungsprogramms für das Surfen im Internet ist allerdings als bewusste Vereitelung des Kontrollrechts des Arbeitgebers und damit als Verstoß gegen das Rücksichtnahmegebot anzusehen.¹²

8.1.3 Eignung einer Maßnahme

Aufgrund der Vielfalt denkbarer Zwecke für die Vornahme einer bestimmten Maßnahme wird für die in diesem Kapitel dargestellten Beispiele typischer Compliance-Maßnahmen jeweils unterstellt, dass sie sich mit einer vertretbaren Begründung als Maßnahme gegen Compliance-Risiken eignen. Sollte dies im Einzelfall in der Praxis nicht der Fall sein, kann sich die Unzulässigkeit einer Maßnahme bereits aus diesem Umstand ergeben, beispielsweise unter dem Gesichtspunkt fehlender Erforderlichkeit gemäß § 26 I 1 BDSG zu Zweifeln an dieser Vorschrift siehe auch EuGH-Urteil vom 30. März 2023 – C-34/21), wenn eine Compliance-Maßnahme mit der Erhebung und Verarbeitung personenbezogener Daten von Mitarbeitern einhergeht, das intendierte Präventionsziel aber nicht erreichen kann. Dies lässt sich am Beispiel des E-Mail-Screening verdeutlichen, das bei einem Mitarbeiter durchgeführt werden soll, der unter dem Verdacht steht, den ausschließlich für die dienstliche Verwendung zur Verfügung stehenden Firmenwagen für private Zwecke einzusetzen. Von Ausnahmefällen abgesehen, wird sich der verbotswidrige Privatgebrauch des Firmenwagens nicht über die E-Mail-Korrespondenz des Betroffenen nachweisen lassen.

8.2 E-Mail-Filterung im Lichte von §§ 206, 303 a StGB

8.2.1 Auswirkungen von § 206 StGB im Bereich der E-Mail-Filterung

8.2.1.1 Geschütztes Rechtsgut

§ 206 StGB schützt das in Art. 10 GG verankerte Post- und Fernmeldegeheimnis sowie die Ungestörtheit des Telekommunikationsverkehrs.¹³ Gemäß § 206 I StGB ist die unbefugte Mitteilung von dem Post- oder Fernmeldegeheimnis unterliegenden Tatsachen an Dritte unzulässig, die dem Mitteilenden als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste („PTK-Unternehmen“) erbringt. Gemäß § 206 II StGB macht sich strafbar, wer eine Sendung, die einem PTK-Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft, eine Sendung, die einem PTK-Unternehmen zur Übermittlung anvertraut wurde, unterdrückt oder eine dieser Handlungen gestattet oder fördert.

¹² BAG NZA 2006, 980.

¹³ Beachtlich sind in diesem Zusammenhang auch weitere Normen, wie etwa Art. 8 EMRK, vgl. Dürig/Herzog/Scholz/Durner GG Art. 10 Rn. 36 ff.; Chandna-Hoppe NZA 2018, 614 (615).

8.2.1.2 Reichweite des Schutzes

§ 206 V StGB stellt klar, dass dem Postgeheimnis die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen und dem Fernmeldegeheimnis der Inhalt der Telekommunikation und ihre näheren Umstände (einschließlich der näheren Umstände erfolgloser Verbindungsversuche) unterliegen, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. § 206 III StGB erweitert die Strafbarkeit auf Personen, die die Aufsicht über ein PTK-Unternehmen wahrnehmen, die Post- oder Telekommunikationsdienstleistungen für dieses erbringen oder mit der Herstellung einer dem Betrieb eines PTK-Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

8.2.1.3 Eingriff in den Normalverlauf der Telekommunikation

Die Filterung von E-Mails ist heute ein absoluter Standard der Aktivitäten eines Unternehmens und in der Mehrheit der Unternehmen, in der einen oder anderen Ausprägung und Intensität, fester Bestandteil des Spektrums an durchgeföhrten Compliance Maßnahmen.¹⁴ Vereinfacht lassen sich zwei Ziele unterscheiden, die mit der E-Mail-Filterung erreicht werden sollen. Zum einen sollen unerwünschte E-Mails (d. h. Spam) und zum anderen E-Mails mit potenziell die Interessen des Unternehmens gefährdenden Inhalten (z. B. mit Viren¹⁵ behaftete E-Mail-Anhänge als Gefährdung der IT-Sicherheit des Unternehmens) herausgefiltert werden.¹⁶ Die Filterung von E-Mails ist von einem E-Mail-Screening¹⁷ abzugrenzen, bei dem E-Mails in Hinblick auf Fehlverhalten untersucht werden.¹⁸

Technisch betrachtet führt der Filterungsprozess entweder zur Verzögerung oder sogar zur Löschung der betroffenen E-Mails (oder zumindest des betroffenen E-Mail-Anhangs). Für die betroffenen E-Mails wird dadurch der Normalverlauf des Telekommunikationsvorgangs beeinflusst. Die Maßnahmen greifen, bevor die Nachrichten den Adressaten erreichen. Dies kann mit dem Schutzgut des § 206 II Nr. 2 StGB, der Ungestörtheit des Telekommunikationsverkehrs, kollidieren. Zugleich ist die Zulässigkeit der Privatnutzung der E-Mail-Software durch die Mitarbeiter eines Unternehmens, sei es durch ausdrückliche Gestattung oder infolge einer betrieblichen Übung, eher die Regel als die Ausnahme.¹⁹

¹⁴ Herrmann/Zeidler NZA 2017, 1499 (1500): bedeutende Rolle bei internen Untersuchungen; ausführlich auch Sauer, K&R 2008, 399; Sassenberg/Lammer, DuD 2008, 461; Braun/Spiegl, AiB 2008, 393.

¹⁵ Zu dem Begriff des Computervirus Auer-Reinsdorff/Conrad/Schmidt IT-R-HdB § 3 Rn. 269.

¹⁶ Vgl. zu einer Mustervereinbarung bezüglich der privaten Nutzung des Internetzugangs sowie der privaten Nutzung des E-Mail-Accounts, Koreng/Lachenmann/Bergt DatenschutzR-FormHdB D. III. 1.

¹⁷ Dazu ausführlich unten in Abschnitt 4.

¹⁸ Kramer/Schulze/Zumkley, IT-Arbeitsrecht, Rn. 1190.

¹⁹ Sozialadäquanz dürfte noch nicht anzunehmen sein; so aber das LAG Rheinland-Pfalz MMR 2005, 176.

8.2.1.4 Taugliche Täter

Taugliche Täter im Sinne von § 206 StGB sind „Inhaber oder Beschäftigte eines Unternehmens“, das sich „geschäftsmäßig mit der Erbringung von Telekommunikationsdienstleistungen befasst“. Die Reichweite dieses Tatbestandsmerkmals ist somit nicht auf Telekommunikationsdienstanbieter im eigentlichen Sinn beschränkt, sondern umfasst jede Person, die das Fernmeldegeheimnis zu wahren hat.²⁰ Zu den relevanten Unternehmen, die hinsichtlich der Zulassung der Privatnutzung als „Provider“ von Telekommunikationsdiensten zu behandeln sind²¹ und damit zugleich das Schutzgut der Ungestörtheit des Telekommunikationsverkehrs zu wahren haben, zählen (nach zunehmend bestrittener Auffassung) auch solche, die ihren Mitarbeitern die Privatnutzung von E-Mail gestattet haben²² oder in denen sich die Zulässigkeit der Privatnutzung aus einer betrieblichen Übung²³ ergibt.

Diese werden dann unabhängig davon, ob ein Entgelt gefordert wird oder nicht, zum Anbieter von Telekommunikationsdiensten nach §§ 3 II Nr. 2 TDDDG, 3 Nr. 61 TKG und damit zum tauglichen Täter i. S. v. § 206 StGB.²⁴ Im Hinblick auf den privaten E-Mails gemäß § 206 II Nr. 2 StGB zuteilwerdenden Schutz haben sie im eigenen Interesse Vorkehrungen zur Wahrung des § 3 TDDDG dergestalt zu treffen, dass sich Daten aus privater und dienstlicher Nutzung deutlich trennen lassen.²⁵ Dies ist – wie noch zu zeigen sein wird²⁶ – insbesondere für das E-Mail-Screening von Bedeutung. Der relevante Unternehmensbegriff ist nicht auf wirtschaftlich tätige Unternehmen beschränkt. Auch Hochschulen, die ihre Server Privatpersonen zur Verfügung stellen, werden von der Strafnorm erfasst.²⁷ Zu beachten ist, dass tauglicher Täter i. S. v. § 206 StGB neben dem die Privatnutzung gestattenden Arbeitgeber selbst zusätzlich der vom Arbeitgeber beauftragte Mitarbeiter ist.²⁸

Auch die Führungsebene des betroffenen Unternehmens bleibt nicht unberührt. Gem. § 14 StGB ist jeder Vertretungsberechtigte eines Unternehmens unabhängig von einem eigenen Eingriff in das Fernmeldegeheimnis strafbar, auch wenn er nach der betrieblichen

²⁰ Voraussetzung ist, dass die E-Mail noch dem Fernmeldegeheimnis unterfällt (vgl. dazu BVerfG NJW 2009, 2431, BVerfG NJW 2006, 976), sich also auf dem Übertragungsweg befindet, siehe auch Dürig/Herzog/Scholz/Durner GG Art. 10 Rn. 124 ff.

²¹ Vgl. dazu Schmidl, MMR 2005, 343 (344).

²² Zur privaten E-Mail-Nutzung am Arbeitsplatz Brink/Schwab ArbRAktuell 2018, 111 (113 f.); Kramer/Hoppe IT-ArbR Rn. 255 ff.; auch Universitäten: OLG Karlsruhe MMR 2005, 178.

²³ Zum Meinungsstand zu betrieblichen Übung Thüsing Beschäftigtendatenschutz und Compliance § 3 Rn. 66 ff.; siehe auch Brink/Schwab ArbRAktuell 2018, 111 (113).

²⁴ Schönke/Schröder/Eisele StGB § 206 Rn. 8a mit weiteren Nachweisen; kritisch auch unter Gelung des TDDDG Wünschelbaum NJW 2022, 1561 (1561 f.).

²⁵ Nach Koch, NZA 2008, 911 (913), strahlt das Fernmeldegeheimnis bei fehlender Trennung auf die betrieblichen Daten aus.

²⁶ Siehe Rn. 54 ff.

²⁷ OLG Karlsruhe MMR 2005, 178.

²⁸ Vgl. Schönke/Schröder/Eisele StGB, § 206 Rn. 9.

Aufgabenverteilung nicht unmittelbar zuständig ist. Management und leitende Angestellte, also die Geschäftsführung, sowie Systemadministratoren laufen bei rechtswidriger Filterung daher ebenfalls Gefahr, der Strafverfolgung ausgesetzt zu sein.

8.2.1.5 E-Mail als taugliches Tatobjekt

Die E-Mail-Filterung ist in aller Regel ein automatisierter Prozess, der nicht mit der Kenntnisnahme von Inhaltsdaten und deren Weitergabe an Dritte einhergeht, sodass in der Regel kein Fall von § 206 I StGB vorliegt. Die E-Mail-Filterung wird von der (noch) herrschenden Meinung wegen des Erfordernisses der „verschlossenen“ Sendung auch nicht an § 206 II Nr. 1 StGB gemessen. Eine Strafbarkeit nach § 206 II Nr. 2 StGB ist allerdings naheliegend. E-Mails kommen als Tatobjekt im Umkehrschluss zu § 206 II Nr. 1 StGB, der die bei E-Mails abzulehnende Verschlossenheit²⁹ der betroffenen Sendung erfordert, gemäß § 206 II Nr. 2 StGB gerade wegen des Verzichts auf das Tatbestandsmerkmal der Verschlossenheit in Betracht.³⁰

8.2.1.6 Ausfiltern und Verzögern als Tathandlung

Die Tathandlung des Unterdrückens umfasst sowohl die Löschung als auch die Verzögerung (sog. Quarantäne-Lösung)³¹ eingehender E-Mails; ein (möglicherweise, z. B. wenn der Arbeitgeber einen Eingriff in den Fernmeldeverkehr nicht einmal für möglich hält, nicht vorsätzliches) Unterdrücken liegt auch bei der Blockierung von E-Mails vor, da diese regelmäßig anhand des gleichfalls vom Fernmeldegeheimnis geschützten³² Headers einer E-Mail erfolgt, die bereits den Server des Adressaten erreicht hat. Es kommt nicht darauf an, ob jeweils einzeln manuell oder aufgrund vorab definierter Routinen automatisch gelöscht, zurückgehalten oder blockiert wird. In das Schutzgut von § 206 II Nr. 2 StGB, die Ungestörtheit des Telekommunikationsverkehrs, wird jedenfalls eingegriffen. Das **OLG Karlsruhe** führt dazu in einer Entscheidung vom 10. Januar 2005 aus:³³

„Ein Unterdrücken der E-Mail ist dann anzunehmen, wenn durch technische Eingriffe in den technischen Vorgang des Aussendens, Übermittlens oder Empfangens von Nachrichten mittels TK-Anlagen verhindert wird, dass die Nachricht ihr Ziel vollständig oder unver-

²⁹ Auch verschlüsselte E-Mails sind nicht in diesem Sinn „verschlossen“, vgl. Schönke/Schröder/Eisele, StGB, § 206 Rn. 17.

³⁰ Ursprünglich wurde § 206 StGB zwar für Sendungen der damaligen Bundespost (§ 354 StGB a. F.) formuliert, wie sich aber aus dem Schutzzweck der Norm ergibt, sollen sämtliche „Sendungen“, die dem Fernmeldegeheimnis unterliegen, von der Norm erfasst werden. Auf die Körperlichkeit des übermittelten Nachrichtenträgers kommt es daher nicht an. Vgl. dazu Schönke/Schröder/Eisele, StGB, § 206 Rn. 20.

³¹ Physische Umleitung der E-Mail auf vom übrigen System getrennte (externe oder interne) Server. Ein Unterdrücken in Form der Verzögerung liegt hierin nur dann nicht, wenn der Adressat auf die gesonderten Server jederzeit unmittelbaren Zugriff hat; vgl. dazu Hoeren, NJW 2004, 3513 (3517).

³² Näher bei Heidrich/Tschoepe, MMR 2004, 75.

³³ OLG Karlsruhe, MMR 2005, 178 (180).

stümmelt erreicht (...). Soweit auch die Auffassung vertreten wird, dass ein Unterdrücken bei einer E-Mail nicht das Zerstören oder Beschädigen der Nachricht, also ihr Löschen, Verstümmeln oder Verkürzen ist, sondern nur ihr vollständiges oder vorübergehendes Zurückhalten oder Umleiten an eine andere Adresse (...), greift dies zu kurz; denn letztlich kann es keinen Unterschied machen, wie verhindert wird, dass die Nachricht ihren Empfänger erreicht, nämlich ob dies durch Zurückhalten oder Umleiten der E-Mail oder durch deren Löschung oder sonstige Verstümmelung geschieht. (...) Das Tatbestandsmerkmal „Unterdrücken“ wird jedenfalls durch eine Ausfilterung der E-Mail erreicht. In diesem Fall findet die Weiterleitung, also das Übermitteln der eingehenden Mail vom Mailserver an den einzelnen Klienten nicht statt (...).“

Die Bejahung des Unterdrückens im Falle des Löschens einer im Zustand des Transports befindlichen E-Mail liegt auf der Hand. Bereits die erhebliche Verzögerung des Transports ist aber eine inkriminierte erhebliche Störung des Telekommunikationsverkehrs und reicht als tatbestandliches Unterdrücken aus, weil § 206 StGB gerade die Integrität des Telekommunikationsverkehrs schützt. Festzuhalten bleibt, dass es in allen Varianten des Unterdrückens nicht darauf ankommt, ob sich der Arbeitgeber Kenntnis vom Inhalt der E-Mails verschafft hat.³⁴

8.2.1.7 Zeitliche Grenze der Tatbestandsverwirklichung

aa) Schutz während der Übermittlung Mit der Feststellung des Schutzes einer im Zustand des Transports befindlichen privaten E-Mail gegen das Unterdrücken in den Ausprägungen des Löschens und Verzögerns ist der Schutzbereich von § 206 II Nr. 2 StGB für das „typische“ Filtern von E-Mails beschrieben. Der Eingriff in den Telekommunikationsverkehr erfolgt in aller Regel, bevor die E-Mail den designierten Empfänger überhaupt erreicht hat. Die Frage, ob der Telekommunikationsverkehr schon abgeschlossen und die Anwendbarkeit von § 206 II Nr. 2 StGB damit beendet sein könnte, stellt sich mithin nicht. Wie wirkt sich § 206 II Nr. 2 StGB aber aus, wenn eine E-Mail nach Erreichen des Adressaten vom Telekommunikationsdienstanbieter (das kann gegebenenfalls auch der Arbeitgeber sein) gelöscht wird? Für die Beantwortung dieser Frage kommt es darauf an, wie lange bei einer privaten E-Mail davon auszugehen ist, dass sie sich im Zustand der Telekommunikation befindet. Nur so lange kann ein Unterdrücken gemäß § 206 II Nr. 2 StGB vorliegen und damit in den (laufenden) Telekommunikationsverkehr eingegriffen werden.

bb) Schutz bis zum Eingang im Herrschaftsbereich des Empfängers Für die Abgrenzung zwischen Telekommunikation und dem nach deren Abschluss folgenden Zustand kann auf zwei Entscheidungen des **BVerfG** zurückgegriffen werden, die für die Ermittlung des genauen zeitlichen Anwendungsbereichs von § 206 II Nr. 2 StGB maßgeblich sind. Die in den Grundrechten zum Ausdruck kommenden verfassungsrechtlichen Wertentscheidungen sind über zivilrechtliche Generalklauseln auch im Arbeitsverhältnis zu beachten.³⁵

³⁴ Zum Tatbestandsmerkmal des Unterdrückens vgl. Schönke/Schröder/Eisele, StGB, § 206 Rn. 20.

³⁵ BVerfG, NJW 2003, 2815.

In der Entscheidung des **BVerfG** vom 2.3.2006³⁶ zur zeitlichen Reichweite des über das Fernmeldegeheimnis vermittelten Schutzes heißt es zum zeitlichen Anwendungsbereich von Art. 10 GG:

„Die nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Verbindungsdaten werden nicht durch Art. 10 I GG, sondern durch das Recht auf informationelle Selbstbestimmung (Art. 2 I in Verbindung mit Art. 1 I GG) und gegebenenfalls durch Art. 13 I GG geschützt.“

Diese Abgrenzung wird durch eine Entscheidung des **BVerfG** vom 16. Juni 2009 bestätigt.³⁷

„Der Grundrechtsschutz erstreckt sich nicht auf die außerhalb eines laufenden Kommunikationsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Kommunikation. Der Schutz des Fernmeldegeheimnisses endet insoweit in dem Moment, in dem die E-Mail beim Empfänger angekommen und der Übertragungsvorgang beendet ist (...).“

Vereinfacht lässt sich den beiden Entscheidungen entnehmen, dass der durch das Fernmeldegeheimnis vermittelte Schutz erst dann beendet ist, wenn der Telekommunikationsvorgang beendet ist. Dies setzt voraus, dass eine private E-Mail beim Empfänger angekommen und in seinem Herrschaftsbereich gespeichert ist. Würde man diese Grundsätze auf den Arbeitgeber als Provider übertragen, so bedeutete dies für die Anwendungsgrenze von § 206 II Nr. 2 StGB, dass es in zeitlicher Hinsicht nicht schon auf das Eintreffen der privaten E-Mail in der IT-Infrastruktur des Unternehmens (d. h. im informationstechnologisch vom Unternehmen beherrschten Bereich) ankommen kann, weil nicht dieses, sondern der betroffene Arbeitnehmer als „Empfänger“ anzusehen ist. Zweifel an der genauen Lage der zeitlichen Zäsur für den Schutz durch das Fernmeldegeheimnis ergeben sich aber daraus, dass das **BVerfG** für die Beendigung des Schutzes durch das Fernmeldegeheimnis als negatives Abgrenzungsmerkmal zusätzlich fordert, dass die „**Inhalte und Umstände der Kommunikation**“ noch nicht im „**Herrschaftsbereich des Kommunikationsteilnehmers**“ gespeichert wurden. Positiv formuliert ist für die Beendigung der Telekommunikation und damit zugleich für die zeitliche Beendigung des über das Fernmeldegeheimnis vermittelten Schutzes somit erforderlich, dass die private E-Mail beim Empfänger (d. h. in seinem Postfach) angekommen ist und von diesem in seinem Herrschaftsbereich gespeichert wurde. Erst zu diesem Zeitpunkt³⁸ würde auch der Schutzbereich von § 206 II

³⁶ BVerfG, NJW 2006, 976.

³⁷ BVerfG, NJW 2009, 2431.

³⁸ Es ist nicht damit zu rechnen, dass für die zeitliche Reichweite von § 206 II Nr. 2 StGB auf das Eintreffen der E-Mail beim Empfänger und damit auf eine frühere Zäsur als für die zeitliche Reichweite von § 206 I StGB abgestellt wird, auch wenn unterschiedliche Schutzgüter (§ 206 I StGB schützt das Fernmeldegeheimnis und § 206 II Nr. 2 StGB die Integrität des Telekommunikationsverkehrs) betroffen sind. Dies dürfte daraus zu schließen sein, dass das BVerfG ausdrücklich keine rein technische Betrachtung zugrunde legen und das Fernmeldegeheimnis nicht auf „bewegte“ Daten beschränken wollte, vgl. BVerfG NJW 2009, 2431 (2432).

Nr. 2 StGB enden, etwa bezüglich des Löschens privater E-Mails durch den Arbeitgeber. Für das Löschen von privaten E-Mails durch den Arbeitgeber bleibt allerdings noch § 303 a StGB relevant.³⁹

Die durch das zusätzliche Kriterium des Abspeicherns im „Herrschungsbereich des Kommunikationsteilnehmers“ wirkte Verschiebung der zeitlichen Anwendungsgrenze des § 206 II Nr. 2 StGB wäre für die übliche E-Mail-Filterung im Unternehmen nicht relevant, weil die E-Mail-Filterung typischerweise bereits unmittelbar nach dem Eintritt einer E-Mail in die IT-Infrastruktur des Unternehmens und damit jedenfalls vor dem Ein treffen beim „Empfänger“ erfolgt,⁴⁰ falls die Filterung nicht sogar schon zuvor durch einen externen Dienstleister vorgenommen wurde. Die Frage, ab wann der „Herrschungsbereich des Kommunikationsteilnehmers“ (d. h. des Arbeitnehmers) erreicht ist, stellt sich in diesen Fällen regelmäßig nicht. Für den zumindest theoretisch denkbaren Fall, dass eine im Postfach des Adressaten auf dem E-Mail-Server des Unternehmens abgespeicherte (d. h. beim Empfänger bereits angekommene) E-Mail vom Arbeitgeber gelöscht wird,⁴¹ würde sich bei Anwendung der Grundsätze der Entscheidung vom 16. Juni 2009 auf das Arbeitsverhältnis aber die Frage stellen, ob noch ein Unterdrücken einer im Zustande der Telekommunikation befindlichen Nachricht vorliegt. Zunächst hatte es das **BVerfG** ausdrücklich offengelassen, ob in den Schutzbereich des Fernmeldegeheimnisses (Art. 10 GG) eingegriffen wird (weil noch ein Telekommunikationsvorgang vorliegt), wenn die Ermittlungsbehörden die auf dem Server eines Providers gespeicherten E-Mails kopieren und auswerten.⁴² Mit dem Leitsatz der Entscheidung vom 16. Juni 2009 (**BVerfG** – 2 BvR 902/06) beantwortete das **BVerfG** diese Frage wie folgt:⁴³

³⁹Vgl. hierzu Schönke/Schröder/Hecker, StGB, § 303 a Rn. 4 f.

⁴⁰Vgl. hierzu bspw. den Sachverhalt der Entscheidung des VG Karlsruhe MMR 2008, 362.

⁴¹Gemäß Schönke/Schröder/Eisele, StGB, § 206 Rn. 20b, erfüllt das Löschen einer E-Mail den Tatbestand des Unterdrückens.

⁴²Vgl. BVerfG, MMR 2007, 169.

⁴³Der BGH NJW 2009, 1828 hatte dies noch anders gesehen und festgestellt: „Die Verwertung von E-Mails des Angeklagten, welche im Ermittlungsverfahren beschlagnahmt wurden, wobei alle in dem jeweiligen E-Mail-Postfach des Angeklagten abgespeicherten – gelesenen und noch nicht gelesenen – E-Mails betroffen waren und erfasst wurden, begegnet letztlich keinen durchgreifenden rechtlichen Bedenken. (...) Jedoch bedurfte es für die im Postfach beim E-Mail-Provider abgespeicherten E-Mails, ob bereits gelesen oder noch ungelesen, auch nicht der Voraussetzungen des § 100 a StPO, denn während der möglicherweise auch nur Sekundenbruchteile andauernden Speicherung in der Datenbank des Mail-Providers ist kein Telekommunikationsvorgang (mehr) gegeben (...). Vielmehr ist die Beschlagnahme von E-Mails bei einem E-Mail-Provider, welche dort bis zu einem ersten oder weiteren Aufruf abgespeichert sind, auch unter Berücksichtigung des heutigen Kommunikationsverhaltens in jeder Hinsicht vergleichbar mit der Beschlagnahme anderer Mitteilungen, welche sich zumindest vorübergehend bei einem Post- oder Telekommunikationsdienstleister befinden, bspw. von Telegrammen, welche gleichfalls auf dem Telekommunikationsweg dorthin übermittelt wurden. Daher können beim Provider gespeicherte, eingegangene oder zwischen gespeicherte, E-Mails – auch ohne spezifische gesetzliche Regelung – jedenfalls unter den Voraussetzungen des § 99 StPO beschlagnahmt werden (...).“.

„Die Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers sind am Grundrecht auf Gewährleistung des Fernmeldegeheimnisses aus Art. 10 I GG zu messen. §§ 94 ff. StPO genügen den verfassungsrechtlichen Anforderungen, die an eine gesetzliche Ermächtigung für solche Eingriffe in das Fernmeldegeheimnis zu stellen sind.“

Diese Entscheidung des **BVerfG** behandelt zwar nicht das Löschen von E-Mails und damit Eingriffe in die durch § 206 II Nr. StGB geschützte Integrität des Telekommunikationsverkehrs, sie kann sich aber in zeitlicher Hinsicht auf die Bestimmung der tauglichen Tatobjekte gemäß § 206 StGB im Unternehmen auswirken, wenn ihr zu entnehmen ist, dass auf den Servern des Arbeitgebers gespeicherte private E-Mails dauerhaft (oder zumindest auch noch nach deren Eintreffen beim Empfänger) durch das Fernmeldegeheimnis geschützt sind.

cc) Arbeitgeber als Provider? Es ist noch immer streitig,⁴⁴ ob die Entscheidung des **BVerfG** vom 16. Juni 2009 (**BVerfG** – 2 BvR 902/06) auf Arbeitgeber als „Provider“ von Telekommunikationsdiensten übertragen werden muss (so etwa die Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mails und anderen Internetdiensten am Arbeitsplatz, 4:⁴⁵ „Wenn der Arbeitgeber den Beschäftigten auch die private Nutzung von Internet und/oder des betrieblichen E-Mail-Postfaches erlaubt, ist zusätzlich das Telekommunikationsgesetz (TKG) bzw. das TDDG zu beachten. Nach Auffassung der Aufsichtsbehörden ist der Arbeitgeber in diesem Fall Telekommunikationsdienste- bzw. Telemediendienste-Anbieter“. Dies hätte zur Folge, dass im E-Mail-System des Arbeitgebers serverseitig gespeicherte und dem Arbeitnehmer in aller Regel nur über eine Netzwerkverbindung zugängliche private E-Mails dem Fernmeldegeheimnis unterliegen, so lange diese vom Arbeitnehmer auf dem Server des Arbeitgebers nicht gelöscht oder ohne Zurücklassen einer Kopie auf einen privaten Datenspeicher verschoben wurden. Diese Unternehmen betreffende Schlussfolgerung könnte aus folgenden Aussagen⁴⁶ in der Entscheidung des **BVerfG** vom 16. Juni 2009 abzuleiten sein:

„Demgegenüber ist der zugangsgesicherte Kommunikationsinhalt in einem E-Mail-Postfach, auf das der Nutzer nur über eine Internetverbindung zugreifen kann, durch Art. 10 I GG geschützt (...). Das Fernmeldegeheimnis knüpft an das Kommunikationsmedium an und will jenen Gefahren für die Vertraulichkeit begegnen, die sich gerade aus der Verwendung dieses Mediums ergeben, das einem staatlichem Zugriff leichter ausgesetzt ist als die direkte Kommunikation unter Anwesenden (...). Die auf dem Mailserver des Providers

⁴⁴ Eine Providereigenschaft des Arbeitgebers bejahend Sassenberger/Mantz BB 2013, 889 (891); Hoppe/Braun MMR 2010, 80 (81); kritisch zuletzt Wünschelbaum, NJW 2022, 1562 (1562 f.); kritisch auch Scheben/Klos CCZ 2013, 88 (90 f.); Fülbier/Splittgerber NJW 2012, 1995 (1999); vgl. auch aus der Rechtsprechung LAG Berlin-Brandenburg NZA-RR 2011, 342.

⁴⁵ DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, vom Januar 2016, https://www.datenschutzkonferenz-online.de/media/oh/201601_oh_email_und_internetdienste.pdf (aufgerufen am 17.07.2024).

⁴⁶ BVerfG NJW 2009, 2431 (2432).

vorhandenen E-Mails sind nicht im Herrschaftsbereich des Kommunikationsteilnehmers, sondern des Providers gespeichert. Sie befinden sich nicht auf in den Räumen des Nutzers verwahrten oder in seinen Endgeräten installierten Datenträgern. Der Nutzer kann sie für sich auf einem Bildschirm nur lesbar machen, indem er eine Internetverbindung zum Mailserver des Providers herstellt. Zwar kann der Nutzer versuchen, die auf dem Mailserver gespeicherten E-Mails durch Zugangssicherungen – etwa durch Verwendung eines Passworts – vor einem ungewollten Zugriff Dritter zu schützen. Der Provider und damit auch die Ermittlungsbehörden bleiben jedoch weiterhin in der Lage, jederzeit auf die auf dem Mailserver gespeicherten E-Mails zuzugreifen. Der Kommunikationsteilnehmer hat keine technische Möglichkeit, die Weitergabe der E-Mails durch den Provider zu verhindern. Dieser technisch bedingte Mangel an Beherrschbarkeit begründet die besondere Schutzbedürftigkeit durch das Fernmeldegeheimnis. Dies gilt unabhängig davon, ob eine E-Mail auf dem Mailserver des Providers zwischen- oder endgespeichert ist. In beiden Fällen ist der Nutzer gleichermaßen schutzbedürftig, weil sie sich hinsichtlich der faktischen Herrschaftsverhältnisse nicht unterscheiden.“

Der nahe liegende Einwand gegen die Erstreckung des Fernmeldegeheimnisses auf „ruhende Daten in Form von E-Mails“ (das könnten auch private E-Mails sein, die bereits im Postfach des Empfängers auf dem Server des Arbeitgebers als „Provider“ angekommen sind), wonach es sich bei solchen E-Mails nicht mehr um Telekommunikation handeln, weil der Transportvorgang spätestens mit der Abspeicherung der E-Mails in den Posteingängen (im Fall eines Arbeitgebers – den Posteingängen der jeweiligen Mitarbeiter) abgeschlossen⁴⁷ sei und damit nur noch „ruhende“ Daten vorlägen, wurde vom BVerfG in der Entscheidung vom 16. Juni 2009 (2 BvR 902/06) mit folgenden Aussagen entkräftet:⁴⁸

„Dem Schutz der auf dem Mailserver des Providers gespeicherten E-Mails durch Art. 10 I GG steht nicht entgegen, dass während der Zeitspanne, während deren die E-Mails auf dem Mailserver des Providers „ruhen“, ein Telekommunikationsvorgang in einem dynamischen Sinne nicht stattfindet. Zwar definiert § 3 Nr. 22 TKG „Telekommunikation“ als den technischen Vorgang des Aussendens, Übermittlens und Empfangens von Signalen mittels Telekommunikationsanlagen und bezieht sich nicht ausdrücklich auch auf statische Zustände. Art. 10 I GG folgt indes nicht dem rein technischen Telekommunikationsbegriff des Telekommunikationsgesetzes, sondern knüpft an den Grundrechtsträger und dessen Schutzbedürftigkeit aufgrund der Einschaltung Dritter in den Kommunikationsvorgang an (...).“

Die dauerhafte Speicherung von E-Mails beim Provider – und analog beim Arbeitgeber als „Provider“ – wegen der großen kostenfreien Speicherkapazitäten, der regelmäßigen Datensicherung und aus Gründen der jederzeitigen Verfügbarkeit (anders als beim Herunterladen von E-Mails auf ein bestimmtes Endgerät bei gleichzeitiger Löschung vom Server), dürfte inzwischen ein übliches Nutzungsbild von privaten wie dienstlichen E-Mail-Systemen darstellen. Gegen die Erstreckung des Fernmeldegeheimnisses auf pri-

⁴⁷Vgl. zu möglichen Gegenargumenten gegen die Erstreckung von Art. 10 GG auf beim Provider gespeicherte E-Mails auch BVerfG, NJW 2009, 2431 (2432).

⁴⁸BVerfG, NJW 2009, 2431.

vate E-Mails auf einem Server des Arbeitgebers als „Provider“ wäre daher weiterhin der Einwand denkbar, dass jedenfalls dann keine Telekommunikation mehr vorliegen kann, wenn der Empfänger die an ihn gerichteten E-Mails bereits zur Kenntnis genommen und von diesen eine „Offline-Kopie“⁴⁹ auf dem von ihm benutzten Rechner (und damit in seinem „Herrschungsbereich“) angefertigt hat.⁵⁰ Zudem könnte argumentiert werden, der Arbeitnehmer benutze die Speicherkapazitäten beim Provider (und analog diejenigen beim Arbeitgeber) als zu seinem „Herrschungsbereich“ gehörig und im vollen Bewusstsein der im Vergleich zu eigenen Speichermedien größeren Anfälligkeit gegen die Zugriffe von unberechtigten Dritten, sodass in Anlehnung an die vom BVerfG in seiner Entscheidung vom 2. März 2006 (BVerfG – 2 BvR 2099/04) getroffenen Unterscheidung „nur“ noch der Schutzbereich des Rechts auf informationelle Selbstbestimmung einschlägig sei. Auch diese Einwände dürften aufgrund folgender Ausführungen⁵¹ in der Entscheidung des BVerfG vom 16. Juni 2009 nicht greifen:

„Der Schutz der auf dem Mailserver des Providers gespeicherten E-Mails durch das Fernmeldegeheimnis entfällt auch nicht dadurch, dass ihr Inhalt oder Eingang vom Empfänger möglicherweise schon zur Kenntnis genommen worden ist. Die Reichweite des Schutzes von Art. 10 I GG endet nicht in jedem Fall mit der Kenntnisnahme des Kommunikationsinhalts durch den Empfänger. Ob Art. 10 I GG Schutz vor Zugriffen bietet, ist mit Blick auf den Zweck der Freiheitsverbürgung unter Berücksichtigung der spezifischen Gefährdungslage zu bestimmen (...). Die spezifische Gefährdungslage und der Zweck der Freiheitsverbürgung von Art. 10 I GG bestehen auch dann weiter, wenn die E-Mails nach Kenntnisnahme beim Provider gespeichert bleiben. Durch die Endspeicherung wird der von Art. 10 I GG zuvor der geschützte Kommunikationsinhalt infolge der Nutzung eines bestimmten Kommunikationsmediums auf einem vom Kommunikationsmittler bereit gestellten Speicherplatz in einer von keinem Kommunikationsteilnehmer beherrschbaren Sphäre abgelegt. Weder bei einer Zwischen- noch bei einer Endspeicherung der E-Mails auf dem Mailserver des Providers ist dessen Tätigkeit beendet; der Provider bleibt dauerhaft in die weitere E-Mail-Verwaltung auf seinem Mailserver eingeschaltet.“

Auch wenn das Bundesverfassungsgericht sich in der zitierten Entscheidung nicht ausdrücklich mit dem Fall befasst hat, dass der Nutzer auf dem von ihm benutzten Rechner eine „Offline-Kopie“ seiner E-Mails angefertigt hat, ist davon auszugehen, dass es zumindest die weiter auf dem Server gespeicherten privaten E-Mails des Arbeitnehmers nicht alleine wegen der Existenz einer parallelen „Offline-Kopie“ aus dem Schutzbereich

⁴⁹Viele Unternehmen richten die auf den Laptops und PC-Systemen ihrer Mitarbeiter installierten E-Mail-Systeme dergestalt ein, dass auf diesen eine netzwerkunabhängig verfügbare Kopie der im E-Mail-System vorhandenen E-Mails (inkl. Anlagen) verfügbar ist, die inhaltlich auf dem Stand der letzten Verbindung zum E-Mail-Server ist. Auf diese Weise ist das Lesen und Bearbeiten von E-Mails auch ohne Verbindung zum E-Mail-Server des Unternehmens möglich. Die auf diese Weise „offline“ verfügbaren E-Mails werden auf dem Mail-Server in der Regel nicht gelöscht.

⁵⁰Vgl. dazu auch BVerfG, NJW 2009, 2431.

⁵¹BVerfG, NJW 2009, 2431.

des Fernmeldegeheimnisses ausnehmen würde.⁵² Auch insoweit greift der Gedanke (siehe oben), dass der Schutz der auf dem Mailserver des Providers gespeicherten E-Mails durch das Fernmeldegeheimnis nicht dadurch entfällt, dass „ihr Inhalt oder Eingang vom Empfänger möglicherweise schon zur Kenntnis genommen worden ist“ und dass der Provider (gegebenenfalls gleichzustellen mit dem Arbeitgeber) „dauerhaft in die weitere E-Mail-Verwaltung auf seinem Mailserver eingeschaltet bleibt“ – an letzterem ändert insbesondere die Anfertigung einer „Offline-Kopie“ nichts.

Für die getrennt zu betrachtende „Offline-Kopie“ kann etwas anderes gelten, wenn diese in einer allein vom Arbeitnehmer beherrschten Sphäre abgespeichert wurde. Es ist eine Frage des Einzelfalls, ob der vom Arbeitnehmer benutzte Rechner einen solchen „Herrschaftsbereich“ darstellt oder nicht. Dies könnte dann zweifelhaft sein, wenn von dem benutzten Rechner seitens des Arbeitgebers regelmäßig und automatisiert vollständige Back-up-Kopien angefertigt werden oder für den Rechner dieselben Zugriffsrechte des Arbeitgebers bestehen, wie für den E-Mail-Server des Arbeitgebers.

Als Folge der oben dargestellten Erwägungen wären private E-Mails auf dem E-Mail-Server des Arbeitgebers dem Fernmeldegeheimnis zu unterstellen und würde der Schutz des Fernmeldegeheimnisses in zeitlicher Hinsicht weder durch die Einsichtnahme der Adressaten mittels der auf ihren Rechnern installierten E-Mail-Software im Wege eines einer Verbindung zum Server voraussetzenden Online-Zugriffs noch durch das Herunterladen der E-Mails auf die Rechner der jeweiligen Mitarbeiter zum Zweck der Anfertigung einer „Offline-Kopie“ beendet, weil auch hier üblicherweise eine Kopie der E-Mails auf dem Server verbleibt. Erst die arbeitnehmerseitige Löschung der privaten E-Mails oder ihre Verbringung in den Herrschaftsbereich des Arbeitnehmers (falls das Löschen oder die Verbringung wegen der Datensicherungsmaßnahmen des Arbeitgebers überhaupt noch möglich sind) würde

- den Schutz durch das Fernmeldegeheimnis,
- den Vorgang der Telekommunikation und damit zugleich
- die Anwendbarkeit von § 206 I und § 206 II Nr. 2 StGB

zeitlich beenden. Die auf private E-Mails bezogenen Maßnahmen der E-Mail-Filterung und des E-Mail-Screening,⁵³ sowohl auf den Servern des Unternehmens als auch in den Postfächern der Mitarbeiter bis zur im vorherigen Satz beschriebenen Zäsur, wäre an den Maßstäben von § 206 StGB zu messen.

⁵²In diese Richtung geht noch eine Entscheidung des VGH Kassel NJW 2009, 2470 ff.: „Gestattet ein Arbeitgeber seinen Mitarbeitern, den Arbeitsplatzrechner auch zum privaten E-Mail-Verkehr zu nutzen und E-Mails, die von den Mitarbeitern nicht unmittelbar nach Eingang oder Versendung gelöscht werden, im Posteingang oder -ausgang zu belassen oder in anderen auf lokalen Rechnern oder zentral gesicherten Verzeichnissen des Systems abzuspeichern, unterliegt der Zugriff des Arbeitgebers oder Dritter auf diese Datenbestände nicht den rechtlichen Beschränkungen des Fernmeldegeheimnisses. Schutz gegen die rechtswidrige Auswertung dieser erst nach Beendigung des Übertragungsvorgangs angelegten Daten wird durch die Grundrechte auf informationelle Selbstbestimmung bzw. auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gewährt“.

⁵³Dazu Rn. 54 ff.

dd) Offene Fragen Die zeitliche Erstreckung des Schutzes für private E-Mails durch das Fernmeldegeheimnis über den Zeitpunkt der **Kenntnisnahme** durch den Adressaten hinaus (d. h. über den Zeitpunkt hinaus, zu dem das „Ankommen beim Empfänger“ und über die Möglichkeit des Löschens oder Verschiebens, zumindest die wichtigste Ausprägung des Eintritts in den „Herrschungsbereich eines Kommunikationsteilnehmers“ gegeben war – diese beiden Kriterien stammen aus der Entscheidung des **BVerfG** vom 16. Juni 2009, 2 BvR 902/06) wäre im Rahmen des Arbeitsverhältnisses nur schwer durchzuhalten. Aus Sicht des Unternehmens gibt es keine sichere Abgrenzungsmöglichkeit zwischen privaten und nicht privaten E-Mails in einem Postfach,⁵⁴ die es rechtfertigen würde in ersterem Fall die Maßstäbe von § 206 StGB, in letzterem Fall „nur“ die Maßstäbe von § 26 BDSG, Art. 6 DS-GVO anzulegen; das Problem der Abgrenzung besteht insbesondere im Fall von sehr persönlich geschriebenen betrieblichen E-Mails oder bei Mischnachrichten. Der Schutz beim Empfänger angekommener und insoweit „ruhender Daten“ durch das Fernmeldegeheimnis bis zur Erreichung der ausschließlich vom Empfänger beherrschten Sphäre bringt beispielsweise die Frage mit sich, wie mit Dateianhängen zu verfahren ist, die direkt aus einer im serverseitig gespeicherten Postfach eines Arbeitnehmers auf dem Server des Arbeitgebers gespeichert werden. Soll sich auch hieran das Fernmeldegeheimnis fortsetzen, wäre ein Zustand erreicht, bei dem beispielsweise zwei Text-Dateien, je nachdem ob sie

- unmittelbar auf dem Server angefertigt (z. B. durch die Benutzung eines Fernzugangs und remote gestarteter Software) oder
- aus einer E-Mail dorthin gespeichert wurden,

einem unterschiedlichen rechtlichen Schutz unterliegen. Auch wäre die Erstreckung des Fernmeldegeheimnisses auf beim Arbeitgeber gespeicherte private E-Mails im Hinblick auf die Unterschiede zwischen der Privatnutzung im Arbeitsverhältnis und der Privatnutzung im Rahmen des Vertragsverhältnisses mit einem kommerziellen Anbieter von E-Mail-Services nicht gerechtfertigt. Die Privatnutzung im Arbeitsverhältnis wird vom Arbeitgeber meist als reine Annehmlichkeit zugunsten der Arbeitnehmer toleriert. Einzelheiten zum Umfang der zulässigen Privatnutzung werden nur teilweise ausdrücklich geregelt. Häufiger entstehen diese mit wenig nachvollziehbarem Inhalt (nach bestrittener Auffassung) aufgrund einer betrieblichen Übung.⁵⁵ Die in der Regel aufgrund Allgemeiner Geschäftsbedingungen zustande kommenden Nutzungsverträge mit den Anbietern von kommerziellen E-Mail-Systemen hingegen enthalten umfangreiche, auf private Endnutzer zugeschnittene Regelungen zu Art und Inhalt der häufig durch Werbung finanzierten und daher kostenlos zur Verfügung gestellten Services. Das betriebliche E-Mail-System dient von seiner Zwecksetzung her ausschließlich der Kommunikation des Unternehmens mit Kunden und sonstigen Dritten. Das von einem kommerziellen E-Mail-Provider zur Verfügung gestellte System dient dagegen ausschließlich der Kommunikation des Nutzers mit

⁵⁴Vgl. hierzu allgemein Koch, NZA 2008, 911 ff.

⁵⁵Vgl. hierzu Fleischmann, NZA 2008, 1397.

von ihm gewählten Dritten. Die Interessenlage beim Arbeitgeber unterscheidet sich damit grundlegend von der des „gewöhnlichen“ Providers. Zwar sind beide (noch) nach herrschender Meinung TK-Diensteanbieter, jedoch dürfte der „echte“ Provider den von ihm transportierten Nachrichten in der Regel eher indifferent gegenüberstehen, während diese für den Arbeitgeber-Provider Bestandteil der Summe aller und damit auch der relevanten geschäftlichen E-Mails sind. Schließlich ist ein Konflikt zwischen der Stellung des Arbeitgebers als Transporteur der privaten E-Mails (hier ist er dem Fernmeldegeheimnis verpflichtet und hat die Rechte der Adressaten an ihnen zustehenden Daten zu beachten) einerseits und als Verantwortlicher für die Abwehr der von eben diesen privaten E-Mails ausgehenden Gefahren für die IT-Sicherheit (hier hat er die Funktionstüchtigkeit des Unternehmens zu erhalten⁵⁶) andererseits denkbar. Es liegt nahe, dass der Arbeitgeber in dieser Situation auf die IT-Sicherheit⁵⁷ bezogene Aufgaben priorisieren und eher ein Übermaß an IT-Sicherheit implementieren wird, um betriebliche Abläufe zu optimieren.⁵⁸ Beim Streben nach IT-Sicherheit zugleich aus dem Fernmeldegeheimnis resultierende Beschränkungen einzuplanen, dürfte bei der häufig rein technisch geprägten Auswahl von Maßnahmen der IT-Sicherheit für viele Unternehmen schwer zu realisieren sein.

8.2.1.8 Zur Übermittlung anvertraut

Weiter setzt § 206 II Nr. 2 StGB voraus, dass die Sendung dem Übermittler „zur Übermittlung anvertraut“ ist. Dies liegt vor, wenn die Sendung wie vorgesehen in den Verkehr gelangt und der versendende Mailserver dem empfangenden Server die Daten übermittelt hat.⁵⁹ Daran ändert grundsätzlich auch eine Einwilligung des Empfängers mit der Ausfilterung nichts, weil § 206 II Nr. 2 StGB sämtliche am Fernmeldeverkehr Beteiligten, d. h. Absender und Empfänger, schützt. Grundsätzlich müsste auch der Absender seine Einwilligung erteilen.

Bei Versendern von Spam ist es plausibel, ein Anvertrauen abzulehnen, sodass die Lösung typischer Spam-E-Mails möglicherweise schon nicht tatbestandsmäßig ist. Selbst wenn die Belange der unternehmensexternen Absender aber generell (d. h. nicht nur für die Versender von Spam) aus pragmatischen Gründen außer Betracht bleiben, weil es unwahrscheinlich ist, dass von diesen rechtliche Einwände gegen die Filterung erhoben werden, bleibt § 206 II Nr. 2 StGB für die Ausfilterung der von Mitarbeitern des Unternehmens versendeten und an diese gerichteten privaten E-Mails ein relevanter Maßstab.

⁵⁶Vgl. dazu auch Schmidl, MMR 2005, 343 (344).

⁵⁷Vgl. zur Auswahl eines geeigneten Computer-Viren-Suchprogramms BSI, OPS.1.1.4: Schutz vor Schadprogrammen, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_1_1_4_Schutz_vor_Schadprogrammen_Edition_2021.pdf?__blob=publicationFile&v=2 (aufgerufen am 17.07.2024).

⁵⁸Vgl. dazu Schmidl, MMR 2005, 343 (344).

⁵⁹Vgl. dazu MüKoStGB/Altenhain § 206 Rn. 55.

8.2.1.9 Rechtswidrigkeit

Für die Frage der Rechtswidrigkeit ist dann zu differenzieren, ob unerwünschte E-Mails (d. h. Spam-E-Mails) oder E-Mails mit potenziell die IT-Sicherheit des Unternehmens gefährdenden Anhängen herausgefiltert werden sollen. Das Herausfiltern (bloß) unerwünschter E-Mails lässt sich in aller Regel nicht unter Berufung auf das Interesse der Erhaltung der IT-Sicherheit rechtfertigen. Spam kann allenfalls dann zum Sicherheitsproblem werden, wenn die schiere Masse an unerwünschten E-Mails zu technischen Störungen führt. Zudem kann der Adressat einer Spam-E-Mail durchaus Interesse am Inhalt der E-Mail haben. Bei infizierten E-Mails stellt sich die Situation anders dar. Die Infizierung einer E-Mail wird in der Regel durch eine automatische Virenkontrolle festgestellt. Über deren Zulässigkeit besteht Einigkeit, wenn diese ohne Inhaltsprüfung erfolgt.⁶⁰ Trotz des aus § 3 III 3 TDDDG folgenden Grundsatzes, dass für Eingriffe in das Fernmeldegeheimnis ein Erlaubnistatbestand vorliegen muss, der sich ausdrücklich auf Telekommunikationsvorgänge bezieht, kann die Löschung einzelner E-Mails (zumindest aber von deren Anhängen) unter dem Gesichtspunkt allgemeiner Rechtfertigungsgründe gerechtfertigt und damit zulässig sein.⁶¹ So ist die Ausfilterung von E-Mails, die mit Viren, Würmern oder trojanischen Pferden behaftet sind, ohne Weiteres gerechtfertigt, weil für das Unternehmen eine relevante Gefahr besteht.⁶² Eine Verpflichtung, potenziell Schaden verursachende E-Mails zuzustellen, existiert nicht. Das Recht zum Filtern und Löschen existiert dabei unabhängig davon, ob der Arbeitgeber die private Nutzung der Telekommunikationseinrichtungen erlaubt hat oder lediglich toleriert. Ein Einverständnis der Adressaten ist nicht erforderlich.

8.2.2 Regelungsgehalt und Auswirkungen von § 303 a StGB

Neben § 206 StGB kommt eine Strafbarkeit gem. § 303 a StGB in Betracht, wenn dem Arbeitnehmer private E-Mails ohne sein Einverständnis vorenthalten werden. § 303 a StGB ist nicht an die Eigenschaft des Arbeitgebers als Telekommunikationsdienstanbieter gebunden. Für die Strafbarkeit nach § 303 a StGB kommt es damit nicht darauf an, ob das Unternehmen seinen Mitarbeitern die private Nutzung von E-Mail und Internet gestattet hat. Grundsätzlich kann jedes „Unterdrücken“ einer Nachricht den Tatbestand des § 303 a StGB verwirklichen, weil das Schutzgut von § 303 a StGB die Verfügungsbefugnis des Empfängers ist.⁶³

⁶⁰Vgl. dazu Spindler/Schmitz/Spindler TMG § 8 Rn. 53 f.

⁶¹Nach OLG Karlsruhe, MMR 2005, 178 (180) m. w. N. gelten dann, wenn besondere Fallgestaltungen vorliegen, die den Rahmen des damaligen § 88 III 3 TKG sprengen auch die allgemeinen Rechtfertigungsgründe; vgl. auch: BeckOK StGB/Weidemann StGB § 206 Rn. 27 f.

⁶²Vgl. auch Sassenberg/Lammer, DuD 2008, 461 (463).

⁶³Vgl. BeckOK StGB/Weidemann StGB § 303a Rn. 5; Schönke/Schröder/Hecker, StGB, § 303 a Rn. 1; vgl. MüKoStGB/Wieck-Noodt § 303a Rn. 2.

Auch wenn sich die Schutzgegenstände von § 206 StGB und § 303 a StGB unterscheiden, ist eine bloß kurze Vorenthaltung⁶⁴ wohl nicht tatbestandsmäßig.⁶⁵ Im Unterschied zu § 206 II Nr. 2 StGB schützt § 303 a StGB allein den Empfänger und dessen Verfügungsrrecht über die übermittelten Daten,⁶⁶ sodass Beeinträchtigungen, die mit Einwilligung des Empfängers erfolgen, nicht tatbestandsmäßig sind.⁶⁷

8.2.3 Lösungsansätze

Für die ausführliche Darstellung der Implementierung der E-Mail-Filterung im Unternehmen, insbesondere im Hinblick auf die Mitbestimmungsrechte des Betriebsrats gemäß § 87 I Nr. 6 BetrVG und die erforderliche Benachrichtigung der Mitarbeiter, wird auf die umfangreichen Beiträge in der Literatur verwiesen.⁶⁸ Ohne Anspruch auf Vollständigkeit sollte die E-Mail-Filterung in einem Unternehmen mit zulässiger Privatnutzung der E-Mail-Software allerdings jedenfalls folgende Eckpunkte berücksichtigen:

- Die zur E-Mail-Filterung eingesetzte Softwarelösung sollte vom Unternehmen selbst verwaltet werden. Soll ein Dritter zum Einsatz kommen, ist dieser vertraglich zur vertraulichen Handhabung der betroffenen Daten zu verpflichten, es sind klare Vorgaben zur Art und Weise der Filterung und zu sonstigen Leistungsmerkmalen zu machen, und der Dritte ist zudem auf Grundlage eines den Anforderungen von Art. 28 DS-GVO genügenden Vertrags zur Auftragsverarbeitung zu verpflichten.
- Die Mitarbeiter sollten die Filtersoftware zumindest für die Ausfilterung von Spam oder sonstigen per Begriffsfiltern ausgesonderten E-Mails durch aktives Tun, z. B. eine ordnungsgemäße, d. h. protokolierte, jederzeit abrufbare und jederzeit mit Wirkung für die Zukunft widerrufliche „Klick-Einwilligung“ aktivieren müssen und damit auch das Recht haben, die entsprechenden Filter zu deaktivieren. Ebenso denkbar ist es, die Privatnutzung vorbehaltlich der Erteilung einer schriftlichen Einwilligung zu gestatten (siehe z. B. „Einwilligungserklärung zur privaten Nutzung des betrieblichen Internetzugangs“ gemäß der Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz).

⁶⁴ Auch im Rahmen von § 303 StGB führt die Sachentziehung nicht zur Tatbestandsverwirklichung. Vgl. dazu Schönke/Schröder/Hecker, StGB, § 303 Rn. 13.

⁶⁵ MüKoStGB/Wieck-Noodt § 303a Rn. 13; Fischer, StGB, § 303 a Rn. 2.

⁶⁶ Schönke/Schröder/Hecker, StGB, § 303 a Rn. 1.

⁶⁷ Vgl. zur Einschränkung des Tatbestands über die Einordnung des Begriffs „rechtswidrig“ als Tatbestandsmerkmal BeckOK StGB/Weidemann StGB § 303a Rn. 6 f.; Lackner/Kühl/Heger StGB § 303a Rn. 4; Fischer, StGB, § 303 a Rn. 13.

⁶⁸ Z. B. Lösungsansatz von Braun/Spiegl, AiB 2008, 393, differenzierend nach der Eindeutigkeit des Betriebsbezugs, z. B. „info@firmenname.de“ mit eindeutiger Zuordnung als dienstliche Mail; Sassenberg/Lammer, DuD 2008, 461 (463).

- Sollen Quarantäne-Ordner zum Einsatz kommen, so ist die jederzeitige und unmittelbare Zugriffsmöglichkeit der Adressaten sicherzustellen. Irrtümlich als Spam identifizierte und in Quarantäne gestellte E-Mails sollten durch einfache technische Abläufe für die Zukunft der Filterung entzogen werden können.
- Regelungen über die Art und Weise der Filterung von unerwünschten E-Mails können im Rahmen der für die entsprechende technische Einrichtung gemäß § 87 I Nr. 6 BetrVG abgeschlossenen Betriebsvereinbarung festgelegt werden,⁶⁹ wobei der Arbeitgeber sich hier große Freiräume vorbehalten sollte. Zur Klarstellung gilt dies auch für das Filtern und Löschen von infizierten E-Mails. Die konkrete Vorgehensweise bei der Filterung von E-Mails sollte den Betriebsangehörigen bekannt gegeben werden. Ebenfalls sollte bekannt gegeben werden, wenn unerwünschte oder infizierte E-Mails automatisch gelöscht werden. In die Betriebsvereinbarung sollten zudem vorsorglich Ausnahmeregelungen aufgenommen werden, die es dem Verantwortlichen ermöglichen, seinen (auch in der Entscheidung des **BGH** vom 17. Juli 2011 – 5 StR 394/08, insbesondere in den Abs.-Nr. 24 ff., konkretisierten) Pflichten zu entsprechen, wenn Straftaten oder Ordnungswidrigkeiten im Raum stehen.
- Von denjenigen Mitarbeitern, die das betriebliche E-Mail-System privat nutzen wollen, sollte die Abgabe einer Einwilligungserklärung gemäß den Vorgaben der Aufsichtsbehörden⁷⁰ verlangt, den anderen die Privatnutzung untersagt werden.
- In vielen Fällen wird es sich anbieten, über die Einwilligung hinaus eine Nutzungsvereinbarung, um mit der Einwilligung nicht abbildbare positive Handlungspflichten der Arbeitnehmer zu begründen. Eine solche Nutzungsvereinbarung sollte u. a. folgende Themen umfassen: Freiwilligkeit und Widerruflichkeit der Gestattung, konkrete Regeln zu Inhalt und Grenzen der gestatteten Nutzung.

8.3 Whistleblowing im Lichte des Datenschutzrechts

8.3.1 Hinweisgeberschutzgesetz

In Umsetzung der EU-Whistleblower-Richtlinie⁷¹ hat der Bundestag am 16. Dezember 2022 das Hinweisgeberschutzgesetz (im Folgenden HinSchG) beschlossen, das am 2.07.2023 (vollständig) in Kraft getreten ist.⁷² Damit wird es in Deutschland erstmals eine allgemeine

⁶⁹Vgl. zu einem Musterentwurf Oberthür/Seitz/Panzer-Heemeier, Betriebsvereinbarungen B V Rn. 147 f.

⁷⁰Siehe Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, vom Januar 2016, S. 30, https://www.datenschutzkonferenz-online.de/media/oh/201601_oh_email_und_internetdienste.pdf (aufgerufen am 17.07.2024).

⁷¹Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden.

⁷²Zum Zeitpunkt der Erstellung dieses Beitrags steht die Zustimmung des Bundesrats zum Hinweisgeberschutzgesetz noch aus. Die nachfolgenden Ausführungen bleiben jedoch aller Voraussicht nach unabhängig vom weiteren Verlauf des Gesetzgebungsverfahrens richtig.

gesetzliche Regelung zum Schutz (i) von natürlichen Personen geben, die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese melden oder offenlegen sowie (ii) von Personen, die Gegenstand einer Meldung oder Offenlegung oder von einer solchen betroffen sind.⁷³ Die folgende Darstellung bietet keinen vollständigen Überblick über das HinSchG, sie hebt lediglich einige in diesem Zusammenhang relevante Punkte hervor.

Anwendungsbereich

Das HinSchG sieht eine Pflicht zur Einrichtung interner Meldestellen für Unternehmen mit in der Regel mehr als 50 Beschäftigten vor, an die sich Whistleblower wenden können.⁷⁴ Für bestimmte Unternehmen im Bereich des Finanzsektors gilt die Pflicht darüber hinaus unabhängig von der Anzahl der Beschäftigten.⁷⁵ Das HinSchG gilt u. a. für Meldungen über Verstöße, die straf- oder bußgeldbewehrt sind, sofern die verletzte Bußgeldvorschrift dem Schutz von Leib, Leben oder Gesundheit oder der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient.⁷⁶ Weitere Meldungen von Verstößen, die unter das HinSchG fallen, sind enumerativ aufgezählt, darunter Verstöße gegen Gesetze mit Vorgaben zur Produktsicherheit und -konformität oder gegen die DS-GVO.⁷⁷

8.3.1.1 Meldestellen

Die Meldestellen richten Kanäle ein, über die Beschäftigte Verstöße melden können.⁷⁸ Die Meldestellen haben die Meldung zu prüfen und ggf. Folgemaßnahmen zu ergreifen.⁷⁹ Dabei sind sie dazu verpflichtet, auch anonyme Meldungen zu ermöglichen und entgegenzunehmen. Wenn eine anonyme Meldung erfolgt, muss sichergestellt werden, dass auch die anschließende Kommunikation anonym geführt wird.⁸⁰ Eine solche anonyme Kommunikation dürfte mit Hilfe eines einfachen Briefkastens, wie ihn bisher viele Unternehmen als Meldekanal aufgestellt hatten, nicht zu gewährleisten sein.⁸¹

8.3.1.2 Vertraulichkeit

Die Meldestellen sind zur Vertraulichkeit verpflichtet.⁸² Konkret haben die Meldestellen die Vertraulichkeit der Identität der folgenden Personen zu wahren: (i) der hinweisgebenden Person, sofern die gemeldeten Informationen Verstöße betreffen, die in den An-

⁷³ Bisher gab es lediglich sektorspezifische Verpflichtungen, Verstöße zu melden, wie z. B. § 6 V GWG oder § 23 VI VAG.

⁷⁴ § 12 I, II HinSchG.

⁷⁵ § 12 III HinSchG.

⁷⁶ § 2 I Nr. 1, 2 HinSchG.

⁷⁷ § 2 I Nr. 3–8 HinSchG.

⁷⁸ § 16 I 1 HinSchG.

⁷⁹ § 17 f HinSchG.

⁸⁰ § 16 I 4, 5, 6 HinSchG.

⁸¹ Steinhauser/Saalwächter-Hirsch/Trouvain, ESG 2023, 3299 (310).

⁸² § 8 HinSchG.

wendungsbereich des HinSchG fallen, oder die hinweisgebende Person zum Zeitpunkt der Meldung hinreichenden Grund zu der Annahme hatte, dass dies der Fall sei, (ii) der Personen, die Gegenstand einer Meldung sind, und (iii) der sonstigen in der Meldung genannten Personen.

Die Verpflichtung zur Vertraulichkeit entfällt unter bestimmten Voraussetzungen.⁸³ Dies ist dann der Fall, wenn eine Person vorsätzlich oder grob fahrlässig unrichtige Informationen über Verstöße meldet. Außerdem gilt die Pflicht zur Vertraulichkeit unter anderem nicht gegenüber Verlangen von Strafverfolgungsbehörden, Gerichten, Behörden zur Einleitung eines Bußgeldverfahrens nach einer Meldung, der Bundesanstalt für Finanzdienstleistungsaufsicht und des Bundeskartellamts. Außerdem gelten Ausnahmen von der Vertraulichkeitspflicht, unter anderem um Folgemaßnahmen nach einer Meldung zu ergreifen.⁸⁴

8.3.2 Zentrale Anforderungen des Datenschutzrechts

8.3.2.1 Schutzziel des Datenschutzrechts

Gemäß Art. 1 DS-GVO ist es Zweck der Verordnung, den Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sicherzustellen. Dieses Ziel umfasst den Schutz des Einzelnen davor, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.⁸⁵ Dieses Ziel soll durch verschiedene Mechanismen erreicht werden. Für eine abschließende Darstellung des Datenschutzrechts ist hier kein Raum. Wesentlicher Grundgedanke der DS-GVO und des BDSG⁸⁶ ist es, dass beim Sammeln und Verarbeiten von personenbezogenen Daten größtmögliche Zurückhaltung zu wahren ist, um den Betroffenen nicht unangemessen zu beeinträchtigen.

Das Schutzziel des Datenschutzrechts steht in einem Spannungsverhältnis zum Whistleblowing.⁸⁷ Die Meldung eines Whistleblowers enthält in aller Regel personenbezogene Daten. Außerdem kann ein Interesse des Whistleblowers und betroffenen Unternehmen daran bestehen, die Meldung und/oder die Identität des Whistleblowers nicht zu offenbaren, um Untersuchungen nicht zu behindern und mögliche Whistleblower nicht abzuschrecken.⁸⁸

⁸³ § 9 I HinSchG.

⁸⁴ § 9 II, III, IV HinSchG.

⁸⁵ BeckOK Datenschutzrecht/Schantz DS-GVO Art. 1 Rn. 5; Gola/Heckmann/Pötters DS-GVO Art. 1 Rn. 1.

⁸⁶ Vgl. zu den Auswirkungen des BDSG 2018 auf das Arbeitsverhältnis z. B. Chandna-Hoppe NZA 2018, 614; Ströbel/Böhm/Breunig/Wybitul CCZ 2018, 14 ff.; MAH ArbR/Reichold § 96 Rn. 119 ff.

⁸⁷ Ausführlich zum Spannungsverhältnis zwischen Datenschutzrecht und Whistleblowing Fehr, ZD 2022, 256 (256 ff.).

⁸⁸ Vgl. dazu Erwägungsgrund 84 der RL (EU) 2019/1937.

8.3.2.2 Datenminimierung

Das Prinzip der Datenminimierung findet in Art. 5 I c), 25 DS-GVO sowie im Grundsatz der Zweckbindung gemäß Art. 5 I b) DS-GVO seinen Ausdruck: Daten dürfen – so ihre Erhebung überhaupt zulässig ist – grundsätzlich nur für den Zweck verwendet werden, für den sie erhoben worden sind. Art. 5 I c) DS-GVO stellt einen allgemeinen Grundsatz bei der Erhebung von Daten dar und ist damit von besonderer Bedeutung für das Whistleblowing. Gemäß Art. 5 I c) DS-GVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Gemäß Art. 25 I 1 DS-GVO hat der Verantwortliche durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden.⁸⁹ Der in Art. 5 I a) DS-GVO verankerte Transparenzgrundsatz legt es nahe, Daten im Regelfall unmittelbar beim Betroffenen zu erheben.⁹⁰

8.3.2.3 Information der Betroffenen

Gemäß Art. 13, 14 DS-GVO sind die Betroffenen unter anderem über die Identität des Verantwortlichen sowie die Zweckbestimmung der Verarbeitung zu informieren. Zum Umfang der Information gehört auch die Benennung der erhobenen Daten. Eine heimliche Datenerhebung ist schon aus diesem Grund problematisch. Bei fehlender Zweckbestimmung ist eine Datenverarbeitung rechtswidrig; eine prophylaktische Erhebung, also „auf Vorrat“, ist unzulässig. Eine spätere „Umwidmung“ – also eine Verwendung der Daten zu einem anderen als dem ursprünglichen Zweck – ist nur bei Vorliegen einer anderen Befugnisnorm und unter den Voraussetzungen von Art. 6 IV DS-GVO gestattet.⁹¹

⁸⁹ Siehe auch EDPB, Leitlinien 4/2019 zu Artikel 25, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Version 2.0, Angenommen am 20. Oktober 2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_de (aufgerufen am 17.07.2024).

⁹⁰ Eine unmittelbare Normierung des Grundsatzes der Direkterhebung, wie in § 4 Abs. 2 BDSG aF, ist in der DS-GVO nicht enthalten.

⁹¹ Vgl. dazu Gola/Heckmann/Schulz DS-GVO Art. 6 Rn. 133 ff. Bei isolierter Betrachtung des Wortlauts könnte man Art. 6 Abs. 4 DS-GVO im Sinne einer umfassenden Öffnungsklausel verstehen. Ein solches Verständnis hätte jedoch zur Folge, dass das zentrale Anliegen der DS-GVO, nämlich die Harmonisierung des Datenschutzrechts, durch das „Hintertürchen“ der Zweckänderung i. S. v. Art. 6 Abs. 4 DS-GVO ad absurdum werden könnte (vgl. dazu schon die Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Datenschutz-Anpassungs- und Umsetzungsgesetzes EU – DSAnpUG-EU vom 31.8.2016, https://cdn.netzpolitik.org/wp-upload/2016/09/BfDI_Stellungnahme_DSAnpUG_EU.pdf (aufgerufen am 17.07.2024)). Art. 6 Abs. 4 DS-GVO ist daher nicht isoliert, sondern im Kontext mit Art. 6 Abs. 2 und Abs. 3 DS-GVO zu lesen. Art. 6 Abs. 2 und Abs. 3 DS-GVO eröffnen den Mitgliedstaaten Raum für die Normierung von Erlaubnistatbeständen, in deren Rahmen eine zweckändernde Datenänderung – vorbehaltlich der Voraussetzungen des Art. 6 Abs. 4 DS-GVO – möglich ist. Vgl. hierzu auch Kühling/Buchner/Buchner/Petri DS-GVO Art. 6 Rn. 178 ff.

Unabhängig von der Unterrichtung des Betroffenen steht ihm außerdem nach Art. 15 DS-GVO das Recht zur Auskunft über ihn betreffende Datenverarbeitung zu. Dies umfasst das Recht des Betroffenen eine Kopie seiner Daten zu verlangen, Art. 15 III DS-GVO. Die Datenkopie ist, wenn der Antrag elektronisch gestellt wird, in einem maschinenlesbaren Format zur Verfügung zu stellen.

Die Befolgung der Informations- und Auskunftspflichten nach der DS-GVO ist geeignet, Whistleblower zu enttarnen, die Vorbereitung von Folgemaßnahmen zu behindern und die Vertraulichkeitspflicht des HinSchG zu unterlaufen. Der Richtliniengeber und der deutsche Gesetzgeber haben dieses Spannungsverhältnis des Schutzes des Whistleblowings und des Datenschutzes erkannt und sehen dazu Ausnahmen von den datenschutzrechtlichen Informations- und Auskunftspflichten vor.⁹² Der deutsche Gesetzgeber verweist auf § 29 I BDSG. Die Informations- und Auskunftspflichten sind daher gem. § 29 I BDSG ausgeschlossen, wenn die Erfüllung dieser Informationen offenbaren würde, die geheim gehalten werden müsse. Das gilt insbesondere dann, wenn sie wegen entgegenstehender Rechte Dritte geheim gehalten werden müssen. Das wird bei Bestehen der Vertraulichkeitspflicht zu Gunsten eines Whistleblowers regelmäßig der Fall sein.

Erlaubnistatbestände

Bisher war die Datenverarbeitung im Zusammenhang mit Whistleblowing auf Art. 6 I f) DS-GVO bzw. § 26 BDSG zu stützen.⁹³ Es bedurfte dafür einer Abwägung zwischen den Interessen des Betroffenen und des Verantwortlichen oder eines Dritten, zu dessen Gunsten die Daten erhoben werden. Mit Einführung des HinSchG sind nunmehr Unternehmen mit in der Regel mehr als 50 Mitarbeitern dazu verpflichtet, einen Meldekanal einzurichten.⁹⁴ Damit liegt es nunmehr nahe, eine Verpflichtung für die Datenverarbeitung im Rahmen einer Meldung nach Art. 6 I c) DS-GVO anzunehmen.

Für Unternehmen, die in der Regel weniger als 50 Mitarbeiter haben und nicht in einem der besonderen Sektoren tätig sind,⁹⁵ würde es bei der Interessenabwägung nach Art. 6 I f) DS-GVO bzw. § 26 BDSG bleiben. Gemäß § 26 I 1 BDSG (zu Zweifeln an dieser Vorschrift siehe auch EuGH-Urteil vom 30.03.2023 – C-34/21) dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Eine strenge Erforderlichkeitsprüfung im Sinne der Analyse, welche von mehreren

⁹² Erwägungsgrund 84 der RL (EU) 2019/1937; BT-Drs. 20/3442, 74.

⁹³ Vgl. Groß/Platzer NZA 2017, 1097 (1102).

⁹⁴ § 12 HinSchG-E.

⁹⁵ Zu den Sektoren, in denen auch bei weniger als in der Regel 50 Mitarbeitern eine Meldestelle einzuführen ist, siehe § 12 III, IV HinSchG-E.

gleich geeigneten Maßnahmen die mildeste Maßnahme ist, soll damit nach der in der Aufsichtspraxis anzutreffenden Auffassung verschiedener Aufsichtsbehörden nicht gefordert sein.⁹⁶ Vielmehr eröffne das Tatbestandsmerkmal der Erforderlichkeit in § 26 I 1 BDSG die Möglichkeit der Prüfung, ob die berechtigten Interessen des Unternehmens auf andere Weise nicht oder nicht angemessen gewahrt werden können.⁹⁷

8.3.2.4 Kein Konzernprivileg

Stellen mehrere Unternehmen jeweils eine eigenständige rechtliche Einheit dar, gehören aber demselben Konzern an, so gelten auch hier die Grundsätze des Datenschutzes. Sollen mithin die Kontrollmaßnahmen zentral für alle Konzernunternehmen, beispielsweise durch die Muttergesellschaft, durchgeführt werden, so gilt hierfür keine Sonderregelung. Für die Verarbeitung innerhalb eines Konzerns müssen die allgemeinen Zulässigkeitsvoraussetzungen einer Datenverarbeitung, z. B. nach Art. 6, 44 DS-GVO oder § 26 BDSG, vorliegen. Die DS-GVO kennt kein „Konzernprivileg“, das den Datenaustausch zwischen konzernangehörigen, aber rechtlich selbstständigen Unternehmen erleichtern oder unter weiteren Zulässigkeitsvoraussetzungen begünstigen würde, die noch unterhalb dessen liegen, was für eine „normale“ Datenübermittlung erforderlich ist.⁹⁸ Dies ergibt sich auch aus Erwägungsgrund Art. 48 DS-GVO, der lediglich besagt, dass Konzernunternehmen „ein berechtigtes Interesse haben“ können, „Daten innerhalb der Unternehmensgruppe … zu übermitteln“:

„(48) Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland bleiben unberührt.“

Die DS-GVO erwähnt die Konzernzugehörigkeit nicht als eigenständigen Erlaubnistatbestand. Aus Erwägungsgrund 48 kann lediglich abgeleitet werden, dass diese ein positives Indiz für die Zulässigkeit einer Übermittlung auf Grundlage einer Interessenabwägung darstellt.⁹⁹

Ein Unternehmen innerhalb eines Konzerns darf mithin einem anderen Konzernunternehmen nur unter Beachtung der Erlaubnistatbestände der DS-GVO, des BDSG oder anderer Gesetze Daten übermitteln.¹⁰⁰

⁹⁶Ausführlich zum Geltungsbereich und den Voraussetzungen des § 26 BDSG nF Gola BB 2017, 1462.

⁹⁷Vgl. zur Auslegung des „Erforderlichkeitskriteriums“ in diesem Sinn Kühling/Buchner/Maschmann BDSG § 26 Rn. 19.

⁹⁸Vgl. dazu Forgó/Helfrich/Schneider/Moos/Zeiter Betr. Datenschutz-HdB Teil VI Rn. 5 ff. mwN; Thüsing NZA 2011, 16 (19).

⁹⁹Vgl. Forgó/Helfrich/Schneider/Moos/Zeiter Betr. Datenschutz-HdB Teil VI. Rn. 16.

¹⁰⁰Vgl. dazu Forgó/Helfrich/Schneider/Moos/Zeiter Betr. Datenschutz-HdB Teil VI Rn. 1 ff. mwN.

8.3.2.5 Anforderungen an internationale Übermittlungen

Gemäß Art. 44 DS-GVO ist eine Übermittlung personenbezogener Daten an ein Drittland nur zulässig, wenn die Voraussetzungen der Art. 45 ff. DS-GVO eingehalten werden. Zwar könnte man ausgehend vom Wortlaut des Art. 44 S. 1 DS-GVO jede Übermittlung von verarbeiteten personenbezogenen Daten unter die Art. 45 ff. DS-GVO subsumieren, weil die Vorschrift nicht (explizit) an die Übermittlung von Daten in Drittstaaten anknüpft. Ein solches Verständnis würde jedoch in Widerspruch zur amtlichen Überschrift des Kapitels V („Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen“) stehen. Um im Übrigen zu gewährleisten, dass in Drittländern ein angemessenes Datenschutzniveau erreicht wird, sind die Art. 44 ff. DS-GVO nach Sinn und Zweck daher auch auf Datenübermittlungen in Staaten anzuwenden, die ihrerseits *nicht* bereits dem Schutzniveau der DS-GVO unterliegen.¹⁰¹

Art. 44 S. 2 DS-GVO erwähnt das gesetzgeberische Motiv der Art. 44–50 DS-GVO. Danach sind die Bestimmungen des Kapitels V anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird. Untergraben werden könnte das Schutzniveau der DS-GVO beispielsweise, wenn personenbezogene Daten im Anwendungsbereich der DS-GVO verarbeitet, ins außereuropäische Ausland übermittelt, dort frei bzw. nach anderen, ein geringeres Schutzniveau bietenden Regelungen „weiterverarbeitet“ und anschließend zurück in die Europäische Union übermittelt werden würden. Dies zu verhindern, bezwecken die Regelungen des Kapitel V.¹⁰² Soweit sich die Empfänger der verarbeiteten personenbezogenen Daten nicht in Ländern befinden, für die ein Angemessenheitsbeschluss gemäß Art. 45 DS-GVO vorliegt und soweit keine Ausnahmen gemäß Art. 49 DS-GVO Anwendung finden, sichern die Art. 44–50 DS-GVO folglich den grundrechtlich gebotenen Schutz von personenbezogenen Daten im Ausland respektive die Einhaltung der EU-Datenschutzmaßstäbe am Zielort.

Grundsätzlich sind zwei Wege denkbar, für eine Daten empfangende Stelle im Ausland ein angemessenes Datenschutzniveau sicherzustellen. Es kann entweder auf das Schutzniveau des Staates abgestellt werden, in dem sich die empfangende Stelle befindet (Art. 45 DS-GVO), oder auf das Schutzniveau der empfangenden Stelle selbst (Art. 46 DS-GVO). Letzteres ist erforderlich, wenn der Staat, in dem sich die empfangende Stelle befindet, kein angemessenes Datenschutzniveau vorweist.¹⁰³

¹⁰¹ Vgl. zu diesen Überlegungen Kühling/Buchner/Schröder DS-GVO Art. 44 Rn. 17; weiterführend zu der Frage, welche Länder als „Drittländer“ iSd Art. 44 S. 1 DS-GVO in Betracht kommen, BeckOK Datenschutzrecht/Beck DS-GVO Art. 44 Rn. 23 ff.; Ehmann/Selmayr/Zerdick DS-GVO Art. 44 Rn. 10.

¹⁰² Vgl. Kühling/Buchner/Schröder DS-GVO Art. 44 Rn. 22.

¹⁰³ Zu den allgemeinen Voraussetzungen internationaler Datentransfers s. Ambrock/Karg ZD 2017, 154.

8.3.3 Lösungsansätze

Die Einwirkungen des Datenschutzrechts auf die Implementierung eines Whistleblowing-Systems im Unternehmen nach dem HinSchG sind vielfältig und komplex und können hier nicht abschließend dargestellt werden. Auch insoweit wird auf die bereits erschienene¹⁰⁴ sowie die noch erscheinenden Veröffentlichungen verwiesen. Ohne dass die folgenden Ausführungen Anspruch auf Vollständigkeit erheben, sollte das in enger Abstimmung mit dem Datenschutzbeauftragten und ggf. erst nach einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO einzuführende Whistleblowing-System in einem Unternehmen allerdings jedenfalls folgende Eckpunkte in Hinblick auf die datenschutzrechtlichen Vorgaben berücksichtigen:

- Allen Mitarbeitern ist unmissverständlich mitzuteilen, dass die Daten der Betroffenen für festgelegte eindeutige Zwecke und aufgrund konkreter Vorkommnisse statt vager Vermutungen erhoben werden;¹⁰⁵
- Das System sollte getrennt von der allgemeinen Personaldatenverwaltung geführt und mit angemessenen technischen und organisatorischen Maßnahmen (z. B. Schutz der Datenbestände durch Verschlüsselung) eingeführt werden und muss Abläufe vorsehen, die sicherstellen, dass fehlerhafte (das umfasst auch als unbegründet erkannte Meldungen) oder unvollständige Daten gelöscht oder berichtet werden;
- Im Lichte der Grundsätze der Datensparsamkeit und der Datenvermeidung ist der von einer konkreten Meldepflicht betroffene Personenkreis möglichst präzise zu beschreiben und – ggf. auch in Abhängigkeit von der betroffenen Meldepflicht – klein zu halten;
- Das Unternehmen hat sicherzustellen, dass die von einer Meldung betroffenen Personen von der sie betreffenden Meldung datenschutzgerecht unterrichtet werden, sobald dies möglich ist, ohne eine mit der Meldung zusammenhängende Untersuchung zu gefährden;
- Das Whistleblowing-Verfahren hat vorzusehen, dass die im Rahmen einer Meldung erhobenen Daten zu löschen sind, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist.¹⁰⁶

¹⁰⁴ Steinhäuser/Saalwächter-Hirsch/Trouvain, ESG 2023, 9 (9 ff.); Fehr, ZD 2022, 256 (256 ff.).

¹⁰⁵ In der Gesetzesbegründung zum HinSchG heißt es: „Bei der Verarbeitung personenbezogener Daten hat die interne Meldestelle die Vorschriften über den Datenschutz einzuhalten.“, BT-Drs. 20/3442, 79.

¹⁰⁶ Dabei muss auch die Aufbewahrungspflicht nach § 11 V HinSchG-E beachtet werden.

8.4 Screening von E-Mail und Internetverkehrsdaten

8.4.1 Screening von E-Mail

8.4.1.1 Interessenlage

Das Bedürfnis der Ermittlung von Sicherheitslücken geht häufig mit dem Wunsch der Unternehmen einher, die über die betrieblichen E-Mail-Accounts an externe Empfänger gesendeten und von externen Empfängern erhaltenen E-Mails, d. h. im Unternehmen (z. B. in „*.pst“-Dateien) gespeicherte Daten, bestimmter Mitarbeiter anhand für die konkrete Pflichtverletzung typischer Suchbegriffe daraufhin zu untersuchen („E-Mail-Screening“), ob sich ein konkreter Verdacht für die vermutete Pflichtverletzung ergibt.¹⁰⁷ Vor dem Hintergrund der in der Regel zulässigen Privatnutzung des E-Mail-Systems stellt sich dann die Frage, ob das E-Mail-Screening gemessen an § 206 StGB und Art. 6 I 1 DS-GVO rechtlich zulässig ist (dazu auch die oben in Nr. 2 genannten Maßstäbe). In diesem Zusammenhang wird von einer Ausstrahlung des Fernmeldegeheimnisses auf die betriebliche Kommunikation¹⁰⁸ gesprochen, wenn sich die einen von den anderen Daten nicht sicher trennen lassen. Bedenken gegen die mit einer solchen „Infektion“ einhergehende Erstreckung des Schutzes für private auf sämtliche E-Mails scheinen zumindest (aber nicht nur) dann angebracht, wenn eine an sich geschäftliche Nachricht bewusst mit privaten Be standteilen versehen und eine Mischnachricht erzeugt wird, um diese der Kontrolle durch ein E-Mail-Screening zu entziehen.

Geht man vom Regelfall aus, dass sich die privaten von den betrieblichen Nachrichten (abseits vom Sonderfall der Mischnachricht) grundsätzlich trennen lassen, so begründet die vorgenannte Ausstrahlung des Fernmeldegeheimnisses in erster Linie ein Auswahlrisiko, weil ein E-Mail-Screening gleichermaßen betriebliche und private E-Mails betreffen kann. Fraglich ist, welchen rechtlichen Anforderungen das E-Mail-Screening genügen muss, um die dienstlichen Nachrichten einer einzelfallbezogenen Überprüfung zugänglich zu machen. Bis zur Entscheidung des BVerfG vom 16.6.2009 (2 BvR 902/06) war das E-Mail-Screening in der praktischen Durchführung und in Absprache mit der Datenschutzaufsicht auf Grundlage der Entscheidung des BVerfG vom 2.3.2006 (2 BvR 2099/04)¹⁰⁹ an den Maßstäben des Datenschutzrechts gemessen (insbes. § 28 I 1 Nr. 2 BDSG aF) worden.

¹⁰⁷ Frank/Heine, CCZ 2021, 195 (195 f.); Wybitul NJW 2014, 3605 (3605 f.).

¹⁰⁸ Vgl. dazu Koch NZA 2008, 911 (913): „Soweit sich also etwa private E-Mails im E-Mail-System des Unternehmens nicht klar von betrieblichen E-Mails unterscheiden lassen, müssen auch die betrieblich veranlassten E-Mails wie private E-Mails der Mitarbeiter behandelt werden und darf der Arbeitgeber sie grundsätzlich nicht einmal lesen.“

¹⁰⁹ BVerfG NJW 2006, 976.

Vor diesem Hintergrund sollte ein E-Mail-Screening trotz des Auswahlrisikos (private oder betriebliche Nachricht) gemäß § 26 I 1 BDSG zulässig sein können, wenn

- es zur Aufklärung eines in einem konkreten Einzelfall bestehenden Verdachts einer Pflichtverletzung oder Sicherheitslücke erfolgt,
- es anhand von wenigen für die Pflichtverletzung oder Sicherheitslücke relevanten Stichworten durchgeführt wird, die die Betroffenheit privater E-Mails als unwahrscheinlich erscheinen lassen,
- es nur bestimmte nach für die gesuchte Pflichtverletzung relevanten Kriterien ausgewählte Mitarbeiter betrifft,
- es nicht mit einer Totalüberwachung einhergeht,
- es mit dem Datenschutzbeauftragten des Unternehmens und dem Betriebsrat abgestimmt ist, und
- die das E-Mail-Screening durchführenden Mitarbeiter, falls nicht bereits zu einem früheren Zeitpunkt geschehen, auf Vertraulichkeit und zum sofortigen Schließen und Nicht-Ausdrucken versehentlich geöffneter privater E-Mails verpflichtet werden.¹¹⁰

8.4.1.2 Anwendung von § 206 StGB

Angesichts der Entscheidung des **BVerfG** vom 16. Juni 2009 (**BVerfG** – 2 BvR 902/06) dürfte für den rechtlichen Rahmen eines im Unternehmen durchgeföhrten E-Mail-Screening danach zu unterscheiden sein,

- ob die vom E-Mail-Screening (potenziell) betroffenen privaten E-Mails noch unter den Schutz des Fernmeldegeheimnisses fallen, weil sie beim jeweiligen Empfänger noch nicht angekommen und noch nicht in seinem Herrschaftsbereich abgespeichert sind oder
- ob dieser Zustand (d. h. Ankunft beim Adressaten und Abspeichern im eigenen Herrschaftsbereich) bereits erreicht und damit der durch das Fernmeldegeheimnis begründete Schutz beendet ist.

Im ersten Fall kann der Tatbestand von § 206 I StGB verwirklicht werden, wenn im Rahmen oder in der Folge des E-Mail-Screening „unbefugt einer anderen Person eine Mitteilung über Tatsachen“ gemacht wird, die „dem Post- oder Fernmeldegeheimnis unterliegen“ und die dem Handelnden „als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt“. Als Tatsache, die dem Fernmeldegeheimnis unterliegt, kommt der Inhalt einer privaten E-Mail auf dem Server des Arbeitgebers in Betracht. Nach der herrschenden Meinung erbringt der Arbeitgeber bei Zulassung der Privatnutzung des E-Mail-Systems geschäftsmäßig Telekommunikationsdienste, wobei es hierfür nicht auf die Entgeltlichkeit der Dienste ankommt.¹¹¹ Fraglich ist, ob das E-Mail-Screening zudem mit der unbefugten Mitteilung über Tatsachen einhergeht. Für ein Mitteilen gemäß § 206 I StGB genügt jede schriftliche, mündliche oder sonstige Bekannt-

¹¹⁰Vgl. zur E-Mail-Auswertung in der betrieblichen Praxis Frank/Heine, CCZ 2021, 195 (196 f.); Wybitul NJW 2014, 3605.

¹¹¹OLG Karlsruhe, MMR 2005, 178 (180).

gabe außerhalb der Normalabwicklung des Fernmeldedienstes, wobei der Empfänger nicht notwendig außerhalb des Fernmeldedienstes stehen muss, sodass auch Mitteilungen unter den Bediensteten selbst den Tatbestand erfüllen können.¹¹² Unter Zugrundlegung dieser Analyse kann das beispielsweise von einem Mitarbeiter der IT-Abteilung eines Unternehmens durchgeführte und private E-Mails bestimmter Arbeitnehmer betreffende E-Mail-Screening, dessen Ergebnisse anschließend der Geschäftsleitung mitgeteilt werden, den Tatbestand von § 206 I StGB erfüllen. Auf diese Weise kann sich das eingangs beschriebene Auswahlrisiko zwischen privaten und betrieblichen E-Mails manifestieren. Dieses Risiko lässt sich durch die beschriebene Vorgehensweise (Auswahl relevanter Stichworte etc.) verringern. Die Wahrscheinlichkeit, beim E-Mail-Screening auch private E-Mails zu öffnen, lässt sich auch reduzieren, indem die Privatnutzung des E-Mail-Systems untersagt oder die Mitarbeiter zumindest verpflichtet werden, (gesendete und empfangene) private E-Mails unverzüglich auszudrucken, zu löschen oder auf andere Weise aus dem E-Mail-System des Arbeitgebers zu entfernen. Besteht eine solche Pflicht der Arbeitnehmer, so kann für die Tatbestandsverwirklichung von § 206 I StGB durch das E-Mail-Screening zumindest der Vorsatz bestritten werden. Gemäß § 3 III TDDDG ist es den Diensteanbietern untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Diese Gründe für ein E-Mail-Screening liegen regelmäßig nicht vor. Für ein E-Mail-Screening können in Einzelfällen aber trotz des restriktiven Wortlauts von § 3 III 3 TDDDG – gefordert ist ein Erlaubnistatbestand, der sich ausdrücklich auf Telekommunikationsvorgänge bezieht – auch die allgemeinen Rechtfertigungsgründe eingreifen, wenn besondere Fallgestaltungen vorliegen, die den Rahmen des § 3 III 3 TDDDG sprengen.¹¹³ Ein E-Mail-Screening könnte möglicherweise dann gerechtfertigt sein, wenn die unmittelbare Gefahr des Verrats von Betriebs- und Geschäftsgeheimnissen besteht, die nur durch das E-Mail-Screening abgewendet werden kann.

8.4.1.3 Anwendung des Datenschutzrechts

Im zweiten Fall (d. h. nach Ankunft beim Adressaten und Abspeichern im eigenen Herrschaftsbereich) ist ein E-Mail-Screening an den Maßstäben des Datenschutzrechts – wegen der nach Ankunft beim Adressaten und Abspeichern im eigenen Herrschaftsbereich endgültigen Beendigung des Übermittlungsvorgangs nicht an den Maßstäben des Telekommunikationsrechts¹¹⁴ – zu messen, sodass § 206 StGB keine Anwendung mehr findet.¹¹⁵ Das E-Mail-Screening und die damit verbundene Verarbeitung und Nutzung von personenbezogenen Daten über bestimmte Mitarbeiter kann dann gemäß Art. 6 I f)

¹¹²MüKoStGB/Altenhain § 206 Rn. 42.

¹¹³Vgl. OLG Karlsruhe, Beschluss vom 10.1.2005 – 1 Ws 152/04 (rechtskräftig), MMR 2005, 178 (180) m. w. N.

¹¹⁴Vgl. dazu bereits Rn. 21.

¹¹⁵Nach BVerfG NJW 2006, 976 ist der von Art. 10 GG eröffnete Schutzbereich nicht betroffen, wenn der Telekommunikationsvorgang als solcher abgeschlossen ist und die Daten nunmehr als „Rückstand“ des Kommunikationsaktes auf dem Privatcomputer des Betroffenen liegen. Ausführlich dazu Günther NStZ 2006, 641 (643 ff.).

DS-GVO zulässig sein, weil die Aufdeckung einer sicherheitsrelevanten Pflichtverletzung ein berechtigtes Interesse des Unternehmens an der Durchführung des E-Mail-Screenings und der damit verbundenen Verarbeitung und Nutzung von personenbezogenen Daten über bestimmte Mitarbeiter darstellen kann. Im Lichte der Entscheidung des **BVerfG** vom 16. Juni 2009 (**BVerfG** – 2 BvR 902/06) stellt sich allerdings die Frage, in welchen Fällen ein E-Mail-Screening „im Herrschaftsbereich des Adressaten“ im betrieblichen Ablauf überhaupt denkbar ist. Nicht zum „Herrschaftsbereich des Adressaten“ zählt jedenfalls der ihn betreffende Posteingang des E-Mail-Systems; für dort gespeicherte E-Mails liegt nach der zuvor genannten Entscheidung des **BVerfG** noch ein Telekommunikationsvorgang vor. Auch der vom Arbeitnehmer regelmäßig genutzte Arbeitsplatzrechner ist möglicherweise kein „eigener Herrschaftsbereich“, wenn der Arbeitgeber auf diesen jederzeit zugreifen kann, etwa um Sicherungskopien herzustellen.

Unter der Voraussetzung, dass sich das E-Mail-Screening gleichwohl auf den „Herrschchaftsbereich des Adressaten“ bezieht, muss es zudem gemäß Art. 6 I f) DS-GVO erforderlich sein. Auch wenn dies eine Frage des Einzelfalls ist, ist gut denkbar, dass vergleichbar aufschlussreiche Maßnahmen mit geringerer Eingriffswirkung für die betroffenen Mitarbeiter nicht ersichtlich sind.¹¹⁶ Die Interessensabwägung gemäß Art. 6 I f) DS-GVO kann im Hinblick auf einen konkreten Verdacht der Begehung einer sicherheitsrelevanten Pflichtverletzung durch eine der Personen, deren E-Mails untersucht werden, und die Auswahl von Suchbegriffen, die eine Involvierung privater Nachrichten mit hoher Wahrscheinlichkeit verhindern, sowie die Anweisung an das mit dem E-Mail-Screening befasste Personal, im Rahmen des Screenings gleichwohl gefundene geöffnete private E-Mails sofort wieder zu schließen, nicht auszudrucken und nicht zu verwerten, zugunsten des Unternehmens und der Durchführung des E-Mail-Screenings ausfallen.

Besondere Bedeutung kommt im Rahmen der Interessensabwägung der Gewichtung der unterschiedlichen Interessen anhand der für sie jeweils drohenden Verletzungsrisiken zu. Durch die Auswahl geeigneter Stichworte für das E-Mail-Screening kann das Risiko der Verletzung des Rechts auf Datenschutz (grundrechtsdogmatisch auf „informationelle Selbstbestimmung“) stark reduziert werden. Der vollständige Ausschluss eines Verletzungsrisikos wird allerdings in der Regel nicht gelingen.

8.4.2 Screening von Internetverkehrsdaten

8.4.2.1 Anwendbarkeit des TDDDG

Wie beim E-Mail-Screening, so stellt sich auch beim Screening von Internetverkehrsdaten die Frage, ob der Arbeitgeber als Anbieter von Telekommunikationsdiensten zu qualifizieren ist. Die Kontrolle der von Mitarbeitern im Falle der zulässigen Privatnutzung auf-

¹¹⁶Grundlegend zum Verhältnismäßigkeitsprinzip als Begrenzung BAG NJW 2003, 3436, (3437 f.) (verdeckte Videoüberwachung); BAG MMR 2008, 777. (Videoüberwachung); BAG NZA 2014, 243 (244 f.) (heimliche Videoüberwachung); BAG NJW 2017, 2853 (Überwachung durch Detektiv); vgl. zur Geltung des Verhältnismäßigkeitsgrundsatzes bei Eingriffen in das Allgemeine Persönlichkeitsrecht im Zusammenhang mit der Videoüberwachung von Arbeitnehmern Venetis/Oberwetter, NJW 2016, 1051 (1052 f.).

gebauten Internetverbindungen unterliegt jedenfalls engen Grenzen.¹¹⁷ Mit der (noch) herrschenden Meinung ist es dem die Privatnutzung zulassenden Arbeitgeber gemäß § 3 II 1 Nr. 1 TDDDG als Anbieter von Telekommunikationsdiensten¹¹⁸ untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes seiner technischen Systeme erforderliche Maß hinaus, Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Gemäß § 3 III 2 TDDDG darf er Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für die in § 3 III 1 TDDDG genannten Zwecke verwenden. § 3 III 3 TDDDG verbietet eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, es sei denn das TTDSG oder eine andere gesetzliche Vorschrift sieht dies vor und bezieht sich dabei ausdrücklich auf Telekommunikationsvorgänge. Die zeitliche Reichweite des Schutzbereichs des Fernmeldegeheimnisses wird beim Screening von Internetverkehrsdaten (im Unterschied zur Situation beim E-Mail-Screening, siehe oben Nr. 2) nicht problematisiert. Auch wenn diese Frage im Ergebnis identisch zu beurteilen sein dürfte, kommt es bei den Internetverkehrsdaten in aller Regel nicht auf die zeitliche Reichweite des durch das Fernmeldegeheimnis vermittelten Schutzes an, u. a. weil die betroffenen Daten mangels einfacher Zugriffsmöglichkeit typischerweise bis zur automatisierten Löschung auf der IT-Infrastruktur des Arbeitgebers (z. B. über das Browser- oder Router-Protokoll) verfügbar verbleiben.

8.4.2.2 Mögliche Erlaubnistatbestände

Selbst aufgrund der beispielsweise vom **OLG Karlsruhe** unter bestimmten Umständen für möglich gehaltenen Anwendung der allgemeinen Rechtfertigungsgründe¹¹⁹ lässt dieser Rahmen wenig Spielraum für die Kontrolle der Internetnutzung. Die Erlaubnisnorm des § 9 I 1 TDDDG gestattet die Verwendung der in § 9 I 1 TDDDG genannten Verkehrsdaten zum Aufbau der Telekommunikation und zur Entgeltabrechnung. Der Begriff der Ver-

¹¹⁷ Zur Bedeutung der Europäischen Menschenrechtskonvention als Ordnungsrahmen für das Internet, jüngst der EGMR NZA 2017, 1443 sowie BAG NZA 2017, 1327 (1328).

¹¹⁸ Ob der Arbeitgeber Anbieter von Telekommunikationsdiensten i. S. v. § 3 II TTDSG ist, ist streitig. Dies wird teilweise mit dem Argument verneint, dass ein dem Fernmeldegeheimnis des Art. 10 Abs. 1 GG unterfallender Zugriff des Arbeitgebers nicht vorliege, wenn der Arbeitgeber auf die im Posteingang oder -ausgang befindliche E-Mails zugreift. Der Telekommunikationsvorgang sei abgeschlossen, sodass der Schutzgehalt des TKG nicht betroffen sei (vgl. z. B. LAG Berlin-Brandenburg NZA-RR 2011, 342 (343); LAG Niedersachsen NZA-RR 2010, 406 (408); Fülbier/Splittgerber NJW 2012, 1995). Gegen diese Sichtweise spricht, dass die private Nutzung des Internets bzw. der E-Mail außerhalb der betrieblichen Sphäre erfolgt, mit der Folge, dass der Arbeitnehmer dem Arbeitgeber **wie ein Dritter** gegenübersteht und letzterer Dienste i. S. v. § 3 II TTDSG anbietet. Nach zutreffender Ansicht ist der Arbeitgeber somit Anbieter von Telekommunikationsdiensten. Ausführlich dazu Scheurle/Mayen/Mayen TKG § 88 Rn. 61; Beck TKG/Bock TKG § 88 Rn. 24; Fischer ZD 2012, 265 (266), die nun entsprechende Anwendung auf § 3 II TTDSG finden. Zur entsprechenden Anwendung Wünschelbaum, NJW 2022, 1561 (1561 f.).

¹¹⁹ Nach OLG Karlsruhe, Beschluss vom 10.1.2005 – 1 Ws 152/04 (rechtskräftig), MMR 2005, 178 (180) m. w. N. gelten dann, wenn besondere Fallgestaltungen vorliegen, die den Rahmen des 88 III 3 TKG sprengen, auch die allgemeinen Rechtfertigungsgründe.

kehrsdaten (§ 3 Nr. 70 TKG) erfasst auch die vom Mitarbeiter aufgerufene IP-Adresse.¹²⁰ Für Zwecke der Vermarktung oder bedarfsgerechten Gestaltung von Telekommunikationsdiensten kann der Endnutzer zudem in die Verarbeitung von Verkehrsdaten nach den Grundsätzen der DS-GVO einwilligen, § 9 II 1 TDDDG. Auch diese Ausnahme dürfte im Rahmen des Arbeitsverhältnisses keine Anwendung finden.

Eine über § 9 I 1 TDDDG hinausgehende Erhebung oder Verwendung der Verkehrsdaten ist gemäß § 9 I 3 TDDDG unzulässig. Die Verkehrsdaten sind nach Beendigung unverzüglich zu löschen, § 9 I 2 TDDDG, soweit sie nicht wegen § 100g StPO zu speichern sind. Im Arbeitsverhältnis kommen §§ 11, 13 TDDDG in aller Regel nicht in Betracht. Die Erlaubnisnormen betreffen die Erstellung eines Einzelverbindungsnnachweises und die Verarbeitung von Standortdaten und passen damit in der Regel nicht auf die kostenfreie Internetnutzung durch Arbeitnehmer.

§ 12 I TDDDG regelt die Befugnisse des Diensteanbieters zur Erhebung und Verwendung von Bestands- und Verkehrsdaten sowie zu weitergehenden Kontrollmaßnahmen, soweit dies erforderlich ist, um Störungen oder Fehler an Telekommunikationsanlagen einzuzgrenzen oder zu beseitigen.¹²¹ Selbst wenn man davon ausgeht, dass diese Erlaubnistatbestände im Interesse eines umfassenden Schutzes der technischen Systeme eine Erhebung von Verkehrsdaten auch ohne konkrete Anhaltspunkte für das Vorliegen einer Störung (d. h. bereits im Vorfeld ihres möglichen Auftretens) legitimieren, eignen sich § 12 I TDDDG jedenfalls nicht als Grundlage für ein flächendeckendes Screening durch den Arbeitgeber mit dem Ziel, die Rechtmäßigkeit der Internetnutzung durch seine Mitarbeiter zu überprüfen.¹²²

8.5 Totalüberwachung im Lichte von Art. 1 GG und sonstige Grenzen

8.5.1 Grenzen der Überwachung aus Art. 1 GG

8.5.1.1 Verbot der Totalüberwachung

Unter dem Gesichtspunkt der Totalüberwachung¹²³ sind sämtliche Maßnahmen unzulässig, die zu einer dauerhaften lückenlosen Erfassung des Verhaltens eines Arbeitnehmers führen; der Gegenpol zur Dauerüberwachung wird durch die Stichprobe gebildet. Die Totalüberwachung kann prinzipiell eine Verletzung der Menschenwürde des Arbeitnehmers

¹²⁰ Zum Begriff der Verkehrsdaten i. S. v. § 9 TTDSG i. V. m. § Nr. 70 TKG siehe Assion/Schramm/Shvets, TTDSG § 9 Rn. 57 ff.

¹²¹ Siehe dazu Assion/Schramm/Shvets, TTDSG § 12.

¹²² Vgl. auch Kömpf/Kunz NZA 2007, 1341.

¹²³ Zu Überwachungsmaßnahmen am Arbeitsplatz allgemein Freckmann/Wahl BB 2008, 1904 ff.; ausf. auch Oberwetter NZA 2008, 609 ff.; vgl. zur (anlasslosen) Videoüberwachung von Arbeitnehmern LAG Hamm NZA-RR 2018, 13 mAnm Buschbaum NZA-RR 2018, 17.

i. S. v. Art. 1 I GG darstellen. Eine Missachtung des Werts als Mensch liegt vor, wenn durch die Überwachung in den absolut geschützten Kernbereich privater Lebensgestaltung eingegriffen wird.¹²⁴ An einem Eingriff in den unantastbar geschützten Kernbereich privater Lebensgestaltung des Arbeitnehmers dürfte es bei der Totalüberwachung durch den Arbeitgeber allerdings in aller Regel fehlen. Der Arbeitnehmer wird seine intimsten Vorgänge und Empfindungen, seine Überlegungen und Erlebnisse höchstpersönlicher Art typischerweise nicht am Arbeitsplatz zum Ausdruck bringen. Zu derartigen Gefühlsäußerungen wird sich der Arbeitnehmer vielmehr nur in seiner, ihm als Rückzugsort dienenden Privatwohnung verleiten lassen.¹²⁵ Soweit die Totalüberwachung nicht gegen die Menschenwürde verstößt, ist daher danach zu fragen, ob die Maßnahme wegen Verletzung des Allgemeinen Persönlichkeitsrechts des Arbeitnehmers i. S. v. Art. 2 I i. V. m. Art. 1 I GG unzulässig ist.¹²⁶ Mit dem Allgemeinen Persönlichkeitsrecht des Arbeitnehmers unvereinbar ist dabei eine Totalüberwachung, die sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Äußerungen des Arbeitnehmers registriert und zur Grundlage für ein Persönlichkeitsprofil verwendet werden können.¹²⁷ Allein der Abschluss des Arbeitsvertrages in Kenntnis dieser Möglichkeiten stellt keine wirksame Einwilligung in die Durchführung derartiger Kontrollen dar.¹²⁸

Dem Verbot der Totalüberwachung kommt als Grenze für Kontrollmaßnahmen auch dann eigenständige Bedeutung zu, wenn die Kontrollmaßnahmen als solche in speziell geschützte Rechte des Mitarbeiters, z. B. in sein Recht auf informationelle Selbstbestimmung oder in das Telekommunikationsgeheimnis, eingreifen.

8.5.1.2 Datenschutzrechtliche Absicherung

Es wäre bspw. denkbar, eine Maßnahme als unzulässige Totalüberwachung und zugleich als rechtswidrige Datenerhebung zu qualifizieren. Das Verbot der Totalüberwachung schützt mithin vor der spezifischen Angriffsrichtung, die in der Verursachung eines kontinuierlichen „Anpassungs- und Überwachungsdrucks“¹²⁹ mit der möglichen Folge eines Einschüchterungseffekts liegt, dem sich der Arbeitnehmer nicht entziehen kann und der sich grundlegend vom Einsatz einer Aufsichtsperson unterscheidet.¹³⁰

8.5.1.3 Bezugspunkt der Totalüberwachung

Eine verbotene Totalüberwachung darf allerdings nicht vorschnell angenommen werden. Vielmehr ist jeweils im Einzelfall¹³¹ zu analysieren, welcher Anteil des Verhaltens

¹²⁴Vgl. BVerfG NJW 2004, 999 (1002); BeckOK Grundgesetz/Hillgruber GG Art. 1 Rn. 27.

¹²⁵Vgl. dazu BVerfG NJW 2004, 999 (1002).

¹²⁶Siehe dazu Kort RdA 2018, 24 (25) mit Verweis auf BAG NZA 2017, 1327; vgl. auch LAG Hamm ZD 2018, 92; BAG NJW 2005, 313 (314); Kühling/Buchner/Maschmann BDSG § 26 Rn. 42.

¹²⁷Vgl. zu dieser Überlegung BVerfG NJW 2012, 907 (909).

¹²⁸Vgl. ErfK/Schmidt GG Art. 2 Rn. 95.

¹²⁹So wörtlich das BAG NJW 2005, 313.

¹³⁰BAG NZA 1988, 92.

¹³¹Zu den Abwägungskriterien ausf. von Steinau-Steinrück/Glanz NJW Spezial 2008, 402.

eines Mitarbeiters für welchen Zeitraum unter welchen Gesichtspunkten erfasst wird. Darüber hinaus ist es denkbar, dass bestimmte Formen der Dauerüberwachung notwendiger Bestandteil einer Betätigung sind, z. B. die Tätigkeit an einem aus Sicherheitsgründen permanent videoüberwachten Bankschalter.¹³² Besonders große Bedeutung kommt der Prüfung der Frage zu, ob sich ein sachlicher Rechtfertigungsgrund für die Maßnahme finden lässt.

8.5.2 Auswirkungen auf typische Maßnahmen

8.5.2.1 Mitlesen von Bildschirmen

Der Arbeitnehmer kann beispielsweise in seinem Allgemeinen Persönlichkeitsrecht verletzt sein, wenn der Arbeitgeber das „Bildschirm-Verhalten“ seiner Mitarbeiter permanent ganztägig mit Überwachungssoftware beobachtet, indem er mittels eines installierten Kontrollprogramms die Tastatureingaben verfolgt.¹³³ Demgegenüber dürfte ein punktueller Einsatz derartiger Überwachungsmaßnahmen beispielsweise zulässig sein, um die veranlasste Fernwartung des Mitarbeiters überprüfen zu können.

8.5.2.2 Einsatz von Keylogger-Software

Typischerweise stellt der permanente die gesamte Arbeitszeit eines Mitarbeiters abdeckende Einsatz von Keylogger-Software eine verbotene Form der Totalüberwachung dar.¹³⁴ Keylogger-Software erfasst sämtliche während des Erfassungszeitraums über die Tastatur eines Computers eingegebenen Zeichen und zwar unabhängig davon, ob und in welchem Zusammenhang diese auf Applikationsebene (z. B. als Sätze in einem mit Hilfe des Textverarbeitungsprogramms erstellten Schreiben) gespeichert wurden.¹³⁵

8.5.2.3 Lückenlose Browser-Überwachung

Ein Verstoß gegen das Verbot der Totalüberwachung ist auch denkbar, wenn permanent eine lückenlose (z. B. welche Seiten wurden wann und wie lange angezeigt) Aufzeichnung der Benutzung des Internetbrowsers durch einen bestimmten Mitarbeiter angefertigt wird, wenn die Benutzung des Internetbrowsers einen hinreichenden großen Teil der Arbeitszeit des Mitarbeiters ausmacht.

¹³²Vgl. dazu ErfK/Schmidt GG Art. 2 Rn. 94 m. w. N.

¹³³Vgl. dazu ArbG Augsburg Beschluss vom 4.10.2012 – 1 BV 36/12, BeckRS 2013, 65588.

¹³⁴Vgl. BAG NZA 2017, 1327; siehe dazu auch Kort RdA 2018, 24 ff.

¹³⁵„Abwehrmaßnahmen“ des Arbeitnehmers gegen die Kontrollen sind jedoch ihrerseits unzulässig, BAG NZA 2006, 980; ob es ein Recht zu Datennotwehr gibt, ist zweifelhaft, vgl. Ronellenfitsch DuD 2008, 110.

8.5.3 Zusätzlicher Schutz bei Telefon- und Videoüberwachung

8.5.3.1 Schutz durch § 201 StGB

aa) Zum Tatbestand Die Totalüberwachung von Mitarbeitern ist auch durch die lückenlose Telefon- und Videoüberwachung denkbar.¹³⁶ Beide Überwachungsmaßnahmen können sich unter Umständen auch zur Kontrolle der Einhaltung von Vorgaben eignen, die Compliance im Unternehmen sicherstellen sollen. Dies begegnet aber jedenfalls dann rechtlichen Bedenken, wenn die Maßnahmen in der Ausprägung „Totalüberwachung“ eingesetzt werden. Wie die bereits genannten anderen Beispiele sind solche Maßnahmen schon wegen der mit ihnen umgesetzten Totalüberwachung und der darin liegenden Verletzung des Allgemeinen Persönlichkeitsrechts der betroffenen Mitarbeiter in aller Regel rechtswidrig. Selbst wenn die Maßnahmen der Telefon- und Videoüberwachung nur punktuell und gezielt – mithin nicht als Mittel der Totalüberwachung – zum Einsatz kommen sollen, unterliegen sie rechtlichen Schranken.

Für die Telefonüberwachung ist § 201 StGB zu beachten. Die Vorschrift erfasst Telefonate aber nur in Teilespekten: gemäß § 201 I StGB macht sich nur strafbar, wer das nicht öffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht. Gemäß § 201 II StGB macht sich ebenso strafbar, wer das nicht zu seiner Kenntnis bestimmte nicht öffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört oder das nach § 201 I Nr. 1 StGB aufgenommene oder nach § 201 II Nr. 1 StGB abgehörte nicht öffentlich gesprochene Wort eines anderen im Wortlaut oder seinem wesentlichen Inhalt nach öffentlich mitteilt.

bb) Reichweite des Schutzes Die von einem Mitarbeiter geführten Privatgespräche sind zwar ebenso wie dienstliche Telefonate ohne weiteres als „nicht öffentlich gesprochenes Wort“ gemäß § 201 StGB geschützt. Das bloße „Mithören“ bleibt aber straflos – „Tonträger“ sind allein Speichermedien, z. B. Tonbandgerät oder digitale Tonträger wie CD und DVD. Als „Abhörgeräte“ im Sinne von § 201 I StGB kommen alle zur Anfertigung einer dauerhaften Aufzeichnung von Sprache geeigneten Mittel in Betracht, d. h. auch eine computerbasierte Mitschneideeinrichtung, wenn ein Telefon an einen Computer angeschlossen ist.¹³⁷ Eine Strafbarkeit des Arbeitsgebers wegen des Mitschneidens von Telefonaten des Arbeitnehmers gemäß § 201 StGB kann aber abzulehnen sein, wenn Gespräche nach der Art des Berufs typischerweise mitgeschnitten respektive aufgezeichnet werden.¹³⁸ Zu denken ist insbesondere an Gespräche von Mitarbeitern eines Callcenters oder der Branche des Telefonbankings,¹³⁹ auch wenn hier typischerweise entsprechende vertragliche Regelungen vorliegen.

¹³⁶Vgl. z. B. BAG NZA 2017, 443; BAG NZA 2008, 1187; ausf. zur Videoüberwachung Venetis/Oberwetter NJW 2016, 1051.

¹³⁷Vgl. MüKoStGB/Graf StGB § 201 Rn. 2.

¹³⁸Vgl. dazu Oberwetter NZA 2008, 609 (611).

¹³⁹Vgl. Oberwetter NZA 2008, 609 (611); ausf. zur Arbeitnehmerkontrolle im Call-Center Jordan/Bissels/Löw BB 2008, 2626; vgl. auch Schröder DatenschutzR Kap. 3. VI. 2, 18 ff.

Auch nach Datenschutzrecht unterliegt das einfache Mithören über technisches Gerät Grenzen: das heimliche Mithören von Telefongesprächen ohne Wissen des Arbeitnehmers dürfte stets unzulässig sein.¹⁴⁰ Hat der Arbeitnehmer Kenntnis oder rechnet er zumindest damit, ist ein gelegentliches Mithören zulässig, sofern dadurch nicht das Persönlichkeitsrecht des (externen) Gesprächspartners beeinträchtigt wird.¹⁴¹

Die Telefondatenerfassung ist eingeschränkt möglich: soweit Telefongespräche dienstlich veranlasst sind, dürfen die Telefondaten zu einer Kosten- und Wirtschaftlichkeitskontrolle oder zum Schutz vor Missbrauch erhoben werden, da sie der Zweckbestimmung des Arbeitsverhältnisses dienen.¹⁴² Gleches gilt für die Erfassung dienstlich veranlasster Privatgespräche. Die Telefondaten dürfen aber nicht zur Verhaltenskontrolle herangezogen werden.¹⁴³

8.5.3.2 Schutz gemäß § 201 a StGB

aa) Zum Tatbestand Eine Videoüberwachung ist unzulässig, wenn die Aufzeichnung den Straftatbestand des § 201a StGB verwirklicht.¹⁴⁴ Gemäß § 201a StGB macht sich strafbar, wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt. Gemäß § 201a II StGB wird bestraft, wer eine durch eine Tat nach § 201a I StGB hergestellte Bildaufnahme gebraucht oder einem Dritten zugänglich macht. Gemäß § 201a III StGB wird bestraft, wer eine befugt hergestellte Bildaufnahme von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, wissentlich unbefugt einem Dritten zugänglich macht und dadurch deren höchstpersönlichen Lebensbereich verletzt. Geschütztes Rechtsgut aller Tatbegehungsalternativen des § 201a StGB ist der Schutz des Rechts am eigenen Bild als Ausprägung des Allgemeinen Persönlichkeitsrechts i. S. v. Art. 2 I i. V. m. Art. 1 I GG.¹⁴⁵

¹⁴⁰Vgl. zum heimlichen Mithören und Aufzeichnen von Telefonaten und Gesprächen etwa Kramer IT-ArbR/Tiedemann Rn. 510 f.; s. auch zum Mithören eines Telefonats BGH NJW 2003, 1727.

¹⁴¹Zur Sondersituation des „Silent Monitoring“ (Überwachung durch unbemerktes Aufschalten eines Supervisors) in einem Callcenter ausf. Bissels/Löw/Jordan, Arbeitnehmerkontrolle im Call-Center durch Silent Monitoring und Voice Recording, BB 2008, 2626 (2627): Hier steht gerade die Gesprächsleistung selbst als Arbeitsleistung im Fokus der Kontrolle. Eine anderweitige Kontrolle der Arbeitsleistung ist wegen der Anonymität des Vorgangs regelmäßig ausgeschlossen. Ein „offenes“ Mithören gibt kein tragfähiges Bild der Arbeitsleistung wieder. Daher soll hier ausnahmsweise auch das heimliche Mithören zulässig sein. AA Oberwetter NZA 2008, 609 (611).

¹⁴²Kramer IT-ArbR/Petri Kap. D Rn. 74.

¹⁴³Oberwetter NZA 2008, 609 (611).

¹⁴⁴Allgemein zur Videoüberwachung von Arbeitnehmern Venetis/Oberwetter NJW 2016, 1051; Byers/Wenzel BB 2017, 2036; Grimm/Schiefer RdA 2009, 329; s. auch BAG NZA 2017, 443; LAG Hamm ZD 2018, 92; LAG Düsseldorf ZD 2016, 443.

¹⁴⁵Kramer IT-ArbR/Petri Kap. D Rn. 14.

bb) Reichweite des Schutzes Eine Videoaufnahme am Arbeitsplatz kann unter dem Gesichtspunkt des „gegen Einblick besonders geschützten Raums“ unter § 201a StGB fallen. Voraussetzung ist allerdings ein „besonderer Schutz“ (wie bei einer Toilette oder Dusche), der gewöhnliche Büroräume dürfte nicht erfasst sein.¹⁴⁶ Für die generelle Beurteilung der Zulässigkeit von Videoüberwachungen ist zudem noch auf Art. 6 I f) DS-GVO bzw. § 4 BDSG hinzuweisen.¹⁴⁷

Auch wenn es für die Verwirklichung des objektiven Tatbestands von § 201a I StGB nicht darauf ankommt, ob die Überwachung offen oder verdeckt erfolgt, ist jedenfalls in **datenschutzrechtlicher** Hinsicht zwischen der heimlichen und der offenen Überwachung sowie der Zugänglichkeit des Raums zu differenzieren.¹⁴⁸ Sollen berechtigte Interessen des Arbeitgebers durch eine offene Videoüberwachung an einem öffentlich zugänglichen Raum geschützt werden (Videokamera am Bahnsteig, in einer Schalterhalle, im Kaufhaus), so ist dies zulässig, auch wenn der Mitarbeiter erfasst wird. Dies ist als arbeitsplatzimmanent¹⁴⁹ hinzuzunehmen. Vorauszusetzen ist aber ein entsprechender Hinweis nach Art. 13 DS-GVO. Nicht-öffentliche zugängliche Räume, wie Büroräume, fallen nicht unter § 4 BDSG, sodass hier eine Gesamtabwägung vorzunehmen ist; eine Berufung des Arbeitgebers auf das Hausrecht ist nicht möglich.¹⁵⁰ Allein mit dem Interesse an der Überwachung der Arbeitsleistung kann eine solche Kontrollmaßnahme nicht gerechtfertigt werden. Eine verdeckte Videoüberwachung ist wegen des Vorrangs der Arbeitnehmerinteressen regelmäßig unzulässig.¹⁵¹

Etwas anderes gilt nur bei überwiegendem Interesse des Arbeitgebers entweder gerade wegen besonderen Gefährdungslagen hinsichtlich des Arbeitsplatzes (Bankschalter), oder als „Quasi-Notwehr“¹⁵² bei schwerwiegender Verdacht strafbarer Handlungen oder anderer gleichrangiger Verfehlungen, sofern andere Mittel ausgeschöpft sind,¹⁵³ wenn also der

¹⁴⁶ Kramer IT-ArbR/Petri Kap. D Rn. 17; BeckOK StGB/Heuchemer StGB § 201a Rn. 15.

¹⁴⁷ Vgl. zu der Frage, inwieweit der deutsche Gesetzgeber unter Geltung der DS-GVO überhaupt noch befugt ist, die Zulässigkeit der Videoüberwachung in § 4 BDSG zu regeln, Kühling/Buchner/Buchner BDSG § 4 Rn. 2 ff. m. w. N. S. im Übrigen siehe auch DSK, Kurzpapier Nr. 15, Videoüberwachung nach der Datenschutz-Grundverordnung, https://www.lda.bayern.de/media/dsk_kpn_15_videoueberwachung.pdf (auferufen am 17.07.2024).

¹⁴⁸ Siehe zur verdeckten Videoüberwachung BAG NJW 2017, 1193; vgl. auch Venetis/Oberwetter NJW 2016, 1051; Bauer/Schansker NJW 2012, 3537; s. zu den Anforderungen an eine Überwachung nach DS-GVO und BDSG-neu Lachenmann ZD 2017, 407; Kramer IT-ArbR/Tiedemann Rn. 556 ff.

¹⁴⁹ Vgl. zu § 32 BDSG aF Beck'sches Rechtsanwalts-Handbuch/Heussen/Hamm § 49 Rn. 126; aA Grimm/Schiefer RdA 2009, 329 (333).

¹⁵⁰ BAG NZA 2005, 839 – dort auch zu den Anforderungen an den Nachweis berechtigter Interessen.

¹⁵¹ BAG NJW 2003, 3436, siehe auch EGMR, NZA 2019, 1697.

¹⁵² Vgl. dazu ErfK/Schmidt GG Art. 2 Rn. 94.

¹⁵³ BAG NJW 2003, 3436: Arbeitnehmer legt die Begehung der Straftat bewusst heimlich an. Beispiele vorrangiger Methoden bei Schwund bei Freckmann/Wahl BB 2008, 1904 (1905): Taschenkontrollen, (in Geschäften) Stichproben bei Kunden, Prüfung des Lieferumfangs, Einsatz von Detektiven.

Einsatz der Aufklärung eines bestimmten Verdachts bei einem begrenzten Personenkreis und nicht einer allgemeinen Verhaltenskontrolle dient. Auch dann ist aber der Einsatz möglichst minimalinvasiv zu gestalten, d. h. dass die Überwachung durch Personal am Bildschirm der Aufzeichnung durch ein Videogerät vorzuziehen ist. Die Aufklärung eines bestimmten Verdachts bedingt regelmäßig bereits eine zeitliche Befristung der Maßnahme, die räumlich nicht auf unbelastete Betriebsteile erweitert werden darf. Die Erweiterung würde eine verdachtsunabhängige und unbegrenzte Totalüberwachung darstellen, die unzulässig ist.¹⁵⁴

8.6 Kontrollmaßnahmen im Lichte des IT-Grundrechts

8.6.1 Schutzbereich des IT-Grundrechts

8.6.1.1 Herleitung und Schutzbereich

Das **BVerfG** hat in seiner Entscheidung vom 27.2.2008¹⁵⁵ aus Art. 1 I und Art. 2 II GG das Recht auf die Vertraulichkeit und Integrität informationstechnischer Systeme („IT-Grundrecht“) abgeleitet. Gegenstand der Entscheidung war die Online-Untersuchung nach Maßgabe bestimmter Vorschriften des Verfassungsschutzgesetzes Nordrhein-Westfalen.¹⁵⁶ Die ihrem Aussagegehalt nach für das Recht der IT-Sicherheit erheblichen Leitsätze des Urteils lauten in Auszügen wie folgt:

- Das allgemeine Persönlichkeitsrecht (Art. 2 I i. V. m. Art. 1 I GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.
- Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.

¹⁵⁴ BAG MMR 2008, 777 mAnm Domke BB 2008, 2748; stRspr seit BAG NZA 1988, 92; vgl. auch BVerfG NJW 2005, 1338 zum Verbot der Totalüberwachung bei strafprozessualen Zwangsmaßnahmen.

¹⁵⁵ BVerfG NJW 2008, 822 m. Anm. Bär, MMR 2008, 325.

¹⁵⁶ Ausführlich zur Begründung Hornung, CR 2008, 299 (300).

- Die heimliche Infiltration eines informationstechnischen Systems ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Das Gesetz, das zu einem solchen Eingriff ermächtigt, muss Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen.
- Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff an Art. 10 I GG zu messen.¹⁵⁷
 - a. Abgrenzung zum Recht auf informationelle Selbstbestimmung

Wie auch das Recht auf informationelle Selbstbestimmung wurde das IT-Grundrecht aus Art. 2 I i. V. m. Art. 1 I GG abgeleitet. Aus dieser Gemeinsamkeit resultiert die Frage der Abgrenzung der beiden Rechte.¹⁵⁸ Nach den Ausführungen des **BVerfG** schützt das IT-Grundrecht vor Eingriffen in informationstechnische Systeme.¹⁵⁹ Der Schutz durch das IT-Grundrecht greift nicht, soweit der Schutz durch andere Grundrechte, insbesondere Art. 10 oder Art. 13 GG, sowie das Recht auf informationelle Selbstbestimmung gewährleistet ist.¹⁶⁰ Für die nähere Ausgestaltung der Abgrenzung sind u. a. folgende Aussagen des **BVerfG** hilfreich:¹⁶¹

„196. Auch die bisher in der Rechtsprechung des Bundesverfassungsgerichts anerkannten Ausprägungen des allgemeinen Persönlichkeitsrechts, insbesondere die Gewährleistungen des Schutzes der Privatsphäre und des Rechts auf informationelle Selbstbestimmung, genügen dem besonderen Schutzbedürfnis des Nutzers eines informationstechnischen Systems nicht in ausreichendem Maße. (...) 199. Die mit dem Recht auf informationelle Selbstbestimmung abzuwehrenden Persönlichkeitsgefährdungen ergeben sich aus den vielfältigen Möglichkeiten des Staates und gegebenenfalls auch privater Akteure (...) zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Vor allem mittels elektronischer Datenverarbeitung können aus solchen Informationen weitere Informationen erzeugt und so Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen des Betroffenen beeinträchtigen als auch Eingriffe in seine Verhaltensfreiheit mit sich bringen können (...).“

8.6.1.2 Übertragbarkeit auf Verhältnisse am Arbeitsplatz

Eines der Hauptelemente der Begründung des **BVerfG** für die Ausprägung des IT-Grundrechts liegt in der Zwangsläufigkeit, mit der sich jeder Einzelne der modernen Datenverarbeitungstechnik bedienen muss. Diese Aussagen werden im Urteil nicht nur auf den Privatbereich beschränkt. Die entsprechenden Ausführungen lassen sich mit gewissen

¹⁵⁷Vgl. zum Urteil auch Petri, DuD 2008, 443 und Kutsch, NJW 2008, 1042; Vgl. auch Eifert, NVwZ 2008, 521; Holznagel/Schumacher, MMR 2009, 3.

¹⁵⁸Vgl. dazu auch Hoeren, MMR 2008, 365 ff.

¹⁵⁹Vgl. BVerfG NJW 2008, 822.

¹⁶⁰Vgl. BVerfG NJW 2009, 2431.

¹⁶¹BVerfG NJW 2008, 822 (826 f.).

Hürden auf die Verwendung von Datenverarbeitungstechnik am Arbeitsplatz übertragen.¹⁶²
Das **BVerfG** führt dazu wie folgt aus:¹⁶³

„Jedoch trägt das Recht auf informationelle Selbstbestimmung den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert. Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus.“

Die in der Entscheidung besonders deutlich zum Ausdruck kommende Ächtung heimlicher Datenerhebungen ist eine weitere Besonderheit des IT-Grundrechts. Zwar verpflichtet beispielsweise auch die dem Schutz des Rechts auf informationelle Selbstbestimmung dienende DS-GVO zur Transparenz bei der Verarbeitung (Art. 13, 14 DS-GVO) von personenbezogenen Daten. Der Schutz vor der Heimlichkeit einer Datenerhebung ist für den Schutzbereich des Rechts auf informationelle Selbstbestimmung aber nicht im gleichen Maße prägend wie für das IT-Grundrecht. Das BVerfG formuliert dies in folgender Weise:¹⁶⁴

„Das allgemeine Persönlichkeitsrecht in der hier behandelten Ausprägung schützt insbesondere vor einem heimlichen Zugriff, durch den die auf dem System vorhandenen Daten ganz oder zu wesentlichen Teilen ausgespäht werden können. Der Grundrechtschutz umfasst sowohl die im Arbeitsspeicher gehaltenen als auch die temporär oder dauerhaft auf den Speichermedien des Systems abgelegten Daten. Das Grundrecht schützt auch vor Datenerhebungen mit Mitteln, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben. So liegt es etwa bei einem Einsatz von sogenannten Hardware-Keyloggern oder bei einer Messung der elektromagnetischen Abstrahlung von Bildschirm oder Tastatur.“

Die wohl typischste und zugleich am schwersten zu diagnostizierende Voraussetzung für die Eröffnung des Schutzbereichs des IT-Grundrechts ist,¹⁶⁵ dass der Betroffene davon

¹⁶²Vgl. Holznagel/Schumacher, MMR 2009, 4, der aus der Entscheidung des BVerfG eine im Arbeitsverhältnis nicht ohne weiteres zu bejahende, in zwei Schritten zu vollziehende Prüfung der Eröffnung des Schutzbereichs des IT-Grundrechts ableitet, wonach erstens ein informationstechnisches System vorliegen muss, dem der Nutzer Daten im Glauben an deren Unzugänglichkeit anvertraut und zweitens dieses System geeignet sein muss, Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder ein aussagekräftiges Bild der Persönlichkeit zu erhalten.

¹⁶³BVerfG NJW 2008, 822 (827).

¹⁶⁴BVerfG NJW 2008, 822 (827).

¹⁶⁵Vgl. zu den Schwierigkeiten bei der Einordnung des IT-Grundrechts sowie zu offenen Fragen bei der Ermittlung der Voraussetzungen für die Eröffnung des Schutzbereichs auch Hoeren, MMR 2008, 365 ff.

ausgehen darf, das IT-System als eigenes und daher in selbstbestimmter Weise zu nutzen.¹⁶⁶ In der Entscheidung heißt es dazu:¹⁶⁷

„Der grundrechtliche Schutz der Vertraulichkeits- und Integritätserwartung besteht unabhängig davon, ob der Zugriff auf das informationstechnische System leicht oder nur mit erheblichem Aufwand möglich ist. Eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung besteht allerdings nur, soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt. Soweit die Nutzung des eigenen informationstechnischen Systems über informationstechnische Systeme stattfindet, die sich in der Verfügungsgewalt anderer befinden, erstreckt sich der Schutz des Nutzers auch hierauf.“

8.6.2 Auswirkungen auf Kontrollmaßnahmen

Unter Zugrundelegung allgemeiner dogmatischer Prinzipien findet das IT-Grundrecht auch im Arbeitsverhältnis Anwendung.¹⁶⁸ Es ist gegenwärtig allerdings noch offen, wie sich das IT-Grundrecht auf Kontrollmaßnahmen des Arbeitgebers auswirken wird und insbesondere, ob das IT-Grundrecht zu gegenüber dem Datenschutzrecht strengeren Anforderungen führen wird.¹⁶⁹

In der Diskussion um die Auswirkungen des IT-Grundrechts stellt sich die Frage, in welchen Grenzen der Arbeitgeber befugt ist, eine Kontrolle der IT-Systeme vorzunehmen, wenn und soweit die private Nutzung der IT-Systeme gestattet ist. Ist eine Nutzung ausschließlich zu dienstlichen Zwecken erlaubt, so dürfte es bereits an der Voraussetzung der Erwartung der Vertraulichkeit fehlen, weil der Arbeitnehmer das System nicht als „ihm zustehend“ nutzt.¹⁷⁰ Das Interesse des Arbeitgebers überwiegt in jedem Fall, sodass einer Kontrolle zumindest

¹⁶⁶Vgl. dazu auch Holznagel/Schumacher, MMR 2009, 4, der für die Anwendbarkeit des IT-Grundrechts davon ausgeht, dass Daten einem System anvertraut werden müssen, während das IT-Grundrecht nicht auf Konstellationen anwendbar sein soll, bei denen das System die Daten „eigenständig sammelt und speichert“.

¹⁶⁷BVerfG NJW 2008, 822 (827).

¹⁶⁸Vgl. MAH ArbR/Reichold § 96 Rn. 4 f.: ErfK/Schmidt GG Art. 2 Rn. 43; Hornung, CR 2008, 299 (303); Bartsch, CR 2008, 613 (614). Das BAG (NJW 2008, 3731, (3739)) hat lediglich ein Mitbestimmungsrecht des Betriebsrates nach § 87 I Nr. 6 BetrVG angenommen, wenn eine Regelung zur Computernutzung in einem US-Unternehmen vorsieht, dass „alle mit IT-Ressourcen des Arbeitgebers erstellte Daten keine privaten Informationen seien“ – unabhängig von der Wirksamkeit der Regelung nach deutschem Recht.

¹⁶⁹Vgl. zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und zu seinem Einfluss auf das Privatrecht Roßnagel/Schnabel, NJW 2008, 3534 ff.

¹⁷⁰Stögmüller, CR 2008, 435 (438): Der Arbeitnehmer hat bei Wartungsarbeiten u. ä. ein Anwesenheitsrecht, um die Überprüfung „seines“ Geräts verfolgen zu können; Daten, die Rückschlüsse auf das Nutzungsverhalten zulassen, müssen gelöscht werden; zu den Auswirkungen vgl. auch Roßnagel/Schnabel, NJW 2008, 3534 (3537).

hinsichtlich des IT-Grundrechts nichts im Wege stehen dürfte. Die Abwägung ist dann allein mit dem Recht auf informationelle Selbstbestimmung vorzunehmen.¹⁷¹

Bei erlaubter Privatnutzung besteht hingegen die Gefahr, dass das IT-Grundrecht das zur Verfügung gestellte System einer effektiven Kontrolle durch den Arbeitgeber entzieht. Dies gilt vor allem dann, wenn der Arbeitnehmer ausschließlich das dienstlich zur Verfügung gestellte System nutzt und auf jegliches Privatgerät verzichtet, weil der Arbeitnehmer dann durch eine entsprechende Kontrolle faktisch umfassend durchleuchtet werden könnte. Die erlaubte Privatnutzung ist möglicherweise sogar ein Ansporn für eine ausschließliche Nutzung, weil der Arbeitnehmer sich auf diese Weise der Kontrolle des Arbeitgebers entziehen könnte. Diese möglichen Auswirkungen des IT-Grundrechts bilden (neben den bereits genannten nachteiligen Folgen der Zulassung der privaten Nutzung von E-Mail und Internet) einen weiteren Anlass, die Privatnutzung der betrieblichen IT-Infrastruktur möglichst nicht zu gestatten.

Für die verschiedenen hierzu vertretenen Auffassungen wird auf die einschlägigen Veröffentlichungen verwiesen.¹⁷²

8.7 Sonstige Folgen unzulässiger Kontrollmaßnahmen

8.7.1 Beweisrechtliche Folgen

Neben den Rechtsfolgen, die sich bereits aus der Verletzung einer der genannten Grenzen für Kontrollmaßnahmen ergeben, sind die beweisrechtlichen Folgen in der Praxis häufig sehr erheblich, beispielsweise wenn aufgrund der Ergebnisse einer Kontrollmaßnahme eine Kündigung ausgesprochen werden soll.¹⁷³ Aus einer Entscheidung des **BAG** vom 13.12.2007 (**BAG** – 2 AZR 537/06) dazu hervor:¹⁷⁴

„Ein „Verwertungsverbot“ von Sachvortrag kennt das deutsche Zivilprozessrecht nicht. Der beigebrachte Tatsachenstoff ist entweder unschlüssig oder unbewiesen, aber nicht „unverwertbar“. Dies gilt umso mehr, wenn der Sachverhalt unstreitig ist. Das Gericht ist an ein Nichtbestreiten (wie auch an ein Geständnis) grundsätzlich gebunden (Baumbach/Lauterbach/Albers/Hartmann aaO § 128 Rn. 23). Es darf für unbestrittene Tatsachen keinen Beweis verlangen und erheben (Stein/Jonas/Leipold aaO § 138 Rn. 31 a). Die Annahme eines „Sachvortragsverwertungsverbots“, so wie ihn das Landesarbeitsgericht im Ergebnis angenommen hat, steht somit in deutlichem Widerspruch zu den Grundprinzipien des deutschen Zivil- und Arbeitsgerichtsverfahrens (siehe auch Heinemann, MDR 2001, 137, 140).“

¹⁷¹ Stögmüller, CR 2008, 435 (437).

¹⁷² Vgl. z. B. MAH ArbR/Reichold § 96 Rn. 4; Stögmüller, CR 2008, 435 (438); Holznagel/Schumacher, MMR 2009, 3.

¹⁷³ Vgl. zu Beweisverwertungsverboten bei privater Internetnutzung am Arbeitsplatz Kratz/Gubbels, NZA 2009, 652.

¹⁷⁴ BAG NJW 2008, 2732 ff. Rn. 24.

Aus der gleichen Entscheidung ergibt sich, dass ein prozessuales Verbot der Verwertung erst in Betracht kommt, wenn durch die Verwertung einer rechtswidrig erlangten Information oder eines Beweismittels ein erneuter bzw. perpetuierender Eingriff in rechtlich erheblich geschützte Positionen der anderen Partei erfolgt.¹⁷⁵ Allein die Verletzung eines Mitbestimmungstatbestands oder die Nichteinhaltung einer Betriebsvereinbarung und deren Verfahrensregelungen können es demnach grundsätzlich nicht rechtfertigen, einen entscheidungserheblichen, unstreitigen Sachvortrag der Parteien nicht zu berücksichtigen und im Ergebnis ein „Sachverhaltsverwertungsverbot“ anzuerkennen.¹⁷⁶ Ein Verwendungs- und Verwertungsverbot kommt zusammenfassend nur dann in Betracht, wenn durch eine Maßnahme Persönlichkeitsrechte des Mitarbeiters erheblich verletzt wurden.¹⁷⁷ In solchen Fällen können die im Rahmen einer Kontrollmaßnahme ermittelten Tatsachen nicht als Grundlage für arbeitsrechtliche Konsequenzen dienen.

In einer Entscheidung vom 20.6.2013 leitete das BAG (2 AZR 546/12)¹⁷⁸ aus einer Verletzung des Datenschutzrechts unmittelbar ein Beweisverwertungsverbot ab, ohne eine zusätzliche (d. h. außerhalb des BDSG verortete und möglicherweise beweisrechtlich geprägte) Interessenabwägung vorzunehmen. Der Ausgangspunkt der Analyse des BAG ist folgende Feststellung:

„1. Beweismittel sind nicht allein deshalb prozessual unverwertbar, weil der Beweisführer sie rechtswidrig erlangt hat. Ein Beweisverwertungsverbot, das zugleich die Erhebung der angebotenen Beweise ausschließt, kommt nur in Betracht, wenn der Schutzzweck der bei der Informationsgewinnung verletzten Norm einer gerichtlichen Verwertung um der Vermeidung eines Eingriffs in höherrangige Rechtspositionen willen entgegensteht.“

Im Hinblick auf die besondere Situation, in der sich der Arbeitgeber Beweise für ein vermutetes Eigentumsdelikt des Arbeitnehmers verschafft hat, kam das BAG in seiner Entscheidung vom 20.6.2013 dann jedoch zu dem Schluss, dass ein Beweisverwertungsverbot vorliegt. Ausschlaggebend für die Annahme eines Beweisverwertungsverbots war die Tatsache, dass der Arbeitgeber einen persönlichen Schrank des Arbeitnehmers ohne dessen Zustimmung und Kenntnis geöffnet und durchsucht hatte. Zur Begründung führt das BAG aus:

¹⁷⁵ BAG NJW 2008, 2732 ff. Rn. 30; vgl. auch Kopke, NZA 1999, 917 und BAG, NJW 2010, 104 (106 Rn. 22). „1. Das zivilrechtliche allgemeine Persönlichkeitsrecht des Gesprächspartners eines Telefongesprächs ist verletzt, wenn der andere einen Dritten durch aktives Handeln zielgerichtet veranlasst, das Telefongespräch heimlich mitzuhören. Aus der rechtswidrigen Erlangung des Beweismittels folgt ein Beweisverwertungsverbot: Der Dritte darf nicht als Zeuge zum Inhalt der Äußerungen des Gesprächspartners vernommen werden, der von dem Mithören keine Kenntnis hat. 2. Konnte ein Dritter zufällig, ohne dass der Beweispflichtige etwas dazu beigetragen hat, den Inhalt des Telefongesprächs mithören, liegt keine rechtswidrige Verletzung des zivilrechtlichen allgemeinen Persönlichkeitsrechts des Gesprächspartners vor. In diesem Fall besteht deshalb auch kein Beweisverwertungsverbot“.

¹⁷⁶ BAG NJW 2008, 2732 ff. Rn. 26.

¹⁷⁷ BAG NJW 2008, 2732 ff. Rn. 34; siehe dazu auch Riesenhuber, BeckOK Datenschutz BDSG § 26 Rn. 190 ff.

¹⁷⁸ BAG NZA 2014, 143.

„2. Arbeitnehmer müssen darauf vertrauen können, dass ihnen zugeordnete persönliche Schränke nicht ohne ihr Einverständnis geöffnet und durchsucht werden. Geschieht dies dennoch, liegt – unbeschadet einer möglichen Verletzung datenschutzrechtlicher Bestimmungen – regelmäßig ein schwerwiegender Eingriff in ihr allgemeines Persönlichkeitsrecht vor, dessen Schutz Art. 2 I GG gewährleistet. Der Eingriff kann nur bei Vorliegen zwingender Gründe gerechtfertigt sein. Hinzu kommt, dass die Heimlichkeit einer in Grundrechte eingreifenden Maßnahme das Gewicht der Rechtsbeeinträchtigung typischerweise erhöht. Schon deswegen ist die prozessuale Verwertung von Ergebnissen einer Schrankdurchsuchung ausgeschlossen, die in Abwesenheit des Arbeitnehmers durchgeführt wurde und in seinem Beisein ebenso effektiv gewesen wäre.“

Aus der auf das Datenschutzrecht gestützten Entscheidung des BAG zum Bestehen eines Beweisverwertungsverbots ist folgende Aussage für die Praxis erheblich:¹⁷⁹

„Die – bestrittene – Behauptung der Bekl., ihre Vorgehensweise sei mit zwei Mitgliedern des Betriebsrats abgestimmt gewesen, von denen eines an der Kontrolle teilgenommen habe, rechtfertigt kein anderes Ergebnis. Aus persönlichkeitsrechtlicher und datenschutzrechtlicher Sicht ist der Eingriff deshalb nicht weniger intensiv. Vielmehr ist davon auszugehen, dass die Privatsphäre des Arbeitnehmers umso stärker verletzt wird, je mehr Personen ohne sein Einverständnis an dem Eingriff beteiligt sind [...].“

Dieser beiläufige Hinweis des BAG dürfte einen in vielen Betriebsvereinbarungen enthaltenen Schwachpunkt zur Regelung von Kontrollmaßnahmen aufzeigen. So ist es nicht selten, dass die Betriebsparteien Kontrollverfahren vorsehen, bei denen ein oder mehrere Mitglieder des Betriebsrats anwesend sind.

Die weitere Entwicklung der Rechtsprechung wird zeigen, ob eine Parallele zwischen dem persönlichen Schrank eines Arbeitnehmers und der ihm zur privaten Nutzung (z. B. für die Abspeicherung privater Daten) zugewiesenen Partition der Festplatte seines Computers gezogen wird. Dies hätte möglicherweise zur Folge, dass die „privaten Partitionen“ einer Festplatte nicht ohne Kenntnis und Zustimmung des Arbeitnehmers untersucht werden können, weil andernfalls die Entstehung eines Beweisverwertungsverbots zu befürchten ist.

Im Detail sind die Voraussetzungen für ein Beweisverwertungsverbot allerdings noch nicht geklärt: Ob z. B. bei einer Videoaufzeichnung in einem öffentlich zugänglichen Raum bereits der bloße Verstoß gegen die Kennzeichnungspflicht i. S. v. § 4 I BDSG ausreicht, um ein Beweisverwertungsverbot zu begründen, hat die Rechtsprechung bislang noch nicht entschieden. Das Beweismittel, d. h. die Videoaufzeichnung, dürfte jedoch verwertbar sein, wenn auch die Voraussetzungen für eine heimliche Aufzeichnung vorliegen.¹⁸⁰

¹⁷⁹ BAG NZA 2014, 143 (148 Rn. 35).

¹⁸⁰ Oberwetter NZA 2008, 609 (610); möglicherweise sollte insgesamt zwischen heimlicher und verdeckter Aufzeichnung (bei letzterer rechnet der Betroffene allgemein mit der Möglichkeit) differenziert werden; s. zur Kennzeichnungspflicht des § 4 Abs. 2 BDSG Kühling/Buchner/Buchner BDSG § 4 Rn. 14 f.; vgl. im Übrigen zur heimlichen Kontrolle der Arbeitnehmer auch Byers NZA 2017, 1086, siehe dazu auch EGMR, NZA 2019, 1697.

8.7.2 Reputationsverlust

Auch wenn die erwähnten beweisrechtlichen Folgen auf den ersten Blick nicht im Zusammenhang mit der Gefahr des (als isolierte Folge dargestellten) Reputationsverlustes stehen, besteht über die Öffentlichkeit von Gerichtsverfahren ein typischer Anlass zur allgemeinen Diskussion über rechtlich angreifbare Methoden der Beweisgewinnung oder Totalüberwachung in einem Unternehmen. Diese Überlegung führt zu der offensichtlichen (wenn auch häufig nicht berücksichtigten) Empfehlung, nur solche Beweise in Gerichtsverfahren anzubieten, deren Erhebung und Verwendung im Einklang mit der Rechtsordnung stehen.

8.7.3 Maßnahmen von Aufsichtsbehörden

Die öffentliche Berichterstattung¹⁸¹ über unzulässige Kontrollmaßnahmen innerhalb eines Unternehmens kann als weiteren Nebeneffekt auch Maßnahmen der zuständigen Aufsichtsbehörden nach sich ziehen.

Welche Maßnahmen die zuständigen Aufsichtsbehörden im Einzelfall treffen können, regelt Art. 58 DS-GVO. Nach dessen Abs. 1–3 haben die Aufsichtsbehörden umfassende Befugnisse. Den Aufsichtsbehörden kommt nicht nur eine Untersuchungs-, sondern auch eine Abhilfe-, eine Genehmigungs- und eine beratende Befugnis zu.¹⁸² Die Befugnisse ergeben sich dabei unmittelbar aus der DS-GVO und eröffnen keinen mitgliedstaatlichen Umsetzungsspielraum.¹⁸³ § 40 BDSG findet insofern nur insoweit Anwendung, als die Vorschrift gegenüber Art. 58 DS-GVO eine Ergänzung der Befugnisse der Aufsichtsbehörde bewirkt.¹⁸⁴

8.7.4 Sonstige Ansprüche und Rechte der Betroffenen

Der Arbeitnehmer hat ferner einen deliktischen Anspruch auf Unterlassung und Be seitigung unzulässig erlangter Aufzeichnungen analog §§ 823 I, 1004 BGB, einen datenschutzrechtlichen Löschungsanspruch aus Art. 17 DS-GVO¹⁸⁵ und einen Schadensersatzanspruch aus Art. 82 DS-GVO.¹⁸⁶

¹⁸¹ Dabei ist bspw. zu denken an die (mutmaßlichen) „Datenschutzskandale“ bei Lidl, Aldi, Telekom oder der Deutschen Bahn, vgl. z. B. <https://www.tagesspiegel.de/wirtschaft/ueberwachung-am-arbeitsplatz-big-boss-is-watching-you/11391628.html> (aufgerufen am 17.07.2024).

¹⁸² Vgl. zu Einzelheiten etwa Kühling/Buchner/Boehm DS-GVO Art. 58 Rn. 13 ff.

¹⁸³ Vgl. Kühling/Buchner/Boehm DS-GVO Art. 58 Rn. 1.

¹⁸⁴ Vgl. dazu BeckOK DatenschutzR/Brink/Wilhelm BDSG § 40 Vor Rn. 1.

¹⁸⁵ Ausführlich dazu Kühling/Buchner/Herbst DSGVO Art. 17 Rn. 1 ff.

¹⁸⁶ Vgl. dazu Kühling/Buchner/Bergt, DSGVO Art. 82 Rn. 1 ff.

und einen Schadensersatzanspruch aus § 823 BGB, §§ 7, 8 BDSG wegen der Verletzung des Art. 1 GG i. V. m. § 253 BGB durch eine Totalüberwachung.

Er kann bezüglich seiner Arbeitsleistung ein Zurückbehaltungsrecht geltend machen, solange er bei der Erbringung der Arbeitsleistung unzulässigen Überwachungsmaßnahmen ausgesetzt ist.

8.7.5 Strafrechtliche und ordnungswidrigkeitenrechtliche Folgen

Rechtswidrige Datenverarbeitungen zulasten von Mitarbeitern können gemäß § 42 BDSG Straftaten und gemäß Art. 83 DS-GVO i. V. m. § 41 BDSG Ordnungswidrigkeiten darstellen. Der Bußgeldrahmen von Art. 83 DS-GVO reicht je nach verletzter Vorschrift bis zu 10.000.000 oder 20.000.000 € oder 2 % beziehungsweise 4 % des konzernweiten Jahresumsatzes.¹⁸⁷



Michael Schmidl ist Co-Leiter der deutschen Informationstechnologie Praxisgruppe und ist im Münchener Büro von Baker McKenzie ansässig und unter anderem als Top IT-Anwalt in der Wirtschaftswoche 2023 ausgezeichnet. Er ist Honorarprofessor an der Universität Augsburg und Fachanwalt für IT-Recht.

Michael Schmidl berät in allen Bereichen des streitigen und unstreitigen Informationstechnologie-rechts, einschließlich Internet-, Computer/Software-, Datenschutz- und Medienrecht. Er berät auch in Fragen des geistigen Eigentums, des unlauteren Wettbewerbs, der Compliance und des allgemeinen Vertragsrechts. Michael Schmidl hat Erfahrung im allgemeinen Wirtschaftsrecht und ist ebenfalls erfahren in der Gestaltung und Verhandlung von Outsourcing-Verträgen sowie in der Durchführung von Compliance-Projekten.

Michael Schmidl hält regelmäßig Vorträge für externe Seminarbieter sowie Inhouse-Seminare bei (inter-)nationalen Unternehmen zu Themen des E-Commerce, des Datenschutzes, der IT-Sicherheit und ist Autor zahlreicher Aufsätze, Bücher und Buchbeiträge sowie Kommentarbeiträge zu Themen des IT-Rechts.

¹⁸⁷ Siehe dazu DSK, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14.10.2019, https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf (aufgerufen am 17.07.2024).



Hinweisgebersysteme als Bestandteil eines effektiven Compliance-Managements

9

Carolin Püschel und Sascha Süße

Inhaltsverzeichnis

9.1	Begriffsdefinitionen	196
9.1.1	Whistleblowing	196
9.1.2	Hinweisgeber (Whistleblower)	198
9.1.3	Internes und externes Whistleblowing	198
9.1.4	Compliance-Management-Systeme und Hinweisgeberschutz	200
9.2	Rechtliche Grundlagen	201
9.2.1	Zu den Regelungen des Sarbanes-Oxley Act	202
9.2.2	Weitere internationale Regelungen	203
9.2.3	Europäische Rechtsprechung	204
9.2.4	Einzelgesetzliche Regelungen des Hinweisgeberschutzes in Deutschland	205
9.2.4.1	Zum Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)	206
9.2.4.2	Zum Lieferkettensorgfaltspflichtengesetz (LkSG)	207
9.2.5	(Gescheiterte) Vorhaben zur Etablierung eines gesetzlichen, flächendeckenden Hinweisgeberschutzes in Deutschland	208
9.2.6	Zur Hinweisgeberschutzrichtlinie der EU	210
9.2.6.1	Zum Ziel und Regelungsgehalt der Richtlinie	210
9.2.6.2	Zum Vertragsverletzungsverfahren der EU-Kommission gegen Deutschland	212

C. Püschel
PARK Wirtschaftsstrafrecht, Dortmund, Deutschland

S. Süße (✉)
Kanzlei Dr. Süße, Kalkar, Deutschland
E-Mail: suesse@kanzlei-suesse.de

9.2.7	Das Hinweisgeberschutzgesetz	213
9.2.7.1	Ziel: Schutz von Hinweisgebern	214
9.2.7.2	Gesetzgebungsprozess	214
9.2.7.3	Systematik und Regelungsgehalt	215
9.2.7.3.1	Aufbau, Anwendungsbereich und vorgesehene Sanktionen ...	215
9.2.7.3.2	Verhältnis der internen und externe Meldestelle(n) nach dem HinSchG	217
9.3	Einführung eines Hinweisgeberschutzgesetzes im Unternehmen	218
9.3.1	Gründe für die Einführung eines Hinweisgebersystems	218
9.3.2	Arten von Hinweisgebersystemen	219
9.3.2.1	Telefon-Hotline	219
9.3.2.2	Internetbasiertes Hinweisgebersystem	219
9.3.2.3	Ombudsmann/-frau bzw. Vertrauensanwalt/-anwältin	220
9.3.3	Anforderungen des HinSchG an die interne Meldestelle	221
9.3.3.1	Pflicht zur Einrichtung einer internen Meldestelle	221
9.3.3.2	Organisation und Aufgaben der internen Meldestelle	222
9.3.3.3	Einrichtung von Meldekanälen	224
9.3.3.4	Verfahren bei internen Meldungen und Folgemaßnahmen	225
9.3.4	Implementierung der internen Meldestelle im Unternehmen	225
9.3.4.1	Besetzung und Auswahl der Meldestelle	225
9.3.4.2	Meldestellen im Konzern	226
9.3.4.3	Auswahl der Meldekanäle	228
9.3.4.4	Abwägung der Vor- und Nachteile der verschiedenen Meldekanäle	228
9.3.4.5	Konkrete Auswahl	231
9.3.4.6	Interne Richtlinien und Kommunikation	232
9.3.4.7	Kommunikation und Integration	232
9.4	Rechtliche Einzelfragen	233
9.4.1	Arbeitsrechtliche Fragestellungen	233
9.4.2	Datenschutzrechtliche Fragestellungen	234
9.4.2.1	Grundsätzliches	235
9.4.2.2	Pflicht zur Benennung eines Datenschutzbeauftragten	236
9.4.3	Strafrechtliche Fragestellungen	237
9.5	Zusammenfassung	239
	Literatur	240

9.1 Begriffsdefinitionen

9.1.1 Whistleblowing

Egal, ob Gammelfleisch-Skandal, Missstände im Pflegeheim, Betrug bei Krebsmedikamenten, Panama Papers, oder LuxLeaks – die Meldung und Veröffentlichung von Hinweisen auf Missstände durch sogenannte Hinweisgeber, auch Whistleblowing genannt, steht heutzutage mehr denn je im Fokus von Unternehmen, Wissenschaft und medialer Öffentlichkeit. Dies gilt umso mehr als es in Deutschland seit dem 2. Juli 2023 – nach mehr als 10 Jahren diverser erfolgloser Anläufe – erstmals eine flächendeckende, branchenunabhängige gesetzliche Regelung für den Schutz von Hinweisgebern gibt (sog. Hinweis-

geberschutzgesetz – HinSchG).¹ Über den Umfang und die Ausgestaltung der damit zusammenhängenden Regelungen war – trotz des zunehmenden Drucks seitens der EU, die nationale Umsetzung der EU-Richtlinie 2019/1937 des Europäischen Parlaments und des Rats vom 23. Oktober 2019 (Hinweisegeberschutzrichtlinie)² voranzutreiben (hierzu ausführlich unter Abschn. 9.2.7) – sowohl in der Politik als auch in der Öffentlichkeit lange und zuletzt geradezu erbittert gestritten worden. Auch auf Compliance-Tagungen gehört das Thema „Whistleblowing“ nach wie vor zu den am meisten diskutierten und nicht selten auch umstrittenen Compliance-Themen.

Der Begriff „Whistleblowing“ im Allgemeinen lässt sich vom Englischen „to blow the whistle“ ableiten, was wörtlich „pfeifen“, „jemanden verpfeifen“ oder auch „abpfeifen“ bedeutet. Zurückgeführt wird er auf das Pfeifen der Londoner Schutzpolizisten oder auch des Schiedsrichters, der mit seiner Trillerpfeife einen Regelverstoß anzeigt. Beide machen die Öffentlichkeit auf etwas aufmerksam.³

Im Kontext von Compliance beschreibt der Begriff Whistleblowing allgemein das Aufmerksammachen auf Fehlverhalten und Missstände durch – zumeist – einen Mitarbeiter eines Unternehmens oder einen externen Dritten, der über entsprechendes Wissen über regelwidrige Vorkommnisse verfügt. Zum Whistleblowing kommt es dann, wenn der Hinweisgeber nicht bereit ist, diese Missstände hinzunehmen, und sich – ggf. unter Geheimhaltung seiner Identität – mit einem Abhilfegesuch an das Unternehmen oder externe Stellen, wie die Staatsanwaltschaft oder Journalisten, wendet.

Ein angemessener deutscher Begriff für Whistleblowing ist nur schwer zu finden. Die bereits benannte Übersetzung des „Verpfeifens“ lässt erkennen, welche Bedenken dem Whistleblowing in Deutschland gegenüberstehen. Wertneutralere Übersetzungen sind daher Begrifflichkeiten wie „etwas anzeigen“ und „auf etwas hinweisen“; auch vom Informanten, Enthüller oder Aufdecker ist zuweilen die Rede. Das am 2. Juli 2023 in Kraft getretene HinSchG, das unter Abschn. 9.2.7 und 9.3.3 ausführlich besprochen wird, verwendet den Begriff der „hinweisgebenden Personen“. Nach der im HinSchG enthaltenen Legaldefinition versteht das Gesetz unter diesem Begriff „natürliche Personen, die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese an die nach diesem Gesetz vorgesehenen Meldestellen melden oder offenlegen“ (vgl. § 1 Abs. 1 HinSchG). Auch um dem Begriff und der dahinterstehenden Zielsetzung jegliche negative Wertung zu nehmen, wird daher in den folgenden Ausführungen überwiegend der Begriff des Hinweisgebers verwendet.

Die unterschiedlichen Organisationstrukturen, die Unternehmen vorhalten können, um einem potenziellen Hinweisgeber die geschützte Möglichkeit der Hinweisabgabe

¹ Gesetz für einen besseren Schutz hinweisgebender Personen (Hinweisegeberschutzgesetz – HinSchG) vom 31.5.2023.

² EU-Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden.

³ Vgl. Groneberg, R. (2011), Whistleblowing – Eine rechtsvergleichende Untersuchung des US-amerikanischen, englischen und deutschen Rechts unter besonderer Berücksichtigung des Entwurfs eines neuen § 612a BGB, S. 34; siehe zur Historie des Begriffs auch: Schemmel, A., Ruhmannseder, F./Witzigmann, T. (2012), Hinweisegebersysteme, Implementierung im Unternehmen, 1. Kapitel, Rn. 7 f.

zur Verfügung zu stellen, werden entsprechend unter dem Oberbegriff „Hinweisgeber-systeme“ zusammengefasst.

9.1.2 Hinweisgeber (Whistleblower)

Liegen in einem Unternehmen Missstände vor, weil beispielsweise erhebliche Arbeitsschutzmaßnahmen nicht eingehalten werden, oder kommt es zu Fehlverhalten einzelner Mitarbeiter, wie beispielsweise dem Verlangen nach unberechtigten Geldzahlungen für die Beauftragung bestimmter Dienstleister (also Korruptionshandlungen), sehen sich Mitarbeiter, die dies beobachten, aber selbst nicht über die Macht oder die Mittel verfügen, etwas an dem Missstand zu ändern, einem Dilemma ausgesetzt:

Einerseits erkennen sie, dass das Verhalten nicht rechtens ist und es dem Unternehmen schadet oder dass sogar offensichtliche Straftaten begangen werden und damit erhebliche Gefahren verbunden sein können. So kann neben finanziellen Schädigungen des Unternehmens als Folge des Missstandes unter Umständen auch eine ernsthafte Gefährdung der körperlichen Unversehrtheit von Kollegen oder Dritten drohen. Der erste Impuls eines Hinweisgebers dürfte es in vielen Fällen sein, den konkret betroffenen Mitarbeiter oder den für einen bestimmten Zustand organisatorisch Verantwortlichen auf diesen Umstand anzusprechen oder, wenn dies nicht gelingt, den Vorgesetzten hierauf aufmerksam zu machen.

Andererseits kann die Aussicht, als Nestbeschmutzer zu gelten,⁴ abschreckend wirken, und es dürfte nicht zuletzt auch die Sorge bestehen, als Verräter, Oberaufseher oder – umgangssprachlich bezeichnet – als Petze dazustehen. Auch wird nicht selten befürchtet, dass das Verhältnis zu der von dem Hinweis betroffenen Person nach einem Hinweis auf absehbare Zeit zerstört ist und aber gleichzeitig mit dieser Person weiterhin zusammen gearbeitet werden muss. Noch schwieriger wird die Situation, wenn es sich bei der von dem Hinweis betroffenen Person nicht nur um einen Kollegen, sondern um den Vorgesetzten handelt oder aber wenn das beobachtete Verhalten oder der Zustand seitens der Unternehmensleitung geduldet oder gar gestützt bzw. gefördert werden.

9.1.3 Internes und externes Whistleblowing

Dass Mitarbeiter entsprechende Verhaltensweisen dennoch melden bzw. offenbaren, ist in der Vergangenheit auch ohne den gesetzlichen Schutz durch das HinSchG vorgekommen. Die Mittel der Wahl sind in diesen Fällen insbesondere Hinweise an den Vorgesetzten oder eine andere Stelle im Unternehmen. Nicht selten sind es auch anonyme Briefe, die, sofern der Hinweisgeber davon ausgeht, dass es sich um eine nicht vom Unternehmen gedeckte Verhaltensweise handelt, an die Unternehmensleitung gerichtet werden. In den Fällen, in denen eine Involvierung der Unternehmensleitung vorliegt oder angenommen wird, lan-

⁴Baade, I./Hößl, T., DStR 2023, 1213.

den entsprechende Briefe oftmals anonym bei der Staatsanwaltschaft oder bei der Presse. Letzteres droht auch gerade dann, wenn der Hinweisgeber sich nicht von ehrbaren Motiven leiten lässt, sondern von der Intention getrieben ist, Einzelnen oder dem Unternehmen insgesamt zu schaden. Eine solche Motivation ist jedoch eher selten – in der weit überwiegenden Anzahl der Fälle wollen Hinweisgeber Abhilfe und Gerechtigkeit erreichen.⁵

Aber auch bei einem in guter Absicht abgegebenen externen Hinweis gerät das Unternehmen durch solche Hinweise an Stellen außerhalb der Unternehmenssphäre in eine defensive Position. Der Hinweis auf das Fehlverhalten wird ihm dann von dritter Seite mitgeteilt, also von außen. Die Hinweiserteilung durch den Hinweisgeber geht damit (zunächst) am Unternehmen vorbei und führt regelmäßig zu direkten, nicht oder nur schwer kontrollierbaren Reaktionen der Außenwelt. In Betracht kommen die Einleitung eines Ermittlungsverfahrens durch die Strafverfolgungsbehörden, mit den damit verbundenen Möglichkeiten öffentlichkeitswirksamer Ermittlungsmaßnahmen, wie etwa Durchsuchungen, oder eine negative Presseberichterstattung, die die (vermeintlichen) Missstände öffentlich macht. Die Folgen, insbesondere Ausmaß und Ablauf externer Untersuchungen, sind für das Unternehmen nur bedingt steuerbar, jedenfalls aber in ihrer Dynamik in der Regel schwer absehbar.⁶ Bei öffentlichem Bekanntwerden der Hinweise tritt aufgrund der Schnelllebigkeit des Mediengeschehens zudem regelmäßig zu einem frühen Zeitpunkt ein unwiederbringlicher Reputationsverlust ein; der formelhafte in der Berichterstattung enthaltene Hinweis auf die Unschuldsvermutung verhält oftmals in der öffentlichen Wahrnehmung.⁷ Diese, für das Unternehmen daher meist schädliche, Form des Whistleblowings wird als externes Whistleblowing bezeichnet.

Abzugrenzen von diesen Sachverhalten ist das interne Whistleblowing, also die Abgabe von Hinweisen durch Mitarbeiter oder Dritte, die zunächst an das Unternehmen selbst gerichtet sind. Als Adressaten entsprechender Meldungen kommen etwa die Geschäftsleitung, die Personalabteilung oder eine hierfür vom Unternehmen ausdrücklich benannte interne Stelle, wie beispielsweise der Compliance Officer, in Betracht. Ferner zählen zum internen Whistleblowing auch solche Fälle, in denen ein vom Unternehmen beauftragter, externer Rechtsanwalt bzw. eine beauftragte externe Rechtsanwältin als Hinweisempfänger/-in bzw. als sogenannte Ombudsperson fungiert und in dieser Funktion im Auftrag des Unternehmens unmittelbar zur Entgegennahme von Hinweisen berechtigt und verpflichtet ist (ausführlich hierzu unter Abschn. 9.2.3).⁸

Internes Whistleblowing ermöglicht es dem Unternehmen, zunächst ohne äußeren Druck die Validität des Hinweises zu überprüfen und gegebenenfalls erforderlich werdende, weitere Untersuchungshandlungen anzustellen. Zudem wird das Unternehmen in die Lage versetzt, den Missstand eigenständig abstellen zu können und – mit wenigen

⁵ Benne, R., CCZ 2014, 189 (189 f.).

⁶ Ausführlich zu den Risiken und Unwägbarkeiten staatlicher Ermittlungsverfahren, die parallel zu internen Untersuchungen geführt werden Süße, S./Püschel, C., CEJ 2016, 39 ff.

⁷ Lehr, G. in: Müller/Schllothauer/Knauer, Münchener Anwaltshandbuch Strafverteidigung, 3. Auflage 2022, § 21 Rn. 19.

⁸ Egger, M., CCZ 2018, 126 (129, 131 f.).

Ausnahmen – über das Ob und gegebenenfalls das Wann des Herantretens an Ermittlungsbehörden und die Öffentlichkeit selbst zu bestimmen.

Durch das HinSchG ist nun eine weitere Unterscheidung hinzugekommen. Das Gesetz sieht zum einen interne Meldestellen in Unternehmen und Behörden vor (§§ 12 ff. HinSchG), zum anderen u. a. bspw. beim Bund eingerichtete externe Meldestellen (§§ 19 ff. HinSchG). Beide werden im Laufe dieses Beitrags noch genauer beleuchtet werden (vgl. insb. Abschn. 9.2.7.3.2 zum Verhältnis der internen und externen Meldestelle nach dem HinSchG sowie Punkt 3.3. zu den Anforderungen des HinSchG an die interne Meldestelle).

9.1.4 Compliance-Management-Systeme und Hinweisgeberschutz

Unternehmen haben – wie bereits gezeigt – naturgemäß ein hohes Interesse daran, dass personen- oder umstandsbezogene Gesetzes- oder sonstige Regelverstöße so frühzeitig entdeckt und abgestellt werden, dass das Risiko eines ernsthaften Schadenseintritts, einer Rufschädigung und einer staatlichen Sanktion möglichst gering gehalten wird. Eine entsprechende Sanktion könnte etwa die Leitungsebene(n) des Unternehmens oder das Unternehmen selbst betreffen (§§ 30, 130 OWIG). Die Bedeutung der Einführung eines diese Risiken aufgreifenden Compliance-Management-Systems ist daher insbesondere seit den 1980er-Jahren stetig gestiegen. Motor für diese Entwicklungen waren gesetzgeberische Aktivitäten in den USA und seit Anfang der 2000er-Jahre auch die steigende Zahl von Regelwerken, die einen international verstandenen Anspruch auf Beachtung bestimmter Compliance Grundsätzen erheben.⁹ Die sanktionsmildernde bzw. -ausschließende Wirkung von Compliance-Management-Systemen ist dabei in Deutschland noch nicht allgemein gültig normiert. Seit dem Jahr 2017 haben entsprechende Klarstellungen jedoch zumindest Eingang in die höchstrichterliche Rechtsprechung des Bundesgerichtshofes gefunden.¹⁰

Ein Compliance-Management-System ist auf die Vorbeugung, Aufdeckung und Abstellung von Gesetzes- oder sonstigen Regelverstößen aus der Unternehmensphäre gerichtet. Um die diesbezügliche Effektivität des Compliance-Management-Systems gewährleisten zu können, bedarf es daher verschiedener Maßnahmen, um entsprechende Risiken oder Missstände schnell erkennen zu können. Das unter Punkt 1.3. beschriebene interne Whistleblowing kann dabei einen wichtigen Beitrag zur Risikoentdeckung leisten; denn potenzielle Hinweisegeber werden im Rahmen ihrer (Arbeits-)Tätigkeit typischerweise unmittelbarer, schneller und häufiger mit relevanten Sachverhalten konfrontiert als die Unternehmensleitung.¹¹

Um zu vermeiden, dass interne Hinweise an unterschiedlichen Stellen im Unternehmen eingehen, ohne dass ihre Weiterleitung an die zuständige Compliance-Stelle oder die Ge-

⁹ Siehe etwa zum UK Bribery Act Süße, S./Püschel, C., ZRFC 2015, 82 ff.

¹⁰ Siehe BGH, Urteil vom 9.5.2017 – 1 StR 265/16 sowie BGH, Urteil vom 27.4.2022 – Az. 5 StR 278/21.

¹¹ Vgl. auch Erwägungsgrund 1 der Richtlinie (EU) 2019/1937.

schäftsleitung sichergestellt ist, und nicht zuletzt um die Hinweisbereitschaft zu fördern, bietet es sich dabei an, ein Hinweisgebersystem einzuführen, das konkrete Strukturen voraussetzt und mit einem Höchstmaß an Transparenz aufzeigt, wie Hinweise behandelt werden und was die möglichen Folgen sind.

Bei all dem bleibt zu beachten, dass internes Whistleblowing nur funktioniert, wenn das Unternehmen bzw. seine Geschäftsleitung ernsthaft gewillt sind, Missstände oder Fehlverhalten abzustellen und dem Hinweisgeber für den Fall einer Meldung keine Repressalien drohen. Denn hinweisgebende Personen, die sich aufgrund ihres hohen Wertearanspruchs und ihrer ethischen Persönlichkeitsstruktur häufig als Einzelkämpfer gegen Missstände sehen, neigen regelmäßig zur Eskalation bzw. Skandalisierung ihres Meldeverhaltens an höhere oder externe Instanzen, wenn sie realisieren, dass ihre Initiative ohne Effekt verhallt.¹² Ein unternehmensseitig transparent kommuniziertes, ernst gemeintes Hinweisgeber(schutz)system kann demgegenüber als Katalysator für die Abgabe von Hinweisen auf Missstände wirken. Dadurch erhöht sich nicht zuletzt auch das Entdeckungsrisiko, sodass nicht nur dem Entstehen von Missständen, sondern auch Gelegenheitsverstößen effektiv begegnet wird. Und auf der anderen Seite müssen Hinweisgeber, die Hinweise in gutem Glauben abgeben, davor geschützt werden, gekündigt, versetzt oder anderweitig Seitens des Unternehmens sanktioniert zu werden. Dieser wichtige Aspekt ist Kern und Ziel sowohl der EU-Hinweisgebersrichtlinie als auch des HinSchG. §§ 33 HinSchG definieren insofern die Schutzmaßnahmen zu Gunsten eines Hinweisgebers.

Es wird abzuwarten bleiben, ob der nunmehr durch das Hinweisgeberschutzgesetz vorgegebene organisatorische Rechtsrahmen zu einer Stärkung des Vertrauens in die Arbeit der internen Meldestellen und des damit verbundenen Hinweisgeberschutzes führen wird. Eines jedoch muss jedem Hinweisgeber klar sein: Letzten Endes wird auch jede noch so gute Umsetzung der Vorgaben des Hinweisgeberschutzgesetzes nicht vollends ausschließen können, dass es zu einer Offenlegung der Person des Hinweisgebers und daran anknüpfend möglicherweise auch zu hinweisbezogenen Repressalien durch die von dem Hinweis betroffenen Personen (wenn auch nicht das Unternehmen) kommen wird. Denn wenn die im Rahmen der Hinweisabgabe mitgeteilten Informationen in Anbetracht der Unternehmensgröße oder des spezifischen Wahrnehmungskontextes zwangsläufig auf eine bestimmte Person zurückgeführt werden können, bleibt Anonymität ein frommer Wunsch. Whistleblowing bleibt damit zu einem gewissen Teil stets ein persönliches Wagnis der hinweisgebenden Person.

9.2 Rechtliche Grundlagen

Bis zum 2. Juli 2023 gab es keine flächendeckende gesetzliche Verpflichtung für Unternehmen in Deutschland, ein Hinweisgebersystem einzuführen. Nur vereinzelt waren Unternehmen aufgrund spezialgesetzlicher Vorgaben oder internationaler Regelungen

¹² Benne, R., CCZ 2014, 189.

zwingend mit den damit verbundenen Fragestellungen konfrontiert (vgl. Abschn. 9.2.1 und 9.2.2). Ebenso fehlte es an expliziten gesetzlichen Regelungen zum Schutz von Hinweisgebern. In den vergangenen 20 Jahren war das allgemein verbindliche Mindestmaß an Hinweisgeberschutz in Deutschland daher vor allem durch die zivil-, arbeits- und europarechtliche Rechtsprechung geprägt (vgl. Abschn. 9.2.3). Erst nach und nach wurden für bestimmte Teilbereiche des Wirtschaftslebens gesetzliche oder quasi-gesetzliche Regelungen bzw. Standards zur Vorhaltung von Hinweisgebersystemen und zum Schutz von Hinweisgebern geschaffen (vgl. Punkt 2.4). Mit der Verabschiedung der EU-Richtlinie 2019/1937 des Europäischen Parlaments und des Rats vom 23. Oktober 2019 und im Zuge der Umsetzung dieser Richtlinie in nationales Recht sind Hinweisgebersysteme in Deutschland seit dem 2. Juli 2023 (nahezu) flächendeckend verpflichtend geworden (vgl. Abschn. 9.2.5).

9.2.1 Zu den Regelungen des Sarbanes-Oxley Act

In den USA ist Whistleblowing seit langem ein gesetzlich normiertes Instrument zur Bekämpfung von insbesondere Wirtschaftsstraftaten.¹³ Spätestens seit der Einführung des Sarbanes-Oxley Act (kurz „SOX“ genannt) im Jahr 2002 ist es ein anerkannter Weg im Rahmen der Bestrebungen und Verpflichtungen von Unternehmen, regelkonformes Verhalten ihrer Mitarbeiter, Organe und des Unternehmens sicherzustellen.

Die Vorhaltung einer solchen Hinweisstelle als Bestandteil der Compliance-Maßnahmen eines Unternehmens ist für an einer US-Börse notierte Unternehmen gesetzlich verankert. Nach Section 301 (4) SOX werden diese Unternehmen zur Einführung eines internen Meldesystems verpflichtet, das es Mitarbeitern ermöglicht, anonym vertrauliche Hinweise zu bedenklichen Buchhaltungs- und Revisionspraktiken zu geben. Section 301 (4) SOX lautet insofern:

Section 301 SOX

- “(4) COMPLAINTS.—Each audit committee shall establish procedures for—
 - “(A) the receipt, retention, and treatment of complaints received by the issuer regarding accounting, internal accounting controls, or auditing matters; and
 - “(B) the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters.

Diese Regelungen des SOX haben seit jeher Ausstrahlungswirkung auch auf deutsche Unternehmen. Sec. 301 SOX ist unmittelbar auf alle Unternehmen und deren Tochtergesellschaften anwendbar, die an einer US-amerikanischen Börse notiert sind, also auch

¹³ Siehe dazu: Schürre, T./Fleck, F., CCZ 2011, 218.

auf solche deutschen Unternehmen.¹⁴ Ergänzt werden diese durch Regelungen des Dodd-Frank-Acts, der den Anwendungsbereich einzelner Regeln auf nicht selbst börsennotierte Töchter- und Schwestergesellschaften eines börsennotierten Unternehmens erweitert.¹⁵

Die konkrete Ausgestaltung des Whistleblowing-Systems wurde dabei nicht im Detail geregelt, sondern kann nach Ermessen des Audit Committees bestimmt werden.

Auch nach Verabschiedung des Hinweisgeberschutzgesetzes bestehen gravierende Unterschiede in der Herangehensweise an das Thema „Whistleblowing“, u. a. in der staatlichen Förderung der Abgabe von Hinweisen in den USA und in Deutschland. So hat etwa die U.S. Securities and Exchange Commission (SEC) – die US-amerikanische Börsenaufsicht – am 5. Mai 2023 bekannt gegeben, dass sie einer Person, die auf Missstände bei der Beachtung von Regularien im Aufsichtsbereich der SEC hingewiesen und die SEC bei der Aufklärung der damit zusammenhängenden Umstände unterstützt hatte, die höchste Summe gezahlt hat, die im Rahmen des sog. Whistleblower Award Programs jemals ausgeschüttet worden ist. Konkret wurde dem Hinweisgeber eine Belohnung in Höhe von 279 Mio. USD gezahlt; bis dato war im Oktober 2020 der höchste Wert einer Whistleblowing-Prämie erreicht worden (114 Mio. USD). Entsprechende Zahlungen stammen aus einem Fonds für Anlegerschutz, der über die Geldstrafen derjenigen finanziert wird, die insbesondere gegen börsenrechtliche Vorgaben verstoßen. Überschreitet die einzelfallbezogene Geldstrafe eine Summe von 1 Mio. USD, kann dem jeweiligen Hinweisgeber aus diesem Fonds eine Belohnung zwischen 10 und 30 % der Geldstrafe zugesprochen werden.¹⁶

Von einer derart massiven staatlichen Förderung des Whistleblowings sind wir in Deutschland (noch) weit entfernt.

9.2.2 Weitere internationale Regelungen

Auf internationaler Ebene wurde das Thema Whistleblowing und Hinweisgeberschutz insbesondere im Zusammenhang mit der Bekämpfung von Korruption diskutiert. Beispielhaft sei hier das im Europarat geschlossene Zivilrechtsübereinkommen über Korruption genannt. Dieses sieht in seinem § 9 vor, dass „Beschäftigte, die den zuständigen Personen oder Behörden in gutem Glauben einen begründeten Korruptionsverdacht mitteilen, angemessen vor ungerechtfertigten Nachteilen geschützt werden.“¹⁷ Auch Artikel 33 des

¹⁴ Vgl. hierzu Reufels, M./Deviard, K., CCZ 2009, 201 (201 ff.); Berndt, T./Hoppler, I., BB 2005, 2623 (2625 f); Obermayr, G. in Hauschka, C./Moosmayer, K./Lösler, T. (2016), § 44 Rn. 111.

¹⁵ Siehe dazu: Schürle, T./Fleck, F., CCZ 2011, 218 (221).

¹⁶ Weitere Informationen sind auf der Seite des SEC zu finden: <https://www.sec.gov/news/press-release/2023-89> (aufgerufen am 14.1.2024).

¹⁷ Dieses Übereinkommen war bislang von Deutschland noch nicht ratifiziert worden; siehe hierzu die Gesetzesbegründung zum Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (kurz: Gesetzentwurf der Bundesregierung), A. I., S. 32 f.

Übereinkommens der Vereinten Nationen gegen Korruption vom 31. Oktober 2003 zielt auf den Schutz von Personen ab, die gegenüber den zuständigen Behörden „in redlicher Absicht und mit hinreichender Begründung“ Angaben zu bestimmten Straftaten machen.¹⁸

9.2.3 Europäische Rechtsprechung

Mit Blick auf den allgemeinen, sprich branchenunabhängigen, Mindestschutz von Hinweisgebern in Deutschland waren daher lange Zeit zuvorderst die – auf den Einzelfall naturgemäß nur bedingt übertragbaren – Vorgaben des Europäischen Gerichtshofs für Menschenrechte (EGMR) aus einer Grundsatzentscheidung vom 21. Juli 2011 maßgebend.¹⁹ In dem der Entscheidung zugrunde liegenden Fall ging es insbesondere um die Frage, ob die außerordentliche Kündigung einer Angestellten, die ihren Arbeitgeber bei der Staatsanwaltschaft Berlin wegen vermeintlich strafbarer Handlungen angezeigt hatte, gegen Artikel 10 der Europäischen Menschenrechtskonvention (EMRK) verstoßen hatte. Dieser Artikel schützt die Freiheit der Meinungsäußerung. Der EGMR nahm bei seiner Entscheidung auf die im Fall *Guja v. Moldova*²⁰ im Jahr 2008 entwickelten Kriterien für die Frage des Schutzes von Hinweisgebern bei einer Enthüllung oder Veröffentlichung unrechtmäßiger Vorgänge am Arbeitsplatz durch hinweisgebende Beamte Bezug und stellte klar, dass Whistleblowing auch außerhalb des öffentlichen Dienstes von dem sachlichen Schutzbereich des Artikel 10 EMRK erfasst sei.²¹ Dieser sei auch verletzt worden, da die deutschen Gerichte im Rahmen der erforderlichen Abwägung zwischen den Rechten und Interessen des Arbeitgebers einerseits – hier die Pflicht des Arbeitnehmers zur Loyalität und Verschwiegenheit – und der Interessen der Hinweisgeberin einschließlich der Interessen der Allgemeinheit andererseits an der Aufdeckung und Sanktionierung entsprechender Verstöße keinen angemessenen Ausgleich herbeigeführt hätten.²²

Die Voraussetzungen, unter denen eine Veröffentlichung von Verdachtsmomenten bzw. Hinweisen auf (mögliche) Verstöße vom Schutzbereich des Artikels 10 EMRK umfasst ist, sind vom EGMR seither konsequent fortentwickelt und präzisiert worden. Ausgangspunkt war in diesem Zusammenhang in der Regel die Beurteilung der Rechtmäßigkeit einer Kündigung des Hinweisgebers durch seinen Arbeitgeber nach öffentlicher Mitteilung (möglicher) Missstände oder Gesetzesverstöße.²³

¹⁸ Gesetzesbegründung zum Gesetzentwurf der Bundesregierung, A. I., S. 33 f., mit weiteren Beispielen auf internationaler Ebene.

¹⁹ EGMR, Urteil vom 21.7.2011, Beschwerde-Nr. 28274/08, Heinisch v. Germany. Siehe hierzu Simon, O./Schilling, J.M., BB 2011, 2421 (2424 ff.).

²⁰ EGMR, Urteil vom 12.2.2008, Beschwerde-Nr. 14277/04, Guja v. Moldova.

²¹ Vgl. Rz. 43 ff. der Entscheidung.

²² Vgl. Rz. 93 ff. der Entscheidung.

²³ Vgl. hierzu etwa EGMR, Urteil vom 8.1.2013, Beschwerde-Nr. 40238/02, Bucur and Toma v. Romania; Urteil vom 21.10.2014, Beschwerde-Nr. 73571/10, Matúz v. Hungary; Urteil vom 16.2.2021, Beschwerde-Nr. 23922/19, Gawlik v. Liechtenstein.

In dem jüngst vom EGMR entschiedenen Fall *Halet v. Luxemburg* ging es demgegenüber um eine straf- und schadensersatzrechtliche Verurteilung eines Hinweisgebers. Der Hinweisgeber hatte zum Zwecke der Aufdeckung komplexer Steuervermeidungsmodelle zugunsten internationaler Konzerne in Luxemburg vertrauliche Steuerdokumente an einen Journalisten herausgegeben (sog. LuxLeaks). Insoweit stellte sich die Frage, ob eine strafrechtlich sanktionierte Veröffentlichung vertraulicher Geschäftsinformationen durch Hinweisgeber nach den vom EGMR aufgestellten Kriterien von der in Artikel 10 Abs. 1 EMRK geschützten Freiheit der Meinungsäußerung geschützt sein kann oder ob die insoweit erfolgte Verurteilung mit Artikel 10 Abs. 2 EMRK vereinbar war. Diese Norm erlaubte allerdings nur solche Strafandrohungen, „*die gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sind für die nationale Sicherheit, die territoriale Unversehrtheit oder die öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung oder zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral, zum Schutz des guten Rufes oder der Rechte anderer; zur Verhinderung der Verbreitung vertraulicher Informationen oder zur Wahrung der Autorität und der Unparteilichkeit der Rechtsprechung*“ (vgl. Artikel 10 Abs. 2 Halbsatz 2 EMRK). Auch in diesem Fall nahm der EGMR eine Verletzung der Meinungsfreiheit aus Artikel 10 EMRK an. Hierzu führte er u. a. aus, dass im Rahmen der gebotenen Interessenabwägung für den entscheidungsgegenständlichen Fall maßgeblich zu berücksichtigen gewesen sei, dass das öffentliche Interesse an der Offenlegung von Informationen zu als solches in der Öffentlichkeit wahrgenommenen Missständen auch dann überwiegen könne, wenn der Hinweisgeber besonderen Geheimhaltungs- und Verschwiegenheitspflichten unterliege, er die fraglichen Informationen unter Vornahme eines strafrechtlich relevanten Verhaltens beschaffe und es sich bei den in Rede stehenden Missständen selbst nicht formal um rechtswidrige Umstände handele.²⁴

9.2.4 Einzelgesetzliche Regelungen des Hinweisgeberschutzes in Deutschland

Der Weg zu einem gesetzlichen und allgemein verbindlichen Hinweisgeberschutzgesetz in Deutschland war lang. Zu Beginn der 2000er-Jahre steckten sowohl der Hinweisgeberschutz als auch das allgemeine Bewusstsein für die positiven Auswirkungen der Förderung des Whistleblowings noch in den Kinderschuhen. Vereinzelt gab es Interessenzusammenschlüsse, wie etwa das 2006 gegründete Whistleblower-Netzwerk, die sich in der Öffentlichkeit für eine Verbesserung des rechtlichen Schutzes und des Ansehens von Hinweisgebern in Deutschland einsetzten.

Nur langsam und vereinzelt wurden gesetzliche Regelungen zur Vorhaltung von Hinweisgebersystemen und zum Hinweisgeberschutz etabliert, die zudem auch einen verhältnismäßig engen Anwendungsbereich hatten. Teilweise resultierten diese aus

²⁴Vgl. EGMR, Urteil vom 14.2.2023, Beschwerde-Nr. 21884/18, *Halet v. Luxembourg*; vgl. Fila, D./Ostermeister, N., CCZ 2023, 118 (120).

europarechtlichen Vorgaben.²⁵ Hierzu zählen bspw.²⁶ § 23 Abs. 6 VAG²⁷ oder § 4d Abs. 1 FinDAG.²⁸

Größere, zusammenhängende Regelungssysteme, die (auch) Regelungen zu dem Umgang mit Whistleblowing enthalten, hat es demgegenüber erst in der jüngeren Zeit gegeben. Hierzu zählen u. a. das im Jahr 2019 in Kraft getretene Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) und das im Jahr 2021 in Kraft getretene Lieferketten-sorgfaltspflichtengesetz (LkSG). Beide Gesetze werden im Folgenden kurz näher betrachtet.

9.2.4.1 Zum Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)

Eine erste allgemeingültige, wenngleich ebenfalls nur mit einem engen Anwendungsbereich versehene, Regelung zu Whistleblowing findet sich in dem im Jahr 2019 in Kraft getretenen Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG).²⁹ Dieses regelt insbesondere aus zivilrechtlicher Sicht den Schutz von Geschäftsgeheimnissen, sieht in § 23 GeschGehG aber auch eine Strafnorm vor. Die früheren diesbezüglichen Regelungen der §§ 17–19 UWG wurden in der Folge aufgehoben.³⁰

Das GeschGehG enthält in §§ 4, 5 Nr. 2 konkrete Regelungen zu den Voraussetzungen der Zulässigkeit des Umgangs mit einem Geschäftsgeheimnis aus Gründen des Whistleblowings: § 4 GeschGehG definiert zunächst Handlungsverbote bezüglich der Erlangung, Nutzung und Offenlegung von Geschäftsgeheimnissen. Verstöße hiergegen sind unter bestimmten Voraussetzungen strafbar nach dem vorgenannten § 23 GeschGehG. § 5 GeschGehG bestimmt jedoch Ausnahmen von § 4 GeschGehG, also Konstellationen, in denen ein eigentlich verbotenes Handeln doch ausnahmsweise erlaubt ist. Strukturell handelt es sich dabei – anders noch als in einem früheren Entwurf des GeschGehG – nicht um einen Rechtfertigungegrund, sondern bereits um einen Tatbestandsausschluss.³¹

Nach § 5 Nr. 2 GeschGehG liegt kein Verbot gemäß § 4 GeschGehG vor, wenn die Erlangung, Nutzung oder Offenlegung des Geschäftsgeheimnisses zur Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens erfolgt und sie dazu geeignet ist, das allgemeine öffentliche Interesse zu schützen. Vereinfacht gesagt, ist in diesen Fällen also die Offenlegung im Rahmen einer Hinweiserteilung erlaubt.

Aus dieser Formulierung ergeben sich für die Praxis durchaus Schwierigkeiten, wozu insbesondere die Auslegung der Begriff des „sonstigen Fehlverhaltens“ gehört sowie die

²⁵ Siehe hierzu ausführlich die Gesetzesbegründung zum Gesetzentwurf der Bundesregierung, A. I., S. 32.

²⁶ Siehe für weitere Beispiele: Egger, M., CCZ 2018, 126 (127).

²⁷ Kritisch dazu Bürkle, J., VersR 2020, 1.

²⁸ Im Einzelnen: Johnson, D., CB 2016, 468.

²⁹ Siehe dazu ausführlich: Süße, S. in Rotsch, T. (2021), S. 379 (397 ff.).

³⁰ BGBI. I 2019, S. 472.

³¹ Vgl. BT-Drs. 19/8300, S. 14.

Frage, wann eine „Geeignetheit zum Schutz des öffentlichen Interesses“ vorliegt.³² Dessen ungeachtet erkennt das Gesetz an, dass eine Notwendigkeit für Hinweisgeber bestehen kann, sogar Geschäftsgeheimnisse preiszugeben.

9.2.4.2 Zum Lieferkettensorgfaltspflichtengesetz (LkSG)

Auch das Lieferkettensorgfaltspflichtengesetz (LkSG) sieht die Einrichtung eines angemessenen Beschwerdeverfahrens vor. Von dem personellen Anwendungsbereich des Gesetzes sind seit dem 1. Januar 2024 alle Unternehmen ungeachtet ihrer Rechtsform erfasst, die ihre Hauptverwaltung, ihre Hauptniederlassung, ihren Verwaltungssitz oder ihren satzungsmäßigen Sitz oder eine Zweigniederlassung gemäß § 13d HGB im Inland haben und in der Regel mindestens 1000 Arbeitnehmenden im Inland beschäftigen (vgl. § 1 Abs. 1 LkSG).³³

Der sachliche Anwendungsbereich des Beschwerdeverfahrens bezieht sich auf die Meldung von menschenrechtlichen und umweltbezogenen Risiken, also von Zuständen, bei denen aufgrund tatsächlicher Umstände mit hinreichender Wahrscheinlichkeit ein Verstoß gegen eines der in § 2 Abs. 2 und Abs. 3 LkSG gelisteten Verbote droht, sowie entsprechenden bereits eingetretenen, beobachteten Verletzungen. Erfasst sind dabei nicht nur Verstöße im unmittelbaren Unternehmensbereich, sondern auch entlang der Lieferkette, d. h. sowohl von unmittelbaren wie mittelbaren Lieferanten (vgl. § 3 LkSG).

Die Pflicht zur Einführung eines Beschwerdemanagementsystems und die Vorgaben für das nähere Beschwerdeverfahren folgen aus § 8 LkSG. Die Einzelheiten des Verfahrens sind danach in wesentlichen Aspekten identisch mit den Vorschriften des HinSchG, etwa hinsichtlich der vertraulichen Behandlung von Beschwerden und Meldungen und der Unabhängigkeit der mit der Entgegennahme von Beschwerden bzw. Meldungen beauftragten Stelle (hierzu sogleich unter Abschn. 9.3.2).³⁴ Anders als das HinSchG sieht das LkSG jedoch keine Konsequenz für eine missbräuchliche Inanspruchnahme des Beschwerdeverfahrens vor (vgl. § 38 HinSchG). Ein weiterer Unterschied liegt darin, dass das LkSG die Veröffentlichung einer Verfahrensordnung in Textform vorsieht (§ 8 Abs. 2 LkSG). Eine solche explizite Vorgabe macht das HinSchG nicht; dessen ungeachtet dürfte die Formulierung schriftlicher unternehmensinterner Regelungen zur Entgegennahme und Bearbeitung von Hinweisen auch unter dem Hinweisgeberschutzgesetz faktisch unverzichtbar sein. Die Gesetze unterscheiden sich ferner hinsichtlich der spezifischen Löschungsfristen, die für ihren jeweiligen Anwendungsbereich gelten (vgl. § 11 Abs. 5 HinSchG und § 10 Abs. 1 Satz 2 LkSG). Dies ist im jeweiligen Lösungskonzept entsprechend zu berücksichtigen.

³² Siehe Stüße, S. in Rotsch, T. (2021), S. 379 (399 f.). Siehe zudem OLG Oldenburg, Beschluss vom 21. Mai 2019 – 1 Ss 72/19, NZWiSt 2021, 30 sowie Colneric, N./Gerdemann, S. (2023), § 5 GeschGehG Rn. 30 ff.

³³ Details zu der Berechnung der Arbeitnehmendenzahl finden sich in § 1 Abs. 2 und 3 LkSG.

³⁴ S. auch die Gegenüberstellung bei Bürger, K./von Dahlen, A., DB 2023, 829 ff.

Insgesamt wird damit deutlich, dass die Gemeinsamkeiten überwiegen und es sich in der Praxis anbieten kann, ein gemeinsames System zur Erfüllung der Unternehmenspflichten aus dem LkSG und dem HinSchG zu implementieren.

9.2.5 (Gescheiterte) Vorhaben zur Etablierung eines gesetzlichen, flächendeckenden Hinweisgeberschutzes in Deutschland

Wie bereits erwähnt hat es lange gedauert, bis es in Deutschland erstmalig zu einer gesetzlichen Normierung der Rechte und Pflichten sowie des Schutzes von Hinweisgebern gekommen ist. Ausgangspunkt der Diskussion speziell der letzten ca. 15 Jahre war das Bekanntwerden des sogenannten „Gammelfleisch-Skandals“ im Jahr 2008. In Reaktion auf die Aufdeckung des Skandals durch einen Hinweisgeber wurde ein Vorschlag für eine gesetzliche Verankerung eines Informantenschutzes in einem neuen § 612a BGB-E diskutiert. Ziel dieser Regelung sollte es laut Gesetzesbegründung sein, „*eine klare und eindeutige Regelung im Bereich des Informantenschutzes zu schaffen und damit die Rechtsicherheit für Arbeitnehmer, die über gesetzeswidrige Praktiken in ihrem Unternehmen informieren, zu verbessern.*“³⁵ Nach erheblicher Kritik verschiedener Verbände wurde das Gesetzgebungsverfahren jedoch nicht weiter verfolgt.³⁶

Nachfolgend gab es weitere erfolglose Versuche der Normierung eines gesetzlichen, flächendeckenden Hinweisgeberschutzes, darunter insbesondere die Folgenden:

Im Juli 2011 – mithin im unmittelbaren zeitlichen Zusammenhang mit der Grundsatzentscheidung des EGMR im Altenpflegefall i. S. *Heinisch v. Germany* (vgl. hierzu oben Abschn. 9.2.3) – forderte die Fraktion DIE LINKE die damalige Bundesregierung dazu auf, einen Entwurf für die Einführung eines gesetzlichen Hinweisgeberschutzes vorzulegen.³⁷

Bis zur Entscheidung *Heinisch v. Germany* hatte die Rechtsprechung eine Rechtfertigung zur Preisgabe von Missständen stets nur für den jeweils konkreten Einzelfall geprüft. Im Februar 2012 wurde daher seitens der oppositionellen SPD-Fraktion der Entwurf eines Gesetzes zum Schutz von Hinweisgebern – Whistleblowern (Hinweisgeberschutzgesetz – HinwGebSchG) in den Bundestag eingebracht, der dieser, Rechtsunsicherheit Rechnung tragen sollte. Zudem sollte ein besserer Schutz hinweisgebender Arbeitnehmer vor arbeitsrechtlichen Nachteilen normiert werden.³⁸ Der Entwurf wurde im Rahmen der 2. Lesung im Bundestag am 13. Juni 2013 mit den Stimmen von CDU/CSU, FDP und BÜNDNIS 90/DIE GRÜNEN abgelehnt.

³⁵Vgl. Ausschussdrucksache 16 (19) 849, S. 2.

³⁶Siehe nur die Stellungnahme des Deutschen Anwaltvereins hierzu, Stellungnahme 31/2008, abrufbar unter www.anwaltverein.de (aufgerufen am 7.2.2024).

³⁷Vgl. BT-Drs. 17/6492.

³⁸Vgl. BT-Drs. 17/8567, S. 1; zu alldem sowie zur Kritik an dem Entwurf siehe Mengel, A., CCZ 2012, 146 (148).

Das gleiche Schicksal ereilte einen im Wesentlichen gleich gerichteten Entwurf der Fraktion BÜNDNIS 90/DIE GRÜNEN aus Mai 2012.³⁹

Die nächsten beiden Anläufe zur Einführung eines flächendeckenden Mindestschutzes für Hinweisgeber wurden von der sich jeweils in der Opposition befindenden Fraktion BÜNDNIS 90/DIE GRÜNEN in der 18. und 19. Legislaturperiode in den Jahren 2014⁴⁰ und 2018⁴¹ unternommen. Der Entwurf aus dem Jahr 2014 sah Änderungen in mehreren Einzelgesetzen vor, so u. a. im Bürgerlichen Gesetzbuch und dem Strafgesetzbuch, und sollte die Voraussetzungen dafür schaffen, dass ein Hinweisgeber sich sowohl an eine (außer)betriebliche als auch an eine (außer)dienstliche Stelle oder Behörde und auch direkt an die Öffentlichkeit wenden kann.⁴² Im Juni 2015 wurde der Gesetzentwurf mit den Stimmen der Großen Koalition abgelehnt. Dem im Koalitionsvertrag vereinbarten Prüfauftrag, der da lautete „*Informantenschutz im Arbeitsverhältnis – Beim Hinweisgeberschutz prüfen wir, ob die internationalen Vorgaben hinreichend umgesetzt sind.*“⁴³ sollte aber trotzdem weiter nachgekommen werden.⁴⁴

Im Juni 2016 wurde die Risikolage für Hinweisgeber in Deutschland auf der Konferenz der Justizminister der Länder stark kritisiert. Die Landesjustizminister forderten die Bundesregierung in diesem Zusammenhang dazu auf, den Bedarf an einer effektiveren Regelung des Schutzes von Hinweisgebern in Form eines Gesetzes „*angesichts der gesellschaftlichen Bedeutung von frühzeitigen Hinweisen auf Missstände in Unternehmen, Behörden und Organisationen und im Hinblick auf internationale Vorgaben*“ erneut zu prüfen.⁴⁵

Zwischenzeitlich wurden in der Finanzdienstleistungsbranche im Juli 2016 durch eine Reform des Finanzdienstleistungsaufsichtsgesetzes durch das Erste Finanzmarktnovellierungsgesetz (konkret insbesondere § 4d FinDAG, s. oben Abschn. 9.2.4) Fakten geschaffen und gesetzliche Vorschriften zum Schutz von Hinweisgebern sowie zur Pflicht der in der Finanzdienstleistungsbranche tätigen Institute zur Einrichtung entsprechender Beschwerdemechanismen geschaffen. Begleitend hierzu richtete auch die BaFin eine Meldeplattform für Whistleblower ein. Hintergrund dieser Neuerungen war die gebotene Umsetzung mehrerer europäischer Rechtsakte in nationales Recht.⁴⁶

³⁹Vgl. BT-Drs. 17/9782.

⁴⁰Entwurf für ein Gesetz zur Förderung von Transparenz und zum Diskriminierungsschutz von Hinweisgeberinnen und Hinweisgebern (Whistleblower-Schutzgesetz; BT-Drs. 18/3039).

⁴¹Vgl. BT-Drs. 19/4558.

⁴²Siehe Newsdienst Compliance 2014, 31027.

⁴³Siehe Koalitionsvertrag der 18. Wahlperiode des Bundestages, S. 70.

⁴⁴Siehe Newsdienst Compliance 2015, 31019.

⁴⁵Siehe den Beschluss der 87. Konferenz der Justizministerinnen und -minister zu Top I.7, https://www.justiz.nrw.de/JM/jumiko/beschluesse/2016/Fruehjahrskonferenz_2016/index.php, (aufgerufen am 14.1.2024).

⁴⁶Vgl. BT-Drs. 18/7482.

Auch der von der Fraktion BÜNDNIS 90/DIE GRÜNEN im September 2018 vorgelegte – in weiten Teilen unveränderte – Entwurf eines Gesetzes zur Förderung von Transparenz und zum Diskriminierungsschutz von Hinweisgeberinnen und Hinweisgebern (Whistleblower-Schutzgesetz) konnte nicht durchdringen; er erledigte sich durch Ablauf der Wahlperiode im Jahr 2021.⁴⁷

9.2.6 Zur Hinweisgeberschutzrichtlinie der EU

Ab Mitte 2018 wurden die nationalen Anläufe einer gesetzlichen Regelung eines Hinweisgeberschutzgesetzes bereits durch die erforderlich werdende Umsetzung der Richtlinie (EU) 2019/1937 vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, überlagert. Ausgangspunkt der Richtlinie war eine offizielle Empfehlung des Ministerausschusses des Europarats aus dem Jahr 2014, die sich für ein europäisches Mindestschutzniveau von Hinweisgebern in bestimmten Bereichen aussprach.⁴⁸ Auf die Inhalte dieser Empfehlung gestützt, veröffentlichte die Europäische Kommission am 23. April 2018 einen Richtlinienvorschlag zum Schutz von Whistleblowern.⁴⁹ Über diesen Vorschlag konnte sodann – nach zwischenzeitlichen Rückschlägen – am 11. März 2019 eine Einigung auf europäischer Ebene erzielt werden.⁵⁰

9.2.6.1 Zum Ziel und Regelungsgehalt der Richtlinie

Ziel der Richtlinie ist es, dass europaweit „gemeinsame Mindeststandards zur Gewährleistung eines wirksamen Hinweisgeberschutzes in Rechtsakten und Politikbereichen gelten, in denen die Notwendigkeit besteht, die Rechtsdurchsetzung zu verbessern, eine unzureichende Meldung von Verstößen durch Hinweisgeber die Rechtsdurchsetzung wesentlich beeinträchtigt und Verstöße gegen das Unionsrecht das öffentliche Interesse ernsthaft schädigen können.“⁵¹

Die Richtlinie enthält insgesamt 29 Artikel, deren Struktur und Inhalt wie folgt zusammengefasst werden können:

Die ersten 6 Artikel skizzieren den sachlichen und persönlichen Anwendungsbereich der Richtlinie (Artikel 2, 4) sowie die notwendigen Begriffsbestimmungen (Artikel 5). So dann werden Voraussetzungen aufgestellt, unter denen die Abgabe eines Hinweises unter den hohen Schutz der Richtlinie fallen soll (Artikel 6). Zudem thematisiert die Richtlinie das Rangverhältnis zu anderen sektorspezifischen Unionsrechtsakten und nationalen Bestimmungen, etwa in Bezug auf die Existenz spezifischer Regelungen über die Meldung von Verstößen; diese gehen den Bestimmungen in der Richtlinie vor (vgl. Artikel 3 Abs. 1).

⁴⁷Vgl. BT-Drs. 19/4558; siehe Newsdienst Compliance 2018, 33012.

⁴⁸Vgl. Newsdienst Compliance 2014, 32130.

⁴⁹Vgl. Newsdienst Compliance 2018, 32007.

⁵⁰Vgl. Newsdienst Compliance 2019, 72007.

⁵¹Vgl. Erwägungsgrund 5 der Richtlinie EU 2019/1937; vgl. auch Artikel 1 der Richtlinie.

In den persönlichen Anwendungsbereich fällt jeder Hinweisgeber, der im privaten oder im öffentlichen Sektor tätig ist und im beruflichen Kontext Informationen über Verstöße erlangt hat. Hierunter fallen gemäß Artikel 2 der Richtlinie Arbeitnehmer im Sinne von Artikel 45 Absatz 1 AEUV, einschließlich Beamte, Selbstständige im Sinne von Artikel 49 AEUV, Anteilseigner und Personen, die dem Verwaltungs-, Leitungs- oder Aufsichtsorgan eines Unternehmens angehören, einschließlich der nicht geschäftsführenden Mitglieder, sowie Freiwillige und bezahlte oder unbezahlte Praktikanten sowie Personen, die unter der Aufsicht und Leitung von Auftragnehmern, Unterauftragnehmern und Lieferanten arbeiten. Der persönliche Anwendungsbereich umfasst auch die Phase der Anbahnung sowie nach der Beendigung eines Arbeitsverhältnisses (Artikel 3 Abs. 2 und 3). Eine Besonderheit des personellen Anwendungsbereiches ist zudem, dass auch sog. verbundene Personen erfasst sind. Hierunter fallen „*Mittler*“ i. S. d. Artikel 5 Nr. 8, also solche Personen, die einen Hinweisgeber bei dem Meldeverfahren in einem beruflichen Kontext unterstützen und deren Unterstützung vertraulich sein sollte sowie „*Dritte, die mit den Hinweisgebern in Verbindung stehen und in einem beruflichen Kontext Repressalien erleiden könnten, wie z. B. Kollegen oder Verwandte des Hinweisgebers, und juristische Personen, die im Eigentum des Hinweisgebers stehen oder für die der Hinweisgeber arbeitet oder mit denen er in einem beruflichen Kontext anderweitig in Verbindung steht.*“ (vgl. Artikel 4 Abs. 4).

Voraussetzung für das Eingreifen des Schutzes der Richtlinie ist es, dass der Hinweisgeber hinreichenden Grund zu der Annahme hatte, dass die gemeldeten Informationen über Verstöße zum Zeitpunkt der Meldung der Wahrheit entsprachen und dass diese Informationen in den Anwendungsbereich dieser Richtlinie fielen, sowie dass der Hinweisgeber intern gemäß Artikel 7 oder extern gemäß Artikel 10 einen Hinweis erstattet oder eine Offenlegung gemäß Artikel 15 vorgenommen hat (vgl. Artikel 6 Abs. 1). Dabei spielt es keine Rolle, ob die Meldung intern oder extern erfolgt (vgl. Artikel 6 Abs. 4).

Die beiden nächsten Kapitel der Richtlinie befassen sich mit den Abläufen, Modalitäten und Pflichten im Zusammenhang mit internen Meldungen und den damit zusammenhängenden Folgemaßnahmen (Kap. II, Artikel 7 bis 9) sowie im Zusammenhang mit externen Meldungen und den damit zusammenhängenden Folgemaßnahmen (Kap. III, Artikel 10 bis 14). Artikel 15 bzw. Kap. 4 der Richtlinie enthält Voraussetzungen, unter denen sogar eine Offenlegung des Hinweises – sprich der Gang an die Öffentlichkeit – gerechtfertigt sein kann. In den nachfolgenden Artikeln des fünften Kapitels finden sich gemeinsame Vorschriften für interne und externe Meldungen, die etwa das Vertraulichkeitsgebot (Artikel 16), die Verarbeitung personenbezogener Daten (Artikel 17) und die Dokumentation der Meldungen (Artikel 18) betreffen.

Kap. 6 der Richtlinie widmet sich sodann dem Aspekt des Hinweisgeberschutzes. Hierzu zählt insbesondere das Repressalienverbot in Artikel 19, das einen nicht abschließenden Beispieldiskatalog für denkbare Repressalien enthält. Zudem sind die Mitgliedstaaten dazu verpflichtet, dafür zu sorgen, dass Hinweisgeber Zugang zu Maßnahmen haben, die sie erforderlichenfalls bei der Information und Beratung über Abwehrmaßnahmen gegen Repressalien unterstützen (vgl. Artikel 20). Daneben müssen die Mitgliedstaaten flankierende Maßnahmen ergreifen, durch die der Schutz des Hinweisgebers vor

Repressalien abgesichert wird (vgl. Artikel 21). Die Mitgliedstaaten sind ferner auch dazu verpflichtet, Maßnahmen zum Schutz der Rechte der von einem Hinweis betroffenen Person zu ergreifen (vgl. Artikel 22). Die in der Richtlinie vorgesehenen Rechte und Rechtsbehelfe dürfen dabei nicht durch Vereinbarungen oder tatsächliche Gegebenheiten ausgehöhlt oder sonst umgangen werden (vgl. Artikel 24). Schließlich wird den Mitgliedstaaten aufgegeben, „wirksame, angemessene und abschreckende Sanktionen“ für Verstöße gegen die Bestimmungen der Richtlinie festzulegen. Diese sollen sich einerseits gegen diejenigen natürlichen oder juristischen Personen richten, die die Meldung oder den Schutz eines Hinweisgebers beeinträchtigen (vgl. Artikel 23 Abs. 1). Andererseits sollen entsprechende Sanktionen auch für einen Hinweisgeber festgelegt werden, wenn ihm nachgewiesen wird, dass er wissentlich falsche Informationen gemeldet oder offengelegt hat; in diesen Fällen soll zudem eine Schadenswiedergutmachungspflicht bestehen (vgl. Artikel 23 Abs. 2).

Kap. 7 betrifft sodann Schlussvorschriften etwa zum gestaffelten Inkrafttreten der Verpflichtungen aus der Richtlinie für juristische Personen mit 50 bis 249 Arbeitnehmern. Diese müssen – grundsätzlich – erst bis zum 17. Dezember 2023 die Rechts- und Verwaltungsvorschriften zur Einrichtung interner Meldestellen nach Artikel 8 Abs. 3 erfüllen (vgl. Artikel 26). Die Mitgliedstaaten sind zudem zur mitunter jährlichen Berichterstattung, Bewertung und Überprüfung der Umsetzung der Richtlinie gegenüber der Kommission verpflichtet (vgl. Artikel 27).

9.2.6.2 Zum Vertragsverletzungsverfahren der EU-Kommission gegen Deutschland

Die Begeisterung der damaligen Bundesregierung für die sich abzeichnenden Pläne aus Brüssel zur Einführung eines europaweiten Mindeststandards für einen Hinweisgeberschutz fiel verhalten aus. So teilte die Bundesregierung auf eine kleine Anfrage der Fraktion FDP vom 5. Juli 2018 mit, man begrüße die Vorschläge der EU-Kommission für einen stärkeren Schutz von Whistleblowern zwar; die im Einzelnen vorgeschlagenen Maßnahmen würden derzeit aber noch auf ihre Erforderlichkeit und Angemessenheit geprüft und diskutiert.⁵²

Die Richtlinie trat schließlich am 16. Dezember 2019 in Kraft. Die daran anschließende Frist zur Umsetzung der Richtlinie von zwei Jahren endete mit Ablauf des 17. Dezember 2021. 23 Mitgliedstaaten – darunter auch Deutschland – ließen diese Frist ergebnislos verstreichen. Die Kommission leitete daraufhin im Januar 2022 wegen der nicht erfolgten Umsetzung ein förmliches Vertragsverletzungsverfahren gegen Deutschland⁵³ und die weiteren Mitgliedstaaten ein.

Angesichts der auch in den Folgemonaten nicht voranschreitenden nationalen Umsetzungsmaßnahmen leitete die Kommission am 15. Juli 2022 gegen Deutschland und die

⁵²Vgl. BT-Drs. 19/3546.

⁵³Vgl. Nummer der Vertragsverletzung: INFR(2022)0052.

zwischenzeitlich noch 15 weiteren Mitgliedstaaten den nächsten Schritt im Vertragsverletzungsverfahren ein. Bei diesem handelte es sich um ein sogenanntes Aufforderungsschreiben nach Artikel 258–260 Abs. 3 AEUV, auch bekannt als „der blaue Brief aus Brüssel“.⁵⁴ Die Empfänger dieser Schreiben hatten im Anschluss an die Übersendung zwei Monate Zeit, um auf die mit Gründen versehene Stellungnahme der Kommission zu der Erforderlichkeit der Umsetzung und der Feststellung des Verstoßes zu antworten.⁵⁵

Mit Blick auf die auch Monate später nicht erfolgte Umsetzung der Richtlinie und „in Abwesenheit nachvollziehbarer Gründe“ hierfür, verklagte die Kommission sodann am 15. Februar 2023 Deutschland und die zu diesem Zeitpunkt nunmehr noch sieben weiteren Mitgliedstaaten (Tschechien, Estland, Spanien, Italien, Luxemburg, Ungarn und Polen) vor dem Europäischen Gerichtshof. Insoweit ist unter Berufung auf ein Antwortschreiben des Bundesjustizministeriums an den CDU-Bundestagsabgeordneten Martin Plum berichtet worden, dass die Kommission in ihrer Klageschrift für jeden Tag seit dem fruchtbaren Ablauf der Umsetzungsfrist bis zum Tag der Behebung des Verstoßes 61.600 €, „mindestens jedoch 17.248.000 €“ fordert und für den Fall, dass die Umsetzung auch bis zum Abschluss des Klageverfahrens nicht erfolge, zudem vorsorglich die Verhängung eines Zwangsgeldes beantragt hat und zwar in Höhe von „240.240 € pro Tag ab dem Tag der Verkündung.“⁵⁶

9.2.7 Das Hinweisgeberschutzgesetz

Am 2. Juli 2023 trat dann mit dem Gesetz für einen besseren Schutz hinweisgebender Personen (HinSchG) das erste, flächendeckende Hinweisgeberschutzgesetz in Deutschland in Kraft. Inhalt und Zielsetzung des Gesetzes laufen zu weiten Teilen mit der europäischen Hinweisgeberschutzrichtlinie gleich, weichen in Teilen jedoch auch von dieser ab. Im Folgenden werden das Ziel des Gesetzes, der phasenweise sehr kontrovers geführte Gesetzgebungsprozess, seine wesentlichen Inhalte und die darin enthaltenen Abweichungen von der Hinweisgeberschutzrichtlinie überblicksartig dargestellt. Dabei ist festzustellen, dass das HinSchG an einigen Stellen über den Regelungsumfang der Richtlinie hinausgeht, an derer Stelle aber – möglicherweise – auch hinter diesem zurückbleibt.

⁵⁴Vgl. zu dem Begriff etwa <https://www.handelsblatt.com/politik/deutschland/vertragsverletzungsverfahren-ueberfaelliges-whistleblower-gesetz-deutschland-bekommt-blauen-brief-aus-bruessel/28056780.html> (aufgerufen am 14.1.2024).

⁵⁵Vgl. Pressemitteilung der Europäischen Kommission zu Entscheidungen in Vertragsverletzungsverfahren vom 15.7.2022, https://ec.europa.eu/commission/presscorner/detail/DE/inf_22_3768 (aufgerufen am 14.1.2024).

⁵⁶Vgl. Newsdienst Compliance 4/2023, 510002. Das Verfahren ist mit Stand vom 14.1.2024 weiterhin anhängig.

9.2.7.1 Ziel: Schutz von Hinweisgebern

Das Gesetz normiert insbesondere die Voraussetzungen des Schutzes natürlicher Personen, die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese an die nach dem HinSchG vorgesehenen Meldestellen melden oder offenlegen (vgl. § 1 Abs. 1 HinSchG). Zugleich werden auch die Personen geschützt, die Gegenstand einer Meldung oder Offenlegung sind, sowie sonstige Personen, die von einer Meldung oder Offenlegung betroffen sind (vgl. § 1 Abs. 2 HinSchG).

9.2.7.2 Gesetzgebungsprozess

Bis zum Inkrafttreten des Gesetzes war es ein langer Weg, der von erheblichen Kontroversen geprägt war:

Ein erster, im November 2020 von dem damaligen Bundesministerium der Justiz und für Verbraucherschutz vorgelegter Referentenentwurf wurde erst einmal doch wieder auf Eis gelegt, da der Entwurf in der damaligen Großen Koalition nicht mehrheitsfähig war. Hintergrund sollen Unstimmigkeiten hinsichtlich der sachlichen Reichweite des Hinweisgeberschutzes gewesen sein sein.⁵⁷

Erst am 13. April 2022 – also bereits rund vier Monate nach Ablauf der Umsetzungsfrist – legte das neue Bundesjustizministerium einen neuen Referentenentwurf vor. Dieser wurde am 27. Juli 2022 vom Bundeskabinett beschlossen. Am 19. Oktober 2022 fand eine öffentliche Anhörung des Rechtsausschusses statt, in der der Gesetzentwurf⁵⁸ grundsätzlich auf Zustimmung stieß.⁵⁹ Der Entwurf ging dabei erneut in Teilen über die Mindestanforderungen der Richtlinie hinaus, etwa soweit der Schutzbereich auch auf die Meldung von Verstößen gegen bestimmtes nationales Recht oder um Schutzmechanismen auch für solche Meldungen erweitert worden war, die sich auf Äußerungen von Beamtinnen und Beamten beziehen, die einen Verstoß gegen die Pflicht zur Verfassungstreue darstellen, aber unterhalb der Strafbarkeitsschwelle liegen (s. § 2 Abs. 1 Nr. 10 HinSchG). Der Rechtsausschuss im Deutschen Bundestag hatte mit der zuletzt genannten Erweiterung auf die Anfang Dezember 2022 aufgekommene Diskussion um den Umgang mit sog. Reichsbürgern im öffentlichen Dienst reagiert.⁶⁰

Nachdem der Bundestag den Gesetzentwurf⁶¹ am 16. Dezember 2022 mit den Stimmen der Koalition aus SPD, BÜNDNIS 90/DIE GRÜNEN und FDP verabschiedet hatte, verweigerte der Bundesrat am 10. Februar 2023 seine für das Inkrafttreten des Gesetzes erforderliche Zustimmung.⁶²

⁵⁷Vgl. <https://www.sueddeutsche.de/wirtschaft/whistleblower-lambrecht-unternehmen-1.5278761> (aufgerufen am 14.1.2024).

⁵⁸Vgl. BT-Drs. 20/3442.

⁵⁹Vgl. Newsdienst Compliance 2022, 43008.

⁶⁰Vgl. Newsdienst Compliance 2023, 410002.

⁶¹Vgl. BT-Drs. 20/4909.

⁶²Vgl. BR-Drs. 20/23.

Die Fraktionen der Regierungskoalition spalteten daraufhin den ursprünglich in Gänze zustimmungspflichtigen Gesetzentwurf in zwei Gesetzentwürfe auf und brachten diese am 17. März 2023 erneut in den Bundestag ein.⁶³ Von diesen beiden Gesetzentwürfen war ihrer Ansicht nach nunmehr nur noch ein Gesetzentwurf zustimmungsbedürftig.⁶⁴ Dieses Vorgehen ist vielfach kritisiert worden.⁶⁵ Zum einen wurde eine Umgehung der gesetzlich vorgesehenen Verfahrensweise bei Uneinigkeit zwischen Bundestag und Bundesrat bemängelt, nämlich der Anrufung des Vermittlungsausschusses nach Artikel 77 Abs. 2 GG i. V. m. der Gemeinsamen Geschäftsordnung des Bundestages und des Bundesrates für den Ausschuss nach Artikel 77 GG. Zum anderen war fraglich, ob die vom Bundesverfassungsgericht entwickelten Voraussetzungen für die Zulässigkeit einer nicht notwendigen Aufsplittung eines Gesetzesvorhabens in einen zustimmungspflichtigen Teil und einen nicht-zustimmungspflichtigen Teil überhaupt erfüllt waren.⁶⁶

Hier von unbeeindruckt fand am 17. März 2023 die erste Lesung der beiden Gesetzentwürfe im Bundestag⁶⁷ und am 27. März 2023 eine entsprechende Anhörung im Rechtsausschuss des Bundestages statt.⁶⁸ Für den 30. März 2023 stand der nicht-zustimmungsbedürftige Gesetzentwurf sodann zur Beratung und Beschlussfassung auf der Tagesordnung des Bundestags, wurde jedoch wenige Stunden zuvor kurzfristig wieder von der Tagesordnung genommen.⁶⁹ Insoweit war bekannt geworden, dass sich Vertreter von Regierung und Opposition am 5. April 2023 im sogenannten Ältestenrat des Parlaments doch noch auf die Anrufung des Vermittlungsausschusses mit dem Ziel der Ermittlung eines Kompromisses verständigt hatten.⁷⁰

Der Vermittlungsausschuss befasste sich daraufhin am 9. Mai 2023 mit dem Entwurf. Schon am 11. und 12. Mai 2023 wurde der ursprüngliche Gesetzentwurf – in einer Kompromissfassung⁷¹ – im Bundestag und Bundesrat verabschiedet und konnte schließlich am 2. Juli 2023 in Kraft treten.

9.2.7.3 Systematik und Regelungsgehalt

9.2.7.3.1 Aufbau, Anwendungsbereich und vorgesehene Sanktionen

Das HinSchG enthält 42 Paragraphen und ist in die folgenden sechs Abschnitte aufgeteilt: Allgemeine Vorschriften, Meldungen, Offenlegung, Schutzmaßnahmen, Sanktionen und

⁶³Vgl. BT-Drs. 20/5991 und BT-Drs. 20/5992.

⁶⁴Vgl. Newsdienst Compliance 2023, 410006.

⁶⁵Vgl. heute im Bundestag vom 28.3.2023, Nr. 222, NZG 2023, 490.

⁶⁶Vgl. BVerfG, Urteil vom 17.7.2002 –1 BvF 1/01, 1 BvF 2/01 zur Verfassungsmäßigkeit des Lebenspartnerschaftsgesetzes.

⁶⁷Vgl. Plenarprotokoll 20/92.

⁶⁸Vgl. BT-Drs. 20/6193.

⁶⁹Vgl. Newsdienst Compliance 2023, 410006.

⁷⁰Vgl. Newsdienst Compliance 2023, 410006.

⁷¹Siehe hierzu Nielebock, H., jurisPR-ArbR 23/2023, Anm. 1.

Schlussvorschriften. Die meisten Vorschriften des HinSchG entfallen dabei auf den Abschnitt 2, der sich ausführlich den Grundsätzen interner und externer Meldungen sowie der anschließenden Verfahren und Folgemaßnahmen widmet.

Einleitend ist festzuhalten, dass der sachliche Anwendungsbereich in § 2 HinSchG über die Mindestvorgaben der Hinweisgeberrichtlinie hinaus alle Straftaten erfasst. Zudem sind alle Bußgeldbewehrten Verstöße erfasst, soweit die verletzte Vorschrift dem Schutz von Leben, Leib, Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient. Darüber hinaus wird der sachliche Anwendungsbereich auch über die nach der Richtlinie einzubeziehenden Rechtsakte der Europäischen Union hinaus – in begrenztem Umfang – auf bestimmte weitere nationale Vorschriften erweitert. Beispielsweise werden nicht nur Verstöße gegen europäisches Kartellrecht, sondern auch gegen deutsches Kartellrecht erfasst.

Insoweit ist jedoch zu beachten, dass gem. § 4 Abs. 1 HinSchG eine ganze Reihe spezifischer Regelungen über die Mitteilung von Informationen über Verstöße den Bestimmungen des HinSchG vorgehen. Hierzu zählen etwa die §§ 6 Abs. 5 und 53 des GwG. Zudem ist der Anwendungsbereich des HinSchG in bestimmten Fällen vorrangiger Sicherheitsinteressen oder bei Bestehen besonderer Verschwiegenheits- und Geheimhaltungspflichten gem. § 5 HinSchG nicht eröffnet.⁷²

Der persönliche Anwendungsbereich ist demgegenüber durch den Konnex der Kenntnisserlangung im Zusammenhang mit oder im Vorfeld einer beruflichen Tätigkeit begrenzt (vgl. § 1 Abs. 1 HinSchG).

Eine zunächst noch diskutierte Pflicht, anonyme Meldungen zu ermöglichen, ist nun nicht mehr vorgesehen. Stattdessen heißt es nunmehr in § 16 Abs. 1 S. 4 und 5 HinSchG: „*Die interne Meldestelle sollte auch anonym eingehende Meldungen bearbeiten. Es besteht allerdings keine Verpflichtung, die Meldekanäle so zu gestalten, dass sie die Abgabe anonymer Meldungen ermöglichen.*“

Die Beweislastumkehr für den Nachweis des fehlenden Zusammenhangs zwischen der von dem Hinweisgeber vorgenommenen Meldung oder Offenlegung eines Missstandes und einer anschließenden Benachteiligung im Zusammenhang mit der beruflichen Tätigkeit ist demgegenüber erhalten geblieben (vgl. § 36 Abs. 2 HinSchG).

Der deutsche Gesetzgeber hat sich zudem Gedanken über die von Artikel 23 Abs. 1 der Richtlinie geforderten „*wirksamen, angemessenen und abschreckenden Sanktionen für Verstöße*“ gemacht und in § 40 HinSchG verschiedene Bußgeldtatbestände normiert. Diese sehen – je nach Verstoß – Geldbußen in Höhe von 10.000 €, 20.000 € oder 50.000 € vor. Vor dem Kompromissentwurf im Vermittlungsausschuss hatte der Höchstsatz des Bußgeldes noch 100.000 € betragen. Im Falle einer Geldbuße gegen eine juristische Person oder Personenvereinigung kann sich das Höchstmaß der Geldbuße in den Fällen des § 40 Abs. 2 Nr. 1 und 3 HinSchG entsprechend § 30 Abs. 2 Satz 3 OWiG verzehnfachen (vgl. § 40 Abs. 6 Satz 2 HinSchG).

⁷²Zum Verhältnis von HinSchG und GeschGehG siehe bereits ausführlich unter Abschn. 9.2.4.1.

9.2.7.3.2 Verhältnis der internen und externe Meldestelle(n) nach dem HinSchG

Hinweisgeber haben unter dem HinSchG grundsätzlich ein Wahlrecht, ob sie sich an eine interne Meldestelle (§§ 12 bis 18 HinSchG; hierzu ausführlich Abschn. 9.3.3) oder an eine externe Meldestelle (§§ 19 bis 24 HinSchG) wenden.

Entsprechende externe Meldestellen sind gegenwärtig zuvorderst beim Bundesamt für Justiz (§ 19 HinSchG) sowie beim Bundeskartellamt (§ 22 HinSchG) und bei der Bundesanstalt für Finanzdienstleistungen (BaFin) (§ 21 HinSchG) eingerichtet. Die Zuständigkeitsbereiche der beim Bundeskartellamt und bei der BaFin eingerichteten Meldestellen richten sich grundsätzlich nach ihrem jeweiligen Aufsichtsbereich. Das Bundeskartellamt ist deshalb etwa für die Entgegennahme von Hinweisen auf Verstöße gegen das Wettbewerbsrecht und gegen den EU Digital Markets Act zuständig. Auch die Länder können externe Meldestellen einrichten (§ 20 HinSchG). Die externe Meldestelle beim Bundesamt für Justiz ist demgegenüber nur dann zuständig, soweit nicht eine der anderen externen Meldestellen nach den §§ 20 bis 23 des HinSchG zuständig ist.⁷³

Mit Blick auf das Rangverhältnis zwischen interner und externer Meldestelle kommt im HinSchG an mehreren Stellen zum Ausdruck, dass Meldungen vorrangig an die interne Meldestelle erfolgen und insoweit entsprechende Anreize durch den Beschäftigungsgeber geschaffen werden sollen (vgl. § 7 Abs. 1 Satz 2, Abs. 3 HinSchG). Diese Regelung ist aus der Unternehmensperspektive heraus zu begrüßen (siehe hierzu Abschn. 9.1.3 und 9.3) und findet auch für die Fälle, in denen intern wirksam gegen den Verstoß vorgegangen werden kann und der Hinweisgeber keine Repressalien befürchtet, ihre Entsprechung in Artikel 7 Abs. 2 der Hinweisgebersrichtlinie.⁷⁴

Darüber hinaus ist explizit vorgesehen, dass „*die externen Meldestellen insbesondere auch über die Möglichkeit einer internen Meldung*“ informieren (vgl. § 24 Abs. 2 Satz 2 HinSchG). Umgekehrt müssen die internen Meldestellen klare und leicht zugängliche Informationen über externe Meldeverfahren vorhalten, vgl. § 13 Abs. 2 HinSchG. Grundsätzlich kommt ein solcher Vorrang einzelnen Behörden, gerade der neu eingerichteten zentralen Meldestelle des Bundes, sicher auch entgegen, da eine Vielzahl der Sachverhalte gut intern aufgeklärt werden kann. Dass dies aber nicht zwingend der Fall ist, und aus Sicht mancher Aufsichts- und Ermittlungsbehörden eine möglichst umfassende Aufklärung, Verfolgung und Sanktionierung eines etwaigen Fehlverhalten vor allem dann gewährleistet ist, wenn der Hinweis direkt an die staatliche Behörde gelangt, wird beispielsweise aus einer Pressemitteilung des Bundeskartellamtes vom 3. Juli 2023 deutlich; dort heißt es:

⁷³ Die nähere Ausgestaltung der Organisation und des Verfahrens der externen Meldestelle des Bundes wird durch die Hinweisgeberschutzgesetz-Externe-Meldestelle-des-Bundes-Verordnung (HEMBV) geregelt (vgl. § 41 HinSchG). Zu dieser Verordnung lag Ende Juli 2023 ein Referentenentwurf vor, der hier abgerufen werden kann: https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/2023_Hinweisgeberschutz_Einrichtung_Meldestelle_Bund.html (aufgerufen am 14.1.2024).

⁷⁴ Für die Einführung einer entsprechenden Regelungen auch bspw. der Deutsche Anwaltverein, Stellungnahme 23/2022, S. 4 f.; a.A. hinsichtlich der Vereinbarkeit mit der Hinweisgeberschutzrichtlinie: Nielebock, H., jurisPR-ArbR 23/2023, Anm. 1.

„Wir ermutigen alle potenziellen Hinweisgeber, von dem Schutz des neuen Hinweisgeberschutzgesetzes Gebrauch zu machen und uns bei Verdachtsmomenten im Zusammenhang mit Wettbewerbsverstößen in ihrem beruflichen Umfeld zu kontaktieren. (...) Das Hinweisgeberschutzgesetz sieht zudem vor, dass Unternehmen eigene interne Meldestellen einrichten müssen. Allerdings hat die hinweisgebende Person das Recht, sich unabhängig von einer internen Meldung jederzeit an die externe Meldestelle beim Bundeskartellamt zu wenden, um eine wirksame Verfolgung zu ermöglichen. Bereits in der Vergangenheit haben Hinweise von Insidern beim Bundeskartellamt zu einer Vielzahl von Verfahren und zu einer Verhängung von hohen Bußgeldern geführt. So konnte der Wettbewerb wirksam geschützt und weitere Schäden verhindert werden.“⁷⁵

9.3 Einführung eines Hinweisgeberschutzgesetzes im Unternehmen

9.3.1 Gründe für die Einführung eines Hinweisgebersystems

Auch wenn es lange Zeit nur vereinzelte Regelungen gab, die die Einführung eines Hinweisgebersystems im Unternehmen verpflichtend machten, verfügten bereits vor In-Kraft-Treten des Hinweisgeberschutzgesetzes viele Unternehmen über Angebote für Mitarbeiter, Compliance-Verstöße intern melden zu können. In einer Untersuchung aus dem Jahr 2021 ergibt sich beispielsweise, dass damals bereits 63,2 % der befragten Unternehmen in Deutschland über ein sog. Whistleblowing-System verfügten.⁷⁶ Dabei war erwartungsgemäß die Verbreitung in großen Unternehmen höher (73,9 %) als in kleinen Unternehmen (43,7 %).⁷⁷ Es zählt bereits seit Längerem zu den best-practice Grundsätzen, dass Hinweisgebersysteme ein besonders geeignetes Instrument sind, um die sich aus dem Aktien- und Gesellschaftsrecht sowie aus den Vorgaben des Ordnungswidrigkeitenrechts ergebenden Compliance-Erfordernisse zu erfüllen.⁷⁸ Das Hinweisgebersystem war schon immer einer von mehreren Bausteinen im Compliance-Management-System eines Unternehmens, und zwar ein nahezu unverzichtbarer.⁷⁹ Insbesondere ist es oft die einzige Compliance-Maßnahme, die in Korruptionsfällen und bei Kartellrechtsverstößen geeignet ist, das Schweigen der Mitarbeiter zu durchdringen und von ihnen die notwendigen Offenbarungen zur Aufklärung entsprechender Vorgänge zu erhalten.⁸⁰ Auch in der Vergangenheit dienten Hinweisgebersysteme bereits der Sicherstellung, dass Hinweise möglichst zunächst intern abgegeben werden, bevor Hinweisgeber sich an externe Stellen oder

⁷⁵ Siehe Pressemitteilung des Bundeskartellamtes vom 3.7.2023, https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2023/03_07_2023_HinschG.html (aufgerufen am 14.1.2024).

⁷⁶ EQS/Hochschule Graubünden, Whistleblowing Report 2021, Chur 2021, S. 23.

⁷⁷ EQS/Hochschule Graubünden, Whistleblowing Report 2021, Chur 2021, S. 24.

⁷⁸ Vgl. Maume, P./Haffke, L., ZIP 2016, 199 m. w. V.; Süße, S. in Rotsch (2015), § 34 Rn. 115. Siehe zudem Grundsatz 5, Empfehlung A.4. des DCGK (Ziffer 4.1.3. DCGK a. F.).

⁷⁹ Bock, D. (2011), Criminal Compliance, S. 732 ff.

⁸⁰ Vgl. auch Moosmayer, K. (2021), Rn. 183.

Behörden wenden. Internes Whistleblowing ermöglicht es dem Unternehmen nämlich zunächst ohne äußeren Druck die Validität des Hinweises zu überprüfen. Zudem wird das Unternehmen in die Lage versetzt, den Missstand eigenständig abstellen zu können und – mit wenigen Ausnahmen – über das Ob und gegebenenfalls das Wann des Herantretens an Ermittlungsbehörden und die Öffentlichkeit selbst zu bestimmen.⁸¹

Die nunmehr gesetzliche Vorgabe zur Einführung eines Hinweisgebersystems als solche stellt daher für viele Unternehmen keine völlige Neuerung dar. Die Notwendigkeit für Anpassungen liegt häufig in den Details, die das Gesetz vorgibt und die durchaus herausfordernd sind.

9.3.2 Arten von Hinweisgebersystemen

In der Vergangenheit hatten sich insbesondere drei Arten von Hinweisgebersystemen entwickelt: Die Möglichkeit der Hinweiserteilung über eine Telefon-Hotline, über eine internetbasierte Kommunikationsplattform oder die Möglichkeit der Hinweisabgabe an einen konkreten externen Ansprechpartner, oftmals Ombudsperson oder Vertrauensanwalt/-anwältin genannt. Kombinationen der einzelnen Verfahren und Kommunikationswege sind denkbar. Zumeist besteht in vielen Unternehmen daneben auch die Möglichkeit, sich auf unterschiedlichen Wegen – persönlich, telefonisch, per E-Mail oder postalisch – an die Compliance-Abteilung oder den direkten Vorgesetzten zu wenden. All diese Verfahren, mit Ausnahme der reinen Telefon-Hotline, deren Praxisrelevanz deutlich zurückgegangen sein dürfte, sind heutzutage etablierte und weit verbreitete Meldekanäle in Unternehmen.

9.3.2.1 Telefon-Hotline

Insbesondere in den ersten Jahren, in denen Hinweisgebersysteme in deutschen Unternehmen etabliert wurden, griffen Unternehmen auf reine Telefon-Hotlines zurück. Anrufe der Hinweisgeber gehen dabei über eine kostenfreie Rufnummer in einem Call-Center ein, wo sie von den dortigen Mitarbeitern erfasst und an vorher definierte Stellen – bspw. die Compliance-Abteilung des Unternehmens oder einen Rechtsanwalt – weitergeleitet werden. Eine inhaltliche Bearbeitung des Hinweises durch die Mitarbeiter findet in der Regel nicht statt. Um einen Dialog mit dem Hinweisgeber zu ermöglichen, können im Erstgespräch aber Kennwörter oder Pseudonyme vergeben werden, damit ein nachfolgender Anruf des Hinweisgebers dem gleichen Sachverhalt zugeordnet werden kann.⁸²

9.3.2.2 Internetbasiertes Hinweisgebersystem

Bei einem internetbasierten bzw. digitalen Hinweisgebersystem kann der Hinweisgeber über eine Softwareapplikation im Internet seinen Hinweis abgeben. Hierzu greift das Unternehmen in der Regel auf einen der Anbieter zurück, von denen sich in den letzten

⁸¹ Siehe auch schon oben ausführlich 1.3.

⁸² Morenz, A., Der Aufsichtsrat, 2010, 172 (173).

Jahren mehrere auf das Thema Whistleblowing spezialisiert und mit ihren Produkten entsprechend etabliert haben. Im Zuge der Diskussion um das Hinweisgeberschutzgesetz haben zudem eine Vielzahl von Rechtsanwalts- und Beratungsgesellschaften eigene Produkte entwickelt oder entwickeln lassen. Eine einfache Suchrecherche im Internet führt hier schnell zu einer guten Übersicht über den Markt der unterschiedlichen Anbieter.

In der Regel über einen Link auf der Unternehmenswebsite gelangt der Hinweisgeber dann zu einer Internetseite, auf der er Schritt für Schritt durch den Meldeprozess geführt und zu den wichtigsten, vom Hinweisempfänger benötigten Informationen befragt wird. Die Hinweisabgabe kann dabei häufig in mehreren Sprachen erfolgen. Auch wird der Hinweisgeber manchmal um eine Selbsteinschätzung gebeten zu welcher Kategorie von Vorfall der Hinweis aus seiner Sicht zählt. Oft wird ihm die Möglichkeit zur Auswahl durch vorgegebene Kategorien erleichtert. Anhand dieser Auswahl wird der Hinweis sodann an im System hinterlegte, definierte Ansprechpartner weitergeleitet. Der Hinweisgeber erhält zumeist die Möglichkeit, einen Postkasten einzurichten, der ihm eine offene oder anonyme Kommunikation mit dem Hinweisempfänger ermöglicht. Dieser gesicherte Dialog kann durch beide Seiten veranlasst werden, sofern der Hinweisgeber einen entsprechenden Postkasten bei Abgabe der Meldung eingerichtet hat. Die am Markt etablierten Anbieter sichern dabei zu, dass durch Verschlüsselungstechniken die Anonymität des Hinweisgebers gewährleistet werden kann und teilweise auch, dass eine Einsichtnahme in die Kommunikation durch den Betreiber nicht möglich ist.

9.3.2.3 Ombudsmann/-frau bzw. Vertrauensanwalt/-anwältin

Eine dritte Option für den Aufbau eines Hinweisgebersystems basiert auf der Implementierung eines konkreten Ansprechpartners für potenzielle Hinweisgeber, der in der Regel außerhalb der Unternehmensorganisation steht, in diese aber durch konkrete Vereinbarungen über die Weiterleitung, Kommunikation und Bearbeitung von Hinweisen integriert ist. Dieser Ansprechpartner wurde in der Vergangenheit häufig als „Ombudsman“ bezeichnet – was selbstverständlich Ombudsfrauen mit einschließt. Nicht zuletzt um Verwechslungen mit anderen Funktionen, die „Ombudsmann“ genannt werden – etwa den Ombudsmann einer Versicherung – zu vermeiden und um den beruflichen Hintergrund vieler Ombudspersonen zu betonen, wird vermehrt auch der Begriff des Vertrauensanwalts/der Vertrauensanwältin gewählt.⁸³ Es handelt sich somit auch hierbei um eine Form des internen Whistleblowings. Diese Form des Hinweisgebersystems basiert nicht zuletzt auf dem Vertrauen des Hinweisgebers zur Ombudsperson, die ihm im Rahmen der Implementierung des Hinweisgebersystems entsprechend vorgestellt und bekanntgemacht wird.

Der Kontakt zur Ombudsperson kann über verschiedene Kanäle erfolgen: Bevorzugt wird zumeist der direkte telefonische Kontakt; daneben werden aber in der Regel ebenso postalische wie E-Mail-Kontaktdaten zur Verfügung gestellt. Zielsetzung des Kontakts zwischen Ombudsperson und Hinweisgeber wird es vielfach sein, ein persönliches

⁸³ Siehe auch: Fassbach, B./Hülsberg, F./Spamer, H., CB 2022, 151.

Gespräch zwischen ihnen beiden zu erreichen, sodass beispielsweise auch Unterlagen und Dokumente direkt ausgetauscht und gemeinsam gesichtet werden können.⁸⁴ Dementsprechend wirkt die Ombudsperson grundsätzlich darauf hin, dass der Hinweisgeber seine Kontaktdaten hinterlässt und sich namentlich jedenfalls gegenüber der Ombudsperson zu erkennen gibt. Diese Konstellation ermöglicht es, dass der Hinweisgeber sich gegenüber der Ombudsperson offenbart, aber gegenüber dem Unternehmen anonym bleibt. Hierzu müssen zwischen Ombudsperson und Unternehmen entsprechende Regelungen getroffen werden, dass das Unternehmen auf einen etwaigen Auskunftsanspruch verzichtet.⁸⁵ Grundsätzlich ist im Rahmen dieses Systems auch eine völlig anonyme, also auch gegenüber der Ombudsperson anonyme, Abgabe von Hinweisen möglich. Zur Sicherung der besonderen Schutzbedürftigkeit des Hinweisgebers handelt es sich bei der Ombudsperson zumeist um einen Rechtsanwalt, da dieser insofern den weitestgehenden Vertrauenschutz bieten kann.⁸⁶

Die Ombudsperson berichtet sodann in der mit dem Unternehmen vereinbarten und gegebenenfalls mit dem Hinweisgeber abgesprochenen Form im Rahmen fest definierter Berichtswege an das Unternehmen, bspw. an die dortige Compliance-Abteilung oder den Leiter für interne Untersuchungen.

9.3.3 Anforderungen des HinSchG an die interne Meldestelle

Während in der Vergangenheit die Entscheidung darüber, wer im Unternehmen Hinweise entgegennimmt, überwiegend dem Unternehmen selbst überlassen war und diese regelmäßig auf best practices zurückgriffen, gibt das Hinweisgeberschutzgesetz nunmehr konkrete Vorgaben, wie eine interne Meldestelle auszustalten ist.

Wie bereits ausgeführt, sieht das Gesetz vor, dass ein Hinweisgeber für den Fall, dass intern wirksam gegen den Verstoß vorgegangen werden kann und der Hinweisgeber keine Repressalien fürchten muss, zunächst den Weg zur internen Meldestelle wählen sollte.⁸⁷ Die Unternehmen wiederum sollen hierzu nach den Vorstellungen des Gesetzgebers entsprechende Anreize schaffen.⁸⁸

9.3.3.1 Pflicht zur Einrichtung einer internen Meldestelle

Unternehmen mit in der Regel mindestens 50 Beschäftigten trifft gemäß § 12 Abs. 1 und 2 HinSchG eine Pflicht, mindestens eine interne Meldestelle vorzuhalten, an die sich Hinweisgeber wenden können, um mögliche Verstöße zu melden. Bestimmte Unternehmen

⁸⁴ Siehe bspw. Buchert, R., CCZ 2008, 148 (149).

⁸⁵ Vgl. Brockhaus, M., CB 2023, 8 (11), Dierlamm, K., SpoPrax 2021, 245 (247).

⁸⁶ Dazu: Dilling, J., CCZ 2019, 214 (217); Egger, M., CCZ 2018, 126 (129 ff.); LG Bochum, Beschluss vom 16.3.2016 – 6 QS 1/16, Newsdienst Compliance, 2016, 21009.

⁸⁷ Vgl. § 7 Abs. 1 Satz 2 HinSchG.

⁸⁸ § 7 Abs. 3 Satz 1 HinSchG.

trifft diese Pflicht unabhängig von der Anzahl der Mitarbeiter (§ 12 Abs. 3 HinSchG). Für Gemeinden und Behörden finden sich Regelungen in § 12 Abs. 1 S. 2 ff. HinSchG. Die Meldestellen müssen mit entsprechenden Befugnissen ausgestattet sein, sodass sie Hinweisen nachgehen und entsprechende Folgemaßnahmen treffen können (§ 12 Abs. 4 HinSchG). Der Gesetzentwurf der Bundesregierung zum HinSchG legte in seinen Überlegungen zugrunde, dass jährlich mit vier Hinweisen je eintausend Mitarbeitern zu rechnen sei.⁸⁹

9.3.3.2 Organisation und Aufgaben der internen Meldestelle

Hinsichtlich der Organisation der internen Meldestelle sieht das HinSchG drei grundsätzliche Formen vor: Entweder kann dies eine bei dem Beschäftigungsgeber (dem Unternehmen) beschäftigte Person sein oder eine aus mehreren beschäftigten Personen bestehende Arbeitseinheit. Ferner kommt die Beauftragung eines Dritten mit der Führung der internen Meldestelle in Betracht (§ 14 Abs. 1 Satz 1 HinSchG). Durch die Beauftragung eines Dritten wird das Unternehmen jedoch nicht von der eigenen Pflicht befreit, selbst Maßnahmen zu treffen, um einen etwaigen Verstoß abzustellen (§ 14 Abs. 1 Satz 2 HinSchG). Eine Besonderheit sieht § 14 Abs. 2 HinSchG vor: Demnach dürfen mehrere private Beschäftigungsgeber mit in der Regel 50 bis 249 Beschäftigten für die Entgegnahme von Hinweisen und das weitere Verfahren eine gemeinsame Meldestelle einrichten und betreiben. Die Pflicht, Maßnahmen zum Abstellen eines etwaigen Verstoßes zu treffen, bleibt aber auch bei dieser Lösung bei jedem einzelnen Unternehmen; ebenso die Pflicht, rechtzeitig eine Rückmeldung an den Hinweisgeber zu erteilen.

Das Gesetz sieht des Weiteren vor, dass die Mitarbeiter der internen Meldestelle ihre Tätigkeit unabhängig wahrnehmen müssen. Dem steht allerdings nicht entgegen, dass sie neben ihrer Tätigkeit für die Meldestelle auch andere Aufgaben im Unternehmen wahrnehmen, solange diese Tätigkeit nicht zu Interessenskonflikten führt (§ 15 Abs. 1 HinSchG). Daneben muss seitens des Unternehmens sichergestellt sein, dass die in der Meldestelle tätigen Mitarbeiter über die notwendige Fachkunde verfügen (§ 15 Abs. 2 HinSchG). Es wird vertreten, dass, sofern diese Voraussetzungen und die Sicherstellung der Wahrung der Vertraulichkeit nicht gewährleistet sind, es an der Einrichtung einer ordnungsgemäßen internen Meldestelle fehlt, was eine Ordnungswidrigkeit nach § 40 Abs. 2 Nr. 2 HinSchG begründen könnte.⁹⁰

Die Unabhängigkeit und die damit verbundene Weisungsfreiheit der Mitarbeiter⁹¹ wird zum Teil auf fachliche, nicht aber organisatorische Weisungen beschränkt. der internen Meldestelle erstreckt sich dabei auch auf die Auswahl und Durchführung von Folgemaßnahmen. Sofern vereinzelt Auch wird angenommen, dass die Unabhängigkeit sich auf diese nicht erstrecken kann, da die in § 18 HinSchG genannten Folgemaßnahmen Teil der

⁸⁹ Gesetzesbegründung zum Gesetzentwurf der Bundesregierung, A. VI. 4, S. 45.

⁹⁰ Greiner S., in ErfK (2024), § 12 Rn. 6; so grundsätzlich auch Szesny, A./Hoppe, P., WiJ 2023, 56.

⁹¹ Fischbach, J. in Thüsing HinSchG (2024), § 18 Rn. 2.

Gesamtverantwortung der Geschäftsleitung für Compliance seien⁹² und daher eine teleologische Reduktion des § 15 HinSchG dahingehend vorgenommen werden müsse, dass Folgemaßnahmen aus dem Merkmal der Unabhängigkeit auszuklammern sind.⁹³ Die Annahme, dass dem Gesetzgeber hier ein planwidriges Versehen unterlaufen ist,⁹⁴ lässt sich allerdings nur schwerlich begründen. Der Gesetzgeber – sowohl jener der EU-Hinweisgeberschutzrichtlinie als auch der des HinSchG – hat als wesentliches Merkmal definiert, dass die interne Meldestelle im Rahmen all ihrer Tätigkeiten unabhängig ist.⁹⁵ Daraus ergibt sich etwa, dass die Unternehmensleitung der internen Meldestelle nicht untersagen kann, eine interne Untersuchung durchzuführen.⁹⁶ Die Aufgaben der Meldestelle sind wiederum in § 13 HinwSchG definiert. Das Abstellen von Compliance-Verstößen liegt danach nicht explizit in der Verantwortung der internen Meldestelle; vielmehr trägt ihr Wirken dazu bei, dass die Unternehmensleitung (der Beschäftigungsgeber) dieser Aufgabe nachkommen kann.⁹⁷ Die interne Meldestelle managt insofern eingehende Meldungen für den Beschäftigungsgeber und entscheidet, wie mit diesen umgegangen werden muss bzw. wer diese am besten bearbeitet.

Soweit zurecht Bedenken bestehen, dass die interne Meldestelle aufgrund ihrer Unabhängigkeit umfangreiche und kostenintensive interne Untersuchungen eigenständig beauftragen könnte, sind diese unbegründet. Unabhängigkeit kann insofern nicht bedeuten, dass alle anderen unternehmensextern bestehenden Regelungen hierhinter zurücktreten müssen. Die interne Meldestelle ist bewusst vom Normgeber als in das Unternehmen integrierte Einheit ausgestaltet worden. Auch eine in ihren fachlichen Entscheidungen unabhängige interne Meldestelle kann aber nicht an den generellen Richtlinien des Unternehmens vorbei agieren und muss interne Genehmigungsprozesse und Wertgrenzen einhalten. Sollte sich wiederum ergeben, dass auch angemessener Aufklärungsaufwand regelmäßig aufgrund dieser Vorgaben nicht zur Verfügung steht und etwa die Durchführung von internen Untersuchungen dadurch verhindert wird, wäre dies eine Frage der angemessenen Ausstattung der internen Meldestelle mit Ressourcen sowie ihrer ordnungsgemäßen Einrichtung. In diesen Fällen wäre die Unabhängigkeit wohl zumindest mittelbar auch eingeschränkt. Verständlich aus Unternehmenssicht sind schließlich die Bedenken hinsichtlich der Unabhängigkeit hinsichtlich der Weitergabe von Sachverhalten an Behörden als Folgemaßnahme im Sinne des § 18 Nr. 4 lit. b HinSchG.⁹⁸ Hier wiederum dürfte zum einen jedoch das Merkmal der Fachkundigkeit der Mitarbeiter als Korrektiv dienen, zum anderen betrifft dies insbesondere Fälle, in denen intern eine Aufarbeitung

⁹² Dilling, J. in BeckOK HinSchG (2024), § 15 Rn. 3.

⁹³ Dilling, J. in BeckOK HinSchG (2024), § 15 Rn. 3 und 8.

⁹⁴ Dilling, J. in BeckOK HinSchG (2024), § 15 Rn. 8.2.

⁹⁵ Vgl. Erwägungsgrund 56 zur EU-Hinweisgeberschutzrichtlinie sowie die Begründung des Gesetzentwurfs der Bundesregierung zu § 14 HinSchG, BT-Drs. 20/5992, S. 90 ff.

⁹⁶ So wiederum offensichtlich auch Dilling, J. in BeckOK HinSchG (2023), § 15 Rn. 4.3 ff.

⁹⁷ Gesetzentwurf der Bundesregierung zu § 18 HinSchG, BT-Drs. 20/5992, S. 95.

⁹⁸ Dilling, J. in BeckOK HinSchG (2024), § 15 Rn. 8.3.

oder ein Abstellen des Verstoßes nicht möglich ist. Anders etwa als Hinweise auf Korruptionshandlungen, die von Mitarbeitern des Unternehmens begangen werden oder etwaige Kartellverstöße, die einer internen Aufklärung zugänglich sein dürften, besteht bei den hier in Rede stehenden Konstellationen in der Regel bereits kein Risiko für eine Sanktionierung des Unternehmens. Darüber hinaus gilt hier das Vorgesagte: Das Unternehmen sollte generelle Prozesse für die Kommunikation mit Behörden implementieren, die dann ebenso für die interne Meldestelle gelten.

Die Meldestellen nehmen gemäß § 13 Abs. 1 HinSchG insbesondere drei Aufgaben wahr: Die Einrichtung der Meldekanäle (§ 16 HinSchG), die Durchführung des Verfahrens nach Eingang und zur Bearbeitung eines Hinweises (§ 17 HinSchG) sowie die Bestimmung und ggf. Durchführung von konkreten Folgemaßnahmen (§ 18 HinSchG). Darüber hinaus sollen die internen Meldestellen klare und leicht zugängliche Informationen hinsichtlich der Möglichkeit, Hinweise an externe Meldestellen geben zu können, bereithalten (§ 13 Abs. 2 HinSchG). Diese Aufgaben werden im Folgenden näher beleuchtet:

9.3.3.3 Einrichtung von Meldekanälen

Unternehmen trifft die Pflicht, interne Meldekanäle einzurichten, über die die beim Unternehmen Beschäftigten sowie die an das Unternehmen überlassenen Leiharbeitnehmerinnen und -arbeitnehmer Hinweise über Verstöße an das Unternehmen melden können (§ 16 Abs. 1 Satz 1 HinSchG). Unternehmen können das Hinweisgebersystem darüber hinaus für bei Geschäftspartnern tätige natürliche Personen öffnen (§ 16 Abs. 1 Satz 3 HinSchG). Auch anonyme Hinweise sollen bearbeitet werden; es besteht jedoch keine Verpflichtung, die Meldekanäle so zu gestalten, dass anonyme Hinweise abgegeben werden können (§ 16 Abs. 1 Satz 5 HinSchG). Da es im Interesse des Unternehmens ist, möglichst frühzeitig von Compliance-Verstößen Kenntnis zu erlangen und das Risiko von bewusst falschen Meldungen in der Regel als eher gering eingeschätzt werden kann, bietet es sich regelmäßig an, auch die Abgabe alterner Meldungen zu ermöglichen.

Die Meldekanäle müssen dabei so ausgestaltet sein, dass entweder eine Meldung in Sprachform oder in Textform möglich ist, wobei Sprachform eine telefonische oder sonstige Art der Sprachübermittlung umfassen muss. Das Gesetz sieht ferner vor, dass auch die Möglichkeit einer persönlichen Zusammenkunft zwischen Hinweisgeber und einem Mitarbeiter der Meldestelle bestehen muss, und zwar auf Ersuchen des Hinweisgebers innerhalb einer angemessenen Zeit (§ 16 Abs. 3 Satz 3 HinSchG). Mit Einwilligung des Hinweisgebers kann hierfür auch eine Videokonferenz, bspw. per Teams, Zoom oder Skype, in Betracht kommen (§ 16 Abs. 3 Satz 4 HinSchG).

Eine weitere wichtige Voraussetzung ist schließlich, dass die Einrichtung der Meldekanäle die Wahrung der Vertraulichkeit unterstützen muss. Insbesondere muss sichergestellt werden, dass nur die für die Bearbeitung der Hinweise zuständigen Mitarbeiter der Meldestelle sowie die sie unterstützenden Personen Kenntnis vom Inhalt der eingehenden Hinweise erhalten (§ 16 Abs. 2 HinSchG).

9.3.3.4 Verfahren bei internen Meldungen und Folgemaßnahmen

Neu für viele Unternehmen, die bereits ein Hinweisgebersystem eingeführt haben, sind sicherlich die relativ detaillierten und vor dem Hintergrund eines durchschnittlichen Unternehmensalltags eng getakteten Vorgaben für das Verfahren zur Bearbeitung der eingehenden internen Meldungen. § 17 Abs. 1 HinSchG sieht insofern vor, dass die Meldestelle prüft, ob der abgegebene Hinweis in den Anwendungsbereich des HinSchG fällt (definiert in § 2 HinSchG) und ob er stichhaltig ist. Zudem soll sie mit der hinweisgebenden Person Kontakt halten und diese gegebenenfalls um weitere Informationen ersuchen. Diese Vorgehensweise dürfte ohne weiteres dem bisherigen Vorgehen bei der Bearbeitung von Hinweisen in Unternehmen, die ein Hinweisgebersystem haben, entsprechen. Neu ist hingegen, dass das Gesetz der Meldestelle Fristen im Rahmen der Bearbeitung auferlegt. So muss der hinweisgebenden Person der Eingang des Hinweises innerhalb von sieben Tagen bestätigt werden (§ 17 Abs. 1 Nr. 1 HinSchG) und ihr eine inhaltliche Rückmeldung innerhalb von drei weiteren Monaten gegeben werden (§ 17 Abs. 2 Satz 1 HinSchG).⁹⁹

Zu den Aufgaben der Meldestelle gehört zudem die Ergreifung von Folgemaßnahmen (§ 17 Abs. 1 Nr. 6, § 18 HinSchG). Als solche sieht das Gesetz in § 18 HinSchG vor: Die Durchführung einer internen Untersuchung, die die Kontaktaufnahme zu den betroffenen Personen einschließt, oder den Verweis der hinweisgebenden Person an andere zuständige Stellen oder den Abschluss des Verfahrens aus Mangel an Beweisen bzw. anderen Gründen oder die Abgabe des Verfahrens zwecks weiterer Untersuchungen an eine bei dem Beschäftigungsgeber für interne Ermittlungen zuständige Arbeitseinheit bzw. eine zuständige Behörde.

Die in § 17 Abs. 2 Satz 1 HinSchG vorgesehene inhaltliche Rückmeldung an den Hinweisgeber soll auch eine Mitteilung über bereits ergriffene sowie geplante Folgemaßnahmen enthalten. Die Grenze ist jedoch da zu ziehen, wo diese Mitteilung die weitere Aufklärung oder die Rechte der betroffenen Personen beeinträchtigen könnte.

9.3.4 Implementierung der internen Meldestelle im Unternehmen

Aus den Anforderungen des HinSchG wird deutlich, dass Unternehmen bestehende Hinweisgebersysteme nicht neu erfinden müssen, aber im Detail prüfen sollten, ob ihr System alle Anforderungen des Gesetzes erfüllt.

9.3.4.1 Besetzung und Auswahl der Meldestelle

Die Meldestelle muss sowohl in fachlicher wie auch personeller Hinsicht angemessen ausgestattet sein. Die konkret mit den Aufgaben der Meldestelle befassten Mitarbeiter müssen daher fachlich geschult sein und über ausreichend Erfahrung in der Bearbeitung von Hin-

⁹⁹Dies entspricht den Vorgaben der EU-Richtlinie.

weisen verfügen.¹⁰⁰ Ihre Unabhängigkeit muss, wie unter Abschn. 9.3.3.2 dargestellt, sichergestellt sein (§ 15 Abs. 1 Satz 1 HinSchG). Interessenskonflikte sind dabei zu vermeiden. Dies schließt aber bereits nach dem Gesetzeswortlaut nicht grundsätzlich aus, dass die Mitarbeiter der Meldestelle daneben auch andere Aufgaben im Unternehmen wahrnehmen können. Die Meldestelle kann aus mehreren Mitarbeitern zusammengesetzt sein.¹⁰¹ In Betracht kommen u. a. Mitarbeiter der Compliance-Abteilung, des Bereichs Interne Untersuchungen oder auch des Legal-Bereichs. In kleineren Unternehmen kann die Aufgabe auch beispielsweise dem Datenschutzbeauftragten oder einem etwaig vorhandenen Anti-Korruptionsbeauftragten übertragen werden. Der Gesetzgeber weist in seiner Gesetzesbegründung zudem darauf hin, dass die Übertragung an bestimmte Mitarbeiter für einige Dauer geschehen sollte, damit ein sachgerechtes Arbeiten und die Gewinnung des Vertrauens potenzieller Hinweisgeber ermöglicht wird.¹⁰² Zulässig ist zudem die Einrichtung der internen Meldestelle bei einem Dritten (§ 14 Abs. 1 Satz 1 HinSchG). Dies zielt insbesondere auf die Wahl einer Ombudsperson- bzw. Vertrauensanwaltslösung ab,¹⁰³ aber auch auf Ausgestaltungen im Konzern. Stets ist dabei eine Abstimmung zwischen dem beauftragenden Unternehmen und dem Dritten notwendig (s. hierzu auch Abschn. 9.3.2.3).

9.3.4.2 Meldestellen im Konzern

Eine der für die Praxis wesentlichen und breit diskutierten Fragen ist die Ausgestaltung der Meldestellen im Konzern. Dadurch, dass grundsätzlich für jedes Unternehmen mit mehr als regelmäßig 50 Mitarbeitern die Verpflichtung zur Vorhaltung einer eigenen Meldestelle vorgesehen ist, hat dies grundsätzlich die Verpflichtung zur Vorhaltung einer Vielzahl parallel nebeneinander existierender Meldestellen im Konzern zur Folge. Dies ist für Unternehmen mit vielen nationalen und internationalen Tochtergesellschaften in der Praxis kaum handhabbar, sodass viele Unternehmen eine konzernweite Lösung in Erwägung ziehen.

Die Vorteile der Konzernlösung liegen auf der Hand: Neben dem Aspekt der Ressourcenschonung wird eine spezialisierte, konzernweite Meldestelle angesichts des bei ihr schneller wachsenden Erfahrungsschatzes sowie angesichts der klaren Verantwortlichkeiten und Meldewege, der besseren Anbindung an die Konzernspitze und der vermutlich auch besseren personellen und fachlichen Ausstattung regelmäßig besonders effektiv arbeiten können. Auch die Unabhängigkeit der Frage der Einleitung einer Untersuchung des Hinweises von regionalen Vorbehalten und die Anonymität sowie der weitergehende Schutz der hinweisgebenden Person dürften bei Einrichtung einer zentralen Meldestelle zumindest im Ausgangspunkt besser gewährleistet und gestärkt werden.¹⁰⁴

¹⁰⁰ Siehe auch § 15 Abs. 2 S. 1 HinSchG sowie die Gesetzesbegründung zum Gesetzentwurf der Bundesregierung, zu § 15 Abs. 2, S. 92.

¹⁰¹ Gesetzesbegründung zum Gesetzentwurf der Bundesregierung, zu § 15 Abs. 1, S. 92.

¹⁰² Gesetzesbegründung zum Gesetzentwurf der Bundesregierung, zu § 14 Abs. 1, S. 90.

¹⁰³ Gesetzesbegründung zum Gesetzentwurf der Bundesregierung, zu § 14 Abs. 1, S. 90.

¹⁰⁴ Dzida, B./Seibt, C., NZA 2023, 657 (662); Eggers, T./Pawel, J., CB 2022, 339 (341).

Sowohl die EU-Hinweisgeberrichtlinie (Artikel 8 Abs. 6) als auch das Hinweisgeber-schutzgesetz (§ 14 Abs. 2 HinSchG) haben daher für Unternehmen mit in der Regel 50 bis 249 Beschäftigten die Möglichkeit eingeräumt, Ressourcen zu teilen und eine gemeinsame Meldestelle zu betreiben.

Über diesen Punkt hinausgehend ist die europäische Hinweisegeberzrichtlinie zu der Frage einer konzernweiten Lösung nicht vollends klar. Die Expertengruppe der EU-Kommission zur europäischen Hinweisegeberrichtlinie hat sich daher im Jahr 2021 mehrmals zu der Frage geäußert, ob bereits die alleinige Einrichtung einer einheitlichen, konzernweiten Meldestelle den Anforderungen der Hinweisegeberrichtlinie genügen kann (sog. Konzernlösung). Die Expertengruppe hat diese Frage unter Verweis auf Artikel 8 Abs. 3 der Richtlinie im Ergebnis abgelehnt. Nach dieser Vorschrift gelte die Pflicht zur Einrichtung einer internen Meldestelle aus Artikel 8 Abs. 1 für juristische Personen des privaten Sektors mit 50 oder mehr Arbeitnehmern; eine Ausnahme von dieser Pflicht sehe die Richtlinie nicht vor.¹⁰⁵ Dieser Rechtsauffassung kommt aber keine ausschlaggebende Bedeutung zu, denn allein der Europäische Gerichtshof kann rechtsverbindlich über die Auslegung von Unionsrechtsakten entscheiden (vgl. Artikel 267 Abs. 1 AEUV).

Bei umfassender Betrachtung der Richtlinie gibt es mehrere Argumente dafür, dass die Einschätzung der Expertengruppe der EU-Kommission im Ergebnis nicht zutreffend ist.¹⁰⁶ Der deutsche Gesetzgeber hat indes klargestellt, dass generell eine Delegation auf einen Dritten möglich ist (§ 14 Abs. 1 HinSchG) und dass unter diesem Dritten auch eine in einem Konzernunternehmen eingerichtete Stelle, die für andere Konzerngesellschaften agiert, zu subsumieren ist.¹⁰⁷ So kann also beispielsweise eine bei der Muttergesellschaft eingerichtete Meldestelle auch für andere Konzerntochterunternehmen tätig werden und ist dann in Bezug auf diese Dritte im Sinne des § 14 Abs. 1 Satz 1 HinSchG. Die Verantwortung, einen festgestellten Verstoß abzustellen und zu untersuchen, verbleibt dabei aber stets beim beauftragenden Konzernunternehmen.¹⁰⁸ Eine Berichterstattung der Meldestelle erfolgt daher auch zunächst an dieses Unternehmen. Sofern eine Berichterstattung an die Konzernleitung notwendig erscheint, muss hier die Vertraulichkeit hinsichtlich der Identität der hinweisgebenden Person gewahrt werden und die Berichterstattung im Auftrag des betroffenen Konzernunternehmens erfolgen.¹⁰⁹

In der Praxis werden viele Unternehmen diesen Weg wählen, da die dargestellten Argumente für eine derartige konzernweite Lösung überzeugen und der deutsche Gesetzgeber diesen Weg eröffnet hat. Im Auge behalten werden sollte dessen ungeachtet, ob sich hier in der Zukunft aufgrund europarechtlicher Vorgaben Änderungen ergeben.

¹⁰⁵ So u. a. im Rahmen des fünften Treffens der Expertengruppe am 14.6.2021, vgl. S. 2 ff. des Sitzungsprotokolls: <https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=28015&fromExpertGroups=3709> (aufgerufen am 14.1.2024).

¹⁰⁶ Bürkle, J., CCZ 2022, 335 (340).

¹⁰⁷ Gesetzesbegründung zum Gesetzentwurf der Bundesregierung, zu § 14 Abs. 1, S. 90 f.

¹⁰⁸ Gesetzesbegründung zum Gesetzentwurf der Bundesregierung, zu § 14 Abs. 1, S. 91.

¹⁰⁹ Gesetzesbegründung zum Gesetzentwurf der Bundesregierung, zu § 14 Abs. 1, S. 91.

Insbesondere, aber nicht nur, im international tätigen Konzern muss zudem sichergestellt sein, dass durch die Einrichtung einer zentralen Meldestelle keine zusätzlichen Barrieren für eine Hinweisabgabe geschaffen werden. Dies schließt mit ein, dass eine Abgabe der Meldung in der in dem jeweiligen Konzernunternehmen vorherrschenden Arbeitssprache erfolgen kann. Die Einhaltung nationaler Schutzrechte hinsichtlich der Identität des Hinweisgebers sowie der Datenschutzregelungen ist eine weitere zu beachtende Notwendigkeit bei der Ausgestaltung der (zentralen) Meldestelle.¹¹⁰ Im internationalen Konzern zu beachten ist allerdings, dass die nationalen Umsetzungsgesetze anderer Mitgliedstaaten nicht explizit eine Konzernlösung vorsehen und dort die Pflicht zur Einrichtung einer internen Meldestelle wohl bestehen dürfte. In diesen Fällen ist neben der zentralen Meldestelle als zusätzliche Option auch ein lokaler Meldekanal einzurichten. Insofern wird dann eine Koordination mit der zentralen Meldestelle vor dem Hintergrund der jeweiligen lokalen Regelungen erforderlich.

9.3.4.3 Auswahl der Meldekanäle

Das Hinweisgeberschutzgesetz sieht hinsichtlich der einzurichtenden Meldekanäle bewusst eine breite Flexibilität vor. § 16 Abs. 1 Satz 1 und 2 HinSchG regelt insofern, dass die Meldekanäle zumindest den eigenen Beschäftigten und etwaigen Leiharbeitnehmerinnen und -arbeitnehmern offenstehen müssen. Fakultativ kann das Unternehmen die Meldekanäle auch für Geschäftspartner öffnen (vgl. 16 Abs. 1 Satz 3 HinSchG). Gleiches gilt für die Frage, ob die Abgabe anonymer Hinweise ermöglicht wird oder nicht. Anonym abgegebene Hinweise sollen jedoch in jedem Fall bearbeitet werden, wenn auch grundsätzlich subsidiär zu nicht anonym abgegebenen Hinweisen (vgl. 16 Abs. 1 Satz 4 HinSchG; zu alldem s. bereits Abschn. 9.3.3.).

Im Übrigen wollte es der Gesetzgeber den Unternehmen im Hinblick auf die Auswahl des oder der geeigneten Meldekanäle möglichst einfach machen. Wie dargestellt reicht es aus, entweder eine Meldung in mündlicher oder in Textform sowie persönliche Treffen zu ermöglichen (§ 16 Abs. 1 und 3 HinSchG). Entscheidend ist insgesamt, dass die Vertraulichkeit der Identität der hinweisgebenden Person gewahrt wird.¹¹¹ Insofern müssen Unternehmen die Vor- und Nachteile der verschiedenen Möglichkeiten, einen Meldekanal auszustalten, vor dem Hintergrund ihrer individuellen Anforderungen abwägen.

9.3.4.4 Abwägung der Vor- und Nachteile der verschiedenen Meldekanäle

Vorteil einer reinen Telefon-Hotline war in der Vergangenheit die üblicherweise sichergestellte Erreichbarkeit rund um die Uhr. Zudem bestehen in der Regel keine Sprachbarrieren, da der Hinweisgeber innerhalb von wenigen Minuten an einen Ansprechpartner in seiner Sprache verbunden werden kann bzw. die ihm bekannt gemachte Telefonnummer ihn automatisch zu einem Kontakt in der jeweiligen Landessprache führt. Eine solche Hotline war daher gerade in internationalen Konzernen eine Möglichkeit, eine

¹¹⁰ Gesetzesbegründung zum Gesetzentwurf der Bundesregierung, zu § 14 Abs. 1, S. 91.

¹¹¹ Gesetzesbegründung zum Gesetzentwurf der Bundesregierung, zu § 16 Abs. 3, S. 94.

weltweite Abdeckung zu erreichen. Die Einrichtung eines Call-Centers als eine auf einen Dritten ausgelagerte Meldestelle im Sinne des Hinweisgeberschutzgesetzes dürfte sich jedoch praktisch schwierig darstellen. Die Möglichkeit zur Abgabe von telefonischen Hinweisen bzw. Meldungen dürfte daher nicht mehr auf diesem Weg sinnvoll sein. Stattdessen kommen lokale Telefonnummern in Betracht, die direkt mit der internen Meldestelle verbinden, die wiederum vom Unternehmen selbst oder einem Dritten, insbesondere in Form einer Rechtsanwaltskanzlei, betrieben werden. Einige Anbieter von internetbasierten Lösungen bieten zudem an, dass neben der Abgabe über das internetbasierte System Hinweise auch über ein Sprachsteuerung abgegeben werden können.

Ein großer Vorteil von internetbasierten Systemen ist vor allem die niedrige Hemmschwelle, die ein Hinweisgeber für seine Nutzung überwinden muss: Der Hinweis kann zu jeder Zeit, zumeist in der eigenen Sprache, ohne die Notwendigkeit eines persönlichen Kontakts mit einer anderen Person und zudem anonym abgegeben werden.¹¹² Den Vorwurf belegende Unterlagen können oftmals direkt per Upload dem Hinweis beigelegt werden; Rückfragen sind möglich, sofern der Hinweisgeber hiermit einverstanden ist. Das System bietet zudem eine deutlich höhere Sicherheit im Hinblick auf die Geheimhaltung der eigenen Identität als beispielsweise eine Hinweiserteilung per E-Mail. Auch die durch technische Filtermechanismen bestehende Möglichkeit, Hinweise themenbezogen Hinweisempfängern zuzuordnen macht die Bearbeitung effizienter. Hinzu kommt eine Reihe von Tools zur Dokumentation, Strukturierung und Auswertung der Hinweise. Auch Erinnerungen und die Fristenkontrolle können über viele Systeme einfach gemanagt werden. Schließlich sind die im System gespeicherten Daten regelmäßig vor fremdem (unbefugtem) Zugriff gesichert.

Von manchen Hinweisgebern wird es als Nachteil angesehen, dass bei diesem Meldekanal zunächst keine persönliche Ansprache in Form einer direkten verbalen Kommunikation zwischen Hinweisemänger und Hinweisgeber erfolgen kann. Als Kehrseite der niedrigen Hemmschwelle wird zuweilen das möglicherweise höhere Risiko von bewusst schädigenden, denunziatorischen Hinweisen sowie etwaiger „Schüsse ins Blaue“ angesehen, d. h. von Hinweisen, bei denen der Hinweisgeber selbst eher einen Missstand vermutet als ihn tatsächlich kennt und durch seinen Hinweis eine Überprüfung in Gang setzen will. In der Praxis bestätigen sich solche Bedenken aber regelmäßig nicht. Ein Aspekt, der sicher beachtet werden muss, ist dass im Rahmen einer Kosten-Nutzen-Analyse geprüft werden sollte, ob sich sowohl der einmalige als auch der laufende finanzielle Aufwand für die Implementierung eines solchen Systems für das konkrete Unternehmen rechnet.

Ein wesentlicher Aspekt hinsichtlich des Ombudsperson-Systems ist, dass die externe Ombudsperson oder der Vertrauensanwalt auch insgesamt die Rolle der internen Meldestelle wahrnehmen kann. Das Hinweisgeberschutzgesetz sieht explizit die Möglichkeit vor, eine unternehmensexterne Person mit der Wahrnehmung der internen Stelle zu beauftragen.

¹¹²Vgl. zu den Vor- und Nachteilen bereits Altenburg, J., Bucerius Law Journal 2008, 3 ff.

Ein besonderer Vorteil des Ombudsperson-Systems wiederum ist, dass die geschulte Ombudsperson durch geschicktes Fragen in der Regel sehr schnell herausfinden kann, wie gravierend der vom Hinweisgeber geschilderte Sachverhalt ist. Auch wird er schnell feststellen können, ob der Hinweisgeber in guter Absicht handelt oder ob die Wahrscheinlichkeit eines denunziatorischen Hinweises besteht. Die Möglichkeit eines persönlichen Treffens kann in dieser Konstellation recht schnell und direkt vereinbart werden. Auch der Gesetzgeber hat offensichtlich erkannt, dass zum einen ein Bedürfnis des Hinweisgebers für ein persönliches Treffen bestehen kann, zum anderen ein persönliches Treffen es aber auch dem Unternehmen ermöglicht, die Informationen auf Plausibilität und Schlüssigkeit hin zu überprüfen und sich ein persönliches Bild vom Hinweisgeber zu machen.

Die höhere Hemmschwelle für den Anrufenden, nämlich das Wissen, dass sein Anliegen direkt einem Dritten, zudem in der Regel einem Anwalt, in einem persönlichen Gespräch vorzutragen ist, reduziert ebenfalls das Risiko von bewussten Falschmeldungen oder von unsachlichen oder unerheblichen Meldungen ganz erheblich. Auf der anderen Seite bietet es denen, die auf Grund des beobachteten oder unter Umständen selbst begangenen Fehlverhaltens in einem Gewissenskonflikt sind, die Möglichkeit, diesen in einem vertrauensvollen Gespräch mit einem erfahrenen Gesprächspartner zu adressieren, der ihnen dann Hinweise geben kann, wo sie weitere Unterstützung finden. Eine inhaltliche Beratung des Hinweisgebers ist der Ombudsperson verwehrt, da sie sich anderenfalls als Vertreter des Unternehmens in einem Interessenskonflikt wiederfindet.¹¹³ Die rechtlich versierte Ombudsperson kann zudem bei der Weiterleitung des Hinweises ihre juristische Bewertung ergänzen.

Klarer Nachteil des Ombudsperson-Systems ist hingegen, dass nur eine eingeschränkte zeitliche Erreichbarkeit gegeben ist: Dies gilt sowohl im Hinblick auf die Erreichbarkeitszeiten, in der Regel die üblichen Geschäftszeiten, wie beispielsweise 8 bis 19 Uhr, als auch während der Geschäftszeiten selbst: Selten wird ein Rechtsanwalt nur die Tätigkeit einer Ombudsperson ausüben und selbst dann wird er sich immer wieder mal in Besprechungen, im Flugzeug oder in anderweitigen Telefonaten befinden. Auch wenn regelmäßig Vorkehrungen getroffen werden, umgehend zurückzurufen, kann es dadurch dazu kommen, dass Hinweisgeber, die zunächst den Mut gefasst haben einen Missstand zu melden, dieses nach einer misslungenen Kontaktaufnahme wieder verwerfen. Zudem kann ein direkter Kontakt mit der Ombudsperson einzelne Hinweisgeber abschrecken. In internationalen Unternehmen wiederum bestehen gegebenenfalls Sprachbarrieren, die allerdings durch ein Netz von lokalen Ombudsleuten kompensiert werden können. Die Implementierungs- und Vorhaltungskosten dürften hingegen bei einer normalen Auslastung regelmäßig weniger ins Gewicht fallen.

Schließlich bietet sich neben allem stets die Möglichkeit, eine direkte telefonische Kontaktaufnahme mit der Meldestelle selbst zu ermöglichen, wofür im Unternehmen eine entsprechende Telefonnummer bekannt gemacht wird. Auch kann grundsätzlich angeboten werden, dass Hinweise per E-Mail oder Brief an die Meldestelle direkt gemeldet

¹¹³ Siehe aber: Goers, M. (2009), S. 34. Ebenso bspw. Brockhaus, M., CB 2023, 8 (14).

werden können. Der klassische Briefkasten wird insofern durchaus noch genutzt. Bei all diesen Varianten stellen sich zunächst auch die oben genannten Vor- und Nachteile im Hinblick auf die Erreichbarkeit, die Hemmschwelle zur Kontaktaufnahme, die Möglichkeit einer anonymen Abgabe und der Möglichkeit, direkt einen konkreten Ansprechpartner persönlich zu erreichen. Ein grundsätzlich zu bedenkender Aspekt, der in diesem Zusammenhang noch erwähnt werden soll, ist, dass die Tatsache, dass es sich bei den Mitarbeitern der Meldestelle um interne Mitarbeiter des Unternehmens handelt, sowohl Vorteil als auch Nachteil sein kann. Ein Vorteil ist, dass diese das Unternehmen in der Regel gut kennen und daher schnell die prinzipielle Validität der Hinweis einschätzen können. Zudem sind einzelne Hinweisgeber im direkten Kontakt mit Kollegen auch offener. Andere Hinweisgeber hingegen werden möglicherweise internen Kollegen mehr misstrauen als beispielsweise einer Ombudsperson. Letztlich stellen sich diese Fragen aber auch auf einer zweiten Stufe, wenn Hinweise über ein Callcenter oder ein internetbasiertes System abgeben und dann an die Mitarbeiter der Meldestelle weitergegeben werden.

Das Hinweisgeberschutzgesetz sieht schließlich vor, dass auch die Möglichkeit eines persönlichen Treffens eingeräumt werden muss (vgl. § 16 Abs. 3 Satz 2 HinSchG). Dies wird regelmäßig mit einer Bitte zur vorherigen Terminabsprache einhergehen.

9.3.4.5 Konkrete Auswahl

Letztlich muss sich die Auswahl an den individuellen Bedürfnissen jeden Unternehmens orientieren, d. h. insbesondere an seiner Größe bzw. Mitarbeiterzahl, der Anzahl der einzubehandelnden Gesellschaften und ihres Sitzes, dem organisatorischen Aufbau, dem Geschäftsmodell und der individuellen Risikoexposition für typische Compliance-Risiken. Während für kleinere Unternehmen die Variante der Ombudsperson bzw. des Vertrauensanwalts eine Lösung sein mag, wird es sich bei größeren Unternehmen regelmäßig empfehlen, einen Mix an Meldekanälen anzubieten. Neben einem internetbasierten System könnte dies die Einrichtung der Möglichkeit einer telefonischen Kontaktaufnahme mit der Meldestelle oder des zusätzlichen Angebots, eine Ombudsperson kontaktieren zu können, sein. Umgekehrt können Hindernisse in der sprachlichen und zeitlichen Erreichbarkeit von bestehenden Ombudsperson-Systemen durch das zusätzliche Angebot eines internetbasierten Tools kompensiert werden. Zudem stellt ein solches Tool regelmäßig eine erhebliche Hilfestellung bei der Verwaltung der Hinweisannahme und -bearbeitung dar. Oftmals kann dies auch mit einem zusätzlichen digitalen Case-Management verknüpft werden. Insgesamt sollte darauf geachtet werden, das Angebot vor allem möglichst niedrigschwellig zu halten.¹¹⁴

Jedes Unternehmen muss daher vor dem Hintergrund finanzieller und personeller Ressourcen den für das konkrete Unternehmen angemessenen Weg wählen. Auswahlmöglichkeiten hat es viele.

¹¹⁴ Siehe zur Bedeutung der Niedrigschwelligkeit auch bei Hauser, C./Stühlinger, L., CB 2018, 443 (448).

9.3.4.6 Interne Richtlinien und Kommunikation

Das Gesetz sieht, wie dargestellt, eine Reihe von Kommunikationspflichten zwischen Meldestelle und Hinweisgeber, aber auch Informationspflichten gegenüber den Betroffenen vor. Hinzu kommt, dass in dem Fall, dass die interne Meldestelle auch als Dritte für andere Konzerngesellschaften fungiert, verschiedene organisatorische Aspekte zu beachten sind. Auch müssen weitere Anforderungen, wie das Vorhalten von Informationen zu externen Meldestellen, eingehalten werden.

In der Regel wird daher die Notwendigkeit für eine entsprechende interne Richtlinie und eine Organisationsanweisung hinsichtlich der Zusammensetzung und der Wahrnehmung der Aufgaben der internen Meldestelle bestehen. Darüber hinaus ist eine Richtlinie zur Bearbeitung eingehender Hinweise, die auch den Mitarbeitern, also den potenziellen Hinweisgebern, zur Verfügung gestellt wird, essenziell.¹¹⁵ Für die Fälle, in denen die interne Meldestelle die Durchführung einer internen Untersuchung an eine andere Stelle im Unternehmen, etwa an eine Abteilung Interne Untersuchungen oder Compliance-Untersuchungen, weitergibt und die Mitglieder dieser Einheit und die der internen Meldestelle nicht identisch sind, muss zudem die Zusammenarbeit zwischen diesen Stellen geregelt werden, bspw. im Hinblick auf die Vertraulichkeit.¹¹⁶

Schließlich – und das ist der für den Erfolg des Hinweisgebersystems entscheidende Faktor – müssen die Einführung und das Vorhalten des Systems von einem überzeugenden internen Kommunikationskonzept begleitet werden.

9.3.4.7 Kommunikation und Integration

Es zeigt sich seit jeher, dass der Erfolg eines internen Hinweisgebersystems nicht zuletzt von seinem Bekanntheitsgrad, seiner Akzeptanz bei Führungskräften und beim Betriebsrat sowie bei den Mitarbeitern selbst abhängt.¹¹⁷

In der Vergangenheit standen der Einführung eines Hinweisgebersystems vielfach jedoch Bedenken entgegen. Nicht selten wurde die Einführung eines Hinweisgebersystems als Einstieg in eine Kultur des Misstrauens angesehen, die nicht mit einer auf Vertrauen basierenden Unternehmensführung in Einklang zu bringen sei. Diese Bedenken treten in der Regel in stärkerem Maße in mittelständischen, oft auch vom Eigentümer selbst geführten, Unternehmen auf, als in internationalen Konzernen. Gerade vor dem Hintergrund der deutschen Geschichte des vergangenen Jahrhunderts besteht vielfach Zurückhaltung gegenüber einem Instrument, das vermeintlich der Besitzelung Tür und Tor öffnet. Zwar kann man die in der Vergangenheit teilweise langwierige Diskussion, ob die Einführung eines Hinweisgebersystems überhaupt erfolgen soll, nunmehr häufig mit Verweis auf das Hinweisgeberschutzgesetz recht kurz halten. Dennoch empfiehlt es sich, solche Vorbehalte ernst zu nehmen, die Ausgestaltung und Zielsetzung des Hinweisgebersystems den

¹¹⁵ Siehe hierzu auch: Clodius, S./Warda, O., CB [2021](#), 137 (138 f.).

¹¹⁶ Siehe dazu auch Gesetzesbegründung zum Gesetzentwurf der Bundesregierung, zu § 18, S. 95.

¹¹⁷ Zur Frage der Akzeptanz auch: Bruns, P., NJW [2023](#), 1609 (1617); Moosmayer, K. ([2021](#)), Rn. 188; Taschke, J./Pielow, T./Volk, E., NZWiSt [2021](#), 85 (91).

Mitarbeitern deutlich zu machen und sie im Rahmen der Einführung frühzeitig abzuholen und einzubinden. Es sollte hervorgehoben werden, dass kein Raum für Denunzierungen geschaffen wird und dass bewusster Missbrauch des Hinweisgebersystems nicht akzeptiert und dagegen vorgegangen werden wird; zudem besteht in diesen Fällen kein Schutz vor Repressalien gemäß dem Hinweisgeberschutzgesetz (vgl. §§ 33 Abs. 1 Nr. 2 i. V. m. § 38 HinSchG). Gleichermassen muss das Vertrauen gutgläubiger Hinweisgeber gestärkt werden; sie müssen die Überzeugung bekommen, dass ihr Schutz ernst genommen wird.

Das Hinweisgebersystem muss zudem gut in das bestehende Compliance-Management-System integriert werden. Neben prozessimmanenten Kontrollen des internen Kontrollsystens stellt das Hinweisgebersystem eine übergreifende Maßnahme dar, die unabhängig vom konkreten operativen Prozess eine Anlaufstelle für Mitarbeiter bei Fehlverhalten darstellt. Für das Compliance-Management-System ist es gerade deshalb von großer Bedeutung, da über diesen Weg unabhängig von konkreten Stichproben und Kontrollen die Möglichkeit zur Aufdeckung von Fehlverhalten besteht. Es ergänzt das Compliance-Management-System um eine Maßnahme zur flächendeckenden und effektiven Überwachung und erhöht somit die Kontrolldichte.¹¹⁸ Nach wie vor wird eine hohe Anzahl von Compliance-Verstößen durch Mitarbeiter aufgedeckt, da diese unmittelbar am Geschäftsgeschehen des Unternehmens beteiligt sind. Die Möglichkeit zur geschützten Hinweiseerteilung stärkt das Compliance-Management-System insgesamt.

9.4 Rechtliche Einzelfragen

9.4.1 Arbeitsrechtliche Fragestellungen

Aus kollektivarbeitsrechtlicher Sicht stellt sich – neben weiteren Detailfragen des Individualarbeitsrechts, wie beispielsweise der Einbeziehung des Hinweisgebersystems in den einzelnen Arbeitsvertrag¹¹⁹ – die Frage, inwieweit bei der Einführung eines Hinweisgebersystems Mitbestimmungsrechte des Betriebsrats bestehen. Der rechtlichen Frage vorweg gestellt sei dabei der Hinweis, dass das Hinweisgebersystem nur dann erfolgreich sein kann, wenn die, die es nutzen sollen – also in der Regel die Arbeitnehmer – es auch akzeptieren. Es dürfte daher im Interesse des Unternehmens sein, den Betriebsrat für das Hinweisgebersystem zu gewinnen.

Der Betriebsrat ist grundsätzlich über die (geplante) Einführung eines Hinweisgebersystems zu informieren (§ 80 Abs. 2 S. 1 BetrVG). Bei der Bestimmung zwischen im Übrigen mitbestimmungspflichtigen und mitbestimmungsfreien Maßnahmen ist¹²⁰ zunächst festzustellen, dass mit Einführung des Hinweisgeberschutzgesetzes die Frage des „Ob“

¹¹⁸ Schemmel, A./Ruhmannseder, F./Witzigmann, T., (2012), 3. Kapitel, Rn. 24.

¹¹⁹ Siehe hierzu im Detail Schemmel, A./Ruhmannseder, F./Witzigmann, T., (2012), 5. Kapitel, Rn. 150 ff.; s. ferner Baade, M.I./Hößl, T., DStR 2023, 1213 ff. und 1265 ff.

¹²⁰ Siehe auch Götz, J., NZA 2023, 1433, 1435.

der Einführung eines Hinweisgebersystems bei unter den Anwendungsbereich fallenden Unternehmen gesetzlich vorgeschrieben und damit nicht mitbestimmungspflichtig ist. Im Übrigen ist bei der Implementierung eines Hinweisgebersystems zwischen dem Ob der Hinweiserteilung und dem Wie, d. h. dem Meldeverfahren, zu unterscheiden.¹²¹

Interne Vorschriften, die das „Ob“ der Hinweiserteilung betreffen und über die arbeitsvertraglichen Hinweispflichten, die Wiederholung gesetzlicher Vorgaben oder das Direktionsrecht des Arbeitgebers hinausgehen, werden von § 87 Abs. 1 Nr. 1 BetrVG erfasst.¹²² Diese Vorschriften beeinflussen nämlich die Zusammenarbeit im Betrieb sowie den offenen Umgang zwischen den Arbeitnehmern untereinander. Es wird auch argumentiert, dass bei der Einführung eines Hinweisgebersystems nicht ausgeschlossen werden könne, dass eine dadurch entstehende Hinweispflicht auf das betriebliche Sozialgefüge Auswirkungen hat, da Arbeitnehmer Angst vor Denunzierung bekommen.¹²³ Nach der Rechtsprechung des Bundesarbeitsgerichts kommt es auch nicht darauf an, ob es sich um eine verbindliche Regelung handelt oder ob dem Arbeitnehmer ein Ermessensspielraum verbleibt.¹²⁴

Bei der Regelung des „Wie“ handelt es sich insoweit ebenfalls um eine mitbestimmungspflichtige Regelung gemäß § 87 Abs. 1 Nr. 1 BetrVG, soweit geregelt wird, auf welche Art der Mitarbeiter seinen Hinweis abgeben soll.¹²⁵

Bei der Einführung einer Telefon-Hotline bzw. einer internetbasierten Möglichkeit zur Hinweiserteilung ist zudem ein Mitbestimmungsrecht gemäß § 87 Abs. 1 Nr. 6 BetrVG zu prüfen, d. h. ein Mitbestimmungsrecht auf Grund der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.¹²⁶ Sofern beispielsweise aufgrund der Erfassung von Daten eine Identifizierung des Meldenden möglich ist, wird vertreten, dass ein solches Mitbestimmungsrecht besteht.¹²⁷ Auszuschließen wäre es aber etwa, wenn die Hotline nur dem Zweck der Informationsübermittlung dient und der Hinweisgeber anonym bleibt und auf eine Überwachung bzw. Aufzeichnung verzichtet wird.¹²⁸

9.4.2 Datenschutzrechtliche Fragestellungen

Das Hinweisgeberschutzgesetz bringt neue datenschutzrechtliche Herausforderungen mit sich:

¹²¹ Siehe im Einzelnen zu diesen Fragen: Klasen, E./Schäfer, S., BB [2012](#), 641 (642) sowie Baade, M.I./Hößl, T., DStR [2023](#), 1213 (1218 f.).

¹²² BAG, NZA [2008](#), 1248; Reinhard, A., NZA [2016](#), 1233 (1234 f.), Götz, J., NZA [2023](#), 1433, 1435.

¹²³ Kock, M., MDR [2006](#), 673 (675).

¹²⁴ BAG, NZA [2008](#), 1248 (1254) (str.).

¹²⁵ Reinhard, A., NZA [2016](#), 1233 (1235).

¹²⁶ Dzida, B./Granetzny, T., NZA [2020](#), 1201 (1205).

¹²⁷ Fahrig, S., NJOZ [2010](#), 975 (979).

¹²⁸ Siehe hierzu: Klasen, E./Schaefer, S., BB [2012](#), 641 (643); s. aber Götz, J., NZA [2023](#), 1433 (1435f.).

9.4.2.1 Grundsätzliches

Im Zuge der Entgegennahme und weiteren Verarbeitung von Hinweisen eines Hinweisgebers werden durch die interne Meldestelle zwangsläufig personenbezogene Daten verarbeitet. Denn gem. Artikel 4 Nr. 1 DSGVO sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Bei der Einrichtung und dem Betrieb der internen Meldestelle sind daher datenschutzrechtliche Anforderungen zu beachten. Für diese soll nachfolgend sensibilisiert werden. Eine detaillierte Auseinandersetzung mit diesem Thema ist bei der Einführung eines Hinweisgebersystems unter Berücksichtigung der weiteren Vorgaben des Compliance-Management-Systems insgesamt durchzuführen (dazu sogleich Abschn. 9.4.2.2).

Zu beachten sind insbesondere die Regelungen des Bundesdatenschutzgesetzes (BDSG) sowie der Datenschutzgrundverordnung (DSGVO), deren Bestimmungen vorrangig zur Anwendung zu bringen sind;¹²⁹ aktuell wird zudem ein erneuter Versuch in Sachen Normierung eines Beschäftigtendatenschutzgesetz unternommen.¹³⁰

Ausgangspunkt jeder Verarbeitung personenbezogener Daten ist Artikel 6 DSGVO, der einen Katalog mit Bedingungen enthält, bei deren Vorliegen die Verarbeitung rechtmäßig ist.¹³¹

Für Unternehmen, die in den Anwendungsbereich des HinSchG fallen, ist die Verarbeitung aus datenschutzrechtlicher Sicht (schon dann) zulässig, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, erforderlich ist (vgl. Artikel 6 Abs. 1 Satz 1 lit. c DSGVO). Parallel zu den im HinSchG enthaltenen Verpflichtungstatbeständen findet sich in § 10 HinSchG ein expliziter Erlaubnisstatbestand. Danach sind Meldestellen dazu befugt, personenbezogene Daten zu verarbeiten, soweit dies zur Erfüllung ihrer in den §§ 13 und 24 des HinSchG bezeichneten Aufgaben erforderlich ist (vgl. § 10 Abs. 1 HinSchG).

Auch die Verarbeitung besonders persönlicher oder sensibler personenbezogener Daten (sog. besonderer Kategorien personenbezogener Daten) durch eine Meldestelle ist ausnahmsweise zulässig. Bei diesen Daten handelt es sich gem. Artikel 9 Abs. 1 DSGVO um personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie um genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder zu der sexuellen Orientierung einer natürlichen Person. Eine Verarbeitung dieser Daten ist grundsätzlich nicht zulässig (vgl. Artikel 9 Abs. 1 DSGVO). Etwas anderes gilt aber, wenn die Verarbeitung dieser Daten zur Erfüllung der Aufgaben der Meldestelle erforderlich ist (vgl. § 10 Abs. 2 HinSchG). In diesem Fall hat die Meldestelle jedoch spezifische und angemessene Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen; § 22 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes ist entsprechend anzuwenden (§ 10 Abs. 3 HinSchG).

¹²⁹ Sydow, G. in: Sydow, G./Marsch, N., DS-GVO | BDSG, Einleitung Rn. 9.

¹³⁰ Schemmel, F., ZD-Aktuell 2023, 01164.

¹³¹ ausführlich hierzu Handel, T. (2023), S. 69 ff.

Unternehmen, die nicht in den Anwendungsbereich des HinSchG fallen, können sich nicht auf § 10 HinSchG berufen. Sie sind für die Zulässigkeit der Datenverarbeitung im Rahmen eines Hinweisgeberschutz- bzw. Meldesystems daher auf die Erfüllung der anderen Bedingungen des Katalogs des Artikel 6 Abs. 1 Satz 1 DSGVO angewiesen.

Weitere datenschutzrechtliche Fragestellungen ergeben sich, soweit es um die Auswirkungen der nach Artikel 14, 15 DSGVO bestehenden Unterrichtungs- und Aufklärungspflichten des Betroffenen sowie um die Löschpflichten nach Artikel 17 Abs. 1 DSGVO im laufenden Hinweisgeberverfahren geht.¹³² Hierzu sollten interne Regelungen getroffen werden bzw. entsprechende Informationen bereitgestellt werden.

9.4.2.2 Pflicht zur Benennung eines Datenschutzbeauftragten

Eine Pflicht zur Benennung eines Datenschutzbeauftragten bestand bislang nicht für alle, insbesondere nicht für kleinere Unternehmen. Denn § 38 Abs. 1 Satz 1 Hs. 2 BDSG, der die Benennung von Datenschutzbeauftragten bei nicht öffentlichen Stellen regelt, nimmt all jene Unternehmen von der Pflicht zur Benennung eines Datenschutzbeauftragten aus, die in der Regel nicht mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

In den Fällen der Durchführung einer Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO ist die Benennung eines Datenschutzbeauftragten gemäß § 38 Abs. 1 Satz 2 Var. 1 BDSG jedoch zwingend. Dies gilt zudem unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen (vgl. § 38 Abs. 1 Satz 2 Var. 1 BDSG a.E.).

Was folgt daraus mit Blick auf das HinSchG? Aus datenschutzrechtlicher Sicht handelt es sich bei dem Betrieb einer internen Meldestelle angesichts der regelhaften Verarbeitung personenbezogener Daten i. S. d. Artikel 4 Nr. 1 DSGVO um einen in datenschutzrechtlicher Sicht risikobehafteten Betrieb.¹³³ Gem. Artikel 35 Abs. 1 DSGVO muss der Verantwortliche vor einem vorgesehenen Verarbeitungsvorgang eine Datenschutz-Folgenabschätzung durchführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Dies wird im Falle der Entgegennahme von Hinweisen zu Missständen i. S. d. HinSchG der Fall sein (s. auch die Beispiele in Artikel 35 Abs. 3 lit. a DSGVO).¹³⁴ Gem. Artikel 35 Abs. 2 DSGVO holt der Verantwortliche bei der Durchführung der Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten ein, sofern ein solcher benannt wurde.

¹³²Vgl. Fehr, S., ZD 2022, 256 (258 f.).

¹³³Vgl. eingehend Fehr, S., ZD 2022, 256 sowie die Abhandlung von Tasch, M., <https://ituso.de/news/hinweisgeberschutzgesetz-notwendigkeit-datenbeschutzbeauftragter/> (aufgerufen am 14.1.2024).

¹³⁴Siehe hierzu auch die DSK-Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines vom 14.11.2018, dort Kap. 9, erhältlich unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/Orientierungshilfen/DSK_20181114_Orientierungshilfe_Whistleblowing_Hot.html (aufgerufen am 14.1.2024).

Daraus folgt, dass jedes Unternehmen ab 50 Mitarbeitern, das in den Anwendungsbereich des HinSchG fällt, ab dem 17. Dezember 2023 nicht nur dazu verpflichtet ist, eine interne Meldestelle nach dem HinSchG einzurichten, sondern für diesen Prozess auch (mindestens) eine Datenschutz-Folgenabschätzung nach Artikel 35 Abs. 1 DSGVO durchzuführen und in diesem Zusammenhang, falls noch nicht vorhanden, einen Datenschutzbeauftragten zu bestellen.

9.4.3 Strafrechtliche Fragestellungen

Aus strafrechtlicher Sicht stellt sich im Rahmen des Hinweisgebersystems zum einen die Frage, ob und wenn ja, wie die Wahrung der Anonymität des Hinweisgebers gegenüber Ermittlungsbehörden durch Zeugnisverweigerungsrechte geschützt werden kann. Zum anderen stellt sich die Frage, ob und wenn ja, wie sichergestellt werden kann, dass erhaltene Hinweise nicht gegen den Willen des Unternehmens oder des Hinweisgebers den staatlichen Ermittlungsbehörden zur Kenntnis gelangen, etwa im Fall der Beschlagnahme von Unterlagen im Rahmen einer Durchsuchung.

Diese Fragen erlangen besondere Bedeutung, wenn der Hinweisgeber selbst in mögliche Straftaten involviert ist. Insofern ist zunächst darauf hinzuweisen, dass § 9 HinSchG diesbezüglich eine explizite Ausnahmeregelung vom Vertraulichkeitsgebot regelt. Gemäß § 9 Abs. 1 HinSchG dürfen Informationen über die Identität einer hinweisgebenden Person oder über sonstige Umstände, die Rückschlüsse auf die Identität dieser Person erlauben, in Strafverfahren auf Verlangen der Strafverfolgungsbehörden an diese herausgegeben werden.¹³⁵

Grundsätzlich ist des Weiteren zu beachten, dass ein Schutz durch Zeugnisverweigerungsrechte dem Hinweisgeber nur in den Fällen zugesichert werden kann, in denen dem Hinweisnehmer auf Grund gesetzlicher Vorgaben ein solches zusteht. Bei einem etwaigen Strafprozess wäre dies insbesondere der Fall, wenn der Hinweisnehmer den Regelungen des § 53 StPO unterfällt. Diese Voraussetzungen wären beispielsweise bei einem als Ombudsperson eingesetzten externen Rechtsanwalt erfüllt, der ein Mandat mit einem Unternehmen über die Wahrnehmung der Tätigkeit als Ombudsperson hat. Die Frage, ob ein als Ombudsperson eingeschalteter Rechtsanwalt hinsichtlich der ihm von einem Mitarbeiter mitgeteilten Informationen zeugnisverweigerungsberechtigt ist, ist ebenfalls zu bejahen. § 53 Abs. 1 S. 1 Nr. 3 StPO schützt auch sogenannte Drittgeheimnisse, d. h. solche Informationen, an deren Geheimhaltung ein erkennbares Interesse besteht, auch wenn sie nicht der Geheimnissphäre des Mandanten entstammen. Entscheidend ist, dass dem Rechtsanwalt diese Geheimnisse in der Ausübung seiner anwaltlichen Tätigkeit anvertraut werden.¹³⁶ Im Ergebnis sind damit alle In-

¹³⁵ Zu den weiteren Voraussetzungen und Informationspflichten siehe im Einzelnen § 9 HinSchG.

¹³⁶ Hessler, M., AnwBl 2019, 212 (217).

formationen, die die Ombudsperson im Rahmen der Ausübung dieser Tätigkeit vom Hinweisgeber erhält, umfasst.¹³⁷

Zu beachten bleibt, dass die Ombudsperson nicht gehindert werden kann, entgegen ihrem bestehenden Zeugnisverweigerungsrecht und ohne von diesem entbunden worden zu sein, Angaben zu machen. Solche Angaben sind auch in aller Regel verwertbar.¹³⁸ Die Wahrscheinlichkeit ist jedoch ausgesprochen gering, da in solchen Fällen regelmäßig eine Strafbarkeit nach § 203 StGB für die Ombudsperson vorliegt.

Interne Stellen im Unternehmen können regelmäßig keinen solchen Schutz bieten; damit droht also die Gefahr der Preisgabe von Informationen durch Zeugenaussagen, wenn der interne Mitarbeiter im Rahmen eines Strafverfahrens durch das Gericht oder im Ermittlungsverfahren durch die Staatsanwaltschaft als Zeuge zu den erhaltenen Informationen befragt wird. Das HinSchG sieht insofern keine Ausnahmen vor.

Inwieweit der Syndikusrechtsanwalt unter den Schutzbereich des § 53 StPO fällt, war lange Zeit strittig. § 53 Abs. 1 Satz 1 Nr. 3 StPO ist durch Gesetz vom 21. Dezember 2015 neu geregelt worden und stellt nunmehr klar, dass Syndikusrechtsanwälten – vorbehaltlich des § 53a StPO – kein Zeugnisverweigerungsrecht für das ihnen in dieser Eigenschaft Anvertraute oder Bekanntgewordene zusteht, d. h. wenn sie allein wie Angestellte für ihr Unternehmen tätig werden.

Auch der Mitarbeiter einer Hotline, der Hinweise entgegennimmt, hat – jedenfalls so lange er nicht als an der beruflichen Tätigkeit eines zeugnisverweigerungsberechtigten Berufsgeheimnisträgers mitwirkende Person gemäß § 53a StPO eingeordnet werden kann – in der Regel kein Zeugnisverweigerungsrecht hinsichtlich der ihm mitgeteilten Informationen.

Sollte eine Befreiung der Ombudsperson von der Verschwiegenheitspflicht gewünscht sein, kann dies im Namen des Unternehmens durch die vertretungsberechtigten Organe erfolgen. In der Praxis wird die Ombudsperson regelmäßig aber auch die Zustimmung des Hinweisgebers einholen.¹³⁹

Schließlich stellt sich die Frage, in welchem Umfang Strafverfolgungsbehörden Zugriff auf Unterlagen erlangen können, die Hinweise betreffen. Grundsätzlich besteht ein Schutz vor Beschlagnahme nur, sofern sich die Unterlagen im Gewahrsam des Zeugnisverweigerungsberechtigten befinden oder aber es sich um Verteidigungsunterlagen im Gewahrsam des Beschuldigten handelt.

Ob der Schutz vor Beschlagnahme für den als Ombudsperson tätigen Rechtsanwalt greift, ist bislang nicht höchstrichterlich geklärt. Insbesondere die Instanzgerichte haben die Verbotstatbestände des § 97 Abs. 1 StPO dahingehend einschränkend ausgelegt, dass lediglich die Beziehung zwischen einem Beschuldigten im Strafverfahren und dem von ihm in Anspruch genommenen Berufsgeheimnisträger geschützt sei, nicht jedoch die Be-

¹³⁷ Ebenso Brockhaus, M., CB 2023, 8 (11).

¹³⁸ Buchert, R., in Bürkle, J./Hauschka, C., (2015), § 10, Rn. 29.

¹³⁹ Hessler, M., AnwBl 2019, 212 (219); Brockhaus, M., CB 2023, 8 (12).

ziehung eines Nichtbeschuldigten zu einem Berufsgeheimnisträger.¹⁴⁰ Legt man dies zu grunde, ist in nahezu allen Konstellationen eine Beschlagnahmemöglichkeit bzw. ein Beschlagnahmerisiko gegeben.¹⁴¹

Wenngleich hiergegen gute Argumente streiten, muss im Hinblick auf diese Rechtsprechung das Risiko, dass Unterlagen auch bei der Ombudsperson beschlagahmt werden können, für die Praxis anerkannt und entsprechend gegenüber den Hinweisgebern kommuniziert werden.

Zu beachten bleibt, dass das Unternehmen zwar nicht Beschuldigter eines Strafverfahrens sein kann, ihm aber in den Fällen, in denen Sanktionen wie Einziehung und Verfall oder aber auch eine Unternehmensgeldbuße gemäß § 30 OWiG drohen, als sogenannter Nebenbeteiligter eine vergleichbare Rolle zukommt (vgl. §§ 431 ff., 442 StPO bzw. § 444 Abs. 1 Satz 1 StPO).¹⁴² In diesen Fällen sind daher Konstellationen denkbar, in denen auch hinsichtlich im Unternehmen vorhandener Unterlagen aus Whistleblowing-Sachverhalten ein Beschlagnahmeverbot besteht.

9.5 Zusammenfassung

Hinweisgebersysteme haben sich in Deutschland nachhaltig etabliert und stellen ein anerkanntes Instrument des Compliance-Management-Systems zur Aufdeckung von Wirtschaftsstraftaten und sonstigen Missständen dar. Mit dem Inkrafttreten der aus dem Hinweisgeberschutzgesetz folgenden Verpflichtungen besteht für viele Unternehmen nunmehr eine gesetzliche Pflicht zur Einrichtung eines Hinweisgebersystems. Auch kleine und mittelständische Unternehmen, die (noch) nicht in den Anwendungsbereich des Hinweisgeberschutzgesetzes fallen, erkennen den Nutzen solcher Systeme vermehrt an.

Der Erfolg eines im Unternehmen implementierten Hinweisgebersystems hängt entscheidend davon ab, dass es einerseits transparent ausgestaltet wird und zum anderen ausgewogen hinsichtlich des Schutzes sowohl des Hinweisgebers als auch des von einem Vorwurf betroffenen Mitarbeiters ist. Implementierung und Monitoring des Hinweisgebersystems müssen insofern von einem passenden Kommunikationskonzept begleitet und die Mitarbeiter des Unternehmens entsprechend geschult werden.

Bei der Auswahl des für das konkrete Unternehmen am besten geeigneten Hinweisgebersystems sind Faktoren wie Erreichbarkeit, Sprachanforderungen, Rückfragemöglichkeiten, Schutz der Unterlagen vor Beschlagnahme, Möglichkeit der Gewährung voller Anonymität und die Kosten zu berücksichtigen. In jedem Fall müssen die diesbezüglichen

¹⁴⁰ LG Bochum, Beschluss vom 16.3.2016. Siehe auch BVerfG, Beschluss vom 27.5.2018 – 2 BVR 1405/17, 2 BvR 1780/17, NJW 2018, 2385.

¹⁴¹ In der Literatur folgert Passarge aus den Regelungen des HinSchG, dass bei der durch einen Ombudsmann wahrgenommenen internen Meldestelle ein Beschlagnahmeverbot nunmehr zu bejahen sei, CB 2023, 390 (395).

¹⁴² Siehe hierzu insbesondere BVerfG, NJW 2018, 2385.

Prozesse klar strukturiert und umfassend dokumentiert sein; entsprechende Richtlinien sollten formuliert werden und eine reibungslose Integration in das Compliance-Management-System sichergestellt sein. Bei der Einführung sind einige rechtliche Fallstricke, insbesondere im Bereich des Arbeits-, Datenschutz- und Strafrechts zu berücksichtigen.

Die Erfahrung zeigt, dass in Unternehmen, in denen das klare Bekenntnis zu Compliance gelebt wird und ein Hinweisgebersystem aus Überzeugung und nicht nur aufgrund rechtlicher Verpflichtungen vorgehalten wird, dieses einen positiven Beitrag zur Ausgestaltung des Compliance-Management-Systems insgesamt leistet und dazu beiträgt, bislang unerkannte, risikobehaftete Missstände aufzudecken.

Literatur

- ALtenburg, J., Whistleblowing – Korruptionsbekämpfung durch Business Keeper Monitoring Systems?, Bucerius Law Journal 2008, 3.
- BAADE, I. / HÖSSL, T., Arbeits- und compliancerechtlicher Handlungsbedarf unter dem neuen Hinweisgeberschutzgesetz (Teil I und Teil II), DStR 2023, 1213 und 1265.
- BENNE, R., Whistleblowing – Wenn Wissen Sensibilität erfordert, CCZ 2014, 189.
- BERNDT, T. / HOPPLER, I., Whistleblowing – ein integraler Bestandteil effektiver Corporate Governance, BB 2005, 2623.
- BOCK, D., Criminal Compliance, Baden-Baden 2011.
- BROCKHAUS, M., Praktische und berufsrechtliche Grenzen bei der anwaltlichen Tätigkeit als Ombudsperson, CB 2023, 8.
- BRUNS, P., Das neue Hinweisgeberschutzgesetz, NJW 2023, 1609.
- BUCHERT, R., Der externe Ombudsman – ein Erfahrungsbericht, Hinweisegeber brauchen Vertrauen und Schutz, CCZ 2008, 148.
- BUCHERT, R. , § 10 Zusammenarbeit mit Ombudsleuten und Whistleblowersysteme in BÜRKLE, J. / HAUSCHKA, C., Der Compliance Officer, München 2015.
- BÜRGER, K. / von DAHLEN, A., Der gut- und bösgläubige Hinweisegeber/Beschwerdeführer – Anforderungen an die Befugnis zur Einleitung von Verfahren nach § 33 HinSchG-E und § 8 LkSG, DB 2023, 829.
- BÜRKLE, J., Die versicherungsrechtliche Regulierung des internen Hinweiseberystems. VersR 2020, 1.
- BÜRKLE, J., Zur Unionsrechtskonformität zentraler Konzernmeldestellen für Hinweisegeber, CCZ 2022, 335.
- COLNERIC, N. / GERDEMANN, S. (Hrsg.), BeckOK HinSchG, 1. Edition, Stand: 15.10.2023.
- CLODIUS, S. / WARDA, O., Einrichtung und Betrieb von Hinweiseberystems – ein Praxisleitfaden, CB 2021, 137.
- DEUTSCHER ANWALTVEREIN, Entwurf eines Hinweiseberschutzgesetzes, Stellungnahme 23/2023 vom 13. Mai 2022.
- DIERLAMM, K., Implementierung von Hinweiseberystems in Sportorganisationen, SpoPrax 2021, 245.
- DILLING, J., Der Schutz von Hinweisebern und betroffenen Personen nach der EU-Whistleblower-Richtlinie, CCZ 2019, 214.
- DILLING, J. in COLNERIC, N./GERDEMANN, S., BeckOK HinSchG, 3. Ed., Stand: 15.04.2024, § 15.

- DZIDA, B. / GRANETZNY, T., Die neue EU-Whistleblowing-Richtlinie und ihre Auswirkungen auf Unternehmen, NZA 2020, 1201.
- DZIDA, B. / SEIBT, C., Neues Hinweisgeberschutzgesetz: Analyse und Antworten auf Praxisfragen, NZA 2023, 657.
- EGGER, M., Hinweisgebersystem und Informantenschutz, CCZ 2018, 126.
- EGGERS, T. / PAWEL, J., Die Einrichtung eines Beschwerdeverfahrens nach § 8 LkSG im Spiegel aktueller Gesetzesvorhaben, CB 2022, 239.
- EQS GROUP / FACHHOCHSCHULE GRAUBÜNDEN, Whistleblowing Report 2021, Chur 2021.
- FAHRIG, S., Verhaltenskodex und Whistleblowing im Arbeitsrecht, NJOZ 2010, 975.
- FASSBACH, B. / HÜLSBERG, F. / SPAMER, H., Hinweisgeberschutz durch Vertrauensanwälte, CB 2022, 151.
- FEHR, S., Whistleblowing und Datenschutz – ein unlösbares Spannungsfeld?, ZD 2022, 256.
- FILA, D. / OSTERMEIER, N., Strafrechtliche Verurteilung eines Whistleblowers als Verletzung der Meinungsfreiheit, CCZ 2023, 118.
- GOERS, M., Der Ombudsmann als Instrument unternehmensinterner Kriminalprävention, Lausanne 2009.
- GÖTZ, J., Betriebsratsaufgaben im Hinweisgebermeldesystem, NZA 2023, 1433.
- GREINER, S., § 12 HinSchG in: Müller-Gloge, R., Preis, U., Gallner, I., Schmidt, I., Erfurter Kommentar zum Arbeitsrecht, 24. Auflage, 2024.
- GRONEBERG, R. (2011), Whistleblowing – Eine rechtsvergleichende Untersuchung des US-amerikanischen, englischen und deutschen Rechts unter besonderer Berücksichtigung des Entwurfs eines neuen § 612a BGB.
- HANDEL, T., Meldestellenbeauftragte – Rechte, Pflichten und Praxishinweise für Beauftragte nach dem HinweisgeberschutzG, Frankfurt am Main 2023.
- HAUSER, C. / STÜHLINGER, L., Meldestellen für Hinweisgeber: Unternehmen und Politik sind gefordert, CB 2018, 443.
- HENSSLER, M., Grundfragen anwaltlicher Verschwiegenheit, AnwBI 2019, 212.
- JOHNSON, D., Die Einführung des § 4d FinDAG: Beginn einer neuen Ära für Whistleblowing?, CB 2016, 468.
- KLASEN, E. / SCHAEFER, S., Whistleblower, Zeuge und „Beschuldigter“ – Informationsweitergabe im Spannungsfeld grundrechtlicher Positionen, BB 2012, 641.
- KOCK, M., Einführung einer Ethikrichtlinie im Unternehmen, MDR 2006, 673.
- MAUME, P. / HAFFKE, L., Whistleblowing als Teil der Unternehmenscompliance – Rechtlicher Rahmen und Best Practice, ZIP 2016, 199.
- MENGEL, A., Der Gesetzesentwurf der SPD-Fraktion zum Whistleblowing, CCZ 2012, 146.
- MOOSMAYER, K., Compliance, 4. Auflage, München 2021.
- MORENZ, A., Hinweisgebersysteme als Instrument zu Risikobekämpfung, Der Aufsichtsrat, 2010, 172.
- MÜLLER, E. / SCHLOTHAUER, R. / KNAUER, C., Münchener Anwaltshandbuch Strafverteidigung, 3. Auflage 2022.
- NIELEBOCK, H., JurisPR-ArbR23/2023, Anm. 1.
- OBERMAYER, G., § 44 Revision in: HAUSCHKA, C. / MOOSMAYER, K. / LÖSLER (2016), T., Corporate Compliance – Haftungsvermeidung im Unternehmen, 3. Auflage, München 2016.
- PASSARGE, M., Das neue HinSchG – Praxistest und offene Rechtsfragen, CB 2023, 390.
- REUFELS, M. / DEVIARD, K., Die Implementierung von Whistleblower-Hotlines aus US-amerikanischer, europäischer und deutscher Sicht, CCZ 2009, 201.
- REINHARD, A., Mitbestimmungsrechte des Betriebsrats bei der Implementierung von Unternehmens-, insbesondere Verhaltensrichtlinien, NZA 2016, 1233.

- SCHEMMEL, A. / RUHMANNSEDER, F. / WITZIGMANN, T., Hinweisgebersysteme, Implementierung im Unternehmen, Heidelberg 2012.
- SCHEMMEL, F., Neuer Anlauf Beschäftigtendatenschutzgesetz – was lange währt, wird endlich gut?, ZD-Aktuell 2023, 01164.
- SCHÜRRLE, T. / FLECK, F., „Whistleblowing Unlimited“ – Der U.S. Dodd-Frank Act und die neuen Regeln der SEC zum Whistleblowing, CCZ 2011, 218.
- SIMON, O. / SCHILLING, J.M., Kündigung wegen Whistleblowing?, BB 2011, 2421.
- SÜSSE, S., Das Gesetz zum Schutz von Geschäftsgeheimnissen und seine Bedeutung im Rahmen von Criminal Compliance in: ROTSCHEID, T., Criminal Compliance – Status quo und Status futurus, Baden-Baden 2021.
- SÜSSE, S., Whistleblowing aus Sicht des externen Compliance-Beraters in: ROTSCHEID, T. (Hrsg.), Handbuch Criminal Compliance, Baden-Baden 2015.
- SÜSSE, S. / PÜSCHEL, C., Collecting Evidence in Internal Investigations in the Light of Parallel Criminal Proceedings, CEJ 2016, 26.
- SÜSSE, S. / PÜSCHEL, C., UKBA 2010: Erste Verurteilung mit Unternehmensbezug – Potenzielle Haftungsrisiken für Unternehmen wieder stärker im Fokus, ZRFC 2015, 82.
- SYDOW, G. / MARSCH, N., DS-GVO | BDSG, 3. Auflage 2022.
- SZESNY, A. / HOPPE, P., Die Sanktionierung von Ordnungswidrigkeiten nach dem Hinweisgeberschutzgesetz, WiJ 2023, 56.
- TASCHKE, J. / PIELOW, T. / VOLK, E., Die EU-Whistleblowing-Richtlinie – Herausforderungen für die Unternehmenspraxis, NZWiSt 2021, 85.
- THÜSING, G. (Hrsg.), HinSchG, 1. Auflage 2024



Carolin Püschel, LL.B. ist seit 2021 als angestellte Rechtsanwältin in den Bereichen Wirtschafts- und Steuerstrafrecht sowie Criminal Compliance für eine der deutschlandweit führenden Rechtsanwaltskanzleien für die Bereiche Wirtschafts- und Steuerstrafrecht tätig. Schwerpunkte ihrer Tätigkeit sind die Individualstrafverteidigung und die Beratung von Einzelpersonen und Unternehmen in den Bereichen Wirtschafts- und Steuerstrafrecht sowie die präventive strafrechtliche Beratung in Compliance-Fragen, einschließlich der Begleitung interner Untersuchungen und Sonderprüfungen. Zuvor war sie als Wissenschaftliche Mitarbeiterin für eine weitere der deutschlandweit führenden Rechtsanwaltskanzleien für die Bereiche Wirtschafts- und Steuerstrafrecht sowie Criminal Compliance tätig und hat mehrere Jahre als Wissenschaftliche Mitarbeiterin in zwei international tätigen Großkanzleien in den Bereichen Kartellrecht und Compliance gearbeitet. Seit 2019 ist sie zertifizierte Compliance Officerin (Bucerius). Püschel wirkt seit 2014 redaktionell an der Erstellung der Beiträge des monatlich erscheinenden Newsdienst Compliance des Verlags C.H. Beck mit; seit 2021 ist sie Mitherausgeberin.



Dr. Sascha Süße, LL.M., M.A. ist Rechtsanwalt und Syndikus-rechtsanwalt. Als Head of Internal Investigations ist er insbesondere mit internen Untersuchungen und dem Hinweisgebersystem sowie der internen Meldestelle befasst. Er war mehrere Jahre Partner einer auf das Wirtschafts- und Steuerstrafrecht spezialisierten Kanzlei, Manager im Fachbereich Forensic & Internal Audit Services einer Wirtschaftsprüfungsgesellschaft sowie Professor für Strafrecht an einer Polizeihochschule. Er verfügt über umfassende Erfahrung in der Compliance-Beratung und strafrechtlichen Vertretung von Unternehmen sowie der Strafverteidigung von Einzelpersonen. Er war zudem für Unternehmen als Ombudsmann im Rahmen des Hinweisgebersystems tätig. Dr. Süße ist erfahrener Referent zu Whistleblowing- und Compliance-Themen und hat vielfach zu diesen Themen publiziert, u. a. als ehemaliger Mitherausgeber des Newsdienst Compliance des C.H. Beck Verlags.

Teil IV

Compliance in der Unternehmensentwicklung



Organisationspsychologische Aspekte der Compliance

10

Silja Kennecke

Inhaltsverzeichnis

10.1	Einführung.....	248
10.1.1	Der Compliance-Begriff in der Psychologie und verwandten Disziplinen.....	249
10.1.2	Non-Compliance im Organisationskontext.....	249
10.2	Gründe für Non-Compliance.....	252
10.2.1	Allgemeine Erklärungsmodelle für organisationales Fehlverhalten.....	252
10.2.1.1	Die Theorie der rationalen Entscheidung.....	252
10.2.1.2	Lerntheorien.....	253
10.2.1.3	Die Theorie des geplanten Verhaltens.....	253
10.2.1.4	Die Theorie der kognitiven Dissonanz.....	254
10.2.1.5	Das Reziprozitätsprinzip.....	254
10.2.2	Bedingungen auf Personenebene.....	255
10.2.2.1	Negative Affektivität und Attributionsstil.....	255
10.2.2.2	Integrität, Gewissenhaftigkeit, Verträglichkeit und emotionale Stabilität.....	256
10.2.2.3	Dunkle Triade: Narzissmus, Psychopathie und Machiavellismus....	256
10.2.2.4	Selbstwertgefühl und Vertrauen in eigene Fähigkeiten.....	257
10.2.2.5	Selbstkontrolle.....	257
10.2.2.6	Moralbewusstsein.....	258
10.2.2.7	Loyalität und Angst vor Exklusion.....	258
10.2.3	Persönliche Umstände.....	258
10.2.3.1	Arbeitsbedingungen.....	258
10.2.3.2	Wettbewerbsdruck, überhöhte Zielvorgaben und Orientierung an kurzfristigen Erfolgsparametern.....	259

S. Kennecke (✉)

CA Strategy Consultants, München, Deutschland

E-Mail: silja.kennecke@ca-strategy.com

10.2.3.3	Probleme im Kontrollsyste.....	259
10.2.3.4	Führung und Unternehmenskultur.....	260
10.2.4	Spezifische Erklärungsmodelle für organisationales Fehlverhalten.....	261
10.2.4.1	Modell der kausalen Schlussfolgerung.....	261
10.2.4.2	Stressor-Emotion Modell.....	261
10.2.4.3	Motivational Rahmenmodell.....	262
10.3	Bedingungen für regelkonformes Verhalten.....	263
10.3.1	Gruppendruck.....	263
10.3.2	Schutzmotivation.....	264
10.3.3	Verantwortlichkeit.....	265
10.3.4	Maßnahmen zur Förderung von Compliance.....	267
10.3.4.1	Personenbezogene Maßnahmen.....	267
10.3.4.1.1	Personalmarketing.....	267
10.3.4.1.2	Personalauswahl.....	268
10.3.4.1.3	Personalentwicklung.....	269
10.3.4.2	Umfeldbezogene Maßnahmen.....	270
10.3.4.2.1	Compliance-Management-Systeme (CMS).....	270
10.3.4.2.2	Entwicklung einer Integritätskultur.....	272
10.3.5	„Unternehmen brauchen einen Kompass, kein Navigationssystem“.....	274
Literatur.....		276

10.1 Einführung

Themen der öffentlichen Diskussion, wie die Offenlegung von Gehältern, Diversität und Gleichberechtigung, ethisches Handeln, ökologische Verantwortung und Nachhaltigkeit haben in den vergangenen Jahren die gesellschaftliche Verpflichtung von Unternehmen betont.¹ Sie fanden Eingang in Gesetze oder Richtlinien, wie etwa den deutschen Corporate Governance Kodex, und sind Inhalt zahlreicher „Sonntagsreden“ über gute und werteorientierte Unternehmensführung.

Leider sieht die Realität hinter den Kulissen oft anders aus: Mitarbeiter und Geschäftspartner verstößen immer wieder gegen gesetzliche Vorschriften oder interne Regeln und riskieren damit schwerwiegende Folgen für ihr Unternehmen. 2022 wurde laut PwC Studie² weltweit knapp jedes zweite Unternehmen Opfer wirtschaftskrimineller Handlungen.

Im Folgenden wird beschrieben, wie und weshalb Mitarbeiter gegen Unternehmensregeln verstößen oder ethische Standards ignorieren, welche Bedingungen Compliance fördern und welche Handlungsmöglichkeiten Unternehmen besitzen, um unternehmensschädigendes Verhalten zu verhindern.

¹Vgl. Hecker (2012), S. 11.

²Vgl. Nestler & Engelmann (2022), S. 3.

10.1.1 Der Compliance-Begriff in der Psychologie und verwandten Disziplinen

Compliance bedeutet im weitesten Sinne das **Befolgen von Vorgaben** und kann als universelles Phänomen bezeichnet werden, das in jedem sozialen Kontext auftritt, in dem Personen miteinander interagieren.³ Der Versuch, Akteure zu vorschrifts- oder wunschgemäßem Handeln zu bewegen, spielt dabei eine zentrale Rolle.

In der **Sozialpsychologie** beschreibt Compliance eine Verhaltensänderung unter sozialem Einfluss, zum Beispiel indem einer direkten Bitte oder Aufforderung entsprochen wird.⁴

Im **Gesundheitswesen** versteht man unter Compliance die Bereitschaft und Fähigkeit eines Patienten, aktiv an der Behandlung seiner Krankheit mitzuwirken, zum Beispiel indem Medikamente vorschriftsmäßig eingenommen und Arzttermine eingehalten werden.⁵

Im **Wirtschaftskontext** bezeichnet Compliance das Handeln in Übereinstimmung mit Gesetzen, Richtlinien und freiwilligen Verhaltensregeln einer Organisation.⁶ Im Sinne dieser Definition wird der Compliance-Begriff nachfolgend verwendet.

10.1.2 Non-Compliance im Organisationskontext

Non-Compliance, als Nicht-Beachtung von Handlungsvorgaben, umfasst verschiedene Konzepte, wie kontraproduktives, deviantes (abweichendes), unethisches und aggressives Arbeitsverhalten oder organisationales Fehlverhalten.

Kontraproduktives Verhalten geschieht per Definition absichtlich, verletzt organisationale Normen und bedroht das Wohl des Unternehmens oder das seiner Mitglieder.⁷ Unbeabsichtigte Fehler oder Schäden, die aufgrund mangelnder Kompetenz oder unglücklicher Umstände entstehen, fallen nicht unter diesen Begriff.⁸ Ein Gabelstaplerfahrer, der bei der Arbeit versehentlich ein Regal rammt, handelt demnach nicht kontraproduktiv.⁹

Welche Verhaltensweisen konkret als „**abweichend**“ bezeichnet werden, hängt von der zugrunde gelegten Norm ab.¹⁰ In diesem Zusammenhang muss zwischen kontraproduktivem und **unethischem Verhalten** unterschieden werden:¹¹ Kontraproduktives Verhalten verletzt unternehmensinterne Regelungen und Vorschriften, unethisches Ver-

³Vgl. Etzioni (1961), S. 4.

⁴Vgl. Aronson, Wilson, & Akert (2004), S. 301.

⁵Vgl. Petermann (1998), S. 9.

⁶Vgl. Czotscher (2009), S. 26.

⁷Vgl. Robinson & Bennett (1995), S. 556.

⁸Vgl. Marcus & Schuler (2004), S. 648.

⁹Vgl. Nerdinger (2008), S. 1.

¹⁰Vgl. Spector & Fox (2005), S. 154.

¹¹Vgl. Robinson & Bennett (1995), S. 556.

halten bezieht sich auf einen Verstoß gegen moralische, gesetzliche oder andere gesellschaftliche Prinzipien. So kann ein bestimmtes Verhalten, wie die Entsorgung von Giftmüll in einem Fluss, unethisch sein, entspricht aber unter Umständen den Regeln des Unternehmens und wird daher nicht als kontraproduktiv bezeichnet. Umgekehrt ist die Meldung solcher Vorgänge an die zuständige Umweltbehörde zwar ethisch korrekt, wird aber dem Unternehmen schaden.

Vardi und Wiener¹² fassen unter den Begriff „**Fehlverhalten in Organisationen**“ sowohl unethisches als auch abweichendes Verhalten, das gesellschaftliche und/oder organisationale Werte verletzt. Abbildung 10.1. zeigt die Definitionen für Compliance- und Non-Compliance im Überblick.

Non-Compliance lässt sich danach kategorisieren, ob es sich um schwerwiegende oder eher geringfügige Regelverstöße handelt und ob das Verhalten primär die Organisation, andere Organisationsmitglieder oder die handelnde Person selbst schädigt (siehe Abbildung 10.2), nächste Seite.¹³ Gängige Formen abweichenden Verhaltens sind beispielsweise Diebstahl, die Annahme von Schmiergeldern, Informationsmissbrauch, Absentismus, der Verstoß gegen Sicherheitsregeln, absichtlich geringe Arbeitsqualität und unangemessenes verbales oder physisches Verhalten.¹⁴

Fehlverhalten kann mit unterschiedlichen Absichten erfolgen. Vardi und Wiener¹⁵ unterscheiden drei Motive, die abweichendem oder unethischem Verhalten zugrunde lie-

Compliance bedeutet Handeln in Übereinstimmung mit...

- a) gesetzlichen Bestimmungen
- b) unternehmensinternen Verhaltensregeln
- c) ethisch-moralischen Prinzipien

Formen von Non-Compliance sind...

- Fehlverhalten in Organisationen (Verstoß gegen a, b, und c)
- kontraproduktives / abweichendes Verhalten (vor allem Verstoß gegen b)
- unethisches Verhalten (vor allem Verstoß gegen c)

Mögliche Leidtragende:

- Einzelpersonen innerhalb der Organisation (Kollegen, Mitarbeiter oder Vorgesetzte)
- Die Organisation
- Stakeholder außerhalb der Organisation (Partner oder Kunden)
- Die Umwelt / Gesellschaft

Abb. 10.1 Begriffsbestimmung: Compliance und Non-Compliance

¹²Vgl. Vardi & Wiener (1996), S. 151.

¹³Vgl. Robinson & Bennett (1995), S. 565.

¹⁴Vgl. Nerdinger, Blickle, & Schaper (2011) S. 417.

¹⁵Vgl. Vardi & Wiener (1996), S. 151.

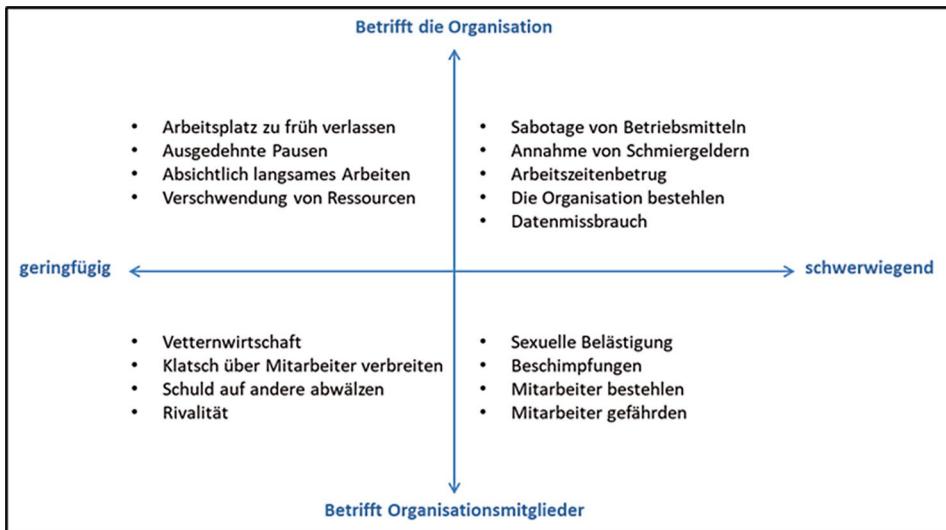


Abb. 10.2 Eine Typologie kontraproduktiven Arbeitsverhaltens. (Nach Robinson & Bennett, 1995; © Adademy of Management (NY) 1995)

gen können: Die Absicht, einen **Nutzen für sich selbst** zu erzielen (Typ S), die Absicht, einen **Nutzen für die Organisation** zu erzielen (Typ O) und die Absicht, der **Organisation oder einzelnen Stakeholdern Schaden zuzufügen** (Typ D). Handlungen von Typ S richten sich zumeist gegen die eigene Organisation, zum Beispiel wenn eine Person stiehlt, um sich persönlich zu bereichern. Typ O Verhalten hingegen kann aus Loyalität und hoher Identifikation mit der Organisation entstehen. Ein Beispiel ist die Manipulation von Daten, um Aufträge für das Unternehmen zu generieren oder Unternehmensziele zu erreichen. Bei Verhalten von Typ D handelt es sich oftmals um Racheakte, wie zum Beispiel die Zerstörung von Unternehmenseigentum oder aggressives Verhalten gegenüber Organisationsmitgliedern.

Nerdinger¹⁶ weist daraufhin, dass kontraproduktives Verhalten mitunter zunächst produktiv wirkt, zum Beispiel wenn durch Vetternwirtschaft oder die Zahlung von Schmiergeldern bürokratische Prozesse beschleunigt oder vereinfacht werden. Auf lange Sicht schafft die Nicht-Beachtung geltender Gesetze oder Regelungen jedoch unklare Prioritäten, fördert das Ausnutzen von Grauzonen und untergräbt ethische Grundsätze der Organisation.¹⁷ Neben direkten Kosten, wie etwa Bußgeld- oder Schadensersatzzahlungen, kann Non-Compliance erhebliche Reputationsschäden und Vertrauensverluste zur Folge haben, die sich negativ auf die Geschäftsbeziehungen einer Organisation auswirken.¹⁸

¹⁶Vgl. Nerdinger (2008), S. 2.

¹⁷Vgl. Wesche, May, Peus, & Frey (2010), S. 320.

¹⁸Vgl. Nerdinger (2008), S. 6.

Einer Umfrage des Managermagazins zufolge, in der rund 2500 Führungskräfte zur Reputation der größten Unternehmen in Deutschland befragt wurden, erlebte beispielsweise Siemens nach dem Schmiergeld-Skandal 2006 einen Reputationsabstieg um 56 Rangplätze.¹⁹ Ähnlich erging es VW nach dem Dieselskandal.²⁰

10.2 Gründe für Non-Compliance

Angesichts von Krisen und Korruptionsaffären neigen Unternehmen dazu, Einzelpersonen für Fehlentwicklungen verantwortlich zu machen²¹ und ziehen personelle Konsequenzen, um intern wie extern ein Umdenken zu signalisieren.

Non-Compliance lässt sich jedoch weder allein durch negative Eigenschaften der handelnden Person noch vollständig durch ungünstige Systemeigenschaften erklären. Fehlverhalten entsteht vielmehr aus einem komplexen **Zusammenwirken von Person- und Situationsfaktoren**.²²

In den meisten Erklärungsmodellen werden daher gleichermaßen Personen- und Organisationsmerkmale berücksichtigt, die Lernerfahrungen, Erwartungen und die Wahrnehmung situativer Gegebenheiten durch die Organisationsmitglieder formen.

Im Folgenden soll zunächst ein Überblick über allgemeine psychologische Theorien zur Erklärung und Vorhersage von (Fehl-)Verhalten gegeben werden, bevor im Anschluss auf konkrete Bedingungen für Non-Compliance und spezifische Erklärungsmodelle eingegangen wird.

10.2.1 Allgemeine Erklärungsmodelle für organisationales Fehlverhalten

10.2.1.1 Die Theorie der rationalen Entscheidung

Erwünschte Handlungskonsequenzen oder Ziele, für die Menschen Energie aufwenden, sind typischerweise das Erlangen von Vorteilen oder die Vermeidung von Nachteilen. In der Logik von Rational Choice Modellen macht Fehlverhalten somit dann Sinn, wenn der erzielte Nutzen möglichst hoch und der erwartete Schaden, zum Beispiel durch Aufdeckung des Verhaltens, gering ist. Auf dieser Logik basiert unter anderem die Theorie der Schutzmotivation, die erklärt, unter welchen Umständen Personen sich gegen korruptes Verhalten entscheiden.

¹⁹Vgl. Managermagazin (2008), S. 3.

²⁰Vgl. GPRA-Vertrauensindex (2015).

²¹Vgl. Paine (1994), S. 106.

²²Vgl. Lewin (1951), S. 170.

10.2.1.2 Lerntheorien

Erwartungen über Vor- und Nachteile bestimmter Verhaltensweisen werden durch Lernerfahrungen gebildet. Verschiedenen Lerntheorien²³ zufolge tritt Fehlverhalten vor allem auf, wenn

- die Belohnung für das Verhalten als hoch erachtet wird (Belohnungslernen)
- die Bestrafung für das Verhalten als gering erachtet wird (Bestrafungslernen)
- Modelle vorhanden sind, die das Verhalten vorleben (Beobachtungslernen).

Erleben Personen wiederholt, dass risikoreiches Verhalten, wie der Verzicht auf unbequeme Schutzkleidung, nicht zu negativen Konsequenzen führt, kann sich eine Monopolhypothese entwickeln: „Alles ist gut und wird gut bleiben“ (**erlernte Sorglosigkeit**).²⁴ So steigt die Wahrscheinlichkeit, das entsprechende Verhalten erneut zu zeigen nach dem Motto „ich bin die letzten Male nicht erwischt worden, dann wird es diesmal auch klappen“. Hat der Akteur dabei Zuschauer, die die gleichen Schlüsse ziehen, kann sich Fehlverhalten nahezu epidemieartig verbreiten und wird über kurz oder lang zur Verhaltensnorm innerhalb der Organisation.

10.2.1.3 Die Theorie des geplanten Verhaltens

Verhalten, das der willentlichen Kontrolle einer Person unterliegt, wird maßgeblich durch drei Faktoren gesteuert:²⁵

- Die **Einstellung** gegenüber dem Verhalten, die sich aus positiven oder negativen Erwartungen und Bewertungen von Handlungskonsequenzen ergibt
- Die Wahrnehmung geltender **Verhaltensnormen**, das heißt Annahmen darüber, wie relevante Personen aus dem sozialen Umfeld das Verhalten bewerten und die Motivation, diesen Erwartungen zu entsprechen
- Die wahrgenommene **Verhaltenskontrolle**, das heißt die Leichtigkeit, mit der das Verhalten aus Sicht des Akteurs ausgeführt werden kann.

Alle drei Faktoren bestimmen die Verhaltensabsicht (Intention), das heißt die Bereitschaft, eine bestimmte Handlung auszuführen, die dem Verhalten unmittelbar vorausgeht. Daraus lässt sich ableiten, dass Fehlverhalten mit höherer Wahrscheinlichkeit gezeigt wird, wenn es positive Konsequenzen verspricht, (vermeintlich) durch das Umfeld akzeptiert wird und die Umsetzung leichtfällt.

²³Vgl. Zimbardo & Gerrig (1999), S. 218.

²⁴Vgl. Schulz-Hardt & Frey (2000), S. 191.

²⁵Vgl. Ajzen (1991), S. 182.

10.2.1.4 Die Theorie der kognitiven Dissonanz

Eine weitere aufrechterhaltende Bedingung für Fehlverhalten ist das menschliche Bedürfnis, begangene Handlungen zum Schutz eines positiven Selbstbildes vor sich selbst und anderen zu rechtfertigen.²⁶ Die Theorie der kognitiven Dissonanz besagt, dass Menschen ein Gefühl des Unbehagens (Dissonanz) verspüren, wenn sie in einer Weise handeln, die ihrem positiven Selbstbild zuwiderläuft. Um diese Dissonanz zu reduzieren, bestehen drei Möglichkeiten:

- Das Verhalten wird verändert (ich decke korrupte Handlungen in meiner Abteilung nicht länger)
- Die Einstellung gegenüber dem Verhalten wird verändert (korrupte Handlungen sind in Ordnung, wenn sie dem Unternehmen nützen)
- Es werden positive Gründe für das Verhalten gesucht (korrupte Handlungen beschleunigen bürokratische Prozesse und unterstützen die Zielerreichung).

10.2.1.5 Das Reziprozitätsprinzip

Wie in jedem sozialen Kontext streben Menschen auch im Arbeitsleben nach einem angemessenen Verhältnis von Kosten (Leistung, Anstrengung) und Nutzen (Gegenleistung, Belohnung).²⁷ Ist dieses Reziprozitätsprinzip verletzt, wird entsprechend entweder die Kosten- oder die Nutzenseite angepasst, um eine subjektive Balance wiederherzustellen. Erleben Mitarbeiter ein Ungleichgewicht, etwa dass sie für ihre Arbeitsleistung nicht ausreichend entlohnt oder gewürdigt werden, reduzieren sie möglicherweise ihre Leistung oder zeigen andere Formen abweichenden Verhaltens, die ihr individuelles „Nutzenkonto“ ausgleichen. Solchermaßen begründetes Fehlverhalten wird auch als vergeltendes Verhalten bezeichnet.²⁸ Wie sensibel Menschen auf Verstöße gegen die Reziprozitätsregel reagieren, ist individuell unterschiedlich.²⁹

Die Reziprozitätsregel kommt auch im Fall von enttäuschten Erwartungen zum Tragen. Erfüllt eine Organisation die (impliziten) Erwartungen von Mitarbeitern an die Arbeitsbeziehung nicht, spricht man von einem **psychologischen Vertragsbruch**.³⁰ Mitarbeiter erhalten nicht das, was ihnen ihrer Meinung nach zusteht und fühlen sich im Gegenzug nicht verpflichtet, sich an organisationale Regeln zu halten. Zu den Konsequenzen eines solchen Vertragsbruches gehören Enttäuschung, Ärger und Vertrauensentzug sowie verringerte Einsatzbereitschaft und eine negative Einstellung zum Unternehmen bis hin zur „inneren Kündigung“.³¹ All diese Faktoren erhöhen die Wahrscheinlichkeit für Fehlverhalten.

²⁶Vgl. Aronson, Wilson, & Akert (2004), S. 188.

²⁷Vgl. Blau (1964), S. 88–91.

²⁸Vgl. Skarlicki & Folger (1997), S. 434.

²⁹Vgl. Cropanzano & Mitchell (2005), S. 877.

³⁰Vgl. Morrison & Robinson (1997), S. 226.

³¹Vgl. Zhao, Wayne, Glibkowski, & Bravo (2007), S. 651.

Unter welchen Bedingungen schädigen Mitarbeiter ihr Unternehmen?

Bedingungen auf Personenebene

- Negative Affektivität
- Attributionsstil (externale Attribution negativer Ereignisse)
- Geringe Ausprägung von Integrität, Gewissenhaftigkeit, Verträglichkeit und emotionaler Stabilität
- Narzissmus und Machiavellismus
- Geringe Selbstkontrolle
- Unterentwickeltes Moralbewusstsein
- Falsch verstandene Loyalität und Angst vor Exklusion
- Persönliche Umstände

Bedingungen auf Organisationsebene

- Wettbewerbsdruck
- Überhöhte Zielvorgaben
- Einseitige Orientierung an kurzfristigen Erfolgsparametern
- Ungünstige Arbeitsbedingungen
- Probleme im Kontrollsysten der Organisation
- Laisser-faire oder autoritärer Führungsstil
- Ethikdefizite in der Unternehmenskultur

Abb. 10.3 Bedingungen für Non-Compliance

Ergänzend zu den angeführten Theorien, werden in den folgenden Abschnitten spezielle Forschungsbefunde zu regelverletzendem Verhalten erläutert. Dabei wird zwischen Bedingungen auf Personen- und Organisationsebene unterschieden, die Non-Compliance begünstigen (siehe Abb. 10.3 für eine Aufzählung).

10.2.2 Bedingungen auf Personenebene

Forschungsergebnisse und Alltagsbeobachtungen zeigen, dass Personen sich in ihrem Erleben und Verhalten selbst dann unterscheiden, wenn sie sich objektiv betrachtet in der gleichen Situation befinden. Hier kommen Persönlichkeitseigenschaften, Werte und Überzeugungen einer Person zum Tragen, die beeinflussen, wie Reize aus der Umgebung interpretiert und welche Verhaltenskonsequenzen daraus abgeleitet werden.³²

10.2.2.1 Negative Affektivität und Attributionsstil

Ein häufig genannter Einflussfaktor ist negative Affektivität, das heißt die Neigung, negative Affekte, wie Nervosität, Angst, Ärger oder Sorge zu erleben und auszudrücken. Perso-

³²Vgl. Amelang & Bartussek (2001), S. 45.

nen mit hoch ausgeprägter negativer Affektivität schenken negativen Aspekten von Situationen mehr Beachtung und nehmen Ungerechtigkeiten daher stärker wahr.³³ Gleichzeitig neigen sie dazu, ihr Umfeld für negative Ereignisse und Niederlagen verantwortlich zu machen (externale Attribution). Wie Douglas und Martinko³⁴ zeigen konnten, hängt dieser Attributionsstil mit aggressivem Verhalten am Arbeitsplatz zusammen.

10.2.2.2 Integrität, Gewissenhaftigkeit, Verträglichkeit und emotionale Stabilität

Des Weiteren hängt abweichendes Verhalten negativ mit Eigenschaften wie Integrität, Gewissenhaftigkeit, Verträglichkeit und emotionaler Stabilität zusammen. In den Vereinigten Staaten werden diese Persönlichkeitsfaktoren daher häufig in Einstellungssituationen mittels Integritätstests erfasst.³⁵

Für den Begriff Integrität existieren unterschiedliche Definitionen, die Schlagworte wie „Unbescholtenheit“, „Unbestechlichkeit“, „Rechtschaffenheit“ oder „Vertrauenswürdigkeit“ umfassen. Typischerweise kann man von einer integren Person erwarten, dass sie über einen wohldefinierten Satz von moralischen Werten und Prinzipien verfügt, diese konsequent in ihr Handeln überträgt und sich auch unter Druck von außen nicht davon abbringen lässt.³⁶ Gewissenhafte Personen sind im Allgemeinen ordentlich, systematisch, zuverlässig, diszipliniert und arbeiten hart. Eine hohe Verträglichkeit misst man bei Personen, die als kooperativ, hilfsbereit, mitfühlend, gutmütig und freundlich gelten. Emotionale Stabilität bildet den Gegenpol zu Neurotizismus und bedeutet, dass eine Person dazu neigt, emotional ausgeglichen, entspannt, gelassen und zufrieden zu sein.³⁷

10.2.2.3 Dunkle Triade: Narzissmus, Psychopathie und Machiavellismus

Unter dem Begriff der „Dunklen Triade“ werden Persönlichkeitseigenschaften zusammengefasst, die gesellschaftlich im Allgemeinen negativ bewertet werden und eng mit organisationalem Fehlverhalten zusammenhängen;³⁸ sie werden in den hier beschriebenen Ausprägungen allerdings nicht als „krankhaft“ angesehen. Narzistische Personen zeichnen sich durch ein starkes Bedürfnis nach Macht und Anerkennung sowie ein instabiles Selbstwertgefühl aus, das zwischen Grandiosität und Minderwertigkeit schwankt. Sie neigen zu abweichendem Verhalten, wenn sie ihr überhöht positives Selbstbild bedroht sehen.³⁹ Psychopathie ist gekennzeichnet durch ein geringes Maß an Empathie und Ängstlichkeit.⁴⁰ Unter Machiavellismus versteht man die Neigung, amoralisch und opportunistisch zu han-

³³Vgl. Martinko, Gundlach, & Douglas (2002), S. 46.

³⁴Vgl. Douglas & Martinko (2001), S. 553.

³⁵Vgl. Marcus, Lee, & Aston (2007), S. 650.

³⁶Vgl. Becker, (1998), S. 157.

³⁷Amelang & Bartussek (2001), S. 366 und S. 371.

³⁸O’Boyle, Forsyth, Banks & McDaniel (2012), S. 557.

³⁹Vgl. Penney & Spector (2002), S. 131.

⁴⁰Vgl. Paulhus & Williams (2002), S. 557.

deln. Vor allem in Führungspositionen mit einem hohen Verantwortungsgrad und Handlungsspielraum können Narzissmus, Psychopathie und Machiavellismus verheerend wirken. Alle drei Eigenschaften wurden wiederholt mit kontraproduktivem und unethischem Verhalten in Verbindung gebracht.⁴¹ Personen mit einem solchen Persönlichkeitsprofil besitzen wenig moralische Skrupel und neigen dazu „über Leichen zu gehen“, um sich oder ihrer Abteilung Vorteile zu verschaffen.⁴² Potenzielle Konkurrenten werden manipuliert und durch unlautere Methoden ausgeschaltet. Gängige Methoden in diesem Zusammenhang sind Intrigen oder Schlechtreden bis hin zum Rufmord. Die eigenen Interessen werden dabei grundsätzlich über die der Allgemeinheit gestellt. Führungskräfte mit narzistischen und machiavellistischen Neigungen sind als Negativmultiplikatoren in Organisationen besonders gefährlich, da sie in der Lage sind, andere durch ihr Charisma und rhetorisches Geschick zu manipulieren und mitzureißen.⁴³ In diesem Zusammenhang wird klar, weshalb gelegentlich diskutiert wird, ob dieses Verhalten unter Umständen zum erwünschten Verhaltensspektrum von Führungskräften gehört.⁴⁴

10.2.2.4 Selbstwertgefühl und Vertrauen in eigene Fähigkeiten

Auch die Beurteilung der eigenen Person in Bezug auf Fähigkeiten, Wertigkeit und Kontrollmöglichkeiten beeinflusst die Neigung, kontraproduktives Verhalten am Arbeitsplatz zu zeigen. Personen mit gesundem Selbstwertgefühl und Vertrauen in eigene Fähigkeiten fühlen sich seltener hilflos einer Situation ausgeliefert und sind daher auch in Stresssituationen in der Lage, positive Handlungsoptionen zu identifizieren oder sich aktiv Unterstützung aus ihrem Umfeld zu suchen.⁴⁵

Ein übermäßiges Vertrauen in die eigenen Fähigkeiten kann, wie bereits beschrieben, jedoch zu einer Illusion von Kontrolle führen, die Fehlverhalten aufrechterhält, da der Akteur der Meinung ist, das Verhalten grundsätzlich straflos ausführen zu können.

10.2.2.5 Selbstkontrolle

Ansätze aus der Kriminologie betonen die Bedeutung von Selbstkontrolle für normverletzendes Verhalten.⁴⁶ Personen mit niedrig ausgeprägter Selbstkontrolle neigen dazu, ihr Handeln an kurzfristigen Vorteilen auszurichten und dabei langfristige Konsequenzen zu vernachlässigen. Marcus und Schuler⁴⁷ konnten zeigen, dass Selbstkontrolle enger mit deviantem Arbeitsverhalten zusammenhängt als eine Vielzahl anderer Variablen, wie Frustration, Stress, Unzufriedenheit oder Sanktionen und Überwachungsmaßnahmen durch das Unternehmen.

⁴¹Vgl. Peneey & Spector (2002), S. 129.

⁴²Vgl. Giacalone & Knouse (1990), S. 56/57.

⁴³Vgl. Padilla, Hogan, & Kaiser (2007), S. 180.

⁴⁴Vgl. Judge, Piccolo & Kosalka, (2009), S. 870.

⁴⁵Vgl. Judge, Erez, & Bono (1998), S. 170.

⁴⁶Vgl. Hirschi & Gottfredson (1993), S. 47.

⁴⁷Vgl. Marcus & Schuler (2004), S. 656.

10.2.2.6 Moralbewusstsein

Ein wichtiger Faktor ist außerdem das Moralbewusstsein einer Person,⁴⁸ also die Orientierung an internalisierten Verhaltensnormen. Kohlberg teilt die Entwicklung moralischen Verhaltens in verschiedene Stufen auf, in denen unterschiedliche Normen handlungsleitend sind, wie die Orientierung an Strafe und Gehorsam (Stufen 1–2), die Orientierung an den Erwartungen des sozialen Umfelds (Stufen 3–4) oder die Orientierung an abstrakten ethischen Prinzipien, wie der Idee eines Gesellschaftsvertrags oder dem kategorischen Imperativ (Stufen 5–6).⁴⁹ Diese Überlegungen können unter anderem bei der Entwicklung praktischer Maßnahmen zu Förderung von Compliance hilfreich sein, da Mitarbeiter auf unterschiedliche Maßnahmen positiv reagieren.

10.2.2.7 Loyalität und Angst vor Exklusion

Risikofaktoren für Fehlverhalten als „Befolgen falscher Normen“ sind falsch verstandene Loyalität gegenüber Autoritäten (zum Beispiel der Führungskraft) und die Angst vor Exklusion aus einer sozialen Gruppe (zum Beispiel dem Arbeitsteam) als Folge von Kritik an unethischen Entscheidungen oder der Weigerung, sich an korrupten Vorgängen zu beteiligen.⁵⁰

10.2.3 Persönliche Umstände

Nicht zuletzt können auch persönliche Umstände eines Mitarbeiters deviantes Verhalten begünstigen, indem sie die Bewertung von Verhaltenskonsequenzen verändern.⁵¹ So kann zum Beispiel Diebstahl in einer finanziellen Notsituation als vorteilhafte Handlungsoption betrachtet werden. Bedingungen auf Organisationsebene Personenfaktoren spielen zwar für die Vorhersage von Verhalten auf individueller Ebene eine wichtige Rolle, können jedoch nicht erklären, weshalb Fehlentwicklungen innerhalb einer Organisation oft gehäuft auftreten. Unethische Vorgänge sind meist keine Einzeltaten im luftleeren Raum, sondern erfordern die Kooperation oder zumindest das Stillschweigen anderer Organisationsmitglieder und spiegeln damit Organisationsmerkmale, wie geteilte Werte, Einstellungen und kollektive Verhaltensmuster wider.⁵²

10.2.3.1 Arbeitsbedingungen

Zu den Organisationsfaktoren, die Fehlverhalten fördern, zählen an erster Stelle Arbeitsbedingungen, die den Bedürfnissen von Mitarbeitern nicht gerecht werden, wie ungerechte Entlohnung, ungesicherte Beschäftigungsverhältnisse, geringe Wertschätzung, wenig Unterstützung oder gar Mobbing durch Führungskräfte oder Teammitglieder sowie man-

⁴⁸Vgl. Trevino (1986), S. 604.

⁴⁹Vgl. Kohlberg, (1984), S. 172.

⁵⁰Vgl. Aronson, Wilson, & Akert (2004), S. 309.

⁵¹Vgl. Vardi & Wiener (1996), S. 159.

⁵²Vgl. Paine (1994), S. 106.

gelnde Bereitstellung von Ressourcen, die zur Ausführung von Arbeitsaufgaben notwendig sind.⁵³ Das Vorhandensein solcher Faktoren trägt in hohem Maße dazu bei, dass Mitarbeiter sich unzufrieden, gestresst, ungerecht behandelt oder ausgenutzt fühlen und die Schuld dafür dem Unternehmen zuschreiben (vgl. Abschn. 10.2.3.1). Je stärker die Wahrnehmung von Ungerechtigkeit und Unfairness ist, desto wahrscheinlicher ist es, dass Mitarbeiter versuchen, sich durch regelverletzendes Verhalten zu revanchieren (vgl. Abschn. 10.2.1.5). Umgekehrt kann die Wahrnehmung von Gerechtigkeit und Wertschätzung Fehlverhalten auch unter ungünstigen Umständen verhindern, zum Beispiel bei geringer Entlohnung. Hier spielt vor allem das Verhalten des direkten Vorgesetzten eine wichtige Rolle.⁵⁴

10.2.3.2 Wettbewerbsdruck, überhöhte Zielvorgaben und Orientierung an kurzfristigen Erfolgsparametern

Häufig resultieren ungünstige Arbeitsbedingungen aus einem hohen Wettbewerbsdruck, dem viele Organisationen heutzutage ausgesetzt sind. Die Angst, von Konkurrenten aus dem Markt gedrängt zu werden, kann zu überhöhten Zielvorgaben und einer einseitigen Orientierung an kurzfristigen Erfolgsparametern führen.⁵⁵ Dies betrifft vor allem Führungskräfte der mittleren Ebene, die permanent zwischen strategischen Vorgaben und operativer Umsetzung vermitteln müssen.

In einem Laborexperiment konnten Schweitzer, Ordóñez und Douma zeigen, dass hoch gesteckte Ziele, vor allem wenn sie nur knapp verfehlt werden, unethisches Verhalten nach sich ziehen⁵⁶ (hier: fälschliche Angaben über den Grad der Zielerreichung, um eine höhere Belohnung zu erzielen). Überhöhte Zielvorgaben steigern somit die Wahrscheinlichkeit, dass versucht wird, Ziele durch Fehlverhalten zu erreichen.

Ein hoher Kosten- und Erfolgsdruck wird meist über alle Ebenen an die Mitarbeiter weitergegeben und manifestiert sich unter anderem in steigenden Krankheitsraten,⁵⁷ hoher Fluktuation, nachlassender Innovationskraft und verringelter Produktivität.⁵⁸ Unter diesen Umständen werden nachhaltige Ziele, wie Kunden- oder Mitarbeiterbindung, oft vernachlässigt. Verschiedene Fallbeispiele aus der Praxis, wie zum Beispiel der Enron-Skandal 2001, zeigen, dass unlautere Aktivitäten nicht selten durch die Führungsspitze initiiert oder zumindest toleriert werden.

10.2.3.3 Probleme im Kontrollsyste

Ein weiterer situationaler Faktor sind Probleme im Kontrollsyste eines Unternehmens, wobei sowohl zu wenig als auch zu viel Kontrolle problematisch sein kann. So können etwa fehlende Kontrollinstanzen das Entstehen **informeller Netzwerke** begünstigen, in

⁵³Vgl. Greenberg (1990), S. 561.

⁵⁴Vgl. Skarlicki & Folger (1997), S. 438.

⁵⁵Vgl. Bruch & Menges (2010), S. 2.

⁵⁶Vgl. Schweitzer, Ordóñez, & Douma (2004), S. 429.

⁵⁷Vgl. Moliner, Martínez-Tur, Peiró, Ramos, & Cropanzano (2005), S. 100.

⁵⁸Vgl. Greve (2010), S. 107–110.

denen man sich gegenseitig zuarbeitet und schützt.⁵⁹ Dabei kann sich innerhalb des Systems ein Gefühl von Unverletzbarkeit oder sogar Rechtmäßigkeit der durchgeführten Aktivitäten einstellen, die die Entscheidungen der Gruppe beeinflussen.⁶⁰ Aufgrund der strukturellen Eigenschaften korrupter Netzwerke (geschlossen und mit starken Bindungen⁶¹) ist es schwierig, solche Systeme zu entlarven. Unklarheiten über Handlungs-erwartungen und -bewertungen durch Entscheidungsträger des Unternehmens begünstigen organisationales Fehlverhalten zusätzlich.

Andererseits kann strikte Kontrolle und Überwachung ebenfalls kontraproduktives Verhalten zur Folge haben. Starke Überwachung signalisiert mangelndes Vertrauen in die Fähigkeit oder Bereitschaft der Mitarbeiter, sich korrekt zu verhalten und kann im Sinne einer selbsterfüllenden Prophezeiung wirken.⁶² So kann zum Beispiel aus einem Gefühl der Entmündigung heraus die Verantwortung für das eigene Handeln abgegeben werden.

Zu viele kaum nachvollziehbare Regeln, die effizientes Arbeiten behindern, führen außerdem zu aktiven Widerstandsreaktionen und Motivationsverlust auf Seiten der Mitarbeiter und resultieren allenfalls in dem Versuch, scheinbar sinnlose Regeln zu umgehen.⁶³ Das Ausnutzen von Grauzonen durch die Suche nach legalen Schlupflöchern im Regelsystem wird von McBarnet als „creative compliance“ bezeichnet und ist auch auf Organisationsebene eine gängige Praxis.⁶⁴

10.2.3.4 Führung und Unternehmenskultur

Führungsverhalten beeinflusst die Neigung zu abweichendem Verhalten innerhalb des Teams. So kann ein Laissez-faire-Stil mit vielen Freiheiten für die Mitarbeiter und wenig Intervention durch die Führungskraft ebenso deviantes Verhalten begünstigen, wie ein autoritärer Führungsstil, der auf Befehl und Gehorsam basiert.⁶⁵ Günstig ist ein **Führungsstil**, der Mitarbeiter durch die Vermittlung von Sinn und Vision motiviert, sich für die Interessen der Organisation einzusetzen (transformationale Führung).⁶⁶ Um Typ O Verhalten vorzubeugen, sollte hierbei jedoch auch adressiert werden, welche Rahmenbedingungen bei der Zielerreichung wichtig sind. Auch ein **partizipativer Führungsstil** kann sich positiv auswirken, da die Möglichkeit, sich an Führungsentscheidungen zu beteiligen, das Kontrollerleben auf Seiten der Mitarbeiter erhöht.⁶⁷

⁵⁹Vgl. Stessl (2012), S. 68–69.

⁶⁰Vgl. Turner & Pratkanis (1998), S. 106.

⁶¹Vgl Granovetter (1973), S. 1361.

⁶²Vgl. Aronson, Wilson, & Akert (2004), S. 507.

⁶³Vgl. Spitzmüller & Stanton (2006), S. 246.

⁶⁴Vgl. McBarnet (2006), S. 1091.

⁶⁵Vgl. Tyler (2006), S. 216.

⁶⁶Vgl. Tyler, (2006), S. 223–224.

⁶⁷Vgl. Nerdinger, Blickle, & Schaper (2011), S. 420.

Wie Tyler ausführt, lässt sich deviantes Verhalten durch die Internalisierung bestimmter **Werte** beeinflussen, sodass Unternehmensregeln freiwillig und selbstreguliert befolgt werden.⁶⁸ Der Autor konnte zeigen, dass die Wahrscheinlichkeit, bei einer unmoralischen Handlung ertappt zu werden, einen deutlich geringeren Einfluss auf das Verhalten von Mitarbeitern ausübt als die Wahrnehmung, dass die Handlung den eigenen Werten widerspricht.⁶⁹ Ein effektiver Ansatz, um kontraproduktives Verhalten zu vermeiden ist somit eine Unternehmenskultur, in der das Handeln nach ethischen Grundsätzen gelebt und gefördert wird und mit der sich die Mitarbeiter identifizieren können.

10.2.4 Spezifische Erklärungsmodelle für organisationales Fehlverhalten

Die im Folgenden beschriebenen spezifischen Erklärungsmodelle für organisationales Fehlverhalten setzen ausgewählte Personen- und Organisationsfaktoren miteinander in Verbindung.

10.2.4.1 Modell der kausalen Schlussfolgerung

Martinko, Gundlach und Douglas zufolge hängt kontraproduktives Verhalten zum einen davon ab, wie eine Situation wahrgenommen wird (Prozesse der **Informationsverarbeitung**), zum anderen davon, wie sich die betroffene Person das Zustandekommen dieser Situation erklärt (**Attribution** von Ursachen).⁷⁰ Die Wahrscheinlichkeit für kontraproduktives Verhalten ist besonders hoch, wenn eine Arbeitssituation als unrechtmäßig, ungerecht oder unerwünscht empfunden wird. Ob kontraproduktives Verhalten gezeigt wird, hängt jedoch entscheidend davon ab, welche Gründe eine Person dieser Situation zuschreibt. Zum Beispiel ob sie für eine verfehlte Zielvorgabe mit entsprechenden Konsequenzen die eigene mangelnde Fähigkeit (internale Attribution) oder unrealistisch gewählte Sollwerte der Führungskraft verantwortlich macht (externale Attribution).

10.2.4.2 Stressor-Emotion Modell

Spector und Fox schlagen zur Erklärung devianten Verhaltens das Stressor-Emotion Modell vor.⁷¹ Demzufolge neigen Personen zu kontraproduktivem Verhalten, wenn sie mit Stressoren konfrontiert werden, die sie als bedrohlich empfinden (zum Beispiel hohe Arbeitsbelastung, störende Einschränkungen des Arbeitsablaufs, Rollenkonflikte, zwischenmenschliche Konflikte oder Ungerechtigkeit). Die wahrgenommene Bedrohung führt zu negativen Emotionen, die vor allem dann in abweichendem Verhalten resultieren, wenn

⁶⁸Vgl. Tyler (2006), S. 217.

⁶⁹Vgl. Tyler (2005), S. 1288.

⁷⁰Vgl. Martinko, Gundlach, & Douglas (2002), S. 43.

⁷¹Spector & Fox, (2005), S. 158.

wenig Kontrolle über die Situation empfunden wird und bestimmte Persönlichkeitseigenschaften (zum Beispiel negative Affektivität oder Narzissmus) stark ausgeprägt sind. Die Aggression richtet sich jedoch häufig nicht gegen die Organisation, sondern gegen die eigene Person (z. B. Alkoholkonsum, Selbstausbeutung) oder gegen Menschen im privaten Umfeld (z. B. Gewalt gegen Familienmitglieder). Damit erfolgt eine indirekte Schädigung der Organisation oder der Gesellschaft.

10.2.4.3 Motivationales Rahmenmodell

Ein umfassendes Erklärungsmodell für verschiedene Formen organisationalen Fehlverhaltens bieten Vardi und Wiener an.⁷²

Sie gehen unter anderem davon aus, dass eine Person motiviert ist, eigennütziges oder schädigendes Verhalten zu zeigen (Typ S und Typ D Verhalten), wenn

- sie sich mit den Unternehmenswerten nicht identifiziert oder gar ein Konflikt mit persönlichen Werten besteht, sodass keine Bereitschaft vorliegt, Verhaltenserwartungen zu erfüllen,
- das Unternehmen ihre Bedürfnisse nicht befriedigt und die Arbeitssituation kontraproduktives Verhalten relativ risikofrei ermöglicht,
- das Erzielen von Belohnungen und Vermeiden von Bestrafungen handlungsleitend ist und
- der Zusammenhalt im Team oder in der Organisation gering ist.

Fehlverhalten gegenüber unternehmensexternen Stakeholdern, wie Kunden, Lieferanten oder Wettbewerbern, das dem eigenen Unternehmen dienen soll (Typ O Verhalten), sollte hingegen besonders häufig vorkommen, wenn

- eine hohe Identifikation mit Unternehmenswerten besteht, sodass eine hohe Bereitschaft besteht, Verhaltenserwartungen zu erfüllen,
- Mitarbeiterbedürfnisse befriedigt werden,
- das Handeln durch soziale Erwartungen im unmittelbaren Umfeld getrieben wird, z. B. durch Kollegen oder Führungskräfte, und
- der Zusammenhalt im Team oder in der Organisation stark ist.

Im Falle von Typ-O Verhalten liegen die Ursachen nahezu ausschließlich in der Organisation und können durch Kontrollen zwar unterdrückt, aber nicht dauerhaft eliminiert werden.

Neben den im letzten Abschnitt beschriebenen spezifischen Annahmen integriert das Modell eine breite Palette der bisher angeführten Wirkfaktoren (Abb. 10.4).

⁷²Vgl. Vardi & Wiener (1996), S. 157.

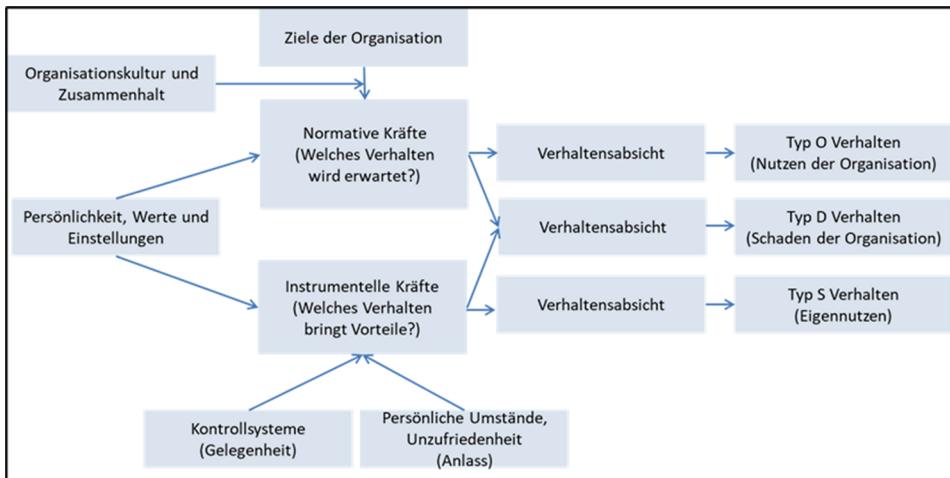


Abb. 10.4 Integratives Rahmenmodell zur Erklärung organisationalen Fehlverhaltens. (In Anlehnung an Vardi & Wiener, (1996); © Institute for Operations Research and the Management Sciences, (1996))

10.3 Bedingungen für regelkonformes Verhalten

Aus den Betrachtungen der vorangegangenen Kapitel geht hervor, dass Mitarbeiter sich mit höherer Wahrscheinlichkeit regelkonform und ethisch korrekt verhalten, wenn sie über Selbstkontrolle, Integrität und bestimmte moralische Standards verfügen, das Gefühl haben, gerecht und wertschätzend behandelt zu werden, keinem außergewöhnlichen situativen Druck ausgesetzt sind und wenig Gelegenheit besitzen, abweichend oder unethisch zu handeln.

Im Folgenden werden darüber hinaus ausgewählte Aspekte beleuchtet, die einen positiven Einfluss auf regelkonformes Verhalten ausüben. Hierzu gehören Gruppenphänomene (Gruppendruck, das Streben nach Einstimmigkeit und eine Abschottung nach außen), die Einschätzung der Risiken regelwidrigen Handelns (Theorie der Schutzmotivation) sowie die Rolle von Verantwortung.

10.3.1 Gruppendruck

Regelkonformes Verhalten wird gezeigt, wenn bei Regelverstoß der Ausschluss aus einer sozialen Gruppe droht. Die Anpassung an implizite und explizite Verhaltensregeln, Werte und Einstellungen kann dabei gegen die eigene innere Überzeugung erfolgen (**öffentliche Compliance** ohne private Akzeptanz).⁷³ Interessanterweise kann die öffentliche Anpassung an bestimmte Normen aber auch dazu führen, dass der Akteur nachträglich seine

⁷³Vgl. Aronson, Wilson, & Akert (2004), S. 315.

Einstellung verändert (**forced compliance**). Hintergrund dieses Phänomens ist, dass Menschen im Allgemeinen versuchen, im Einklang mit ihren Wahrnehmungen, Einstellungen und Absichten zu handeln. Stimmen Verhalten und Einstellung nicht überein, wird dies als unangenehm empfunden (vgl. Abschnitt 10.2.1.4).⁷⁴

Die Bereitschaft sich dem Einfluss einer Gruppe zu beugen, ist besonders hoch, wenn die Gruppenzugehörigkeit als wichtig empfunden wird, die anderen Gruppenmitglieder sich einig sind und die Gruppe mehr als drei Personen umfasst.⁷⁵

Zu beachten ist, dass konformes Verhalten nicht automatisch positiv ist, sondern im Gegenteil auch die Gefahr birgt, dass **falsche** oder **nicht mehr angemessene Normen** befolgt und nicht hinterfragt werden.

Die Tendenz, Gruppennormen unreflektiert zu übernehmen, ist besonders stark, wenn ein enger **Gruppenzusammenhalt** und eine starke **Abschottung nach außen** bestehen.⁷⁶ In diesen Fällen können sogenannte „groupthink“-Phänomene auftreten, die dazu führen, dass sich Gruppenmitglieder gegenseitig in bestimmten Wahrnehmungen bestärken und dabei alternative Erklärungen oder Handlungsoptionen vernachlässigen. Die Gruppe ist sich dabei des Unrechts oft nicht (mehr) bewusst, fühlt sich unangreifbar und empfindet das eigene Verhalten sogar als moralisch.⁷⁷

Maßnahmen zur Erhöhung der Compliance sollten daher immer in einem Rahmen erfolgen, der das kritische Hinterfragen bestehender Regelsysteme erlaubt und fördert.

10.3.2 Schutzmotivation

Die Theorie der Schutzmotivation wurde ursprünglich im Rahmen der Risikokommunikationsforschung entwickelt und später zur Vorhersage von Gesundheitsverhalten herangezogen. Ebenso eignet sie sich zur Erklärung, unter welchen Umständen sich Personen gegen korruptes Verhalten entscheiden.⁷⁸

Eine Person entscheidet sich dem Modell zufolge zu ihrem eigenen Schutz für regelkonformes Verhalten, wenn

- ein Vergehen als schwerwiegend angesehen wird (kein „Kavaliersdelikt“) und hoch negative Sanktionen wahrscheinlich sind
- regelkonforme Verhaltensoptionen für die vorliegende Situation existieren und sie sich in der Lage fühlt, diese anzuwenden
- die Anreize der regelkonformen Verhaltensoption die Anreize der regelverletzenden Option übersteigen.

⁷⁴Ebd.

⁷⁵Ebd.

⁷⁶Vgl. McCauley (1989), S. 350.

⁷⁷Vgl. Turner & Pratkalis (1998), S. 106.

⁷⁸Vgl. Frey, Stahlberg, & Gollwitzer, (1993), S. 361 ff.

10.3.3 Verantwortlichkeit

Verantwortung ist ein vielschichtiger Begriff.⁷⁹ Je nachdem, wie eine Person ihre eigenen Fähigkeiten und Ressourcen einschätzt, kann sie eine hohe Verantwortung als Last oder Auszeichnung empfinden. Verantwortlich sein bedeutet, für die Herbeiführung eines Ergebnisses oder die Konsequenzen einer Handlung geradezustehen. Eine Person ist verantwortlich, wenn sie für die Erreichung vorgeschriebener Leistungsstandards unter der Beachtung vereinbarter Auflagen, Verpflichtungen und Erwartungen zur Rechenschaft gezogen werden kann.⁸⁰ Verantwortlichkeit hängt demnach eng mit sozialer Kontrolle zusammen und ermöglicht es externen Parteien, Verantwortungsträger positiv oder negativ zu sanktionieren.⁸¹ Träger von Verantwortung können sowohl Personen als auch Organisationen sein. Kaschube unterscheidet außerdem zwischen Verantwortung als „pflichtgetreue Übernahme der Perspektive einer Außeninstanz“ und **Eigenverantwortung** als „Reflexion auf eine Instanz innerhalb der eigenen Person“.⁸²

Schlenker et al. integrieren verschiedene Ansätze zur Verantwortungsübernahme, -attribution und -abwehr in einem Rahmenmodell (Abb. 10.5).

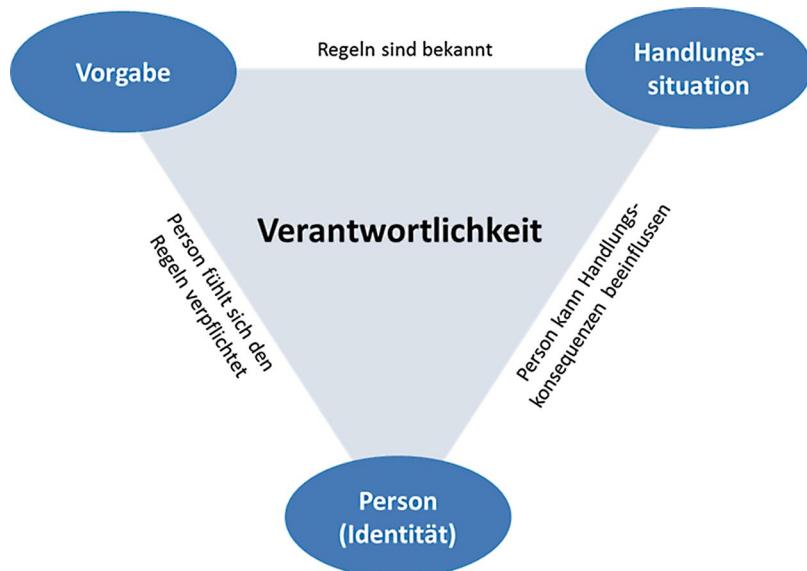


Abb. 10.5 Dreiecksmodell der Verantwortlichkeit. (In Anlehnung an Schlenker, Britt, Pennington, Murphy & Doherty, (1994); © American Psychological Association, Inc., (1994))

⁷⁹Vgl. Kaschube (2006), S. 18.

⁸⁰Vgl. Schlenker, Britt, Pennington, Murphy, & Doherty (1994), S. 632.

⁸¹Ebd.

⁸²Kaschube (2006), S. 19.

Das **Dreiecksmodell der Verantwortung** besagt, dass Verantwortlichkeit wahrgenommen wird, wenn (a) eine Person sich darüber im Klaren ist, welche Regelungen oder Vorgaben in einer Handlungssituation zu beachten sind (Verbindung zwischen Vorgabe und Handlungssituation), (b) die Person sich der Einhaltung dieser Regelungen persönlich verpflichtet fühlt (Verbindung zwischen Person und Vorgabe) und (c) die Person eine hohe Kontrolle darüber besitzt, wie die Handlung und ihre Konsequenzen aussehen (Verbindung zwischen Person und Handlungssituation). Je stärker die Verbindungen sind, desto höher ist die wahrgenommene Verantwortung.⁸³

Das Verantwortungsgefühl steigert sich demnach, wenn Ziele und Ausführungsregeln transparent sind, die eigene Rolle innerhalb einer Situation klar ist und der Akteur den Handlungsausgang aktiv beeinflussen kann. Geringe Verantwortlichkeit wird empfunden, wenn Ziele oder Mittel der Zielerreichung unklar sind oder unpräzise kommuniziert werden, der Aufgabenbereich nicht klar abgegrenzt ist und der Akteur wenig Einfluss auf die Situation nehmen kann. Das Dreiecksmodell lässt sich sowohl auf das eigene Verantwortungsgefühl (Selbstbewertung) als auch auf die Bewertung durch andere Personen (Fremdbewertung) beziehen. Experimentelle Studien zeigen, dass Versuchsteilnehmer die Verantwortlichkeit anderer Akteure danach bewerten, inwiefern sie geltende Vorgaben kennen, diese anwenden können und Kontrolle über die Situation besitzen.⁸⁴

Um stabile Verantwortungsübernahme und regelkonformes Verhalten im Unternehmen zu fördern, ist ein transparentes Regelsystem und eine klare Kommunikation von Zielen und Erwartungen notwendig, sodass jeder Mitarbeiter zu jedem Zeitpunkt eine Vorstellung davon hat, welches Verhalten im Sinne des Unternehmens „richtig“ oder „falsch“ ist. Gelingt die klare Zuteilung von Verantwortung nicht, erhöht sich die Wahrscheinlichkeit der Verantwortungsdiffusion („alle sehen zu, aber niemand schreitet ein“). Bedingt durch die Komplexität moderner Organisationen ist es allerdings unrealistisch, vollkommen klare Verantwortlichkeiten für alle potenziell auftretenden Situationen schaffen zu können.⁸⁵ Idealerweise wird also ein System strukturierter Verantwortung durch die Übernahme von Eigenverantwortung ergänzt. Dies bedeutet, dass Mitarbeiter Regeln und Vorschriften nicht nur stumpf anwenden, sondern aktiv reflektieren und, wenn nötig, weiterentwickeln (vgl. Abschn. 10.3.4.2.2). Die Übernahme von Eigenverantwortung kann als eine Form von extraproduktivem Verhalten verstanden werden, die durch eine hohe Identifikation mit der eigenen Arbeitsaufgabe und den Grundwerten der Organisation gefördert wird.⁸⁶ Wichtig ist eine gute Balance zwischen Handlungsspielräumen und Kontrollmechanismen im Unternehmen nach dem Grundsatz „Vertrauen ist gut, aber Kontrolle darf nicht fehlen“. Im Idealfall empfindet sich jedes Organisationsmitglied als mitverantwortlich für die Einhaltung von Regeln und gesetzlichen Bestimmungen. So können erste Anzeichen abweichenden Verhaltens durch Whistleblowing und handlungsnahes Feedback bereits im Keim ersticken werden.

⁸³Vgl. Schlenker, Britt, Penningston, Murphy, & Doherty (1994), S. 634.

⁸⁴Vgl. Schlenker, Britt, Penningston, Murphy, & Doherty (1994), S. 634.

⁸⁵Vgl. Kaschube (2006), S. 164.

⁸⁶Vgl. Vardi & Wiener (1996), S. 161.

10.3.4 Maßnahmen zur Förderung von Compliance

Geht man davon aus, dass Menschen im Hinblick auf eigene Interessen und nach dem Reziprozitätsprinzip handeln,⁸⁷ macht es Sinn, faire organisationale Rahmenbedingungen zu schaffen, die unethisches Verhalten mit hohen Kosten und geringem zusätzlichem Nutzen verbinden. Bestenfalls besteht für Mitarbeiter und Führungskräfte des Unternehmens so weder Anlass noch Gelegenheit, sich auf unlautere Weise einen Nutzen zu verschaffen.

Grundsätzlich können Maßnahmen zur Förderung von Compliance an der Person des Mitarbeiters (personenbezogen) oder an der Organisation (umfeldbezogen) ansetzen. Wie Tyler beschreibt, sind dabei zwei Wege möglich: Methoden der **Kontrolle** („Vermeide Fehlverhalten!“) oder die **Vermittlung von Werten** und das Zulassen von **Handlungsspielraum** („Fördere richtiges Verhalten!“).⁸⁸ Während Kontrollmechanismen eher die öffentliche Compliance steigern (Mitarbeiter verhalten sich regelkonform, ohne zwangsläufig ihre Überzeugungen anzupassen), zielen werteorientierte Maßnahmen darauf ab, die Identifikation mit den Unternehmenswerten zu erhöhen und somit regelkonformes Verhalten zu einem inneren Standard zu erheben. Letzteres zeigt im Allgemeinen eine nachhaltigere Wirkung.⁸⁹

Aus praktischer Perspektive scheint ein **Methodenmix** sinnvoll, in dem sich kontrollierende und werteorientierte Maßnahmen ergänzen.

10.3.4.1 Personenbezogene Maßnahmen

Personenbezogene Maßnahmen betreffen klassische Aufgaben der Personalarbeit: Die Anwerbung, Auswahl und Schulung von Mitarbeitern.

10.3.4.1.1 Personalmarketing

Erfolgreiches Personalmarketing in Bezug auf Compliance soll bewirken, dass vor allem solche Bewerber auf das Unternehmen aufmerksam werden, die bereit sind, Gesetze, Richtlinien und unternehmensinterne Verhaltensregeln zu befolgen. Hier spielt das Image des Unternehmens eine wichtige Rolle. Repräsentiert sich eine Organisation, zum Beispiel durch entsprechende **CSR-Aktivitäten**, nach außen als Institution, die sich ihrer gesellschaftlichen Verantwortung und der Bedeutung nachhaltigen unternehmerischen Handelns bewusst ist, wird sie Interessenten anziehen, denen solche Werte wichtig sind.⁹⁰ Um eine echte Passung zu erzielen, ist es daher notwendig, dass die Außenwirkung **authentisch** ist, also den wahren Überzeugungen und Handlungsgrundlagen innerhalb des Unternehmens entspricht. Die besten Botschafter eines Unternehmens mit der höchsten Glaubwürdigkeit sind die dort beschäftigten Mitarbeiter, die selbst einen Teil der Unter-

⁸⁷Vgl. Homann & Suchanek (2005), S. 381.

⁸⁸Vgl. Tyler (2005), S. 1287.

⁸⁹Vgl. Paine, (1994), S. 117.

⁹⁰Vgl. Nerdinger, Blickle, & Schaper (2011), S. 217–218.

nehmensrealität ausmachen.⁹¹ Viele Unternehmen nutzen informelle Kontakte ihrer Mitarbeiter zur Rekrutierung. In der Regel besitzen solche Bewerber ähnliche Einstellungen und Werthaltungen wie die empfehlende Person, kommen mit realistischen Erwartungen in das Unternehmen und integrieren sich leichter.⁹² Die Wahrscheinlichkeit eines wahrgenommenen psychologischen Vertragsbruches mit entsprechenden negativen Konsequenzen (vgl. Abschn. 10.2.1.5) ist somit geringer. Ein Nachteil dieser Strategie besteht darin, dass die Mitarbeiterschaft sehr homogen wird. Eine geringe Perspektivenvielfalt unterstützt regelkonformes Verhalten, wirkt sich jedoch negativ auf das kritische Hinterfragen von Regeln und Vorschriften aus und verringert die Innovationskraft.⁹³

10.3.4.1.2 Personalauswahl

„In looking for people to hire, look for three qualities: integrity, intelligence, and energy. And if they don't have the first one, the other two will kill you.“ (Warren Buffett, amerikanischer Großinvestor).

Bei der Personalauswahl sollte neben der fachlichen Qualifikation auch auf Persönlichkeitsmerkmale, Einstellungen und Werte der Bewerber geachtet werden. Eine Möglichkeit, Bewerber mit problematischen Verhaltensneigungen frühzeitig zu identifizieren, sind **Persönlichkeits- oder Integritätstests**.⁹⁴

Integrität kann gemessen werden, indem Bewerber direkt nach ihrer Einstellung zu devianten Verhaltensweisen, wie Diebstahl oder Betrug, gefragt werden (einstellungsorientierte Integritätstests). Diese Methode wird im anglo-amerikanischen Raum häufig eingesetzt. Die Aussagekraft des Tests basiert darauf, dass Personen mit Neigung zu abweichendem Verhalten sich in Bezug auf ihr Antwortmuster vom Bevölkerungsdurchschnitt unterscheiden. Alternativ können verwandte Persönlichkeitsmerkmale, wie Vertrauen, Zuverlässigkeit, Impulskontrolle oder die Neigung zu Risikoverhalten erfasst werden (eigenschaftsorientierte Tests).⁹⁵ Vor dem Einsatz von Integritätstests sollte bedacht werden, welche Eigenschaften und Fähigkeiten tatsächlich am Arbeitsplatz benötigt werden. Es gibt zum Beispiel Hinweise, dass Personen mit hoch ausgeprägter Integrität weniger Eigenverantwortung übernehmen und weniger unternehmerisches Handeln zeigen.⁹⁶ Eine gezielte Stärkung regelkonformen Arbeitsverhaltens kann somit zu einem Verlust von innovativem und gestalterischem Potenzial in der Organisation führen.⁹⁷

Im Vergleich mit anderen Instrumenten der Personalauswahl, zum Beispiel Bebungsgespräche, Arbeitsproben, Arbeitszeugnisse oder Intelligenztests, empfinden Bewerber Persönlichkeits- und vor allem Ehrlichkeitstests überdies als **weniger akzeptabel**.

⁹¹Vgl. Moser (1995), S. 105.

⁹²Vgl. Nerdinger, Blickle, & Schaper (2011), S. 219.

⁹³Vgl. Van Knippenberg, & Schippers (2007), S. 518.

⁹⁴Vgl. Nerdinger, Blickle, & Schaper (2011), S. 419.

⁹⁵Vgl. Wanek, Sacket & Ones (2003), S. 874.

⁹⁶Vgl. Koch (2005), S. 165.

⁹⁷Vgl. Kaschube & Gasteiger (2005), S. 189 ff.

bel – einzig grafologische Gutachten schneiden noch schlechter ab.⁹⁸ Zu beachten ist auch, dass die Neigung, auf Persönlichkeitsfragen eher sozial erwünscht als ehrlich zu antworten, die Ergebnisse solcher Tests verfälschen kann. Sie sind daher nur als ergänzendes Auswahlverfahren einzusetzen und sollten von Psychologen durchgeführt werden, die in der Interpretation von Persönlichkeitstests geschult sind.

Weitere Methoden zur Identifizierung von Personen mit aggressiven Neigungen sind das Einholen von Hintergrundinformationen und **Referenzen** von früheren Arbeitgebern oder Fragen nach erlebter unfairer Behandlung.⁹⁹

Grundsätzlich sollte eine Organisation, die ethisch-moralisches Verhalten von ihren (künftigen) Mitarbeitern erwartet, selbst mit gutem Beispiel vorangehen und **ethisch-moralische Standards in der Personalauswahl** einhalten. Dazu gehören Transparenz über die Art und Durchführung des Auswahlverfahrens sowie ein respektvoller und wertschätzender Umgang mit allen Bewerbern.¹⁰⁰ Ebenso wichtig ist eine realistische Tätigkeitsvorschau, die auch unangenehme Aspekte der künftigen Tätigkeit anspricht. Earnest, Allen und Landis betonen in diesem Zusammenhang die bislang noch wenig untersuchte symbolische Wirkung einer realistischen Tätigkeitsbeschreibung, die Ehrlichkeit, Bereitschaft zur Unterstützung und Fürsorge von Seiten des Unternehmens signalisiert.¹⁰¹ Bewerber, die ihre Stelle mit realistischen Erwartungen antreten, zeigen im Allgemeinen weniger Schwierigkeiten in der Einarbeitungsphase und kündigen deutlich seltener innerhalb ihres ersten Beschäftigungsjahrs.¹⁰²

10.3.4.1.3 Personalentwicklung

Maßnahmen der Personalentwicklung bestehen vor allem darin, Mitarbeiter über gesetzliche Bestimmungen, Normen und unternehmensinterne Verhaltensregeln zu **informieren**.¹⁰³ Es empfiehlt sich dabei, ethische Grundsätze, Regelungen und Standards sowohl mündlich als auch schriftlich zu kommunizieren. Neu eingestellte Mitarbeiter sollten außerdem auf drohende Strafen oder Sanktionen bei persönlichem Fehlverhalten hingewiesen werden. Zusätzlich kann es aber auch darum gehen, Mitarbeiter für Anzeichen von Korruption oder kontraproduktivem Arbeitsverhalten zu **sensibilisieren** und ihnen Handlungsmöglichkeiten für entsprechende Situationen aufzuzeigen. Auf diese Weise werden Mitarbeiter zu Multiplikatoren von Compliance, die abweichendes Verhalten früh-

⁹⁸Vgl. Hausknecht, Day & Thomas, (2004), S. 624.

⁹⁹Vgl. Nerdinger, Blickle, & Schaper (2011), S. 420.

¹⁰⁰Vgl. Nerdinger, Blickle, & Schaper (2011), S. 248.

¹⁰¹Vgl. Earnest, Allen, & Landis (2011), S. 888.

¹⁰²Vgl. Nerdinger, Blickle, & Schaper (2011), S. 222.

¹⁰³Vgl. Paine (1994), S. 109.

zeitig identifizieren und gegensteuern können („Whistleblowing“). Außerdem können **Schulungsmaßnahmen** angeboten werden, die den Umgang mit schwierigen Situationen erleichtern, wie etwa soziale Kompetenz-, Konflikt- oder Stressmanagementtrainings.¹⁰⁴

Eine besondere Zielgruppe für die Personalentwicklung sind die **Führungskräfte** einer Organisation. Sie agieren als Vorbilder und Identifikationsfiguren und gelten damit als wichtige Träger von Unternehmenskultur.¹⁰⁵ Eine ethikorientierte Führung, die Leistung einfordert, dabei jedoch Werte und Menschlichkeit vermittelt, kann als Grundpfeiler einer Compliance- und Integritätskultur begriffen werden.¹⁰⁶ Entsprechend sollten Führungs-kräfte so ausgewählt und geschult werden, dass ein **ethikorientiertes Führungsklima** in der Organisation entsteht. Wichtige Elemente sind dabei ein ehrliches Interesse für die Mitarbeiter und ihre Bedürfnisse, die klare Kommunikation realistischer und ehrgeiziger Ziele, eine sensible Verteilung von Ressourcen, die Einbettung der Arbeit in ein sinnvolles Ganzes (Vermittlung von Sinn und Vision) und regelmäßige konstruktive Rückmeldung über die erbrachte Leistung.¹⁰⁷

10.3.4.2 Umfeldbezogene Maßnahmen

Umfeldbezogene Maßnahmen betreffen die Gestaltung von Rahmenbedingungen innerhalb der Organisation, die Compliance fördern.

10.3.4.2.1 Compliance-Management-Systeme (CMS)

Die meisten Organisationen verfügen bereits über mehr oder weniger umfangreiche **Ethik-Richtlinien** und einen **Verhaltenskodex** (Code of Conduct), die eine Orientierung für erwünschtes Verhalten darstellen.

Immer mehr Unternehmen gehen einen Schritt weiter und investieren in **Compliance-Management-Systeme (CMS)**, die die Arbeit von Controlling- und Revisionsabteilungen ergänzen. CMS umfassen alle Maßnahmen und Prozesse innerhalb des Unternehmens, die darauf abzielen, Regelverstöße zu verhindern, Verfehlungen so schnell wie möglich zu erkennen und möglichst effektiv und konsequent darauf zu reagieren.¹⁰⁸ 2018 verfügten bereits etwa 75 % der Unternehmen mit mehr als 500 Mitarbeitern und 97 % aller Großunternehmen über ein CMS.¹⁰⁹ Compliance-Maßnahmen dienen dem Zweck, Haftungsrisiken zu verringern, strafrechtlichen Sanktionen zu entgehen und Reputationsschäden vorzubeugen; es geht aber auch um den Schutz der eigenen Arbeitnehmer und ein positives Image in der Öffentlichkeit (ebd.). Hier ergibt sich eine Verbindung zum Konzept der Corporate Social Responsibility (CSR) eines Unternehmens.

¹⁰⁴Vgl. Nerdinger (2008), S. 78.

¹⁰⁵Vgl. Schein, (1995), S. 17.

¹⁰⁶Vgl. Frey, Streicher, & Aydin (2012), S. 236.

¹⁰⁷Vgl. Frey, Oswald, Peus, und Fischer (2011), S. 245.

¹⁰⁸Vgl. Pütz (2011), S. 20.

¹⁰⁹Vgl. Bussmann, Nestler, & Salvemmoser (2018), S. 24.

Grundsätzlich kann ein CMS als eigenständige Abteilung unter der Leitung eines Compliance-Managers, als Teil der Rechtsabteilung, der internen Revision, oder als interdisziplinärer Lenkungskreis in eine Organisation integriert werden.¹¹⁰ Berichtet wird meist direkt an die Geschäftsführung oder an den Aufsichtsrat. Der **Aufbau eines Compliance-Systems** (siehe Abb. 10.6) richtet sich individuell nach den Bedürfnissen einer Organisation und beinhaltet in der Regel eine Risikoanalyse, die Ermittlung erforderlicher Schritte zur Risikovorsorge, die Festlegung von Verfahrensabläufen bei vermuteten oder tatsächlichen Regelverstößen und die Einrichtung eines Kontrollsystems, zum Beispiel indem eine entsprechende Abteilung oder Stellen gebildet werden.

Typische Elemente im Aufbau eines Compliance-Systems

- *Identifikation spezieller Risikofelder:*
Analyse der rechtlichen Rahmenbedingungen in denen die Organisation sich bewegt, Ermittlung der Eintrittswahrscheinlichkeit und des potentiellen Schadensumfangs von Regelverstößen. Risikofaktoren können z. B. ein hohes Auftragsvolumen, ein korruptes Geschäftsfeld, Umweltrisiken, kulturelle Besonderheiten oder die Komplexität der Unternehmensorganisation sein.
- *Ermittlung erforderlicher Schritte zur Risikovorsorge:*
Analyse bereits existierender Schutzmechanismen und Bestimmung weiterer notwendiger Maßnahmen, Zuordnung von Verantwortlichkeiten, Ermittlung des Schulungsbedarfs und ggf. Schulung der Verantwortlichen.
- *Festlegung von Verfahrensabläufen bei Regelverstößen:*
Einrichtung eines Frühwarn- und Meldesystems für Regelverstöße, z. B. Kontaktangebote für Dilemma-Situationen, vertrauliche Meldewege für Hinweisegeber, etwa über Email oder spezielle Hotlines, und ggf. die Ernennung von Ombudsmännern, an die sich Mitarbeiter vertrauenvoll wenden können, wenn sie einen Verdacht haben.
- *Einrichtung eines Kontrollsystems:*
Installation eines Compliance-Bereichs, ggf. Berufung eines Compliance-Beauftragten, Entwicklung von unternehmensinternen Verhaltensrichtlinien und Mindeststandards für Dritte (z. B. Geschäftspartner), Festlegen von Kommunikationsabläufen, Einführung einheitlicher Sanktionsmaßnahmen, Entwicklung von Audit- und Kontrollverfahren und ggf. Zertifizierung des Systems
- *Kommunikation nach innen und außen:*
Bedeutsamkeit des Themas unterstreichen, z. B. durch Information und Schulung der Mitarbeiter, regelmäßige Kommunikation zu Compliance-Themen, Dialog mit Mitarbeitern, Partnern und Kunden, Austausch von „best practices“

Abb. 10.6 Typische Elemente im Aufbau eines Compliance-Systems

¹¹⁰Vgl. Cauers, Haas, Jakob, Kremer, Schartmann, & Welp (2008), S. 2717.

10.3.4.2.2 Entwicklung einer Integritätskultur

Während das klassische Compliance-Management sich vornehmlich darauf konzentriert die Einhaltung von Regeln und gesetzlichen Bestimmungen zu kontrollieren, wird im modernen Verständnis des Konzepts eine **ganzheitlichere Perspektive** eingenommen: „Erfolgreiche Compliance (...) erfordert den gesamthaften Blick auf die innere Verfassung der Organisation und des Miteinanders im Unternehmen“.¹¹¹

Diese Sichtweise impliziert, dass es neben der Einrichtung notwendiger Kontrollmechanismen auch eine Einbindung von Compliance in die Unternehmenskultur geben muss. Thielemann (2005) unterscheidet dabei zwischen **Compliance** als „doing what one must do, because it ought to be done“ und **Integrität** als „wanting what ought to be done“.¹¹² Er argumentiert, dass Compliance und Integrität auf Organisationsebene als zwei Seiten einer Medaille verstanden werden können, die sich wechselseitig bedingen: Compliance bedeutet die Schließung der Organisation für organisationales Fehlverhalten, Integrität die Öffnung der Organisation für ethische Einsichten.

In einer Compliance-Kultur besteht der Anreiz, sich korrekt zu verhalten vor allem darin, negative Sanktionen zu vermeiden. Eine Integritätskultur geht über Compliance hinaus und bildet alle Organisationsmitglieder zu mündigen Teilnehmern bzw. Kulturträgern aus, die sich aus einem moralischen Bewusstsein heraus für die Befolgung von Regeln und Vorschriften entscheiden und diese bei Bedarf auch kritisch reflektieren (Abb. 10.7).

Markenzeichen einer effektiven Integritäts-Strategie

(nach Paine, 1994)

- Die Unternehmenswerte machen Sinn, werden klar kommuniziert und auf allen Organisationsebenen ernst genommen
- Führungskräfte bekennen sich zu den Unternehmenswerten und setzen sich konsequent für sie ein
- Die Unternehmenswerte lassen sich sinnvoll in den Unternehmensalltag integrieren und fließen in Zielsysteme, Entscheidungen, Leistungsbeurteilung und Förderung ein
- Organisationsstrukturen und interne Systeme unterstützen und bestärken das Handeln im Einklang mit den Unternehmenswerten
- Führungskräfte verfügen über die notwendige Grundeinstellung, ausreichende Entscheidungskompetenz, Wissen und Fähigkeiten, um ethisch einwandfreie Entscheidungen zu treffen

Abb. 10.7 Markenzeichen einer effektiven Integritätsstrategie nach Paine (1994)

¹¹¹Vgl. Mahlert (2009), zit. nach Pütz (2011), S. 33.

¹¹²Vgl. Thielemann (2005), S. 31.

Mitarbeiter handeln also nicht nur pflichtschuldig, sondern aus Überzeugung (intrinsisch motiviert) im Einklang mit den Unternehmenswerten. Zugleich plädiert Thielemann dafür, einen Interessenskonflikt zwischen Geschäftszielen und Compliance zu vermeiden, indem das Handeln nach ethisch-moralischen Grundprinzipien und im Einklang mit den Unternehmenswerten zum Bestandteil von Zielvereinbarungen, Beurteilungs- und Belohnungssystemen innerhalb der Organisation gemacht wird (extrinsische Anreize).

Einer der ersten Unternehmensvertreter, der Führungskräfte zugleich nach ihrer Zielerreichung und dem Handeln nach Unternehmenswerten beurteilte, war Jack Welch, der umstrittene ehemalige CEO von General Electric.

In seiner **Performance-Value-Matrix** (Abb. 10.8) schneiden diejenigen Führungskräfte am besten ab, die unter Berücksichtigung von Unternehmenswerten und Richtlinien ihre Ziele erreichen oder übertreffen. Sie sollten Lob, Wertschätzung und Förderung innerhalb der Organisation erfahren, da sie als Multiplikatoren einer positiven Unternehmenskultur agieren. Führungskräfte hingegen, die weder ihre Ziele erreichen noch werteorientiert handeln, passen nicht in das Unternehmen. Besonders interessant im Hinblick auf die Werteausrichtung eines Unternehmens ist der Umgang mit Führungskräften, die ihre Ziele nicht erreichen, jedoch im Einklang mit Unternehmenswerten handeln und Managern, die zwar ihre Ziele erreichen oder übertreffen, dabei aber Unternehmenswerte verletzen. Für die erste Gruppe lautet die Empfehlung, sie in der Entwicklung notwendiger Kompetenzen zu unterstützen, zum Beispiel durch Trainings oder Coaching, oder sie nach Möglichkeit an anderer Stelle in der Organisation einzusetzen. Die zweite Gruppe ist für eine werteorientierte Unternehmenskultur die Gefährlichste: Führungspersonen, die eine gute oder sogar exzellente Leistung erbringen, dabei jedoch Werte und Spielregeln des Fairplay missachten, sind Multiplikatoren einer negativen und korruptionsanfälligen Unternehmenskultur. Oft ist es so, dass Personen mit schwierigen Persönlichkeitsdispositionen (vgl. Abschn. 10.2.2.3) in Führungspositionen gelangen oder sich, wenn sie dort sind, negativ entwickeln. Unter hohem Erfolgsdruck fällt es dann unter Umständen schwer, solche Leistungsträger zu entlassen, selbst wenn ihr Handeln durch Opportunis-

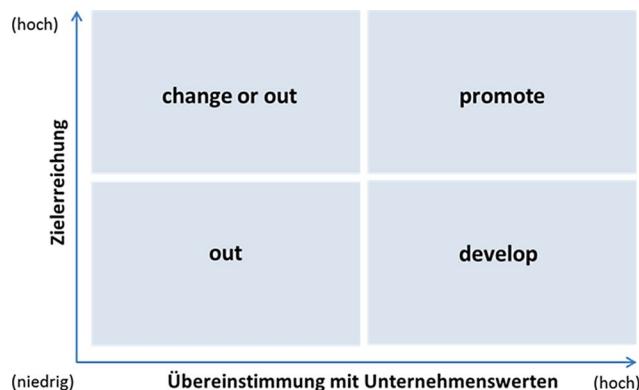


Abb. 10.8 Die Performance-Value Matrix nach Jack Welch

mus, Narzissmus, Rücksichtslosigkeit und Streben nach machtpolitischer Selbstverwirklichung geprägt ist. Die Entscheidung gegen unethische Führungspersonen signalisiert aber eine konsequente Haltung in Bezug auf werteorientiertes Handeln.

Eine PwC Studie (2011) zeigt, dass Compliance und Werteorientierung zum Selbstverstärker werden können: Mitarbeiter in Organisationen mit einer positiven Unternehmenskultur akzeptieren Compliance-Initiativen nicht nur besser, sondern sind auch seltener Bestechungsversuchen ausgesetzt.¹¹³

10.3.5 „Unternehmen brauchen einen Kompass, kein Navigationssystem“

Die Entwicklung einer Integritätskultur sollte von der Unternehmensführung ausgehend alle Ebenen der Organisation erfassen.¹¹⁴ Sie beginnt mit einem durch das **Topmanagement initiierten Dialog** über unternehmensleitende Werte, Ziele, Denk- und Handlungsmuster.¹¹⁵ Neben universellen moralischen Grundprinzipien kommen dabei auch individuell bedeutsame Werte zum Tragen, die sich aus der Unternehmensgeschichte oder organisationalen Rahmenbedingungen, wie zum Beispiel der Art des Produktes oder der Branche, ergeben.¹¹⁶ Laut Thielemann besitzt das Management bei der Formulierung eines Wertekanons nicht zwangsläufig die Definitionsmacht.¹¹⁷ Aufgabe der Führungskräfte ist es vielmehr, den Dialog anzuregen, Werte und moralische Grundsätze zu kommunizieren, in Zielsysteme zu integrieren und im Unternehmensalltag sowie auch in Krisensituationen konsequent zu vertreten (Abb. 10.7). Führungskräfte sind damit Schlüsselfiguren und bilden eine Art Kompass für die Umsetzung abstrakter Werte in alltägliche Handlungen und Entscheidungen der Mitarbeiter.¹¹⁸

Eine Herausforderung liegt in der Balance verschiedener Ziele, denn der wirtschaftliche Erfolg einer Organisation darf im Zuge der Wertediskussion nicht in den Hintergrund geraten. Genau genommen sind ethikorientierte Führungspersonen für zwei Kulturen verantwortlich: Einerseits eine Kultur von **Exzellenz**, die über ein reines Befolgen von Regeln hinaus gewährleistet, dass die Organisation leistungsorientiert und innovativ handelt, sich an äußere Gegebenheiten oder den Markt anpasst und hohe Qualitätsstandards einhält;¹¹⁹ andererseits eine Kultur von **Menschenwürde**, die einen fairen Umgang mit internen und externen Stakeholdern sicherstellt¹²⁰ (Abb. 10.9).

¹¹³Vgl. Bussmann, Krieg, Nestler, & Salvenmoser (2010), S. 18 und S. 41.

¹¹⁴Vgl. Frey, Faulmüller, Winkler, & Wendt (2002), S. 136.

¹¹⁵Vgl. Paine (1994), S. 112.

¹¹⁶Vgl. Braun, Wesche, Frey, Weisweiler, & Peus (2012), S. 436.

¹¹⁷Vgl. Thielemann (2005), S. 32.

¹¹⁸Vgl. Frey, Frey, Peus, & Oßwald (2008), S. 227.

¹¹⁹Vgl. Frey, Jonas, & Greitemeyer (2002), S. 156.

¹²⁰Vgl. Frey, Streicher, & Aydin (2012), S. 236.



Abb. 10.9 Das Konzept ethikorientierter Führung nach Frey, Streicher & Aydin (2012)

Ein Unternehmen, das die Exzellenz-Säule vernachlässigt, lässt sich vergleichen mit einer Fußballmannschaft, die niemals gelbe oder rote Karten erhält – aber auch keine Tore erzielt. Compliance allein garantiert keinen Markterfolg. Entscheidend ist ein professionelles und effizientes Zusammenspiel von Entscheidungsträgern und Mitarbeitern, um Synergieeffekte zu produzieren und Höchstleistungen zu erreichen.¹²¹ Dieses Zusammenspiel funktioniert jedoch nur, wenn faire Bedingungen herrschen und Verstöße gegen eine Kultur der Menschenwürde, zum Beispiel durch Machtmissbrauch, Mobbing oder Rufmord, nicht toleriert werden. Hier hilft eine **Kultur der hierarchiefreien Kommunikation**, in der Positiv- wie Negativbeispiele offen angesprochen werden dürfen.¹²²

Um Unternehmen in die Lage zu versetzen ihren eigenen Standort in Bezug auf Compliance und ethikorientierte Führungskultur zu bestimmen, ist die Entwicklung differenzierter **Messinstrumente** hilfreich. Abhängig von der Messintention können in die Beurteilung des Compliance-Bereichs verschiedene Datenquellen einfließen: Von Mitarbeiterbefragungen mittels Fragebögen, Diskussionen in Fokusgruppen oder strukturierten Interviews bis hin zu objektiven Unternehmensdaten. Unter anderem vor dem Hintergrund der ISO 37301 gewinnt die Beschäftigung mit Kennzahlen im Compliance-Bereich an Bedeutung.¹²³

¹²¹Vgl. Frey, Kerschreiter, Winkler, & Gaska (2004), S. 49.

¹²²Vgl. Frey, Oßwald, Peus, & Fischer (2011), S. 245.

¹²³Vgl. Quast (2019), S. 4.

Für die Messung einer ethikorientierten Organisationskultur stehen Fragenkataloge zur Verfügung, wie zum Beispiel das Integrity Thermometer¹²⁴ oder dessen Kurzform.¹²⁵ Der Fragebogen erfasst die persönliche Einschätzung der Mitarbeitenden, inwiefern Regeln und Unternehmenswerte bekannt sind, durch die direkte Führungskraft sowie im Top Management vorgelebt werden, ausreichende Ressourcen und Unterstützung vorhanden ist, um die Arbeit regelkonform ausführen zu können, entsprechende Kontrollen etabliert sind und moralische Dilemma-Situationen offen diskutiert werden können.

Die Integration von Grundwerten in die Unternehmenskultur und entsprechende Sozialisation von Mitarbeitenden und Führungskräften fördert ethisches Verhalten gegenüber Organisationsmitgliedern, Kunden und anderen Stakeholdern. Hierzu gehört auch Vertrauen in positive Kräfte und Potenziale des Unternehmens. Denn wie bereits Goethe erkannte: „Wer die Menschen behandelt, wie sie sind, macht sie schlechter. Wer sie aber behandelt, wie sie sein könnten, macht sie besser“.

Literatur

- AJZEN, I. (1991): The Theory of Planned Behavior, aus: *Organizational Behavior and Human Decision Processes*, Heft 2/1991.
- AMELANG, M. & BARTUSSEK, D. (2001): *Differentielle Psychologie und Persönlichkeitsforschung*, Stuttgart.
- ARONSON, E., WILSON, T. D., & AKERT, R. M. (2004): *Sozialpsychologie*, München.
- BECKER, T. E. (1998): Integrity in Organizations: Beyond Honesty and Conscientiousness, aus: *Academy of Management Review*, Heft 1/1998.
- BLAU, P. (1964): *Exchange and power in social life*, New York.
- BRAUN, S., WESCHE, J. S., FREY, D., WEISWEILER, S., & PEUS, C. (2012): Effectiveness of Mission Statements in Organizations – A review, aus: *Journal of Management & Organization*, Heft 4/2012.
- BRUCH, H., & MENGES, J. I. (2010): The Acceleration Trap, aus: *Harvard Business Review*, Heft 4/2010.
- BUSSMANN, K.D., KRIEG, O., NESTLER, C., & SALVENMOSEN, S. (2010): *Compliance und Unternehmenskultur. Zur aktuellen Situation in deutschen Großunternehmen.*, Frankfurt a.M.
- BUSSMANN, K.D., NESTLER, C., & SALVEMMOSEN, S. (2018): *Wirtschaftskriminalität 2018. Mehrwert von Compliance – forensische Erfahrungen*, Frankfurt a. M.
- CAUERS, L., HAAS, K., JAKOB, A., KREMER, F., SCHARTMANN, B., & WELP, O. (2008): Ist der gegenwärtig viel diskutierte Begriff „Compliance“ nur alter Wein in neuen Schläuchen?, aus: *Der Betrieb*, Heft 50/2008.
- CROPANZANO, R., & MITCHELL, M. S. (2005): Social Exchange Theory: An Interdisciplinary Review, aus: *Journal of Management*, Heft 6/2005.
- CZOTSCHER, E. (2009): *Managementkompass Wertemanagement*, Frankfurt am Main.
- DOUGLAS, S.C. & MARTINKO, M. J. (2001): Exploring the role of individual differences in the prediction of workplace aggression, aus: *Journal of Applied Psychology*, Heft 4/2001.

¹²⁴Vgl. Kaptein (2008), S. 978–1008.

¹²⁵Vgl. DeBode, Armenakis, Feild, & Walker (2013), S. 460–484.

- DEBODE, J. D., ARMENAKIS, A. A., FEILD, H. S., & WALKER, A. G. (2013): Assessing ethical organizational culture: Refinement of a scale, aus: *The Journal of Applied Behavioral Science*, Heft 4/2013.
- EARNEST, D. R., ALLEN, D. G., LANDIS, R. S. (2011): Mechanisms linking realistic job previews with turnover: a meta-analytic path analysis, aus: *Personnel Psychology*, Heft 4/2011.
- ETZIONI, A. (1961): A comparative analysis of complex organizations: On Power, Involvement, and their Correlates, New York.
- FREY, D., FAULMÜLLER, N., WINKLER, M. & WENDT, M. (2002). Verhaltensregeln als Voraussetzung zur Realisierung moralisch-ethischer Werte in Firmen. *Zeitschrift für Personalforschung*, 16, 2, 2002.
- FREY, D., FREY, A., PEUS, C. & OSSWALD, S. (2008). Warum es so leicht ist, Werte zu proklamieren und so viel schwieriger, sich auch entsprechend zu verhalten. In E. Rohmann, M.J. Herner & D. Fetchenhauer (Hrsg.): *Sozialpsychologische Beiträge zur Positiven Psychologie* (eine Festschrift für Hans-Werner Bierhoff). 226–247. Lengerich: Pabst.
- FREY, D., JONAS, E. & GREITEMEYER, T. (2002). Intervention as a major tool of a psychology of human strength: Examples from organizational change and innovation. In L.G. Aspinwall & U.M. Staudinger (Eds.), *A psychology of human strength: Perspectives on an emerging field*. Washington, DC: American Psychological Association. 149–164.
- FREY, D., KERSCHREITER, R., WINKLER, M. & GASKA, A. (2004). Wie viel Moral braucht der Mensch? Die Bedeutung von Werten und ethischen Prinzipien bei der Führung von Mitarbeitern. In: H. Bohlander & M. Büscher (Hrsg.): *Werte im Unternehmensalltag erkennen und gestalten*. DNWE Schriftenreihe, Folge 13, 49–69. München: Rainer Hampp Verlag.
- FREY, D., OSSWALD, S., PEUS, C. & FISCHER, P. (2011). *Positives Management, ethikorientierte Führung und Center of Excellence: Wie Unternehmenserfolg und Entfaltung der Mitarbeiter durch neue Unternehmens- und Führungskulturen gefördert werden können*. In: M. Ringlstetter, S. Kaiser & G. Müller-Seitz (Hrsg.): *Positives Management*. 239–270. Wiesbaden: Gabler: Edition Wissenschaft.
- FREY, D., STAHLBERG, D., GOLLWITZER, P. M. (1993): Einstellung und Verhalten: Die Theorie des überlegten Handelns und die Theorie des geplanten Verhaltens, aus: FREY, D./IRLE, M. (Hrsg.), *Theorien der Sozialpsychologie*, Bd. I., Bern.
- FREY, D., STREICHER, B. & AYDIN, N. (2012): Center of Excellence Kulturen sowie professionelle ethikorientierte Führung als Voraussetzung für ökonomischen Erfolg, aus: GROTE, S. (Hrsg.), *Die Führung der Zukunft*, Berlin.
- GIACOLONE, R. & KNOUSE, S. (1990): Justifying wrongful employee behavior: The role of personality in organizational sabotage, aus: *Journal of Business Ethics*. 9, 55–61.
- GPRA-Vertrauensindex (2015): Sippenhaft für deutsche Automobilbauer – VW belastet Vertrauen in die deutsche Automobilindustrie, aus: <https://www.gpra.de/gpra-vertrauensindex/sippenhaft-fuer-deutsche-automobilbauer-vw-belastet-vertrauen-in-die-deutsche-automobilindustrie/>, zuletzt überprüft am 22.8.2023.
- GRANOVETTER, M. (1973): The Strength of Weak Ties, aus: *American Journal of Sociology*, Heft 6/1973.
- GREENBERG, J. (1990), Employee Theft as a Response to Underemployment Inequity: The Hidden Cost of Pay Cuts, aus: *Journal of Applied Psychology*, Heft 5/1990.
- GREVE, G. (2010): Organizational Burnout, das versteckte Phänomen ausgebrannter Organisationen, Wiesbaden.
- HAUSKNECHT, J. P., DAY, D. V., & THOMAS, S. C. (2004): Applicant reactions to selection procedures: An updated model and meta-analysis, aus: *Personnel Psychology*, Heft 3/2004.
- HECKER, F. (2012): *Management-Philosophie*, Wiesbaden.

- HIRSCHI, T., & GOTTFREDSON, M. (1993): Commentary: Testing the General Theory of Crime, aus: *Journal of Research in Crime and Delinquency*, Heft 1/1993.
- HOMANN, K., & SUCHANEK, A. (2005): *Ökonomik, eine Einführung*, Tübingen.
- JUDGE, T.A., LOCKE, E.A., DURHAM, C.C., KLUGER, A.N. (1998): Dispositional effects on job and life satisfaction: the role of core evaluations, aus: *The Journal of Applied Psychology*, 83, 17–34.
- JUDGE, T.A., PICCOLO, R. F., & KOSALKA, T. (2009): The bright and dark sides of leader traits: A review and theoretical extension of the leader trait paradigm, aus: *Leadership Quarterly*, Heft 6/2009
- Kaptein, M. (2008): Developing a measure of unethical behavior in the workplace: A stakeholder perspective, aus: *Journal of management*, Heft 5/2008.
- KASCHUBE, J. & GASTEIGER, R.M. (2005): Eigenverantwortung im Spannungsfeld von Organisation und Individuum, aus: *Gruppendynamik und Organisationsberatung*, Heft 2/2005
- KASCHUBE, J. (2006): Eigenverantwortung – eine neue berufliche Leistung, Göttingen.
- KOCH, S. (2005): Berufliches Selbstkonzept und eigenverantwortliche Leistung, aus: *Gruppendynamik und Organisationsberatung*, Heft 2/2005
- KOHLBERG, L. (1984): Moral stages and moralization: The cognitive developmental approach, aus: KOHLBERG, L. (Hrsg.), *The psychology of moral development: the nature and validity of moral stages*, San Francisco.
- LEWIN, K. (1951): Field theory in social science, aus: CARTWRIGHT, D. (Hrsg.), *selected theoretical papers*, New York.
- Managermagazin, (2008): Imageprofile 2008, Olympiade der Konzerne, retrieved from <https://www.managermagazin.de/unternehmen/imageprofile/a-530209.html>
- MARCUS, B., & SCHULER, H. (2004): Antecedents of Counterproductive Behavior at Work: A General Perspective, aus: *Journal of Applied Psychology*, Heft 4/2004.
- MARCUS, B., LEE, K., & ASHTON, M. C. (2007): Personality dimensions explaining relationships between integrity tests and counterproductive behavior: Big Five, or one in addition?, aus: *Personnel Psychology*, Heft 60/2007.
- MARINKO, M. J., GUNDLACH, M. J., & DOUGLAS, S. C. (2002): Toward an Integrative Theory of Counterproductive Workplace Behavior: A Causal Reasoning Perspective, aus: *International Journal of Selection and Assessment*, Heft 1/2, 2002.
- MCBARNET, D. (2006): After Enron will ‘Whiter than White Collar Crime’ Still Wash? aus: *The British Journal of Criminology*, Volume 46, Issue 6, November 2006, Pages 1091–1109
- MCCAULEY, C. (1989): The Nature of Social Influence in Groupthink: Compliance and Internalization, aus: *Journal of Personality and Social Psychology*, Heft 2/1989.
- MOLINER, C. MARTÍNEZ-TUR, V., PEIRÓ, J. M., RAMOS, J., CROPANZANO, R. (2005): Relationships Between Organizational Justice and Burnout at the Work-Unit Level, aus: *International Journal of Stress Management*, Heft 2, 2005.
- MORRISON, E. W., & ROBINSON, S. L. (1997): When Employees feel Betrayed: A Model of how Psychological Contract Violation Develops, aus: *Academy of Management Review*, Heft 1/1997.
- MOSER, K. (1995): Vergleich unterschiedlicher Wege der Gewinnung neuer Mitarbeiter, aus: *Zeitschrift für Arbeits- und Organisationspsychologie*, Heft 3/1995.
- NERDINGER, F. W. (2008): Unternehmensschädigendes Verhalten erkennen und verhindern, Göttingen.
- NERDINGER, F. W., BLICKLE, G., & SCHAPER, N. (2011): *Arbeits- und Organisationspsychologie*, Berlin Heidelberg.
- NESTLER, C., & ENGELMANN, A. (2022): PwC’s Global Economic Crime and Fraud Survey.

- O'BOYLE JR., E. H.; FORSYTH, D. R.; BANKS, G. C. & MCDANIEL, M. A. (2012): A meta-analysis of the Dark Triad and work behavior: A social exchange perspective, aus: *Journal of Applied Psychology*, Heft 3/2012
- PADILLA, A., HOGAN, R. and KAISER, R.B. (2007): The Toxic Triangle: Destructive Leaders, Susceptible Followers and Conducive Environments, aus: *The Leadership Quarterly*, 18, 176–194.
- PAINÉ, L. S. (1994): Managing for Organizational Integrity, aus: *Harvard Business Review*, Heft 3/1994.
- PAULHUS, D.L. & WILLIAMS, K.M. (2002): The Dark Triad of personality: Narcissm, Machiavellism, and psychopathy, aus: *Journal of research in personality*, Heft 6/2002
- PENNEY, L. M., & SPECTOR, P. E. (2002): Narcissism and counterproductive work behavior: Do bigger egos mean bigger problems? *International Journal of Selection and Assessment*, Heft 10/2002.
- PETERMANN, F. (1998): Eine Einführung in die Themenbereiche, aus: PETERMANN, F. (Hrsg.), *Compliance und Selbstmanagement*, Göttingen.
- PÜTZ, L. (2011): Compliance, Eine Einführung in die Thematik, aus: *Arbeitshilfe für Aufsichtsräte*, Heft 15/2011.
- Quast, V. (2019): Messbarkeit von Compliance im Unternehmen, aus: *Recht relevant. für Compliance Officers*. Heft 3/2019.
- ROBINSON, S. L., & BENNETT, R. J. (1995): A typology of deviant work behaviors: A multi-dimensional scaling study, aus: *Academy of Management Journal*, Heft 2, 1995.
- SCHEIN, E. H. (1995): Unternehmenskultur. Ein Handbuch für Führungskräfte, Frankfurt a.M.
- SCHLENKER, B. R., BRITT, T. W., PENNINGTON, J., MURPHY, R., & DOHERTY, K. (1994): The Triangle Model of Responsibility, aus: *Psychological Review*, Heft 4/1994.
- SCHULZ-HARDT, S. & FREY, D. (2000): Gelernte Sorglosigkeit als Zukunftshemmnis: Wenn das Management rosa-rot sieht, aus: MÖLLER, S. (Hrsg.), *Psychologie und Zukunft*, Göttingen.
- SCHWEITZER, M. E., ORDÓÑEZ, L., & DOUMA, B. (2004): Goal setting as a moderator of unethical behavior, aus: *Academy of Management Journal*, Heft 3/2004.
- SKARICKI, D. P., & FOLGER, R. (1997): Retaliation in the Workplace: The Roles of Distributive, Procedural, and Interactional Justice, aus: *Journal of Applied Psychology*, Heft 3/1997.
- SPECTOR, P. E., & FOX, S. (2005): The Stressor-Emotion Model of Counterproductive Work Behavior, aus: FOX, S./SPECTOR, P.E. (Hrsg.), *Counterproductive work behavior: Investigations of actors and targets*, Washington DC.
- SPITZMÜLLER, C., & STANTON, J. M. (2006): Examining employee compliance with organizational surveillance and monitoring, aus: *Journal of Occupational and Organizational Psychology*, Vol. 79/2006.
- STESSL, A. (2012): Effektives Compliance Management in Unternehmen, Wiesbaden.
- THIELEMANN, U. (2005): Compliance und Integrity - Zwei Seiten ethisch integrierter Unternehmenssteuerung, aus: *Zeitschrift für Wirtschaft und Unternehmensethik*, Heft 6/2005.
- TREVINO, L. K. (1986): Ethical Decision Making in Organizations: A Person-situation Interactionist Model, aus: *Academy of Management Review*, Heft 11/1986.
- TURNER, M. E., & PRATKANIS, A. R. (1998): Twenty-Five Years of Groupthink Theory and Research: Lessons from the Evaluation of a Theory, aus: *Organizational Behavior and Human Decision Processes*, Heft 2/3, 1998.
- TYLER, T.R. (2005): Promoting Employee Policy Adherence and Rule Following in Work Settings: The Value of Self-Regulatory Approaches, *Brooklyn Law Review*, Heft 4/2005. (Retrieved from http://digitalcommons.law.yale.edu/fss_papers)
- TYLER, T.R. (2006): Self-sacrifice and Self-interest, aus: RHODE, D.L. (Hrsg.), *Moral Leadership*, San Francisco.

- VAN KNIPPENBERG, D., & SCHIPPERS, M. C. (2007): Work Group Diversity, aus: The Annual Review of Psychology, Heft 1/2007.
- VARDI, Y., & WIENER, Y. (1996): Misbehavior in Organizations: A Motivational Framework, aus: Organization Science, Heft 2, 1996.
- WANEK, J.E., SACKETT, P.R. & ONES, D.S. (2003): Towards an understanding of integrity test similarities and differences: An item-level analysis of seven tests, aus: Personnel Psychology, Heft 4/2003.
- WESCHE, J. S., MAY, D., PEUS, C., & FREY, D. (2010): Leadership corruption: Influence factors, process, and prevention, aus: B. Schyns & T. Hansbrough (Hrsg.), When leadership goes wrong: Destructive leadership, mistakes, and ethical failures (pp. 305–353). IAP Information Age Publishing.
- ZHAO, H., WAYNE, S. J., GLIBKOWSKI, B. C., & BRAVO, J. (2007). The impact of psychological contract breach on workrelated outcomes: A meta-analysis. *Personnel Psychology*, 60(3), 647–680.
- ZIMBARDO, P. G. & GERRIG R. J. (1999): Psychologie, Berlin.



Dr. Silja Kennecke arbeitet als Head of People & Culture in einer Unternehmensberatung sowie freiberuflich als Trainerin, Coach und Dozentin. Sie studierte Psychologie mit Nebenfach Betriebswirtschaftslehre an der Universität Heidelberg und der Cornell University (Ithaca, New York). Nach Abschluss ihres Studiums 2011 arbeitete sie als wissenschaftliche Mitarbeiterin am Institut für Führung und Personalmanagement der Universität St. Gallen und promovierte 2016 am LMU Center for Leadership and People Management unter der Leitung von Prof. Dieter Frey.



Arbeitsrechtliche Implementierung von Compliance in Unternehmen

11

Andreas Katzer

Inhaltsverzeichnis

11.1	Grundlagen	282
11.1.1	Arbeitsrecht und Compliance	282
11.1.2	Pflichten von Arbeitgebern	283
11.1.3	Compliance-Management-System (CMS)	284
11.2	Implementierung	285
11.2.1	Compliance-Pflichten als arbeitsvertragliche Nebenpflichten	285
11.2.2	Gestaltungsinstrumente	286
11.2.2.1	Direktionsrecht	286
11.2.2.1.1	Inhalt und Umfang des Direktionsrechts	286
11.2.2.1.2	Rechtliche Anforderungen	286
11.2.2.1.3	Vor- und Nachteile	287
11.2.2.2	Arbeitsvertrag	287
11.2.2.2.1	Rechtliche Anforderungen	287
11.2.2.2.2	Vor- und Nachteile	288
11.2.2.2.3	Änderungskündigung	289
11.2.2.3	Betriebsvereinbarung	289
11.2.2.3.1	Allgemeines	289
11.2.2.3.2	Vor- und Nachteile	290
11.2.2.4	Regelungsabrede und Tarifvertrag	291
11.2.2.5	Unternehmensstrategie	292

Ausschließlich aufgrund besserer Lesbarkeit des vorliegenden Beitrags wird die männliche sprachliche Form verwendet. Selbstverständlich ist damit keine wie auch immer geartete Diskriminierung verbunden.

A. Katzer (✉)

Sonntag & Partner, Augsburg, Deutschland
E-Mail: andreas.katzer@sonntag-partner.de

11.2.3	Mitbestimmung des Betriebsrats bei der Implementierung	293
11.2.4	Dokumentation und Kommunikation	294
11.3	Allgemeines Gleichbehandlungsgesetz (AGG)	295
11.3.1	Grundsätze	295
11.3.2	Pflichten von Arbeitgebern	297
11.3.3	Rechte von Arbeitnehmern	297
11.4	Überwachung und Sanktionierung	298
11.4.1	Allgemeines	298
11.4.2	Überwachung des Arbeitnehmers durch den Arbeitnehmer	298
11.4.3	Interne Ermittlungen im Verdachtsfall	299
11.4.4	Whistleblowing	300
11.4.5	Compliance-Beauftragter	300
11.4.6	Maßnahmen bei Verstößen von Arbeitnehmern und Arbeitgebern	301
11.4.7	Verwertung vor Gericht	302
11.5	Exkurs: Gesetz zum Schutz von Geschäftsgeheimnissen	302
11.6	Mitarbeiterdatenschutz	304
11.6.1	Grundsätze	304
11.6.2	Erlaubte Datenverarbeitungen im Arbeitsverhältnis	305
11.6.2.1	Erfüllung eines Vertrags, Art. 6 Abs. 1 lit. b DSGVO	305
11.6.2.2	Wahrung berechtigter Interessen, Art. 6 Abs. 1 lit. f DSGVO	305
11.6.2.3	Aufdeckung von Straftaten, § 26 Abs. 1 S. 2 BDSG	306
11.6.2.4	Einwilligung als Rechtsgrundlage für Datenverarbeitungen regelmäßig untauglich	307
11.6.2.5	Kollektivvereinbarungen, § 26 Abs. 4 BDSG	307
11.6.2.6	Zweckänderung	307
11.6.2.7	Umgang mit besonderen Kategorien personenbezogener Daten	308
11.6.2.8	Pflichten von Arbeitgebern vor und bei der Durchführung von Überwachungsmaßnahmen	309
11.6.3	Rechte und Pflichten des Betriebsrats	310
11.6.4	Besondere Falkonstellation: Datenschutz im Home-Office	311
11.6.5	Haftung und Sanktionen bei Verstößen	312
Literatur		313

11.1 Grundlagen

11.1.1 Arbeitsrecht und Compliance

Compliance hat als wesentlicher Bestandteil modernder Unternehmensstrukturen zahlreiche Berührungspunkte mit dem Arbeitsrecht. Bei der Implementierung, Überwachung und durch Setzung von Compliance-Systemen geht es stets um die Festlegung und Umsetzung von bestimmten Verhaltenspflichten des Arbeitnehmers.¹ Das Verhältnis von Arbeitsrecht und Compliance lässt sich dabei als ambivalent bezeichnen: Einerseits sollen Com-

¹ Mengel, Compliance, § 1 Rn. 10.

pliance-Vorschriften sicherstellen, dass sich ein Unternehmen selbst bzw. dessen Mitarbeiter regelkonform verhalten, um mögliche Schäden und Haftungsrisiken von dem Unternehmen abzuwenden. Andererseits darf der damit bezweckte Schutz des Unternehmens nicht dazu führen, dass die Schutzfunktion des Arbeitsrechts zulasten der Arbeitnehmer unterlaufen wird. Insbesondere bei der Implementierung und Überwachung von Compliance-Maßnahmen dürfen die Rechte des Arbeitnehmers nicht unzulässig eingeschränkt werden; Compliance muss schließlich selbst „compliant“ sein.

Die Berührungspunkte zwischen Compliance und Arbeitsrecht verdichten sich vor diesem Hintergrund zu drei Aspekten: Erstens sind aus der Perspektive des Arbeitgebers mehrere Materien des Arbeitsrechts, namentlich das Arbeitszeitgesetz oder das Arbeitsschutzgesetz, Gegenstand von Compliance-Vorschriften. Werden zwingende Regeln des Arbeitsschutzes nicht eingehalten, kann der Arbeitgeber mit Bußgeldern oder strafrechtlichen Konsequenzen sanktioniert werden.²

Zweitens liefert das Arbeitsrecht die zur Implementierung von Compliance-Vorschriften wesentlichen Gestaltungsinstrumente (Arbeitsvertrag, Direktionsrecht und Betriebsvereinbarung). Dadurch können unternehmensinterne Verhaltenspflichten („Code of Ethics“) für den einzelnen Arbeitnehmer individual- oder kollektivrechtlich verbindlich gemacht werden.

Drittens stellen die Rechte der Arbeitnehmer wie gesehen eine wichtige Grenze bei der Ausgestaltung und Durchsetzung von Compliance-Maßnahmen dar.

11.1.2 Pflichten von Arbeitgebern

Anders als das anglo-amerikanische Recht kennen weder das europäische noch das deutsche Recht eine einheitliche Compliance-Gesetzgebung. Soweit sich US-amerikanische Gesetze nicht ausnahmsweise auf international tätige deutsche Unternehmen auswirken (wie etwa der Sarbanes-Oxley-Act oder der Foreign Corrupt Practices Act), greifen daher allenfalls punktuelle Regelungen in unterschiedlichen Rechtsgebieten. Dazu zählen insbesondere das Bilanzrecht, das Bank- und Kapitalmarktrecht sowie das Kartellrecht.³ Von hoher Relevanz sind auch die in der Whistleblowing-Richtlinie der EU vorgesehenen und im Hinweisgeberschutzgesetz umzusetzenden Compliance-Vorschriften (siehe Abschn. 11.4.4).

Darüber hinaus können Unternehmensleitungen gesellschaftsrechtlich dazu verpflichtet sein, zur Einhaltung der für das Unternehmen geltenden zwingenden Vorschriften (vgl. § 93 Abs. 1 des Aktiengesetzes (AktG)) geeignete Überwachungssysteme einzuführen, sog. Corporate Governance. Demnach kann das Unterlassen der Implementierung eines solchen Compliance-Systems seitens des Vorstandes einer Aktiengesellschaft einen haftungsauslösenden Gesetzesverstoß (§ 93 Abs. 1 AktG) darstellen, wenn die konkrete

² Mengel, Compliance, § 1 Rn. 10.

³ Vgl. Hauschka NJW 2004, 257 (258).

Gefährdungslage des Unternehmens eine solche Maßnahme erforderlich macht.⁴ Sowohl eine zivilrechtliche als auch eine strafrechtliche Haftung steht dabei aber unter dem Vorbehalt, dass der Vorstand bei einer unternehmerischen Entscheidung vernünftigerweise nicht mehr annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln (sog. business judgement rule).

Eine vergleichbare Verpflichtung der Unternehmensleitung kennt schließlich auch das Ordnungswidrigkeitsrecht. Gemäß § 130 des Ordnungswidrigkeitsgesetzes (OWiG) hat die Unternehmensleitung dafür zu sorgen, dass innerhalb des Unternehmens nicht gegen Gesetze bzw. Verhaltenspflichten verstoßen wird, die den Inhaber betreffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist. Dies umfasst ggf. auch die Einführung und Durchsetzung effektiver Präventionssysteme.⁵

Eine allgemeine Pflicht des Arbeitgebers zur Einführung eines umfassenden Compliance-Management-Systems besteht dagegen grundsätzlich nicht; insbesondere ist der Arbeitgeber aus arbeitsrechtlichen Gründen nicht generell dazu verpflichtet, potenziellen Gesetzesverstößen seiner Arbeitnehmer vorzubeugen und solche ggf. arbeitsrechtlich zu sanktionieren.⁶

11.1.3 Compliance-Management-System (CMS)

Bei der Compliance-Organisation sind die drei Phasen der Implementierung von Compliance-Strukturen, der Überwachung der eingeführten Regeln, sowie die Sanktionierung von Regelverstößen zu unterscheiden.⁷ Im Rahmen der ersten beiden Phasen empfiehlt sich die Arbeit mit einem Compliance-Management-System (CMS). Zwar besteht gerade für kleinere Unternehmen keine generelle gesetzliche Verpflichtung zur Einführung umfassender CMS. Gleichwohl erleichtert ein wirksames CMS die Aufdeckung gesetzeswidrigen Verhaltens und kann damit auch in kleineren Unternehmen unangenehme Rechtsfolgen vermeiden.⁸

Ein CMS muss unternehmensspezifisch und präventiv ausgerichtet sein. Es existiert weder „das“ eine Compliance-System noch „die“ eine Variante zur Realisierung von Compliance; entscheidend ist nur, dass das unternehmerische Konzept hinreichend effektiv ist und auf die Bedürfnisse des Unternehmens abgestimmt ist. Zwingend erforderlich ist vor diesem Hintergrund, dass das CMS auf einer kontinuierlichen und individuellen Risikoanalyse basiert, sodass bei vorhandenen oder drohenden Schadensfällen ggf. ein besonders aufwendiges Compliance-Konzept erforderlich ist. Alle Präventionsmaßnahmen und sons-

⁴Vgl. LG München I, NZG 2014, 345.

⁵Heißner/Benecke, BB 2013, 2923.

⁶Handbuch Corporate Compliance/Pelz, § 5 Rn. 2; Schaefer/Baumann, NJW 2011, 3601 (3603).

⁷SWK-Arbeitsrecht/Mengel, „Compliance“, Rn. 4.

⁸Kempter/Steinat, NZA 2017, 1505.

tigen CMS-Bestandteile müssen stets darauf abzielen, die im Rahmen der Risikoanalyse festgestellten Risiken zu reduzieren.⁹

Um zu vermeiden, dass die Compliance selbst „incompliant“ wird, ist aber darauf zu achten, dass insbesondere die Rechte und Interessen der betroffenen Arbeitnehmer nicht unzulässig beeinträchtigt werden.

11.2 Implementierung

Die Phase der Implementierung umfasst die Einführung und Durchsetzung konkreter Compliance-Maßnahmen. Soweit sich diese nicht ausnahmsweise im Vorfeld des Arbeitsverhältnisses abspielen (z. B. das präventive Mitarbeiter-Screening), ist zu klären, ob sich entsprechende Verhaltenspflichten des Arbeitnehmers bereits aus dem bestehenden Arbeitsvertrag ergeben (Abschn. 11.2.1) und inwieweit eine Durchsetzung mit arbeitsrechtlichen Gestaltungsinstrumenten erforderlich und zweckdienlich ist (Abschn. 11.2.2).

11.2.1 Compliance-Pflichten als arbeitsvertragliche Nebenpflichten

Eine spezielle Implementierung von Compliance-Vorschriften ist rechtlich nicht zwingend notwendig, soweit inhaltsgleiche Verhaltenspflichten des Arbeitnehmers bereits aus dem Arbeitsvertrag resultieren. Anerkannt ist, dass neben den explizit geregelten Hauptpflichten auch ungeschriebene arbeitsvertragliche Nebenpflichten bestehen, die das Arbeitsverhältnis insgesamt prägen. Dazu zählen etwa die Fürsorge- und Schutzpflicht des Arbeitgebers, sowie die Geheimhaltungspflichten und das Wettbewerbsverbot auf Seiten des Arbeitnehmers. Compliance-relevant sind ferner die Pflicht zur Wahrung der betrieblichen Ordnung, die Pflicht zur Vermeidung von Interessenskonflikten und die Pflicht zur Anzeige von drohenden Schäden.¹⁰

Problematisch ist allerdings, dass zahlreiche dieser ungeschriebenen Regeln dem Arbeitnehmer unbekannt sind oder zumindest deren praktische Anwendung im konkreten Betrieb zweifelhaft ist. Die Arbeitsgerichte nehmen in der Praxis regelmäßig eine Abwägung der widerstreitenden Interessen im Einzelfall vor, deren Ergebnis sich nicht mit Sicherheit vorhersehen lässt.¹¹ Rechtssicherheit erlangen Arbeitgeber und Arbeitnehmer daher nur, wenn die ungeschriebenen Compliance-Regeln gegenüber dem einzelnen Arbeitnehmer bzw. im einzelnen Betrieb ausgefüllt und fixiert werden.¹²

Entscheidendes Gestaltungsinstrument ist insoweit das Direktionsrecht des Arbeitgebers nach § 106 der Gewerbeordnung (GewO).

⁹ Schulze in: Kramer, IT-Arbeitsrecht, Rn. 1097 ff.; vgl. BGH NZWiSt 2018, 379.

¹⁰ Hohmuth, BB 2014, 3061 (3062); vgl. Kempter/Steinat, NZA 2017, 1505 (1507 ff.).

¹¹ Hohmuth, BB 2014, 3061, 3062.

¹² Mengel, Compliance, § 1 Rn. 12.

11.2.2 Gestaltungsinstrumente

11.2.2.1 Direktionsrecht

11.2.2.1.1 Inhalt und Umfang des Direktionsrechts

Die erste Option eines Arbeitgebers ist es, von seinem Direktionsrecht (§ 106 GewO) Gebrauch zu machen und entsprechende Weisungen an seine Arbeitnehmer zu erteilen. Gemäß § 106 GewO kann der Arbeitgeber Inhalt, Ort und Zeit der Arbeitsleistung nach billigem Ermessen näher bestimmen, soweit diese Arbeitsbedingungen nicht durch den Arbeitsvertrag, Bestimmungen einer Betriebsvereinbarung, eines anwendbaren Tarifvertrages oder gesetzliche Vorschriften festgelegt sind. Soweit die Grenzen des Weisungsrechts beachtet werden, sind die Weisungen für den Arbeitnehmer verbindlich; weigert er sich diese umzusetzen, kann der Arbeitgeber Sanktionen bis hin zur Kündigung verhängen. Die Ausübung des Direktionsrechts sollte dabei aus Nachweisgründen stets schriftlich erfolgen.

Das Weisungsrecht erstreckt sich nicht nur auf das Verhalten des Arbeitnehmers bei der Erbringung seiner Arbeitsleistung („Arbeitsverhalten“), sondern auch auf Ordnung und Verhalten des Arbeitnehmers im Betrieb („Ordnungsverhalten“, § 106 S. 2 GewO), wobei hier regelmäßig ein besonderes Mitbestimmungsrecht des Betriebsrats zu beachten ist (§ 87 Abs. 1 Nr. 1 des Betriebsverfassungsgesetzes (BetrVG)).

Der Arbeitgeber kann dabei aber nur bereits bestehende arbeitsvertragliche Pflichten konkretisieren und ausfüllen. Durch Weisungen kann er keine neuen Pflichten für den Arbeitgeber schaffen. Die Implementierung von Compliance-Vorschriften durch die Erteilung von einseitigen Weisungen kommt damit nur dann in Betracht, wenn entsprechende Pflichten bereits Inhalt des bestehenden Arbeitsverhältnisses sind.¹³

11.2.2.1.2 Rechtliche Anforderungen

Im Übrigen ist hinsichtlich der rechtlichen Anforderungen an konkretisierende Weisungen zwischen drei Sphären zu unterscheiden: Tätigkeitsbezogene Weisungen können in der Regel vom Arbeitgeber erteilt werden, weil sie unmittelbar die vom Arbeitgeber zu erbringende Hauptleistungspflicht betreffen. Sie bilden den Kernbereich des arbeitgeberseitigen Weisungsrechts ab. Bei verhaltensbezogenen Weisungen ist wiederum zu unterscheiden: Regelungen, die sich nicht nur auf konkretisierbare Nebenpflichten des Arbeitgebers, sondern auch auf sein sonstiges Verhalten beziehen, können nur bei hinreichend gewichtigen Gründen des Arbeitgebers berücksichtigt werden. Problematisch sind dagegen Weisungen, mit denen allein das außerdienstliche Verhalten des Arbeitnehmers geregelt werden soll. Solche Regelungen sind nur ausnahmsweise zulässig, wenn sie einen konkreten Bezug zur geschuldeten Tätigkeit aufweisen und die Interessen des Arbeitgebers die grundrechtlich geschützten Belange des Arbeitnehmers wesentlich überwiegen.¹⁴

¹³ Hohmuth, BB 2014, 3061 (3063).

¹⁴ Mengel, Compliance, § 1 Rn. 8.

Unabhängig davon, welche der drei Sphären von einer Weisung des Arbeitgebers betroffen ist, ist bei der Ausübung des Direktionsrechts stets die Grenze des „billigen Ermessens“ zu beachten (§ 315 BGB; § 106 GewO). Maßgeblich ist insofern eine umfassende Abwägung der beiderseitigen Interessen, wobei zugunsten des Arbeitgebers etwaige Verpflichtungen zur Einführung von Compliance-Vorschriften (vgl. etwa § 80 WpHG), zugunsten des Arbeitnehmers seine Handlungsfreiheit und sein allgemeines Persönlichkeitsrecht zu berücksichtigen sind.¹⁵

11.2.2.1.3 Vor- und Nachteile

Ein Vorteil der Einführung von Compliance-Vorschriften durch die Ausübung des arbeitgeberseitigen Direktionsrechts liegt vor allem in der damit verbundenen Flexibilität. Der Arbeitgeber kann – sei es gegenüber der gesamten Belegschaft, sei es gegenüber einzelnen Arbeitnehmern – konkretisierende Verhaltenspflichten einseitig einführen, ohne dass eine Zustimmung der Arbeitnehmer erforderlich ist.¹⁶ Bei Bedarf kann er seine erteilten Weisungen auch jederzeit wieder einseitig abändern, wobei freilich auch hier etwaige Mitbestimmungsrechte des Betriebsrats zu beachten sind (§ 87 Abs. 1 BetrVG).

Der zentrale Nachteil dieser Gestaltungsvariante liegt auf der Hand: Weil das Weisungsrecht keine neuen Verhaltenspflichten des Arbeitnehmers begründen, sind die einseitigen Handlungsmöglichkeiten des Arbeitgebers stark eingeschränkt. Dies gilt umso mehr, als hinsichtlich der Frage, welche konkreten Compliance-Vorschriften bereits aus dem Arbeitsverhältnis hergeleitet werden können, Rechtsunsicherheit besteht. Stellt die Weisung keine Konkretisierung, sondern eine Erweiterung der arbeitsrechtlichen Pflichten dar, so kommt ihr jedoch keine rechtliche Bindungswirkung zu. Des Weiteren besteht ein Nachweisproblem, wenn der Arbeitgeber seine einseitigen Weisungen nicht schriftlich dokumentiert. Schließlich darf die einseitige Auferlegung bestimmter Compliance-Pflichten keine grundrechtlichen Positionen des Arbeitnehmers verletzen; insbesondere bei Weisungen, die (auch) das außerdienstliche Verhalten betreffen, sind erhöhte Rechtfertigungsanforderungen zu beachten. Auch insofern fehlt es dem Arbeitgeber an Rechtssicherheit.

11.2.2 Arbeitsvertrag

11.2.2.2 Rechtliche Anforderungen

Angesichts des begrenzten Umfangs des arbeitgeberseitigen Weisungsrechts (§ 106 GewO), kommt im Hinblick auf die Neuregelung oder Erweiterung von Verhaltenspflichten eine entsprechende Vereinbarung im Arbeitsvertrag in Betracht. In dem Arbeitsvertragsmuster kann der Arbeitgeber eine Einbeziehung von Compliance-Regelungen vorsehen. Um eine Überfrachtung des Arbeitsvertrages zu vermeiden, bietet es sich dabei an,

¹⁵ SWK-Arbeitsrecht/Mengel, „Compliance“, Rn. 8.

¹⁶ Kempter/Steinat, NZA 2017, 1505 (1510).

den Verhaltenskodex in einem separaten Dokument zu regeln, auf das im Arbeitsvertrag im Wege einer statischen Verweisung Bezug genommen wird.¹⁷

Die Implementierung von Compliance-Vorschriften im Wege arbeitsvertraglicher Regelungen begegnet jedoch erhöhten rechtlichen Anforderungen:

Zum einen unterliegen grundsätzlich sowohl die Regelungen des Arbeitsvertrages selbst als auch der in Bezug genommene Verhaltenskodex der AGB-Kontrolle (§§ 305 ff. BGB). Im Rahmen des § 307 Abs. 1 BGB sind dabei die grundrechtlichen Belange der Parteien umfassend gegeneinander abzuwägen. Wie bei der Ausübung des Direktionsrechts (§ 106 GewO) gilt aber, dass die Rechtfertigungsanforderungen gegenüber dem Arbeitgeber umso höher sind, je weiter sich die eingeführten oder abgeänderten Compliance-Regelungen von der eigentlichen Arbeitspflicht entfernen. Ob und inwieweit auch Erwartungen von Geschäftspartnern oder Dritten, wie etwa der New Yorker Börse, die Einführung bzw. Neuregelung von Compliance-Regelungen rechtfertigen kann, ist nicht geklärt. Nach geltender Rechtslage dürften solche Gründe aber jedenfalls nur in Ausnahmefällen zugunsten des Arbeitgebers zu berücksichtigen sein.¹⁸

Zum anderen kann eine Änderung bestehender arbeitsvertraglicher Pflichten nicht ohne die Zustimmung des Arbeitnehmers erfolgen, weil der Abschluss eines Änderungsvertrages nach allgemeinen Grundsätzen zwei übereinstimmende Willenserklärungen voraussetzt. Während die Einbeziehung von Compliance-Vorschriften im Rahmen des Neuabschlusses eines Arbeitsvertrages nicht besonders problematisch ist, stößt die Einführung im Wege einer Neuregelung gerade in größeren Unternehmen auf praktische Hindernisse. Bereits der organisatorische Aufwand, der mit der Änderung jedes einzelnen Arbeitsvertrages einhergeht, ist immens. Darüber besteht seitens des Arbeitnehmers keine Pflicht zum Abschluss eines Änderungsvertrages; verweigert er seine Zustimmung, kommt eine vertragliche Änderung nicht zustande.¹⁹ Von einer konkludenten Annahme eines Änderungsangebots durch das schlichte Weiterarbeiten im Betrieb kann nach der Rechtsprechung nur in seltenen Ausnahmefällen ausgegangen werden.²⁰

11.2.2.2 Vor- und Nachteile

Ein formeller Vorteil bei der Einführung bzw. Neuregelung von Compliance-Vorschriften durch eine arbeitsvertragliche Einigung liegt darin, dass diese – anders als die Ausübung des arbeitgeberseitigen Direktionsrechts – regelmäßig in der Schriftform erfolgt. Die Implementierung kann damit erforderlichenfalls vor Gericht nachgewiesen werden. Des Weiteren steigt die Akzeptanz der Mitarbeiter, wenn Compliance-Vorschriften nicht einseitig auferlegt, sondern individualvertraglich vereinbart werden. Zwar handelt es sich insoweit freilich um vorformulierte Vertragsbedingungen, die vom Arbeitgeber gestellt werden;

¹⁷ Hohmuth, BB 2014, 3061 (3061); Mengel, Compliance, § 1 Rn. 49.

¹⁸ Hohmuth, BB 2014, 3061, (3063).

¹⁹ Schreiber, NZA-RR 2010, 617 (623); vgl. Mengel, Compliance, § 1 Rn. 70.

²⁰ Schreiber, NZA-RR 2010, 617 (618); vgl. BAG NZA 1986, 474 (475).

gleichwohl kommt eine vertragliche Änderung nur mit der Zustimmung des Arbeitnehmers zustande.²¹

Weil die Einführung mittels arbeitsvertraglicher Regelungen die Zustimmung jedes einzelnen Arbeitgebers erfordert, eignet sich diese Gestaltungsoption grundsätzlich nur im Rahmen des Neuabschlusses von Arbeitsverträgen oder bei der Änderung von Compliance-Vorschriften in kleineren Betrieben.

11.2.2.2.3 Änderungskündigung

Sofern ein Arbeitnehmer einer Änderung der arbeitsvertraglichen Compliance-Regelungen nicht zustimmt, stellt sich die Frage, ob der Arbeitgeber sein Ziel im Wege einer Änderungskündigung erreichen kann. Unter einer Änderungskündigung versteht man eine (ordentliche oder außerordentliche) Kündigung des Arbeitsverhältnisses, verbunden mit einem Angebot auf Abschluss eines neuen Arbeitsvertrages zu geänderten Bedingungen (vgl. § 2 KSchG).

Die Änderung der Arbeitsbedingungen muss gemäß § 1 Abs. 2 Satz 1 KSchG sozial gerechtfertigt sein. Dies ist nach überwiegender Auffassung jedoch nur dann der Fall, wenn der Arbeitgeber rechtlich zur Einführung entsprechender Compliance-Maßnahmen verpflichtet ist. Die Umsetzung von bloßen Empfehlungen oder das Interesse des Arbeitgebers an einer Vereinheitlichung der Arbeitsbedingungen stellen dagegen in der Regel keine „dringenden betrieblichen Erfordernisse“ im Sinne des § 1 Abs. 2 Satz 1 KSchG dar. Vor diesem Hintergrund kann der Arbeitgeber im Fall der Verweigerung des Einverständnisses seitens des Arbeitnehmers grundsätzlich nicht in zulässiger Weise auf das Mittel der Änderungskündigung zurückgreifen.²²

11.2.2.3 Betriebsvereinbarung

11.2.2.3.1 Allgemeines

Besteht im Unternehmen ein Betriebsrat, so kann die Implementierung von Verhaltenspflichten im Wege einer Betriebsvereinbarung erfolgen. Eine Betriebsvereinbarung ist ein Normenvertrag zwischen Arbeitgeber und Betriebsrat, dessen Regelungen unmittelbare und zwingende Wirkung auf die einzelnen Arbeitsverhältnisse haben, § 77 Abs. 2, 4 BetrVG.²³ Betriebsvereinbarungen sind gegenüber einzelvertraglichen Regelungen grundsätzlich vorrangig, es sei denn, die Regelungen des Arbeitsvertrages sind für den Arbeitnehmer günstiger (sog. Günstigkeitsprinzip).

Zu beachten ist, dass Betriebsvereinbarungen von mehreren Gremien der betrieblichen Mitbestimmung abgeschlossen werden können. Auf der Ebene des einzelnen Betriebs ist der gemäß § 1 BetrVG zu errichtende Betriebsrat für die Mitbestimmung zuständig. Bestehen in einem Unternehmen mehrere Betriebsräte, so kommt gemäß § 47 BetrVG die

²¹ Hohmuth, BB 2014, 3061.

²² Hohmuth, BB 2014, 3061, (3063).

²³ BeckOK ArbR/Werner BetrVG § 77 Rn. 9.

Errichtung eines Gesamtbetriebsrats in Betracht. Dieser ist zuständig für Belange, die das gesamte Unternehmen betreffen und daher nicht durch einen oder mehrere Betriebsräte auf der Betriebsebene geregelt werden können. Entsprechendes gilt, wenn ein Konzern (vgl. § 18 Abs. 1 AktG) mit mehreren Gesamtbetriebsräten besteht. Geht es um Belange, die einer übergeordneten Koordinierung bedürfen, ist der gemäß § 54 BetrVG zu errichtende Konzernbetriebsrat zuständig.

Vertragspartner des Arbeitgebers ist bei der Einführung von Compliance-Vorschriften regelmäßig der Gesamtbetriebsrat oder der Konzernbetriebsrat, weil Compliance-Regelungen möglichst einheitlich auf der Ebene des Unternehmens oder des Konzerns eingeführt werden sollen.

Der persönliche Geltungsbereich von Betriebsvereinbarungen wird durch § 5 BetrVG eingeschränkt, dem zufolge „Leitende Angestellte“ vom Anwendungsbereich des BetrVG ausgenommen sind. Solche Mitarbeiter sind demnach nicht an Compliance-Regelungen in Betriebsvereinbarungen gebunden. Soweit im Betrieb ein Sprecherausschuss existiert, kann der Arbeitgeber aber entsprechende Vereinbarungen mit diesem Gremium abschließen, die dann auch normative Wirkung für die Leitenden Angestellten entfalten. Alternativ kann der Arbeitgeber sich um eine individualvertragliche Einführung von Verhaltensvorschriften bemühen.²⁴

11.2.2.3.2 Vor- und Nachteile

Ein wesentlicher Vorteil der Implementierung von Compliance-Pflichten durch die Betriebsvereinbarung ist die damit verbundene Vereinfachung. Anders als bei der individualvertraglichen Vereinbarung besteht mit dem Betriebsrat nur ein Vertragspartner; die übrigen Arbeitnehmer sind grundsätzlich kraft der normativen Wirkung von Betriebsvereinbarungen an die getroffenen Compliance-Regelungen gebunden, ohne dass es hierzu ihrer individuellen Zustimmung bedürfte.

Ein weiterer Vorteil liegt darin, dass Betriebsvereinbarungen im Gegensatz zu arbeitsvertraglichen Regelungen keiner AGB-Kontrolle unterliegen (§ 310 Abs. 4 BGB). Das BAG unterwirft Betriebsvereinbarungen lediglich einer „Rechtskontrolle“, die insbesondere auf die Wahrung der Grundsätze der Gleichbehandlung und der Verhältnismäßigkeit bei der Ausgestaltung von Betriebsvereinbarungen gerichtet ist.²⁵

Ferner werden durch den Abschluss einer Betriebsvereinbarung auch etwaige Mitbestimmungsrechte des zuständigen Gremiums erfüllt. Eine Betriebsvereinbarung ist daher insoweit vorteilhaft, als umfassende Mitbestimmungsrechte des Betriebsrats zu beachten sind (vgl. § 87 Abs. 1 Nrn. 1, 6 BetrVG). Schließlich gilt auch hier, dass im Vergleich zur einseitigen Auferlegung von Verhaltenspflichten (§ 106 GewO) eine höhere Akzeptanz seines der Arbeitnehmer zu erwarten ist, wenn die Vorschriften durch die Arbeitnehmervertreter ausgehandelt worden sind.²⁶

²⁴ Mengel, Compliance, Rn. 71.

²⁵ Münchener Handbuch zum Arbeitsrecht/Arnold, Bd. 4, § 316 Rn. 129, 130.

²⁶ Mengel, Compliance, § 1 Rn. 81.

Die mit der normativen Wirkung von Betriebsvereinfachungen verbundene Vereinfachung des Implementierungsverfahrens führt allerdings zu erheblichen Flexibilitätseinbußen. Eine arbeitsvertragliche Erweiterung oder Änderung von Compliance-Pflichten ist grundsätzlich nicht mehr möglich, weil die Betriebsvereinbarung in ihrem Geltungsrang über den Regelungen des Arbeitsvertrages steht. Daher grundsätzlich selbst bei Zustimmung des Arbeitnehmers keine neuen Compliance-Vorschriften eingeführt werden, wenn nicht die Betriebsvereinbarung selbst geändert wird. Etwas anderes gilt nach dem „Günstigkeitsprinzip“ nur dann, wenn sich die arbeitsvertragliche Änderung als für den Arbeitnehmer vorteilhaft erweist.²⁷

Wenngleich das Günstigkeitsprinzip demnach eine vorteilhafte Abweichung von einer bestehenden Betriebsvereinbarung ermöglicht, kann es der Einführung neuer Compliance-Vorschriften auch entgegenstehen, wenn im Arbeitsvertrag bereits vorteilhaftere Regelungen existieren. Insoweit entfaltet die Betriebsvereinbarung keine normative Wirkung, weil die arbeitsvertraglichen Regelungen günstiger sind als die Vorschriften in der Betriebsvereinbarung.²⁸ Dies könnte sich insbesondere dann als problematisch erweisen, wenn sich nur in bestimmten Arbeitsverträgen günstigere Regelungen finden, sodass die Betriebsvereinbarung nur für einzelne Mitarbeiter zwingende Wirkung entfaltet. Das Günstigkeitsprinzip steht bei der Implementierung von Compliance-Vorschriften im Wege der Betriebsvereinbarung damit nicht nur in einem Spannungsverhältnis zum Flexibilisierungsinteresse des Arbeitgebers, sondern befindet sich auch in einem Zielkonflikt mit dem Interesse an einer einheitlichen Einführung der Verhaltensvorschriften.

Ein weiterer Nachteil dieser Gestaltungsvariante liegt schließlich darin, dass die Regelungskompetenz des Betriebsrats von seiner funktionellen Zuständigkeit abhängt: Es muss ein Bezug zum Betrieb (bzw. dem Unternehmen oder dem Konzern) und zu den Interessen der vom Betriebsrat vertretenen Arbeitnehmer bestehen. Regelungen, die das Arbeitsverhältnis unmittelbar als solches betreffen, sind dagegen unzulässig. Compliance-Regelungen zur Verschwiegenheit, zu Wettbewerbs- und Nebentätigkeitsverboten können damit beispielsweise nicht im Rahmen einer Betriebsvereinbarung geregelt werden.²⁹

11.2.2.4 Regelungsabrede und Tarifvertrag

Das kollektive Arbeitsrecht kennt als Mittel zur Gestaltung des Arbeitsverhältnisses weiterhin die Regelungsabrede und den Tarifvertrag, wobei im Ergebnis beide Instrumente nicht zur Implementierung von Compliance-Vorschriften geeignet sind.

Neben der gemäß § 77 Abs. 2 S. 1 BetrVG formbedürftigen Betriebsvereinbarung können Arbeitgeber und Betriebsrat auch formlose Vereinbarungen abschließen, die gemeinhin als Regelungsabrede oder Betriebsansprache bezeichnet werden. Einer darauf beruhenden Implementierung von Verhaltensvorschriften steht aber bereits entgegen, dass die zwingende Mitbestimmung des Betriebsrats (z. B. § 87 BetrVG) durch eine

²⁷ Mengel, Compliance, § 1 Rn. 86.

²⁸ Hohmuth, BB 2014, 3061, (3063).

²⁹ Richardi BetrVG/Richardi § 77 Rn. 54; BeckOK ArbR/Werner BetrVG § 77 Rn. 35.

Regelungsabrede nicht gewahrt wird. Außerdem entfaltet eine Regelungsabrede keine normative Wirkung, sodass die einzelnen Regelungen noch individualvertraglich umgesetzt werden müssen.³⁰

Eine tarifvertragliche Einführung von Compliance-Regelungen ist zwar rechtlich – auch mit unmittelbarer und zwingender Wirkung (§ 4 Abs. 1 TVG) – möglich, spielt in der Praxis aber keine Rolle. Compliance-Vorschriften sind nämlich typischerweise unternehmens- und konzernbezogen und daher kein geeigneter Regelungsgegenstand für Verbandstarifverträge, denen ein konkreter Zuschnitt auf die betriebs- oder unternehmensspezifischen Bedürfnisse wesensfremd ist.³¹

11.2.2.5 Unternehmensstrategie

Im Ergebnis stehen einem Unternehmen zur Implementierung von Compliance-Vorschriften in der Praxis die drei Instrumente Weisungsrecht, Arbeitsvertrag und Betriebsvereinbarung zur Verfügung. Wichtig ist es, die Vor- und Nachteile der jeweiligen Gestaltungsinstrumente unternehmensspezifisch im Hinblick auf die entwickelten Ethik-Richtlinien zu analysieren, um die für die Unternehmensinteressen beste Gestaltung zu ermitteln.

Dies setzt zuvorderst eine Prüfung der bereits bestehenden Compliance-Regelungen voraus. Zum einen hängt davon die Reichweite des arbeitgeberseitigen Weisungsrechts ab, weil einseitige Weisungen den Pflichtenkreis des Arbeitnehmers nicht erweitern, sondern lediglich konkretisieren können. Zum anderen ist die Frage, ob und inwieweit schon entsprechende Verhaltensvorschriften bestehen, unter dem Gesichtspunkt der Mitbestimmung relevant, weil das Mitbestimmungsrecht des Betriebsrats hinsichtlich eines bestimmten Regelungsgegenstandes bereits mit der erstmaligen Zustimmung erlischt. Schließlich sind die neuen Compliance-Vorschriften mit den bereits bestehenden Regelungen zu harmonisieren, um widersprüchliche Vorgaben oder Konflikte mit dem arbeitsrechtlichen Günstigkeitsprinzip zu vermeiden.³²

Bei der Abwägung des Für und Wider der verschiedenen Gestaltungsinstrumente bietet es sich an, zwischen konkretisierenden und pflichterweiternden Vorschriften zu unterscheiden. Des Weiteren kann zwischen mitbestimmungspflichtigen und nicht mitbestimmungspflichtigen Regelungen differenziert werden.³³

Sinnvoll ist oftmals eine Mischung der verschiedenen Instrumente: arbeitsbezogene Regelungen (etwa die Buchhaltungs- oder Bilanz-Compliance) können durch einseitige Weisungen durchgesetzt werden, während sonstige Verhaltenspflichten (z. B. Wettbewerbsverbote oder Diskriminierungsverbote) durch arbeitsvertragliche Regelungen oder Betriebsvereinbarungen implementiert werden. Die Abstimmung einzelner Regelungsarten auf konkrete Regelungsgegenstände ist allerdings eine Frage des Einzel-

³⁰Vgl. Hohmuth, BB 2014, 3061, (3065).

³¹Mengel, Compliance, § 1 Rn. 89.

³²Vgl. Hohmuth, BB 2014, 3061 (3063).

³³Hohmuth, BB 2014, 3061, (3063).

falls. Entscheidend sind Faktoren wie Unternehmensgröße, Mitarbeiteranzahl, Art und Umfang der einzuführenden Compliance-Regelungen sowie der Frage, ob ein Betriebsrat besteht und wie sich das Verhältnis zwischen Arbeitgeber und Betriebsrat im Unternehmen darstellt. Jedenfalls ist die Einbeziehung des gesamten Verhaltenskodex in den Arbeitsvertrag regelmäßig nachteilhaft, weil eine solche Implementierung den spezifischen Interessen des Unternehmens nicht hinreichend Rechnung trägt.³⁴

Nach wirksamer arbeitsrechtlicher Umsetzung der Compliance-Vorschriften können diese innerhalb des Unternehmens bzw. Konzerns als „einheitlicher“ Verhaltenskodex („Code of Ethics“) veröffentlicht werden, und zwar unabhängig davon, mittels welcher Gestaltungsvarianten die Regelungen verbindlich gemacht worden sind.³⁵

11.2.3 Mitbestimmung des Betriebsrats bei der Implementierung

Bei der Implementierung von Compliance-Regelungen sind für den Fall, dass ein Betriebsrat besteht, dessen Mitbestimmungsrechte zu beachten. Entsprechendes gilt auf der Ebene größerer Unternehmen bzw. eines Konzerns für die Mitbestimmungsrechte des Gesamt- und Konzernbetriebsrats. Im Hinblick auf die Zuständigkeitsbereiche der verschiedenen mitbestimmungsrechtlichen Gremien kann auf die vorstehenden Ausführungen (Abschn. 11.2.2.3.1) verwiesen werden.

Die Mitbestimmungsrechte bestehen unabhängig davon, für welche der drei Implementierungsvarianten sich der Arbeitgeber entscheidet. Auch bei der Einführung von Compliance-Vorschriften durch das Direktionsrecht oder arbeitsvertragliche Regelungen muss der Betriebsrat nach Maßgabe der zwingenden Mitbestimmungsrechte des Betriebsrats beteiligt werden; andernfalls sind die neu eingeführten bzw. geänderten Verhaltensvorschriften unwirksam. Die zwingende Beteiligung des Betriebsrats darf nämlich nicht durch Rückgriff auf individualvertragliche Gestaltungsvarianten unterlaufen werden.³⁶ Gegen Compliance-Vorschriften, die mangels Beteiligung des Betriebsrats unwirksam sind, kann der Betriebsrat Unterlassungsansprüche gegenüber dem Arbeitgeber geltend machen.³⁷

Bei der erstmaligen Einführung von Compliance-Vorschriften sind zwei zwingende Mitbestimmungsrechte des Betriebsrats von besonderer Bedeutung:

Ein Mitbestimmungsrecht besteht gemäß § 87 Abs. 1 Nr. 1 BetrVG zunächst bei Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb. Darunter fallen alle Maßnahmen, die das Ordnungsverhalten des Arbeitnehmers im Betrieb betreffen, also darauf gerichtet sind, die vorgegeben Ordnung im Betrieb zu gewährleisten bzw. aufrechtzuerhalten. Maßnahmen, die sich auf das Arbeitsverhalten des Arbeitnehmers beziehen,

³⁴ Mengel, Compliance, § 3 Rn. 2; Hohmuth, BB 2014, 3061 (3063).

³⁵ Mengel/Hagemeister, BB 2007, 1386 (1391).

³⁶ BAG NZA 1992, 749 (759); Fitting BetrVG § 87 Rn. 599.

³⁷ BAG NZA 1995, 40 (42).

weil sie unmittelbar Modalitäten der von ihm zu erbringenden Tätigkeit regeln, sind dagegen nicht mitbestimmungspflichtig.³⁸ Wichtig ist, dass die Mitbestimmungspflichtigkeit eines Verhaltenskodex nicht für das gesamte Regelungswerk einheitlich, sondern für die einzelnen Bestimmungen getrennt zu beurteilen ist.³⁹ Beispiele für compliance-relevante Vorschriften, die das Ordnungsverhalten des Arbeitnehmers betreffen, sind nach der Rechtsprechung etwa Tor- und Taschenkontrollen, der Erlass einer Benutzungsordnung oder ein generelles Rauchverbot.⁴⁰

Ein Mitbestimmungsrecht besteht zudem bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind das Verhalten und die Leistung der Arbeitnehmer zu überwachen, § 87 Abs. 1 Nr. 6 BetrVG. Dieses spezielle Mitbestimmungsrecht soll das allgemeine Persönlichkeitsrecht der Arbeitnehmer vor Eingriffen durch den Arbeitgeber schützen. Technische Einrichtungen in diesem Sinne sind alle Geräte und Anlagen, die über eine eigenständige Kontrollwirkung verfügen, weil sie Tätigkeiten verrichten, die sonst der überwachende Mensch wahrnehmen muss. Mitbestimmungspflichtige Überwachungseinrichtungen sind demnach etwa Film- und Video-geräte, Software zur Kontrolle des Internetverhaltens sowie Zeiterfassungsgeräte, nicht aber bloße Hilfsmittel, die keine eigenständige Überwachungsleistung erbringen (z. B. Uhr, Fernglas, Taschenrechner).⁴¹ Ein Mitbestimmungsrecht des Betriebsrats besteht allerdings nur dann, wenn durch die Datenverarbeitung mittels der technischen Einrichtung tatsächlich Persönlichkeitsrechte der Arbeitnehmer betroffen sind (siehe hierzu auch Abschn. 11.6.3).⁴²

11.2.4 Dokumentation und Kommunikation

Eine Pflicht zur Dokumentation von bestimmten neu eingeführten Compliance-Vorschriften folgt aus dem Datenschutzrecht. Gemäß Art. 5 Abs. 2 DS-GVO ist der Verantwortliche nicht nur für die Einhaltung der datenschutzrechtlichen Grundsätze verantwortlich, sondern hat auch deren Einhaltung nachzuweisen. Dies gilt umso mehr, als der Arbeitnehmer gemäß Art. 15 DS-GVO einen Anspruch auf Auskunft darüber hat, welche personenbezogenen Daten von ihm durch den Arbeitgeber verarbeitet werden.⁴³

Darüber hinaus ist eine Dokumentation bestimmter Compliance-Vorschriften auch im Interesse des Unternehmens, um mögliche Haftungsrisiken zu vermeiden. Mangels einschlägiger Spezialregelungen gilt dabei für die Aufbewahrungsfrist, dass personen-

³⁸ Vgl. Stück, ArbRAktuell 2015, 337 (338).

³⁹ BAG NJW (2008), 3731 („kein Klammereffekt“).

⁴⁰ Hohmuth, BB 2014, 3061 (363).

⁴¹ Vgl. BeckOK ArbR/Werner BetrVG § 87 Rn. 92.

⁴² Ludwig, NZA 2023, 321, (323 f.).

⁴³ Vgl. Schulze in: Kramer, IT-Arbeitsrecht, 2. Auflage 2019 Rn. 1097 ff.

bezogene Daten so lange aufbewahrt werden dürfen, wie ein anerkennenswertes rechtliches Aufbewahrungsinteresse des Arbeitgebers besteht (vgl. Art. 6 Abs. 1 S. 1 lit. f der Datenschutzgrundverordnung (DS-GVO)). Soweit die Daten z. B. zur Verteidigung gegen eine datenschutzrechtliche Haftung aufbewahrt werden, wird die Aufbewahrungsfrist in der Regel drei Jahre betragen, weil die in der DS-GVO vorgesehenen Geldbußen gemäß § 31 Abs. 2 Nr. 1 OWiG in drei Jahren verjähren.

Schließlich setzt die erfolgreiche Implementierung von Compliance-Vorschriften deren Kommunikation innerhalb des Konzerns bzw. Unternehmens voraus. Hierbei kommen verschiedene Kommunikationsmöglichkeiten in Betracht: Neben der einheitlichen Publikation eines umfassenden Verhaltenskodex im Inter- oder Intranet bietet sich auch die Ausgabe eines Compliance-bezogenen Mitarbeiter-Handbuchs oder zumindest entsprechender Merkblätter an. Als flankierende Maßnahmen können regelmäßige Auffrischungen und Mitarbeiterschulungen in Erwägung gezogen werden. Dies gilt insbesondere für Mitglieder der Unternehmensleitung, weil die Akzeptanz von Verhaltenspflichten seitens der Mitarbeiter maßgeblich davon abhängt, ob diese Regelungen auch von der Unternehmensleitung vorgelebt werden („tone from the top“).

11.3 Allgemeines Gleichbehandlungsgesetz (AGG)

11.3.1 Grundsätze

Mit den Grundsätzen des allgemeinen Gleichbehandlungsgesetzes (AGG) müssen sich Arbeitgeber zwingend auseinandersetzen, um eine verbotene Benachteiligung von bestimmten Arbeitnehmern zu vermeiden. Das Ziel des AGG ist es, Benachteiligungen aus Gründen der Rasse oder wegen der ethnischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität zu verhindern oder zu beseitigen (§ 1 AGG).

Das AGG findet nicht nur für Arbeitnehmer und Auszubildende Anwendung, sondern auch für Bewerber sowie Leiharbeitnehmer (§ 6 AGG). Diese Personen dürfen aufgrund einer der oben genannten Gründe nicht benachteiligt werden, es sei denn es liegt hierfür eine Rechtfertigung oder Ausnahme nach den §§ 5, 8–10 AGG vor. Dies bedeutet nicht, dass eine Ungleichbehandlung oder eine sog. „Diskriminierung“ allgemein unzulässig ist. Das AGG verbietet vielmehr das Treffen von nachteiligen Maßnahmen gegenüber Arbeitnehmern und anderen geschützten Personen aufgrund der in § 1 AGG aufgezählten Merkmale.⁴⁴ Eine solche ungünstige Behandlung kann nach § 3 AGG nur im Vergleich zu einer anderen Person in einer vergleichbaren Situation festgestellt werden.⁴⁵

⁴⁴ BeckOGK/Benecke, AGG, § 7 Rn. 22, ErfK/Schlachter, AGG, § 1 Rn. 2.

⁴⁵ EuGH (10. Kammer), NZA 2018, 291 Rn. 30.

Beachten Sie, dass nicht nur ein aktives Tun eine verbotene Benachteiligung begründen kann, sondern auch ein Unterlassen.⁴⁶ So kann etwa ein Nicht-Verlängern eines befristeten Arbeitsvertrages aufgrund einer der in § 1 AGG genannten Merkmale eine verbotene Benachteiligung darstellen.⁴⁷

Eine (sexuelle) Belästigung am Arbeitsplatz kann ebenfalls eine Benachteiligung im Sinne des AGG darstellen, § 3 Abs. 3, 4 AGG.

Sollten bestimmte Personengruppen als faktische Konsequenz einer Bestimmung des Arbeitgebers benachteiligt werden, kann ein Fall der mittelbaren Benachteiligung gem. § 7 Abs. 2 AGG vorliegen.⁴⁸ Als Definition kann die der Gleichbehandlungsrichtlinie Richtlinie (EU) 2006/54 (Gleichbehandlungs-RL) herangezogen werden: „*Eine Situation, in der dem Anschein nach neutrale Vorschrift, Kriterien oder Verfahren Personen des einen Geschlechts in besonderer Weise gegenüber Personen des anderen Geschlechts benachteiligen können [...]*“. Das Merkmal „Geschlecht“ kann sodann gegen jedes beliebige Merkmal des § 1 AGG ausgetauscht werden. Eine mittelbare Benachteiligung kann also festgestellt werden, wenn durch eine Bestimmung des Arbeitgebers – etwa in einem Tarifvertrag – die Personengruppe, die ein bestimmtes Merkmal aufweist, im Vergleich zu anderen Personen benachteiligt ist.⁴⁹ Auch hier kann eine Differenzierung zwischen Personengruppen gerechtfertigt sein, insoweit diesbezüglich ein rechtmäßiges Ziel vorliegt.⁵⁰ Als zulässig anerkannt ist – einzelfallabhängig – etwa die Unterscheidung nach Länge der Betriebszugehörigkeit, Berufsausbildung und Sprachenkenntnis.⁵¹

§ 8 AGG schafft eine allgemeine Ausnahme vom Benachteiligungsverbot. So kann eine unterschiedliche Behandlung wegen eines „Diskriminierungsgrundes“ im Sinne des § 1 AGG aufgrund beruflicher Anforderungen zulässig sein, wenn dieser Grund wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung eine wesentliche und entscheidende berufliche Anforderung darstellt, sofern der Zweck rechtmäßig und die Anforderung angemessen ist. Darüber hinaus stellen § 9 AGG und § 10 AGG spezifische Ausnahmetatbestände dar, wonach speziell die Ungleichbehandlung aufgrund der Religion oder Weltanschauung sowie des Alters zulässig sein kann. So kann etwa eine Altershöchstgrenze für die Einstellung in Berufen, die eine besondere körperliche Leistungsfähigkeit fordern (Berufsfeuerwehr, Verkehrspiloten, etc.), rechtmäßig sein.⁵²

⁴⁶ MüKoBGB/Thüsing, AGG, § 3 Rn. 12.

⁴⁷ So etwa BAG NZA 2014, 21 Rn. 34, BAG NZA 2012, 1345 Rn. 25, EuGH (5. Kammer) NZA 2001, 1243 (Rs. C-438/99 Maria Luisa Jiménez Melgar/Ayuntamiento de Los Barrios).

⁴⁸ BeckOK ArbR/Roloff, AGG, § 3 Rn. 17.

⁴⁹ ErfK/Schlachter, AGG, § 3 Rn. 10, BeckOK ArbR/Roloff, AGG, § 3 Rn. 17.

⁵⁰ BeckOK ArbR/Roloff, AGG, § 3 Rn. 19.

⁵¹ ErfK/Schlachter, AGG, § 3 Rn. 14, BeckOK ArbR/Roloff, AGG, § 3 Rn. 26.

⁵² ErfK/Schlachter, AGG, § 8 Rn. 1.

11.3.2 Pflichten von Arbeitgebern

Die allgemeinen Grundsätze des AGG vorausgeschickt, kommt es in der Compliance-Praxis vor allem auf die Pflichten von Arbeitgebern an. Diese sind in § 12 AGG geregelt:

- Treffen von erforderlichen (vorbeugenden) Maßnahmen zum Schutz vor Benachteiligungen
- Unterbindung der Benachteiligung (etwa durch Abmahnung, Umsetzung, Versetzung oder Kündigung)
- Hinweisen auf Unzulässigkeit und Hinwirken auf Unterbleiben von Benachteiligungen (insbesondere im Rahmen der beruflichen Aus- und Fortbildung)
- Schutz vor Benachteiligung durch Dritte (u. a. Arbeitskollegen)
- Bekanntmachung der Regelungen des AGG und den besonderen Regelungen zur Klageerhebung im Arbeitsgerichtsgesetz (ArbGG).

11.3.3 Rechte von Arbeitnehmern

Sollten sich Arbeitnehmer diskriminiert fühlen, sind sie dazu berechtigt, sich bei der entsprechenden zuständigen Stelle des Betriebs zu beschweren (§ 13 AGG). Darüber hinaus kann Arbeitnehmern im Falle einer (sexuellen) Belästigung sogar ein Leistungsverweigerungsrecht zustehen, insofern der Arbeitgeber keine oder offensichtlich ungeeignete Maßnahmen zur Unterbindung trifft und die Einstellung der Tätigkeit zu ihrem Schutz erforderlich ist (§ 14 AGG).

Arbeitnehmern kann außerdem ein Entschädigungs- und Schadensersatzanspruch zustehen, wobei das Verschulden des Arbeitgebers gesetzlich vermutet wird (§ 15 AGG). Ersatzfähig sind hierbei sowohl materielle als auch immaterielle Schäden des Arbeitnehmers. Zu beachten ist, dass auch diskriminierende Verhaltensweisen von Mitarbeitern dem Arbeitgeber zugerechnet werden können, insofern diese als Erfüllungsgehilfen des Arbeitgebers tätig werden, was typischerweise bei Beschäftigten in Vorgesetztenstellung zutreffen wird.⁵³

Im Falle einer diskriminierenden Kündigung können betroffene Arbeitnehmer – in europarechtskonformer Auslegung des § 2 Abs. 4 AGG – einen Verstoß gegen ein Diskriminierungsverbot im Sinne des § 1 AGG geltend machen; ein Verstoß gegen ein Diskriminierungsverbot hätte dann die Unwirksamkeit der Kündigung nach § 1 Abs. 2 KSchG zur Folge.⁵⁴

⁵³ ErfK/Schlachter, AGG, § 15 Rn. 6.

⁵⁴ BeckOK BGB/Horcher, AGG, § 2 Rn. 40.

11.4 Überwachung und Sanktionierung

11.4.1 Allgemeines

Ein effektives CMS setzt voraus, dass die arbeitsrechtlich implementierten Verhaltensvorschriften auch tatsächlich befolgt werden. Wenngleich ein Verstoß gegen Compliance-Regelungen sowohl vonseiten des Arbeitgebers als auch vonseiten des Arbeitnehmers ausgehen kann, geht es im Rahmen der Überwachung und Sanktionierung von Compliance-Verstößen ganz überwiegend um Eingriffe in die Rechte der Arbeitnehmer.

Im Grundsatz gilt, dass der Arbeitnehmer die arbeitsvertragliche Nebenpflicht hat, Überwachungs- und Kontrollmaßnahmen zu dulden.⁵⁵ Soweit in Grundrechte des Arbeitnehmers eingegriffen wird, ist aber eine Interessenabwägung erforderlich. Das „Ob“ und das „Wie“ der Überwachungsmaßnahmen müssen verhältnismäßig sein, das heißt bei mehreren zur Verfügung stehenden Mitteln muss das Mittel der geringsten Eingriffsintensität gewählt werden. Ferner darf die Intensität des Eingriffs nicht außer Verhältnis zu dem Gewicht des damit verfolgten Ziels stehen.⁵⁶ Maßgebliche Faktoren bei der Interessenabwägung sind insbesondere

- die größtmögliche Wahrung der Anonymität
- die Betroffenheit unbeteiligter Dritter
- die Dauer und Art der Kontrolle, gerade im Hinblick darauf, ob es sich um offene oder verdeckte Kontrollmaßnahmen handelt sowie
- die Frage, ob es sich um verdachtsunabhängige oder konkret anlassbezogene Maßnahmen handelt.⁵⁷

11.4.2 Überwachung des Arbeitnehmers durch den Arbeitnehmer

Bei der Überwachung des Arbeitnehmers findet regelmäßig ein weitreichender Eingriff in dessen allgemeines Persönlichkeitsrecht statt, weil personenbezogene Daten erhoben und verarbeitet werden. Die datenschutzrechtlichen Grenzen von Überwachungsmaßnahmen werden im Rahmen der nachstehenden Ausführungen zum Beschäftigtendatenschutz erläutert (Abschn. 11.6.2.8). Dabei muss auch berücksichtigt werden, dass sich der Arbeitgeber im Fall einer unzulässigen Datenerhebung gemäß § 201 StGB wegen Verletzung der Vertraulichkeit des Wortes strafbar machen kann.

Das Verhalten des Arbeitnehmers kann durch diverse Maßnahmen überwacht werden. In Betracht kommt etwa das E-Mail-Screening, die Analyse des Telefonverhaltens, der Ein-

⁵⁵Vgl. Günther/Böglmüller, NZA 2017, 546 (550).

⁵⁶Mengel, Compliance, § 4 Rn. 2.

⁵⁷Mengel, Compliance, § 4 Rn. 2.

satz von Spyware oder die Videoüberwachung.⁵⁸ Hinsichtlich der rechtlichen Zulässigkeit dieser Kontrollmaßnahmen muss im Ausgangspunkt zwischen privaten und dienstlichen Daten unterschieden werden: Der Zugriff auf dienstliche Daten ist ohne Weiteres erlaubt, weil dabei nicht in das allgemeine Persönlichkeitsrecht des Arbeitnehmers eingegriffen wird.⁵⁹ Bei personenbezogenen Daten ist wiederum regelmäßig danach zu unterscheiden, ob und inwieweit der Arbeitgeber die private Nutzung von Arbeitsmitteln gestattet hat.

Ein uneingeschränkter Zugriff auf den E-Mail-Account des Arbeitnehmers ist demnach nur zulässig, wenn die Nutzung für private Zwecke ausdrücklich untersagt worden ist.⁶⁰ Ist die Privatnutzung (teilweise) gestattet, ist der Zugriff des Arbeitgebers dagegen grundsätzlich unzulässig. In diesem Fall findet das Telekommunikationsgesetz (TKG) Anwendung, sodass der Arbeitgeber gegenüber dem Arbeitnehmer zur Wahrung des Fernmeldegeheimnisses verpflichtet ist.⁶¹ Eine andere Beurteilung kann sich aber ergeben, dass bei gestatteter Privatnutzung die dienstlichen und die privaten Daten streng getrennt aufbewahrt werden – in solchen Konstellationen bleibt ein Zugriff auf die dienstlichen Daten des Arbeitnehmers freilich erlaubt. Diese Grundsätze gelten nicht nur für die Nutzung des E-Mail-Accounts, sondern können im Wesentlichen auch auf die Überwachung des Arbeitnehmers durch das E-Mail-Screening oder die Analyse des Telefonverhaltens übertragen werden.⁶²

11.4.3 Interne Ermittlungen im Verdachtsfall

Bei einem Verdacht auf Compliance-Verstöße seitens des Arbeitgebers oder des Arbeitnehmers können unternehmensinterne Ermittlungen („Internal Investigations“) eingeleitet werden. Insoweit gilt es zu beachten, dass der Arbeitgeber den Arbeitnehmer kraft seines Weisungsrechts zur Mitwirkung an der Sachverhaltsaufklärung verpflichten kann, wenn der Arbeitgeber ein berechtigtes Interesse an der Aufklärung hat und diese den Arbeitnehmer nicht unzumutbar belasten würde.⁶³ Anders als im Strafprozessrecht kann sich der Arbeitnehmer nach überwiegender Auffassung allerdings nicht auf einen Schutz vor Selbstbelastung berufen; ein Auskunftsverweigerungsrecht (vgl. § 55 der Strafprozessordnung (StPO)) steht ihm gegenüber dem Arbeitgeber gerade nicht zu. Dafür spricht, dass das Auskunftsverweigerungsrecht auch im Strafverfahren keine absolute Geltung beansprucht.⁶⁴

⁵⁸ SWK-Arbeitsrecht/Mengel, „Compliance“, Rn. 14 ff.

⁵⁹ Mengel, Compliance, § 4 Rn. 11; 13: Ob die Daten elektronisch oder in Papierform gespeichert sind, kann insofern keinen Unterschied machen; Göpfert/Merten/Siegrist, NJW 2008, 1703 (1705).

⁶⁰ Vgl. SWK-Arbeitsrecht/Mengel, „Compliance“, Rn. 15.

⁶¹ Computerrechts-Handbuch/Polenz, Teil 13, Kap. 136 Rn. 25; BeckOK. DatenschutzR/Riesenhuber BDSG § 26 Rn. 176.

⁶² Vgl. Schulze in: Kramer, IT-Arbeitsrecht, Rn. 1190.

⁶³ Klengel/Mückenberger, CCZ 2009, 81 (82).

⁶⁴ Vgl. Greco/Caracas NStZ 2015, 7 (15) mwN.

Im Rahmen von Internal Investigations kann es zur Beschleunigung der Sachverhaltsermittlung und des Change-Managements im Interesse des Unternehmens liegen, arbeitsrechtliche Amnestieprogramme (Leniency) oder Kronzeugenregelungen einzuführen, um die Kooperation und Aussagen von Mitarbeitern im Gegenzug gegen den Verzicht auf arbeitsrechtliche Sanktionen zu erlangen.⁶⁵

11.4.4 Whistleblowing

Compliance-Verstöße können nicht nur durch Überwachungs- und Kontrollmaßnahmen des Arbeitgebers aufgedeckt werden. Gerade potenzielle Verstöße von Führungskräften werden vermehrt durch diskrete Hinweise von Arbeitnehmern („Whistleblowing“) an die Unternehmensleitung aufgedeckt. Insoweit ist seit 2019 die Whistleblower-Richtlinie (RL (EU) 2019/1937, kurz: WBRL) zu beachten. Zwar wurde diese (Stand: Mai 2023) noch nicht in das deutsche Recht umgesetzt; jedoch ist bereits ein konkreter Entwurf für ein „Hinweisgeberschutzgesetz“ (Hin-SchG-E) erlassen worden, an dem sich die Praxis auch jetzt schon orientieren kann, zumal die Vorgaben der Richtlinie in jedem Fall zwingend beachtet werden müssen.

Eine umfassende Darstellung der rechtlichen Vorgaben ist im Rahmen dieses Beitrages nicht möglich. Es sei aber darauf hingewiesen, dass Unternehmen ab einer Größe von 50 Mitarbeitern zur Einrichtung interner Meldekanäle, etwa einer Hotline oder einer Beschwerdestelle, verpflichtet werden. Bei der Ausgestaltung des Hinweisgeberschutzsystems sind zum Schutz der Hinweiser insbesondere umfassende datenschutzrechtliche Anforderungen zu beachten, wobei mit § 10 HinSchG-E eine spezielle Verarbeitungsgrundlage vorgesehen ist.

11.4.5 Compliance-Beauftragter

Um die Compliance im Unternehmen sicherzustellen, kann die Auslagerung von Compliance-Aufgaben auf spezialisierte Fachkräfte empfehlenswert sein. Ab einer gewissen Unternehmensgröße kann unter gesellschaftsrechtlichen und ordnungswidrigkeitsrechtlichen Gesichtspunkten (vgl. § 93 Abs. 1 AktG; § 130 OWiG) sogar eine Pflicht zur Einstellung einer Vollzeitkraft bestehen; entscheidend sind die unternehmensspezifischen Umstände im Einzelfall.⁶⁶

In erster Linie ist für die Compliance ein zentraler Compliance-Beauftragter („Compliance-Officer“) zuständig, der an die Unternehmensleitung berichtet. Zu seinen Aufgaben gehört es, mit der Unternehmensleitung ein wirksames Compliance-Konzept zu entwickeln und durchzusetzen. Wichtig ist, dass der Compliance-Officer bei Erfüllung sei-

⁶⁵ Mengel, NZA 2017, 1494 (1498).

⁶⁶ Vgl. BGH BeckRS 2010, 17534.

ner Aufgaben möglichst unabhängig und weisungsfrei agieren sollte; insbesondere darf der Compliance-Officer zur Vermeidung von Interessenkonflikte nicht in die zu kontrollierende Unternehmensabteilung integriert werden.⁶⁷ Allerdings folgt aus § 130 Abs. 1 S. 1 OWiG, dass auch der Compliance-Officer in gewissen Umfang kontrolliert werden muss, wenn die Unternehmensleitung ihren erforderlichen Aufsichtsmaßnahmen genügen will.⁶⁸

Der Compliance-Officer genießt keinen besonderen Kündigungsschutz. Auch das allgemeine Maßregelungsverbot des § 612a BGB greift nur, wenn die Tätigkeit als Compliance-Officer das wesentliche Motiv für die Kündigung ist – ein Nachweis, der praktisch kaum erbracht werden kann. Die arbeitsvertragliche Vereinbarung eines besonderen Kündigungsschutzes, etwa in Anlehnung an das Amt des Immissionsschutzbeauftragten (vgl. § 58 des Bundesimmissionsschutzgesetzes – BimSchG), kann aber unter Umständen im Interesse des Unternehmens liegen.⁶⁹

Kraft seines Amtes kann den Compliance-Officer eine strafrechtliche Garantienpflicht (§ 13 StGB) treffen. Das vom Compliance-Officer übernommene Risiko sollte daher aus seiner Sicht möglichst (1.) durch den Abschluss einer D&O-Versicherung und (2.) durch eine tendenziell enge Formulierung des Aufgabenkreises im Arbeitsvertrag abgemildert werden.⁷⁰

11.4.6 Maßnahmen bei Verstößen von Arbeitnehmern und Arbeitgebern

Compliance-Verstöße des Arbeitnehmers kann der Arbeitgeber mit diversen arbeitsrechtlichen Mitteln sanktionieren. In Betracht kommen insbesondere die Ermahnung, die Abmahnung und die Kündigung (ordentlich oder außerordentlich), wobei nach dem Verhältnismäßigkeitsgrundsatz das möglichst mildeste Mittel zu wählen ist. Insbesondere bei vermögensbezogenen Straftaten des Arbeitnehmers kann aber eine außerordentliche Kündigung ausgesprochen werden.⁷¹ Aus strategischer Sicht spielt auch die befürchtete Innen- bzw. Außenwirkung eine Rolle.

Bei schwerwiegenden Compliance-Verstößen der Unternehmensleitung kann diese abberufen bzw. gekündigt werden (vgl. z. B. § 84 Abs. 3 S. 1, 2 AktG). Sanktionen im weiteren Sinne sind auch Beweisverwertungsverbote im Fall unzulässiger Überwachungsmaßnahmen sowie etwaige Unterlassungsansprüche des Betriebsrats bei der Verletzung zwingender Mitbestimmungsrechte. Schließlich drohen dem Arbeitgeber bei Compliance-Verstößen auch straf- und ordnungswidrigkeitsrechtliche Konsequenzen, insbesondere kann ein Verstoß gegen die allgemeine Aufsichtspflicht des § 130 OWiG mit einer Geldbuße in Höhe von bis zu einer Millionen Euro geahndet werden (§ 130 Abs. 3 OWiG).

⁶⁷ SWK-Arbeitsrecht/Mengel, „Compliance“, Rn. 28.

⁶⁸ Schulze in: Kramer, IT-Arbeitsrecht, 2. Auflage 2019 Rn. 1117.

⁶⁹ Schulze in: Kramer, IT-Arbeitsrecht, 2. Auflage 2019 Rn. 1117.

⁷⁰ SWK-Arbeitsrecht/Mengel, „Compliance“, Rn. 32; Kraft/Winkler, CCZ 2009, 29, (32).

⁷¹ SWK-Arbeitsrecht/Mengel, „Compliance“, Rn. 21; Mengel, BB 2007, 1386 (1392).

11.4.7 Verwertung vor Gericht

Im Fall einer unzulässigen Überwachung stellt sich die Frage, ob und inwieweit der Arbeitgeber die erhobenen Daten gleichwohl prozessual verwerten darf. Im Wesentlichen sind zwei Prinzipien zu beachten: Zum einen werden Beweisverwertungsverbote im Zivilprozess nicht von Amts wegen berücksichtigt, sondern müssen jeweils von den Parteien geltend gemacht werden.⁷² Zum anderen beurteilt sich das Bestehen eines Beweisverwertungsverbots nach einer umfassenden Abwägung zwischen der Intensität der unzulässigen Datenerhebung und dem Verwertungsinteresse der anderen Partei, wobei die Rechtsprechung bei der Annahme von Beweisverwertungsverbots im Zivilprozess eine grundsätzlich restriktive Haltung hat.⁷³

Ein Verwertungsverbot wurde beispielsweise im Fall einer anlasslosen und heimlichen Überwachung des Arbeitnehmers „ins Blaue hinein“ vom Bundesarbeitsgericht bejaht.⁷⁴

11.5 Exkurs: Gesetz zum Schutz von Geschäftsgeheimnissen

(als Umsetzung der Know-How-Schutz-Richtlinie (EU) 2016/943)

Mit Inkrafttreten des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) am 26. April 2019 wurde die Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung in Deutschland umgesetzt. Das nationale Gesetz hat somit insbesondere die europaweite Harmonisierung des Schutzes von Know-How zum Ziel.⁷⁵

Das GeschGehG definiert erstmals den Begriff „Geschäftsgeheimnis“:

Definition Geschäftsgeheimnis

„Information,

- a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und
- b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und
- c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht“.

⁷² Balthasar, JuS 2008, 35 (39).

⁷³ Vgl. BAG NZA 2017, 112 (114).

⁷⁴ BAG NZA 2017, 1327 („Keylogger“).

⁷⁵ BT-Drs. 19/4724 S. 1.

Als Geschäftsgeheimnisse zu qualifizieren sind u. a. Marktstrategien, Entwicklungs- und Forschungsprojekte, Herstellungsverfahren, Formeln und Umsätze.⁷⁶

Weiterhin erlaubt sind nach § 3 GeschGehG u. a. eigenständige Entdeckungen und Schöpfungen (sog. Reverse Engineering). Verbotene Handlungen sind in § 4 GeschGehG geregelt und umfassen etwa den „*unbefugten Zugang zu [...] oder das unbefugte Kopieren von Dokumenten [...] oder elektronischen Dateien, die der rechtmäßigen Kontrolle des Inhabers des Geschäftsgeheimnisses unterliegen und die das Geschäftsgeheimnis enthalten [...]*“.⁷⁷ Ausnahmsweise gerechtfertigt können solche unerlaubten Handlungen nach § 5 GeschGehG sein, wenn die Nutzung oder Offenlegung des Geschäftsgeheimnisses zum Schutz eines berechtigten Interesses (etwa zur Aufdeckung einer rechtswidrigen Handlung) dient. Diese Ausnahmeverordnung schützt somit auch – bei Vorliegen der Voraussetzungen – Whistleblower vor negativen rechtlichen Konsequenzen.⁷⁸

Arbeitgeber können nun unmittelbar auf Grundlage der §§ 6–8 GeschGehG Ansprüche auf Beseitigung/Unterlassung, Vernichtung, Herausgabe, Rückruf, Entfernung und Rücknahme vom Markt und Auskunft gegenüber Personen geltend machen, die deren Geschäftsgeheimnis verletzt haben. Hierbei kommen als Anspruchsgegner nicht nur (ehemalige) Mitarbeiter, sondern auch die neuen Arbeitgeber der ehemaligen Mitarbeiter in Betracht.⁷⁹ Als Besonderheit des GeschGehG kann ein Anspruch allerdings ausgeschlossen sein, wenn die Erfüllung im Einzelfall unverhältnismäßig wäre. Hierbei werden gem. § 9 GeschGehG etwa der Wert des Geschäftsgeheimnisses oder getroffene Geheimhaltungsmaßnahmen berücksichtigt.

Das GeschGehG betont die Unabdingbarkeit des Ergreifens von Schutzmaßnahmen von Arbeitgebern, damit diese aus dem neuen Gesetz überhaupt Vorteile ziehen können.⁸⁰ Arbeitgeber müssen also bei der Geltendmachung ihrer Ansprüche darlegen können, dass hinsichtlich des verletzten Geschäftsgeheimnisses konkrete angemessene Schutzmaßnahmen ergriffen worden sind.⁸¹ Regelmäßig allein nicht ausreichend sind hier allgemein formulierte arbeitsvertragliche Geheimhaltungsklauseln (sog. Catch-All-Klauseln); vielmehr sollten Arbeitgeber ein hinreichendes Geheimnisschutzkonzept ausarbeiten und nutzen.⁸² Welche Maßnahmen zum Schutz eines Geschäftsgeheimnisses angemessen sind, bestimmen sich immer anhand des Einzelfalls – ein optimaler Schutz wird hierbei nicht vorausgesetzt.⁸³ Als angemessene Schutzmaßnahmen kommen beispielsweise Zugangsbeschränkungen (Need-to-Know-Prinzip), Verschlüsselungstechnologien, betriebsinterne

⁷⁶ BVerfG BeckRS 2006, 134696 Rn. 72; Baade/Reiserer, DStR 2022, 890 (891).

⁷⁷ Ibel, MMR 2021, 929.

⁷⁸ Baade/Reiserer, DStR 2022, 890.

⁷⁹ Baade/Reiserer, DStR 2022, 890.

⁸⁰ So etwa ArbG Aachen NZA-RR, 2022, 178 Rn. 67 ff.

⁸¹ Baade/Reiserer, DStR 2022, 890 (893 ff.); MüKoUWG/Hauck, GeschGehG § 2 Rn. 21 ff.

⁸² LAG Baden-Württemberg MMR 2022, 79 Rn. 33.

Richtlinien, nachvertragliche Wettbewerbsverbote oder ein vertragliches Untersagen von Reverse Engineering in Betracht.⁸³

Beachten Sie, dass ein ausgearbeitetes Geheimnisschutzkonzept – als Bestandteil eines CMS – stets überprüft und gegebenenfalls (beispielsweise bei Hinzukommen von Know-How) angepasst werden muss.⁸⁴ Um etwaige Ansprüche aus dem GeschGehG gerichtlich hinreichend darlegen zu können, ist auch eine vollumfängliche Dokumentation der ergriffenen Geheimnisschutzmaßnahmen unabdingbar.⁸⁵

11.6 Mitarbeiterdatenschutz

Dem Schutz der personenbezogenen Daten von Mitarbeitern kommt im Rahmen der Implementierung von Compliance in Unternehmen zwangsläufig eine bedeutende Rolle zu. Denn nicht nur etwa bei einer Überwachung von Mitarbeitern, sondern bereits bei dem Abspeichern von Bewerberunterlagen findet in der Regel eine Verarbeitung von personenbezogenen Daten statt.

11.6.1 Grundsätze

Die Verarbeitung personenbezogener Daten ist größtenteils in der europäischen Datenschutzgrundverordnung (DSGVO) geregelt. Jegliche Datenverarbeitungen sind nach Art. 6 Abs. 1 DSGVO grundsätzlich erst einmal unzulässig, insofern keine Ausnahme – in Form einer Rechtfertigung oder einer Einwilligung durch den Betroffenen – vorliegt (sog. Verbot mit Erlaubnisvorbehalt).⁸⁶ Welche Grundsätze hierbei stets einzuhalten sind, sind in Art. 5 DSGVO aufgezählt:

- Rechtmäßigkeit
- Verarbeitung nach Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

⁸³ MüKoUWG/Hauck, GeschGehG, § 2 Rn. 23 ff.; Baade/Reiserer, DStR 2022, 890 (892 f.); MüKoStGB/Joecks/Miebach, GeschGehG, § 23 Rn. 33 ff.

⁸⁴ MüKoUWG/Hauck, GeschGehG, § 2 Rn. 48; Baade/Reiserer, DStR 2022, 890 (893).

⁸⁵ MüKoUWG/Hauck, GeschGehG, § 2 Rn. 48; Baade/Reiserer, DStR 2022, 890 (893).

⁸⁶ Sydow/Marsch/Ingold, DSGVO, Art. 7 Rn. 8.

Spezielle Vorschriften hinsichtlich der Verarbeitung personenbezogener Daten im Arbeitsverhältnis finden sich in der DSGVO allerdings nicht. Die europäische Verordnung wird allerdings durch das Bundesdatenschutzgesetz (BDSG) und einige weitere bereichsspezifische Gesetze, etwa das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG), ergänzt. Die Regelungen der DSGVO finden weiterhin zwar Anwendung, allerdings nur insoweit es keine einschlägigen spezielleren gesetzlichen Regelungen gibt.⁸⁷ Die Zulässigkeit der Verarbeitung von Mitarbeiterdaten durch Arbeitgeber wird insbesondere durch § 26 BDSG modifiziert. In § 26 Abs. 5 BDSG wird ausdrücklich angeordnet, dass Arbeitgeber geeignete Maßnahmen ergreifen müssen, um sicherzustellen, dass insbesondere die oben aufgezählten Grundsätze des Art. 5 DSGVO bei einer Verarbeitung von Beschäftigtendaten eingehalten werden.

11.6.2 Erlaubte Datenverarbeitungen im Arbeitsverhältnis

In der Praxis stellt sich somit die Frage, ob und wenn ja, unter welchen Voraussetzungen nun Bewerberdaten gespeichert, Arbeitszeiten erfasst, Mitarbeiterbilder aufgenommen und die E-Mail-Korrespondenz von Mitarbeitern kontrolliert werden dürfen.

Voranzustellen ist, dass nach aktuellem Urteil des EuGH (Urteil vom 30. März 2023 Az. C-34/21) § 26 Abs. 1 S. 1 BDSG (bisher die zentrale Norm im deutschen Beschäftigten-datenschutzrecht!) keine taugliche Ermächtigungsgrundlage für etwaige Datenverarbeitungen für Zwecke des Beschäftigungsverhältnisses darstelle, da dieser die Voraussetzungen des Art. 88 Abs. 1, 2 DSGVO nicht erfülle und somit europarechtswidrig sei. Für eine datenschutzkonforme Verarbeitung von Beschäftigtendaten ist von nun an – jedenfalls vorläufig – unmittelbar auf Art. 6 Abs. 1 DSGVO abzustellen, der allerdings eine zu § 26 Abs. 1 S. 1 BDSG vergleichbare Rechtsgrundlage bietet.

11.6.2.1 Erfüllung eines Vertrags, Art. 6 Abs. 1 lit. b DSGVO

Personenbezogene Daten von Beschäftigten können nach Art. 6 Abs. 1 lit. b DSGVO zur Erfüllung eines Vertrags (sprich eines Arbeitsvertrags), dessen Vertragspartei die betroffene Person ist, rechtmäßig erhoben und verarbeitet werden. Zur „Erfüllung eines Vertrages“ zählen – wie beim bisher angewandten § 26 Abs. 1 S. 1 BDSG: „Begründung, Durchführung oder Beendigung“ – neben den Hauptpflichten aus dem Beschäftigungsverhältnis auch sämtliche Nebenpflichten sowie nachvertragliche und vorvertragliche Pflichten.⁸⁸

11.6.2.2 Wahrung berechtigter Interessen, Art. 6 Abs. 1 lit. f DSGVO

Auch zur Wahrung berechtigter Interessen des Arbeitgebers ist eine Datenverarbeitung nach Art. 6 Abs. 1 lit. f DSGVO möglich. Eine Datenverarbeitung ist nach Art. 6 Abs. 1 lit. f DSGVO zulässig, wenn (1.) dem Arbeitgeber ein berechtigtes Interesse an der Datenver-

⁸⁷ Paal/Pauly/Gräber/Nolden, BDSG, § 26 Rn. 10.

⁸⁸ Kühling/Buchner/Buchner/Petri, DSGVO, Art. 6, Rn. 33 f.

arbeitung zusteht, (2.) die konkrete Datenverarbeitung zur Wahrung dieses Interesses erforderlich ist und (3.) im Rahmen einer abschließenden Interessenabwägung festgestellt werden kann, dass die Interessen des Arbeitgebers überwiegen.⁸⁹ Sämtliche wirtschaftlichen, ideellen und rechtlichen Interessen können grundsätzlich ein berechtigtes Interesse des Arbeitgebers darstellen.⁹⁰ Ein Datenverarbeitungsinteresse des Arbeitgebers kann somit regelmäßig auf das grundrechtlich geschützte Recht auf Eigentum oder die unternehmerische Freiheit gestützt werden. Ist die Datenverarbeitung zur Wahrung der Interessen des Arbeitgebers auch erforderlich (kein milderer, gleich effektives Mittel), sind die Interessen des Betroffenen (Recht auf informationelle Selbstbestimmung) mit möglichen Interessen des Arbeitgebers anhand des konkreten Einzelfalls abzuwagen und zu einem Ausgleich zu bringen.⁹¹ Zentrale Bewertungskriterien sind hierbei unter anderem Art, Inhalt und Aussagekraft der Daten sowie Zweck, Art und die konkrete technische Aufmachung der Datenverarbeitung und eine etwaige Einflussmöglichkeit der betroffenen Person auf die Datenverarbeitung.⁹²

11.6.2.3 Aufdeckung von Straftaten, § 26 Abs. 1 S. 2 BDSG

Nach § 26 Abs. 1 S. 2 BDSG dürfen Beschäftigtendaten zur Aufdeckung von Straftaten verarbeitet werden, wenn (1.) zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, (2.) die Verarbeitung zur Aufdeckung erforderlich ist und (3.) das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Das bedeutet konkret, dass die Verarbeitung erst erfolgen darf, nachdem konkrete Anhaltspunkte – nicht lediglich ein vager Verdacht – vorliegen.⁹³ Den Arbeitgeber trifft hierbei die Pflicht, einen etwaigen konkreten Tatverdacht zu dokumentieren.

Eine „präventive“ Datenverarbeitung ist nach § 26 Abs. 1 S. 2 BDSG mithin nicht zulässig.⁹⁴ Eine Datenverarbeitung zur Aufdeckung von schwerwiegenden Pflichtverletzungen, die jedoch keine Straftaten darstellen, kann ebenso wenig auf § 26 Abs. 1 S. 2 BDSG gestützt werden.⁹⁵

⁸⁹ Kühling/Buchner/Buchner/Petri, DSGVO, Art. 6, Rn. 146 ff.

⁹⁰ Paal/Pauly/Frenzel, DSGVO, Art. 6 Rn. 28; Kühling/Buchner/Buchner/Petri, DSGVO, Art. 6 Rn. 146a ff.

⁹¹ Kühling/Buchner/Buchner/Petri, DSGVO, Art. 6 Rn. 147a; Paal/Pauly/Gräber/Nolden, BDSG, § 26 Rn. 13, Gola/Heckmann/Schulz, DSGVO, Art. 6 Rn. 69.

⁹² Kühling/Buchner/Buchner/Petri, DSGVO, Art. 6 Rn. 149 ff., Paal/Pauly/Frenzel, DSGVO, Art. 6 Rn. 31.

⁹³ Kühling/Buchner/Maschmann, BDSG, § 26 Rn. 59.

⁹⁴ Datenschutzkonferenz, Kurzpapier Nummer 14 Beschäftigtendatenschutz, S. 2.

⁹⁵ Paal/Pauly/Gräber/Nolden, BDSG, § 26 Rn. 23.

11.6.2.4 Einwilligung als Rechtsgrundlage für Datenverarbeitungen regelmäßig untauglich

Grundsätzlich kann eine zulässige Verarbeitung von Beschäftigtendaten auch auf Grundlage einer Einwilligung erfolgen. Allerdings kommt eine wirksame Einwilligung als geeignete Rechtsgrundlage in der Praxis selten in Betracht. Denn eine Einwilligung muss eindeutig, *freiwillig* und stets widerrufbar sein (Art. 7 DSGVO in Verbindung mit Erwägungsgrund 43, § 26 Abs. 2 BDSG). Von einer freiwilligen Einwilligung kann nur dann ausgegangen werden, wenn die betroffene Person *eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden* (vgl. Erwägungsgrund 43). Aufgrund des zwischen Arbeitgeber und Arbeitnehmer bestehenden Über-/Unterordnungsverhältnisses werden diese Voraussetzungen regelmäßig nicht gegeben sein.

Die Freiwilligkeit einer Einwilligung kann allerdings ausnahmsweise nach § 26 Abs. 2 S. 2 BDSG angenommen werden, wenn der Beschäftigte einen rechtlichen oder wirtschaftlichen Vorteil erhält oder wenn Arbeitgeber und Beschäftigte gleich gelagerte Interesse verfolgen. In der Praxis findet diese Regelvermutung nur dann Anwendung, wenn nicht das Beschäftigungsverhältnis selbst, sondern zusätzliche Leistungen des Arbeitgebers betroffen sind (z. B. bei Gestattung privater Nutzung des betrieblichen Internetzugangs).⁹⁶

11.6.2.5 Kollektivvereinbarungen, § 26 Abs. 4 BDSG

Auch eine Verarbeitung von Beschäftigtendaten (ggf. inklusive sensibler Daten) auf Grundlage von Kollektivvereinbarungen kann nach § 26 Abs. 4 BDSG zulässig sein. Wollen Arbeitgeber Betriebs- oder Dienstvereinbarungen als Rechtsgrundlage für eine Datenverarbeitung nutzen, müssen diese allerdings den Anforderungen des Art. 88 Abs. 1, 2 DSGVO entsprechen. Etwaige Vereinbarungen müssen also *spezifischere* Vorschriften zu denen der DSGVO darstellen, die geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen. Sollte das Schutzniveau der DSGVO durch Kollektivvereinbarungen gesenkt werden, sind diese als Rechtsgrundlage für eine Datenverarbeitung untauglich.⁹⁷

11.6.2.6 Zweckänderung

Sollten Arbeitgeber Beschäftigtendaten zu einem anderen als dem zuvor eindeutigen festgelegten Zweck verarbeiten (*Grundsatz der Zweckbindung*), ist dies nur auf Grundlage einer Einwilligung des Betroffenen oder einer Rechtsvorschrift zulässig *oder* wenn der neue Zweck mit dem ursprünglichen Zweck kompatibel ist (Art. 6 Abs. 4 DSGVO). Für die Beurteilung, ob ein Zweck kompatibel oder inkompatibel ist, zählt Art. 6 Abs. 4 DSGVO einige Kriterien auf (nicht abschließend):

- Verbindung zwischen ursprünglichem und neuem Zweck
- Zusammenhang, in dem personenbezogene Daten erhoben werden

⁹⁶ Datenschutzkonferenz, Kurzpapier Nummer 14 Beschäftigtendatenschutz, S. 2.

⁹⁷ Datenschutzkonferenz, Kurzpapier Nummer 14 Beschäftigtendatenschutz, S. 1.

- Art der personenbezogenen Daten
- Mögliche Folgen der beabsichtigten Weiterverarbeitung für die betroffene Person
- Vorhandsein geeigneter Garantien (z. B. Verschlüsselung oder Pseudonymisierung)

So kann eine Zweckänderung der Datenverarbeitung etwa zulässig sein, wenn aufgrund einer Auslagerung der Lohnabrechnung Daten an die externe Lohnabrechnungsstelle übermittelt werden.

Eine spezielle Regelung zur Zweckänderung von Datenverarbeitungen lässt sich auf nationaler Ebene finden: § 24 Abs. 1 BDSG erlaubt eine Zweckänderung, wenn sie (1.) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten oder (2.) zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist.

11.6.2.7 Umgang mit besonderen Kategorien personenbezogener Daten

Arbeitgeber können unter anderem unter den Voraussetzungen des § 26 Abs. 3 S. 1 BDSG auch Beschäftigtdaten besonderer Kategorien verarbeiten. Hierzu gehören etwa biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder die Gewerkschaftszugehörigkeit (Art. 9 Abs. 1 DSGVO). Eine Verarbeitung dieser Daten ist zulässig, wenn sie (1.) zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und (2.) kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Auf Grundlage von § 26 Abs. 3 DSGVO kann beispielsweise der Betriebsrat von einer etwaigen Krankheit oder Schwerbehinderung eines Arbeitnehmers unterrichtet werden.⁹⁸

Hierbei stets einzuhalten sind die Anforderungen des § 22 Abs. 2 BDSG: Zur Wahrung der Interessen der betroffenen Person müssen Arbeitgeber angemessene und spezifische Maßnahmen, die § 22 Abs. 2 S. 2 BDSG beispielhaft aufgezählt werden, vorsehen. Welche Maßnahmen im konkreten Einzelfall angemessen sind, bestimmt sich unter Berücksichtigung folgender Kriterien:

- Stand der Technik
- Implementierungskosten
- Art der Datenverarbeitung
- Umfang der Datenverarbeitung
- Umstände der Datenverarbeitung
- Zweck der Datenverarbeitung
- Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen

Eine Datenverarbeitung zur Beurteilung der Arbeitsfähigkeit eines Arbeitnehmers ist unmittelbar auf Art. 9 Abs. 2 lit. h DSGVO zu stützen. Sensible Daten von Beschäftigten dürfen zu diesem Zwecke nur dann verarbeitet werden, wenn diese Daten von Fachperso-

⁹⁸ Kühling/Buchner/Maschmann, BDSG, § 26 Rn. 24.

nal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt (Art. 9 Abs. 3 DSGVO) – sprich durch Ärzte oder sonstiges (Hilfs-)Personal.⁹⁹ Die Verarbeitung von sensiblen Daten kann auch durch eine wirksame Einwilligung legitimiert sein, § 26 Abs. 3 S. 2 BDSG in Verbindung mit § 26 Abs. 2 BDSG.

11.6.2.8 Pflichten von Arbeitgebern vor und bei der Durchführung von Überwachungsmaßnahmen

Wollen Arbeitgeber Überwachungsmaßnahmen am Arbeitsplatz durchführen, sind auch hierbei sämtliche datenschutzrechtlichen Anforderungen zu beachten. Denn Überwachungsmaßnahmen, wie beispielsweise E-Mail-Kontrollen, Videoüberwachung, GPS-Ortung des Firmenwagens oder Zugangskontrollen stellen eine Verarbeitung von personenbezogenen Daten dar. Gestützt werden kann die Zulässigkeit von Überwachungsmaßnahmen etwa auf Art. 6 Abs. 1 lit. b, f DSGVO oder § 26 Abs. 1 S. 2 BDSG.

Eine dauerhafte und/oder heimliche Überwachung ist nur ausnahmsweise datenschutzrechtlich zulässig, da diese Maßnahmen einen sehr intensiven Eingriff in das Recht auf informationelle Selbstbestimmung von Arbeitnehmern darstellen. Das Interesse des Arbeitgebers an einer „Totalüberwachung“ kann also nur in sehr seltenen Fällen, beispielsweise bei konkretem Straftatverdacht oder bei Verdacht einer anderen erheblichen Pflichtverletzung, überwiegen.¹⁰⁰

Eine Überwachung zur reinen Leistungskontrolle von Arbeitnehmern ist nicht erlaubt. Auch eine Überwachung im Rahmen der Intim- oder Persönlichkeitssphäre (etwa in Form einer Videoüberwachung in Sanitärräumen oder Umkleidekabinen) von Arbeitnehmer ist ebenfalls stets unzulässig.¹⁰¹

Bei einer Arbeitnehmerüberwachung, die beispielsweise aufgrund eines berechtigten Interesses des Arbeitgebers an dieser zulässig und erforderlich ist, treffen diesen diverse Pflichten, die *bei Beginn* der Überwachung erfüllt sein müssen.¹⁰²

- Hinweispflichten, Art. 12 ff. DSGVO
- Dokumentations- und Rechenschaftspflichten, Art. 5 Abs. 2, Art. 24 Abs. 1 S. 1 DSGVO; welche Mittel zur Erbringung des Nachweises der Einhaltung der datenschutzrechtlichen Grundsätze tauglich sind, bestimmt sich nach dem Risikograd der Datenverarbeitung im Einzelfall

⁹⁹ Kühling/Buchner/Maschmann, BDSG, § 26 Rn. 26.

¹⁰⁰ DSK Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen vom 17. Juli 2020, S. 25; Mengel, Compliance, § 7 Rn. 54.

¹⁰¹ DSK Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen vom 17. Juli 2020, S. 25.

¹⁰² Siehe hierzu DSK Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen vom 17. Juli 2020, S. 15 ff.

- Aufnahme in das Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DSGVO
- Durchführung einer Datenschutz-Folgenabschätzung, Art. 35 DSGVO
- Nachweisbare Umsetzung geeigneter technisch-organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus, Art. 24, 25, 32 DSGVO

Die erhobenen Daten sind unverzüglich zu löschen, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind (Art. 17 DSGVO). Auch schutzwürdige Interessen der Beschäftigten können einer fort dauernden Speicherung entgegenstehen (*Grundsatz der Datenminimierung und Speicherbegrenzung*). Die Speicherfrist ist auf das unbedingt erforderliche Mindestmaß zu beschränken (DSGVO Erwägungsgrund 34 S. 8). Beispielsweise die Speicherung von Videoüberwachungsdaten von 72 h wird als zulässig erachtet.¹⁰³

Besonders im Hinblick auf die jüngste Entscheidung des EuGH hinsichtlich der (mittelbaren) Unanwendbarkeit des § 26 Abs. 1 S. 2 BDSG sollten sämtliche Datenverarbeitungsvorgänge regelmäßig auf deren Rechtmäßigkeit anhand der aktuellen Rechtslage überprüft und gegebenenfalls angepasst, sowie deren Geeignetheit und Erforderlichkeit neu bewertet werden.

Beachten Sie, dass die datenschutzrechtlichen Vorgaben nur eingehalten werden müssen, insofern tatsächlich *personenbezogene* Daten verarbeitet werden. Erteilt ein Mitarbeiter eine ausschließlich sachbezogene Auskunft über eine ihm übertragene Aufgabe, stellt dies nach Art. 4 Nr. 1 DSGVO keine Verarbeitung personenbezogener Daten dar.¹⁰⁴ Datenschutzrechtliche Regelungen finden hier keine Anwendung.

11.6.3 Rechte und Pflichten des Betriebsrats

Auch für Betriebsräte spielt der Beschäftigtendatenschutz eine wichtige Rolle. Zum einen hat der Betriebsrat nach § 80 Abs. 1 BetrVG die Pflicht, die Einhaltung der datenschutzrechtlichen Vorschriften des Arbeitgebers zu überwachen und nach § 75 Abs. 2 BetrVG mitzuwirken. Ihm steht diesbezüglich gegenüber dem Arbeitgeber auch ein Auskunftsanspruch zu (§ 80 Abs. 2 S. 1 BetrVG). Eine Weitergabe von Beschäftigtendaten an den Betriebsrat ist gleichwohl stets auf eine Rechtsgrundlage der DSGVO bzw. des BDSG zu stützen und an dieser zu messen.¹⁰⁵

Zum anderen hat nach § 79a BetrVG auch der Betriebsrat selbst bei der Verarbeitung von Beschäftigtendaten sämtliche datenschutzrechtlichen Vorschriften einzuhalten. Verantwortlicher bleibt nach § 79a BetrVG allerdings der Arbeitgeber; der Betriebsrat haftet für etwaige Datenverstöße somit nicht selbst.

¹⁰³ DSK Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen vom 17. Juli 2020, S. 22 f.

¹⁰⁴ Maschmann, NZA-Beilage, 2018, 115.

¹⁰⁵ BAG NZA 2019, 1055 (1057) Rn. 24 ff.

Der Betriebsrat hat hinsichtlich der Einhaltung datenschutzrechtlicher Vorschriften allerdings trotz Überwachungs- und Mitwirkungspflicht kein Mitbestimmungsrecht. Denn die DSGVO und das BDSG regeln die Verarbeitung von Beschäftigertendaten bereits verbindlich und zwingend, sodass dem Betriebsrat diesbezüglich kein Ermessensspielraum zusteht.¹⁰⁶ Setzt der Arbeitgeber allerdings technische Einrichtungen ein, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, kann hinsichtlich dieser nach § 87 Abs. 1 Nr. 6 BetrVG ein Mitbestimmungsrecht des Betriebsrats bestehen (siehe oben Abschn. 11.2.3). In einer etwaigen Betriebsvereinbarung sollte zur Wahrung der Arbeitnehmerinteressen dann festgelegt werden, dass eine Überwachung durch den Arbeitgeber nicht der Leistungs-, bzw. Verhaltenskontrolle dient.¹⁰⁷ Sollte eine Leistungs-, bzw. Verhaltenskontrolle der Aufklärung von Straftaten dienen, steht dem Betriebsrat wiederum aufgrund der abschließenden und zwingenden gesetzlichen Regelung in § 26 Abs. 1 S. 2 BDSG mangels Ermessensspielraum kein Mitbestimmungsrecht zu.¹⁰⁸

Der Betriebsrat ist außerdem mit einer Reihe weiterer Rechte ausgestattet, welche regelmäßig datenschutzrechtlich relevant werden können:

- Einsicht in Lohn- und Gehaltslisten, § 80 Abs. 2 S. 2 Hs. 2 BetrVG
- Zustimmung bei Personalfragebögen, § 94 BetrVG
- Zustimmung bei Auswahlrichtlinien für personelle Maßnahmen, § 95 BetrVG
- Mitbestimmung Kündigungen, §§ 102 f. BetrVG
- Mitwirkung bei Betriebsänderungen, Interessenausgleichen, Sozialplänen, § 111 ff. BetrVG.

11.6.4 Besondere Fallkonstellation: Datenschutz im Home-Office

Besondere Relevanz hat in den letzten Jahren die datenschutzrechtliche Compliance vor dem Hintergrund der Nutzung von „Home-Office“ erlangt. Grundsätzlich existieren diesbezüglich keine speziellen datenschutzrechtlichen Vorschriften. Der Arbeitgeber bleibt insbesondere datenschutzrechtliche Verantwortlicher (Art. 4 Nr. 7 DSGVO), da der Arbeitnehmer auch zu Hause nach Weisung des Arbeitgebers handelt (Art. 29 DSGVO). Allerdings birgt die Nutzung von Home-Office spezielle Risiken, welchen der Arbeitgeber durch das Treffen geeigneter Maßnahmen entgegenwirken muss.

Da sich der Arbeitnehmer außerhalb der Kontroll- und Einflussmöglichkeiten des Arbeitgebers befindet, besteht etwa mangels entsprechender Sensibilisierung der Arbeitnehmer ein erhöhtes Risiko eines unberechtigten Zugriffs Dritter auf bzw. einer Kenntnis-

¹⁰⁶ Ludwig, NZA 2023, 321 (322).

¹⁰⁷ DSK Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen vom 17. Juli 2020, S. 28.

¹⁰⁸ Ludwig, NZA 2023, 321 (325).

nahme Dritter von Daten.¹⁰⁹ Auch die IT-Sicherheit ist nicht gleichermaßen gewährleistet wie im Betrieb selbst.¹¹⁰

Insbesondere folgende technischen und organisatorischen Maßnahmen bieten sich an, um Verstöße gegen datenschutzrechtliche Vorgaben und die damit verbundenen Haftungsrisiken zu vermeiden:

- Erstellen einer Homeoffice-Richtlinie
- Verpflichtung zur ausschließlichen Nutzung von Firmensoftware und -hardware sowie entsprechende Ausstattung
- Einrichtung und Verwendung von VPN
- Kommunikation und Arbeiten ausschließlich über verschlüsselte elektronische Wege
- Erweiterte Zugriffsbeschränkungen (beispielsweise durch Zwei-Faktor-Authentifizierung)
- Sperrung von (USB-)Anschlüssen
- Sicherstellung der technischen Trennung von privaten und geschäftlichen Inhalten
- Sichtschutz für Bildschirme und sperren des Bildschirms bei Abwesenheit sowie Sicherstellung der Vertraulichkeit bei Telefonaten
- Sicherer Transport und Entsorgung von Unterlagen und Datenträgern (beispielweise durch gesicherte Mitnahme in einem geschlossenen Verhältnis in den Betrieb und ggf. dortige Entsorgung)
- Sensibilisierung der Arbeitnehmer (durch Schulungen oder Fortbildungen)
- Sicherstellung von geeigneten häuslichen Räumlichkeiten und Arbeitsmitteln zum sicheren Ausschluss eines unberechtigten Datenzugriffs Dritter (beispielsweise durch ein abschließbares Arbeitszimmer sowie einen verschließbaren Schrank zur Verwahrung von Unterlagen)
- Beteiligung des Datenschutzbeauftragten
- Vertragliche Festlegung und Verpflichtung zur Einhaltung der datenschutzrechtlichen Vorgaben.¹¹¹

11.6.5 Haftung und Sanktionen bei Verstößen

Bei einer Missachtung datenschutzrechtlicher Vorgaben droht Unternehmen ein Bußgeld von bis zu 20.000.000 € oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs (Art. 83 DSGVO). Gegenüber der betroffenen Person (Arbeitnehmer) sieht die DSGVO außerdem eine Haftung für materielle und immaterielle Schäden der Verantwortlichen (Arbeitgeber) vor (Art. 82 DSGVO).

¹⁰⁹ Paal/Pauly, DSGVO, vor Art. 1 Rn. 26 f.

¹¹⁰ Paal/Pauly, DSGVO, vor Art. 1 Rn. 27.

¹¹¹ Paal/Pauly, DSGVO, vor Art. 1 Rn. 26 ff.; Gilga, ZD-Aktuell 2020, 07113; BfDI, Flyer Telearbeit und Mobiles Arbeiten von Juli 2020.

Auch im BDSG finden sich strafrechtliche Vorschriften: Möglich sind bis zu 3 Jahre Haft oder eine Geldbuße (§ 42 BDSG). Bei Ordnungswidrigkeiten (§ 43 BDSG) drohen auch Bußgelder gegen das Unternehmen (§ 30 OWiG/§ 130 OWiG).

Literatur

- BAADE, M. I./REISERER, K. (2022): Aktuelles zum Schutz von Geschäftsgeheimnissen – Handlungsoptionen für Arbeitgeber, DStR 2022, 890.
- BALTHASAR, S. (2008): Beweisverwertungsverbote im Zivilprozess, JuS 2008, 35.
- BfDI, Flyer Telearbeit und Mobiles Arbeiten, Juli 2020, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Flyer/Telearbeit.pdf?__blob=publicationFile&v=8.
- Datenschutzkonferenz, Kurzpapier Nummer 14 Beschäftigtendatenschutz, 24.9.2020, abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_14.pdf.
- Datenschutzkonferenz, Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, 17.7.2020, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf.
- ERB, V./SCHÄFER, J. (Hrsg.): Münchener Kommentar zum StGB, 3. Auflage 2019, München.
- FITTING, K. (Hrsg.): Betriebsverfassungsgesetz, 31. Auflage 2022, München.
- GILGA, C. (2020): Beschäftigtendatenschutz und Covid-19: Daten sicher im Homeoffice?, ZD-Aktuell 2020, 07113.
- GOLA, P./HECKMANN, D. (Hrsg.): Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Auflage 2022, München.
- GÖPFERT, B./MERTEN, F., SIEGRIST, S. (2008): Mitarbeiter als „Wissensträger“ – Ein Beitrag zur aktuellen Compliance-Diskussion, NJW 2008, 1703.
- GRECO, L./CARACAS, C. (2015): Internal Investigations und Selbstbelastungsfreiheit, NStZ 2015, 7.
- GROBYS, I./PANZER-HEERMEIR, A. (Hrsg.): Stichwort-Kommentar-Arbeitsrecht (zitiert als: SWK/Bearbeiter), 4. Auflage 2020, Baden-Baden.
- GSELL, B./KRÜGER, W./LORENZ, S./REYMAN, C. (Gesamt-Hrsg.)/LOOSCHELDERS, D. (Hrsg.): beck-online.GROSSKOMMENTAR, AGG, 2022.
- GÜNTHER, J./BERGMÜLLER, M. (2017): Digital Leadership – Mitarbeiterführung in der Arbeitswelt 4.0, NZA 2017, 546.
- HAU, W./POSECK, R. (Hrsg.): Beck'scher Online-Kommentar BGB, 63. Edition 2022.
- HAUSCHKA, C./MOSSMAYER, K./LÖSLER, T (Hrsg.): Corporate Compliance. Handbuch der Haftungsvermeidung im Unternehmen, 3. Auflage 2016, München.
- HAUSCHKA, C. (2004): Compliance, Compliance-Manager, Compliance-Programme: Eine geeignete Reaktion auf gestiegene Haftungsrisiken für Unternehmen und Management, NJW 2004, 257.
- HEERMANN, P. W./SCHLINGLOFF, J. (Hrsg.): Münchener Kommentar zum Lauterkeitsrecht, 3. Auflage 2022, München.
- HEISSNER, S./BENECKE, F. (2013): Compliance-Praxis im Wandel: Von der reinen Kontrolle zum Integrity Management, BB 2013, S. 2923.
- HOHMUTH, M. (2014): Die arbeitsrechtliche Implementierung von Compliance-Pflichten, BB 2014, 3061.
- IBEL, F. (2021): Whistleblower-Schutz – aktuelle Entwicklungen, MMR 2021, 929.
- KEMPTER, M./STEINAT, B (2017): Compliance – arbeitsrechtliche Gestaltungsinstrumente und Auswirkungen in der Praxis, NZA 2017, 1505.
- KIEHL, H./LUNK, S./OETKER, H (Hrsg.): Münchener Handbuch zum Arbeitsrecht, Band 4, 5. Auflage 2022, München.

- KLENGEL, D./MÜCKENBERGER, O. (2009): Internal Investigations – typische Rechts- und Praxisprobleme unternehmensinterner Ermittlungen, CCZ 2009, 81 (83).
- KRAFT, O./WINKLER, K. (2009): Zur Garantenstellung des Compliance-Officers – Unterlassungsstrafbarkeit durch Organisationsmangel?, CCZ 2009, 29.
- KRAMER, S. (Hrsg.): IT-Arbeitsrecht, 2. Auflage 2019, München.
- KÜHLING, J./BUCHNER, B. (Hrsg.): Datenschutz-Grundverordnung BDSG Kommentar, 3. Auflage 2020, München.
- LUDWIG, D. (2023): IT-Mitbestimmung und Datenschutz: Grenzen der Rechte des Betriebsrats, NZA, 2023, 321.
- MASCHMANN, F. (2018): Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht, NZA-Beilage, 2018, 115.
- MENGEL, A.: Compliance und Arbeitsrecht, Implementierung Durchsetzung – Organisation, 2. Auflage 2023, München.
- DIES./HAGEMEISTER, V. (2008): Compliance und arbeitsrechtliche Implementierung im Unternehmen, BB 2007, 1386.
- DIES. (2017): Internal Investigations – Arbeitsrechtliche Lessons Learned und Forderungen an den Gesetzgeber, NZA 2017, 1494.
- MÜLLER-GLÖGE, R./PREIS, U./SCHMIDT, I. (Hrsg.): Erfurter Kommentar zum Arbeitsrecht, 23. Auflage 2023, München.
- PAAL, B. P./PAULY, D. A. (Hrsg.): Datenschutzgrundverordnung Bundesdatenschutzgesetz, 3. Auflage 2021, München.
- RICRADI, R. (Hrsg.): Betriebsverfassungsgesetz mit Wahlordnung, 17. Auflage 2022, München.
- ROLFS, C./GIESEN, R./MEßLING, M./UDSCHING, P. (Hrsg.): Beck'scher Online-Kommentar Arbeitsrecht, 66. Edition 2022.
- SÄCKER, J./RIXECKER, R./OETKER, H./LIMPERG, B. (Hrsg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch, 9. Auflage 2021, München.
- SCHAEFER, S./BAUMANN, S. (2011): Compliance-Organisation und Sanktionen bei Verstößen, NJW 2011, 3601.
- SCHREIBER, A. (2019): Implementierung von Compliance-Richtlinien, NZA-RR 2010, 617.
- STÜCK, V. (2015): Compliance und Mitbestimmung, ArbRAktuell 2015, 337.
- TAEGER, J./POHLE, J (Hrsg.): Computerrechts-Handbuch. Informationstechnologie in der Rechts- und Wirtschaftspraxis, 37. Ergänzungslieferung, Stand: Mai 2022, München.
- SYDOW, G./MARSCH, N. (Hrsg.): DS-GVO BDSG, 3. Auflage 2022, Baden-Baden.
- WOLFF, A./BRINK, S. (Hrsg.): Beck'scher Online-Kommentar Datenschutzrecht, 43. Edition 2023.



Professor Dr. Andreas Katzer Herr Rechtsanwalt Professor Dr. Andreas Katzer berät seit mehr als zwei Jahrzehnten Unternehmen und Wirtschafts- sowie Sportverbände an der Schnittstelle zwischen Arbeits-, Steuer- und Sozialversicherungsrecht. Mit Schwerpunkten wie Fremdpersonaleinsatz, Auslandstätigkeit oder auch dem Profisport sind Compliance-bezogene Fragestellungen von hoher praktischer Relevanz in seiner Beratungstätigkeit. Seine Erfahrungen bei der Umsetzung eines ganzheitlichen Compliance-Ansatzes fließen in die Lehrtätigkeit am ZWW vollumfänglich ein, wo er seit vielen Jahren den Bereich des Arbeitsrechtes beim Compliance-Officer vermittelt.



Compliance, Kundenschutz und Product Governance

12

Daniel Sandmann

Inhaltsverzeichnis

12.1	Einleitung.....	315
12.2	Fallbeispiele und Unternehmens(fehl)entwicklung.....	317
12.2.1	Kreditversicherungen in Großbritannien.....	318
12.2.2	T-Mobile US – rural calls – Falsche Klingeltöne in den U.S.A.....	320
12.3	Unternehmensentwicklung.....	321
12.3.1	Von der rechtsgebietsbezogenen Compliance zur prozessbezogenen Compliance.....	323
12.3.2	Kundenschutz und Produkt-Compliance in Abgrenzung zu Qualitätssicherung und Produkthaftung.....	323
12.3.3	Erkenntnisquellen, Risikobewertung und Unternehmenssteuerung.....	324
12.4	Produkt-Compliance – Prozesse am Beispiel Finanzindustrie.....	326
12.5	Fazit und Ausblick.....	327
	Literatur.....	327

12.1 Einleitung

Ein Compliance-Management-System in Unternehmen zu implementieren bedeutete in einer langjährigen Praxis, ausgewählte Teilrechtsgebiete zu einem „Compliance-Risiko“ zu klassifizieren. So gab es Programme zur Kartellrechts-Compliance, Anti-Korruptions-Compliance, Kapitalmarkt-Compliance etc. Apple Inc. (als derzeit nach Marktkapitalisierung global größtes Unternehmen) fasst es für die eigene Compliance zusammen:

D. Sandmann (✉)

Rechtsanwalt Daniel Sandmann, München, Deutschland

E-Mail: sandmann@mindsol.de

„A number of compliance functions are deeply integrated into our business organization. Apple’s Business Conduct and Global Compliance team focuses on Business Conduct, Political Compliance, Export and Sanctions Compliance, Health Compliance, Antitrust Compliance, and Anti-Corruption Compliance.“¹

Management des jeweiligen Risikos hieß und heißt in der Folge, bekannte und bewährte Elemente eines Compliance Management Systems auf da jeweilige Rechtsgebiet anzuwenden, darunter Risikoanalysen, Trainings und entsprechende Richtlinien. In der Folge bauten Compliance-Funktionen in deutschen Unternehmen in den vergangene 20 Jahren seriell Gerüste zur Bekämpfung von Korruption, von Kartellen, von Geldwäsche und Terrorismusfinanzierung und für viele weitere Teilrechtsgebiete. Erst viel später wurden auch Querschnittsthemen integriert, etwa zum Compliance-Management von Drittseiteisiken, bei denen Vertriebe, Dienstleister und Zuliefernde systematisch im CMS eingefügt wurden, ohne dass es dabei nur um ein spezifisches Risiko ging. Hier entwickelte sich der Ansatz, dass nicht in einem durch Rechtsgebiete geordneten Vorgehen, sondern entlang der Wertschöpfungskette Compliance-Risiken identifiziert und gehandhabt wurden. Neuere Kodifizierungen haben dies aufgenommen. Die Ansätze im UK Bribery Act und die EU-Vorgaben zur Überwachung von Lieferketten sind nur zwei Beispiele. Gleichzeitig wird bei der ersten Betrachtung offensichtlich, dass hier stets ausgewählte Zwischenelemente der Wertschöpfung eine Rolle spielen. Einige Compliance-Funktionen gehen weiter und haben bereits eine umfassende Ausweitung vorgenommen, die einen Compliance-Überblick von der Produktschöpfung bis zum Einsatz bei der Kundschaft umfasst. Erst damit werden auch Product Compliance und Kundenschutz tatsächlich relevante Größen und die vormalige Ordnung von Compliance nach Rechtsgebieten wird aufgelöst zu Gunsten einer funktions- und prozessübergreifenden Compliance (vergl. am Beispiel Dieselskandal Grützner/Boerger/Momsen: Die „Dieselaffäre“ und ihre Folgen für Compliance-Management- Systeme – Evolution durch Einbeziehung des Bereichs Produkt-Compliance in ein CMS, CCZ 2018, 50, 53).

Damit wird ein neuer Ansatz möglich: Produkt-Compliance bezieht sich daher nicht lediglich auf die Erfüllung von Kundenschutz- oder Sicherheitsstandards. Es verschiebt auch nicht Qualitätssicherung oder Gewährleistungsabwicklung in den Zuständigkeitsbereich der Compliance-Funktion. Vielmehr stellt die Compliance mit den üblichen Maßnahme-Katalogen sicher, dass die anderen Funktionen ihre Ziele erreichen und das Unternehmen vor unberechtigter Inanspruchnahme und Reputationsrisiken noch besser geschützt wird. Produkt-Compliance umfasst eine Vielzahl von Aspekten, beginnend mit den rechtlichen Anforderungen, aber auch auf Marktusancen und rationale, angemessene Kundenerwartungen an Eigenschaften von Produkten oder Dienstleistungen aufbauend. Vor allem aber ist Produkt-Compliance nicht lediglich die Einhaltung der Anforderungen aus den verschiedensten schon bestehenden Standards für Technik, Umwelt- und Gesund-

¹Vergl. <https://www.apple.com/compliance/> zul. abgerufen am 29. Januar 2024.

heitsschutz, Nachverfolgbarkeit, Produkthaftungsrecht oder gar Produktstrafrecht. Jeder weiß um die nichtzählbare Zahl an komplexen Normen zu Kennzeichnungspflichten, Rücknahmeverpflichtungen, Haftung und Gewährleistung. Die Product Compliance integriert diese Themen, ohne sie in ihren technischen Details zu vervielfachen oder zu perpetuieren. Produkt-Compliance beinhaltet aber auch die nicht geschriebenen und auch kaum beschreibbaren Dimensionen, wie sie vergleichbar etwa bei dem Abgleich mit ESG-Standards gefragt werden – was ist der Nutzen für Kundschaft und Gesellschaft? Erfüllen wir als Unternehmen die Erwartungen, die andere an unsere Produkte und Dienstleistungen berechtigterweise haben?

12.2 Fallbeispiele und Unternehmens(fehl)entwicklung

Durch alle Sektoren, Branchen und über alle Kontinente und Rechtssysteme hinweg haben in den vergangenen 20 Jahren Fehlentwicklungen und Missstände bei den Produkten schlagzeulenträchtige Skandale gezeitigt, gigantische finanzielle Auswirkungen gehabt und bisweilen sogar Menschenleben gekostet. Gleich ob Gammelfleisch in der Lebensmittelindustrie, Steuerausfälle in Milliarden-Höhe durch Cum-Ex Strukturen, Sicherheitsrisiken bei Flug- und Fahrzeugbauern, Missstände bei Pharma und Health Care-Anbietern, Behörden und öffentliche Institutionen – schnell fallen den Compliance-Themen zugeneigten Lesenden Namen und Nachrichten ein, in denen intern durchaus bekannte, aber nach außen verborgene Fehler, Mängel und Gefahren sich realisierten und erst dadurch bekannt wurden. Abhilfe wurde immer zugesagt – die langfristigen Erfolge dieser Abhilfemaßnahmen stellen sich jedoch nicht immer ein. Wir betrachten hier zwei Fallbeispiele, ihre Zusammenhänge mit der Unternehmensentwicklung und die Rolle von Compliance-Funktionen und externe Überwachungsmechanismen und rechtliche Anforderungen. Ganz überwiegend werden dabei die Zusammenhänge offenbar, bei denen Schwächen bei Produktinnovation, erodierende Margen und ver-spätete Reaktion auf Marktentwicklungen zu Fehlverhalten und Missständen führen. Frühzeitige Berücksichtigung von Compliance-Aspekten und Antizipation von Entwicklungen in den Märkten, in den Lieferketten und bei den rechtlichen Anforderungen an Produkte helfen hingegen, bei Entscheidungen über die Ausrichtung der Unternehmensorganisation und der Produkt- und Dienstleistungspalette die finanziellen Lockungen eines Fehlverhaltens deutlich zu reduzieren. So lässt sich aus der Sicht der Produkt-Compliance in jedem Fall von Missständen eine direkte Verbindung zur Unternehmensentwicklung zurückverfolgen. Seien es Einsparmaßnahmen in der Produktion eines Flugzeugherstellers (Boeing), Spaltung von Vergütung und Risiko in den Bonus-systemen in der Finanzindustrie (Subprime) oder mangelnde Investitionen in die Weiterentwicklung sparsamere Kfz-Motoren (Diesel-Skandal) – die Compliance-Probleme folgen aus Entscheidungen, die langer zuvor die Rahmenbedingung definiert haben, aber in der Kausalkette häufig nicht erkannt werden (sollen).

12.2.1 Kreditversicherungen in Großbritannien

Ein Skandal, dessen Abarbeitung zwei Jahrzehnte dauern sollte und in dessen Folgen primär britische Banken insgesamt mehr als 60 Mrd. Pfund an Ausgleichszahlungen und Sanktionen zahlen mussten, war der Verkauf von Restschuldversicherungen gegen Zahlungsprobleme an Privatkunden und kleine Unternehmen als Kreditnehmer im Vereinigten Königreich (vergl. Frances Coppola, The U.K.'s Biggest Financial Scandal Bites Its Biggest Bank – Again in Forbes, 31.7.2019 <https://www.forbes.com/sites/francescopolpa/2019/07/31/the-u-k-s-biggest-financial-scandal-bites-its-biggest-bank-again/>, zuletzt abgerufen 17. August 2024). Diese Payment Protection Insurances („PPI“) sollten bei Finanzierungen jeder Art – gleich ob Baufinanzierung, Autokredit oder dem Ratenzahlungsplan für die neue Wachmaschine – Sicherheit bieten, in dem eine Versicherung die Zahlung der Raten übernommen hätte, wenn Schicksalsschläge wie Krankheit, Arbeitslosigkeit oder Tod zu finanziellen Engpässen bei den Kreditnehmenden geführt hätten. Was sich zunächst nach einem sinnvollen Schutz für Schuldnerinnen und Schuldner anhört, war in der konkreten Gestaltung jedoch mit deutlichen Nachteilen aufgrund der Struktur der Produkte und der Vertriebspraktiken verbunden. So wurden für die Vermittlung dieser Restschuldversicherungen durch Banken, Autohandel, Elektronikmärkten und andere hohe Provisionen gezahlt, meist über 60 % der von der Kundschaft gezahlten Versicherungsprämie. Die Kosten für den Risikoschutz waren hingegen vergleichsweise gering. Die hohen Margen machten das Produkt für die vermittelnden Stellen finanziell sehr attraktiv und in den 1980er und 1990er-Jahren verbreiteten sich die Produkte nicht aufgrund einer originären Nachfrage von Verbrauchern, sondern weil diese mit den Krediten fest gebündelt wurden. Verbraucher bekamen also keine Finanzierung, ohne gleichzeitig ein solches Versicherungsprodukt zu erwerben. Gleichzeitig hatten die PPI für die finanzierenden Banken noch einen anderen Vorteil – der bestehende Schutz verringerte ihr Kreditrisiko. Während sie sonst bei diesen Schicksalsschlägen Probleme hatten, die Kreditraten zu erhalten, sprang nun eine Versicherung ein.

Ab Ende der 1990er-Jahre deckten zunächst Verbraucherschutzorganisationen auf, dass es zu unlauteren Vertriebspraktiken kam. Sie hatten durch Inkognito-Käufe, das sogenannte Mystery-Shopping, geprüft, wie sich damals bereits durch die Versicherungs- und Bankaufsicht regulierte Produkte und Vertriebspraktiken in der Wirklichkeit darstellten. Neben der zwangswise Bündelung mit Kreditverträgen war dies vor allem das sog. Misselling, das heißt die Vermittlung z.B. auch an Menschen, die dort keine Risiken hatten, etwa, weil sie als Selbstständige oder Beamte nicht arbeitslos werden konnten oder die bereits ausreichende andere Absicherungen hatten. Weitgehende Leistungsausschlüsse in den Verträgen und Hürden verschiedenster Art bei der Geltendmachung von Ansprüchen taten ein Übriges, sodass Verbraucher häufig das Gefühl hatten, die Versicherungen seien völlig wertlos. Dabei war das Volumen der jährlichen Prämien zu der Zeit bis auf 5 Mrd. Pfund gestiegen. Wenig später wurden auch die Wettbewerbsbehörde und die Finanzaufsicht tätig, prangerten Missstände an und veröffentlichten regulatorische Vorgaben für den Vertrieb. Ab 2006 wurden dabei von der Finanzaufsicht auch Sanktionen verhängt. Nach-

dem diese nicht wirklich durchschlagende Wirkung hatten und zudem in größerem Umfang auch in Zivilverfahren vor den britischen Gerichten die zweifelhaften Vertriebspraktiken aufgearbeitet wurden, kam es schließlich zu einer großen Auseinandersetzung, als die britischen Bankenvereinigung eine retrospektive Anwendung der neuen Regeln der Finanzaufsicht gerichtlich untersagen lassen wollte – und unterlag. Damit wurde 2011 ein Kompensationsprogramm für die Versicherungskundschaft ins Leben gerufen, nach dem Banken und teilweise Versicherungen über einen Zeitraum von 8 Jahren die Kundschaft entschädigen mussten. Je nach Marktanteilen im Verbrauchergeschäft waren daraus erhebliche finanzielle Verpflichtungen für die Industrie erwachsen, als am stärksten involvierte Institute mussten die Banken für den Zeitraum 2010 bis 2019 Rückstellungen von über 57 Mrd. Pfund für dieses Thema bilden, davon wurden alleine von der Lloyds Bank über 22 Mrd. Pfund Entschädigungen an Kunden ausgezahlt (vgl. Georgette Fernandez Larisi, Scandal or Repetitive Misconduct: Payment Protection Insurance (PPI) and the not so Little „Skin in Lending Games“ in Moral Cents Vol. 9 Issue 1, Winter/Spring 2020, S. 9).

Jedoch kam es auch bei diesen Kompensationsprogrammen bei Lloyds und anderen Banken zu Praktiken, die die Geltendmachung von Ansprüchen der Verbraucher erschwerten. Im Falle von Lloyds gehörte dazu etwa Falschaussagen über den Umfang und das Ergebnis der Prüfungen der Beschwerdesachbearbeitenden (vgl. Financial Conduct Authority, Lloyds Banking Group fined £117 m for failing to handle PPI complaints fairly: Examples of customer experiences, London 2015, <https://www.fca.org.uk/publication/corporate/lloyds-ppi-complaints-examples-customer-experiences.pdf>, zuletzt abgerufen 29. Januar 2024). Die Finanzaufsicht FCA veröffentlichte diese Missstände und bebußte Lloyds Bank mit 117 Mio. Pfund.

Zu den Feststellungen in diesem Verfahren gehörte, dass den Sachbearbeitenden im Beschwerdemanagement Weisungen erteilt worden waren, damit diese dabei von einer grundsätzlichen Compliance der Vertriebsprozesse mit den regulatorischen Vorgaben ausgehen sollten und somit die Kundschaft beweisbelastet war, dass dem nicht so war. Gerade durch die Mystery Shoppings und die Zivilprozesse war jedoch schon mannigfaltig nachgewiesen worden, dass eben keine grundsätzliche systematische Compliance mit den Vorgaben für den Vertrieb bestand (vgl. Financial Conduct Authority, Lloyds Banking Group fined £117 m for failing to handle PPI complaints fairly, final notice, <https://www.fca.org.uk/publication/final-notices/lloyds-banking-group-2015.pdf>, zuletzt abgerufen 29. Januar 2024).

In der Folge wurden bei allen beteiligten Banken Compliance-Programme gestärkt und die von der FCA und anderen Behörden kritisierten Missstände einer laufenden Compliance-Überwachung unterworfen. Wichtiger aber ist, dass es in Großbritannien, aber auch auf EU-Ebene regulatorische Reaktionen gab, der Umsetzung und laufende Befolgung zu einer ganzheitlichen Sicht auf Produkte, Vertriebskanäle und Eignung für Kunden bezog. Das Ausmaß des Skandals hatte wesentlichen Anteil an der Beschleunigung wichtiger regulatorischer Veränderungen. Das Thema Verbraucherschutz rückte ins Zentrum der Ziele von Finanzaufsichtsbehörden, die sich zuvor eher dem System des Finanzsektors als Ganzem verpflichtet sahen, nicht aber speziell dem Verbraucherschutz. Die herausstechenden Ergebnisse dieser Umbrüche sind zahlreiche ambitionierte Rechtsakte der europäischen

Union: Die revidierte Finanzmarktrichtlinie (MiFID II/MiFIR), die Versicherungsvermittlungsrichtlinie (IDD) und die PRIIPS-Verordnung. Es gab aber auch gezielte-EU weite Studien der europäischen Versicherungsaufsicht EIOPA speziell zu PPI und ähnlichen Produkten. Für die Finanzindustrie enthalten diese EU-Vorgaben einen gemeinsamen Nenner: Die Produktanbieter und Vertriebe müssen gegenüber deren Kunden stets ehrlich, redlich und professionell in deren bestmöglichem Interesse handeln. Hieraus leiten sich die wesentlichen Leitmotive ab, die für die Compliance-Praxis mit vielfältigen Neuerungen verbunden sein werden. Das Prinzip des bestmöglichen Kundeninteresses führt zu weitgehenden Eingriffen in Vergütungssystem und Vertriebssteuerung, aber auch die Gestaltung von Produkten. Die Vermeidung und Identifizierung von Interessenkonflikten hat zukünftig eine vorrangige Stellung, um diesem Schutzauftrag gerecht zu werden. Die Professionalisierung der internen und externen Mitarbeiter in Produktentwicklung und Vertrieb muss sicher gestellt werden. Vor allem ist aber ein Zeitmoment wichtig. Gegenwärtig reicht die Prozesskette der Produkterschaffung bis zu dem Zeitpunkt, an dem der Vertrieb es dem Kunden verkauft. Mit der Vorgabe „stets“ signalisiert die Richtlinie, dass die Überwachung der Einhaltung der Vorgaben weit über diesen Moment hinausreicht. Eigenschaften des Produktes oder ein ungünstiges Risiko-/Renditeverhältnisse spiegeln sich hingegen der Einschätzung des „Retail Risk“ nieder. Dies kann sich niederschlagen in Strafen oder in Produktverboten, vor allem aber auch in der Möglichkeit, Kundeninteressen im Wege des Zivilrechts durchzusetzen, das hier ein erhöhtes Haftungspotenzial birgt. Nicht zuletzt können auch Produkte durch die Aufsichtsbehörden verboten werden, was jedoch bisher nur in sehr wenigen Fällen umgesetzt wurde. Das passgenaue Zusammenspiel zwischen den Wünschen und Bedürfnissen des Kunden und dem Leistungsspektrum des Produkts muss bestmöglich über die Lebensdauer des Produkts gewährleistet sein. Hierzu tragen vielfältige Auklärungs- und Beratungspflichten bei. Die Kundschaft für jegliche Finanzprodukte muss sich mehrschichtigen Tests unterziehen lassen. Verständnis für die individuellen Bedürfnisse und Risikotragfähigkeit der Kundschaft muss verbessert und so berücksichtigt werden, dass die nachprüfbar ist. Hierzu gehören die Prozesse Eingruppierung in Zielmärkte, die Erforschung von Wünschen und Bedürfnissen des Kunden, aber auch die Prüfung von Geeignetheit und Angemessenheit.

Umfassende Überwachungs- und Berichtspflichten der Compliance-Funktion sollen die laufende Einhaltung sicherstellen. Die Produkt-Compliance hat damit Einzug in die Regulierung gehalten und bietet einen Ansatz, der weit über die Finanzindustrie hinaus zur Anwendung kommen kann.

12.2.2 T-Mobile US – rural calls – Falsche Klingeltöne in den U.S.A.

Aber nicht nur bei Produkten, sondern auch bei technischen Dienstleistungen wie der Mobiltelefonie kann Produkt-Compliance beitragen, Risiken deutlich zu reduzieren. Ein Fallbeispiel für solche Risiken ist ein Verfahren der U.S. Behörde für Telekommunikation, der Federal Communications Commission („FCC“). Die FCC hat den führenden Mobilfunkanbieter, T-Mobile US, im Jahre 2018 mit einer Zahlung von 40 Mio. US-Dollar sanktionsiert.

tioniert und zum Ausbau eines speziellen Compliance-Programms verpflichtet, da T-Mobile US in ländlichen Gebieten das Mobilfunknetz nicht ausreichend ausgebaut hatte, so dass teilweise keine Mobiltelefonverbindungen aufgebaut werden konnten. Um dies gegenüber der eigenen Kundschaft zu verbergen, wurden bei Anrufversuchen von oder zu Mobilfunkkunden Freizeichen beim Verbindungsaufbau eingespielt, obwohl keine Verbindung bestand. Die FCC hielt dazu fest:

„.... es Diensteanbietern untersagt ist, bei Telefongesprächen falsche Freizeichen vorzuspielen. Falsche Freizeichen lassen den Anrufer glauben, dass das Telefon beim Angerufenen läutet, obwohl dies nicht der Fall ist. Der Anrufer kann dann auflegen, weil er denkt, dass niemand den Anruf entgegennehmen kann. Falsche Freizeichen erwecken auch den irreführenden Eindruck, dass der Dienstanbieter des Anrufers nicht verantwortlich ist, wenn der Anruf fehlschlägt. Falsche Freizeichen sind ein Problem bei Anrufen in ländlichen Gebieten und sind ein Symptom für die Probleme, die mit der schlechten Qualität und dem schlechten Abschluss von Anrufen in ländlichen Gebieten verbunden sind.“ (Federal Communications Commission/T-Mobile US Inc., DA 18-373, Final Order April 16, 2018, S. 1).

Die FTC nannte die große Bedeutung des Verstoßes: „Die Probleme beim Verbindungsaufbau von Anrufen in ländlichen Gebieten haben erhebliche und unmittelbare Auswirkungen auf das öffentliche Interesse. Sie führen dazu, dass Unternehmen in ländlichen Gebieten Umsatzeinbußen erleiden, dass medizinische Fachkräfte Patienten in ländlichen Gebieten nicht erreichen können, dass Familien von ihren Angehörigen abgeschnitten werden und dass es zu gefährlichen Verzögerungen bei der Kommunikation im Bereich der öffentlichen Sicherheit kommen kann.“ (Federal Communications Commission/T-Mobile US Inc., S. 1).

Der Fall zeigt, dass noch bei den Abwägungen in den Jahren 2016–2017, ob die regulatorischen Standards erfüllt werden, und den kommerziellen Interessen, hier der erforderliche, aber nicht einfach mögliche bzw. wirtschaftlich lohnende Netzausbau auch zu Lasten der rechtlichen Anforderungen ausgeht, obwohl deutsche wie U.S.-Unternehmen wissen, dass die Sanktionen in den U.S.A. massiv sein können. Mit Blick auf Vorermittlungen und Anfragen der FCC lange vor 2018 und dem 2015 vorher bekannt gewordenen Volkswagen Diesel-Skandal ein aufschlussreiches Indiz hinsichtlich der Compliance-Kultur.

In der Folge des Vorgehens der FCC musste T-Mobile ein eigenes Compliance-Programm für die Vorgaben hinsichtlich des Mobilfunk-Betriebs in ländlichen Gebieten ausbauen mit speziellen Anforderungen an die Kompetenz und Seniorität der Leitungspersonen, mit Trainings- und Kommunikationsmaßnahmen und mit sehr detaillierten Überwachungs- und Berichtspflichten.

12.3 Unternehmensentwicklung

Die Produkt-Compliance wird in der Unternehmensentwicklung daher bei Unternehmen mit einem hohen Reifegrad sehr früh berücksichtigt. Unternehmensentwicklung umfasst hier eine weite Spanne von strategischem Business Development,

Forschung & Entwicklung, Vertriebspartnerschaften, Preispolitik, Personalentwicklung, Produktion, Restrukturierung, Maßnahmen zur Erschließung neuer Zielmärkte, M&A mit Relevanz für Produkt, Vertrieb oder Service, Digitalisierungsprojekte, Beschwerdemanagement, Marketing. Dies muss nicht in formalisierten Prozessen oder durch direkte Beteiligung der Compliance-Funktion geschehen. Im Produktsicherheitsrecht wurde hier der Begriff der „Wirtschaftakteure“ in die gesetzlichen Regelungen aufgenommen (vergl. § 2 Nr. 29 Produktsicherheitsgesetz), um eben das Zusammenspiel verschiedenster Bereiche inner- und außerhalb von Unternehmen zu umfassen (vergl. Polly, Lach: Das neue Produktsicherheitsgesetz – Empfehlungen an Wirtschaftsakteure zur Compliance in der Produktsicherheit, CCZ 2012, 59, 60). Die Berücksichtigung bei Abwägungen und unternehmerischen Entscheidungen ist – auch nach Business-Judgement-Rule-Gesichtspunkten – entscheidend. Expertise für die Themen herrscht auch bei Geschäftsleitungspersonal mit Zuständigkeiten für Produkt oder Vertrieb, hier müssen nur Interessenkonflikte vermieden werden und Incentives die Produkt-Compliance-Ziele fördern.

Folgende Punkte sind in jedem der oben genannten Bereiche der Unternehmensentwicklung zu analysieren, um Produkt-Compliance-Risiken zu erkennen:

- Wettbewerbsdruck bei Innovation und Margen
- Kräfteverhältnisse Produktgeber, Vertrieb und Kunden, Definition vulnerable Kundengruppen.
- Produkte oder Initiativen mit hoher Visibilität, etwa durch Ankündigungen in Medien, gegenüber Investoren oder anderen wesentlichen Einflussgruppen
- Angemessene Erwartungen der Kundschaft, selbst durch Marketing geweckte Erwartungen und tatsächliche Leistungen und Fähigkeiten
- „Follow the money“ – wo sind ungewöhnlich hohe oder Margen, wo sind die Marktverhältnisse eher schwierig, die regulatorischen Anforderungen schwer zu erreichen und Margen vergleichsweise gering?

Die Compliance-Funktion kann hier früh das Bewusstsein schaffen, beratend tätig werden, genau wie weitere Bereiche, die mit den vorgenannten Themen Berührungs punkte haben. Gerade das Prinzip „Follow the Money“ führt rasch zu Einblicken und Praktiken mit erhöhten Compliance-Risiken, wie es auch sonst bei Ermittlungen hilft (Borrell and Cashinella: Crime in Britain Today, London, 1975). Tatsächlich sind auch in den rechtlichen Regimen, die sich mit Produkt-Compliance beschäftigen, deutliche persönliche Verantwortlichkeiten für die Geschäftsleitungen vorgesehen, an die berichtet werden muss (vergl. Buck-Heeb: Compliance bei vertriebsbezogener Product Governance – Neuerungen durch die MiFID II bzw. das Kleinanlegerschutzgesetz, CCZ 2016, 2, 3), die sich nach den bekannten Grundsätzen für Compliance durch eine entsprechend aufgestellte und tatsächlich gelebte Compliance auch ihre Haftungsrisiken reduzieren können.

12.3.1 Von der rechtsgesetzlichen Compliance zur prozessbezogenen Compliance

Die Perspektive Produkt-Compliance durchbricht die gängigen Herangehensweisen vieler nach den eigenen Rechtsthemen ausgerichteter Compliance-Programme. Mit der hier dargestellten Methodik lassen sich vielfältige rechtliche Risiken bewerten und handhaben, dabei immer in Orientierung an den Wertschöpfungsketten des Unternehmens. Auch Themen wie Korruptionsrisiken, Bekämpfung von Geldwäsche und Terrorismusfinanzierung, die Einhaltung von Sanktionen oder die Kartellrechts-Compliance können im Rahmen von Produkt-Compliance Prozessen integriert werden. Nur wer die Wertschöpfungs- und Vertriebsketten kennt, kann auch diese Risiken einschätzen und für angemessene Compliance sorgen. Mängel beim Produkt erzeugen gleichzeitig hohe Anfälligkeitkeiten etwa für korruptive Handlungen, um diese zu verbergen, um Zulassungen zu erhalten etc. Nicht wettbewerbsfähige Produkte werden durch kick backs, Marketingzuschüsse oder Geschenke und Einladungen doch noch zum Vertriebserfolg gekauft. Die Einbettung von Produkt-Compliance erfolgt aber nicht durch Compliance-eigene Prozesse, sondern die Compliance wird mit den Geschäftsprozessen verknüpft. Produkt-Compliance ist daher immer prozessbezogen zu gestalten und kann nur funktionieren, wenn es keine Paralleluniversum gibt, sondern Compliance eingebettet ist in Denken und Handeln in der Unternehmens- und Produktentwicklung sowie den Vorgaben für den Vertrieb.

12.3.2 Kundenschutz und Produkt-Compliance in Abgrenzung zu Qualitätssicherung und Produkthaftung

Ist Produkt-Compliance nicht eine Doppelung dessen, was sonst auch schon in Funktionen wie dem Qualitätsmanagement, dem Risikomanagement, dem Arbeitsschutz oder der Revision geschieht? Nein. Produkt-Compliance kann diesen Funktionen helfen, ihre Ansätze mit dem eines Compliance-Management-Systems zu verbinden und auch dort für systematische Risikoanalysen, Training und Kommunikation, klare Vorgaben und auf diese bezogene Prüf- und Verbesserungsprozesse sorgen. Meist ist dies aber gar nicht erforderlich. Produkt-Compliance ist eine ergänzende Ebene, die viel mehr auf die außerhalb technischer Normen liegenden Anforderungen abstellt. Welche Erwartungen weckt das eigene Marketing? Wie kompetent sind die Mitarbeitenden im Vertrieb und was motiviert sie, versprechen sie eventuell das Blaue vom Himmel um ihre Zielvorgaben zu erreichen? Gibt es Belohnungen für schnelles und kurzfristig orientiertes Handeln, oder stehen langfristige Bindungen mit Vertrieb und Kundschaft im Vordergrund der Incentive-Systeme? Diese Themen verlassen die Prüfroutinen der technischen Compliance und stellen lediglich sicher, dass es auch für diese Zuständigkeiten und Informationsweitergaben gilt. In dem Fallbeispiel der Payment Protection Insurance konnten die Finanzaufsichtsbehörden lange in den Versicherungen und den Bankhäusern keine Defizite feststellen. Erst der Realitätstest im Mystery Shopping hat die tatsächlichen Verkaufspraktiken aufgedeckt, die mit der in

Richtlinien und Schulungsdokumentationen festgehaltene Idealvorstellung nicht viel zu tun hatte. Auch bei T-Mobile US funktionierte das Netz – da wo es vorhanden war. Auch dort hätte eine interne Qualitätssicherung vermutlich nicht einmal Auffälligkeiten festgestellt – weil die Frage der Erreichbarkeit auch in anderen Gegenden keine Frage der technischen Mängel des vorhandenen Netzes war, sondern an erster Stelle eine Frage der Unternehmensentwicklungen bei der Entscheidung über die Ressourcenallokation im Netzausbau.

Kurzum: Produkt-Compliance hat eine Verbindung zu allen Funktionen, die bei der Entwicklung, Herstellung, Vermarktung und den Services rund um Produkte und Dienstleistungsangebote eines Unternehmens involviert sind. Compliance kann immer von diesen Funktionen lernen und profitieren und manchmal auch dort Anregungen geben. Produkt-Compliance bedeutet aber, die rein technische Betrachtungsebene zu verlassen und die externen Erwartungen der verschiedensten Stakeholder einzubeziehen, inklusive des kulturellen Kontextes und der verschiedenen Usancen in den jeweiligen Märkten. Das Testen der Produkte ermöglicht wiederum, die Übereinstimmung von Zielmarktdefinition und den tatsächlichen Kundengruppen und deren Bedürfnissen über den Lebenszyklus des Produkts immer wieder zu betrachten. Gerade hierdurch ergeben sich Synergiepotenziale zu anderen Compliance-Themen wie der Vorbeugung von Geldwäsche oder Fraud. Produkte mit kritischem Potenzial für Kunden können systematisch identifiziert werden. Auch wenn die Richtlinien den Umgang mit derartigen Produkten nicht genau vorschreiben, werden ein rascher Austausch mit geeigneteren Produkten oder ähnliche Maßnahmen die Kundenbindung erhöhen. Zudem werden kritische Produkte unter Umständen gar nicht erst zur Marktreife gebracht, was Entwicklungsaufwand und Haftungspotenzial bereits auf einer frühen Stufe der Unternehmensentwicklung reduzieren kann.

12.3.3 Erkenntnisquellen, Risikobewertung und Unternehmenssteuerung

Ständige Kommunikation und enge Kontakte zu allen involvierten Bereichen, vor allem „dem Business“ sind unerlässlich für den Erfolg der Produkt-Compliance. Tabellen mit technischen Risikoanalysen oder klassischen Compliance-Trainings und -Richtlinien sind in dieser Kommunikation nachteilig und nicht förderlich. Wo es gut läuft und wo es knirscht, erfährt man beim Lunch und nicht in einer Besprechung mit 15 Teilnehmenden, die über die Eintrittswahrscheinlichkeiten eines Risikos sinnieren, ob dies nun eher „3“ oder schon „4“ (oder eine beliebige Frage oder Prozentzahl) sein müsste. Selbstverständlich ist aber auch eine strukturierte Herangehensweise erforderlich, die dann vorhanden Informationen einbinden kann (instruktiv für mittelständische Maschinebauer z. B. Remberg in Moosmayer, Compliance-Risikoanalyse, § 6. Compliance-Risikoanalyse in mittelständischen Unternehmen, Rn. 37). Dazu können gehören:

- Wettbewerbsanalysen, z. B. aus Marketing
- Preisbestimmung zuständigen Funktionen

- Mängelstatistiken aus der Qualitätssicherung
- Geschäftszahlen aus dem Controlling,
- Informationen über Incentive-Systeme und die tatsächlichen Incentives aus Human Ressources oder Vertrieb
- Beschwerdemanagement und den Rechtsabteilungen Informationen über Reklamationen, Unzufriedenheit oder gar rechtsförmlich verfolgte Ansprüche,
- Informationen aus Whistleblowings.

Verbände informieren über Themen auf der regulatorisch-politischen Agenda, die relevant werden können, und wenn die Produkt-Compliance auch auf die Verlautbarungen von Organisationen, die die Kundschaft repräsentieren – gerade Verbraucherschutzorganisationen – achtet, ist dies häufig ebenfalls eine gute Quelle, um frühzeitige auf relevante Entwicklungen aufmerksam zu werden. Im internationalen Konzern kann man auch Trends feststellen, die in bestimmten Ländern – häufig der für Compliance-Themen weiter prägende anglo-amerikanische Rechtsraum – beginnen und sich dann langsam evolutiv durchsetzen (Fallbeispiel Skandal um Payment Protection Insurance, begonnen in Großbritannien Ende des letzten Jahrtausends: In Deutschland werden diese Produkte ab 2025 ebenfalls strenger reguliert.).

Die Erkenntnisse aus diesen Quellen helfen rasch und erlauben ein zeitnahe Monitoring auf abstrakter Ebene. Wie mit den Lunches können aber komplementäre Maßnahmen sehr helfen, angefangen bei dem sogenannten Random Walk – man schaut sich einfach mal Teile der Wertschöpfungskette selbst genauer an – aber auch das Mystery Shopping, um die Realität aus Kundensicht kennenzulernen.

Der Einsatz von quantitativen Messgrößen zur Bestimmung des „Product Compliance Risikos“ ermöglicht hierbei eine laufende Überwachung und ein Reporting, mit dem kundenrelevante Risiken in der Produktstruktur selber, aber auch bei Servicefaktoren wie Nachberatung, Umgang mit Schäden oder Produkten mit schlechter Perzeption seitens der Kundschaft rasch angegangen werden können. Dies kann erheblich zur Reduzierung von Haftungs- und Reputationsrisiken genutzt werden.

Auf Basis dieser Datenpunkte können Risiken zumindest näherungsweise bestimmt werden, wobei gerade bei an Verbraucher gerichteten Produkt- und Dienstleistungsangeboten Risiken auch davon abhängen, wie schnell aus einem Einzelfall ein Skandal gemacht werden kann. Dies wiederum hängt ab von der dynamischen Sensitivität der Märkte und Medien (vergl. Jahn/Guttmann/Krais, Krisenkommunikation bei Compliance-Verstößen, § 14 Rn. 3).

Die so bewerteten Risiken können dann in den Entscheidungsprozessen der Unternehmens- und Produktentwicklung gesteuert werden. dazu gehört auch, dass z. B. in Szenarien geprüft wird, wie sich ein Produkt in bestimmten Situationen verhält (wenn es nicht schon anderweitige Prüf- und Zulassungsprozesse gibt wie z. B. bei Pharma- und Medizinprodukten). Ebenso gehört dazu auch, dass im Reklamations- und Beschwerdemanagementprozessen ein laufendes Monitoring stattfindet und bei Hinweisen auf systematische Mängel oder Missstände im Vertrieb an diesen Stellen geeignete

Gegenmaßnahmen getroffen werden. Die inhaltliche Behandlung derartiger Beschwerden sollte sich ebenfalls nach etablierten Maßstäben des Reputationsrisikomanagements richten.

12.4 Produkt-Compliance – Prozesse am Beispiel Finanzindustrie

Auch wenn die Finanzindustrie und die Compliance dort aufgrund der hohen Regulierungs-dichte besondere Anforderungen hat, so lohnt für die Etablierung einer Produkt-Compliance auch außerhalb der Finanzindustrie ein Blick auf einige wesentliche Aspekte.

Dies beginnt mit den Anforderungen, dass die verantwortlichen Personen – Geschäftsleitung und erste Führungsebene – als Kollektiv die eigenen Produkte kennen und verstehen können müssen. Was banal klingt, ist eine Grundvoraussetzung für erfolgreiche Unternehmensentwicklung und fachlich fundierten Austausch. Welche Ressorts bei dem Thema Produkt-Compliance eine Rolle spielen, ist eingangs dargestellt worden und insofern sind auch für Human Resources zuständige Geschäftsleitungsmitglieder ebenso zu involvieren wie die für Marketing oder eben Vertrieb, Marktsegmente und Produktparten.

Jedes Produkt, jede Dienstleistung hat Eigenschaften und diese machen es für bestimmte Zielgruppen besonders geeignet oder ungeeignet. Dies zu bestimmen ist ein weiteres wesentliches Element erfolgreicher Produkt-Compliance – Know your Customer – Know Your Product. Die Definition von Zielgruppen und welche Produkte für diese geeignet sind – oder halt auch für welche Zielgruppen ein Produkt eher ungeeignet ist – hilft bei allen weiteren Prozessen. Die Einhaltung der Produktvorgaben und die Eignung für die jeweiligen Zielgruppen sind durch angemessene Governance-Strukturen zu verankern. Auch durch dokumentierte Product-Governance-Leitlinien, Vertriebsregeln, einen dedizierten Neuproduktprozess und regelmäßige Prüfungsaktivitäten muss die tatsächliche Wirksamkeit der Vorkehrungen sichergestellt werden (s. auch Sandmann, Daniel, Produkt-Compliance als Governance-Aufgabe: IDD und MiFID II in der Praxis, Compliance Praxis 2017, S. 31).

Neue und bestehende Produkte müssen umfangreich getestet werden. Dies kann durch Szenarien (kann auch eine 80-jährige Person das Batteriefach öffnen, kann ein nicht mit der deutschen Sprache vertrauter Mensch die Anleitung zum Dosieren von Dünger verstehen?) und Modelle geschehen.

Die Vertriebe müssen sorgfältig ausgewählt und ebenfalls regelmäßig überprüft werden, wobei etwa die Erklärkompetenz und Zugang zu den jeweiligen Zielgruppen ein wesentliches Kriterium ist. Dazu gehört auch die laufende wechselseitige Information, ob die Zielgruppe tatsächlich erreicht wird bzw. wenn außerhalb der Zielgruppe verkauft werden soll (Buck-Heeb, Petra: Compliance bei vertriebsbezogener Product Governance – Neuerungen durch die MiFID II bzw. das Kleinanlegerschutzgesetz, CCZ 2016, 2, 3 f.).

Derartige organisatorische Vorkehrungen sind in der Finanzindustrie Teil der Organisationspflichten, die wiederum Voraussetzung für die Erlaubnis sind, die Geschäftstätigkeit auszuüben. In der Folge müssen die Compliance-Organisationen aufgrund der Bedeutung die Einhaltung dieser Vorgaben mit prüfen.

12.5 Fazit und Ausblick

Für Compliance bieten die auf Produkte und Vertrieb fokussierte Product-Compliance-Synergien mit verwandten Themen (etwa Verhinderung von Geldwäsche, Terrorismusfinanzierung oder Betrugshandlungen) zukünftig besser angehen zu können. Die Einbettung von Compliance in Geschäftsprozesse und der Überblick über die gesamte Wertschöpfungskette sind ebenfalls Garanten für die Entwicklung zu einem höheren Reifegrad. Das Beispiel Dieselskandal hat gezeigt, dass die Beschränkung eines CMS auf einen Katalog aus wenigen Rechtsgebieten häufig große Risiken ausklammert. Dies verhindert ein holistischer Ansatz wie die Product Compliance. Analytik durch technologische Fortschritte gerade bei Machine Learning können in Compliance genutzt werden, um Produkte besser „in der Wildbahn“ prüfen zu können, wie es bei Software-Anbietern schon üblich ist.

Literatur

- Ohne Autor; Apple Compliance; <https://www.apple.com/compliance/> zul. abgerufen am 29.1.2024.
- BORRELL, CLIVE / CASHINELLA, BRIAN: Crime in Britain Today, London, Routledge & Kegan Paul, 1975.
- BUCK-HEEB, PETRA: Compliance bei vertriebsbezogener Product Governance – Neuerungen durch die MiFID II bzw. das Kleinanlegerschutzgesetz, CCZ 2016, 2, 3.
- COPPOLA, FRANCES; The U.K.’s Biggest Financial Scandal Bites Its Biggest Bank – Again, <https://www.forbes.com/sites/francescoppola/2019/07/31/the-u-k-s-biggest-financial-scandal-bites-its-biggest-bank-again/> zul. abgerufen 29.1.2024.
- FEDERAL COMMUNICATIONS COMMISSION / T-Mobile USA, Inc., DA 18-373, Final Order April 16, 2018.
- Financial Conduct Authority, Lloyds Banking Group fined £117m for failing to handle PPI complaints fairly: Examples of customer experiences, London 2015, <https://www.fca.org.uk/publication/corporate/lloyds-ppi-complaints-examples-customer-experiences.pdf> zul. abgerufen 29.1.2024
- Financial Conduct Authority, Lloyds Banking Group fined £117m for failing to handle PPI complaints fairly, final notice, <https://www.fca.org.uk/publication/final-notices/lloyds-banking-group-2015.pdf> zul. abgerufen 29.1.2024.
- GRÜTZNER, THOMAS/BOERGER, BJÖRN/MOMSEN, CARSTEN: Die „Dieselaffäre“ und ihre Folgen für Compliance-Management- Systeme – Evolution durch Einbeziehung des Bereichs Produkt-Compliance in ein CMS, CCZ 2018, 50.
- JAHN, JOACHIM/GUTTMANN, MICHA/KRAIS, JÜRGEN: Krisenkommunikation bei Compliance-Verstößen, 1. Auflage 2020.
- LARISI, GEORGETTE FERNANDEZ; Scandal or Repetitive Misconduct: Payment Protection Insurance (PPI) and the not so Little “Skin in Lending Games” in Moral Cents Vol. 9 Issue 1, Winter/Spring 2020, S. 3.
- POLLY, SEBASTIAN U. LACH, SEBASTIAN: Das neue Produktsicherheitsgesetz – Empfehlungen an Wirtschaftsakteure zur Compliance in der Produktsicherheit, CCZ 2012, 59, 60.
- REMBERG, MEINHARD, § 6. Compliance-Risikoanalyse in mittelständischen Unternehmen, in Moosmayer, Klaus: Compliance-Risikoanalyse, 2. Aufl. München 2020.
- SANDMANN, DANIEL, Produkt-Compliance als Governance-Aufgabe: IDD und MiFID II in der Praxis, Compliance Praxis 2017, S. 31.



Daniel Sandmann, E.-M.B.L (St. Gallen) ist Rechtsanwalt und Syndikusrechtsanwalt in München und Lehrbeauftragter am ZWW der Universität Augsburg und an der FOM Hochschule Berlin. Er war 2004–2010 bei der Deutsche Bank AG im Bereich Legal, Risk & Compliance u. a. als Head of Regulatory Contact Office für die Beziehungen zu den Aufsichtsbehörden zuständig, hat das operative Reputationsrisikomanagement geleitet und zahlreiche regulatorische Umsetzungsprojekte verantwortet. 2010–2019 hat er u. a. die konzernweiten Programme Sales Compliance und Integrity Culture in der Allianz SE geleitet.

Teil V

Compliance als Bestandteil der Unternehmenskultur



Compliance als Führungsaufgabe – Ethische Verantwortung im Bereich Compliance

13

Thomas Schwartz, Nikolaus Seitz und Twain Stolz

Inhaltsverzeichnis

13.1	Ethische Aspekte des Compliance-Managements	331
13.2	Compliance als moderne Managementaufgabe?	332
13.2.1	Good Governance und der Begriff der „Compliance“	332
13.2.2	Rolle und Selbstverständnis des Compliance Officers aus ethischer Sicht	335
13.2.3	Die fachliche Expertise des Compliance Officers in ethischer Perspektive	336
13.3	Compliance als Führungsaufgabe	338
13.4	Compliance-Management als Wertemanagement	340
13.5	Ausblick und Herausforderungen	342
	Literatur	343

13.1 Ethische Aspekte des Compliance-Managements

Der vorliegende Beitrag nähert sich dem Compliance-Begriff zunächst über eine wirtschafts- und unternehmensethische Perspektive. Compliance oder Compliance-Management wird dabei nicht nur als Minimalziel zur Erfüllung rechtlicher Rahmenbedingungen verstanden. Damit soll hier ein Plädoyer für die ethische Ergänzung des oftmals nur rechtlich betrachteten Compliance-Begriffes eröffnet werden. Denn: Eine lediglich auf der Ein-

N. Seitz (✉)
Bauhaus-Universität Weimar, Weimar, Deutschland
E-Mail: nikolaus.seitz@uni-weimar.de

T. Schwartz · T. Stolz
Wirtschaftswissenschaftliche Fakultät, Universität Augsburg, Augsburg, Deutschland
E-Mail: thomas.schwartz@wiwi.uni-augsburg.de; twain.stolz@uni-a.de

haltung von Gesetzen basierende Compliance wird zukünftigen Entwicklungen hinterherlaufen, statt diese aktiv voranzutreiben und mitgestalten zu können (Schneider 2020). Mehr noch, wird ein ganzheitliches und integratives Compliance-Konzept zur zentralen Strategie- bzw. Führungsaufgabe erfolgsorientierten Managements während der Post-Covid Ära (vgl. Velte 2022). Umso bedeutender wird allerdings auch die Notwendigkeit einer professionalisierten Compliance; und umso wichtiger auch die Rolle des Compliance Officers – seine fachliche Expertise, Kommunikationskompetenz und seine moralische Grundhaltung. Kurzum: sein „ethisches Wissen“.

13.2 Compliance als moderne Managementaufgabe?

Ganz gleich, ob mittelständisches Familienunternehmen oder globaler Großkonzern, aktuell präsentieren sich Unternehmen „verantwortungsvoller“ denn je.: Nachhaltigkeitsberichte, Social Accounting, ESG Reporting, Compliance-Statements und „Codes of Ethics“ bezeugen diesen Trend nicht nur eindrucksvoll, sondern fungieren als beste Chronisten dieses jüngst vollzogenen Paradigmenwechsels. Responsibility ist „[...] new business imperative“ (Waddock et al. 2002). Die jüngst verabschiedete und nun stufenweise in Kraft gesetzte EU-Taxonomie für ESG-Aktivitäten bestärkt diesen Eindruck. Die Einführung des deutschen LksG, gemeinhin als Lieferkettengesetz bekannt, ergänzt die ESG-Perspektive und rückt ferner Menschen- und Kinderrechte in den Fokus. Beide Gesetzesinitiativen zeigen dabei nur allzu gut, wie aus „soft law“ und der viel beschworenen „Selbstverpflichtung“ „hard law“ wird, das Unternehmen und ihrer Verantwortung einen klaren Regelungsrahmen vorgibt. Allerdings spiegelt diese Entwicklung natürlich auch wider, dass es ohne verbindliches und sanktionierbares Compliance-Regelwerk offenbar auch nicht geht. Dabei sollte ein modernes Compliance-Management doch heute mehr sein als der berühmte „Dienst nach Vorschrift“, mehr als die Einhaltung von Regeln: Es geht um Legitimität statt Legalität.

Seit einigen Jahren sieht sich die globale Unternehmenspraxis einem beispiellosen Legitimitätsdruck ausgesetzt. Betrugsskandale, Umweltsünden, Korruptionsaffären, Kartellverstöße, Zinsmanipulationen, brennende Fabriken, fragwürdige Arbeitsbedingungen, Bilanzfälschungs- und Spekulationsskandale läuteten eine neue Ära von Kapitalismus- und Globalisierungskritik ein. Mehr noch, in Zeiten von Post-Covid, Diesel-Gate und Klimawandel fordert die Gesellschaft eine neue soziale Umweltverantwortung von Unternehmen ein – **mehr Transparenz, mehr Nachhaltigkeit, Fairness und Integrität**.

Und im Kern dieser neuen Verantwortungspflicht steht ein ganzheitlicher Compliance-Management Ansatz – der guten, heißt **moralisch unbescholtenen Unternehmensführung**. Doch was heißt das genau? Und welche Führungsaufgaben muss sich ein Compliance Officer zukünftig stellen?

13.2.1 Good Governance und der Begriff der „Compliance“

Spätestens seit der Verabschiedung des in seiner Art richtungsweisenden US-amerikanischen **Sarbanes-Oxley Acts** im Jahre 2002 gilt **Compliance** nicht mehr nur als

reiner Rechtsbegriff. Aktuelle Medienberichterstattungen, die Fülle an veröffentlichten Compliance-Reports und Unternehmensstatements zeigen, dass sich der Begriff der Compliance längst zum geflügelten Schlagwort und zu einer betriebswirtschaftlichen Sollgröße entwickelt hat. Dass der Anglizismus auch hierzulande nicht mehr nur als US-amerikanisches **legal transplant** gehandelt wird, sondern verstärkt Eingang in die Management- und deutschen Vorstandsetagen gefunden hat, ist dabei sicherlich auch ein Ergebnis jüngster Wirtschaftsskandale und den teils sehr kostspieligen Folgen und Reputationsschäden für die delinquenten Unternehmen (z. B. Deutsche Bank, Siemens, Dieselgate). Der ehemalige US-Staatsanwalt Paul McNulty kommentierte die jüngste Diskussion um die Bedeutung einer professionalisierten Corporate Compliance mit „If you think compliance is expensive, try non-compliance“ (WB Compliance 2020). Trotz der zunehmenden Relevanz von Compliance existiert bis heute allerdings weder eine global und einheitlich gültige Definition von Compliance, noch sind die dahinterliegenden Konzepte und Instrumente systematisiert und klar abgegrenzt. So konkurrieren noch immer eine Reihe populärer Definitionsversuche mit teils differenzierten, teils ergänzenden Leitideen und Praxiskonzepten.

Compliance lässt sich im Allgemeinen mit **Befolgung**, **Einhaltung**, **Erfüllung** oder **Folgsamkeit** ins Deutsche übersetzen. Im medizinischen und wirtschaftsrechtlichen Kontext wird damit traditionell die Befolgung bzw. Einhaltung gesetzter Verhaltensmaßregeln und geltender Regelvorschriften, bspw. durch den Patienten, Mitarbeiter bzw. Entscheidungsträger eines Unternehmens umschrieben.¹ Dabei ist es gerade Letzterem, d. h. der definitorischen Unschärfe des allzu interpretationsfreudlichen Begriffs der **Verhaltensmaßregel** oder **Regelvorschrift** anzulasten, dass die Bemühungen um ein global einheitliches und disziplinübergreifendes Verständnis von Compliance bisher scheiterten. Denn was gilt als **gesetzter Verhaltensmaßstab**, was als **Regelvorschrift** und was muss folglich eingehalten oder befolgt werden? Nicht zuletzt an diesen Fragen, aber mehr noch an ihren Antworten hängt sich die Diskussion dessen, was Compliance von Unternehmen systematisch einfordert und abverlangt, seit jeher auf.

Sowohl in der Literatur wie in den aktuellen öffentlichen Diskussionen lassen sich zwei grundsätzliche Positionen wiederfinden. Dabei ist beiden Standpunkten gemein, dass sie ihr jeweiliges (Pflicht-)Verständnis von Compliance systematisch an die als legitim wahrgenommene Verantwortungsreichweite von Unternehmen koppeln: Unter Berufung auf die provokanten Thesen des Nobelpreisträgers und bekennenden Neoklassikers, Milton Friedman, wurde die soziale Verantwortung der Unternehmung lange Zeit auf die bloße Pflicht zur Gesetzmäßigkeit und rechtlicher Unbescholtenheit reduziert.² Im traditionellen Verständnis bedeutet Compliance daher lediglich Konformität der Unternehmensgeschäfte und -operationen mit externen, gesetzlich und formal-vertraglich vereinbarten Regelwerken. In dieser engen Auslegung wird unter Compliance die „[...] **Gesamtheit**

¹ Vgl. auch den medizinischen Begriff der „Komplianz“.

² Zur weiteren Lektüre vgl. Friedman, (1970).

aller (Anm. der Verfasser: organisationellen) **Vorkehrungen, die das rechtskonforme Verhalten eines Unternehmens [...] gewährleisten“** (Zimmermann 2004 zit. nach Wieland 2010, S.18) aufsummiert.

Seit den aufsehenerregenden Unternehmensskandalen und globalen Entwicklungs-tendenzen der vergangenen Jahre lässt sich ein fundamentaler Wandel im Verständnis von Compliance erkennen. So werden Forderungen nach einem holistischen Compliance-Verständnis zunehmend lauter (vgl. Fatima und Elbana 2022). Vielfach gefordert wird heute eine explizit moralische Perspektive, fernab der bloßen Legalitätspflicht, der sog. **Legal Compliance** und rechtlicher Unbescholteneit. Solch ganzheitliche Compliance-Ansätze setzen regelkonformes Verhalten mit moralkonformem Handeln gleich und erweitern damit den Legalitätsgedanken um die ethische Dimension der Legitimität. Als **moralkonformes** bzw. **legitimes Handeln** gelten im Allgemeinen jene Handlungsweisen, die im Einklang mit sämtlichen vorfindlichen formellen wie informellen gesellschaftlichen Regelsätzen bzw. Institutionen stehen. Darunter fallen sowohl Gesetze wie auch nicht explizit auskodifizierte Sitten, allgemeingesellschaftliche Werte, Erwartungen und Gebräuche – kurzum: das gesamte Moralsystem einer Gesellschaft und eines Unternehmens zu einem bestimmten Zeitpunkt (vgl. North 1992, S. 3 ff.). In einer weiter gefassten Definition könnte man unter **Compliance** dementsprechend – und analog zum erstgenannten Definitionsversuch – sämtliche (organisationelle) Maßnahmen, die regelkonformes Handeln, d. h. Handeln in Übereinstimmung mit dem geltenden Recht, den sittlichen Geboten, kulturellen Normen und Erwartungen unternehmerischer Anspruchsgruppen gezielt auf allen Organisationsebenen und entlang der gesamten Wertschöpfungskette durchzusetzen versuchen.³

Vergleicht man beide oben genannten Definitionsversuche, zeigt sich, dass Compliance – ganz gleich, welchem der oben genannten Ansätze man dabei folgt – im Wesentlichen auf zwei Kerngedanken aufbaut: erstens dem übergeordneten **Prinzip der Freiwilligkeit**, zweitens dem **Grundsatz der Regelkonformität**. Compliance als Forderung nach Gesetzesstreue und rechtlicher Unbescholteneit kann gegenwärtig entsprechend als Minimalziel verantwortungsvoller Unternehmensführung verstanden werden – ein Basisziel, auf das sich alle Akteure bzw. Definitionsversuche unabhängig kultureller oder politischer Herkunft einigen können. Insofern scheint es nicht verwunderlich, dass Compliance als Inbegriff und gleichsam erste Grundvoraussetzung jedweder unternehmensethischer Bemühungen gilt (vgl. Michaelson 2006). Angesichts der gegenwärtigen Vertrauenskrise und der damit einhergehenden veränderten gesellschaftlichen Erwartungshaltungen kann jedoch begründet davon ausgegangen werden, dass die Forderung nach einer ganzheitlichen **Social Compliance** auch weiterhin zunehmend an Bedeutung für die erfolgsorientierte Unternehmensführung gewinnen wird. Vor diesem Hintergrund stellt die Einhaltung – mehr noch: die unbedingte Haltung eines Unternehmens im Blick auf die Wahrung ganzheitlichen regelkonformen Wirtschaftens schon jetzt eine der zentralen Führungsaufgaben modernen und vor allem dauerhaft zukunftsgerechten Managements

³Eine ähnliche Definition bieten u. a. PriceWaterhouseCoopers AG (2005), S. 8 und Wieland (2010), S. 19.

dar. Dieses Ziel sollte nicht nur für Konzerne und Groß-Unternehmen gelten, sondern genauso von kleinen Unternehmen angestrebt werden. Auch wenn hier der gesellschaftliche und mediale Druck auf den ersten Blick geringer ausfällt, ist die Notwendigkeit auch hier real. Damit stellt sich aber zugleich die Frage, wer die grundlegenden Haltungen eines Unternehmens hinsichtlich der Regelkonformität im umfänglichen Sinne des Wortes definiert und wie dies zu geschehen hat.

13.2.2 Rolle und Selbstverständnis des Compliance Officers aus ethischer Sicht

Die Aufgabe, einen unternehmensweiten Verhaltenskodex zu formulieren, ihn zu kommunizieren, seine Implementierung zu organisieren, seine Einhaltung zu kontrollieren und schließlich zu dokumentieren, wird im Allgemeinen dem Compliance Officer zugeschrieben.⁴ Beschränkt sich seine Aufgabe damit auf die einer reinen Sachbearbeiter-Funktion ohne Führungskompetenz oder umfasst das Aufgabenfeld eines Compliance Officers neben solch eher „technischen“ Aufgaben im Rahmen des Management-Prozesses nicht viel mehr auch genuine Führungsaufgaben? Es stellt sich die Frage nach der Rolle und dem Selbstverständnis des Compliance Officers. Sie hat bislang in der wissenschaftlichen Literatur nur wenig Aufmerksamkeit erfahren: zu akut und zu brisant waren die inhaltlichen Fragen, denen man sich zunächst widmen musste. Dennoch ist sie unbedingt einer Klärung zuzuführen, will man nicht beim Aufbau von Compliance-Strukturen im Rahmen einer unternehmensweiten Organisation auf Dauer Konfliktpotenziale ins Gras schießen lassen, die dem eigentlichen Auftrag von Compliance in einem Unternehmen mehr Schaden zufügen als Nutzen schaffen können.

Compliance kann aus ethischer Sicht nicht nur auf die Koordination und Formulierung rechtlicher und organisationaler Regelungsmechanismen beschränkt bzw. eingegrenzt werden. Es genügt gerade nicht, Prozesse zu organisieren, Aufgaben effektiv zu delegieren, deren Umsetzung zu kontrollieren und gerichtsfest zu dokumentieren. Besonders offensichtlich wird dies, wenn man an die Formulierung eines unternehmensweiten Code of Conduct bzw. weiterer ethisch relevanter Kodizes, bspw. im Blick auf ökologische und soziale Aspekte denkt. Eine solche Aufgabe umfasst nicht nur die Kenntnis rechtlicher Rahmenordnungen und weiterer interner und externer, formeller wie informeller institutioneller Vorgaben, sondern zugleich die Kenntnis der Unternehmensorganisation mit ihren möglichen Risikofeldern und auch der herrschenden Unternehmenskultur mit ihren Gewohnheiten, Mythen und ihrer Geschichte. Außerdem ist eine vertiefte Kompetenz und Sensibilität für ethische Fragestellungen zu erwarten, die sich im Rahmen unternehmerischer Tätigkeiten ergeben können.

Wenn auch die Kenntnis ethischer Prinzipien und Theorien nicht zwingend als Führungsaufgabe bezeichnet werden kann, so stellt bereits die Formulierung ethischer

⁴Zur weiteren Lektüre vgl. Mörkle und Weinen, 2021.

Standards für die Unternehmensorganisation eine immense Herausforderung an die beauftragten Personen dar, da sie dieselben nur durch langjährige Erfahrung im Unternehmen oder durch eine entsprechende Funktion mit Durchgriffsmöglichkeiten hinsichtlich zugänglicher Informationen erwerben können. Darüber hinaus ist die Mitgestaltung der Unternehmenskultur und der mit ihr verbundenen allgemein gültigen Werte und Grundhaltungen ein Thema, das die Position eines Compliance Officers deutlich in die Führungsebene eines Unternehmens verweist. Denn eine wirksame und effektive Compliance im o.g. holistischen Sinn fordert von den Verantwortlichen selbst glaubwürdig und transparent vorzuleben, was für die Gesamtorganisation des Unternehmens gefordert wird. Anfragen an eine Compliance-Organisation erfolgen ja nicht im luftleeren Raum, gleichsam anonymisiert und von konkreten Sachverhalten und Menschen enthoben, sondern ergeben sich gerade in der Auseinandersetzung mit ethischen wie rechtlichen Grauzonen, die mitunter gar Dilemma-Charakter haben können. Beispielhaft hierfür ist die digitale Sphäre (KI, Web3 etc.) oder der Trend zum Remote Working bzw. Home-Office, welche neue Risiken, Grauzonen sowie Herausforderungen für Compliance Manager birgt. In entsprechenden Bereichen kann nicht immer eine eindeutige und einzige richtige Antwort geben werden. Es gilt vielmehr, Güterabwägungen vorzunehmen, Argumente hin und her zu bewegen, Plausibilitäten darzustellen und Lösungswege aufzuweisen, die es den Beteiligten ermöglichen, mit gutem Gewissen, zumindest aber mit dem Bewusstsein, nicht falsch zu handeln, Entscheidungen zu treffen. Der Compliance Officer hat in diesem Kontext stets eine Referenzposition inne. Er wird nicht einem binär denkenden Computer entsprechend befragt. Vielmehr wird erwartet, dass er situations- und menschengerecht urteilt und berät. Er hat Handlungssicherheit zu vermitteln. Damit übernimmt er aber Führungsaufgaben, für die er selbst geeignet sein muss. Nicht jeder ethisch bzw. rechtlich gut Ausgebildete ist dazu in der Lage. Dementsprechend kann man auch nicht nur aufgrund einer in diesen Bereichen vorliegenden Expertise die Verantwortung eines Compliance Officers übernehmen. Gleichwohl ist es ohne entsprechendes Fachwissen in diesen Gebieten ebenso wenig möglich, diese Aufgabe in einem Unternehmen einzunehmen. Von daher ist in einem ersten Schritt zu klären, worin das geforderte Fachwissen besteht.

13.2.3 Die fachliche Expertise des Compliance Officers in ethischer Perspektive

Die Fragen nach den rechtlichen, betriebswirtschaftlichen und psychologischen Kompetenzen eines Compliance Officers werden an anderer Stelle ausführlich behandelt. Hier soll dementsprechend auf die ethische Expertise eines Compliance Officers eingegangen werden, die als notwendige, aber nicht hinreichende Bedingung zur Übernahme einer entsprechenden Tätigkeit bezeichnet werden kann.

Ethik ist eine philosophische Disziplin, die allgemein als **vernünftige Rede über das menschliche Handeln** bezeichnet werden kann. Menschliches Handeln ist gekennzeichnet durch einige grundlegende Eigenschaften: Vernünftigkeit ... (s.o.) im Sinne der

Diskursfähigkeit und Generalisierbarkeit, Willentlichkeit ... (s.o.) als der Kraft, vom reinen Denken zur Ausführung, mithin zum Handeln fortzuschreiten, Freiheit ... (s.o.) als der gegebenen Möglichkeit, dies auch vollziehen zu können und schließlich Zielorientierung ... (s.o.) als der grundlegenden Fähigkeit, Gründe für das, was man tut, angeben zu können. Von daher erhellt, dass auch und gerade wirtschaftliches bzw. unternehmerisches Handeln immer ethisch relevant ist, denn es sind immer nur Menschen, die sich im Rahmen von institutionellen Vorgaben darum mühen, möglichst effektiv und effizient knappe Ressourcen so zu verwenden, dass dadurch ein möglichst optimaler Nutzen für alle Beteiligten hervorgeht, der sie in die Lage versetzt, die eigene Existenz und jene aller anderen an einem wirtschaftlichen Prozess Beteiligten zu sichern. Dabei hat im Kontext des wirtschaftlichen bzw. unternehmerischen Handelns immer zugleich zu gelten, dass dadurch ein Wohlfahrtsgewinn geschaffen werden muss, d. h. dass der erwirtschaftete Nutzen für die Gesellschaft größer ist als der Schaden, der prinzipiell immer entsteht, wenn der Mensch gestaltend und verändernd in seine Umwelt eingreift. Ziel der einzelnen Unternehmung ist es dabei, die „license to operate“ i.S. einer gesellschaftlichen Betriebslizenz zu sichern, also durch die von ihm zur Verfügung gestellten Güter und Dienstleistungen einen gesamtgesellschaftlichen Nutzen zu schaffen. Gerade weil Wirtschaft ein „Menschenwerk“ ist, entstehen in diesem Zusammenhang immer wieder Fragen, welches Handeln geeignet ist, diesem Ziel der Wirtschaft allgemein und des einzelnen Unternehmens im Speziellen wirkungsvoll zu dienen.

Dazu sind in einer arbeitsteiligen Gesellschaft Regelwerke unumgänglich. Sie geben Kriterien, Standards und Prinzipien vor, die es ermöglichen, Handlungen einzuordnen, Verhaltensweisen zu beurteilen und so ethische Verallgemeinerungsdiskurse zu führen. Diese werden als Normen bezeichnet. Sie sind ebenso wie die Handlungen selbst vom Menschen formuliert, fallen also nicht „vom Himmel“ und müssen sich letztlich stets im Spiegel der Vernunft als verallgemeinerungsfähig erweisen, um Geltung erheischen zu können. In der ethischen Forschung haben sich hier unter anderem die sog. „Goldene Regel“ (was du nicht willst, was man dir tut, das füg auch keinem andern zu!) sowie der Kantische „Kategorische Imperativ“, der in vier verschiedenen Formulierungen mit je unterschiedlichen Schwerpunktsetzungen vorliegt, als tragfähige Kriterien für normgerechtes Handeln herausgebildet. Ihre Kenntnis und die Fähigkeit, konkretes Handeln im Rahmen einer Unternehmensorganisation im Hinblick auf diese Kriterienkataloge zu hinterfragen, kann als eine wesentliche fachliche Kompetenz eines Compliance Officers in ethischer Perspektive verstanden und gefordert werden. Was als richtig und gesellschaftlich akzeptiert gilt, ist stärker denn je im Wandel. Die Tätigkeit des Compliance Officers ist damit als dynamischer Prozess zu betrachten. Es bleibt festzuhalten, dass es sich dabei nicht um Zauberei handelt; vielmehr handelt es sich um eine Leistung des „gesunden Menschenverstandes“, der aber Zeit und Muße aufbringen muss, sich immer neu die Fragen nach einem richtigen und gesellschaftlich akzeptierten Verhalten zu stellen. Selbst in einer Compliance-Organisation ist dies aber nur beschränkt möglich, weswegen die Stärkung des ethischen Grundgerüstes der Mitarbeiter zu einer der zentralen Aufgaben eines Compliance Officers gehören sollte. Aber auch diese Aufgabe erfordert persönliche und

organisationale Führungskompetenz, womit wir wieder mit der Rolle und dem Selbstverständnis des Compliance Officers konfrontiert sind. Dieser gilt nun im Folgenden unsere Aufmerksamkeit.

13.3 Compliance als Führungsaufgabe

Aus unterschiedlichen Blickwinkeln betrachtet sind wir jeweils zum selben Ergebnis gekommen: Compliance ist Führungsaufgabe; ein Compliance Officer hat in einem Unternehmen Führungsverantwortung zu übernehmen. Ist das ebenso erlernbar wie das ethische Wissen, von dem im vorigen Abschnitt die Rede war?

Dass man Führung, speziell Unternehmensführung lernen kann, weiß jeder, der schon einmal einen Fuß in die mehr oder minder ehrwürdigen Hallen einer Wirtschaftsfakultät gesetzt hat. Lehrstühle für Unternehmensführung sind zahlreich und in aller Regel gut ausgestattet.

Aber um Unternehmensführung geht es an dieser Stelle nicht. Corporate Governance ist zwar ein wichtiges Thema auch und gerade bei der Frage nach einer effektiven Compliance; an dieser Stelle jedoch geht es um Führung im Sinne der Menschenführung. Und auch dieses Führen ist zumindest teilweise erlernbar.

Was erlernbar ist, hat etwas mit Wissen zu tun. Führen ist nicht allein eine dem Menschen in die Wiege gelegte Fähigkeit, andere Menschen, die zu ihm in einem gewissen Abhängigkeitsverhältnis stehen, zu einem erwünschten Handeln zu bewegen. Vielmehr geht es beim Führen auch und besonders darum, zu wissen, was man in diesem Prozess tut. Das ist etwas anderes als die Methodenkenntnis, die benötigt wird, um gewisse unternehmerische Prozesse erfolgreich steuern bzw. beurteilen zu können.

Führen bedeutet, etwas bzw. jemanden in Bewegung zu setzen. Führung hat stets eine motivationale Dimension. Wer erinnert sich nicht an eine Führungspersönlichkeit, die uns in früheren Lebenssituationen dazu begeistert hat, Zeit und Energie aufzuwenden, um ein gemeinsames Ziel zu erreichen? Welches Ziel erreicht oder zumindest angestrebt werden soll, ist dabei zunächst nebensächlich. Es kommt vor allen Dingen darauf an, ein Ziel aufzeigen zu können, es sichtbar zu machen und als erstrebenswert darstellen zu können. Stößt man in einer Gruppe eine Bewegung auf ein gemeinsames Ziel hin an, sind Veränderungen auszumachen, die auch messbar sind: Eine Fußballmannschaft wird umgekrempelt und ist wieder willens und fähig, Spiele zu gewinnen; ein Verein findet neue Mitglieder, eine politische Partei neue Wähler; ein Unternehmen verbessert seine Performance. Führen motiviert zu Veränderungsprozessen.

Damit ist aber erst **eine** Dimension des Führens bezeichnet. Wer eine Bewegung angestoßen hat, muss sie auch **steuern** können. Eine Bewegung zu steuern ist jedoch gar nicht so einfach. Nicht umsonst ist der Steuermann auf einem Schiff einer der erfahrensten Seeleute der Besatzung. Führung ohne Erfahrung ist nur selten mit Erfolg gekrönt. Erfahrung zu sammeln, bedeutet aber immer auch den Umgang mit eigenen und fremden Misserfolgen. Erfahrung ist nicht allein die Summe meiner Erfolge, sondern – mindestens

genauso notwendigerweise – auch die Geschichte meines oder fremden Scheiterns. Beides muss aufgearbeitet und reflektiert werden, damit aus Erfahrungen Erfahrung wird. Wer in einer Führungsaufgabe Bewegung steuert, ist deshalb aufgefordert, sich angstfrei mit seinen eigenen Fehlern und dem eigenen Scheitern auseinander zu setzen. Das gilt in besonderer Weise für den Compliance Officer. Die Beschäftigung mit seinem eigenen ethischen Versagen stärkt seine personale Integrität und macht ihn als Gesprächspartner glaubwürdiger. Und von dieser Glaubwürdigkeit hängt der Erfolg seiner Aufgabe in hohem Maße ab.

Eine dritte Dimension des Führens umfasst die Aufgabe, jemanden in Bewegung zu **halten**. Auch das ist einfacher gesagt als getan: Der Zauber des ersten Augenblicks verfliegt nicht nur in Liebesbeziehungen. Der Alltag mit seinen Anforderungen, die immer stärker administrativer Natur sind, weil im Rahmen standardisierter oder auch reglementierter Governance immer mehr Prozesse dokumentiert, validiert und zertifiziert werden müssen, versperrt nicht selten den Blick darauf, dass es beim Führen in aller Regel um Menschen geht. Für sie Zeit aufzubringen, in einem kommunikativen Prozess ihre jeweiligen Befindlichkeiten wahrzunehmen und mit ihnen umzugehen, ist eine der wichtigsten Aufgaben verantwortlicher Führung. Dabei geht es stets darum, die Menschen mit ihren Bedürfnissen und Ansprüchen wahr- und ernst zu nehmen. Nur so wird es möglich sein, frühzeitig den „Sand im Getriebe“ zu erkennen, der Bewegung nicht nur einschränkt oder lähmmt, sondern nach einer gewissen Zeit unmöglich macht oder gar in eine unerwünschte Richtung führen kann. Deswegen ist der Compliance Officer, dessen Aufgabe darin besteht, diesen „Sand im Getriebe“ wahrzunehmen und womöglich zu entfernen, nicht nur ein wichtiger Ansprechpartner für die operativ tätigen Mitarbeiter einer Unternehmung. Er muss vielmehr auch bewusst seinen Platz auf der Ebene des strategischen und normativen Managements einnehmen, um auch von dieser Position aus immer wieder für die Neujustierung von Prozessen eintreten zu können.

Bewegung anstoßen, Bewegung steuern, in Bewegung halten – diese drei Aufgaben moderner Führung sind keineswegs neue Erfindungen der Personalforschung. Kein „neuer Wein“ also. Was aber in den vergangenen Jahren immer mehr vergessen wurde, ist das Faktum, dass man nur erfolgreich führen kann, wenn man nicht nur andere bewegt, sondern auch selbst „bewegt“ ist. Der Compliance Officer wird hier in Zukunft immer stärker eine Rolle als Motivator, Steuermann und Motor einnehmen müssen, der die anderen Führungspersonen eines Unternehmens daran zu erinnern haben wird, dass man in seiner Führungsfunktion nur dann akzeptiert wird, wenn man die Ziele, die man als erstrebenswert darstellt, selbst mitträgt. Führung ist nicht Coaching! Das gilt auch für den Compliance Officer. Es ist nicht egal, in welchem Unternehmen, bzw. in welcher Organisation jemand Führungsverantwortung übernimmt. Wer sich aber in den Führungsetagen großer Unternehmen umschaut, wird immer wieder „alte Bekannte“ treffen, die zwischen verschiedenen Unternehmen hin und her switchen. Das ist an sich kein Problem. Problematisch wird es allerdings dann, wenn die Funktion innerhalb der Unternehmensleitung völlig unabhängig davon übernommen und ausgeübt wird, welchen eigentümlichen Charakter das jeweilige Unternehmen hat: wenn es also nicht mehr auf Menschen, sondern einzig

auf Zahlen ankommt. Deswegen hat der Compliance Officer aus der Kenntnis der Werte, zu denen sich ein Unternehmen in seinen Leitlinien und seinem Code of Conduct bekennt, und der daraus resultierenden angestrebten Unternehmenskultur, die anderen Mitglieder der Unternehmensführung immer wieder daran zu erinnern, mitunter zu mahnen und damit die Position eines „Unternehmens-Gewissens“ zu übernehmen und nachhaltig weiterzuentwickeln. Das wird ihm nur dann gelingen, wenn er selbst von den Werten des Unternehmens zutiefst überzeugt ist und eine solch gefestigte, ethisch integre Persönlichkeit ist, dass ihm auch von der Unternehmensleitung her Respekt, Anerkennung und damit Vertrauen entgegengebracht wird. Dies ist allerdings nur möglich, wenn seine Position in der Führung klar definiert ist und letztlich keine „Gefahr“ für die Stellung anderer darstellt. Nur dann wird es dem Compliance Officer möglich sein, andere Führungskräfte vor der Gefahr rein „technischen“ Führens bewahren zu können.

Die Gefahr, dass Führung zu einem rein technischen Unterfangen wird, ist in unserer globalisierten Wirtschaft immer evidenter. Wie soll in einem global aufgestellten Unternehmen Führung aber anders als „technisch“, mithin nach externen Governance-Regeln ablaufend, überhaupt möglich sein? Dass ein Manager nicht alle Mitarbeiter seines Unternehmens kennen kann, ist selbstverständlich. Aber sich dennoch für sie zu interessieren, sollte Kennzeichen einer Führungskraft sein. Das unterlassen zu haben, also keinen glaubwürdigen Bezug zum eigenen Unternehmen und seinen Mitarbeitern hergestellt zu haben, ist einer der Vorwürfe, die neuerdings Managern gemacht werden. Sich nur noch am eigenen Bonus orientiert zu haben und darüber die Welt außerhalb der Führungsetage vergessen zu haben, ist ein weiterer. Beides zerstört Vertrauen – innerhalb und außerhalb der Unternehmen. Der Compliance Officer kann hier durch die Regeln, die er im vertrauensvollen Umgang mit Kollegen und Mitarbeitern entwickelt, für einen Neuaufbau von Reputation sorgen.

„Vertrauen ist der Anfang von allem“ – so warb vor Jahren ein großes deutsches Bankhaus. Wir stehen heute wieder an einem Anfang. Die alten Führungseliten haben viel dafür getan, Vertrauen in die Wirtschaft und in verantwortungsvolles unternehmerisches Handeln zu zerstören. Umso größer sind die Erwartungen an eine neue Generation von Führungspersonal und zugleich an eine Neuausrichtung der Organisation des Managements. In diesem Prozess hat Compliance eine zentrale Rolle einzunehmen. Das zeigt sich besonders in den gegenwärtigen Ansätzen, ein modernes Wertemanagement in den Unternehmen aufzubauen (vgl. Wieland 2004). Auch dabei gilt es, Compliance nicht nur im Blick auf rechtlich-legalistische Blickrichtungen zu verkürzen, sondern vielmehr stets eine umfassende Perspektive, die immer auch ethische Elemente enthalten muss, einzunehmen.

13.4 Compliance-Management als Wertemanagement

Werte sind ins Wort gegossene Gegenstände des menschlichen Strebens und sind als solche handlungsleitende und handlungsorientierende Teile einer jeden menschlichen Gemeinschaft. Menschliches Streben lässt sich nicht auf ethische Inhalte beschränken,

sondern umfasst das ganze Feld dessen, was eine Gemeinschaft ausmacht. Josef Wieland identifiziert in seiner bekannten Wertematrix vier Wertefelder, in denen sich das Streben des Menschen manifestiert (vgl. Wieland 2004, S. 24). Werte haben für menschliche Gemeinschaften identitätsstiftende Bedeutung, insofern sie die Zugehörigkeit zu einer sozialen Gruppe, einer Organisation oder einem kulturellen Raum bezeichnen (vgl. Wieland 2011, S. 246). Deshalb wird es beim Aufbau eines Compliance-Management-Systems immer auch darauf ankommen, die kollektiven Werte des korporativen Akteurs (d. h. des Unternehmens) in den Blick zu nehmen. Zurecht stellt Wieland fest: „**Unternehmenswerte sind (...) nicht die Summe oder der gewichtete Durchschnitt der individuellen Überzeugungen, die es in einem Unternehmen gibt, sondern sie sind die Werte des kollektiven Akteurs >Unternehmung<, die dieser gegenüber all seinen individuellen Akteuren als bindend zur Geltung bringt**“ (ebd.). Wirksame Compliance beginnt dementsprechend in der Benennung dieser kollektiv gelten sollenden Werte, die in einem ersten Schritt **kodifiziert** werden, d. h. identifiziert und formell niedergelegt werden (vgl. zu den Bausteinen des Wertemanagements im Unternehmen Wieland 2011).

In einem zweiten Schritt wird es darum gehen, die identitätsstiftenden Werte des Unternehmens für den Geschäftsalltags greifbar zu machen. „**Es sind erst diese Leitlinien und Verfahren, die die konkreten praktischen Konsequenzen moralischer Überzeugungen benennen, einfordern und damit überprüfbar machen**“ (Wieland 2011, S. 249). Ziel dieser Phase des Aufbaus eines Wertemanagements ist es, die kollektiven Werte in verbindliche Routinen eines Unternehmens umzuwandeln und sie auf diese Weise in die Organisation zu implementieren. Wieland weist zurecht darauf hin, dass hier von einer Analogie zum individualistischen Ansatz einer Tugendethik gesprochen werden kann. Tugenden sind erworbene Charakterdispositionen, die den Menschen durch Einübung in die Lage versetzen, schnell, spontan, mühelos und mit Freude das Richtige zu tun, mithin zu einer Routine des guten Handelns zu gelangen. Wer regelmäßig tugendhaft handelt, wird dadurch als Mensch insgesamt tugendhaft, d. h. Tugenden sind nicht nur handlungsqualifizierende, sondern subjektqualifizierende Eigenschaften. Übertragen auf die Unternehmenskultur kann man daraus Folgendes ableiten: Die Einübung organisationaler Werte und die Implementierung derselben in Unternehmensprozesse und -verfahren machen nicht nur einzelne unternehmerische Entscheidungen, sondern das Unternehmen als Ganzes glaubwürdiger; sie stärken die Reputationen des Unternehmens und damit letztlich auch die Nachhaltigkeit seiner Performance durch geringere Transaktionskosten (vgl. Sing und Misra 2021). Dies gilt nicht nur für die großen Unternehmungen. Vielmehr müssen spätestens jetzt auch kleine und mittelständische Unternehmen die Notwendigkeit einer wirksamen und ethisch erweiterten Compliance erkennen, sonst drohen vermehrt gesellschaftliche Sanktionen und Gesichtsverlust.

Dieses hehre Ziel wird jedoch nur gelingen, wenn „**die verschiedenen einzelnen Leitlinien und Verfahren der Stufe 2 systematisiert, aufeinander bezogen und (...) als Compliance- bzw. CSR-Programm den relevanten Stakeholdern des Unternehmens zugänglich gemacht wird**“ (Wieland 2011, S. 249). Allgemein wird dieser Prozess als **Systematisierung** bezeichnet. In ihm geht es um die Festlegung allgemein gültiger

Instrumente, um die Kommunikation des systematischen Charakters aller Maßnahmen und um den Aufbau einer effektiven Plattform, die eine regelmäßige Überprüfung im Sinne einer Evaluation bzw. eines Monitorings ermöglichen sollen.⁵

Erst an dieser Stelle stellt sich die Frage nach der Morphologie der Organisation, die ein solches wertefundiertes Management sicher zu stellen vermag. Viele Unternehmen haben in den vergangenen Jahren – aufgeschreckt durch die bereits im ersten Teil dieses Beitrags aufgezeigten unternehmerischen und organisationalen Fehlleistungen – einen anderen Weg beschritten: Sie haben zunächst mit erheblichen Kosten eine Compliance-Organisation aufgebaut, die dann erhebliche Zeit und große Energie darauf zu verwenden hatte, ihre eigene Rolle im Unternehmen zu finden und zu organisieren. Im Endeffekt wird das Ergebnis nicht unähnlich dem sein, was durch ein wertefundiertes Managementsystem entwickelt werden wird; aber der Weg zu diesem Ziel ist gepflastert gewesen mit Unsicherheiten, Ineffizienzen und einer Fülle von Problemen, die man bei einem systematischen Vorgehen hätte vermeiden können. Das hätte seitens der Unternehmensführung viel Zeit und den Mut zu klaren und wegweisenden Entscheidungen verlangt, die sich nicht kurzfristig auf die Performance eines Unternehmens auswirken können, jedem beteiligten Stakeholder aber die Wichtigkeit der entsprechenden normativen und strategischen Entscheidungen verdeutlicht hätte. Diejenigen Unternehmen, die einen solchen Weg beschritten haben und ein Compliance-Management als Wertemanagement in ihrer Organisation aufgebaut haben, haben in jedem Fall den großen Vorteil, dass sie Veränderungsprozesse in Richtung auf integres unternehmerisches Verhalten an dem Punkt ansetzen, der aller Erfahrung nach am schwierigsten für Veränderungen offen ist: bei der Unternehmenskultur. Gelingt es, diese zu wandeln und ethisch sowie rechtlich fragwürdige oder gar illegale und illegitime Verhaltensweisen zu überwinden, ist für das Unternehmen und seine Zukunft mehr getan als durch jede organisationale Umstrukturierung.

13.5 Ausblick und Herausforderungen

Dem Compliance Officer kommt heute eine zentrale, strategische Aufgabe zu, die menschlich und fachlich fordert und die nur angemessen zu bewältigen ist, wenn Compliance von allen Beteiligten, d. h. von der Unternehmensspitze bis zum untersten Glied in der Unternehmenshierarchie, – als ganzheitliches, integratives Führungsprinzip verstanden und umgesetzt wird. Nur so kann ein echter und nachhaltiger Wandel im Einklang mit der eigenen Unternehmenskultur vollzogen werden.

Zu den jüngsten Herausforderungen zählt der Umgang mit der Covid-19 Pandemie. Zum einen hat Covid die Chance einer Re-Integration von Wertschöpfungsprozessen sowie neue Standards und Prüfverfahren mit sich gebracht, zum anderen wurden Home-Office und Remote Working normalisiert. Auch hier war und ist es erforderlich, dass Compliance Management über die Gesetzeskonformität hinaus agiert, denn mit diesen neuen

⁵Exkurs zur CSR-Entwicklung und Zukunft vgl. Carroll, 2021.

Arbeitswirklichkeiten ergeben sich auch neue rechtliche und ethische Herausforderungen, die sich aus der Ungleichzeitigkeit von Kontrollmöglichkeiten ergeben.

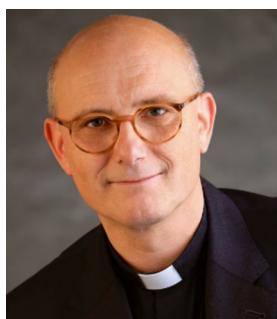
Die kommende Dekade bringt zudem angesichts der von der Politik so bezeichneten „Zeitenwende“ zahlreiche weitere und in ihrer Form neue Problemfelder mit sich. So erfordern etwa geopolitische Fragestellungen wie die Verhängung und Durchsetzung von Sanktionen etc. eine veränderte Global Compliance. Auch der gesamte Bereich der digitalen Herausforderungen wächst stetig. So wirft neben der fortlaufenden ICT-Integration vor allem das Thema KI neue Fragen auf: Wer kann bspw. wofür noch rechtlich bzw. ethisch verantwortlich gemacht werden, wenn es sich bei den Autoren bzw. Verursachern von problematischen Inhalten und Vereinbarungen nicht mehr um Personen, sondern um eine Künstliche Intelligenz handelt?

In diesem Zusammenhang wird sich auch die Frage stellen, wie sich den kommenden Jahren ein strategisch orientiertes Compliance-Management zu dem Themenkreis verhält, der in den letzten Jahrzehnten unter dem Begriff der Corporate Social Responsibility (CSR) subsumiert wurde. Werden sich Compliance-Management und CSR auf Dauer zu einem Wertemanagement weiterentwickeln, wobei der Wertebegriff durchaus die ganze Bedeutungsbreite umfasst, die ihm seitens von Philosophie und Ökonomik zugesprochen werden? So verweisen die Diskussionen um die Implementierung eines europäischen Lieferkettengesetzes bereits darauf, dass zukünftig durch politische Entscheidungen nicht mehr allein rechtliche Regelungsmechanismen, sondern auch gesellschaftlich und ethisch relevante Fragestellungen untrennbar miteinander verwoben werden. Das muss und wird Auswirkungen auf das Verständnis und die Wirkmechanismen sowie schließlich auch die strategische Verortung von Compliance in der Governance von Unternehmen zeitigen.

Literatur

- CARROLL, A. B. (2021): Corporate social responsibility: Perspectives on the CSR construct's development and future. *Business & Society*, 60(6), 1258–1278.
- FATIMA, T., & ELBANNA, S. (2022): Corporate social responsibility (CSR) implementation: a review and a research agenda towards an integrative framework. *Journal of Business Ethics*, 1–17.
- FRIEDMAN, M. (1970): The Social Responsibility of Business is to Increase its Profits. In: *The New York Times Magazine*, September 13, 1970.
- MICHAELSON, C. (2006): Compliance and the Illusion of Ethical Progress. In: *Journal of Business Ethics* 66 (2/3), S. 241–251.
- MÖHRLE, H.; WEINEN, R. (2021): Professionelle Compliance-Kommunikation. Wie Sie Ihr Unternehmen gegen Regelverletzungen immunisieren. Wiesbaden: Springer Gabler.
- NORTH, D.C (1992): Institutionen, institutioneller Wandel und Wirtschaftsleistung: Tübingen: Mohr PriceWaterhouseCoopers AG (Hg.) (2005): Compliance kann Mehrwert schaffen. Abrufbar unter: http://pwcplus.pwc.de/fileserver/RepositoryItem/Compliance_Menzies_pwc_05_05.pdf?itemID=353886 (zuletzt abgerufen am: 10.Februar 2013).
- SCHNEIDER, T. (2020): Das Fundament der Compliance. In: Werkzeuge wirkungsvoller Compliance, S. 27–40. Berlin, Heidelberg: Springer Gabler.

- SINGH, K., & MISRA, M. (2021): Linking corporate social responsibility (CSR) and organizational performance: The moderating effect of corporate reputation. *European Research on Management and Business Economics*, 27(1), 100139.
- VELTE, P. (2022): Meta-analyses on corporate social responsibility (CSR): a literature review. *Management Review Quarterly*, 72(3), 627–675.
- WADDOCK, S. A.; BODWELL, C.; GRAVES, S (2002): Responsibility: The new business imperative. In: *Academy of Management Executive* 16 (2), S. 132–148.
- WB Compliance (2020): If you think compliance is expensive, try non compliance. Abrufbar unter <https://www.wbcompliance.be/article/conduct-costs-compliance-budget> (zuletzt aufgerufen am: 18.1.2023).
- WIELAND, J. (Hg.) (2004): Handbuch Wertemanagement: Erfolgsstrategien einer modernen Corporate Governance. Hamburg: Murmann.
- WIELAND, J. (Hg.) (2010): Compliance Management als Corporate Governance – konzeptionelle Grundlagen und Erfolgsfaktoren. In: Wieland, J.; Steinmeyer, R. ; Grüninger, S. (Hg.): Handbuch Compliance-Management. Konzeptionelle Grundlagen, praktische Erfolgsfaktoren, globale Herausforderungen, S. 15–38. Berlin: Schmidt.
- WIELAND, J (2011): Wertemanagement. In: Aßländer, M. S. (Hg.): Handbuch Wirtschaftsethik, S. 245–252. Stuttgart: Metzler Verlag.
- ZIMMERMANN, R. (2004): Compliance – Grundlage der Corporate Governance. In: Wieland, J. (Hg.): Handbuch Wertemanagement: Erfolgsstrategien einer modernen Corporate Governance, S. 200–221. Hamburg: Murmann.



Professor Dr. Thomas Schwartz studierte Philosophie und Theologie in Münster, Augsburg und Rom, wo er 1990 zum Priester geweiht wurde. Nach Kaplanszeit und moraltheologischer Promotion in Freiburg i.Br. war er von 1999 bis 2009 als Hochschulpfarrer in Augsburg tätig. Von 2005 bis 2014 war er Professor für Angewandte Ethik an der Hochschule Augsburg, darüber hinaus ist er seit 2014 Honorarprofessor für Wirtschafts- und Unternehmensethik an der Wirtschaftsfakultät der Universität Augsburg. Von 2010 bis 2021 war er Pfarrer der katholischen Pfarrgemeinde Mering (bei Augsburg). Seit Oktober 2021 ist er Hauptgeschäftsführer und Vorstandsvorsitzender von Renovabis, dem Osteuropa-Hilfswerk der Kath. Kirche in Deutschland. Zudem berät er namhafte internationale Unternehmen in unternehmensethischen Fragen. Darüber hinaus ist er als Fernsehmoderator und Vortragsredner im In- und Ausland bekannt. Derzeit moderiert er gemeinsam mit Harald Lesch die ZDF-Sendung „Lesch sieht Schwartz“. Seine Forschungsschwerpunkte liegen im Bereich der Nachhaltigkeitstheorie, der Corporate Social Responsibility sowie der Führungsethik.



Prof. Dr. Nikolaus Seitz (Jun.-Prof.) Juniorprofessor für Entrepreneurship und Technologietransfer an der Bauhaus-Universität Weimar. Zuvor war er als Akademischer Rat und Habilitand am Lehrstuhl für Unternehmensführung und Organisation (Prof. Dr. Erik E. Lehmann) an der Universität Augsburg tätig. Zwischen 2019 und 2022 vertrat er den Lehrstuhl für Internationales Management an der LMU Munich School of Management. Seine Forschungsschwerpunkte liegen in den Bereichen Innovation, strategisches Unternehmertum und Technologietransfer. Seine wissenschaftlichen Arbeiten sind in führenden internationalen Fachzeitschriften publiziert. Darüber hinaus ist Prof. Seitz Research Fellow am Institute for Development Strategies der Indiana University und hält verschiedene Lehraufträge, unter anderem an der EMLYON Business School sowie der Hochschule München. Zudem war er Co-Geschäftsführer des Augsburg Center for Entrepreneurship (ACE) an der Universität Augsburg und engagiert sich aktiv als Mentor und Innovationscoach für Startups.



Twain Stoltz M.A., M.Sc. absolvierte sein Studium der Betriebswirtschaftslehre sowie der Kunstgeschichte an der Universität Augsburg. Seine Studien schwerpunkte sind im Bereich Unternehmensführung, Wirtschaftsethik und Kunstmarkt angesiedelt. Im Rahmen seines Dissertationsprojektes forscht er derzeit im Bereich der Kunstökonomie. Seit April 2024 ist er Leiter des Gründungszentrums der Universität Augsburg (StartHub). In dieser Funktion berät er Gründerinnen und Gründer der Universität.



Compliance als Führungsaufgabe

14

Gerald Marimón

Inhaltsverzeichnis

14.1	Prolog zur Compliance	348
14.2	Eine Arbeitsplatzbeschreibung	349
14.2.1	Ist Compliance Ihre Aufgabe?	349
14.2.2	Einer für alle oder alle für einen?	350
14.2.3	Compliance-Kommunikation	351
14.3	Typen, Ziele, Abenteuer	353
14.3.1	Haben Sie Ziele?	353
14.3.2	Karriere mit Compliance	355
14.3.3	Eine Typenschule	355
14.4	Ein Haus der Compliance bauen	357
14.4.1	Statik und Mechanik	357
14.4.2	Negative Zonen und Blind Spots	358
14.4.3	Sensoren und Aktoren – Die Haustechnik	360
14.5	Compliance wird bei uns gemanagt	362
14.5.1	Die vier Gebote der Compliance	362
14.5.2	Wertbeitrag der Compliance	363
	Literatur	364

G. Marimón (✉)

Rechtsanwalt Dr. Gerald Marimón, Augsburg, Deutschland

E-Mail: gerald.marimon@marimon.de

14.1 Prolog zur Compliance

Sind Sie bereit mit Vorurteilen umzugehen? Wer Compliance als Führungsaufgabe erfüllen möchte, der muss sich dieser Herausforderung stellen. Ich berichte hier, das sei mir gestattet, vom Kurs, von den Gedankengängen und Ergebnissen, zu welchen wir mit wechselnden Teilnehmerteams in der Kursarbeit gelangt sind.

Compliance in einem Unternehmen einzuführen, sie zu führen und durchzusetzen, ist immer auch eine Herausforderung für die Belegschaft, die etablierte Führungsriege und das **Immunsystem der Unternehmung**. Dieses Immunsystem setzt sich – wie bei jedem neuen Themenfeld in einer Unternehmung – als soziologisches Phänomen aus einem kollektiven *Abwehr-Teil* und als psychologisches Phänomen aus einem individuellen *Widerstands-Teil* zusammen. Es wacht so darüber, was Aufnahme im Einzel- und im Kollektivdenken und auch im Einzel- und Kollektivverhalten in der Organisation finden kann. Im Regelfall reagiert dieses unternehmenseigene System zunächst einmal damit, die neue Idee mit Worten (also logisch oder auch rhetorisch) auf die innere Widerspruchsfreiheit zu prüfen. Die Waffen dieses Logik- und Rhetorik-Wettstreits sind Worte. Hinzukommen können wie bei allen Changethemen Widerstände in der tatsächlichen Zusammenarbeit.¹

In den Kurseinheiten habe ich die Teilnehmenden immer schon zu Anfang gefragt, welche Vorurteile sie zur Compliance kennen, welchen sie bereits begegnet sind, oder mit welchen sie rechnen. Es war jedem der Teilnehmenden klar, dass Führung immer etwas Persönliches ist und die zu Führenden immer persönlich auf den an sie erhobenen Führungsanspruch reagieren. Hier spielen Vorurteile eine entscheidende Rolle, denn sie repräsentieren einen gewichtigen Teil der vorgegebenen oder gelebten Ordnung. Alle Kursteilnehmenden haben dann auch reichlich Vorurteile in die Kurssammlung einbringen können. Gängige Vorurteile zu Compliance sind beispielsweise diese: „*Es ist ein Beispitzelungssystem!*“ oder „*Es ist der Misstrauensbeweis der Geschäftsführung an die Belegschaft!*“ oder „*Es ist eine neue Arbeitsbeschaffungsmaßnahme!*“, aber auch „*Compliance ist überflüssig! Sie ist teuer und bringt nichts!*“ bis hin zu „*Sie ist wieder so eine Management-Mode!*“

Um den kurzen Prolog zur Compliance als Führungsaufgabe hier abzuschließen, soll es also nachfolgend darum gehen, wie man Akzeptanz für das Themenfeld Compliance, die Aufgaben der Compliance und nicht zuletzt für die Akteure – die Führungskräfte – der Compliance gewinnen kann.

Ich möchte nachfolgend aufzeigen, wie und mit welchen Ansätzen eine Akzeptanz für die Compliance erreicht werden kann. Dazu haben wir in den Kurssitzungen erarbeitet, was eine Arbeitsplatzbeschreibung des Compliance-Officers sein kann, welche Ziele mit der Arbeit verfolgt werden können, in welcher Struktur und Systematik die Aufgaben erfüllt werden sollten und wie die Leistung der Compliance darstellbar gemacht werden kann. Akzeptanz für Compliance ist dabei kein Selbstzweck, sondern immer nur das Mit-

¹ Siehe Deekeling/Barghop (2003, S. 5 ff.).

tel, um die Führungsaufgabe überhaupt erfüllen zu können und der Verantwortung, die man mit der Aufgabe übernommen hat, auch gerecht zu werden – sie zu erfüllen im Sinne des genannten „*to comply with*“.

Die nachfolgenden Betrachtungen geben einmal den geneigten Lesern aus mehreren Kursen, aber auch Interessierten am Thema, zusammengefasst einige Stationen wieder, die die Teilnehmenden und ich im Schlaglicht behandelt haben. Es folgt also nun ein Bericht, sozusagen aus der *Compliance-Führungs-Werkstatt*.

14.2 Eine Arbeitsplatzbeschreibung

Wenn wir heutzutage unsere Berufstätigkeit arbeitsteilig erledigen, ist entscheidend, was zu unseren Aufgaben gehört – eine rationale Abgrenzung. Dies gilt umso mehr, wenn wir eine Führungsaufgabe ausfüllen wollen. Was liegt also näher, als die Arbeitsplatzbeschreibung, wie sie sich in einer Stellenanzeige finden lässt, genauer zu betrachten und im Kurs abzugleichen, ob die Arbeitsplatzwirklichkeit der Kursteilnehmer mit den einzelnen Merkmalen einer Stellenannonce übereinstimmen. Solche Anzeigen finden sich in Fachzeitschriften ebenso wie in den großen Jobportalen des Internets. Die Struktur der Anzeigen ist weitgehend gleich aufgebaut! Es geht um die Beschreibung der Aufgabe und die Beschreibung des Profils geeigneter Bewerber. In unserer Compliance-Führungs-Werkstatt haben wir uns ganz subjektiv genähert – mit einer Frage.

14.2.1 Ist Compliance Ihre Aufgabe?

Welche Verantwortung haben Sie übernommen, als Sie Compliance-Officer wurden? Oder anders gefragt: Welche Verantwortung hat man Ihnen übertragen, als Sie Compliance-Officer wurden? Es war recht spannend, mit den Teilnehmenden eine Stellenannonce aus dem Stellenteil einer dem Titel und der Ausgabe nach willkürlich gewählten Juristischen Wochenschrift anzuschauen und dabei genau zu betrachten, was da von einem Compliance-Officer gefordert wird. Wir fanden gleich im Eingang der Annonce den Aufgabenkreis des Compliance-Systems, um das sich der gesuchte Bewerber kümmern sollte. Die Erwartung an den Kümmerer: Compliance sollte implementiert, aufgebaut, weiterentwickelt, aktualisiert und realisiert werden. Damit wurde die Aufgabe des Compliance-Officers zu einer, die man mit **Systemmanager** bezeichnen kann. Enthalten waren Regelwerke und Kontrollinstrumente als Ausprägungen eines solchen Systems. Der Compliance-Officer kümmert sich demgemäß um die Erhöhung der System-Effizienz.²

In Stellenanzeigen wie der von uns betrachteten, wird der Compliance-Officer immer auch als unabhängiger Ansprechpartner für das Unternehmen beschrieben. Er soll **Berater**

²Vgl. Malik (2009, S. 80 ff.); wegweisend zuletzt der BGH, Urteil vom 27.4.2022 (Az. 5 StR 278/21).

sein und Mitgestalter. Er soll folglich souveräner Unterstützer sein für die Unternehmensteile und die dafür Verantwortlichen.³

Im Aufgabenfeld des Compliance-Officers sind oft auch lehrende Tätigkeiten mit enthalten. Das Thema der Schulung und der Workshops hat ein Compliance-Officer als **Lehrkraft** zu erfüllen. Der Compliance-Officer kümmert sich zudem also um die Erhöhung der Kompetenz im Unternehmen, allgemein im Feld der Compliance.

Allen diesen Aufgabeninhalten ist gemeinsam, dass kein vorgegebenes Feld verwaltet werden soll. Es ist offenkundig, dass die genannten Inhalte – der Neuartigkeit des Aufgabenbereiches (aus der Warte des inserierenden Unternehmens) geschuldet – im Schwerpunkt entwickelt, gestaltet, erstellt und ausgebaut werden sollen. Es sollen die eigenen Mitarbeiter und die Belegschaft ausgebildet und mitgenommen werden.

Es zeigt sich damit, dass das Aufgabenfeld, die Compliance ein- und durchzuführen, dynamisch und vor allem Führung gefragt ist.

14.2.2 Einer für alle oder alle für einen?

Compliance wird heute in Fachabteilungen erledigt. In DAX Unternehmen werden gar Abteilungsstärken von bis zu mehreren Hundert Personen erreicht. Als wir uns im Kurs mit der Compliance-Stelle befasst und unsere Stellenannonce genauer betrachtet haben, fiel uns auf, dass diese und auch andere Stellenannoncen so beschrieben waren, dass von dem Bewerber ausdrücklich Verantwortung übernommen werden sollte. Ein verantwortungsvoller Aufgabenbereich steigert die Attraktivität der Stelle. Das Thema der Haftung kam dann recht rasch im Kurs auf die Agenda. Wir fragten uns: *Wessen Verantwortung soll da getragen werden? Was soll der Compliance-Officer an Verantwortung tragen? Was kann er tragen?* Hierüber bestand oftmals Unklarheit in den Kursen. Nicht klar war oft, dass die Compliance-Verantwortung eine schlichte Ausprägung der Verantwortung der Geschäftsführung oder des Vorstandes war. Die Normen des § 43 GmbHG und des § 93 AktG dienten als Hilfestellung,⁴ um einschätzen zu können, welche Verantwortung getragen werden muss.⁵ Aus eben diesen Normen ergibt sich für die gängigen Unternehmensformen die primäre Haftung jedes einzelnen Mitglieds der Geschäftsleitung (Geschäftsführer/Vorstände). Es war zu diskutieren, ob da **einer für alle – persönlich** – auf der nächsttieferen Ebene – eben als Compliance-Officer – für alle Verantwortung übernehmen soll (das wäre der riskanteste Fall), oder im Wege der Organisation und Dele-

³Vgl. Niedereichholz (2000, S. 64 ff.).

⁴Als Beispiel der Wortlaut des § 43 Abs. 1 GmbHG: „Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden“ und des § 93 Abs. 1 AktG: „Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden.“

⁵Siehe Ries/Peiniger (2009, S. 19).

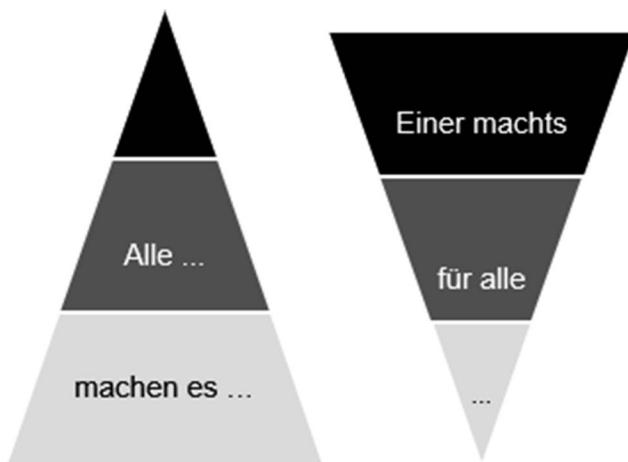


Abb. 14.1 Modell „Einer für alle“

tion – *organisatorisch* – eine Stelle geschaffen wurde, in der die delegierte Verantwortung wieder gebündelt werden soll und so **alle für einen** und für das Unternehmen als solches miteinstehen können.

In unseren Diskussionen haben wir ganz offen ausgetauscht, wie die einzelnen Kursteilnehmenden zu ihrem Aufgabenfeld kamen und welchem Modell ihre Arbeit eher entspricht. *Alle für einen oder einer für alle*. Das Unwohlsein im Modell „Einer für alle“ (siehe Abb. 14.1) war ganz klar zu spüren. Es war die kritische Frage zu diskutieren, ob in solch einer Konstellation von *Führung* gesprochen werden kann oder tatsächlich nur ein *Feigenblatt* den gängigen Vorurteilen entspricht, dass nämlich auf diese Weise jeder sich nur um sich selbst sorgt, um nicht zur Rechenschaft gezogen zu werden.⁶ Jedenfalls ging es damit nun auch darum, wie über die Stelle kommuniziert werden und wie man die Diskussion zur eigenen Stelle führen kann.

14.2.3 Compliance-Kommunikation

Wer führen will, muss kommunizieren. Jedem muss an dieser Stelle klar sein, dass man nicht „nicht-kommunizieren“ kann. Kommunikation findet immer statt. Auch ein Schweigen der Compliance-Verantwortlichen ist der Deutung zugänglich!⁷ Wenn wir zu Beginn gesehen haben, dass Compliance-Führung in der Praxis oft mit Vorurteilen konfrontiert wird, so ist die Frage, welche Führungsstrategie die richtige ist, um in dieser Lage einer (immer auch persönlichen) Herausforderung zu bestehen und Vertrauen für die eigene Arbeit und Person zu gewinnen. Was also kann dazu eine angemessene Kommunikation

⁶Vgl. Urteil des BGH vom 17.7.2009 (Az 5 StR 394/08), Nachweis in BB 2009, 2263.

⁷Instruktiv Deekeling/Barghop (2003, S. 234 ff.).

sein? Ist es eine, mit welcher Compliance ordentlich und werblich „auf den Busch haut“ – eine *offensive Strategie*? Ist es eine, die erklären will, warum Compliance sinnvoll ist und alle Vorurteile falsch? Eine *defensive Strategie*? Ist es eine, die nur das Nötigste sagt und sich um die Arbeit kümmert, allen Stürmen entgeht – eine *Überwinterungsstrategie*?

Ganz gleich, welche Strategie betrachtet wird, ob offensive, defensive oder Überwinterungs-Strategie – die Kommunikationsstrategie der Compliance sollte zum Ziel führen und das Ziel, so haben wir es eingangs festgelegt, sollte mindestens eine größtmögliche Akzeptanz für die Compliance sein. Einer guten Compliance-Kommunikation – erinnert sei hier an die Abb. 14.1 – sollte im Unternehmen stets gelingen, die Basis und ihr Handeln mit der Spalte und ihren Verantwortungen und Zielen und umgekehrt zu verbinden. Betrachtet man so die Compliance als Führungsaufgabe, unterscheidet sie sich nicht von den anderen Führungsfeldern, in denen überall gilt, dass Führung Kommunikation ist und Vermittlung leisten muss zwischen den Zielen der Unternehmung und den Fach-Zielen und -Operationen.

Wie kommunizieren Sie Ihre Compliance, Ihre Compliance-Abteilung und Ihre Compliance-Verantwortung? Vermitteln Sie noch (verteidigen Sie gar?) oder schaffen Sie schon Verständnis und praktische Akzeptanz? Moderne Fachkräfte in einer freiheitlich demokratischen Gesellschaft wollen rational nachvollziehen können, worauf sie mit ihrer Arbeit „einzahlen“.⁸

Im Kurs haben wir diskutiert, was solche Inhalte der Compliance-Kommunikation sind. Wie füllen die Teilnehmenden ihre Führungsaufgabe als Compliance-Officer aus? Natürlich sind in einer so heterogenen Gruppe ganz unterschiedliche Ausprägungen des Berufsfeldes „Compliance-Officer“ vertreten. Es gab Teilnehmende, die die Aufgabe in einer geschäftsführenden Position wahrnahmen, genauso aber auch Teilnehmende in Bereichsleitungs-, Abteilungsleitungs- oder Expertenfunktionen. Es gab auch Teilnehmende, die in einer Stabsfunktion noch gänzlich ohne weitere Spezifikation Compliance aufbauen, verantworten und damit kommunizieren mussten. Letzteres ist wohl der schwierigste Fall des Führens ohne (hierarchische) Führungsrolle!

Will man über gute Kommunikation führen, und das im Bereich der Compliance, so kann man über die Geschäftsführung und ihre Ideen, das Unternehmen und die Erwartungen und Anforderungen, die an es gestellt werden, berichten. Man kann über die eigene Organisation und die Aufgaben des eigenen Aufgabenbereichs informieren. Man kann über das Compliance-System im Unternehmen, enthaltene Regelwerke sowie Kontrollmechanismen und -instrumente, Fortbildungen veranstalten. Man kann im Unternehmen Diskussionen über generelle und aktuelle Fragestellungen und Themen der Compliance moderieren. Man kann über Schulungsinhalte und Übungsfälle im Austausch bleiben. Dazu kann man sich ansprechen lassen oder das Gespräch suchen. Der Compliance-Officer kann dazu Termine einberufen und Schulungen abhalten. Zusätzlich stehen interaktive Schulungsinstrumente in reichhaltiger Zahl am Markt zur Verfügung (Compliance E-Learning).

⁸Vgl. Deekeling/Barghop (2003, S. 234 ff., sowie S. 94 ff.).

Zur Führungsaufgabe der Compliance gehört es, zu dem konkreten Sender-Botschaft-Empfänger-Modell im eigenen Unternehmen ein systematisches Kommunikationsmanagement zu finden, zu strukturieren, aufzubauen, zu betreiben und kontinuierlich zu verbessern.⁹ Als Hilfsmittel, so stellten wir im Kurs fest, kann ein **Themenfahrplan** für alle Zielgruppen mit Terminen über das Geschäftsjahr sehr hilfreich sein und dafür sorgen, dass Compliance mit ihren Produkten in der Wahrnehmung einen wertvollen Beitrag für die Ziele der Unternehmung kommunizieren kann.

14.3 Typen, Ziele, Abenteuer

So unterschiedlich die Teilnehmenden des Compliance-Kurses sind, so unterschiedlich ist auch ihr Führungstypus, den sie leben und darstellen. Ganz unterschiedlich sind auch die Ziele, die sie verfolgen oder aufgegeben bekommen haben. Wie sie das ganze Feld der Compliance in ihrem Arbeitsalltag erleben, klingt oft nach einem Abenteuer mit ungewissem Ausgang. Nachfolgend soll also betrachtet werden, welche Ziele, welche Wege ein Compliance-Officer verfolgen und wie er sich dazu selbst einschätzen kann – dem ganz persönlichen Typus nach.

14.3.1 Haben Sie Ziele?

Natürlich verfolgt jeder, der täglich zur Arbeit aufbricht, gewisse Ziele. Rechnungen wollen bezahlt werden, das eigene Fortkommen vorangebracht und eine gewisse Form von Erfüllung und Selbstverwirklichung soll – idealerweise – auch damit erreicht werden. Danach gefragt, ob bei der Übertragung der Aufgaben klar formulierte Ziele mit besprochen worden sind, war die häufige Antwort im Kurs eher ein *Nein*. Zielvereinbarungen sind im modernen Führungsalltag gängig, doch gerade in einem Feld wie der Compliance vielleicht auch schwierig zu formulieren.

Die allgemeine Anforderung für Führungs- und Management-Ziele in der Unternehmensführung¹⁰ ist ganz pragmatisch, dass solche Ziele zumindest spezifisch, messbar, akzeptiert, realistisch und terminierbar sein sollen (sog. SMART-Formel; aus dem Englischen *Specific, Measurable, Accepted, Realistic, Timely*). In dem von uns betrachteten Feld der Compliance bestehen die Herausforderungen darin, diese für den Compliance-Bereich allgemein oder einem Compliance-Officer im Besonderen festzulegen. Einige Teilnehmende waren in ihren Unternehmen sozusagen „die ersten ihrer Art“, konnten also nicht auf eine Historie und etablierte Ziele zurückgreifen. Sie sahen sich auch in der Verantwortung, diese Ziele überhaupt erst zu finden und zu verankern. Sicher muss man dabei

⁹Vgl. Deekeling/Barghop (2003, S. 191 ff.); zum Compliance Management System schon BGH, Urteil vom 9.5.2017 (Az.: 1 AtR 265/17).

¹⁰Vgl. Link, (2011, S. 6 f.).

trennen, welche Ziele die Compliance überhaupt hat und dann der Compliance-Officer für sein Unternehmen persönlich zu erfüllen hat. Compliance für das Unternehmen soll aktuellen und auch dauerhaften zeitlichen Standards gerecht werden. „*Man hat heute eine Compliance-Abteilung*“ war eine Aussage – eine Compliance-Funktion vorzuhalten wird also, oft auch je nach Firmengröße, selbst zum Standard. Ganz allgemein konnte festgestellt werden, dass alle Unternehmen die Gesetze zu beachten haben. Alle Unternehmen, ganz gleich welcher Größe, haben sich zudem selbst Ge- und Verbote gesetzt, die sie beachtet sehen wollen.

Eine Compliance-Abteilung oder ein Compliance-Officer allein kann zu diesen Zielen einen Beitrag leisten, für diese Ziele, die effektivsten und effizientesten Vorgehensweisen analysieren und übernehmen, aber sicher nicht allein für alle Zielstellungen und die Gesetzeskonformität einstehen. Wenn also nach der o. g. SMART-Formel konkrete Ziele für den Compliance-Officer festgelegt werden sollen, so ähneln die Ziele sicher den Stellenausschreibungen und Stellenbeschreibungen, die es zu solchen Stellen gibt.

Im Kurs haben wir vor diesem Hintergrund festgelegt, dass Ziele, die ein Compliance-Officer übernehmen kann und auch mag, dahingehend vorliegen sollten, dass erreichbare Zustände die Ziele bilden sollten. Vielfach ist da, wo schon Ziele formuliert wurden, festzustellen, dass gar keine erreichbaren Zustände, sondern nur Vorgehensweisen und Messzahlen in der Praxis der Teilnehmenden formuliert worden sind. Eine Erfolgskontrolle und der Erfolgsnachweis gelingen hier selten. Darauf sollte geachtet werden!

Für die Aufgaben der Teilnehmenden konnten wir herausarbeiten, dass Compliance-Officer auf mehrere Zielfelder ihrer Stelle, ihres Bereichs und ihres Unternehmens mit ihrer Tätigkeit „einzahlen“. Diese Zielfelder stellen dann auch, in sich verbunden und kausal miteinander verknüpft, den Rahmen, den wir als **Compliance-Zielkontenrahmen** bezeichnen können, der für die Stelle des Compliance-Officers die meiste Akzeptanz erhielt. Dieser besondere Ordnungsrahmen bietet den Vorteil, dass eine klare Zuordnung erfolgen kann, wie dies in der Buchhaltung die Arbeit erleichtert und nachvollziehbar machen hilft. Wir machten uns nach dieser Diskussion und zu deren Abschluss ans Buchen eines idealen Zielhaushalts. Unsere Buchungssätze lauteten:

- Für das Unternehmen, den Compliance-Bereich und die Compliance-Stelle sind alle **Gebote und Verbote**, Regeln und Normen in ihrer Hauptaussage systematisch aufgeschrieben.
- Für die vorgenannten Einheiten ist die Kompetenzanforderung systematisch in **Profilen** festgelegt. Darin enthalten sind neben Verantwortlichkeiten auch die Kompetenzen und die Aufgaben genannt. Alle für das Feld „Compliance“ relevanten Abläufe und Steuerungen sind anschaulich niedergelegt.
- Alle von der Compliance zu erzeugenden Produkte, wie die vorgenannten Darstellungen aber auch andere Erzeugnisse, sind umfassend in einem **Katalog von Leistungen und Produkten** festgehalten.
- Mit allen internen und externen Partnern der Compliance sind **Leistungs- und Schnittstellenvereinbarungen** schriftlich fixiert und gesammelt dokumentiert. Über sämtliche Leistungserbringungen wird in Text und in Zahlen **ein periodengerechter Bericht** erstellt.

14.3.2 Karriere mit Compliance

Compliance ist eine in ihrer objektiven Wertigkeit hoch angesiedelte Stelle. Dazu haben wir im Kurs die gängigen Organigramme der Unternehmen und die Darstellungen der Teilnehmenden unseres Kurses betrachtet. Meist befindet sie sich in unmittelbarer sachlicher und hierarchischer „Nähe“ zur Unternehmensleitung. Ein idealer Platz im klassischen Sinn für eine Führungs-Karriere. Wie eingangs erwähnt, nehmen Compliance-Bereiche beachtliche Größen an. Die Verantwortung für eine Vielzahl von Menschen und damit von hohen Personal- und Sachkostenbudgets geht damit einher. Die Organisation in Berichtsebenen, die unmittelbar oder sogar über mehrere Stufen vermittelt an die Unternehmensleitungen berichten, ist die logische Folge. Ein geeignetes Feld, um in der oder mit Compliance Karriere zu machen? Ist Ihr Aufgabengebiet so aufgeteilt, dann ist aus der Compliance ein aufgabenteiliges Sachgebiet geworden, in dem die Aufgabenerfüllung neben anderen weichen Faktoren darüber entscheidet, ob es für den Compliance-Officer ein Fortkommen im Sinne einer Karriere gibt.

Einige Teilnehmende haben das Feld jedoch nicht so übernommen, sondern erledigen ihre Aufgaben *neben ihren „eigentlichen“ Aufgaben* als Führungs- oder Fachkräfte der Rechtsabteilung, der Revisionsabteilung oder der internen Beratungsabteilung, um nur einige zu nennen. Sich hier im Sinne der Karriere weiterzuentwickeln, ist sicher verbunden mit der Kunst, das eine zu tun (Compliance), ohne das andere zu lassen (z. B. Revision, juristisches Ressort). Die Arbeit ist an die Person gekoppelt und wird demgemäß viel subjektiver auf ihren Wertbeitrag und ihr Gelingen eingeschätzt.

Wieder andere Teilnehmende waren weder mit klassischen Aufgaben der Rechts- oder Revisionsabteilung oder mit Aufgaben einer organisierten und definierten Compliance-Abteilung vertraut, sondern hatten ihre Aufgaben eher wie Beauftragte zu erfüllen bzw. auszufüllen. Damit ähnelten sie eher Datenschutzbeauftragten oder Beauftragten für die Arbeitssicherheit; dies jedoch mit dem nicht unerheblichen Unterschied, dass es für die Compliance nicht wie für Datenschützer und die Arbeitssicherheit klar konturierte Gesetzeswerke und (Schutz-)Standards gibt. Wer von den Teilnehmenden auf diese Weise für berufliches Fortkommen sorgen wollte, war sich klar, dass er seinen Weg ganz alleine finden und dazu die Akzeptanz der vorgesetzten Stellen bzw. direkt der Unternehmensleitung gewinnen musste. Karriere im Einzelkampf. In dieser Konstellation sahen sich die entsprechenden Teilnehmenden auf kluge Partnerschaften, geschickte Allianzen und auch auf ein gerütteltes Maß an Protektion angewiesen.

14.3.3 Eine Typenschule

Fragen

Würden Sie für Compliance eine Party geben? Oder würden Sie zur Compliance bei Ihnen im Unternehmen ein umfassendes Kompendium schreiben? Wären Sie bereit, für Compliance Bündnisse im eigenen Haus mit Bereichen oder Personen zu schließen, mit denen Sie noch nie etwas zu tun gehabt haben?

Ganz unterschiedliche Wege haben wir vorausgehend und in unseren Kursen betrachtet, die ganz unterschiedliche Typenanforderungen an den Compliance-Officer stellen. Welcher Job in der Compliance passt zu wem? Nicht jeder ist ein Organisator, nicht jeder ein Gestalter, nicht jeder ein Verwalter – naturgemäß wollte nicht jeder der Teilnehmer jeden Weg gehen. Es ist sicher immer eine Typenfrage, auf welchen Weg man sich einstellen mag, wenn man auf die Zielkonten der Compliance einzahlen will oder soll.

So unterschiedlich waren denn auch die Teilnehmenden der bisherigen Zertifikatskurse des Compliance-Officers am Augsburger ZWW. Führungsarbeit ist immer auch Selbsterkenntnis und ein Lernweg. – Mit gängigen Typisierungsmodellen wollten wir im Kurs recht vorsichtig umgehen. Wenn wir die eingangs betrachteten Strategieformen zugrunde legen, so findet sich doch zumindest ein empirischer Ansatz, drei Typen als Arbeitshypothese zu definieren.

Zur offensiven Strategie des Auf- und Ausbaus der Compliance als Bereich und auch Einflussbereich passt **der Typus des forschen, ja extrovertierten, und standfesten Compliance-Officers**. Er definiert, bewahrt und verteidigt die Grenzen des Bereichs. Er sorgt für die eigene „Truppe“ und weitet den Einfluss- und auch Machtbereich der Compliance durchaus offensiv aus. Wenn hier noch Arbeit auf diesen Typus zukommt, so liegen Potenziale in der Messbarkeit, Nachvollziehbarkeit und Kontinuität, wenn alles Handeln derart persönlich und individuell ausgefüllt wird. Einen blinden Fleck können auch Akzeptanzdefizite bilden, für die das Gespür fehlt und die man deshalb nur schwerlich wahrnimmt.

Ein gänzlich anderer Typus ist **der Compliance-Officer, der eher vorsichtig und behutsam, eher introvertiert ist** und auf die sachliche Richtigkeit und den Bestand des Themas in all seinen Ausprägungen achtet. Compliance als Führungsaufgabe übersetzt dieser Typus des Compliance-Officers mit einem sachlich nüchternen Themenfeld, das in seinen Standardisierungen sehr streng auf Einhaltung überwacht wird. Dieser Typus in seiner hypothetischen Reinform stößt allerdings an seine Grenzen, wenn es um die Akzeptanz, Durchsetzung und Sanktionierung gehen muss, die meist mit viel Kommunikation und Interaktion und gegebenenfalls auch mit „Powerplay“ verbunden ist.

Als dritten Typus betrachten wir in unserem *Compliance-Führungstypen-Dreiklang*, den **Compliance-Officer, der das Feld zwar mit einem hohen Anspruch, aber spielerisch und mit einem Eventcharakter gestaltet und kontinuierlich weiterentwickeln will**. Hierarchien und Standards, die für die vorgenannten Typen unerlässlich sind, sind für ihn nur Mittel zum Zweck und Inhalt der Veranstaltungen, mit denen er Compliance für sein Unternehmen und die darin Tätigen übersetzt und inszeniert. Eine mögliche „Schwachstelle“ dieses Typus ist, dass das Aufrechterhalten der Spannung für seinen Eventansatz eine permanente kreative Schöpfungsleistung erfordert – mit anderen Worten, dass die Ideen nicht ausgehen, um die Akzeptanz für die Sache nachhaltig aufrechtzuhalten.

In der abschließenden Diskussion zu diesem Themenfeld fanden alle Teilnehmer einschließlich meiner Person heraus, dass wohl jeder etwas von allen Typen in sich vereint und die Risiken und Nebenwirkungen, wir sagten Potenziale, für die eigene Person etwas

genauer auch für die weitere Arbeit herauskamen. Dabei war auch wichtig zu sehen, dass die Kultur im Unternehmen, von der einen Eigenschaft mehr, von jener Eigenschaft weniger, zulassen würde. Alles eine Frage der Akzeptanz im ganz konkreten eigenen Haus.

14.4 Ein Haus der Compliance bauen

Bauen wir der Compliance ein Haus – ein Haus der Compliance! Hier und im Kurs betrachten wir Compliance als Führungsaufgabe. Der Compliance-Officer soll dazu nachfolgend einmal als Bauherr betrachtet werden. Er baut das Haus der Compliance, er baut das Haus für die Compliance. Er baut das Haus für die Mitarbeitenden des Unternehmens, in das diese einziehen sollen, in das er sie einführen soll. Werden sie sein Gebäude, werden sie seine Gestaltungen akzeptieren? Wie bei der Betrachtung der Aufgaben gesehen, ist der Compliance-Officer in seiner Führungsverantwortung Bauherr, Architekt und auch Bauunternehmer in einer Person. Eigentlich erstellt er aber ein Konzept, das er nicht als weiteres Haus neben dem Gebäude des Unternehmens konstruiert. Nein, eigentlich gestaltet er Räume im bereits bestehenden Haus des Unternehmens. Es ist eher ein Umbau, sodass das bestehende Unternehmen zum Haus der Compliance werden soll. Alle Plan- und Bauarbeiten finden also statt, während im Haus täglich gelebt und gearbeitet wird. Mit dieser Herausforderung wird unsere Compliance zu einem echten Akzeptanz-Projekt.

14.4.1 Statik und Mechanik

Gewiss kann man als Bauherr, Architekt und Bauunternehmer nur erfolgreich sein, wenn man die physikalischen Gesetzmäßigkeiten und Wirkmechanismen beachtet. Oben ist oben und unten ist unten. Mit anderen Worten: es ist zu beachten, wo im Haus der Compliance die Unternehmensleitung und wo die ausführenden Organe und Mitarbeitenden angesiedelt sind. In einem klassischen Organigramm zeigt sich der Raum für die Compliance als Stabsbereich, wenn er schon ein Bereich ist oder als Stabsaufgabe, wenn es noch keinen Bereich gibt. Oder er zeigt sich in einigen Modellen als Aufgabenpaket innerhalb eines Stabsbereiches, wie der Rechtsabteilung oder der internen Revision.

Wenn man die Mechanik bei der Gestaltung und Ausführung des Bauplans für die Compliance betrachtet, so ist zu beachten, dass die Zielvorgaben und deren Überwachung zunächst einmal „von oben“ von der Geschäftsleitung kommen. Dem gegenüber muss man sehen, dass die eigentlichen Impulse für die Compliance aus den operativen Bereichen stammen und zur Geschäftsleitung vermittelt werden müssen. In meinen Kursen lehre ich immer, dass die letztgenannten Impulse von der Basis einer gewissen **Schwerkraft der Compliance** gehorchend eher *nach unten* tendieren, als nach oben zur Geschäftsleitung zu gelangen. In dieser Sachverhaltsannahme ist die denklogisch verbundene Kehrseite, dass die Plan- und Zielvorgaben und der Umsetzungsabgleich derselben vor genannten Schwerkraft der Compliance gehorchend nicht nach unten tendieren, also in die

Fachbereiche „geerdet“ werden können, sondern eher in unserem Denkmodell *nach oben* („in den blauen Himmel“) tendieren. Eine Herausforderung der Compliance als Führungsaufgabe ist es, mit den Räumen, in denen die Compliance sein und stattfinden soll, diese scheinbaren Schwerkräfte zu überwinden. Denn sie sind es, die verhindern oder erschweren, dass sich Ziele und Umsetzungswahrnehmungen begegnen. Eine Herausforderung für Kommunikation und letztendlich für das Berichtswesen.

14.4.2 Negative Zonen und Blind Spots

Oft schildern die Teilnehmenden dann auch aus ihrem Arbeitsalltag, dass Geschehnisse und Informationen zur Compliance, dass Überlegungen, Wissen und Informationen darüber nur zu einem verschwindend geringen Prozentsatz zur Unternehmensleitung, also „nach oben“ gelangen. Informationen dieser Art sind dann von der Basis des Unternehmens über die Hierarchieebenen mit gewissen Verlusten im Inhalt oder in der Menge nach oben befördert worden. Solche Zwischenstufen, welche die Baustatik eines Organigramms tragen, fungieren in der bisherigen Bausubstanz dynamisch wie Verdichter- und Förderstationen. Wir kennen sie aus der Öl- und Gasförderung. Allerdings ist dies, wie hier geschildert, verbunden mit einem hohen Verlust an Wirkungsgrad. „*Wenn das Unternehmen wüsste, was das Unternehmen weiß*“, ist ein Teilnehmerzitat, das sehr schön ausdrückt, dass das Wissen aus dem operativen Geschäft oftmals durch die Infrastruktur der Führung und des Mittelmanagements, wie sie ein Organigramm abbildet, zumindest in Teilen verloren gehen.¹¹ Das ist kritisch, betrachtet man die daraus einhergehenden Haftungsrisiken.

Wollen wir Compliance als Führungsaufgabe ernst nehmen, sollte uns daran gelegen sein, den *Wirkungsgrad der Compliance* trotz der genannten Schwerkraft der Compliance und organisatorisch-infrastruktureller und psychologisch-individueller „Trägheiten“ zu erhöhen. Mein Ansatz und meine Empfehlung stelle ich den Teilnehmenden immer in einem Denkmodell vor. Dabei soll dieses Denkmodell genau diesen Gesetzmäßigkeiten Rechnung tragen. Eine Hierarchie ist immer wie eine Pyramide aufgebaut, die sich mit einer Spitze auf einer mehr oder weniger breiten Basis abstützt. Gelangt das breite Wissen der Basis im entscheidenden Moment nicht zur Spitze, so gerät die Spitze in die Verantwortung und Haftung.¹² Ist der Compliance-Officer eine maßgebliche Hemmnis auf dem Weg der Informationen und bei der Behandlung von Compliance-Sachverhalten, so kann ihn selbst eine Haftung treffen.¹³

¹¹Vgl. Marimón (2012, S. 7 f.).

¹²Vgl. Pflaeging (2008, S. 57 ff.); siehe auch Lohmann (2012, S. 11 ff.) und Semler (1993 S. 98 ff.).

¹³Vgl. Urteil des BGH vom 17.7.2009 (Az 5 StR 394/08), Nachweis in BB 2009, 2263. Ferner Urteil des BGH vom 9.5.2017 (Az 1 StR 265/17) und Urteil des BGH vom 27.4.2022 (Az 5 StR 278/21).

Die fünf Le-Corbusier-Stühle (Eine Compliance-Anekdote)

Im Kurs schildere ich zur Veranschaulichung aus eigenem Erleben den Diebstahl von fünf wertvollen *Le-Corbusier*-Stühlen aus dem Aufsichtsratsraum eines großen Unternehmens. Dieser Aufsichtsratsraum befand sich im fünften Stock des Zentralgebäudes. Dieses Stockwerk war nur über einen Lift und die entsprechende Eingabe eines Sicherheitscodes zu erreichen. Dennoch fehlten eines Tages besagte fünf sehr wertvolle Stühle und ließen die im Hause Alarmierten von der Geschäftsführung bis zum Pförtner einschließlich meiner Person, damals Personalleiter und Facility-Manager, ratlos. Niemals konnte ganz aufgeklärt werden, wie derart sperrige Möbel in dieser Zahl durch das Nadelöhr von baulichen und sicherheitstechnischen Gegebenheiten unbemerkt gebracht werden konnten. ◀

Mit etwas Abstand und einigem Nachdenken ließ sich dafür jedoch eine Erklärung finden, die nicht den tatsächlich kriminellen Weg, aber doch die Vorgeschichte erklären konnte. Dies lässt sich unter dem **Begriff der negativen Zone** bestimmen. Immer dort, wo Beschäftigte über einen längeren Zeitraum nicht mehr dazu kommen können, dass ihr Job und ihre Arbeit in angemessener Weise anerkannt, wertgeschätzt und vergütet wird, beginnen zunächst kleine *Korrekturbewegungen*, die wir als **Negative Zone der Compliance** begreifen können. Das kann sich äußern darin, dass die Bereitschaft für überplanmäßige Einsätze sinkt, dass die Genauigkeit bei der Ausführung von Arbeiten abnimmt, dass die Toleranz für Fehler im eigenen Betätigungsfeld oder Zulieferungen steigt und dass beginnend mit kleinen Entwendungen von Büromaterial bis hin zu Wertgegenständen (wie unsere gerade genannten fünf *Le Corbusier* Stühle) offenbar eine Tauschgerechtigkeit wieder hergestellt wird. Dahinstehen kann, ob der Täterkreis aus der eigenen Belegschaft stammt oder von Internen „bloß“ Beihilfe geleistet wurde. Die Personalabteilung des eigenen Unternehmens oder auch der sogenannte „Flurfunk“ kann dem Compliance-Officer hier Aufschluss darüber geben, wo Misskänge in der Menschenführung wahrnehmbar sind. Die Sensibilität für derartige Entwicklungen unterstützt die Präventionsarbeit der Compliance.

Wenn auch keine solchen Negativen Zonen entstehen, in denen schlimmstenfalls gegen das Unternehmen gearbeitet wird, so können doch auch **Blind Spots der Compliance** entstehen (den Begriff des blinden Flecks habe ich der von meinem eigenen Institut mitbetriebenen Kommunikationswissenschaft zum Feedback entnommen¹⁴). Dies sind unbeobachtete bzw. inzwischen unbeobachtbare Leistungseinheiten, in denen zwar nicht die Arbeit, aber doch das Berichten und Transparentmachen der Fortschritte und Ergebnisse der Arbeiten vermindert bis eingestellt wird. Mitarbeiter, Teams oder ganze Bereiche gehen auf „Tauchstation“. Hier gelingt weder den aktuell zur Unterstützung und zum Controlling vorgesetzten Stellen noch letztlich der Unternehmensleitung, eine Kenntnis und ein Wissen zu erlangen über die tatsächliche tägliche Güte der Wertschöpfung in diesen

¹⁴Vgl. Fengler (2009, S. 16 f.).

Unternehmensteilen. Aus haftungsrechtlicher Sicht stehen die Unternehmensleitung und alle nachfolgenden Stellen entsprechend – die juristische Garantenstellung unterstellt – in der Haftung für Fahrlässigkeit oder fahrlässige Unterlassung, wenn Verletzungen und Verstöße gegen die Gesetz- und Regelkonformität in diesem Blind Spot der Compliance stattfinden. Ein Defizit, das dem Compliance-Officer bekannt sein sollte und in dem er Führung übernehmen muss.

14.4.3 Sensoren und Akteuren – Die Haustechnik

Gegen die vorgenannten Negativen Zonen und Blind Spots der Compliance sollte der Compliance-Officer mit der notwendigen Unterstützung von innen oder von außen eine intelligente Haustechnik in die umgestalteten oder neuen Räume des Unternehmens einbauen. Dabei kann er auch auf die längst bewährten Bauteile der konventionellen Haustechnik eines Unternehmens zurückgreifen. Zu denken ist hier an das Berichtswesen aus Controlling und Revision. Buchhalterische Werte können durchaus Indikator sein, ob ein Geschäftsbereich anfällig ist für *Negative Zonen oder Blind Spots der Compliance*. Hier sollte im Sinne einer funktionierenden Haustechnik eine Schnittstelle eingebaut werden. Eine weitere Schnittstelle kann zur Revision, was die Ordnungsgemäßheit der Funktionen und zur Personalabteilung, was die Ordnungsgemäßheit der Personen anbelangt, hergestellt werden. Akzeptanz gewinnt der Compliance-Officer sicher auch, wenn er sorgsam, kompetent und auch wirtschaftlich mit vorhandenem Material umgeht, bevor er neues Material (Berichte, Abfragen, Analysen etc.) erzeugt bzw. mit Fremdaufwand erzeugen lässt. In Abschlüssen und anderen Berichten kann man die Geschäftsentwicklung einzelner Bereiche und Teile nachvollziehen und aufmerksam analysieren, ob und wann sich Veränderungen ergeben – z. B. die Vertriebsleistung lässt nach, der Einkauf setzt keine Preisverbesserungen durch, die Entwicklung oder die Auftragsabwicklung gerät mit Projekten in zeitlichen Verzug. Der Beginn einer negativen Zone oder eines Blind Spots in der Compliance?

Eine ganz *eigene Haustechnik der Compliance* ist u. a. die des sog. „Whistle-Blowings“. Der Deutsche Bundestag hat das Hinweisgeberschutzgesetz (HinSchG) am 16. Dezember 2022 nun mit den Änderungsvorschlägen des Rechtsausschusses verabschiedet. Der Bundesrat hat in seiner Sitzung am 10. Februar 2023 dem Gesetz jedoch nicht zugestimmt. Mit dem Hinweisgeberschutzgesetz soll der bislang lückenhafte und unzureichende Schutz von hinweisgebenden Personen ausgebaut und die EU-Whistleblower-Richtlinie (Richtlinie (EU) 2019/1937) in nationales Recht umgesetzt werden. Mit seinem Inkrafttreten am 02.07. 2023 ist die Gesetzeskraft eingetreten. Mit der Verabschiedung dieses Gesetzes kommt eine gesetzliche Verpflichtung zur Einführung eines Hinweisgeberver-

fahrens für Beschäftigungsgeber mit mehr als 250 Mitarbeitenden sofort nach Inkrafttreten des Gesetzes und für Beschäftigungsgeber mit mehr als 50 Mitarbeitenden (und bis 249 Mitarbeitende) ab dem 17. Dezember 2023.

Gemeint ist hier die Möglichkeit, allgemeine Gefahren, von denen am Arbeitsplatz oder in anderen Zusammenhängen Kenntnis erlangt werden konnte, an entsprechend vorbezeichnetener Stelle zur Kenntnis zu bringen. Dazu werden allgemein Hotlines und Kommunikations-Infrastrukturen eingerichtet, die zu den konventionellen Techniken von Detektion und Prävention der Compliance zu rechnen sind.

Den von mir erarbeiteten Präventions-Ansatz einer Compliance-Technologie neuester Art habe ich im Kurs mit den Teilnehmern als alle Formen der Haustechnik integrierenden Ansatz diskutiert.

Dabei betrachteten wir die oben als Schwerpunkt der Compliance dargestellte Wirkungsbedingung für die Compliance-Kommunikation gleich mit. Die skizzierte Pyramide stellt sich damit für die Zwecke besserer Compliance-Kommunikation „auf den Kopf“. Ziele erreichen die Basis. Meldungen erreichen die Spitze.

Meine Überlegungen instrumentalisieren für die Compliance-Kommunikation und – Führung den Ansatz der dienenden Führung (in der Management-Literatur bekannt als Servant Leadership. Instruktiv dazu Ricardo Semler, Das Semco System, München 1993; Niels Pfläging, Führen mit flexiblen Zielen, Frankfurt 2008). Auf unser Thema der Compliance als Führungsaufgabe bezogen finden sich diese Gedanken grafisch dargestellt in der folgenden Abbildung (Abb. 14.2).

Dieses **von mir entwickelte**, in der Praxis bewährte (**digital-gestützte**) **Compliance-by-Feedback** oder **Compliance-Management-by-Feedback** basiert auf der Informations-

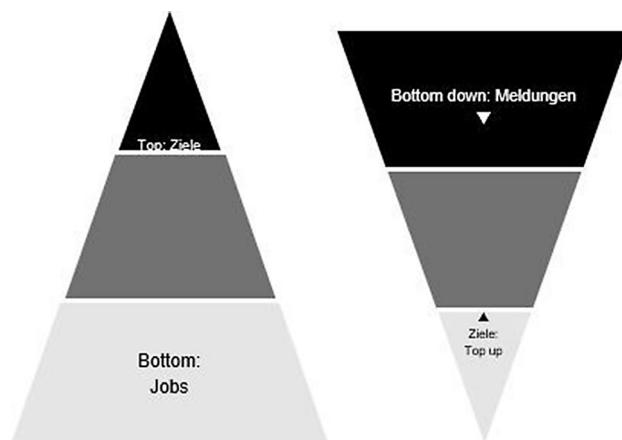


Abb. 14.2 Servant Leadership Ansatz für die Compliance

logistik von operativen Meldungen, die aus allen Stellen von allen Stelleninhabern in den Compliance-Prozess mit eingebracht werden müssen.¹⁵ Dies geschieht im vorgestellten Praxismodell auf periodischer Basis (z. B. einmal wöchentlich) mit einer rationalisierten Syntax über alle Hierarchiestufen hinweg. Dabei geht es vornehmlich nicht darum, die kritischen Entwicklungen aufzuzeigen, sondern bereits im Vorfeld dafür zu sorgen, dass solche negativen Entwicklungen erst gar nicht entstehen.

Alle Mitarbeiter werden damit Mitarbeiter der Compliance. Alle verantwortlichen Führungskräfte werden Führungskräfte der Compliance. Compliance ist damit **eine für alle** – aber damit sind auch **alle für eine (Compliance)** eingebunden. Im Kurs diskutierten wir, ob dies *zu schön, um wahr zu sein* sei – oder *zu wahr, um schön zu sein*. Anhand entsprechender Referenzprojekte und mehrjähriger Projekterfahrungen aus meiner Praxis in mittelständischen Firmen wie auch in international operierenden Firmengruppen diskutierten wir im Kurs daher die Anwendbarkeit in meinem Unternehmen, ebenso wie für das eigene Unternehmen und den eigenen Verantwortungsbereich der Teilnehmenden.

14.5 Compliance wird bei uns gemanagt

Für unseren Kurs haben wir bewusst auf die eher akademische Trennung der Begriffe Führung und Management verzichtet.¹⁶ Für unseren Kurs haben wir uns darauf verständigt, dass Führung und Management eins sind. Es geht also sowohl um das „Richtunggeben“ (Führung) als auch um das beherzte „In-die-Handnehmen“ (Management, maneggiare) bei der Compliance. Es geht um Vorbildfunktion und in diesem Sinne auch um klare Ansagen und Vorgaben. „*So wird bei uns die Compliance gemanagt!*“ ist eine selbstbewusste und handfeste Ansage, sie ist aber auch Führungsaufgabe und soll hier dargestellt werden.

14.5.1 Die vier Gebote der Compliance

In jedem der Kurse und somit auch in diesem Beitrag bin ich auf die Haftungsposition der Geschäftsführung wie auch der Managementebenen eingegangen. In diesen Managementebenen finden sich auch die Compliance-Officer. Eine Orientierung gibt aus diesem haftungsrechtlichen Blickwinkel die eingangs benannte Norm des § 43 GmbHG und auch des § 93 AktG. Zwar steht darin nur, dass **die Sorgfalt eines ordentlichen Kaufmanns bzw. Geschäftsleiters für die Geschäftsführung** gefordert ist,¹⁷ doch in der näheren Ausprägung soll es immer auch um vier Kardinalpflichten gehen, die hier genannt seien.

¹⁵Vgl. Link (2011, S. 131).

¹⁶Vgl. Link (2011, S. 3 ff.).

¹⁷Als Beispiel der Wortlaut des § 43 Abs. 1 GmbHG: „Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.“ und des § 93 Abs. 1 AktG: „Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden.“

Organisieren, Delegieren, Kontrollieren und Dokumentieren können als die obersten Pflichten für die Geschäftsführung verstanden werden, die sie entsprechend auf die nachgeordneten Führungsebenen übertragen darf. Mit unseren Betrachtungen in den vorhergehenden Kapiteln haben wir das Thema Organisation mit der Statik einer Unternehmung näher betrachtet. Letztlich findet sich diese Statik in jedem Organigramm ohne weiteres wieder, welches für eine Unternehmung erstellt wird. Die Pflicht der Delegation haben wir voranstehend mit der Definition der Aufgabe des Compliance-Officers ebenfalls näher betrachtet. Die Kontrollpflicht als Dritte der Kardinalpflichten haben wir mit einem eigenen Konzept im Sinne der Sensorik und Aktorik in unserem Haus der Compliance betrachtet. Die Dokumentation als letzte der vier Pflichten soll nachfolgend unter dem Begriff der Nachhaltigkeit betrachtet werden.

Führt ein Compliance-Officer das Themenfeld Compliance in die **Nachhaltigkeit**, so sorgt er dafür, dass sein Tun nicht nur für eine kurze Weile und vielleicht sogar vergebens war. Die Compliance *nachhaltig* zu bewirtschaften meint damit auch, den kontinuierlichen Verbesserungsprozess am Laufen zu halten. Hier bekommt die Dokumentation ihren Sinn.¹⁸ Sie dient nicht nur dem Wissenserhalt, der Weitergabe und der Nachprüfbarkeit aktueller Informationen, sie kann auch der Aufdeckung und Weiterverarbeitung von Compliance-Inhalten dienen. In den vorangehenden Kapiteln habe ich aufgezeigt, dass die Beschreibung der Stellen, der Aufgaben und der Verantwortungen bzw. Kompetenzen auf diese Dokumentationspflicht *einzhalt*.

Wer führt, muss Rechenschaft ablegen. Das ist die wahre Essenz von Verantwortung. Compliance ist, auch wenn die Vorurteile anders lauten, eine wirtschaftliche Tätigkeit, da sie dem Geschäftszweck dienen soll. Es ist somit immer auch zu fragen, was in einer unternehmerischen Tätigkeit investiert wird und was sie unter dem Strich bringt. Am leichtesten tun sich solche Funktionen, wie der Vertrieb oder die Fertigung, bei denen ganz klar mit Messzahlen ermittelt werden kann, in welcher Weise die Bereiche ihren Wertbeitrag zum Unternehmenserfolg leisten. Leistungen werden so vergleichbar und die Entscheidung über die Reduzierung von Aufwänden oder die Erhöhung von Erträgen möglich gemacht.

Linienfunktionen werden seit jeher über diese Art des Controllings gesteuert. Administrative Bereiche und solche Funktionen wie die Compliance tun sich da schwerer.

14.5.2 Wertbeitrag der Compliance

Hier schließt sich der Kreis zwischen Vorurteil und Akzeptanz. Die zu Beginn erwähnten Vorurteile, dass Compliance unnötige Kosten verursacht, ohne Ertrag zu bringen, müssen entkräftet werden, um Vorurteile abzubauen und Akzeptanz zu gewinnen. Natürlich ist Compliance personalintensiv. Die Compliance automatisieren zu wollen: das ist eine von KI-Begeisterten noch eher theoretisch verfolgte Arbeitsannahme. Dass die Personalkosten für die, die sich um Compliance kümmern, gerechtfertigt sind, muss vertretbar dargestellt werden können. Hier ist der Ansatzpunkt, dass Compliance mit ihren Produkten und Diensten einen Wertbeitrag zur Unternehmensstätigkeit leistet.

¹⁸Vgl. Imai (1994, S. 126 ff.).

Verhinderte Strafverfahren oder verhinderte Konventionalstrafen sind sicher zu erwähnen, wenn solche Verfahren bereits in Gang gebracht wurden. Schwieriger ist es, zu substanziieren, dass diese Einsparungen tatsächlich stattgefunden haben, wenn weder Staatsanwaltschaften noch Vertragspartner überhaupt Zivil- oder Straf-Verfahren in Gang gebracht haben. Wie viel Zeit und Kraft solche Verfahren in Anspruch nehmen, können sich die meisten im Unternehmen theoretisch gar nicht vorstellen. Der Einwand in diesem Umfeld ist zu erwarten: „*Alles theoretisch!*“

Der Sach- und Personalmitteleinsatz lässt sich jedoch auch darüber rechtfertigen, dass der Wertbeitrag der Compliance darin besteht, dass *Negative Zonen und Blind Spots der Compliance* gar nicht erst entstehen oder eben vermindert und – bestenfalls – beseitigt werden. Damit zahlt Compliance unmittelbar auf Effektivität und Effizienz der Unternehmung ein. Sie wird damit selbst zum **Teil guter Führung (Good Governance)**, die ganz allgemein als Werttreiber einer guten Unternehmung gesehen wird.¹⁹ In den Unternehmen sprechen daher manche schon von „*Integrity Management*“, wobei Compliance als dessen Teil erscheint.

Weniger Fehler, mehr Durchgängigkeit für Ideen und Verbesserungsvorschläge, ein allgemein besseres Leistungsklima und eine gute Verbindung zu den Leistungsträgern schützen vor inneren Kündigungen, Bummeldienst, Diebstählen oder gar Sabotage.

Aus der Perspektive der Führung geht es im Wesentlichen darum, Akzeptanz und Mitstreiter für die Aufgabe der Compliance zu gewinnen und damit die Leistungsfähigkeit der Unternehmung nachhaltig zu sichern.

Literatur

- DEEKELING, D./BARGHOP E. (2003): Kommunikation im Corporate Change, Wiesbaden.
- FENGLER, J. (2009): Feedback, 4 Aufl., Weinheim.
- IMAI, M. (1994): KAIZEN, 4. Aufl., München.
- LINK, J. (2011): Führungssysteme, 6. Aufl., München.
- LOHMANN, D. (2012): ... und Mittags geh ich heim, Wien.
- MALIK, F. (2009): Strategie des Management Komplexer Systeme, 7. Aufl., Bern.
- MARIMÓN, G. (2012): FEEDBACK, Norderstedt.
- NIEDEREICHHOLZ, C. (2000): Internes Consulting, München.
- PFLÄGING, N. (2008): Führen mit flexiblen Zielen, Frankfurt/New York.
- RIES, G./PEINIGER, G. (2009): Haftung und Versicherung von Managern, 2. Aufl., Regensburg.
- SEMLER, R. (1993): Das SEMCO-System, München.
- TRANSKI, J. S./RADTKE, C./UHLEMANN, C. (2009): Managementhaftung und Risikomanagement, München.

¹⁹Vgl. Transki/Radtke/Uhlemann (2009, S. 8 ff.).



Gerald Marimón Der Verfasser ist gebürtiger Westfale. Nach den juristischen Staatsexamina in Hamm und Düsseldorf arbeitete er als Syndikus langjährig für ein DAX-Unternehmen in den Aufgabenfeldern Personal und Organisation. Er promovierte an der Universität Augsburg berufsbegleitend zu praktischen Fragestellungen der Unternehmensumstrukturierung.

Marimón ist Rechtsanwalt in Augsburg mit den Interessengebieten Arbeits- und Gesellschaftsrecht im Schwerpunkt der Prävention von Mobbing, Burnouts und Haftung. Er ist Gründer und Leiter des fiib® feedlab-institute, das im Bereich Governance, Legaltech, Compliance und Management-Qualität inzwischen Mittelstandunternehmen und international operierende Unternehmensgruppen für Beratungen, Schulungen und Software zu seinen Kunden zählt.

Er lehrte viele Jahre an der Juristischen Fakultät der Universität Augsburg und am ZWW zu den Themen Arbeitsrecht, Kanzleimanagement und Compliance.

Autorin des Stichwortverzeichnisses

Clara Slawik¹ studierte in Regensburg Musik- und bewegungsorientierte Soziale Arbeit, nebenbei arbeitete sie als Tutorin für Familienrecht und als studentische Hilfskraft. Nach ihrem Abschluss und mehreren Semestern im Studiengang Rechtswissenschaften widmet sie sich aktuell dem Lehramtsstudium an der Universität Augsburg. Seit Oktober 2023 arbeitet sie als studentische Hilfskraft im Bereich der Juristischen Weiterbildung am ZWW der Universität Augsburg und ist dort für die Compliance-Weiterbildungen zuständig.



¹Clara Slawik, Augsburg, Deutschland, E-Mail: Clara.Slawik@zww.uni-augsburg.de.

Stichwortverzeichnis

A

Abkauf von Wettbewerb 78
Ablaufmatrix 120
Ad-hoc-Publizitätspflicht 136
AI Act 8
Allgemeines Gleichbehandlungsgesetz (AGG),
 siehe Vorschriften
Amtsträger, Bestechung, *siehe Korruption*,
 Amtsträger
Anic-Regeln, *siehe Kartell, Anic-Regeln*
Anomalie 135, *siehe auch: Red Flag*
Anzeigepflicht 72, 135, 285
Arbeitgeber, Direktionsrecht 234, 285, 286
Arbeitnehmer, persönliche Rechte 149, 181,
 191, 294, 297, 298
arbeitsrechtliche Mittel 301
Aufbauorganisation, steuerliche 120
Aufsichtsbehörde 25, 126, 128, 137, 138,
 167, 193
Aufsichtspflicht, allgemeine 301
Auskunftsverweigerungsrecht 90, 299
Auslandsbestechung, *siehe Korruption*,
 Auslandsbestechung

B

BaFin, *siehe Bundesanstalt für
 Finanzdienstleistungsaufsicht*
Bank- und Kapitalmarktrecht
 Aufgabe der Compliance 135
 siehe auch Marktmisbrauch
 bei Organisationspflicht 142

Clara Slawik, Augsburg, Deutschland,
E-Mail: Clara.Slawik@zww.uni-augsburg.de.

Berater, Korruption 168
Beschwerdestelle 25, 300
Bestechung, *siehe Korruption*
Betriebsinhaberhaftung 110, 116, 200, 360,
 siehe auch Geschäftsleitung,
 Haftung der
Betriebsrat 54, 192, 232, 233, 289–291, 293,
 301, 308, 310, 311
Mitbestimmungsrecht 90, 166, 233, 286,
 287, 292–294
Betriebsvereinbarung 167, 191, 286, 289
Betrug
 Association of Certified Fraud Examiner
 (ACFE) 33
 Betrugshandlung 33
 Folgeschäden 33
 Fraud 33, 324
 Fraud Triangle 34
Bundesanstalt für Finanzdienstleistungsaufsicht
 (BaFin) 128, 135, 138, 140, 141, 208
Bundesarbeitsgericht (BAG),
 Rechtsprechung 190
Bundesdatenschutzgesetz (BDSG) 169,
 235, 304
Bundesgerichtshof (BGH), Rechtsprechung 9,
 10, 116, 200
Bundesverfassungsgericht (BVerfG),
 Rechtsprechung 149, 156, 176,
 177, 186
Bußgeld
 allgemein 252
 Anzeigepflicht 135
 Arbeitsschutz 283
 Datenschutz 14, 194, 312
 Haftung für Mitarbeiterfehlern 116
 Hinweisgeberschutzgesetz 167, 213

- Insiderhandel 127
Kartellverstoß 80, 81, 83, 84, 86, 87, 89
leichtfertige Steuerverkürzung 115
Verdachtsmeldung, Geldwäsche 103,
105, 109
Verletzung von Organisations- und
Kontrollpflichten 55
- C**
- Chinese Walls 130
Code of Conduct (Verhaltenskodex) 13, 63, 70,
270, 288, 335, 340
Code of Ethics 5, 283, 293
Compliance
 Akzeptanz 348, 363
 Anti-Korruptions-Compliance 61
 Arbeitsrecht 283
 Arbeitsvertrag, Verankerung im 285
 Beauftragter *siehe Compliance Officer*
 Bedingungen für regelkonformes
 Verhalten 263
 Berichte 141
 betriebswirtschaftliche Aspekte 21, 26
 Blind Spots 359, *siehe auch: Non-*
 Compliance
 Competition Compliance 85, 89
 Compliant Compliance, *siehe auch:*
 Compliance, Übererfüllung
 Compliance Management System (CMS)
 7, 10, 21, 26, 29, 113, 116, 118,
 200, 270, 284, 298, 316, 327
 Compliance-by-Feedback 361
 Corporate Compliance 20
 Creative Compliance 260
 Definitionen 13, 249, 333
 Dokumentation 294, *siehe auch*
 Dokumentation
 Einführung 348
 Emittenten-Compliance 136
 ESG 36
 ethischer Aspekt 331
 Fachdisziplin 12
 Forced Compliance 264
 Führungsaufgabe 135
 Funktion 139, 322, 354
 ganzheitliche Perspektive 272, 332
 Geldwäsche-Compliance 96, 324, *siehe*
 auch Geldwäsche
 Geschichte der 232
- Interdisziplinarität 10
IT 28
Kommunikation 123, 266, 275, 295,
351, 361
Kultur 28, 119, 139, 272
Legal Compliance 334
Maßnahmen 85, 88, 122, 130, 141, 149,
267, 268, 287, 294, *siehe auch*
 Schulung
Maßnahmen, Grenzen der 149
Negative Zone 358, *siehe auch Non-*
 Compliance
Non-Compliance, *siehe Non-Compliance*
öffentliche 263
Product Compliance 316, 317, 320,
323–326, *siehe auch Product*
 Compliance
rechtliche Voraussetzungen 5
Regelungen 287
Richtlinien und Policies 63
Risiken 33, 89, 316, *siehe auch Risiko*
Social Compliance 334
Tax Compliance, *siehe Tax Compliace*
Übererfüllung 149
Überwachung 124, 149, 283, 319
Verantwortung der Geschäftsleitung 61
Verstöße 29
Vorschriften 291
Vorurteile 348, 363
Wertemanagement 5, 340, 341–343
Wirkungsgrad 358
Ziel 113, 116, 119
Zielkontenrahmen 354
Compliance Officer 8, 9, 14
 Aufgaben 300, 335, 349
 Garantenpflicht des Compliance Officer 301
Haftung 83, 300, 358
Kardinalpflicht 362
Karriere 355
Persönlichkeit 140
Rolle 339
Schlüsselkompetenzen 138
Selbstverständnis 335, 338
Typen von 356
Unabhängigkeit 140
Vertreter 141
Corporate Governance Kodex 5, 25, 28, 248,
283, 338
Corporate Social Responsibility (CSR) 270,
 siehe auch Richtlinie, Corporate

- Sustainability Reporting Directive (CSRD)*
- Corporate Sustainability Due Diligence Directive (CSDDD) 25
- Corporate Sustainability Reporting Directive (CSRD) 9, 22, 23
- COSO-Rahmenkonzept/-Framework 29
- COSO-Würfel 29, *siehe auch COSO-Rahmenkonzept/-Framework*
- CSDDD 25, *siehe Corporate Sustainability Due Diligence Directive (CSDDD)*
- CSRD 9, 22, 23, *siehe Corporate Sustainability Reporting Directive (CSRD)*
- D**
- Datenschutz, mitarbeiterbezogener 304
- Datenschutzbeauftragter 237
- Datenschutzrecht 151, 169, 294, *siehe auch Richtlinie, DSGVO*
- Dawn Raids, *siehe Kartell, Dawn Raids*
- Deutscher Corporate Governance Kodex (DCGK) 5
- Director's Dealings 137
- Direktionsrecht des Arbeitgebers 234, 285
- Dokumentation/dokumentieren
- Aufgabe des Compliance Officers 335
 - Compliance Management System 26
 - Nachweis 36, 69, 70, 89, 122, 124, 126, 130, 210, 287, 353
 - Pflicht 102, 103, 123, 239, 294, 302, 306, 309, 326
- Doppelte Wesentlichkeit/Materialität 23
- Due Diligence 24, 68–70
- Due Diligence-Prozess 69
- E**
- Eigengeschäft 137
- E-Mail
- Filterung 150, 152, 153, 166
 - Privatnutzung/private Mails 153, 154, 156
 - Screening 154, 162
 - Überwachung 150, 299, 309
- ESG, *siehe Nachhaltigkeit*
- ESRS, *siehe Standards, internationale*
- Ethik, Definition 336
- Europäischer Gerichtshof (EuGH), Rechtsprechung 82, 310
- Europäischer Gerichtshof für Menschenrechte (EGMR), Rechtsprechung 204, 208
- F**
- Fallbeispiel 317
- Fehlverhalten, Motive 249
- Folgeschaden 33
- Foreign Corrupt Practices Act (FCPA) 59, 283
- Fraud, *siehe Betrug*
- Fraud Triangle, *siehe Betrug*
- Führung
- Aufgabe moderner 338
 - Definition 338
- Führungsperson/-kraft 137, 273, 274, 339, 340
- G**
- Gebietsschutz, absoluter 79
- Geldwäsche
- Bargelobergrenze 111
 - Dreiphasenmodell 97
 - Financial Action Task Force (FATF) 96
 - FIU-Typologie 104
 - Gegenstand der 97
 - Gesamtkontamination 98
 - Güter 97, 99, 111
 - Güterhändler 96, 99, 100, 111
 - Güterhändler, privilegierter 101
 - Kernpflicht 101
 - Kundensorgfaltspflicht im Verdachtsfall 107
 - leichtfertige 106, 109
 - Meldung von Verdachtsfällen 101, 105, *siehe auch Anzeigepflicht*
 - Mitwirkung 108
 - PEP-Risiko 108
 - rechtliche Rahmenbedingungen 97
 - Schwellenwerte 99, 102
 - Selbstanzeige 109, *siehe auch Selbstanzeige*
 - Sorgfaltspflicht 101, 107, 108, 109
 - Surrogate 97
 - Terrorismusfinanzierung 98, 323
 - Tipping-Off-Verbot 109
 - Verdachtsmeldepflicht 103
 - Wartefrist 106
 - wirtschaftlich Berechtigter 107

- Geschäftsgeheimnis 206, 302, 303
 Geschäftsleitung
 Bericht an 32, 124, 141, 177, 199, 322
 Delegation durch 123
 Eigeninteresse 67
 Gesamtverantwortung für Compliance 139, 360
 Haftung der 55, 61, 83, 110, 114, 149, 301, 312, 350, 362, *siehe auch Betriebsinhaberhaftung*
 Legalitätskontrollpflicht 61
 Produktkenntnis 326
 Whistleblowing 198, 200
 Geschenk
 Indizien zur Zulässigkeit 67
 steuerlich relevantes 67
 Gesetz, *siehe Vorschriften*
 Gesetz über Ordnungswidrigkeiten (OWiG),
 siehe Vorschriften, Gesetz über Ordnungswidrigkeiten; siehe auch Haftung nach § 130 OWiG
 Gesetz zum Schutz von Geschäftsgeheimnissen 206, 302
 Good Governance 332
 Guidelines 26
 Gut 337, *siehe auch Geldwäsche, Güter*
- H**
 Haftung 11, 27, 69, 90, 105, 117, 130, 270, 283, 284, 294, 295, 312, 317, 324, 350
 Haftung nach § 130 OWiG, *siehe Betriebsinhaberhaftung; Compliance Officer, Haftung; Geschäftsleiter, Haftung*
 Helpdesk 13
 Hinweisgeber 196,
 siehe Whistleblowing
 Hinweisgeberschutzgesetz (HinwGebSchG),
 siehe Vorschriften, Hinweisgeberschutzgesetz
 Hinweisegeberstelle 128
 Hinweisegebersonsystem 8, 13, 60, 71, 198, 201, 202, 205, 218–220, 225, 232–234, 237
 Homeoffice 311, 312, 336, 342
- I**
 IdW PS 980 7, 26, 118
 Immunsystem der Unternehmung 348
 Indikator 21, 31, 79, 91, 136, 360
 Informationsaustausch 77, 80
 informelle Netzwerke 259
 Insider
 Barrieren 131
 Insiderhandel 127, 129, 132, 135
 Insiderinformation, Definition 129, 136
 Insiderliste 130
 Ziel des Insiderhandelsverbots 130
 Integrität 256, 263
 Definition 256
 Integrity Management (System) 35, 364
 Integrity Thermometer 276
 Kultur 272
 Messung 276
 Internationale Übereinkommen 42
 Internetverkehrsdaten 175, 178, 179
 Interne Kontrolle 29
 Compliance Audits 71, 74
 Dokumentation 123, *siehe auch Dokumentation/dokumentieren*
 Institute of Internal Auditors (IIA) 31
 Internal Audits 31
 Internal Investigations 14, 74, 299
 Internes Kontrollsysteem (IKS) 7, 29, 60, 123
 Kontrollaudits 93
 ISAE 3000, *siehe Standards, internationale ISO-Norm, siehe Standards, internationale ISSA 5000, siehe Standards, internationale IT-Grundrecht 151, 186–189*
 IT-Sicherheit 151, 153, 164, 165
- K**
 Kartell
 Anic-Regeln 80
 Arten von 76
 Aufsichtsbehörde 85
 Compliance-Maßnahme 88, *siehe auch Compliance, Maßnahmen*
 Dawn Raids 86
 Ermittlungsverfahren 87
 Folgen von Verstößen 131

- Follow-on-Klagen 87
Grundsatzentscheidungen des EuGH 82
Haftung des Compliance-Beauftragten 83
Kartellverbot 76, 81
Kartellverfahren 85
Marktbeherrschung 79, *siehe auch Marktmissbrauch*
nachhaltige Wertschöpfung durch effektive Competition Compliance 85
Passing-on-Einwand 82
relevant im Kontakt zu Lieferanten und Händlern 78
relevant im Kontakt zu Wettbewerbern 78
Risiken von Mock Dawn Raids 93
Risikoindikatoren 91
Selbstanzeige 86, *siehe auch Selbstanzeige*
Selbstreinigung 84
Unternehmenskäufe 80
Verfahrensrechte 87
Verjährung 82, 88
Know-Your-Customer (KYC) 102, 107, 121, 326
Kollegenlieferung 78
Kontrolle 267
Kontrolle, Folgen unzulässiger Maßnahmen 190
Kontrolllücke 31
Korruption 42
 Amtsträger 48, 56
 Anforderung an Compliance 61
 Anzeigepflicht 72, *siehe auch Anzeigepflicht*
 Arbeitnehmervertreter 54
 ausländische Rechtsvorschrift 60
 Auslandsbestechung 45
 Bekämpfung von 21, 203, 316
 branchenspezifische Richtlinien 64
 Folgen 44, 72
 freiwillige Meldung 73, 218
 Geschäftspartner 69
 Geschenke, *siehe Geschenk*
 im Ausland 55
 im Gesundheitssektor 43, 44
 im privaten Sektor 44, 51, 57
 internationale Empfehlungen 203
Korruptionsdelikt 42–46, 48, 55
Mandatsträger 53, 57
Prophylaxe 61, 62
Reaktion auf entdecktes Verhalten 72
Rechtslage in Deutschland 44
Richtlinien und Policies 63
Risikoanalyse 62, *siehe auch Risiko, Risikoanalyse*
sozialadäquate Zuwendung 54
Tathandlung 55
Unrechtsvereinbarung 47, 49, 51
Vermittler 68
Vorteil 46, *siehe auch Vorteil*
wesentliche Merkmale 46
Kronzeuge 83, 86, 88, 89, 300
Kryptowährung 126, 128
Kultur 36, *siehe auch Unternehmen, Unternehmenskultur*
Kundensorgfaltspflicht 107
Künstliche Intelligenz (KI) 343
KYC 102, *siehe Know-Your-Customer-(KYC)*
- L**
Lean-Back-Syndrom 31
Legalitätskontrollpflicht der Geschäftsleitung 61
Legitimität 332, 334
Lieferkettensorgfaltspflichtengesetz (LkSG) 9, 24, 28, 206, 207, 332, 343
Loyalität 34, 204, 251, 258
- M**
MaComp 7, 139
Marktmanipulation 126, 128, 129
 Ausnahmen des Tatbestandes 135
 Verbot 132
Marktmissbrauch 81, 129, 143
Marktmissbrauchsverordnung 129, 130, 133, 136, 137, 143
Materiality
 Financial 23
 Impact 23
Meldepflicht 103–105, 127
Meldestelle, -kanäle 168, 214
 interne 168, 200, 201, 212, 217
Mock Dawn Raids 92, *siehe auch Kartell*

- N**
- Nachhaltigkeit 363
 - ESG 8, 317, 332
 - Nachhaltigkeitsbericht 22, 23, 26
 - Nichtfinanzielle Erklärung 20
 - Non-Compliance 249, 255
 - Arten und Kategorisierungen 249
 - Bedingungen auf Personen- und Organisationsebene 255, 261
 - Erklärungsmodelle 252
 - Folgen 251
- O**
- Ombudsperson 199, 219
 - Organigramm 355, 357, 358, 363
- P**
- Passing-on-Einwand, *siehe Kartell, Passing-on-Einwand*
 - Post- und Fernmeldegeheimnis 152
 - Prävention 33, 34
 - Preisbindung der zweiten Hand 79
 - Prinzipienorientierung 30
 - Product Compliance 317, 320, 323-326
 - Definition 316
 - Risiken 321
 - Publizitätspflicht, Ad-hoc- 136
- R**
- Rechtsnorm 61, *siehe Vorschriften*
 - Rechtsprechung *siehe*
 - Bundesarbeitsgericht (BAG), *Rechtsprechung*
 - Bundesgerichtshof (BGH), *Rechtsprechung*
 - Bundesverfassungsgericht (BVerfG), *Rechtsprechung*
 - Europäischer Gerichtshof für Menschenrechte (EGMR), *Rechtsprechung*
 - Europäischer Gerichtshof (EuGH), *Rechtsprechung*
 - Red Flags 14, 34
 - Regulation Technologie 136
 - Remote Working 336, 342, *siehe auch Home-Office*
- S**
- Sanktion
 - Arbeitnehmerschutz 283, 298
 - Datenschutzverstoß 151, 312

- Durchsetzung von 343
Fallbeispiel 320
Hinweisgeberschutz 201, 211, 218, 221, 222
Kartellverstoß 81–85, 87–89, 91, 93, 224
Kommunikationsmittel 126
Korruption 42, 69, 72
Mitarbeiter 258, 263, 269, 270, 286, 357
Sarbanes-Oxley-Act (SOX) 5, 30, 202,
 283, 332
Schadensersatz 72, 76, 130, 133, 193, 251, 297
Schulung 13, 55, 60, 70, 85, 88, 122, 130, 141,
 149, 267, 268, 287, 294, 350, 352
Screening 90–92, 152–154, 175–179
 von E-Mail 175
 von Internetverkehrsdaten 178
Selbstanzeige 72, 86, 109
Speak-up-policy 36
Spende 67
Sponsoring 67
Stakeholder 25, 27, 251, 274, 276, 324,
 341, 342
Standards, internationale
 European Sustainability Reporting
 Standards (ESRS) 23
 Global Reporting Initiative (GRI) 22
 International Standard on Assurance
 Engagements (ISAE) 3000 27
 International Standard on Sustainability
 Assurance (ISSA) 5000 27
ISO 19600 7, 26, 275
ISO 37001 7, 26
ISO 37002 26
ISO 37301 26
Steuer, *siehe Tax Compliance*
Steuerhinterziehung 45, 115
 durch Unterlassen 117
steuerliche Aufbauorganisation 116
Strafbarkeit
 E-Mail-Überwachung 153, 155, 165,
 183, 298
 Garantenpflicht des Compliance Officer 301
 Geldwäsche 96, 98, 103, 106, 109
 Kartellverstoß 76, 83, 84
 Korruption 44, 59, 73
 Ombudsperson 237
 Telefon- und Videoüberwachung 183, 298
Strafgesetzbuch (StGB), *siehe Vorschriften, Strafgesetzbuch; Strafbarkeit*
Submissionsabsprache 77, 83
- T**
Tax Compliance
 Aufgabenfeld 114
 Definition 113
 Konfliktfall 114
 Maßnahmen 118–124
 rechtliche Grundlagen 116
 Steuerhinterziehung 114, 117, *siehe auch Steuerhinterziehung*
 Steuerkürzung 114
 Tax Risk Management 114
Telefonüberwachung 183
Terrorismusfinanzierung, *siehe Geldwäsche, Terrorismusfinanzierung*
Three Lines of Defense 31
tone from the top/tone-of-the-top 12, 30,
 63, 93, 295
Tugend, Definition 341
- U**
Überwachung 298
UK Bribery Act 2010 58, 61, 316
Unternehmen
 Dimensionen der
 Unternehmenskultur 36
 Governance-Struktur des
 Unternehmens 22, 326
 Unternehmensentwicklung 321
 Unternehmensführung 332
 Unternehmenskultur 14, 28, 34–36, 85, 93,
 123, 260, 261, 272–274, 276, 335,
 340, 342
 Unternehmensleitlinie 28
 Unternehmensleitung 25, 283, 300, 301,
 339, 355
 Unternehmensreputation 15, 33, *siehe auch Reputation*
- V**
Verantwortung 263, 265, 350, 358
 Begriffsdefinition 265, 363
 Dreiecksmodell 266
Verbot des Onlinevertriebs 79
Verhaltenskodex 270, 295, *siehe auch Code of Conduct; Code of Ethics*
Vermittler, Korruption 68
Videoüberwachung 183, 299

- Vorgesetzte 12, 198, 259, 261, 262, 297
Vorschriften (Gesetze und andere
Rechtsnormen; national,
supranational, international), *siehe auch* Richtlinie
AI Act 8
Allgemeines Gleichbehandlungsgesetz
(AGG) 295
Anic-Regeln, *siehe Kartell, Anic-Regeln*
Bundesdatenschutzgesetz (BDSG) 169,
235, 305
Deutscher Corporate Governance Kodex
(DCGK) 5
Foreign Corrupt Practices Act
(FCPA) 59, 283
Geldwäschegegesetz (GwG) 96
Gesetz über Ordnungswidrigkeiten
(OWiG) 5, 55, 81, 83, 110, 116, 200,
216, 239, 284, 295, 300, 301, *siehe auch Haftung nach § 130 OWiG*
Gesetz zum Schutz von
Geschäftsgeheimnissen 206, 302
Gesetz zur Kontrolle und Transparenz
im Unternehmensbereich
(KonTraG) 5
Hinweisgeberschutzgesetz 8, 13, 167, 168,
197, 201, 203, 205, 207, 208, 210,
213, 214, 218, 220, 221, 227–229,
231, 232, 234, 239, 283, 360
Kartellverbot 81
Lieferkettensorgfaltspflichtgesetz
(LkSG) 9, 24, 28, 206, 207, 332, 343
MaComp 7, 139
Marktmissbrauchsverordnung 129, 130,
133, 137, 143
Sarbanes-Oxley-Act (SOX) 5, 30, 202,
283, 332
Strafgesetzbuch (StGB) 44, 45, 48, 49, 51,
53, 56–58, 77, 84, 96–98, 103,
104, 109, 135, 150–152, 154,
165, 166, 176, 177, 183, 184,
238, 298, 301, *siehe auch Strafbarkeit*
UK Bribery Act 2010 58, 61
Vorteil
Definition 46
Drittvorteile 47
materieller und immatrieller 46
- W**
Wertematrix 341
Wettbewerb, Abkauf von 78
Whistleblowing 167, 171, 270, 300, 303,
325, 360
Aufreten 169, 171, 174, 266
Definition 196
internes und externes 198
Motive 199
Unterschiede USA – Deutschland 202
- Z**
Zertifikatskurs 12
Zertifizierung
gemäß ISO-Norm 26
Nutzen und Herausforderung 26
Prüfungsbereich 26
Zuwendung, sozialadäquate 54
Zeugnisverweigerungsrecht 237