Münchener AnwaltsHandbücher

Münchener Anwaltshandbuch Verteidigung in Wirtschafts- und Steuerstrafsachen

von

Prof. Dr. Dr. h.c. Klaus Volk, Dr. Heiko Ahlbrecht, Dr. Markus Berndt, Dr. Stephan Beukelmann, Dr. Dieter Bohnert, Dr. Marcus Böttger, Dr. Guido Britz, Dr. Matthias Dann, Dr. Felix G. Dörr, Hanns W. Feigen, Dr. Walther Graf, Dr. Gina Greeve, Dr. Bettina Grunst, Dr. Simone Kämpfer, Eberhard Kempf, Dr. Christoph Knauer, Thomas C. Knierim, Dr. Klaus Köpp, Dr. Daniel M. Krause, Dr. Klaus Leipold, Dr. Werner Leitner, Prof. Dr. Heiko Lesch, Prof. Dr. Jörg-Andreas Lohr, Dr. Ingo Minoggio, Prof. Dr. Ursula Nelles, Dr. Anna Oehmichen, Prof. Dr. Tido Park, Dr. Hans-Joachim Prieß, Prof. Dr. Thomas Rönnau, Dr. Markus Rübenstahl, Prof. Dr. Franz Salditt, Dr. Wolf Schiller, Dr. Hellen Schilling, Dr. André-M. Szesny, Dr. Michael Tsambikakis, Renate Verjans, Prof. Dr. Joachim Vogel, Prof. Dr. Jürgen Wessing, Peter Witting

2., überarbeitete und erweiterte Auflage

Verlag C.H. Beck München 2014

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 406 64369 9

Zu Inhalts- und Sachverzeichnis

mungen und definiert die verschiedenen Teilnehmer des Außenwirtschaftsrechts sowie deren Tätigkeiten. In seinem dritten Teil finden sich Strafvorschriften, Bußgeldvorschriften und Überwachungsvorschriften, was gleichzeitig Durchsetzung und Überprüfung der Durchsetzung sichern soll. Das Gesetz ist in weiten Bereichen ein Blankettgesetz, wenn es auf Listen, Rechtsverordnungen, Rechtsakte der europäischen Gemeinschaften oder Europäischen Union verweist. Es enthält in § 34 Abs. 6 **Verbrechenstatbestände,** die zum Teil begrifflich mit Generalklauseln oder unbestimmten Rechtsbegriffen wie „der Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland" verbunden sind. In diesen Fällen ist die Strafandrohung nicht unter zwei Jahren, ansonsten endet der Strafrahmen bei fünf Jahren. Die fahrlässige Begehung ist in weiten Bereichen unter Strafe (Geldstrafe und Freiheitsstrafe bis max. 3 Jahre) gestellt.

- Die **Außenwirtschaftsverordnung,**[345] anknüpfend an § 7 des Außenwirtschaftsgesetzes, enthält im einzelnen formulierte Verbote sowie Genehmigungspflichten.
- Als Anlage zur Außenwirtschaftsverordnung enthält die **Ausfuhrliste** eine Aufzählung nach Kategorien der von den Verboten und Genehmigungspflichten betroffenen Waren.
- Korrespondierend zur Außenwirtschaftsverordnung existiert die so genannte **Dual-Use-Verordnung.**[346] Sie betrifft den Export all jener Waren und Güter, die ihrem potentiellen Verwendungszweck nach auch für kriegerische Zwecke verwandt werden können.
- Zu beachten sind darüber hinaus alle jenen Regelungen, die aufgrund von **Embargos** der UN oder der OSZE erlassen werden.
- All diejenigen Personen und Unternehmen, die mit Gütern handeln, die ursprünglich aus dem Bereich der **Vereinigten Staaten** stammen, haben die in den Vereinigten Staaten für solche Fälle geltenden Regelungen zu beachten.[347]

f) IT. In dem gleichen Maße, in dem sich elektronische Datenverarbeitung in allen Bereichen des Wirtschaftslebens ausgebreitet hat, haben sich rechtliche Regelungen entwickelt – mit der gleichen Komplexität[348] und mit den gleichhohen Anforderungen. Daraus resultiert häufig, dass Aufgaben und Überwachung der EDV-Struktur eines Unternehmens von der Leitungsebene so weit weg delegiert werden, dass letztendlich Verständnis und Kontrolle auf der Organebene nicht mehr stattfindet.[349] Auch die Tatsache, dass IT eben nicht nur reine Datenverarbeitungsthemen berührt, sondern mit anderen Bereichen, wie beispielsweise dem Steuerrecht, eng vernetzt ist, erleichtert die **Akzeptanz** nicht. Eine unzureichende IT-Compliance kann aber in gleicher Weise Haftungen nach §§ 93 Abs. 2, 116 Abs. 1 AktG und § 43 GmbHG auslösen, wie jede andere Missachtung von Organisationsaufgaben. Würde in manchen Unternehmen ein Bruchteil der Zeit, die im Führungsbereich auf Bilanzfragen verwendet wird, der IT gewidmet, würden deutlich weniger Probleme im Bereich der EDV ent- und fortbestehen – und damit auch einige Bilanzprobleme vermieden. Auch strafrechtlich bietet der Bereich der EDV eine Menge an Stolperfallen nicht nur im Bereich des Datenschutzgesetzes oder der EDV-spezifischen Normen des Strafgesetzbuches wie § 202a (Ausspähen von Daten), § 202b (Abfangen von Daten), § 202c (Vorbereiten des Ausspähens und Abfangens von Daten), § 263a (Computerbetrug) oder § 303a (Computerbetrug). So kann es beispielsweise auch eine Untreue darstellen, Daten nicht zu schützen oder gar weiterzugeben. Eine ganz wesentliche Rolle spielen Daten auch im Bereich des § 17 UWG. Die einfache Portierbarkeit von Datenmengen, die der Mitnahme einer ganzen Bibliothek entsprechen, auf Datenträgern, die in jede Hosentasche passen, hat das Problem deutlich vertieft und zu größerer Häufigkeit von Verstößen geführt. Die wesentlichen Subbereiche der IT sind: **130**

aa) Sicherheit. Daten sind davor zu schützen, dass sie entwendet oder manipuliert werden. Dieser Schutz geht nach innen wie nach außen. Wenn das Unternehmen es unterlässt, **131**

[345] Nachzulesen unter www. gesetze-im-internet.de/awv_1986/; letzte Änderung in Kraft ab 30. 1. 2013.
[346] Zur Dual-use-Verordnung *Karpenstein* EuZW 2000, 677.
[347] Zum US-Außenwirtschaftsrecht s. *Krebs/Sachs* CCZ 2013, 60 (63).
[348] Die Existenz von ca. 25.000 Compliance-Anforderungen im IT-Bereich beschreibt unter Hinweis auf weitere Nachweise *Rath* in Wecker/van Laak, Compliance in der Unternehmerpraxis, S. 151.
[349] Zur Organverantwortung: *Bauer* in Compliance in der Unternehmerpraxis, S. 171.

Schutzmechanismen für seine Daten einzurichten, wird ihm zum Teil auch der gesetzliche Schutz versagt.[350] Die wesentlichen Anforderungen an ein derartiges Schutzkonzept sind:

- Die Existenz eines allgemeinen **Sicherheitskonzeptes.** Dazu gehört auch die Festlegung, welcher Mitarbeiter auf welcher Ebene in Datenverarbeitung eingreifen kann und die Verwaltung von Programmrechten
- **Anweisung für den** EDV-mäßigen **Notfall** wie z. B. einen Angriff auf die Homepage mittels denial of service Attacken
- eine **Datensicherungsstrategie** mit einem garantierten und kompletten täglichen Sicherungslauf und Verbringung der Daten an eine sichere Auslagerungsstelle
- Vorbereitung für den Fall eines technisch bedingten **Systemabsturzes** einschließlich der Wiederherstellung der Funktionsfähigkeit des Systems
- **Verhinderung** der Einbringung von Fremdprogrammen und externen Daten ohne Kontrolle auf deren Integrität und Sicherheit
- **Kontrolle,** dass für jedes im Unternehmen genutzte Programm die notwendige Anzahl an Lizenzrechten vorhanden ist.

132 *bb) Bestandsschutz.* Nicht nur die aktuellen Daten sind zu schützen, auch historische Daten sind entsprechend der gesetzlichen Anforderung zu verwalten. Sowohl Handelsrecht (§ 257 HGB) als auch Steuerrecht (§ 147 AO)[351] konstituieren Aufbewahrungspflichten. Im Bereich der Daten heißt dies, dass sie in lesbarer Form vorgehalten werden,[352] was zum Teil zwingt, auch veraltete Datenverarbeitungssysteme zumindestens noch potenziell aktiv zu halten.[353] Dazu gehört auch, dass Passwörter für Systemzugriffe ebenso aufzubewahren sind, wie die Passwörter für verschlüsselte E-Mails.

133 Bestandsschutz heißt allerdings nicht nur, die Daten überhaupt zu sichern und damit zu besitzen, sie müssen auch zur Verfügung stehen. Das bedeutet, dass Systeme zum Wiederauffinden konkreter Informationen eingerichtet sein müssen wie beispielsweise Datenbanken in so genannten DMS-Systemen.[354] Diese Systeme sind sowohl in ihrer Einrichtung, wie allerdings auch in ihrer Handhabung, recht komplex und mit den üblichen an Bürosoftware ausgerichteten Kenntnissen von Unternehmensmitarbeitern nicht ohne weiteres handhabbar. Es bedarf in diesem Bereich besonderer Schulung, um die Verfügbarkeit nicht nur theoretisch, sondern auch **praktisch zu gewährleisten.**

134 *cc) E-Mail.* Der Einsatz von E-Mails hat in weiten Bereichen das Schreiben konventioneller Briefe ersetzt, das Internet als Informationsmedium ist aus der Unternehmenspraxis nicht mehr hinwegzudenken. Die Abgrenzung dieser unternehmensnotwendigen Nutzung der Hard- und Software eines Unternehmens von der privaten Nutzung sollte klar und eindeutig geregelt sein. Nicht nur aus arbeitsrechtlichen Gesichtspunkten empfiehlt es sich ganz allgemein, die private Nutzung aller Informationssysteme in jeder Form zu untersagen. Die ansonsten entstehende Gemengelage zwischen privaten und geschäftlichen Daten führt zu großen Schwierigkeiten, wie z. B. der Anwendung der speziellen datenschutz- und telekommunikationsrechtlichen Regelungen, die einen so genannten Telekommunikationsdienstanbieter (§ 3 Nr. 6 Telekommunikationsgesetz) treffen. Den Mitarbeitern ein separates, vom Unternehmensnetzwerk völlig getrenntes Terminal zur Verfügung zu stellen, befreit auch von der Prüfung der Frage, ob nicht trotz Verbot eine Duldung vorliegt und deshalb trotzdem die Regeln des Telekommunikationsgesetzes anzuwenden sind. Beseitigt wären damit gleichzeitig Fallen in Richtung des Strafrechtes: Grundsätzlich unterliegen private Mitteilungen in Form von E-Mails dem Briefgeheimnis, so dass eine Kenntnisnahme eine Verletzung von § 202 StGB sein kann. Wird dabei noch ein Passwortschutz überwunden, steht

[350] So gehört es bereits zum Tatbestand des §§ 202a StGB, dass Daten gegen unberechtigten Zugang besonders gesichert sein müssen.

[351] Siehe dazu die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) des Bundesfinanzministeriums, welches nach deren Maßgabe auf alle digitalen und steuerrelevanten Daten des Unternehmens zugreifen kann.

[352] §§ 239 Abs. 4, 257 Abs. 3 HGB.

[353] Umnuß/*Rath/Hunecke* Corporate Compliance Checklisten, S. 207.

[354] Dokumentenmanagement.

§ 202 a StGB in Rede. Zudem kennt das Telekommunikationsgesetz in den §§ 148 und 194 einen langen Katalog von Straftatbeständen und Ordnungswidrigkeiten.

Eine **IT-Richtlinie** oder eine eindeutige **E-Mail Anweisung** an die Mitarbeiter sowie deren Überwachung gehören mithin zum Grundkonzept von IT-Compliance. Wesentliche Strukturen einer solchen Regelung sind nicht nur Verbote, sondern auch Handlungsanweisungen zum Umgang mit Dateien, wie z. B. der Ablage in bestimmten, im Unternehmen generalisierten und einheitlichen, Verzeichnissen. **135**

dd) Internet. Für die private Nutzung von Zugängen zum Internet gilt grundsätzlich das gleiche wie zu E-Mails: Eine klare und eindeutige Regelung ist erforderlich. Eine generelle Untersagung der Nutzung der unternehmenseigenen Computer zum Surfen im Internet wird nur in den Fällen sinnvoll sein, in denen die Tätigkeit des einzelnen Mitarbeiters keinerlei Bezug zum Internet hat. In allen anderen Fällen sind Richtlinien erforderlich, nicht zuletzt zur Vermeidung von Kontaminierung des Unternehmens eigenen Datennetzes durch **malware.** Eine Gestattung der privaten Nutzung weicht den Schutz vor Schadenprogrammen grundsätzlich auf: Derartige Programme finden sich häufig auf Internetseiten, die deutlich dem privaten Bereich zuzuordnen sind wie solche mit sexualbezogenen Themen oder Glücksspielen. **136**

ee) Datenschutz. Wer Daten benutzt oder verwaltet unterliegt dem Bundesdatenschutzgesetz. Dort sind die verschiedenen formelle Vorgaben bereits implementiert, die im Rahmen einer IT-Compliance-Struktur zu beachten sind. Die Installation eines Datenschutzbeauftragten – letztlich ein Compliance Beauftragter mit Spezialaufgaben im IT-Bereich – ist beispielsweise ab zehn Mitarbeitern, die regelmäßig mit Daten umgehen, erforderlich. Die Aufgaben des Datenschutzbeauftragten sind vielfältig, sie lassen sich aus der Anlage zu § 9 S. 1 BDSG ableiten:[355] **137**

- Zutrittskontrolle – die Aufbewahrung wesentlicher Hardwarebestandteile geschützt vor dem Zugriff unbefugter Dritter
- Zugangskontrolle – Passwortschutz
- Zugriffskontrolle – hierarchisch gegliederte Zugriffsberechtigung
- Weitergabekontrolle – Überwachung der Export- und Importvorgänge der Datenverarbeitung
- Verfügbarkeitskontrolle – Sicherung und Erreichbarkeit aller Daten müssen gewährleistet sein
- Trennungsverbot – zu verschiedenen Zwecken erhobene Daten müssen physikalisch oder logisch getrennt voneinander verarbeitet werden
- Eingabekontrolle – revisionssichere Protokollierung nach dem Datenschutzgesetz und den Grundsätzen ordnungsgemäßer Buchführung
- Auftragskontrolle – auf Weisung Dritter zu verarbeitende Daten müssen strikt entsprechend der Weisung verarbeitet werden.

g) Gesundheitswesen. Compliance hat in der Pharmazeutischen und Medizintechnologischen Industrie eine vergleichsweise lange Tradition. Motor war u. a. der sog. Herzklappenskandal.[356] Obwohl die Zusammenarbeit mit Ärzten und Krankenhäusern im StGB, HWG, SGB V und den Berufsordnungen der Landesärztekammern reglementiert wird, besteht immer wieder Unsicherheit, wo genau die Grenze zwischen zulässiger und rechtswidriger Kooperation verläuft. Dieser für die Praxis missliche Umstand mag dazu beigetragen haben, dass beachtliche Selbstregulierungsmechanismen wie z. B. der FSA- und der AKG-Kodex installiert wurden, die inzwischen als Wettbewerbsregeln anerkannt sind. Von überragender Bedeutung sind die Prinzipien der Trennung, der Transparenz/Genehmigung, der Äquivalenz und der Dokumentation.[357] Sie finden sich in jedem guten Anti-Korruptionskonzept wieder. **138**

Auch wenn der Große Strafsenat inzwischen entschieden hat, dass niedergelassene Vertragsärzte bei der Verordnung von Arzneimitteln weder als Amtsträger noch als Beauftragte **139**

[355] Der Auswertung von Umnuß/*Rath/Hunecke* Corporate Compliance Checklisten, S. 213 f. folgend.
[356] Dieners/*Dieners,* Handbuch Compliance im Gesundheitswesen, 3. Aufl., Kap. 1 Rn. 1.
[357] Dieners/*Dieners,* Handbuch Compliance im Gesundheitswesen, 3. Aufl., Kap. 5.

der Krankenkassen tätig werden,[358] sind pharmazeutische Unternehmen gut beraten, die insbesondere im SGB V und den Berufsordnungen der Länder gezogenen Grenzen für Vorteilszuwendungen zu akzeptieren. Zum einen nimmt der politische Druck zu, einen speziellen Straftatbestand zu schaffen,[359] zum anderen hat der 5. Strafsenat erkennen lassen, dass er ärztliche Abrechnungen, die auf Schmiergeldzahlungen zurückzuführen sind, unter dem Blickwinkel der §§ 263, 266 StGB für überprüfenswert erachtet.[360]

Neben Strukturen, die auf die Verhinderung von Korruption im weiteren Sinne gerichtet sind, spielen solche eine wichtige Rolle, die kartellrechtliche Compliance gewährleisten sollen. Einige Unternehmen der pharmazeutischen Industrie sind bereits mit empfindlichen Geldbußen belegt worden, so dass sie ein großes Interesse daran haben, einschlägige Regelverstöße in Zukunft zu vermeiden.

Während ganzheitliche Compliance in einigen größeren Krankenhäusern bereits gelebt wird, scheint bei mittleren und kleineren Einrichtungen noch eine deutliche Skepsis vorzuherrschen, soweit es um den Mehrwert von Compliance geht. Es steht allerdings zu erwarten, dass sich dies in Anbetracht einer Reihe medial verstärkter Ermittlungsverfahren gegen nicht-ärztliche Verantwortliche in Kliniken ändern wird.

III. Compliance-Organisation

140 In den vorangehenden Abschnitten haben wir Art und Umfang der rechtlichen Risiken, auf deren Vermeidung Compliance abzielt, zunächst allgemein und sodann in Bezug auf verschiedene Bereiche und Branchen dargestellt. Wie eingangs jedoch bereits festgestellt wurde, ist dies nur eine Seite der Compliance-Medaille. Compliance bedeutet eben nicht nur Regelbefolgung, sondern – in der allerkürzesten Definition – *organisierte* Rechtstreue. Im Folgenden wollen wir uns mit dem organisatorischen Aspekt befassen.

1. Strukturelle Elemente

141 Um es gleich zu Anfang deutlich zu sagen: Allgemeinverbindliche Vorgaben, wie die Organisation von Compliance im Unternehmen auszusehen hat, lassen sich nicht aufstellen.[361] Dies folgt logisch schon daraus, dass es – von Bereichsausnahmen abgesehen – keine allgemeine Pflicht zur Schaffung einer Compliance-Organisation gibt.[362] Zu den Faktoren, welche das konkrete „Ob" und „Wie" der Compliance-Organisation beeinflussen, zählen u. a. Branche, Tätigkeitsgebiet, Auslandsbezug, Kapitalmarktorientierung, Kundenstruktur, Größe, Rechtsform, Organisation und Kultur des jeweiligen Unternehmens.[363] Für ein kleines Ingenieurbüro gilt nicht dasselbe wie für einen großen Baukonzern mit zahlreichen öffentlichen Auftraggebern.

142 Allzu häufig wird die Compliance-Diskussion mit Tunnelblick auf DAX-Konzerne geführt, während **kleine und mittelständische Unternehmen,** die in Deutschland noch immer die überwältigende Mehrheit stellen, entweder ausgeblendet oder mit aus der Welt der Global Player stammenden Konzepten überfordert werden. Erst in jüngster Zeit werden diese Defizite allmählich erkannt und speziell auf kleine und mittlere Unternehmen zugeschnittene Compliance-Lösungen vorgeschlagen.[364] Aus strafrechtlicher Sicht ist diese Entwicklung durchaus begrüßenswert, wird doch das Haftungsrisiko von Entscheidungsträgern in besagtem Bereich erfahrungsgemäß unterschätzt.

---

[358] Beschl. v. 29. 3. 2012, GSSt 2/11 – NJW 2012, 2530.
[359] Vgl. *Meseke* KrV 2012, 211 f.
[360] Beschl. v. 11. 10. 2012, 5 StR 115/11 – NStZ-RR 2011, 303. Zu diesem Themengebiet auch *Dann* GuP 2012, 201 ff. m. w. N.
[361] *Bock,* Criminal Compliance, S. 744; Hauschka/*Lampert* S. 166.
[362] → Rn. 30 ff.
[363] *Behringer,* Compliance kompakt, S. 384; Hauschka/*Hauschka* § 1 Rn. 33.
[364] Vgl. grundlegend *Behringer* (Hrsg.), Compliance für KMU, 2012; *Campos-Nave/Zeller* BB 2012, 132; *Fissenewert* (Hrsg.), Compliance für den Mittelstand, 2013.

a) **Abgrenzung zu anderen Kontrollfunktionen.** Teilweise wird behauptet, Compliance sei eigentlich „alter Wein in neuen Schläuchen".[365] Dahinter steht nicht in erster Linie Misstrauen gegenüber Compliance als Aufgabe für Unternehmen, sondern vor allem die Vorstellung, die Wahrnehmung dieser Aufgabe erfordere überhaupt keine neuartigen organisatorischen Anstrengungen. Das ist indessen falsch.[366] Zwar trifft es zu, dass verschiedene andere Stellen im Unternehmen einen Bezug zu und teilweise sogar Überlappungen mit der Compliance-Funktion aufweisen. Richtig ist auch, dass eine Verzahnung der Funktionen in vielen Fällen erstrebenswert ist. Gleichwohl unterscheidet sich die Compliance-Funktion klar von anderen Funktionen im Unternehmen. **143**

Zu denken ist diesbezüglich zunächst an die Rechtsabteilung, sofern eine solche unternehmensintern existiert. Häufig wird es die Rechtsabteilung sein, die gegenüber der Geschäftsleitung für den Aufbau eines Compliance-Systems eintritt, diesen in die Wege leitet und koordiniert.[367] Dadurch empfiehlt sie sich jedoch nicht automatisch selbst als Compliance-Stelle. Zwar bündelt die Rechtsabteilung ein hohes Maß an branchenspezifischem juristischem Fachwissen. Allerdings ist ihre Perspektive eine andere als im Rahmen der Compliance-Funktion maßgeblich. Die Rechtsabteilung prüft die Vereinbarkeit bestimmter Handlungsweisen mit den einschlägigen Bestimmungen im Regelfall bezogen auf einen konkreten Sachverhalt. Im Compliance-Bereich kommt es jedoch auf den **Blick über den Einzelfall hinaus** an. Gefordert ist eine umfassende Perspektive auf mögliche Risiken und deren Prävention. Hinzu kommen organisatorisches Know-how und Kenntnisse des Informationsmanagements und der Krisenkommunikation.[368] Wenn man ferner den Compliance-Begriff weit fasst und nicht auf die Einhaltung *gesetzlicher* Vorschriften begrenzt, wird man die Rechtsabteilung als nur beschränkt für die interdisziplinäre Aufgabe „Compliance" geeignet ansehen.[369] Trotzdem hat gut die Hälfte der in einer Studie untersuchten deutschen Großunternehmen die Compliance-Funktion der Rechtsabteilung angegliedert.[370] **144**

Ein weiterer Gutteil der deutschen Unternehmen ordnet die Compliance-Funktion der **internen Revision** zu.[371] Der Grund dafür liegt in den augenfälligen Überschneidungen beider Bereiche. Auch die Revision wacht schließlich über die Einhaltung bestimmter rechtlicher oder unternehmensinterner Vorgaben und ist mit der Aufklärung dolosen Handelns befasst.[372] Gerade bei der Sachverhaltsermittlung kann sie deshalb die Compliance-Funktion unterstützen.[373] Allerdings bestehen auch hier perspektivische Unterschiede. Die Revision agiert prozessunabhängig und eher retroaktiv, während Compliance proaktiv in die Prozesse integriert ist.[374] Zudem schließt der Prüfauftrag der Revision die Überprüfung des Compliance-Systems mit ein. Da sie diese Aufgabe nicht mehr unabhängig wahrnehmen könnte, müssten stets externe Prüfer bestellt werden.[375] **145**

Auch zur **Personalabteilung** besteht ein Bezug, aber keine funktionelle Deckungsgleichheit.[376] Zutreffend wird Criminal Compliance manchmal als strafbewehrte Personalverantwortung definiert.[377] Dies macht die Verbindung deutlich. Auch sind Aus- und Weiterbildung zentrale Aufgaben sowohl der Compliance-Funktion als auch der Personalstelle. Zudem wird diese engen Kontakt zum Betriebsrat unterhalten, der Ermittlungsmaßnahmen **146**

---

[365] Vgl. *Cauers/Haas/Jakob/Kremer/Schartmann* DB 2008, 2717.
[366] So auch *Behringer,* Compliance kompakt, S. 55.
[367] Hauschka/*Lampert* § 9 Rn. 9 und 11.
[368] *Behringer,* Compliance kompakt, S. 391.
[369] Vgl. Hauschka/*Hauschka/Spiekermann* § 15 Rn. 27.
370 Vgl. PwC/Martin-Luther-Universität Halle-Wittenberg, Compliance und Unternehmenskultur, 2010, S. 21 f.
[371] Vgl. PwC/Martin-Luther-Universität Halle-Wittenberg, Compliance und Unternehmenskultur, 2010, S. 21 f.
[372] Hauschka/*Bürkle* § 8 Rn. 54; *Cauers/Haas/Jakob/Kremer/Schartmann* DB 2008, 2717 (2718).
[373] Hauschka/*Pauthner-Seidel/Stephan* § 27 Rn. 43.
[374] Hauschka/*Bürkle* § 8 Rn. 55.
[375] *Bürkle* ebd; *Cauers/Haas/Jakob/Kremer/Schartmann* DB 2008, 2717 (2718).
[376] Hierzu ausführlich *Behringer,* Compliance kompakt, S. 389 f.
[377] Ähnlich etwa *Bock,* Criminal Compliance, S. 601.

im Unternehmen und erst recht Sanktionierungen von Verstößen meist zustimmen muss. Allerdings fehlt es der Personalabteilung meist an juristischer und finanzwissenschaftlicher Kompetenz. Deshalb wird die Übertragung der Compliance-Funktion an sie allenfalls in kleinen Unternehmen ohne eigene Rechtsabteilung in Betracht kommen.[378]

147 Aus unserer Sicht sprechen – jedenfalls bei größeren Unternehmen – gute Gründe dafür, eine *eigenständige* Organisationseinheit mit der Compliance-Funktion zu betrauen.[379] Diese sollte die folgenden grundlegenden Merkmale aufweisen:[380]

- ***Unabhängigkeit und Fachkompetenz:*** Für Compliance zuständige Unternehmensangehörige müssen weisungsunabhängig sowie fachkompetent sein und dürfen nicht dadurch in Interessenkonflikte gebracht werden, dass sie zugleich andere Aufgaben verrichten.
- ***Stabsstelle:*** Die Compliance-Funktion sollte unmittelbar der Geschäftsleitung unterstellt sein und durch mind. einen Mitarbeiter von hohem Rang überwacht werden.
- ***Integration:*** Die Compliance-Organisation sollte, auch um Redundanzen und unnötige Kosten zu vermeiden, mit anderen Kontrollsystemen des Unternehmens vernetzt und abgestimmt sein.

148 In der Regel wird es klug sein, einen **Compliance-Officer** (CO) zu bestellen, der als zentraler Ansprechpartner für Compliance-Fragen im Unternehmen fungiert und das diesbezügliche Wissen bündelt.[381] Gesetzlich vorgeschrieben ist dies zwar – unabhängig von ihrer Größe – nur für im Bereich des Wertpapierhandels tätige Unternehmen.[382] Aber auch für andere Unternehmen in anderen Branchen dürfte ab einer gewissen Größe oder Risikoexposition die Schaffung einer entsprechenden Position zum zumutbaren Mindeststandard zählen. In manchen Fällen ist schon allein wegen der Größe des Unternehmens die Schaffung einer Compliance-Abteilung mit mehreren Mitarbeitern kaum noch zu umgehen.[383] Deren Leiter wird üblicherweise als „Chief Compliance Officer" bezeichnet.

149 Die Abstimmung mit anderen Kontroll- und Überwachungsfunktionen im Unternehmen kann ein sog. **„Compliance Committee"** unterstützen.[384] Regelmäßig werden darin neben dem Compliance Officer Mitarbeiter des Risikomanagements, der Internen Revision, der Personal- und Rechtsabteilung sowie ggf. besondere Beauftragte (etwa für Umwelt oder Geldwäsche) sitzen. Durch die enge Abstimmung werden Redundanzen vermieden und die Reichweite der Compliance-Funktion im Unternehmen erheblich verbessert.

150 **b) Compliance als Leitungsaufgabe.** Dass die Unternehmensleitung selbst bislang nicht als potenzieller Träger der Compliance-Funktion in Betracht gezogen wurde, hat einen einfachen Grund: Es besteht weitgehende Einigkeit darin, dass sich die Rolle des Unternehmers bzw. der Unternehmensleitung und die des Compliance-Verantwortlichen nur schlecht vertragen.[385] Zu groß ist im Regelfall der Konflikt zwischen Umsatz- und Compliance-Verantwortung. Auch bleibt neben der Geschäftsleitung meist nicht hinreichend Zeit für die Wahrnehmung anderer Aufgaben.

151 Diese pragmatischen Erwägungen sollten aber nicht darüber hinwegtäuschen, dass es sich bei Compliance durchaus um eine **genuine Leitungsaufgabe** handelt.[386] Die Legalitätspflicht trifft nach dem Grundsatz der All- und Gesamtzuständigkeit primär die Leitungsorgane einer Gesellschaft.[387] Dasselbe gilt für die flankierenden Organisations- und Kontrollpflichten. Vorstand und Geschäftsführer haben für die Rechtstreue der Unternehmensangehörigen in angemessener Weise Sorge zu tragen. Dabei werden sie selbst **vom Aufsichtsrat überwacht**

[378] *Behringer,* Compliance für KMU, S. 242.
[379] Anders Görling/Inderst/Bannenberg/*Rieder/Falke* Compliance S. 25; zu anderen Organisationsmodellen Görling/Inderst/Bannenberg/*Inderst* Compliance S. 98 ff.
[380] Görling/Inderst/Bannenberg/*Beste* Compliance S. 139. S. auch unten IV. 1. a).
[381] Genauer → Rn. 223 ff.
[382] Vgl. § 33 Abs. 1 Satz 2 Nr. 5 WpHG; § 12 Abs. 4 WPDVerOV.
[383] *Bock,* Criminal Compliance, S. 744; Siemens soll 600 Mitarbeiter im Bereich Compliance haben.
[384] Dazu Görling/Inderst/Bannenberg/*Beste* Compliance S. 140 f.
[385] Ausführlich *Behringer,* Compliance für KMU, S. 238 ff.
[386] *Hüffer* AktG § 76 Rn. 8; Schneider ZIP 2003, Schneider ZIP 2003, 645 (647); Görling/Inderst/Bannenberg/*Rieder/Falge* Compliance S. 24.
[387] Hauschka/*Schmidt-Husson* Coroporate Compliance § 7 Rn. 2 f.

(vgl. § 111 Abs. 1 AktG).[388] Dieser hat nicht nur die Existenz eines Compliance-Systems zu prüfen, sondern auch eigenständig dessen Wirksamkeit zu beurteilen.[389]

c) Delegation. Aus den genannten Gründen wird die Compliance-Pflicht von den Leitungsorganen regelmäßig in Teilen delegiert. Dies ist grundsätzlich zulässig.[390] Ebenso wie die Geschäftsleitung nicht jede Aufgabe im Unternehmen selbst wahrnehmen muss, sondern ihre Mitarbeiter damit betrauen darf, kann sie – jedenfalls grundsätzlich – auch die Pflicht zur Überwachung der aus eben dieser Übertragung folgenden Risiken selbst delegieren. Trotz Delegation verbleibt die Kernverantwortung für Compliance jedoch bei der Geschäftsleitung, die sich auch durch eine Pflichtenübertragung nicht einfach für unzuständig erklären kann. **152**

Zu unterscheiden ist zwischen horizontaler, vertikaler und externer Delegation.[391] Mit **horizontaler Delegation** ist die Übertragung der Compliance-Pflicht auf einen von mehreren Geschäftsführern oder Vorständen qua Satzung oder Geschäftsordnungsplan gemeint. Abbedungen wird damit also der Grundsatz der Gesamtzuständigkeit. Die Zulässigkeit dieser Vorgehensweise ist unstrittig und ergibt sich – jedenfalls für die AG – bereits aus § 77 Abs. 1 S. 2 AktG.[392] **153**

Bei der **vertikalen Delegation** erfolgt die Übertragung der Pflicht nicht im Gleichordnungsverhältnis sondern an nachgeordnete Mitarbeiter wie Prokuristen oder besondere Beauftragte. Die Leitungsorgane weichen hier also vom Grundsatz der Allzuständigkeit ab. Auch dies ist unstreitig zulässig.[393] Die Bestellung eines Compliance Officers ist in der Regel ein Unterfall der vertikalen Delegation. **154**

Mit **externer Delegation** meint man das Outsourcing von Compliance-Funktionen an nicht dem Unternehmen zugehörige Dritte. Häufig wird es sich dabei um Rechtsanwälte handeln.[394] Die Bestellung eines externen Compliance Officers ist dabei ebenso möglich wie die Auslagerung bestimmter Einzelfunktionen.[395] Lediglich ein vollständiges Outsourcing des gesamten Compliance-Managements wird als unzulässig angesehen.[396] **155**

Delegation zur Entlastung und Haftungsbegrenzung der Geschäftsleitung ist durchaus sinnvoll und teilweise sogar geboten.[397] Allerdings sind diesem Vorgehen Grenzen gesetzt. Zwar sind die Grundsätze der All- und Gesamtzuständigkeit nicht zwingend. Auch durch die Übertragung von Pflichten können sich aber Geschäftsführer und Vorstände ihrer **Gesamt*verantwortung*** für deren ordnungsgemäße Erfüllung nicht entledigen.[398] Sie bleiben dafür stets gemeinsam verantwortlich und haften bei Pflichtverletzungen gesamtschuldnerisch.[399] Denn die Delegation an eine andere Stelle ist ihrerseits „eine Modalität der eigenen Pflichterfüllung".[400] **156**

Dies ist jedoch nicht gleichbedeutend mit einer verschuldensunabhängigen Einstandspflicht. Eine Zurechnung fremden Verschuldens findet ebenfalls nicht statt.[401] Strafrechtlich würde sie einen Verstoß gegen das Schuldprinzip darstellen und ist schon deshalb unzulässig. Aber auch eine zivilrechtliche Zurechnung über §§ 278 Abs. 1 oder 831 Abs. 1 BGB ist **157**

[388] Dazu *Kort* NZG 2008, 81 (84); zu den Strafbarkeitsrisiken des Aufsichtsrats vgl. *Wessing* in: Dehnen (Hrsg.), Der professionelle Aufsichtsrat, 2011, S. 19 ff.
[389] Dehnen/*Wessing,* Der professionelle Aufsichtsrat, 2011, S. 21.
[390] Ausführlich *Bock,* Criminal Compliance, S. 601 ff.
[391] Zum Ganzen Hauschka/*Schmidt-Husson* Coroporate Compliance § 7 Rn. 5 ff.
[392] Baumbach/Hueck/*Zöllner/Noack* AktG § 35 Rn. 33.
[393] Hauschka/*Schmidt-Husson* Coroporate Compliance § 7 Rn. 6; KK-AktG/*Mertens* § 93 Rn. 46.
[394] *Behringer,* Compliance für KMU, S. 246.
[395] Vgl. *Behringer,* Compliance für KMU, S. 245 f.; MünchKommAkt/*Spindler* § 76 Rn. 19 ff.
[396] Vgl. Hauschka/*Bürkle* Coroporate Compliance, § 8 Rn. 58.
[397] Hauschka/*Schmidt-Husson* Coroporate Compliance § 7 Rn. 6; zu den Grenzen zulässiger Delegation ebd. Rn. 13 ff.
[398] BGHZ 133, 370 (377 f.); BGH NJW 2002, 1585 (1587); 1990, 2560 (2564 f.); *Bock*, Criminal Compliance, S. 603.
[399] *Fleischer* Hdb.VorstR § 1 Rn. 53 f. und § 8 Rn. 5 ff.; Hauschka/*Schmidt-Husson* Coroporate Compliance § 7 Rn. 2.
[400] *Bock,* Criminal Compliance, S. 602.
[401] Hauschka/*Schmidt-Husson* Coroporate Compliance § 7 Rn. 9.

nicht möglich, denn derjenige, an den die Organpflicht delegiert wurde, ist weder Verrichtungs- noch Erfüllungsgehilfe des Organmitglieds.[402]

158 Dem Organmitglied kann folglich nicht vorgeworfen werden, dass derjenige, an welchen eine Aufgabe delegiert wurde, einen Regelverstoß begangen hat. Vielmehr muss stets ein **eigenes Verschulden des Delegierenden** festgestellt werden. Dieses kann darin bestehen, dass er den pflichtwidrig handelnden nicht richtig ausgewählt, eingewiesen oder überwacht hat. Die organschaftliche Gesamtverantwortung wird durch die Delegation nicht aufgehoben, sondern wandelt sich zu einer umfassenden Aufsichtspflicht. Mangelnde *diligentia in delegando* kann zu einer straf- und zivilrechtlichen Haftung des Delegaten führen.[403]

159 Wichtigster Ansatzpunkt für die Verteidigung gegen derartige Vorwürfe ist die Frage, welches Maß an Misstrauen vom aufsichtspflichtigen Delegaten verlangt werden kann.[404] Delegation soll anerkanntermaßen der Entlastung des Organmitglieds dienen. Eine Aufsichtspflicht, die bezüglich ihres Aufwandes kaum hinter der Erfüllung der delegierten Pflicht zurückbleibt, würde diesen Zweck konterkarieren. Der Delegat schuldet daher nur eine **angemessene Aufsicht, aber keine paranoide Totalüberwachung.** Daran muss der Verteidiger immer wieder erinnern. Die Rechtsprechung neigt ferner dazu, eine umso geringere Kontrolldichte zu verlangen, je weiter das Ressort des Delegaten vom dem entfernt ist, wo sich der Verstoß ereignet hat.[405] Die Verteidigung wird daher bemüht sein, die Sachnähe als möglichst gering darzustellen.

2. Implementierung der Compliance-Funktion

160 Jede Compliance-Organisation muss auf das konkrete Unternehmen und dessen spezifische Risikoexposition zugeschnitten sein. Geschuldet sind nur solche Maßnahmen, die möglich, erforderlich und zumutbar – kurz: **verhältnismäßig** – sind.[406] Was darunter im Einzelfall zu verstehen ist, lässt sich nicht immer leicht beantworten. Die Antizipation strafrechtlicher Verantwortung ist grundsätzlich mir tiefgreifenden praktischen, rechtlichen und psychologischen Schwierigkeiten verbunden.[407] Was der Richter sieht, nachdem es trotz aller Anstrengungen zu einem strafrechtlich relevanten Zwischenfall gekommen ist, unterscheidet sich mitunter erheblich von der Ex-ante-Perspektive des Beteiligten. Rechtsverbindliche Best-practice-Standards wie der *Australian Standard*,[408] die den Unternehmen Rechtssicherheit und Orientierung bieten, existieren in Deutschland bislang nicht.

161 Im Jahr 2010 hat allerdings der Hauptfachausschuss des Instituts der Wirtschaftsprüfer (IDW) den Entwurf eines Prüfungsstandards über die „Grundsätze ordnungsgemäßer Prüfung von Compliance-Management-Systemen" vorgelegt.[409] Damit sollten den Wirtschaftsprüfern einheitliche Leitlinien für die Beurteilung der Effizienz solcher Systeme an die Hand gegeben werden. Ein Jahr später wurde die überarbeitete Endfassung des Standards – der sog. IDW PS 980 – veröffentlicht.[410] Er behandelt Compliance aus einer umfassenden Perspektive – von der Zielsetzung über die Organisation bis hin zur Überprüfung und Verbesserung existierender Programme. Anwendbar ist der Standard auf Unternehmen sämtlicher Branchen mit Ausnahme der Finanzwirtschaft. Dieses Bemühen um Flexibilität und branchenübergreifende Relevanz führt unvermeidlich zu einer gewissen Vagheit der angewandten Kriterien, schafft aber andererseits ein **allgemein akzeptables Grundraster,** welches die Verunsicherung in der Wirtschaft mindern kann.

---

[402] Näher Hauschka/*Schmidt-Husson* Coroporate Compliance § 7 Rn. 9.
[403] Vgl. Hauschka/*Schmidt-Husson* Coroporate Compliance § 7 Rn. 10.
[404] Ausführlich dazu *Bock,* Criminal Compliance, S. 688 ff.
[405] VG Frankfurt a. M. VersR 2005, 57.
[406] Ausführlich zur Bestimmung der Compliance-Schuld *Bock,* Criminal Compliance, S. 459 ff., mwN aus der Rspr.
[407] Vgl. *Rotsch* ZIS 2010, 614 (616).
[408] Dazu → Rn. 27 f.
[409] Dazu ausführlich *Eisolt* BB 2010, 1843; *Gelhausen/Wermelt* CCZ 2010, 208.
[410] IDW PS 980 „Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen" (Stand: 11. 3. 2011) WPg Supplement 2/2011, S. 78 ff., FN-IDW 4/2011, S. 203 ff.