Strafbarkeitsrisiken des Unternehmers

Mansdörfer / Habetha

2. Auflage 2026
ISBN 978-3-406-73754-1
C.H.BECK

– von der Größe des Betriebes,
– der Anzahl der Beschäftigten,
– deren Sachkunde und Sorgfalt,
– der innerbetrieblichen Organisation,
– den realen Überwachungsmöglichkeiten sowie
– der Bedeutung der einzuhaltenden Vorschriften ab.[574]

Unterschiedliche Bedeutung misst der Gesetzgeber Vorschriften im Allgemeinen dadurch zu, dass er deren Durchsetzung entweder (allein) mit Mitteln des Verwaltungs(vollstreckungs)rechts, des Ordnungswidrigkeitenrechts oder sogar des Strafrechts sicherzustellen versucht.

b) Compliancesysteme bei Unternehmen mit Tochtergesellschaften, Holding- und Konzernstrukturen

Organisatorische Widrigkeiten bestehen bei Unternehmen mit verschiedenen Tochtergesellschaften oder Holding- und Konzernstrukturen. Das Compliance System muss hier so ausgestaltet sein, dass ein Informationsfluss aus allen Unternehmensteilen gewährleistet ist und umgekehrt eine Einflussnahme auf alle Teile des Unternehmens möglich ist. **464**

Ein rechtliches Hindernis ist grundsätzlich die gesellschaftsrechtliche Selbstständigkeit von Tochtergesellschaften in Form von GmbHs oder AGs. Hier muss die Wirksamkeit des Compliancesystems durch entsprechende Verträge zwischen den einzelnen Gesellschaften sichergestellt werden. Auf der Basis solcher Verträge können die Gemeinkosten für das Compliancesystem auf verschiedenen Gesellschaften übertragen werden. Bei der Weitergabe von Informationen zwischen den Unternehmen müssen zudem die datenschutzrechtlichen Vorgaben der DSGVO eingehalten werden.

Praxishinweis (Complianceausschuss als zentrales Organisationselement):

In Großkonzernen werden häufig für einzelne Sparten und Länder eigene Compliancesysteme eingerichtet und in einer Matrixorganisation zusammengefügt. Für mittelständische Unternehmen ist eine solche Organisation zu aufwendig. Stattdessen bietet es sich an, dem Complianceofficer einen die einzelnen Gesellschaften übergreifenden Complianceausschuss bzw. ein sog. Complianceboard zur Seite zu stellen.[575] Dieser Complianceausschuss kann dann in zu verschiedenen Themen unterschiedlicher und jeweils angepasster Zusammensetzung einberufen werden. Das Thema kann im Complianceausschuss auch durch externe Kompetenzen bereichert werden und so zum zentralen Kommunikationsorgan innerhalb der wirtschaftlichen Einheit „Unternehmen" werden.

c) Erhöhte Anforderungen bei konkreten Gefährdungen und nahe liegenden Exzesstaten

Gesteigerte Anforderungen haben Unternehmen und ihre Leitungspersonen dort zu ergreifen, wo konkrete Gefährdungen oder schwer kontrollierbare Gefahrenpotenziale bekannt oder gesetzlich gekennzeichnet sind.[576] Solche Gefährdungen können einzelfallbezogen bekannt werden oder strukturell angelegt sein. Hier muss die Unternehmensleitung devianten Verhaltensstrukturen zeitnah, klar und wirksam gegensteuern, die eingeleiteten Maßnahmen dokumentieren und den Erfolg dieser Maßnahmen kontrollieren. **465**

Im Schrifttum wird weiter die Auffassung vertreten, Vorkehrungen gegen Handlungen, die ein Betriebsangehöriger zu eigenen Zwecken begehe, seien durch Aufsichtsmaßnahmen praktisch ausgeschlossen (sog. **Exzesstaten**).[577] Eine generalisierende Freizeichnung der Leitungspersonen von Verantwortlichkeit scheint indessen verfehlt. Im Gegenteil sind dort,

[574] *Schmalenbach e. V.* DB 2010, 1509 (1510).
[575] Weiterführend dazu *Mansdörfer* Compliance-Berater 2019, 269 ff.
[576] Einen Überblick über bereichsspezifische spezialgesetzliche Regelungen gibt *Rack* CB 2014, 279.
[577] *Rogall* in KK-OWiG § 130 Rn. 46.

wo Exzesstaten zu erwarten sind, erhöhte Anforderungen an die Aufsicht zu stellen.[578] Dies gilt erst recht, wenn bereits einzelne Beschwerden bekannt wurden.

Beispiel (gesteigerte Anforderungen bei Hochrisikobereichen):

Im Bereich der Exportkontrolle hat die Rechtsprechung bereits im Regelbetrieb mit zuverlässigem Personal wegen der Gefahr von fehlerhaften Ausfuhren „mindestens monatliche" stichprobenartige Kontrollen von „mindestens einem Drittel der Importe" verlangt.[579] Ist bereits ein Bußgeld ergangen, so sind „zahlreiche Kontrollen" durchzuführen, bis das Personal „nach einer Reihe von Kontrollen als zuverlässig" eingestuft werden kann.[580] Gerade in Hochrisikobereichen ist daher eine 100 %-Kontrolle ratsam.

Beispiel (aktive Reduktion von Tatgelegenheiten):

Ein strukturell erhöhtes Gefahrenpotenzial beinhaltet der Umgang von Pflegern mit hilfebedürftigen Patienten bzw. Bewohnern von Krankenhäusern oder Pflegeeinrichtungen. Die Durchsetzung etwa des Verbots der Annahme von Zuwendungen in Heimen (§ 14 HeimG) stellt erhöhte Anforderungen, da das Pflegepersonal bei Verstößen regelmäßig eigennützig handelt. Der Heimbetreiber sollte hier besonders strikt bereits die Tatgelegenheiten reduzieren. Konkret empfiehlt sich etwa das Verbot einer „Kaffeekasse", die Befragung von Besuchspersonen oder Angehörigen nach entsprechenden Vorkommnissen, ein rollierender Wechsel des Pflegepersonals über verschiedene Stationen. Ein individuell erhöhtes Risiko besteht etwa, wenn ein bestimmter Patient oder Bewohner bereits unangemessen aufgefallen ist oder konkrete Beschwerden von Angehörigen vorgebracht wurden. Beschwerden müssen in Form eines Beschwerdemanagements aufgenommen und in jedem Einzelfall sogfältig hinterfragt werden.

466 Auch in solchen Situationen erhöhter Anforderungen gilt zunächst das allgemeine Pflichtenbündel von Leitungs- und Koordinations-, Kontroll- und Organisationspflichten.[581] Die Sorgfaltsmaßstäbe sind freilich erhöht und an die konkrete Situation anzupassen. Zu den Leitungsmaßnahmen gehört es, dass zurückliegendes Fehlverhalten deutlich – auch in Form von in den Personalakten festzuhaltenden Abmahnungen, Kündigungen oder Schadensersatzprozessen[582] – sanktioniert und dokumentiert wird. Teil der organisatorischen Maßnahmen ist, Betriebsabläufe neu zu strukturieren, auffällige Personen in Zukunft personell zunächst unter die Kuratel von als zuverlässig bekanntem und erprobtem Personal zu stellen sowie Zugangsberechtigungen zu Datenverarbeitungssystemen neu zu regeln. Nachfolgende gezielte Kontrollmaßnahmen müssen belegen, dass die getroffenen Maßnahmen effektiv und wirksam waren. Schulungen etc sollten in angemessenen zeitlichen Abständen wiederholt und der Lerneffekt kontrolliert werden.

Beispiel (Umsetzung von Hausverboten):

Einer Reinigungsfrau in einem Seniorenstift wird Hausverbot erteilt, weil sie pflegebedürftige Heimbewohner bestohlen oder entgegen §§ 14, 15 HeimG um Geldzuwendungen gebeten hatte. Da der Reinigungsfrau damit der Zutritt über den Haupteingang verwehrt war, nahm sie vor ihren Besuchen telefonischen Kontakt zu den Bewohnern und bat um Einlass über den Hintereingang. Die getroffene Maßnahme war damit ungeeignet. Eingänge zu einer Einrichtung müssen (zB durch mit einem akustischen Alarm) gesicherte Panikschlösser oder durch Überwachungskameras – gesichert werden. Bei richtigem Verhalten der Heimleitung hätten das Pflegepersonal über die Vorfälle unterrichtet und ggf. über die gesetzlichen Regelungen und deren Zweck nochmals geschult, die Sanktionen gegen die Reinigungsfrau offengelegt, das Pflegepersonal in die Überwachung des Hausverbots einbezogen und in angemessenem zeitlichen Abstand die Angehörigen bzw. den Heimbewohner nach neuen Besuchen der betroffenen Dame befragt werden müssen. Bei Hausverboten gegen eine größere Anzahl von Einzelpersonen (zB in einer öffentlichen Badeanstalt zum Schutz vor Belästigungen) müssen die mit einem Hausverbot belegten Personen auf einer Fotodatei dem Servicepersonal gegebenenfalls mit Hintergründen und Klassifizierungen nähergebracht werden, die Abläufe zur Entfernung solcher Personen eingeübt und präventiv in bekannten Foren im Internet etc nach auffälligen Vereinbarungen recherchiert werden.

[578] In diesem Sinne explizit vor dem Hintergrund der unternehmensinternen Compliance *Schünemann* GA 2013, 193 (196); dazu → Rn. 465 ff.
[579] BayObLG NJW 2002, 766 (777); BGHSt 9, 319 (323): Stichproben „in angemessenen zeitlichen Abständen".
[580] BayObLG NJW 2002, 766 (777).
[581] Dazu bereits → Rn. 461.
[582] Zu den praktischen Problemen einer solchen Kündigung aus Arbeitgebersicht *Rieble* BB Heft 26/2011, I.

Praxishinweis (Schadensersatzprozesse und Adhäsionsverfahren gegen Mitarbeiter des eigenen Unternehmens):

Bei Straftaten von Mitarbeitern gegen das Unternehmen bestehen regelmäßig Schadensersatzansprüche des Unternehmens. Zum Wesen einer effektiven Compliance gehört es, auch solche Ansprüche zielgerichtet zu verfolgen. Begeht ein Mitarbeiter zusammen mit einer außenstehenden Person etwa einen Betrug gegenüber dem Unternehmen, so kann der Anspruch auf Schadensersatz gegenüber dem Dritten bereits im Strafverfahren im Wege eines sog. Adhäsionsverfahrens geltend gemacht werden. Für den Anspruch gegen den Mitarbeiter besteht gem. § 2 Abs. 1 Nr. 3 lit. a oder d ArbGG zwar eine ausschließliche Zuständigkeit der Arbeitsgerichte. Im Einzelfall ist freilich oft nicht eindeutig zu erkennen, ob die unerlaubte Handlung in einer besonderen Eigenart des Arbeitsverhältnisses und den ihm eigentümlichen Reibungs- und Berührungspunkten wurzelt oder nur gelegentlich im Rahmen des Arbeitsverhältnisses begangen wurde. Aus diesem Grund kann es sinnvoll sein, die Adhäsionsklage gegen alle Beteiligten zu erheben und sich ggf. für das Verfahren gegen den Mitarbeiter an das Arbeitsgericht verweisen zu lassen. Im Übrigen besteht unter dem Eindruck des laufenden Strafverfahrens oft eine erhöhte Bereitschaft zur (teilweisen) Wiedergutmachung des Schadens.

d) Sektorspezifische Compliance-Pflichten

Die allgemeinen Compliance-Pflichten werden je nach Einzelfall und konkretem Sektor durch spezifische Complianceanforderungen ergänzt. **467**

Beispiele (Sektoren mit bereichsspezifischen Complianceanforderungen):

Praktisch bedeutsame Sektoren sind etwa Nahrungsmittel und Chemie, Abfall, Energie, Bau und Immobilien, Pharma und Gesundheit, Banken und Versicherungen sowie Glücksspiel. Die dortige „Compliance Landscape" weist Schwerpunkte zB in den Bereichen Produktsicherheit,[583] Betriebssicherheit,[584] Kundenklassifizierung oder Suchtprävention auf.

Inhaltlich enthalten diese Anforderungen in erster Linie Konkretisierungen und an den Gegenstand des Unternehmens angepasste Organisations- und Verhaltensnormen. Daneben eröffnet der Gesetzgeber den Unternehmen einzelner Branchen aber bewusst den Zugriff auf erhöhte Mindeststandards, um im Rahmen der allgemeinen Unternehmensethik über die normativ verbindliche Minimalcompliance besonderen Standards gerecht werden zu können. **468**

Beispiele (sektorspezifische Compliance-Ansätze und überobligatorische Selbstverpflichtungen):

Die **Nahrungsmittelindustrie** wird wesentlich durch die Lebensmittelhygieneverordnung (LMHV) mit der speziell für die Nahrungsmittelindustrie entwickelten HACCP (Hazard Analysis Critical Control Points), das Lebensmittelgesetzbuch (LMBG) und nach diesen erlassenen Verordnungen sowie die Kennzeichnungspflichten nach der Lebensmittel-Kennzeichnungsverordnung (LMKV) geprägt.

Im **Finanzsektor** werden wesentliche Regelungen etwa durch § 25a KWG oder § 80 WpHG getroffen.

Eine an § 25a KWG angelehnte Regelung findet sich für **Versicherungsunternehmen** in § 23 VAG.

§ 56 KrWG sieht für **Entsorgungsfachbetriebe** freiwillige Selbstzertifizierungen zur Dokumentation der eigenen Zuverlässigkeit und Selbstkontrolle vor.

Je nach **Gesellschaftsform** folgen Vorgaben aus §§ 93 Abs. 1, 161 AktG iVm Grundsatz 5 u. Empfehlung D.3 DCGK, § 43 Abs. 1 GmbHG.

Spezifische Anforderungen an ein internes Kontroll- und Risikomanagementsystem in der (Konzern) **Rechnungslegung** stellen die §§ 289, 315 HGB.[585]

Die strafrechtliche Bedeutung über das gesetzliche Minimalmaß hinausgehender Selbstverpflichtungen ist bislang weder in der Rechtsprechung noch in der Strafrechtswissenschaft abschließend geklärt. Eine besondere Verpflichtung nach den Grundsätzen insbesondere der allgemeinen unechten Unterlassungsdelikte nach § 13 StGB kommt vor allem dort in **469**

[583] Dazu näher → Rn. 358 ff.
[584] Dazu näher → Rn. 370 ff.
[585] Vertiefend etwa *Wolf* DStR 2009, 920.

Betracht, wo das Unternehmen die besondere Selbstverpflichtung explizit – und nicht nur im Rahmen allgemeiner Werbung – zum Gegenstand vertraglicher Vereinbarungen gemacht hat.

e) Gezielter Einsatz zur Profitmaximierung

470 Der gezielte Einsatz bestimmter Compliancesysteme und weitergehende Selbstverpflichtungen steigern den Unternehmenswert, wenn und wo Endkunden, Vertragspartner oder Behörden eine über das übliche Maß hinaus gewährleistete Zuverlässigkeit durch die Vergabe öffentlich-rechtlicher bzw. zivilrechtlicher Aufträge und Genehmigungen oder durch eine vertiefte Kooperation wirtschaftlich honorieren. Eine funktionierende Compliance ist ein wesentlicher Schlüssel für eine glaubhafte Kommunikation der Verbindlichkeit entsprechender (unter Umständen selbst gesetzter) Standards.

Beispiele (gezielter Einsatz von Compliance zur Profitmaximierung):

471 Gezielte Schulung von Personal eines mittelständischen Spielcasinos im Minderjährigenschutz und in der Suchtprävention zur Bestätigung der eigenen glückspielrechtlichen Zuverlässigkeit; eine aufgrund von zivilrechtlichen Integritätsklauseln zu garantierende Zuverlässigkeit; Selbstverpflichtungen zur Steigerung des Kundenvertrauens; Selbstzertifizierungen nach § 56 KrWG für Entsorgungsfachbetriebe.

472 In der Zwischenzeit geklärt ist, dass überobligatorische Bemühungen um eine unternehmerische Compliance bei gleichwohl vorkommenden Verstößen positiv zu Gunsten eines Unternehmens berücksichtigt werden können.[586] Die allgemeinen Grundsätze für die Zumessung von Strafen und Sanktionen sprechen insoweit eine klare Sprache: Wesentliche Faktoren für die Zumessung von Sanktionen sind das „Maß der Pflichtwidrigkeit" (§ 46 Abs. 2 StGB) bzw. „der Vorwurf, der den Täter trifft" (§ 17 Abs. 3 S. 1 OWiG). Die unternehmensinterne Compliance kann belegen, dass eine Tat nicht Ausdruck eines strukturellen Defizits[587] in einem Unternehmen ist und sich eine einer Leitungsperson anzulastende Pflichtwidrigkeit im unteren Bereich befindet. Werden Taten erst aufgrund der eigenen betrieblichen Selbstüberwachung festgestellt, wird im Schrifttum zu Recht für eine Einstellung des Verfahrens geworben.[588]

f) Reaktive Systemoptimierung

473 Compliancesysteme haben stets einen dynamischen Charakter und müssen den sich ändernden Rahmenbedingungen laufend angepasst werden. Strafrechtlich relevante Vorfälle sollten stets ex post dahin analysiert werden, welche Schwachstellen sie in dem Unternehmen offenbaren.[589] Diese Defizite sind anschließend konsequent zu beheben, sodass das Compliancesystem insgesamt im Hinblick auf die bekannten Defizite optimiert ist.

474 Größere Unternehmen können ihren Willen zu einer reaktiven Compliance auch dadurch belegen, dass die Aufarbeitung der internen Defizite durch einen externen Experten (sog. compliance monitor) überwacht und bestätigt wird. Derartige Maßnahmen wurden bislang in erster Linie auf Betreiben ausländischer Strafverfolgungsbehörden – etwa im Fall des Unternehmens Siemens namentlich auf Betreiben der SEC – eingeführt. In der Sache handelt es sich bei dem **externen Compliancemonitoring** um eine externe, unabhängige, sowie im Einzelfall längerfristige Erfolgskontrolle.

475 Ähnliche Möglichkeiten bietet auch das deutsche Ordnungswidrigkeitenrecht insbesondere auf Grundlage gem. § 47 Abs. 1 OWiG zulässiger Auflagen. § 47 Abs. 3 OWiG untersagt lediglich die Einstellung des Verfahrens gegen Geldauflagen. Andere Auflagen

[586] Befürwortend *Schmalenbach e. V.* DB 2010, 1509 (1509); näher dazu auch *Engelhart,* Sanktionierung von Unternehmen und Compliance, 440 f.
[587] Vgl. zu strukturellen Defiziten *Ost,* Das strukturelle Integritätsmissmanagement als Verbandsschuld, 2024.
[588] *Seitz/Bauer in* Göhler OWiG § 47 Rn. 12.
[589] Vgl. auch → Rn. 466.

oder Weisungen sind hierdurch nicht ausgeschlossen. In der Praxis wurden solche Auflagen bislang allerdings erst sehr vereinzelt verhängt.

Praxishinweis (Compliancemonitoring als Auflage im Rahmen einer Verfahrenseinstellung):

476 Auch wenn ein Compliancemonitoring von Seiten der Hoheitsträger bislang erst vereinzelt zur Auflage gemacht wird, können entsprechende Maßnahmen im Rahmen einer Unternehmensverteidigung von dem betroffenen Unternehmen selbst angeregt werden. Dabei sollte das Compliancemonitoring in einer Weise ausgestaltet werden, dass die Justiz die Einhaltung der Auflagen einfach überwachen und deren Erfüllung für die Beteiligten eindeutig festgestellt werden kann.

Praxishinweis (Weisungsrecht der Fachaufsichtsbehörden und unzulässige Koppelungen durch die Behörden):

477 Bei Ordnungswidrigkeitenverfahren unterliegt die zunächst ermittelnde Verwaltungsbehörde Weisungen der Fachaufsichtsbehörden. Dies gilt auch für die Frage, ob ein Verfahren einzustellen ist. Die Einstellung des Ordnungswidrigkeitenverfahrens kann nach § 47 Abs. 3 OWiG auch im Zusammenhang mit einem Verwaltungsverfahren erfolgen, wenn etwa die Verständigung auf Maßnahmen zur Abhilfe gegen Missstände ein Ordnungswidrigkeitenverfahren einstellungsgeeignet werden lassen. Begehrt die Verwaltungsbehörde umgekehrt die Zahlung einer Geldbuße oder eines Verfallsbetrages und kündigt anderenfalls verwaltungsrechtliche Maßnahmen wie zB den Entzug von Genehmigungen etc an, können damit die Straftatbestände (unter anderem) der §§ 253, 331 ff. StGB erfüllt werden.

g) Zusammenfassung

478 Unternehmenscompliance ist ein Teil des von der Unternehmensführung geforderten strategischen Managements. Betroffen sind die rechtlichen Rahmenbedingungen aller Einzelbereiche des Unternehmens, das Qualitätsmanagement in der Produktion, das Informationsmanagement, das Risikomanagement[590] und die allgemeine Governance.

Praxishinweis (unzureichende Compliance als Untreue):

479 Sind Straftaten in oder gegen ein Unternehmen auf eine defizitäre Unternehmensstruktur zurückzuführen und erleidet das Unternehmen dadurch einen Schaden, könnten die Leitungspersonen künftig – jenseits von Ordnungswidrigkeiten gem. § 130 OWiG – auch wegen Untreue (§ 266 StGB) zum Nachteil ihres Unternehmens strafbar sein (sog. Untreue durch Aufsichtspflichtverletzungen).[591] In der Sache handelte es sich um eine Verantwortlichkeit für strategische Managemententscheidungen.[592] Das tatsächliche Risiko einer derartigen Haftung steigt künftig in dem Maße, wie sich konkrete Standards (state of the art) verfestigen (Erfordernis der Pflichtverletzung) und in der Verfehlung eines Mitarbeiters gerade die mangelhafte Compliance zum Ausdruck kommt (Erfordernis der Zurechenbarkeit). Das Erfordernis der Zurechenbarkeit weicht die Rechtsprechung aktuell durch sinkende Anforderungen bei der richterlichen Überzeugungsbildung (§ 261 StPO) auf.

Praxishinweis (konkrete Wahl des Compliancesystems durch die Unternehmensleitung):

480 Hinsichtlich der konkreten Ausgestaltung des Compliancesystems sind die Unternehmen grundsätzlich frei. Auf dem professionalisierten Markt der Unternehmensberatung konkurrieren derzeit eine erhebliche Anzahl verschiedener Modelle. Für Leitungspersonen größerer Unternehmen bieten sich durchaus Systeme an, die den Leitungspersonen aus dem Bereich des allgemeinen strategischen Managements bekannt sind. Wenn CM-Systeme neu in ein Unternehmen eingeführt werden, sollten diese Systeme zur Erfolgsmessung von Beginn an hinreichend berücksichtigt werden.

[590] Näher dazu → Rn. 73 ff.
[591] *Bock*, Criminal Compliance, 2011, S. 350; zur Geschäftsherrenhaftung im Übrigen bereits ausführlich → Rn. 66 ff.
[592] Näher dazu bereits → Rn. 70.

Beispiel (Compliancesysteme auf der Basis strategischer Managementsysteme):

Compliance-Managementsysteme, die der Unternehmensführung bekannten Managementsystemen ähneln, sind solche auf der Basis des von *Kaplan* und *Norton* entwickelten sog. Balanced-Scorecard-Systems[593] oder CMS-Systeme auf der Basis von Kennzahlensystemen.

II. Compliancestandards und ihre Implementierung

1. Generelle Standards guter Compliance und Entscheidungsspielräume

481 Die Compliance- und Präventionsberatung hat sich in den letzten Jahren etabliert. Compliance wird daher immer weniger situativ und singulär, sondern zunehmend systematisch und revolvierend durchgeführt.

Beispiel (singuläre und situative Compliance):

482 Das Unternehmen U führt nach Bekanntwerden eines Verstoßes gegen Vergaberecht eine Schulung der Mitarbeiter durch und ändert seine unternehmensinternen Verhaltensrichtlinien (Code of Conduct, Handbuch usw). In den Folgejahren werden keine weiteren Maßnahmen unternommen. Nach drei Jahren wird das Unternehmen erneut in einen ähnlichen Vorfall verwickelt. Der Hinweis auf die vereinzelte, Jahre zurückliegende Schulung wird die Staatsanwaltschaft nicht von einer aktiven Präventionspolitik seitens der Geschäftsführung überzeugen. Im Gegenteil besteht Erklärungsbedarf, warum die damaligen Bemühungen nicht konsequent fortgeführt wurden.

483 Zur Leitungsaufgabe der Unternehmensorgane gehört es, dass die von ihnen eingeführten Compliance-Maßnahmen dem inzwischen gesicherten Stand der kriminologischen Verhaltenswissenschaft entsprechen.[594] Dazu gehören sowohl Compliance-Standards wie derjenige des *Instituts für Wirtschaftsprüfer* (**IDW PS 980** (09.2022)) oder der *Schmalenbachgesellschaft*[595] als auch Risikomanagementmodelle. Zu den Risikomanagementmodellen gehören etwa **GRC-Modelle** (GRC = Governance, Risk und Compliance) mit der Idee einer einheitlichen Governance, Risikomanagement- und Compliance-Struktur oder die vom Committee of Sponsoring Organizations of the Treadway Commission (COSO) propagierte Idee eines **Enterprise(-wide) Risk Management (ERM-Modell bzw. COSO II).**[596] Als internationaler Standard legt **ISO 31000** die Prinzipien eines unternehmensinternen Risikomanagements und Kriterien für ein entsprechendes Rahmenwerk, und **ISO 37301** Anforderungen an die Compliance Management Systeme fest.[597] Ergänzt werden diese allgemeinen Standards durch spezielle Branchenkonzepte.[598]

Beispiel (branchenspezifische Compliance-Konzepte):

Branchenspezifische Compliance für private **Wohnungsverwaltungsgesellschaften** wird sich auf folgende Hauptrisikobereiche erstrecken: DV-gestützte Compliance im gewöhnlichen Geschäftsgang; Korruption, Umgang mit vertraulichen Daten über Immobilien (Kauf, Verkauf, Verpachtung inkl. Erbpacht), marktbezogene Informationen zB Projektierungsplanungen von Bauträgern, kundenbezogene Informationen (Bonität, Zwangsversteigerung, Untersagung bzw. Genehmigungspflicht von bestimmten Mitarbeitergeschäften), Meldeverfahren für Mitarbeitergeschäfte sowie bei öffentlich–rechtlichen Wohnungsverwaltungsgesellschaften eine Ergänzung um spezielle Regelungen zur Verwendung öffentlicher Mittel und Subventionen.

484 In der strafrechtlichen Rechtsprechung hat die Entscheidung des Bundesgerichtshofs zur strafrechtlichen **Verantwortlichkeit eines Compliance-Officers** erste inhaltliche Maßstäbe gesetzt, zugleich aber weitere Fragen aufgeworfen.[599] Schon im eigenen Interesse

[593] *Kaplan/Norton,* Balanced Scorecard, 1997.
[594] Zum aktuellen kriminologischen Stand etwa *Burkatzki,* Kriminalität im Marktkontext, 2015. Zur Compliance-Pflicht als einem der vier großen Pflichtenkreise des GmbH-Geschäftsführers OLG Zweibrücken v. 18.8.2022 – 4 U 198/21; entsprechend für „Unternehmen ab einer bestimmten Größe" *Schieffer* in Minkoff/Sahan/Wittig Konzernstrafrecht § 29 Rn. 8.
[595] *Schmalenbachgesellschaft e. V.* DB 2010, 1509 (1510).
[596] Nähere Informationen unter www.coso.org/documents/coso_erm_executivesummary.pdf.
[597] International Organization for Standardization (ISO) (Hrsg.), ISO 31000:2018 und ISO 37301:2021.
[598] ZB die IATF-Standards für die Automobilbranche.
[599] BGH NJW 2009, 3173 (3175).

muss die Unternehmensleitung die Aufgaben- und Stellenbeschreibung der von ihr eingesetzten Hilfspersonen – wie zB Compliance-Officer, bereichsspezifisch Beauftrage[600] oder einem Lenkungsausschuss Compliance – möglichst klar und eindeutig fassen. Unklarheiten gehen zu Lasten der Unternehmensleitung, da die Aufsichts– und Überwachungspflichten nach der gesetzlichen Aufgabenverteilung gerade in ihren Zuständigkeitsbereich fallen.

Allgemein wird etwa von der *Schmalenbachgesellschaft* ein dreistufiges Vorgehen zur Bewältigung von Compliance-Risiken vorgeschlagen:[601] **485**

– Erste Stufe: Feststellen der Compliance-Risiken,
– Zweite Stufe: Entwicklung eines Compliance-Programms,
– Dritte Stufe: Kontrolle und Sanktionierung von Compliance-Verstößen.

Zu unterscheiden ist zwischen bereichsspezifischen und umfassenden Compliance-Programmen. Bereichsspezifische Programme sind in erster Linie bei kleineren und (auch größeren) mittelständischen Unternehmen angemessen, die etwa aufgrund ihrer Produktpalette oder Vertriebsstrukturen gerade in Einzelbereichen erhöhten Risiken ausgesetzt sind. **486**

Beispiel (bereichsspezifische Compliance):

Das mittelständische Unternehmen U ist Weltmarktführer für spezielle, primär in der Verkehrsleitung eingesetzte Steuerungssysteme. Die Produkte werden weltweit vertrieben. Es bestehen hohe Risiken für (internationale) Korruptionshandlungen oder für (wettbewerbsbeschränkende) Absprachen mit Wettbewerbern. Hier kann es ausreichen, in diesen beiden Bereichen spezielle Compliance-Programme einzuführen.

Ein umfassendes Compliance-Programm wird insbesondere solchen Unternehmen empfohlen, die Compliance-Risiken in verschiedenen Bereichen identifiziert haben, so dass der alternative Einsatz einzelner Beauftragter der Gesamtsituation im Unternehmen nicht mehr gerecht wird.[602] Ansonsten differiert gerade im Mittelstand der konkrete Umfang des Compliance-Programms je nach Größe eines Unternehmens. Zur Bestimmung des Umfangs eines Complianceprogramms wird aktuell ein **Zwei-Faktoren-Modell** vorgeschlagen, das zum einen nach dem Grad einzelner Gefährdungen und zum anderen nach der Größe (bzw. dem Reifegrad) des jeweiligen Unternehmens unterscheidet.[603]

Praxishinweis (Internationale Anerkennung von Compliancesystemen):

Global tätige Unternehmen sollten darauf achten, dass das von ihnen praktizierte System international – eventuell gerade auch von der US-amerikanischen SEC – anerkannt ist. Die SEC erkennt etwa neben COSO II auch die Guidance on Assessing Control vom Canadian Institute of Chartered Accountants und die Leitlinien des „Turnbull Report des Institute of Chartered Accountants in England and Wales" an.[604] Im Detail divergierenden Standards kann durch ein dezentrales Compliancesystem Rechnung getragen werden. **487**

2. Konkrete Implementierung eines Compliance-Programms durch die Unternehmensleitung

a) Erster Schritt: Budgetplanung, Compliance in der innerbetrieblichen Kostenrechnung und Compliance-Design

Am Anfang jeder Compliance-Strategie steht – wie bei anderen unternehmerischen Maßnahmen auch – die Planung des konkret zur Verfügung stehenden Budgets. **488**

[600] Beispiele für solche Beauftrage sind Kartellbeauftragte, Korruptionsbeauftragte, Betriebssicherheitsbeauftragte.
[601] *Schmalenbachgesellschaft e. V.* DB 2010, 1509 (1511).
[602] *Schmalenbachgesellschaft e. V.* DB 2010, 1509 (1512).
[603] Eine sachangemessene Differenzierung erlaubt etwa der Ansatz von *Mackert/Karabier* CB 2014, 242 (245 ff.) angelehnt an entsprechende Differenzierungen der United States Sentencing Commission und der UK Bribary Act Guidance des UK Ministery of Justice.
[604] Näheres unter www.sec.gov/rules/final/33–8238.htm#iib3a.

Praxishinweis (Compliancekosten in der innerbetrieblichen Kostenrechnung):

489 Die Kosten für die Compliancestruktur lassen sich im Rahmen der Kostenträgerrechnung in Gemeinkosten und Einzelkosten aufteilen. Eine Aufteilung ist insbesondere dort sinnvoll, wo konkrete Einzelaufträge einen erhöhten oder spezifischen Aufwand nach sich ziehen. Im Übrigen kann es im Einzelfall sinnvoll sein, zum Nachweis der eigenen Zuverlässigkeit dem Kunden den konkreten Aufwand explizit vor Augen zu führen.

490 Für das konkrete Compliance-Design hat sich ein zumindest grober formaler Rahmen aus acht Grundelementen etabliert, an dem die Wirksamkeit einer entsprechenden Organisation grundsätzlich gemessen wird.[605] Auch wenn ein Unternehmen zunächst nur bereichsbezogen einzelne Compliancemaßnahmen durchführen möchte, sollte dieser elementare Organisationsrahmen berücksichtigt werden. Eine hervorgehobene Stellung nimmt insoweit der IDW PS 980 (09.2022) ein. Hierbei handelt es sich um den Prüfungsstandard des Instituts der Wirtschaftsprüfer, anhand dessen Wirtschaftsprüfer und andere die grundsätzliche Wirksamkeit und Angemessenheit des Gesamtsystems überprüfen.

Praxishinweis (Verbindlichkeit des IDW PS 980 (09.2022)):

491 Der IDW PS 980 (09.2022) ist in verschiedener Hinsicht bedenklich. Es ist zunächst ein Standard, der vom Institut der Wirtschaftsprüfer erlassen wurde. Dieser Standard hat daher keinen Gesetzesrang und ist für Gerichte und Staatsanwaltschaften nicht verbindlich. Auch setzt der Standard in Nr. 3.1 und 3.2 PS 980 (09.2022) eine Prüfung durch Wirtschaftsprüfer – also nicht Volljuristen und erst recht nicht Strafrechtsspezialisten – voraus. Die Züge einer gruppenspezifischen Interessenvertretung sind daher deutlich. Trotz dieser Bedenken scheint es angemessen, den Prüfungsstandard zumindest für Unternehmen mit mehr als 700 Mitarbeitern und einem Umsatz von mehr als 100 Millionen Euro als Referenzrahmen anzunehmen.[606]

492 Der IDW PS 980 (09.2022) nennt als **acht Grundelemente** eines Compliance-Managementsystems:
- die Compliance-Kultur
- die Compliance-Ziele
- die Compliance-Risiken
- das Compliance-Programm
- die Compliance-Organisation
- die Compliance-Kommunikation sowie
- die Compliance-Überwachung und
- die Compliance-Verbesserung.

Nur wenn diese acht Grundelemente optimal im Unternehmen implementiert seien, könne ein Compliance-Managementsystem funktionieren.[607]

493 Konkrete Vorgaben zum Umfang der entsprechenden Grundelemente macht der IDW PS 980 (09.2022) nicht. Es bleibt daher dem konkreten Beratungsmandat überlassen, die erforderlichen Maßnahmen am vorgegebenen Budget auszurichten. Im Zweifel kann die Summe des Budgets mit den Beratern gemeinsam ermittelt werden. Grundsätzlich müssen neben den Kosten für die erste Implementierung eines solchen Systems auch die laufenden Kosten berücksichtigt werden.

b) Zweiter Schritt: Einführung der konkreten Compliance-Struktur in das Unternehmen

494 Zentrale inhaltliche Elemente eines Compliancesystems sind eine allgemeine Beschreibung des Complianceprogramms und seiner Struktur, eine klare Risikoanalyse, einfache und verständliche Verhaltenskodizes und klare Verantwortungsbereiche (zB im Geschäftsvertei-

[605] Zu diesen acht Grundelementen → Rn. 492.
[606] Vgl. bereits → Rn. 14.
[607] Siehe auch Checkliste 27 Punkt III.