Münchener Anwaltshandbuch Verteidigung in Wirtschafts- und Steuerstrafsachen

3. Auflage 2020
ISBN 978-3-406-72936-2
C.H.BECK

über 12 Millionen Bücher, eBooks, Loseblattwerke, Zeitschriften, DVDs, Online-Datenbanken und Seminare. Besonders geschätzt wird beck-shop.de für sein umfassendes Spezialsortiment imBereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

- Die **Kenntnis** der Gefahrenquellen und der Verantwortung für diese,
- die **Überprüfung** der Sorgfaltsanforderungen und darauf basierend der Aufbau von Kontrollsystemen,[453]
- die **Information** des Produktanwenders über potentielle Gefahren aus dem Produkt, auch bei Fehlanwendungen[454] und
- die **Installation** von Handlungsroutinen für den Krisenfall, namentlich Rückrufaktionen[455] und Warnungen[456] an Verwender des Produktes.

Allgemein lässt sich sagen, dass die Anforderungen an ein Compliance-System umso hö- **164**
her sind, je größer das Gefahrenpotenzial eines Produktes ist. Die Beobachtung beschränkt sich nicht nur auf das eigene Produkt. Wenn dieses üblicherweise zusammen mit anderen Produkten angewendet wird, müssen auch die aus der Kombination mehrerer Produkte resultierenden Gefahren mit in das Kontrollsystem einbezogen werden.[457] Wie der „Diesel-Skandal" gezeigt hat, ist jenseits von Sicherheitsvorgaben generell auf die Einhaltung aller technischen Regeln zu achten, die für die die Zulassung oder Genehmigung eines Produkts relevant sind.

e) **Außenwirtschaftsrecht.**[458] Im Außenwirtschaftsrecht fanden sich schon früh Vorschrif- **165**
ten, die faktisch eine Compliance-Organisation erforderten. Die Fragen, **was** aus dem deutschen Wirtschaftsraum heraus **an wen** exportiert werden kann bzw. darf und **in welcher Form** dieser Export zu geschehen hat, ist in einer Vielzahl von Vorschriften und Verordnungen geregelt. Besonders zahlreiche und detaillierte Regelungen existieren dabei naturgemäß für den Export von Waffen und anderen Rüstungsgütern. Zur Beachtung dieser filigranen, zum Teil sehr kurzfristig wechselnden und zum größten Teil strafbewehrten Vorschriften muss Compliance Grundlage jedes Unternehmens mit dem Schwerpunkt Export oder Import sein. Hierbei sind nicht nur deutsche Rechtsvorschriften zu beachten, sondern es gilt gleichfalls europäisches Recht. In vielen Fällen muss auch ausländisches Recht wie zB das **US-Reexportkontrollrecht**[459] Beachtung finden.

Im deutschen Recht gilt primär das **Außenwirtschaftsgesetz** (AWG) in seiner Ergänzung **166**
durch die **Außenwirtschaftsverordnung** (AWV). Daneben gelten für bestimmte Bereiche Spezialgesetze wie zB das Kriegswaffenkontrollgesetz (KrWaffKontrG) nebst Durchführungsverordnungen, das Waffengesetz (WaffG) oder das Ausführungsgesetz zum Chemiewaffenübereinkommen (CWÜ). § 1 Abs. 1 S. 1 AWG normiert zwar, dass „der Güter-, Dienstleistungs-, Kapital-, Zahlungs- und sonstige Wirtschaftsverkehr mit dem Ausland sowie der Verkehr mit Auslandswerten und Gold zwischen Inländern (**Außenwirtschaftsverkehr**)" grundsätzlich frei ist. Von dieser Generalklausel darf man sich jedoch nicht täuschen lassen: Die **Regel ist die Reglementierung** (vgl. auch § 1 Abs. 1 S. 2 und Abs. 2 AWG). In Deutschland ist das **Bundesamt für Wirtschaft und Ausfuhrkontrolle** (BAFA) die für die Exportkontrolle zuständige Bundesbehörde. Bereits ein Blick auf die Homepage des Amtes[460] belegt, welch ein rechtliches Minenfeld voller Stolperdrähte sich im Außenwirtschaftsrecht auftut. Ohne Compliance wird ein Unternehmen auf diesem Feld schnell ins Straucheln geraten.

Trotz des damit einhergehenden Drucks in Richtung Compliance ist eine Rechtspflicht **167**
zum Aufbau einer Compliance-Organisation im Bereich des Außenwirtschaftsrechts nicht normiert.[461] Aus der Tatsache, dass § 8 Abs. 2 AWG die Zuverlässigkeit des Exporteurs für die Erteilung von Genehmigungen voraussetzt, ergibt sich jedoch eine **mittelbare Pflicht zur**

[453] Graf v. Westphalen/*Foerste* Produkthaftungshandbuch § 24 Rn. 290.
[454] BGH NJW 1999, 2815 – Papierreißwolf; MüKoBGB/*Wagner* § 823 Rn. 826.
[455] MüKoBGB/*Wagner* § 823 Rn. 848 ff.; Graf v. Westphalen/*Foerste* Produkthaftungshandbuch § 24 Rn. 258.
[456] MüKoBGB/*Wagner* § 823 Rn. 846 f.
[457] BGH NJW 1987, 1009 – Hondalenker.
[458] Ausführlich bei Hauschka/Moosmayer/Lösler/*Merz* § 32.
[459] Vgl. hierzu Umnuß/*Schlegel/Cammerer,* Corporate Compliance Checklisten, Kap. 4 Rn. 79, 26.
[460] https://www.bafa.de/DE/Aussenwirtschaft/aussenwirtschaft_node.html.
[461] Vgl. Merkblatt BAFA, Firmenexterne Exportkontrolle. Betriebliche Organisation im Außenwirtschaftsverkehr, S. 4.

Compliance. Denn Zuverlässigkeit heißt, die Einhaltung geltender Gesetze gewährleisten zu können. Insoweit enthält das Merkblatt der BAFA zur firmeninternen Exportkontrolle, welches im März 2018 in 2. Auflage erschienen ist, konkretisierte Compliance-Pflichten. Es widmet sich Compliance-Management-Programmen, die speziell dazu dienen, die Einhaltung der gesetzlichen Bestimmungen im Außenwirtschaftsverkehr zu unterstützen. Diese werden als Internal Compliance Programme (ICP) bezeichnet. Das Merkblatt soll Unternehmen dabei helfen, ein ICP aufzubauen bzw. ein bestehendes ICP weiter zu optimieren. Es zeigt auf, unter welchen Voraussetzungen die Unternehmensleitung ein ICP einrichten sollte. Außerdem benennt es Kriterien, die ein wirksames ICP ausmachen:[462]

1. Bekenntnis der Unternehmensleitung zu den Zielen der Exportkontrolle,
2. Risikoanalyse,
3. Aufbauorganisation/Verteilung von Zuständigkeiten,
4. Personelle und technische Mittel sowie sonstige Arbeitsmittel,
5. Ablauforganisation,
6. Führen von Aufzeichnungen und Aufbewahrung von Unterlagen,
7. Personalauswahl, Schulungen und Sensibilisierungen,
8. Prozessbezogene Kontrollen/Systembezogene Kontrollen (ICP-Audit)/Korrekturmaßnahmen/Hinweisgebersystem,
9. Physische und technische Sicherheit.

168 Auf europäischer Ebene regelt Art. 12 Abs. 2 der Verordnung (EG) Nr. 428/2009 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr von Gütern und Technologien mit doppeltem Verwendungszweck (**EG-Dual-Use-VO**), dass eine Einzel- oder gar eine globale Genehmigung zur Durchführung von bestimmten Exportgeschäften nur dann erteilt werden kann, wenn „der Ausführer angemessene und verhältnismäßige Mittel und Verfahren anwendet, um die Einhaltung der Bestimmungen und Ziele dieser Verordnung und der Genehmigungsauflagen zu gewährleisten". Damit setzt dieser Artikel faktisch ein Compliance-System voraus, auch wenn er nichts zu dessen Ausgestaltung sagt.

169 In aller Kürze sei auf die **rechtlichen Grundlagen** hingewiesen, an denen sich Compliance beweisen muss:[463]

- Das **AWG** definiert in seinem ersten Teil ua die verschiedenen Teilnehmer des Außenwirtschaftsrechts sowie deren Tätigkeiten. In seinem dritten Teil finden sich Strafvorschriften (§ 17 f. AWG), Bußgeldvorschriften (§ 19 AWG), eine Regelung zur Einziehung (§ 20 AWG) und Überwachungsvorschriften (vgl. § 23 ff. AWG). Das AWG ist in weiten Bereichen ein Blankettgesetz und verweist auf Rechtsverordnungen und Rechtsakte der europäischen Gemeinschaften bzw. der Europäischen Union.
- Die **AWV,** welche auf Basis von § 12 AWG erlassen wurde, enthält im Einzelnen formulierte Verbote sowie Genehmigungspflichten.
- Als Anlage 1 zur AWV enthält die **Ausfuhrliste** eine kategorisierte Aufzählung der von den Verboten und Genehmigungspflichten betroffenen Waren. Teil I der Liste enthält Waffen, Munition und Rüstungsmaterial (Abschnitt A) sowie national erfasste Dual-Use-Güter (Abschnitt B). Teil II der Liste enthält Waren pflanzlichen Ursprungs.
- Korrespondierend zur AWV existiert die **EG-Dual-Use-VO.**[464] Sie betrifft den Export all jener Waren und Güter, die ihrem potentiellen Verwendungszweck nach auch für kriegerische Zwecke verwandt werden können.
- Darüber hinaus gelten für bestimmte Bereiche (zB Kulturgüter, Folterinstrumente, Feuerwaffen, Rohdiamanten) weitere ausfuhrbeschränkende europäische Verordnungen.[465]
- Zu beachten sind ferner all jene Regelungen, die aufgrund von **Embargos** der Vereinten Nationen (UN) oder der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) erlassen werden.

[462] Vgl. Merkblatt BAFA, Firmenexterne Exportkontrolle. Betriebliche Organisation im Außenwirtschaftsverkehr, S. 12 ff.

[463] Anforderungen an ein außenwirtschaftliches Compliance-Programm beschreiben *Krebs/Sachs* CCZ 2013, 60 ff.

[464] Zur EG-Dual-Use-VO *Karpenstein* EuZW 2000, 677.

[465] Vgl. hierzu Umnuß/*Schlegel/Cammerer,* Corporate Compliance Checklisten, Kap. 4 Rn. 13.

- Alle Personen und Unternehmen, die mit Gütern handeln, welche ursprünglich aus dem Bereich der **Vereinigten Staaten** stammen, haben die in den Vereinigten Staaten für solche Fälle geltenden Regelungen – insbesondere die **Export Administration Regulations** (**EAR**) – zu beachten.[466]

f) Informationstechnologie (IT). In gleichem Maße und mit derselben Komplexität,[467] mit der sich elektronische Datenverarbeitung (EDV) in allen Bereichen des Wirtschaftslebens ausgebreitet hat, haben sich rechtliche Regelungen für diese „IT-Welt" entwickelt. In der Folge, werden Entwicklung, Pflege und Überwachung der EDV-Struktur eines Unternehmens von der Leitungsebene häufig so weit weg delegiert, dass es auf der Organebene an Verständnis und Kontrolle mangelt.[468] Letzteres wird dadurch verstärkt, dass IT nicht nur reine Datenverarbeitungsthemen berührt, sondern mit anderen Bereichen (zB dem Steuerrecht) eng vernetzt ist. Eine unzureichende IT-Compliance kann aber in gleicher Weise **Haftungen nach §§ 93, 116 AktG und § 43 GmbHG** auslösen, wie jede andere Missachtung von Organisationsaufgaben. Zudem trifft die Obliegenheit zum Schutz von Daten Unternehmen neuerdings auch im Hinblick auf ihre **Geschäftsgeheimnisse,** vgl. § 2 Nr. 1b Geschäftsgeheimnisgesetz (GeschGehG). Nur wenn das Unternehmen „angemessene Geheimhaltungsmaßnahmen" ergreift, stehen ihm im Falle der Verletzung seiner Geheimnisse die zivilrechtlichen Ansprüche der §§ 6 ff. GeschGehG zur Seite.[469] Widmete die Führungsebene mancher Unternehmen ein Bruchteil der Zeit, welche sie auf Bilanzfragen verwendet, der IT, so würden deutlich weniger Probleme im Bereich der EDV ent- und fortbestehen – und damit auch einige Bilanzprobleme vermieden. **170**

Auch **straf- und ordnungswidrigkeitenrechtlich** birgt das Gebiet der EDV eine Menge an Stolperfallen. Diese bestehen nicht nur im Bereich des Bundesdatenschutzgesetzes (BDSG) und der Datenschutzgrundverordnung (EU) 2016/679 (DS-GVO) sondern auch durch die EDV-spezifischen Normen des Strafgesetzbuches wie § 202a (Ausspähen von Daten), § 202b (Abfangen von Daten), § 202c (Vorbereiten des Ausspähens und Abfangens von Daten), § 202d (Datenhehlerei), § 263a (Computerbetrug), § 303a (Datenveränderung) oder § 303b (Computersabotage). Ferner spielt die Geheimhaltung von Daten auch im Rahmen der Strafvorschriften des § 23 GeschGehG eine entscheidende Rolle. Die wesentlichen Aspekte im Bereich der IT-Compliance sind: **171**

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, Schutzmechanismen für seine Daten einzurichten, wird ihm zum Teil auch der gesetzliche Schutz versagt. So gehört es bereits zum Tatbestand der §§ 202a ff. StGB, dass die in Rede stehenden Daten gegen unberechtigten Zugang besonders gesichert sein müssen. Auch liegt ein Geschäftsgeheimnis iSd GeschGehG gemäß dessen § 2 Nr. 1b nur vor, wenn die relevante Information Gegenstand von „angemessenen Geheimhaltungsmaßnahmen" ist. In Bezug auf die zu ergreifenden Compliance-Maßnahmen gilt es für bestimmte Unternehmen spezieller Sektoren (Energie, Informationstechnik, Telekommunikation, Transport, Verkehr, Gesundheit, Wasser, Ernährung sowie das Finanz und Versicherungswesen) die Vorgaben des IT-Sicherheitsgesetzes vom 15. Juli 2015 zu beachten.[470] Unternehmen können ein eingerichtetes Information Security Management System (ISMS) vom Bundesamt für Sicherheit und Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz zertifizieren lassen.[471] Die wesentlichen Anforderungen an ein derartiges Schutzkonzept sind: **172**

[466] Zum US-Außenwirtschaftsrecht siehe *Krebs/Sachs* CCZ 2013, 60 (63), Umnuß/*Schlegel/Cammerer,* Corporate Compliance Checklisten, Kap. 4 Rn. 78 ff.

[467] Weltweit soll es ca. 25.000 Compliance-Anforderungen im IT-Bereich geben, vgl. Wecker/Ohl/*Rath,* Compliance in der Unternehmerpraxis, S. 131 mit einzelnen Nachweisen.

[468] Zur Organverantwortung: Wecker/Ohl/*Bauer,* Compliance in der Unternehmerpraxis, S. 149 ff. mwN.

[469] Vgl. hierzu ausführlich *Dann/Markgraf* NJW 2019, 1774 ff.

[470] Vgl. hierzu ausführlich Umnuß/*Rath/Kuß,* Corporate Compliance Checklisten, Kap. 8 Rn. 6 ff.

[471] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Zertifizierungsschema.pdf?__blob=publicationFile&v=4.

- Die Existenz eines allgemeinen **Sicherheitskonzeptes.** Dazu gehört neben der Festlegung, welcher Mitarbeiter auf welcher Ebene auf Daten zugreifen bzw. in die Datenverarbeitung eingreifen kann auch die Verwaltung von Programmrechten.
- **Verhaltensanweisungen für EDV-Notfälle** wie zB einen Angriff auf die Homepage mittels einer denial of service Attacke.
- Eine **Datensicherungsstrategie** mit einem garantierten und kompletten täglichen Sicherungslauf und Verbringung der Daten an eine sichere Auslagerungsstelle.
- Die Vorbereitung für den Fall eines technisch bedingten **Systemabsturzes** einschließlich der Wiederherstellung der Funktionsfähigkeit des Systems.
- Die **Verhinderung** der Einbringung von Fremdprogrammen und externen Daten ohne Kontrolle auf deren Integrität und Sicherheit.

173 *bb) Archivierung.* Nicht nur aktuelle Daten sind zu schützen, auch historische Daten sind entsprechend der gesetzlichen Anforderungen zu verwalten. Sowohl das Handelsrecht (§ 257 HGB) als auch das Steuerrecht (§ 147 AO)[472] konstituieren **Aufbewahrungspflichten.** Im Bereich der Daten heißt dies, dass sie in **lesbarer Form** vorgehalten werden müssen (vgl. §§ 239 Abs. 4 S. 2, 257 Abs. 3 S. 1 HGB, 147 Abs. 2 AO). Dies setzt voraus, dass auch veraltete Datenverarbeitungssysteme zumindest noch potenziell aktiv gehalten und Passwörter für Systemzugriffe oder verschlüsselte E-Mails aufbewahrt werden.

174 Da eine pflichtgemäße Archivierung neben der Speicherung und Sicherung der Daten auch deren Verfügbarkeit fordert, sollten Systeme zum Wiederauffinden konkreter Informationen eingerichtet werden, zB Datenbanken in sog. Dokumentenmanagement (DMS)-Systemen. Diese Systeme sind sowohl in ihrer Einrichtung als auch in ihrer Handhabung recht komplex und mit den üblichen an Bürosoftware ausgerichteten Kenntnissen von Unternehmensmitarbeitern nicht ohne weiteres zu bedienen. Daher bedarf es in diesem Bereich besonderer Schulung, um die Verfügbarkeit der Daten nicht nur theoretisch, sondern auch **praktisch zu gewährleisten.**

175 *cc) E-Mails und Internet.* Der Einsatz von E-Mails hat in weiten Bereichen das Schreiben konventioneller Briefe ersetzt, das Internet als Informationsmedium ist aus der Unternehmenspraxis nicht mehr wegzudenken. 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, **die private Nutzung aller Informationssysteme in jeder Form zu untersagen.** Die ansonsten entstehende Gemengelage zwischen privaten und geschäftlichen Daten führt zu großen Schwierigkeiten. Denn in diesem Fall treffen den Arbeitgeber – je nachdem welcher Meinung man folgt – die für Telekommunikationsdienstanbieter (§ 3 Nr. 6 TKG) und Telemedienanbieter (§ 2 Nr. 1 TMG) speziellen datenschutz- und telekommunikationsrechtlichen Regelungen zum Schutz des **Fernmeldegeheimnisses** (§§ 88 TKG, 7 Abs. 3 S. 2 TMG).[473] Den Mitarbeitern sollte daher zur privaten Internetnutzung und E-Mail Korrespondenz ein separates, vom Unternehmensnetzwerk getrenntes Terminal zur Verfügung gestellt werden. Dies befreit auch von der Prüfung der Frage, ob nicht trotz eines Verbots der privaten Nutzung eine entsprechende betriebliche Übung und damit eine konkludente Duldung vorliegen. Beseitigt werden hiermit gleichzeitig strafrechtliche Risiken: Grundsätzlich unterliegen private Mitteilungen in Form von E-Mails dem Fernmeldegeheimnis, sodass in der Kenntnisnahme eine Verletzung von § 206 StGB liegen kann. Wird dabei noch ein Passwortschutz überwunden, steht § 202a StGB in Rede.[474] Zudem kennt das Telekommunika-

[472] Siehe dazu die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) des Bundesfinanzministeriums vom 14.11.2014, welches nach deren Maßgabe auf alle digitalen und steuerrelevanten Daten des Unternehmens zugreifen kann. Abrufbar unter https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/2014-11-14-GoBD.pdf?__blob=publicationFile.

[473] Überblick zum Streitstand u. a. bei *Brink/Schwab* ArbRAktuell 2018, 111; Schönke/Schröder/*Eisele* § 206 Rn. 8a; *Wybitul* NJW 2014, 3605 (3607 ff.).

[474] Ausführlich hierzu MüKoStGB/*Graf* § 202a Rn. 25 f.

tionsgesetz in den §§ 148 und 149 TKG einen langen Katalog von Straftatbeständen und Ordnungswidrigkeiten.

Eine **IT-Richtlinie,** die auch den Umgang mit E-Mails durch die Mitarbeiter eindeutig regelt, sowie deren Überwachung gehören mithin zum Grundkonzept von IT-Compliance. Wesentliche Strukturen einer solchen Richtlinie sind nicht nur Verbote, sondern auch Handlungsanweisungen zum Umgang mit Dateien, wie zB der Ablage in bestimmten, im Unternehmen generalisierten und einheitlichen Verzeichnissen. 176

Für die private Nutzung von Zugängen zum Internet gilt grundsätzlich dasselbe wie für E-Mails: Eine klare und eindeutige Regelung ist erforderlich. Eine generelle Untersagung der Nutzung der unternehmenseigenen Computer zum Surfen im Internet wird nur dann sinnvoll sein, wenn die Tätigkeit des einzelnen Mitarbeiters keinerlei Bezug zum Internet hat. In allen anderen Fällen sind Richtlinien erforderlich, nicht zuletzt zur Vermeidung von Kontaminierung des unternehmenseigenen Datennetzes durch **Malware.** Eine Gestattung der privaten Nutzung weicht den Schutz vor Schadprogrammen grundsätzlich auf: Derartige Programme finden sich häufig auf Internetseiten, die deutlich dem privaten Bereich zuzuordnen sind (zB sexualbezogene Themen oder Glücksspiele). 177

ee) Lizenzen. Zu einem wirksamen IT-Compliance-System gehört ferner die Sicherstellung eines rechtskonformen Umgangs mit Lizenzen. Es muss laufend überprüft werden, ob das Unternehmen in Bezug auf jedwede im Unternehmen verwendete Software die notwendigen Nutzungsrechte besitzt. Ein effektives Lizenzmanagement ist insbesondere deshalb notwendig, weil die Folgen eines Lizenzverstoßes für ein Unternehmen vergleichbar schwerwiegend sein können wie bei einem Ausfall der Informationstechnik. So stehen dem Lizenzgeber bei Lizenzverstößen umfassende Rechte, wie Unterlassungsansprüche und Schadenersatzansprüche, zu.[475] 178

ff) Datenschutz. Wer personenbezogene Daten (Art. 4 Nr. 1 DS-GVO) verarbeitet (Art. 4 Nr. 2 DS-GVO), unterliegt der DS-GVO und dem BDSG. Letzteres ergänzt und konkretisiert die unmittelbar geltende DS-GVO (vgl. § 1 Abs. 5 BDSG). Die verschiedenen formellen Vorgaben, die im Rahmen einer IT-Compliance-Struktur zu beachten sind, können diesen Regelwerken entnommen werden. Beispielsweise ist die Installation eines **Datenschutzbeauftragten** – letztlich ein Compliance-Beauftragter mit Spezialaufgaben im IT-Bereich – ab zehn Mitarbeitern, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, erforderlich (§ 38 BDSG Abs. 1 S. 1 iVm Art. 37 Abs. 4 S. 1 aE DS-GVO). Die Aufgaben des Datenschutzbeauftragten sind vielfältig und ergeben sich ua aus Art. 39 DS-GVO. Danach obliegen dem Datenschutzbeauftragten **zumindest** folgende Aufgaben: 179

- Unterrichtung und Beratung der Unternehmensleitung und der Mitarbeiter, die Daten verarbeiten, hinsichtlich ihrer Pflichten nach der DS-GVO sowie nach sonstigen Datenschutzvorschriften (insb. BDSG);
- Überwachung der Einhaltung der Vorschriften der DS-GVO, anderer Datenschutzvorschriften (insb. BDSG) sowie der unternehmensinternen Richtlinien zum Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und diesbezüglicher Überprüfungen;
- Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35 DS-GVO;
- Zusammenarbeit mit den Datenschutzbeauftragten des Bundes und der Länder als Aufsichtsbehörde iSd Art. 51 DS-GVO;
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Art. 36 DS-GVO, und ggf. Beratung zu allen sonstigen Fragen.

Im Übrigen enthält das BDSG in seinem § 64 einen umfassenden Katalog mit Anforderungen an die Sicherheit der Datenverarbeitung, die es seitens der Unternehmensleitung zu ge-

[475] Ausführlich hierzu Umnuß/*Rath/Kuß,* Corporate Compliance Checklisten, Kap. 8 Rn. 15 ff.

währleisten gilt. Verstöße gegen datenschutzrechtliche Vorgaben sind straf- bzw. bußgeldbewährt (vgl. §§ 42 und 43 BDSG und Art. 83 und 84 DS-GVO).

180 **g) Gesundheitswesen.** Compliance hat in der pharmazeutischen und medizintechnologischen Industrie eine vergleichsweise lange Tradition. Diese hat ihren Ursprung im sog. **Herzklappen-Skandal,** der ab dem Jahr 1994 zu Ermittlungsverfahren ua gegen leitende Ärzte fast aller deutschen Herzkliniken geführt hat. Ihnen wurde vorgeworfen, von Herstellern künstlicher Herzklappen Vorteile und Drittmittel angenommen zu haben. Im Gegenzug bezogen die Ärzte deren Herzklappen zu überteuerten Preisen und rechneten diese zulasten der Krankenkassen ab.[476] Die Kooperation zwischen Arzneimittel-/Medizinprodukteherstellern und Ärzten bzw. Krankenhäusern wird zwar durch das StGB, das Heilmittelwerbegesetz (HWG), das SGB V und die Berufsordnungen der Landesärztekammern reglementiert. Dennoch – oder gerade deshalb – besteht immer wieder Unsicherheit, wo genau die Grenze zwischen zulässiger und rechtswidriger Kooperation verläuft.

181 Diese Unsicherheit wurde mit der Einführung der **§ 299a StGB** (Bestechlichkeit im Gesundheitswesen) und **§ 299b StGB** (Bestechung im Gesundheitswesen) durch das Gesetz zur Bekämpfung von Korruption im Gesundheitswesen vom 30.5.2016 noch verschärft.[477] Dem ging eine Entscheidung des Großen Strafsenats voraus, wonach niedergelassene Vertragsärzte bei der Verordnung von Arzneimitteln weder als Amtsträger noch als Beauftragte der Krankenkassen tätig werden.[478] Korrupte Verhaltensweisen waren daher weder von den §§ 331 ff. noch von § 299 StGB erfasst. Ärztliche Abrechnungen, die auf Schmiergeldzahlungen zurückzuführen sind, bargen daher lediglich die – nach wie vor bestehende – Gefahr einer Strafbarkeit nach **§§ 263, 266 StGB**.[479] Da der Gesetzgeber die vermögensstrafrechtliche Sanktionierung nicht als ausreichend erachtete, sah er sich zur Schaffung der §§ 299a, 299b StGB veranlasst.[480]

182 **Pharmazeutische Unternehmen** sind insb. vor dem Hintergrund des § 299b StGB gut beraten, die vor allem im SGB V und den Berufsordnungen der Länder gezogenen Grenzen für Vorteilszuwendungen zu akzeptieren. Außerdem sollten Selbstregulierungsmechanismen wie zB die Kodizes des „Freiwillige Selbstkontrolle für die Arzneimittelindustrie e. V." und der Verhaltenskodex des „Arzneimittel und Kooperation im Gesundheitswesen e. V." berücksichtigt werden. Im Allgemeinen sind, um dem Vorwurf der Korruption im Rahmen einer Kooperation entgegenzuwirken, die Prinzipien der **Trennung,** der **Transparenz/**Genehmigung, der **Äquivalenz** und der **Dokumentation** von überragender Bedeutung.[481]

183 Neben der Verhinderung von Korruption, müssen Unternehmen im Gesundheitswesen bei der Etablierung einer Compliance-Organisation insbesondere steuerrechtliche[482] und kartellrechtliche[483] aber auch produkthaftungsrechtliche und datenschutzrechtliche Risiken im Blick haben. Während ganzheitliche Compliance in einigen größeren Krankenhäusern bereits gelebt wird,[484] 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

184 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

[476] Hierzu Dieners/*Dieners,* Handbuch Compliance im Gesundheitswesen, 3. Aufl., Kap. 1 Rn. 5 mwN.
[477] Überblick über die §§ 299a, 299b bei *Dann/Scholz* NJW 2016, 2077 ff.
[478] BGH NJW 2012, 2530.
[479] BGH NStZ-RR 2017, 313 f. Zu diesem Themengebiet auch *Dann* GuP 2012, 201 ff. mwN.
[480] BT-Drs. 18/6446, S. 11 f.
[481] Ausführlich hierzu Dieners/*Dieners,* Handbuch Compliance im Gesundheitswesen, Kap. 5.
[482] Ausführlich hierzu Dieners/*Lembeck,* Handbuch Compliance im Gesundheitswesen, Kap. 8.
[483] Ausführlich hierzu Dieners/*Besen,* Handbuch Compliance im Gesundheitswesen, Kap. 9.
[484] Vgl. hierzu ausführlich Wenzel/*Dann,* Handbuch des Fachanwalts Medizinrecht, Kap. 16.

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 daher mit den organisatorischen Dimensionen befassen.

1. Strukturelle Elemente

Um es gleich zu Anfang deutlich zu sagen: **Allgemeinverbindliche Vorgaben,** wie die Organisation von Compliance im Unternehmen auszusehen hat, **lassen sich nicht aufstellen.**[485] Zu den Faktoren, welche das konkrete „Ob" und „Wie" der Compliance-Organisation beeinflussen, zählen ua Branche, Tätigkeitsgebiet, Auslandsbezug, Kapitalmarktorientierung, Kundenstruktur, Größe, Rechtsform, Organisation und Kultur des jeweiligen Unternehmens.[486] Beispielsweise gilt für ein kleines Ingenieurbüro nicht dasselbe wie für einen großen Baukonzern mit zahlreichen öffentlichen Auftraggebern. 185

Allzu häufig ist die Compliance-Diskussion mit Tunnelblick auf DAX-Konzerne geführt worden, 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 wurden. In den letzten Jahren sind diese Defizite jedoch allmählich erkannt und speziell auf kleine und mittlere Unternehmen zugeschnittene Compliance-Lösungen vorgeschlagen worden.[487] In diesem Zusammenhang ist der internationale Standard **ISO 19600** zu nennen,[488] der aufgrund seiner Flexibilität auch für kleinere Unternehmen als Leitfaden bei der Etablierung eines Compliance-Systems dienen kann.[489] Hilfestellung kann ferner der Prüfstandard des Instituts der deutschen Wirtschaftsprüfer betreffend die „Grundsätze ordnungsgemäßer Prüfung von Compliance Management Systemen" (**IDW PS 980**) leisten.[490] Aus strafrechtlicher Sicht ist diese Entwicklung durchaus begrüßenswert, wird doch das Haftungsrisiko von Entscheidungsträgern in kleinen und mittelständischen Unternehmen erfahrungsgemäß unterschätzt. 186

a) Abgrenzung zu anderen Kontrollfunktionen. Teilweise wird behauptet, Compliance sei eigentlich „alter Wein in neuen Schläuchen".[491] 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.[492] 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. 187

Zunächst ist an die **Rechtsabteilung** zu denken, sofern eine solche unternehmensintern existiert. Häufig wird es diese Abteilung sein, die gegenüber der Geschäftsleitung für den Aufbau eines Compliance-Systems eintritt, diesen in die Wege leitet und koordiniert. Dadurch empfiehlt sie sich jedoch nicht automatisch selbst als Compliance-Abteilung. Zwar bündelt die Rechtsabteilung ein hohes Maß an branchenspezifischem, juristischem Fachwissen. Allerdings ist ihre Perspektive eine andere als die im Rahmen der Compliance-Funktion maßgebliche. Die Rechtsabteilung wurde jedenfalls in der Vergangenheit nur reaktiv tätig und hat Schäden begrenzt, wenn der Schadensfall bereits eingetreten war. Sie prüft daher traditionell die Vereinbarkeit bestimmter Handlungsweisen mit den einschlägigen Bestimmungen bezogen auf einen konkreten Sachverhalt. Im Compliance-Bereich kommt es jedoch auf den in die Zukunft gerichteten Blick über den Einzelfall hinaus 188

[485] *Bock,* Criminal Compliance, S. 744; Hauschka/Moosmayer/Lösler/*Hauschka* § 1 Rn. 31.
[486] *Vgl. Behringer,* Compliance kompakt, S. 380; Hauschka/Moosmayer/Lösler/*Hauschka* § 1 Rn. 31.
[487] Vgl. grundlegend *Behringer (Hrsg.),* Compliance für KMU; zum Mittelstand *Fissenewert* NZG 2015, 1009 ff.; zu Start-Ups *Nothhelfer/Bacher* CCZ 2016, 64 ff.
[488] → Rn. 34.
[489] *Fissenewert* NZG 2015, 1009 (1010 ff.).
[490] Näher hierzu → Rn. 205 f.; *Nothhelfer/Bacher* CCZ 2016, 64 (66 f.).
[491] Vgl. *Cauers/Haas/Jakob/Kremer/Schartmann/Welp* DB 2008, 2717.
[492] Vgl. auch *Behringer,* Compliance kompakt, S. 43 ff.

an. Gefordert ist eine umfassende Perspektive auf mögliche Risiken und deren Prävention.[493] Hinzu kommen organisatorisches Know-how und Kenntnisse des Informationsmanagements und der Krisenkommunikation.[494] Wenn man ferner den Compliance-Begriff weit fasst und nicht auf die Einhaltung *gesetzlicher* Vorschriften begrenzt,[495] wird man die Rechtsabteilung als nur beschränkt für die interdisziplinäre Aufgabe „Compliance" geeignet ansehen.[496] Trotzdem geht eine Mehrzahl der Verantwortlichen in Unternehmen (63 %) davon aus, dass die Aufgaben der Compliance-Funktion am besten bei der Rechtsabteilung verortet sind.[497]

189 In Betracht zu ziehen ist ferner eine Zuordnung der Compliance-Funktion zur **Internen Revision.** 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.[498] Gerade bei der Sachverhaltsermittlung kann sie deshalb die Compliance-Funktion unterstützen.[499] Allerdings bestehen auch hier perspektivische Unterschiede. Die Revision agiert prozessunabhängig und eher retroaktiv, während Compliance proaktiv in die Prozesse integriert ist.[500] Zudem schließt der Prüfauftrag der Revision die Überprüfung des Compliance-Systems mit ein. Da sie diese Aufgabe nicht mehr unabhängig wahrnehmen könnte, müssten für deren Erfüllung externe Prüfer bestellt werden.[501] Da dies jedoch ohne Zweifel machbar ist, handelt es sich hierbei nicht um ein Totschlagargument.

190 Auch zur **Personalabteilung** besteht ein Bezug, aber keine funktionelle Deckungsgleichheit.[502] Zutreffend wird Criminal Compliance manchmal als strafbewehrte Personalverantwortung definiert.[503] Dies macht die Verbindung deutlich. Auch sind Aus- und Weiterbildung zentrale Aufgaben sowohl der Compliance-Funktion als auch der Personalabteilung. Zudem wird letztere engen Kontakt zum Betriebsrat unterhalten, der unternehmensinternen Untersuchungen 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.[504]

191 Aus unserer Sicht sprechen – jedenfalls bei größeren Unternehmen – gute Gründe dafür, eine **eigenständige Organisationseinheit** mit der Compliance-Funktion zu betrauen.[505] Diese sollte die folgenden grundlegenden Merkmale aufweisen:

- ***Unabhängigkeit und Fachkompetenz:*** Für Compliance zuständige Unternehmensangehörige müssen inhaltlich weisungsunabhängig sowie fachkompetent sein und dürfen nicht dadurch in Interessenkonflikte gebracht werden, dass sie zugleich andere Aufgaben verrichten.
- ***Stabsstelle:*** Da es sich bei Compliance um eine Leitungsaufgabe handelt, sollte die Compliance-Funktion unmittelbar der Geschäftsleitung unterstellt sein und durch mindestens einen Verantwortlichen von hohem Rang überwacht werden.[506]

---

[493] Vgl. *Wiedmann/Greubel* CCZ 2019, 88 (90) mwN.
[494] *Behringer,* Compliance kompakt, S. 384 ff.
[495] Hierzu → Rn. 4.
[496] Vgl. Hauschka/Moosmayer/Lösler/*Spiekermann* § 38 Rn. 28 f.
[497] Vgl. *PwC/Martin-Luther-Universität Halle-Wittenberg,* Wirtschaftskriminalität und Unternehmenskultur, 2013, S. 31.
[498] Hauschka/Moosmayer/Lösler/*Bürkle* § 36 Rn. 71; *Cauers/Haas/Jakob/Kremer/Schartmann/Welp* DB 2008, 2717 (2718).
[499] Hauschka/Moosmayer/Lösler/*Pauthner/Stephan* § 16 Rn. 63 f.; Hauschka/Moosmayer/Lösler/*Bürkle,* Corporate Compliance, § 36 Rn. 72.
[500] Hauschka/Moosmayer/Lösler/*Bürkle* § 36 Rn. 73.
[501] Hauschka/Moosmayer/Lösler/*Bürkle* § 36 Rn. 73; *Cauers/Haas/Jakob/Kremer/Schartmann/Welp* DB 2008, 2717 (2718).
[502] Hierzu ausführlich *Behringer,* Compliance kompakt, S. 384 ff.
[503] Ähnlich etwa *Bock,* Criminal Compliance, S. 601.
[504] *Behringer,* Compliance für KMU, S. 242.
[505] So auch *Wiedmann/Greubel* CCZ 2019, 88 (90). Zu anderen Organisationsmodellen insb. der „Matrixorganisation" Inderst/Bannenberg/Poppe/*Hülsberg/Laue,* Compliance, Kap. 3 Rn. 182 ff.
[506] Genauer → Rn. 194 ff.