



■ Impressum

Herausgeber:	BITKOM Bundesverband Informationswirtschaft Telekommunikation und neue Medien e. V. Albrechtstraße 10 A 10117 Berlin-Mitte Tel.: 030.27576-0 Fax: 030.27576-400 bitkom@bitkom.org www.bitkom.org
Ansprechpartner:	Thomas Kriesel Tel.: 030.27576-146 t.kriesel@bitkom.org
Copyright:	BITKOM 2012
Grafik/Layout:	Design Bureau kokliko / Eugen Regehr (BITKOM)
Titelbild:	© Ben Chams – Fotolia.com

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im BITKOM zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim BITKOM.



Leitfaden Compliance

Rechtliche Anforderungen an ITK-Unternehmen

Inhaltsverzeichnis

1	Einleitung	6
2	Was ist Compliance?	8
3	Rechtlicher Rahmen für Unternehmenscompliance	10
3.1	Gesetzliche Grundlagen	10
3.2	Verantwortlichkeiten in Kapitalgesellschaften	11
3.3	Verantwortlichkeiten in Personenunternehmen	12
3.4	Sanktionen für Compliance-Verstöße	12
4	Korruptionsprävention	16
4.1	Korruptionsprävention in Deutschland	16
4.1.1	Bestechung und Bestechlichkeit von Amtsträgern	16
4.1.2	Begriff des Amtsträgers	16
4.1.3	Bestechung und Bestechlichkeit im geschäftlichen Verkehr	17
4.1.4	Begriff des »Angestellten« und des »Beauftragten«	17
4.1.5	Abgrenzung zwischen legaler Kundenpflege und Korruption	17
4.2	Korruptionsprävention im US-Recht: Foreign Corrupt Practices Act	18
4.2.1	Anwendungsbereich	19
4.2.2	Zuständige Strafverfolgungsbehörden	19
4.2.3	Begriff des ausländischen Amtsträgers	19
4.2.4	Inhalt des FCPA	19
4.2.5	Verantwortung für Dritte	19
4.2.6	Sanktionen	20
4.2.7	Anwendbarkeit für deutsche Unternehmen	20
4.3	Korruptionsprävention im britischen Recht: UK Bribery Act	20
4.3.1	Inhalt des UKBA	21
4.3.2	Zuständige Strafverfolgungsbehörden	21
4.3.3	Begriff des ausländischen Amtsträgers	21
4.3.4	Präventive Massnahmen zur Verhinderung von Korruption	21
4.3.5	Verantwortung für Dritte	22
4.3.6	Sanktionen	22
4.3.7	Anwendbarkeit für deutsche Unternehmen	23
4.4	Handlungsempfehlung	23
5	Wettbewerbsrecht	24
5.1	Wesentliche Unlauterkeitstatbestände	24
5.2	Rechtsfolgen im Wettbewerbsrecht	28
6	Kartellrecht	29
6.1	Rechtsgrundlagen des Kartellrechts	29
6.2	Ziel des Kartellrechts und Risiken von Complianceverstößen	29
6.3	Verhalten im Umgang mit Kartellbehörden, Kronzeugenregelung	30
6.4	Das Verbot wettbewerbsbeschränkender Vereinbarungen	31
6.4.1	Überblick	31

6.4.2	Tatbestandsmerkmale des Verbots	32
6.4.3	Ausnahmen (Freistellung) vom Verbot	33
6.4.4	Bedeutung der Selbstprüfung	35
6.4.5	Fallgruppen horizontaler Vereinbarungen zwischen Wettbewerbern	36
6.4.6	Fallgruppen vertikaler Vereinbarungen (Vertriebsbeschränkungen)	38
6.5	Missbrauch einer marktbeherrschenden Stellung	41
6.5.1	Definition einer marktbeherrschenden Stellung	41
6.5.2	Diskriminierungsverbot bei marktbeherrschender Stellung	41
6.5.3	Behinderung von Wettbewerbern bei marktbeherrschender Stellung	41
6.5.4	Ausnutzen von Marktmacht gegenüber abhängigen Unternehmen	42
7	Exportkontrolle und Außenwirtschaftsrecht	43
7.1	Zweck von Exportkontrollen	43
7.2	Rechtsgrundlagen	43
7.3	Instrumente des Exportkontrollrechts	43
7.4	Exportkontrollierte Güter	44
7.5	Besonderheiten bei Outsourcing und Cloud Computing	44
7.6	Besonderheiten bei grenzübergreifender Software-Entwicklung	44
7.7	Besonderheiten für Vermittlungsgeschäfte	44
7.8	Umgang mit Embargoländern	45
7.9	Beachtlichkeit des US-amerikanischen Rechts	45
7.10	Compliance im Exportkontrollrecht	45
8	Finanzberichterstattung	46
8.1	Buchführungspflicht	46
8.2	Anforderungen an eine elektronische Buchführung	49
8.3	Verantwortlichkeiten und Sanktionen	49
8.4	Interne Kontrollen	50
8.5	Externe Kontrollen	51
9	Besteuerung	52
9.1	Steuerrechtliche Mitwirkungspflichten	52
9.2	Sanktionen	53
10	Archivierungspflichten	54
10.1	Archivierungspflichten nach Handelsrecht	54
10.2	Archivierungspflichten im Steuerrecht	54
10.3	Archivierungsrichtlinie im Unternehmen	56
11	Unternehmenspublizität	57
11.1	Anmeldungen zum Handelsregister	57
11.2	Veröffentlichungen im Unternehmensregister	57
11.3	Pflichtangaben in der geschäftlichen Korrespondenz	59
11.4	Anbieterkennzeichnung für Internetseiten	59
12	Abgaben	60
12.1	Rundfunkgebühren	60
12.2	Urheberrechtsabgaben	60



13	Management von Software-Lizenzen	62
13.1	Risiken beim Software-Lizenzmanagement	62
13.2	Lizenzmodelle	62
13.3	Lizenzmanagement	63
13.4	Nutzen des Lizenzmanagements	64
13.5	Einrichtung eines Lizenzmanagements	65
13.6	Softwarelizenz-Audits	66
13.7	Besonderheiten im Lizenzmanagement für Open Source Software	66
13.8	Alternative: Software as a Service (SaaS)	67
13.9	Verkauf von überschüssigen Lizenzen – Gebrauchtssoftware	68
14	Datenschutz und Datensicherheit	70
14.1	Datensicherheit	70
14.2	Schutz personenbezogener Daten	70
14.3	Datenverarbeitung durch Dritte	71
14.4	Besondere Arten personenbezogener Daten	72
14.5	Datenschutzrechtliche Mindestanforderungen	72
15	Umweltrechtliche Compliance-Anforderungen	73
15.1	Entsorgung von Elektro-Altgeräten	73
15.2	Stoffvorgaben für Gerätehersteller	74
15.3	Entsorgung von Verkaufsverpackungen	76
16	Anforderungen durch europäische Produktstandards	77
17	Compliance-Management im Unternehmen	78
17.1	Elemente eines Compliance-Management-Systems	78
17.2	Einführung eines Compliance-Management-Systems	79
17.3	Ausgestaltung des Compliance-Management-Systems	80
17.4	Restriktionen des Compliance-Managements	82
18	Compliance-Beauftragter	83
18.1	Aufgaben eines Compliance-Beauftragten	83
18.2	Stellung des Compliance-Beauftragten	84
18.3	Haftung des Compliance-Beauftragten	84

Autorenteam

Wir danken folgenden Personen herzlich für ihre Beiträge zum BITKOM-Leitfaden Compliance und für die konstruktive Mitarbeit bei der Erstellung des Leitfadens:

- Mehmet-Adem Bayrak; Purchasing Manager Global Sourcing Software, Fujitsu Technology Solutions GmbH
- Bernd H. Harder; Rechtsanwalt, Büsing Müffelmann Theye
- Christian Herzog; Bereichsleiter technische Regulierung und Umwelt, BITKOM e.V.
- Matthias Horn; Rechtsreferendar, BITKOM e.V.
- Dr. Philip Kempermann LL.M.; Rechtsanwalt & Salaried Partner, Heuking Kühn Lüer Wojtek
- Jens Lechleitner; Rechtsanwalt / Chief Compliance Officer, ALSO - Actebis Holding AG
- Christine Mayer; Senior Director Legal Services, Regulatory & Compliance Operations ASG, Nordics, Gallia, Accenture Holding GmbH & Co. KG
- Alexandra Schramm LL.M. (USyd); Rechtsanwältin, Deputy General Counsel Central & Eastern Europe, Capgemini Deutschland Holding GmbH
- Dr. Thilo Streit, Rechtsanwalt; LL.M., Senior Associate DLA Piper UK LLP
- Dr. Renate Vondenhoff-Mertens; Leiterin der Rechtsabteilung, DATEV eG
- Dr. Stephan Witteler; Rechtsanwalt & Partner, Heuking Kühn Lüer Wojtek

Darüber hinaus danken wir folgenden Personen herzlich für die kritische Durchsicht einzelner Kapitel und für ihre daran anschließenden Anmerkungen, Ergänzungen und wertvollen Hinweise:

- Sonja Bjeloborodov; Tectum Consulting GmbH
- Compliance-Mitarbeiter der Telekom Deutschland GmbH
- Christof Höfner; Rechtsanwalt
- Dr. Wulf Kamlah; Rechtsanwalt, SKW Schwarz Rechtsanwälte
- Heike Lehmann; Transportation Manager, Motorola Solutions Germany GmbH
- Marja von Oppenkowski, M.E.S., Rechtsanwältin, Leiterin Hauptstadtbüro, Kabel Deutschland Vertrieb und Service GmbH
- Dr. Axel Pols; Bereichsleiter Marktforschung und Außenwirtschaft, BITKOM e.V.
- Dipl.-Ing., Dipl.-Wirtsch.-Ing. Peter Steffek; CEO, KTC-Karlsruhe Technology Consulting GmbH
- Judith Steinbrecher; Bereichsleiterin Urheberrecht, BITKOM e.V.
- Antje Strohbach; Wirtschaftsprüferin und Steuerberaterin, Knischewski & Boßlet GmbH
- Bernhard Zöller; Geschäftsführer Zöller & Partner GmbH

1 Einleitung

Wie bereits der Begriff nahe legt, stammt Compliance ursprünglich nicht aus der deutschen Rechtsordnung. Allerdings hat dieses vom US-amerikanischen Recht geprägte Konzept in den letzten Jahren auch in Deutschland zunehmend an Bedeutung gewonnen. Das ist nicht nur darauf zurückzuführen, dass die global ausgerichtete deutsche Wirtschaft vielfach mit ausländischen Rechtsordnungen konfrontiert ist. Vielmehr erhielt das Thema Compliance in Deutschland selbst durch Aufsehen erregende Rechtsverstöße in großen Unternehmen erhöhte Priorität. In der Folge sahen sich die Unternehmen gezwungen, zur Wiederherstellung ihres Ansehens Maßnahmen zu ergreifen, um die Rechtsdurchsetzung aktiv zu fördern und ähnliche Rechtsverstöße zukünftig zu vermeiden.

Der vorliegende Compliance-Leitfaden unternimmt den Versuch, aktuelle Compliance-Anforderungen an Unternehmen aus den Branchen Informationstechnologie, Telekommunikation, Consumer Electronics und neue Medien (ITK-Branchen) zu systematisieren, überschaubar darzustellen und implementierbar zu machen. Er richtet sich an Juristen, juristisch vorgebildete Manager und Führungsverantwortliche in ITK-Unternehmen, die einen Einstieg und eine erste Orientierung zu Fragen der Unternehmenscompliance suchen.

Nach einer Auseinandersetzung mit dem Compliance-Begriff und den Rechtsgrundlagen für Compliance in Wirtschaftsunternehmen werden rechtliche Pflichten aus verschiedenen Rechtsgebieten dargestellt, die für Unternehmen aus den ITK-Branchen besonders relevant sind. Dabei konzentriert sich die Darstellung auf zwingende Compliance-Anforderungen, die mit gesetzlichen Sanktionen bewehrt sind.

Insoweit werden nur die minimalen Grundanforderungen beim Betrieb eines Unternehmens dargestellt. An eine kurze Erläuterung der gesetzlichen Vorgaben schließt sich eine Beschreibung der jeweiligen Compliance-Risiken, insbesondere von Haftungsrisiken und

Sanktionsmechanismen, an. Auf Möglichkeiten zur Vermeidung oder zumindest Abmilderung von Compliance-Risiken wird ebenfalls hingewiesen. Zum Abschluss geht der Leitfaden auf die Umsetzung der rechtlichen Anforderungen und auf die mögliche Ausgestaltung einer Compliance-Struktur im Unternehmen ein.

Da nicht sämtliche rechtlichen Anforderungen an ein Unternehmen dargestellt werden können, konzentriert sich dieser Leitfaden auf die für ITK-Unternehmen spezifischen juristischen Themen. Folgende Rechtsgebiete werden z. B. nicht behandelt:

- Arbeits- und Sozialversicherungsrecht,
- Produkthaftung,
- Insolvenzrecht,
- Gewerberecht,
- Markenrecht,
- Immissionsschutzrecht,
- Wertpapier- und Börsenrecht.

Die dargestellten Rechtspflichten sind für alle ITK-Unternehmen gleichermaßen relevant, also auch für kleine und mittlere Unternehmen, die lediglich im Inland aktiv sind. Die Relevanz ergibt sich schon aus den drohenden Sanktionen, die sehr empfindlich, teilweise sogar Existenz bedrohend sein können. Inwieweit ein Unternehmen von den dargestellten Rechtspflichten betroffen ist, hängt aber auch von der konkreten Unternehmensstätigkeit ab.

Dieser Leitfaden soll eine Orientierung und Hilfestellung sein, kann den Unternehmensverantwortlichen aber die Auseinandersetzung mit den Compliance-Anforderungen und die Auswahl der jeweils im konkreten Fall einschlägigen Bestimmungen nicht abnehmen. Da an vielen Stellen die rechtlichen Grundsätze nur skizziert werden können, wird jeweils auf weiterführende Literatur hingewiesen.



Auch wenn sich die Darstellung auf das deutsche Recht konzentriert, kann der Einfluss ausländischer Rechtsordnungen aufgrund der globalen Ausrichtung der deutschen Wirtschaft nicht völlig ausgeblendet werden. Deshalb finden sich an einzelnen Stellen Hinweise zu anderen Rechtsordnungen.

2 Was ist Compliance?

Compliance meint zunächst nichts anderes als die Einhaltung des geltenden Rechts. Das wichtigste Ziel von Compliance besteht darin, Rechtsverstöße zu unterbinden und damit Gefahren für den Fortbestand des Unternehmens abzuwenden.

Bei der Umsetzung in Wirtschaftsunternehmen (»Corporate Compliance«) beschreibt Compliance die Gesamtheit der Maßnahmen, die das rechtmäßige Verhalten eines Unternehmens, seiner Leitungs- und Aufsichtsorgane und seiner Mitarbeiter sicherstellen soll. Dabei geht es nicht zuletzt auch darum, die Mitarbeiter selbst vor rechtlichen Konsequenzen zu schützen.

In einem weiteren Verständnis können auch ethische und gesellschaftliche Anforderungen unter den Compliance-Begriff subsumiert werden. Teilweise wird Compliance sogar als ganzheitliches Konzept zur Unternehmensoptimierung entsprechend den selbst gesetzten Unternehmenszielen verstanden, das auch unternehmensinterne Vorgaben zum Umgang mit Geschäftspartnern und zum allgemeinen Verhalten des Unternehmens im Geschäftsverkehr sowie das gesellschaftliche Auftreten des Unternehmens umfasst. Die Darstellung im vorliegenden Leitfaden beschränkt sich allerdings auf die zwingenden rechtlichen Compliance-Anforderungen. Eine weitergehende begrüßenswerte Orientierung des Unternehmens an ethischen und gesellschaftlichen Anforderungen oder an einem bestimmten Unternehmensleitbild wird hier nicht untersucht.

Bei Verstößen gegen Compliance-Anforderungen des geltenden Rechts drohen zum einen juristische Konsequenzen, beispielsweise Haftungs- und Schadenersatzansprüche gegen das Unternehmen und dessen Leitung, Bußgelder, Entzug von staatlichen Genehmigungen, Importverbote und in Extremfällen strafrechtliche Sanktionen. Zum anderen muss mit dem Verlust unternehmerischer Reputation, mit negativen Kundenreaktionen und mit Umsatzeinbußen bis hin zu Herabstufungen beim Kreditrating durch Banken und Rating-Agenturen oder

Höherstufungen bei der Risiko- und Prämienbewertung durch Versicherungen gerechnet werden. Diese wirtschaftlichen Konsequenzen können für das Unternehmen noch schmerzhafter sein als rechtliche Sanktionen.

Die Identifizierung, Steuerung, Überwachung und Begrenzung der genannten Risiken, also ein Risiko-Management, ist untrennbar mit dem Verständnis von Compliance verbunden. Dabei sind rechtliche Risiken aufgrund von Verstößen gegen eine Rechtspflicht und betriebswirtschaftliche Risiken aufgrund von nicht angemessener Steuerung des Unternehmens und seiner Geschäftstätigkeit zu unterscheiden.

Um den angesprochenen Anforderungen gerecht zu werden, sollten in jedem Unternehmen ein Compliance-Management und eine Compliance-Kultur implementiert werden. Zwar ordnet der deutsche Gesetzgeber nicht ausdrücklich an, dass Unternehmen ein Compliance-Management aufbauen müssen. Denn die Einhaltung des geltenden Rechts ist selbstverständlich. Die systematische und kontrollierte Ausrichtung der unternehmensinternen Prozesse an den rechtlichen Anforderungen mit festen Verantwortlichkeiten nach entsprechenden Vorgaben der Leitungsorgane im Unternehmen (Compliance-Management) macht jedoch gerade den Aspekt aus, der Compliance über bloße Rechtsanwendung hinaushebt.

Zur Durchsetzung von Compliance im Unternehmen kann Informationstechnologie (IT) unterstützend eingesetzt werden. Der IT-Einsatz wirft jedoch eigene spezifische Fragen zur IT-Compliance auf. Denn die IT-Infrastruktur und die Datenhaltung im Unternehmen unterliegen ihrerseits rechtlichen Vorgaben und Anforderungen. Bei größerem Datenverlust kann sogar der Fortbestand des gesamten Unternehmens gefährdet sein. Auch beim IT-Einsatz sind daher rechtliche und wirtschaftliche Risiken zu berücksichtigen.

Elemente des Compliance-Begriffs

- Systematische Ausrichtung der betrieblichen Organisation an rechtlichen Vorgaben und Anforderungen
 - Transformation der allgemeinen rechtlichen Anforderungen in unternehmensinterne Richtlinien und Handlungsanweisungen
 - Kontrolle und Vermeidung von Haftungs- und Geschäftsrisiken für das Unternehmen und seine Mitarbeiter
 - Überwachung des rechtskonformen Verhaltens im Unternehmen und Einleitung von Maßnahmen bei festgestellten Rechtsverstößen
 - Feste Verantwortlichkeiten
 - »Top-Down«-Ansatz
-

3 Rechtlicher Rahmen für Unternehmenscompliance

■ 3.1 Gesetzliche Grundlagen

Die dicht regulierte deutsche Rechtsordnung enthält für die unternehmerische Tätigkeit recht genaue Vorgaben. Neben besonderen branchenspezifischen Vorschriften (z. B. Umwelt- und Gesundheitsauflagen, Betriebserlaubnisse, Qualifizierungsnachweise) gelten für jeden Betrieb allgemeine Compliance-Anforderungen, die mit der Teilnahme am geschäftlichen Verkehr verbunden sind. Die allgemeine Compliance-Pflicht, Recht und Gesetz zu befolgen, ist vielfach konkretisiert durch

- Antragspflichten,
- Informationspflichten,
- Dokumentationspflichten,
- Kontroll- und Überwachungspflichten,
- Unterlassungspflichten,
- Pflichten zur Einhaltung bestimmter Standards.

Diese Pflichten dienen zum Schutz des allgemeinen Rechts- und Geschäftsverkehrs und sollen verschiedene Interessen zum Ausgleich bringen. Teilweise wird die Einhaltung dieser Schutzvorschriften in Deutschland durch externe Überwachungsstellen kontrolliert (z. B. Gewerbeaufsicht, Handelsregister, Finanzverwaltung, Kartellbehörden, staatliche Datenschutzbeauftragte, mit staatlichen Hoheitsrechten beliehene Personen des Privatrechts) oder durch staatlich unterstützte Interessensgruppen zur Geltung gebracht (z. B. Umwelt- und Verbraucherschutzorganisationen, Gewerkschaften).

Für die Frage, wie die Befolgung der verschiedenen rechtlichen Verhaltensanordnungen im Unternehmen zu organisieren ist, enthält die deutsche Rechtsordnung kaum konkrete Aussagen. Aus den allgemeinen rechtlichen Vorgaben können jedoch Verhaltensanforderungen für Unternehmensführung und Geschäftsabwicklung abgeleitet werden. Zu diesen allgemeinen Grundlagen gehören:

- das Strafrecht (z. B. §§ 263, 266, 298, 299, 13, 14 StGB),
- das Recht der Ordnungswidrigkeiten (insbesondere §§ 130, 30, 9, 10 OWiG),
- das Wettbewerbsrecht (insbesondere § 81 GWB),
- das Gesellschaftsrecht (z. B. § 91 AktG oder § 161 AktG mit Bezug zum Deutschen Corporate Governance-Kodex, hier vor allem Ziff. 4.1.3, 3.4 und 5.3.2),
- die allgemeinen deliktischen Haftungsgrundlagen (insbesondere §§ 823 ff. BGB).

Der rechtliche Rahmen für Compliance im Unternehmen ergibt sich also aus dem Zusammenwirken der verschiedenen allgemeinen Vorschriften. Teilweise wird aus der Zusammenschau der allgemeinen Vorschriften eine Pflicht für alle Unternehmen abgeleitet, eine Compliance-Organisation aufzubauen. Eine solche allgemeine Verpflichtung lässt sich jedoch aus den einschlägigen Vorschriften nicht entnehmen. Nur vereinzelt erlegt das Gesellschaftsrecht der Unternehmensleitung konkrete Maßnahmen auf. Im Übrigen lässt die Rechtsordnung der Geschäftsführung in Unternehmen einen eigenen Entscheidungsspielraum, den sie nach eigenem Ermessen ausfüllen kann (business judgment rule gem. § 93 Abs. 1 S. 2 AktG).

Damit hängen die Einrichtung eines Compliance-Managements und seine Ausgestaltung weitgehend von der Einschätzung der Geschäftsführungsorgane eines Unternehmens ab. Die Entscheidung sollte unter Abwägung der für das Unternehmen bestehenden rechtlichen Risiken und dem mit einem Compliance-Management zusammenhängenden Aufwand getroffen werden. Dabei spielen auch die Größe des Unternehmens, die Überschaubarkeit seiner Strukturen, die Anzahl und Sachkunde der Beschäftigten und die tatsächlichen Überwachungsmöglichkeiten eine Rolle. Soweit sich die Unternehmensführung zutraut, bei einer überschaubaren Unternehmensstruktur selbst durch eigene Kontrollen die Rechtskonformität im Unternehmen zu gewährleisten, kann dies für eine angemessene Compliance durchaus ausreichen. Diese Entscheidung muss aber wegen der gesellschaftsrechtlichen Sorgfaltsanforderungen an Führungsorgane der Unternehmen bewusst und nach umfassender Abwägung getroffen werden. Die Unternehmensführung muss sich also jedenfalls mit dem Thema Compliance auseinandersetzen.

■ 3.2 Verantwortlichkeiten in Kapitalgesellschaften

Die Geschäftsleitung eines jeden Unternehmens ist zu verantwortungsvoller Unternehmensführung (Corporate Governance) angehalten. Dazu gehört die Aufgabe, Compliance im Unternehmen zu gewährleisten. Damit nimmt die Compliance-Betrachtung in den Verantwortungszuweisungen der gesellschaftsrechtlichen Corporate Governance ihren Ausgangspunkt.

Für die Vorstände von Aktiengesellschaften leitet sich die Pflicht zur verantwortungsvollen Unternehmensführung und zur Abwendung von Unternehmensrisiken aus § 93 Abs. 1 AktG ab. Der Vorstand hat die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters zu beachten (§ 93 Abs. 1 S. 2 AktG). Diesen Sorgfaltsmaßstab präzisiert das Aktiengesetz weiter. Der Vorstand muss ein Überwachungssystem einrichten, um Risiken für das Unternehmen frühzeitig erkennen und entsprechende Gegenmaßnahmen treffen zu können (§ 91 Abs. 2 AktG). Dieses System ist mit einem engmaschigen Berichtswesen

auszustatten und zu dokumentieren (LG München, Urteil vom 5.4.2007, Az. 5 HK O 15964/06). Hat der Vorstand kein Risikomanagementsystem eingerichtet oder dieses nicht dokumentiert, liegt darin ein Gesetzesverstoß.

Allerdings steht es mit den gesetzlichen Sorgfaltsanforderungen im Einklang, wenn der Vorstand die Erfüllung von Compliance-Aufgaben an andere Personen im Unternehmen delegiert. Damit kann er sich jedoch nicht vollständig von seiner Verantwortung befreien. Die Gesamtverantwortung für Compliance reduziert sich lediglich auf eine Pflicht zur Überwachung des eingesetzten Compliance-Beauftragten und der eingerichteten Kontrollprozesse sowie zur Verfolgung von festgestellten Rechtsverstößen.

Aufgabe des Aufsichtsrates in einer Aktiengesellschaft ist es, den Vorstand und dessen Geschäftsführung zu überwachen (§ 111 Abs. 1 AktG). Die Überwachung schließt den Rechnungslegungsprozess, das interne Kontrollsystem, das Risikomanagementsystem, die interne Revision und die Funktionstüchtigkeit dieser Systeme ein (§ 107 Abs. 3 S. 2 AktG). Damit der Aufsichtsrat diese Funktion ordnungsgemäß wahrnehmen kann, hat ihn der Vorstand über Risikolage, Risikomanagement und Compliance im Unternehmen zu informieren. Der Aufsichtsrat soll diese Informations- und Berichtspflicht des Vorstands näher konkretisieren (vgl. *Corporate Governance Kodex* in der Fassung vom 15. Mai 2012, Tz. 3.4, vgl.).

Die Pflichten für Vorstände und Aufsichtsratsmitglieder von Genossenschaften orientieren sich an den Vorgaben für Organe von Aktiengesellschaften. Vorstände einer Genossenschaft haben ebenfalls die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters zu beachten und sind zur Vertraulichkeit verpflichtet (§ 34 Abs. 1 GenG). Eine Verletzung ihrer Pflichten kann zu Ersatzansprüchen der Genossenschaft führen (§ 34 Abs. 2 GenG). Für Aufsichtsratsmitglieder der Genossenschaft sind Überwachungs- und Prüfungspflichten in § 38 GenG niedergelegt. Sie können ebenfalls bei Pflichtverletzung zur Verantwortung gezogen werden (§ 41 GenG).

Für Gesellschaften mit beschränkter Haftung (GmbH) findet sich im Gesetz keine explizite Aussage zu Compliance. Für GmbH-Geschäftsführer ist lediglich in § 43 Abs. 1 GmbHG bestimmt, dass sie bei der Geschäftsführung die Sorgfalt eines ordentlichen Geschäftsmannes zu beachten haben. Die Regelungen zum Vorstand einer Aktiengesellschaft werden aber für GmbH-Geschäftsführer weitgehend entsprechend angewendet. Für die Einrichtung eines Compliance-Managements im Unternehmen besteht auch in der GmbH ein weiter Beurteilungsspielraum. Der Geschäftsführer kann aber seine Sorgfaltspflicht verletzen, wenn er über die Einrichtung eines Compliance-Managements im Unternehmen nicht zumindest nachgedacht hat, insbesondere, wenn bereits Rechtsverstöße von Mitarbeitern aufgedeckt wurden.

■ 3.3 Verantwortlichkeiten in Personenunternehmen

Für Einzelkaufleute und Personengesellschaften wie OHG und KG (Personenunternehmen) definiert das Gesetz nur einen allgemeinen Sorgfaltsmaßstab der verantwortlichen Personen beim Abschluss von Geschäften des Unternehmens (§ 347 Abs. 1 HGB). Danach ist Maßstab die Sorgfalt eines ordentlichen Kaufmannes. Die Rechtsordnung erwartet von Kaufleuten, dass sie sich im Geschäftsverkehr auskennen und die einschlägigen rechtlichen Vorgaben sorgfältig beachten. Zwingende Vorschriften für eine bestimmte Organisation des Unternehmens und damit bestimmte Compliance-Anforderungen enthält das Gesetz für Personenunternehmen aber nicht. Der Grund hierfür liegt darin, dass die geschäftsführenden Gesellschafter einer Personengesellschaft und der Inhaber eines Handelsgeschäfts nach dem Leitbild des Gesetzes unbeschränkt auch mit ihrem gesamten privaten Vermögen für unternehmerisches Fehlverhalten haften. Daher müssen sie schon aus Eigeninteresse um Rechtskonformität in ihrem Unternehmen bemüht sein.

Auch wenn das Gesetz nur ausnahmsweise bestimmte Maßnahmen zur Vermeidung von Rechtsverstößen im Unternehmen vorschreibt, lässt sich doch aus den allgemeinen gesellschaftsrechtlichen Verantwortlichkeiten eine Pflicht der Unternehmensführung ableiten, für die Einhaltung der Gesetze in ihren Unternehmen zu sorgen. Diese Pflicht umfasst die Aufgabe, die rechtlichen Risiken zu analysieren und das Unternehmen so zu organisieren, dass systematische Rechtsverstöße ausgeschlossen sind. Dabei können es Größe, Struktur und Geschäftstätigkeit des Unternehmens erforderlich machen, eine Compliance-Struktur aufzubauen. Eine spezifische gesetzliche Pflicht hierfür besteht aber nicht, wenn sich Fehlverhalten in der Unternehmensorganisation durch andere Maßnahmen vermeiden lässt. Allerdings kann die Unternehmensführung nicht für jegliches individuelles Fehlverhalten von Unternehmensmitarbeitern verantwortlich gemacht werden. Wenn ein Unternehmensmitarbeiter bewusst ihm bekannte rechtliche Grenzen überschreitet, kann dies regelmäßig nicht der Unternehmensführung vorgeworfen werden. Sanktionen drohen aber dann, wenn durch Lücken in der Unternehmensorganisation (z. B. fehlende Kontrollen) rechtswidriges Verhalten begünstigt wird.

■ 3.4 Sanktionen für Compliance-Verstöße

Entsprechend ihrer herausgehobenen Verantwortlichkeiten sind die Mitglieder der Führungsorgane in den Unternehmen mit erhöhten Haftungsrisiken konfrontiert. Allerdings hat der BGH erst kürzlich klar gestellt, dass diese Verantwortlichkeit nur gegenüber dem vertretenen Unternehmen, nicht gegenüber außen stehenden Dritten besteht (vgl. Urteil vom 10.7.2012, Az. VI ZR 341/10). Nach Ansicht des BGH folgt aus der Organstellung und der Pflicht zur ordnungsmäßigen Geschäftsführung (z. B. nach § 43 GmbHG oder § 93 AktG) zwar die Pflicht, für die Rechtmäßigkeit des Handelns der Gesellschaft Sorge zu tragen. Eine Garantenstellung und die Pflicht, Vermögensschäden von Personen außerhalb der Gesellschaft abzuwenden, ergibt sich daraus nicht.

Aber auch Mitarbeiter können haftbar sein. Zu unterscheiden ist zwischen einer zivilrechtlichen Haftung einerseits und einer strafrechtlichen Verantwortlichkeit andererseits. Die zivilrechtliche Haftung dient der Kompensation von Schäden, die ein Fehlverhalten bei anderen Personen verursacht hat. Mit Strafe oder Bußgeld setzt der Staat das Gebot zur Einhaltung des Rechts durch. Beide Haftungskategorien können nebeneinander zur Anwendung kommen. So können z. B. Verstöße gegen das Kartellrecht und sonstige strafrechtlich sanktionierten Handlungen gleichfalls Pflichtverletzungen des Arbeitsvertrages darstellen, die einen Schadenersatzanspruch nach §§ 280, 311 Abs. 2, 241 Abs. 2 BGB begründen können.

Realisiert sich ein Risiko in einem konkreten Schaden, so reicht allein dies nach der deutschen Rechtsordnung nur in Ausnahmefällen (z. B. bei Produkthaftung oder bei Haftung für Kartellabsprachen) zur Begründung eines Schadenersatzanspruchs aus. Regelmäßig setzt eine Haftung zusätzlich die persönliche Vorwerfbarkeit eines Fehlverhaltens voraus. Voraussetzungen für eine Haftung sind also regelmäßig:

- Verletzung einer gesetzlichen Pflicht (z. B. Pflicht zur sorgfältigen Geschäftsführung in § 93 AktG) oder einer vertraglichen Pflicht (z. B. arbeitsvertragliche Pflicht),
- Eintritt eines Schadens,
- Ursächlicher Zusammenhang (Kausalität) zwischen Pflichtverletzung und Schadenseintritt und
- Persönliche Vorwerfbarkeit der Pflichtverletzung (Verschulden).

Persönlich vorwerfbar ist ein Verhalten, wenn der Handelnde einen bestimmten Sorgfaltsmaßstab nicht beachtet und damit fahrlässig handelt. Sorgfaltspflichten für Unternehmensverantwortliche finden sich z. B. in den schon erwähnten §§ 93 Abs. 1 S. 1, 116 AktG, § 43 Abs. 1 GmbHG, § 347 Abs. 1 HGB. Die Rechtsprechung hat bereits begonnen, den Sorgfaltsmaßstab der Geschäftsleitungsorgane in Bezug auf ihre Compliance-Verantwortlichkeit für ein Unternehmen zu konkretisieren. Danach beachtet derjenige den Sorgfaltsmaßstab eines gewissenhaften Geschäftsleiters i.S. der §§ 93 Abs. 1 AktG, 43 GmbHG nicht,

der gegen unternehmensinterne Compliance-Richtlinien verstößt (vgl. LG Darmstadt, Urteil vom 14.05.2007, 712 Js 5213/04 - 9 Kls). Der Geschäftsführer einer GmbH muss sich über die wirtschaftliche Lage seines Unternehmens stets vergewissern und für eine Organisation des Unternehmens sorgen, die ihm eine laufende Beobachtung der wirtschaftlichen Lage ermöglicht. Insbesondere bei Anzeichen einer wirtschaftlichen Krise hat er sich einen genauen Überblick über den Vermögensstand zu verschaffen. Tut er dies nicht, handelt er fahrlässig (BGH, Urteil vom 19.6.2012, Az. II ZR 243/11).

Dagegen ist kein Pflichtenverstoß anzunehmen, soweit ein Vorstandsmitglied einer Aktiengesellschaft auf der Grundlage angemessener Informationen zum Wohle des Unternehmens gehandelt hat (sog. business judgement rule gem. § 93 Abs. 1 S. 2 AktG). Dies gilt entsprechend für Geschäftsführer einer GmbH und Aufsichtsratsmitglieder von Aktiengesellschaften. Allerdings muss der Entscheidungsträger zuvor die Grundlagen seiner Entscheidung durch Ausschöpfen sämtlicher verfügbarer Informationsquellen ermitteln sowie Risiken, Vor- und Nachteile seiner Handlungen sorgfältig abschätzen (BGH, Beschluss vom 14.7.2008, Az. II ZR 202/07). Verstöße gegen Gesetz oder Satzung des Unternehmens, insbesondere eine wirtschaftliche Betätigung außerhalb des Unternehmensgegenstands, können nicht durch die business judgement rule gerechtfertigt sein (OLG Düsseldorf, Beschluss vom 9.12.2009, Az. 6 W 45/09).

Auch die Frage der Beweislastverteilung bei Haftungsansprüchen gegen Vorstandsmitglieder wurde durch die Rechtsprechung bereits teilweise konkretisiert. Nach Auffassung des OLG Stuttgart (Urteil vom 25.11.2009, Az. 20 U 5/09) hat die Gesellschaft für einen auf § 93 AktG gestützten Anspruch nur ein möglicherweise pflichtwidriges Verhalten des Vorstandsmitglieds, den Eintritt und die Höhe des entstandenen Schadens sowie die Ursächlichkeit des Vorstandshandelns für den Schaden darzulegen und zu beweisen. Demgegenüber hat das in Anspruch genommene Vorstandsmitglied darzulegen und gegebenenfalls zu beweisen, dass es seiner Sorgfaltspflicht genügt und nicht schuldhaft gehandelt hat.

Kommen die Vorstandsmitglieder einer Aktiengesellschaft ihrer Pflicht zur Einrichtung und Überwachung eines Risikomanagement-Systems im Unternehmen nicht nach, obwohl angesichts der unternehmerischen Risiken die Einrichtung eines solchen Systems angezeigt war, liegt darin eine Pflichtverletzung, die zu einer Haftung nach § 93 Abs. 2 AktG führen kann. Dabei handelt es sich um eine persönliche Haftung des Vorstandsmitglieds. Sie umfasst den gesamten Schaden, den die Gesellschaft aufgrund der fehlenden Kontrollen erleidet.

Die Mitglieder von Vertretungsgremien in Kapitalgesellschaften können sich durch Abschluss einer sog. D&O-Versicherung gegen zivilrechtliche, nicht jedoch gegen strafrechtliche Haftungsrisiken absichern. Durch das im Juni 2009 verabschiedete Vorstandsvergütungsgesetz wurde Vorständen und Aufsichtsräten allerdings auferlegt, einen gewissen Selbstbehalt bei der Haftung zu tragen.

Allgemeine Haftungstatbestände für Unternehmensführer

Haftung wegen persönlichen Fehlverhaltens			
Gesetzliche Vorschrift	Normadressat	Sanktioniertes Fehlverhalten	Sanktion
§ 823 BGB	Jeder Mitarbeiter eines Unternehmens	Verletzung von Rechtsgütern (z. B. Leben, Gesundheit, Eigentum) anderer Personen	Schadenersatz (§ 249 BGB), ggf. Schmerzensgeld, evtl. Kündigung
§§ 280, 311 Abs. 2, 241 Abs. 2 BGB	Jeder Mitarbeiter eines Unternehmens	Verletzung von Pflichten des Arbeitsvertrags	Kündigung, ggf. Schadenersatz
§ 30 OWiG	Person in leitender Stellung in einem Unternehmen (z. B. Geschäftsführer, Prokurist)	Begehung einer Straftat oder einer Ordnungswidrigkeit durch den Normadressaten und dadurch verursachte Pflichtverletzung oder Bereicherung des vertretenen Unternehmens	Geldbuße bis zu 1 Mio. Euro (vom vertretenen Unternehmen zu zahlen) sowie Gewinnabschöpfung nach § 17 Abs. 4 OWiG, Kündigung

Haftung wegen Organisationsverschuldens			
Gesetzliche Vorschrift	Normadressat	Sanktioniertes Fehlverhalten	Sanktion
§ 93 Abs. 2 AktG	Vorstandsmitglieder von Aktiengesellschaften	Verletzung von Sorgfaltspflichten, z. B. Nichteinrichtung einer Compliance-Organisation trotz entsprechender Notwendigkeit	Ersatz des Schadens, der für die AG entsteht
§§ 111, 116 i.V.m. 93 AktG	Aufsichtsratsmitglieder von Aktiengesellschaften	Mangelhafte Wahrnehmung von Aufsichtspflichten	Ersatz des Schadens, der für die AG entsteht
§ 43 Abs. 2 GmbH	Geschäftsführer einer GmbH	Verletzung von Sorgfaltspflichten	Ersatz des Schadens, der für die GmbH entsteht
§ 34 GenG	Vorstandsmitglieder einer Genossenschaft	Verletzung von Sorgfalts- oder Deheimhaltungspflichten	Ersatz des entstandenen Schadens
§ 41 GenG	Aufsichtsratsmitglieder einer Genossenschaft	Verletzung von Sorgfaltspflichten	Ersatz des entstandenen Schadens
§ 130 OWiG	Inhaber eines Unternehmens	Verletzung von Aufsichtspflichten und dadurch ermöglichte Rechtsverstöße durch Unternehmensmitarbeiter	Geldbuße bis zu 1 Mio. Euro



4 Korruptionsprävention

■ 4.1 Korruptionsprävention in Deutschland

Aufgrund Aufsehen erregender Korruptionsfälle in jüngerer Vergangenheit ist die Aufmerksamkeit für strafrechtlich relevantes Verhalten in den Beziehungen von Unternehmen zu Kunden und Lieferanten erheblich gestiegen. Besonders sensibel sind die Beziehungen zwischen Wirtschaft und Verwaltung; denn die Unabhängigkeit und Integrität von Amtsträgern ist ein hohes Gut. Die Vorgaben sind streng. Ein Verstoß kann sowohl für den beschenkten Amtsträger als auch für den Zuwendungsgeber ernste strafrechtliche Konsequenzen haben. Die klassischen Korruptionstatbestände finden sich im deutschen Strafgesetzbuch (StGB) in den §§ 331 bis 338. Sie sehen in schweren Fällen mehrjährige Haftstrafen vor.

Die Bestechung und Bestechlichkeit im rein privatrechtlichen Geschäftserkehr, also von Personen, die keine Amtsträger sind, sind in den §§ 299 bis 302 StGB geregelt. Damit wird die Beeinflussung von Geschäftsbeziehungen durch Gewährung persönlicher Vorteile an Angestellte oder Beauftragte eines geschäftlichen Betriebes sanktioniert. Wiederum können sowohl Vorteilsempfänger als auch Zuwendungsgeber strafbar sein.

4.1.1 Bestechung und Bestechlichkeit von Amtsträgern

Nach § 332 StGB steht die Bestechlichkeit von Amtsträgern unter Strafe. Danach ist strafbar, wer als Amtsträger oder dem öffentlichen Dienst besonders Verpflichteter einen Vorteil für sich oder Dritte als Gegenleistung dafür fordert, sich versprechen läßt oder annimmt, daß er eine Diensthandlung vorgenommen hat oder zukünftig vornehmen wird und dadurch seine Dienstpflichten verletzt. Der Zuwendungsgeber wird spiegelbildlich gemäß § 334 StGB bestraft.

Weiterhin sind gemäß §§ 331, 333 StGB bereits die Vorteilssannahme und Vorteilsgewährung strafbar. Der Tatbestand des § 331 StGB ist erfüllt, wenn ein Amtsträger für

die Dienstaussübung einen Vorteil fordert, sich versprechen läßt oder annimmt. Entsprechend wird nach § 333 StGB bestraft, wer dem Amtsträger für die Dienstaussübung einen Vorteil anbietet, verspricht oder gewährt.

Bei den §§ 331 und 333 StGB bedarf es im Unterschied zu den §§ 332 und 334 StGB keiner konkreten pflichtwidrigen Diensthandlung. Es ist bereits ausreichend, daß der Vorteil für die Ausübung der Diensthandlung allgemein gewährt wird. Somit sind auch Vorteile erfaßt, die »allgemeines Wohlwollen« herbeiführen sollen. Gemäß § 331 Abs. 3 StGB entfällt die Strafbarkeit, wenn die zuständige Behörde die Annahme vorher genehmigt oder der Täter unverzüglich bei ihrer Anzeige erstattet und sich die Annahme genehmigen läßt.

4.1.2 Begriff des Amtsträgers

Die Regelungen der §§ 331 ff. StGB richten sich an Amtsträger. Der Status des Amtsträgers ist in § 11 Abs. 1 Nr. 2 StGB definiert. Dazu zählen eindeutig Beamte und Richter. In der Praxis oft relevant ist die Frage, wie der Begriff der »sonstigen Stelle« in § 11 Abs. 1 Nr. 2c StGB auszulegen ist. Nach Ansicht der Rechtsprechung handelt es sich dabei um staatliche Gesellschaften, die typische klassische öffentliche Aufgaben wahrnehmen, auch wenn diese in ihrer Organisationsform privatisiert sind, wie z. B. die Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH oder die Flughafen München GmbH.

Abgeordnete sowie kirchliche Mandatsträger sind keine Amtsträger im Sinne des § 11 Abs. 1 Nr. 2 StGB. Den Amtsträgern stehen im Rahmen der §§ 331 ff. StGB die für den »öffentlichen Dienst besonders Verpflichteten« gleich. Diese sind in § 11 Abs. 1 Nr. 4 StGB definiert. Mitarbeiter ehemaliger Staatsunternehmen (z. B. Deutsche Telekom AG oder Deutsche Post AG) haben teilweise eine Sonderstellung, die sich aus ihrem ehemaligen Beamtenstatus ableitet. Insoweit entsprechen auch ihre Rechte und Pflichten denen von Beamten.

4.1.3 Bestechung und Bestechlichkeit im geschäftlichen Verkehr

Die §§ 299 bis 304 StGB bilden den rechtlichen Rahmen für die »Angestelltenbestechung«, also die Bestechung und Bestechlichkeit im geschäftlichen Verkehr. Die Vorschrift des § 299 StGB wurde durch das Korruptionsbekämpfungsgesetz 1997 in das StGB aufgenommen und ersetzte den bislang geltenden § 12 UWG. Mit der Übernahme der Vorschrift ins Strafgesetzbuch wollte der Gesetzgeber das Bewusstsein in der Bevölkerung schärfen, dass es sich auch bei Korruption im geschäftlichen Bereich um eine Kriminalitätsform handelt, die nicht nur die Wirtschaft selbst betrifft, sondern Ausdruck eines allgemeinen sozialetisch zu missbilligenden Verhaltens ist. 2002 wurde dann noch § 299 Abs. 3 StGB aufgenommen, der Handlungen im Ausland mit umfaßt.

Ein Angestellter oder Beauftragter eines geschäftlichen Betriebs macht sich nach § 299 Abs. 1 StGB strafbar, wenn er einen Vorteil fordert, sich versprechen läßt oder annimmt und als Gegenleistung dafür im Wettbewerb den Bestechenden beim Bezug von Waren oder gewerblichen Leistungen bevorzugt. Entsprechend wird spiegelbildlich nach § 299 Abs. 2 StGB bestraft, wer einem Angestellten oder Beauftragten einen Vorteil als Gegenleistung für eine Bevorzugung anbietet, verspricht oder gewährt.

4.1.4 Begriff des »Angestellten« und des »Beauftragten«

Angestellte sind Personen, die in einem Dienst- oder Auftragsverhältnis zum Inhaber eines Geschäftsbetriebes stehen und weisungsgebunden sind. Beispiele sind der klassische Arbeitnehmer oder aber auch angestellte Geschäftsführer einer GmbH. Beauftragte sind solche Personen, die keine Angestellten sind, aber aufgrund ihrer Stellung berechtigt und verpflichtet sind, für den Geschäftsbetrieb tätig zu werden. Hierzu zählen z. B. Berater und Handelsvertreter. Der Begriff des Beauftragten ist nach geltender Rechtsprechung weit auszulegen.

Vom Tatbestand des § 299 Abs. 1 StGB ausgenommen sind die Geschäftsinhaber.

4.1.5 Abgrenzung zwischen legaler Kundenpflege und Korruption

Vorgaben zur Annahme von Vorteilen finden sich für Angehörige des öffentlichen Dienstes auch außerhalb des Strafrechts. Nach § 71 Abs. 1 des Bundesbeamtengesetzes (BBG, vgl.) und § 3 Abs. 2 des Tarifvertrages für den öffentlichen Dienst (TVöD) dürfen Beschäftigte der Bundesverwaltung ohne Zustimmung des Arbeitgebers keine Belohnungen, Geschenke oder sonstigen Vorteile annehmen. Dennoch sind Aktivitäten zur Kundenbindung oder Kundengewinnung weiterhin zulässig. Damit ergeben sich in der Praxis vielfältige Abgrenzungsschwierigkeiten zwischen erlaubter Kundenpflege einerseits und verbotener Korruption andererseits. Eine vollständige Sicherheit im Umgang mit Zuwendungen und deren Annahme gibt es nicht, vielmehr bleiben zahlreiche Grauzonen, da das Strafgesetzbuch keinerlei Wertegrenzen enthält und bereits geringfügige Zuwendungen eine Strafbarkeit auslösen können.

Generell können sich Beschäftigte der Bundesverwaltung die Annahme von Belohnungen und Geschenken von der zuständigen Dienststelle genehmigen lassen. Kleinere Aufmerksamkeiten in Form von Sachgeschenken bis 25,- Euro können jedoch als stillschweigend genehmigt angesehen werden. Dies gilt z. B. für geringwertige Dienstleistungen wie der Mitnahme im Taxi vom Flughafen zur Besprechung oder für Reklameartikel wie Kugelschreiber. Geldgeschenke sind dagegen niemals zulässig. Für Bewirtungen und Einladungen gilt die Wertgrenze von 25,- Euro nicht. Hier kann auch ein höherer Gegenwert unbedenklich sein, wenn die Bewirtung üblich und angemessen ist. Die Grundsätze für die Annahme von Belohnungen und Geschenken in der Bundesverwaltung sind in einem Rundschreiben des Bundesinnenministeriums vom 8. November 2004 niedergelegt. In einzelnen Behörden können jedoch restriktivere Regelungen gelten.

Bei der Abgrenzung von Korruption und legaler Kundenpflege sind nachfolgende Aspekte zu beachten:

Sozialadäquanz der Zuwendung: Zuwendungen sind sozialadäquat, wenn sie im Rahmen von Höflichkeit und

Gefälligkeit sowohl sozial üblich als auch unter Gesichtspunkten des Rechtsgüterschutzes allgemein gebilligt sind. Beispiele sind moderate Bewirtung mit Speisen und Getränken während einer Besprechung oder auch das Bereitstellen von Schreibmaterialien (typischerweise Block und Kugelschreiber mit eigenem Firmen-Logo). Es ist nach den Umständen des Einzelfalls zu beurteilen, ob Art und Umfang des gewährten Vorteils als ungeeignet zur unlauteren Beeinflussung angesehen werden kann.

Sozialadäquate Zuwendungen von geringfügigem Wert sind in der Regel sowohl bei Amtsträgern als auch bei Privaten zulässig. Für Amtsträger ist allerdings ein deutlich engerer Rahmen anzusetzen, da hier die Zuwendung von Vorteilen schon dann strafbar sein kann, wenn sie im Sinne eines »Anfütterns« bzw. einer Klimapflege zugunsten des »allgemeinen Wohlwollens« im Hinblick auf die Amtsstellung – »für die Dienstausbübung« – erfolgt.

Trennungsprinzip: Zuwendungen sollten klar und eindeutig von offenen geschäftlichen Transaktionen bzw. Diensthandlungen getrennt sein. Es ist kritisch, wenn eine Zuwendung im Zusammenhang mit einer konkreten Geschäftsbeziehung oder zur Anbahnung eingeräumt wird. Dies gilt umso mehr, wenn Vorteile einzelnen oder einer kleinen Gruppe von Beschäftigten eingeräumt werden, die mit diesem Geschäft unmittelbar in Verbindung stehen oder Entscheidungsträger im Hinblick auf diese Transaktion sind.

Verboten sind Zuwendungen sowohl gegenüber Amtsträgern als auch im geschäftlichen Verkehr, wenn nachfolgende Merkmale zutreffen:

- Vorteile, auf welche kein Anspruch besteht, werden konkret eingefordert;
- Zuwendungen, bei denen das Trennungsprinzip nicht gewahrt ist;
- Zuwendungen, die für eine dienstliche Tätigkeit bzw. im geschäftlichen Verkehr gewährt werden, wenn der Anschein einer Unrechtsvereinbarung oder unlauteren Bevorzugung entstehen könnte (z. B. bei einem potentiellen Interessenkonflikt);
- Geldgeschenke oder geldähnliche Geschenke (z. B. auch Darlehen, Wertpapiere, die Stundung einer Schuld oder der Verzicht auf einen Anspruch);
- Zuwendungen sexueller oder anstößiger Natur;
- Außergewöhnliche oder luxuriöse Einladungen mit sehr hohem Kostenaufwand.

Weitere Hinweise finden sich im »Kodex zur Abrenzung legaler Kundenpflege und Korruption« des Arbeitskreises Corporate Compliance im Institut for European Affairs sowie in einem »Fragen- und Antwortenkatalog zur Korruptionsprävention«, der vom Initiativkreis Korruptionsprävention Wirtschaft/Bundesverwaltung herausgegeben wurde.

■ 4.2 Korruptionsprävention im US-Recht: Foreign Corrupt Practices Act

Der Foreign Corrupt Practices Act (FCPA) wurde 1977 als Bundesgesetz in den USA erlassen (<http://www.justice.gov/criminal/fraud/fcpa>). Er verbietet Zuwendungen an ausländische Amtsträger (»foreign officials«), die den Zweck haben, den Zuschlag für ein Geschäft zu bekommen oder eine Geschäftsbeziehung aufrechtzuerhalten (»for the purpose of obtaining or retaining business for or with, or directing business to any person«). Untersagt werden jegliche Zahlungen, Angebote von Geld oder anderen Wertgegenständen (»anything of value«) zum Zweck der Korruption.

4.2.1 Anwendungsbereich

Der Anwendungsbereich des FCPA ist weit auszulegen, das Gesetz hat extraterritoriale Wirkung, kann also auch deutsche Unternehmen betreffen (vgl. dazu unten 4.2.7). Dem Strafvollzug durch die US Behörden unterliegen US-börsennotierte Unternehmen («issuer») sowie Privatpersonen, Unternehmen, Beamte, Angestellte oder Anteilseigner, die entweder in den USA ansässig oder nach den Gesetzen der USA organisiert sind («domestic concern»). Entsprechend gilt der FCPA auch für alle ausländischen Tochterfirmen in USA gelisteter Konzerne sowie auch für deren Angestellte, Anteilseigner oder jede sonstige Mittelspersonen, die im Auftrag des Unternehmens oder seiner ausländischen Töchter handeln. Er gilt auch, wenn diese Dritte anstiften, die Bestimmungen des Gesetzes zu verletzen.

4.2.2 Zuständige Strafverfolgungsbehörden

Das US-Justizministerium («Department of Justice», DOJ) ist für die straf- und zivilrechtliche Verfolgung von Verstößen zuständig. Für US-börsennotierte Unternehmen ist die US Börsenaufsicht («US Securities and Exchange Commission», SEC) für die zivilrechtliche Ahndung verantwortlich. In Zusammenarbeit beider Behörden ist ein sehr aktueller Leitfaden mit umfangreichen Erläuterungen zum FCPA entstanden («A Resource Guide to the U.S. Foreign Corrupt Practices Act» vom November 2012)

4.2.3 Begriff des ausländischen Amtsträgers

Das Verbot des FCPA erstreckt sich ausschließlich auf Bestechungszahlungen an ausländische Amtsträger («Foreign Official»), eine ausländische politische Partei oder einen Parteivertreter oder einen Kandidaten für ein politisches Amt im Ausland. »Foreign Official« ist jeder Staatsbeamte oder Angestellte einer ausländischen Regierung, einer internationalen Organisation, einer Abteilung oder Dienststelle sowie jede Person im öffentlichen Dienst. Rang und Position dieser Person spielen dabei keine Rolle. Darüber hinaus gelten auch Angestellte

von Unternehmen, bei denen die öffentliche Hand eine erhebliche Beteiligung hält, als Amtsträger, selbst wenn diese Unternehmen in ihrem Heimatland privatrechtlich organisiert sind. Mitarbeiter dieser Unternehmen sollten im Geschäftsverkehr mit US-amerikanischen Partnern entsprechend sensibilisiert sein. Der Begriff des Amtsträgers im US-Recht ist also nicht identisch mit dem der §§ 11 Abs. 1 Nr. 2 und Nr. 4, 331 ff StGB. Die Bestechlichkeit bzw. die Bestechung im geschäftlichen Verkehr, im deutschen StGB in den §§ 299 ff. geregelt, wird unter dem FCPA nicht verfolgt.

4.2.4 Inhalt des FCPA

Das Verbot des FCPA umfaßt jegliche Zahlungen oder sonstige Zuwendungen von Werten, die zum Ziel haben, einem Unternehmen oder einer Person einen Geschäftsabschluss zu verschaffen, eine Geschäftsbeziehung zu verlängern oder ein Geschäft an jemanden zu vermitteln. Dieses Tatbestandsmerkmal wird vom US Justizministerium weit ausgelegt. Dabei geht es nicht nur um Geschäfte, die direkt mit einer ausländischen Regierung oder einem ausländischen Staatsunternehmen in Bezug stehen, sondern es fallen alle Geschäfte darunter, auch mit nichtstaatlichen Organisationen, Unternehmen und Privatpersonen.

Die Zuwendung muß mit Bestechungsvorsatz («corrupt intent») erfolgen. Sie muss den Zweck haben, den Empfänger dazu zu bringen, seine offizielle Stellung zu missbrauchen, um dem Zuwendenden oder einer dritten Partei den Zuschlag für ein Geschäft zu geben. Dabei kommt es nicht darauf an, daß der beabsichtigte Erfolg auch eintritt, bereits das Angebot oder Versprechen einer solchen Zahlung kann eine Verletzung des Gesetzes bedeuten.

4.2.5 Verantwortung für Dritte

Eine besondere Bedeutung kommt der Behandlung von Schmiergeldzahlungen durch Dritte («intermediaries») zu. Es ist nach dem FCPA verboten, eine Zahlung an Dritte zu leisten, mit dem Wissen («knowing»), daß diese ganz oder teilweise an einen ausländischen Amtsträger

weitergeleitet wird. »Wissen« wird hierbei weit ausgelegt und umfasst vorsätzliches Nichtwissen genauso wie bewußte Nichtbeachtung von Umständen, die als ausreichende Warnsignale (s.u.) für eine illegale Handlung angesehen werden könnten.

Der Personenkreis der »Dritten« im Sinne des FCPA ist sehr weit und umfasst Subunternehmer, Partner bei Joint Ventures, Agenten, Handelsvertreter und andere Geschäftspartner. Um zu vermeiden, daß man für das Handeln eines Dritten verantwortlich gemacht wird, wird verlangt, den Dritten einer sorgfältigen Prüfung (»Due Diligence«) zu unterziehen. Unternehmensvertreter sollten daher sicherstellen, daß sie nur mit zuverlässigen Geschäftspartnern mit gutem Ruf in Geschäftsbeziehung treten. In der Regel beinhaltet diese Prüfung eine Zuverlässigkeitsprüfung (»Background Check«), d.h. es werden umfangreiche Hintergrundinformationen zu strafrechtlich relevanter Historie, Bonität und Reputation des Dritten und seiner Führungskräfte abgefragt. Darüber hinaus sind Unternehmen angehalten, bestimmte Warnsignale, sog. »Red Flags« zu identifizieren. Red Flags sind z. B. eine außergewöhnlich hohe Vergütung, mangelnde Qualifikation des Dritten für die vertraglich vereinbarte Leistung, ein zweifelhafter Ruf, das Verlangen einer Behörde im Ausland, den Dritten für Geschäfte einzuschalten, besonders nahe Beziehungen (familiär, persönlich oder geschäftlich) des Dritten zu maßgeblichen Regierungsvertretern, ungewöhnlicher Zahlungsmodus, intransparente Spesenabrechnung oder Buchführung, oder das Einschalten weiterer, verdeckter oder nicht näher zu ermittelnder Dritter durch den Dritten.

4.2.6 Sanktionen

Sowohl gegen die betroffenen Unternehmen als auch gegen beteiligte Einzelpersonen können empfindliche Strafen verhängt werden. Einzelpersonen können Geldstrafen bis zu 100.000 USD pro Verstoß und Gefängnisstrafen von bis zu 10 Jahren erhalten. Dem Unternehmen können Geldstrafen bis zu 2 Mio. USD pro Verstoß auferlegt werden. Weiterhin können hohe Zivilstrafen (»civil penalties«) verhängt werden.

Darüber hinaus kann ein Verstoß andere nachteilige Folgen nach sich ziehen, wie z. B. die Suspendierung oder den Ausschluss von Regierungsverträgen, Widerruf oder Suspendierung von Exportlizenzen. Nicht selten drohen ferner Klagen seitens der Aktionäre sowie langwirkende Beeinträchtigung des guten Rufs des Unternehmens im In- und Ausland.

4.2.7 Anwendbarkeit für deutsche Unternehmen

Deutsche Unternehmen, die sich in den USA wirtschaftlich betätigen oder Geschäftsbeziehungen mit US Unternehmen unterhalten, müssen sich über die weit reichende Bedeutung und die extraterritoriale Wirkung des FCPA im Klaren sein. Dieser findet unmittelbar Anwendung, wenn die Geschäftstätigkeit in den USA in Form einer US-Tochter ausgeübt wird. Seit 1998 gilt der FCPA darüber hinaus auch für ausländische Gesellschaften und Staatsbürger, die direkt oder indirekt Korruptionszahlungen über die USA leiten oder sonstige Aktivitäten ausüben, die nach dem FCPA untersagt sind. Dabei kommt es nicht darauf an, daß tatsächlich ein US-Bankkonto benutzt wird oder die Zahlung auf sonstige Weise in den USA verbucht wird. Nach geltender Praxis reicht es bereits aus, daß die Zahlung über einen in den USA gelegenen Server geleitet wird.

■ 4.3 Korruptionsprävention im britischen Recht: UK Bribery Act

Der neue UK Bribery Act (UKBA) trat in Großbritannien am 01.07.2011 in Kraft. Für deutsche Unternehmen kann er schon dann Bedeutung erlangen, wenn eine Geschäftsbeziehung zu einem Unternehmen in Großbritannien besteht. Der UKBA ist vergleichbar mit dem US-amerikanischen Foreign Corrupt Practices Act (FCPA), jedoch sind seine Vorschriften noch deutlich strenger. Der UKBA sanktioniert vor allem Korruption im Ausland, beschränkt dies aber im Unterschied zum FCPA nicht auf Amtsträger. In verschiedenen Publikationen wird der UKBA gerne als das »weltweit wohl härteste Anti-Korruptionsgesetz« bezeichnet.

Allerdings fehlen aufgrund der kurzen Dauer seit Inkrafttreten derzeit noch Erfahrungswerte für die Umsetzung durch Behörden und Rechtsprechung.

4.3.1 Inhalt des UKBA

Strafbar nach dem UKBA sind vier unterschiedliche Tatbestände:

- die aktive Bestechlichkeit im privaten und im öffentlichen Bereich (§ 1 UKBA: »... person offers, promises or gives a financial or other advantage to another person...«), unabhängig davon, ob der Vorteil durch den Bestechenden selbst oder eine dritte Person gewährt wird;
- die passive Bestechlichkeit (§ 2 UKBA: »... person requests, agrees to receive or accepts a financial or other advantage...«) im Falle der Annahme eines Vorteils als Gegenleistung für unrechtmäßiges Verhalten oder bei Untätigkeit trotz Kenntnis rechtswidrigen Handelns, ohne dass vorsätzliches Handeln des Täters notwendig wäre;
- die Bestechung ausländischer Amtsträger (§ 6 UKBA: »Bribery of foreign public officials«) mit dem Ziel, den Amtsträger in seiner Funktion zum Erreichen eines geschäftlichen Vorteils zu beeinflussen;
- Unterlassen präventiver Massnahmen zur Verhinderung von Korruption durch Firmen (§ 7 UKBA: »Failure of commercial organisations to prevent bribery«).

Diese Straftatbestände des UKBA sind mit den deutschen Straftatbeständen der Bestechung (§ 334 StGB) und Bestechlichkeit (§ 332 StGB) sowie Bestechlichkeit und Bestechung im geschäftlichen Verkehr (§ 299 StGB) vergleichbar.

4.3.2 Zuständige Strafverfolgungsbehörden

Die britische Strafverfolgungsbehörde für schwere Betrugsdelikte und Korruption »Serious Fraud Office« (»SFO«) ist für die Verfolgung von Straftaten nach UKBA zuständig, unabhängig davon, ob sie von einer natürlichen Person oder einem Unternehmen begangen wurden.

4.3.3 Begriff des ausländischen Amtsträgers

Mit »ausländischer Amtsträger« sind nicht nur gewählte oder ernannte Inhaber eines legislativen, exekutiven oder judikativen Amtes außerhalb Großbritanniens gemeint, sondern auch solche Personen, die eine öffentliche Funktion für ein Land außerhalb Großbritanniens ausüben oder für eine öffentliche internationale Organisation tätig sind. Vergleichbar ist dies mit den Regelungen des US-amerikanischen FCPA und der OECD Konvention gegen Korruption von 1997.

4.3.4 Präventive Massnahmen zur Verhinderung von Korruption

Mit Einführung des UKBA kommt der Korruptionsprävention entscheidende Bedeutung zu. Nach § 7 UKBA sind jetzt auch Unternehmen selbst strafbar, wenn eine rechtswidrige Tat von einer mit dem Unternehmen »verbundenen Person« zugunsten des Unternehmens begangen wurde und das Unternehmen es versäumt hat, geeignete präventive Massnahmen zur Vermeidung dieser Tat zu ergreifen. Zur Frage, was »geeignete Vorkehrungen zur Vermeidung von Korruption« sind, hat das britische Justizministerium erste Orientierungshilfen veröffentlicht. Es werden die nachfolgenden sechs Prinzipien definiert:

- Risikobewertung: Das Unternehmen muß Korruptionsrisiken, die sich aus dem Geschäft ergeben können, regelmäßig und kontinuierlich identifizieren, untersuchen und bewerten.
- Top Level Commitment: Die oberste Führungsebene gibt klare Anweisungen, daß Korruption nicht akzeptiert und verfolgt wird, und etabliert eine Unternehmenskultur, die sich gegen Korruption in jeglicher Form wendet.

- Klare und praktikable Richtlinien und Prozesse: Das Unternehmen definiert Handlungsanweisungen und Policies für den Umgang mit Korruptionsrisiken. Diese müssen einfach zugänglich, verständlich und klar sein. Es werden Prozesse definiert für erforderliche Entscheidungen sowie auch zur Meldung von Verstößen oder Verdachtsfällen.
- Due Diligence: Das Unternehmen wählt Geschäftspartner mit der gebotenen Sorgfalt aus. Geschäftsbeziehungen werden auf ihre Vereinbarkeit mit den unternehmenseigenen Anti-Korruptionsrichtlinien hin geprüft.
- Effektive Implementierung und Kommunikation (intern und extern): Das Unternehmen etabliert in seiner gesamten Organisation ein umfassendes Anti-Korruptionsprogramm. Dies beinhaltet eine effektive Kommunikation der Inhalte und Prozesse ebenso wie die Durchführung entsprechender Trainingsmaßnahmen.
- Überwachung und Überprüfung: Das Unternehmen überwacht laufend die Wirksamkeit der getroffenen Antikorruptionsmaßnahmen. Dabei ist nicht nur sicherzustellen, daß Verstöße gefunden werden, sondern auch, daß Schwachstellen und notwendiger Verbesserungsbedarf identifiziert werden.

Mit einem [Quick Start Guide](#) und weiteren Richtlinien hat das britische Justizministerium zentrale Dokumente zur Interpretation des UKBA im Internet zugänglich gemacht.

4.3.5 Verantwortung für Dritte

Im Gegensatz zum FCPA enthält der UK Bribery Act weder eine spezielle Regelung für das Verhalten Dritter, noch ist der Begriff des »Dritten« klar definiert. Unternehmen haften jedoch auch dann, wenn ein Geschäftspartner oder andere »verbundene Personen« gegen den UKBA verstoßen. Unter verbundenen Personen sind nach § 8 UKBA sowohl natürliche als auch juristische Personen zu verstehen. Dies können Mitarbeiter oder Vertreter des Unternehmens, Personen oder Betriebe, die Leistungen für dieses Unternehmen erbringen, oder aber eine Tochtergesellschaft oder Niederlassung dieses Unternehmens sein. Nach weit verbreiteter Ansicht zählen dazu auch externe Berater wie z. B. Wirtschaftsprüfer oder Anwälte. Entsprechend wichtig ist die Einführung präventiver Maßnahmen, insbesondere auch einer Due Diligence für Dritte (vgl. Ziffer 3.3.4).

4.3.6 Sanktionen

Sowohl gegen die betroffenen Unternehmen als auch gegen beteiligte Einzelpersonen können empfindliche Strafen verhängt werden: Einzelpersonen müssen mit Haftstrafen bis zu 10 Jahren oder mit einer der Höhe nach nicht begrenzten Geldstrafe rechnen. Gegen Unternehmen können Bußgelder in unbegrenztem Umfang verhängt werden.

Darüber hinaus kann ein Verstoß sowie auch schon der bloße Verdacht, daß ein Verstoß vorliegt, auch andere für den Geschäftsbetrieb nachteilige Folgen nach sich ziehen. Dazu gehören z. B. der Ausschluß von Regierungsaufträgen, der Verlust des Ansehens auf dem Markt, umfangreiche Ermittlungen der britischen Strafverfolgungsbehörden, Kosten der Rechtsverteidigung.

4.3.7 Anwendbarkeit für deutsche Unternehmen

Aufgrund fehlender Erfahrungen mit dem relativ neuen Gesetz ist noch nicht ganz klar, wie weit der Arm der britischen Strafverfolgungsbehörden zukünftig reichen und wie die Verfolgungspraxis aussehen wird. Eindeutig betroffen sind Unternehmen, die Zweigniederlassungen, Produktionsstätten oder Repräsentanzbüros in Großbritannien unterhalten. Für die Strafbarkeit juristischer Personen ist es bereits ausreichend, wenn sie in Geschäftsverbindung mit Unternehmen in Großbritannien stehen bzw. auf dem britischen Markt vertreten sind, auch wenn sie dort weder Sitz noch Niederlassung unterhalten. Dabei ist es unerheblich, ob die unrechtmäßige Handlung in oder außerhalb von Großbritannien erfolgt (§ 12 UKBA: »... territorial application«).

Voraussetzung für die Strafbarkeit natürlicher Personen ist, dass die Korruptionshandlung entweder auf britischem Gebiet stattgefunden hat oder der Täter eine enge Verbindung zu Großbritannien hat, etwa als britischer Staatsbürger oder Einwohner Großbritanniens.

■ 4.4 Handlungsempfehlung

Deutsche Unternehmen, die Geschäftsbeziehungen in Großbritannien oder USA unterhalten, haben mit dem FCPA und UKBA deutlich erhöhte Risiken. Die Einrichtung eines Anti-Korruptionsprogramms, sofern noch nicht vorhanden, sollte mit höchster Priorität vorangetrieben bzw. bestehende interne Antikorruptions-Richtlinien entsprechend überarbeitet werden. Darüber hinaus sollten alle Mitarbeiter zusätzlich mit den strengen ausländischen Regeln und deren Folgen vertraut gemacht werden.

5 Wettbewerbsrecht

Das Wettbewerbsrecht stellt die Regeln auf, die Unternehmen im gegenseitigen Konkurrenzkampf einzuhalten haben. Im Mittelpunkt steht das Gesetz gegen den unlauteren Wettbewerb (UWG). Es dient dem Schutz von Mitbewerbern, Verbrauchern, sonstigen Teilnehmern am Marktgeschehen und dem Interesse der Allgemeinheit an einem freien, unverfälschten und fairen Wettbewerb um das Angebot und die Nachfrage von Produkten und Dienstleistungen

(§ 1 UWG). Die Bestimmungen in §§ 3 Abs. 1, 4, 5, 5a, 6, 7 UWG enthalten gesetzliche Verbote bestimmter Geschäftspraktiken (»unlautere geschäftliche Handlungen«). In den §§ 8 ff. UWG werden die Rechtsfolgen geregelt, die wettbewerbsrechtliche Verstöße nach sich ziehen. Neben dem UWG gibt es noch eine Reihe von weiteren Gesetzen, die für bestimmte Branchen oder bestimmte Sachverhalte Ergänzungs- oder Sonderregeln enthalten. Beispiele sind das Heilmittelwerbegesetz (HWG) oder die Preisangabenverordnung (PAngV).

Jede geschäftliche Handlung eines Unternehmers, die den Wettbewerb »spürbar« beeinträchtigen kann, ist nach den gesetzlichen Bestimmungen des Wettbewerbsrechts zu beurteilen. Das UWG und weitere flankierende Gesetze regeln aber im Wesentlichen nur, welches Verhalten verboten bzw. in der Sprache des Wettbewerbsrechts »unzulässig« ist. Grundsätzlich gilt: was nicht verboten ist, ist wettbewerbsrechtlich erlaubt.

■ 5.1 Wesentliche Unlauterkeitstatbestände

Die Generalklausel des § 3 (1) UWG definiert: »Unlautere geschäftliche Handlungen sind unzulässig, wenn sie geeignet sind, die Interessen von Mitbewerbern, Verbrauchern oder sonstigen Marktteilnehmern spürbar zu beeinträchtigen.« Seit der letzten Reform des UWG wird diese Generalklausel primär durch eine sogenannte »schwarze Liste« konkretisiert, die im Anhang zu § 3 UWG hinterlegt ist. Bevor andere Tatbestände im UWG geprüft werden,

ist der Katalog der 30 dort aufgezählten Handlungen zu beachten. Diese sind gegenüber Verbrauchern stets unzulässig (z. B. Lockvogelangebote), gegenüber anderen Unternehmen aber unter Umständen erlaubt. Das Gesetz trägt damit den Vorgaben des EU-Gesetzgebers und einem gestuften Schutzbedürfnis von Konkurrenzunternehmen und Verbrauchern Rechnung.

Neben der Generalklausel führt das Gesetz in §§ 4 ff. UWG weitere Beispiele geschäftlicher Handlungen auf, die generell gegenüber allen Marktteilnehmern verboten sind. Hierzu gehören:

1. Beeinträchtigung der Entscheidungsfreiheit der Verbraucher oder sonstiger Marktteilnehmer durch Ausübung von Druck, in menschenverachtender Weise oder durch sonstigen unangemessenen unsachlichen Einfluss (§ 4 Nr. 1 UWG).

Unter der unzulässigen Ausübung von Druck versteht man das Zufügen oder die Androhung von Nachteilen, die die Rationalität der Entscheidung völlig in den Hintergrund treten lässt. Dies kann durch physischen Zwang (körperliche Gewalt, Freiheitsberaubung: »wer nicht unterschreibt, kommt hier nicht raus«), psychischen oder moralischer Druck (»wenn Sie nicht kaufen, muss ich alle Mitarbeiter entlassen«), rechtswidrige Drohung (Erpressung, Nötigung) oder das Erzeugen von Angst (»wenn Sie unser Produkt nicht nutzen, werden sie krank«) geschehen.

2. Ausnutzung geistiger oder körperlicher Gebrechen, der geschäftlichen Unerfahrenheit, des Alters, der Leichtgläubigkeit, der Angst oder der Zwangslage von Verbrauchern (§ 4 Nr. 2 UWG). Hierher gehören z. B. Fälle, in denen Kinder durch gezielte Werbung als Verkaufsförderer instrumentalisiert werden sollen.
3. Schleichwerbung (§ 4 Nr. 3 UWG): Unter Schleichwerbung versteht man die von einem Unternehmer finanzierte Werbung, die vom Adressaten gar nicht

als Werbung erkannt werden kann. Der werbliche Charakter einer Tätigkeit kann zum Beispiel verschleiert werden, indem ein Kontakt unter einem nicht geschäftlichen Vorwand hergestellt wird, um den Betroffenen dann mit einem geschäftlichen Angebot zu konfrontieren (zum Beispiel ein als Meinungsfrage getarnter Werbeanruf). Auch getarnte Werbung (Aufmachung als wissenschaftliche oder fachliche Äußerung, amtliches Aussehen von Werbematerial) fällt hierunter.

4. Unklarheiten bei der Bewerbung oder Durchführung von besonderen Verkaufs- oder Vertriebsaktionen (§ 4 Nr. 4 UWG): Bei der Durchführung von Verkaufsfördermaßnahmen wie Preisnachlässen, Zugaben oder Geschenken müssen die Bedingungen der Inanspruchnahme klar und transparent sein. Hierzu gehört auch, dass eventuelle Beschränkungen zeitlicher Art oder der zur Verfügung stehenden Menge wahrheitsgemäß angegeben werden müssen.
5. Unklarheiten bei Preisausschreiben oder Gewinnspielen (§ 4 Nr. 5 UWG): Preisausschreiben, Gratisverlosungen und Gewinnspiele müssen von der Lotterie abgegrenzt werden. Bei einer Lotterie muss der Teilnehmer einen eigenen Einsatz aufbringen, die Teilnahme an Preisausschreiben oder Gewinnspielen erfordert einen solchen Einsatz nicht. Lotterien müssen behördlich genehmigt werden. Wer ohne eine solche Genehmigung Lotterien veranstaltet, macht sich u.U. sogar strafbar. Gewinnspiele und Preisausschreiben können wettbewerbswidrig sein, wenn mit ihnen in irreführender Weise der Erwerb einer Ware oder einer Leistung gekoppelt wird oder eine unsachliche Einflussnahme auf die Entscheidungsfreiheit des Verbrauchers stattfindet (§ 4 Nr. 6 UWG). Auch die Ausübung eines psychologischen Kaufzwangs und die Irreführung über Teilnahmebedingungen oder Gewinne sind unzulässig.
6. Herabsetzung eines Konkurrenten oder seiner Waren oder Dienstleistungen (§ 4 Nr. 7 UWG): Es ist wettbewerbsrechtlich nicht zulässig, die Kennzeichen (Marken), Produkte oder persönlichen oder geschäftlichen Verhältnisse eines Mitbewerbers herabzusetzen oder zu verunglimpfen. Sachliche Kritik an einem Mitbewerber oder dessen Produkten ist erlaubt, unsachliche Kritik hingegen nicht. Wahre Tatsachenbehauptungen sind – wenn sie sich geschäftsschädigend auswirken können – nur dann zulässig, wenn ein sachlich berechtigtes Informationsinteresse besteht und die Kritik in angemessener Weise geäußert wird.
7. Äußerung oder Weitergabe von Unwahrheiten (Gerüchten) über den Konkurrenten oder seine Waren oder Dienstleistungen (§ 4 Nr. 8 UWG): Das UWG sieht einen Schutz nur vor unwahren geschäftsschädigenden Tatsachenbehauptungen vor. Negative, aber wahre Tatsachenbehauptungen sind hingegen zulässig. Auch reine Meinungsäußerungen fallen nicht unter den Schutz des UWG. Eine Abgrenzung in diesem Bereich fällt im Einzelfall oft schwer. Da jedoch unwahre, schädigende Behauptungen unter Umständen auch strafrechtlich relevant sein können, ist hier größte Vorsicht geboten.
8. Nachahmung von Waren oder Dienstleistungen eines Konkurrenten unter bestimmten Umständen (§ 4 Nr. 9 UWG): Das Anbieten von Nachahmerprodukten ist dann wettbewerbswidrig, wenn über die ursprüngliche Herkunft getäuscht wird, die Wertschätzung der nachgeahmten Ware unangemessen ausgenutzt oder beeinträchtigt wird oder die für die Nachahmung erforderlichen Kenntnisse oder Unterlagen unredlich erlangt wurden.
9. Gezielte Behinderung von Konkurrenten (§ 4 Nr. 10 UWG): Unter Behinderung versteht man die Beeinträchtigung der wettbewerbliehen Entfaltungsmöglichkeiten eines Mitbewerbers. Darunter fallen alle Bereiche der geschäftlichen Tätigkeit, z. B. Vertrieb, Einkauf, Produktion, Marketing, Forschung/Entwicklung, Personalrekrutierung und -entwicklung. Voraussetzung für die wettbewerbsrechtliche Unzulässigkeit

ist ein gezieltes Vorgehen in Behinderungsabsicht. Die Maßnahme muss also in erster Linie auf die Störung und Behinderung des Mitbewerbers gerichtet sein. Unter diesen Tatbestand fallen beispielsweise Boykottaufrufe oder gezieltes Überkleben oder Verunstalten von Werbeplakaten eines Konkurrenten.

Eine gezielte Behinderung von Konkurrenten kann auch in der aggressiven Abwerbung von Mitarbeitern bestehen. Dem kommt in einer durch zunehmenden Fachkräftemangel bedrohten Branche wie der ITK-Branche zunehmende Bedeutung zu. Es ist grundsätzlich nicht verboten, sich als attraktiver Arbeitgeber zu präsentieren und durch eigene Anziehungskraft Mitarbeiter von Konkurrenzunternehmen für sich zu gewinnen. Selbst ein planwidriges Abwerben von Mitarbeitern anderer Unternehmen, z. B. erste Informationsanrufe eines Headhunters, sind in der Regel zulässig. Die Grenze zur Wettbewerbswidrigkeit wird jedoch überschritten, sobald ein verwerflicher Zweck oder der Einsatz verwerflicher Mittel hinzutreten. So ist eine Abwerbung wettbewerbswidrig, wenn sie in Behinderungsabsicht vorgenommen wird. Dies wäre z. B. bei der Abwerbung von Mitarbeitern der Fall, die beim aufnehmenden Unternehmen gar nicht benötigt werden, dem abgebenden Unternehmen aber fehlen sollen. Unzulässig ist es auch, wenn durch die Kontaktaufnahme zu Mitarbeitern des Konkurrenten dessen Geschäftsablauf unangemessen beeinträchtigt oder der Konkurrent beim Abwerbversuch herabgewürdigt wird (vgl. LG Heidelberg, Urteil v. 23.5.2012 - 1 S 58/11). Im zitierten Urteil des LG Heidelberg hatte ein Arbeitnehmer zwei Mitarbeiter eines Konkurrenzunternehmens über XING angesprochen und dabei den Arbeitgeber der Angesprochenen in schlechtem Licht dargestellt.

Als gezielte Behinderung von Konkurrenten ist schließlich anzusehen, was Juristen »Verleiten zum Vertragsbruch« nennen. Wer einen Kunden zum Vertragsbruch (z. B. zum Verstoß gegen eine mit einem Konkurrenten getroffene Exklusivitätsvereinbarung) verleitet, behindert gezielt und in wettbewerbswidriger Weise den betroffenen Mitbewerber. Das

pure Ausnutzen eines nicht durch den Handelnden hervorgerufenen Vertragsbruchs (zum Beispiel das Nichteinhalten einer Kündigungsfrist) wird hingegen nicht ohne weiteres als eine wettbewerbswidrige Behinderung gewertet.

10. Irreführung durch aktives Tun oder durch Unterlassen (§§ 5, 5a UWG): Eine irreführende Geschäftshandlung liegt vor, wenn eine Information über ein Produkt oder eine Dienstleistung objektiv von der Wahrheit abweicht. Das Verschweigen einer Tatsache ist dann irreführend, wenn die verschwiegene Tatsache von wesentlicher Bedeutung für die geschäftliche Entscheidung ist. Daneben ist zu berücksichtigen, inwieweit das Verschweigen geeignet ist, die Kaufentscheidung zu beeinflussen.

Beispiel: Die Werbung für einen als »Räumungsverkauf wegen Geschäftsaufgabe« bezeichneten Sonderverkauf ist dann irreführend, wenn das Unternehmen gar nicht schließen will. Als irreführend wird es auch gewertet, wenn ein Unternehmen mit Preissenkungen wirbt, obwohl die angeblichen Ursursungspreise nie oder nur kurze Zeit verlangt worden sind (Mondpreise).

Für die Werbung im Internet gilt nichts anderes als für Werbung auf »herkömmlichem Wege«. Jedoch ist wegen der erhöhten Entdeckungswahrscheinlichkeit von wettbewerbsrechtlichen Verstößen hier zu besonderer Vorsicht zu raten. Für Werbe- oder Unternehmensauftritte im Internet sind einige spezielle Sonderregelungen zu beachten, insbesondere Informationspflichten. Das sind vor allem die Anbieterkennzeichnungspflichten (§ 5 TMG), Informationspflichten im Fernabsatz (Art. 246 EGBGB i.V. m. Anlage 1 und 2 zum EGBGB) und Pflichten bei Preisangaben im Internet (§ 1 Abs. 2 PAngV). Verstöße hiergegen können Unterlassungsansprüche nach dem UWG begründen, weil es sich um verbraucherschützende Normen handelt.

11. Vergleichende Werbung (§ 6 UWG): Vergleichende Werbung ist dann zulässig, wenn sie wahrheitsgemäß, nachprüfbar und sachlich ist. Nicht zulässig ist es aber z. B., mit einem im Vergleich günstigeren Preis zu werben, gleichzeitig aber wesentliche abweichende Konditionen zwischen den verglichenen Angeboten zu verschweigen.
12. Belästigende Werbung (§ 7 UWG): Werbung wird als belästigend gewertet, wenn erkennbar ist, dass der Empfänger diese Werbung nicht wünscht (z. B. durch Aufkleber auf dem Briefkasten). Das Gesetz ist hier sehr streng: Verboten ist Werbung durch E-Mail, Telefax oder automatische Anrufmaschinen, wenn sie sich an einen Verbraucher richtet und dieser einer solchen Werbung nicht positiv zugestimmt hat („opt-in“). Zudem muss bei allen elektronischen Formen der Werbung die Identität des Absenders klar erkennbar sein und eine Möglichkeit benannt werden, derartige Werbung abzubestellen. Dabei dürfen die Kosten der Abbestellung die Übermittlungskosten nach den Basistarifen nicht übersteigen. Verboten ist auch jede Form von Werbeanrufen in Privathaushalten, wenn der angerufene Verbraucher hierfür nicht ausdrücklich seine Einwilligung erklärt hat. Bei Telefonwerbung gegenüber Unternehmen ist nur eine mutmaßliche Einwilligung erforderlich, d.h. hier reicht es aus, wenn der Anrufer mit einer Einwilligung rechnen kann. Dies kann aber nur in Ausnahmefällen bei Vorliegen konkreter Umstände, die auf ein Interesse an Inhalt und Art der Werbung hindeuten, unterstellt werden. Unaufgeforderte E-Mail Werbung ist nur dann zulässig, wenn der Angeschriebene mit dem Werbenden bereits vorher wegen einer ähnlichen Dienstleistung in Kontakt getreten ist und ihm dabei seine E-Mail-Adresse offenbart hat. Außerdem muss der Kunde bei jeder Zuschrift klar und deutlich darauf hingewiesen werden, dass er einer weiteren Verwendung seiner E-Mail-Adresse jederzeit widersprechen kann. Sobald der Kunde erklärt hat, keine Werbung empfangen zu wollen, ist eine weitere Verwendung seiner E-Mail-Adresse für Werbezwecke unzulässig. Erst wenn der Kunde erneut seine Einwilligung erklärt hat, darf ihm wieder Werbung zugesandt werden („opt-in“).
13. Verrat von Betriebs- und Geschäftsgeheimnissen (§§ 17, 18 UWG): Das Wettbewerbsrecht verbietet die Weitergabe, die Annahme und die unbefugte Verwertung von Geschäfts- und Betriebsgeheimnissen. Entsprechende Handlungen sind in den §§ 17, 18 UWG mit Freiheitsstrafe bis zu 3 Jahren oder mit Geldstrafe sanktioniert.

6 Kartellrecht

■ 6.1 Rechtsgrundlagen des Kartellrechts

Zu den Regelungsgegenständen des Kartellrechts gehören:

- das Verbot wettbewerbsbeschränkender Vereinbarungen,
- das Verbot eines Missbrauchs von Marktmacht (insbesondere bei marktbeherrschender Stellung),
- die Fusionskontrolle (M&A),
- das Kartellvergaberecht (öffentliche Aufträge).

Die Fusionskontrolle und das Vergaberecht werden hier nicht behandelt, da sie nur bei entsprechendem Anlass zu beachten sind.

Europäisches Kartellrecht ist anwendbar, wenn eine Wettbewerbsbeschränkung »den Handel zwischen den Mitgliedstaaten zu beeinträchtigen geeignet ist« (Art. 101 bzw. 102 AEUV, vgl. hierzu auch die Leitlinie der Kommission, Abl. 2004 C 101/81). Eingriffe in den Wettbewerb ohne spürbare grenzüberschreitende Auswirkungen sind nach dem nationalen Kartellrecht (§§ 1,2 bzw. 19, 20 GWB) zu beurteilen. Für wettbewerbsbeschränkende Vereinbarungen spielt die Unterscheidung jedoch in der Praxis kaum eine Rolle, da das nationale Kartellrecht dem europäischen Kartellrecht mittlerweile weitgehend angeglichen ist. Hinsichtlich der Regulierung einer marktbeherrschenden Stellung hat der Gesetzgeber in § 20 GWB (Diskriminierungsverbot) allerdings von der Möglichkeit Gebrauch gemacht, schärfere Sanktionen vorzusehen. Die europarechtliche Grundlage hierfür findet sich in der VO (EG) Nr. 1/2003, die im Übrigen das Kartellverfahren im Einzelnen regelt.

■ 6.2 Ziel des Kartellrechts und Risiken von Complianceverstößen

Das Kartellrecht verfolgt wie das Wettbewerbsrecht das Ziel, die Freiheit und Wirksamkeit der Märkte und damit die Funktionsfähigkeit des Wettbewerbs zu sichern. Aus diesem Grund sind wettbewerbsbeschränkende Vereinbarungen und ähnliche Verhaltensweisen grundsätzlich verboten.

Wegen der Höhe der drohenden Bußgelder ist ein Kartellrechtsverstoß für ein Unternehmen besonders risikoreich. Bei Verstößen gegen das Kartellrecht können die Europäische Kommission oder das Bundeskartellamt Geldstrafen in Höhe von bis zu 10 Prozent des weltweiten Jahresumsatzes verhängen. Im Wiederholungsfall kann das Bußgeld verdoppelt werden. Die Höhe der Bußgelder ist in den letzten Jahren erheblich gestiegen.

Insbesondere horizontale Wettbewerbsbeschränkungen, d.h. Absprachen zwischen direkten Wettbewerbern desselben Marktes, beeinträchtigen den Wettbewerb in hohem Maße und werden deshalb von den Kartellrechtsbehörden besonders streng geahndet. So hat z. B. die EU-Kommission 2008 wegen Preisabsprachen und Marktaufteilung im sog. Autoglas-Kartell 1,38 Mrd. Euro an Bußgeldern verhängt. Wegen eines Informationsaustausches über Händlerprovisionen in den Niederlanden mussten 2011 drei Mobilfunkbetreiber ein Bußgeld von 16,25 Mio. Euro zahlen.

Für vertikale Wettbewerbsbeschränkungen, d.h. für Absprachen zwischen Lieferanten und Abnehmern, hat das Bundeskartellamt u.a. folgende Bußgelder verhängt:

- 2,5 Mio. Euro in 2010 wegen unzulässiger Preisbindung beim Vertrieb von Navigationsgeräten,
- 9 Mio. Euro in 2009 für die unzulässige Einflussnahme bei der Festlegung des Wiederverkaufspreises des Softwarepakets »Office Home and Student 2007«.

Auch ein Bußgeld wegen Missbrauchs einer marktbeherrschenden Stellung kann extrem hoch sein. In 2004 hat die EU-Kommission wegen Koppelung des Media Players an das marktbeherrschende Betriebssystem Windows ein Bußgeld von 457 Mio. Euro ausgesprochen.

Daneben haben Kartellverstöße auch zivilrechtliche Folgen. Verträge oder Vereinbarungen, die gegen kartellrechtliche Bestimmungen verstoßen, sind teilweise oder vollständig nichtig und entsprechend rückabzuwickeln. Wirtschaftsorganisationen, Wettbewerber und andere von einem Kartellrechtsverstoß betroffene Marktbeteiligte können Beseitigungs- und Unterlassungsansprüche geltend machen. Auch bei lediglich fahrlässigen Verstößen hat der Betroffene umfassende Schadenersatzansprüche.

Schließlich können Verstöße gegen das Kartellrecht auch persönliche Konsequenzen für die beteiligten Mitarbeiter haben und als Ordnungswidrigkeit (§ 81 GWB) oder sogar als Straftat (§ 298 StGB, Submissionsbetrug) verfolgt werden.

■ 6.3 Verhalten im Umgang mit Kartellbehörden, Kronzeugenregelung

Zuständige Kartellbehörden sind die Europäische Kommission, Generaldirektion Wettbewerb, und auf nationaler Ebene das Bundeskartellamt bzw. in rein regionalen Fällen die Landeskartellbehörden. Die Beamten der EU-Kommission dürfen unter der Voraussetzung einer gerichtlichen Genehmigung alle Räumlichkeiten und Transportmittel des Unternehmens, wenn nötig sogar private Räumlichkeiten, betreten. Sie dürfen nach Art. 20 VO (EG) Nr. 1/2003:

- Geschäftsunterlagen einsehen,
- Kopien aus Akten oder Datenträgern anfertigen,
- betriebliche Räumlichkeiten versiegeln,
- mündliche Erklärungen für eine Nachprüfung anfordern,
- Personen vor Ort zur Sache vernehmen.

Widersetzt sich ein Unternehmen diesen Maßnahmen, kann die Kommission von den nationalen Behörden Unterstützung anfordern, die eine Kontrollmaßnahme nach nationalem Recht auch per Zwang (z. B. durch Beschlagnahme) durchsetzen können.

Grundsätzlich ist zu empfehlen, mit den Kartellbehörden zu kooperieren. Eine vollständige Kooperation und Unterstützung bei der Aufklärung kann zu einer Bußgeldermäßigung führen. Dasjenige Unternehmen, das an einem Kartell beteiligt ist und ein Kartell durch eine umfängliche Anzeige als erstes aufdeckt, geht in der Regel sogar völlig straffrei aus (Kronzeugenregelung, »Leniency«, vgl. »Mitteilung der Kommission über den Erlass und die Ermäßigung von Geldbußen in Kartellsachen«, Abl. 2006 C 298/17). Voraussetzung ist, dass die Kommission noch keine Kenntnis von dem Kartellverstoß hatte. Das Bundeskartellamt verfährt in rein nationalen Fällen entsprechend (vgl. »Bekanntmachung Nr. 9/2006 über den Erlass und die Reduktion von Geldbußen in Kartellsachen« – Bonusregelung – vom 7. März 2006). Die Kronzeugenregelung ist der Grund dafür, dass heutzutage der überwiegende Teil von Kartellverstößen durch Selbstanzeigen aufgedeckt wird.

■ 6.4 Das Verbot wettbewerbsbeschränkender Vereinbarungen

6.4.1 Überblick

Nach Art 101 Abs. 1 AEUV bzw. § 1 GWB sind »alle Vereinbarungen zwischen Unternehmen, Beschlüsse von Unternehmensvereinigungen und aufeinander abgestimmte Verhaltensweisen, welche [...] eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs innerhalb des Binnenmarkts bezwecken oder bewirken«, verboten. Tatbestandsmerkmale des Verbots (vgl. dazu im Einzelnen unten 6.4.2) sind also

- Vereinbarungen/Beschlüsse/abgestimmte Verhaltensweisen,
- durch Unternehmen/Unternehmensvereinigungen,
- die eine Wettbewerbsbeschränkung bezwecken oder bewirken,
- sofern die Wettbewerbsbeschränkung spürbar ist (ungeschriebenes, vom EuGH entwickeltes Tatbestandsmerkmal).

Wettbewerbsbeschränkende Vereinbarungen kommen in einer horizontalen oder in einer vertikalen Ausprägung vor. Bei horizontalen Wettbewerbsbeschränkungen sind Unternehmen derselben Produktionsstufe beteiligt, die auf demselben Markt tätig sind oder sein könnten. Eine vertikale Wettbewerbsbeschränkung wird dagegen zwischen Unternehmen vollzogen, die in einem Verhältnis von Lieferant und Kunde zueinander stehen.

Das Verbot der Wettbewerbsbeschränkung gilt nicht ohne Ausnahmen. Art. 101 Abs. 3 AEUV i.V.m. Art. 1 Abs. 2 VO (EG) Nr. 1/2003 bzw. § 2 GWB enthalten Legalausnahmen (Freistellungen) von diesem Verbot. Freigestellt vom Verbot sind wettbewerbsbeschränkende Verhaltensabstimmungen, die folgende Voraussetzungen erfüllen:

- Effizienzgewinn (Verbesserung der Warenerzeugung oder –verteilung, Förderung des technischen oder wirtschaftlichen Fortschritts),
- angemessene Beteiligung der Verbraucher an dem entstehenden Gewinn,
- Unerlässlichkeit der Einschränkungen,
- Keine Ausschaltung des Wettbewerbs.

Sofern eine Vereinbarung unter eine Gruppenfreistellungsverordnung (GVO) fällt, gelten die Freistellungs Voraussetzungen des Art. 103 Abs. 3 AEUV kraft Rechtsnorm als erfüllt. Näheres dazu ist in Abschnitt 6.4.3 a erläutert.

Die relevanten GVOen sind:

- VO (EU) Nr. 330/2010 betreffend Vertikalvereinbarungen (Vertikal-GVO),
- VO (EU) Nr. 1217/2010 betreffend Vereinbarungen über Forschung und Entwicklung,
- VO (EU) Nr. 1218/2010 über Spezialisierungsvereinbarungen,
- VO (EU) Nr. 772/2004 über Technologietransfervereinbarungen.

Zur Erleichterung der Anwendung der europäischen Kartellrechtsvorschriften hat die Kommission darüber hinaus verschiedene Leitlinien veröffentlicht, die allerdings für Gerichte keinen rechtsverbindlichen Charakter haben.

6.4.2 Tatbestandsmerkmale des Verbots

a) Vereinbarung, Beschluss, abgestimmte Verhaltensweise

Das Verbot wettbewerbsbeschränkender Verhaltensabstimmungen ist umfassend und schließt alle Formen bewusster Koordinierung ein, die eine praktische Zusammenarbeit an die Stelle des mit Risiken verbundenen Wettbewerbs treten lassen (ständige Rechtsprechung des EuGH). Erfasst sind also schriftliche sowie mündliche Absprachen und Gentleman Agreements. Selbst reiner Informationsaustausch zu wettbewerbsrelevanten Tatsachen kann als wettbewerbswidrige Verhaltensweise anzusehen sein, wenn er geeignet ist, Unsicherheiten hinsichtlich des von den betreffenden Unternehmen ins Auge gefassten Verhaltens auszuräumen (EuGH C-8/08 – T-Mobile Netherlands BV). Zulässig ist dagegen ein ohne Abstimmung, aufgrund Marktbeobachtung erfolgreiches Parallelverhalten am Markt (allseits bekannt ist hier die Problematik der parallelen Preiserhöhungen an Tankstellen).

b) Unternehmen, Unternehmensvereinigungen

Unternehmen sind alle am Markt tätigen Wirtschaftssubjekte. Ausgenommen ist die hoheitliche Tätigkeit des Staates. Mit Unternehmensvereinigungen sind Wirtschaftsverbände wie z. B. BITKOM gemeint.

c) Wettbewerbsbeeinträchtigung bezweckt oder bewirkt

Eine Wettbewerbsbeeinträchtigung liegt vor, wenn durch Aufgabe der autonomen Bestimmung von Wettbewerbsparametern und durch Beeinträchtigung von Chancen Dritter die Marktbedingungen verfälscht werden. Bezweckt ist die Wettbewerbsbeschränkung, wenn die Verhaltensabstimmung aufgrund ihres Inhalts und Zwecks und unter Berücksichtigung ihres rechtlichen und wirtschaftlichen Zusammenhangs konkret geeignet ist, zu einer Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs zu führen. Ob eine wettbewerbsbeschränkende Wirkung tatsächlich eintritt, ist unerheblich, wenn eine solche Folge »bezweckt« ist.

Als generell wettbewerbsbeschränkend einzustufen sind sogenannte Kernbeschränkungen (»Hardcore-Vereinbarungen«) wie

- Preisabsprachen,
- Quoten(=Mengen)absprachen, z. B. durch Produktionsbeschränkungen,
- die Aufteilung von Märkten hinsichtlich der Kunden oder der Absatzgebiete bei horizontalen Absprachen zwischen direkten Wettbewerbern sowie
- die Festlegung der Wiederverkaufspreise (Preisbindung der Zweiten Hand) bei vertikalen Absprachen zwischen Lieferant und Abnehmer.

Ist eine Wettbewerbsbeschränkung jedoch nicht »bezweckt«, muss eine Beeinträchtigung auf dem relevanten Markt tatsächlich gegeben sein. Hierfür ist eine Bestimmung des sachlich und räumlich relevanten Marktes durch Marktabgrenzung erforderlich.

d) Spürbarkeit der Wettbewerbsbeeinträchtigung

Der EuGH hat ferner das ungeschriebene Tatbestandsmerkmal der »Spürbarkeit« der Wettbewerbsbeeinträchtigung geschaffen. Damit sollen Bagatellfälle ausgeschlossen werden, bei denen aufgrund der geringen Marktanteile der beteiligten Unternehmen, der Marktstruktur oder der Geringfügigkeit der Beeinträchtigung negative Auswirkungen auf den Markt nicht zu befürchten sind. Die Spürbarkeit fehlt insbesondere bei Vereinbarungen kleiner und mittlerer Unternehmen. Hierfür hat die EU-Kommission in der sog. deminimis Bekanntmachung (ABl. 2001, C 368/13) folgende Marktanteils Grenzen aufgestellt: haben die beteiligten Unternehmen bei einer horizontalen Wettbewerbsbeschränkung zusammen einen Marktanteil von nicht mehr als 10% und bei einer vertikalen Beschränkung nicht mehr als jeweils 15%, liegt keine spürbare Beeinträchtigung vor. Nicht privilegiert werden jedoch die Kern- oder Hardcorebeschränkungen (Preis- und Mengenabsprachen, die Aufteilung von Märkten oder Kunden sowie Preisbindungen Zweiter Hand). Bei solchen Kernbeschränkungen greift die deminimis Praxis für KMU somit nicht.

6.4.3 Ausnahmen (Freistellung) vom Verbot

Das Verbot wettbewerbsbeschränkender Vereinbarungen gilt nicht ohne Ausnahme. Für die Frage, ob eine wettbewerbsbeschränkende Handlungsweise vom Verbot freigestellt, d.h. ausgenommen ist, sollte zunächst geprüft werden, ob die Voraussetzungen für eine Freistellung nach einer Gruppenfreistellungsverordnung (GVO) gegeben sind. Ist dies nicht der Fall, bleibt eine Freistellung für den individuellen Fall aufgrund der allgemeinen Regelung in Art. 101 Abs. 3 AEUV möglich.

a) Gruppenfreistellungsverordnungen (GVOen)

Die von der EU aufgrund der Ermächtigung in Art. 101 Abs. 3, 103 AEUV erlassenen GVOen sind in den EU-Mitgliedstaaten unmittelbar anzuwendende Rechtsnormen, binden also auch die Gerichte. Über den Verweis in § 2 Abs. 2 GWB gelten die GVOen in der jeweiligen Fassung auch für rein innerdeutsche Fälle ohne Auslandsbezug.

Fällt eine Vereinbarung unter eine GVO, so ist sie vom Kartellverbot ausgenommen. Wie bei der Frage der »Spürbarkeit« wird auch bei den meisten GVOen der Marktanteil relevant. Nur unterhalb bestimmter Schwellenwerte sind danach die von der jeweiligen GVO beschriebenen Vereinbarungen zwischen Unternehmen freigestellt. Die einzelnen GVOen sehen folgende Marktanteilsgrenzen vor:

- Art. 3 Vertikal-GVO (VO (EU) Nr. 330/2010): Freigestellt sind vertikale Vereinbarungen grundsätzlich bis zu einem Marktanteil von Lieferant bzw. Abnehmer von jeweils für sich max. 30%.
- Art. 4 der FuE-GVO betreffend Vereinbarungen über Forschung und Entwicklung (VO (EU) Nr. 1217/2010): Freigestellt sind unter weiteren Voraussetzungen horizontale Vereinbarungen zwischen Wettbewerbern über die gemeinsame Forschung und Entwicklung von Produkten oder Technologien bzw. die gemeinsame Verwertung der erzielten Ergebnisse, sofern der gemeinsame Marktanteil der Parteien auf den

relevanten Produkt- und Technologiemärkten nicht mehr als 25% beträgt.

- Art. 3 der GVO über Spezialisierungsvereinbarungen (VO (EU) Nr. 1218/2010): Freigestellt sind unter weiteren Voraussetzungen horizontale Vereinbarungen, mit denen eine Partei einseitig oder gegenseitig zugunsten der anderen auf die Herstellung bestimmter Waren oder die Vorbereitung bestimmter Dienstleistungen verzichtet (»Spezialisierungsvereinbarungen«) und aus Vereinbarungen, mit denen sich die Parteien verpflichten, bestimmte Waren nur gemeinsam herzustellen oder bestimmte Dienstleistungen nur gemeinsam vorzubereiten (»gemeinsame Produktion«), wenn der gemeinsame Marktanteil nicht mehr als 20% beträgt.
- Art. 3 der GVO über Technologietransfervereinbarungen (VO (EU) Nr. 772/2004): Freigestellt sind horizontale Patentlizenzvereinbarungen, Knowhow-Vereinbarungen, Softwarelizenzvereinbarungen und weitere Technologietransfervereinbarungen, wenn die lizenzierte Technologie Voraussetzung für die Produktherstellung ist und der gemeinsame Marktanteil 20% nicht überschreitet.

Die GVOen sehen jeweils Vorschriften für die Bestimmung des Marktanteils vor und Erleichterungen, wenn die Marktanteilsschwellen erst im Nachhinein überschritten werden.

Ausgenommen von der Freistellung sind wiederum in den GVOen benannte Kernbeschränkungen, sog. »Schwarze Klauseln«. Kernbeschränkungen umfassen u.a. Preis- oder Mengenabsprachen sowie Vereinbarungen zur Aufteilung von Märkten oder Kundensegmenten. Enthält eine Vereinbarung eine solche Kernbeschränkung, scheidet eine Freistellung nach der GVO aus. Eine Freistellung nach dem allgemeinen Freistellungstatbestand des Art. 101 Abs. 3 AEUV ist in diesem Fall zwar nicht ausgeschlossen (s. EuGH, Urt. v. 13.10.2011 Rs C-439/09 – Pierre Fabre, Rn. 57, 59). Allerdings tragen die Unternehmen dann die Beweislast für die positiven Effekte auf den Wettbewerb. Dies dürfte bei Vorliegen einer Kernbeschränkung

nur selten gelingen. Nach den GVOen kann schließlich die Kommission in Einzelfällen die an sich gesetzlich gegebene Freistellung entziehen.

b) Tatbestandliche Freistellung

Greift keine GVO ein, so kann die Wettbewerbsbeschränkung dennoch nach den allgemeinen Freistellungs Voraussetzungen gem. Art. 101 Abs. 3 AEUV bzw. § 2 GWB zulässig sein:

- Effizienzgewinne: Zunächst ist erforderlich, dass die zu erwartenden technischen oder kaufmännischen Effizienzvorteile die Nachteile der Wettbewerbsbeschränkung spürbar überwiegen. Effizienzgewinne sind etwa Kosteneinsparungen durch Senkung der Produktions- oder Vertriebskosten oder qualitative Effizienzgewinne durch Verbesserung des Produkt- oder Dienstleistungsangebotes. Vorteile, die unmittelbare Folgen der Wettbewerbsbeschränkungen sind (z. B. Einsparung von Marketingkosten aufgrund von Preisabsprachen), sind nicht erfasst.
- Angemessene Beteiligung der Verbraucher am Effizienzgewinn: Ferner muss der Verbraucher angemessen am Effizienzgewinn partizipieren. Der Begriff »Verbraucher« ist nicht im Sinne des deutschen Rechts zu verstehen, sondern erfasst alle Nutzer der von der Vereinbarung betroffenen Waren und Dienstleistungen, also Großhändler, Einzelhändler und Endkunden sowie alle Produzenten, die die Ware als Vorprodukt benötigen. Eine »angemessene Beteiligung« liegt vor, wenn die Vorteile die Nachteile, die durch die Wettbewerbsbeschränkung entstehen, zumindest ausgleichen (z. B. höhere Qualität bei höherem Preis).
- Unerlässlichkeit der Wettbewerbsbeschränkung zur Erzielung der Effizienzgewinne: Ferner muss die Wettbewerbsbeschränkung »unerlässlich« sein zur Erzielung der Effizienzgewinne. Dies ist der Fall, wenn ohne sie die sich aus der Vereinbarung ergebenden Effizienzgewinne beseitigt oder erheblich geschmälert würden oder die Wahrscheinlichkeit zurückgehen würde, dass sich diese Effizienzgewinne realisieren. Die Unternehmen müssen erklären, warum sich z. B. Kostenvorteile nicht ebenso gut durch internes Wachstum und Preiswettbewerb erzielen lassen.
- Keine Ausschaltung des Wettbewerbs: Eine Freistellung setzt schließlich voraus, dass durch die Vereinbarung nicht ein wesentlicher Teil des Wettbewerbs ausgeschaltet wird. Je stärker der Wettbewerb auf dem betreffenden Markt bereits geschwächt ist, desto geringer brauchen die Wettbewerbsbeschränkungen zu sein, damit man von einer »Ausschaltung des Wettbewerbs« i.S.v. Art. 101 Abs. 3 AEUV ausgehen kann.

c) Mittelstandskartelle nach § 3 GWB

Für rein innerdeutsche Fälle sieht § 3 GWB eine besondere Freistellung für kleine und mittlere Unternehmen (KMU) vor. Horizontale Vereinbarungen zwischen miteinander im Wettbewerb stehenden KMU, die eine Rationalisierung wirtschaftlicher Abläufe durch zwischenbetriebliche Zusammenarbeit zum Gegenstand haben und den Wettbewerb auf dem Markt nicht wesentlich beeinträchtigen, sind danach freigestellt. Die europarechtlichen Schwellenwerte für KMU (mind. zwei von drei der Kriterien: max. 250 Mitarbeiter, max. 50 Mio. Euro Jahresumsatz, max. 43 Mio. Euro Jahresbilanzsumme) sind dabei nicht ohne weiteres übertragbar. Vielmehr geht das Bundeskartellamt von einem relativen, an der jeweiligen Marktstruktur ausgerichteten Verständnis der KMU aus, so dass auch ein Unternehmen mit 100 Mio. Euro Umsatz in einem Umfeld mit Umsatzmilliardären ein mittleres Unternehmen sein kann (vgl. Merkblatt vom Juli 2007 über Kooperationsmöglichkeiten für kleinere und mittlere Unternehmen, Rn. 12).

6.4.4 Bedeutung der Selbstprüfung

Sind die Freistellungs Voraussetzungen einer GVO oder nach Art. 101 Abs. 3 AEUV bzw. § 2 oder 3 GWB erfüllt, ist die Wettbewerbsbeschränkung kraft Gesetzes vom Kartellverbot ausgenommen. Eines Antrags und einer Entscheidung der Kartellbehörde über die Freistellung bedarf es anders als nach früherem Recht nicht mehr. Dies bedeutet einerseits eine bürokratische Entlastung. Auf der anderen Seite trägt nun das Unternehmen die Last der juristischen Prüfung und das Risiko des Irrtums, etwa wenn für die Frage der Freistellung nach einer bestimmten GVO der Marktanteil zu bestimmen ist oder Effizienzvorteile nach Art. 101 Abs. 3 AEUV vorliegen müssen. Die Kommission versucht dem zu begegnen, indem sie Leitlinien mit Fallbeispielen veröffentlicht. Diese haben zwar keinen Rechtsnormcharakter, bewirken aber eine Selbstbindung und gestalten die Anwendung in der Praxis dadurch rechtssicherer. Es liegen vor:

- »Leitlinie zur Anwendung von Art. 81 Abs. 3 EG-Vertrag«, jetzt Art. 101 Abs. 3 AEUV (ABl. 2004 C 101/97),
- »Leitlinien zur Anwendbarkeit von Artikel 101 des Vertrags über die Arbeitsweise der Europäischen Union auf Vereinbarungen über horizontale Zusammenarbeit« (ABl. 2011 C 11/1) – Horizontalleitlinien,
- »Leitlinien für vertikale Beschränkungen« (ABl. 2010 C 130/1) - Vertikalleitlinien.

Die Horizontal- und Vertikalleitlinien enthalten nicht nur eine Art Kommentierung zu den einzelnen GVOen. Sie enthalten auch Aussagen, in welchen Fallgruppen regelmäßig schon keine Wettbewerbsbeschränkung vorliegt.

Daneben besteht die Möglichkeit, bei erheblicher Rechtsunsicherheit zu noch nicht entschiedenen Fragen, z. B. im Vorfeld erheblicher Investitionen, die Kommission um ein Beratungsschreiben zu bitten (vgl. Erwägungsgrund 38 der VO (EG) Nr. 1/2003 und die Bekanntmachung der Kommission hierzu, ABl. 2004 C 101/78). Das Beratungsschreiben ist kein formeller Rechtsakt und bindet daher in der rechtlichen Beurteilung weder Gerichte, noch nationale

Kartellbehörden noch die Kommission selbst. Es bewirkt lediglich eine Selbstbindung der Kommission dahingehend, dass sie bei einer Änderung ihrer Rechtsansicht das Unternehmen nicht mehr sanktionieren kann.

Schließlich haben Unternehmen die theoretische Möglichkeit, bei den Kartellbehörden den Erlass einer Nichttätigkeitsverfügung anzuregen (Art. 10 bzw. 5 S. 3 VO (EG) Nr. 1/2003 i.V.m. § 32c GWB). Die Behörde kann dann im Rahmen einer vorläufigen Beurteilung feststellen, dass Verbotsvoraussetzungen nicht vorliegen. Ein echtes Antragsrecht mit Bescheidspflicht bietet dieses Verfahren allerdings für die Unternehmen nicht. Ob die Behörde tätig wird, liegt in ihrem Ermessen (vgl. § 54 Abs. 1 S. 2 GWB). Die Kommission wird dies nur in wirtschaftlich äußerst bedeutenden Ausnahmefällen in Betracht ziehen, da die Umstellung vom System der administrativen Einzelfreistellung zur Legalausnahme gerade bezweckte, dass die Kommission ihre Ressourcen auf die Verfolgung von Verstößen konzentriert. Etwas großzügiger dürfte das Bundeskartellamt sein, da es im nationalen Recht für KMU für eine Übergangsphase bis 2009 nach § 3 Abs. 2 GWB ein echtes Antragsrecht mit einem Anspruch auf eine Entscheidung gab. Das Bundeskartellamt macht in seinem Merkblatt vom Juli 2007 über KMU-Kooperationen darauf aufmerksam, dass auch nach 2009 weiterhin die Möglichkeit bleibt, informell um eine kartellrechtliche Einschätzung der Kooperation nachzusuchen (Rn. 46 des Merkblattes).

6.4.5 Fallgruppen horizontaler Vereinbarungen zwischen Wettbewerbern

a) Absprachen über Preise oder sonstige Vertragskonditionen

Marktbeeinflussende Absprachen zwischen direkten Wettbewerbern (horizontale Wettbewerbsbeschränkungen) treten in vielfältiger Form auf. Verboten und mit besonders hoher Geldbuße bedroht sind Absprachen über Preise und preisrelevante Vertragskonditionen, z. B. Absprachen über

- Höchst- oder Mindestpreise,
- Kalkulationsgrundlagen für Preise,
- Preisveränderungen, auch hinsichtlich des Timing,
- Zahlungsbedingungen und Kreditziele,
- Verzugszinsen.

Beispiel: Die Verkaufsleiter zweier im Wettbewerb stehender Hersteller verabreden, ihre Wiederverkaufspreise angesichts der gestiegenen Rohstoffkosten um jeweils 5% anzuheben.

Eine Freistellung kommt für solche Hardcore-Vereinbarungen nicht Betracht.

Dagegen bleibt ein nachahmendes Verhalten (Parallelverhalten) ohne eine zugrundeliegende Vereinbarung zulässig. Beispiel: Hersteller A hebt mit Blick auf die gestiegenen Rohstoffkosten nach öffentlicher Ankündigung seine Preise um 5% an. Hersteller B nimmt die Preiserhöhung zum Anlass, nunmehr ebenfalls seine Preise um 5% zu erhöhen.

Auch Vereinbarungen über nicht wettbewerbsrelevante Preisbestandteile wie z. B. die Umsatzsteuer können mangels Wettbewerbsbeschränkung zulässig sein. Beispiel: Im Rahmen eines Branchentreffens beschließen ITK-Lieferanten, das Reverse Charge-Verfahren (Abnehmer schuldet die Umsatzsteuer anstelle des Lieferanten) für CPUs und Mobilfunkgeräte nach § 13b UStG bis zur Klärung durch die Finanzverwaltung in zweifelhaften Fällen einheitlich anhand gemeinsam festgelegter Produktkataloge anzuwenden.

b) Marktaufteilungen

Verboten sind Marktaufteilungen durch

- Absprachen über die Belieferung einzelner Kunden oder die Aufteilung von Kundengruppen,
- Absprachen über die Aufteilung von Absatzgebieten,
- Absprachen über die Festsetzung von Marktanteilsquoten.

Die wettbewerbsschädigende Wirkung liegt hier darin, dass der Anreiz, zu niedrigen Preisen anzubieten, ausgeschaltet wird. Deshalb kommt eine Freistellung für diese Hardcore-Beschränkungen grundsätzlich nicht Betracht. Beispiel: Hersteller A und Hersteller B verabreden, die jeweils unabhängig voneinander entwickelten, neuartigen Konkurrenzprodukte zunächst nur in unterschiedlichen Regionen anzubieten, um eine hohe Marge zu erhalten.

c) Austausch von Informationen

Vorsicht ist geboten beim Austausch sensibler Informationen unter Wettbewerbern. Zu den sensiblen Informationen zählen beispielsweise Angaben zu Preisen, Preisnachlässen, Lieferbedingungen, Gewinnmargen, Kostenstrukturen, Preiskalkulationen, Vertriebspraktiken, Liefergebieten und Kunden. Besondere Sensibilität ist für Mitarbeiter im Rahmen von Mitgliedschaften in einem Verband oder bei Veranstaltungen geboten, die auch von Vertretern von Wettbewerbern besucht werden.

Tauschen Wettbewerber sensible und nicht öffentlich zugängliche Marktinformationen aus, so verzichten sie auf den Geheimwettbewerb. Die Ungewissheit über die Positionierung des Wettbewerbers geht verloren. Die Wettbewerbsbehörden schließen daher vom Informationsaustausch auf ein abgestimmtes Verhalten. Bezieht sich der Informationsaustausch zudem auf ein Kernelement des Wettbewerbs wie künftiges Preis- oder Absatzverhalten, ist hiermit auch eine Wettbewerbsbeschränkung »bezweckt«, so dass der Tatbestand des Kartellverbotes auch ohne tatsächliche Umsetzung des angekündigten Verhaltens erfüllt ist (vgl. Horizontalleitlinien ABl. 2011 C 11/1, Rz. 74).

Beispiel (EuGH v. 4.6.2009, Rs. C-8/08 »T-Mobile Netherlands«): Bei einem einmaligen Treffen besprechen die Vertreter dreier Mobilfunkbetreiber die künftige Kürzung der Standardvertragshändlervergütungen für Postpaid-Verträge. Der EuGH sah hierin eine bezweckte Wettbewerbsbeschränkung, so dass es unerheblich war, ob die Provisionen später tatsächlich gekürzt wurden und dass der Austausch nur einmalig war.

Abseits der Kernbeschränkungen sind beim Informationsaustausch allerdings viele Fallkonstellationen denkbar, in denen die erhöhte Markttransparenz zu positiven Auswirkungen auf dem Markt und zu niedrigeren Preisen für den Verbraucher führt, so dass es an spürbaren Wettbewerbsbeschränkungen fehlt oder der Freistellungstatbestand erfüllt ist. Dies gilt insbesondere für öffentlich zugängliche Informationen, die nicht nur den Wettbewerbern zur Verfügung stehen, sondern auch deren Kunden. Beispiel: Anbindung von Herstellern oder Händlern an kostenlose Preissuchmaschinen im Internet.

Allerdings darf ein öffentlicher Informationsaustausch auch nicht dazu dienen, eine vorgelagerte Absprache zu überwachen.

Ausführliche Hinweise zur kartellrechtlichen Bewertung des Informationsaustausches mit weiteren Beispielen liefern die Horizontalleitlinien (ABl. 2011 C 11/1, Rz. 55 - 110).

d) Vereinbarungen über Forschung und Entwicklung

Vereinbarungen über die gemeinsame Durchführung von Forschungsarbeiten oder die gemeinsame Weiterentwicklung der Forschungsergebnisse bis zur Produktionsreife fallen grundsätzlich nicht unter das Verbot des Artikels 101 Abs. 1 AEUV. Das Verbot greift aber wiederum ein, wenn die Parteien sich darauf verständigen, auf weitere Forschungs- und Entwicklungstätigkeiten in demselben Feld zu verzichten oder sich in der Verwertung der Forschungsergebnisse beschränken, und damit die Möglichkeit ausschließen, gegenüber den übrigen Parteien Wettbewerbsvorteile zu erlangen. Dafür sind komplexe Untersuchungen der Auswirkungen auf die betroffenen Märkte erforderlich.

Liegt eine spürbare Wettbewerbsbeschränkung vor, so kommt bei gemeinsamem Marktanteil bis 25% für Wettbewerber eine Freistellung nach der GVO FuE (VO (EU) Nr. 1217/2010) in Frage. Ansonsten sind mögliche positive Auswirkungen im Rahmen der individuellen Freistellung nach der allgemeinen Freistellungsregelung in Art. 101 Abs. 3 AEUV zu prüfen. Zur Veranschaulichung hat die EU-Kommission in den Horizontalleitlinien Beispielfälle beschrieben und bewertet (vgl. ABl. 2011 C 11/1, Rz. 148).

e) Vereinbarungen über gemeinsame Produktion

Vereinbarungen über die gemeinsame Produktion bestimmter Produkte, etwa über ein Joint-Venture, sind unproblematisch, wenn sie die Parteien erst in die Lage versetzen, neue Waren oder Dienstleistungen einzuführen oder in den Markt einzutreten, insbesondere wenn sich die Kompetenzen der Parteien ergänzen.

Beispiel: Ein Hardware- und ein Softwarehersteller möchten ein neues Produkt herstellen, das beide Komponenten benötigt. Anstatt die jeweils fehlende Komponente als künftige Wettbewerber unter hohem zeitlichen und finanziellen Aufwand selbst zu entwickeln, kooperieren sie und stellen das neue Produkt gemeinsam her. Dies ist grds. zulässig.

Problematisch sind dagegen Vereinbarungen über eine Zusammenarbeit in einem vorgelagerten Markt, die z. B. aufgrund der Marktmacht der beteiligten Unternehmen zu einem Abschottungseffekt auf dem nachgelagerten Markt führen (»Spillover Effekt«). Einzelheiten finden sich in den Horizontal-Leitlinien ABl. 2011 C 11/1, Rz. 150-193 und der GVO über Spezialisierungsvereinbarungen (VO (EU) Nr. 1218/2010).

Je nach Ausgestaltung unterliegen Produktionsvereinbarungen als Joint-Venture auch der Fusionskontrolle.

f) Einkaufskooperationen

Die Verbesserung von Einkaufskonditionen durch Bündelung von Nachfragemacht (Einkaufskooperation) ist zwischen KMU unproblematisch zulässig, die einen gemeinsamen Marktanteil von 10% nicht überschreiten und damit unter die »de minimis«-Regelung fallen. Es fehlt dann an einer spürbaren negativen Auswirkung auf den Wettbewerb. Bei einem gemeinsamen Marktanteil bis 15% sowohl auf den Einkaufs- als auf den Verkaufsmärkten sieht die Kommission negative Auswirkungen wie fehlenden Preiswettbewerb aufgrund weitgehender Kostenangleichung mangels Marktmacht als unwahrscheinlich an (Horizontalleitlinien ABl. 2011 C 11/1, Rz. 208). Im Übrigen ist der Einzelfall zu untersuchen.

Ein Beispiel findet sich in den Horizontal-Leitlinien (ABl. 2011 C 11/1, Rz. 221).

g) Vermarktungsvereinbarungen

Die gemeinsame Vermarktung von Waren oder Dienstleistungen fällt unter den Verbotstatbestand, wenn damit die Abstimmung von Preisen oder die Aufteilung von Märkten verbunden ist, also eine Kernbeschränkung betroffen ist. Allerdings bleibt eine Freistellung möglich, wenn im Einzelfall die Voraussetzungen des Art. 103 Abs. 3 AEUV erfüllt sind. Die Kommission nimmt dies im Regelfall an bei einem gemeinsamen Marktanteil bis zu 15% (Horizontalleitlinien ABl. 2011 C 11/1, Rz. 240). Wird dieser Marktanteil überschritten, so kommt eine Freistellung dennoch in Betracht, wenn die gemeinsame Preisfestsetzung ausnahmsweise unerlässlich für den Marktzutritt ist.

Beispiele finden sich in den Horizontalleitlinien (ABl. 2011 C 11/1 Rz. 252 ff.).

6.4.6 Fallgruppen vertikaler Vereinbarungen (Vertriebsbeschränkungen)

Das Verbot vertikaler Wettbewerbsbeschränkungen betrifft Absprachen zwischen Unternehmen verschiedener Marktstufen, also zwischen Lieferanten und Abnehmern, durch die die Wettbewerbsfreiheit des jeweiligen Geschäftspartners oder eines Dritten eingeschränkt wird.

a) Exklusivitätsvereinbarungen

Exklusivitätsvereinbarungen sind Abreden, in denen sich ein Händler verpflichtet, ein bestimmtes Endprodukt nur an einen einzigen Abnehmer abzugeben, oder sich ein Kunde verpflichtet, bestimmte Waren ganz oder zu einem erheblichen Teil nur bei einem Händler zu beziehen.

Solche Exklusivitätsvereinbarungen sind nicht in allen Fällen unzulässig.

Zulässige Exklusivitätsvereinbarungen sind:

- das Gewähren von exklusiven Vertriebs-, Bezugs-, Franchise- oder Lizenzrechten in einem bestimmten Gebiet,
- das Untersagen, dass außerhalb des bestimmten Exklusivitätsgebietes eine aktive Verkaufspolitik betrieben wird.

Außerhalb des vertraglich vereinbarten Gebietes und in Bezug auf die vereinbarten Waren kann der Geschäftspartner deshalb verpflichtet werden, aktive Kundenwerbung, die Errichtung einer Zweigstelle oder die Aufrechterhaltung einer Vertriebsstelle zu unterlassen.

Verbotene Klauseln in Exklusivitätsvereinbarungen sind:

- einem Vertriebsunternehmen zu untersagen, die Bestellung eines Kunden anzunehmen, der sich außerhalb des Exklusivitätsgebietes befindet,
- Vorgabe, dass Kunden von außerhalb des vereinbarten Exklusivitätsgebietes nicht über Dritte beliefert werden dürfen,
- einem Vertriebsunternehmen zu untersagen, die Waren auf Anfrage an andere Vertriebskanäle abzugeben,
- Aufträge von Vertriebsunternehmen, die Waren exportieren, mit dem Hinweis auf eine Gebietsbeschränkung abzulehnen.

Einzelheiten finden sich in den »Leitlinien für vertikale Beschränkungen« (Vertikalleitlinien, ABl. 2010 C 130/1, Rz. 151 ff.).

b) Wettbewerbsbeschränkung durch Kopplung

Der Wettbewerb kann durch Kopplungsvereinbarungen eingeschränkt sein (Art. 101 Abs. 1 lit e) AEUV). Eine Kopplungsvereinbarung liegt vor, wenn der Lieferant den Verkauf einer Ware vom Abschluss eines anderen Geschäfts abhängig macht.

Kopplungsvereinbarungen sind zulässig, wenn sie sachlich begründet werden können und nicht zu einer Gefährdung der Wettbewerbsstruktur führen.

Zulässige Kopplungsvereinbarungen sind:

- in Lizenzvereinbarungen den Kauf spezieller Materialien und Werkzeuge vorzuschreiben, die für eine ordnungsgemäße Nutzung der Lizenz notwendig sind,
- von einem Kunden zu verlangen, komplette Produktsortimente abzunehmen.

Verbotene Kopplungsvereinbarungen sind:

- die Lieferung eines Produktes von dem Kauf andersartiger, sachfremder Produkte abhängig zu machen,
- die Lieferung eines Produktes vom Abschluss einer Vereinbarung über bestimmte Dienstleistungen abhängig zu machen.

Einzelheiten finden sich in den »Leitlinien für vertikale Beschränkungen« (Vertikalleitlinien, ABl. 2010 C 130/1, Rz. 214 ff.). Daneben können Kopplungen auch eine missbräuchliche Ausnutzung einer marktbeherrschenden Stellung nach Art. 102 lit d) AEUV darstellen.

c) Wettbewerbsbeschränkung durch Preisbindung

Die autonome Preisfestlegung durch den Groß- oder Einzelhändler ist von entscheidender Bedeutung für einen funktionierenden Wettbewerb. Ein Lieferant darf daher dem Händler den Verkaufspreis seiner Ware nicht verbindlich vorgeben (Verbot der Preisbindung der zweiten Hand nach Art. 101 Abs. lit. a) AEUV).

Allerdings darf nach der Vertikal-GVO bis zu einem Marktanteil der Parteien von jeweils nicht mehr als 30%, im Einzelfall auch darüber hinaus, eine unverbindliche Preisempfehlung ausgesprochen werden, wenn zu ihrer Durchsetzung kein Druck angewendet wird. Zulässig ist beispielsweise das bloße Überreichen einer Liste mit Empfehlungen für Wiederverkaufspreise durch einen Lieferanten an ein nachfragendes Handelsunternehmen oder auch der Aufdruck des unverbindlichen Einzelhandelspreises auf Etiketten. Der Lieferant darf auch die Gründe für seine Preisempfehlungen erläutern und grundsätzlich erklären, welche Strategie er im Hinblick auf die Positionierung und Vermarktung seiner Produkte verfolgt.

Unzulässige Maßnahmen sind dagegen:

- Vorgaben zu Absatzspannen, Preisnachlässen, Zeitspannen für Preisnachlässe,
- Unterstützung von Werbemaßnahmen des Handels durch produktbezogene Vergütungen oder Pauschalrabatte durch den Lieferanten, wenn hierbei von einem der beiden Vertragspartner konkrete Aktionspreise verlangt werden,
- Vereinbarungen oder Abstimmungen zwischen Herstellern und Handelsunternehmen über eine Spannenneutralität bzw. Verbesserung der Spannen bei Erhöhung der Herstellerabgabepreise mit gleichzeitiger Erhöhung der Wiederverkaufspreise (gleitende Preisbindung),
- Benennung von verbindlichen Wiederverkaufspreisen oder Wiederverkaufspreisuntergrenzen durch den Lieferanten in Bestellvordrucken oder sonstigen Dokumenten.

Eine unverbindliche Preisempfehlung wird unzulässig, wenn sie mit der Androhung oder Durchsetzung von Nachteilen oder mit dem Versprechen oder Gewähren von Vorteilen verbunden wird. Einzelheiten hierzu finden sich in dem Schreiben des Bundeskartellamtes vom 13. April 2010 (veröffentlicht im Rundschreiben 4/2010 der Studienstiftung des Deutschen Kaisers) und in den Vertikalleitlinien (ABl. 2010 C 130/1, Rz. 223 ff.).

d) Wettbewerbsbeschränkung durch selektive Vertriebssysteme, Beschränkung des Online-Handels

In einem selektiven Vertriebssystem wählt der Lieferant seine Vertriebspartner nach festgelegten qualitativen oder quantitativen Kriterien aus. Qualitative Kriterien sind z. B. das Angebot einer Produktberatung, das Produktspektrum oder die Garantie einheitlicher Qualitätsstandards. Quantitative Kriterien sind z. B. die Beschränkung der Anzahl von Händlern in einem bestimmten Gebiet oder die Beschränkung auf Händler mit einem bestimmten Umsatz.

Bis zu einem Marktanteil von jeweils 30% sind selektive Vertriebssysteme nach der Vertikal-GVO grundsätzlich erlaubt, darüber hinaus u.U. aufgrund Freistellung nach Art. 103 Abs. 3 AEUV (zu letzterem vgl. Vertikal-Leitlinien, ABl. 2010 C 130/1, Rz. 174 ff.). Bei qualitativem Selektivvertrieb fehlt es zudem unabhängig von Marktanteilen schon an einer Wettbewerbsbeschränkung, wenn die Auswahl der Händler nach einheitlichen Kriterien diskriminierungsfrei erfolgt und die Kriterien erforderlich sind, um die Qualität oder den richtigen Gebrauch des Produktes zu gewährleisten (EuGH, Urt. v. 13.10.2011 Rs C-439/09 – Pierre Fabre, Rz. 41).

Beispiel: Der Hersteller eines Markengerätes beobachtet, dass seine Geräte bei Discountern zu einem besonders günstigen Preis angeboten werden. Die Kunden neigen dazu, sich in Fachgeschäften beraten zu lassen, erwerben die Geräte dann aber billiger bei den Discountern. Der Hersteller schließt deshalb nur noch mit Fachhändlern Verträge ab. Er schließt somit Discountern vom Wettbewerb aus, indem er ihnen den Vertragsschluss verweigert und auch seinen Distributoren auferlegt, Discountern nicht zu beliefern. Dies ist grundsätzlich erlaubt.

Auch ein qualitatives selektives Vertriebssystem ist jedoch nicht schrankenlos zulässig. Nach Ansicht des EuGH verstößt ein Hersteller gegen Art 4c Vertikal-GVO, wenn er seinem Vertriebspartner im Rahmen eines qualitativen selektiven Vertriebssystems den Vertrieb über das Internet untersagt. In Betracht kommt insoweit lediglich eine Freistellung aufgrund Art. 101 Abs. 3 AEUV, wenn die Voraussetzungen im Einzelfall erfüllt sind (EuGH, Urt. v. 13.10.2011 Rs C-439/09 – Pierre Fabre, Rz. 56 ff.).

■ 6.5 Missbrauch einer marktbeherrschenden Stellung

Marktbeherrschende Unternehmen handeln rechtswidrig, wenn sie ihre Marktstellung missbrauchen.

6.5.1 Definition einer marktbeherrschenden Stellung

Eine marktbeherrschende Stellung liegt vor, wenn ein Unternehmen die Möglichkeit hat, einen wirksamen Wettbewerb zu verhindern. Gemäß § 19 Abs. 2 GWB ist ein Unternehmen marktbeherrschend, wenn es auf dem relevanten Markt ohne Wettbewerber ist, keinem wesentlichen Wettbewerb ausgesetzt ist oder eine im Verhältnis zu seinen Wettbewerbern überragende Marktstellung hat. Dies wird nach deutschem Recht bei einem Marktanteil von einem Drittel vermutet. Im Europäischen Wettbewerbsrecht wird eine marktbeherrschende Stellung – bezogen auf den jeweils zu betrachtenden Markt – regelmäßig erst bei einem höheren Anteil angenommen.

Der relevante Markt wird vorwiegend anhand von sachlichen und geographischen Kriterien festgelegt:

- der sachlich relevante Markt umfasst die angebotenen Produkte oder Dienstleistungen, die von Verbrauchern hinsichtlich ihrer Eigenschaften, Preise und ihres vorgesehenen Verwendungszwecks als austauschbar oder ersetzbar angesehen werden;
- geographisch relevant ist das Gebiet, in dem die beteiligten Unternehmen ihre relevanten Produkte oder Dienstleistungen anbieten und in dem die Wettbewerbsbedingungen hinreichend homogen sind.

Ist der Markt in sachlicher und geographischer Hinsicht abgegrenzt, wird festgestellt, welche Anbieter und welche Verbraucher auf diesem Markt aktiv sind. Auf dieser Grundlage lassen sich die Marktgröße insgesamt und, unter Zugrundelegung von Verkaufszahlen der relevanten Produkte in dem jeweiligen Gebiet, die Marktanteile der einzelnen Anbieter berechnen.

6.5.2 Diskriminierungsverbot bei marktbeherrschender Stellung

Ein Unternehmen mit einer marktbeherrschenden Stellung darf seine Kunden nicht diskriminieren (Art. 102 lit. c AEUV, § 20 GWB). Es ist z. B. verboten, unter gleichen Voraussetzungen gleichartigen Kunden unterschiedliche Preise oder Rabatte zu gewähren. Hingegen kann es zulässig sein, Kunden unterschiedliche Rabatte oder abweichende Verkaufsbedingungen zu gewähren, sofern diese besondere Leistungen erbringen.

6.5.3 Behinderung von Wettbewerbern bei marktbeherrschender Stellung

Ein Unternehmen mit einer marktbeherrschenden Stellung darf seinen Wettbewerbern den Zugang zu Kunden oder Händlern nicht versperren (§ 19 Abs. 4 Nr. 1 GWB).

Beispiele für eine Behinderung von Wettbewerbern sind:

- Verkauf unter Einstandspreis (Dumpingpreis) mit dem Ziel der Ausschaltung der Konkurrenz,
- Boykott sowie sachlich nicht gerechtfertigte Lieferverweigerung,
- Treuerabatte und Bonus-Systeme mit Bindungswirkung. Dadurch würde das Unternehmen seine Marktstellung weiter verstärken, weil Nachfrager – um die Rabatte zu erhalten – noch mehr beim Marktbeherrscher einkaufen würden.
- »Englische Klausel« in Verträgen: Danach wird es Kunden zwar gestattet, Produkte von Wettbewerbern zu beziehen, allerdings nur, wenn diese vorher über den Namen des Wettbewerbers, die Bezugsmenge und den vereinbarten Preis informieren.
- Koppelungen: Die Ware, auf deren Markt die Marktstellung vorliegt, wird nur gemeinsam mit einer anderen Ware verkauft (Art. 102 lit. d AEUV).

6.5.4 Ausnutzen von Marktmacht gegenüber abhängigen Unternehmen

Das Kartellrecht verbietet auch das Ausnutzen von Marktmacht auf der Nachfrageseite (§ 20 Abs. 2 GWB). Dieses Verbot richtet sich an marktmächtige Unternehmen, soweit von ihnen kleinere oder mittlere Anbieter bestimmter Waren in der Weise abhängig sind, dass sie faktisch keine Möglichkeit haben, andere Kunden zu beliefern.

Die Abhängigkeit eines Lieferanten oder eines Einzelhändlers wird dann vermutet, wenn er einem Abnehmer zusätzlich zu den branchenüblichen Preisnachlässen oder sonstigen Leistungsentgelten regelmäßig weitere Vergünstigungen gewährt, die andere Abnehmer mit vergleichbarem Zuschnitt nicht erhalten. Von abhängigen Lieferanten darf auch keine Spanngarantie eingefordert werden. Das bedeutet, dass ein marktmächtiger Abnehmer keine nachträgliche Änderung von Konditionen nur deswegen verlangen darf, weil ein Wettbewerber ein vergleichbares Produkt günstiger anbietet.

7 Exportkontrolle und Außenwirtschaftsrecht

7.1 Zweck von Exportkontrollen

Die Exportkontrolle dient dazu, die Verbreitung von Waffen und Rüstungsgütern in Krisengebieten zu verhindern. Ihr unterliegen aber auch Waren, Software und Technologie, die sowohl für zivile als auch für militärische Zwecke eingesetzt werden können (sog. Dual use-Güter).

7.2 Rechtsgrundlagen

Die wesentlichen Rechtsgrundlagen des Exportkontrollrechts sind:

- das Außenwirtschaftsgesetz (AWG);
- die Außenwirtschaftsverordnung (AWV);
- die Dual-Use-Verordnung der EU (VO [EG] 428/2009 vom 05.05.2009) mit ihren Anhängen, insbesondere Anhang I zur EG-Dual-Use-VO 428/2009
- die Ausfuhrliste;
- die Embargovorschriften;
- das Kriegswaffenkontrollgesetz (KrWaffKontrG)

Zu beachten ist, dass sowohl das AWG als auch die AWV derzeit neu gefasst werden. Die Bundesregierung hat Mitte August 2012 einen Neuentwurf für das AWG vorgelegt. Die AWV wird in der Folge eine Neufassung finden. Die Neuregelungen zielen vielfach auf eine verbesserte Anpassung an europäische Regeln und mehr Klarheit der gesetzlichen Grundlagen.

Das Außenwirtschaftsgesetz (AWG) schafft die Voraussetzungen zum Erlass der Außenwirtschaftsverordnung. Es enthält die Ermächtigungsgrundlage für die Bundesregierung, zur Umsetzung internationaler Vereinbarungen (z. B. von UN-Embargos) Beschränkungen des Außenwirtschaftsverkehrs anzuordnen. Des Weiteren finden sich in den §§ 33, 34 AWG die Ordnungswidrigkeiten und strafrechtliche Sanktionen bei Verstößen gegen Vorschriften des AWG, der AWV, der Dual-use-VO und gegen Embargos. In der Außenwirtschaftsverordnung (AWV) werden die Beschränkungen der Ausfuhr von Gütern und die einzuhaltenden Verwaltungsverfahren konkretisiert.

Die Dual-Use-Verordnung der EU regelt das Verfahren für den Umgang mit Gütern, die sowohl im zivilen als auch im militärischen Bereich zum Einsatz kommen können (= Güter mit doppeltem Verwendungszweck). Dies ist grundsätzlich hinsichtlich fast aller Waren vorstellbar. Aus diesem Grund hat die EU eine einheitliche Liste geschaffen (vgl. Anhang I der EG-Dual-use-VO). Die Liste enthält die technischen Parameter für Güter, deren Ausfuhr einer Genehmigungspflicht unterliegt. Zu diesen Gütern gehören z. B. Mikroprozessoren, integrierte Schaltungen, Rechner und elektronische Baugruppen, Software, digitale Funkempfänger, Systeme der Kryptotechnik.

7.3 Instrumente des Exportkontrollrechts

Instrumente der Exportkontrolle sind das Ausfuhrverbot und die Genehmigungspflicht für die Ausfuhr von Gütern. Jede Ausfuhr und Verbringung ist stets auf das Vorliegen von Verboten und Genehmigungspflichten zu überprüfen. Genehmigungspflichtig ist die Ausfuhr immer dann, wenn das Gut in einer europäischen oder nationalen Güterliste des Exportkontrollrechts genannt («gelistet») ist. Als Ausfuhr wird die Lieferung von Gütern aus der EU in Drittländer bezeichnet. Eine Verbringung ist die Lieferung aus Deutschland in andere EU-Staaten.

Lieferungen innerhalb der EU sind jedoch nur selten genehmigungspflichtig, z. B. bei Waffen und Waffentechnologie gemäß Abschnitt A der Ausfuhrliste oder bei anschließendem Export in ein Drittland. Auch muss nicht für jedes Gut, das der Exportkontrolle unterliegt, eine Einzelausfuhrgenehmigung des BAFA (Bundesamt für Wirtschaft und Ausfuhrkontrolle) eingeholt werden. Für bestimmte Staaten und Güter gibt es Allgemeine Genehmigungen, deren Nebenbestimmungen zwingend einzuhalten sind.

Daneben existieren auch Einfuhrbeschränkungen, wobei die hierzu bestehenden Regelungen den ITK-Bereich kaum berühren dürften.

■ 7.4 Exportkontrollierte Güter

Güter im Sinne des Exportkontrollrechts sind Waren, Technologien und Software. Selbst Dienstleistungen wie technische Unterstützung (z. B. Schulungen und Reparaturen) können nach §§ 45 ff. AWV genehmigungspflichtig sein, wenn der Dienstleister vom BAFA darauf hingewiesen wird oder Informationen hat, dass die Dienstleistung bestimmten, als risikoreich angesehenen Zwecken dient.

Güter unterliegen der Exportkontrolle, wenn sie strategische Bedeutung haben, insbesondere, wenn sie als Waffen oder zur Rüstung verwendet werden können. Daneben gehören auch Güter mit doppeltem Verwendungszweck (Dual-Use-Güter) zu den exportkontrollierten Gütern. Selbst Güter, die nicht in einer Liste des Exportkontrollrechts enthalten sind, können nach Art. 4 der Dual-Use-Verordnung genehmigungspflichtig sein. Das ist der Fall, wenn der Ausführer vom BAFA informiert wurde oder selbst Informationen hat, wonach diese Güter einer sensiblen Verwendung dienen können (z. B. dem Bau von Kernwaffen oder von Militärgütern). Für ähnliche Bereiche sehen auch die §§ 5c, 5d AWV Genehmigungspflichten vor.

■ 7.5 Besonderheiten bei Outsourcing und Cloud Computing

Eine Ausfuhr ist nach Ansicht des BAFA bereits dann anzunehmen, wenn Technologie im Wege des Outsourcing auf Servern außerhalb der EU abgelegt wird. Dabei handelt es sich insbesondere um Daten (z. B. abgelegte Produktionszeichnungen oder Produktionsprozessanweisungen), die bei der Herstellung von Waffen bzw. von gelisteten Dual-Use-Gütern genutzt werden können. Für das BAFA stellt bereits der Transfer der Daten die Ausfuhr dar (nicht-gegenständliche Übermittlung). Dies gilt entsprechend für das Cloud-Computing, aber auch für Zugriffsmöglichkeiten von nicht in der EU ansässigen Nutzern auf einen im Inland befindlichen Server.

■ 7.6 Besonderheiten bei grenzübergreifender Software-Entwicklung

Bei der Entwicklung von Software, die in Kooperation von mehreren Standorten in verschiedenen Ländern durchgeführt wird, muss beachtet werden, dass für diese Aktivitäten exportkontrollrechtliche Genehmigungen erforderlich sein können. Wenn die Software genehmigungspflichtig ist, muss bei der Kommunikation über diese Software ein möglicher genehmigungspflichtiger Technologietransfer geprüft werden. Das Exportkontrollrecht ist auch bei der firmeninternen Weitergabe von Software zu beachten, wenn die Software genehmigungspflichtig ist und sich der Empfängerstandort in einem Drittland befindet.

■ 7.7 Besonderheiten für Vermittlungsgeschäfte

Von der Genehmigungspflicht betroffen sind des Weiteren Vermittlungs- und Handelsgeschäfte über Güter, die sich nicht in der EU befinden und in ein Nicht-EU-Land verkauft werden sollen. Das ist der Fall, wenn es sich um Güter der Ausfuhrliste Abschnitt A (also insb. Waffen bzw. Technologie für deren Herstellung oder Software für deren Betrieb) handelt. Schließlich können Vermittlungsgeschäfte auch dann nach Art. 5 der Dual-Use-VO genehmigungspflichtig sein, wenn der Ausführer Informationen hat oder vom BAFA informiert wird, dass die vermittelten Güter sensiblen Zwecken dienen.

■ 7.8 Umgang mit Embargoländern

EU-Embargos sind unmittelbar wirksam und bedürfen keiner nationalen Umsetzung. Die Liste der jeweils in Kraft befindlichen Embargos kann über die [Webseite des BAFA](#) eingesehen werden. Hierbei ist zu beachten, dass sich die Embargos von Land zu Land deutlich unterscheiden (z. B. Reisebeschränkungen, Verbot des Bereitstellens von Geldern und wirtschaftlichen Ressourcen).

Am strengsten ist derzeit das Embargo gegen den Iran, wonach z. B. der Abschluss von Versicherungen (mit wenigen Ausnahmen, etwa Krankenversicherungen, Pflicht- und Haftpflichtversicherungen) mit iranischen Unternehmen verboten ist. Dies gilt auch für Unternehmen, die ihren Sitz in Deutschland haben, aber im Eigentum eines iranischen Unternehmens, einer im Iran lebenden Privatperson oder der iranischen Regierung stehen. Darüber hinaus ist auch die Ausfuhr bestimmter Technologien und Software zur Überwachung des Fernmeldeverkehrs oder für die Ferneinbringung von Computerviren ohne entsprechende Genehmigung untersagt. Die gegen Syrien verhängten Embargomaßnahmen stehen hinter denen gegenüber dem Iran mittlerweile kaum mehr zurück.

■ 7.9 Beachtlichkeit des US-amerikanischen Rechts

Auch das US-amerikanische Recht enthält Exportkontrollvorschriften. Ob diese vom exportierenden Unternehmen zu beachten sind, ist im Einzelfall zu prüfen. Das US-amerikanische Recht kontrolliert u.a. den Reexport von US-amerikanischen Gütern sowie ausländischen Gütern mit US-Bestandteilen. Zu beachten ist, dass die US-amerikanischen Vorschriften andere Embargos vorsehen als die EU.

■ 7.10 Compliance im Exportkontrollrecht

Aufgabe der Compliance ist es, Verstöße gegen das Exportkontrollrecht auszuschließen. Dazu bedarf es entsprechender Vorkehrungen (neben Schulungen von Mitarbeitern auch technische Vorkehrungen), die stets auf dem aktuellen Stand zu halten sind. Das Exportkontrollrecht ist häufigen Veränderungen unterworfen.

Unternehmen, die Güter des Teils I Abschnitt A der Ausfuhrliste sowie Güter des Anhangs I EG-Dual-use-VO ausführen wollen, haben grundsätzlich einen Ausfuhrverantwortlichen zu benennen. Dieser muss der Vorstands-/Geschäftsführungsebene angehören und über eine entsprechende Zuverlässigkeit verfügen. Der Ausfuhrverantwortliche haftet selbst im Rahmen von Straftaten und Ordnungswidrigkeiten. Zudem kann ein Versagen der Compliance-Mechanismen dazu führen, dass das BAFA den Ausfuhrverantwortlichen als unzuverlässig ansieht. In diesem Falle können Ausfuhrgenehmigungen an das Unternehmen erst wieder erteilt werden, wenn die entsprechende Person nicht mehr der Vorstands-/Geschäftsführungsebene angehört.

Verstöße gegen die Exportkontrollvorschriften der Bundesrepublik und der EU können als Ordnungswidrigkeiten, in vielen Fällen sogar als Straftaten geahndet werden. Wer eine Ausfuhr ohne erforderliche Genehmigung oder unter Mißachtung eines Ausfuhrverbots veranlasst, muss mit Bußgeldern bis zu 500.000 Euro pro Einzelfall rechnen. Für besonders schwere Verstöße drohen Freiheitsstrafen von mindestens 2 Jahren.

8 Finanzberichterstattung

Gewerbliche Unternehmen müssen sämtliche unternehmerischen Aktivitäten, die Einfluss auf Gewinn und Betriebsvermögen haben, nach gesetzlichen Vorgaben in ihren Geschäftsbüchern abbilden. Ausnahmen von diesem Grundsatz lässt das Gesetz nur für sehr kleine Einzelkaufleute zu (vgl. im Einzelnen unter Ziff. 8.1). Da die Ergebnisse der Buchführung in den Jahresabschluss einfließen und der Jahresabschluss im Fokus vieler Interessen steht (Gesellschafter, Kunden, Lieferanten, Banken, Finanzverwaltung, Kapitalmarkt, Arbeitnehmer), hat der Gesetzgeber für die Buchführung vergleichsweise strenge Vorgaben geschaffen.

■ 8.1 Buchführungspflicht

Jeder Kaufmann ist nach §§ 238 ff. HGB verpflichtet, seine Geschäfte und die Entwicklung seiner Vermögenslage lückenlos in einer kontinuierlichen Buchführung aufzuzeichnen sowie am Ende eines jeden Geschäftsjahres aus der Buchführung einen Jahresabschluss zu entwickeln. Zur Buchführung gehört beispielsweise die lückenlose Aufzeichnung des Wareneingangs und –ausgangs, die Inventarisierung des Unternehmensvermögens und die Überprüfung von Eingangs- und Ausgangsrechnungen. Der Jahresabschluss besteht aus einer Bilanz sowie einer Gewinn- und Verlustrechnung, die – abhängig von der Größe und der Rechtsform des Unternehmens – um einen Anhang und einen Lagebericht zu erweitern sind. Zur Buchführung verpflichtet ist jeder Kaufmann. Als Kaufmann gilt jeder Inhaber eines Gewerbebetriebs. Personenhandelsgesellschaften (OHG, KG) und Kapitalgesellschaften (AG, GmbH, eG, SE, KG aA, wirtschaftliche Vereine, Kapitalgesellschaften ausländischer Rechtsformen) sind aufgrund gesetzlicher Vorgaben als Kaufleute anzusehen und damit buchführungspflichtig. Nicht von der handelsrechtlichen Buchführungspflicht betroffen sind alle selbständigen Berufe (z. B. Rechtsanwälte, Ärzte, Architekten, Ingenieure). Von der Buchführungspflicht ausgenommen sind Einzelkaufleute, deren Jahresumsatz 500.000 Euro und

deren Jahresüberschuss 50.000 Euro nicht überschreiten (§ 241a HGB).

Bei der Buchführung und bei der Erstellung des Jahresabschlusses sind in Deutschland die Grundsätze ordnungsmäßiger Buchführung (GoB) zu beachten (§§ 238 Abs. 1 S. 1, 243 Abs. 1 HGB). Dabei handelt es sich um allgemein akzeptierte Standards, die sich im Laufe der Zeit im Rechnungswesen von Unternehmen etabliert haben. Teilweise sind diese Standards gesetzlich kodifiziert, so beispielsweise die Grundsätze der Vollständigkeit, Richtigkeit, Zeitgerechtigkeit und Geordnetheit der Buchführung (§ 239 Abs. 2 HGB) und das »Radierverbot« (§ 239 Abs. 3 HGB). Darüber hinaus schreibt der Gesetzgeber in §§ 246 – 278 HGB recht detailliert vor, wie und mit welchen Wertansätzen einzelne Geschäftsvorfälle im Jahresabschluss abzubilden und entsprechend zu verbuchen sind. Insgesamt muss die Buchführung so beschaffen sein, dass sich ein sachverständiger Dritter in angemessener Zeit einen Überblick über alle Geschäftsvorfälle und über die wirtschaftliche Lage des buchführungspflichtigen verschaffen kann (§ 238 Abs. 1 S. 2 HGB). In anderen Ländern gelten jeweils eigene Buchführungsvorschriften. Weit verbreitet sind die International Financial Reporting Standards (IFRS).

Der Umfang der Buchführungspflicht hängt von der Größe und der Rechtsform des jeweiligen Unternehmens ab. Während kleinen Personenunternehmen (Einzelkaufleute und Personenhandelsgesellschaften) nur eine recht grobe und allgemeine Gliederung ihrer Bilanz vorgeschrieben ist (§ 247 HGB), müssen Kapitalgesellschaften die Gliederungsvorgaben der §§ 266, 275 HGB genau befolgen und zusätzliche Informationen in einem Anhang zur Bilanz und in einem ergänzenden Lagebericht mitteilen. Bei kapitalmarktorientierten Unternehmen muss der Lagebericht auch einen Prognosebericht über die voraussichtliche weitere Geschäftsentwicklung und die damit verbundenen Chancen und Risiken enthalten (§§ 289 Abs. 1 S. 4, 315 Abs. 1 S. 5 HGB). Ein Unternehmen wird als kapitalmarktorientiert bezeichnet, wenn von

ihm ausgegebene Eigenkapitalanteile oder Schuldtitel an einer Börse gehandelt werden oder dies beantragt ist (vgl. auch § 264d HGB). Für gesellschaftsrechtlich verbundene Unternehmen kommt noch die Pflicht zur Erstellung eines Konzernabschlusses hinzu, in dem die Konzernmutter die Jahresergebnisse und die Bilanzen

aller in den Konzernkreis einbezogener Unternehmen zusammenfassen muss (§§ 290 ff. HGB). Kapitalmarktorientierte Muttergesellschaften von Konzernen müssen den Konzernabschluss nach den Internationalen Rechnungslegungsstandards IFRS aufstellen.

Übersicht zur handelsrechtlichen Rechnungslegung

Rechtsform	Gesetzliche Pflichten			
	Buchführungspflicht	Pflicht zur Erstellung eines Jahresabschlusses	Pflicht zur Abschlussprüfung	Publizitätspflicht
Kleiner Einzelkaufmann (Umsatz < 500 T€, Gewinn < 50 T€)	nein (§ 241a HGB)	nein (§ 242 Abs. 4 HGB)	entfällt	entfällt
Einzelkaufmann (Umsatz > 500 T€, Gewinn > 50 T€)	ja (§ 238 HGB)	ja: Bilanz, Gewinn- und Verlustrechnung (§§ 242 Abs. 1–3, 247 HGB);	nein	nein
Kleine und mittlere Personenhandels-gesellschaften (OHG, KG)	ja (§ 238 HGB)	ja: Bilanz, Gewinn- und Verlustrechnung (§§ 242 Abs. 1–3, 247 HGB)	nein	nein
Kapitalistische Personenhandels-gesellschaften (voll haftende Gesellschaf-ter sind ausschließlich Kapitalgesellschaften)	ja (§§ 238, 266, 275 HGB)	ja: Bilanz, Gewinn- und Verlustrechnung, Anhang, Lagebericht (§§ 264a, 264 Abs. 1 S. 1 HGB)	ja (§§ 264a, 316 HGB)	ja: Jahresabschluss mit Anhang und Bestätigungsvermerk, Lagebericht, Ergebnis-Verwendung (§§ 325, 264a HGB)
	Größenabhängige Erleichterungen wie für Kapitalgesellschaften			
Großes Personen-unternehmen (Einzelkaufmann oder Personenhandels-gesellschaft) mit Bilanzsumme > 65 Mio. €, Umsatz > 130 Mio. € oder > 5.000 Arbeit-nehmer (§ 1 PublG)	ja (§ 238 HGB)	ja: Bilanz, Gewinn- und Verlustrechnung (§§ 5 PublG, 265 ff. HGB)	ja (§ 6 PublG)	ja: Bilanz, Gewinn- und Verlustrechnung (§ 9 PublG)
Kleine Kapitalgesell-schaft Bilanzsumme: < 4,84 Mio. €, Umsatzerlöse: < 9,68 Mio. € Arbeitnehmer: < 50, vgl. § 267 Abs. 1 HGB)	ja (§ 238 HGB)	ja: verkürzte Bilanz (§ 266 Abs. 1 S. 3 HGB), verkürzte Gewinn- und Verlustrechnung (§ 276 HGB), reduzierter Anhang (§ 288 Abs. 1 HGB)	nein (§ 316 Abs. 1 S. 1 HGB)	ja: Bilanz, Anhang (§ 326 HGB)

Rechtsform	Gesetzliche Pflichten			
	Buchführungspflicht	Pflicht zur Erstellung eines Jahresabschlusses	Pflicht zur Abschlussprüfung	Publizitätspflicht
Mittelgroße Kapitalgesellschaft (Bilanzsumme: < 19,25 Mio. Euro, Umsatzerlöse: < 38,5 Mio. Euro, Arbeitnehmer: < 250; vgl. § 267 Abs. 2 HGB)	ja (§ 238 HGB)	ja: Bilanz (§ 266 HGB), verkürzte Gewinn- und Verlustrechnung (§ 276 HGB), Anhang, Lagebericht (§ 264 Abs. 1 HGB)	ja (§ 316 Abs. 1 HGB)	ja: Jahresabschluss mit Anhang und Bestätigungsvermerk, Lagebericht, Bericht des Aufsichtsrates, Ergebnisverwendung (§ 325 HGB)
Große Kapitalgesellschaft	ja (§ 238 HGB)	ja: Bilanz (§ 266 HGB), Gewinn und Verlustrechnung (§ 275 HGB), Anhang, Lagebericht (§ 264 Abs. 1 HGB)	ja (§ 316 Abs. 1 HGB)	ja: Jahresabschluss mit Anhang und Bestätigungsvermerk, Lagebericht, Bericht des Aufsichtsrates, Ergebnisverwendung (§ 325 HGB)
kapitalmarkt-orientierte Kapitalgesellschaft	ja (§ 238 HGB)	ja: Bilanz, Gewinn- und Verlustrechnung, Anhang, Lagebericht, Kapitalflussrechnung, Eigenkapitalpiegel (§ 264 Abs. 1 HGB)	ja (§ 316 Abs. 1 HGB)	ja: Jahresabschluss mit Anhang und Bestätigungsvermerk, Lagebericht, Ergebnisverwendung, Erklärung zur Corporate Governance (§ 325 HGB)
Kapitalmarktorientiertes Mutterunternehmen von Konzernen	ja (§ 238 HGB)	ja: Bilanz, Gewinn- und Verlustrechnung, Anhang, Lagebericht (§ 264 Abs. 1 HGB), zusätzlich Konzernabschluss nach IFRS (§ 315a HGB)	ja (§ 316 Abs. 1 HGB)	ja: Jahresabschluss mit Anhang und Bestätigungsvermerk, Lagebericht, Ergebnisverwendung, Erklärung zur Corporate Governance (§ 325 HGB), Konzernabschluss und Konzernlagebericht (§ 290 HGB)

■ 8.2 Anforderungen an eine elektronische Buchführung

Das Gesetz gestattet es, für die Buchführung elektronische Datenverarbeitung (EDV) einzusetzen (§ 239 Abs. 4 HGB). Für die EDV-Buchführung gelten im Wesentlichen dieselben Anforderungen wie für die Buchführung auf Papier: Sämtliche Geschäftsvorfälle des Unternehmens sind vollständig auf Konten aufzuzeichnen, Belege und sonstige Unterlagen sind während der gesetzlichen Fristen aufzubewahren. Jeder Geschäftsvorfall muss sich in den Aufzeichnungen und Unterlagen der Buchführung niederschlagen. Darüber hinaus muss sich jeder Geschäftsvorfall von seiner Auswirkung auf den Jahresabschluss bis zum Beleg (retrograd) und vom Beleg über die Konten bis zur Position im Jahresabschluss (progressiv) nachverfolgen lassen (§ 238 Abs. 1 S. 3 HGB). Desgleichen sind beim Einsatz von EDV für die Buchführung die Grundsätze ordnungsmäßiger Buchführung zu beachten (§ 239 Abs. 4 S. 1 HGB). Mit dem Einsatz elektronischer Medien für die Buchführung sind einige Besonderheiten verbunden. Diese sind in den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) niedergelegt.

Die gesetzlichen Anforderungen des HGB und sonstige gesetzliche Vorgaben an die Buchführung sind in der am Markt angebotenen Buchhaltungssoftware standardmäßig abgebildet und berücksichtigt. Die Installation einer Buchhaltungssoftware reicht jedoch noch nicht aus. Daneben ist auf eine angemessene Organisation der Buchführung, die korrekte rechtliche Beurteilung und Verbuchung der einzelnen Geschäftsvorfälle, die Einrichtung eines internen Kontrollsystems (organisatorische Maßnahmen zum Schutz und zur Sicherung des Betriebsvermögens sowie der Berichterstattung über die betriebliche Entwicklung), die Dokumentation der eingerichteten Verfahren und der eingesetzten Programme und auf die korrekte Berichterstattung im Jahresabschluss zu achten.

■ 8.3 Verantwortlichkeiten und Sanktionen

Die Verantwortlichkeiten für die Buchführung im Unternehmen sind gesetzlich klar geregelt. In Aktiengesellschaften ist der Vorstand für die Buchführung verantwortlich (§ 91 Abs. 1 AktG). Für die GmbH liegt die Verantwortlichkeit für die Buchführung bei den Geschäftsführern (§ 41 GmbHG), für die Genossenschaft beim Vorstand (§ 33 Abs. 1 GenG). Ein Einzelkaufmann ist vollumfänglich selbst verantwortlich für die Ordnungsmäßigkeit der Buchführung. In Personenhandelsgesellschaften obliegen die Organisation und Überwachung der Buchführung den geschäftsführenden Gesellschaftern (vgl. z. B. für die OHG §§ 114, 116 Abs. 1 HGB, für die KG in Verbindung mit §§ 161 Abs. 2, 164 HGB). Im Rahmen ihrer Kontrollpflichten haben sich die Aufsichtsgremien von Kapitalgesellschaften bei den geschäftsführenden Organen nach der Organisation der Buchführung und nach möglichen Risiken in diesem Bereich zu erkundigen und die Ordnungsmäßigkeit der Buchführung zu kontrollieren.

Da die Pflicht zur Buchführung eine gesetzlich zwingende Pflicht ist, kann sie nicht durch Regelungen im Gesellschaftsvertrag oder im Anstellungsvertrag der vertretungsberechtigten Personen eines Unternehmens umgangen werden. Es ist zwar zulässig, für die Buchführung externe Dienstleister oder unternehmensintern weitere Personen einzuschalten. Dies entbindet die geschäftsführenden Personen im Unternehmen jedoch nicht von ihrer Verantwortung für die Buchführung. Dies kommt nicht zuletzt dadurch zum Ausdruck, dass der Kaufmann, die persönlich haftenden Gesellschafter einer Personenhandelsgesellschaft bzw. die vertretungsberechtigten Organe einer Kapitalgesellschaft den Jahresabschluss zu unterzeichnen haben (§ 245 HGB). Sie haben ihre Verantwortung bei Delegation der Buchführung durch sorgfältige Auswahl des Auftragnehmers, durch seine Überwachung und die Kontrolle seiner Arbeit wahrzunehmen.

An die Verletzung der Buchführungspflicht knüpft das Gesetz vergleichsweise harte Sanktionen. Bereits die Missachtung der gesetzlichen Vorgaben für einzelne Positionen der Bilanz oder der Gewinn- und Verlustrechnung stellt eine Ordnungswidrigkeit dar, die eine Geldbuße bis zu 50.000 Euro nach sich ziehen kann (§ 334 HGB). Die vorsätzliche unrichtige Darstellung der Unternehmensverhältnisse im Jahresabschluss ist eine Straftat (§ 331 HGB, § 283b StGB), die mit Freiheitsstrafe bis zu drei Jahren geahndet werden kann. Treten zur Missachtung der Buchführungspflichten weitere Umstände hinzu (z. B. Insolvenz des Unternehmens und Verschleierung der Vermögensverhältnisse), sind sogar Freiheitsstrafen bis zu 5 Jahren möglich (§ 283 StGB). Verstößt ein Geschäftsführer oder ein Vorstandsmitglied gegen seine Kontrollpflichten, so kann dies außerdem das Unternehmen zu einer fristlosen Kündigung des Arbeitsvertrages nach § 626 Abs. 1 BGB berechtigen. Hinzu kommen mögliche Schadenersatzforderungen nach den allgemeinen Haftungsvorschriften (z. B. §§ 93 Abs. 2 AktG, 43 Abs. 2 GmbHG, 34 Abs. 2 GenG).

■ 8.4 Interne Kontrollen

Die Verantwortlichkeit der Unternehmensführung für den Bereich der Buchführung konkretisiert sich vor allem in der Pflicht zur Einrichtung effektiver Kontrollsysteme. So obliegt nach Auffassung des OLG Jena (Urteil vom 12.08.2009, 7 U 244/07) dem Geschäftsführer einer GmbH, ein effizientes Kontrollsystem zur Aufdeckung und Unterbindung von Scheinrechnungen und entsprechenden fehlerhaften Buchungen einzurichten. Ist die GmbH Muttergesellschaft eines Konzerns, müsse das Kontrollsystem die Geschäfte aller konzernangehörigen Unternehmen umfassen. Da die Buchführung zum Aufgabenkreis der Geschäftsführung insgesamt gehört, bestehe bei mehreren Geschäftsführern eine Pflicht zur Kontrolle der Buchführung auch dann, wenn die Aufgaben zwischen den Geschäftsführern aufgeteilt sind.

Insoweit hat die Rechtsprechung für GmbH-Geschäftsführer eine ähnliche Kontrollpflicht postuliert wie sie für Vorstandsmitglieder von Aktiengesellschaften in § 91 Abs. 2 AktG gesetzlich niedergelegt und mit Hinblick auf die Rechnungslegung kapitalmarktorientierter Gesellschaften in § 289 Abs. 5 HGB konkretisiert ist. Danach müssen kapitalmarktorientierte Unternehmen über die Einrichtung eines Kontroll- und Risikomanagements in ihrem Lagebericht Auskunft geben (§§ 289, 317 HGB). Ein solches System soll die Ordnungsmäßigkeit und Verlässlichkeit der Buchführung gewährleisten, die korrekte Anwendung der gesetzlichen Buchführungsvorschriften kontrollieren und letztlich auch Schädigungen des Unternehmensvermögens verhindern helfen. Für nicht börsennotierte Kapitalgesellschaften und andere Unternehmen enthält das HGB keinen Hinweis auf ein Kontrollsystem für Buchführung oder Rechnungslegung.

Eine gesetzliche Pflicht zur Einrichtung eines effektiven Kontrollsystems für die Finanzberichterstattung ergibt sich auch aus Section 404 des US-amerikanischen Sarbanes-Oxley-Act. Dieses Gesetz betrifft jedoch nur deutsche Tochtergesellschaften US-amerikanischer Konzerne, die eine einheitliche Rechnungslegung mit ihrer Muttergesellschaft gewährleisten müssen. In Deutschland wird die Pflicht zur Einrichtung eines internen Systems für Kontrollen bei der Buchführung (IKS) insbesondere für die EDV-Buchführung aus den Grundsätzen ordnungsmäßiger Buchführung abgeleitet, die für alle Unternehmen gelten. Zur Ordnungsmäßigkeit interner Buchführungskontrollen gehört nicht zuletzt, dass sie mit ihren Eigenheiten im jeweiligen Unternehmen dokumentiert werden.

In Aktiengesellschaften ist neben dem Vorstand der Aufsichtsrat ebenfalls zur Kontrolle der Rechnungslegung berufen (§§ 111, 107 Abs. 3 AktG). Dabei hat er insbesondere zu prüfen, ob der Vorstand seinen Sorgfaltspflichten bei der Buchführung und bei der Erstellung des Jahresabschlusses nachkommt. Daher muss in den Aufsichtsräten für kapitalmarktorientierte Kapitalgesellschaften mindestens ein Mitglied über Sachverstand auf den Gebieten der Rechnungslegung oder der Abschlussprüfung verfügen (§ 100 Abs. 5 AktG).

■ 8.5 Externe Kontrollen

Mittelgroße und große Kapitalgesellschaften i.S.d. § 267 HGB sowie Personengesellschaften ohne persönlich haftende natürliche Personen (§ 264a HGB) müssen ihren Jahresabschluss durch unabhängige Wirtschaftsprüfer überprüfen lassen. Im Rahmen der Jahresabschlussprüfung von kapitalmarktorientierten Kapitalgesellschaften untersucht der Wirtschaftsprüfer auch das Vorhandensein und die Beschreibung des Risikomanagementsystems in Bezug auf den Rechnungslegungsprozess (§§ 317 Abs. 2 S. 2 i.V.m. § 289 Abs. 5 HGB). Bei börsennotierten Aktiengesellschaften hat der Abschlussprüfer nach § 317 Abs. 4 HGB insbesondere zu prüfen, ob der Vorstand seinen Pflichten zur Einrichtung eines Überwachungssystems nach § 91 Abs. 2 AktG nachgekommen ist. Da über die eingerichteten Risikoerkennungs- und Kontrollsysteme im Jahresabschluss zu berichten ist, unterliegt die Ordnungsmäßigkeit dieser Systeme wie der Jahresabschluss selbst der Prüfung durch den Wirtschaftsprüfer (§ 171 Abs. 1 AktG).

Die Abschlüsse börsennotierter Gesellschaften werden zusätzlich in einem halbstaatlichen Verfahren kontrolliert (»Enforcement-Verfahren«). In einer ersten Stufe prüft die (privatrechtlich als Verein organisierte) Deutsche Prüfstelle für Rechnungslegung (DPR), ob die Vorschriften über Buchführung und Abschlusserstellung eingehalten wurden. Stellt die DPR dabei Fehler fest, weist sie das geprüfte Unternehmen darauf hin und veranlasst eine Korrektur der Fehler. Weigert sich das Unternehmen, die Korrekturen vorzunehmen, schaltet sich die Bundesanstalt für Finanzdienstleistungsaufsicht als staatliche Behörde ein. Bei Verstößen gegen Rechnungslegungspflichten drohen neben Bußgeldern und ggf. strafrechtlichen Sanktionen vor allem negative Folgen für Image, Aktienkurs und Geschäftsbeziehungen des Unternehmens. Denn Verstöße gegen Rechnungslegungspflichten müssen veröffentlicht werden.

9 Besteuerung

Die Steuer-Compliance umfasst die Pflicht, die geltenden Steuergesetze zu befolgen, zeitgerecht Steuererklärungen und -anmeldungen abzugeben und verschiedene Dokumentationen zu erstellen (z. B. über Verrechnungspreise). Diese Pflichten der Unternehmen im Besteuerungsverfahren ergeben sich vor allem aus der Abgabenordnung (AO). Compliance bei der Besteuerung setzt voraus, dass das Unternehmen seine steuerlichen Pflichten und die Sanktionen bei Nichterfüllung kennt. Da das Steuerrecht an vielen Stellen (z. B. bei der steuerlichen Beurteilung grenzüberschreitender Geschäftsvorfälle) komplex und unübersichtlich ist und sich außerdem ständig ändert, erfordert die »richtige« Anwendung des Steuerrechts vielfach ein hohes Maß an spezialisiertem Wissen. Dieses Wissen lässt sich nicht im Rahmen eines Compliance-Leitfadens vermitteln. Deshalb kann hier nur ein sehr grober Überblick gegeben werden.

■ 9.1 Steuerrechtliche Mitwirkungspflichten

Neben der Pflicht zur Zahlung der festgesetzten Steuern gehören Mitwirkungspflichten bei der Feststellung der Besteuerungsgrundlagen zu den wichtigsten steuerlichen Pflichten eines Unternehmens. Dies fängt schon bei der Unternehmensgründung mit der Pflicht an, die Aufnahme einer gewerblichen Tätigkeit bei der Gemeinde (§ 138 AO) und die Gründung einer Kapitalgesellschaft beim zuständigen Finanzamt (§ 138 AO) anzuzeigen. Die wesentlichen Mitwirkungspflichten sind jedoch die Steuererklärungspflichten (§§ 149 ff. AO in Verbindung mit Einzelsteuergesetzen). Weitere Mitwirkungspflichten sind z. B. die Pflicht zur Aufzeichnung des Wareneingangs und –ausgangs (§ 143, 144 AO). Diese Aufzeichnungen sind allerdings bereits im Rahmen der handelsrechtlichen Buchführungspflicht zu führen. Darüber hinaus enthält § 153 AO die Pflicht, unrichtige Angaben gegenüber der Finanzverwaltung zu berichtigen, sobald der Steuerpflichtige oder sein Berater die Unrichtigkeit erkennt. Geschieht dies nicht, droht eine Strafbarkeit wegen Steuerhinterziehung nach § 370 Abs. 1 Nr. 2 AO.

Mittlerweile verlangt der Gesetzgeber, dass Steueranmeldungen und Steuererklärungen für alle wesentlichen Steuerarten (Körperschaftsteuer, Einkommensteuer für Unternehmer, Gewerbesteuer, Umsatzsteuer, Lohnsteuer) in elektronischer Form bei der Finanzverwaltung eingereicht werden. Das bedeutet, dass entweder das Unternehmen selbst oder sein Steuerberater über einen internetfähigen Computer verfügen muss. Die notwendigen Formulare hält die Finanzverwaltung in elektronischer Form unter www.elster.de im Internet bereit. Die elektronischen Schnittstellen der Finanzverwaltung zur Annahme von elektronisch übermittelten Steuerdaten können aber auch von sämtlichen gängigen Steuer- und Buchführungsprogrammen bedient werden.

Da die Besteuerung letztendlich an die Betrachtung von Einnahmen und Ausgaben sowie sonstige Veränderungen des Betriebsvermögens anknüpft und diese Vorgänge in der Buchführung des Unternehmens abgebildet werden, gehört eine ordnungsmäßige Buchführung auch im Steuerrecht zu den Grundanforderungen (vgl. §§ 140 ff. AO). Während das Handelsrecht keine geografische Begrenzung der Buchführung kennt, also auch die Führung von Büchern und Aufzeichnungen im Ausland erlaubt, ist das Steuerrecht an diesem Punkt strenger. Nach § 146 Abs. 2 S. 1 AO sind steuerliche Aufzeichnungen in Deutschland zu führen und aufzubewahren. Soweit die steuerlichen Aufzeichnungen und Unterlagen in elektronischer Form vorliegen, kann die Verarbeitung und Aufbewahrung jedoch im Ausland erfolgen. Hierfür müssen allerdings verschiedene Voraussetzungen erfüllt sein, insbesondere muss die vorherige Zustimmung des zuständigen Finanzamts vorliegen (§ 146 Abs. 2a AO).

Am Ende eines jeden Geschäftsjahres müssen die Unternehmen gegenüber der Finanzverwaltung ihre wirtschaftlichen Ergebnisse offen legen. Hierzu sind neben der Steuererklärung entweder eine Einnahmen-Überschuss-Rechnung (Einzelkaufleute mit kleinerem Geschäftsbetrieb, Selbständige) oder ein Jahresabschluss mit zusätzlichen steuerlichen Angaben (größere Unternehmen) beim Finanzamt einzureichen. Ab dem Geschäftsjahr 2013 besteht auch für den Jahresabschluss eine Pflicht zur elektronischen Übermittlung (E-Bilanz). Die hierfür notwendigen Anpassungen in der Buchführung sollten möglichst zeitnah vorgenommen werden.

Für die Sammlung, Verbuchung und Aufbereitung steuerrelevanter Daten setzen die Unternehmen heutzutage überwiegend IT ein. Dabei ist darauf zu achten, dass die verwendete Software die jeweils aktuelle Rechtslage abbildet und nachvollzieht. Deshalb ist es sinnvoll, die eingesetzte Besteuerungssoftware mindestens einmal pro Veranlagungszeitraum (Geschäftsjahr) per Update zu aktualisieren.

Soweit ein Unternehmen ein elektronisches Buchführungssystem in Betrieb hat, muss es der Finanzverwaltung im Rahmen von Steueraußenprüfungen und neuerdings auch bei Umsatzsteuernachschauen einen elektronischen Datenzugriff auf die Buchführungsdaten ermöglichen. Weitere Informationen hierzu können dem BITKOM-Leitfaden zum elektronischen Datenzugriff der Finanzverwaltung entnommen werden.

■ 9.2 Sanktionen

Die wesentliche Sanktion für unzureichende Steuer-Compliance ist eine überhöhte Steuerlast. Die Vermeidung überhöhter Steuerzahlungen gehört damit zu den wichtigsten Aufgaben von Steuer-Compliance. Ist beispielsweise die Buchführung für steuerliche Zwecke unzureichend, kann die Finanzverwaltung die Besteuerungsgrundlagen schätzen. Dabei baut die Finanzverwaltung regelmäßig einen Risikozuschlag zulasten des Steuerpflichtigen ein. Daraus ergibt sich als wichtiges Tätigkeitsfeld für die steuerrechtliche Compliance die zeitnahe und ordnungsmäßige Dokumentation steuerrelevanter Vorgänge. Daneben drohen einschneidende strafrechtliche Konsequenzen. Sind gegenüber der Finanzverwaltung unrichtige oder unvollständige Angaben gemacht, falsche Angaben nicht nachträglich korrigiert oder sogar steuerrelevante Sachverhalte verschwiegen worden, kann dies als Steuerhinterziehung nach § 370 AO mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe geahndet werden.

Zur Durchsetzung einzelner Anordnungen kann die Finanzverwaltung wie jede andere Verwaltungsbehörde auf Zwangsmittel wie Zwangsgeld oder Ersatzvornahme zurückgreifen. Als weitere Sanktion steht der Finanzverwaltung das sog. Verzögerungsgeld zur Verfügung. Es kann nach § 146 Abs. 2b AO festgesetzt werden, um den Steuerpflichtigen zur Einräumung des elektronischen Datenzugriffs oder zur Erfüllung von Mitwirkungspflichten anzuhalten. Das Verzögerungsgeld beträgt mindestens 2.500 Euro und höchstens 250.000 Euro.

10 Archivierungspflichten

■ 10.1 Archivierungspflichten nach Handelsrecht

Zur handelsrechtlichen Buchführung gehört neben der eigentlichen Verarbeitung der Informationen aus den Geschäftsvorfällen in Form von Buchungen auch die geordnete Aufbewahrung der geschäftlichen Unterlagen (Archivierung). So verpflichtet § 257 HGB alle Buchführungspflichtigen zur Aufbewahrung von Geschäftsunterlagen. Dazu gehören alle Schriftstücke, die das Handelsgeschäft betreffen (Handelsbriefe), Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse und Buchungsbelege. Bei Handelsbriefen gilt die Aufbewahrungspflicht nicht nur für empfangene Dokumente, sondern auch für Kopien der vom Kaufmann versandten Korrespondenz, die er nach § 238 Abs. 2 HGB anzufertigen hat. Handelsbriefe sind sechs Jahre aufzubewahren, die restlichen Geschäftsunterlagen 10 Jahre (§ 257 Abs. 4 HGB). Die Aufbewahrungsfrist beginnt aber erst am Schluss des Kalenderjahres, in dem die Unterlagen angefertigt wurden (§ 257 Abs. 5 HGB). Im Regierungsentwurf des Jahressteuergesetzes 2013 ist eine Verkürzung von Aufbewahrungsfristen enthalten; der weitere gesetzgeberische Prozess bleibt abzuwarten.

Nicht nur für die Buchführung selbst, sondern auch für die Aufbewahrung von Unterlagen sind die Grundsätze ordnungsmäßiger Buchführung (GoB) zu beachten, die die gesetzlichen Vorgaben konkretisieren. Das bedeutet, dass alle Buchführungsunterlagen vollständig sein müssen, insbesondere müssen sämtliche Buchungsbelege aufbewahrt werden. Die Unterlagen dürfen nicht nachträglich verändert werden und müssen innerhalb der gesetzlichen Aufbewahrungsfristen jederzeit vorgelegt werden können.

Wie bei der Aufzeichnung von Geschäftsvorfällen hat der Buchführungspflichtige auch bei der Aufbewahrung von Belegen und sonstigen Unterlagen eine freie Wahl des Datenträgers (§§ 238 Abs. 2, 257 Abs. 3 HGB), soweit die gewählte Aufbewahrungsform den Grundsätzen

ordnungsmäßiger Buchführung entspricht. Das bedeutet, die Archivierung kann auch auf elektronischen Medien erfolgen. Voraussetzung dafür ist insbesondere, dass die Unterlagen oder originalgetreue Kopien während der Aufbewahrungsfrist wieder lesbar gemacht werden können. Das Handelsrecht lässt zu Aufbewahrungszwecken auch eine Konvertierung von elektronischen Unterlagen (z. B. geschäftliche E-Mails) in Papierunterlagen und umgekehrt zu (§ 257 Abs. 3 HGB). Lediglich Eröffnungsbilanzen und Abschlüsse sind zwingend in Papierform aufzubewahren (§ 257 Abs. 3 S. 1 HGB). Die gesetzlichen Vorgaben sind standardmäßig in Programmen zum Dokumentenmanagement berücksichtigt, die zur Unterstützung des Buchführungspflichtigen bei der Archivierung von Unterlagen eingesetzt werden können.

■ 10.2 Archivierungspflichten im Steuerrecht

Unternehmen, die nach anderen Vorschriften zur Buchführung und zur Aufbewahrung von Unterlagen verpflichtet sind, müssen diese Pflichten auch für die Besteuerung erfüllen (vgl. § 140 AO). Dies bedeutet jedoch nicht, dass Unternehmen von sämtlichen Aufzeichnungs- und Archivierungspflichten befreit sind, wenn eine anderweitige Buchführungspflicht nicht besteht. Denn das Steuerrecht begründet in § 141 AO eine eigene Buchführungspflicht für steuerliche Zwecke, die eine Pflicht zur Aufbewahrung der steuerrelevanten Daten und Unterlagen einschließt. Die steuerlichen Aufbewahrungspflichten sind im Wesentlichen identisch mit den handelsrechtlichen Aufbewahrungspflichten, gehen aber in einigen Details über diese hinaus. Aufzubewahren sind nach § 147 Abs. 1 AO Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen, die empfangenen Handels- oder Geschäftsbriefe, Wiedergaben der abgesandten Handels- oder Geschäftsbriefe und Buchungsbelege.

Eine Sonderregelung für Rechnungen enthält § 14b UStG. Bei Rechnungen – Papierrechnungen und elektronische Rechnungen werden inzwischen rechtlich gleichbehandelt – muss der Unternehmer die Echtheit der Herkunft, die Unversehrtheit des Inhalts und die Lesbarkeit gewährleisten (§ 14 Abs. 1 S. 2 UStG). Dies kann bei elektronischen Rechnungen durch eine qualifizierte elektronische Signatur, das EDI-Verfahren (§ 14 Abs. 3 UStG) oder durch innerbetriebliche Kontrollverfahren erreicht werden, die einen verlässlichen Prüfpfad zwischen Rechnung und Leistung schaffen (sog. »dritter Weg«, § 14 Abs. 1 S. 6 UStG). Wenn der Unternehmer elektronische Rechnungen mit qualifizierter elektronischer Signatur akzeptiert, ist neben der Rechnung selbst auch die qualifizierte elektronische Signatur und das Prüfprotokoll als Nachweis der gültigen Signaturprüfung zu archivieren (§ 14b Abs. 1 S. 2 UStG). Bei der Annahme von sonstigen elektronischen Rechnungen (»dritter Weg«) muss die Echtheit der Rechnungserkunft, die Unversehrtheit ihres Inhalts und die Lesbarkeit für den gesamten Aufbewahrungszeitraum erhalten bleiben (§ 14b Abs. 1 S. 2 UStG; vgl. zu elektronischen Rechnungen auch BMF-Schreiben vom 2. Juli 2012).

Die steuerrechtliche Aufbewahrungsfrist für einzelne Unterlagen ergibt sich aus § 147 Abs. 1 und Abs. 3 AO. Danach sind Handels- und Geschäftsbriefe sechs Jahre, andere Buchführungsunterlagen und Buchungsbelege zehn Jahre aufzubewahren. In Ausnahmefällen kann auch eine längere Frist gelten. Wie im Handelsrecht beginnt die Aufbewahrungsfrist erst am Ende des Jahres, in dem die jeweilige Aufzeichnung vorgenommen wurde (§ 147 Abs. 4 AO). Für Rechnungen gilt nach § 14b Abs. 1 S. 1 UStG ebenfalls eine zehnjährige Aufbewahrungsfrist. Im Regierungsentwurf des Jahressteuergesetzes 2013 ist eine Verkürzung von Aufbewahrungsfristen enthalten; der weitere gesetzgeberische Prozess bleibt abzuwarten.

Nach § 147 Abs. 2 AO ist im Steuerrecht ebenso wie im Handelsrecht eine elektronische Archivierung zulässig. Mit Ausnahme der Jahresabschlüsse, der Eröffnungsbilanz und bestimmter Unterlagen für Zollanmeldungen, die in Papierform aufbewahrt werden müssen, können steuerliche Unterlagen auch als Wiedergabe auf einem Bildträger oder auf anderen Datenträgern aufbewahrt

werden. Voraussetzung ist, dass dies den Grundsätzen ordnungsmäßiger Buchführung entspricht und sichergestellt ist, dass die Wiedergabe oder die Daten mit den empfangenen Handels- oder Geschäftsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden (§ 147 Abs. 2 Ziff. 1 AO). Weiterhin müssen die Dokumente während der Dauer der Aufbewahrungsfrist jederzeit verfügbar sein, unverzüglich lesbar gemacht und maschinell ausgewertet werden können (§ 147 Abs. 2 Ziff. 2 AO). Soweit eine ordnungsgemäße elektronische Archivierung stattgefunden hat, ist auch die Vernichtung der Originaldokumente nach dem Einscannen aus steuerrechtlicher Sicht zulässig. Hierbei ist jedoch zu beachten, dass in einem etwaigen Zivilverfahren der Beweiswert von digitalisierten Unterlagen geringer sein kann als der Beweiswert von Originaldokumenten. Auch nach anderen Rechtsvorschriften kann die Aufbewahrung im Original vorgeschrieben sein. Originär digitale, steuerrelevante Daten und Unterlagen sind zwingend elektronisch aufzubewahren.

Steuerrelevante Daten und Unterlagen müssen während der Aufbewahrungsfristen für Prüfungen durch die Finanzverwaltung zur Verfügung stehen. Dafür verlangt die Finanzverwaltung auch einen elektronischen Zugang zu den steuerlichen Daten und Aufzeichnungen sowie die Möglichkeit maschineller Auswertungen (§ 147 Abs. 6 AO). Das Unternehmen hat dafür Sorge zu tragen, dass ein solcher elektronischer Zugang für die Finanzverwaltung besteht, gleichzeitig aber das Zugriffsrecht auf steuerrelevante Daten und Unterlagen beschränkt bleibt. Dies lässt sich durch Berechtigungskonzepte erreichen, die sich in gängiger betriebswirtschaftlicher Software einrichten lassen. (vgl. zu weiteren Einzelheiten den BITKOM-Leitfaden zum elektronischen Datenzugriff der Finanzverwaltung, S. 17).

■ 10.3 Archivierungsrichtlinie im Unternehmen

Gewissermaßen als Kehrseite der Aufbewahrungspflichten sind bestimmte Löschungspflichten zu beachten. Diese ergeben sich zwar nicht aus dem Handels- oder Steuerrecht, wohl aber aus dem Datenschutzrecht, insbesondere aus § 35 Abs. 2 Bundesdatenschutzgesetz (BDSG). Demnach sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist (§ 35 Abs. 2 Ziff. 3 BDSG). Folglich sollten Dokumente mit personenbezogenen Daten ohne handelsrechtliche oder steuerliche Relevanz, die für den Geschäftsbetrieb nicht mehr benötigt werden, möglichst zeitnah gelöscht werden.

Für international tätige Unternehmen können neben den Anforderungen durch das deutsche Recht die sogenannten »Electronic Discovery«-Regelungen von Bedeutung sein. Demnach können auch deutsche Unternehmen bei einer rechtlichen Auseinandersetzung in den USA verpflichtet sein, elektronisch gespeicherte Daten zu reproduzieren und vorzulegen.

Um die Löschungspflichten einerseits und die Archivierungspflichten andererseits rechtskonform im Unternehmen umzusetzen, ist die Erarbeitung einer unternehmensinternen Archivierungs-Richtlinie bzw. einer E-mail-Policy empfehlenswert. Diese sollte zum Ziel haben, eine unnötige Speicherung von Daten zu vermeiden und die Löschung von solchen Datensätzen zu verhindern, die bei einem möglicherweise bevorstehenden Rechtsstreit oder für anstehende externe Prüfungen gebraucht werden.

11 Unternehmenspublizität

Der Betrieb eines Unternehmens ist mit vielfältigen Informations- und Berichtspflichten verbunden. Grundlegende Daten zum Unternehmen müssen in der geschäftlichen Korrespondenz angegeben und in öffentlichen Registern hinterlegt werden. Tritt das Unternehmen mit einer eigenen Seite im Internet auf, muss es die Urheberschaft für diese Internetseite offen legen. Die Unternehmenspublizität im weiteren Sinne umfasst auch die Informations- und Mitwirkungspflichten gegenüber der Finanzverwaltung (vgl. dazu Kapitel 10).

■ 11.1 Anmeldungen zum Handelsregister

Zur Information des allgemeinen Geschäftsverkehrs hat jeder Kaufmann grundlegende rechtliche Vorgänge mit Bezug zu seinem Unternehmen an das Handelsregister zu melden und durch dieses öffentlich zu machen. Kaufmann ist jede Person, die einen Gewerbebetrieb von gewissem Umfang betreibt (§ 1 HGB). Kapitalgesellschaften und Personenhandelsgesellschaften sind schon aufgrund ihrer Rechtsform als Kaufleute anzusehen.

Im Handelsregister eintragungspflichtig sind z. B.:

- Firma (Bezeichnung des Unternehmens im Geschäftsverkehr) und Geschäftsanschrift des Unternehmens (§ 29 HGB);
- Änderungen, Übertragungen oder Erlöschen der Firma, Verlegung einer Niederlassung, Änderung der Geschäftsanschrift (§ 31 HGB);
- Erteilung und Erlöschen von Prokura (§ 53 HGB);
- bei OHG: Firma, Sitz, Geschäftsanschrift, Namen und Wohnort der Gesellschafter, Vertretungsberechtigung (§§ 106, 143 HGB).

Seit dem 1. Januar 2007 werden alle Handelsregister elektronisch geführt (§ 8 Abs. 1 HGB). Entsprechend sind alle Eintragungen zum Handelsregister elektronisch anzumelden (§ 12 Abs. 1 S. 1 HGB). Da außerdem die eingereichten Dokumente vom Unternehmen bzw.

seinen geschäftsführenden Organen unterschrieben und die Unterschriften notariell beglaubigt werden müssen, empfiehlt sich, die Anmeldungen vom Notar vornehmen zu lassen.

Kaufleute, persönlich haftende Gesellschafter oder die vertretungsberechtigten Organe (Geschäftsführer, Vorstand) einer Gesellschaft können durch Zwangsgeld bis zu 5.000 Euro zur Anmeldung eintragungspflichtiger Vorgänge angehalten werden (§ 14 HGB). Auf eintragungspflichtige Tatsachen kann sich ein Unternehmen nur berufen, soweit sich die Tatsachen auch aus dem Handelsregister ergeben (Publizitätswirkung des Handelsregisters nach § 15 HGB).

Da es sich beim Handelsregister um ein öffentliches Register handelt, kann jedermann Auskunft über die eingetragenen Rechtsverhältnisse verlangen und Einblick in die eingereichten Unterlagen nehmen.

■ 11.2 Veröffentlichungen im Unternehmensregister

Zum Aufgabenbereich der Unternehmensführung gehört es, die Eigentümer des Unternehmens über die geschäftlichen Aktivitäten und die Entwicklung des Unternehmens auf dem Laufenden zu halten. Für Personenunternehmen ab einer bestimmten Größenordnung (zu den einschlägigen Größenmerkmalen vgl. § 1 PubLG) und für Kapitalgesellschaften besteht darüber hinaus eine Pflicht zur Information über die Geschäftsentwicklung und über die finanzielle Lage des Unternehmens gegenüber der allgemeinen Öffentlichkeit bzw. einem nicht eingegrenzten Kreis von Interessenten (Publizitätspflicht). Diese Publizitätspflicht ist durch regelmäßige Aufstellung von Jahresabschlüssen und durch Einreichung der Jahresabschlüsse beim Betreiber des elektronischen Bundesanzeigers (<https://www.bundesanzeiger.de>) zu erfüllen. Soweit weitere Abschlussunterlagen zu erstellen sind (Lagebericht, Bericht des Aufsichtsrates, Prüfvermerk des

Wirtschaftsprüfers, Erklärung zum Corporate Governance Kodex nach § 161 AktG, Angaben zur Ergebnisverwendung), müssen auch diese Unterlagen beim Betreiber des elektronischen Bundesanzeigers eingereicht werden.

Wie bei der Buchführungspflicht kennt das Gesetz bei der Publizitätspflicht aber ebenfalls Erleichterungen für kleine und mittelgroße Unternehmen. Nach § 326 HGB müssen z. B. kleine Kapitalgesellschaften im Sinne des § 267 HGB lediglich ihre Bilanz mit Anhang einreichen. Kleine Personenunternehmen sind gänzlich von der Publizitätspflicht befreit. Erst wenn die Bilanzsumme höher ist als 65 Mio. Euro, die Umsatzerlöse eines Geschäftsjahres 130 Mio. Euro übersteigen oder innerhalb von 12 Monaten im Durchschnitt mehr als 5.000 Mitarbeiter beschäftigt sind, kommt auch für Personenunternehmen die Publizitätspflicht zur Anwendung. Personengesellschaften, bei denen ausschließlich Kapitalgesellschaften voll haftende Gesellschafter sind, werden hinsichtlich der Publizitätspflicht Kapitalgesellschaften gleich gestellt (§ 264a HGB).

Nach §§ 325 HGB, 9 PublG sind die gesetzlichen Vertreter von Kapitalgesellschaften, großen Personenhandels-gesellschaften und großen Einzelunternehmen für die Einreichung der Jahresabschlussunterlagen verantwortlich. Die Frist zur Einreichung der Unterlagen beträgt 12 Monate ab Abschlussstichtag. Unternehmen, die am 31. Dezember eines Jahres Stichtag für ihren Jahresabschluss haben, müssen diesen Abschluss also bis zum 31. Dezember des Folgejahres beim elektronischen Bundesanzeiger eingereicht haben. Die Frist ist nur gewahrt, wenn vor ihrem Ablauf die zur Veröffentlichung bestimmten Unterlagen vollständig eingereicht wurden. Für börsennotierte Unternehmen ist die Einreichungsfrist verkürzt und läuft bereits 4 Monate nach Abschlussstichtag ab (§ 325 Abs. 4 HGB).

Wird die Frist zur Einreichung der Jahresabschlussunterlagen versäumt, kann das hierfür zuständige Bundesamt der Justiz (BfJ) zunächst ein Mahnschreiben versenden (§ 335 Abs. 3 HGB), das mit Gebühren von 53,50 Euro verbunden ist. Darin werden die zur Vertretung des Unternehmens berufenen Personen mit Setzung einer Frist von

sechs Wochen ab Zugang der Mahnung zur Einreichung der notwendigen Unterlagen beim elektronischen Bundesanzeiger aufgefordert (§ 335 Abs. 3 HGB). Werden die Unterlagen dennoch nicht eingereicht, kann das BfJ gegen die Vertretungsorgane des Unternehmens ein Ordnungsgeld bis zu 25.000 Euro verhängen (§ 335 Abs. 1 HGB). Allein im Jahr 2010 wurden entsprechende Verfahren gegen etwa 144.000 Unternehmen geführt. Wird die Frist zur Einreichung der Unterlagen nur geringfügig überschritten, kann das BfJ das Ordnungsgeld auf ein Zehntel des ursprünglich angedrohten Betrages herabsetzen (§ 335 Abs. 3 S. 5 HGB). Die Rechtsprechung sieht eine Fristüberschreitung von maximal 2 Wochen als geringfügig an (LG Bonn, Beschluss v. 21.3.2011, Az. 35 T 1620/10). Ein Ordnungsgeld kann auch mehrmals festgesetzt werden, wenn ein Unternehmen seine Abschlussunterlagen trotz eines bereits verhängten Ordnungsgeldes nicht oder nicht vollständig einreicht.

Gegen die Pflicht zur Unternehmenspublizität und die damit verbundenen Sanktionen wurde bereits mehrfach Verfassungsbeschwerde beim Bundesverfassungsgericht erhoben. Das Bundesverfassungsgericht hat jedoch weder in der Offenlegungspflicht nach § 325 HGB noch in der Sanktionierung nach § 335 HGB und auch nicht in der praktischen Anwendung dieser Regelungen verfassungsrechtliche Bedenken gesehen (vgl. zuletzt BVerfG, Nichtannahmebeschluss vom 1.2.2011, Az.- 2 BvR 1236/10).

Seitdem zum 1. Januar 2007 das »Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister« (EHUG vom 10.11.2006, BGBl I S. 2553) in Kraft trat, sind sämtliche Unternehmensangaben und Unterlagen nicht mehr in Papierform zu überreichen, sondern elektronisch zu übermitteln. Als Standard für die elektronische Übermittlung der Unternehmensdaten hat sich das kostenlos zugänglich Format XBRL etabliert. Dabei handelt es sich um ein Datenformat, das speziell für die Verarbeitung und Übertragung von handelsrechtlichen Jahresabschlussdaten entwickelt wurde.

Gleichzeitig wurde unter www.unternehmensregister.de ein elektronisches Unternehmensregister eingerichtet.

Hier stehen alle wesentlichen Unternehmensdaten (z. B. Handelsregistereintragungen, Jahresabschlüsse, gesellschaftsrechtliche Bekanntmachungen) für alle Interessierten zum Online-Abdruck bereit. Damit wurde eine zentrale Informationsquelle für den Rechts- und Wirtschaftsverkehr geschaffen, bei der alle veröffentlichten Daten der Unternehmen gebündelt werden.

■ 11.3 Pflichtangaben in der geschäftlichen Korrespondenz

Nach § 37a Abs. 1 HGB sind in allen Geschäftsbriefen eines Unternehmens folgende Angaben zu machen: Firma, Rechtsform, Ort der Handelsniederlassung (in der Regel der Unternehmenssitz), zuständiges Gericht für Eintragungen zum Handelsregister und Registernummer, unter der das Unternehmen im Handelsregister eingetragen ist. Kapitalgesellschaften müssen darüber hinaus auch die Mitglieder ihres Vorstands bzw. der Geschäftsführung, den Vorsitzenden des Vorstandes bzw. der Geschäftsführung und den Vorsitzenden des Aufsichtsrates mit Vor- und Zunamen mitteilen (vgl. §§ 80 AktG, 35a GmbHG, 25a GenG).

Der Begriff des Geschäftsbriefs umfasst nicht nur Handelsbriefe, sondern alle rechtsgeschäftlich erheblichen Mitteilungen des Unternehmens, die nach außen gerichtet sind und geschäftsbezogenen Inhalt besitzen. Geschäftsbriefe können z. B. an einen bestimmten Geschäftspartner, an andere Konzernunternehmen, an Behörden oder an eigene Mitarbeiter adressiert sein, soweit diese als Vertragspartner betroffen sind.

Das Gesetz unterscheidet nicht zwischen elektronischer und schriftlicher Geschäftskommunikation. Die Angabepflichten gelten daher auch für die elektronische Kommunikation (z. B. über Fax, E-Mail oder bei Nachrichtenaustausch über eine Internetseite). Damit will der Gesetzgeber sicher stellen, dass jede Person, die im Rechtsverkehr als Kaufmann auftritt, identifizierbar und erreichbar ist. Mögliche zukünftige Vertragspartner sollen leicht erkennen können, mit wem sie es zu tun haben und wie ein Unternehmen zu erreichen ist.

Das Registergericht kann die Unternehmen mit Zwangsgeld bis zu 5.000 Euro zur Aufnahme der Pflichtangaben in die geschäftliche Korrespondenz anhalten (§§ 37a Abs. 4, 14 S. 2 HGB). Fehlt eine der vorgeschriebenen Angaben in der Geschäftskommunikation, könnte dies eine irreführende geschäftliche Unterlassung im Sinne des § 5a Abs. 3 Nr. 2 UWG darstellen, die eine wettbewerbsrechtliche Abmahnung von Konkurrenten nach sich ziehen kann.

■ 11.4 Anbieterkennzeichnung für Internetseiten

Das Telemediengesetz (TMG) erlegt den Betreibern von Internetseiten und den Anbietern sonstiger Telemediendienste die Pflicht auf, ihre Internetseiten mit einer Anbieterkennung zu versehen. Diese Pflicht wird auch »Impressumpflicht« für Internetseiten genannt und dient dazu, Geschäftskunden und Verbraucher über die Urheberschaft einer Internetseite und über die Identität des Seiteninhabers zu informieren. So verlangt § 5 TMG, dass der Seitenbetreiber seinen Namen, seine Anschrift, die Rechtsform und Vertretungsberechtigung (bei juristischen Personen), Umsatzsteuer-Identifikationsnummer, Informationen zur Registereintragung und E-Mail-Adresse auf seiner Internetseite hinterlegt.

Ein Verstoß gegen die Pflicht zur Anbieterkennzeichnung kann mit einer Geldbuße bis zu 50.000 Euro belegt werden (§ 16 TMG). Außerdem drohen bei einem solchen Verstoß Abmahnungen von Wettbewerbern nach dem Wettbewerbsrecht.

Das Bundesministerium der Justiz hat einen Leitfaden mit weiteren Einzelheiten zur Anbieterkennzeichnung im Internet veröffentlicht.

12 Abgaben

■ 12.1 Rundfunkgebühren

Wie bereits dargestellt, ist die Erfüllung verschiedener Compliance-Pflichten ohne internetfähigen Computer kaum noch möglich. Insbesondere die zwingend vorgeschriebene elektronische Kommunikation mit der Finanzverwaltung (z. B. bei der Abgabe von Umsatzsteuer-Voranmeldungen oder Lohnsteuerermeldungen) erfordert einen Computer mit Internetanschluss im Unternehmen. Da internetfähige Computer und internetfähige Mobiltelefone auch dazu benutzt werden können, um Rundfunk- oder Fernsehsendungen zu empfangen, gelten sie als Rundfunkgeräte und unterliegen entsprechend der Pflicht zur Zahlung von Rundfunkgebühren nach dem Rundfunkgebührenstaatsvertrag (RGebStV). Diese zunächst umstrittene Rechtsauffassung ist inzwischen von der höchstrichterlichen Rechtsprechung bestätigt (vgl. Urteile des BVerwG vom 27. Oktober 2010, Az. 6 C 12.09; 6 C 17.09; 6 C 21.09). Nach Auffassung des BVerwG kommt es für die Gebührenpflicht nur darauf an, dass ein Gerät zum Empfang von Rundfunksendungen bereit gehalten wird. Ist also ein Computer technisch dafür ausgerüstet, über Livestreams Rundfunksendungen zu empfangen, fallen nach Auffassung des BVerwG für ihn auch dann Rundfunkgebühren an, wenn das Gerät gar nicht an das Internet angeschlossen ist.

Ein internetfähiger Computer sei nur dann von der Gebührenpflicht ausgenommen, wenn der Besitzer bereits für ein anderes angemeldetes Rundfunk- oder Fernsehgerät Gebühren entrichtet (Zweitgerätebefreiung). Dasselbe gilt für internetfähige Mobiltelefone. Dabei kommt es nicht darauf an, ob das erste gebührenpflichtige Gerät privat oder für Unternehmenszwecke genutzt wird (BVerwG, Urteile vom 17. August 2011, 6 C 15.10, 45.10 und 20.11).

Aufgrund der Zweitgerätebefreiung nach § 5 Abs. 3 RGebStV ist nur eine Rundfunkgebühr pro Monat und Betrieb zu zahlen, auch wenn in dem Betrieb mehrere Computer eingesetzt werden. Die Nutzung eines internetfähigen Computers ist gegenüber der jeweiligen

Landesrundfunkanstalt anzuzeigen (vgl. § 3 RGebStV). Erfolgt diese Anzeige nicht oder wird die fällige Rundfunkgebühr nicht entrichtet, liegt darin eine Ordnungswidrigkeit, die von der Landesrundfunkanstalt mit einer Geldbuße geahndet werden kann (§ 9 RGebStV).

Die gegenwärtige Rechtslage gilt noch bis zum 1. Januar 2013. Dann soll auf der Grundlage eines geänderten Rundfunkgebührenstaatsvertrages die gerätebezogene Abgabe durch eine Haushaltsabgabe ersetzt werden. Die Rundfunkgebühren für Unternehmen bemessen sich dann nicht mehr nach Zahl und Art der Empfangsgeräte, sondern nach der Anzahl der Mitarbeiter pro Unternehmensstandort. Zusätzlich fallen weitere Rundfunkgebühren an für Betriebsfahrzeuge, die mit einem Rundfunkempfangsgerät ausgestattet sind.

■ 12.2 Urheberrechtsabgaben

Urheberrechtliche Abgaben werden pauschal für Geräte und Speichermedien (z. B. Kopierer, DVD-Recorder oder CD-Rohlinge) erhoben, soweit diese Geräte geeignet sind, urheberrechtlich relevante Vervielfältigungen zum privaten oder sonstigen Gebrauch herzustellen. Die Abgabe soll eine finanzielle Kompensation für die durch das Urheberrecht garantierte Privatkopie (§ 53 UrhG) schaffen.

Die ZPÜ (Zentrale für private Überspielungsrechte), ein Zusammenschluss von deutschen Verwertungsgesellschaften (z. B. GEMA, VG WORT), hat die Aufgabe, einen Großteil dieser Abgabenansprüche gegenüber den Herstellern, Importeuren und Händlern der Geräte und Speichermedien geltend zu machen. Weitere Ansprüche werden von der VG WORT direkt wahrgenommen. Verwertungsgesellschaften sind Einrichtungen, die treuhänderisch urheberrechtlich geschützte Rechte für eine große Zahl von Rechteinhabern wahrnehmen. Die Verwertungsgesellschaften schütten die von der ZPÜ gesammelten Abgaben anhand eines definierten Verteilungsschlüssels an ihre Mitglieder (Urheber der jeweiligen Werk wie Autoren, Komponisten) aus.

Abgabepflichtig sind Hersteller, Importeure und Händler der abgabepflichtigen Produkte und zwar gesamtschuldnerisch (§ 54b Abs.1 UrhG). Wenn sie von der ZPÜ dazu aufgefordert werden, sind sie verpflichtet, über die Art und Stückzahl der für die Abgabe relevanten Produkte Auskunft zu erteilen (§ 54f Abs. 1 UrhG). Importeure haben darüber hinaus eine Meldepflicht. Sie müssen Geräte und Speichermedien, die sie nach Deutschland einführen, monatlich melden (§ 54e Abs. 1 UrhG). Kommt der Meldepflichtige seiner Meldepflicht nicht, nur unvollständig oder unrichtig nach, kann der doppelte Vergütungssatz verlangt werden (§ 54e UrhG). Die Zahlungspflicht des Händlers entfällt, soweit sein Zulieferer Mitglied eines sogenannten Gesamtvertrages (z. B. des BITKOM) ist (§ 54b Abs. 3 Nr. 1 UrhG), oder der Händler halbjährlich Art und Stückzahl der in Deutschland in den Markt gebrachten relevanten Produkte angibt und die Bezugsquelle der ZPÜ/VG WORT schriftlich mitteilt. Die Zahlungspflicht entfällt für die Händler, die lediglich als Spediteur, Frachtführer oder in einer ähnlichen Stellung tätig werden (§ 54b Abs. 2 UrhG). Die Abgabepflicht besteht für Reprographiegeräte (Kopierer, Drucker, Scanner, Faxgeräte), so genannte Multifunktionsgeräte, PCs, Ton- und Bildaufzeichnungsgeräte (z. B. MP3-Player, Tonbandgeräte, DVD-Rekorder) und diverse Speichermedien (z. B. CD-/DVD-Rohlinge, USB-Sticks und Speicherkarten).

Die konkrete Höhe der Abgabensätze muss zwischen den Verwertungsgesellschaften und den Verbänden der Hersteller, Händler und Importeure ausgehandelt werden. Die Abgabenhöhe soll dabei nach dem Maß der tatsächlichen Nutzung der Geräte und Speichermedien für Vervielfältigungen im Sinne der Privatkopie (§ 54a Abs.1 UrhG) bestimmt werden. Darüber hinaus wird berücksichtigt, inwieweit technische Schutzmaßnahmen (z. B. DRM-Systeme) eingesetzt werden (§ 54a Abs.1 S. 2 UrhG), in welchem Ausmaß mehrere Geräte und Speichermedien in die Vervielfältigungskette eingebunden sind (sog. Gerätekombinationen wie PC/Drucker/USB-Stick), welche nutzungsrelevanten Eigenschaften wie Leistungsfähigkeit und Speicherkapazität vorliegen (§ 54a Abs.2 und 3 UrhG) und inwieweit die Abgabe im Vergleich zum Kaufpreis wirtschaftlich angemessen ist (§ 54a Abs. 4 UrhG).

Die ZPÜ und die VG WORT veröffentlichen ihre Abgabeforderungen im Bundesanzeiger (§ 13 UrhWahrnG). Übersichten finden sich auch auf der Internetseite der VG Wort (vgl. <http://www.vgwort.de/publikationen-dokumente/tarif-uebersicht.html>) und der GEMA (vgl. <https://www.gema.de/musiknutzer/lizenzieren/meine-lizenz/hersteller-von-leermedien-und-geraeten.html>). Die von ZPÜ/VG WORT für Geräte und Speichermedien angeforderten Meldungen und Abgabenzahlungen sollten kritisch geprüft werden. Denn viele der Forderungen werden von den Mitgliedern des BITKOM oder von anderen Industrieverbänden in der Abgabenhöhe oder aber bereits dem Grunde nach als unbegründet abgelehnt. Dort bleibt vorerst die Rechtsprechung abzuwarten. Auch laufen zu einzelnen Produkten noch Verhandlungen mit den Verwertungsgesellschaften, die nicht beeinflusst werden sollten.

Verwertungsgesellschaften sind verpflichtet, mit Vereinigungen von Herstellern, Händlern und Importeuren wie dem BITKOM so genannte Gesamtverträge abzuschließen (§ 14 UrhWahrnG). Derartige Rahmenverträge räumen den BITKOM-Mitgliedern, die mit gesonderter Erklärung dem Vertrag beigetreten sind, Vergünstigungen ein. Für BITKOM-Mitglieder besteht derzeit lediglich für Reprographiegeräte ein Gesamtvertrag. Für die übrigen Geräte und Speichermedien laufen derzeit Verhandlungen bzw. gerichtliche Verfahren.

13 Management von Software-Lizenzen

■ 13.1 Risiken beim Software-Lizenzmanagement

Die Nutzung von Software ist heutzutage für Unternehmen unverzichtbar. Gleichzeitig birgt sowohl die Eigenentwicklung von Software als auch die Verwendung vorgefertigter Software erhebliche Risiken. Es ist aber möglich, sich mit den vom geltenden Recht bereitgestellten Mitteln gegen Risiken abzusichern und seine eigenen Entwicklungen wirtschaftlich zu schützen.

Die Risiken bei der Verwendung von Software bestehen vor allem darin, die Software nicht im Einklang mit den für sie gültigen Lizenzbestimmungen zu verwenden. Häufig erfolgt z. B. eine Unterlizenzierung, also eine Nutzung von Software in einem Umfang, der von den erworbenen Lizenzen nicht mehr gedeckt ist. Es sind aber auch Fehlnutzungen anzutreffen, etwa wenn einfache Nutzungslizenzen erworben werden, obwohl eigentlich Entwicklungslizenzen notwendig wären (vgl. dazu sogleich unter 13.2). In den Fällen von Über- oder Fehlnutzung drohen dann Auskunft-, Schadensersatz- und Unterlassungsansprüche der Lizenzgeber.

Bei der Entwicklung von Software muss zudem darauf geachtet werden, dass ein Unternehmen Codeelemente, für die es keine Nutzungsrechte besitzt, nicht zum Bestandteil des eigenen Source Codes macht. Dies kann z. B. geschehen, wenn Entwickler Elemente einbauen, die sie unter Umständen für einen früheren Arbeitgeber entwickelt hatten. Auch ist bei der Entwicklung von Software besondere Sorgfalt im Umgang mit Open Source-Elementen anzuwenden (vgl. dazu sogleich unter 13.7). Wird fremder Quellcode verwendet, so sollte dies stets ausreichend dokumentiert werden und – soweit notwendig – die Nutzung dieses fremden Quellcodes vertraglich abgesichert werden.

Im Rahmen von Softwareeigenentwicklungen kann das Lizenzrecht aber auch zum eigenen Vorteil eingesetzt werden. Eine geschickte Lizenzgestaltung kann den wirtschaftlichen Wert der Eigenentwicklung erheblich steigern.

Bei der Lizenzgestaltung muss neben der wirtschaftlichen Verwertbarkeit der Eigenentwicklung außerdem darauf geachtet werden, dass bei Verwendung fremden Quellcodes bzw. bei Vertrieb fremder Software in den eigenen Lizenzbestimmungen und sonstigen vertraglichen Regelungen dem Kunden keine Rechte eingeräumt werden, die über die Rechte hinausgehen, die man selbst von seinem eigenen Lizenzgeber, im Normalfall dem Softwarehersteller, erhalten hat. Geschieht dies nicht, drohen zum einen Schadenersatz- und Unterlassungsansprüche des Softwareherstellers. Zum anderen entstehen aber auch Haftungslücken, die bei Gewährleistungspflichten oder beim Haftungsrahmen zulasten des eigenen Unternehmens gehen können, da sie nicht gegenüber dem Softwarehersteller im Wege des Regresses geltend gemacht werden können.

Ein effizientes Softwarelizenzmanagementsystem hilft dabei, diese Risiken einzudämmen und so Schaden vom Unternehmen abzuwenden.

■ 13.2 Lizenzmodelle

Wichtigste Aufgabe eines Softwarelizenzmanagementsystems ist, die Bedeutung der einzelnen Softwarelizenzmodelle zu erkennen und sie richtig einzusetzen. Nachfolgend werden einige Lizenzmodelle umrissen. Wegen der Komplexität der einzelnen Lizenzmodelle und der Vielfalt an unterschiedlichen Lizenzen, die die Softwarehersteller anbieten, ist ein abschließender Überblick nicht möglich. Es ist stets erforderlich, sich mit den jeweiligen vertraglichen Regelungen detailliert auseinanderzusetzen, um Auswirkungen auf das Unternehmen richtig einzuordnen.

Als Freeware oder Public Domain werden Lizenzen für Programme bezeichnet, die nach dem Willen ihrer Hersteller in unbeschränkter Anzahl genutzt und kopiert werden dürfen. Es ist allerdings nicht gestattet, sie zu modifizieren oder sie in modifizierter oder unmodifizierter Form weiterzuveräußern.

Mit Shareware bezeichnet man Programme, deren Nutzung zunächst kostenfrei ist, damit man sie für eine begrenzte Zeit testen kann. Möchte man sie nach Ablauf der Testzeit weiternutzen, muss man eine entsprechende Lizenz erwerben. Tut man dies nicht, ist man verpflichtet, die Nutzung einzustellen und das Programm wieder zu löschen. Eine Variante von Shareware sind solche Nutzungsmodelle, in denen die Nutzung nicht zeitlich beschränkt, sondern der Nutzungsumfang eingeschränkt wird. Erst mit dem Kauf des Programms kann der jeweilige Nutzer den vollen Funktionsumfang verwenden.

Eine Einzellizenz dürfte das meistverbreitete Lizenzmodell sein. Sie erlaubt dem Nutzer die Installation und Nutzung der Software auf genau einem Rechner.

Eine Variante der Einzellizenz ist die Mehrfachlizenz: Sie erlaubt es, das jeweilige Programm auf verschiedenen Rechnern zu installieren und zu verwenden. Je nach Ausgestaltung des Mehrfachlizenzmodells im Einzelfall ist es dann zulässig, die Software auf einer beschränkten oder unbeschränkten Anzahl von Rechnern zu installieren. Im Bereich der Forschung und Lehre gibt es die Campuslizenz als Variante der Mehrfachlizenz, die dann ausdrücklich auf den Nutzungsbereich von Universitäten oder Forschungsinstituten zugeschnitten ist.

Bei einer Concurrent User Lizenz wird in aller Regel die Software auf einem Server installiert. Der Server lässt dann den Zugriff von Nutzern in dem Umfang zu, wie es die Lizenzbestimmungen erlauben. Wollen mehr Nutzer darauf zugreifen, ist den zusätzlich zugreifenden Nutzern die Verwendung des Programms nicht möglich. Concurrent User Lizenzen können auch so ausgestaltet sein, dass zwar das jeweilige Programm auch auf Einzelrechnern installiert ist, bei Start des Programms aber eine Abfrage beim Lizenzserver erfolgt, mit der der gegenwärtige Stand der Nutzung des Programms abgefragt und verifiziert wird.

Eine Entwicklungslizenz erlaubt es dem Verwender, mittels der jeweiligen Software weitere Anwendungen oder auch Variationen der Anwendung zu entwickeln.

Bei einer CPU-Lizenz ist es Pflicht, die Software auf einem Rechner mit der in der Lizenz beschriebenen CPU zu installieren. Außerdem ist diese Lizenz im Regelfall anzahlmäßig wie die Einzellizenz beschränkt.

Eine Cluster-Lizenz ermöglicht die Zusammenfassung verschiedener Rechner zu einem Gesamtsystem für die Verwendung der Software.

Bei einer Update-Lizenz erwirbt der jeweilige Lizenznehmer nur das Recht, eine ältere Version der Software auf einen neuen Stand zu bringen.

■ 13.3 Lizenzmanagement

Durch das Softwarelizenzmanagement soll innerhalb des Unternehmens der legale und effiziente Umgang mit proprietärer Software (Software, deren Source Code nicht verändert werden darf) und mit Open Source Produkten (Software, deren Nutzung die Befugnis zur Veränderung einschließt) sichergestellt werden. Es ist Teil der von jedem Unternehmen zu erbringenden Maßnahmen im Bereich des Risikomanagements und der Risikoversorge (§ 91 Abs. 2 AktG, Ziffer 4.1.4 Corporate Governance Codex).

Das Softwarelizenzmanagement schafft Rechtssicherheit bei der Verwendung von Software. Es beugt rechtlichen Risiken vor, die aus Ansprüchen des Software-Urhebers (z. B. Anspruch auf Unterlassung der Software-Nutzung und auf Schadenersatz) oder aus Straf- und Bußgeldtatbeständen nach §§ 106 ff. UrhG resultieren können.

Zudem dient das Softwarelizenzmanagement dazu, den tatsächlichen Softwarebedarf des Unternehmens zu ermitteln, wodurch Kosten zumindest optimiert, ggf. aber sogar reduziert werden können. Eine solche Kostenoptimierung kann insbesondere im Bereich der häufig anfallenden Wartungsgebühren anfallen, da diese unmittelbar mit der Nutzungsintensität der Software verknüpft sind.

Üblicherweise besteht ein Softwarelizenzmanagement aus vier Stufen:

Auf der ersten Stufe wird die gesamte Software, die auf Rechnern im Unternehmen installiert ist, in einer Datenbank erfasst. In der zweiten Stufe wird erfasst, welche und wie viele Lizenzen das Unternehmen bisher erworben hat. Anschließend wird auf der dritten Stufe geprüft, welche Nutzungsrechte die erworbenen Lizenzen gewähren. Dabei muss insbesondere auf inhaltliche, zeitliche oder räumliche Beschränkungen geachtet werden. Im letzten Schritt, der dann für die Einhaltung der Compliance relevant ist, wird der Bestand an Lizenzen mit dem Bestand an Software verglichen. Das Ergebnis dieses Vergleiches wird in einer Lizenzbilanz aufgeführt.

Anhand der Lizenzbilanz lässt sich dann erkennen, welcher Handlungsbedarf besteht, ob etwa Lizenzen nach erworben werden müssen oder womöglich in bestimmten Bereichen abgemeldet werden können.

Zur Implementierung eines Lizenzmanagements ist es erforderlich, dass zunächst die notwendigen Prozesse im Rahmen von entsprechenden Richtlinien und Arbeitsanweisungen eingerichtet werden. Dabei müssen auch klare Verantwortlichkeiten für die jeweiligen Handlungsbereiche geschaffen werden. Wichtiger Bestandteil der festzulegenden Prozesse ist es, wer auf welche Art und Weise die Planung des zukünftigen Softwarebedarfs und ihrer Beschaffung durchführt. Hier bietet es sich an, dass jegliche Beschaffung von Software zumindest durch das Lizenzmanagement freigegeben wird, besser wäre es noch, wenn die Beschaffung durch das Lizenzmanagement gemeinsam mit dem Einkauf geschieht. Gleichzeitig kann das Lizenzmanagement nur erfolgreich sein, wenn sich alle relevanten Entscheidungsebenen, also insbesondere die Geschäftsführung, der Einkauf, die IT-Abteilung und das Controlling auf die Einhaltung der festgelegten Prozesse verpflichten und deren Befolgung im Unternehmen propagieren.

Sobald das Lizenzmanagement einmal eingerichtet ist, sollte eine Archivierung der jeweiligen Lizenzverträge durch das Lizenzmanagement stattfinden, um die Führung der Lizenzbilanz zu erleichtern. Anschließend sollte das Lizenzmanagement regelmäßig die Anzahl der

Installationen von Software und ihre Verwendung überprüfen. Dazu gehört es auch, zu prüfen, ob die jeweilige Software wirklich im Einklang mit den Lizenzbestimmungen genutzt wird, also insbesondere, ob die Anzahl der (gleichzeitigen) Nutzer eingehalten und die Installation auf den zutreffenden Prozessoren durchgeführt wurde.

■ 13.4 Nutzen des Lizenzmanagements

Ein effektives Lizenzmanagement dient in erster Linie dem Schutz vor rechtlichen und damit meist verbundenen wirtschaftlichen Risiken. So besteht bei einer Unterlizenzierung das Risiko, dass die Lizenzgeber zunächst Unterlassungsansprüche geltend machen. In diesem Fall könnte die Software für die Zwecke des Unternehmens nicht mehr eingesetzt werden, was im schlimmsten Fall zum Stillstand von Produktionsprozessen führen kann. Des Weiteren stehen dem Softwarehersteller in diesen Fällen Schadensersatzansprüche zu, die die ansonsten anfallenden Lizenzkosten schnell erheblich übersteigen können. Außerdem kann der Softwarehersteller verlangen, dass nicht lizenzierte Vervielfältigungsstücke gelöscht werden und verkörperte Vervielfältigungsstücke an den Hersteller herausgegeben werden müssen. Das kann vor allem dann erhebliche Folgen haben, wenn die Software des Herstellers möglicherweise ein Bestandteil von Produkten ist, die das Unternehmen vertreibt, und durch die entsprechenden Ansprüche das gesamte Produkt vernichtet werden muss, somit also nicht mehr verkauft werden kann.

Außerdem stellt eine Unterlizenzierung gleichzeitig einen Verstoß gegen das Urheberrecht dar, was auch strafrechtliche Folgen haben kann. Verstöße gegen das Urheberrecht können nach § 106 ff. UrhG einen Straftatbestand begründen und mit Geld- oder sogar Freiheitsstrafe sanktioniert werden. Außerdem haben die Ermittlungsbehörden die Möglichkeit, bei Urheberrechtsverstößen auch Hausdurchsuchungen durchzuführen, die zu einer Beschlagnahme der Geräte führen kann, auf denen unlicenzierte Software gefunden wird. Das kann insbesondere Server betreffen, sodass anschließend das Unternehmen unter Umständen nicht mehr handlungsfähig ist.

Gleichzeitig kann das Lizenzmanagement aber auch dazu dienen, die Nutzung von Softwarelizenzen innerhalb des Unternehmens bedarfsgerechter auszugestalten. Damit lassen sich Kosten senken, indem etwa zu umfangreiche Lizenzen gekündigt oder abgemeldet werden, um so Pflegegebühren zu senken und den Aufwand für Softwareupdates zu verringern. Eine genaue Kenntnis der Softwarenutzung im Unternehmen hilft zusätzlich dabei, bei Gesprächen mit den Softwareherstellern über eine Vertragsverlängerung oder Vertragserweiterung die eigene Position besser zu vertreten, wodurch häufig höhere Rabatte für den Bezug von Software und Pflegeleistungen ausgehandelt werden können. Daneben gibt es aber auch noch weitere wichtige Aspekte des Lizenzmanagements. So bietet es sich an, eine ständige Versionskontrolle durchzuführen, um zu gewährleisten, dass die Software stets auf dem aktuellen Stand ist. Gerade bei Software für die Buchhaltung und Personalverwaltung ist dies erforderlich, um sicherzustellen, dass stets die aktuellsten rechtlichen Entwicklungen innerhalb der Software abgebildet sind.

Daneben gilt es, auch steuerliche Aspekte durch das Lizenzmanagement zu berücksichtigen. Softwarelizenzen stellen Vermögensgüter dar, die in der Bilanz berücksichtigt werden müssen. Diese Berücksichtigung sollte stets im Rahmen der tatsächlichen Nutzung erfolgen, sodass weder zu große Posten noch zu geringe Posten hinsichtlich der Lizenzen in die Bilanz eingestellt werden müssen. Zudem kann eine Fehl- oder Übernutzung von Softwarelizenzen auch im Rahmen von Unternehmenstransaktionen relevant werden. Die Nutzung von Lizenzen ist regelmäßig Bestandteil der Due Diligence-Prüfung vor einer Unternehmensübernahme. Stellt der Käufer Unstimmigkeiten in diesem Bereich fest, kann das nicht nur zu Nachfragen und tiefer gehenden Prüfungen führen, sondern auch Einfluss auf den Kaufpreis haben.

Innerhalb eines Konzerns ist zusätzlich darauf zu achten, dass die Gewährung konzerninterner Dienstleistungen der Softwarenutzung stets zu marktgerechten Preisen erfolgt (»at arms lengths«). Ansonsten besteht das Risiko, dass die Gewährung der Softwarenutzung innerhalb des Unternehmens etwa als verdeckte Gewinnausschüttung

gewertet wird. Das Lizenzmanagement sollte weiter darauf achten, dass bei Software, die für die täglichen Geschäftsprozesse relevant ist, wirksame und effiziente Hinterlegungsvereinbarungen bestehen, so dass im Insolvenzfall des Softwareanbieters Nutzung und Pflege der Software weiter gewährleistet werden kann.

■ 13.5 Einrichtung eines Lizenzmanagements

Bei der Einrichtung eines Lizenzmanagements sollten vor allem die folgenden Prozesse beachtet werden: Einer der wichtigsten Aspekte der Effizienzsteigerung bei der Softwarenutzung ist es, innerhalb des Unternehmens die eingesetzte Software so weit wie möglich zu standardisieren. Dies führt zu einer Reduktion des Supportaufwands, indem sich die IT-Mitarbeiter auf die Unterstützung weniger Anwendungen konzentrieren können und sich nicht jeweils in die Arbeitsumgebung der Mitarbeiter neu einarbeiten müssen. In diesem Zusammenhang sollte für die eingesetzte Software auch die Lizenzmetrik vereinheitlicht werden, sodass an allen Standorten und in allen Unternehmensteilen dieselben Arten von Lizenzen für die jeweiligen Einsatzbereiche verwendet werden.

Um die Zahl der eingesetzten Softwareprodukte zukünftig klein und überschaubar zu halten, ist die Beschaffung von Software einheitlich über den Einkauf oder eine sonstige Abteilung zu steuern. Jeder Mitarbeiter muss dabei verpflichtet werden, vor der Beschaffung von Software stets mit dieser zentralen Stelle in Kontakt zu treten.

Durch eine gute Kenntnis der Softwarelizenzverträge und der Softwarekosten innerhalb des Lizenzmanagements lassen sich bei der tatsächlichen Beschaffung auf diese Art und Weise weitere Einsparpotentiale herausarbeiten.

Außerdem sollten die Mitarbeiter dazu angehalten werden, dem Lizenzmanagement zu melden, falls sie den Einsatz von unlizenzierter Software bemerken. Hierbei sollte gegebenenfalls klargestellt werden, dass dies nicht zur Sanktionierung eines Fehlverhaltens, sondern zur Verringerung der wirtschaftlichen und rechtlichen Risiken



für das Unternehmen dient, um den Mitarbeitern die Scheu vor einer solchen Meldung zu nehmen.

■ 13.6 Softwarelizenz-Audits

Die urheberrechtswidrige Nutzung von Software kann neben Unterlassungs- und Schadensersatzansprüchen des jeweiligen Rechteinhabers auch zur Folge haben, dass der Rechteinhaber ein Auskunftsrecht gegenüber dem Unternehmen hat, in welcher Form und in welchem Umfang das Unternehmen Software nutzt. Da aber Softwareanbieter selten ohne Weiteres einen entsprechenden Lizenzverstoß feststellen können, behalten sich die Anbieter in ihren Lizenzverträgen häufig sogenannte Auditrechte vor. Nach diesen Bestimmungen können die Softwareanbieter vom Nutzer Auskunft darüber verlangen, wie und in welchem Umfang er die lizenzierte Software nutzt. Zusätzlich dazu sehen die Verträge häufig noch vor, dass der Softwareanbieter auch eine Vorortüberprüfung durchführen kann, die dann meist durch Wirtschaftsprüfungsgesellschaften abgewickelt wird. Ihre rechtliche Grundlage findet eine solche Bestimmung in § 101 UrhG, § 809 BGB sowie in strafprozessualen Vorschriften.

Um die Auswirkungen einer entsprechenden Überprüfung möglichst gering zu halten, empfiehlt es sich, innerhalb des Softwarelizenzmanagements für eine solche Situation vorzusorgen. Insbesondere sollte die Lizenzbilanz jeweils ausweisen, welche Software wie und in welchem Umfang genutzt wird, damit darüber gezielt dem Softwareanbieter auch Auskunft erteilt werden kann. Dadurch lässt sich meistens der Wunsch nach einer weitergehenden Überprüfung vermeiden.

Falls eine Überprüfung doch durchgeführt werden soll, muss zu allererst rechtlich geprüft werden, ob die entsprechende Klausel überhaupt wirksam ist. Insbesondere vor dem Hintergrund der rechtlichen Anforderungen an allgemeine Geschäftsbedingungen kann eine solche Klausel häufig zweifelhaft sein. Das wäre sie nach § 307 BGB insbesondere, wenn sie eine unangemessene Benachteiligung des jeweiligen Lizenznehmers zur Folge hätte. Dies ist vor allem damit begründet, dass ein entsprechendes

Audit auch hinsichtlich datenschutzrechtlicher Vorgaben problematisch ist und zudem Geheimhaltungsinteressen des Softwareverwenders berührt.

Daher sollte bereits bei der Vertragsgestaltung darauf geachtet werden, dass dem Softwarehersteller nur ein Anspruch auf Selbstauskunft des Softwareverwenders eingeräumt wird, der gegebenenfalls durch entsprechende eidesstattliche Versicherungen abgesichert wird.

Bei einem entsprechenden Auskunftsverlangen des Softwareanbieters sollte dann das Lizenzmanagement zunächst die Rechtmäßigkeit des entsprechenden Verlangens prüfen und anschließend anhand der eigenen Lizenzüberwachung die geforderte Auskunft geben. Die Auskunft sollte nur in dem Umfang erfolgen, wie sie zur Beantwortung der Anfrage des Softwareanbieters erforderlich ist.

■ 13.7 Besonderheiten im Lizenzmanagement für Open Source Software

Open Source Software (OSS) wird in zunehmendem Maße verwendet, um Lizenzkosten zu verringern. Kosten- und Wettbewerbsdruck erlauben es nur den wenigsten Software-Nutzern, das mannigfaltige Angebot an frei verfügbaren OSS-Komponenten zu ignorieren. So hat z. B. die Stadt München bekanntgegeben, dass sie im Rahmen des LiMux-Projekts 4 bis 5 Millionen Euro und damit gegenüber einer vergleichbaren Windows-Installation ca. ein Viertel der Kosten gespart habe. Auch ist der Funktionsumfang bei Open Source Software in einigen Bereichen inzwischen annähernd mit den Einsatzmöglichkeiten proprietärer Software identisch.

Allerdings birgt der Einsatz von Open Source Software auch gewisse Risiken. So ist nicht immer vertraglich gewährleistet, dass für entstehende Fehler auch Updates erstellt werden. Durch die offene Natur von Open Source Produkten kann der Softwareanwender dieses Problem jedoch umgehen, indem er die Fehlerbehebung selbst vornimmt. Die Entscheidung für oder gegen die Verwendung

von Open Source Software kann daher vor allem unter wirtschaftlichen oder operativen Gesichtspunkten getroffen werden; bei sorgfältiger Vorbereitung lässt sie sich jedenfalls relativ rechtssicher gestalten.

Erhöhte Sorgfalt sollte aber ein Software-Anbieter auf jeden Fall aufbringen, wenn er Open Source Software in seine eigene, kommerziell vertriebene Software integriert. Open Source Software ist nämlich zwar kostenlos, aber nicht frei von lizenzrechtlichen Vorgaben. Lizenzbestimmungen für Open Source Software sehen für deren Weiterverwendung in kommerziellen Produkten häufig erhebliche Einschränkungen vor. Außerdem besteht die Gefahr, dass bei einer zu sorglosen Verwendung von Open Source Bestandteilen in kommerziellen Produkten die Open Source Lizenz die Lizenzierbarkeit der eigenen Software »infiziert«. Dann kann die eigene Software nicht mehr als proprietäre Software vertrieben werden, sondern muss ebenfalls unter die Open Source Lizenz gestellt und der Quellcode muss offengelegt werden (sogenannter viraler Effekt). Daher sollte vor einer Verwendung von Open Source Bestandteilen in selbst entwickelter Software stets geprüft werden, wie die Lizenzbestimmungen für eine solche Verwendung ausgestaltet sind. Eine Verwendung sollte nur dann erfolgen, wenn der virale Effekt ausgeschlossen werden kann.

In mehrstufigen Lieferketten, in denen (auch) Software weitergereicht wird, sollten allen Beteiligten eine umfassende Dokumentation und vollständige Stücklisten der gelieferten Software zur Verfügung stehen, so wie es bei Hardware schon lange üblich ist. Die Vielzahl der in einer Lieferkette zu beachtenden Lizenzauflagen und Nutzungsbeschränkungen stellt eine wachsende Herausforderung dar. Software-Anbieter müssen zu ihrer eigenen Absicherung von ihren Lieferanten die lückenlos dokumentierte Beachtung der Lizenzbedingungen für die in den gelieferten Produkten enthaltenen OSS-Komponenten fordern. Je mehr (unterschiedliche) OSS-Komponenten dabei zum Einsatz kommen, desto schwieriger wird das manuelle Erfassen und Pflegen der Lizenzen, Versionen, Auflagen und Konflikte, die dabei entstehen können. Der Einsatz eines Werkzeugs, mit dem automatisch ermittelt wird, welche Komponenten und

damit Lizenzen im Einsatz sind, hilft dabei, das Risiko einer Lizenz-Verletzung zu verringern. Helfen kann auch ein standardisiertes Übergabeformat der Dokumentation, wie SPDX (Software Package Data Exchange, vgl. www.spdx.org/), eine von der Linux Foundation ins Leben gerufene Initiative. Der Standard verlangt, für jede einzelne Datei eines Projekts den Nachweis ihrer Herkunft und die für sie geltenden Lizenz(en) festzuhalten. Die Open Source-Eingangskontrolle kann sich bei den Unternehmen somit auf die Auswertung solcher Dokumente beschränken, vorausgesetzt, sie wurden von den Lieferanten mit entsprechender Sorgfalt oder unter Zuhilfenahme geeigneter Werkzeuge automatisiert erstellt. Der manuelle Weg ist an dieser Stelle insofern problematisch, als es als nahezu ausgeschlossen betrachtet werden kann, sämtliche z. B. per Cut-and-Paste aus OSS-Projekten übernommene Code-Fragmente bei einem Code-Review zu entdecken. Eine vollständige Erfassung aller OSS-Codes und damit eine umfängliche Compliance kann auf diesem Weg kaum gewährleistet werden.

■ 13.8 Alternative: Software as a Service (SaaS)

SaaS oder »On-Demand«-Software bezeichnet (im Gegensatz zu »lokal installierter Software«) eine Methode zur Nutzung von Software-Anwendungen, bei denen die Software im Regelfall nur beim Anbieter oder bei einem Dienstleister installiert ist und von diesem gewartet und aktualisiert wird. Der Nutzerzugriff auf die Anwendungen erfolgt meist über das Internet und ist daher losgelöst von stationären Beschränkungen. Die Bezahlung für die Nutzung erfolgt über eine regelmäßige, häufig nutzungsunabhängige Abonnementgebühr. Der Erwerb von Lizenzen entfällt. Der Kunde mietet hier allerdings nicht nur die Software, er mietet auch die dazugehörige Infrastruktur und die dazugehörigen Dienstleistungen. Ein eigenes Rechenzentrum oder einen eigenen Server für den Betrieb der Software muss er daher nicht mehr betreiben.

Die Verwendung von Software as a Service eröffnet Einsparpotentiale, da z. B. eine bedarfsgerechte Erweiterung oder Reduzierung der genutzten Ressourcen vereinbart werden kann oder die Einsparung von Hardware beim Nutzer möglich ist. Allerdings ist auch zu berücksichtigen, dass bei einem Ausfall der Softwaredienste die Software gar nicht mehr verwendet werden kann und so unter Umständen die Prozesse stillstehen. Außerdem muss beachtet werden, dass die Anbieter von solchen Diensten häufig außerhalb der EU ansässig sind. So können etwa datenschutzrechtliche Konflikte entstehen, wenn personenbezogene Daten auf die Server der entsprechenden Anbieter transferiert werden sollen und diese Server z. B. in den USA stehen. Daher muss bei der Auswahl des Anbieters sowie bei Gestaltung der entsprechenden Nutzungsverträge auf diese Aspekte besonderer Wert gelegt werden, um die Kosteneinsparungspotentiale nicht durch höhere Ausfall- und Sicherheitsrisiken oder durch mögliche Verstöße gegen Datenschutzrecht zu erkaufen.

■ 13.9 Verkauf von überschüssigen Lizenzen – Gebrauchtssoftware

In den vergangenen Jahren sind vermehrt Anbieter von »Gebrauchtssoftware« aufgetreten. Dieses Angebot erfolgt in unterschiedlicher Form. Teilweise kaufen die Anbieter alte Einzelplatzlizenzsoftware auf, wie etwa Word- oder Windows-Kopien und vertreiben diese dann mit einem Original-Datenträger weiter. Andere Anbieter kaufen von ehemaligen Softwarenutzern Softwarelizenzen, die die ehemaligen Nutzer nicht mehr benötigen, und verkaufen nur die Lizenzen ohne Datenträger weiter. In diesem Fall muss der Käufer sich die Software zu der Lizenz anderweitig, etwa durch Download beim Softwareanbieter, beschaffen. Häufig erfolgt der Verkauf unter Beifügung eines notariellen Testats, dass es sich um eine rechtmäßige Kopie handelt und der ursprüngliche Softwareverwender die Nutzung der Software eingestellt hat. Die Verwendung von Gebrauchtssoftware im Unternehmen kann wirtschaftlich attraktiv sein, da die so vertriebenen Lizenzen preislich erheblich günstiger sind als Neulizenzen. Umgekehrt können durch Verkauf nicht mehr benötigter Lizenzen an entsprechende Händler Einnahmen generiert werden.

Ob der Einsatz von Gebrauchtssoftware zweckmäßig ist, bestimmt sich danach, für welchen Zweck die Software beschafft werden soll und welcher Art sie ist. Sollen z. B. für ERP-Systeme zusätzliche Lizenzen erworben werden, könnte ein Einsatz zweckmäßig sein, da dann wahrscheinlich schon ein Pflegevertrag für die Software besteht, sodass auch weiterhin auf die neuesten Software-Updates zugegriffen werden kann. Dasselbe könnte bei einzelnen Einzelplatzlizenzen gelten. Kritischer ist der Einsatz von Gebrauchtssoftware dagegen, wenn die Software noch nicht im Unternehmen verwendet wird und für eine langfristig zuverlässige und effiziente Nutzung der Abschluss eines Pflegevertrages notwendig ist, da dieser Pflegevertrag unter Umständen beim Einsatz von Gebrauchtssoftware nicht zu erhalten ist.

Unabhängig von den Wirtschaftlichkeits- und Zweckmäßigkeitfragen der Nutzung bzw. Veräußerung von Gebrauchtssoftware muss jedoch rechtlich erhöhte Vorsicht bei ihrer Verwendung an den Tag gelegt werden. Die Zulässigkeit des Einsatzes von Gebrauchtssoftware ist heftig umstritten. Vor allem große Softwareanbieter gehen intensiv gegen deren Nutzung vor.

Die Rechtsprechung in Deutschland sah die Verwendung von Gebrauchtssoftware bisher eher kritisch. Nur einzelne Gerichte ließen den Einsatz in bestimmten Fällen zu. Ansonsten haben die Instanzgerichte häufig das Angebot von Gebrauchtssoftware für unzulässig erklärt mit der Begründung, dass der Anbieter von Gebrauchtssoftware keine wirksamen Lizenzen einräumen könne. Zu dieser Ansicht tendierte wohl auch der BGH, sah aber europäisches Recht berührt und hatte Zweifel in diesbezüglichen Auslegungsfragen. Mit Beschluss vom 03.02.2011 (Az.: I ZR 129/08 – Used Soft) legte er daher dem Europäischen Gerichtshof (EuGH) die Frage vor, wie die Zulässigkeit eines Verkaufs gebrauchter Software zu beurteilen sei.

Der EuGH hat mit Urteil vom 03.07.2012 entschieden, dass beim Verkauf von Software der Grundsatz der Erschöpfung eingreift, dessen Ziel es ist, »eine Abschottung der Märkte zu vermeiden«. Nach Meinung des EuGH ist es grundsätzlich unzulässig, die Weiterveräußerung von Software vertraglich zu untersagen. Erforderlich ist allerdings, dass der Veräußerer alle verbleibenden Kopien der Software löscht bzw. zerstört oder sonst sicherstellt, dass die Software nicht mehr verwendet werden kann. Außerdem müssen stets alle Lizenzen eines Softwarepakets zusammen veräußert werden. Es ist nicht zulässig, ein Lizenzpaket oder eine Volumenlizenz in verschiedene Teile aufzuteilen. Zudem ist der Softwareanbieter berechtigt, durch technische Maßnahmen sicherzustellen, dass die Software nach der Veräußerung durch den ursprünglichen Lizenznehmer nicht mehr verwendet werden kann. Der BGH wird nun im Ausgangsverfahren entscheiden müssen, welche Auswirkungen diese Grundsätze auf die Veräußerung von Gebrauchtssoftware in Deutschland haben.

14 Datenschutz und Datensicherheit

■ 14.1 Datensicherheit

Im allgemeinen Sprachgebrauch werden Datenschutz und Datensicherheit gleich gestellt. Aus juristischer Sicht bestehen hier allerdings erhebliche Unterschiede. Die Datensicherheit betrifft nicht nur – wie der Datenschutz – personenbezogene Daten im Sinne von § 3 Abs. 1 BDSG, sondern alle denkbaren unternehmenskritischen Daten (z. B. Bilanzdaten, Produktionszahlen, Kundendaten, Forschungsergebnisse). Ziel der Datensicherheit ist es, die Unternehmensdaten vor unbefugtem Zugriff und die betriebliche IT-Infrastruktur vor Schäden zu schützen. Unberechtigte Einsicht, Manipulation, Löschung und sonstige Schädigung der Unternehmensdaten sind zu vermeiden. Die IT-Sicherheit orientiert sich dabei an den Grundsätzen Vertraulichkeit, Verfügbarkeit und Integrität der Unternehmensdaten. Zu deren Durchsetzung ist die IT-Infrastruktur des Unternehmens zunächst gegen externe Bedrohungen (z. B. Viren, Hacker, Spam) zu schützen. Aber auch für interne Bedrohungen wie Stromausfall, Hardware-Defekte, Wasser- und Feuerschäden sollten im Rahmen des Risiko-Managements Notfallpläne aufgestellt werden. Daten aus geschäftskritischen Systemen sollten in regelmäßigen Abständen in einem räumlich getrennten Back-up-System gesichert werden, sodass sie bei Ausfall des Hauptsystems zeitnah zur Verfügung stehen. Die Vertraulichkeit lässt sich z. B. durch die Verschlüsselung von Daten oder durch die Vergabe von Lese- und Editierrechten erreichen.

Insgesamt sind Maßnahmen und Aufwand für technische Vorkehrungen zur Gewährleistung von Datensicherheit (z. B. Firewall, Verschlüsselung, Backup-Speicherung) je nach Bedeutung und Sensibilität der Daten für das Unternehmen anzusetzen. Die Bewertung erfolgt im Rahmen des allgemeinen Risikomanagements. Kriterien für die technische und organisatorische Umsetzung der Datensicherheit im Unternehmen können den Standards zum IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) entnommen werden. Um eine optimale Datensicherheit zu erreichen, sollten die IT-Systeme jeweils auf dem aktuellen Stand der Technik sein.

Schwierig wird die Gewährleistung von Datensicherheit, wenn sie mit dem Schutz anderer Interessen kollidiert. Gestattet ein Unternehmen z. B. seinen Mitarbeitern die private Mitbenutzung der unternehmenseigenen IT- und Telekommunikationsinfrastruktur, so kann der Einsatz von Virenprogrammen, Spam-Filtern oder sonstigen Datenkontrollen zu Verstößen gegen das Post- oder Telekommunikationsgeheimnis und zu strafrechtlichen Sanktionen führen. Es empfiehlt sich daher, Transparenz zu schaffen und ggf. entsprechende Betriebsvereinbarungen abzuschließen.

Die Einhaltung der Grundsätze für Datensicherheit liegt in erster Linie im Eigeninteresse des Unternehmens. Denn Datensicherheit ist in den meisten Unternehmen essentiell für die Geschäftstätigkeit. Bestimmte Unternehmensdaten sind aber auch für den Gesetzgeber von besonderem Interesse (z. B. Daten der Buchführung oder personenbezogene Daten), sodass rechtliche Sanktionen drohen, wenn diese Daten nicht verfügbar oder nicht ausreichend gesichert sind.

■ 14.2 Schutz personenbezogener Daten

Für den Umgang mit personenbezogenen Daten sind über die Anforderungen der Datensicherheit hinaus weitere Schutzvorschriften zu beachten, die vor allem im Bundesdatenschutzgesetz (BDSG), im Telemediengesetz (TMG) und im Telekommunikationsgesetz (TKG) niedergelegt sind. Das Anwendungsverhältnis der datenschutzrechtlichen Vorschriften bestimmt sich nach § 1 Abs. 3 BDSG. Auf europäischer Ebene gelten die Regelungen der EU-Datenschutzrichtlinie 95/46/EG sowie der sog. E-Privacy-Richtlinie. Diese Richtlinien mussten in den EU-Mitgliedstaaten in nationales Recht umgesetzt werden und sind auch zur Auslegung nationaler Rechtsvorschriften heranzuziehen. Wann die derzeit im Entwurf diskutierte EU-Datenschutz-Grundverordnung, die einen modernen bzw. zeitgemäßen Datenschutz sicherstellen soll, in Kraft treten wird, ist nicht absehbar.

Der Anwendungsbereich des Datenschutzrechts ist bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten eröffnet. Daten sind personenbezogen, wenn sie persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person betreffen (§ 3 Abs. 1 BDSG), z. B. Name, Anschrift, Verdienst, Kontonummer, Kaufverhalten. Streitig ist, ob auch sog. personenbeziehbare Daten in den Anwendungsbereich der Datenschutzgesetze fallen. Dabei handelt es sich um Daten, die Rückschlüsse auf Identität oder Verhalten einer bestimmten natürlichen Person zulassen, z. B. IP-Adresse, Besuch einer bestimmten Internetseite, Verbindungsdaten eines Telefongesprächs.

Grundlegendes Leitbild des Datenschutzrechts ist das Verbot mit Erlaubnisvorbehalt (§ 4 Abs. 1 BDSG). Die Erfassung, Verarbeitung und Nutzung personenbezogener Daten ist daher nur zulässig, wenn hierzu eine klare gesetzliche Erlaubnis besteht (z. B. zur Erfüllung und Abwicklung eines Vertragsverhältnisses), oder wenn eine ausdrückliche Einwilligung des Betroffenen vorliegt. Diese Einwilligung ist nach § 4a BDSG grundsätzlich schriftlich zu erteilen, soweit nicht wegen besonderer Umstände eine andere Form geboten ist. Eine elektronische Einwilligung sieht § 13 TMG unter bestimmten Voraussetzungen vor, die in der jeweiligen Softwarelösung implementiert sein müssen (u.a. jederzeitige Auskunftsmöglichkeit über die gespeicherten Daten sowie jederzeitiges Widerrufsrecht).

Die Anforderungen des Datenschutzes geben auch Grenzen vor für Maßnahmen im Unternehmen, die unter Compliance-Gesichtspunkten wünschenswert wären. So sind z. B. Screenings von Mitarbeitern, insbesondere von Funktionsträgern in sensiblen Positionen, vom Arbeitnehmerdatenschutz nach § 32 BDSG untersagt, sofern kein konkreter Straftatverdacht vorliegt.

■ 14.3 Datenverarbeitung durch Dritte

Nutzt ein Unternehmen die »Economy of Scale« oder die »Economy of Scope«, indem es die Informationsverarbeitung komplett oder teilweise zu einem anderen Unternehmen auslagert, bedarf es in jedem Fall eines spezifischen Vertrages. Stellt die Auslagerung eine Auftragsdatenverarbeitung dar, sind in diesem Vertrag die Rechte und Pflichten nach § 11 Abs. 2 BDSG festzulegen, wenn von der Auslagerung personenbezogene Daten betroffen sind. Diese Verpflichtung besteht auch bei der Auslagerung an verbundene Unternehmen, da es kein Konzernprivileg gibt.

Die Übermittlung von Daten ins Ausland stellt lediglich innerhalb der Europäischen Union kein Problem dar, da hier das gleiche Datenschutzniveau besteht wie in Deutschland. Bei einem Datentransfer in Drittstaaten (z. B. USA) sind allerdings erheblich höhere Hürden zu überwinden, was durch die Unterwerfung unter die »Safe Harbor Principles« oder den Abschluss von EU-Standardklauseln erfolgen kann. Demgegenüber ist das Verfahren für die sog. »Binding Corporate Rules« in einem internationalen Unternehmensverbund als dritte Alternative noch sehr aufwendig. Möglicherweise wird die EU-Datenschutzverordnung längerfristig dieses Verfahren vereinfachen. Zu beachten ist allerdings, dass beim Drittlandverkehr die Auftragsdatenverarbeitung nicht privilegiert ist.

■ 14.4 Besondere Arten personenbezogener Daten

Soweit besondere Arten von personenbezogenen Daten verarbeitet werden, gelten stärkere Restriktionen: hierunter fallen Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Eine Übermittlung derartiger Daten an Dritte oder ins Ausland ist praktisch ohne dezidierte schriftliche Einwilligung des Betroffenen nicht möglich.

■ 14.5 Datenschutzrechtliche Mindestanforderungen

Beschäftigt ein Unternehmen mindestens 10 Personen mit der automatisierten Verarbeitung von personenbezogenen Daten, hat es einen Datenschutzbeauftragten nach § 4 f BDSG zu bestellen. Dieser ist der Geschäftsführung zu unterstellen und kann Mitarbeiter des Unternehmens oder externer Beauftragter sein. Ein externer Datenschutzbeauftragter ist in die Geschäftsprozesse so zu integrieren, dass er die teils sogar gesetzlich vorgeschriebenen Vorabkontrollen durchführen kann.

Darüber hinaus hat das Unternehmen ein sog. Verfahrensverzeichnis zu erstellen (§ 4 g BDSG). Das Verfahrensverzeichnis hat alle DV-Verfahren aufzulisten, in denen personenbezogene Daten verarbeitet werden. Dieses Verfahrensverzeichnis ist dem Datenschutzbeauftragten zur Verfügung zu stellen und dient der Erfüllung der Auskunftspflicht gegenüber den nachfragenden Betroffenen sowie der Umsetzung der Verfahrensrechte nach §§ 33 bis 35 BDSG. Weitere Vorgaben für technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten ergeben sich aus der Anlage zu § 9 BDSG.

Relativ neu ist die Verpflichtung, Datenschutzpannen anzuzeigen (breach notification). Diese Verpflichtung kann insbesondere bei börsennotierten Unternehmen erhebliche Auswirkungen haben und ist daher in ein allgemeines Risikomanagement zu integrieren.

Aus alledem folgt, dass die IT-Compliance verstärkt und einzelfallbezogen in das Risikomanagement der Geschäftsführung einbezogen werden muss. Denn auch das BDSG enthält in den §§ 43 und 44 Bußgeld- und Strafvorschriften.

15 Umweltrechtliche Compliance-Anforderungen

Bei Herstellung und Vertrieb von ITK-Hardware gelten besondere rechtliche Anforderungen, die dem Schutz der Umwelt dienen. Zu beachten sind Verbote und Meldepflichten bestimmter Stoffe bei der Herstellung von Hardware, bestimmte Standards zur Produktsicherheit und Verträglichkeit elektronischer Geräte, Vorgaben bei der Verpackung und Pflichten zur Entsorgung nicht mehr verwendbarer Altgeräte. Verpflichtungen nach dem Umweltrecht beruhen auf dem Verursachungsprinzip bzw. der sogenannten erweiterten Produzentenverantwortung (engl.: Extended Producer Responsibility). Danach sind Hersteller bzw. Vertreiber für die Umweltauswirkungen der von ihnen in Verkehr gebrachten Produkte über den gesamten Produktlebenszyklus hinweg verantwortlich (von der Entwicklung bis zur Entsorgung). Dieses Prinzip findet seinen gesetzlichen Niederschlag in § 22 des Kreislaufwirtschafts- und Abfallgesetz (KrW-/AbfG).

Nach § 22 Abs. 2 KrW/AbfG umfasst die Produktverantwortung

- die Entwicklung, Herstellung und das Inverkehrbringen von Erzeugnissen, die mehrfach verwendbar, technisch langlebig und nach Gebrauch zur ordnungsgemäßen und schadlosen Verwertung und umweltverträglichen Beseitigung geeignet sind,
- den vorrangigen Einsatz von verwertbaren Abfällen oder sekundären Rohstoffen bei der Herstellung von Erzeugnissen,
- die Kennzeichnung von schadstoffhaltigen Erzeugnissen, um die umweltverträgliche Verwertung oder Beseitigung der nach Gebrauch verbleibenden Abfälle sicherzustellen,
- den Hinweis auf Rückgabe-, Wiederverwendungs- und Verwertungsmöglichkeiten oder -pflichten und Pfandregelungen durch Kennzeichnung der Erzeugnisse und

- die Rücknahme der Erzeugnisse und der nach Gebrauch der Erzeugnisse verbleibenden Abfälle sowie deren nachfolgende Verwertung oder Beseitigung.

■ 15.1 Entsorgung von Elektro-Altgeräten

Das umweltrechtliche Verursachungsprinzip konkretisiert sich für Hersteller von ITK-Hardware im Elektro- und Elektronikgerätegesetz (ElektroG) aus dem Jahr 2005. Das Gesetz setzt die EU-Richtlinien 2002/96/EG (WEEE) und 2002/95/EG (RoHS) in deutsches Recht um. Es begründet für Hersteller von Elektrogeräten die Pflicht, die umweltgerechte Entsorgung ihrer Produkte zu gewährleisten. Inzwischen hat die EU eine neue Richtlinie (2012/19/EU) erlassen, die die bestehende Richtlinie ersetzt und bis August 2018 in deutsches Recht umzusetzen ist. Ziel der neuen Richtlinie ist es, die Recyclingquote von Elektro-Altgeräten zu erhöhen sowie die Rückgewinnung von Sekundärrohstoffen und eine effiziente Ressourcennutzung zu fördern.

Die Pflichten des aktuellen ElektroG richten sich nicht nur an Produzenten im eigentlichen Sinne, sondern sie können darüber hinaus auch Händler und Importeure treffen. Hersteller im Sinne des ElektroG ist jeder, der Elektro- und Elektronikgeräte herstellt und erstmals in Deutschland in Verkehr bringt, Geräte anderer Anbieter unter eigenem Markennamen in Deutschland verkauft, Elektro- oder Elektronikgeräte erstmals nach Deutschland einführt und in Verkehr bringt oder sie in einen anderen Mitgliedstaat der Europäischen Union ausführt und dort unmittelbar an einen Nutzer abgibt (vgl. § 3 Abs. 11 ElektroG). Die Definition der betroffenen Geräte ist ebenfalls weit und umfasst alle Geräte, die auf den Betrieb mit Wechselspannung von höchstens 1.000 Volt oder Gleichspannung von höchstens 1.500 Volt ausgelegt sind (§ 3 Abs. 1 ElektroG), also insbesondere Geräte der Informations- und Kommunikationstechnik sowie Geräte der Unterhaltungselektronik (vgl. § 2 Abs. 1 ElektroG).

Daneben sind die Hersteller aber auch angehalten, die Rücknahme und Entsorgung ausgedienter Elektrogeräte in Selbstverwaltung zu organisieren. Für diese Aufgabe hat die Wirtschaft das Elektro-Altgeräte-Register in der Rechtsform einer Stiftung gegründet (Stiftung EAR). Die Stiftung EAR kontrolliert und steuert als sog. gemeinsame Stelle die Erfüllung der Entsorgungspflichten durch die Hersteller. Um ihre Aufgabe ordnungsgemäß erfüllen zu können, wurde die Stiftung EAR nach § 17 ElektroG vom Bundesumweltamt mit besonderen öffentlich-rechtlichen Befugnissen beliehen.

Die eigentliche Entsorgungspflicht ist in § 10 ElektroG niedergelegt. Danach hat jeder Hersteller jährlich eine bestimmte Menge ausgedienter Altgeräte bei den kommunalen Sammelstellen abzuholen und sie wieder zu verwenden oder umweltgerecht zu entsorgen. Die zu entsorgende Gerätemenge pro Hersteller wird von der Stiftung EAR festgelegt und richtet sich nach der Menge der Geräte, die der Hersteller im Jahr in Verkehr bringt. Alternativ kann die zu entsorgende Gerätemenge auch danach festgelegt werden, wie hoch der Anteil der Geräte eines Herstellers an der Gesamtmenge zurückgegebener Altgeräte eines Jahres ist (§ 14 Abs. 5 ElektroG).

Zur effektiven Durchsetzung der Entsorgungsverpflichtung sieht das ElektroG verschiedene weitere Pflichten vor. So muss sich nach § 6 Abs. 2 ElektroG jeder Hersteller bei der Stiftung EAR registrieren lassen, bevor er Elektro- oder Elektronikgeräte in Deutschland in Verkehr bringen darf. Weiterhin sind umfassende Dokumentations-, Mitteilungs- und Informationspflichten zu erfüllen (§ 13 ElektroG). Insbesondere haben die Hersteller der Stiftung EAR monatlich mitzuteilen, welche Geräteart sie in welcher Menge in den Verkehr gebracht haben. Darüber hinaus treffen die Hersteller Pflichten zur Gerätekennzeichnung und zum Führen der von der Stiftung EAR erteilten Registrierungsnummer im Geschäftsverkehr. Die Gerätekennzeichnung muss eine Identifizierung des Herstellers und die Feststellung ermöglichen, wann das Gerät erstmalig in Verkehr gebracht wurde (§ 7 ElektroG). Außerdem müssen die Hersteller nach § 6 Abs. 3 ElektroG jährlich eine insolvenz sicherere Finanzierungsgarantie nachweisen. Diese Garantie soll gewährleisten, dass die Kosten für die

Rücknahme und Entsorgung der ausgedienten Altgeräte abgedeckt sind, auch wenn der Hersteller aus dem Markt ausscheidet (eine solche Garantie kann z. B. über das von BITKOM eingerichtete Garantiesystem Altgeräte erbracht werden).

Nach § 6 Abs. 2 S. 5 ElektroG dürfen Hersteller, die ihrer Registrierungspflicht bei der Stiftung EAR nicht nachgekommen sind, keine Elektrogeräte in Verkehr bringen. Im Übrigen können Verstöße gegen Registrierungs- und Kennzeichnungspflichten als Ordnungswidrigkeiten klassifiziert und mit Bußgeldern bis zu 50.000 Euro geahndet werden (§ 23 ElektroG).

■ 15.2 Stoffvorgaben für Gerätehersteller

Zum Schutz von Umwelt und Verbrauchern unterliegen Herstellung und Vertrieb von Elektrogeräten verschiedenen weiteren Auflagen. Auch hiervon sind ITK-Hersteller betroffen. So sieht § 5 ElektroG Grenzwerte für die Verwendung bestimmter Inhaltsstoffe wie Blei, Quecksilber, Chrom oder Cadmium in Elektrogeräten vor. Geräte, die die zulässigen Grenzwerte für diese Stoffe überschreiten, dürfen nicht in den Verkehr gebracht werden. Außerdem müssen die Geräte so konstruiert sein, dass nach beendeter Nutzung ihre Demontage und die Wiederverwertung einzelner Komponenten und Inhaltsstoffe unkompliziert möglich ist (§ 4 ElektroG).

Des Weiteren ist die EU-Verordnung Nr. 1907/2006 zur Registrierung, Bewertung, Zulassung und Beschränkung von Chemikalien (sog. REACH-Verordnung) zu beachten. Sie enthält unmittelbar in allen EU-Mitgliedstaaten geltende Informations- und Notifizierungspflichten über die Verwendung von Chemikalien als Inhaltsstoffe für Produkte, die in der EU in Verkehr gebracht werden (zu weiteren Einzelheiten vgl. die BITKOM-Publikation »REACH und die ITK-Branche«).

Besondere Stoffvorgaben gelten auch für die Hersteller und Vertrieber von Batterien. Das Batteriegesetz (BattG) gilt seit dem 01.12.2009 und setzt die europäische Alt-batterierichtlinie (Richtlinie 2006/66/EG über Batterien

und Akkumulatoren sowie Altbatterien und Altakkumulatoren) in nationales Recht um. Es ersetzt die seit 1998 geltende Batterieverordnung und enthält folgende Vorgaben:

- Vertriebsverbot für Batterien, die unzulässig hohe Mengen an Cadmium und Quecksilber enthalten (§ 3 BattG);
- Pflicht für Vertrieber von Batterien, diese für den Verbraucher unentgeltlich zur Entsorgung zurück zu nehmen (§ 9 BattG);
- Pflicht für Hersteller zur Einrichtung eines von ihnen getragenen Rücknahmesystems für Alt-Batterien (§ 6 BattG);
- Pflicht für Hersteller zur Anzeige ihrer Marktteilnahme gegenüber dem Umweltbundesamt (§ 4 BattG), dabei müssen sie auch anzeigen, an welchem Rücknahmesystem sie teilnehmen;
- Kennzeichnungs- und Hinweispflichten (§§ 17, 18 BattG).

Das BattG legt prozentuale Rücknahmequoten fest, die in Verkehr gebrachte und zurückgenommene Mengen an Batterien berücksichtigen. Die Finanzierung der Rücknahme- und Entsorgungsverantwortung für Altbatterien und Altakkumulatoren liegt grundsätzlich in den Händen der Hersteller (hierzu zählen auch Importeure und Vertrieber). Die für Endverbraucher kostenfreie Entsorgung wird weitgehend über den Handel abgewickelt.

Das beim Umweltbundesamt geführte Melderegister für Hersteller, Importeure und Vertrieber von Batterien und Akkus soll dafür sorgen, dass diese ihrer Verantwortung bei Rücknahme und Entsorgung ihrer Produkte nachkommen. Das Melderegister ist über die Internetseite des Umweltbundesamts zu erreichen. Verstöße gegen das BattG werden als Ordnungswidrigkeit geahndet und mit Bußgeldern bis zu 50.000 Euro belegt.

Schließlich ist darauf hinzuweisen, dass auch beim Transport von Batterien und batteriegetriebenen Elektroprodukten besondere Vorgaben zu beachten sind. Lithium-Batterien gelten als gefährliche Güter im Sinne von § 3 der Verordnung über die innerstaatliche und grenzüberschreitende Beförderung gefährlicher Güter auf der Straße, mit Eisenbahnen und auf Binnengewässern (GGVSEB). Der Charakter als Gefahrgut von Lithium-Batterien ergibt sich aus Unterabschnitt 2.2.9 des Europäischen Übereinkommens über die internationale Beförderung gefährlicher Güter auf der Straße (ADR). Neue Vorschriften für die Beförderung von Lithium-Batterien und für die Beförderung von Geräten, in denen Lithium-Batterien eingebaut sind, gelten ab dem 1. Juli 2013. Denn dann endet die Übergangsvorschrift zum bedenkenlosen Transport von Lithium-Batterien (vgl. Ziff. 1.6.1.10 ADR). Ab diesem Zeitpunkt dürfen Lithium-Batterien nur noch transportiert werden, wenn sie nach einem besonderen Verfahren geprüft wurden und diese Prüfung zertifiziert wurde. Das Zertifikat muss der Batterie-Nutzer bei sich führen.

Lithium-Batterien und auch Geräte, die solche Batterien enthalten, werden vom Gesetzgeber als Gefahrgut der Klasse 9 eingestuft und unterliegen deshalb besonderen Vorschriften zur Ladungssicherung und zum Transport.

■ 15.3 Entsorgung von Verkaufsverpackungen

Die aus dem Jahre 1991 stammende Verpackungsverordnung (VerpackV) ist mehrfach novelliert und EU-Vorgaben angepasst worden. Die aktuell gültige fünfte Novelle der VerpackV ist im April 2008 in Kraft getreten und zielt darauf ab, die Umweltbelastungen aus Verpackungsabfällen zu verringern und die Wiederverwendung oder Verwertung von Verpackungen zu fördern. Sie richtet sich an »Erstinverkehrbringer«, also an Hersteller und Vertreiber, die zusammen mit ihren Waren auch Warenverpackungen an Endverbraucher abgeben.

Wer als Hersteller (zur Definition vgl. § 3 Abs. 8 VerpackV) oder Vertreiber (zur Definition vgl. § 3 Abs. 9 VerpackV) Verpackungen in Verkehr bringt, ist verpflichtet, sich an einem flächendeckenden Rücknahmesystem zu beteiligen (§ 6 Abs. 1 VerpackV). Das Rücknahmesystem hat für die Rücknahme und Entsorgung der Verpackungen zu sorgen, wobei für den Endverbraucher keine Kosten entstehen dürfen. Überschreitet ein Hersteller oder Vertreiber mit den von ihm verwendeten Verpackungen bestimmte Schwellenwerte, so hat er über die von ihm in Verkehr gebrachten Verpackungen jährlich eine Vollständigkeitserklärung nach § 10 VerpackV abzugeben. Die Erklärung ist durch einen externen Sachverständigen (z. B. Wirtschaftsprüfer) zu prüfen und bei der zuständigen Industrie- und Handelskammer zu hinterlegen. Verstöße gegen die VerpackV können als Ordnungswidrigkeiten mit einer Geldbuße bis zu 50.000 Euro geahndet werden (vgl. § 15 VerpackV in Verbindung mit § 61 Krw-/AbfG). Die verschiedenen Pflichten für Hersteller und Vertreiber von ITK-Produkten im Zusammenhang mit der Sammlung und Entsorgung von Verkaufsverpackungen sind in einem speziellen BITKOM-Leitfaden »Anforderungen der neuen Verpackungsverordnung« zusammengestellt.

16 Anforderungen durch europäische Produktstandards

Elektronische Produkte, also insbesondere auch ITK-Geräte, müssen verschiedenen technischen Vorgaben entsprechen, die auf europäischer Ebene durch EU-Richtlinien festgelegt werden. Diese Richtlinien enthalten z. B. Anforderungen an bestimmte technische Standards, an die Produktsicherheit, an die elektromagnetische Verträglichkeit oder allgemein an die Betreiber von Funkanlagen und Telekommunikationsendeinrichtungen. Die Vorgaben sollen technische Anforderungen und Mindeststandards für die Geräte vereinheitlichen und dadurch technische Handelsbeschränkungen reduzieren und den freien Wettbewerb zwischen den Anbietern der regulierten Produkte innerhalb des gesamten EU-Gebiets sicherstellen. Die Anbieter der betroffenen Produkte müssen die Konformität ihrer Produkte mit den Vorgaben des EU-Rechts durch das CE-Kennzeichen (für »Communautés Européennes«) dokumentieren. Das Kennzeichen darf aber erst auf den Produkten angebracht werden, nachdem das Produkt im Einklang mit der einschlägigen EU-Richtlinie hergestellt und die Konformität mit den Richtlinienvorgaben festgestellt wurde. Die von der CE-Kennzeichnungspflicht betroffenen Produkte sind z. B. im Hinweisblatt des bayerischen Staatsministeriums für Wirtschaft, Infrastruktur, Verkehr und Technologie aufgeführt (dort S. 5).

Nähere Erläuterungen zu den Anforderungen bei der CE-Kennzeichnung finden sich im Leitfaden »Marktzulassung und CE-Kennzeichnungspflicht von Produkten der ITK- und Unterhaltungselektronik-Industrie«. Eine Auflistung der gesetzlichen Anforderungen bei der CE-Kennzeichnung verschiedener Produktgruppen ergeben sich aus den Leitfäden zur produktneutralen Beschaffung.

Diese Leitfäden fassen alle gesetzlichen Anforderungen an Unternehmen zusammen, die ITK-Geräte in den Verkehr bringen. Sie gliedern sich in die vier Bereiche Gerätesicherheit, elektromagnetische Verträglichkeit, Telekommunikation und Umwelt. Für jeden dieser vier Bereiche sind zunächst die ordnungspolitischen Regelungen (Gesetze, Rechtsverordnungen des Bundes und der Länder, Satzungen von Körperschaften und Anstalten des öffentlichen Rechts, kommunale Satzungen) aufgeführt. Auf diese Regelungen folgen untergesetzliche, konkretisierende Bestimmungen (Normen, Standards, marktübliche Anforderungen), die sich auf die vorgenannten ordnungspolitischen Regelungen beziehen (Ausnahme – Bereich Umwelt). Werden ITK-Produkte in speziellen Bereichen eingesetzt, können sich weitere Anforderungen ergeben, z. B. beim Einsatz von Computern im medizinischen Umfeld.



17 Compliance-Management im Unternehmen

■ 17.1 Elemente eines Compliance-Management-Systems

Um die Risiken aufgrund von Verstößen gegen gesetzliche Regelungen und sonstige rechtliche Vorgaben zu minimieren, führen viele Unternehmen Compliance-Management-Systeme ein. Ein Compliance-Management-System (CMS) bezeichnet die Gesamtheit aller

unternehmensinternen Strukturen und systematisch aufeinander bezogenen Maßnahmen zur Aufdeckung und Vermeidung von Gesetzes- und Regelverstößen im Unternehmen. Dabei ist die Abgrenzung zu anderen Kontroll- und Überwachungsinstanzen im Unternehmen fließend. Die jeweiligen Kontrollbereiche überdecken sich teilweise.

Kontroll- und Überwachungsinstanzen im Unternehmen	
Compliance-Management-System (keine gesetzliche Grundlage)	Gesamtheit aufeinander abgestimmter Maßnahmen im Unternehmen zur Aufdeckung und Abwehr rechtlicher Risiken
Risikomanagementsystem	Definition nach IDW PS 340, Tz. 4: Gesamtheit der Methoden und Verfahren zur Identifikation, Bewertung, Kommunikation, Überwachung und Steuerung von Risiken im Unternehmen; aufgedeckte Risiken und Verfahren zur Risikoerkennung müssen im Lagebericht beschrieben werden (§ 289 Abs. 2 S. 1 HGB)
Überwachungssystem (§§ 91 Abs. 2 AktG, 317 Abs. 4 HGB)	Das Überwachungssystem soll gewährleisten, dass Bestandsrisiken für das Unternehmen, erhöhte Gefahren aus riskanten geschäftlichen Transaktionen, Fehler bei der Rechnungslegung und Rechtsverstöße mit negativen Auswirkungen auf Finanz- und Ertragslage des Unternehmens frühzeitig erkannt werden. Es richtet sich auf wirtschaftliche Geschäftsrisiken, nicht in erster Linie auf rechtliche Risiken, ist nur für Aktiengesellschaften verpflichtend.
Internes Informations- und Kontrollsystem (§ 289 Abs. 5 HGB)	Definition nach Gesetzesbegründung zum BilMoG: Unter einem internen Kontrollsystem werden die Grundsätze, Verfahren und Maßnahmen zur Sicherung der Wirksamkeit und Wirtschaftlichkeit der Rechnungslegung, zur Sicherung der Ordnungsmäßigkeit der Rechnungslegung sowie zur Sicherung der Einhaltung der maßgeblichen rechtlichen Vorschriften verstanden. Eine explizite Pflicht zur Einrichtung eines internen Kontrollsystems kennt das Gesetz nicht, lediglich eine Pflicht zur Darstellung eines vorhandenen Systems im Lagebericht (vgl. § 289 Abs. 5 HGB). Das IKS ist verpflichtend einzurichten von deutsche Tochterunternehmen US-amerikanischer Konzerne nach Sarbanes-Oxley-Act.
Interne Revision (§ 25a Abs. 1 KWG)	Die Interne Revision befasst sich mit der (vergangenheitsbezogenen) Prüfung von Geschäftsprozessen mit dem Ziel, die Ordnungsmäßigkeit der betrieblichen Prozesse (insbesondere der Kontrollprozesse) zu gewährleisten, Unregelmäßigkeiten aufzudecken und die Effektivität betrieblicher Abläufe zu verbessern.

Controlling	Das Controlling bereitet Informationen zum Zwecke der Unternehmenssteuerung auf und begleitet das Management bei der Identifizierung von unternehmerischen Zielen sowie bei der Erreichung dieser Ziele durch Planung und Kontrolle.
Externe Audits	Externe Audits sind Prüfungen bestimmter abgegrenzter Unternehmensbereiche oder Themenkomplexe durch außerhalb des Unternehmens stehende, besonders qualifizierte Personen (z. B. Wirtschaftsprüfer oder Rechtsanwälte).
Datenschutzbeauftragter	Nach § 4f des Bundesdatenschutzgesetzes muss jedes Unternehmen einen Datenschutzbeauftragten bestellen, wenn mehr als neun Mitarbeiter regelmäßig mit der automatischen Verarbeitung personenbezogener Daten befasst sind. Erfolgt die Datenverarbeitung personenbezogener Daten im Unternehmen nicht automatisiert, liegt die entsprechende Grenze für die Bestellung des Datenschutzbeauftragten bei 20 Mitarbeitern. Dabei kann es sich auch um einen beauftragten externen Datenschutzbeauftragten handeln.
IT-Sicherheitsbeauftragter	Verantwortlicher für Daten- und IT-Sicherheit im Unternehmen

■ 17.2 Einführung eines Compliance-Management-Systems

Da die Einrichtung eines Compliance-Management-Systems nicht verpflichtend ist, sollte von einer Einschätzung der spezifischen Risiken im Unternehmen abhängig gemacht werden, ob der Aufbau eines solchen Systems erforderlich ist. Die Durchführung dieser Analyse zur Erfassung und Bewertung der betrieblichen und geschäftlichen Risiken ist Aufgabe der Geschäftsführung. Die Risikosituation hängt von vielen Faktoren ab, z. B. von der Art und der Gefahrneigung der Produkte, von Größe und Struktur des Unternehmens, von der Qualifikation der Mitarbeiter, von bereits vorgekommenen Compliance-Verstößen, von der möglichen Schadenshöhe oder von den Gegebenheiten des Marktes. Die Risikoanalyse kann zu dem Ergebnis kommen, dass die vorhandenen Risiken auch ohne ein besonderes Compliance-Management beherrschbar sind. Ergibt die Risiko-Analyse nur geringe Risiken und ist die Größe und Struktur des Unternehmens überschaubar, kann ein ausreichendes Compliance-Management schon darin bestehen, die jeweiligen Unternehmensmitarbeiter anzuweisen, auf die Einhaltung der einschlägigen Rechtsvorgaben zu achten.

Ist aufgrund der Analyse ein Compliance-Management sinnvoll oder gar notwendig, hat die Geschäftsführung weiter über dessen Ausgestaltung und Funktion zu entscheiden. Auch insoweit gibt es keine verbindlichen gesetzlichen Vorgaben. Das Compliance-Management sollte auf die individuellen Verhältnisse im jeweiligen Unternehmen zugeschnitten sein, um die wesentlichen rechtlichen Erfordernisse mit möglichst geringem Aufwand zu adressieren. Insbesondere ist zu prüfen, inwieweit Compliance von ähnlichen, bereits im Unternehmen vorhandenen Kontrollinstanzen (z. B. Controlling, Rechtsabteilung, Revision oder sogar Rechnungswesen) mit übernommen werden kann. Eine Zusammenlegung, zumindest jedoch eine effiziente Koordination von Kontrollinstanzen bietet sich aus dem Gesichtspunkt der Synergie und der Verhinderung gegenläufiger Aktivitäten an. Jedenfalls sollte für die Überwachung und Steuerung von Compliance-Risiken und anderen Risiken nur ein IT-System erforderlich sein. Compliance sollte die Unternehmensabläufe und die Durchsetzung des Unternehmenszwecks unterstützen und möglichst wenig behindern. Dabei ist zu bedenken, dass auch das beste Compliance-Management nicht jedes denkbare Fehlverhalten verhindern kann.

■ 17.3 Ausgestaltung des Compliance-Management-Systems

Wesentliche Aufgabe eines Compliance-Management-Systems (CMS) ist die Umsetzung von abstrakten rechtlichen Vorgaben in konkrete und verständliche Handlungsanweisungen und Verhaltensrichtlinien für die Mitarbeiter. Die Aufklärung der Mitarbeiter über das rechtliche Risikoprofil des Unternehmens und über die notwendigen Verhaltensweisen zur Abwehr dieser Risiken gehören zu den unverzichtbaren Standard-Elementen eines CMS. Neben den Vorgaben zur Einhaltung gesetzlicher Vorschriften können unternehmensinterne Compliance-Richtlinien auch weitere Details der betrieblichen Tätigkeit wie den Umgang mit Kunden, Behörden und Geschäftspartnern, die Zulässigkeit von Nebentätigkeiten, die Zuwendung von Geschenken, die Gewährung von Gefälligkeiten oder Preisnachlässen enthalten.

Damit solche Richtlinien nicht nur beschriebenes Papier bleiben, sollten ihre Hintergründe und Ziele sowie Einzelheiten ihrer Durchführung den Mitarbeitern in regelmäßigen Schulungen nahe gebracht werden. Schulungen für die Mitarbeiter sind ebenfalls grundlegender Bestandteil eines Compliance-Management-Systems. Besondere Vorgaben für Compliance-Schulungen gibt es nicht. Sie können daher – wenn eine Präsenzveranstaltung aufgrund geringer rechtlicher Risiken nicht erforderlich erscheint – auch online durchgeführt werden. Empfehlenswert sind jährliche Wiederholungen und die Dokumentation, wer an den Schulungen teilgenommen hat, ggf. auch Bestätigungen der Mitarbeiter, daß sie sich korrekt verhalten haben.

Ziel eines Compliance-Managements sollte sein, eine Compliance-Kultur im Unternehmen zu etablieren, also Unternehmenskultur und Compliance-Bewußtsein zur Deckung zu bringen und die Mitarbeiter vom Sinn rechtskonformen Handelns zu überzeugen. Die Unternehmensmitarbeiter sollten Compliance nicht als Behinderung, sondern als selbstverständlichen Teil ihrer täglichen Arbeit ansehen. Hierbei kann ein unternehmensspezifischer Code of Conduct helfen, der das gewünschte Verhalten und die gewünschte Wertorientierung aus

Sicht der Unternehmensführung als Idealbild beschreibt. Besonders wichtig ist in diesem Zusammenhang die Vorbildfunktion des Managements. Das Management sollte die Bedeutung von Compliance betonen und im eigenen Verhalten vorleben.

Darüber hinaus ist die Einrichtung eines Hinweisgebersystems im Unternehmen (sog. Whistleblowing) zu empfehlen, um die Aufdeckung von Regelverstößen zu erleichtern oder erst zu ermöglichen. Nach US-amerikanischem Recht gehört die Einrichtung einer Whistleblower-Hotline sogar zu den zwingenden Compliance-Anforderungen an Wirtschaftsunternehmen. Dabei handelt es sich um ein zusätzliches anonymes Hinweissystem außerhalb der hierarchischen Berichtswege, das Mitarbeiter zur anonymen Anzeige von normwidrigem Verhalten und Compliance-Verstößen nutzen können. In Deutschland gibt es keine gesetzlichen Vorgaben für ein solches Hinweissystem. Damit ein Hinweissystem erfolgreich funktioniert, sollte den Hinweisgebern Anonymität zugesichert werden und die Person zur Entgegennahme der Hinweise sollte neutral und für die Mitarbeiter vertrauenswürdig sein. Für die Hinweise der Mitarbeiter könnte eine Telefon-Hotline, ein E-Mail-Postfach oder eine spezielle Internet-Adresse eingerichtet werden. In kleineren Unternehmen bietet sich stattdessen oftmals eher die Bestellung eines externen Ombudsmannes (z. B. unabhängiger Rechtsanwalt) an, der anonyme Hinweise aus dem Unternehmen entgegennimmt.

Aus den Vorgaben für ein Überwachungssystem gemäß § 91 Abs. 2 AktG, dessen Einrichtung allerdings nur für Aktiengesellschaften zwingend ist, können weitere Hinweise für die Ausgestaltung eines Compliance-Management-Systems abgeleitet werden. Denn nach der Rechtsprechung gehört die Schaffung von klar zugewiesenen und klar dokumentierten Verantwortlichkeiten, Zuständigkeiten und Berichtswegen zu einem Risikofrüherkennungs- und Überwachungssystem dazu (LG München, Urteil vom 5.4.2007, 5 HK O 15964/06; in: BB 2007, 2170). Es sollte im Unternehmen also klar und auch dokumentiert sein, welche Personen sich mit Compliance beschäftigen, welche Compliance-Maßnahmen im Unternehmen getroffen wurden und welche Stelle Hinweise auf Verstöße

aufnimmt. Darüber hinaus hat das Unternehmen sicher zu stellen, dass rechtlich relevante Informationen, z. B. die Insolvenz eines wichtigen Kunden, den zuständigen Entscheidungsträgern im Unternehmen bekannt werden (BGH, Urteil vom 15. Dezember 2005 - IX ZR 227/04).

Je nach den betrieblichen Anforderungen können z. B. folgende Maßnahmen Bestandteil eines Compliance-Managements sein:

- Aufklärung und Schulung der Unternehmensmitarbeiter über rechtliche Risiken;
 - Einrichtung eines betriebsinternen Informationssystems (z. B. über E-Mail oder Intranet), das eine schnelle Verbreitung von rechtlich relevanten Informationen unter den Mitarbeitern gewährleistet;
 - Erarbeitung eines Werte-Systems/Werte-Leitbildes für das Unternehmen;
 - Umsetzung der abstrakten rechtlichen Vorgaben in konkrete und verständliche Handlungsanweisungen und Verhaltensrichtlinien für die Mitarbeiter.
 - Einrichtung eines 4-Augen-Prinzips;
 - Funktionstrennung;
 - Rotation von Mitarbeitern in exponierten Funktionen;
 - Begrenzung von Budgets, die einzelnen Mitarbeitern zur Verfügung stehen;
 - Klare Zuweisung von Zuständigkeiten für die Verfolgung von Compliance-Verstößen und für die Entgegennahme von Hinweisen auf bestehende Compliance-Risiken;
 - Würdigung von Compliance-gerechtem Verhalten durch die Geschäftsführung;
 - Einrichtung von Hinweissystemen, z. B. einer Whistleblower-Hotline.
- Einsetzung eines Compliance-Beauftragten;
 - Durchführung von Stichprobenkontrollen bestimmter Geschäftsvorfälle;
 - Compliance-Monitoring (systematische Überprüfung der Unternehmenstätigkeit auf Rechtsverstöße durch die Geschäftsführung) und Compliance-Audits (Prüfungen durch außerhalb des Unternehmens stehende Dritte);
 - Ermittlung und Verfolgung von Verdachtsmomenten auf Compliance-Verstöße;
 - Anregung von Disziplinarmaßnahmen.

Mögliche Organisationsformen für das Compliance-Management

- Compliance-Management als eigene Abteilung unter Führung eines Compliance-Officers mit Berichtslinie an die Geschäftsführung
- Compliance-Management als Aufgabe der Rechtsabteilung
- Compliance-Management als Aufgabe der Internen Revision, des Controlling oder einer sonstigen Stabsabteilung
- Compliance-Management als Aufgabe eines besonderen Lenkungskreises aus den Leitern verschiedener Unternehmensfunktionen (z. B. Interne Revision, Rechtsabteilung, Unternehmenssicherheit, Controlling, Buchhaltung, Personal)
- Compliance-Management als Aufgabe eines Mitglieds der Geschäftsführung.

Auch wenn ein Compliance-Beauftragter im Unternehmen bestellt und ein Compliance-Management eingerichtet wurde, bleibt zumindest die Kontrolle über das Compliance-Management Aufgabe der Geschäftsführung. Denn in diesem Fall muss die Geschäftsleitung im Rahmen ihrer allgemeinen Sorgfaltspflicht (§§ 76 Abs. 1, 93 Abs. 1 AktG, 43 Abs. 2, 3 GmbHG) für das Unternehmen sicher stellen, dass das System auch verlässlich funktioniert. Es sind also kontinuierliche und wirksame Kontrollen erforderlich und es muss gewährleistet sein, dass Compliance-Gesichtspunkte in die Entscheidungen der Geschäftsführung einfließen. Die Verantwortlichkeit für Compliance sollte daher in der ersten Führungsebene klar geregelt sein und z. B. im Geschäftsverteilungsplan einem Mitglied der Geschäftsleitung zugeordnet werden.

Ob ein Compliance-System den spezifischen Anforderungen entspricht und wirksam funktioniert, kann ein Unternehmen durch einen Wirtschaftsprüfer kontrollieren lassen. Die Durchführung solcher externen Audits hilft der Geschäftsführung bei dem Nachweis, dass sie ihre Pflichten zur Durchsetzung von Compliance erfüllt hat. Für die Compliance-Prüfung hat das Institut der Wirtschaftsprüfer (IDW) am 11. März 2011 einen Prüfungsstandard verabschiedet. Der Prüfungsstandard enthält auch eine Beschreibung der Grundelemente für ein Compliance-Management im Unternehmen.

■ 17.4 Restriktionen des Compliance-Managements

Da das Compliance-Management Rechtsverstöße verhindern soll, ist es in besonderer Weise selbst an die Vorgaben des Rechts gebunden. Alle Maßnahmen des Compliance-Managements sind insbesondere am Arbeitsrecht, am Datenschutzrecht und am Strafrecht, aber auch am Telekommunikationsrecht zu messen. Denn wenn ein Unternehmen seinen Mitarbeitern die private Nutzung von Internet und E-Mail am Arbeitsplatz erlaubt, ist es bereits als Diensteanbieter i.S.d. § 3 Nr. 6 TKG anzusehen. Infolgedessen hat der Arbeitgeber das Fernmeldegeheimnis des § 88 TKG zu beachten, das es ihm untersagt, sich vom Inhalt der Korrespondenz seiner Mitarbeiter Kenntnis zu verschaffen.

Ist dem Arbeitnehmer die Nutzung von Telekommunikationsmitteln am Arbeitsplatz nur zu dienstlichen Zwecken gestattet, sind Maßnahmen zur Kontrolle von Mitarbeitern am Betriebsverfassungsgesetz (BetrVG) und am Bundesdatenschutzgesetz (BDSG) zu messen. So unterliegen z. B. technische Maßnahmen zur Leitung, Kontrolle und Führung von Mitarbeitern oder ein systematischer Abgleich von Mitarbeiterdaten der Zustimmung des Betriebsrates (§ 87 Abs. 1 Nr. 6 BetrVG). Aus datenschutzrechtlicher Sicht sind solche Maßnahmen nur zulässig, wenn sie auf § 32 BDSG oder auf § 28 BDSG gestützt werden können. Auch bei Einrichtung eines innerbetrieblichen Systems zur Aufnahme anonymer Hinweise auf Compliance-Verstöße (»Whistleblower-Hotline«) ist das Datenschutzrecht zu beachten. Hierzu gibt es eine Empfehlung der sogenannten Artikel-29-Datenschutzgruppe aus dem Jahr 2006. Danach sollte z. B. der Kreis der Personen, die zu einer Meldung von Missständen berechtigt sind, begrenzt und die zu meldenden Rechtsverstöße spezifiziert werden.

18 Compliance-Beauftragter

■ 18.1 Aufgaben eines Compliance-Beauftragten

Compliance-Beauftragte sollen ihrem Auftrag gemäß dazu beitragen, dass es in ihrem Unternehmen nicht zu Rechtsverstößen und Pflichtverletzungen kommt. Der Aufgaben- und Pflichtenkreis eines Compliance-Beauftragten (oder Compliance-Officers) ist aber nicht gesetzlich festgelegt. Er ergibt sich vielmehr im Wesentlichen aus dem Anstellungsvertrag und richtet sich nach den spezifischen Unternehmensrisiken, die durch eine Risikoanalyse festgestellt wurden.

Der Compliance-Beauftragte organisiert insbesondere den Aufbau des Compliance-Management-Systems im Unternehmen, legt weitergehende Verantwortlichkeiten für einzelne Mitarbeiter fest, bereitet die im Unternehmen wichtigen Compliance-Themen strukturiert auf, definiert Kontrollen, erarbeitet unternehmensinterne Compliance-Richtlinien und Handlungsanweisungen, überwacht deren Einhaltung, führt Schulungen durch. Regelverstöße meldet er an die Geschäftsleitung, die dann die entsprechenden Sanktionen verhängt.

Zu den Aufgaben eines Compliance-Beauftragten gehören:

- Analyse der rechtlichen Risiken im Unternehmen;
- Erarbeitung von Verhaltensrichtlinien und Anweisungen für die Mitarbeiter;
- regelmäßige Prüfung des Compliance-Systems (ggf. in Zusammenarbeit mit Externen), Aufdeckung und Behebung von Defiziten;
- eigene regelmäßige Fortbildungen;
- Durchführung von Informations- und Schulungsveranstaltungen für Mitarbeiter;
- Prüfung, ob bestehende Compliance-Richtlinien im Unternehmen tatsächlich eingehalten werden und ob Compliance-Maßnahmen effektiv sind;
- Anpassung von Compliance-Maßnahmen, falls erforderlich;
- Informierung der Unternehmensführung über festgestelltes Fehlverhalten; dabei kann es in Einzelfällen erforderlich sein, den Betriebsrat einzuschalten (§§ 87 Abs. 1 Nr. 1, Nr. 6, 94 BetrVG);
- Verhinderung geplanter Straftaten, von denen er weiß.

Zu den Aufgaben eines Compliance-Officers gehört es nicht generell, Straftaten oder Ordnungswidrigkeiten von Unternehmensmitarbeitern bei Behörden anzuzeigen. Hiervon ausgenommen, also anzeigepflichtig, sind die Straftaten, deren Nichtanzeige nach § 138 StGB strafbar ist: z. B. Gewaltdelikte, gemeingefährliche Straftaten, Geld- und Wertpapierfälschung.

Um seine Aufgaben ausfüllen zu können, sollte der Compliance-Beauftragte sowohl über juristische als auch betriebswirtschaftliche Kenntnisse verfügen, Geschäftsmodell und Prozesse des Unternehmens verstehen, vertrauenswürdig und kommunikativ sein.

■ 18.2 Stellung des Compliance-Beauftragten

Die Bestellung eines eigenen Compliance-Beauftragten oder Compliance-Officers im Unternehmen ist rechtlich genauso wenig zwingend wie die Einrichtung eines besonderen Compliance-Managements. Allerdings kann die Einrichtung der Position eines Compliance-Officers in größeren Unternehmen als state of the art angesehen werden. Bei kleineren und mittleren Unternehmen bietet es sich dagegen eher an, das Compliance-Management organisatorisch in die Rechtsabteilung zu verlegen oder an die interne Revision anzubinden.

Die Position des Compliance-Beauftragten mit seinen Querschnittsaufgaben ist als Stabsstelle anzusehen, die nur der Geschäftsleitung untersteht. Deshalb muss für die mit Compliance beauftragten Personen ein direkter Berichtsweg an die Unternehmensleitung eingerichtet sein. Denn auch wenn die Durchführung des Compliance-Managements delegiert wird, verbleibt die Verantwortung für Compliance und für die Kontrolle des Compliance-Managements bei der Unternehmensführung. Der Compliance-Beauftragte ist damit Ansprechpartner der Unternehmensleitung einerseits, andererseits aber auch Vertrauensperson der Mitarbeiter.

Des Weiteren benötigt der Compliance-Beauftragte seinen Aufgaben entsprechende Kompetenzen. Er muss mit Zugangs- und Einsichtsrechten (einschließlich IT-Zugriff) und Weisungsbefugnissen gegenüber operativen Einheiten ausgestattet sein. Dabei setzt sich der Compliance-Beauftragte aber nicht an die Stelle der disziplinarisch Vorgesetzten, sondern bringt gemeinsam mit diesen die notwendigen Maßnahmen oder Konsequenzen bei festgestellten Rechtsverstößen auf den Weg.

Kompetenzen und Aufgaben des Compliance-Beauftragten sollten schriftlich in einer Funktionsbeschreibung festgehalten und den übrigen Mitarbeitern im Betrieb auch bekannt sein. Die detaillierte Aufgabenzuweisung an den Compliance-Officer gehört zu den Führungsaufgaben der obersten Leitungsebene im Unternehmen. Desgleichen sollte der Compliance-Beauftragte die von ihm festgestellten Rechtsrisiken im Unternehmen, die von ihm durchgeführten Compliance-Maßnahmen, festgestellte

Compliance-Verstöße und daraufhin eingeleitete Sanktionen dokumentieren. Letztlich dient dies auch zu seiner Entlastung. Er kann damit nachweisen, mit welcher Sorgfalt er die ihm übertragenen Aufgaben erfüllt hat.

■ 18.3 Haftung des Compliance-Beauftragten

Da der Compliance-Beauftragte im Unternehmen für die Einhaltung des Rechts verantwortlich ist, befindet er sich in einer exponierten Position mit erhöhten Haftungsrisiken. Er kann aber nicht für sämtliches Fehlverhalten von Unternehmensmitarbeitern (mit-)verantwortlich gemacht werden. Ein rechtserheblicher Vorwurf kann den Compliance-Beauftragten nur treffen, soweit die von ihm beeinflussbaren Geschäfts- und Verfahrensabläufe oder sonstige Unternehmensstrukturen systematische Rechtsverstöße ermöglicht oder begünstigt haben. Es muss also für eine jede Inanspruchnahme des Compliance-Beauftragten nachgewiesen sein, dass er den konkreten Rechtsverstoß im Unternehmen verhindern konnte und dies auch zu seinem Aufgabenbereich gehörte.

Für den Compliance-Officer ist wie für die Unternehmensleitung eine zivilrechtliche und eine strafrechtliche Verantwortlichkeit zu unterscheiden. Die zivilrechtliche Verantwortlichkeit des Compliance-Beauftragten ergibt sich aus seinem Arbeitsvertrag und ggf. aus den Compliance-Richtlinien des Unternehmens. Meist sind darin Pflichten für den Compliance-Beauftragten festgelegt, die über das Pflichtenspektrum anderer Unternehmensmitarbeiter hinausgehen. Die zivilrechtliche Haftung kann zu Schadenersatzansprüchen des Arbeitgebers oder Dritter führen. Sowohl für den Compliance-Beauftragten als auch für die Unternehmensführung ist es sinnvoll, dem Compliance-Beauftragten nur solche Aufgaben aufzuerlegen, die er realistischerweise auch bewältigen kann. Ansonsten kommt neben einer Haftung des Compliance-Officers auch eine Haftung der Geschäftsleitung für Organisationsverschulden in Betracht. Das Haftungsrisiko für den Compliance-Beauftragten kann abgedeckt werden, indem für ihn eine D&O-Versicherung abgeschlossen wird.

Da der Compliance-Beauftragte weitgehend eigenverantwortlich agiert, gilt auch für ihn die von der Geschäftsführung abgeleitete business-judgement-rule. Das bedeutet, er verfügt über einen eigenen Ermessensspielraum. Eine Haftung scheidet aus, soweit er seine Entscheidungen auf der Grundlage angemessener Informationen zum Wohle des Unternehmens trifft. Dies sollte sorgfältig dokumentiert sein.

Zur strafrechtlichen Verantwortlichkeit eines Compliance-Beauftragten hat sich der BGH bereits in einem Urteil aus dem Juli 2009 geäußert (vgl. BGH-Urteil vom 17.07.2009, Az. 5 StR 394/08). Eine gefestigte Rechtsprechung gibt es hierzu aber noch nicht. Nach Auffassung des höchsten deutschen Strafgerichts kann sich für den Compliance-Officer aus seiner besonderen Aufgaben- und Vertrauensstellung eine Garantenpflicht ergeben. Das bedeutet, er ist zur Verhinderung von Rechtsverstößen, insbesondere von Straftaten verpflichtet. Stellt er Rechtsverstöße fest, die aus seinem Unternehmen heraus begangen werden, muss er diese Rechtsverstöße beanstanden und sie den Leitungsorganen seines Unternehmens melden. Unterlässt er dies schuldhaft, muss er strafrechtliche Sanktionen befürchten.

Haftungsrisiken des Compliance-Beauftragten

Gesetz	Haftung für
Strafrechtliche Verantwortlichkeit	
§ 266 in Verbindung mit § 13 StGB	Nicht-Verhinderung von Vermögensschädigungen durch andere Unternehmensmitarbeiter trotz Garantenstellung
Zivilrechtliche Verantwortlichkeit	
§ 823 Abs. 2 BGB in Verbindung mit § 266 StGB	Vermögensschädigungen Dritter, die der Compliance-Beauftragte hätte verhindern können
§ 280 BGB	Verstöße gegen Pflichten des Arbeitsvertrages

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.700 Unternehmen, davon über 1.200 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu gehören fast alle Global Player sowie 800 leistungsstarke Mittelständler und zahlreiche gründergeführte, kreative Unternehmen. Mitglieder sind Anbieter von Software und IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien und der Netzwirtschaft. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.



Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org