Gregor Wecker
Bastian Ohl *Hrsg.*

Compliance in der Unternehmerpraxis

Grundlagen, Organisation und Umsetzung

3. Auflage

Springer Gabler

Compliance in der Unternehmerpraxis

Gregor Wecker • Bastian Ohl
(Hrsg.)

Compliance in der Unternehmerpraxis

Grundlagen, Organisation und Umsetzung

3., aktualisierte und erweiterte Auflage

Springer Gabler

Herausgeber
Dr. Gregor Wecker
Luther Rechtsanwaltsgesellschaft mbH
Köln
Deutschland

Bastian Ohl
Luther Rechtsanwaltsgesellschaft mbH
Köln
Deutschland

ISBN 978-3-658-00892-5
ISBN 978-3-658-00893-2 (eBook)
DOI 10.1007/978-3-658-00893-2

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Gabler

Lektorat: Anna Pietras, Imke Sander

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Gabler ist eine Marke von Springer DE. Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media
www.springer-gabler.de

Vorwort zur 3. Auflage

Drei turbulente Jahre sind seit dem Erscheinen der 2. Auflage vergangen. Das Thema Compliance ist wichtiger denn je, wie man auch an der sich explosionsartig vermehrenden Literatur zum Thema feststellen kann. Immer mehr kleine und mittelständische Unternehmen und insbesondere auch die öffentliche Hand und Unternehmen der öffentlichen Hand beschäftigen sich mit dem Thema „Aufbau einer Compliance-Struktur". Die Sensibilität für das Thema ist nicht zuletzt durch vermehrte Berichterstattung in den Medien und durch generell erhöhte Transparenzanforderungen sehr groß.

Dabei sind die Anforderungen je nach Ausgangslage des Unternehmens (insbesondere abhängig vom Geschäftsgegenstand und -umfeld) sehr unterschiedlich. Eine systematische Herangehensweise mit Blick für das Wesentliche ist daher unerlässlich.

Dass Compliance nicht nur bei großen Dax-Unternehmen ein wichtiges Thema ist, zeigt sich für die Herausgeber und Autoren in ihrer täglichen Praxis und – nicht zuletzt – auch am Erfolg der Vorauflagen. Diese Entwicklungen und die große Aktivität des Gesetzgebers, die eine Vielzahl von Gesetzesänderungen nach sich gezogen hat, sind Anlass genug, eine aktualisierte und erweiterte Auflage vorzulegen.

Unter Fortführung des Konzepts der Vorauflagen wurden die Beiträge daher durchgängig auf den Stand der Rechtsentwicklung bis 31. Dezember 2012 gebracht. Mit einem Beitrag zum Thema „Praxistipps Unternehmenskrise" zollen wir den praktischen Anforderungen der letzten (Krisen-)Jahre Tribut. „Compliance in Unternehmen der öffentlichen Hand" wird unserer Ansicht nach in den nächsten Jahren weiter an Bedeutung gewinnen, so dass wir nunmehr auch einen Einstieg in diesen Themenbereich bieten.

Auch der Beitrag zur Tax Compliance wurde stark erweitert. Als Bestandteil der „Gesamt-Compliance" des Unternehmens geht das Thema Tax Compliance heute weit über die korrekte und pünktliche Erfüllung von Steuererklärungspflichten hinaus, so dass umfassende organisatorische Maßnahmen erforderlich sind. Dies haben wir zum Anlass genommen, uns mit den erforderlichen Maßnahmen noch wesentlich intensiver zu beschäftigen.

Es bleibt aber bei dem Anliegen der Herausgeber – wie schon in den Vorauflagen – dem Leser über einen praxisnahen Zugang einen allgemeinen Einstieg in das Thema Compliance ebenso zu ermöglichen, wie vertiefende Einblicke in besonders Compliance-relevante Schwerpunktthemen. Die Herausgeber möchten dem Leser mit diesem Werk weiter eine praxisnahe Arbeitshilfe anbieten.

Der Dank der Herausgeber gilt erneut den Autoren, die eine schnelle Überarbeitung und Erweiterung erst ermöglicht haben. Insbesondere freuen wir uns, dass sich erstmals auch externe Autoren beteiligt haben. Den Lesern der Vorauflagen sei ebenso gedankt, nicht zuletzt für Ihre Fragen und Anregungen, die im jetzt vorliegenden Werk verarbeitet werden konnten. Ein besonderer Dank geht auch an den bisherigen Co-Herausgeber Hendrik van Laak, der sich bereits im Oktober 2009 für einen Wechsel auf die Richterbank entschieden hat. Auch zur dritten Auflage bleiben die Leserinnen und Leser weiter aufgefordert, Ihre Fragen und Anregungen über *vorname.nachnahme@luther-lawfirm.com* jederzeit direkt an die jeweiligen Autoren oder an die Herausgeber zu richten.

Köln, im Januar 2013

Dr. Gregor Wecker
Bastian Ohl

Inhaltsverzeichnis

Autorenverzeichnis

Silvia C. Bauer, Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: silvia.bauer@luther-lawfirm.com

Guido Dornieden, Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: guido.dornieden@luther-lawfirm.com

Dr. Stefan Galla, Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: stefan.galla@luther-lawfirm.com

Katharina Henschel, An der Welle 10, 60322 Frankfurt a. M., Deutschland
E-Mail: katharina.henschel@luther-lawfirm.com

Dr. Helmut Janssen, Avenue Louise 240, 1050 Brüssel, Belgien
E-Mail: helmut.janssen@luther-lawfirm.com

Christoph Kromer, An der Welle 10, 60322 Frankfurt a. M., Deutschland
E-Mail: christoph.kromer@luther-lawfirm.com

Dr. Detlef Mäder, Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: detlef.maeder@luther-lawfirm.com

Ole-Jochen Melchior, Gildehofstraße 1, 45127 Essen, Deutschland
E-Mail: ole.melchior@luther-lawfirm.com

Christofer Rudolf Mellert, Graf-Adolf-Platz 15, 40213 Düsseldorf, Deutschland
E-Mail: christofer.mellert@luther-lawfirm.com

Robert Nagelschmitz, Auf dem Hügel 34, 53347 Alfter, Deutschland
E-Mail: robert.nagelschmitz@berlin.de

Katja Neumüller, Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: katja.neumueller@luther-lawfirm.com

Bastian Ohl, Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: bastian.ohl@luther-lawfirm.com

Reinhard Pumpler, Immofinanz AG, Wienerbergstr. 11, 1100 Wien, Österreich
E-Mail: r.pumpler@immofinanz.com

Dr. Michael Rath, Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: michael.rath@luther-lawfirm.com

Dr. Eva Rütz, Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: eva.ruetz@luther-lawfirm.com

Volker Steimle, Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: volker.steimle@luther-lawfirm.com

Katrin Süssbrich, Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: katrin.suessbrich@luther-lawfirm.com

Dr. Eberhard Vetter, Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: eberhard.vetter@luther-lawfirm.com

Dr. André Große Vorholt, Karlstraße 10–12, 80333 München, Deutschland
E-Mail: andre.groszevorholt@luther-lawfirm.com

Dr. Gregor Wecker, Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: gregor.wecker@luther-lawfirm.com

Thomas Weidlich, Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: thomas.weidlich@luther-lawfirm.com

Reinhard Willemsen, Karlstraße 10–12, 80333 München, Deutschland
E-Mail: willemsen@luther-lawfirm.com

Abkürzungsverzeichnis

A

a. a. O.	am angegebenen Ort
Abs.	Absatz
AG	Die Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AGG	Allgemeines Gleichbehandlungsgesetz
AktG	Aktiengesetz
AL	Ausfuhrliste
AO	Abgabenordnung
ArbSchG	Arbeitsschutzgesetz
ArbZG	Arbeitszeitgesetz
Art.	Artikel
ASiG	Arbeitssicherheitsgesetz
AuA	Arbeit und Arbeitsrecht
AufenthG	Aufenthaltsgesetz
Aufl.	Auflage
AÜG	Arbeitnehmerüberlassungsgesetz
AWG	Außenwirtschaftsgesetz
AWR	Außenwirtschaftsrecht
AWV	Außenwirtschaftsverordnung
Az.	Aktenzeichen

B

BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
BAFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAKred	Bundesaufsichtsamt für das Kreditwesen
BB	Betriebs-Berater
BDSG	Bundesdatenschutzgesetz
Beschl.	Beschluss
betr.	betrifft

BetrVG	Betriebsverfassungsgesetz
BFH	Bundesfinanzhof
BFHE	Bundesfinanzhof-Entscheidungen
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGHZ	Entscheidungssammlung des Bundesgerichtshofs in Zivilsachen
BI	Business Intelligence
BilMoG	Bilanzrechtsmodernisierungsgesetz
BKartA	Bundeskartellamt
BKR	Bank- und Kapitalmarktrecht
BMF	Bundesministerium für Finanzen
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Errichtungsgesetz
bspw.	beispielsweise
BR-Drucks.	Bundesratsdrucksachen
BT-Drucks.	Bundestagsdrucksachen
bzw.	beziehungsweise

C

CC	Common Criteria for Information Technology Security Evaluation
CCO	Chief Compliance Officer
CIO	Chief Information Officer
CobiT	Control Objectives for Business Information and Related Technologies
Corp.	Corporation
COSO	Committee of Sponsoring Organisations of the Treadway Commission
CR	Computer und Recht
CSO	Chief Security Officer
CSR	Corporate Social Responsibility
CWÜ	Chemiewaffenübereinkommen

D

D&O	Directors and Officers
d. h.	das heißt
DB	Der Betrieb
DCGK	Deutscher Corporate Government Kodex
DoD	Department of Defense
DPL	Denied Persons List
DSD	Duales System Deutschland
DStR	Deutsches Steuerrecht
DZWIR	Deutsche Zeitschrift für Wirtschaft und Insolvenzrecht

E

e. V.	eingetragener Verein
EAR	Export Administration Regulations
ebd.	ebendort
ECM	Enterprise Content Management
EG	Europäische Gemeinschaft
EnSEC	Enterprise Security Management
ERP	Enterprise Resource Planning
EStG	Einkommensteuergesetz
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUR	EURO
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWR	Europäischer Wirtschaftsraum

F

f.	folgende
FBA	Foreign Business Act
ff.	folgende
FIE	Foreign Invested Enterprises
FIPB	Foreign Investment Promotion Board
Fn.	Fußnote
FS	Festschrift

G

GASP	Gemeinsame Außen- und Sicherheitspolitik
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GewO	Gewerbeordnung
GG	Grundgesetz
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	GmbH-Gesetz
GmbHR	GmbH Rundschau
GoB	Grundsätze ordnungsgemässer Buchführung
GoBS	Grundsätze ordnungsgemässer EDV-gestützter Buchführungssysteme
GPSG	Geräte- und Produktsicherheitsgesetz
GRC	Governance Risk Compliance
GWB	Gesetz gegen Wettbewerbsbeschränkungen

H

HGB	Handelsgesetzbuch
HIPAA	Health Insurance Portability and Accountability Act
Hrsg.	Herausgeber

I

i. S.	im Sinne
i.V.m.	in Verbindung mit
ICC	International Chamber of Commerce
ICSID	International Center for Settlement of Investment Disputes
IDW	Institut der Wirtschaftsprüfer
IKS	Internes Kontrollsystem
InsO	Insolvenzordnung
IP	Intellectual Property
ISA	Instrumentation, Systems and Automation Society
ISG	Information Security Governance
ISO	International Standards Organisation
IStR	Internationales Steuerrecht
IT	Informationstechnologie
ITIL	Information Technology Infrastructure Library
ITRB	Information Technology Review Board

J

JZ	Juristenzeitung

K

K&R	Kommunikation & Recht
KG	Kommanditgesellschaft
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KrWaffG	Kriegswaffengesetz
KschG	Kündigungsschutzgesetz
KWG	Kreditwesengesetz

L

LAG	Landesarbeitsgericht
LG	Landgericht

M

M&A	Merger & Acquisition
M.A.	Magister Artium
m.w.N.	mit weiteren Nachweisen
MAH	Mindestanforderungen an das Betreiben von Handelsgeschäften bei Kreditinstituten
MaIR	Mindestanforderungen an die Interne Revision
MaK	Mindestanforderungen für das Kreditgeschäft
MaRisk	Mindestanforderung an das Risikomanagement
MMR	Multimedia und Recht

MRC	Management Risk Controlling
Mrd.	Milliarde
MTCR	Missile Technology Control Regime
MüKo	Münchener Kommentar

N

NJW	Neue juristische Wochenschrift
Nr.	Nummer
NSG	Nuclear Suppliers Group
NVwZ	Neue Verwaltungsrecht-Zeitung
NZA	Neue Zeitschrift für Arbeitsrecht
NZA-RR	Neue Zeitschrift für Arbeitsrecht – Rechtsprechungsreport

O

ÖBA	Bank-Archiv
OEM	Original equipment manufacturer
OFT	Office of Fair Trading
OHG	Offene Handelsgesellschaft
OLG	Oberlandesgericht
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
OwiG	Ordnungswidrigkeitengesetz

P

PC	Personal Computer
ProdHaftG	Produkthaftungsgesetz
PS	Prüfungsstandards

R

RDV	Rahmendienstvereinbarung
RegBegr	Regierungsbegründung
RIW	Recht der Internationalen Wirtschaft
Rn.	Randnummer

S

S.	Seite
s. u.	siehe unten
SAM	Steueranwaltsmagazin
SchiedsVZ	Die neue Zeitschrift für Schiedsverfahren
SEC	Securities and Exchange Commission
SGB	Sozialgesetzbuch
SiG	Signaturgesetz
SOA	Sarbanes-Oxley Act
SOD	Segregation of Duties

SOX	Sarbanes-Oxley Act
StGB	Strafgesetzbuch
StuW	Steuern und Wirtschaft
T	
t	Tonne
TKG	Tele-Kommunikations-Gesetz
TMG	Telemediengesetz
U	
u. ä.	und ähnliches
UN	United Nations
Urt. v.	Urteil vom
USD	United States Dollar
V	
VAG	Versicherungsaufsichtsgesetz
VersR	Versicherungsrecht
vgl.	vergleiche
VO	Verordnung
VVG	Versicherungsvertragsgesetz
W	
WM	Wertpapiermitteilungen
WpHG	Wertpapierhandelsgesetz
WTO	World Trade Organisation
X	
XAM	Extensible Access Method
XBRL	Extensible Business Reporting Language
Z	
z. B.	zum Beispiel
ZBB	Zeitschrift für Bankrecht und Bankbetriebswirtschaft
ZfIR	Zeitschrift für Immobilienrecht
ZGR	Zeitschrift für Unternehmens- und Gesellschaftsrecht
ZIP	Zeitschrift für Wirtschaftsrecht und Insolvenzpraxis
ZRP	Zeitschrift für Rechtspolitik mit Rechtspolitischer Umschau
ZWeR	Zeitschrift für Wettbewerbsrecht

Compliance im Unternehmen

Eberhard Vetter

Inhaltsverzeichnis

Zusammenfassung

In den neunziger Jahren des letzten Jahrhunderts war Compliance in Deutschland, nimmt man die Kreditwirtschaft aus (Siehe z. B. *Weiss*, Die Bank 1993, 136, 137), noch ein weitgehend unbekannter Begriff (Siehe aber auch z. B. *Assmann*, AG 1994, 237, 255; *Eisele*, WM 1993, 1021). Der dem anglo-amerikanischen Rechtskreis entstammende Rechtsbegriff umschreibt die Pflicht, die für das Unternehmen geltenden

E. Vetter (✉)
Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: eberhard.vetter@luther-lawfirm.com

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2_1, © Springer Fachmedien Wiesbaden 2013

Gesetze einzuhalten. Damit verbindet sich zweifelsfrei keine neue Erkenntnis. Insoweit ist Compliance zu Recht als eine Binsenweisheit bezeichnet worden (*Uwe. H. Schneider*, ZIP 2003, 645, 646; zustimmend etwa *Goette*, ZHR 175 (2011), 388, 391; *Hüffer*, FS G. H. Roth, 2011, S. 299, 302; siehe z. B. auch *Zöllner/Noack*, in: Baumbach/Hueck, GmbHG, 19. Aufl. 2010, § 35 Rn. 68a). Neu ist jedoch die Einbettung der Compliance in einen größeren Zusammenhang. Es wäre für die Geschäftsleitung eine Illusion zu glauben, Compliance vollziehe sich im Unternehmen stets von selbst. Richtig ist vielmehr, dass eine vorbildliche Compliance sowohl aus organisationstheoretischer Sicht wie auch aus rechtlicher Sicht ein proaktives Vorgehen der Geschäftsleitung erforderlich macht und das gesamte Unternehmen erfassen muss. Compliance beschränkt sich deshalb nicht allein auf das Postulat der Rechtstreue des Unternehmens, sondern umschreibt die Summe der organisatorischen Maßnahmen eines Unternehmens, mit denen gewährleistet werden soll, dass sich die Geschäftsleitung wie auch die Mitarbeiter des Unternehmens rechtmäßig verhalten (*Bürkle,* BB 2005, 565, 569; *Kiethe,* GmbHR 2007, 393, 394; *Uwe. H. Schneider,* ZIP 2003, 645, 646). Der Begriff der Compliance erfährt damit eine Erweiterung hin zur Compliance-Organisation.

1 Einleitung

Angesichts des immer umfangreicher werdenden Verantwortungs- und Handlungsrahmens der Geschäftsleitung, der durch zivilrechtliche und öffentlich-rechtliche Pflichten bestimmt wird und aus dem sich eine Vielzahl von rechtlichen Risiken für das Unternehmen ergeben, haben die Vorstände und Geschäftsführer vieler Gesellschaften erkannt, dass sie in weitem Umfang präventiv und proaktiv tätig zu werden haben, wenn sie ihrer Compliance-Verantwortung nachkommen wollen. Sie wollen es gerade nicht allein damit belassen, darauf zu vertrauen, dass sich die Organisation, für die sie Verantwortung tragen, gesetzeskonform und ordnungsgemäß verhält, sondern sie haben Compliance zur Chefsache erklärt. Sie verstehen Compliance nicht nur als bloße Prävention gegenüber Risiken aus Rechtsverstößen, sondern erkennen nicht selten den Wert eines funktionierenden Compliance-Managements als einen strategischen Vorteil gegenüber dem Wettbewerb. Dabei ist nicht nur daran zu denken, dass mit Hilfe von Compliance-Maßnahmen vermieden werden kann, dass z. B. ein Unternehmen wegen Rechtsverstößen auf die sog. Schwarze Liste gerät und damit von künftigen lukrativen Aufträgen ausgeschlossen wird. Bemerkenswert ist vielmehr auch die generell wachsende Erkenntnis, dass es Unternehmen in der Regel vorziehen, ihre Geschäftsbeziehungen nur mit Gesellschaften aufzunehmen, bei denen sie nicht mit dem Risiko rechnen müssen, dass dort Rechtsverstöße und Unregelmäßigkeiten festgestellt werden, die auf ihre eigenen Geschäftsaktivitäten durchschlagen

können und ihre eigene Reputation am Markt beeinträchtigen.[1] Damit erweist sich Compliance nicht nur als Bestandteil einer good Corporate Governance sondern auch als Marketing-Faktor.[2]

Die Bedeutung der Compliance darf auch aus volkswirtschaftlicher Sicht nicht unterschätzt werden. Nach Schätzungen des Bundeskriminalamtes beträgt der durch Wirtschaftskriminalität verursachte Schaden in Deutschland rund 4,7. Mrd. €; pro Unternehmen belief sich der durchschnittliche Schaden auf 8,4 Mio. €.[3] Bemerkenswert ist auch, dass nach einer Umfrage unter Inhouse-Juristen in den USA vor wenigen Jahren dem Thema Compliance die oberste Priorität noch vor der Kostenkontrolle eingeräumt wurde.[4] Die zunehmende Zahl von Compliance-Beauftragten oder Compliance-Abteilungen in deutschen Unternehmen bestätigen diesen Befund.

2 Compliance als Geschäftsleitungsaufgabe

2.1 Begriff und Zweck der Compliance

Abgesehen von branchenspezifischen Sondernormen gibt es weder eine gesetzliche Definition von Compliance, noch ist bislang eine allgemein anerkannte Definition vorhanden. Aber seit der Neufassung des Deutschen Corporate Governance Kodex, die am 20. Juli 2007 im elektronischen Bundesanzeiger bekannt gemacht worden ist,[5] steht eine Umschreibung zur Verfügung, die sich zwar primär an börsennotierte Aktiengesellschaften richtet (§ 161 AktG), die aber durchaus auch als allgemeine Definition der Corporate Compliance gelten kann.[6]

Ziff. 4.1.3 Deutscher Corporate Governance Kodex formuliert wie folgt:

> Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance).

Hinzuweisen ist darauf, dass die Kodex-Kommission die Pflicht zur Compliance zu Recht nicht nur auf die Beachtung der gesetzlichen Bestimmungen beschränken will, sondern

---

[1] Freiwillige ISO-Zertifizierungen und vergleichbare Maßnahmen zur Zertifizierung der Einhaltung von Umwelt und Sozialstandards mögen hier als Vorbilder dienen.

[2] *Bergmoser/Theusinger/Gushorst*, BB-Special zu Heft 5 2008, 1, 2; *Grundmeier*, Rechtspflicht zur Compliance im Konzern, 2011, S. 13; *Kort*, NZG 2008, 81; *Lösler*, NZG 2005, 104, 105.

[3] Vgl. Börsen-Zeitung v. 26. 10. 2011, S. 9.

[4] Umfrage der Association of Corporate Counsel (ACC), Juve Datenbank vom 6. November 2006, im Internet zugänglich über www.juve.de; siehe auch *Kort*, NZG 2008, 81, 85.

[5] Im Internet zugänglich unter www.bundesanzeiger.de.

[6] Vgl. *Bürkle*, BB 2007, 1797, 1998; *E. Vetter*, DB 2007, 1963.

auch die unternehmensinternen Regelwerke einbezogen hat, so dass sich die Compliance-Verantwortung sowohl auf die Bestimmungen von Satzung und Geschäftsordnung aber darüber hinaus z. B. auch auf Ethik-Richtlinien, Merk- und Informationsblätter, Unterschriftenregelungen, Arbeitsanweisungen und Konzernrundschreiben erstreckt.[7] Mit Letzterem geht sie allerdings über die Beschreibung des geltenden Rechts hinaus. Dies entspricht aber auch dem Verständnis, wie es im Prüfungsstandard IDW PS980 niedergelegt ist.[8]

Compliance dient sowohl der Risikovorbeugung als auch der Schadensabwehr im Unternehmen. Sie ist regelmäßig geeignet, Schadensersatzansprüche Dritter gegen die Gesellschaft (sog. Außenhaftung) abzuwehren wie auch Ansprüche der Gesellschaft gegen die Mitglieder des Geschäftsleitungs- und des Aufsichtsorgans (sog. Innenhaftung) zu vermeiden. Dabei ist von erheblicher Bedeutung, dass im Bereich der Innenhaftung die Mitglieder des Vorstands einer AG die Beweislast dafür tragen, dass sie bei ihrer Geschäftsführung die notwendige Sorgfalt beachtet haben (§ 93 Abs. 2 Satz 2 AktG). Das GmbHG enthält zwar keine mit § 93 Abs. 2 AktG vergleichbare Vorschrift. Für die Geschäftsführer einer GmbH gilt nach allgemeiner Meinung gleichwohl die Regelung des § 93 Abs. 2 Satz 2 AktG analog.[9]

Compliance versteht sich nach zutreffender Ansicht[10] auch als Teil des Risikofrüherkennungs- und Überwachungssystems (sog. Risikomanagement), zu dessen Einrichtung und Unterhaltung der Vorstand einer AG nach § 91 Abs. 2 AktG im Hinblick auf existenzgefährdende Risiken verpflichtet ist, wie es auch in Ziff. 4.1.4 Deutscher Corporate Governance Kodex ausdrücklich angesprochen wird. Die Vorschrift von § 91 Abs. 2 AktG ist zwar nach herrschender Meinung nicht geeignet, eine Verpflichtung zum Aufbau einer Compliance-Organisation zu stützen.[11] Da zweifelsfrei zahlreiche Risiken aus Rechtsverstößen eine bestandsgefährende Dimension einnehmen können, lässt sich die enge Beziehung der Compliance zum Risikofrüherkennungssystem

---

[7] *Kort*, NZG 2008, 81, 86; *E. Vetter*, FS Graf von Westphalen, 2010, S. 719, 728; siehe auch *Kremer/Klahold*, ZGR 2010, 113, 117; Skepsis hingegen bei *Hüffer*, FS G. H. Roth, 2011, S. 299, 302.

[8] IDW PS 980, Tz. 5; siehe zur rechtlicher Einordnung z. B. *Böttcher*, NZG 2011, 1054, 1055; *Klindt/Pelz/Theusinger*, NJW 2010, 2385, 2387.

[9] BGH v. 4. 11. 2002 – II ZR 224/00, BGHZ 152, 280, 283; *Altmeppen*, in: Roth/Altmeppen, GmbHG, 7. Aufl. 2012, § 43 Rn. 110; *Zöllner/Noack*, in: Baumbach/Hueck, GmbHG, 20. Aufl. 2013, § 43 Rn. 22.

[10] *Fleischer*, AG 2003, 291, 298; *Hauschka*, in: Gesellschaftsrecht in der Diskussion 2007, 2008, S. 51, 53, 59; *Uwe H. Schneider*, ZIP 2003, 645, 649.

[11] *Bachmann*, in: Gesellschaftsrecht in der Diskussion 2007, 2008, S. 65, 73; *Fleischer*, in: Spindler/Stilz, AktG, 2. Aufl. 2010, § 91 Rz. 47; *Grundmeier*, Rechtspflicht zur Compliance im Konzern, 2011, S. 27; *Hüffer*, FS G. H. Roth, 2011, S. 299, 304; *Immenga*, FS Schwark, 2009, S. 199, 201; *Kindler*, FS G. H. Roth, 2011, S. 367, 370; *Koch*, WM 2009, 1013, 1014; *E. Vetter*, FS Graf von Westphalen, 2010, S. 719, 727; a. A. *Berg*, AG 2007, 271; *Dreher*, FS Hüffer, 2010, S. 161, 171; *Schwintowski*, NZG 2005, 200, 201.

im Sinne § 91 Abs. 2 AktG kaum leugnen.[12] Das GmbHG enthält zwar keine mit § 91 Abs. 2 AktG vergleichbare Vorschrift. Gleichwohl besteht allgemein Einigkeit, dass auch die Geschäftsführung einer GmbH eine entsprechende Pflicht trifft und systematische Maßnahmen zur Erfassung bestandsgefährdender Risiken zu ergreifen hat, sofern das Unternehmen eine kritische Größe erreicht hat.[13] Entsprechendes lässt sich auf die Compliance-Verantwortung der Geschäftsführung der GmbH übertragen.

Compliance versteht sich primär als Prävention, sie reicht aber darüber hinaus. Allerdings ist auch anzuerkennen, dass selbst eine vorbildliche Compliance-Organisation Regelverstöße im Einzelfall nicht vollkommen auszuschließen vermag.[14] Compliance umfasst deshalb auch das Krisenmangement im Unternehmen. Bei Eintritt einer Krise durch einen Regelverstoß findet die Compliance Ausdruck in den Maßnahmen zur Krisenbewältigung und Schadensminderung wie auch der angemessenen Kommunikationsstrategi[15], für die im Rahmen der Compliance-Organisation Notfallpläne zu erarbeiten sind.[16]

2.2 Rechtsgrundlage der Compliance

Das Deutsche Recht kennt keine Gesetzesnorm, die die Geschäftsleitung einer AG oder GmbH allgemein zur Vornahme systematischer Compliance-Maßnahmen und zur Einrichtung einer allgemeinen Compliance-Organisation verpflichtet. Allerdings sieht § 76 Abs. 1 AktG vor, dass der Vorstand die Gesellschaft unter eigener Verantwortung zu leiten hat und, wie § 93 Abs. 1 AktG bestimmt, dabei die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden hat. Für die GmbH Geschäftsführer findet sich, was ihre Sorgfaltspflichten anbetrifft, die Parallele zu § 93 Abs. 1 AktG in § 43 Abs. 1 GmbHG. Aus den §§ 76 Abs. 1 und 93 Abs. 1 AktG lässt sich grundsätzlich eine organschaftliche Pflicht des Vorstands zur Legalitätskontrolle der im Unternehmen tätigen Mitarbeiter und der Ergreifung von geeigneten organisatorischen Maßnahmen ableiten.[17] Als weitere Rechtsgrundlage für die Ergreifung von Compliance-Maßnahmen lassen sich auch die §§ 3, 9 und 130 OWiG heranziehen. § 130 OWiG weist die Pflich-

[12] Ähnlich *Mertens/Cahn*, in: Kölner Kommentar AktG, 3. Aufl. 2010, § 91 Rn. 34; *Uwe H. Schneider*, ZIP 2003, 645, 649; siehe auch *Berg*, AG 2007, 271, 274; Zweifel bei *Immenga*, FS Schwark, 2009, S. 199, 201.

[13] *Altmeppen*, in: Roth/Altmeppen, GmbHG, 7. Aufl. 2012, § 43 Rn. 17; *Kleindiek*, in: Lutter/Hommelhoff, GmbHG, 18. Aufl. 2012, § 43 Rn. 31; *Zöllner/Noack*, in: Baumbach/Hueck, GmbHG, 20. Aufl. 2013, § 43 Rn. 17.

[14] Unstreitig siehe z. B. *Kremer/Klahold*, ZGR 2010, 113, 118.

[15] Siehe dazu z. B. *Jahn*, in: Krieger/Uwe H. Schneider (Hrsg.), Handbuch Managerhaftung, 2. Aufl. 2010, § 38 Rn. 14.

[16] Vgl. dazu z. B. *Rodewald/Unger*, BB 2007, 1629, 1633.

[17] *Fleischer*, AG 2003, 291, 299; *Fleischer*, CCZ 2008, 1, 2; *Hüffer*, FS G. H. Roth, 2011, S. 299, 302; *Mertens/Cahn*, in: Kölner Kommentar AktG, 3. Aufl. 2010, § 91 Rn. 35; *Uwe. H. Schneider*, ZIP 2003, 645, 648; *E. Vetter*, in: Krieger/Uwe H. Schneider (Hrsg.), Handbuch Managerhaftung, 2. Aufl. 2010,

tenstellung der Aktiengesellschaft als Inhaberin des Betriebes bzw. des Unternehmens dem Vorstand, beziehungsweise der Geschäftsführung der juristischen Person zu mit der Folge, dass das Organmitglied grundsätzlich für alle Verletzungen bußgeldbewehrter Pflichten in einem Unternehmen zur Rechenschaft gezogen werden kann, soweit der Verstoß auf eine Verletzung von Aufsichtspflichten zurückgeführt werden kann. Berücksichtigt man, dass eine Vielzahl öffentlichrechtlicher Pflichten eines Unternehmens in irgendeiner Form mit einem Bußgeld bewehrt sind (z. B. Kartellrecht, Kapitalmarktrecht, Umweltrecht, Datenschutzrecht, Arbeitsstrafrecht, Außenwirtschaftsrecht), lässt sich dem Ordnungswidrigkeitenrecht damit jedenfalls mittelbar die Verpflichtung zur Einrichtung einer Compliance-Organisation entnehmen, für die die Mitglieder des Geschäftsleitungsorgans selbst verantwortlich sind.[18] Darüber hinaus ist auch auf die sektorspezifischen Anforderungen von § 25a KWG[19], § 64a VAG und § 33 WpHG hinzuweisen, die von Kreditinstituten, Versicherungsunternehmen[20] oder Wertpapierdienstleistungsunternehmen[21] die Einrichtung einer ordnungsgemäßen Organisation zur Einhaltung der von diesen jeweils zu beachtenden gesetzlichen Bestimmungen verlangen. Gleichwohl ist dabei festzuhalten, dass eine sektorenübergreifende Anwendung dieser aufsichtsrechtlichen Anforderungen in aufsichtsfreie Wirtschaftsbereiche im Wege der Analogie nicht in Betracht kommt,[22] auch wenn sich eine gewisse Ausstrahlungswirkung nicht vermeiden lässt.[23]

Die Verantwortung für die Einrichtung eines Compliance-Systems trägt die Geschäftsleitung im Rahmen ihrer Leitungsaufgabe.[24] Eine Verpflichtung für konkrete

§ 18 Rn. 29; zurückhaltend freilich *Hauschka*, ZIP 2004, 877, 882; siehe auch die Nachweise oben in Fußnote 15.

[18] Zur Kartellrechts-Compliance siehe den Beitrag von *Janssen* in Kap. 10 und weiter z. B. *Dreher*, in: Krieger/Uwe. H. Schneider (Hrsg.), Managerhaftung, 2. Aufl. 2010, § 31 Rn. 59 ff.; *Pampel*, BB 2007, 1636; zur Kapitalmarktrechts-Compliance z. B. *Krämer*, in: Krieger/Uwe. H. Schneider (Hrsg.), Managerhaftung, 2. Aufl. 2010,§ 28 Rn. 83 ff. und zur Umweltrechts-Compliance z. B. *Uwer*, in: Krieger/Uwe. H. Schneider (Hrsg.), Managerhaftung, 2. Aufl. 2009, § 34 Rn. 23 ff.

[19] Siehe dazu z. B. *Gebauer/Kleinert*, in: Krieger/Uwe H. Schneider (Hrsg.), Handbuch Managerhaftung, 2. Aufl. 2010, § 20.

[20] Siehe dazu z. B. *Dreher*, WM 2008, 1765; *Preusche*, in: in: Hauschka (Hrsg.), Corporate Compliance, 2. Aufl. 2010, § 37.

[21] Siehe dazu z. B. *Casper*, FS Karsten Schmidt, 2009, S. 199; *Gebauer/Kleinert*, in: Krieger/Uwe H. Schneider (Hrsg.), Handbuch Managerhaftung, 2. Aufl. 2010, § 20; *Gebauer/Niermann*, in: Hauschka (Hrsg.), Corporate Compliance, 2. Aufl. 2010, § 36.

[22] *Bürkle*, BB 2005, 567; *Grundmeier*, Rechtspflicht zur Compliance im Konzern, 2011, S. 34; Koch, WM 2009, 1013, 1020; *Spindler*, WM 2008, 905, 908; *Verse*, ZHR 175 (2011), 401, 403.

[23] *Hüffer*, AktG, 10. Aufl. 2012, § 76 Rz. 9a; von "Schrittmacherrolle" spricht insoweit z. B. *Fleischer*, ZIP 2003, 1, 10; *Fleischer*, in: Spindler/Stilz, AktG, 2. Aufl. 2010, § 91 Rn. 52; siehe auch *Grundmeier*, Rechtspflicht zur Compliance im Konzern, 2011, S. 24; *Kort*, NZG 2008, 81, 83.

[24] *Bürkle*, in: Hauschka (Hrsg.), Corporate Compliance, 2. Aufl. 2010, § 8 Rn. 12; *Fleischer*, in: Fleischer (Hrsg.), Handbuch des Vorstandsrechts, 2006, § 8 Rn. 44; *Mertens/Cahn*, in: Kölner Kommentar AktG, 3. Aufl. 2010, § 91 Rn. 35; *Uwe. H. Schneider*, ZIP 2003, 645, 646; *Spindler*, WM 2008, 905, 909; *Zöllner/Noack*, in: Baumbach/Hueck, GmbHG, 20. Aufl. 2013, § 35 Rn. 68a.

Compliance-Maßnahmen in einem Unternehmen lässt sich aus den genannten Vorschriften jedoch nicht ableiten.[25] Auch der Deutsche Corporate Governance Kodex enthält keine konkreten Vorgaben oder Empfehlungen zu Art und Umfang der Compliance. Compliance ist keine konfektionierte Standard-Organisation. Die konkrete Ausgestaltung der Compliance in einem Untenehmen hängt nach zutreffender herrschender Ansicht vom jeweiligen Geschäftszweig und dem konkreten Unternehmensgegenstand, der Größe und Komplexität des Unternehmens und der Unternehmensstruktur und damit letztlich von seinem individuellen Risikoprofil ab.[26] Die individuellen Compliance-Maßnahmen stehen im Übrigen generell unter dem Vorbehalt des unternehmerischen Ermessens des Vorstands im Sinne von § 93 Abs. 1 Satz 2 AktG und unterliegen damit der sog. Business Judgment Rule.[27] Der Vorstand hat über Art und Umfang der organisatorischen Maßnahmen zu entscheiden, wie für die Rechtstreue im Unternehmen gesorgt werden soll und auf welche Weise Rechtsverstöße verhindert werden sollen. Dies bedeutet, dass das Geschäftsleitungsorgan bei der Festlegung der Anforderungen und der Dimensionierung einer Compliance-Organisation nach sorgfältiger Ermittlung der relevanten Risikofaktoren das individuelle Gefahrenpotential und Risikoszenario des Unternehmens beurteilen und bewerten muss. Die Geschäftsleitung muss die jeweiligen Konsequenzen für das Unternehmen vor Augen haben, die bei Eintritt eines spezifischen Risikos entstehen können. Versäumnisse können einen Sorgfaltsverstoß im Sinne von § 93 Abs. 2 AktG und § 43 Abs. 2 GmbHG bilden und Schadensersatzansprüche der Gesellschaft gegen die verantwortlichen Organmitglieder nach sich ziehen.[28]

2.3 Compliance im Konzern

Bildet ein Unternehmen die Spitze eines Konzerns, so ist umstritten, ob sich die Compliance auch auf die nachgeordneten Konzernunternehmen erstreckt. Ziff. 4.1.3 Deutscher Corporate Governance Kodex setzt dies offensichtlich als geltendes Recht voraus, indem

---

[25] *Bürkle*, BB 2005, 565, 569; *Hauschka*, ZIP 2004, 877, 878; *Kort*, FS Hopt, 2010, S. 983, 994; *E. Vetter*, FS Graf von Westphalen, 2010, S. 719, 729; weitergehend allerdings *Krieger/Sailer-Coceani*, in: K. Schmidt/Lutter, AktG, 2. Aufl. 2010, § 93 Rn. 6; *Uwe H. Schneider*, ZIP 2003, 645; *Uwe H. Schneider*, in: Scholz GmbHG, 11. Aufl. 2012, § 43 Rz. 361; vgl. auch *Preußner*, NZG 2004, 57, 60.

[26] Siehe allgemein *Fleischer*, in: Fleischer (Hrsg.), Handbuch des Vorstandsrechts, 2006, § 8 Rn. 44; *Hauschka*, AG 2004, 461, 465; *Hüffer*, FS G. H. Roth, 2011, S. 299, 304; *Kiethe*, GmbHR 2007, 393, 396; *Immenga*, FS Schwark, 2009, S. 199, 203; *Koch*, WM 2009, 1013, 1014; *Reichert/Ott*, ZIP 2009, 2173, 2174; *Spindler*, in: Münchener Kommentar AktG, 3. Aufl. 2008, § 91 Rn. 36; *E. Vetter*, FS Graf von Westphalen, 2010, S. 719, 728; *Zöllner/Noack*, in: Baumbach/Hueck, GmbHG, 20. Aufl. 2013, § 43 Rn. 17.

[27] Ebenso *Bachmann*, in: Gesellschaftsrecht in der Diskussion 2007, 2008, S. 65, 85; *Bürkle*, BB 2005, 565, 568; *Fleischer*, in: Spindler/Stilz, AktG, 2. Aufl. 2010, § 91 Rn. 53; *Goette*, ZHR 175 (2011), 388, 393; *Hüffer*, FS G. H. Roth, 2011, S. 299, 305; *Kort*, FS Hopt, 2010, S. 983, 991; *Mertens/Cahn*, in: Kölner Kommentar AktG, 3. Aufl. 2010, § 91 Rn. 37; *Spindler*, in: Münchener Kommentar AktG, 3. Aufl. 2008, § 91 Rn. 36; *M. Winter*, FS Hüffer, 2010, S. 1103, 1106.

[28] *Fleischer*, AG 2003, 291, 300; *Kleindiek*, in: Lutter/Hommelhoff, GmbHG, 17. Aufl. 2009, § 43 Rn. 22; *Kort*, NZG 2008, 81, 84; *Kort*, FS Hopt, 2010, S. 983, 990; *Kremer/Klahold*, ZGR 2010, 113, 141; siehe auch *Kindler*, FS G. H. Roth, 2011, S. 367, 372 ff.

sie ausdrücklich festhält, dass der Vorstand auch auf die Beachtung der Gesetze durch die Konzernunternehmen hinwirkt. Der Europäische Gerichtshof sieht dies nicht wesentlich anders. Nach ständiger Rechtsprechung werden Mutter- und Tochtergesellschaft als wirtschaftliche Einheit betrachtet, wenn die Mutter entscheidenden Einfluss auf die Geschäftsaktivitäten der Tochter ausübt. So hat der EuGH in einem Urteil aus dem Jahre 2009 die Holdinggesellschaft an der Konzernspitze bei der Verhängung von Geldbußen einbezogen, obwohl ihr selbst kein Verstoß wegen kartellrechtswidriger Absprachen vorgeworfen wurde, sondern die Verstöße von Tochter- und Enkelgesellschaften begangen worden waren. Diese Konzerngesellschaften wurden der Konzernspitze zugerechnet.[29]

Über die Rechtsgrundlage und die Reichweite der Compliance im Konzern besteht keine gefestigte Meinung. Gleichwohl ist anerkannt, dass die Geschäftsleitung der Obergesellschaft im Rahmen ihrer Geschäftsleitungsverantwortung (§§ 76, 93 Abs. 1 AktG, § 43 GmbHG) Kontrollpflichten im Konzern wahrzunehmen hat.[30] Diese besteht unabhängig von der Compliance-Verantwortung der Geschäftsführung der einzelnen Konzernggesellschaften. In jedem Fall muss aber der konkreten Konzernform und der sich daraus ergebenden spezifischen Einwirkungsmöglichkeiten der Konzernleitung Rechnung getragen werden, das heißt, es ist stets zu prüfen, in wieweit ist die Konzernspitze rechtlich auch in der Lage, eigene Compliance-Vorstellungen im Konzernunternehmen durchzusetzen.[31] Dies ist kraft Weisungsrecht nach § 308 AktG dann möglich, wenn zwischen dem herrschenden Unternehmen und der Tochtergesellschaft ein Beherrschungsvertrag i. S. von § 291 AktG besteht. Ist die Tochtergesellschaft in der Rechtsform der GmbH organisiert, kann die Weisung auch durch einen entsprechenden Beschluss der Gesellschafterversammlung nach § 37 Abs. 1 GmbHG erfolgen, der für die Geschäftsführer der Tochtergesellschaft bindend ist.[32] Bei einer Tochtergesellschaft in der Rechtsform der AG bleibt im faktischen Konzern infolge der Schranken der §§ 311 ff. AktG jedoch der Konzernspitze nur die Möglichkeit, gegenüber der Geschäftsleitung der Tochtergesellschaft auf die Beachtung der Compliance-Vorstellungen der Konzernspitze in geeigneter Weise

[29] EuGH v. 10. 9. 2009 – C–97/08, EUZW 2009, 816, 820 (Akzo Nobel); siehe bereits EuGH v. 16. 11. 2000 – C–286/98 P, Slg. 2000, I 9925 Rn. (Stora); siehe dazu eingehend *Koch*, ZHR 171, 554, 556; *Grundmeier*, Rechtspflicht zur Compliance im Konzern, 2011, S. 62 ff.

[30] OLG Jena v. 12. 8. 2009 – 7 U 244/07, NZG 2010, 226, 227; *Bachmann*, in: Gesellschaftsrecht in der Diskussion 2007, 2008, S. 65, 94; *Fleischer*, CCZ 2008, 1, 3; *Grundmeier*, Rechtspflicht zur Compliance im Konzern, 2011, S. 83; *Lutter*, FS Goette, 2011, S. 289, 291; *Mertens/Cahn*, in: Kölner Kommentar AktG, 3. Aufl. 2010, § 76 Rn. 65; *Uwe H. Schneider*, NZG 2009, 1321, 1325; *Uwe H. Schneider/Sven H. Schneider*, ZIP 2007, 2061, 2063; *Verse*, ZHR 175 (2011), 401, 413; *M. Winter*, FS Hüffer, 2010, S. 1103, 1108; zurückhaltend aber *Hüffer*, FS G. H. Roth, 2011, S. 299, 306; *Koch*, WM 2009, 1013, 1019.

[31] *Bachmann*, in: Gesellschaftsrecht in der Diskussion 2007, 2008, S. 65, 94; *Fleischer*, DB 2005, 759, 763; *Fleischer*, CCZ 2008, 1, 3; *Ringleb*, in: Ringleb/Kremer/Lutter/v. Werder, Deutscher Corporate Governance Kodex, 4. Aufl. 2010 Rn. 616; vgl. auch *Sven H. Schneider/Uwe H. Schneider*, AG 2005, 57, 59.

[32] *Altmeppen*, in: Roth/Altmeppen, GmbHG, 7. Aufl. 2012, § 37 Rn. 3 und § 43 Rn. 7; *Zöllner/Noack*, in: Baumbach/Hueck, GmbHG, 20. Aufl. 2013, § 37 Rn. 20.

hinzuwirken. Rechtliche Instrumente zur unmittelbaren Durchsetzung der Vorstellungen der Konzernspitze bestehen in diesem Fall nicht. Die Aufnahme von entsprechenden Regelungen in den Anstellungsvertrag der Mitglieder des Vorstands, die sie zur Beachtung der Konzernrichtlinen verpflichtet, erweisen sich in der Praxis im Hinblick auf § 311 AktG kaum von Wert. Der Wortlaut von Ziff. 4.1.3 Deutscher Corporate Governance Kodex lässt deutlich das Bemühen erkennen den von der spezifischen Konzernform abhängigen unterschiedlich starken Einwirkungsmöglichkeiten der Konzernleitung Rechnung zu tragen.[33]

2.4 Das Risikopotential der Unternehmen bei Rechtsverstößen

Die Risiken der Unternehmen aus Gesetzesverstößen, Schadensfällen oder sonstigen Missständen der Beachtung von Regeln und Verhaltensstandards infolge von unterlassenen oder unzureichenden Compliance-Maßnahmen sind vielfältig und dürfen keinesfalls unterschätzt werden. Jüngste Negativbeispiele, die in der Öffentlichkeit große Aufmerksamkeit erzielt haben, können dabei als Mahnung dafür dienen (VW, Siemens, Lidl, Ferrostahl, MAN), welche Wirkungen das Bekanntwerden von Gesetzes- und Regelverstößen auf das öffentliche Ansehen eines Unternehmens, die Motivation seiner Mitarbeiter, die Akzeptanz seiner Produkte am Markt und damit letztlich auf seine wirtschaftliche Situation haben kann.

Ein Rechtsverstoß und Compliance-bezogener Misstand im Unternehmen kann dramatische Konsequenzen für das Unternehmen bedeuten, die vom Reputationsverlust und dem Ausschluss von öffentlichen und privaten Auftragsvergaben über erhebliche finanzielle Einbußen bis hin zu strafrechtlichen Maßnahmen gegen Management und Mitarbeiter reichen. Beispielhaft lassen sich die folgenden Konsequenzen nennen:

- Gefährdung des Unternehmens durch negative Berichte in den Medien über Missstände im Unternehmen
- Werteverfall für die Shareholder
- Eingreifen des Aufsichtsrates
- Eingreifen von Aufsichtsbehörden
- Vergabesperre und „Blacklisting“ für künftige Aufträge
- Betriebsstillegung
- Unternehmenskrise, Gefährdung der Arbeitsplätze
- Bußgelder bis zu 10 % des Konzernumsatzes
- Verfall des mit inkriminierten Geschäften erzielten Gewinns an die Staatskasse
- Untersuchungshaft und Freiheitsstrafe für Manager
- Geldstrafen für Management und Unternehmen
- Einstweilige Verfügung gegen die Durchführung einzelner Geschäftsaktivitäten

[33] Vgl. *Ringleb*, in: Ringleb/Kremer/Lutter/v. Werder, Deutscher Corporate Governance Kodex, 4. Aufl. 2010, Rn. 616.

- Pfändung von Bankkonten
- Schadensersatzforderungen durch Kunden, Wettbewerber und Verbraucher
- Aufwändige Beschäftigung des Managements mit Verteidigungsaktivitäten zu Lasten der Konzentration auf das Geschäft
- Bedrohung der beruflichen Existenz der Organmitglieder

3 Compliance als Aufgabe des Aufsichtsrats

Compliance geht auch den Aufsichtsrat als Überwachungsorgan an[34]. Ziff. 3.4 Abs. 2 Deutscher Corporate Governance Kodex konkretisiert die Berichtspflichten des Vorstands gegenüber dem Aufsichtsrat nach § 90 AktG und ergänzt sie ausdrücklich um Informationen zur Compliance im Unternehmen. Die Kodex-Regel geht davon aus, dass der Vorstand den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevante Fragen der Compliance zu informieren hat. Aus Ziff. 3.4 Abs. 2 wie auch aus Ziff. 5.3.2 Deutscher Corporate Governance Kodex wird damit deutlich, dass Compliance auch im Verantwortungsbereich des Aufsichtsrats liegt, der im Rahmen seiner allgemeinen Überwachungsaufgabe nach § 111 Abs. 1 AktG die Rechtmäßigkeit und Ordnungsmäßigkeit der Geschäftsleitung des Vorstands zu kontrollieren hat.[35] Dabei hat der Aufsichtsrat den Vorstand auch dahin zu überwachen, ob er seiner Compliance-Verantwortung nachgekommen ist und das Commitment, das der Vorstand innerhalb des Unternehmens wie auch gegenüber der Öffentlichkeit erklärt hat, auch tatsächlich gelebt wird[36]. Bestandteil der Überwachungsaufgabe des Aufsichtsrats ist auch die Verantwortung zu prüfen, ob der Vorstand bei seiner Entscheidung über Präventions- und Kontrollmaßnahmen wie auch bei der Auswahl und dem Aufbau von Sicherungseinrichtungen von seinem unternehmerischen Ermessen pflichtgemäß Gebrauch gemacht hat. Insoweit besteht auch eine enge Beziehung zur Verantwortung des Aufsichtsrats für die Kontrolle des Frühwarnsystems zur Erfassung bestandsgefährdender Risiken im Sinne von § 91 Abs. 2 AktG.[37]

Mit Einzelheiten der Compliance-Organisation oder des Programms oder einzelnen Verstößen muss sich der Aufsichtsrat hingegen nicht befassen. Dies ist jedoch anders zu

[34] Eingehend zur Compliance des Aufsichtsrats in eigenen Angelegenheiten *E. Vetter*, Liber Amicorum Martin Winter, 2011, S. 701 ff.; siehe auch *Bachmann*, in: Gesellschaftsrecht in der Diskussion 2007, 2008, S. 65, 93; *Bürkle*, BB 2007, 1797, 1800.

[35] Vgl. *Bachmann*, in: Gesellschaftsrecht in der Diskussion 2007, 2008, S. 65, 92; *Kort*, NZG 2008, 81, 84; *E. Vetter*, in: Marsch-Barner/Schäfer (Hrsg.), Handbuch börsennotierte AG, 2. Aufl. 2009, § 26 Rn. 10; *Wiesner*, in: Hoffmann-Becking (Hrsg.), Münchener Handbuch Gesellschaftsrecht AG, 3. Aufl. 2007, § 25 Rn. 5.

[36] *M. Winter*, FS Hüffer, 2010, S. 1103, 1121; siehe auch *E. Vetter*, FS Graf von Westphalen, 2010, S. 719, 732.

[37] *Ringleb*, in: Ringleb/Kremer/Lutter/v. Werder, Deutscher Corporate Governance Kodex, 4. Aufl. 2010, Rn. 629; *E. Vetter*, DB 2007, 1963, 1966.

beurteilen, wenn konkrete Verstöße eingetreten sind und es sich dabei um Vorfälle von gravierendem Ausmaß handelt oder bei den Verstößen der Verdacht auf ein Systemversagen vorliegt.[38]

Die Überwachung dieser wichtigen Vorstandsverantwortung durch den Aufsichtsrat soll nach der Empfehlung in Ziff. 5.3.2 Satz 1 Deutscher Corporate Governance Kodex vorrangig vom Prüfungsausschuss (Audit Committee) wahrgenommen werden. Dies entspricht verbreiteter Praxis. [39] Nachdem die Einrichtung des Prüfungsausschusses durch § 107 Abs. 3 Satz 2 AktG für kapitalmarktorientierte Unternehmen i. S. von § 264d HGB neuerdings gesetzlich erfasst worden – wenn auch nicht verbindlich vorgeschrieben ist[40] – kann davon ausgegangen werden, dass die Verbreitung und Bedeutung des Prüfungsausschusses weiter zunehmen wird.[41]

4 Die Bandbreite der Compliance-relevanten Rechtsgebiete

Die Risikoanalyse der Unternehmensleitung muss auf die konkrete Unternehmenssituation ausgerichtet werden. Dies gilt insbesondere für die von einem Unternehmen zu beachtenden Rechtsregeln, die naturgemäß von vielen Faktoren bestimmt werden, vor allem von seiner Rechtsform, Organisation, Größe und Komplexität wie auch dem speziellen Wirtschafszweig, in dem es tätig ist. Typischerweise handelt es sich bei den relevanten Compliance-Bereichen um ein ganzes Bündel von Rechtsgebieten, für deren Beachtung die Geschäftsleitung Verantwortung trägt.

5 Fünf Elemente der Compliance

Compliance versteht sich als aktive Risikovorbeugung im Unternehmen. Neben vielen einzelnen organisatorischen Maßnahmen, die ein effizientes Compliance-Management voraussetzt, verlangt sie eine Compliance-Kultur, die im Unternehmen breit verankert ist

[38] Ebenso *Drygala*, in: K. Schmidt/Lutter, AktG, 2. Aufl. 2010, § 111 Rn. 9; *Kremer/Klahold*, ZGR 2010, 113, 124; *Kremer*, in: Ringleb/Kremer/Lutter/v. Werder, Deutscher Corporate Governance Kodex, 4. Aufl. 2010, Rn. 992a; *Ringleb*, in: Ringleb/Kremer/Lutter/v. Werder, Deutscher Corporate Governance Kodex, 4. Aufl. 2010, Rn. 629; *Spindler*, in: Spindler/Stilz, AktG, 2. Aufl. 2010, § 107 Rz. 131; *E. Vetter*, FS Graf von Westphalen, 2010, S. 719, 732; siehe auch *Bachmann*, in: Gesellschaftsrecht in der Diskussion 2007, 2008, S. 65, 92; *M. Winter*, FS Hüffer, 2010, S. 1103, 1121.

[39] Siehe dazu *Kort*, FS Hopt, 2010, S. 983, 1000; *E. Vetter*, FS Graf von Westphalen, 2010, S. 719, 734; *M. Winter*, FS Hüffer, 2010, S. 1103, 1120.

[40] Siehe dazu z. B. *Hüffer*, AktG, 10. Aufl. 2012, § 107 Rz. 17a; *E. Vetter*, ZGR 2010, 751, 757.

[41] *M. Winter*, FS Hüffer, 2010, S. 1103, 1124 spricht bei der Delegation der Compliance-Überwachung auf den Prüfungsausschuss bereits von „best practice"; siehe auch *E. Vetter*, ZGR 2010, 751, 778.

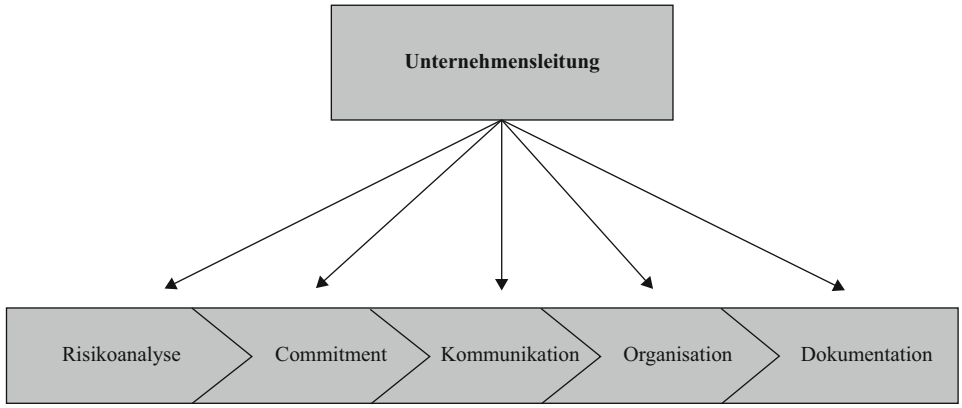


Abb. 1 Elemente der Compliance

und sowohl von der Geschäftsleitung als auch der Belegschaft tatsächlich gelebt wird. Für die Einrichtung einer Compliance-Organisation bedarf es bestimmter organisatorischer Maßnahmen im Rahmen einer strukturierten Vorgehensweise, die sich in fünf Schritten wie folgt gliedern lässt (Abb. 1):[42]

5.1 Risikoanalyse

Der erste Schritt zur Absicherung gegen Rechtsrisiken ist eine Bestandsaufnahme durch Identifikation der im jeweiligen Unternehmen vorhandenen typisierten Rechtsrisiken,[43] die Abschätzung des möglichen Schadensumfangs bei Eintritt des einzelnen Risikos nach sachlichem Gehalt und monetärer Größe sowie die Abschätzung der jeweiligen Eintrittswahrscheinlichkeit eines künftigen Rechtsverstoßes und des damit verbundenen Schadensumfangs sowie der daraus abzuleitenden Schritte zur Risikovorbeugung[44].

Als konkretes Beispiel der Risikoanalyse soll das Korruptionsproblem dienen.[45] Zur Erkennung von Korruptionsrisiken im Unternehmen kann z. B. der Katalog herangezogen werden, der bei steuerlichen Betriebsprüfungen der Oberfinanzdirektion Düsseldorf zur Anwendung kommt.[46] Er ist nicht nur geeignet, im Unternehmen daraus eigene Präventionsmaßnahmen im Bereich der Korruptionsbekämpfung zu entwickeln, sondern kann

[42] Ebenso *Hauschka*, in: Hauschka (Hrsg.), Corporate Compliance, 2. Aufl. 2010, § 1 Rn. 33, *Kindler*, FS G. H. Roth, 2011, S. 367, 370.

[43] Ebenso z. B. *Liese*, BB-Special zu Heft 5 2008, 17, 21; dies schließt die Erfassung von Verstößen in der Vergangenheit ein, z. B. *Itzen*, BB-Special zu Heft 5 2008, 12, 14; zum Risk Assessment im Zusammenhang mit dem Prüfungsstandard IDW PS 980 siehe z. B. *von Busekist/Schlitt*, CCZ 2012, 86, 88.

[44] Siehe dazu z. B. *Powilleit*, GWR 2010, 28, 29.

[45] Vgl. dazu z. B. *Hauschka/Greve*, BB 2007, 165.

[46] Leitfaden der Oberfinanzdirektion Düsseldorf. Die Behandlung von Vorteilszuwendungen im Sinne des § 4 Abs. 5 S. 1 Nr. 10 EStG, 2002.

auch als generelles Muster für einen unternehmensspezifischen Prüfkatalog in anderen Compliance-relevanten Bereichen dienen.
Der Katalog der Oberfinanzdirektion Düsseldorf führt die folgenden Gesichtspunkte auf:

- Verbuchung ohne Empfängerbenennung oder nicht existierender Empfänger;
- keine schriftliche Vereinbarung mit dem Empfänger;
- Bankkonto des Geldempfängers ist Nummernkonto;
- Konten an Off-Shore-Plätzen (z. B. Bahamas, Bermuda, Cayman lslands, Libanon, Liechtenstein, Schweiz);
- Zahlungen an Vermittler, Makler, Provisionen, Erfolgshonorare;
- Geldempfänger ist eine „Briefkastenfirma";
- Barzahlungsvorgänge;
- Speisung „schwarzer Kassen";
- fingierte Leistungsinhalte und Überfakturierungen.

5.2 Commitment

Die Erfahrungen der Unternehmenspraxis aber auch die in der Öffentlichkeit bekannt gewordenen Fälle von groben Misständen führen zu der Erkenntnis, dass die Compliance-Organisation steht und fällt mit dem glaubwürdigen Bekenntnis der Unternehmensspitze zur Compliance im Unternehmen. Compliance darf kein Formalakt und keine bloße Pflichtübung sein. Die Unternehmensleitung muss sich vielmehr uneingeschränkt der Sache verpflichtet fühlen und Compliance als Chefsache behandeln, sodass sie zum festen Bestandteil der Führungskultur des Unternehmens wird[47]. Dies setzt ein proaktives Herangehen an das Thema Compliance durch die Unternehmensleitung voraus verbunden mit klaren Botschaften an die Mitarbeiter, in denen unmissverständlich deutlich gemacht wird, dass Rechtsverstöße im Unternehmen seitens der Geschäftsleitung nicht geduldet werden und bei Verstößen entsprechende Sanktionen ergriffen werden.[48] Dies schließt zwingend das unmissverständliche Signal der Geschäftsleitung an die Belegschaft ein, dass ein Geschäftsabschluss unter Missachtung der im Unternehmen geltenden Compliance-Grundsätze keinesfalls dem Unternehmensinteresse dient, sondern Geschäfte, die unter Verstoß gegen Rechtsvorschriften zustande kommen, dem Unternehmen schaden. In der Unternehmenspraxis finden zunehmend Ethik-Regeln Verbreitung,[49] die u. a. Standards

[47] Gleichsinnig z. B. *Fleischer*, CCZ 2008, 1, 3; *Klindt/Pelz/Theusinger*, NJW 2010, 2385; *Kremer/Klahold*, ZGR 2010, 113, 123; *Lösler*, WM 2007, 676, 679; *Reichert/Ott*, ZIP 2009, 2173, 2176; *Uwe H. Schneider*, ZIP 2003, 645, 647.

[48] Vgl. zur sog. Zero Tolerance Policy *Uwe H. Schneider*, ZIP 2003, 645, 649 einerseits und *Hauschka*, ZIP 2004, 877, 882; *Reichert/Ott*, ZIP 2009, 2173, 2178 andererseits.

[49] Vgl. dazu z. B. BAG 22. 7. 2008 – 1 ABR 40/07, DB 2008, 2485; LAG Düsseldorf 14. 11. 2005 – 10TaBV 46/05, DB 2006, 162; *Kort*, NJW 2009, 129; *Mengel*, CCZ 2008, 85; *Rosbach*, CCZ 2008, 101.

zur Frage der Compliance im Allgemeinen und z. B. zur Mitarbeiterführung, oder zum Verhalten gegen Kartellabsprachen oder Korruption enthalten.

5.3 Kommunikation

Das Commitment der Geschäftsleitung und die Botschaft, dass sich das Unternehmen an die maßgeblichen Rechtsvorschriften wie auch an die internen Vorschriften und Regularien halten will und dazu entsprechende Maßnahmen zur Prävention und Kontrolle getroffen hat, muss in geeigneter Weise sowohl im Unternehmen aber auch an Geschäftspartner kommuniziert werden.[50] Hierdurch kann ein wesentlicher Beitrag zur Erhaltung der Unternehmensreputation bei Kunden, Mitarbeitern und Marktteilnehmern geleistet werden.[51] Hierfür bieten sich aus praktischer Sicht verschiedene Instrumente an:

- „Mission Statement" der Geschäftsleitung
- Code of Conduct und Ethik-Regeln des Unternehmens
- Internet-Homepage des Unternehmens
- Intranet-Seiten zu Compliance-Themen, E-Mails der Geschäftsleitung an die Mitarbeiter
- Informationsbroschüren, Richtlinien
- Schulungen und Veranstaltungen mit externen Trainern und Beratern
- Präsentationen des Korruptions-, Umwelt-, etc.-, Beauftragten
- Tagungen der Vertriebs- oder Niederlassungsleiter zu Compliance-Themen
- Informationstermine bei Umwelt-, Sicherheitsbeauftragten etc.
- Besprechung der internen Dokumentation für den „Schadensfall"
- „e-Schulungen" im Kartellrecht, Datenschutz, Arbeitsrecht (AGG), in der Korruptionsbekämpfung etc.[52]

Kommunikation setzt schließlich auch voraus, dass die im Unternehmen bestehenden Rechtsrisiken in den jeweiligen Hierarchieebenen kommuniziert werden, damit von den entsprechenden Stellen im Unternehmen auch die zur Risikobeherrschung notwendigen Maßnahmen ergriffen werden können.[53]

---

[50] Ebenso z. B. *Hauschka*, DB 2006, 1143, 1144; *Liese*, BB-Special zu Heft 5 2008, 17, 18.

[51] Teilweise wird deshalb bereits von der Marketing-Funktion der Compliance gesprochen, vgl. *Lösler*, NZG 2005, 104, 105; zustimmend *Grundmeier*, Rechtspflicht zur Compliance im Konzern, 2011, S. 13.

[52] Vgl. z. B. www.interactive-dialogues.com.

[53] *Pietzke*, CCZ 2010, 45, 47; siehe z. B. auch LG München I v. 5. 4. 2007 – 5 HK O 15964/06, AG 2007, 417 zum Risikofrüherkennungssystem.

5.4 Organisation

Compliance setzt eine klare Organisationsstruktur im Unternehmen voraus. Sie erfasst zuerst das Geschäftsleitungsorgan, für das kraft Gesetzes das Prinzip der Gesamtzuständigkeit und Gesamtverantwortung gilt (vgl. z. B. § 77 Abs. 1 AktG). Die moderne Unternehmenspraxis erzwingt hier bei einem mehrköpfigen Geschäftleitungsorgan regelmäßig Modifikationen, um den vielfältigen Anforderungen und der Komplexität der Leitungsaufgabe angemessen Rechnung zu tragen. Richtiger Ort für solche Regelungen ist die Geschäftsordnung, in der auch die Ressortzuständigkeiten der einzelnen Mitglieder der Geschäftsleitung sowie die dem Gesamtorgan vorbehaltenen Angelegenheiten und die dabei notwendigen Beschlussmehrheiten geregelt werden sollten. Fehlen entsprechende Regelungen zur Beschlussfassung, gilt kraft Gesetzes das Prinzip der Einstimmigkeit[54] und der Gesamtgeschäftsführung, was in der modernen Unternehmenspraxis kaum mit einer praktikablen und effizienten Wahrnehmung der Leitungsaufgabe vereinbar ist. In einem mehrköpfigen Geschäftleitungsorgan wird man derartige Regelungen deshalb zu den Voraussetzungen einer guten Corporate Governance zu zählen haben. Dies bestätigt auch Ziff. 4. 2.1 Satz 2 Deutscher Corporate Governance Kodex, die ausdrücklich den Erlass entsprechender Regelungen empfiehlt.[55]

Die Geschäftsverteilung in der Geschäftleitung durch Einrichtung spezieller Ressorts führt infolge der veränderten Verantwortung zwangsläufig zu einer gespaltenen Pflichtenstellung des einzelnen Geschäftleitungsmitglieds.[56] Im eigenen Ressort übernimmt das Mitglied eine leitende und verwaltende Tätigkeit. Hinsichtlich der Ressorts der anderen Mitglieder hat es keine Führungs- und Entscheidungsfunktion sondern nur eine beaufsichtigende Funktion. Von der Ressortbildung und Einzelgeschäftsführung unberührt bleiben die Aufgaben, die dem Geschäftleitungsorgan kraft Gesetzes zwingend als Gesamtaufgabe zugewiesen sind und die als originäre Führungsfunktionen zu qualifizieren sind.[57] Hierzu zählt auch die Verantwortung für die Einrichtung einer dem Risikoprofil des Unternehmens angemessenen Corporate Compliance-Organisation als Präventionsmaßnahme.[58]

---

[54] *Kort*, in: Großkommentar AktG, 4. Aufl. 2002, § 77 Rn. 6 und 10; *Wiesner*, in: Hoffmann-Becking (Hrsg.), Münchener Handbuch Gesellschaftsrecht AG, 3. Aufl. 2007, § 22 Rn. 6; *Zöllner/Noack*, in: Baumbach/Hueck, GmbHG, 20. Aufl. 2013, § 37 Rn. 29.

[55] Siehe dazu *E. Vetter*, DB 2007, 1963, 1964.

[56] *Fleischer*, NZG 2003, 449, 452; *Spindler*, in: Münchener Kommentar AktG, 3. Aufl. 2008, § 77 Rn. 59; *Zöllner/Noack*, in: Baumbach/Hueck, GmbHG, 20. Aufl. 2013, § 37 Rn. 32; *E. Vetter*, in: Krieger/Uwe H. Schneider (Hrsg.), Handbuch Managerhaftung, 2. Aufl. 2010, § 18 Rn. 19.

[57] *Hoffmann-Becking*, ZGR 1998, 497, 508; *Hüffer*, AktG, 10. Aufl. 2012 § 76 Rn. 8; *Zöllner/Noack*, in: Baumbach/Hueck, GmbHG, 20. Aufl. 2013, § 37 Rn. 32; siehe auch OLG Düsseldorf v. 15. 11. 1984 – 8 U 22/84, ZIP 1984, 1476, 1478.

[58] *Fleischer*, in: Spindler/Stilz, AktG, 2. Aufl. 2010, § 91 Rz. 58; *Hauschka*, NJW 20004, 257, 259; *Hüffer*, AktG, 10. Aufl. 2012 § 76 Rn. 9a; *Spindler*, in: Münchener Kommentar AktG, 3. Aufl. 2008, § 76 Rn. 17; *Rodewald/Unger*, BB 2006, 113; *Uwe H. Schneider*, ZIP 2003, 645, 647; *E. Vetter*, FS Graf von Westphalen, 2010, S. 719, 728.

Dies schließt z. B. die Einsetzung eines Compliance-Beauftragten im Unternehmen[59] oder die Einrichtung einer Compliance-Abteilung ein.

Neben der horizontalen Aufteilung von Aufgaben und Verantwortung innerhalb des Geschäftleitungsorgans durch die Begründung von Ressortzuständigkeiten besteht die Möglichkeit der vertikalen Delegation auf nachgeordnete Hierarchieebenen, soweit nicht originäre Führungsfunktionen verlagert werden sollen oder gesetzliche Schranken einer Delegation entgegenstehen. Im weiteren Sinne der Delegation ist darunter auch das Outsourcing auf externe Dritte zu verstehen.[60]

Aus formaler Sicht gilt sowohl für die Organisation innerhalb des Geschäftsleitungsorgans wie auch für die Delegation auf nachgeordnete Unternehmensebenen, dass die jeweiligen Zuständigkeiten unmissverständlich festgelegt und die Funktionen und Maßnahmen klar und eindeutig definiert sein müssen. Dabei ist sicherzustellen, dass die verschiedenen Verantwortungsbereiche überschneidungsfrei sind und Doppelzuständigkeiten vermieden werden. Es versteht sich von selbst, dass die Organisations- und Delegationsentscheidungen ebenso wie die Berichtswege und Kompetenzen schriftlich niedergelegt werden müssen, damit die Entscheidungen im Unternehmen kommuniziert und jederzeit nachvollziehbar und nachprüfbar sind.[61]

In inhaltlicher Hinsicht muss bei der Organisation und Delegation von Aufgaben und Verantwortlichkeiten beachtet werden, dass die Personalauswahl sorgfältig erfolgt, eine gründliche Einweisung der Person in die neue Aufgabe stattfindet und auch eine regelmäßige Überwachung der ordnungsgemäßen Wahrnehmung der übernommenen Aufgabe erfolgt.[62]

Die Organisation erstreckt sich auch auf systematische und verfahrensmäßige Vorkehrungen im Unternehmen zur Einrichtung einer Informations- und Kommunikationsorganisation, die gewährleisten sollen, dass die unternehmerischen Entscheidungen der Geschäftsleitung den Kriterien der Verfahrenskontrolle im Sinne von § 93 Abs. 1 Satz 2 AktG genügen und bei der Anwendung des unternehmerischen Ermessens[63] die Informationen der Geschäftsleitung als Entscheidungsgrundlage auch zur Verfügung stehen.[64]

---

[59] Vgl. z. B. *Bürkle*, in: Hauschka (Hrsg.), Corporate Compliance, 2. Aufl. 2010, § 8 Rn. 7 ff.

[60] Vgl. dazu z. B. *Fleischer*, ZIP 2003, 1, 10; *E. Vetter*, in: Krieger/Uwe H. Schneider (Hrsg.), Handbuch Managerhaftung, 2. Aufl. 2010, § 18 Rn. 73; speziell zur Versicherungswirtschaft *Dreher*, WM 2008, 1765, 1770.

[61] Siehe dazu z. B. LG München I v. 5. 4. 2007 – 5 HK O 15964/06, AG 2007, 417 zum Risikofrüherkennungssystem.

[62] Vgl. z. B. *Liese*, BB-Special zu Heft 5 2008, 17, 22; *Schmidt-Husson*, in: Hauschka (Hrsg.), Corporate Compliance, 2. Aufl. 2010, § 7 Rn. 21 ff.; *E. Vetter*, in: Krieger/Uwe H. Schneider (Hrsg.), Handbuch Managerhaftung, 2. Aufl. 2010, § 18 Rn. 63 und 68.

[63] Vgl. dazu auch die Regeln des Arbeitskreises "Externe und interne Überwachung der Unternehmung" der Schmalenbach Gesellschaft für Betriebswirtschaft e. V., ZIP 2006, 1068.

[64] Vgl. dazu z. B. *Buck-Heeb*, in: Hauschka (Hrsg.), Corporate Compliance, 2. Aufl. 2010, § 2 Rn. 15 ff.; siehe auch *Kinzl*, DB 2004, 1653, 1654.

5.5 Dokumentation

Es versteht sich fast von selbst, dass ein Unternehmen nur dann als ordentlich geführt bezeichnet werden kann und über eine effiziente Compliance verfügt, wenn diese Tatsache auch belegt werden kann. Damit ist der letzte Baustein der Compliance angesprochen, nämlich die Dokumentation der Entscheidungen, Prozesse, Maßnahmen und Berichtswege im Unternehmen.[65] Ihre Bedeutung wird auch mit Blick auf die Beweislastregelung von § 93 Abs. 2 Satz 2 AktG offensichtlich, nach der die betroffenen Mitglieder des Vorstands oder der Geschäftsführung im Zweifelsfall die Einhaltung der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters zu beweisen haben.[66] Die Notwendigkeit der Dokumentation besteht ungeachtet des Umstandes, dass unter Umständen im Ernstfall dank der Dokumentation auch Fehler festgestellt werden können, die den verantwortlichen Organmitgliedern oder anderen Betroffenen zur Last gelegt werden können. Dieses systemimmanente Risiko des „Beweises gegen sich selbst" ist hinzunehmen.[67]

Die Geschäftsordnung des Vorstands bzw. der Geschäftsführung bedarf nach einhelliger Ansicht von Rechtsprechung und Schrifttum der Schriftform.[68] Dabei ist darauf zu achten, dass die Geschäftsordnung von dem durch Gesetz oder Satzung bestimmten Gremium erlassen wird. Auch die Ressortverteilung ist schriftlich niederzulegen.[69] Wie die Unternehmenspraxis zeigt, ist dies nicht immer der Fall. Vielfach ist festzustellen, dass entweder eine Aufgabenverteilung in schriftlicher Form nicht vorhanden ist oder aber die im Unternehmen geltende Ressortverteilung längst nicht mehr den tatsächlichen Gegebenheiten entspricht und die für die Festlegung der Ressorts zuständigen Organe und Gremien hierüber nicht informiert sind.

Die Beratungen und Entscheidungen des Geschäftsleitungsorgans finden im Regelfall in entsprechenden Sitzungen statt und müssen in ausreichender Form protokolliert werden. Gleiches gilt für Entscheidungen, die auf telefonischem Wege gefasst worden sind. Schulungen von Mitarbeitern müssen ebenso schriftlich festgehalten werden wie Kontrollroutinen, Prüfungen und Tests.

---

[65] *Kiethe*, GmbHR 2007, 393, 399.

[66] Die Regelung gilt analog auch im GmbH-Recht, vgl. BGH v. 4. 11. 2002 – II ZR 224/00, BGHZ 152, 280, 283.

[67] *Goette*, ZHR 175 (2011), 388, 397; siehe auch *Hauschka*, in: Hauschka (Hrsg.), Corporate Compliance, 2. Aufl. 2010, § 1 Rn. 29.

[68] OLG Koblenz v. 9. 6. 1998 – 3 U 1662/89, NZG 1998, 953, 954; *Dreher*, ZGR 1992, 22, 59; *Hüffer*, AktG, 10. Aufl. 2012, § 77 Rn. 21; *Seibt*, in: K. Schmidt/Lutter, AktG, 2. Aufl. 2010, § 77 Rn. 28; *E. Vetter*, in: Krieger/Uwe H. Schneider (Hrsg.), Handbuch Managerhaftung, 2. Aufl. 2010, § 18 Rn. 31 und 32.

[69] BFH v. 4. 3. 1986 – VII S 33/85, BFHE Tz. 11 = DB 1986, 1555; BFH v. 26. 4. 1984 – V R 128/79, BFHE 141, 443 Tz. 19 = DB 1984, 2543; *Kort*, in: Großkommentar AktG, 4. Aufl, 2002, § 77 Rn. 78; *Seibt*, in: K. Schmidt/Lutter, AktG, 2. Aufl. 2010, § 77 Rn. 28; weniger streng *Kleindiek*, in: Lutter/Hommelhoff, GmbHG, 18. Aufl. 2012, § 37 Rn. 37.

Nur wenn die im Unternehmen durchgeführten Compliance-Maßnahmen ausreichend dokumentiert sind und entsprechende Nachweise z. B. im Fall eines Regelverstoßes oder eines Unfalls einer im Übrigen ernsthaft betriebenen und sonst funktionierenden Compliance vorgelegt werden können, besteht die berechtigte Hoffnung, dass Schadensersatzansprüche Dritter gegen das Unternehmen oder die Mitglieder der Geschäftsleitung sowie sonstige Sanktionen gegen Unternehmen, die Mitglieder der Geschäftsleitung oder andere handelnde Personen erfolgreich abgewendet oder abgemildert werden können.[70]

[70] Vgl. z. B. *Buchta*, DB 2006, 1939, 1943; *Hauschka*, DB 2006, 1143, 1145; *Kiethe*, GmbHR 2007, 393,399; *Kremer/Klahold*, ZGR 2010, 113, 139; *Rodewald/Unger*, BB 2006, 113, 115; siehe auch die Hinweise von *Hopson/Koehler*, CCZ 2008, 208, 212 zur US-amerikanischen Praxis im Sinne der United States Federal Sentencing Guidelines.

Pflichten der Geschäftsleitung & Aufbau einer Compliance-Organisation

Gregor Wecker und Stefan Galla

Inhaltsverzeichnis

G. Wecker (✉)
Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: gregor.wecker@luther-lawfirm.com

S. Galla
E-Mail: stefan.galla@luther-lawfirm.com

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2_2,

Zusammenfassung

Aufgrund der unterschiedlichen Anforderungen, die an Unternehmen vom Gesetzgeber gestellt werden, kann es keinen allgemeingültigen Compliance-Begriff geben. Vielmehr variieren die Anforderungen individuell bei jedem Unternehmen. Entsprechend kann man in der täglichen Beratungspraxis feststellen, wie unterschiedlich das Thema Compliance angegangen wird. Während Banken und Versicherungen aufgrund der hohen Regulierungsdichte in diesem Geschäftsbereich längst eine diversifizierte Compliance-Struktur – meist mit Compliance-Officer – eingeführt haben und das Thema unternehmensintern einen hohen Stellenwert hat, kennt man den Begriff Compliance in kleinen und mittelständischen Unternehmen teilweise nur vom Hörensagen. Das soll natürlich nicht bedeuten, dass sich solche Unternehmen nicht bemühen die für sie geltenden Vorschriften einzuhalten.

In vielen Unternehmen wird mittlerweile versucht das Thema „Aufbau einer Compliance-Organisation" strukturiert anzugehen. Für die Umsetzung bieten sich unter anderem IT-Programme an. Über solche Programme können u. a. Schulungen (eLearning), z. B. hinsichtlich des Inhalts von Handbüchern, gezielt für spezielle Mitarbeitergruppen durchgeführt werden. Heutige IT-Programme bieten darüber hinaus vielschichtige Möglichkeiten die Compliance-Struktur in einem Unternehmen zu verbessern. Über Beteiligungsmanagement- und Vertragsverwaltungssysteme können Datenbanken aufgebaut werden, die über das Internet weltweit von Führungskräften des Unternehmens genutzt werden können. Die bei richtiger Anwendung hierdurch entstehende Datengenauigkeit ist sicherlich ein wichtiger Baustein in einer Compliance-Struktur eines weltweit vernetzten Konzerns. Jedoch nicht nur große – weltweit operierende – Unternehmen profitieren von einer guten Compliance-Struktur. Auch auf kleine und mittelständische Unternehmen sind die meisten der nachfolgend dargestellten Bausteine einer Compliance-Struktur übertragbar.

Aber auch die beste IT-Infrastruktur, Schulungen und Handbücher sowie die Schaffung einer Personalstruktur mit genau definierten Überwachungspflichten nutzen nur dann wirklich, wenn die Mitarbeiter für das Thema Compliance gewonnen werden können und dieses Thema nicht als Behinderung ihrer täglichen Arbeit betrachten.

Nachfolgend sollen zunächst einige Begrifflichkeiten geklärt werden, bevor die These überprüft wird, ob eine Pflicht der Geschäftsleitung zur Errichtung einer Compliance-Organisation besteht und auf verschiedene Möglichkeiten zur Errichtung einer Compliance-Struktur eingegangen wird. Hierbei wird auch thematisiert, inwieweit sich aus dem Gesetz bzw. aus der Rechtsprechung die Pflicht zur Einrichtung einer internen Revision als Teil einer Compliance-Organisation bzw. die Pflicht zur effizienten Informationsorganisation ergibt.

1 Corporate Compliance – Begriffsdefinition und -abgrenzung

Der Begriff Compliance ist ein Oberbegriff und bedeutet:

Einhaltung sämtlicher für das jeweilige Unternehmen relevanten gesetzlichen Pflichten, Vorschriften, Regeln, fachliche Kompetenz und persönliche Verantwortung im Umgang mit externen Regeln, internen Regeln und Vorgaben der Gesellschafter und Vertragspartner sowie Einhaltung von Vorgaben der Zentrale durch Konzerneinheiten.

Seit der Überarbeitung des Deutschen Corporate Governance Kodex (DCGK) vom 14. Juni 2007 wird der Begriff Compliance in Ziffer 4.1.3 DCGK zudem wie folgt legal definiert:

> Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance).

Der Begriff ist zur Klarstellung zunächst abzugrenzen von weiteren Begriffen, die häufig mit dem Begriff Corporate Compliance verwechselt werden.

Der Begriff **Corporate Governance** umfasst beispielsweise als weiterer Begriff alle gesetzlichen Regeln und anerkannten Standards sorgfältiger Unternehmensführung.

Der Begriff **Code of Conduct** beinhaltet als Baustein eines Compliance-Systems, Handlungs- und Verhaltensanweisungen an die Mitarbeiter.

Bei **Risk Management Systemen** i. S. d. § 91 Abs. 2 AktG handelt es sich um Früherkennungs- und Überwachungssysteme für bestandsgefährdende Entwicklungen der Gesellschaft und somit ebenfalls um einen Baustein eines Compliance-Systems.

Des Weiteren gibt es über die gesetzlichen Pflichten hinaus noch soziale und ethische Pflichten der Geschäftsführung, die unter dem Begriff **Corporate Social Responsibility/Business Ethics** zusammengefasst werden. Während das Gesetz das ethische Minimum darstellt, geht die von der Gesellschaft geprägte Moral häufig darüber hinaus. Maßnahmen im Bereich Corporate Social Responsibility/Business Ethics werden gerne als Werbemaßnahmen von Unternehmen eingesetzt.

1.1 Corporate Governance

Die von der Bundesministerin für Justiz im September 2001 eingesetzte „Regierungskommission Deutscher Corporate Governance Kodex" verabschiedete am 26. Februar 2002 den Deutschen Corporate Governance Kodex, der die gesetzlichen Regeln und anerkannten Standards sorgfältiger Unternehmensführung zusammenfassen soll. Der Kodex besitzt über die Entsprechenserklärung gemäß § 161 AktG (eingefügt durch das Transparenz- und Publizitätsgesetz, in Kraft getreten am 26. Juli 2002) eine gesetzliche Flankierung. Vorstand und Aufsichtsrat von börsennotierten Gesellschaften erklären danach jährlich, dass den vom Bundesministerium der Justiz im amtlichen Teil des Bundesanzeigers bekannt gemachten Empfehlungen der „Regierungskommission Deutscher

Corporate Governance Kodex“ entsprochen wurde und wird oder welche Empfehlungen nicht angewendet wurden oder werden.

Mit dem Deutschen Corporate Governance Kodex sollen die in Deutschland geltenden Regeln für Unternehmensleitung und -überwachung für nationale wie internationale Investoren transparent gemacht werden, um so das Vertrauen in die Unternehmensführung deutscher Gesellschaften zu stärken. Der Kodex adressiert alle wesentlichen – vor allem internationalen – Kritikpunkte an der deutschen Unternehmensverfassung, nämlich

mangelhafte Ausrichtung auf Aktionärsinteressen;
die duale Unternehmensverfassung mit Vorstand und Aufsichtsrat;
mangelnde Transparenz deutscher Unternehmensführung;
mangelnde Unabhängigkeit deutscher Aufsichtsräte;
eingeschränkte Unabhängigkeit der Abschlussprüfer.

Seitdem der Deutsche Corporate Governance Kodex erstmalig in Kraft getreten ist, wurde zudem eine Reihe von Änderungen beschlossen, letztmalig mit Datum vom 15. Mai 2012.

Von Gesellschaften mit beschränkter Haftung wird in Zukunft zunehmend – sei es von Kapitalgebern oder den Gerichten – verlangt werden, dass sie sich ebenfalls an die Empfehlungen des Deutschen Corporate Governance Kodex halten. Es ist davon auszugehen, dass Gerichte hinsichtlich der Beurteilung sorgfältiger Unternehmensführung – wenigstens mittelbar – zunehmend Wertungen des Deutschen Corporate Governance Kodex heranziehen werden.

1.2 Code of Conduct/Code of Ethics

Je nach Unternehmensgröße kann ein sogenannter Code of Conduct bzw. ein Code of Ethics integraler Bestandteil eines Compliance-Systems sein. Darunter versteht man auf der einen Seite Handlungs- und Verhaltensanweisungen an die Mitarbeiter, um so den Umgang der Mitarbeiter untereinander und gegenüber Dritten zu regeln. Zwar gibt es für die Einführung derartiger Richtlinien keine rechtliche Verpflichtung, die Entwicklungen im Ausland, insbesondere in den USA, die entsprechende Richtlinien schon lange kennen und teilweise rechtlich einfordern, haben aber auch hier das Bewusstsein für die Notwendigkeit eines Verhaltenskodex geschärft. Hinzu tritt die Erkenntnis der Unternehmen, dass im „Kampf“ um die Anwerbung hochqualifizierten Personals, die Bewerber gerade auch den Umgang des Unternehmens mit seinen Mitarbeitern zu einem maßgeblichen Entscheidungskriterium bei der Wahl Ihrer künftigen Arbeitsstätte erhoben haben.

Aus rechtlicher Sicht wird man sich davor hüten müssen, Ethikrichtlinien aus dem angloamerikanischen Rechtsraum eins-zu-eins auf inländische Unternehmen zu übertragen. Dem steht das deutsche Arbeitsrecht in zweifacher Hinsicht – nämlich auf individualvertraglicher Ebene und auf kollektivrechtlicher Ebene – entgegen. Eine Vielzahl von Regelungen eines Code of Ethics werden den Bestimmungen des § 87 Abs. 1 Nr. 1 Be-

trVG unterfallen, wonach der Betriebsrat in Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb mitzubestimmen hat.[1] Auf individualvertraglicher Ebene stellt sich daneben die Frage, ob die einzuführenden Regelungen noch vom Direktionsrecht des Arbeitgebers gedeckt sind, oder aber es einer einvernehmlichen Vereinbarung bedarf.[2] Vorgelagert dürfte sich immer die Frage stellen, ob die Regelung im Hinblick auf einen Eingriff in die Privatautonomie überhaupt zulässig ist, wie dies bspw. bei dem Verbot privater Liebesbeziehungen von Arbeitskollegen („Wal Mart") der Fall ist, welches das OLG Düsseldorf als verfassungswidrig eingestuft hat.[3]

1.3 Corporate Social Responsibility/Business Ethics

Corporate Social Responsibility (CSR) – also soziale Verantwortung des Unternehmens – richtet über die Vorgaben, die das Gesetz als ethisches Minimum an die Unternehmen vorsieht, das Augenmerk auf den Standort und die Verantwortung des Unternehmens im gesellschaftlichen Umfeld. Die Unternehmen werden sich zunehmend auch bewusst, dass sie gesellschaftliche Verantwortung zu übernehmen haben, wobei insbesondere ökologische und soziale Aspekte in den Mittelpunkt gerückt werden.

In den letzten Jahren haben die Unternehmen daher auf diesem Gebiet ihre Aktivitäten enorm verstärkt, indem Sie Mitarbeiter entsprechend geschult oder ganze CSR Abteilungen eingerichtet haben. Auf der anderen Seite wurde das Thema auch von Non-Profit Organisationen aufgegriffen und vorangetrieben, Medienhäuser haben Rankings initiiert.[4]

Dabei ist die Erkenntnis gereift, dass entsprechendes Engagement nicht nur Selbstzweck ist, sondern durchaus einen positiven Effekt auf die Geschäftsentwicklung haben kann. Teilweise wird dieses Engagement als direktes Marketing Tool eingesetzt. Man denke nur an die BP Fernsehwerbung zum Thema Umweltschutz, oder aber die Verknüpfung des Kaufs von Krombacher Bier mit der Rettung des Regenwaldes, die der BGH in seinen Entscheidungen vom 26. Oktober 2006 als grundsätzlich zulässig eingestuft hat.[5]

1.4 Risk Management Systeme

Anknüpfungspunkt für die Pflicht zur Einrichtung eines Früherkennungs- und Überwachungssystems für bestandsgefährdende Entwicklungen der Gesellschaft ist § 91 Abs. 2 AktG.

---

[1] Vgl. nur LAG Düsseldorf v. 14.11.2005 – 10 TaBV 46/05, NZA-RR 2006, 81 ff.

[2] Vgl. zu diesen Problemen ausführlich Kap. 11. und *Schreiner*, Compliance Report, Februar 2007, 5 f.

[3] LAG Düsseldorf v. 14.11.2005 – 10 TaBV 46/05, NZA-RR 2006, 81 ff.

[4] Vgl. zu dieser Entwicklung: *Unger*, Compliance Report, Februar 2007, 2, 4.

[5] BGH v. 26.10.2006 – I ZR 33/04 (Regenwaldprojekt I), NJW 2007, 919 ff.; BGH v. 26.10.2006 – I ZR 97/04 (Regenwaldprojekt II), MDR 2007, 598.

Die auf das KonTraG von 1998 zurückgehende Norm[6] formuliert eine Bestandssicherungspflicht des Vorstandes und konkretisiert insoweit einen Teilaspekt der allgemeinen Leitungsaufgabe des Vorstands.[7] Ohne dass die Vorschrift die Verpflichtung zur Einführung eines allgemeinen „risk management" begründet, wie es Teile der Betriebswirtschaftslehre und der Prüfungspraxis verstehen,[8] hat der Vorstand gleichwohl Maßnahmen zu treffen, die es ihm ermöglichen, die umschriebenen Entwicklungen[9] frühzeitig zu erkennen (vgl. dazu sogleich unter 2.8).

2 Aufbau einer Compliance-Organisation als Pflicht der Geschäftsleitung?

Während teilweise Möglichkeiten zur Errichtung und Verbesserung der Compliance-Organisation freiwillig sind, gibt es für viele Bereiche weitreichende Pflichten der Geschäftsleitung aus denen man auf eine rechtliche Pflicht zum Aufbau einer Compliance-Organisation schließen kann.

2.1 Pflichten der Geschäftsleitung

Eine rechtliche Pflicht zum Aufbau einer Compliance-Organisation könnte sich bereits aus dem Umstand ergeben, dass die vertretungsbefugten Organe von AG und GmbH gegenüber der Gesellschaft eine Vielzahl von Pflichten zu beachten haben. Die Verletzung dieser Pflichten kann sowohl zur persönlichen Haftung der Geschäftsleitung gegenüber der Gesellschaft sowie gegenüber Dritten als auch zu einer Reihe weiterer Rechtsfolgen führen. Diese weiteren Rechtsfolgen können insbesondere strafrechtlicher Natur sein, Sanktionen des Ordnungswidrigkeitenrechts beinhalten, aber auch zu aufsichtsrechtlichen, steuerrechtlichen und gesellschaftsrechtlichen Konsequenzen führen. Des Weiteren steigt die Zahl der Tatbestände, die mit Bußgeld bedroht sind, weiter an. Bei den Geschäftsleitern eines Kreditinstituts oder eines Versicherungsunternehmens besteht zudem die Möglichkeit der Abberufung durch die Bundesanstalt für Finanzdienstleistungsaufsicht (vgl. § 36 KWG).

Geschäftsleiter müssen bei der Verletzung von Pflichten grundsätzlich auch mit der fristlosen Kündigung des Anstellungsvertrages und den sich daran anschließenden finanziellen Einbußen rechnen.

---

[6] Art. 1 Nr. 9 KonTraG v. 27. April 1998 (BGBl. I, 786).

[7] Vgl. RegBegr. BT-Drucks. 13/9712S. 15 liSp.

[8] Vgl. *Hüffer*, AktG, 10. Aufl. 2012, § 91 Rn. 1, 8.

[9] Beispielhaft nennt die Regierungsbegründung die Aufnahme risikobehafteter Geschäfte, Verstöße gegen Vorschriften der Rechnungslegung oder gegen sonstige gesetzliche Vorschriften, vgl. RegBegr. BT-Drucks. 13/9712S. 15 liSp.

Im Folgenden sollen nunmehr exemplarisch einige wichtige Pflichtenbereiche der Geschäftsleitungsorgane aufgezeigt werden.

2.2 Allgemeine Sorgfalts- und Treuepflicht

Zunächst hat die Geschäftsleitung – ebenso wie die Gesellschafter – gegenüber der Gesellschaft und den Gesellschaftern allgemeine Sorgfalts- und Treuepflichten einzuhalten.[10] Die einzelnen Sorgfalts- und Treuepflichten sind überwiegend nicht kodifiziert, sondern leiten sich aus der Organstellung der Geschäftsleitung innerhalb der Gesellschaft ab. Dabei hat die Geschäftsleitung die Sorgfalt eines ordentlichen Geschäftsmannes an den Tag zu legen, vgl. §§ 93 Abs. 1 S. 1 AktG, 43 Abs. 1 GmbHG. Dazu zählt unter anderem die Pflicht zur ordnungsgemäßen Unternehmensleitung unter Einhaltung der durch Gesetz, Satzung und Anstellungsvertrag festgelegten Grenzen.

In diesem Zusammenhang ist die Geschäftsleitung insbesondere an die durch Satzung und Anstellungsvertrag vorgegebene Kompetenzordnung der Gesellschaft gebunden. Die Geschäftsleitung hat sämtliche Geschäfte der Gesellschaft im Interesse und zum Wohle der Gesellschaft wahrzunehmen und alles zu unterlassen, was die Gesellschaft schädigen könnte. Die Geschäftsleitung hat stets den wirtschaftlichen Vorteil der Gesellschaft zu verfolgen und ist grundsätzlich nicht berechtigt in Wettbewerb zur Gesellschaft zu treten und der Gesellschaft Geschäftschancen zum eigenen Wohle zu entziehen.[11] Bei Verletzung dieser Pflicht steht der Gesellschaft nicht bloß ein Unterlassungsanspruch gegenüber der Geschäftsleitung, sondern auch ein Schadensersatzanspruch zu.

Aufgrund der Beachtung des Wohles der Gesellschaft als höchstem Gut, ist es dem Geschäftsführer einer GmbH auch strafbewehrt untersagt, Betriebs- oder Geschäftsgeheimnisse der Gesellschaft unbefugt weiterzugeben, vgl. § 85 GmbHG. Die Geheimhaltungspflicht gilt dabei auch für den Vorstand einer AG, vgl. § 93 Abs. 1 S. 3 AktG.[12]

Ausfluss der Business Judgement Rule ist die Pflicht zur angemessenen Vorbereitung einer Geschäftsführerentscheidung durch Einholung der entscheidungsrelevanten Informationen und der sich daran anschließenden Abwägung von Risiken bei Ausübung der Entscheidung.[13] Diese Pflicht kommt selbstverständlich nur bei unternehmerischen – also nicht gebundenen – Entscheidungen der Geschäftsleitung in Betracht. Solche unternehmerischen Entscheidungen beinhalten notwendigerweise eine von der Geschäftsleitung vorzunehmende Prognose. Sollte z. B. die Geschäftsleitung die Entscheidung treffen, ein anderes Unternehmen zu erwerben ohne zuvor ausreichende Informationen über das zu erwerbende Unternehmen eingeholt zu haben und bei Unklarheiten

[10] Vgl. *Baumbach/Hueck*, GmbHG, 19. Aufl. 2010, § 35 Rn. 38; *Hüffer*, AktG, 10. Aufl. 2012, § 93 Rn. 5.

[11] *Baumbach/Hueck*, GmbHG, 19. Aufl. 2010, § 35 Rn. 42.

[12] Vgl. hierzu auch *Hüffer*, AktG, 10. Aufl. 2012, § 93 Rn. 6 ff.

[13] Vgl. *Heidel*, Aktienrecht und Kapitalmarktrecht, 3. Aufl. 2011, § 93 Rn. 98.

eine „Due Diligence" durchgeführt zu haben, so kann dies eine Schadensersatzpflicht begründende Pflichtverletzung der Geschäftsleitung darstellen.[14] Ebenso ist die Geschäftsleitung beispielsweise verpflichtet vor der Kreditvergabe an einen Dritten zunächst eine Kreditwürdigkeitsprüfung vorzunehmen.[15]

2.3 Überwachungspflichten/Risikokontrollpflichten

Da die Geschäftsleitung nicht alle Maßnahmen im Unternehmen selbst vorzunehmen braucht, was rein faktisch bei Überschreitung einer bestimmten Unternehmensgröße auch gar nicht mehr möglich wäre, ist die Geschäftsleitung befugt, einzelne Aufgabengebiete an Dritte (nachgeordnete Mitarbeiter) zu delegieren. Dabei hat die Geschäftsleitung jedoch verschiedene Überwachungs- und Risikokontrollpflichten selbst wahrzunehmen.

Bei der Delegation von Aufgaben hat die Geschäftsleitung insbesondere für die ordnungsgemäße Auswahl der Mitarbeiter, eine den übertragenen Aufgaben entsprechende Einweisung und eine ordnungsgemäße Überwachung der entsprechenden Mitarbeiter einzustehen.[16] Die Auswahl eines Mitarbeiters zur Delegation einer Aufgabe hat erst nach vorhergehender Prüfung der persönlichen Eignung (Zuverlässigkeit, Belastbarkeit) und der fachlichen Befähigung (Ausbildung, Qualifikation, Erfahrung) des Mitarbeiters durch die Geschäftsleitung zu erfolgen. Nach Auswahl hat die Geschäftsleitung den Delegierten in seinen Verantwortungsbereich einzuweisen und ihm die zur Bewältigung der übertragenen Aufgaben notwendigen Kenntnisse und sachlichen Mittel zur Verfügung zu stellen. Nachdem der Mitarbeiter die ihm übertragene Tätigkeit unter Beachtung der vorgenannten Grundsätze aufgenommen hat, ist die Geschäftsleitung noch immer nicht aus ihrer Pflicht entlassen. Denn die Geschäftsleitung darf nicht blind auf die pflichtgemäße Erfüllung der übertragenen Aufgaben durch den Mitarbeiter vertrauen, sondern im Rahmen des objektiv Zumutbaren hat die Geschäftsleitung die Tätigkeit des Mitarbeiters ständig zu überwachen.[17]

Dies gilt grundsätzlich auch bei einer Aufteilung von verschiedenen Ressorts innerhalb der Geschäftsleitung. Der jeweilige Geschäftsführer oder das Vorstandsmitglied bleibt für die Überwachung ressortfremder Geschäftsführer und Vorstandsmitglieder verantwortlich, obwohl bei ordnungsgemäßer Geschäftsverteilung nur das zuständige Geschäftsleitungsorgan die volle Handlungsverantwortung trägt.[18] Sollten Zweifel an der Zuverlässigkeit des Mitgeschäftsführers entstehen, so sind die übrigen Geschäftsführer gegebenenfalls verpflichtet, den übertragenen Aufgabenbereich in das Gesamtgremium

[14] Vgl. OLG Oldenburg v. 22.6.2006 – 1 U 34/03, GmbHR 2006, 1263 ff.

[15] Vgl. zur strafrechtlichen Verantwortlichkeit BGH v. 15.11.2001 – 1 StR 185/01, NJW 2002, 1211 ff.

[16] Sehr weitgehend BGH v. 21.1.1997 – VI ZR 338/95, NJW 1997, 1237 ff.

[17] *Schmidt-Husson,* in: Hauschka (Hrsg.), Corporate Compliance, 2007, § 7 Rn. 24.

[18] Vgl. *Hüffer*, AktG, 10. Aufl. 2012, § 93 Rn. 13a; *Lutter/Hommelhoff*, GmbHG, 18. Aufl. 2012, § 43 Rn. 17.

zurückzuholen. Des Weiteren sind die übrigen Geschäftsführer verpflichtet, etwaigen pflichtwidrigen Entscheidungen des Mitgeschäftsführers zu widersprechen.

Zu den Überwachungs- und Risikokontrollpflichten der Geschäftsleitung zählt auch das nach § 91 Abs. 2 AktG durch den Vorstand einer AG zu installierende Frühwarnsystem, welches später noch näher behandelt und erläutert wird.

2.4 Buchführungs-/Bilanzierungspflichten

Nach § 238 HGB ist jeder Kaufmann verpflichtet, Bücher zu führen und in diesen sein Handelsgeschäft und die Lage seines Vermögens nach den Grundsätzen ordnungsgemäßer Buchführung darzustellen. Als Formkaufmann sind die Kapitalgesellschaften Normadressat der Bestimmung des § 238 HGB. Aus § 264 HGB folgt die Verpflichtung der gesetzlichen Vertreter einer Kapitalgesellschaft, also Vorstand und Geschäftsführung, zur Rechnungslegung. Die Rechnungslegung umfasst nach den §§ 238 ff. HGB die Vornahme der Inventur, die Aufstellung der (Eröffnungs-) Bilanz, die Aufstellung der Gewinn- und Verlustrechnung sowie die Anfertigung des Anhangs und des Lageberichts. Zwar ist auch die Rechnungslegungspflicht rein faktisch auf Dritte (z. B. externe Berater) übertragbar, allerdings haftet der Vorstand bzw. die Geschäftsführung gem. §§ 91 Abs. 1 AktG, 41 GmbHG für die ordnungsgemäße Erfüllung dieser Verpflichtung.[19]

Nach § 325 HGB haben die gesetzlichen Vertreter einer Kapitalgesellschaft auch den Jahresabschluss (größenabhängige Erleichterungen ergeben sich aus den §§ 326 ff. HGB i. V. m. § 267 HGB) beim Betreiber des elektronischen Handelsregisters einzureichen. Die haftungsrechtliche Verantwortlichkeit für die ordnungsgemäße Buchführung kann dabei weder durch die Satzung noch durch einen entsprechenden Beschluss der Haupt- oder Gesellschafterversammlung auf Dritte übertragen werden, so dass sich die Geschäftsführung letztendlich nicht der umfangreichen Verantwortung entziehen kann und aus diesem Grund zumindest die bereits oben beschriebenen Überwachungsaufgaben wahrzunehmen hat.

Bei Verletzung der Rechnungslegungspflichten drohen sowohl steuerrechtliche Konsequenzen (vgl. beispielhaft §§ 162, 370 Abs. 1 AO) als auch ordnungs- und strafrechtliche Sanktionen (vgl. §§ 331, 335 HGB, 283 Abs. 1 Nr. 5–7, 283a, 283b StGB).

In einem jüngeren Urteil hat der BGH klargestellt, dass es Pflicht des Geschäftsführers einer GmbH ist, darzulegen und gegebenenfalls zu beweisen, dass ihm jederzeit eine Übersicht über die wirtschaftliche und finanzielle Situation möglich ist, sei es durch Anschauung, sei es durch eine entsprechende Organisation des Geschäftsbetriebs.[20]

---

[19] Vgl. für die AG: *Hüffer*, AktG, 10. Aufl. 2012, § 91 Rn. 2.

[20] BGH II ZR 243/11, in: NJW-Spezial 2012, S. 529 ff.

2.5 Gesellschaftsrechtliche und öffentlich-rechtliche Pflichten

Darüber hinaus treffen die gesetzlichen Vertreter von Kapitalgesellschaften auch gesellschaftsrechtliche Pflichten, wie etwa die Verpflichtung zur Anmeldung eintragungsrelevanter Tatsachen beim zuständigen Handelsregister (vgl. z. B. §§ 181, 188 AktG, 40 GmbHG). Unterlässt der Verpflichtete die Vornahme von anmeldepflichtigen Tatsachen, so droht insbesondere die Zwangsgeldverhängung gegen die Mitglieder der Geschäftsführung, vgl. §§ 407 Abs. 1 AktG, 79 GmbHG. Im Rahmen der durch das MoMiG (Gesetz zur Modernisierung des GmbH-Rechts und zur Bekämpfung von Missbräuchen)[21] eingeführten Möglichkeit des gutgläubigen Erwerbs von GmbH-Geschäftsanteilen (vgl. § 16 Abs. 3 GmbHG) hat zudem die Gesellschafterliste stark an Bedeutung gewonnen. Sie ist nunmehr Anknüpfungspunkt des gutgläubigen Erwerbs von GmbH-Geschäftsanteilen, so dass sich der Geschäftsführer als Folge der Einreichungspflicht nach § 40 Abs. 1 GmbHG nicht nur noch einer Haftung gegenüber den Gesellschaftsgläubigern ausgesetzt sieht, sondern zusätzlich gegenüber denjenigen, deren Beteiligung sich geändert hat (d. h. im Fall der Anteilsveräußerung Veräußerer und Erwerber), vgl. § 40 Abs. 3 GmbHG. Diese Haftungsverschärfung und die zusätzlich durch das MoMiG eingeführten Prüfungspflichten (vgl. § 40 Abs. 1 S. 2 GmbHG, „Mitteilung und Nachweis") zulasten der Geschäftsführung dehnen die Haftungsrisiken des Geschäftsführers einer GmbH deutlich aus.

Weiterhin sind die Vertretungsorgane der Kapitalgesellschaften zur Vorbereitung und Einberufung von Gesellschafterversammlung und Hauptversammlung verpflichtet (vgl. §§ 121 Abs. 2 AktG, 49 Abs. 1 GmbHG) sowie zur Durchsetzung der dort getroffenen Beschlüsse.

Darüber hinaus bestehen viele zusätzliche Verpflichtungen der Geschäftsführung. Dazu zählen insbesondere die Pflicht zur Abführung der Steuern (wozu die gesetzlichen Vertreter persönlich verpflichtet sind, vgl. §§ 34, 69 S. 1 AO), die Pflicht zur fristgerechten Abführung von Sozialversicherungsbeiträgen und schließlich die Pflicht bei Zahlungsunfähigkeit oder Überschuldung rechtzeitig Insolvenzantrag zu stellen (vgl. § 15 a InsO).

Bei Erreichen bestimmter Beteiligungsschwellen an einer börsennotierten Gesellschaft ist der Vorstand gegenüber der Bundesanstalt für Finanzdienstleistungen nach dem Gesetz über den Wertpapierhandel (WpHG) zur Anzeige verpflichtet, vgl. § 21 Abs. 1 WpHG.[22]

Zusätzlich ist der Vorstand einer AG zur regelmäßigen Berichterstattung an den Aufsichtsrat hinsichtlich der beabsichtigten Geschäftspolitik und der Wirtschaftlichkeit der laufenden Geschäfte verpflichtet, vgl. § 90 Abs. 1 AktG. Vorstand und Aufsichtsrat von börsennotierten Gesellschaften haben gem. § 161 AktG einmal jährlich eine Entsprechenserklärung abzugeben, ob und inwieweit den von der Regierungskommission Deutscher Corporate Governance Kodex gemachten Empfehlungen entsprochen wurde. Nach § 15 WpHG ist der Vorstand zur Veröffentlichung von Tatsachen verpflichtet, wenn sie wegen

[21] Mit Wirkung vom 1. November 2008.

[22] Hierbei sind die Änderungen des WpHG zu beachten die durch das am 27. Juni 2008 verabschiedete Risikobegrenzungsgesetz eingetreten sind.

ihrer Auswirkungen auf die Vermögens- oder Finanzlage oder auf den allgemeinen Geschäftsablauf geeignet sind, den Börsenpreis der Aktie zu beeinflussen. Bei Geschäften mit Aktien der Gesellschaft ist der Vorstand gegenüber der Gesellschaft und der Bundesanstalt für Finanzdienstleistungen offenlegungspflichtig, vgl. § 15 a WpHG.

2.6 Pflicht zur Compliance

Aus der lediglich exemplarischen Aufzählung der oben beschriebenen Pflichten der Geschäftsleitung folgt bereits im eigenen Interesse der jeweiligen Geschäftsleitung die Notwendigkeit der Einrichtung einer Compliance-Organisation. Aufgrund der zunehmenden Anzahl von Haftungstatbeständen kann sich die Geschäftsleitung letztlich nur durch die Schaffung einer funktionierenden Struktur zur Einhaltung der gesetzlichen Verpflichtungen gegenüber der Gesellschaft und/oder Dritten absichern. Insbesondere geht es aber bei der Schaffung einer funktionierenden Compliance-Organisation darum, den langfristigen Unternehmenserfolg zu sichern. Unternehmen, die durch eine gut funktionierende Compliance-Organisation rechtliche Fehlerquellen und Zwischenfälle durch Rechtsverstöße minimieren, werden hiervon generell profitieren, i) durch den verbesserten internen Informationsfluss und Kontrollmaßnahmen, ii) durch frühzeitiges Entdecken (auch nicht rechtlicher) Fehler, iii) durch eine bessere Außendarstellung gegenüber Kunden und Dritten.

2.7 Internationales Unternehmensstrafrecht und seine Auswirkung auf deutsche Unternehmen

Für deutsche Unternehmen gilt formal betrachtet auch heute noch kein Unternehmensstrafrecht. Tatsächlich existieren aber gesetzliche Instrumente, mit denen Unternehmen, aus deren Sphäre Korruptionszahlungen geleistet worden sind, sanktioniert werden können. So können beispielsweise gemäß § 30 OWiG Geldbußen gegen juristische Personen verhängt werden, oder über § 30 Abs. 3 OWiG i. V. m. § 17 Abs. 4 StGB der Gewinn abgeschöpft werden, den ein Unternehmen im Zusammenhang mit den auf Korruption basierenden Aufträgen generiert hat. Des Weiteren kommt über § 73 ff. StGB das Institut des Verfalls zur Vermögensabschöpfung in Betracht.[23]

Für international tätige Unternehmen war es auch bisher schon zunehmend wichtig, internationale Antikorruptionsgesetze, wie den US Foreign Corrupt Practises Act (FCPA) im Auge zu behalten. Mit Wirkung zum 1. Juli 2011 ist in Großbritannien zusätzlich der sogenannte UK Bribery Act in Kraft getreten. Voraussetzung für die Anwendbarkeit des Gesetzes ist lediglich ein „geschäftlicher Bezug" zu Großbritannien, wobei dieser Begriff

[23] Hinzu kommen zivilrechtliche Folgen (§ 138 BGB), mögl. Vergabesperre, Rücknahme von Genehmigungen, etc.

nicht genauer definiert wird.[24] Bedeutsam ist dieses Gesetz insbesondere deshalb, weil es Strafnormen enthält, die direkt an Unternehmen adressiert sind und nach denen eine Strafbarkeit bereits in Betracht kommt, wenn eine dem Unternehmen nahestehende Person („associated person") eine andere Person (im privaten oder öffentlichen Sektor) besticht und dabei im Unternehmensinteresse handelt.[25] Der Begriff der nahestehenden Person soll dabei weit auszulegen sein und sogar Mitarbeiter von Joint Ventures und im Einzelfall auch Lieferanten umfassen.[26] Nach dem Willen des Gesetzgebers können sogar Personen umfasst sein, zu denen überhaupt kein formalisiertes Verhältnis besteht. Im Rahmen dieser Strafnorm findet quasi eine Beweislastumkehr statt, indem davon ausgegangen wird, dass das Unternehmen für das Fehlverhalten der „associated person" strafrechtlich haftet. Das Unternehmen hat lediglich die Möglichkeit, sich durch den Verweis auf ein bereits bestehendes, effektives Compliance-System zu exkulpieren.[27]

2.8 Informationsorganisation

Mit seinem Urteil vom 15. Dezember 2005[28] hat der BGH die Notwendigkeit der Einrichtung einer unternehmensinternen Informationsorganisation betont. Ein Unternehmen habe durch organisatorische Maßnahmen zu gewährleisten, dass eine Information alle Stellen des Unternehmens erreicht, für die diese Information relevant sein kann.

Dem Urteil lag ein Fall zugrunde, in dem trotz einer über das Vermögen eines Schuldners im Insolvenzverfahren veröffentlichten Verfügungsbeschränkung dieser Schuldner ein Bankkonto eröffnete und über die dort eingehenden Beträge verfügte. Der BGH ging davon aus, dass die Bank die Verfügungsbeschränkungen seit dem Wirksamwerden der Veröffentlichung im Amtsblatt gekannt hat. Aufgrund der Vermutungswirkung, die durch die Veröffentlichung entstand (vgl. §§ 82 Satz 2, 9 Abs. 3 InsO) war es an der Bank zu beweisen, dass ihr die Verfügungsbeschränkung unbekannt war.

Dieser Beweis ist ihr insbesondere deshalb nicht gelungen, weil Sie eine funktionierende Informationsorganisation nicht darlegen konnte. Der BGH forderte von der Bank den Nachweis einer organisatorischen Vorsorge, damit ihre Kunden betreffende Informationen über die Eröffnung von Insolvenzverfahren oder Sicherungsmaßnahmen im Vorfeld der Insolvenzeröffnung von ihren Entscheidungsträgern zur Kenntnis genommen werden.

Diese Verpflichtung ist in einer entsprechenden, wegen der Möglichkeiten des Zugriffs auf Datenspeicher auch zumutbaren Organisation dergestalt umzusetzen, dass ein Informationsfluss in alle Richtungen gewährleistet ist. Erforderlich ist also zunächst ein

---

[24] § 7 Abs. 5 UK Bribery Act: „*relevant commercial organization*" *means* „(*b*) *any other body corporate* (*wherever incorporated*) *which carries on a business, or part of a business, in any part of the United Kingdom*".

[25] § 7 Abs. 1 UK Bribery Act:„*A relevant commercial organization* („*C*") *is guilty of an* offence under this section if a person („A") associated with C bribes another person intending . . . (. . .).

[26] *Hugger/Röhrich*, in BB 2010, S. 2643(2644); *Deister/Geier/Rew*, in CCZ 3/2001, S. 81(84).

[27] *Kappel/Ehling*, in BB 2011, S. 2115(2116); vgl. auch *Deister/Geier/Rew*, in CCZ 3/2001, S. 81(86).

[28] BGH v. 15.12.2005 – IX ZR 227/04, NJW-RR 2006, 771 ff.

Informationsfluss von oben nach unten. Umgekehrt müssen Erkenntnisse, die von einzelnen Angestellten gewonnen werden, jedoch auch für andere Mitarbeiter und spätere Geschäftsvorgänge erheblich sind, die erforderliche Breitenwirkung erzielen. Dazu kann auch ein horizontaler und filialübergreifender Austausch erforderlich sein.[29]

Die Konsequenzen, die der BGH aus dem Fehlen einer entsprechenden Organisation zieht, sind erheblich: „Jedenfalls dann, wenn es an derartigen organisatorischen Maßnahmen fehlt, muss sich die Bank das Wissen einzelner Mitarbeiter – auf welcher Ebene auch immer diese angesiedelt sind – zurechnen lassen". Diese Aussage des BGH kann – wenn man darin nicht lediglich die Aussage sehen möchte, dass sich die Bank all das Wissen zurechnen lassen muss, das ihr bei sachgerechter Organisation zur Verfügung gestanden hätte – auch dahingehend verstanden werden, dass eine Wissenszurechnung davon abhängt, welche Vorkehrungen das Unternehmen getroffen hat, um einen angemessenen Informationsaustausch in vertikaler und horizontaler Richtung zu ermöglichen.

Die Wissenszurechnung würde damit von einem Verschuldenselement abhängig gemacht. Jedenfalls dann, wenn das Unternehmen zu wenig getan hat, um seiner Verpflichtung zur Gewährleistung einer angemessenen Informationsorganisation nachzukommen, wird der juristischen Person alles Wissen zugerechnet, was einem Mitarbeiter gleich auf welcher Ebene bekannt ist. Im Umkehrschluss kann man daraus schließen, dass sich die juristische Person vor Wissenszurechnungen dann schützen kann, wenn sie einen solchen Informationsfluss nachweisen kann. Bei Vorhandensein einer ordentlichen Informationsorganisation dürften sich Fehler wie im zugrundeliegenden Fall ohnehin meist vermeiden lassen, so dass es auf die Frage der Zurechnung nicht mehr ankommt.

Dass diese Grundsätze nur auf Banken beschränkt aufgestellt wurden, ist dem Urteil nicht zu entnehmen. Plausible Gründe wird man für eine Differenzierung auch nicht angeben können.

Deshalb tun Unternehmen gut daran, eine Organisation vorzuhalten, die für einen geregelten Informationsfluss innerhalb des Unternehmens sorgt. Denn sie beugen damit in zweifacher Hinsicht möglichen Schäden vor: Zum einen können Fehler vermieden werden, weil die Entscheidungsträger die richtigen Informationen zugrunde legen. Zum Zweiten führt eine nachgewiesen gute Informationsorganisation zu größeren Entlastungsmöglichkeiten, wenn es um Wissenszurechnung geht. Wenn also eine Information trotz einer guten Vorsorge gleichwohl nicht an die richtige Stelle gelangt, wird diese Information – wenn man den Gedanken des BGH konsequent zu Ende denkt – auch nicht mehr zugerechnet.

2.9 Notwendigkeit der Einrichtung einer Abteilung „Interne Revision"[30]

Wie bereits oben dargestellt ist Anknüpfungspunkt für die Pflicht der Einrichtung eines Früherkennungs- und Überwachungssystems für bestandsgefährdende Entwicklungen der Gesellschaft die Vorschrift des § 91 Abs. 2 AktG.

[29] Vgl. BGH v. 1.6.1989 – III ZR 261/87, WM 1989, 1364, 1367; BGH v. 15.1.2004 – IX ZR 152/00, WM 2004, 720, 722.

[30] Vgl. hierzu umfassend: *Berwanger/Kullmann*, Interne Revision – Wesen, Aufgaben und rechtliche Verankerung, 2008.

2.9.1 Früherkennungs- und Überwachungssystem (§ 91 Abs. 2 AktG)

Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Die Maßnahmen, die der Vorstand ergreift, müssen geeignet sein, die Früherkennung bestandsgefährdender Entwicklungen zu gewährleisten. „Dazu gehört namentlich, die frühzeitige und umfassende Kenntnis des Vorstands sicherzustellen, und zwar des Gesamtvorstands, nicht nur seines Vorsitzenden oder bestimmter Ausschüsse oder Arbeitsgruppen".[31] Frühzeitig ist die Kenntniserlangung dann, wenn eine nachteilige Entwicklung noch so rechtzeitig dem Vorstand bekannt wird, dass dieser der Entwicklung entgegenwirken und so eine Bestandsgefährdung abwenden kann.[32]

Wie bei anderen Leitungsentscheidungen auch hat der Vorstand ein Leitungsermessen insbesondere hinsichtlich der Art und Form der zu ergreifenden Maßnahmen. Das Ermessen ist am Maßstab der konkreten Umstände im Unternehmen (Größe, Branche, Risikopotenzial der Märkte, Struktur, Lage des Unternehmens, Kapitalmarktzugang) auszurichten und entsprechend der in Betracht kommenden nachteiligen Entwicklungen auszuüben.[33]

Was den neben den „Maßnahmen" angesprochenen zweiten Aspekt der Norm – das Überwachungssystem – betrifft, herrscht Unklarheit, ob das System zur Überwachung der eingeleiteten Maßnahmen (so die überwiegende Ansicht) dient oder aber die risikoträchtigen Entwicklungen selbst zu überwachen sind. Da letztlich dem Begriff der „geeigneten Maßnahmen" auch die Einrichtung einer informationsvermittelnden Organisation zuzuordnen sein wird, dürfte die dargelegte Unklarheit für die Praxis kaum eine Rolle spielen.[34]

Das Überwachungssystem meint daher eine unternehmensinterne Kontrolle, die sicherstellen soll, dass die zur Früherkennung eingeleiteten Maßnahmen auch greifen, dass also die im Rahmen der Früherkennung gewonnenen Erkenntnisse zeitnah an den Vorstand weitergeleitet werden. Im Ergebnis wird man § 91 Abs. 2 AktG daher als eine Organisationsanforderung zu verstehen haben. Durch klar abgegrenzte Zuständigkeiten, ein engmaschiges Berichtswesen und eine entsprechende Dokumentation der Vorgänge wird man daher den Anforderungen genügen.

In der Regel dürfte zu einem angemessenen Überwachungssystem die Interne Revision sowie eine Controlling-Abteilung gehören.[35] Auch hier kommt es für die Frage der Ausgestaltung aber entscheidend auf die Größe,[36] Struktur und Lage des Unternehmens, das Risikopotential der Märkte, auf denen das Unternehmen tätig ist, sowie die Art des Kapitalmarktzugangs an. Keineswegs kann aus § 91 Abs. 2 AktG etwa eine konkrete Zuständigkeit

---

[31] *Hüffer*, NZG 2007, 47, 49.

[32] RegBegr. BT-Drucks. 13/9712S. 15 reSp.

[33] *Spindler*, in: Münchner Kommentar zum AktG 3. Aufl. 2008, § 91 Rn. 24.

[34] *Spindler*, in: Münchner Kommentar zum AktG 3. Aufl. 2008, § 91 Rn. 26.

[35] *Spindler*, in: Münchner Kommentar zum AktG 3. Aufl. 2008, § 91 Rn. 28.

[36] Als Indiz wird man hier die in § 267 HGB aufgeführten Größenklassen mit heranziehen können.

oder Ablauforganisation der Risikoerfassung gefolgert werden, etwa bis hin zum Erfordernis von Schadensformularen etc. Derartiges mag betriebswirtschaftlich sinnvoll sein, rechtlich zwingend ist es nicht. Die Praxis sollte sich gleichwohl darauf einstellen, dass Einrichtungen geschaffen werden müssen, die die Funktion der bestehenden Controlling- und Revisionseinrichtungen des Unternehmens überwachen und eine kurzfristige Information des Vorstands sicherstellen.[37]

Für Kreditinstitute und Finanzdienstleistungsinstitute besteht mit § 25 a KWG eine aufsichtsrechtliche Sonderregelung, die von den Instituten eine ordnungsgemäße Geschäftsorganisation verlangt, die die Einhaltung der von den Instituten zu beachtenden gesetzlichen Bestimmungen gewährleistet. Nach § 25 a Abs. 1 Nr. 1 KWG umfasst eine ordnungsgemäße Geschäftsorganisation insbesondere ein angemessenes Risikomanagement. Dies beinhaltet auf der Grundlage von Verfahren zur Ermittlung und Sicherstellung der Risikotragfähigkeit die Festlegung von Strategien sowie die Einrichtung interner Kontrollverfahren, die aus einem internen Kontrollsystem und einer internen Revision bestehen, wobei das interne Kontrollsystem dabei insbesondere umfasst:

Aufbau- und ablauforganisatorische Regelungen, die eine klare Abgrenzung der Verantwortungsbereiche umfassen, und

„Prozesse zur Identifizierung, Beurteilung, Steuerung sowie Überwachung und Kommunikation der Risiken; dabei soll den in Anhang V der Bankenrichtlinie niedergelegten Kriterien Rechnung getragen werden."

Entsprechend dürfte man in diesen Wirtschaftsbereichen über die sich aus § 91 Abs. 2 AktG ergebenden Anforderungen hinaus ohne ein „risk management", ohne Compliance-Regelungen und ohne ablaufimmanente Kontrollen nicht auskommen.[38]

Interessant ist § 23a KWG insbesondere im Hinblick auf ihr Verhältnis zu § 91 Abs. 2 AktG. Die ganz überwiegende Ansicht möchte diese Vorschrift zwar nicht branchenübergreifend zur Konkretisierung des § 91 Abs. 2 AktG heranziehen, hält aber eine entsprechende Berücksichtigung für zulässig.[39] Andererseits hat die Rechtsprechung die Norm schon zur Ausfüllung des § 91 AktG auch bei branchenfremden Unternehmen herangezogen.[40] In seiner Entscheidung vom 8. Juli 2004 war das Verwaltungsgericht Frankfurt a. M. der Ansicht „dass sich diese Norm (d. h. § 91 Abs. 2 AktG, Anm. d. Verf.) und § 25a Abs. 1 KWG ihrer rechtlichen Bedeutung entsprechen (. . .), so dass die in § 25a KWG gesetzlich genauer gefassten Anforderungen bei der Auslegung des § 91 Abs. 2 AktG herangezogen werden können (. . .). Diese weitgehende Sichtweise entspricht nach Auffassung der erkennenden Kammer der Gesamtintention des Gesetzgebers der (. . .) die Verpflichtung der Geschäftsleitung hervorheben wollte, Risikofrüherkennungs- sowie Risikoüberwachungssysteme in den Unternehmen einzurichten, um Entwicklungen

[37] *Hüffer*, NZG 2007, 47, 49.

[38] *Hüffer*, ebd.

[39] *Hüffer*, ebd. m. w. N.

[40] VG Frankfurt a. M. v. 8. Juli 2004 – 1 E 7363/03 (I), WM 2004, 2157, 2160.

vorzubeugen, die den Fortbestand der Gesellschaft gefährden können".[41] Auch wenn die nachfolgende Argumentation des Gerichts darauf hindeuten könnte, dass man die entsprechende Heranziehung des § 25a KWG nur auf Versicherungsunternehmen erstrecken möchte, ist es für die Praxis empfehlenswert sich an den Vorgaben des § 25a KWG zu orientieren.

2.9.2 Ausstrahlungswirkung auf GmbH?

Inwieweit § 91 Abs. 2 AktG, der grundsätzlich nur auf Vorstände von Aktiengesellschaften Anwendung findet, auch auf andere Gesellschaftsformen zu übertragen ist, wird – jedenfalls was das Ausmaß der Auswirkungen betrifft – unterschiedlich beurteilt. Der Gesetzgeber hat eine Ausstrahlungswirkung – ohne deren konkrete Reichweite darzulegen – ausdrücklich formuliert:

> In das GmbHG soll keine entsprechende Regelung aufgenommen werden. Es ist davon auszugehen, dass für Gesellschaften mit beschränkter Haftung je nach ihrer Größe, Komplexität ihrer Struktur usw. nichts anderes gilt und die Neuregelung Ausstrahlungswirkung auf den Pflichtenrahmen der Geschäftsführer auch anderer Gesellschaftsformen hat.[42]

Da der Gesetzgeber jedoch – obwohl es ihm leicht gefallen wäre – keine entsprechende Regelung in das GmbHG eingeführt hat, wird man eine gänzlich gleichlaufende Verpflichtung nicht annehmen dürfen. Auch die Struktur bspw. der GmbH mit einem dem Vorstand gegenüber nicht ähnlich starken, nämlich weisungsgebundenen Leitungsorgan widerspricht einer „eins-zu-eins" Übertragung. Vielmehr wollte der Gesetzgeber die Reichweite der Norm der weiteren Entwicklung in Rechtsprechung und Literatur überlassen.[43] Andererseits lässt sich schon aus § 43 Abs. 1 GmbHG ableiten, dass den Geschäftsführer die Verpflichtung trifft, sich um die rechtzeitige Erkennung von Krisen-Anzeichen zu bemühen.[44] Schon ohne einen Rückgriff auf die Norm des § 91 Abs. 2 AktG wird sich ein Geschäftsleiter nur dann – bei Nichteinrichtung einer Abteilung „Interne Revision" – der Haftung entziehen können, wenn er auf ausreichender Informationsbasis eine den Gegebenheiten des Unternehmens angemessene Ermessensentscheidung über Einführung, Ausgestaltung und Umfang einer internen Kontrolle trifft.[45]

Bei dieser Entscheidung ist jedoch die gesetzgeberische Intention in § 91 Abs. 2 AktG mit zu berücksichtigen. Wenn auch die Reichweite der Ausstrahlung unklar ist, ist man

---

[41] Ebd.

[42] RegBegr. BT-Drucks. 13/9712S. 15 reSp.

[43] *Drygala/Drygala*, ZIP 2000, 297, 300 m. w. N.

[44] *Westermann*, DZWIR 2006, 485, 387.

[45] In diese Richtung argumentierend *Drygala/Drygala*, ZIP 2000, 297, 303 f. Nur klarstellend ist festzuhalten, dass es in der Frage, ob nachgeordnete Entscheidungsebenen von der Führungsebene zu überwachen sind, sicherlich kein unternehmerisches Leitungsermessen gibt, allerdings ist es eine andere Frage, ob eine derartige Überwachung in der von § 91 Abs. 2 AktG angestrebten Organisationsstruktur umzusetzen ist.

sich doch einig, dass die Norm auch in andere Rechtsformen hineinwirkt. Der Gesetzgeber hat aber deutlich gemacht, dass er grundsätzlich auf eine Einrichtung derartiger Maßnahmen und entsprechender Überwachungssysteme hinarbeitet. Dies bedeutet für die Geschäftsleiter, dass sie sich von vornherein einem erhöhten Rechtsfertigungsdruck aussetzen, wenn sie sich gegen die Einrichtung entsprechender Systeme entscheiden.

Die Notwendigkeit der Einrichtung einer Abteilung „Interne Revision" wird man für die GmbH daher erst dann aus § 91 Abs. 2 AktG ableiten können, wenn diese dem in § 91 Abs. 2 AktG zugrunde gelegten Leitbild eines komplexen Großunternehmens so stark entspricht, dass eine Nichtanwendung der aktienrechtlichen Vorschrift systemwidrig wäre.[46] Wie bei der Aktiengesellschaft kommt es damit auch bei der GmbH letztlich auf eine unternehmensangemessene Organisationsstruktur an, die je nach Größe, Struktur und Risikopotential des Unternehmens auszugestalten ist.

Praxishinweis

Kann das Unternehmen – auch wenn es in der Rechtsform der GmbH besteht – nach den in der Regierungsbegründung beispielhaft genannten Faktoren (Struktur, Größe o. ä.) dem Kreis der Unternehmen zugeordnet werden, die einer Aktiengesellschaft entsprechen, wie sie § 91 Abs. 2 AktG vor Augen hat, spricht vieles dafür, auch in einer Gesellschaft in der Rechtsform einer GmbH eine interne Revision einzurichten. Vorzugsweise dürften mit Hilfe eines externen Beraters zunächst die revisionsrelevanten Risken zu identifizieren sein, um eine entsprechende Themenliste für die interne Revision und entsprechend die notwendigen Kapazitäten der Revisionsabteilung herausarbeiten zu können.

Kommt der Vorstand einer AG den Verpflichtungen aus § 91 Abs. 2 AktG nicht nach, haften die Vorstandsmitglieder der Gesellschaft gegenüber gemäß § 93 Abs. 2 S. 1 AktG. Die Nichteinhaltung der Pflichten nach § 91 Abs. 2 AktG kann zudem ein wichtiger Grund zur Abberufung und fristlosen Kündigung sein. Für die Geschäftsleitung einer GmbH könnte man – wenn man § 91 Abs. 2 AktG in seiner Ausstrahlungswirkung als Konkretisierung des § 43 Abs. 1 GmbHG verstehen möchte – eine Haftung nach § 43 Abs. 2 GmbHG annehmen.

2.10 Fazit: Pflicht zum Aufbau einer Compliance-Organisation

Für Geschäftsführer und Vorstandsmitglieder besteht, abhängig von Größe, Struktur und Risikopotential des Unternehmens, ein umfangreicher nur schwer zu überblickender Pflichtenkatalog. Die Rechtsprechung stellt zunehmend höhere Anforderungen an Informationsorganisation und Früherkennungs- und Überwachungssysteme. Bei Fehlen

[46] *Veil*, ZGR 2006, 374, 376 f. m. w. N.; *Drygala/Drygala*, ZIP 2000, 297, 305; noch strenger *Altmeppen*, ZGR 1999, 291, 301 f.

einer ordentlichen Compliance-Organisation droht im Schadensfall die Haftung der Organe. Im Umkehrschluss besteht daher eine Handlungspflicht. Wer in seiner Funktion als Geschäftsführer oder Vorstandsmitglied ein möglichst hohes Maß an Sicherheit hinsichtlich des eigenen Haftungspotentials sicherstellen möchte, muss sich um die Errichtung oder den Erhalt einer möglichst effizienten Compliance-Organisation kümmern.[47]

3 Umsetzung einer Compliance-Organisation

Außer der Einrichtung einer internen Revision als Teil einer Compliance-Organisation – zumindest für große Unternehmen – gibt es weitere organisatorische Möglichkeiten, eine Compliance-Organisation aufzubauen.

3.1 Planung der Compliance-Organisation

Für die Planung der Compliance-Organisation sollte zunächst im Rahmen einer unternehmensinternen „Due Diligence" eine Art Bestandsaufnahme bereits bestehender Abläufe und Überwachungssysteme durchgeführt werden. Im Anschluss sollten die Ziele des Gesamtprojekts definiert und die grundsätzliche Herangehensweise festgelegt werden.

3.1.1 Baukastensystem vs. Komplettlösung

Je nachdem welches Überwachungssystem im Unternehmen bereits etabliert ist und welche Faktoren für das Unternehmen eine Rolle spielen (Größe/Branche/Risikopotential der Märkte), muss entschieden werden, ob die Einführung einer umfassenden „Komplettlösung/Teilsysteme" erforderlich ist. Vorhandene Systeme müssen auf Einheitlichkeit von Abläufen und eventuelle Verknüpfbarkeit überprüft werden.

3.1.2 Identifikation Pflichtenkreise

Im Rahmen einer Due-Diligence oder einer Compliance-Prüfung[48] müssen die für das Unternehmen und seine Mitarbeiter relevanten Pflichtenkreise definiert werden. Hierbei gibt es **branchenunabhängige Pflichtenkreise** wie beispielsweise

Arbeitssicherheit
Allgemeine Gleichbehandlung
Wettbewerbsrecht
Datenschutzrecht
Strafrecht
Außenhandelsrecht
Geldwäscherecht

[47] So auch *Schneider*, ZIP 2003, 645, 648.

[48] „Complianc-Audit".

Aus diesen Pflichtenkreisen resultierende Vorgaben und notwendigen Abläufe müssen definiert und Verantwortungsbereichen und somit auch Mitarbeiterkreisen zugeordnet werden. Ergänzend muss diese Vorgehensweise **für branchenbezogene Pflichtenkreise durchgeführt werden**. Beispiele hierfür sind:

Umweltrecht (insb. Immissionsschutzrecht/Kreislaufwirtschafts- und Abfallrecht)
Gentechnikrecht
Arzneimittelrecht
Kreditwesenrecht
Versicherungsaufsichtrecht

Die aus diesen Pflichtenkreisen resultierenden Handlungsanweisungen, Verhaltensvorschriften Standards und Sanktionen können z. B. im Rahmen eines Handbuchs festgehalten und über Schulungsmaßnahmen den Mitarbeitern aufgezeigt werden (s. u.).

3.1.3 Entwicklung der Compliance-Organisation

Für das Grundgerüst einer Compliance-Organisation werden stets einige Grundlagen zu beachten sein. Zunächst wird der Chief Compliance Officer („CCO"), oder falls eine solche Position nicht geschaffen werden soll, die für Compliance im Unternehmen verantwortliche Person, dem Vorstandsvorsitzenden direkt unterstellt und berichtspflichtig sein müssen, um für eine weitgehende Unabhängigkeit im Unternehmen zu sorgen. Sofern erwünscht kann dem CCO ein unabhängiges Kontrollgremium (Compliance-Committee) zur Seite gestellt werden, das aus externen Experten bestehen kann. Sofern als Teil der Compliance-Organisation auch ein Ombudsmann im Rahmen einer Whistle-Blowing Hotline installiert werden soll, wird dieser der Geschäftsleitung und dem Compliance Officer berichtspflichtig sein müssen, um Unabhängigkeit zu gewährleisten. In den Stabsabteilungen und in allen weiteren Unterabteilungen sind jeweils für die Überwachung der Compliance verantwortliche Mitarbeiter zu benennen, welche natürlich auch entsprechend zu schulen sind. Auf allen Ebenen besteht die Pflicht zur eigenständigen Überwachung und Kontrolle im eigenen Verantwortungsbereich. Entsprechend sollte eine Dokumentationspflicht über die Compliance-Tätigkeit bestehen. Die Struktur einer Compliance-Organisation könnte beispielsweise folgendermaßen aussehen (Abb. 1)[49]:

3.2 Handbücher und Compliance-Systeme

Zur Begrifflichkeit und Grundlage eines sog. Code of Conduct bzw. Code of Ethic wurde bereits oben Stellung genommen.

[49] In Anlehnung an: *Rodewald/Unger*, BB 2007, 1629, 1632.

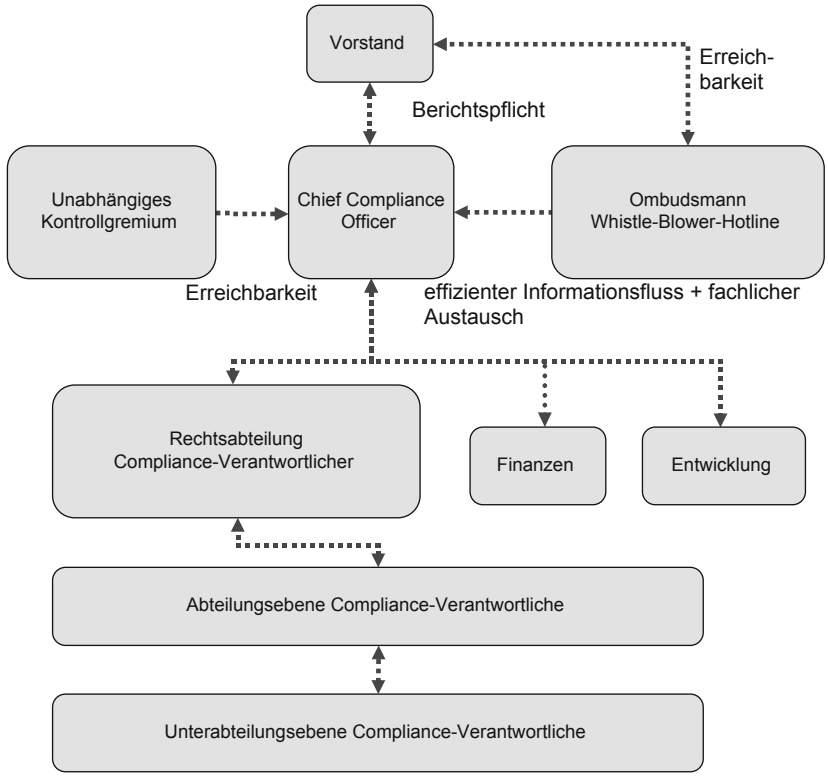


Abb. 1 Struktur einer Compliance-Organisation

3.2.1 Compliance-Handbücher

Handbücher können ein sinnvoller Baustein einer Compliance-Organisation sein. Wichtig ist hierbei zunächst eine genaue Festlegung der Adressatenkreise des Handbuchs. Sinnvoll sind, neben allgemeinen Handlungs- und Verhaltensanweisungen, getrennte Handbücher für unterschiedliche Pflichtenkreise im Unternehmen, da sich etwa für die Produktion oder den Vertrieb völlig andere Pflichtenkreise ergeben können, als beispielsweise für die Verwaltung. Die genaue Zuordnung der gesetzlichen Pflichtenkreise und der Adressaten im Unternehmen ist daher Erfolgsvoraussetzung.

Da über Handbücher den Mitarbeitern die von ihnen zu beachtenden Pflichten und gesetzlichen Vorgaben erläutert werden, reicht es nicht aus, Handbücher bloß zur Verfügung zu stellen. Vielmehr muss sichergestellt und überprüft werden, dass jeder Mitarbeiter die für ihn geltenden Lektionen kennt. Es bietet sich daher an, die Mitarbeiter in Pflichtschulungen über die relevanten Pflichtenkreise zu schulen. Dies kann in herkömmlicher Art oder über Internet oder Telefonschulungen bewältigt werden. Bei der Auswahl des Schulungsmediums ist zu berücksichtigen, wie eine möglichst hundertprozentige Abdeckung der betroffenen Mitarbeiter sichergestellt werden kann. Je nach Unternehmen kann eine

hohe Einbeziehungsquote am besten über Internetschulungen erreicht werden. Zudem haben solche „modernen" Schulungsmaßnahmen den Vorteil, dass jeder Mitarbeiter die Schulung zu einem ihm passenden Zeitpunkt am PC durchführen kann und ein minimaler Zeitaufwand hierfür notwendig ist. Die Vermeidung von Arbeitsausfall und Reisekosten ist bei der Entscheidung zwischen herkömmlicher Schulungsveranstaltung und eLearning sicher ein wichtiger Faktor, der ggf. mögliche Mehrkosten z. B. für eLearning-Programme ausgleichen kann. Des Weiteren ist es wichtig sicherzustellen, dass Nachweismöglichkeiten über durchgeführte Schulungsmaßnahmen und -inhalte bestehen. Auch dies ist bei Internetschulungen leichter möglich.

3.2.2 IT-Systeme zur Sicherstellung der Compliance

Vision der Systemhersteller ist es, Compliance-Management Lösungen bereitzustellen, die dauerhaft die laufenden Compliance-Kosten senken. Hauptziele sind hierbei die Erfassung aller gesetzlichen Pflichten, die Rationalisierung und Sammlung von Compliance-Daten und die Erweiterung der Nachweisführung durchgeführter Compliance-Maßnahmen. Die Benutzerfreundlichkeit und die Verknüpfung mit weiteren Anwendungen wie z. B. einem integrierten Dokumentenmanagement spielen hierbei ebenfalls eine wichtige Rolle.

Beteiligungsmanagementsysteme Beteiligungsmanagementsysteme können gerade bei großen Konzernen mit einer großen weltweiten Streuung von Tochterunternehmen für Transparenz trotz unglaublicher Daten- und Informationsdichte sorgen. Sind die Informationen erst eingepflegt, stehen sie weltweit auf Knopfdruck über die Internetoberfläche allen berechtigten Nutzern zur Verfügung.

Voraussetzung für ein erfolgreiches Beteiligungsmanagement ist jedoch, dass bei der Eingabe der entsprechenden Unternehmensdaten mit äußerster Sorgfalt vorgegangen wird. Werden Daten von zuvor genutzten alten Systemen einfach ungeprüft auf ein neues globales IT-System überspielt, werden auch die Fehler mit übernommen. Die Akzeptanz einer fehlerbehafteten Datenbank dürfte sich dann in Grenzen halten.

Für gesellschaftsrechtliche Kerninformationen empfiehlt sich daher bei der Einrichtung eines solchen Systems vor der Datenmigration zunächst eine Überprüfung (Due-Diligence) der Daten vorzunehmen.

Es bietet sich zudem an, Beteiligungsmanagementsysteme um weitere Komponenten einer Compliance-Organisation zu ergänzen. Moderne Systeme bieten die Möglichkeit der Durchführung von Schulungen über das Internet an. Die heute am Markt verfügbaren Systeme bieten die technischen Möglichkeiten, um beispielsweise Schulungen für bestimmte Personenkreise durchzuführen und dies auch zu dokumentieren. Darüber hinaus bringt der Einsatz solcher Systeme eine enorme Datensicherheit und sorgt folglich in hohem Maße zur Verbesserung der Compliance im Unternehmen.

Zur Gewährung einer fortlaufenden Datensicherheit gibt es verschiedene Möglichkeiten. So ist es beispielsweise möglich, weltweit die verantwortlichen Personen über regelmäßig über das Internet durchgeführte Befragungen zum Datenabgleich zu verpflichten. Sofern die Fragebögen nicht ausgefüllt werden, wird die Compliance-Abteilung

umgehend informiert und kann den Verantwortlichen gezielt ansprechen. Bei weltweit operierenden Unternehmen ist für die Gewährleistung der Datengenauigkeit eines internetgestützten Compliance-Systems empfehlenswert, in jedem Land nur wenigen Personen die Möglichkeit zur Dateneingabe oder Änderung zu gewähren und vor einer Freigabe weitere Überprüfungsmechanismen zu installieren.

IT-Systeme und eLearning Andere Systeme, wie beispielsweise ein kanadisches System, dienen vornehmlich der Überprüfung des aktuellen Compliance-Maßstabs und ersetzen insofern in erster Linie händische Checklisten. Ähnlich wie bei den Compliance-Handbüchern werden zunächst die Pflichtenkreise nebst konkret anwendbaren Vorschriften analysiert. Diese Analyse wird in den jeweiligen Ländern von Juristen durchgeführt. Anschließend werden die anwendbaren gesetzlichen Vorschriften in separat zuweisbare Aufgaben einzelner Führungskräfte übersetzt. Diese Führungskräfte werden dann über das Internet halbjährlich einer Prüfung unterzogen und müssen zu wichtigen Sachverhalten und Pflichten konkret Stellung nehmen. Dabei werden die gesetzlichen Vorschriften jeweils in vereinfachter Sprache dargestellt und es wird erklärt, warum welche gesetzliche Vorschrift einzuhalten ist. Die so abgelieferten Compliance-Berichte werden auf Übereinstimmung mit den gesetzlichen Vorschriften geprüft und gespeichert. Sofern Beanstandungen erforderlich sind, erhält die jeweilige Führungskraft eine Aufforderung zur Nachbesserung. Dieses System verknüpft somit Schulung und Reporting.

4 Beispiele und Kontrollsysteme

Täglich vorkommende Pressemeldungen zu Compliance-bezogenen Vorfällen machen deutlich, dass das Thema Compliance bei vielen Unternehmen noch nicht mit letzter Konsequenz bearbeitet wird. Als bekannte Beispiele können die Korruptionsfälle bei Siemens und MAN, sowie die Vorfälle mit Sonderzahlungen und Vergnügungsreisen für Betriebsräte herangezogen werden.[50] Laut Zeitungsmeldungen waren beispielsweise bei Siemens jeweils hoch in der Hierarchie angesiedelte Führungskräfte in diese Fälle verwickelt, allerdings liegen keine Indizien für eine Bereicherung der Manager zu Lasten ihres Arbeitgebers vor. Hieraus lässt sich wiederum schließen, dass die Manager glaubten, bei der Bestechung zur Erlangung von Aufträgen im Interesse ihres Unternehmens zu handeln. Gerade die zweite und dritte Führungsebene kann man durch Schulungen leicht auf Verhaltensvorschriften einschwören. Hätte der Vorstand somit unmissverständlich über Verhaltensanweisungen zum Ausdruck gebracht, dass die Zahlung von Bestechungsgeldern dem Unternehmen schadet und zwingend zu unterlassen ist, wäre ein solcher Irrglauben der Manager eigentlich ausgeschlossen.

[50] Als aktuelleres Beispiel mag der Korruptionsskandal bei Ferrostahl dienen.

Hätte die Bank in dem vom BGH[51] entschiedenen und oben zum Thema Informationsorganisation dargestellten Fall ein System eingeführt, in welches Verfügungsbeschränkungen eingetragen und mit den Namen und Kontendaten von Kunden verknüpft werden, wäre es zu einem solchen Fall nicht gekommen.

Die Beispielsfälle zeigen, dass die notwendigen Compliance-Maßnahmen für Unternehmen je nach Branche sehr unterschiedlich ausfallen können. Nicht immer sind IT-gestützte Lösungen der Weisheit letzter Schluss. Grundsätzlich gilt jedoch, dass moderne Systeme insbesondere für große Unternehmen eine enorme Erleichterung darstellen können. Angefangen mit der Verbesserung der Datengenauigkeit durch Nutzung von Beteiligungsmanagement – oder Vertragsmanagementsystemen, über eLearning und Handbücher – dürfte im Schadensfall eins jedenfalls immer gelten: Wer umfangreiche Maßnahmen getroffen hat, steht sowohl vor der Staatsanwaltschaft als auch in der Öffentlichkeit und bei Investoren besser dar. Zudem dürfte den Organen der Unternehmen die Möglichkeit vieler IT-Systeme, Compliance-Maßnahmen genau zu dokumentieren, im Hinblick auf eine drohende Haftung bei unterlassener Überwachung sehr gelegen kommen. Für kleinere Unternehmen, die sich keines IT-Systems bedienen können oder wollen, gilt es sich auf „analogem" Wege ähnlich gut zu organisieren und zu dokumentieren.

5 Fazit

Als Fazit bleibt die Aussage: Arbeite ordentlich und dokumentiere, dass du ordentlich gearbeitet hast!

Dies gilt insbesondere in Zeiten, in denen zunehmend auch von den Unternehmen selbst mehr (insbesondere staatliche) Kontrolle und Transparenz gefordert wird.

[51] BGH v. 15.12.2005 – IX ZR 227/04, NJW-RR 2006, 771 ff.

Praxistipps Produkthaftung

Volker Steimle und Guido Dornieden

Inhaltsverzeichnis

Zusammenfassung

Schlechtes Krisenmanagement beim Umgang mit einer Produktkrise kann für das betroffene Unternehmen in jeglicher Hinsicht teuer werden. Im „worst case" endet sie in der strafrechtlichen Verantwortlichkeit der handelnden Personen. Ein gut aufgestelltes Unternehmen sorgt deshalb auch für diesen Ernstfall rechtzeitig vor – und entledigt sich durch ein vorausschauendes Handeln bereits im Vorfeld einer Vielzahl von Problemen. Der vorliegende Beitrag erläutert, woran hier im Einzelnen zu denken ist.

V. Steimle (✉)
Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: volker.steimle@luther-lawfirm.com

G. Dornieden
E-Mail: guido.dornieden@luther-lawfirm.com

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2_3, © Springer Fachmedien Wiesbaden 2013

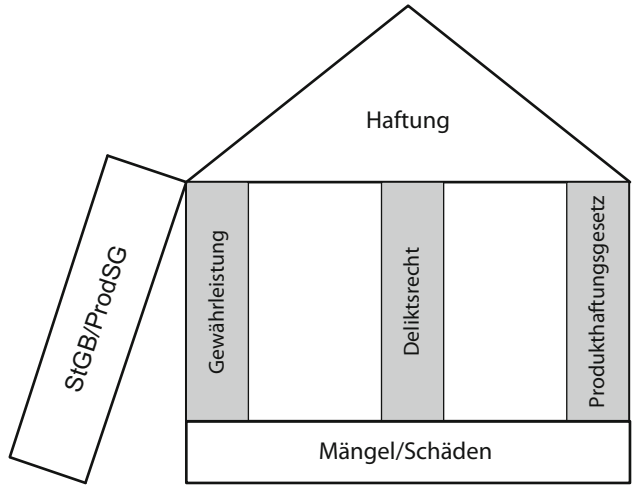


Abb. 1 Die drei Säulen der Produkthaftung

1 Einleitung

Die Vermeidung von Produkthaftungsansprüchen stellt insbesondere in produzierenden Unternehmen ein sehr weites Feld dar. Die proaktive Vermeidung von Schäden und Risiken aus Produkthaftung – das Betätigungsfeld von „Compliance" – verlangt nicht zuletzt deshalb sehr umfangreiche und komplexe Prozesse. Im Rahmen einer proaktiven Betrachtung sollte der Umgang mit Produkthaftung nicht auf die Produkthaftung im engeren rechtlichen Sinne begrenzt werden, sondern sämtliche Gefahren und Schäden aus schadhaften, riskanten, nicht regelkonformen oder sonstig schadensstiftenden Produkten mit umfassen. Ausgehend von der rechtlichen Natur möglicher Ansprüche gegen den Hersteller solcher Produkte, sind hier zunächst einmal drei zivilrechtliche Rechtsquellen zu berücksichtigen: vertragliche Gewährleistung (etwa §§ 433 ff. BGB bei Kaufverträgen), Deliktsrecht (§§ 823 ff. BGB) sowie das Produkthaftungsgesetz (Abb. 1)[1].

Diese drei möglichen Anspruchsgrundlagen zu Gunsten eines Geschädigten stehen im Wege der **Anspruchskonkurrenz** nebeneinander. Der Geschädigte hat folglich die freie Wahl, auf welche der verschiedenen Anspruchsgrundlage er die von ihm begehrte Rechtsfolge, etwa einen Anspruch auf Schadensersatz, stützen möchte. Das Wesen der Anspruchskonkurrenz hat darin seine innere Logik, dass die verschiedenen Anspruchsgrundlagen unterschiedliche Voraussetzungen, aber auch unterschiedliche Rechtsfolgen haben.[2] Je nach Lage des Einzelfalls kann es daher für einen Geschädigten erfolgverspre-

[1] Abbildung aus *Steimle*, Vertragsrecht für Nichtjuristen (Convent-Seminare).

[2] Bis zum Inkrafttreten des 2. Schadensersatzänderungsgesetzes vom 18. April 2002 war etwa Schmerzensgeld nur bei einer Haftung des Schädigers aus Deliktsrecht zu erhalten, nicht aber etwa aus verschuldensunabhängiger Gefährdungshaftung wie dem Produkthaftungsgesetz.

chender sein, sich auf eine dieser Anspruchsgrundlagen zu stützen, die für ihn in der Rechtsverfolgung sicherer erscheint als eine andere der Anspruchsgrundlagen.
Vereinfacht ausgedrückt, sind die jeweiligen Ziele dieser Anspruchsgrundlagen folgende:

Vertragliche Gewährleistung Sicherstellung des vertraglich vereinbarten Gleichgewichts zwischen Leistung und Gegenleistung; Äquivalenzinteresse.

Deliktsrecht Schutz bestimmter, sogenannter „absoluter" Rechtsgüter gegenüber jedermann (Leben, Gesundheit, Eigentum etc.); Integritätsinteresse.

Produkthaftungsgesetz Schutz von Leben, Gesundheit und in eingeschränktem Umfang Eigentum von Verbrauchern.

Während Ansprüche aus vertraglicher Gewährleistung zwar die Lieferung unsicherer Produkte zur Grundlage haben können, aber nicht müssen (die Lieferung eines pinkfarbenen Ferrari statt des georderten Sportwagens in der traditionellen Farbe „Rosso" würde sicherlich Gewährleistungsansprüche begründen, ohne deswegen ein weniger sicheres Produkt darzustellen), greifen Deliktsrecht und Produkthaftungsgesetz immer nur dann ein, wenn unsichere Produkte Schäden verursachen bzw. zu verursachen drohen.

Neben diesen Rechtsquellen des Zivilrechts werden produkthaftungsrechtliche Fragen zunehmend auch durch das **öffentliche Recht** bestimmt. Insbesondere das europarechtlich geprägte **Produktsicherheitsgesetz**[3] weist den jeweils zuständigen Aufsichtsbehörden weitreichende Befugnisse zu (inklusive der Befugnis, den Rückruf gefährlicher Produkte hoheitlich anzuordnen, Verbraucher öffentlich vor gefährlichen Produkten zu warnen oder das Inverkehrbringen bestimmter gefährlicher Produkte zu untersagen). Gleichzeitig führt es auch zusätzliche Pflichten für die Hersteller ein. So etwa Informationspflichten gegenüber den Behörden, aber auch die Pflicht zum Vorhalten eines Rückrufmanagementsystems beim Vertrieb von Verbraucherprodukten.

Zunehmende Sensibilität ist im Zusammenhang mit produkthaftungsrechtlichen Fragen auch gegenüber den Vorgaben des **Strafrechts** erforderlich. Spätestens seit der bekannten „Lederspray-Entscheidung"[4] unterliegt es keinem Zweifel mehr, dass sich die Entscheidungsträger eines Unternehmens auch persönlich strafrechtlich für Produkthaftungsschäden zu verantworten haben. Und schließlich ist auch das **Versicherungsrecht** von großer Bedeutung in Produkthaftungs-Szenarien.

Neben den vorgenannten rechtlichen Fragen beinhaltet der proaktive Umgang mit Produkthaftungs-Themen aber natürlich noch eine weit größere Zahl von Faktoren im Unternehmen und verlangt zahlreiche eingespielte Prozesse quer durch das jeweilige Unternehmen.

---

[3] Text erhältlich u. a. über die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin.

[4] BGH v. 6.7.1990 – 2 StR 549/89, NJW 1990, 2560.

Ein proaktives Herangehen an „Produkthaftung“ im Unternehmen soll hier wie folgt gegliedert werden:

- Einhaltung produktspezifischer Vorschriften
- Vermeidung von Risiken aus dem Produkt
- Vermeidung von Schäden aus riskanten Produkten
- Vermeidung von Kosten aus Schäden
- Vermeidung persönlicher Verantwortlichkeit

2 Einhaltung produktspezifischer Vorschriften

In zahlreichen Vorschriften und Regelwerken sind detaillierte Vorgaben für die **Beschaffenheit** verschiedenster Produkte vorgegeben. Diese Vorgaben können unmittelbar verbindliche Wirkung besitzen, etwa in den zahlreichen und umfangreichen Verordnungen zum ProdSG, aber auch in zahlreichen sonstigen Einzelverordnungen und Nebengesetzen[5]. Die Feststellung, welche Regularien für ein bestimmtes Produkt jeweils gelten, ist einem externen Juristen oftmals nahezu unmöglich. Hier stehen technische Fragen sowie Besonderheiten einzelner Produktgattungen im Vordergrund, die meist nur von erfahrenen Inhouse-Beratern oder Branchenvertretern abschließend überblickt werden können. Neben verbindlichen (gesetzlichen) Vorgaben für die Beschaffenheit von Produkten sind auch „freiwillige“ Regelwerke wie DIN-Normen, Verbandsempfehlungen etc. von Bedeutung. Auch wenn diese keine direkte Zwangswirkung auf den Hersteller eines Produkts besitzen, können sie indirekt doch größte Bedeutung erfahren. Ein Produkt das nicht den vorgeschlagenen Sicherheitsstandard solcher Empfehlungen oder Normenkataloge aufweist, wird im Streitfalle nicht die erforderliche Sicherheit zugesprochen bekommen, mindestens aber die Beweislast für die Einhaltung der erforderlichen Sicherheitsstandards zulasten des Herstellers verschieben. Gleichzeitig kann das Abweichen von derartigen Standards in verschiedenen Konstellationen auch zum Verlust des Versicherungsschutzes führen.

Weiterhin sind auch Vorgaben für die vom Hersteller einzuhaltenden **Prozesse** zu beachten. Diese können Entwicklung und Erprobung der Produkte regeln. Besonders deutlich wird dies etwa im Arzneimittelzulassungsverfahren, wo detaillierteste Vorschriften die Prozesse im Vorfeld des Inverkehrbringens dieser Produktgattung regeln. Ähnliche Beispiele sind in anderen sehr sicherheitskritischen Produktbereichen zu finden (z. B. Flugzeugbau, Schienenverkehr, Nukleartechnik etc.). Auch hier ist neben direkt anwendbaren Gesetzen und Verordnungen die Bedeutung von Standards, Normen und Verbandsempfehlungen nicht zu unterschätzen.

[5] Vgl. die Auflistung des Bundesministeriums für Arbeit und Soziales, www.bmas.de, „Service“, „Gesetze“.

Vorgaben für Prozesse können sich auch auf Sicherheitsvorkehrungen beziehen; etwa oblag dem Arzneimittelgroßhandel bereits lange vor Erlass des ProdSG, eine Rechtspflicht zum Vorhalten eines Rückrufmanagementsystems.

3 Vermeidung von Risiken aus dem Produkt

Hersteller, Lieferanten, teils aber auch Importeure[6] sind sowohl zivilrechtlich als auch nach ProdSG verpflichtet, nur solche Produkte in den Verkehr zu bringen, die die vom Benutzer berechtigterweise zu erwartende Sicherheit aufweisen. Die hierfür erforderlichen Prozesse umfassen Entwicklung, Beschaffung, Produktion und Instruktion.

Entwicklung Proaktiv sollte ein Hersteller Qualität und Sicherheit stets bereits in sein Produkt hinein entwickeln (Prinzip der integrierten Sicherheit). Entscheidend ist, welche Sicherheit der Benutzer berechtigterweise erwarten darf. Auch wenn insoweit aktuell keine „amerikanischen Verhältnisse" drohen, ist doch stets auch ein zu erwartender Fehlgebrauch[7] der Produkte zu berücksichtigen. Die sorgfältige Entwicklung sollte dabei nicht nur als Durchgangsstation hin zur Herstellung sicherer Produkte verstanden werden. Sie ist auch als Kriterium an sich zu verstehen – und sorgfältig zu dokumentieren. Dies kann Bedeutung erlangen, um etwa im Schadensfall demonstrieren zu können, dass ein bestimmtes Risiko im Zeitpunkt der Entwicklung des Produkts noch nicht erkennbar war (z. B. Handy-Strahlung?). Weiterhin ist dies etwa für den Erhalt des Versicherungsschutzes zentral. In nahezu allen Rückruf-Policen ist die sogenannte „Experimentierklausel" enthalten. Danach besteht Versicherungsschutz nur dann, wenn das betreffende Produkt nach dem Stand von Wissenschaft und Technik entwickelt und erprobt wurde und nicht etwa unter dem Fangnetz einer Versicherungs-Police voreilig in den Markt gedrückt wurde.

Beschaffung Jeder Hersteller ist unter dem Gesichtspunkt der Produzentenhaftung verpflichtet, seine eigenen Vorlieferanten sorgfältig auszuwählen, zu überprüfen (auditieren?) und fortlaufend zu überwachen. Auch Versäumnisse in diesem Bereich können anderenfalls zu Schadensersatzansprüchen gegen den Hersteller führen.

Produktion Naturgemäß ist eine lückenlose Qualitätssicherung während des Fertigungsprozesses zur Vermeidung von Produkthaftungsansprüchen unabdingbar. Nur mit einer derart dokumentierten Produktion ist es überhaupt möglich, der Haftung für „Ausreißer", d. h. unverschuldeten und unvermeidbaren Einzelfällen,[8] entgehen zu können. Zugegebenermaßen gelingt dies in der Praxis aber selbst dann nur in Einzelfällen.

---

[6] Vgl. § 4 ProdHaftG; aber auch BGH v. 28.3.2006 – VI ZR 46/05, NJW 2006, 1589.

[7] BGH v. 12.11.1991 – VI ZR 7/91, BGHZ 116, 60, 65.

[8] Vgl. *Sprau*, in: Palandt, BGB, 72. Aufl. 2013, § 823 BGB, Rn. 170.

Instruktion Die umfassende und sorgfältige Instruktion der Benutzer eines Produkts über mögliche Risiken hieraus ist von großer Bedeutung. Allerdings kann auch sie nicht die gefährliche Konstruktion eines Produkts ausgleichen. Produkte müssen stets so konstruiert sein, dass sie im größtmöglichen Umfang Risiken von vornherein vermeiden. Der bloße Warnhinweis auf konstruktiv vermeidbare Risiken führt im Regelfall nicht zu einer Enthaftung des Herstellers.[9] Richtige Instruktion klärt darüber auf, i) welches Verhalten gefährlich ist, ii) was hierdurch passieren kann und iii) welche Schäden dem Nutzer daraus drohen. Wichtig ist, dass der Hersteller den Erhalt dieser Hinweise beim Kunden im Streitfall auch nachweisen kann. Die Hinweise müssen jeweils in der betreffenden Landessprache erfolgen.[10] Bei schwerwiegenden Risiken müssen diese auch am Produkt selbst angebracht sein und nicht lediglich in einer beigefügten Bedienungs- oder Betriebsanleitung. Oft sind hier auch Aufkleber mit Gefahrensymbolen, Piktogrammen etc. nach Maßgabe einschlägiger Vorschriften und Standards zu deren Gestaltung erforderlich. Zur Vermeidung von Gewährleistungsansprüchen sollte dabei auch auf Schäden hingewiesen werden, die zwar nicht dem Nutzer, aber dem jeweiligen Produkt drohen, wenn es in bestimmter Weise eingesetzt wird.

4 Vermeidung von Schäden aus riskanten Produkten

Produktbeobachtung Nach den Grundsätzen der Produzentenhaftung ist der Hersteller eines Produkts auch nach Inverkehrbringen des Produkts verpflichtet, sein Produkt „im Auge zu behalten". Dies gilt nach der bekannt gewordenen „Honda-Entscheidung"[11] nicht nur für das eigene Produkt, sondern auch für typischerweise damit gemeinsam verwendete Produkte Dritter (z. B. Accessoires, Zubehör etc.). Neben dieser Rechtspflicht ist es auch zur Vermeidung von teuren Schäden bzw. persönlicher Verantwortlichkeit ratsam, in jedem Unternehmen ein entsprechendes Beschwerdemonitoring einzurichten. Viele Schadensfälle wären vermeidbar gewesen, hätten die betroffenen Unternehmen ihren Kunden besser zugehört. Nicht nur ist es der Kundenbindung und dem Image eines Unternehmens abträglich, wenn dieses erst lange nach Auftreten entsprechender Diskussionsforen im Internet auf eine Produktkrise reagiert. Es kann darüber hinaus auch strafrechtliche Folgen haben, wenn ein Unternehmen erkennbare Risiken nicht oder zu spät beseitigt. Problematisch ist hierbei, dass die strafrechtliche Rechtsprechung das Bestehen einer Rückrufpflicht bei Gefahren für Leib und Leben der Benutzer bislang unterstellt – und z. B. eine Strafbarkeit wegen Körperverletzung durch Unterlassen annimmt, wird in dieser Situation kein Rückruf vorgenommen –, während die zivilrechtliche Rechtsprechung um die Konturen

[9] *Foerste*, in: Graf von Westphalen (Hrsg.), Produkthaftungshandbuch 3. Aufl. 2012, § 24 Rn. 127.

[10] ebd., Rn. 208.

[11] BGH v. 9.12.1986 – VI ZR 65/86, NJW 1987, 1009, 1010 f.

der Voraussetzungen und Inhalte einer Rückrufpflicht ringt.[12] Obendrein droht auch hier wieder der Verlust des Versicherungsschutzes, wenn ein Unternehmen Produkte unverändert auf den Markt liefert, während gleichzeitig bereits Erkenntnisse vorhanden sind, dass hier Sicherheitsrisiken bestehen können.

Die Installation eines schlüssigen Beschwerdemonitorings beinhaltet einige zu beachtende Kriterien, etwa zur Besetzung eines entsprechenden Gremiums, der Kriterien zur Auswertung erhaltener Informationen, Entscheidungs- und Eskalationskriterien etc. Neben einigen wenigen rechtlichen Fragen sind hier in erster Linie sichere Prozesse, also organisatorische Fragen entscheidend.

Rückrufmanagement Die proaktive Installation eines Rückrufmanagements ist für eine große Zahl von Unternehmen bereits heute gesetzliche Rechtspflicht. Dies gilt nach § 6 Abs. 2 ProdSG insbesondere für Hersteller von Verbraucherprodukten im Sinne des ProdSG (§ 2 Nr. 26 ProdSG). Auch für alle anderen Hersteller von Produkten ist es jedoch im eigenen Interesse sehr ratsam, um nicht im Falle einer Produktkrise die Handlungsfähigkeit zu verlieren, sondern gegenüber Anspruchstellern, Presse, Behörden und anderen gewappnet zu sein. Kriterien, die hier in noch stärkerem Maße als beim Beschwerdemonitoring zu berücksichtigen sind, sind die Zusammensetzung eines entsprechenden Gremiums, Personen, Kontaktdetails, Stellvertretungsregelungen etc.; Definition der Entscheidungskriterien; Kanäle der Informationsbeschaffung intern und extern (z. B. technische Analysefähigkeit, Rückverfolgbarkeit, Vertriebskanäle etc.); Kommunikationsregeln; Einbindung von Behörden; Pressearbeit, Rechtsberatung; Regeln zur Dokumentation der Entscheidungsfindung im Krisenfall etc.

Am Ende muss hier eine fundierte Entscheidung über einen möglichen Rückruf oder einen Warnhinweis stehen, diese rasch und effizient umgesetzt werden, gleichzeitig die Anspruchswahrung gegenüber Vorlieferanten und Versicherung gewahrt sein und möglichen Ansprüchen Geschädigter nicht unnötig Tür und Tor geöffnet werden.

5 Vermeidung von Kosten aus Schäden

Vertragliche Haftungsbegrenzung im Verkauf Vertragliche Haftungsbeschränkungen entfalten nur Wirkung gegenüber dem Vertragspartner. Erleidet ein außenstehender Dritter aufgrund eines Produktfehlers einen Schaden und kann er aufgrund dessen von dem Hersteller Schadensersatz nach Deliktsrecht bzw. dem Produkthaftungsgesetz verlangen, spielen hierbei Haftungsbegrenzungen, die der Hersteller mit seinem Vertragspartner vereinbart hat, keine Rolle – der Dritte muss sich diese nicht entgegenhalten lassen.

[12] vgl. die „Pflegebetten-Entscheidung“: BGH v. 16.12.2008 – VI ZR 170/07, NJW 2009, 1080 und die hierzu ergangenen Kommentierungen im Schrifttum.

Für den Hersteller eines Produkts ist die zivilrechtlich vorgesehene Haftung so klar wie ungünstig. Bei einem Produktfehler wird nicht nur Mangelbeseitigung geschuldet, sondern darüber hinaus auch der Höhe nach unbegrenzt auf den Ersatz sämtlicher Schäden einschließlich entgangenen Gewinns gehaftet. Dies resultiert daraus, dass der Hersteller – anders als der Händler – den Produktfehler regelmäßig verursacht hat und damit bei ihm das für die Verpflichtung zum Schadensersatz erforderliche Verschulden vorliegt.

Im Interesse eines effektiven Risk Managements sollte daher nach Möglichkeit die gesetzlich vorgesehene Haftung aus Gewährleistung vertraglich eingegrenzt werden. Ideal sind hier natürlich zunächst **individualvertragliche Haftungsbeschränkungen**, z. B.

- Haftung auf Schadensersatz nur bei Vorsatz und grober Fahrlässigkeit (auch individualvertraglich kann die Haftung für den eigenen Vorsatz nicht ausgeschlossen werden, § 276 Abs. 3 BGB. Gleiches gilt für die zwingende Haftung eines Herstellers nach dem Produkthaftungsgesetz.)
- Haftung nur für Schäden am Produkt selbst/keine Haftung auf entgangenen Gewinn
- Verkürzung der gesetzlich vorgesehenen Gewährleistungsfristen

Derartige Vereinbarungen bieten sich vor allem bei größeren Projekten mit hohem Haftungsrisiko an.

Im Übrigen sollte bei Vertragsschluss auf die eigenen **allgemeinen Verkaufsbedingungen** mit passenden Haftungsbeschränkungen verwiesen werden. Hierbei muss man sich jedoch über folgendes im Klaren sein:

In AGB sind Haftungsbeschränkungen nur in weit geringerem Rahmen zulässig als bei Individualvereinbarungen. Unzulässig sind Haftungsbeschränkungen bei

- Verletzung von Leben, Körper und Gesundheit, § 309 Nr. 7a BGB[13]
- grob fahrlässiger Pflichtverletzung durch den AGB-Verwender, vorsätzlich oder grob fahrlässige Pflichtverletzung des gesetzlichen Vertreters oder Erfüllungsgehilfen, § 309 Nr. 7b BGB
- auch bei einfacher Fahrlässigkeit nur sehr eingeschränkt bei der Verletzung einer sog. Kardinalpflicht[14], d. h. einer Pflicht, deren ordnungsgemäße Erfüllung die Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Vertragspartner vertraut und regelmäßig vertrauen darf.

Soweit der Kunde bei Vertragsschluss auf seine allgemeinen Einkaufsbedingungen mit für ihn günstigen Haftungsregelungen verweist, finden die sich widersprechenden AGB

[13] Dies gilt auch bei Verkürzung der Verjährungsfristen; BGH v. 15.11.2006 – VIII ZR 3/06, NJW 2007, 674.

[14] Vgl. z. B. BGH v. 20.7.2005 – VIII ZR 121/04, NJW-RR 2005, 1496 ff.

keine Anwendung und es bleibt damit bei der für den Verkäufer ungünstigen gesetzlichen Regelung.[15]

Befindet sich der Kunde in einer starken Verhandlungsposition, werden von ihm regelmäßig weder die AGB des Lieferanten, geschweige denn die vorstehenden individualvertraglichen Haftungsbeschränkungen akzeptiert. So ist es im Automotive-Bereich vielmehr üblich, dass von Seiten des OEM gegenüber seinen Zulieferern auf Klauseln bestanden wird, die das Haftungsrisiko sogar noch über das gesetzliche Maß hinaus ausweiten (z. B. Verlängerung der Gewährleistungsfristen von 24 auf bis zu 60 Monaten oder aber Möglichkeit der Durchführung eines Produktrückrufs auf Kosten des Zulieferers nach freiem Ermessen). Hier bietet sich eine andere Möglichkeit an, das eigene Haftungsrisiko sachgerecht zu begrenzen, nämlich die **Risikominimierung durch sachgerechte Leistungsbeschreibung**. Ein Produktfehler, der zu einer Haftung aus Vertrag führen kann, liegt grundsätzlich nur dann vor, wenn das gelieferte Produkt von der vertraglich vereinbarten Beschaffenheit abweicht (§ 434 Abs. 1 BGB). Eine effektive Risikominimierung kann der Hersteller gegenüber dem Kunden also auch schon dadurch erreichen, dass er bei Vertragsschluss sachgerecht bzw. zurückhaltend/vorsichtig festlegt

- was sein Produkt kann und was es nicht kann
- unter welchen Bedingungen sein Produkt die angegebene Leistung erbringt
- welche äußeren Einflüsse/sonstigen Faktoren negativen Einfluss auf das Produkt haben.

Einschränkungen in dieser Hinsicht stoßen erfahrungsgemäß auch bei einem verhandlungsstarken Gegenüber auf deutlich mehr Verständnis als der Wunsch nach haftungsbeschränkenden Klauseln.

Aber Achtung: Auch wenn der Lieferant eines gefahrstiftenden Einzelteils auf diese Weise seine vertragliche Haftung gegenüber seinem Kunden, etwa dem Hersteller des Endprodukts, erfolgreich beschränkt, bedeutet dies nicht gleichzeitig, dass er aus seiner Lieferung gegenüber einem geschädigten Benutzer des Endprodukts nicht doch auf Grundlage des Deliktsrechts haften kann. Zwar ist es in der Praxis eher selten, dass ein geschädigter Endkunde nicht gegen den Hersteller des Gesamtprodukts, sondern gegen dessen Vorlieferanten vorgeht. Ist dies allerdings doch einmal der Fall, so nützt dem Vorlieferanten seine vertragliche Haftungsbeschränkung gegenüber dem geschädigten Dritten nichts. Insoweit kann er seine Haftung nur dadurch beschränken – von der eher theoretischen Möglichkeit einer vertraglichen Freistellung durch den Hersteller einmal abgesehen –, dass er es ablehnt, ein von ihm als gefahrstiftend erkanntes Teil zu liefern.

Vertragliche Regresswahrung im Einkauf Die allgemeinen Einkaufsbedingungen müssen das im Verkauf übernommene Risiko widerspiegeln. Der haftungsrechtliche „Worst case" für den Hersteller eines Produkts ist es, dass er gegenüber dem Kunden aufgrund der Verantwortlichkeit für das Endprodukt für einen Fehler einzustehen hat, der durch

[15] z. B. BGH v. 23.1.1991 – VIII ZR 122/90, NJW 1991, 1606.

ein Zulieferteil verursacht wurde, er selbst aber bei dem Zulieferer keinen Regress nehmen kann. Im Rahmen des Einkaufs sollte daher sichergestellt werden, dass die Haftung der eigenen Zulieferer nicht hinter dem zurückbleibt, was man selbst dem Kunden gegenüber als Haftung übernommen hat. Dies macht eine enge Abstimmung zwischen Ein- und Verkauf erforderlich. Muss dem Kunden beispielsweise eine Verjährungsfrist von 48 Monaten für Sachmängel ab Ablieferung der Ware beim Kunden gewährt werden, so sollte darauf gedrängt werden, dass die Verjährungsfrist für den Zulieferer ebenfalls nicht vorher endet.

Vorsicht Im Einzelfall ist eine lückenlose Absicherung wichtig. Es wäre im vorgenannten Beispiel nicht ausreichend, selbst wiederum eine Verjährungsfrist von 48 Monaten ab Ablieferung durch den Zulieferer zu vereinbaren. Zwischen Anlieferung des Zulieferteils und Ablieferung des Endprodukts liegt häufig ein nicht unerheblicher Zeitraum. Dies gilt oft selbst bei just-in-time Belieferung. Die Verjährungsfrist beginnt also für den Zulieferer gegenüber dem Hersteller früher als die Frist für den Hersteller gegenüber dem Endkunden.

Mögliche Vorgehensweise Der Zulieferer wird bei Vertragsschluss dazu verpflichtet, die Einkaufsbedingungen des Endkunden zu akzeptieren und in dem gleichen Umfang zu haften, wie der Hersteller gegenüber dem Endkunden verantwortlich ist.

Soweit günstigere Individualvereinbarungen nicht durchsetzbar oder eine detaillierte Verhandlung der Konditionen (z. B. im Hinblick auf ein begrenztes Auftragsvolumen) nicht angebracht ist, sollte streng auf eine **wirksame Einbeziehung der eigenen allgemeinen Einkaufsbedingungen** geachtet werden – dies allein schon deshalb, damit nicht ansonsten die allgemeinen Verkaufsbedingungen des Vertragspartners zur Anwendung kommen.

Vorsicht Im inländischen Geschäftsverkehr zwischen Unternehmern reicht es für die wirksame Einbeziehung der allgemeinen Geschäftsbedingungen in das Angebot aus, dass auf diese allgemein im Bestellschreiben verwiesen wird und die Gegenseite die Möglichkeit der Kenntnisnahme hat (z. B. durch Anfrage beim Vertragspartner oder durch Download von der Homepage des Bestellers).[16] Im grenzüberschreitenden Rechtsverkehr ist dies anders. Hier müssen dem Empfänger die AGB übersandt oder anderweitig zugänglich gemacht werden – es besteht also eine „Übermittlungspflicht" des Verwenders statt einer „Anforderungsobliegenheit" des Empfängers.[17] Zudem müssen die AGB in der Vertragssprache übermittelt werden.[18] Wird also zwischen den Parteien in englischer Sprache korrespondiert, reicht es nicht aus, die deutschsprachigen Einkaufsbedingungen dem Bestellschreiben beizufügen.

[16] BGH v. 30.6.1976 – VIII ZR 267/75, NJW 1976, 1886; BGH v. 3.2.1982– VIII ZR 316/80, NJW 1982, 1750.

[17] BGH v. 31.10.2001 – VIII ZR 60/01, NJW 2002, 370 ff.

[18] Hanseatisches Oberlandesgericht v. 1.6.1979 – 11 U 32/79, NJW 1980, 1232, 1233.

„To do's" zur Sicherstellung der richtigen Vorgehensweise in der Praxis – „Prozessqualität sichert Produktqualität":

Die Umsetzung der vorgenannten Punkte obliegt in der Praxis den Mitarbeitern der Ein- und Verkaufsabteilung. Diese sollten entsprechend geschult und für mögliche Probleme in rechtlicher Hinsicht sensibilisiert werden.

Im Hinblick darauf, dass gerade die Rechtsprechung zu allgemeinen Geschäftsbedingungen sehr komplex und immer noch im Fluss ist, ist es zudem ratsam, die eigenen AGB in regelmäßigen Abständen auf Änderungsbedarf hin überprüfen zu lassen. Die Rechtsprechung gewährt hier auch keinen „Bestandsschutz" für AGB, die bei Vertragsschluss noch als wirksam angesehen wurden, wenn sich zu einem späteren Zeitpunkt die Rechtsprechung ändert.[19] Im Übrigen kann es sich auch anbieten, interne Regularien aufzustellen die festlegen, welches Haftungsrisiko bei Vertragsschluss akzeptiert werden darf und welches nicht – bzw. der Genehmigung durch die Geschäftsführung bedarf.

Die Auswahl geeigneten **Versicherungsschutzes,** zugeschnitten auf die Produkte und die Vertriebswege des jeweiligen Unternehmens, sollte mit fachkundiger Beratung erfolgen. Hier sollten stets versierte Versicherungsmakler mit herangezogen werden. Die verschiedenen Möglichkeiten des Versicherungsschutzes (z. B. First Party/Third Party Recall) haben schon des Öfteren im Schadensfall für Überraschungen gesorgt. Gleichzeitig muss sichergestellt sein, dass der vorgehaltene Versicherungsschutz auch dem entspricht, wozu sich Lieferanten gegenüber ihren Kunden oft vertraglich verpflichten mussten.

Faktische Haftungsabwehr/faktische Regresswahrung Einige Punkte, die in diesem Zusammenhang unbedingt beachtet werden müssen: Wichtig ist die Rückverfolgbarkeit schadhafter Teile, Chargen, Lieferlose sowohl im Verhältnis zu Vorlieferanten als auch gegenüber Kunden. Die rechtzeitige Mängelrüge im Sinne von § 377 HGB muss unbedingt eingehalten werden. Im Rückruffall muss in jedem Fall auch eine umfangreiche und dokumentierte Beweissicherung stattfinden. Gemeinsam mit den Rechtsberatern sollte geklärt werden, ob dies im Rahmen eines selbständigen Beweisverfahrens stattfinden soll. In jedem Falle Aufbewahrung getauschter Teile für möglichen späteren Regressprozess. Dokumentation angefallener Kosten für Rückruf oder andere Feldmaßnahmen von Anfang an aufgeteilt nach den Vorgaben rechtlicher Durchsetzbarkeit verschiedener Schadenspositionen, weil sich dies später nie wieder aufgliedern lässt.

Bewusste Entscheidung über schriftliche Dokumentation im Krisenfalle unter Berücksichtigung eines möglichen Zugriffs von außen auf diese Dokumente (z. B. US-Pre-Trial-Discovery). Zahlungen stets nur unter Vorbehalt (faktisches Anerkenntnisverbot!).

6 Vermeidung persönlicher Verantwortlichkeit

Eine **zivilrechtliche Haftung** der handelnden Personen in einem Unternehmen gegenüber Dritten stellt grundsätzlich die Ausnahme dar. Dies gilt jedenfalls dann, wenn das Unternehmen als juristische Person (z. B. GmbH, AG) organisiert ist und die betreffenden

[19] BGH v. 5.3.2008 – VIII ZR 95/07, NJW 2008, 1438.

Mitarbeiter und Entscheidungsträger ausdrücklich nicht im eigenen Namen, sondern für das Unternehmen handeln. Es ist das Wesen des Handelns für eine juristische Person, dass dessen Folgen nur das Unternehmen und nicht die handelnden Personen selbst treffen. Von diesem Grundsatz gibt es jedoch Ausnahmen („Piercing the corporate veil"):

Eine Haftung gegenüber außenstehenden Dritten kann etwa nach Deliktsrecht dann erfolgen, wenn der betreffende Entscheidungsträger durch sein Handeln – mag dies auch für das betroffene Unternehmen erfolgt sein – schuldhaft absolute Rechte Dritter verletzt.[20] Hierbei kann es sich um Eigentumsverletzungen, aber auch um die Verletzung von Leben oder Gesundheit handeln. Voraussetzung hierfür ist es jedoch, dass etwa ein Geschäftsführer durch sein Handeln sämtliche Tatbestandsvoraussetzungen einer unerlaubten Handlung (§ 823 BGB) in seiner Person verwirklicht. Eine persönliche Haftung nach Deliktsrecht kommt aber nach § 823 Absatz 2 BGB auch dann in Betracht, wenn der Geschäftsführer durch sein Handeln gegen eines der dort in Bezug genommenen Schutzgesetze verstößt. Dies ist insbesondere bei strafrechtlich relevantem Handeln der Fall (z. B. fahrlässige Körperverletzung oder Tötung durch Unterlassung). Desweiteren kann dies auch bei Verstößen gegen Produktsicherheitsrecht der Fall sein.[21] Andere Fallgruppen der persönlichen Haftung gegenüber Dritten, wie etwa der Inanspruchnahme besonderen persönlichen Vertrauens, spielen im Bereich der Produkthaftung üblicherweise keine Rolle.

Eine **zivilrechtliche Haftung** gegenüber der Gesellschaft kann dagegen auf Grundlage der gesetzlichen Vorschrift in § 43 GmbHG (für Geschäftsführer einer GmbH), von § 93 AktienG (für Vorstände einer AG) oder auf Grundlage des jeweiligen Anstellungsvertrages (für sonstige Mitarbeiter) vergleichsweise leichter erfolgen. Wenn hier auch stets die Besonderheiten des jeweiligen Einzelfalls zu berücksichtigen sind, ist doch das jeweilige Organ/der jeweilige Mitarbeiter der betroffenen Gesellschaft verpflichtet, gegenüber der Gesellschaft deren Interessen zu wahren und Schäden von der Gesellschaft abzuwenden. Hier mag es durchaus im Einzelfall Zielkonflikte geben, wenn es etwa darum geht, die oft nicht unbeträchtlichen Kosten eines Produktrückrufs gegenüber den im Worst Case deutlich höheren aber im Zeitpunkt der Entscheidungsfindung nur hypothetisch zu bewertenden Kosten eingetretener Schadensfälle gegeneinander abzuwägen. Allerdings dürfte hier im Zweifel die in jedem Fall bestehende Pflicht der Gesellschaft, sich rechtskonform zu verhalten, eine wichtige Entscheidungshilfe für die betroffenen Geschäftsführer, Vorstände oder Mitarbeiter sein.

Eine **strafrechtliche Verantwortlichkeit** der Entscheidungsträger eines Unternehmens muss spätestens seit der „Lederspray-Entscheidung" des Bundesgerichtshofs als ernst zu nehmende Gefahr betrachtet werden und kann nicht mehr als eher theoretische Problematik abgetan werden. Im Bereich der Produkthaftung drohen hier persönliche Verantwortlichkeiten im Bereich der fahrlässigen Körperverletzung oder Tötung durch Unterlassen. Dies kann etwa dann eintreten, wenn die Entscheidungsträger eines Unternehmens von einer ernstzunehmenden Gefahr für die Benutzer eines Produkts aus

[20] BGH v. 5.12.1989 – VI ZR 335/88, BGHZ 109, 297, 302.

[21] BGH v. 28.3.2006 – VI ZR 46/05, NJW 2006, 1589.

Sicherheitsmängeln wissen und dennoch untätig bleiben. Der Unterlassungsvorwurf kann dabei zweierlei Stoßrichtungen haben: i) es unterlassen zu haben, das Produkt aus dem Verkehr zu nehmen und es in Kenntnis der Sicherheitsrisiken weiter hergestellt und vertrieben zu haben sowie ii) es unterlassen zu haben, die bereits im Markt befindlichen Produkte zurückzurufen bzw. einen Warnhinweis an die Benutzer zu verbreiten.

Um sich sowohl hinsichtlich einer zivilrechtlichen Verantwortlichkeit, als auch hinsichtlich einer strafrechtlichen Verantwortlichkeit im Rahmen des Möglichen abzusichern, ist es von entscheidender Bedeutung, dass die Entscheidungsträger des Unternehmens ein stringentes System der **Delegation** einrichten. Im Bereich der Produkthaftung setzt dies schlüssige Prozesse für Entwicklung, Beschaffung, Produktion und Instruktion voraus; weiterhin aber auch für Produktbeobachtung und Rückrufmanagement. Um hier in den Genuss einer möglichen Enthaftung zu kommen, müssen diese Prozesse aber nicht nur theoretisch vorgegeben sein. Sie müssen vielmehr tatsächlich erfolgreich implementiert werden. Dies beinhaltet, dass die betroffenen Mitarbeiter sorgfältig ausgewählt werden, fortlaufend geschult aber auch kontrolliert werden.[22] Nur ein solches in sich geschlossenes System kann für das Management eines Unternehmens dazu führen, dass im Falle von dennoch auftretenden Schäden keine persönliche Verantwortlichkeit der Entscheidungsträger vorliegt.

Wichtig ist, dass etwa einzelne Mitglieder eines Geschäftsführungsgremiums sich nicht darauf berufen können, dass die Verantwortung gemäß der internen Geschäftsverteilung nicht in ihr Ressort fällt. Im Falle erkannter Risiken ist – wie auch bei anderen Compliance-Fragen – eine Verantwortlichkeit des Gesamtgremiums Geschäftsführung bzw. Vorstand anzunehmen.[23] Jedes einzelne Mitglied des Unternehmensmanagements muss daher die in seiner Macht stehenden Schritte zur Vermeidung von Schäden ergreifen, um einer persönlichen Verantwortlichkeit entgehen zu können.

[22] Vgl. *Schneider,* in: Scholz, GmbHG, Bd. 2, 10. Aufl. 2007, § 43 Rn. 41.

[23] ebd., Rn. 39.

Compliance bei M&A-Transaktionen

Christofer Rudolf Mellert

Inhaltsverzeichnis

Zusammenfassung

Im Rahmen der aktuellen Compliance Diskussion wird der Bereich der M&A-Transaktionen oftmals ausgespart. Dies geschieht – wie die nachfolgenden Ausführungen zeigen werden – zu Unrecht, haben doch die involvierten Parteien selbstverständlich auch bei der Durchführung derartiger Transaktionen sicherzustellen, dass nicht gegen geltendes Recht verstoßen wird.[1]

Ein Bereich, in dem dies in besonderem Maße sicherzustellen ist, ist die Due Diligence, d. h. die Untersuchung des zu erwerbenden Unternehmens durch den Käufer.[2]

[1] Hierzu existieren auch Compliance Checklisten, z. B. *Fietz*, in: Umnuß, Corporate-Compliance Checklisten, 2. Aufl. 2012.

[2] *Werner,* GmbHR 2007, 678; allgemein zur Due Diligence: *Berens/Brauner/Strauch*, Due Diligence bei Unternehmensakquisitionen, 6. Aufl. 2011.

C. R. Mellert (✉)
Graf-Adolf-Platz 15, 40213 Düsseldorf, Deutschland
E-Mail: christofer.mellert@luther-lawfirm.com

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2_4,

Hintergrund einer solchen Due Diligence ist die Schaffung einer Basis für die Entscheidung über den Kauf. Damit ist eine Due Diligence zum einen dem Bereich der Sorgfaltspflichten der Geschäftsleitung (Vorstand, Aufsichtsrat und Geschäftsführung) des Käufers zuzuordnen. Zum anderen stellt sich für den Verkäufer bei der Due Diligence die Frage, welche Informationen er ohne Verstoß gegen geltendes Recht oder gegen Vereinbarungen mit Dritten offen legen darf.

Auch in Bezug auf die Vertraulichkeit bei M&A-Transaktionen sollte ein Unternehmen über ein entsprechendes Compliance Management verfügen. M&A-Transaktionen unterliegen meist einer sehr hohen Vertraulichkeitsstufe. Bei den beteiligten Unternehmen ist in der Regel nur ein kleiner Personenkreis über die Transaktion und ihre Details informiert. Üblicherweise sind dies die Geschäftsleitung sowie Mitarbeiter der M&A-Abteilung, der Steuerabteilung, des Controlling und der Rechtsabteilung. Bei komplexeren Transaktionen sind diesem Personenkreis noch die externen Berater, d. h. im Allgemeinen Rechtsanwälte, Steuerberater, M&A-Berater etc. hinzuzurechnen. Hierbei gilt es zum einen, das nachteilige Durchsickern von Informationen aus verhandlungstaktischen Gründen oder um das Bekanntwerden von Betriebsgeheimnissen am Markt zu vermeiden. Zum anderen kann Vertraulichkeit auch gesetzlich angeordnet sein, etwa in Bezug auf Insider-Informationen bei börsennotierten Unternehmen.[3] Daneben werden häufig vertragliche Vertraulichkeitsverpflichtungen (mit oder ohne Vertragsstrafen) mit Drittparteien (z. B. Kunden des Zielunternehmens) abgeschlossen, deren Bestimmungen es ebenfalls einzuhalten gilt.

Daneben ist die Einhaltung nationaler und EU-rechtlicher Kartellvorschriften zwingend zu beachten, da ansonsten hohe Bußgelder und die zivilrechtliche Unwirksamkeit der Transaktion drohen.

Schließlich drängt sich die Frage nach einer spezifischen Compliance Due Diligence förmlich auf, bei der das Zielunternehmen auf das Vorhandensein und die Leistungsfähigkeit der Compliance-Organisation des Zielunternehmens überprüft bzw. die Kompatibilität dieser Compliance-Organisation mit der eigenen bewertet wird. Andere typische Compliance-Themen wie Korruptions- und Schmiergeldtatbestände sind in diesem Zusammenhang ebenfalls zu prüfen, wobei dies – zumindest teilweise – im Rahmen der Financial bzw. Legal Due Diligence erledigt werden kann.

1 Due Diligence als Bestandteil der unternehmerischen Sorgfalt

Die Geschäftsleitung des kaufinteressierten Unternehmens hat die Entscheidung zu treffen, ob das Zielunternehmen gekauft wird oder nicht und trägt insoweit für diese Entscheidung auch die Verantwortung. Vor diesem Hintergrund ist sicherzustellen, dass den gesetzlichen

[3] Zur Weitergabe von Insiderinformationen bei M&A-Transaktionen mit börsennotierten Aktiengesell schaften: *Hasselbach,* NZG 2004, 1087 ff.

Vorgaben für solche Entscheidungen entsprochen wird, um eine persönliche Haftung der Geschäftsleiter zu verhindern.

Dem Vorstand einer AG steht bei Ausübung seiner Unternehmensleitungsfunktion bei unternehmerischen Entscheidungen ein weitreichender, gerichtlich nicht überprüfbarer Ermessensspielraum zu.[4] Ähnliches gilt für den Geschäftsführer einer GmbH, solange er sich nicht am Willen der Gesellschafter zu orientieren hat.[5]

Dieses unternehmerische Ermessen ist jedoch insoweit eingeschränkt, als dass der Geschäftsleiter seine Entscheidung nicht ins Blaue hinein treffen darf. Die Entscheidung ist vielmehr auf Basis ausreichender Informationen und Außerachtlassung sachfremder Erwägungen und Eigeninteressen zu treffen. Eine Pflichtverletzung liegt daher solange nicht vor, wie das Vorstands- bzw. Geschäftsführungsmitglied bei seiner Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln.

Speziell für Unternehmenskäufe bedeutet dies, dass der Geschäftsleiter die Zielgesellschaft vor Erwerb mehr oder weniger umfassend zu prüfen hat, um sich ein Bild über diese zu verschaffen und etwaige Risiken zu erkennen. Das übliche Verfahren für eine solche Prüfung ist die aus dem anglo-amerikanischen Rechtskreis stammende Due Diligence. Ob eine solche heute bereits kraft Verkehrssitte etabliert ist, so dass der Verzicht auf eine solche Prüfung im Zweifelsfall einen Sorgfaltsverstoß indiziert, ist umstritten.[6] Vereinzelte Gerichtsurteile lassen jedoch einen Trend der Rechtsprechung hin zu einer Haftungsverschärfung für die Geschäftsleitungsmitglieder insgesamt erkennen, was sich auch im Bereich der Due Diligence auswirkt.[7] So lässt sich einem Urteil des OLG Oldenburg entnehmen, dass das Unterlassen einer Due Diligence beim Unternehmenskauf durch die Geschäftsführung des kaufenden Unternehmens eine Sorgfaltspflichtverletzung darstellen kann. Wörtlich heißt es im Leitsatz 2:

> Das dem Geschäftsführer bei unternehmerischen Entscheidungen zuzubilligende weite Ermessen ist beim Erwerb eines anderen Unternehmens (hier eines weiteren Klinikbetriebs) beschnitten, wenn die Grundlagen, Chancen und Risiken der Investitionsentscheidung nicht ausreichend aufgeklärt worden sind. Zumindest dann, wenn nicht ausreichende, gesicherte Erkenntnisse über das zu erwerbende Unternehmen vorhanden sind oder wenn vorhandene Informationen Unklarheiten aufweisen, wird eine umfassende Due Diligence durchzuführen sein. Wird dies unterlassen, kommt bei einer zu erheblichen Verlusten führenden Fehlinvestition eine Geschäftsführerhaftung in Betracht. (OLG Oldenburg v. 22.06.2006 – 1 K 34/03, NZG 2007, 434 ff.)

Eine Pflicht zur Durchführung einer Due Diligence ist allerdings abhängig von der tatsächlichen Möglichkeit der Durchführung. Eine umfassende Due Diligence kann etwa dann

---

[4] BGH v. 21.4.1997 – II ZR 175/95, BGHZ 135, 244, 253 (ARAG-Garmenbeck-Entscheidung).

[5] *Lutter,* GmbHR 2000, 301, 306.

[6] *Werner*, GmbHR 2007, 678, 679 m. w. N. in Fn. 19; nicht zielführend ist in diesem Zusammenhang die nicht fundierte Feststellung bei *Peemöller/Reinel-Neumann*, BB 2009, 206, 207, wonach der Verzicht auf eine Due Diligence grundsätzlich eine fahrlässige Pflichtverletzung der Geschäftsleitung sei.

[7] LG Frankfurt a. M. v. 7.10.1997 – 3/11 O 44/96, WM 1998, 1181, 1185.

nicht durchgeführt werden, wenn das Management des Zielunternehmens die Herausgabe relevanter Informationen ganz oder teilweise verweigert (so z. B. bei börsennotierten Unternehmen nicht unüblich bzw. gesetzlich gefordert oder auch beim Verkauf durch einen Insolvenzverwalter, der ggf. nicht über alle relevanten Informationen verfügt). In einem solchen Fall kann dennoch die Entscheidung zum Erwerb des entsprechenden Unternehmens im Rahmen des unternehmerischen Ermessenspielraums liegen. In einem solchen Fall müssen dann etwaige Risiken durch weitreichende Garantien oder Freistellungsverpflichtungen des Verkäufers abgedeckt werden**.** Ist selbst dies nicht möglich, kann eine Due Diligence aber auch dann entbehrlich sein, wenn etwaige Risiken bereits bei der Höhe des Kaufpreises berücksichtigt sind, d. h. der Kaufpreis entsprechend vermindert ist.[8]

2 Grenzen der Zurverfügungstellung von Informationen in der Due Diligence

Im Rahmen der Durchführung einer Due Diligence stellen sich rechtliche Fragen jedoch auch auf Seiten des Verkäufers und des Zielunternehmens. Insofern geht es hier mehr um die Frage der Zulässigkeit der Zurverfügungstellung von Informationen,[9] als um etwaige Pflichten des Verkäufers, d. h. der Gesellschafter des zu verkaufenden Unternehmens selbst.

Grundsätzlich gilt für einen Geschäftsführer oder ein Mitglied des Vorstandes, dass vertrauliche Informationen, die das Unternehmen betreffen, Dritten nicht zugänglich gemacht werden dürfen, wenn dies dem Interesse des Unternehmens widerspricht.[10] Das gilt im Prinzip auch bei einer Due Diligence. Jedenfalls in Konstellationen, in denen die Person des Gesellschafters eines Unternehmens irrelevant oder in Bezug auf den potentiellen Erwerber für das Zielunternehmen sogar nachteilig ist, dürfte daher der Geschäftsführer des Zielunternehmens grundsätzlich überhaupt keine vertraulichen Informationen im Rahmen einer Due Diligence zur Verfügung stellen.[11] Dies gilt insbesondere in Fällen, in denen der Erwerber ein Wettbewerber des kaufgegenständlichen Unternehmens ist.[12] Bei der GmbH lässt sich dieses Verbot jedoch im Allgemeinen durch eine – rechtmäßige – Weisung der Gesellschafterversammlung aushebeln.[13] Ein Mehrheitsgesellschafter als

[8] So geben Insolvenzverwalter üblicherweise nur ganz wenige Garantien ab, so dass der Käufer diesen Umstand einpreisen muss.

[9] *Liese*, DB 2010, 1806 ff. *Rittmeister,* NZG 2004, 1032 ff.

[10] Für den Vorstand einer AG siehe *Thiel* in: Semler/Volhard, Arbeitshandbuch für Unternehmensübernahmen Bd. 2, 2003, § 54 Rn. 41; für den GmbH- Geschäftsführer siehe *Dietzel* in: Semler/Volhard, Arbeitshandbuch für Unternehmensübernahmen Bd. 1, 2001, § 9 Rn. 78.

[11] *Bremer*, GmbHR 2000, 176.

[12] *Schiessl/Böhm*, Münchener Handbuch des Gesellschaftsrechts Bd. 3, 4. Aufl. 2012, § 33 Rn. 20.

[13] *Götze*, ZGR 1999, 202, 227; vgl. auch LG Köln v. 26.3.2008 – AZ 90 O 11/08, BB 2009, 186 (mit Anm. *Liese/Theusinger*), wonach für einen entsprechenden Weisungsbeschluss Einstimmigkeit erforderlich ist, a. A.: einfache Mehrheit ausreichend: *Engelhardt*, GmbHR 2009, 237.

Verkäufer kann daher das Management des Zielunternehmens zur Bereitstellung der Due Diligence Unterlagen zwingen, ohne dass die Geschäftsführer des Zielunternehmens hierbei eine Haftung trifft.[14] Darüber hinaus hat aber auch jeder Gesellschafter, d. h. Mehrheits- oder Minderheitsgesellschafter, einer GmbH das Recht, von der Geschäftsführung umfassend über die Geschäfte der Gesellschaft informiert zu werden.[15] Die Geschäftsführung ist daher insoweit verpflichtet, ihre Gesellschafter mit entsprechenden Informationen zu versorgen.[16]

Bei einer Aktiengesellschaft ist dies grundsätzlich anders. Es besteht zum einen schon kein Weisungsrecht der Aktionäre bzw. der Hauptversammlung gegenüber dem Vorstand, d. h. es gilt die allgemeine Regel, dass vertrauliche Informationen nur weitergegeben werden dürfen, wenn dies im Interesse des Unternehmens liegt. Zum anderen ist die Informationspflicht des Vorstands gegenüber Aktionären gesetzlich auf hauptversammlungsrelevante Themen beschränkt. Damit unterliegt es der unternehmerischen Entscheidung des Vorstands, ob und inwieweit er einem Aktionär oder dem Erwerber vertrauliche Informationen für eine Due Diligence zur Verfügung stellt. Hierbei hat er eine Abwägung der Interessen des Unternehmens gegen die des Aktionärs vorzunehmen.[17] In der Praxis wird dieses rechtliche Idealbild jedoch meist nicht gelebt, d. h. ein starker Hauptaktionär wird seinen Einfluss auf den Vorstand immer zu seinen Gunsten auszuüben wissen (mit entsprechenden Haftungsrisiken der beteiligten Personen). Einen Sonderfall bildet der Paketverkauf von Aktien börsennotierter Unternehmen außerhalb der Börse. Dort findet meist nur eine sehr eingeschränkte Due Diligence statt, da das börsennotierte Zielunternehmen bzw. dessen Organe aus insiderrechtlichen Gründen diverse Informationen nicht zur Verfügung stellen dürfen.[18]

Neben der Frage der Zulässigkeit der Herausgabe vertraulicher Informationen durch die Geschäftsleitung des Zielunternehmens ist in zweiter Linie zu prüfen, inwieweit der Verkäufer, d. h. der Gesellschafter bzw. Aktionär des Zielunternehmens selbst berechtigt ist, das Zielunternehmen betreffende vertrauliche Informationen an Dritte weiterzugeben. Er unterliegt ebenfalls einer Treuepflicht gegenüber der Zielgesellschaft, die allerdings weniger intensiv ausgeprägt ist als die Treuepflicht des Geschäftsführers bzw. Vorstandsmitglieds. Darüber hinaus ist bei der eher personalistisch geprägten GmbH der Gesellschafter grundsätzlich weitergehend zur Treue verpflichtet als der Aktionär einer als Publikumsgesellschaft ausgestalteten AG. Auch hier ist eine Abwägung vorzunehmen zwischen den

---

[14] Vgl. aber LG Köln a. a. O. (Fn. 12), wonach der verkaufswillige Gesellschafter einem Stimmverbot unterliegt. Dies kann jedoch in der Satzung geändert werden.

[15] Vgl. § 51 a GmbHG; *Schmiegelt/Gerber* in: Beck'sches Handbuch der GmbH, 4. Aufl. 2009, § 3 Rn. 63.

[16] *Koppensteiner,* in: Rowedder/Schmidt-Leithoff, GmbHG, 4. Aufl. 2002, § 51 a Rn. 5: informationsver- pflichtet ist insofern nur die Gesellschaft, die dabei aber durch die Geschäftsführer vertreten wird.

[17] *Richter,* in: Semler/Peltzer, Arbeitshandbuch für Vorstandsmitglieder, München 2005, § 4 Rn. 362; OLG Hamm v. 10.5.1995 – 8 U 59/94, AG 1995, 512, 514.

[18] Vgl. hierzu *Körber*, NZG 2002, 263, 267.

Interessen der zu veräußernden Gesellschaft und ihres Gesellschafters bzw. Aktionärs.[19] Das LG Köln hat eine im juristischen Schrifttum vertretene Meinung[20] bestätigt, nach der die Weitergabe von Informationen an einen Dritten zwecks Durchführung einer Due Diligence einen einstimmigen Beschluss der Gesellschafter der Zielgesellschaft voraussetzt.[21] Der verkaufswillige Gesellschafter soll diesbezüglich sogar einem Stimmverbot unterliegen. Dies würde bedeuten, dass ein Minderheitsgesellschafter, der nur eine Beteiligung von z. B. 1 % hielte, die Veräußerung der weiteren 99 % der Geschäftsanteile durch den Mehrheitsgesellschafter verhindern könnte. Bei entsprechenden Konstellationen empfiehlt sich jedenfalls die Aufnahme einer Satzungsregelung, nach der eine bestimmte Mehrheit für den Beschluss über die Durchführung einer Due Diligence ausreichend ist.[22]

Zu beachten ist jedenfalls, dass Informationen eines höheren Vertraulichkeitsgrades nicht gleich zu Beginn der Due Diligence zur Verfügung gestellt werden, sondern erst, wenn eine Kaufabsicht des Käufers hinreichend konkret ist und die Weitergabe dieser höchst vertraulichen Informationen eine notwendige Voraussetzung für den Kauf bildet. In jedem Fall ist mit dem Kaufinteressenten eine Verschwiegenheitsvereinbarung abzuschließen.

3 Compliance-bezogene Due Diligence

Vor dem Hintergrund diverser „Compliance-Desaster" bei deutschen Unternehmen[23] etabliert sich neben den klassischen Formen der Due Diligence (rechtliche, steuerliche, finanzielle, technische, umweltbezogene etc.) eine compliance-bezogene Due Diligence.[24] Eine solche Due Diligence muss nicht ein in sich geschlossenes Untersuchungsverfahren sein, sondern kann auch aufgespaltet als Bestandteile einer rechtlichen, financial, organizational oder IT–Due Diligence stattfinden. Zunächst muss sich ein Käuferunternehmen, bei dem bereits ein funktionierendes Compliance-Management besteht, im Vorfeld eines Kaufes ein Bild darüber machen, inwieweit ein Compliance-Management bei dem zu erwerbenden Unternehmen überhaupt besteht bzw. welcher Aufwand zur Einführung eines solchen Systems nach Erwerb betrieben werden muss. Besteht bereits eine Compliance-Organisation, so ist zu untersuchen, inwieweit sich diese in die Eigene integrieren lässt. Ist dies nicht möglich bzw. besteht noch keine Compliance-Organisation, so

[19] Zur Geheimhaltungspflicht von Gesellschaftern vgl. *Ziegler,* DStR 2000, 249 ff.

[20] *Engelhardt*, GmbHR 2009, 237; *Körber*, NZG 2002, 263; *Götze*, ZGR 1998, 2002, jeweils mit weiteren Nachweisen.

[21] Vgl. Fn. 12

[22] *Schneider* in: Scholz, GmbHG, 10. Aufl. 2007, § 43 Rz. 148.

[23] Man erinnere sich nur an die aus der Tagespresse jedermann bekannten Fälle Ferrostaal, Siemens, Deutsche Telekom und Deutsche Bahn.

[24] Einen Überblick aus betriebswirtschaftlicher Sicht bieten *Peemöller/Reinel-Neumann*, BB 2009, 206.

muss man sich über den Aufwand ein Bild machen, der erforderlich ist, um die eigene Compliance-Organisation beim Zielunternehmen einzuführen.

Bestehen beim Zielunternehmen keine Compliance-Organisation oder ähnliche Systeme bzw. ist das Vorhandene nicht ausreichend, so können hieraus (müssen aber nicht) auch Schlüsse in Bezug auf etwaige Risiken gezogen werden. Dies dürfte jedoch sehr von der Branche des Zielunternehmens abhängen. So wäre auch im Rahmen einer Compliance Due Diligence zu prüfen[25], inwieweit das Zielunternehmen Compliance Risiken jeglicher Art ausgesetzt ist, z. B. in welchem Umfang Geschäfte mit öffentlichen Auftraggebern abgewickelt werden, in welchen Riskoländern das Zielunternehmen tätig ist oder in welchem Umfang etwa eine Abstimmung mit Wettbewerbern besteht. Soweit sich aus den bekannten Geschäftsfeldern ein erhöhtes Risiko für Compliance Verstöße (z. B. Schmiergeldzahlungen) ergibt, kann im Rahmen der rechtlichen, steuerlichen oder Financial Due Diligence gezielt nach tatsächlichen Verstößen gesucht werden.[26] In der Regel ist jedoch davon auszugehen, dass insbesondere Korruptionstatbestände durch eine übliche Due Diligence mangels vorhandener Informationen nicht aufgedeckt werden können.[27] Auch Fragen an die Verkäufer oder das Management des Zielunternehmens im Hinblick auf etwaige Korruptionstatbestände werden im Allgemeinen nicht Ziel führend sein. Damit ist der Käufer oft auf eine allgemeine Einschätzung des Risikos und etwaige Garantien oder Zusicherungen des Verkäufers angewiesen. Eine rasche Einbindung des Zielunternehmens in die eigene Compliance-Organisation nach dem Erwerb kann hier auch zur gezielten Suche nach Verstößen in der Vergangenheit genutzt werden, um etwaige Garantieansprüche gegen den Verkäufer rechtzeitig, d. h. vor Ende der in Unternehmenskaufverträgen üblicherweise eher kurzen bemessenen Verjährungsregelungen, geltend zu machen. Bei konkreten Hinweisen auf Compliance-Verstöße kann neben einem Kaufpreisabschlag[28] auch eine Freistellungsverpflichtung gegenüber Schäden aus solchen Verstößen mit einer längeren Verjährungsfrist vereinbart werden.[29] Solche Regelungen sind bereits bei konkreten Hinweisen auf Umweltschäden üblich, so dass hier bezüglich der rechtlichen Umsetzung kein Neuland betreten werden muss.

Im Bereich der Compliance Due Diligence ist noch vieles im Fluss und bis zur Bildung eines Marktstandards wird noch einige Zeit vergehen. Wie wichtig eine Compliance Due Diligence ist, zeigt sich in der Praxis immer häufiger. Verstöße des Zielunternehmens gegen Kartellrecht, z. B. verbotene Preisabsprachen, können Bußgelder bis zu 10 % des Jahresumsatzes des gesamten Konzerns betragen (vgl. unten 5).

---

[25] Vgl. Liese, BB Special 4, 2010, 27 ff. zum Inhalt der Fragelisten.

[26] *Leisch/Lohner*, M&A Review 2009, 133, 135.

[27] *Leisch/Lohner*, M&A Review 2009, 133.

[28] Zur Berechnung vgl. *Peemöller/Reinel-Neumann*, BB 2009, 206.

[29] *Leisch/Lohner*, M&A Review 2009, 133, 136.

4 Geheimhaltung

Wie eingangs bereits beschrieben, ist bei M&A-Transaktionen unbedingt absolute Vertraulichkeit zu gewährleisten. Dies gilt zum einen im Hinblick auf das Verhindern des Durchsickerns von Informationen und dient damit der Stärkung der eigenen Verhandlungsmacht. Zum anderen sind aus Gründen des Wettbewerbs aber auch bei börsennotierten Unternehmen nachteilige Folgen mit der Weitergabe von vertraulichen Informationen verbunden.

Darüber hinaus gibt es vertrauliche Informationen, die dem Käufer vor Abschluss des Kaufvertrages überhaupt nicht zur Verfügung gestellt werden können. Dies sind in erster Linie Informationen, die aufgrund einer Vertraulichkeitsvereinbarung mit Dritten (z. B. Vertragspartnern) nicht weitergegeben werden dürfen, ohne gleichzeitig Vertragsstrafen oder Kündigungsrechte für den Dritten auszulösen. Insbesondere wenn es sich bei dem Erwerber um einen Wettbewerber handelt, werden solche Informationen oftmals auch erst nach Vertragsabschluss offengelegt, soweit diese Informationen einen wesentlichen nachteiligen Effekt für das Zielunternehmen hätten, falls es nicht zu einem Vertragsabschluss kommt (z. B. Preiskalkulationen in einer Wettbewerbssituation u. ä.).[30]

In größeren Unternehmen sowie bei auf M&A-Transaktionen spezialisierten Beratern ist es daher üblich, Verhaltensrichtlinien für M & A – Transaktionen an die Mitarbeiter zu verteilen. Solche Regeln gehen oft einher mit IT-Sicherheit und Compliance, da ohne IT-Support eine Transaktion heutzutage kaum noch denkbar ist. Insbesondere der E-Mail-Verkehr mit vertraulichen Informationen sollte möglichst eingedämmt bzw. kanalisiert werden. Zur Verbesserung der Geheimhaltung eignen sich z. B. virtuelle webbasierte Plattformen, in die sämtliche relevanten Informationen und Dokumente eingestellt werden und auf die nur ein ausgewählter Personenkreis Zugriff hat.

5 Kartellrechtliche Compliance bei Transaktionen

Kartellrechtliche Compliance bedeutet bei Transaktionen[31] im Wesentlichen zweierlei: Erstens, vor der Genehmigung der Kartellbehörde alle Handlungen zu unterlassen, die einen Vollzug der Transaktion darstellen könnten. Zweitens, den Austausch von Informationen zu vermeiden, die eine Abstimmung über das Wettbewerbsverhalten der Beteiligten ermöglichen.

Bei jeder Transaktion ist zunächst zwingend zu ermitteln, ob sie der Genehmigung durch Kartellbehörden (Europäische Kommission, Bundeskartellamt, ausländische Wettbewerbsbehörden) bedarf. Hiervon hängt (zumindest nach deutschem Recht) ihre

[30] *Semler* in: Hölters, Handbuch des Unternehmens- und Beteiligungskaufs, 6. Aufl. 2005, Teil VII Rn. 51.

[31] Zur weiteren Kartellrechts-Compliance siehe den Beitrag von *Janssen* in diesem Band.

zivilrechtliche Wirksamkeit ab. Da oft eine Anmeldepflicht in mehr als einem Land in Betracht kommt, die maßgeblichen Schwellenwerte von Land zu Land unterschiedlich sind (meist kommt es auf Umsatzgrößen, zuweilen aber auch auf Marktanteile an) und die Folgen von Fehleinschätzungen gravierend sind (hohe Geldbußen, Unwirksamkeit, Rückabwicklung), sollte man die Arbeit unbedingt einem Fachmann überlassen. Wer, etwa in der Erwartung, die Behörden würden später die Transaktion ohnehin freigeben, schon vor Erteilung der Genehmigung vollzieht (*gun jumping*), muss mit verzögernden kartellbehördlichen Ermittlungen rechnen und ein nicht unerhebliches Bußgeld einkalkulieren (das Bundeskartellamt verhängte z. B. in einem solchen Fall mehr als 4 Millionen Euro).[32] Aus denselben Gründen ist auch bei der Gestaltung des Transaktionsvertrags darauf zu achten, dass Fortführungsklauseln für die Zeit zwischen *Signing* und *Closing* (also Klauseln, die dem Käufer nach Abschluss des Vertrages und vor Übernahme des Zielunternehmens einen werterhaltenden Einfluss auf dieses Unternehmen sichern wollen) nicht auf einen vorzeitigen Vollzug hinauslaufen.

Während der Due Diligence dürfen die Parteien nicht mehr über sich preisgeben, als kartellrechtlich zulässig ist. Ansonsten können sie schon während des Fusionskontrollverfahrens in das Visier der Kartellbehörden geraten.[33] Denn ein unzulässiger Informationsaustausch kann unter Umständen einen verbotenen Teil-Vollzug der Transaktion bedeuten – mit den oben beschriebenen Folgen.[34]

Insbesondere wenn der Kaufinteressent ein Wettbewerber des Zielunternehmens ist, kann der Informationsaustausch darüber hinaus auch eine Abstimmung über das Wettbewerbsverhalten der Beteiligten ermöglichen. Dann liegt ein gefährlicher Verstoß gegen das Kartellverbot nahe. Dieses untersagt Unternehmen, Informationen auszutauschen und damit den Wettbewerb zu beschränken. Verstöße kosten bis zu 10 % des jährlichen Gruppenumsatzes.[35] Daher müssen bei der Informationsweitergabe, insbesondere bei der Due Diligence (und auch bei der Vorbereitung einer fusionskontrollrechtlichen Anmeldung) Unternehmens- und Marktdaten mit Vorsicht bei den Parteien und dem Zielunternehmen erhoben werden. Grundsätzlich gilt, dass sich die ausgetauschten Informationen auf den Unternehmenskauf beschränken müssen. In der Regel wird es zum Beispiel keine sachlichen Gründe dafür geben, wenn der Erwerber Informationen über sein Geschäft preisgibt. Ist der Markt eng und ist eine genauere fusionskontrollrechtliche Untersuchung – vielleicht sogar eine Untersagung – nicht auszuschließen, mag es die Vorsicht gebieten, die Due Diligence auf mehrere Phasen der Transaktion zu verteilen und insbesondere

[32] Pressemitteilung des BKartA vom 13. Februar 2009 (Druck- und Verlagshaus Frankfurt am Main GmbH, DuV).

[33] So etwa das Unternehmen Norsk Hydro, dessen Anmeldung eines Zusammenschlusses bei der Europäischen Kommission es nicht vor einer Durchsuchung bewahrte (siehe Pressemitteilung der Europäischen Kommission vom 13. Dezember 2007).

[34] *Linsmeier/Balssen*, BB 2008, 741, 743.

[35] Das BKartA hat zum Beispiel Bußgelder i. H. v. 124,5 Mio. € wegen verbotener Preisabsprachen verhängt; Pressemitteilung BKartA vom 5. Juli 2012.

sehr sensible Informationen erst nach der kartellbehördlichen Freigabe mitzuteilen. Auch eine nachträgliche Due Diligence kann in Betracht kommen. Die Zusammenstellung der Projektgruppen („*Clean Teams*“[36]) kann wichtig sein. Externe Berater können darüber hinaus kritische Informationen herausfiltern und ihren Mandanten bereinigte Unterlagen zukommen lassen. Auf diese Weise können Kartellverstöße vermieden werden.

6 Weitere transaktionsbezogene Compliance-Themen

Die obigen Aspekte bilden nur einen Ausschnitt der wichtigsten Compliance-Themen bei M&A-Transaktionen. Darüber hinaus sind aber noch eine Vielzahl weiterer Umstände nicht außer Acht zu lassen. Der Verzicht auf deren Behandlung in diesem Beitrag ist dem Gesamtkonzept des Werkes geschuldet, dessen Rahmen ansonsten gesprengt würde.

Kurz erwähnt sei jedenfalls, dass Unternehmenskäufe heute einer eigenen, anglo-amerikanisch geprägten Systematik unterliegen. Die Komplexität ist für den (Transaktions-)Laien teils nicht mehr überschaubar.[37] Hier zählt vor allem Erfahrung, sei es im eigenen Unternehmen, in der M&A- oder Rechtsabteilung, oder sei es bei den hinzugezogenen externen Beratern, wie M&A-Beratern, Steuerberatern, Rechtsanwälten, Wirtschaftsprüfern und sonstigen Spezialisten. Eine entsprechende Expertise sollte vom Unternehmer möglichst hergestellt werden.

7 Fazit

Wie die vorausgehenden Ausführungen zeigen, ist ein funktionierendes Compliance-Management aufgrund der einzuhaltenden Vorschriften und damit verbunden Risiken vom Anfang bis zum Ende eines M&A-Transaktionsprozesses höchst relevant. Ist ein Unternehmen erworben, muss sichergestellt werden, dass die etwa vorhandenen verschiedenen Compliance-Systeme kompatibel sind oder es muss das eigene Compliance-System bei dem erworbenen Unternehmen eingeführt werden. Dies erfordert eine genaue und zeitnahe Vorbereitung. Der Compliance-Officer ist frühzeitig in den Transaktionsprozess einzubinden, damit eine reibungslose Integration des erworbenen Unternehmens auch aus Compliance-Gesichtspunkten möglich ist.

---

[36] *Clean Teams* sind üblicherweise Mitarbeiter oder Berater des Käufers, die die Informationen nur für Zwecke der Transaktion auswerten und für einen bestimmten Zeitraum aus dem operativen Geschäft des Erwerbers herausgenommen werden, um nicht dort die erhaltenen Informationen zu verwerten; vgl. *Besen/Gronemeyer*, CCZ 2009, S. 67 ff. In der Praxis lässt sich jedoch auch durch diese Vorgehensweise ein „Durchsickern“ vertraulicher Informationen nicht verhindern, so dass der hierfür zu betreibende Aufwand beim Erwerber in keinem Verhältnis zum Nutzen steht.

[37] Einen guten Überblick aus dem rechtlichen Blickwinkel bietet *Gran*, NJW 2008, 1409, vgl. auch Mellert, BB 2011, 1667.

Compliance in der Außenwirtschaft: Exportkontrolle

Ole-Jochen Melchior

Inhaltsverzeichnis

In der Vorauflage wurde dieses Kapitel von Volker Schlegel und Gwenn Schanze verfasst, denen ich für ihre Arbeit herzlich danke und deren Ausführungen in Teilen übernommen wurden.

O.-J. Melchior (✉)
Gildehofstraße 1, 45127 Essen, Deutschland
E-Mail: ole.melchior@luther-lawfirm.com

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2_5, © Springer Fachmedien Wiesbaden 2013

Zusammenfassung

Der gesamteBereich der Ausfuhren von Gütern und Dienstleistungen hat gerade für Deutschland eine ganz besondere wirtschaftliche und politische Bedeutung:

In Deutschland werden mehr als ein Drittel des Sozialprodukts (Geldwert sämtlicher Güter, Dienste und Nutzungen) durch den Export erwirtschaftet, bis vor kurzer Zeit war Deutschland noch „Export-Weltmeister"; die Sicherstellung eines reibungslosen, effizienten und freien – d. h. möglichst wenig eingeschränkten – Exports gehört deshalb zu den „Lebensnerven" dieses Staates und seiner Gesellschaft.

Andererseits ergeben sich aus der Geschichte und der Stellung Deutschlands innerhalb der Europäischen Union sowie der Vereinten Nationen Verpflichtungen, die für das Ansehen und die politische Handlungsfähigkeit der Bundesrepublik besondere Bedeutung haben.

Diese Zielsetzung könnte erheblich beeinträchtigt werden, wenn exportierte Güter oder Technologien an den falschen Adressaten geraten; deshalb gibt es auf nationaler Ebene Export-Kontrollvorschriften insbesondere in Form des Außenwirtschaftsgesetzes (AWG) sowie des Kriegswaffenkontrollgesetzes (KrWaffKontrG) und auf EU-Ebene in Form zahlreicher Embargos sowie der sog. „EG Dual-Use-Verordnung". Verstöße gegen diese Rechtsvorschriften können sowohl für das betroffene Unternehmen als auch für die handelnden Personen gravierende, vor allem strafrechtliche Konsequenzen haben.

Deshalb gibt es für jedes Unternehmen, das mittelbar oder unmittelbar mit Exporten zu tun hat, keine Alternative, sich mit Theorie und Praxis des Exportkontrollrechts zu beschäftigen und nicht die geringste Frage offen zu lassen – diese Pflicht gilt für jeden mit Exporten betrauten Mitarbeiter, von der Geschäftsführung bis zum Sachbearbeiter.

Die Unternehmensorganisation muss daher auf die besonderen Bedürfnisse und Vorgaben des Exportkontrollrechts ausgerichtet sein, um jedem späteren Vorwurf, die einschlägigen Vorschriften nicht beachtet zu haben, von vornherein weitestgehend entgegenzuwirken.

Die nachfolgenden Ausführungen beinhalten einen groben, aufgrund der Komplexität dieses Rechtsgebietes keinesfalls abschließenden Überblick über die wichtigsten Regelungen im Bereich der Exportkontrolle. Zu beachten ist dabei, dass nur sehr wenig

Rechtsprechung zu dieser Thematik existiert und der Rechtsanwender sich vielfach unbestimmten Rechtsbegriffen ausgesetzt sieht. Wo Zweifel über die Auslegung derartiger Begriffe oder die Zulässigkeit einer beabsichtigten Handlung bestehen, sollte deshalb unbedingt im Vorfeld eine Klärung mit den zuständigen Behörden erfolgen und gegebenenfalls Rechtsrat eingeholt werden. (In Anlehnung an die Zusammenfassung von Volker Schlegel und Gwenn Schanze in der Vorauflage.)

1 Rechtsgrundlagen für die Beschränkungen des Außenwirtschaftsverkehrs

1.1 Internationale Abkommen/Exportkontrollregime[1]

Infolge der politischen Spannungen zwischen der westlichen Welt und den kommunistisch orientierten Ländern im Rahmen des Ost-West Konflikts wurde im Jahre 1949 das sogenannte „Coordinating Committee" (**CoCom**) gegründet, zunächst, um sich gegenseitig über Exporte in den Osten abzustimmen und dann gemeinsame Regeln aufzustellen, mit denen dem Sicherheitsbedürfnis der westlichen Welt Rechnung getragen werden konnte.

Nach der Auflösung des kommunistischen Blocks hatte das CoCom in seiner ursprünglichen Form seine Existenzberechtigung jedoch verloren. Gleichwohl wollte man die bewährte Kontrolle aber nicht aufgeben, sondern eine ungezügelte Aufrüstung weiterhin verhindern. So begannen nach dem Weltwirtschaftsgipfel 1993 in Tokio Verhandlungen über eine Nachfolgeorganisation für das CoCom, die auf allgemeinen Wunsch zunächst „Neues Forum" heißen sollte. Im Laufe der langwierigen Verhandlungen einigte man sich dann jedoch schließlich auf die Bezeichnung „**Wassenaar Arrangement**" – nach dem Ort der Verhandlungen, einem Vorort von Den Haag. Wie schon CoCom ist auch das Wassenaar Arrangement kein völkerrechtlicher Vertrag mit entsprechenden Rechtsfolgen, sondern eine politische Absprache, eine Art „Gentleman's Agreement", zwischen den beteiligten Ländern.

Das Wassenaar Arrangement richtet sich nicht mehr gegen eine Staatengruppe, vielmehr soll es generell die konventionelle Aufrüstung und die Beschaffung von Dual-Use-Gütern für militärische Zwecke verhindern, „wenn das Verhalten eines Landes zu ernster Besorgnis Anlass gibt."[2] Insoweit existiert auch keine Länderliste mehr, die Teilnehmerstaaten verständigen sich bei aktuellem Anlass, von welchem Staat eine Gefahr für den Weltfrieden ausgehen könnte. Die praktische Kontrolle im Rahmen des Wassenaar Arrangements wird gewährleistet durch gemeinsame Kontrolllisten und Informationspflichten aller Teilnehmerstaaten, die Verantwortung für den jeweiligen Exportfall bleibt jedoch in nationaler Verantwortung des betroffenen Staates.

---

[1] In Anlehnung an die Ausführungen von Volker Schlegel und Gwenn Schanze in der Vorauflage.

[2] *Bieneck*, in: Bieneck (Hrsg.), Handbuch des Außenwirtschaftsrechts, 2. Aufl. 2005, § 7 Rn 82.

Der Ost-West Konflikt war aber nicht das einzige Feld, von dem ernsthafte Gefahren für den Weltfrieden ausgingen. So haben die furchtbaren Vorgänge in Helabja/Irak während des iranisch-irakischen Krieges gezeigt, dass auch in der Neuzeit die Gefahr eines Angriffs mit chemischen Waffen immer noch nicht gebannt ist; es gab bei einigen Staaten weiter Bemühungen (wie in Rabta/Libyen Ende der 80er Jahre), Produktionsanlagen für solche Kampfstoffe zu errichten, zumindest um damit für politische Auseinandersetzungen ein Druckpotenzial mit völlig neuen Dimensionen in die Hand zu bekommen. Um dies zu blockieren und in Zukunft gar nicht mehr entstehen zu lassen, hat sich eine internationale Staatengemeinschaft, die sogenannte „**Australische Gruppe**", darauf verständigt, den Außenhandel mit jenen Stoffen und Vorprodukten, die für die Herstellung von chemischen Waffen gebraucht werden, streng zu kontrollieren, beziehungsweise zu unterbinden.

Seit Hiroshima und Nagasaki weiß die Welt, welches „Doomsday-Potenzial" die Anwendung von atomaren Waffen nach sich ziehen kann. Auch in diesem Bereich ist deshalb mit der „**Nuclear Suppliers Group**" (NSG) eine zwischenstaatliche Vereinbarung getroffen worden, um den Handel mit Produkten, die zur Herstellung von atomaren Waffen geeignet sind, zu kontrollieren beziehungsweise zu verbieten.

Als letztes Beispiel dieser Art sei die Gefahr erwähnt, die von dem unkontrollierten Handel mit Raketentechnologie ausgehen kann; auch hier haben sich die interessierten Staaten zusammengefunden, um mit dem „**Missile Technology Control Regime**" (MTCR) ein Regime zur Kontrolle beziehungsweise zum Verbot solcher Technologie zu gründen und in effizienter Weise aufrecht zu erhalten.

All diesen sogenannten Exportkontrollregimen ist gemein, dass es sich hierbei „lediglich" um internationale Absprachen handelt, die nicht die Qualität eines völkerrechtlichen Vertrages haben und auch keine verbindlichen Vorgaben für die Exportkontrolle treffen, die jedoch ihre Teilnehmerstaaten politisch verpflichten und die inhaltliche sowie teilweise auch konzeptionelle Grundlage für nationale Exportkontrollen bilden.[3]

1.2 EU-Embargos

Ist von Embargos die Rede, denkt man häufig zunächst an die vom Sicherheitsrat der Vereinten Nationen in Form von Resolutionen beschlossenen Sanktionen gegen bestimmte Staaten, welche zwar für die jeweiligen Mitgliedstaaten verbindlich sein mögen, jedoch gegenüber den Bürgern und Unternehmen des einzelnen Staates als Privatperson wie die vorgenannten Exportkontrollregime ebenfalls keine unmittelbare Wirkung entfalten. Die Vereinten Nationen erlassen keine Gesetze, welche die Bürger der Mitgliedstaaten direkt verpflichten. Hierzu bedarf es zunächst einer Umsetzung in nationales bzw. national geltendes Recht. Dies geschieht auf europäischer Ebene regelmäßig in Form von Gemeinsamen Standpunkten des Rates der Europäischen Union im Bereich der Gemeinsamen Außen- und Sicherheitspolitik (GASP). Auf Basis dieser Beschlüsse ergehen **EU-Verordnungen**,

[3] *Weith, Wegner, Ehrlich*: Grundzüge der Exportkontrolle, 2006, S. 49 Rn. 50.

die sodann für die Bürger und Unternehmen der EU-Mitgliedstaaten unmittelbare Rechtswirkung haben. Es bedarf dann also keines nationalen Gesetzes mehr (wobei natürlich auch rein nationale Embargos möglich wären).

Diese EU-Embargos sind **lex specialis** gegenüber den allgemeinen ausfuhrrechtlichen Regelungen und gehen diesen vor, ohne diese jedoch auszuschließen: Verstößt eine beabsichtigte Handlung zwar nicht gegen ein Embargo, kann sie gleichwohl nach den allgemeinen Regelungen unzulässig sein. Ist umgekehrt die beabsichtigte Handlung bereits aufgrund eines Embargos verboten, bedarf es keiner weitergehenden Prüfung mehr. Jeder „allgemeinen" Exportkontrolle muss folglich eine Embargo-Kontrolle vorausgehen.

Embargos sind Wirtschaftssanktionen, die gegenüber einem bestimmten Staat oder bestimmten Personen verhängt werden. Man unterscheidet demgemäß zwischen **länderbezogenen** Embargos (wie etwa derzeit gegenüber Iran oder Syrien) und **personenbezogenen** Embargos (wie z. B. die sogenannten „Anti-Terror-Listen"), wobei Überschneidungen möglich sind: So finden sich häufig personenbezogene Beschränkungen in länderbezogenen Embargos. Achtung: Personenbezogene Sanktionen gelten unabhängig von dem Wohn- oder Aufenthaltsort der Person oder dem Sitz des Unternehmens, auch Inlandsgeschäfte können daher betroffen sein.

Des Weiteren lassen sich Embargos unterscheiden nach ihrem Umfang: **Totalembargos** beinhalten ein Verbot jeglichen Handels mit dem oder zugunsten des Adressaten. **Teilembargos** schränken nur bestimmte Handlungen ein, zum Teil auch nur gegenüber bestimmten Personen (Kombination länder-/personenbezogene Maßnahmen), durch einzelne Verbote und Genehmigungsvorbehalte.

Schließlich sind Embargos nach dem **Inhalt** ihrer Beschränkungen zu unterscheiden: In Betracht kommen insbesondere

- Waffenembargos,
- sonstige Güterembargos (mit eigenen Güterlisten),
- Verbot technischer und finanzieller Hilfe,
- Finanzsanktionen in Form der Einschränkung des Kapital- und Zahlungsverkehrs einschließlich sogenannter Bereitstellungsverbote,
- Erfüllungsverbote,
- Einfuhrverbote,
- Reisebeschränkungen
- und nicht zuletzt auch Importverbote.

1.3 Chemiewaffenübereinkommen

Eine gewisse Sonderstellung nimmt das „Übereinkommen über das Verbot der Entwicklung, Herstellung, Lagerung und des Einsatzes chemischer Waffen und über die Vernichtung solcher Waffen" (Chemiewaffenübereinkommen, CWÜ) vom 13. Januar 1993 ein, welches als völkerrechtlicher Abrüstungs- und Rüstungskontrollvertrag für den

einzelnen Privatmann wiederum zunächst einmal keine unmittelbaren Rechtsfolgen entfaltet, welches mit einem entsprechenden Ausführungsgesetz (**CWÜAG**) vom 2. August 1994 sowie einer Ausführungsverordnung (**CWÜV**) jedoch in nationales Recht umgesetzt wurde, dessen Regelungen damit von jedermann zu beachten sind.

1.4 Kriegswaffenkontrollgesetz

Im Prinzip ähnlich verhält es sich mit dem Kriegswaffenkontrollgesetz (**KrWaffKontrG** oder **KWKG**) vom 22. November 1990, welches einerseits die Vorgabe in Art. 26 Abs. 2 des Grundgesetzes ausführt, wonach zur Kriegführung bestimmte Waffen nur mit Genehmigung der Bundesregierung hergestellt, befördert und in Verkehr gebracht werden dürfen, und in welchem andererseits aber auch die internationalen Rüstungskontroll- und Abrüstungsvereinbarungen zur Verhinderung der Weiterverbreitung von Massenvernichtungswaffen umgesetzt wurden.

Das KrWaffKontrG nebst der ihm als Anhang beigefügten Kriegswaffenliste (**KWL**) sowie seinen Durchführungsverordnungen regelt den Umgang mit Kriegswaffen als einen besonderen Bereich der Rüstungsgüter. Sonstige Rüstungsgüter, die keine Kriegswaffen sind, fallen demgegenüber unter die Exportbeschränkungen des Außenwirtschaftsgesetzes.

1.5 Außenwirtschaftsgesetz und Außenwirtschaftsverordnung

„Der Waren-, Dienstleistungs-, Kapital-, Zahlungs- und sonstige Wirtschaftsverkehr mit fremden Wirtschaftsgebieten (. . .) ist grundsätzlich frei.“, heißt es vielversprechend in § 1 Abs. 1 S. 1 des im Jahre 1962 in Kraft getretenen Außenwirtschaftsgesetzes (**AWG**). Doch gibt es von Grundsätzen stets auch Ausnahmen und so hält § 1 Abs. 1 S. 1, Abs. 2 AWG sogleich fest, dass der Außenwirtschaftsverkehr den Einschränkungen unterliegt, „die dieses Gesetz enthält oder die durch Rechtsverordnung auf Grund dieses Gesetzes vorgeschrieben werden. Unberührt bleiben Vorschriften in anderen Gesetzen und Rechtsverordnungen, zwischenstaatliche Vereinbarungen, denen die gesetzgebenden Körperschaften in der Form eines Bundesgesetzes zugestimmt haben, sowie Rechtsvorschriften der Organe zwischenstaatlicher Einrichtungen, denen die Bundesrepublik Deutschland Hoheitsrechte übertragen hat.“

Und diese Einschränkungen sind beträchtlich: Rechtsgeschäfte und Handlungen können unter einen Genehmigungsvorbehalt gestellt oder gänzlich verboten sein (§ 2 Abs. 1 AWG) und zwar

- „zur Erfüllung zwischenstaatlicher Vereinbarungen“ (§ 5 AWG),
- „um schädlichen Folgen für die Wirtschaft oder einzelne Wirtschaftszweige im Wirtschaftsgebiet vorzubeugen oder entgegenzuwirken, wenn solche Folgen durch Maßnahmen in fremden Wirtschaftsgebieten drohen oder entstehen, die den Wettbewerb einschränken, verfälschen oder verhindern oder zu Beschränkungen des Wirtschaftsverkehrs mit dem Wirtschaftsgebiet führen“ (§ 6 Abs. 1 AWG),

- „um Auswirkungen von in fremden Wirtschaftsgebieten herrschenden, mit der freiheitlichen Ordnung der Bundesrepublik Deutschland nicht übereinstimmenden Verhältnissen auf das Wirtschaftsgebiet vorzubeugen oder entgegenzuwirken" (§ 6 Abs. 2 AWG) oder
- „um die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland zu gewährleisten, eine Störung des friedlichen Zusammenlebens der Völker zu verhüten, zu verhüten, dass die auswärtigen Beziehungen der Bundesrepublik Deutschland erheblich gestört werden oder die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland im Sinne von Art. 46 und 58 Absatz 1 des EG-Vertrags zu gewährleisten" (§ 7 Abs. 1 AWG).

Diese Zielsetzung in § 7 Abs. 1 AWG fasst eigentlich sämtliche Intentionen des Gesetzgebers zusammen: Es geht um die **öffentliche Sicherheit und Ordnung**, zu deren Gunsten hoheitlich in den privatwirtschaftlichen Warenverkehr eingegriffen wird. Und so listet § 7 Abs. 2 AWG denn auch beispielhaft („insbesondere") auf, welche Handlungen zur Erreichung dieses Ziels beschränkt werden können, nämlich

- die Ausfuhr oder Durchfuhr von Waffen, Munition und Kriegsgerät sowie Gegenständen, die bei deren Entwicklung, Erzeugung oder Einsatz nützlich sind, ferner von Konstruktionszeichnungen und sonstigen Fertigungsunterlagen für diese Gegenstände, vor allem wenn die Beschränkung der Durchführung einer in internationaler Zusammenarbeit vereinbarten Ausfuhrkontrolle dient;
- die Ausfuhr von Gegenständen, die zur Durchführung militärischer Aktionen bestimmt sind;
- die Einfuhr von Waffen, Munition und Kriegsgerät;
- Rechtsgeschäfte über gewerbliche Schutzrechte, Erfindungen, Herstellungsverfahren und Erfahrungen in Bezug auf die eingangs bezeichneten Gegenstände;
- Rechtsgeschäfte über den Erwerb deutscher Unternehmen, die Kriegswaffen oder andere Rüstungsgüter herstellen oder entwickeln oder Kryptosysteme herstellen, die für eine Übertragung staatlicher Verschlusssachen von dem Bundesamt für Sicherheit in der Informationstechnik mit Zustimmung des Unternehmens zugelassen sind, oder Rechtsgeschäfte über den Erwerb von Anteilen an solchen Unternehmen, um wesentliche Sicherheitsinteressen der Bundesrepublik Deutschland zu gewährleisten;
- Rechtsgeschäfte über den Erwerb deutscher Unternehmen überhaupt oder von Anteilen an solchen Unternehmen durch einen außerhalb der EG ansässigen Erwerber, wenn dadurch die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland gefährdet ist.

Weitere Beschränkungsmöglichkeiten finden sich in §§ 8ff AWG.

Das AWG ist jedoch lediglich ein Rahmengesetz, die konkreten Beschränkungen ergeben sich erst aus der Außenwirtschaftsverordnung (**AWV**) und der ihr als Anlage beigefügten sogenannten Ausfuhrliste (**AL**).

- **Teil I A** der AL beinhaltet die Liste für **Waffen, Munition und Rüstungsmaterial**.
- **Teil I C** der AL beinhaltet die Liste für **Güter mit doppeltem Verwendungszweck, also Güter,** die sowohl für zivile als auch für militärische Zwecke **(„dual-use")** verwendet werden können. Diese Liste ist zwar abgestimmt auf die entsprechende Liste der EG Dual-Use-Verordnung (siehe unten), jedoch ergänzt um einige nationale Besonderheiten. Soweit sich Teil I C der AL mit den Beschränkungen der EG Dual-Use-Verordnung überschneidet, kommt der EG Dual-Use-VO ein Anwendungsvorrang zu[4]; die europäischen Vorschriften überlagern das nationale Recht. Es ist gleichwohl stets ein Abgleich zwischen Teil I C der AL und der EG Dual-Use-VO vorzunehmen.

Doch Vorsicht: Selbst Güter, die nicht in der AL aufgeführt sind, können gleichwohl Beschränkungen unterliegen, nämlich verkürzt dargestellt bei Kenntnis von einem kritischen Verwendungszweck und Bestimmung für ein kritisches Land („catch-all").

1.6 Neufassung von AWG und AWV

In ihrer Kabinettssitzung vom **15. August 2012** hat die Bundesregierung einen Gesetzesentwurf zur Modernisierung des Außenwirtschaftsgesetzes verabschiedet; damit einhergehend wird auch die Außenwirtschaftsordnung überarbeitet. Dieses neue Gesetz war bei Abfassung dieses Beitrags noch nicht in Kraft getreten.

Mit der Novellierung bezweckt die Bundesregierung eine Straffung der Regelungen im AWG, welches derzeit einem „Flickenteppich" gleiche; die Vorschriften sollen einfacher formuliert werden und auch für Nicht-Juristen verständlich sein. Hierzu soll das AWG unter anderem von 50 auf 28 Paragraphen verschlankt und an die moderne Technologie angepasst werden. Die grundlegenden Wertungen des deutschen Außenwirtschaftsrechts sollen sich hingegen nicht ändern. Neu gestaltet werden allerdings die Straf- und Bußgeldvorschriften: Auf unbestimmte Rechtsbegriffe soll verzichtet werden und die Straf- und Bußgeldbewehrungen sollen stärker als bisher am Grad der Vorwerfbarkeit ausgerichtet sein. Viele Verstöße, die bislang als Ordnungswidrigkeiten geahndet wurden, sollen künftig als Straftaten verfolgt werden. Das Strafmaß für vorsätzliche Verstöße wird zum Teil verschärft, andererseits sollen fahrlässige Verstöße (ausgenommen Missachtungen von Waffenembargos) in Zukunft nicht mehr als Straftat, sondern nur noch als Ordnungswidrigkeit behandelt werden, um der Fehleranfälligkeit der unternehmensinternen Exportkontrolle Rechnung zu tragen. Im Gegenzug sollen solchen Unternehmen allerdings außenwirtschaftsrechtliche Genehmigungen wegen mangelnder Zuverlässigkeit versagt werden können.[5]

---

[4] *Weith, Wegner, Ehrlich*: Grundzüge der Exportkontrolle, 2006, S. 66 Rn. 107.

[5] Näheres unter http://www.bmwi.de/DE/Presse/pressemitteilungen, did = 503568.html.

1.7 EG Dual-Use-VO

Das europäische Pendant zur AWV bzw. zu Teil I C der AL bildet die – gemäß Art. 249 des EG-Vertrages im Bundesgebiet unmittelbar rechtsverbindliche und (siehe oben) das nationale Recht überlagernde – Verordnung (EG) Nr. 428/2009 des Rates vom 5. Mai 2009 „über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck", die sogenannte „EG Dual-Use-Verordnung" (**EG Dual-Use-VO**).

Der **Anhang I** der EG Dual-Use-VO beinhaltet eine Liste aller Güter, für deren Ausfuhr aus dem Gemeinschaftsgebiet eine Genehmigungspflicht besteht. In **Anhang IV** der EG Dual-Use-VO finden sich die Güter, deren Verbringung innerhalb der Gemeinschaft genehmigungspflichtig ist.

2 Begrifflichkeiten/Definitionen

Die vorgenannten zahlreichen nationalen wie europäischen Rechtsvorschriften machen es erforderlich, einige grundsätzliche Begriffe zu erläutern.

2.1 Ortsbezogene Begriffe

„**Wirtschaftsgebiet**" meint den Geltungsbereich des AWG sowie der AWV, also die Bundesrepublik Deutschland einschließlich der österreichischen Gebiete Jungholz und Mittelberg (§ 4 Abs. 1 Nr. 1 AWG).

„**Gebietsansässige**" sind natürliche Personen mit Wohnsitz oder gewöhnlichem Aufenthalt bzw. juristische Personen und Personenhandelsgesellschaften mit Sitz oder Ort der Leitung im Wirtschaftsgebiet, aber auch die Zweigniederlassungen gebietsfremder Personen, wenn sie ihre Leitung im Wirtschaftsgebiet haben und für sie eine gesonderte Buchführung besteht, ebenso bloße Betriebsstätten gebietsfremder Personen, wenn sie ihre Verwaltung im Wirtschaftsgebiet haben (§ 4 Abs. 1 Nr. 5 AWG).

„**Fremde Wirtschaftsgebiete**" sind alle Gebiete außerhalb des Wirtschaftsgebiets einschließlich des Gebietes von Büsingen im Falle des Verbringens von Sachen und Elektrizität (§ 4 Abs. 1 Nr. 2 AWG).

„**Gebietsfremde**" sind demnach natürliche Personen mit Wohnsitz oder gewöhnlichem Aufenthalt sowie juristische Personen und Personenhandelsgesellschaften mit Sitz oder Ort der Leitung in fremden Wirtschaftsgebieten; Zweigniederlassungen Gebietsansässiger in fremden Wirtschaftsgebieten gelten als Gebietsfremde, wenn sie dort ihre Leitung haben und für sie eine gesonderte Buchführung besteht; entsprechend gelten Betriebsstätten Gebietsansässiger in fremden Wirtschaftsgebieten als Gebietsfremde, wenn sie dort ihre Verwaltung haben (§ 4 Abs. 1 Nr. 7 AWG).

„**Gemeinschaftsgebiet**“ ist das Zollgebiet der Europäischen Gemeinschaften (§ 4 Abs. 1 Nr. 3 AWG).

„**Gemeinschaftsansässige**“ sind die in den Europäischen Gemeinschaften ansässige Personen (§ 4 Abs. 1 Nr. 6 AWG).

„**Drittländer**“ sind demgegenüber alle Gebiete außerhalb des Gemeinschaftsgebiets (§ 4 Abs. 1 Nr. 4 AWG).

„**Gemeinschaftsfremde**“ sind schließlich alle anderen Personen als Gemeinschaftsansässige (§ 4 Abs. 1 Nr. 8 AWG).

2.2 Güter

„**Güter**“ sind Waren und zwar einschließlich Datenverarbeitungsprogrammen (Software) und Technologie; Technologie erfasst dabei auch Unterlagen zur Fertigung von Waren oder Teilen davon (§ 4 Abs. 2 Nr. 3 AWG).

„**Waren**“ sind bewegliche Sachen, die Gegenstand des Handelsverkehrs sein können, einschließlich Elektrizität, nicht jedoch Wertpapiere und Zahlungsmittel (§ 4 Abs. 2 Nr. 2 AWG).

„**Rüstungsgüter**“ sind einerseits Kriegswaffen im Sinne des KrWaffKontrG und andererseits sonstige Rüstungsgüter im Sinne von Teil I A der AL zur AWV.

„**Güter mit doppeltem Verwendungszweck**“ sind solche, die sowohl für zivile als auch für militärische Zwecke verwendet werden können; darin eingeschlossen sind alle Waren, die sowohl für nichtexplosive Zwecke als auch für jedwede Form der Unterstützung bei der Herstellung von Kernwaffen oder sonstigen Kernsprengkörpern verwendet werden können (Art. 2 Abs. 1 EG Dual-Use-VO).

2.3 Ausfuhr, Durchfuhr, Verbringung

„**Ausfuhr**“ im nationalen Sinne ist das Verbringen von Sachen, Gütern und Elektrizität aus dem Wirtschaftsgebiet nach fremden Wirtschaftsgebieten einschließlich der nicht gegenständlichen Übermittlung von Datenverarbeitungsprogrammen und Technologie durch Daten- oder Nachrichtenübertragungstechnik (§ 4 Abs. 2 Nr. 4 AWG).

„**Ausfuhr**“ im europäischen Sinne ist ein Ausfuhrverfahren im des Zollkodex der Gemeinschaften, das heißt die Verbringung von Gemeinschaftswaren aus dem Zollgebiet der Gemeinschaft; ferner eine Wiederausfuhr im Sinne des Zollkodex, sofern Güter nicht bloß durchgeführt werden; und schließlich die Übertragung von Software oder Technologie mittels elektronischer Medien wie Telefax, Telefon, elektronischer Post oder sonstiger elektronischer Träger nach einem Bestimmungsziel außerhalb der Europäischen Gemeinschaft, einschließlich des Bereitstellens (Stichwort: „Download“) solcher Software oder Technologie in elektronischer Form für juristische oder natürliche Personen oder Personenvereinigungen außerhalb der Gemeinschaft sowie der telefonischen Weitergabe von Technologie (Art. 2 Abs. 2 EG Dual-Use-VO).

„**Durchfuhr**" im nationalen Sinne ist die Beförderung von Sachen aus fremden Wirtschaftsgebieten durch das Wirtschaftsgebiet, ohne dass die Sachen im Wirtschaftsgebiet in den zollrechtlich freien Verkehr gelangen, einschließlich der Beförderung von Sachen des zollrechtlich freien Verkehrs aus einem anderen Mitgliedstaat der Europäischen Gemeinschaften durch das Wirtschaftsgebiet (§ 4 Abs. 2 Nr. 7 AWG).

„**Durchfuhr**" im europäischen Sinne ist die Beförderung nichtgemeinschaftlicher Güter mit doppeltem Verwendungszweck in und durch das Zollgebiet der Gemeinschaft zu einem Bestimmungsziel außerhalb der Gemeinschaft (Art. 2 Abs. 7 EG Dual-Use-VO).

„**Verbringung**" ist schließlich ein Sonderfall der Ausfuhr, nämlich im nationalen Sinne die Ausfuhr aus dem Wirtschaftsgebiet in andere Mitgliedstaaten der Europäischen Union (§ 4 Abs. 2 Nr. 5 AWG; s. a. Art. 22 Abs. 1 EG Dual-Use-VO).

3 Beschränkungen des Außenwirtschaftsverkehrs

Der Außenwirtschaftsverkehr kann beschränkt sein entweder aufgrund von Verboten bestimmter Handlungen oder aufgrund der Anordnung eines Genehmigungsvorbehalts (vgl. § 2 Abs. 1 AWG). Gelangt man im Rahmen der Prüfung zu dem Ergebnis, dass die beabsichtigte Handlung einem Verbot unterliegt, erledigt sich jede weitere Überlegung, da es von bestehenden Verboten bereits (in aller Regel) keine Ausnahme gibt.

Das Prüfungsschema muss daher stets wie folgt aussehen:

- Unterliegt die beabsichtigte Handlung einem Verbot?
  Wenn ja: Die Durchführung der Handlung ist nicht möglich!
- Wenn nein: Steht die beabsichtigte Handlung unter einem Genehmigungsvorbehalt?
  Wenn ja: Genehmigung beantragen (sofern nicht Allgemeingenehmigung vorliegt).
- Wenn nein: Die Handlung kann vorgenommen werden.

Bereits an dieser Stelle ist jedoch darauf hinzuweisen, dass der Umstand, dass kein Verbot besteht und das auszuführende Gut auch nicht auf einer der einschlägigen Listen aufgeführt ist, noch nicht bedeutet, dass das Gut ohne vorherige Genehmigung ausgeführt werden darf. Auch die Ausfuhr nicht gelisteter Güter kann unter einem Genehmigungsvorbehalt stehen („catch-all").

3.1 Verbote, insbesondere Embargos

Verbote bestehen zum Beispiel unter dem Anwendungsbereich des **Kriegswaffenkontrollgesetzes** (s. §§ 17ff. KrWaffKontrG betreffend ABC-Waffen und Anti-Personen-Minen) sowie nach den sog. „**Anti-Terror-Listen**", das heißt der Verordnung (EG) Nr. 881/2002 des Rates vom 27. Mai 2002 (Maßnahmen gegen Osama bin Laden, das Al-Qaida-Netzwerk

und die Taliban), der Verordnung (EU) Nr. 753/2011 des Rates vom 1. August 2011 (restriktive Maßnahmen gegen bestimmte Personen, Gruppen, Unternehmen und Einrichtungen angesichts der Lage in Afghanistan) und der Verordnung (EG) Nr. 2580/2001 des Rates vom 27. Dezember 2001(spezifische, gegen bestimmte Personen und Organisationen gerichtete restriktive Maßnahmen zur Bekämpfung des Terrorismus). Zu nennen ist an dieser Stelle zudem die Verordnung (EG) Nr. 1236/2005 DES RATES vom 27. Juni 2005 („**Anti-Folter-Verordnung**").

Besonders hervorzuheben sind jedoch die zahlreichen **EU-Embargos** gegen verschiedene Länder, die oft genug nicht nur länderbezogene, sondern auch personenbezogene Verbote enthalten.[6]

Exemplarisch und aufgrund seiner sehr weitreichenden Beschränkungen sei hier das Iran-Embargo gemäß der Verordnung (EU) Nr. 267/2012 des Rates vom 23. März 2012 genannt, nach deren Art. 2 Abs. 1 es zum Beispiel verboten ist, „die in Anhang I oder II aufgeführten Güter und Technologien mit oder ohne Ursprung in der Union unmittelbar oder mittelbar an iranische Personen, Organisationen oder Einrichtungen oder zur Verwendung in Iran zu verkaufen, zu liefern, weiterzugeben oder auszuführen", oder nach deren Art. 17 Abs. 1 lit. a) „die Gewährung von Darlehen oder Krediten an in Absatz 2 genannte iranische Personen, Organisationen oder Einrichtungen" verboten ist. Deutlich wird hieran, dass die Embargo-Verordnungen wiederum **eigene (Güter- und Personen-) Listen** enthalten, die sorgfältig überprüft sein wollen, bevor man in den Anwendungsbereich der EG Dual-Use-VO und der AWV gelangt.

Von einer ganz besonderen Bedeutung sind in diesem Zusammenhang die sogenannten **Bereitstellungsverbote**, die bereits aufgrund ihrer sehr vagen und mehrdeutigen Formulierung in der Praxis häufig zu Problemen führen. So bestimmt etwa das Iran-Embargo in Art. 23 Abs. 3:

> Den in Anhang VIII und IX aufgeführten natürlichen und juristischen Personen, Organisationen und Einrichtungen dürfen weder unmittelbar noch mittelbar Gelder oder wirtschaftliche Ressourcen zur Verfügung gestellt werden oder zugutekommen.

Aus der Formulierung „dürfen nicht" ergibt sich zunächst einmal, dass es sich hierbei um ein Verbot handelt (sehr eng umgrenzte Ausnahmen und Genehmigungsmöglichkeiten ergeben sich aus Art. 27ff.). Ferner handelt es sich hierbei um eine personenbezogene Maßnahme, die **unabhängig von dem tatsächlichen Aufenthaltsort** oder Sitz der gelisteten Personen gilt; sanktioniert wird hier nicht die Ausfuhr, sondern die Bereitstellung an welchem Ort auch immer.

Fraglich ist jedoch, was mit dem sehr sperrigen Begriff „wirtschaftliche Ressourcen" gemeint ist. Art. 1 lit. h) der Iran-Embargo-Verordnung definiert wirtschaftliche Ressourcen als „Vermögenswerte jeder Art, unabhängig davon, ob sie materiell oder immateriell, beweglich oder unbeweglich sind, bei denen es sich nicht um Gelder handelt, die aber für

[6] Eine laufend aktualisierte Auflistung der bestehenden Embargos findet sich auf der Homepage des BAFA http://www.ausfuhrkontrolle.info/ausfuhrkontrolle/de/embargos/index.html.

den Erwerb von Geldern, Waren oder Dienstleistungen verwendet werden können". Dies bedeutet, dass **jede Lieferung von Handelsgütern an die gelisteten Personen verboten** ist, was im Falle des Iran-Embargos faktisch wie ein Totalembargo wirkt. Die Erbringung von Dienstleistungen soll nach der Auslegung des BAFA dagegen grundsätzlich nicht gegen das Bereitstellungsverbot verstoßen, da mit der Dienstleistung keine wirtschaftliche Ressource erbracht werde. Etwas anderes kann sich freilich dann ergeben, wenn die Dienstleistung entscheidend dazu beiträgt, die Verfügungsgewalt über eine wirtschaftliche Ressource zu verschaffen (Stichwort: Aufbau-, Montage- und Inbetriebnahmeleistungen).

Völlig undurchsichtig wird es dann jedoch spätestens bei der Frage, wann eine „unmittelbare" und wann eine „mittelbare" Bereitstellung wirtschaftlicher Ressourcen (oder Gelder) vorliegt bzw. was der Unterschied ist. Eine gesetzliche Definition fehlt, es handelt sich um unbestimmte Rechtsbegriffe.

Nach der Auslegung des **BAFA** soll eine mittelbare Bereitstellung jedenfalls dann vorliegen, „wenn eine Güterlieferung an ein nicht gelistetes Unternehmen erfolgt, an dem ein gelistetes Unternehmen 50 % oder mehr der Geschäftsanteile hält oder auf Grund anderweitiger Sonderrechte ein beherrschender Einfluss des gelisteten auf das nicht gelistete Unternehmen wie ein Mehrheitsgesellschafter anzunehmen ist".[7]

Der **Bundesgerichtshof** hat darauf abgestellt, dass eine unmittelbare Bereitstellung den tatsächlichen Vorgang des Zur-Verfügung-Stellens betrifft, also einen Realakt (z. B. Zahlung, Lieferung, nicht aber Vertragsabschluss). Demgegenüber liege eine mittelbare Bereitstellung z. B. vor bei der Lieferung wirtschaftlicher Ressourcen an nicht gelistete Dritte, die aber zur Weitergabe an gelistete Personen bereit sind. Allerdings müsse die gelistete Person auch auf die wirtschaftliche Ressource zugreifen können, sonst fehle es an der notwendigen Verbesserung ihrer materiellen Grundlage. Ziel des Verbotes sei nämlich gerade die Verhinderung des Zugriffs auf wirtschaftliche Ressourcen; den gelisteten Personen solle die materielle Grundlage ihrer Tätigkeit entzogen werden.[8]

Wiederum anders sieht es der **Europäische Gerichtshof**: Entgegen der Auffassung des Bundesgerichtshof sei (unmittelbare) Bereitstellung nicht nur die Verschaffung der vollständigen Verfügungsbefugnis, sondern bereits jede Handlung, die erforderlich ist, damit eine Person die Verfügungsbefugnis über den Vermögenswert erlangen kann. Dazu gehörten z. B. nicht nur die Lieferung und das Aufstellen des Vermögenswertes, sondern auch Handlungen zur Vorbereitung und Überwachung der Lieferung/Aufstellung oder die Kontaktvermittlung. Es sei nicht erforderlich, dass der Vermögenswert nach seiner Lieferung oder Aufstellung sofort verwendungsbereit ist. Ein mittelbares Bereitstellen könne vorliegen bei der Lieferung an einen nicht gelisteten Dritten, der im Namen, unter der Kontrolle oder auf Weisung einer gelisteten Person handelt. Das Bereitstellungsverbot sei nach sei-

[7] Merkblatt des Bundesamtes für Wirtschaft und Ausfuhrkontrolle zum „Außenwirtschaftsverkehr mit dem Iran", Stand 04.07.2012.

[8] BGH, Beschluss vom 23.04.2010, AK 2/10.

nem Sinn und Zweck **auf alle Personen, die an der untersagten Handlung beteiligt sind, zu erstrecken**.[9]

Die Tendenz geht also dahin, den Anwendungsbereich der EU-Embargos und speziell der Bereitstellungsverbote möglichst weit zu fassen, was es für den Unternehmer nur noch schwerer macht: Es lässt sich in bestimmten Fällen kaum noch abschätzen, welche Handlung erlaubt und welche verboten ist.

Insofern verwundert es nicht, wenn in der Praxis nach Wegen gesucht wird, ein beabsichtigtes Liefergeschäft durchführen zu können, das möglicherweise verboten ist. An dieser Stelle greifen dann aber weitere Wirtschaftssanktionen in Form der sogenannten **Umgehungsverbote** ein. Ein solches findet sich ebenfalls in der Iran-Embargo-Verordnung, wenn es in deren Art. 41 heißt: *„Es ist verboten, wissentlich und absichtlich an Tätigkeiten teilzunehmen, mit denen die Umgehung der in Artikel (. . .) 23 (. . .) genannten Maßnahmen bezweckt oder bewirkt wird."*

Nach der Rechtsprechung des Europäischen Gerichtshofes werden hiervon Aktivitäten erfasst, die unter dem Deckmantel einer Form vorgenommen werden, mit der eine Verwirklichung des Bereitstellungsverbotes vermieden wird, die jedoch unmittelbar oder mittelbar bezwecken, das Bereitstellungsverbot auszuhebeln.[10]

Auch hieraus wird deutlich, dass eine umfassende und möglichst lückenlose Sanktionierung gewollt ist und jeder Versuch einer Umgehung der Embargo-Verbote (straf-) rechtliche Konsequenzen nach sich ziehen kann. Die mit den EU-Embargos angeordneten Verbote sind daher sehr ernst zu nehmen.

3.2 Genehmigungsvorbehalte

Ist eine bestimmte Handlung nicht bereits per se verboten, kann sie unter einem Genehmigungsvorbehalt stehen.

Im Bereich der Embargos ist an dieser Stelle exemplarisch die Kontrolle von **Finanztransaktionen** zu nennen. So sind etwa im Rahmen des Iran-Embargos Geldtransfers an eine iranische Person, Organisation oder Einrichtung oder von einer solchen iranischen Person, Organisation oder Einrichtung ab einem Betrag von 40.000,00 € in der Regel genehmigungspflichtig (vgl. Art. 30a Abs. 1 lit. c des Iran-Embargos in der Fassung der Verordnung (EU) Nr. 1263/2012 des Rates vom 21. Dezember 2012). Zuständig für die Erteilung einer solchen Genehmigung ist innerhalb Deutschlands die Deutsche Bundesbank, wobei die Genehmigung im Regelfalle aber nicht etwa von dem Auftraggeber oder Begünstigten, sondern vielmehr von dem Kreditinstitut zu beantragen ist. Das heißt, ein deutsches Kreditinstitut würde z. B. eine Zahlung aus Iran zunächst entgegennehmen, müsste aber sodann die Genehmigung bei der Deutschen Bundesbank beantragen, bevor es die Zahlung dem Konto des Begünstigten gutschreiben darf. Der damit einhergehende Verwaltungsaufwand sowie die Sorge, bei der Ausführung derartiger Finanztransaktionen gegen

[9] EuGH, Urteil vom 21.12.2011, C-72/11.

[10] EuGH, a. a. O.

US-amerikanische Sanktionen zu verstoßen, haben dazu geführt, dass nahezu sämtliche europäischen Kreditinstitute die Bearbeitung von Geldtransfers mit Iran-Bezug mittlerweile schlicht ablehnen. Europäische Exporteure sehen sich mit dem Problem konfrontiert, dass an sich unbedenkliche und genehmigungsfreie oder einer bestehenden Allgemeingenehmigung unterfallende Rechtsgeschäfte praktisch nicht durchführbar sind, weil die Frage der Finanzierung und Bezahlung zumindest auf den herkömmlichen Wegen nicht geklärt ist. Stattdessen wird dann nach alternativen Zahlungswegen gesucht, was aber sogleich die Gefahr in sich birgt, mit dem Vorwurf der Umgehung einer Embargo-Vorschrift konfrontiert zu werden.

Im Bereich des **Warenverkehrs**, also der Ausfuhr, Verbringung oder Durchfuhr von Gütern in dem o. g. Sinne einschließlich Software und Technologie, ist zu unterscheiden zwischen

- dem Export von Kriegswaffen, dessen Zulässigkeit sich nach dem KrWaffKontrG richtet,
- dem Export von sonstigen Rüstungsgütern, dessen Genehmigungsfähigkeit sich nach dem AWG sowie der AWV richtet, sowie
- dem Export von Gütern mit doppeltem Verwendungszweck („Dual-Use-Güter"), für den sowohl das AWG in Verbindung mit der AWV, insbesondere aber die EG Dual-Use-VO Genehmigungsvorbehalte vorsehen.

Kriegswaffen sind gemäß § 1 Abs. 1 KrWaffKontrG all diejenigen Gegenstände, die in der dem Gesetz als Anlage beigefügten Kriegswaffenliste (KWL) genannt sind. Das Gesetz und die KWL unterscheiden dabei wiederum zwischen Massenvernichtungswaffen (Teil A der KWL), also Atomwaffen sowie biologische und chemische Waffen, und sonstigen Kriegswaffen (Teil B der KWL), dies sind insbesondere Flugkörper, Kampfflugzeuge und Kampfhubschrauber, Kriegsschiffe, Kampffahrzeuge, Rohrwaffen, Panzerabwehrwaffen, Torpedos, Minen, Bomben, bestimmte Munition, bestimmte wesentliche Bestandteile von Kriegswaffen sowie bestimmte Laserwaffen.

Während die Entwicklung, Herstellung und jegliche Form des Überlassens von **Massenvernichtungswaffen** sowie die Förderung derartiger Handlungen schlicht verboten ist (vgl. §§ 17ff KrWaffKontrG), besteht für die Herstellung und die Beförderung von bzw. den Handel mit **sonstigen Kriegswaffen** die Möglichkeit der Erteilung einer Genehmigung. Insoweit sei auf die Regelungen in §§ 2ff KrWaffKontrG verwiesen. Entscheidend ist hier der Grundsatz, dass jeder Export von Kriegswaffen einer Genehmigung bedarf, sofern er nicht bereits verboten ist.

Im Bereich der **sonstigenRüstungsgüter**, also Waffen, Munition und Rüstungsmaterial im Sinne des Teils I A der Ausfuhrliste (AL) zur AWV, gilt, dass sowohl die Ausfuhr aus Deutschland in ein Land, das nicht zur EU gehört (§ 5 Abs. 1 AWV), als auch die Verbringung aus Deutschland in einen EU-Mitgliedstaat (§ 7 Abs. 1 AWV) der Genehmigung bedarf. Von der Genehmigungspflicht im Rahmen der Verbringung gibt es allerdings drei Ausnahmen, nämlich für bestimmte Feuerwaffen, bestimmte Munition und Wiederladegeräte für derartige Munition.

Die Exportkontrolle von **Gütern mit doppeltem Verwendungszweck („Dual-Use-Güter“)** ist, wie eingangs bereits dargestellt wurde, anhand von zwei Rechtsquellen vorzunehmen: zunächst nach der EG Dual-Use-VO und sodann nach der AWV.

Gemäß Art. 3 Abs. 1 EG Dual-Use-VO bedarf die *Ausfuhr* der in Anhang I gelisteten Dual-Use-Güter aus dem Zollgebiet der Gemeinschaft der vorherigen Genehmigung. Entsprechendes gilt gemäß § 5 Abs. 2 AWV für die Ausfuhr der in Teil I C der AL in den Kennungen 901 bis 999 gelisteten Dual-Use-Güter aus Deutschland in ein Land, das nicht zur EU gehört.

Die innergemeinschaftliche *Verbringung* ist gemäß Art. 22 Abs. 1 EG Dual-Use-VO genehmigungspflichtig in Bezug auf solche Dual-Use-Güter, die in Anhang IV gelistet sind. Ergänzend sieht § 7 Abs. 2 AWV vor, dass die Verbringung von Dual-Use-Gütern des Teils I C der AL aus Deutschland in einen EU-Mitgliedstaat der vorherigen Genehmigung bedarf, wenn dem Verbringer bekannt ist, dass das endgültige Bestimmungsziel der Güter außerhalb der Europäischen Union liegt.

Gemäß Art. 6 Abs. 1 und 2 EG Dual-Use-VO kann die *Durchfuhr* nichtgemeinschaftlicher Dual-Use-Güter, die in Anhang I aufgeführt sind, schließlich von den jeweils zuständigen Behörden des Mitgliedstaats, durch den die Güter durchgeführt werden, verboten werden, wenn die Güter ganz oder teilweise für einen der in Art. 4 Absatz 1 genannten Verwendungszwecke bestimmt sind oder bestimmt sein können (das heißt zur Verwendung im Zusammenhangmit der Entwicklung, der Herstellung, der Handhabung, dem Betrieb, der Wartung, der Lagerung, der Ortung, der Identifizierung oder der Verbreitung von chemischen, biologischen oder Kernwaffen oder sonstigen Kernsprengkörpern oder zur Entwicklung, Herstellung, Wartung oder Lagerung von Flugkörpern für derartige Waffen). Ein Mitgliedstaat kann aber vorsehen, dass, bevor eine Entscheidung über ein Durchfuhrverbot getroffen wird, seine zuständigen Behörden in Einzelfällen eine Genehmigungspflicht für die betreffende Durchfuhr auferlegen können. Die entsprechende Ermächtigungsnorm auf nationaler Ebene findet sich in § 38 AWV.

3.3 „catch-all“: Genehmigungspflichten bei nicht gelisteten Gütern

Die Überprüfung einer bestehenden Genehmigungspflicht oder gar eines Verbotes anhand der Güterlisten (Embargo-Listen, KWL zum KrWaffKontrG, Teil I A und C der AL zur AWV, Anhänge I und IV zur EG Dual-Use-VO) mag zumindest in der Theorie relativ einfach erscheinen (praktisch kann allerdings die Einordnung eines Gutes durchaus erhebliche Fragen und Probleme aufwerfen, die nur ein technisch versierter Spezialist beantworten kann). Kompliziert wird es jedoch, soweit auch der Export von *nicht* gelisteten Gütern gemäß Art. 4 Abs. 1 bis 3 EG Dual-Use-VO bzw. §§ 5c, 5d, 7 Abs. 3 und 4 AWV unter einen Genehmigungsvorbehalt gestellt wird.

Hintergrund der Einführung derartiger Auffangtatbestände („catch-all“) ist der Umstand, dass schon aufgrund der ständigen technologischen Weiterentwicklung naturgemäß nicht alle bedenklichen oder sensitiven Güter in Listen erfasst werden können bzw. die Aktualisierung der Listen kaum mit dem technologischen Fortgang Schritt halten kann.

Genehmigungspflichtig ist gemäß Art. 4 Abs. 1 EG Dual-Use-VO die Ausfuhr nicht gelisteter Dual-Use-Güter, wenn der Ausführer von den zuständigen Behörden des Mitgliedstaats, in dem er niedergelassen ist, davon unterrichtet worden ist, dass diese Güter ganz oder teilweise bestimmt sind oder bestimmt sein können zur Verwendung im Zusammenhang mit chemischen, biologischen oder Kernwaffen oder Flugkörpern für derartige Waffen.

Weiterhin genehmigungspflichtig ist gemäß Art. 4 Abs. 2 EG Dual-Use-VO die Ausfuhr nicht gelisteter Dual-Use-Güter, wenn gegen das Käufer- oder Bestimmungsland ein Waffenembargo verhängt wurde und wenn der Ausführer von den zuständigen Behörden des Mitgliedstaats, in dem er niedergelassen ist, davon unterrichtet worden ist, dass diese Güter ganz oder teilweise für eine militärische Endverwendung bestimmt sind oder bestimmt sein können.

Genehmigungspflichtig ist schließlich gemäß Art. 4 Abs. 3 EG Dual-Use-VO die Ausfuhr nicht gelisteter Dual-Use-Güter, wenn der Ausführer von den zuständigen Behörden des Mitgliedstaats, in dem er niedergelassen ist, davon unterrichtet worden ist, dass diese Güter ganz oder teilweise für die Verwendung als Bestandteile von militärischen Gütern bestimmt sind oder bestimmt sein können, die in der nationalen Militärliste aufgeführt sind und aus dem Hoheitsgebiet dieses Mitgliedstaats ohne Genehmigung oder unter Verstoß gegen eine aufgrund innerstaatlicher Rechtsvorschriften dieses Mitgliedstaats erteilte Genehmigung ausgeführt wurden.

Diesen drei Genehmigungstatbeständen ist mithin gemein, dass es zunächst auf den **Verwendungszweck** des jeweiligen Gutes ankommt, es nur um die **Ausfuhr** von Gütern geht und der Ausführer aufgrund einer Unterrichtung durch die zuständigen Behörden **positive Kenntnis** von dem Verwendungszweck haben muss.

Doch Vorsicht: Hat der Ausführer aus anderen Quellen positive Kenntnis von einem dieser Verwendungszwecke, trifft ihn gemäß Art. 4 Abs. 4 EG Dual-Use-VO die Pflicht, die zuständigen Behörden des Mitgliedstaats, in dem er niedergelassen ist, von der beabsichtigten Ausfuhr zu unterrichten. Die Behörden entscheiden sodann, ob die Ausfuhr einer Genehmigung bedarf.

Ergänzend sind die catch-all-Regelungen auf nationaler Ebene zu beachten. So bedarf gemäß § 5c Abs. 1 AWV die Ausfuhr nicht gelisteter Güter der Genehmigung, wenn der Ausführer vom Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) darüber unterrichtet worden ist, dass diese Güter ganz oder teilweise für eine militärische Endverwendung bestimmt sind oder bestimmt sein können und das Käufer- oder Bestimmungsland ein Land der sog. „Länderliste K" ist, auf welcher aktuell allerdings nur Kuba steht. Hat er diese Kenntnis aus anderen Quellen erlangt, trifft ihn gemäß § 5c Abs. 2 AWV auch hier die Pflicht, das BAFA über die beabsichtigte Ausfuhr zu unterrichten.

Genehmigungspflichtig ist gemäß § 5d Abs. 1 AWV auch die Ausfuhr nicht gelisteter Güter, wenn der Ausführer vom BAFA darüber unterrichtet worden ist, dass diese Güter ganz oder teilweise für die Errichtung, den Betrieb oder zum Einbau in eine Anlage für kerntechnische Zwecke im Sinne der Kategorie O des Teils I Abschnitt C der Ausfuhrliste (Anlage AL) bestimmt sind oder bestimmt sein können und das Käufer- oder

Bestimmungsland Algerien, Irak, Iran, Israel, Jordanien, Libyen, Nordkorea, Pakistan oder Syrien ist. Eine Unterrichtungspflicht des Ausführers besteht wiederum gemäß § 5d Abs. 2 AWV.

Doch nicht nur die Ausfuhr in ein Land, das nicht zur EU gehört, sondern auch die **Verbringung** von nicht gelisteten Gütern aus Deutschland in einen anderen EU-Mitgliedstaat bedarf gemäß § 7 Abs. 3 AWV der Genehmigung, wenn das endgültige Bestimmungsziel der Güter außerhalb der Europäischen Union liegt und der Verbringer vom BAFA darüber unterrichtet worden ist, dass diese Güter ganz oder teilweise für eine militärische Endverwendung im Sinne des § 5c Abs. 1 Satz 2 AWV bestimmt sind oder bestimmt sein können und das Käufer- oder Bestimmungsland ein Land der Länderliste K oder gegen das Land ein Waffenembargo verhängt wurde. Hat der Ausführer die positive Kenntnis hierüber aus anderen Quellen erlangt, besteht auch hier eine Unterrichtungspflicht.

Entsprechendes gilt gemäß § 7 Abs. 4 AWV schließlich für die Verbringung nicht gelisteter Güter, wenn es um einen Fall des § 5d Abs. 1 AWV geht, wenn also das endgültige Bestimmungsziel der Güter außerhalb der Europäischen Union liegt und der Verbringer vom BAFA darüber unterrichtet worden ist, dass diese Güter ganz oder teilweise für die Errichtung, den Betrieb oder zum Einbau in eine Anlage für kerntechnische Zwecke im Sinne der Kategorie O des Teils I Abschnitt C der Ausfuhrliste (Anlage AL) bestimmt sind oder bestimmt sein können und das Käufer- oder Bestimmungsland Algerien, Irak, Iran, Israel, Jordanien, Libyen, Nordkorea, Pakistan oder Syrien ist. Es ist fast schon müßig zu erwähnen, dass die vorgenannte Unterrichtungspflicht des Ausführers im Falle der anderweitigen Kenntniserlangung auch hier besteht.

3.4 Vermittlungstätigkeiten („Brokering“)

Nicht nur der Export im engeren Sinne, also die Ausfuhr, Verbringung oder Durchfuhr von Gütern einschließlich Software und Technologie, sei es in Form des körperlichen Überlassens, sei es in Form der nicht gegenständlichen Übermittlung durch Daten- oder Nachrichtenübertragungstechnik, unterliegt Einschränkungen. Auch damit im Zusammenhang stehende Vermittlungstätigkeiten unterstehen einer „Exportkontrolle“. Unter Vermittlungstätigkeiten oder Vermittlungsdiensten („Brokering“) versteht man ganz allgemein die Aushandlung oder Veranlassung bzw. das Herbeiführen, eben die Vermittlung eines Vertrages oder den Nachweis der Gelegenheit zum Abschluss eines Vertrages, also eine Maklertätigkeit, die allerdings auch unentgeltlich erfolgen kann; auf eine Vergütung der Vermittlungstätigkeit kommt es nicht an. Ebenfalls unter den Begriff der Vermittlungstätigkeit fällt zudem der Abschluss des Vertrages selbst, falls er lediglich zwecks Verbringung des Leistungsgegenstands in ein Drittland erfolgt, der Vermittler also bloß als Zwischenhändler auftritt.

Im Detail unterscheiden sich die Begrifflichkeiten dann allerdings, je nachdem welche Rechtsnorm einschlägig ist:

Im Rahmen der **Embargos**, hier speziell des Iran-Embargos, geht es bei den Vermittlungsdiensten um die Vermittlung von Transaktionen zum Kauf, zum Verkauf oder zur Lieferung von Gütern und Technologien oder von Finanzdienstleistungen oder technischen Dienstleistungen, nicht nur, sondern „auch" von einem Drittland aus in ein anderes Drittland, oder aber den Verkauf oder Kauf von Gütern oder von Finanzdienstleistungen oder technischen Dienstleistungen und zwar wiederum nicht nur, sondern „auch" dann wenn sie sich in Drittländern befinden, zwecks Verbringung in ein anderes Drittland (Art. 1 lit. b des Iran-Embargos).

Verboten ist sodann gemäß Art. 5 Abs. 1 lit. b und Art. 9 lit. a des Iran-Embargos die unmittelbare oder mittelbare Erbringung derartiger Vermittlungsdienste für iranische Personen, Organisationen oder Einrichtungen oder zur Verwendung in Iran im Zusammenhang mit den in Anhang I oder II des Iran-Embargos aufgeführten Gütern oder der in Anhang VI aufgeführten Schlüsselausrüstung und -technologie, mag es auch nur um deren Bereitstellung, Wartung oder Verwendung gehen. Die Erbringung von solchen Vermittlungsdiensten im Zusammenhang mit den in Anhang III aufgeführten Gütern kann gemäß Art. 5 Abs. 2 lit. a des Iran-Embargos hingegen genehmigt werden.

In diesem Zusammenhang ist auch noch einmal auf die oben bereits angeführte Rechtsprechung des Europäischen Gerichtshofes hinzuweisen, der entgegen der Auffassung des Bundesgerichtshofes eine verbotene Bereitstellung wirtschaftlicher Ressourcen im Sinne von Art. 23 Abs. 3 des Iran-Embargos an gelistete Personen nicht nur in der Verschaffung der vollständigen Verfügungsbefugnis sieht, sondern bereits in jeder Handlung, die erforderlich ist, damit eine Person die Verfügungsbefugnis über den Vermögenswert erlangen kann. Dazu gehören nach Auffassung des Europäischen Gerichtshofes nicht nur die Lieferung und das Aufstellen des Vermögenswertes, sondern auch Handlungen zur Vorbereitung und Überwachung der Lieferung/Aufstellung oder die Kontaktvermittlung. Es sei nicht erforderlich, dass der Vermögenswert nach seiner Lieferung oder Aufstellung sofort verwendungsbereit ist. Ein mittelbares Bereitstellen könne vorliegen bei der Lieferung an einen nicht gelisteten Dritten, der im Namen, unter der Kontrolle oder auf Weisung einer gelisteten Person handelt. Das Bereitstellungsverbot sei nach seinem Sinn und Zweck auf alle Personen, die an der untersagten Handlung beteiligt sind, zu erstrecken.[11]

Anders als im Rahmen des Iran-Embargos regelt die **EG Dual-Use-VO** hingegen ausschließlich Vermittlungstätigkeiten mit „Drittlandsbezug", das heißt der Vermittler muss in der EU ansässig sein, während es um eine Warenbewegung von einem Drittland in ein anderes Drittland geht. Der Begriff „Vermittlungstätigkeiten" bezeichnet nämlich so wörtlich die Aushandlung oder das Herbeiführen von Transaktionen zum Kauf, zum Verkauf oder zur Lieferung von Gütern mit doppeltem Verwendungszweck „von einem Drittland in ein anderes Drittland", oder den Verkauf oder Kauf von Gütern mit doppeltem Verwendungszweck, die sich in Drittländern befinden, zwecks Verbringung in ein anderes Drittland (Art. 2 Nr. 5 und 6 EG Dual-Use-VO). Ausdrücklich ausgenommen ist hier allerdings die ausschließliche Erbringung von Hilfsleistungen, nämlich Beförderung,

[11] EuGH, Urteil vom 21.12.2011, C-72/11.

Finanzdienstleistungen, Versicherung oder Rückversicherung oder allgemeine Werbung oder Verkaufsförderung.

Tatbestandlich „kombiniert" die EG Dual-Use-VO sodann das Erfordernis der Listung eines Dual-Use-Gutes mit den oben erläuterten „catch-all" Kriterien: So bedarf gemäß Art. 5 Abs. 1 EG Dual-Use-VO die Erbringung einer Vermittlungstätigkeit in Bezug auf Güter mit doppeltem Verwendungszweck, die in Anhang I aufgeführt sind, einer Genehmigung, wenn der Vermittler von den zuständigen Behörden des Mitgliedstaats, in dem er ansässig oder niedergelassen ist, darüber unterrichtet wurde, dass die betreffenden Güter ganz oder teilweise bestimmt sind oder bestimmt sein können zur Verwendung im Zusammenhang mit chemischen, biologischen oder Kernwaffen oder Flugkörpern für derartige Waffen. Ist dem Vermittler anderweitig bekannt, dass die in Anhang I aufgeführten Güter mit doppeltem Verwendungszweck, für die er Vermittlungstätigkeiten anbietet, ganz oder teilweise für einen solchen Verwendungszwecke bestimmt sind, so hat er die zuständigen Behörden davon zu unterrichten; diese entscheiden sodann, ob die Erbringung dieser Vermittlungstätigkeiten genehmigungspflichtig sein soll.

Innerhalb der **AWV** bezeichnet eine Vermittlungstätigkeit das Vermitteln eines Vertrages über den Erwerb oder das Überlassen von Gütern oder den Nachweis einer Gelegenheit zum Abschluss eines solchen Vertrages oder den Abschluss eines Vertrages über das Überlassen von Gütern („Handels- und Vermittlungsgeschäft"); ebenfalls ausgenommen ist hier die ausschließliche Erbringung von Hilfsleistungen, dies sind auch hier Beförderung, Finanzdienstleistungen, Versicherung oder Rückversicherung oder allgemeine Werbung oder Verkaufsförderung (§ 4c Nr. 6 AWV). Sodann ist zu unterscheiden, um was für eine Art von Gut es sich handelt:

Die Vornahme eines Handels- und Vermittlungsgeschäftes über sonstige Rüstungsgüter im Sinne von Teil I A der AL zur AWV bedarf gemäß § 40 Abs. 1 AWV der vorherigen Genehmigung, wenn sich die Güter entweder in einem Drittland oder zwar im Wirtschaftsgebiet befinden, aber noch nicht einfuhrrechtlich abgefertigt sind, und in ein anderes Drittland ausgeführt werden sollen.

Die Vornahme eines Handels- und Vermittlungsgeschäftes über die in Teil I C der AL in den Kennungen 901 bis 999 gelisteten Dual-Use-Güter bedarf gemäß § 41 Abs. 1 AWV der Genehmigung, wenn sich die Güter entweder in einem Drittland oder zwar im Wirtschaftsgebiet befinden, aber noch nicht einfuhrrechtlich abgefertigt sind, und in ein anderes Drittland ausgeführt werden sollen, und wenn der Vermittler vom BAFA zudem darüber unterrichtet worden ist, dass diese Güter ganz oder teilweise bestimmt sind oder bestimmt sein können zur Verwendung im Zusammenhang mit chemischen, biologischen oder Kernwaffen oder Flugkörpern für derartige Waffen und wenn das Käufer- oder Bestimmungsland in den Kennungen 901 bis 999 der AL genannt ist. Hat der Vermittler von diesen Voraussetzungen anderweitig positive Kenntnis erlangt, trifft ihn gemäß § 41 Abs. 2 AWV die Pflicht, das BAFA hiervon zu unterrichten.

Die Vornahme eines Handels- und Vermittlungsgeschäftes über die in Anhang IV der EG Dual-Use-VO gelisteten Dual-Use-Güter bedarf gemäß § 41a Abs. 1 AWV der Genehmigung, wenn sich die Güter entweder in einem Drittland oder zwar im Wirtschaftsgebiet

befinden, aber noch nicht einfuhrrechtlich abgefertigt sind, und in ein anderes Drittland ausgeführt werden sollen, und wenn der Vermittler vom BAFA darüber unterrichtet worden ist, dass diese Güter ganz oder teilweise für einen der Verwendungszwecke und Bestimmungsländer des Art. 4 Abs. 2 EG Dual-Use-VO bestimmt sind oder bestimmt sein können. Sofern der Vermittler die positive Kenntnis von diesen Voraussetzungen aus anderen Quellen erlangt hat, trifft ihn gemäß § 41a Abs. 2 AWV wiederum eine Unterrichtungspflicht.

Die Vornahme von Handels- und Vermittlungsgeschäften, die durch gebietsansässige Deutsche in einem Drittland vorgenommen werden, bedürfen gemäß § 42 Abs. 1 AWV der Genehmigung, wenn das Käufer- oder Bestimmungsland ein Embargoland im Sinne von Art. 4 Abs. 2 EG Dual-Use-VO ist oder auf der Länderliste K steht (derzeit nur Kuba) oder wenn sich das Geschäft auf die in § 42 Abs. 1 Nr. 2 AWV genannten Kriegswaffen bezieht.

Die Vornahme eines Handels- und Vermittlungsgeschäftes durch einen gebietsansässigen Deutschen in einem Drittland in Bezug auf Güter mit doppeltem Verwendungszweck, die in Anhang I der EG Dual-Use-VO aufgeführt sind und sich entweder in einem Drittland oder zwar im Wirtschaftsgebiet befinden, aber noch nicht einfuhrrechtlich abgefertigt sind, und in ein anderes Drittland ausgeführt werden sollen, bedarf gemäß § 42 Abs. 2 AWV einer Genehmigung, wenn der Vermittler vom BAFA darüber unterrichtet worden ist, dass diese Güter ganz oder teilweise bestimmt sind oder bestimmt sein können zur Verwendung im Zusammenhang mit chemischen, biologischen oder Kernwaffen oder Flugkörpern für derartige Waffen. Hat der Vermittler von diesen Voraussetzungen anderweitig positive Kenntnis erlangt, trifft ihn gemäß § 42 Abs. 3 AWV die Pflicht, das BAFA hiervon zu unterrichten.

Das **KrWaffKontrG** schließlich regelt, dass derjenige, der einen Vertrag über den Erwerb oder das Überlassen von Kriegswaffen, die sich außerhalb des Bundesgebietes befinden, vermitteln oder die Gelegenheit zum Abschluss eines solchen Vertrags nachweisen will, der Genehmigung bedarf (§ 4a Abs. 1 KrWaffKontrG).

3.5 Dienstleistungen, technische Unterstützung

Schließlich kann auch die Erbringung von Dienst- und Serviceleistungen und technischer Unterstützung bzw. Hilfe exportkontrollrechtlichen Einschränkungen unterliegen, denn wer erst einmal im Besitz des erforderlichen Know-how ist, könnte ein sanktioniertes Gut unter Umständen selbst produzieren und wäre auf dessen gegenständliche Überlassung gar nicht mehr angewiesen. Im Fokus der Exportkontrolle steht daher auch die geistige sowie manuelle technische Hilfeleistung, etwa in Form von Ausbildungs- und Lehrtätigkeiten oder durch Montage- und Inbetriebnahmeleistungen.

Häufig wird es dabei zu Überschneidungen mit der Exportkontrolle im eigentlichen Sinne kommen, also mit der Einschränkung der Warenausfuhr. So ist es zur Vornahme einer Wartungs- oder Reparaturleistung regelmäßig erforderlich, zuvor das benötigte

Werkzeug und gegebenenfalls Ersatzteile in das Bestimmungsland auszuführen und bereits diese Ausfuhr könnte unter einem Genehmigungsvorbehalt stehen. Ebenso kann es sich bei vermeintlichen Dienstleistungen tatsächlich um Ausfuhren handeln, etwa wenn eine Beratung mittels Übersendung bestimmter Unterlagen erfolgt und diese Unterlagen Technologien enthalten.

Die EG Dual-Use-VO enthält keine Regelungen in Bezug auf die Einschränkung der Erbringung technischer Hilfeleistungen. Wohl aber finden sich auf europäischer Ebene derartige Beschränkungen in den einschlägigen **Embargos**. So ist z. B. gemäß Art. 1 lit. r des Iran-Embargos „technische Hilfe" jede technische Unterstützung im Zusammenhang mit Reparaturen, Entwicklung, Herstellung, Montage, Erprobung, Wartung oder jeder anderen technischen Dienstleistung, wobei diese in Form von Anleitung, Beratung, Ausbildung, Weitergabe von praktischen Kenntnissen oder Fertigkeiten oder in Form von Beratungsdiensten erfolgen kann, einschließlich Hilfe in verbaler Form.

Verboten ist gemäß Art. 5 Abs. 1 lit. a und b sowie Art. 9 lit. a des Iran-Embargos die unmittelbare oder mittelbare technische Hilfe für iranische Personen, Organisationen oder Einrichtungen oder zur Verwendung in Iran im Zusammenhang mit den in der Gemeinsamen Militärgüterliste aufgeführten Gütern und Technologien oder im Zusammenhang mit der Bereitstellung, Herstellung, Wartung und Verwendung der in dieser Liste aufgeführten Güter sowie im Zusammenhang mit den in Anhang I oder II des Iran-Embargos aufgeführten Gütern oder der in Anhang VI aufgeführten Schlüsselausrüstung und -technologie, mag es auch nur um deren Bereitstellung, Wartung oder Verwendung gehen. Die Erbringung technischer Hilfe im Zusammenhang mit den in Anhang III aufgeführten Gütern kann gemäß Art. 5 Abs. 2 lit. a des Iran-Embargos hingegen genehmigt werden.

Darüber hinaus kann gemäß Art. 37 des Iran-Embargos die Erbringung von Bunker-, Versorgungs- oder Wartungsdiensten für im Eigentum oder unter der direkten oder indirekten Kontrolle von iranischen Personen, Organisationen oder Einrichtungen stehende Schiffe unter den dort genannten Voraussetzungen verboten sein, ebenso die Erbringung von technischen und Wartungsdiensten für im Eigentum oder unter der direkten oder indirekten Kontrolle von iranischen Personen, Organisationen oder Einrichtungen stehende Frachtflugzeuge.

Auch hier sei zudem nochmals auf die oben bereits angeführte Rechtsprechung des Europäischen Gerichtshofes zu dem Bereitstellungsverbot gemäß Art. 23 Abs. 3 des Iran-Embargos hingewiesen, dessen Zweck es schließlich sei, alle an der untersagten Handlung beteiligte Personen zu erfassen.[12]

Auf nationaler Ebene geht es im Rahmen der **AWV** um jede technische Unterstützung in Verbindung mit der Reparatur, der Entwicklung, der Herstellung, der Montage, der Erprobung, der Wartung oder jeder anderen technischen Dienstleistung, wobei die technische Unterstützung in Form von Unterweisung, Ausbildung, Weitergabe von praktischen Kenntnissen oder Fähigkeiten oder in Form von Beratungsleistungen erfolgen kann

[12] EuGH, Urteil vom 21.12.2011, C-72/11.

und auch mündliche, fernmündliche und elektronische Formen der Unterstützung erfasst (§ 4c Nr. 7 AWV).

Sodann kann gemäß § 45 Abs. 1 AWV die Erbringung technischer Unterstützung außerhalb des Gemeinschaftsgebietes durch Gebietsansässige (einschließlich nicht gebietsansässiger Deutschen, § 45d AWV) der vorherigen Genehmigung bedürfen, wenn der Gebietsansässige vom BAFA darüber unterrichtet worden ist, dass diese technische Unterstützung zur Verwendung im Zusammenhang mit chemischen, biologischen oder Kernwaffen oder Flugkörpern für derartige Waffen bestimmt ist. Hat der Vermittler von diesen Voraussetzungen anderweitig positive Kenntnis erlangt, trifft ihn gemäß § 45 Abs. 2 AWV die Pflicht, das BAFA hiervon zu unterrichten.

Ebenfalls kann die Erbringung technischer Unterstützung außerhalb des Gemeinschaftsgebietes durch Gebietsansässige (wiederum einschließlich nicht gebietsansässiger Deutschen) gemäß § 45a Abs. 1 AWV der vorherigen Genehmigung bedürfen, wenn der Gebietsansässige vom BAFA darüber unterrichtet worden ist, dass die technische Unterstützung im Zusammenhang mit einer militärischen Endverwendung steht und in einem Embargoland im Sinne des Art. 4 Abs. 2 EG Dual-Use-VO oder in einem Land der Länderliste K (derzeit nur Kuba) erbracht wird. Sofern der Gebietsansässige die positive Kenntnis von diesen Voraussetzungen aus anderen Quellen erlangt hat, trifft ihn gemäß § 45a Abs. 2 AWV wiederum eine Unterrichtungspflicht.

Für die technische Unterstützung innerhalb des Wirtschaftsgebietes durch Gebietsansässige (oder nicht gebietsansässige Deutsche) enthält § 45b Abs. 1 und 2 AWV einen Genehmigungsvorbehalt, wenn die technische Unterstützung in mündlicher, fernmündlicher, elektronischer oder schriftlicher Form erfolgen soll und wenn der Gebietsansässige vom BAFA darüber unterrichtet worden ist, dass die technische Unterstützung entweder zur Verwendung im Zusammenhang mit chemischen, biologischen oder Kernwaffen oder Flugkörpern für derartige Waffen bestimmt ist und gegenüber Gebietsfremden erbracht wird, die nicht in einem Land ansässig sind, das in Anhang IIa Teil 2 der EG Dual-Use-VO genannt oder Mitglied der Europäischen Union ist, oder im Zusammenhang mit einer militärischen Endverwendung steht und gegenüber Gebietsfremden erbracht wird, die in einem Embargoland im Sinne des Art. 4 Abs. 2 der EG Dual-Use-VO oder in einem Land der Länderliste K ansässig sind. § 45b Abs. 3 AWV normiert wiederum die bereits mehrfach erwähnte Unterrichtungspflicht für den Fall, dass dem Gebietsansässigen diese Voraussetzungen anderweitig bekannt geworden sind.

Schließlich kann die technische Unterstützung durch Gebietsansässige (oder nicht gebietsansässige Deutsche) gemäß § 45c Abs. 1 AWV ebenfalls der Genehmigung bedürfen, wenn der Gebietsansässige vom BAFA darüber unterrichtet worden ist, dass die technische Unterstützung im Zusammenhang mit der Errichtung oder dem Betrieb von Anlagen für kerntechnische Zwecke in Algerien, Irak, Iran, Israel, Jordanien, Libyen, Nordkorea, Pakistan oder Syrien steht, oder ihn kann gemäß § 45c Abs. 2 AWV eine Unterrichtungspflicht treffen, wenn er diese Kenntnis aus anderen Quellen erlangt hat.

Allgemein gilt jedoch, dass keine Genehmigungspflicht besteht, sofern die technische Unterstützung durch die Weitergabe von Informationen erfolgt, die allgemein zugänglich

oder Teil der Grundlagenforschung sind. Weitere Ausnahmetatbestände finden sich in §§ 45ff AWV.

3.6 US – (Re) Export[13]

Im Exportkontrollrecht gilt grundsätzlich das Territorialitäts- und Nationalitätsprinzip; dies bedeutet, dass die Vorschriften von AWG und AWV grundsätzlich nur auf Handlungen in Deutschland – ausnahmsweise auch auf deutsche Staatsbürger im Ausland – Anwendung finden.

Völlig anders ist jedoch das Verständnis von Exportkontrollrecht in den USA. Die US-Vorschriften gelten grundsätzlich nicht nur auch außerhalb des eigenen Hoheitsgebiets, sondern sie entwickeln auch weitreichende Bindungswirkungen für Nicht-US-Bürger/-Gesellschaften (= extraterritoriale Wirkung). Die entsprechenden Rechtsfolgen entstehen durch Anknüpfung an Exportvorgänge bei denen das Gesamtprodukt oder Teile davon einen Bezug zu den USA besitzen[14].

Den Export-Administration-Regulations (EAR) der USA unterliegen damit weltweit folgende Güter:

- Waren mit Ursprung in den USA,
- Produkte mit einem Mindestanteil US-amerikanischer Bestandteile (25 %, bzw. 10 %, wenn die Waren in aus US-Sicht besonders sensible Staaten geliefert werden sollen),
- mit US-Technologie oder Software hergestellte ausländische Ware (Foreign Produced Direct Products).

Wenn also z. B. ein deutsches Unternehmen Waren, die es von einem Hersteller aus den USA bezogen hat, von Deutschland aus in ein anderes Land exportieren will, so liegt aus Sicht der USA ein sogenannter Re-Export vor, für den ggf. eine Genehmigung bei den Exportkontrollbehörden der USA eingeholt werden muss.

Die Voraussetzungen, unter denen nach US-Verständnis ein Re-Export gegeben ist, sind vielschichtig und kompliziert; man darf sich auf keinen Fall von dem Größen- oder Wertverhältnis zwischen dem Gesamtprodukt und dem US-Teil täuschen lassen. Bei Verarbeitung von amerikanischen Bestandteilen jeder Art ist auf jeden Fall eine sorgfältige Prüfung notwendig, um nicht Gefahr zu laufen, von den zum Teil weitreichenden Sanktionen der US-Behörden getroffen zu werden.

In diesem Zusammenhang ist wichtig, dass die Einhaltung des US-Re-Exportrechts von den europäischen Behörden nicht geprüft wird, so dass das Fehlen einer eigentlich notwendigen US-Exportgenehmigung keine direkten Auswirkungen darauf hat, ob das

[13] Dieser von Volker Schlegel und Gwenn Schanze verfasste Abschnitt wurde nahezu unverändert aus der Vorauflage übernommen.

[14] Vgl. *Bundesamt für Wirtschaft und Ausfuhrkontrolle* (Hrsg.), Haddex (FN 8), Teil 12.

jeweils betroffene Ausfuhrgeschäft in Europa genehmigt wird oder nicht. Dieser Sachverhalt hat schon oft dazu geführt, dass die einschlägigen US-Vorschriften nicht ernsthaft genug geprüft worden sind, was wiederum zu erheblichen Konsequenzen führte. Die Nicht-Beachtung des Exportkontrollrechts der USA kann schwerwiegende Beeinträchtigungen des USA-Geschäfts von international tätigen Unternehmen nach sich ziehen; zu den möglichen Rechtsfolgen gehören unter anderem:

- Eintrag auf der Denied-Persons-List (DPL, sog. „Schwarze Liste"), die ein Verbot für US-Unternehmen bedeutet, mit dem gelisteten Unternehmen weiterhin Geschäfte jeglicher Art abzuschließen,
- Einfrieren von Vermögen in den USA,
- strafrechtliche Sanktionen, die vollstreckt werden können, sobald der Betroffene amerikanischen Boden betritt.

4 Genehmigungsverfahren[15]

Ist nach den vorstehenden Ausführungen für ein Exportgeschäft eine Genehmigung erforderlich, so ist diese grundsätzlich beim Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) in Eschborn zu beantragen. Die Dauer eines Genehmigungsverfahrens beträgt dabei je nach Umfang der Lieferung und Sensibilität der Güter und je nach Bestimmungsland zwischen 14 Tagen und mehreren Monaten. Der Antragssteller kann seinen Teil für ein zügiges Verfahren beitragen, indem er eine klare und ausführliche Beschreibung der zu exportierenden Güter erstellt. Dabei kommt es sowohl auf die verständliche Beschreibung der technischen Merkmale als auch auf die Verwendungsmöglichkeiten des Gutes an. Je klarer dem Sachverständigen beim BAFA das Gut und dessen Verwendung beschrieben wird, desto schneller wird er seine Prüfung vollziehen können. Auf die Herstellung eines persönlichen Kontakts zum BAFA sollte ebenfalls viel Wert gelegt werden. Die persönliche Beziehung zu den zuständigen Mitarbeitern des BAFA und die sofortige Nachfrage bei Unklarheiten können einem zügigen und erfolgreichen Genehmigungsverfahren nur förderlich sein.

4.1 Arten von Genehmigungen

Zu unterscheiden ist zwischen individuell beantragten Genehmigungen und sog. Allgemeinen Genehmigungen.

Individuell beantragte Genehmigungen können in drei verschiedenen Formen erteilt werden:

[15] Dieser Abschnitt basiert auf den Ausführungen von Volker Schlegel und Gwenn Schanze in der Vorauflage und wurde weitestgehend unverändert übernommen.

- Grundform ist die **Einzelgenehmigung** für einen konkreten Exportvorgang.
- Eine Sonderform ist die **Höchstbetragsgenehmigung**, die mehrfache oder gestückelte Lieferungen an denselben Empfänger bis zu einer bestimmten Gesamtmenge gestattet. Beispiel: Es wird ein Vertrag über die Lieferung von insgesamt 500t einer bestimmten Chemikalie geschlossen, die der Empfänger über den Zeitraum von drei Jahren in beliebig großen Tranchen abrufen darf.
- Und schließlich besteht die Möglichkeit, eine **Sammelausfuhrgenehmigung** zu beantragen, die auf einen bestimmten Zeitraum befristet für verschiedene Produkte eine unbestimmte Zahl von Ausfuhren an verschiedene Empfänger gestattet. Wegen ihres weiten Gestattungsbereiches werden hohe Anforderungen an die Zuverlässigkeit des Ausführers gestellt. Beispiel: Typischer Anwendungsbereich für Sammelausfuhrgenehmigungen sind internationale Rüstungskooperationen, bei denen einzelne Komponenten in unterschiedlichen Staaten gefertigt werden.

Neben den individuell beantragten Genehmigungen gibt es die sog. **Allgemeinen Genehmigungen** als eine Sonderform der Ausfuhrgenehmigung. Allgemeine Genehmigungen gibt es nur für bestimmte Güter, sie werden von Amts wegen bekanntgegeben und vom BAFA veröffentlicht. Ein wichtiges Beispiel ist die Allgemeine Ausfuhrgenehmigung Nr. EU001, die Ausfuhren bestimmter Güter nach Norwegen, Schweiz, USA, Kanada, Japan, Australien und Neuseeland erlaubt.

Auf diese Allgemeine Genehmigung kann sich grundsätzlich jeder Ausführer berufen und muss keine gesonderte Genehmigung beantragen. Er muss sich allerdings beim BAFA einmalig registrieren lassen. Hierfür stellt das BAFA einen Vordruck zur Verfügung. Nach Eingang der Registrierung erteilt das BAFA eine sog. AG-Nummer. Unter dieser Nummer muss das Unternehmen je nach den Bestimmungen der jeweiligen Allgemeinen Genehmigung in bestimmten Abständen eine Meldung über die ausgeführten Güter abgeben.[16]

Die Nutzung einer Allgemeinen Genehmigung erfolgt in eigener Verantwortung. Da bei der Nutzung einer allgemeinen Genehmigung kein Antrag beim BAFA gestellt wird und das BAFA die Ausfuhr nicht prüft, muss das Unternehmen selbst durch geeignete, betriebsinterne Maßnahmen sicherstellen, dass die Voraussetzungen für die Nutzung erfüllt sind. Sollten die Voraussetzungen nicht erfüllt sein, hat das Unternehmen unter Umständen eine ungenehmigte Ausfuhr durchgeführt, die strafrechtliche Sanktionen nach sich ziehen kann. Deshalb ist es von herausragender Bedeutung, die Voraussetzungen der jeweiligen Allgemeinen Genehmigung genau zu kennen, sich streng an den Wortlaut zu halten (d. h. die Bestimmungen nicht zu Gunsten des Unternehmens weiter zu interpretieren) und die Voraussetzungen zu erfüllen. Ferner ist der gesamte Text der bekanntgemachten Genehmigung genau zu lesen, da sich aus ihm oft weitere Beschränkungen ergeben.

[16] *Bundesamt für Wirtschaft und Ausfuhrkontrolle* (Hrsg.), HADDEX (FN 8), Rn. 465g bis 465i.

4.2 Antrag

Der Antrag auf Erteilung einer Genehmigung ist stets vom Ausführer zu stellen. Für die Bestimmung, wer „Ausführer" eines Gutes ist, kommt es im Exportkontrollrecht nicht unbedingt darauf an, wer zivilrechtlicher Eigentümer des auszuführenden Gutes ist, sondern, wer über das „ob" und „wie" der Versendung der Waren entscheidend bestimmt. In der Regel ist dies derjenige, der sich vertraglich verpflichtet hat, das Gut an den Empfänger zu exportieren.

Die Antragsformulare stellt das BAFA online zur Verfügung. Dort besteht auch die Möglichkeit, den Antrag elektronisch zu stellen (sog. ELAN-Verfahren). Auf die Bedeutung eines persönlichen Kontakts zum BAFA für ein erfolgreiches Genehmigungsverfahren wurde bereits oben hingewiesen. Bereits vor der Antragsstellung kann es ratsam sein, eventuelle Unklarheiten und komplizierte Sachverhalte mit dem zuständigen BAFA-Sachbearbeiter zu besprechen.

Ferner ist neben technischen Unterlagen häufig auch ein Endverbleibsdokument vorzulegen, das eine Erklärung des Empfängers über den Endverbleib oder die Verwendung der Güter enthält. Mustervordrucke zu Endverbleibserklärungen sind online auf der Homepage des BAFA erhältlich. Eine präzise Formulierung der Endverbleibsdokumente ist für den Erfolg einer Genehmigung von entscheidender Bedeutung. Zweck dieses Dokuments ist es, mögliche Zweifel des Sachverständigen über den Verbleib und die Verwendung des Gutes auszuräumen. Der Antragsteller sollte deshalb insbesondere bei sensiblen Lieferungen auf die Glaubhaftigkeit und Vollständigkeit des Endverbleibsdokuments achten. Auch hier gilt, dass im Vorhinein durch persönlichen Kontakt beim BAFA ermittelt werden sollte, wo eventuell Zweifel auf Seiten des Sachverständigen bestehen, die dann im Endverbleibsdokument anzusprechen und auszuräumen sind.

4.3 Ausfuhrverantwortlicher

Bei der Beantragung einer Genehmigung ist gegenüber dem BAFA auch ein Ausfuhrverantwortlicher[17] zu benennen, der für die Einhaltung der Exportkontrollvorschriften persönlich verantwortlich und ein Mitglied des Vorstandes oder der Geschäftsführung ist. Rechtsgrundlage ist § 3 Abs. 2 AWG i. V. m. den „Grundsätzen der Bundesregierung zur Prüfung der Zuverlässigkeit von Exporteuren" vom 10. August 2001. Dem Ausfuhrverantwortlichen obliegen im Wesentlichen vier Hauptpflichten:

[17] Ausführlich zur Bedeutung des Ausfuhrverantwortlichen und seinen Aufgaben vgl. *Bundesamt für Wirtschaft und Ausfuhrkontrolle* (Hrsg.), HADDEX (FN 8), Rn. 71, 345 ff.

- **Personalauswahlpflicht**: Der Ausfuhrverantwortliche muss dafür sorgen, dass im exportsensiblen Bereich hinreichend fachkundiges und zuverlässiges Personal beschäftigt ist.
- **Organisationspflicht**: Der Ausfuhrverantwortliche muss zum einen die Exportkontrolle im Organigramm des Unternehmens richtig anordnen (Aufbauorganisation) und zum anderen durch geeignete Mittel die Arbeitsabläufe so organisieren, dass Verstöße gegen das Außenwirtschaftsrecht ausgeschlossen sind (Ablauforganisation).
- **Überwachungspflicht**: Der Ausfuhrverantwortliche muss durch geeignete Maßnahmen kontrollieren, ob die organisatorischen Anordnungen tatsächlich eingehalten werden (z. B. Stichproben, regelmäßige Systemprüfungen und Routineprüfungen, Dokumentation).
- **Weiterbildungspflicht**: Der Ausfuhrverantwortliche muss für die eigene Weiterbildung und die seiner Mitarbeiter auf dem Gebiet des Außenwirtschaftsrechts sorgen. Hierzu gehört auch, dass die außenwirtschaftsrechtlichen Vorschriften im Betrieb vorhanden sind und ständig aktualisiert werden.

Für die Behörden ist der Ausfuhrverantwortliche aufgrund seiner zentralen Rolle bei der unternehmensinternen Exportkontrolle der wichtigste Ansprechpartner. Der Ausfuhrverantwortliche sollte über Inhalt, Struktur und Systematik der Exportkontrolle sehr gut informiert sein, um den genannten Pflichten nachkommen zu können. Der Ausfuhrverantwortliche ist persönlich verpflichtet, alles zu unternehmen, um die Einhaltung der exportrechtlichen Vorgaben zu gewährleisten. Deren Missachtung hat erhebliche strafrechtliche Sanktionen zur Folge, die den Ausfuhrverantwortlichen auch dann persönlich treffen, wenn er die Exportkontrolle an andere Mitarbeiter delegiert hat. Um sich vor einer strafrechtlichen Inanspruchnahme zu schützen, ist es für den Ausfuhrverantwortlichen besonders wichtig, die Wahrnehmung seiner Pflichten belegen zu können. Deshalb sollte der Ausfuhrverantwortliche sämtliche von ihm vorgenommenen Maßnahmen dokumentieren.

4.4 Auskunft zur Güterliste

Hilfreich für eine Vielzahl von Exportvorhaben des gleichen Gutes in verschiedene Länder ist eine vom BAFA erteilte Auskunft zur Güterliste (AzG, ehemals Negativbescheinigung). Die AzG ist ein güterbezogenes technisches Gutachten darüber, dass die darin bezeichneten Güter nicht von Anhang I der EG Dual-Use-Verordnung und/ oder Teil I der Ausfuhrliste erfasst werden. Eine AzG wird nur erteilt, wenn sie als Beweismittel für den Zoll benötigt wird. Sie ist ein Jahr gültig.

5 Zugelassener Wirtschaftsbeteiligter/Authorized Economic Operator[18]

Seit dem 1. Januar 2008 kann sich ein in der EU ansässiges Unternehmen als sog. Zugelassener Wirtschaftsbeteiligter (ZWB)/Authorized Economic Operator (AEO) beim zuständigen Hauptzollamt am Sitz des Unternehmens registrieren lassen. Den ZWB gibt es in zwei Ausprägungen: „Zollrechtliche Vereinfachungen" und „Sicherheit". Die Entscheidung über die Beantragung ist individuell abzuwägen, da der Aufwand, den ein Unternehmen zur Erfüllung der Bewilligungsvoraussetzungen betreiben muss, beträchtlich ist.

Voraussetzung für die Erteilung des Status „ZWB – Zollrechtliche Vereinfachung" sind:

- keine strafrechtliche Verurteilung im Zusammenhang mit wirtschaftlicher Tätigkeit und kein Insolvenzverfahren anhängig,
- bisher angemessene Einhaltung der Zollvorschriften,
- eine zufriedenstellende Buchführung (Geschäftsbücher und ggf. Beförderungsunterlagen), die angemessene Zollkontrollen ermöglicht,
- nachweisliche Zahlungsfähigkeit.

Für den Status „ZWB – Sicherheit" sind außerdem angemessene Sicherheitsstandards erforderlich. Dies umfasst Gebäudesicherung, Zugangskontrollmaßnahmen, Maßnahmen, die eine eindeutige Feststellung der Handelspartner ermöglicht, Sicherheits- und Hintergrundüberprüfungen der Bediensteten, sowie aktive Teilnahme der Bediensteten an Programmen zur Förderung des Sicherheitsbewusstseins.

Die rechtlichen Vorteile des ZWB-Status richten sich nach der Art der ZWB Zulassung. Eine „ZWB – Zollrechtliche Vereinfachung" erhält im Rahmen der Risikoanalyse eine niedrige Risikobewertung, die weniger Kontrollen und Vereinfachungen bei Bewilligungen zur Folge hat. Die Sicherheitserleichterungen im Rahmen des „ZWB – Sicherheit" umfassen die Möglichkeit, bei summarischen Einfuhr- und Ausfuhranmeldungen lediglich einen reduzierten Datensatz zu übermitteln, sowie eine Vorabinformation über eine bevorstehende Warenkontrolle, sofern dies die Durchführung der Kontrolle nicht gefährdet.

Wirtschaftliche Vorteile sind geringere Kontrolldichte und Grenzwartezeiten, verminderter Bearbeitungsaufwand und dadurch Einsparungen bei Personal- und sonstigen Kosten. Der entscheidende Vorteil des ZWB-Status liegt in dem „Qualitätsnachweis" den das Unternehmen mit dem Status erhält und es zu einem bevorzugten Vertragspartner werden lässt.[19]

---

[18] Dieser Abschnitt basiert auf den Ausführungen von Volker Schlegel und Gwenn Schanze in der Vorauflage und wurde weitestgehend unverändert übernommen.

[19] *Wolffgang/Natzel*, EuZW 2008, 39, 42.

6 Risiken und Compliance

Verstöße gegen exportkontrollrechtliche Vorschriften können erhebliche Konsequenzen nach sich ziehen, insbesondere (aber nicht nur) strafrechtlicher Natur.

6.1 Strafrechtliche Folgen von Verstößen

Die strafrechtlichen Rechtsfolgen ergeben sich aus dem AWG sowie dem KrWaffKontrG in Verbindung mit den allgemeinen Vorschriften des Strafgesetzbuches (StGB) und des Ordnungswidrigkeitengesetzes (OWiG). Die erhebliche Höhe der Strafandrohungen erklärt sich dabei aus der Zielsetzung des AWG, nämlich u. a. die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland zu gewährleisten und eine Störung des friedlichen Zusammenlebens der Völker zu verhüten (vgl. § 7 Abs. 1 AWG), also übergeordnete Rechtsgüter und Interessen zu schützen.

Neben den weitreichenden Straf- und Bußgeldvorschriften, die bei einem Verstoß gegen das KrWaffKontrG drohen (siehe dort §§ 19ff.) gilt nach der derzeitigen Rechtslage insbesondere:

Die vorsätzliche Ausfuhr oder Verbringung von sonstigen Rüstungsgütern im Sinne des Teils I A der AL und bestimmter Dual-Use-Güter im Sinne des Teils I C der AL ohne Genehmigung oder aufgrund einer durch unrichtige oder unvollständige Angaben erschlichenen Genehmigung oder die bloße Förderung einer solchen Ausfuhr bzw. Verbringung durch das Zurverfügungstellen dieser Güter wird gemäß § 34 Abs. 1, 3 und 8 AWG mit **Freiheitsstrafe bis zu fünf Jahren** oder mit Geldstrafe bestraft. Bereits der Versuch ist gemäß § 34 Abs. 5 AWG strafbar. Eine fahrlässige Begehung der Tat wird gemäß § 34 Abs. 7 AWG mit **Freiheitsstrafe bis zu drei Jahren** oder mit Geldstrafe bestraft. Wird durch die Handlung allerdings die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeigeführt oder das friedliche Zusammenleben der Völker gestört oder werden die auswärtigen Beziehungen der Bundesrepublik Deutschland erheblich gestört oder handelt der Täter „gewerbsmäßig", droht gemäß § 34 Abs. 6 Nr. 1 und 2 AWG eine **Freiheitsstrafe nicht unter zwei Jahren**. Die Tat ist dann ein Verbrechen im Sinne von § 12 Abs. 1 StGB. Zu beachten ist dabei, dass ein gewerbsmäßiges Handeln bereits dann vorliegt oder vorliegen kann, wenn der Täter mit der Absicht handelt, sich durch eine wiederholte Begehung solcher Taten eine fortlaufende Einnahmequelle von einiger Dauer und einigem Umfang zu verschaffen; liegt diese Absicht vor, so ist bereits die erste und ggf. einzige Tat als gewerbsmäßig begangen einzustufen.[20] Da im unternehmerischen Verkehr stets eine Gewinnerzielungsabsicht besteht, kommt mithin regelmäßig auch eine Ahndung der Tat als Verbrechen in Betracht!

[20] *Stree/Sternberg-Lieben* in: Schönke/Schröder, StGB, 28. Aufl. 2010, Vorbem. §§ 52 ff Rn. 95 m. w. N.

Entsprechendes gilt gemäß § 34 Abs. 4 AWG für den (vorsätzlichen, fahrlässigen, versuchten oder gewerbsmäßigen) Verstoß gegen ein Embargo, wobei dort im Falle des Vorsatzes eine **Mindestfreiheitsstrafe von sechs Monaten** droht und keine Geldstrafe vorgesehen ist.

Im Falle sonstiger Verstöße gegen die AWV oder die EG Dual-Use-VO, etwa bei der ungenehmigten Ausfuhr/Verbringung sonstiger Dual-Use-Güter oder bei ungenehmigter Vermittlungstätigkeit oder technischer Unterstützung, ist zu differenzieren:

Grundsätzlich werden derartige sonstige Verstöße, mögen sie vorsätzlich oder fahrlässig begangen worden sein, gemäß § 33 Abs. 1 und 4 AWG als Ordnungswidrigkeit verfolgt und gemäß § 33 Abs. 6 AWG mit einer **Geldbuße bis zu 500.000,00 €** geahndet. Der Versuch einer solchen Ordnungswidrigkeit kann gemäß § 33 Abs. 7 AWG ebenfalls geahndet werden. Zudem kann die Geldbuße nicht nur gegen den Handelnden selbst, sondern auch gegen das Unternehmen verhängt werden.

Wird die grundsätzlich nur als Ordnungswidrigkeit verfolgte Handlung hingegen vorsätzlich begangen und ist sie geeignet, die äußere Sicherheit der Bundesrepublik Deutschland, das friedliche Zusammenleben der Völker oder die auswärtigen Beziehungen der Bundesrepublik Deutschland erheblich zu gefährden, wird die Tat gemäß § 34 Abs. 2 AWG ebenfalls als Straftat verfolgt und wiederum mit **Freiheitsstrafe bis zu fünf Jahren** oder mit Geldstrafe bzw. in den o. g. schweren Fällen wiederum mit **Freiheitsstrafe nicht unter zwei Jahren** bestraft.

Da es sich bei den vorgenannten Straftatbeständen um sog. Allgemeindelikte handelt, kann grundsätzlich jeder Täter sein, der in dem Exportvorgang entscheidend mitwirkt, insbesondere also der Ausführer und der Ausfuhrverantwortliche, aber auch jeder sonstige Mitarbeiter mit Entscheidungskompetenz. Im Übrigen droht stets auch eine Strafbarkeit wegen einer Tätigkeit als bloßer Gehilfe.[21]

Im Übrigen gelten die Straftatbestände gemäß § 35 AWG unabhängig vom Recht des Tatorts und somit auch im Ausland, sofern der Täter Deutscher ist.

Besonders gravierende Folgen kann im Übrigen die gemäß § 36 Abs. 1 und 2 AWG in Verbindung mit §§ 74ff StGB bzw. §§ 22ff OWiG mögliche Anordnung der (erweiterten) **Einziehung** der Gegenstände, auf die sich die Tat bezieht oder die zu ihrer Begehung oder Vorbereitung gebraucht worden oder bestimmt gewesen sind, haben. Darüber hinaus ist im Falle der vorsätzlichen Verwirklichung eines Straftatbestands gemäß § 36 Abs. 3 AWG in Verbindung mit §§ 73ff StGB von Amts wegen der (erweiterte) **Verfall** dessen anzuordnen, was der Täter bzw. das Unternehmen, für das er gehandelt hat, für die Tat oder aus ihr erlangt hat. Betroffen hiervon ist aufgrund des geltenden Bruttoprinzips grundsätzlich der gesamte Kaufpreis, der aus dem Rechtsgeschäft erzielt wurde, und nicht etwa nur der reine Gewinn nach Abzug der Kosten.[22]

---

[21] *Weith, Wegner, Ehrlich*: Grundzüge der Exportkontrolle, 2006, S. 237 Rn. 6.

[22] BGH v. 21.08.2002 – 1 StR 115/02, BGHSt 47, 369, 370.

6.2 Zivilrechtliche Risiken

Was in der einschlägigen Literatur wie auch in der Vertragspraxis gerne übersehen wird, sind die nicht unerheblichen zivil- und vertragsrechtlichen Risiken: Wer sich zur Lieferung eines Gutes verpflichtet, dieses mangels einer erforderlichen Ausfuhrgenehmigung dann aber nicht ausliefern kann, macht sich seinem Vertragspartner gegenüber unter Umständen schadensersatzpflichtig.

Entsprechendes gilt in der umgekehrten Richtung im Verhältnis zu einem etwaigen Zulieferer: Der Exporteur muss einen Vertrag mit seinem Zulieferer grundsätzlich erfüllen, das heißt die zuzuliefernde Ware abnehmen und bezahlen, auch wenn er die Ware dann ggf. nicht wie geplant weiterveräußern kann.

Auf höhere Gewalt wird sich der Exporteur dabei nur in Ausnahmefällen berufen können, etwa wenn überraschend ein Embargo in Kraft tritt, mit dem bei Eingehung der Rechtsgeschäfte nicht zu rechnen war.

Im Übrigen droht Vorstandsmitgliedern und Geschäftsführern gemäß § 93 AktG bzw. § 43 GmbHG auch eine persönliche zivilrechtliche Haftung gegenüber der Gesellschaft.

6.3 Sonstige Konsequenzen

Da die Erteilung von (Ausfuhr-) Genehmigungen von der Zuverlässigkeit des Ausfuhrverantwortlichen abhängt, kann das BAFA bei begründeten Anhaltspunkten für einen erheblichen Rechtsverstoß von der Bescheidung eines Antrags auf Erteilung der Genehmigung absehen bzw. diese davon abhängig machen, dass die Zweifel an der Zuverlässigkeit durch personelle und organisatorische Maßnahmen ausgeräumt werden.[23]

Völlig unabhängig von den rechtlichen Konsequenzen sind schließlich die enormen Imageschädigungen zu bedenken, die eine negative Presseberichterstattung im Falle einer Ermittlung wegen eines Verstoßes gegen das Außenwirtschaftsrecht zwangsläufig mit sich bringt.

6.4 Risikomanagement

Zur Vermeidung der geschilderten Risiken und Sanktionen ist eine funktionierende innerbetriebliche Exportkontrolle unabdingbar. Diese beginnt mit einer **Identifizierung** der möglicherweise problematischen Sachverhalte, gefolgt von einer **Sensibilisierung** der Mitarbeiter für die Thematik „Exportkontrolle". Nur wer zumindest ahnt, dass eine Handlung überhaupt problematisch sein könnte, kann die Probleme zu beseitigen helfen. Zu diesem Zwecke muss jeder an einem Export beteiligte Mitarbeiter wissen, wie er Probleme von

[23] Bekanntmachung der Grundsätze der Bundesregierung zur Prüfung der Zuverlässigkeit von Exporteuren von Kriegswaffen und rüstungsrelevanten Gütern vom 25. Juli 2001, Nr. 3 und 5.

vornherein vermeiden kann bzw. wie er sich beim Erkennen eines möglicherweise relevanten oder problematischen Sachverhaltes zu verhalten hat und wen er im Zweifelsfalle über derartige Erkenntnisse informieren und hinzuziehen muss. Dies bedingt die **Implementierung** einer unternehmensinternen Verfahrensanweisung sowie als Mindestmaß die Einrichtung einer EDV-gestützten Abgleichung der existierenden Namenslisten.

Die Verantwortung für die innerbetriebliche Exportkontrolle trifft letztlich den Ausfuhrverantwortlichen, ihm obliegen insbesondere die **Organisations-, Personalauswahl-, Weiterbildungs- und Überwachungspflichten**. Er hat dafür zu sorgen, dass Verstöße gegen das Außenwirtschaftsrecht zumindest weitestgehend ausgeschlossen sind. Nur wer diesen Pflichten gewissenhaft und nachhaltig nachkommt, wird gegenüber den Ermittlungsbehörden für den Fall der Fälle argumentieren können, alles Erforderliche getan zu haben. Dass dazu auch der regelmäßige und offene Kontakt zu den zuständigen Behörden gehört, wurde oben bereits angesprochen.

Klarzustellen ist an dieser Stelle allerdings, dass bei aller gebotenen Vorsicht niemandem die Pflicht obliegt, unbekannte Sachverhalte mit geradezu detektivischem Spürsinn aufzuklären. Es gibt grundsätzlich keine Nachforschungspflichten, niemand muss sich „bösgläubig" machen, sondern darf sich auf die Richtigkeit und Vollständigkeit der ihm erteilten Informationen verlassen. Gleichwohl darf man nicht leichtfertig die Augen verschließen und sozusagen auf der Hand liegende Erkenntnismöglichkeiten ignorieren.

Ebenso ist innerhalb des Unternehmens natürlich der Informationsfluss sicherzustellen. Erlangt ein Mitarbeiter Kenntnis von einem relevanten Sachverhalt, muss er diese Kenntnis mit anderen möglicherweise betroffenen Kollegen teilen, um eine Wissenszurechnung zu vermeiden. Das Sammeln von Informationen an einer zentralen Stelle sowie deren Auswertung ist das „A und O" einer funktionierenden innerbetrieblichen Exportkontrolle.

Compliance – Auslandsrisiken erkennen und steuern (Schwerpunkt Asien)

Thomas Weidlich und Katja Neumüller

Inhaltsverzeichnis

T. Weidlich (✉) · K. Neumüller
Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: thomas.weidlich@luther-lawfirm.com

K. Neumüller
E-Mail: katja.neumueller@luther-lawfirm.com

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2_6, © Springer Fachmedien Wiesbaden 2013

Zusammenfassung

Compliance ist ein Thema, mit dem sich Unternehmen nicht nur in ihren Heimatländern befassen müssen, sondern in jedem Land, in dem sie geschäftlich aktiv sind. In vielen Ländern sind Compliance-Anforderungen bereits beim Eintritt in den ausländischen Markt zu beachten, die sich auf komplexe Themen wie insbesondere die vertragliche Gestaltung von Rechtsverhältnissen, die Beschäftigung von Mitarbeitern im Ausland und die Durchsetzung von Ansprüchen vor Ort erstrecken. Die Nichtbeachtung lokaler Anforderungen kann zu gravierenden Nachteilen führen und den Erfolg einer Investition im Ausland gefährden.

1 Compliance im Zeitalter der Globalisierung

Deutschland ist Exportweltmeister und sowohl große deutsche Konzerne als auch mittelständische Unternehmen operieren heute in der ganzen Welt. Mit Ausdehnung der Geschäftsaktivitäten ins Ausland stellt sich immer wieder die Frage nach den dort zu beachtenden Compliance-Anforderungen.[1] Während die Risiken bei einer Nichtbeachtung von Compliance-Anforderungen im innereuropäischen Ausland häufig mit deutschem Recht vergleichbar sein mögen, kann der rechtliche Rahmen in Ländern außerhalb Europas erheblich von der deutschen Situation abweichen und Verstöße dagegen schwerwiegende Folgen haben. Auch Großkonzerne machen immer wieder unliebsame Erfahrungen bei ihren Auslandsinvestitionen (dazu noch näher unten im Text).

Vor dem Hintergrund der vielfältigen Compliance-Risiken bei Geschäftstätigkeiten im Ausland ist die frühzeitige und intensive Auseinandersetzung mit den in den einzelnen Ländern geltenden Bestimmungen und Anforderungen notwendig, um Haftungsrisiken für das Unternehmen zu vermeiden und den Erfolg einer Investition im Ausland nicht zu gefährden. Mit zunehmender Internationalität nimmt die Komplexität innerhalb einer Unternehmensgruppe zu. Knappe Managementkapazitäten, fehlende Transparenz und divergierende nationale Regelungen sind typische Merkmale, die sich im Zuge der Globalisierung verstärken – bei gleichzeitiger Zunahme der Risiken.

2 Regulatorische Minenfelder beim Markteintritt im Ausland

Im Zuge der weltweiten Finanzkrise werden protektionistische Maßnahmen – allen Beteuerungen der Regierungen zum Freihandel und zu offenen Märkten zum Trotz – weltweit wieder zunehmen. Viele asiatische Märkte, einschließlich der beiden Boomländer China

[1] Zur Errichtung einer Compliance-Organisation *Hauschka*, ZIP 2004, 877 ff.; zu den Compliance-Regelwerken in den USA, Großbritannien und Australien *Bergmoser/Theusinger/Gushurst*, BB Special 5 (zu BB 2008, Heft 25), S. 1 ff.; zu Haftungsrisiken von Multinationals in Schwellenländern und Compliance-Defiziten insbesondere beim Umweltschutz und den Arbeitsbedingungen lokaler Mitarbeiter *Margolis*, International Bar News, April 2009, S. 14 ff.

und Indien, sind ausländischen Investoren nicht frei zugänglich. So unterliegen Ausländer in bestimmten Industriebereichen oftmals Beteiligungsobergrenzen oder sind von sensiblen Wirtschaftsbereichen sogar gänzlich ausgeschlossen. Der Umgang mit solchen Beschränkungen ist nicht immer einfach.

Für eine Geschäftstätigkeit in **China** sind eine Vielzahl von Genehmigungen und Registrierungen erforderlich, die vor Beginn und auch für den täglichen Geschäftsablauf zu beantragen sind. Bereits die Gründung von Unternehmen durch ausländische Investoren ist in China – anders als in Deutschland – nur nach entsprechender Genehmigung durch die zuständige Handelsbehörde und Registrierung durch die Gewerbebehörden möglich. Nach Erteilung der Genehmigung und Registrierung muss dann eine Geschäftslizenz (sog. *Business License*) beantragt werden, ohne die eine Gesellschaft in China nicht agieren darf. Ob und in welcher Form die Genehmigung erteilt wird, hängt von dem konkret geplanten Vorhaben ab. Generell unterliegen ausländische Investitionen in China einer umfassenden Reglementierung.[2] In der Praxis sind westliche Unternehmen oft gezwungen, bei ihren Investitionen in China zumindest kleine Kompromisse einzugehen, um Geschäfte in China tätigen zu können und wettbewerbsfähig zu sein.[3] Die maßgeblichen Vorschriften für ausländische Investitionen, die *Provisions on Directing Foreign Investment,* werden durch einen Lenkungskatalog, den *Catalogue for Directing Foreign Investment,* ergänzt. Der Lenkungskatalog enthält eine Liste aller Industriesektoren und teilt diese in die Kategorien *prohibited* (verboten), *restricted* (beschränkt zulässig) und *encouraged* (gefördert) ein. Investitionsvorhaben, die in keine dieser Kategorien fallen, sind grundsätzlich zulässig und gehören damit der Kategorie *permitted* (erlaubt) an. Die Nationale Entwicklungs- und Reformkommission hat gemeinsam mit dem Handelsministerium im Dezember 2011 einen aktualisierten Investitionskatalog vorgelegt. Dieser ist am 30. Januar 2012 in Kraft getreten und ersetzt den zuletzt im November 2007 aktualisierten Lenkungskatalog. Ein Schwerpunkt des neuen Lenkungskatalogs liegt auf der Förderung von Investitionen in hochtechnologisierten Industriezweigen, umweltfreundlichen Technologien sowie der weiteren Entwicklung moderner Dienstleistungen.

Zu den derzeit für ausländische Investoren generell verbotenen Betätigungsfeldern gehören der Bau und der Betrieb von Stromnetzen, die Luftverkehrsüberwachung, der Betrieb von Postunternehmen und von Fernseh- und Radiostationen, die traditionelle Teeherstellung und das Druck und Verlagswesen. Beschränkt zulässig sind hingegen die Konstruktion und der Betrieb von Raffinerien, die Betätigung in bestimmten Sektoren der chemischen und pharmazeutischen Industrie sowie in Bereichen des Finanzdienstleistungssektors. Die Anzahl der verbotenen und beschränkt zulässigen Investitionen hat sich insgesamt im aktualisierten Katalog verringert. In die Kategorie der geförderten Investitionsvorhaben fallen umweltfreundliche Projekte wie Baustoffrecycling oder Wasserrückgewinnung,

---

[2] Hierzu ausführlich: *Dickinson/Vietz*, GmbHR 2006, 245, 248 f.; *Michael J. Moser* (Hrsg.), Doing Business in China, Vol. 1 2008.

[3] *FAZ* vom 11.12.2012, In China Geschäfte wagen; http://www.faz.net/frankfurter-allgemeine-zeitung/in-china-geschaefte-wagen-11990598.html.

die Automobilzulieferung für Elektroautos oder alternative Antriebstechniken sowie die Produktion von Gasmotoren.

Von der Einteilung in diese Kategorien hängt ab, ob und inwieweit das Projekt staatlichen Regulierungen unterliegt oder durch Vergünstigungen gefördert wird. Regulierungen können hinsichtlich der zulässigen Beteiligungsform (beispielsweise in Form eines Joint Ventures mit einem chinesischen Partner) oder auch der maximalen Beteiligungshöhe eines ausländischen Investors bestehen, während geförderte Projekte unter Umständen steuerlich bevorzugt behandelt werden oder andere Vorteile erfahren. Neben diesen Regulierungen können sich Zulassungsbeschränkungen für Investitionen aber auch aus Vorschriften außerhalb des Lenkungskatalogs ergeben. Zu nennen ist hier insbesondere die *Automobile Industry Development Policy*, die eine Joint Venture-Pflicht für ausländische Automobilhersteller in der Automobilindustrie in China vorschreibt.

Indiens Wirtschaftspolitik zielt im Grundsatz auf eine Förderung ausländischer Direktinvestitionen und begrüßt diese heute in nahezu allen Wirtschaftszweigen.[4] Ausgenommen sind allerdings einige Bereiche, die politisch oder wirtschaftlich von wesentlicher strategischer Bedeutung sind und unter die sog. *Prohibited List* fallen. In diesen Bereichen sind ausländische Investitionen generell nicht zulässig. Hierzu gehören etwa der Atomsektor, die Verteidigungsindustrie, der Schienenverkehr, die Lotterie und das Glücksspiel, Geschäfte mit Immobilien sowie der Tabakanbau.[5] In den meisten Wirtschaftszweigen und für fast alle Produktionsvorhaben sind aber ausländische Direktinvestitionen ohne eine Genehmigung durch die indischen Behörden zulässig (sog. *Automatic Route*). Einige wenige Ausnahmen zu der *Automatic Route* sind gesetzlich festgelegt und unterliegen der sog. *Approval Route*. Diese Ausnahmen erfordern eine Genehmigung durch das *Foreign Investment Promotion Board* (FIPB). In bestimmten Wirtschaftszweigen bedürfen ausländische Beteiligungen an indischen Unternehmen zudem einer besonderen Genehmigung bei Überschreitung bestimmter Beteiligungsquoten (sog. *Sectoral Caps*). So können Beteiligungen im Finanz-, Versicherungs- und Telekommunikationssektor alleine aus diesem Grund genehmigungspflichtig sein.

Trotz Genehmigungsvorbehalten in einigen Bereichen öffnet sich der indische Markt für ausländische Investoren aber immer weiter. Erst in jüngster Vergangenheit hat die indische Regierung mit der Veröffentlichung der Press Note 5/2012 lang erwartete Erleichterungen für ausländische Direktinvestitionen verkündet. Die größten Veränderungen ergeben sich dabei für den Einzelhandel. Im *single-brand*-Bereich (einzelne Markenprodukte) gibt es künftig keine Beteiligungsgrenze für ausländische Investitionen mehr und an indischen Supermärkten (*multi-brand-retail*) ist nunmehr für ausländische Investoren eine 51 %ige Beteiligung möglich. Allerdings werden ausländische Investitionen im Bereich des Einzelhandels trotz der Öffnung noch an individuelle Auflagen geknüpft. So sind Investitionen nur in bestimmten Gebieten und nur mit einem Mindestinvestitionsvolumen von 100 Mio. US Dollar möglich.

---

[4] *Ströhlein,* M & A und Greenfield-Investitionen in Indien, ASIA BRIDGE 1/2008, S. 45.

[5] *Adam*, Energiepoker: Das beste Blatt gewinnt, ASIA BRIDGE 9/2007, S. 8.

Ob in Indien eine besondere Genehmigung eingeholt werden muss, richtet sich somit entscheidend nach dem Wirtschaftszweig, in welchem das auslandsinvestierte Unternehmen tätig werden soll, sowie nach der angestrebten Beteiligungshöhe.[6] Die Genehmigungsprozesse können wesentlich erleichtert werden, wenn man mit dem jeweiligen Bundesstaat ein sog. *Single-Window* (Kontakt mit ausschließlich einer Behörde) für alle Genehmigungsfragen vereinbart. Allerdings ist dadurch nicht gewährleistet, dass man nicht mit weiteren Behörden, insbesondere auf Bundesebene, in Kontakt treten muss.[7]

Auch in **Indonesien** existieren umfangreiche Beschränkungen für Ausländer. Das *Investment Law* ermächtigt die Regierung, eine sog. *Negative List* aufzustellen. Die *Negative List* beinhaltet eine Aufzählung von Geschäftstätigkeiten, bei denen ausländische Investitionen nur beschränkt zulässig oder aber verboten sind. Damit soll ein gewisser Schutz von indonesischen Marktteilnehmern gewährleistet werden. Neben dem Verbot einer ausländischen Investition sieht die *Negative List* auch vor, dass gewisse Wirtschaftsbereiche nur für kleine und mittelständische Unternehmen zugänglich sind und wieder andere Geschäftszweige nur zusammen mit einem indonesischen Anteilsinhaber ausgeübt werden können. Die *Negative List* wird regelmäßig aktualisiert und veröffentlicht. Zuletzt erließ die indonesische Regierung im Oktober 2010 eine überarbeitete *Negative List*, die die bisher geltende *Negative List* aus dem Jahr 2007 ersetzt. Die größten Veränderungen liegen vor allem im Bereich der Beteiligungsgrenzen für ausländische Investoren. So wurden die Grenzen im Stromversorgungsmarkt, im Gesundheits- und im Bauwesen sowie im Direktvertrieb weiter gelockert. Ferner wird nun auch der Wechsel von Anteilseignern durch Übernahmen und Verschmelzungen in der *Negative List* ausdrücklich geregelt.[8] Eine Rückwirkung entfaltet die neue *Negative List* jedoch nicht, so dass bereits vor deren Inkrafttreten genehmigte Investitionen und Gesellschafterverhältnisse nicht angepasst werden müssen. Sofern die *Negative List* für bestimmte Geschäftszweige keine höhere indonesische Beteiligung vorschreibt, gilt im Übrigen die Regelung, wonach bei Gesellschaften mit 100 %iger ausländischer Beteiligung innerhalb eines Zeitraumes von 15 Jahren mindestens 5 % der Anteile an indonesische Gesellschafter übertragen werden müssen.

In **Thailand** unterliegen Unternehmen mit ausländischer Mehrheitsbeteiligung den Beschränkungen des *Foreign Business Act 1999* (FBA). Dieser beschränkt die Geschäftstätigkeiten ausländischer Investoren oder normiert Zustimmungserfordernisse der thailändischen Behörden. Eine ausländische Mehrheitsbeteiligung an einem thailändischen Unternehmen ist nur dann nicht gegeben, wenn Thais tatsächlich die effektive Kapital- und Stimmenmehrheit ausüben können. In allen anderen Fällen gilt das thailändische Unternehmen nach dem *Foreign Business Act 1999* als sog. „Alien", womit die Beschränkungen zu beachten sind.

Der *Foreign Business Act 1999* untergliedert die Beschränkungen in drei Listen. Die sog. *List One* des FBA sieht die verbotenen Geschäftsfelder vor. Hierzu zählen Bereiche des Kommunikationswesens, der Landwirtschaft und der Viehzucht sowie das Fischereiwesen. Bei Geschäftsaktivitäten, die in der sog. *List Two* des FBA genannt sind, ist eine

---

[6] OAV Wirtschaftshandbuch Asien-Pazifik 2011/2012, S. 181.

[7] *Ströhlein* aaO (FN 4).

[8] *Pfaar/Rehling;* IStR 2011, S. 828.

Genehmigung des thailändischen Handelsministeriums erforderlich. Dies insbesondere auf den Gebieten der nationalen Sicherheit, der Kunst und Kultur sowie bei bestimmten natürlichen Ressourcen. Die sog. *List Three* des FBA enthält Geschäftsgebiete, in denen Ausländer eine sog. *Foreign Business License* benötigen. Diese wird durch den Generaldirektor *des Department of Business Development* (DBD) erteilt. Die *List Three* ist recht umfangreich und schließt unter anderem den Einzelhandel, den Großhandel und den Dienstleistungssektor ein. In den nicht genannten Bereichen des *Foreign Business Act 1999* können ausländische Investoren grundsätzlich ohne Beschränkungen tätig werden. Genehmigungserfordernisse bei Geschäftsaktivitäten der *List Two* und *List Three* können sich allerdings auch aus anderen Gesetzen ergeben. Zu nennen sind hier insbesondere der *Industrial Estate Authority of Thailand Act* oder der *Investment Promotion Act*.[9]

Auch **Malaysia** kennt vergleichbare Beteiligungsgrenzen für Ausländer und hat in vielen Wirtschaftsbereichen zudem Quoten zugunsten der sog. *Bumiputras* eingeführt. Das Wort bedeutet „Söhne der Erde" und umfasst die einheimischen und ethnischen Malaien, die mit dieser Politik gefördert werden sollen. Ausländische Investoren können daher in vielen Fällen nicht oder nur mit Einschränkungen im operativen Geschäft eine 100 %ige Beteiligung an einem Unternehmen in Malaysia erwerben, auch wenn Ausnahmen inzwischen einfacher genehmigt werden.[10] Die malaysische Regierung hat in den letzten Jahren vermehrt die Beschränkungen für ausländische Investoren abgebaut. So wurde das Erfordernis einer 30 %igen *Bumiputra*-Beteiligung an börsennotierten Unternehmen ebenso aufgehoben wie Beschränkungen im Bereich des Banken-, Finanz – und Versicherungssektors. Zudem wurde die Richtlinie des für ausländisches Investment zuständigen *Foreign Investment Committee* (FIC) über den Erwerb von Anteilen, Verschmelzungen und Übernahmen ersatzlos gestrichen.[11]

In den **Philippinen** können ausländische Investoren in bestimmten Bereichen einen 100 %igen Anteilsbesitz an philippinischen Unternehmen halten. Eine 100 %ige Beteiligung ist nur dann ausgeschlossen, wenn die Investition in einem Geschäftsbereich getätigt werden soll, der unter die sog. *Negative List* des *Foreign Investment Act* fällt. In den Bereichen Medien und Einzelhandel ist eine ausländische Investition beispielsweise gänzlich untersagt. In anderen Bereichen wie der Werbebranche oder der Bewirtschaftung mit natürlichen Ressourcen existieren Beteiligungsbeschränkungen für Ausländer, die bei einem Investment zu beachten sind. Fraport hatte diese Beteiligungsbeschränkungen 2006 als Minderheitsgesellschafterin der philippinischen Gesellschaft PIATCO auf schmerzhafte Weise erfahren.[12]. PIATCO war Inhaberin einer Konzession zum Bau und Betrieb eines

[9] *Schlüter*; RiW 2011, S. 207.

[10] Investieren in Malaysia, aktuell ASIABRIDGE, 05/2006, S. 28.

[11] OAV Wirtschaftshandbuch Asien-Pazifik 2011/2012, S. 340.

[12] Handelsblatt vom 28. Juli 2006, Fraport- Mitarbeiter nach Investition in Philippinen angeklagt, http://www.handelsblatt.com/News/Unternehmen/Handel-Dienstleistungen/_pv/grid_id/1227365/_p/200040/_t/ft/_b/1114023/default.aspx/fraport-mitarbeiter-nach-investition-in-philippinen-angeklagt.html

neuen Flughafenterminals auf dem Flughafen in Manila. Kurz vor Fertigstellung hatte die philippinische Regierung die Konzession sowie sämtliche mit PIATCO geschlossenen Verträge aus verschiedenen Gründen für nichtig erklärt. Fraport hatte daraufhin im September 2003 ein Investitionsschutzverfahren eingeleitet, nachdem Verhandlungen über eine Entschädigung für Fraports Investitionen in Höhe von ca. 300 Mio. US Dollar ergebnislos verlaufen waren. Die Klage von Fraport wurde aber mit der Begründung abgewiesen, dass der deutsch-philippinische Investitionsschutzvertrag nur solche Vermögenswerte schütze, die mit dem lokalen Recht in Einklang stehen. Die philippinische Regierung hatte argumentiert, dass Fraports Beteiligung an PIATCO gegen philippinisches Recht verstoße, weil Fraport direkt und indirekt 61 % der Anteile an PIATCO halte. Dieser Einfluss sei teilweise durch gegenüber der philippinischen Regierung lange geheim gehaltene Kontrollabkommen zustande gekommen. Zulässig seien aber nur maximal 40 %. Fraport habe dies zwar gewusst, den erhöhten Einfluss aber für notwendig gehalten, um die Kontrolle über seine erheblichen Investitionen zu gewinnen. Fraports Investitionen seien daher nicht im Einklang mit philippinischem Recht erfolgt. Daraufhin wurde der Terminal ohne Entschädigung von der philippinischen Regierung enteignet. Als Reaktion darauf erhob Fraport vor dem *International Centre of Settlement of Investment Disputes* (ICSIS) in Washington Klage auf Entschädigung gegen die philippinische Regierung. Diese wurde jedoch als unzulässig abgewiesen, da sich das Washingtoner Gericht als nicht zuständig ansah.[13] Zur Verringerung des Verlustes wurde Fraport 2007 von der Bundesregierung mit ca. 42 Mio. Euro entschädigt. Dabei handelte es sich um Bundesgarantien für Kapitalanlagen im Ausland, die das Unternehmen für die Eigenkapitalbeteiligung am Flughafen von Manila zum Schutz vor politischen Risiken in Anspruch genommen hat.[14] Neben diesen Beteiligungsbeschränkungen gibt es aber auch einige Branchen, die in den jährlichen *Investment Priority Plan* aufgenommen werden, erhalten eine umfassende Unterstützung durch das *Board of Investments* (BOI) erhalten. Dies sind unter anderem die landwirtschaftliche Produktion, die Infrastruktur sowie umweltschonende und energieeffiziente Projekte.[15]

Im November 2012 wurde in **Myanmar** ein neues Gesetz für ausländische Investitionen verabschiedet und in Kraft gesetzt. Dieses löst das alte Investitionsgesetz aus dem Jahr 1998 ab und soll dem Reformgeist des aufstrebenden Staates und dessen Öffnung für ausländische Investoren entsprechen. Wichtigste Änderungen gegenüber dem alten Gesetz sind die Aufhebung der Begrenzung einer ausländischen Beteiligung von bisher 49 % bei einem Joint Venture mit einem lokalen Partner in bestimmten Bereichen wie dem Abbau reichhaltiger Bodenschätze oder der Fischerei. Zudem wurde das Erfordernis einer Mindestinvestitionssumme von 5 Mio. US Dollar grundsätzlich aufgehoben. Die *Myanmar*

[13] Handelsblatt vom 17. August 2007, Fraport blitzt bei der Weltbank mit Schadensersatzklage ab, http://www.handelsblatt.com/unternehmen/handel-dienstleister/fraport-blitzt-bei-weltbank-mit-schadenersatzklage-ab;

[14] Pressemitteilung vom 16. April 2008, http://www.presseportal.ch/de/pm/100006878/100559280/fraport_ag_frankfurt_airport_services_worldwide?search=16.04.2008.

[15] OAV Wirtschaftshandbuch Asien-Pazifik 2011/2012, S. 431.

Investment Commission kann eine solche jedoch in einzelnen Wirtschaftsbereichen weiterhin festsetzen. Ferner können ausländische Unternehmen nun von Steuererleichterungen bzw. steuerlichen Vereinfachungen bei Investitionen profitieren. Die weitere Ausgestaltung liegt bei der *Myanmar Investment Commission*, welcher in dem neuen Gesetz ein weiter Ermessens- und Entscheidungsspielraum eingeräumt wurde. Zudem wird erwartet, dass die Regierung noch weitere Richtlinien und Ausführungsbestimmungen zum neuen Investitionsgesetz erlässt, welche das Investitionsgesetz hinreichend präzisieren sollen.[16]

Ähnliche Investitionsbeschränkungen bestehen in den meisten asiatischen Ländern, auch wenn in den letzten Jahren insgesamt ein Trend zur Liberalisierung erkennbar ist. Schon beim Markteintritt sollten ausländische Investoren überlegen, wie sie damit umgehen. Umgehungsversuche über fragwürdige Treuhandlösungen sind dabei meistens keine gute Antwort; stattdessen sollte der regulatorische Rahmen richtig genutzt oder direkte Absprachen mit den zuständigen lokalen Behörden getroffen werden. Damit lassen sich Beteiligungs- und andere Beschränkungen in rechtssicherer Weise oftmals ganz oder auf ein akzeptables Maß reduzieren.

3 Korruption

Korruption im Ausland gilt trotz der Skandale der jüngeren Vergangenheit (Siemens, MAN, Ferrostal) noch immer vielfach als Kavaliersdelikt oder notwendiges Übel.[17] Deutsche Firmen sollen Schätzungen zufolge allein im Jahr 2006 ca. 25 Mrd. Euro an Korruptionsmitteln im Ausland eingesetzt haben[18]. International tätige deutsche Unternehmen dürfen das sich verschärfende rechtliche Umfeld für Korruptionsdelikte im In- und Ausland jedoch nicht ignorieren. Auch wenn das Unrechtsbewusstsein lokal oft nur schwach ausgeprägt ist, hat sich die Rechtslage für Unternehmen in Deutschland in den letzten Jahren fundamental geändert.[19] Große Veränderungen im Bereich der (internationalen) Korruptionsbekämpfung haben sich insbesondere durch das Inkrafttreten des *UK Bribery Act* im Juli 2011 ergeben. Dessen Anwendungsbereich geht so weit, dass deutsche Unternehmen, die eine geschäftliche Beziehung nach England unterhalten, von englischen Strafbehörden wegen der Zahlung von Bestechungsgeldern in irgendeinem Land nach dem *UK Bribery Act* belangt werden können.[20] Der *UK Bribery Act* ermöglicht eine Strafverfolgung gegen deutsche Unternehmen, obwohl die Bestechung nicht in England stattgefunden hat und zudem kein englischer Staatsbürger involviert war.[21] Auch

[16] *von Dresky*, Unternehmer Edition 11/2012, S. 52.

[17] *Hetzer,* EuZW 2007, S. 75 ff.

[18] *Schemmel, Hacker,* ZRP 2009, S. 4 ff.

[19] *Fietz/Weidlich,* RIW 2005, 423 ff.; *Sedemund*, DB 2003, 323 ff.

[20] *Pörnbacher/Mark*, NZG 2010, 1372, 1373.

[21] *Pörnbacher/Mark*, NZG 2010, 1372, 1375.

im Strafmaß geht die neue britische Regelung über den US-amerikanischen *Foreign Corrupt Practices Act* (FCPA) weit hinaus; Können Unternehmen nach dem *Foreign Corrupt Practices Act* mit einer Geldbuße von bis zur Höhe des doppelten jährlichen Kapitalertrages belegt werden, ermöglicht der *UK Bribery Act* Geldbußen in unbegrenzter Höhe. Die genauen Auswirkungen für die internationale Praxis werden jedoch erst in Zukunft ersichtlich sein. Nichtsdestotrotz müssen Unternehmen beachten, dass die Bestechung ausländischer Amtsträger ebenso wie die Bestechung von Mitarbeitern privater Unternehmen in ausländischen Märkten inzwischen in vielen Ländern strafbar ist und im Ausland gezahlte Bestechungsgelder in Deutschland steuerlich nicht mehr abzugsfähig sind. In Asien kommen Singapur und Hong Kong besondere Bedeutung zu, weil Bestechungshandlungen – anders als in den meisten Nachbarländern – dort konsequent verfolgt werden und viele Unternehmen von diesen Standorten aus Entscheidungen für die ganze Region treffen.[22] Vertragsgestaltungen und geschäftliche Praktiken sind auf ihre globalen Auswirkungen zu überdenken und erforderlichenfalls neu zu regeln.

3.1 Schmiergelder in Asien

Asien ist die größte Wachstumsregion weltweit. Die deutschen Exporte nach Asien-Pazifik sind in den letzten Jahren stark angestiegen und liegen deutlich über dem Durchschnitt der gesamten deutschen Ausfuhren. Der innerasiatische Handel erlebt seit gut 15 Jahren phänomenale Zuwachsraten. Allein in China sind seit Beginn der wirtschaftlichen Öffnung im Jahr 1978 mehr als 800 Mrd. US Dollar an ausländischen Direktinvestitionen geflossen und ein Ende dieses Booms ist gerade bei deutschen Unternehmen nicht in Sicht. Viele deutsche Unternehmen sind geschäftlich in ganz Asien tätig oder planen entsprechende Investitionen.

Vielfach kommen Unternehmen im Ausland jedoch nur „ins Geschäft", wenn sie Schmiergelder an Entscheidungsträger ihrer Geschäftspartner tätigen. Ein häufig anzutreffendes Beispiel ist die Zahlung von sog. *kick-backs* an einen Einkaufsmitarbeiter, Geschäftsführer oder nicht selten auch den Firmeninhaber selbst, der überhöhte Lieferpreise akzeptiert und dafür im Gegenzug von dem Vertragspartner einen Teil des überhöhten Einkaufspreises persönlich zurückerhält. Bestechungsgelder sind in vielen Ländern Asiens an der Tagesordnung und können bei öffentlichen Aufträgen bis zu 30 % der Auftragssumme oder mehr ausmachen.[23] Der Politik nahestehende Unternehmer finanzieren teilweise die Wahlkämpfe der Regierungspartei und erhalten danach ohne Ausschreibung staatliche Großaufträge.[24] Teure Geschenke und unangemessene Bewirtung von Behördenvertretern

[22] *Fietz/Weidlich*, RIW 2005, S. 362 ff.

[23] *Bhargava/Bolongaita* (Hrsg.), Challenging Corruption in Asia, 2004.

[24] *Heberer,* Unter- und überschätzt: Die fixen Kosten der Korruption. Ein globales Phänomen und seine Ausprägungen in Südostasien, http://www.gruene-linke.de/themen/korruption/17_asienhaus_fixe-kostenkorruption.pdf.

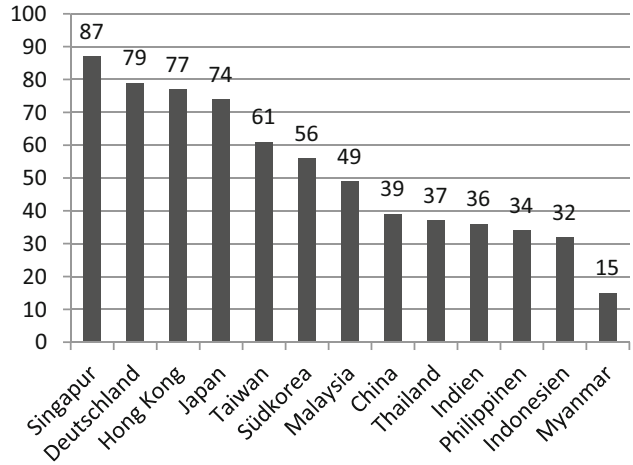


Abb. 1 Korruptionsgrad Deutschlands und der wichtigsten asiatischen Länder. (http://www.transparency.org/cpi2012/results)

sind in Asien ebenfalls gang und gebe, wobei oft sehr kreativ vorgegangen wird, um ein Aufdecken solcher Vorgänge durch interne oder externe Prüfer zu verhindern.[25]

Der *Corruption Perceptions Index* (CPI)[26] stellt jährlich den Grad der Korruption in 176 Ländern der Welt dar. Die Skala reicht von Index 0 (absolut korrupt) bis 100 (korruptionsfrei). Dem CPI aus dem Jahr 2012 zufolge verzeichnen die asiatischen Länder unterschiedliche Erfolge im Kampf gegen Korruption. Während etwa Singapur und Hong Kong an der Spitze stehen, verbleiben die Wachstumsmärkte China und Indien am Ende der Skala (Abb. 1).

Als besonders korruptionsanfällige Branchen gelten nach dem *Bribe Payers Index* (BPI) 2011[27] die Bauwirtschaft (5,3), die Öl- und Gasindustrie (6,2) und die Bergbauindustrie (6,3), wobei der BPI vom Index 0 (hohe Korruption) bis zum Index 10 (niedrige Korruption) reicht (Abb. 2).

Eines der problematischsten Länder ist weiterhin Indien. Viele Inder (und häufig auch ausländische Investoren) sehen Korruption traditionell als einen Weg, Dinge schneller und einfacher zu regeln. Insoweit ist Bestechung in Indien vielfach eine (allzu menschliche) Reaktion auf die ausufernde Bürokratie des Landes. Beamte missbrauchen ihre Position, ohne ernsthaft mit rechtlichen Folgen rechnen zu müssen; vielfach leben Beamte von Zuwendungen, da die Einkommen im öffentlichen Dienst sehr niedrig sind. Entsprechend befand sich Indien im *Corruption Perceptions Index (CPI)* von Transparency International im Jahr 2012 lediglich auf Rang 94 von 176 untersuchten Ländern. Angetrieben von der Antikorruptionsbewegung um die Aktivisten Anna Hazare und Arvind Kejriwal scheint sich das Bild in Indien nun aber zu wandeln. In jüngster Vergangenheit wurden mehrere größere Bestechungsskandale im Land aufgedeckt. So hätten Unregelmäßigkeiten bei der

[25] *Haselberger*, Blickpunkt Asia Pacific 6/12.

[26] http://www.transparency.org/cpi2012/results.

[27] http://bpi.transparency.org/bpi2011/results.

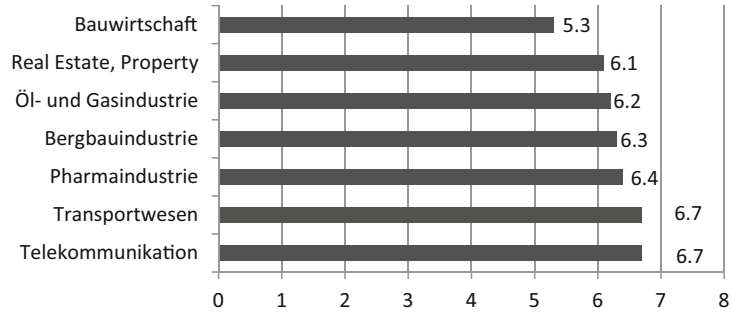


Abb. 2 Korruptionsanfällige Branchen. (http://bpi.transparency.org/bpi2011/results)

Auftragsvergabe für die Commonwealth-Games Indien 2010 beinahe die Spiele gekostet. Die Vergabe von Telefonlizenzen zu Schleuderpreisen ohne die üblichen Versteigerungen führte gar zur Entlassung des Telekommunikationsministers. Betroffen von dem Skandal war unter anderem die norwegische Telenor, fünftgrößter Mobilfunkanbieter weltweit. Dem Staat sollen bis zu 28 Mrd. Euro Lizenzeinnahmen entgangen sein. Da verwundert es nicht, dass die Korruption als eine der größten Wachstumsbremsen Indiens angesehen wird. Studien gehen davon aus, dass bei nur zehn Punkten Gewinn auf der CPI-Skala (z. Zt. 36/100) ein zusätzliches Wirtschaftswachstum von 3 % möglich wäre.

Singapur und Hong Kong ist es durch spezielle Programme und strenge Gesetze gelungen, die Korruption auf ihrem Gebiet deutlich einzudämmen und sich damit von ihren korruptionsgeplagten Nachbarstaaten abzuheben. Es ist kein Zufall, dass gerade diese Standorte in den vergangenen Jahren für ausländische Investoren besonders attraktiv waren und zugleich zum stabilen Standbein für Transaktionen in benachbarte Länder wurden. Inzwischen gibt es Anzeichen, dass immer mehr asiatische Länder ernsthafter gegen Korruption vorgehen.[28] Dies gilt beispielsweise schon seit Längerem für Malaysia, Südkorea oder China,[29] wo sich die politische Führung dem Thema sichtbar angenommen hat und es regelmäßig zu einer Reihe von Verhaftungen hochrangiger Amtsträger und Unternehmer im Zusammenhang mit Korruptionsvorwürfen kommt. Insbesondere China verschärft seine Anstrengungen, der omnipräsenten Korruption entgegen zu wirken. Die Volksrepublik steht zurzeit auf Rang 80 des CPI. Die chinesische Regierung hat verkündet, dass sie dies nicht länger hinnehmen und nun härter gegen Korruption vorgehen werde. Eine im Mai 2011 in Kraft getretene Änderung des chinesischen Strafgesetzbuches (Art. 164 Abs. 2) bezieht nun ähnlich wie der *UK Bribery Act*, der *Foreign Corrupt Practices Act* und das deutsche Strafgesetzbuch (StGB) die Bestechung ausländischer staatlicher Funktionäre und besonders auch die Begehung von Bestechungen im Ausland mit ein.

[28] *Kleine- Brockhoff*, Korruptionsvorwürfe gegen Siemens in Indonesien, http://www.tagesspiegel.de/wirtschaft/Siemens-Korruption-Siemens;art975,2399634.

[29] *Qiao*, Bestechung ist der falsche Weg, China Contact, 1/2007, S. 31.

Ein besonderes Augenmerk legt die chinesische Regierung auf Sanktionen gegen bestechliche Beamte und Parteikader. Allein im Jahr 2010 wurden über 28.000 Beamte überführt. Hierzu passt die öffentlichkeitswirksame Entmachtung des chinesischen Politikers Bo Xilai, der in einen der größten Politskandale Chinas verwickelt sein soll.[30] Aber auch das operative Management staatlicher Unternehmen wird immer öfter strafrechtlich zur Verantwortung gezogen. In den vergangenen Jahren wurden teilweise drakonische Strafen gegen sog. „staatliche Manager" verhängt. So wurde zum Beispiel ein hochrangiger Mitarbeiter des staatlichen Telekommunikationsriesen China Mobile im Zusammenhang mit den Korruptionsskandalen um Siemens im Juni 2011 zur Todesstrafe (unter Aufschub) verurteilt. Schließlich wird auch in der Privatwirtschaft härter durchgegriffen: Der ehemalige Vorstandsvorsitzende der großen Elektromarktkette Gome wurde 2010 wegen Bestechung und Insiderhandels zu 14 Jahren Haft und zu einer Geldstrafe von etwa 70 Mio. Euro verurteilt. Weitere Fälle sind etwa die Verurteilung des stellvertretenden Bürgermeisters von Peking im Jahr 2006 zum Tode sowie die Verurteilungen mehrerer Mitarbeiter des britisch-australischen Minengiganten Rio Tinto im Jahr 2010.

3.2 Die strafrechtliche Ausgangslage in Deutschland

Die Bestechung ausländischer Amtsträger wird in Deutschland als Folge der OECD Antikorruptions-Konvention seit dem 15. Februar 1999 bestraft.[31] Das 1997 erlassende Gesetz zur Bekämpfung internationaler Bestechung (IntBestG) stellt ausländische Amtsträger und Richter hinsichtlich der Vorschriften der §§ 334 ff. StGB deutschen Amtsträgern und Richtern gleich. Gleiches gilt für Deutsche, die Bestechungen gegenüber ausländischen Amtsträgern oder Abgeordneten begehen. Darüber hinaus droht deutschen Firmen und deren Repräsentanten seit dem 1. September 2002 auch im privatwirtschaftlichen Sektor bei Bestechungshandlungen im Ausland eine strafrechtliche Verfolgung in Deutschland. Nach § 299 Abs. 2 StGB macht sich strafbar, „wer im geschäftlichen Verkehr zu Zwecken des Wettbewerbs einem Angestellten oder Beauftragten eines geschäftlichen Betriebes einen Vorteil für diesen oder einen Dritten als Gegenleistung dafür anbietet, verspricht oder gewährt, dass er ihn oder einen anderen bei dem Bezug von Waren oder gewerblichen Leistungen in unlauterer Weise bevorzugt". Nicht darunter fallen der Erwerb zur eigenen Verwendung und mangels Außenwirkung betriebsinterne Tätigkeiten.[32] Zu Zwecken des Wettbewerbs handelt der Täter, wenn die Tat objektiv geeignet ist, den eigenen oder fremden Absatz zu fördern und der Täter in der Absicht handelt, sich oder einem Dritten einen Vorteil am Markt zu verschaffen.[33] Die Person des Mitkonkurrenten muss dabei noch

[30] http://www.zeit.de/politik/ausland/2012-09/bo-xilai-china-partei-ausschluss

[31] *Gildeggen/Willburger*, Internationale Handelsgeschäfte, 4. Aufl. 2012, S. 240.

[32] *Heine*, in: Schönke/Schröder, Kommentar zum Strafgesetzbuch, 28. Aufl. 2010, § 299 Rn. 9.

[33] *Dannecker*, in: Kindhäuser/Neumann/Paeffgen, Kommentar zum Strafgesetzbuch, 4. Auflage 2013, § 299 Rn. 67.

nicht im Einzelnen feststehen, um eine Strafbarkeit aus § 299 Abs. 2 StGB begründen zu können.[34] Zudem setzt eine Vollendung keine erfolgreiche Bevorzugung des Mitbewerbers voraus; es genügt, dass die Handlung darauf abzielt.[35] Mit § 299 Abs. 3 StGB sind grundsätzlich alle bestechungsrelevanten Tatbestände auch im Ausland erfasst, sei es inner- oder außerhalb der Europäischen Union.[36]

Die meisten Bestechungsfälle im privaten Sektor können in Deutschland strafrechtlich verfolgt werden, wenn der Täter Deutscher und die Tat am Tatort mit Strafe bedroht ist oder der Tatort keiner Strafgewalt unterliegt (§ 7 Abs. 2 Nr. 1 StGB). Die Vorschrift ermöglicht damit eine Bestrafung deutscher Täter in Deutschland, wenn am ausländischen Tatort eine dem § 299 StGB entsprechende Vorschrift zur Bestechung/Bestechlichkeit im Wirtschaftsverkehr in Kraft ist.[37] Denkbar ist ferner eine Strafverfolgung gestützt auf § 7 Abs. 1 StGB, wenn die Tat im Ausland „gegen einen Deutschen" begangen wurde. Auch wenn die im Ausland begangene Bestechungstat dort nicht unter Strafe steht und ein Deutscher dafür in Deutschland nicht verfolgt werden kann, sind Teilnahmehandlungen in Deutschland strafbar. Anstiftung oder Beihilfe etwa durch das Bereitstellen von Bestechungsgeldern im deutschen Mutterhaus für Auslandsgeschäfte eines deutschen Mitarbeiters können verfolgt werden, da eine rechtswidrige, vorsätzliche Haupttat (§ 9 Abs. 2 StGB) stets vorliegt. Im Übrigen ist für den Teilnehmer deutsches Strafrecht anwendbar, wenn er an einer Auslandstat im Inland Hilfe geleistet hat, selbst wenn die Haupttat nach dem Recht des Tatorts nicht unter Strafe steht (§ 9 Abs. 2 S. 2 StGB). Bei der Bestechung von Entscheidungsträgern von Unternehmen wie auch Amtsträgern ist ein Durchgriff auf die hinter den Bestechenden stehenden Unternehmen möglich. § 130 OWiG verpflichtet den Betriebsinhaber, bestimmte Aufsichtsmaßnahmen auch zur Korruptionsvermeidung durchzuführen. Werden vorsätzlich oder fahrlässig diese betriebsbezogenen Pflichten verletzt, kann über den nach § 30 OWiG möglichen Durchgriff auch ein Bußgeld gegen das Unternehmen selbst verhängt werden. Da die Geldbuße nach § 17 Abs. 4 OWiG den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen soll, kann ein Bußgeld im Falle des Nachweises in praktisch unbegrenzter Höhe verhängt werden.[38]

---

[34] *Dannecker*, in: Kindhäuser/Neumann/Paeffgen, Kommentar zum Strafgesetzbuch, 4. Auflage 2013, § 299 Rn. 67.

[35] *Lackner/Kühl*, Kommentar zum Strafgesetzbuch, 27. Aufl. 2011, § 299 Rn. 7.

[36] *Heine*, in: Schönke/Schröder, Kommentar zum Strafgesetzbuch, 28. Aufl. 2010, § 299 Rn. 2.

[37] *Eser*, in: Schönke/Schröder, Kommentar zum Strafgesetzbuch, 28. Aufl. 2010, § 7 Rn. 17.

[38] *Bohnert*; Kommentar zum Ordnungswidrigkeitengesetz, 3. Aufl., § 17 Rn. 1.

3.3 Fazit

Vor dem Hintergrund der internationalen Bestrebungen zur Bekämpfung von Korruption und Geldwäsche, der wachsenden Zahl einschlägiger nationaler Strafgesetze und der zunehmenden Verfolgung von Korruptionsdelikten in vielen Ländern sollten global operierende Unternehmen dem Thema erhöhte Aufmerksamkeit widmen. Mit der Regelung des § 299 Abs. 3 StGB rücken auch Auslandssachverhalte verstärkt ins Blickfeld der deutschen Strafverfolgungsbehörden. Der Bundesgerichtshof hat im sog. Siemens-Prozess[39] bereits das Bilden schwarzer Kassen als Untreue gem. § 266 Abs. 1 StGB gegen das Unternehmen gewertet. Bei Siemens hatte sich ein System zur Leistung von Bestechungsgeldern (sog. nützliche Aufwendungen) entwickelt, dass die Deponierung von Geldern auf Konten bei diversen Banken in Liechtenstein, der Schweiz und Dubai vorsah, die auf die Namen verschiedener anderer Unternehmen lauteten. Die Staatsanwaltschaft bezifferte die Summe in diesen schwarzen Kassen auf ca. 200 Mio. Euro. Nach Ansicht des Bundesgerichtshofs stellt bereits das Entziehen und Vorenthalten erheblicher Vermögenswerte unter Einrichtung von verdeckten Kassen einen endgültigen Nachteil im Sinne des § 266 Abs. 1 StGB dar. Auf die Absicht, das Geld im wirtschaftlichen Sinne des Treugebers verwenden zu wollen, kommt es dabei nicht an. Mit der BGH-Rechtsprechung wird die Bestrafung korrupter Mitarbeiter bereits im Vorfeld von Schmiergeldzahlungen ermöglicht. Diese Fälle werden zunehmen, nicht zuletzt aufgrund der Meldepflichten der Finanzbehörden. Es steht zu erwarten, dass die deutschen Finanzbehörden auch Auslandssachverhalte im Rahmen von Betriebsprüfungen vermehrt aufgreifen werden. Auch aufgrund der aktiven Zusammenarbeit zwischen den Strafverfolgungsbehörden und den Finanzverwaltungen hat sich das Entdeckungsrisiko für Unternehmen deutlich erhöht.

Die Korruptionsrisiken sind eindeutig: neben hohen Haftstrafen und empfindlichen Geldbußen kann es zu einer nationalen oder sogar internationalen Sperre des betroffenen Unternehmens beispielsweise für öffentliche Aufträge kommen. Darüber hinaus droht der Verlust staatlicher Kreditgarantien. Der allgemeine Imageverlust durch öffentlichkeitswirksame Hausdurchsuchungen und negative Presseberichterstattung ist vielmals nicht mit Geld aufzuwiegen. Ein Bestechungsskandal auch weitab des Mutterhauses kann im „*global village*“ schnell zu „*global news*“ werden. US-amerikanische Multinationals sehen sich bereits seit 1977 unter dem *Foreign Corrupt Practices Act* dem Risiko einer Strafverfolgung führender Mitarbeiter, einem Reputationsverlust für das Unternehmen und den damit verbundenen Kosten ausgesetzt. Viele amerikanische Firmen haben dementsprechend seit geraumer Zeit detaillierte Verhaltensregeln („*Code of Conduct and Business Ethics*“) für ihre Mitarbeiter. Auch deutsche Unternehmen und ihre Mitarbeiter sollten über die regionalen Gegebenheiten in Asien informiert sein, um neben einer etwaigen Strafverfolgung in Deutschland nicht in Konflikt mit den lokalen Strafgesetzen zu kommen. Vertragsgestaltungen und geschäftliche Praktiken sollten überdacht und erfor-

[39] BGH v. 29.8.08– 2 StR 587/08, NJW 2009, S. 89.

derlichenfalls neu geregelt werden. Verantwortlichkeiten müssen deutlich gemacht und dokumentiert werden.

Der Bundesgerichtshof fordert in mehreren Urteilen[40] eine organisatorische Vorsorge. Ein Unternehmen kann sich vor Wissenszurechnung nur dann schützen, wenn es einen angemessenen Informationsfluss nachweisen kann. Im Schadensfall kann eine Entlastung dann durch gute Informationsorganisation und den Nachweis einer regelmäßigen Kontrolle und Schulung erfolgen.[41] Klare Konzerndirektive muss sein, dass Korruption an keiner Stelle und in keiner Form geduldet und unternehmensintern streng sanktioniert wird. Dies darf sich jedoch nicht auf die bloße Erstellung von Moralkodizes beschränken.[42] Als Konsequenz aus dem Korruptionsskandal versucht Siemens, seine Mitarbeiter mit verschärften sog. *Business Conduct Guidelines* zu gesetzestreuem Verhalten anzuhalten.[43]

Andere Großkonzerne wie die Deutsche Bahn AG zeigen sich entschlossen, jedes einzelne Korruptionsdelikt zur Anzeige zu bringen.[44] Dort wie auch in anderen Unternehmen haben die damit verbundenen internen Untersuchungen und Überwachungen allerdings eine Diskussion ausgelöst, ob man bei den Bemühungen, Korruption bereits im Ansatz zu ersticken, teilweise nicht über das Ziel hinaus geschossen ist.

4 Beschäftigung von Mitarbeitern im Ausland

4.1 Arbeitnehmerentsendung

Vor allem in der Anfangsphase werden Schlüsselpositionen einer ausländischen Tochtergesellschaft regelmäßig durch sog. *Expatriates* besetzt. Zu den Gründen zählen vor allem die Sicherung europäischer Qualitätsmaßstäbe und eine bessere Umsetzung der Unternehmensphilosophie des Mutterhauses.[45] Dazu werden häufig deutsche oder europäische

[40] BGH v. 8.12.1989– V ZR 246/87, DNotZ 1991, 122; BGH v. 2.2.1996– V ZR 239/94, DNotz 1996, 986, 988.

[41] Zur Errichung einer Compliance-Organisation *Hauschka*, ZIP 2004, S. 877 ff.

[42] *Bannenberg/Schaupensteiner*, Korruption in Deutschland-Portrait einer Wachstumsbranche, S. 67.

[43] http://www.compliancemagazin.de/markt/unternehmen/complianceprogramme/igmetall111206.html.

[44] Die Deutsche Bahn hatte über mehrere Monate bei einem der Korruption verdächtigen Angestellten Kontobewegungen und Bankunterlagen überwacht; http://www.sueddeutsche.de/wirtschaft/145/ 464743/text/.

[45] *Kolvenbach/Hölzchen*, Nicht Jugend, Erfahrung zählt: Personalentsendungen nach Asien, China Contact, 10/2007, S. 47.

Mitarbeiter ins Ausland entsandt. Im Vorfeld sollte allerdings eine sorgfältige Planung aller rechtlichen und persönlichen Angelegenheiten des Auslandseinsatzes erfolgen.[46]

Die Gestaltung der Arbeitsverträge entsandter Mitarbeiter richtet sich hauptsächlich nach der Dauer der Entsendung. Handelt es sich um einen kurzfristigen Auslandseinsatz, wird der deutsche Arbeitsvertrag meist um eine Entsendevereinbarung ergänzt. Im Falle eines langfristigen Auslandeinsatzes ruht in der Regel das deutsche Arbeitsverhältnis und es wird ein befristeter Arbeitsvertrag mit dem Unternehmen im Ausland abgeschlossen. Bei einem unbefristeten Auslandseinsatz schließlich wird das deutsche Arbeitsverhältnis typischerweise aufgehoben und als Folge des „Übertritts" ein Arbeitsverhältnis mit dem ausländischen Unternehmen eingegangen. In diesem Fall erhält der Mitarbeiter dann meistens keine Rückkehrgarantie mehr.[47]

In der Praxis finden sich vielfach Mischformen oder – sehr häufig anzutreffen – schlicht unklare oder unverbindliche Regelungen. Die Verhandlung eines Entsendevertrages sollte gerade aufgrund der erhöhten Komplexität der Rechtsbeziehungen zum Anlass genommen werden, eine übersichtliche und die aktuellen Gegebenheiten reflektierende Vertragsgrundlage zu schaffen. Zu den wichtigen Regelungspunkten gehören eine genaue Beschreibung von Position, Aufgabenbereich und ggf. Berichtspflichten, Bestimmungen zur Vergütung nebst etwaiger Auslandszulagen, Anpassungsregelungen bei Währungskursschwankungen und die Festlegung der Steuerpflichten im Gast- und/oder Entsendeland. Weiterhin sind besondere Klauseln hinsichtlich der Ausreise sowie zu regelmäßigen Familienheimflügen, zu den Rechten und Pflichten bei einer Versetzung und der anschließenden Rückkehr sowie zu Kündigungsfristen und sonstigen bei Beendigung des Arbeitsverhältnisses zu regelnden Fragen erforderlich.

Auch im Arbeitsrecht gilt zunächst das Prinzip der Vertragsautonomie, d. h. die Parteien können das Arbeitsverhältnis einem von ihnen gewählten Recht unterwerfen.[48] Überlagert wird eine solche Rechtswahl aber ggf. von zwingenden arbeitsrechtlichen Vorschriften des objektiven Vertragsstatuts. Schon dessen Bestimmung ist jedoch nicht ganz einfach: Wurde kein besonderes Recht vereinbart, unterliegt der Arbeitnehmer grundsätzlich dem Recht des Staates, in dem er gewöhnlich seine Arbeit verrichtet, selbst wenn er vorübergehend in einen anderen Staat entsandt wurde. Bis zu welchem Zeitraum eine lediglich vorübergehende Entsendung vorliegt, ist zweifelhaft. Soweit der Einsatz im Ausland nicht auf Dauer angelegt ist und drei Jahre nicht überschreitet, dürfte der vorübergehende Cha-

[46] *Brandt*, Gold im Kopf oder Klotz am Bein: Wer nach China entsandt wird, braucht die volle Unterstützung durch das Mutterhaus – vor, während und nach dem Aufenthalt, ASIA BRIDGE, 4/2006, 34.

[47] *Braun/Gröne*, in: Henssler/Braun, Arbeitsrecht in Europa, 3. Aufl. 2011, Europäisches IPR des Arbeitsrechts, Rn. 44.

[48] *Reithmann/Martiny*, Internationales Vertragsrecht, 6. Aufl. 2004, 5. Teil: Einzelne Vertragstypen V. Arbeitsvertrag, Rn. 1871.

rakter gewahrt sein, mit der Folge, dass aus deutscher Sicht deutsches Arbeitsrecht auf das Arbeitsverhältnis mit dem Heimatunternehmen Anwendung findet.[49]

Bei Arbeitsverträgen mit entsandten ausländischen Arbeitnehmern sollte – im Interesse beider Parteien – sorgfältig überlegt werden, ob nicht ausdrücklich deutsches oder ein anderes ausländisches Recht vereinbart wird. Bei entsprechendem Sachzusammenhang und mit gewissen Einschränkungen ist eine solche Rechtswahl bei ausländischen Arbeitnehmern aus Sicht der meisten ausländischen Rechtsordnungen regelmäßig zulässig.

Stets von besonderem Interesse ist die steuerliche Gestaltung einer Entsendung. Die individuelle Steuerlast kann oftmals durch verschiedene Gestaltungsmöglichkeiten verringert werden, etwa den Abschluss dualer Arbeitsverträge oder die Gewährung geldwerter Vorteile. Vor Umsetzung sollte dies jedoch sorgfältig bedacht und erforderlichenfalls Rat eingeholt werden. Die Steuererklärungen von *Expatriates* werden in vielen Ländern verstärkt geprüft und Fehler oder unterlassene Informationen können sehr kostspielige Konsequenzen haben. Die Steuerbehörden können Bußgelder bis zur doppelten Höhe der zu wenig gezahlten Steuern erheben, in Betrugsfällen kann das Bußgeld teilweise sogar bis zu drei- oder viermal so hoch sein. Häufige Fehler sind die unterlassene Angabe aller Sachleistungen wie insbesondere Pensionsbeiträge, Wohnungs- oder Schulzulagen und sonstige Zuschüsse.

4.2 Beschäftigung lokaler Arbeitnehmer

Viele Länder in Asien haben sehr arbeitnehmerfreundliche Gesetze, die teilweise in ihrer Komplexität kaum hinter den deutschen Regelungen zurückstehen. Außerdem gibt es zahlreiche lokale Praktiken, die aus deutscher Sicht sehr gewöhnungsbedürftig sind.

In **China** sind Anfang 2008 mit dem Arbeitsvertragsgesetz (AVG), dem Arbeitskonfliktgesetz und dem Arbeitsförderungsgesetz drei umfangreiche Gesetze auf dem Gebiet des Arbeitsrechts mit der Maßgabe in Kraft getreten, die individuellen Rechte und Interessen der Arbeitnehmer zu kodifizieren und zu stärken.[50] In der Praxis bestehen jedoch weiterhin Einschränkungen für die direkte Rekrutierung von Mitarbeitern durch ausländisch investierte Gesellschaften (*Foreign Invested Enterprises* (FIE)). So kann für eine Anzeige zur Suche nach Arbeitnehmern beispielsweise die Genehmigung der örtlichen Arbeitsbehörde vorgeschrieben sein.[51] Vielfach neigen FIEs deshalb dazu, Arbeitnehmer aus einer von den örtlichen Arbeitsbehörden getroffenen Bewerbervorauswahl auszusuchen. Anstellungsverträge mit chinesischen Arbeitnehmern müssen schriftlich abgefasst und der örtlichen Arbeitsbehörde binnen einen Monats nach Vertragsschluss zur Zertifizierung vorgelegt

[49] *Braun/Gröne,* aaO, (FN 46).

[50] *Binding, Thum,* RdA 2008, S. 347 ff.; einen Überblick über die wesentlichen, durch das AVG bedingten Veränderungen des chinesischen Arbeitsrechts geben auch *Däubler, Wang*, RdA 2008, S. 141 sowie *Li/Frik*, NZA 2008, S. 86.

[51] *Falder*, Neue Spielregeln im chinesischen Arbeitsrecht: Arbeitsvertragsgesetz tritt am 1. Januar 2008 in Kraft, China Contact, 9/2007, S. 33.

werden. Falls das Schriftformerfordernis nicht eingehalten wird, entsteht ein faktisches Arbeitsverhältnis mit unbefristeter Dauer. Mit Blick auf die restriktiven Kündigungsvoraussetzungen ist diese Rechtsfolge eine gravierende Sanktion. Es ist daher üblich, mit den zuständigen Behörden bzw. Gewerkschaften einen Standardarbeitsvertrag abzustimmen. Darüber hinaus werden viele größere Unternehmen durch § 4 AVG angehalten, eine Übersicht über alle wesentlichen Regeln und Entscheidungen zu den Angelegenheiten der Arbeitnehmer innerhalb der jeweiligen Arbeitgebereinheit zu führen (sog. *Employee Handbook*) und diese den Arbeitnehmern bekannt zu machen.[52] Diese Bestimmungen können vor allem für verhaltensbedingte Kündigungen sehr wichtig werden und sollten sorgfältig mit den Standardarbeitsverträgen abgestimmt sein. Zweifelsfragen in Bezug auf das Arbeitsverhältnis werden grundsätzlich im Sinne des Arbeitnehmers entschieden, so dass auf klare Regelungen besonders geachtet werden muss. Wettbewerbsverbote oder ähnliche Regelungen zum Schutz des Arbeitgebers sind zulässig, unterliegen jedoch Einschränkungen wie beispielsweise der Zahlung einer Karenzentschädigung und Beschränkungen in zeitlicher, geographischer und branchenbezogener Hinsicht, die mit denen in westlichen Rechtssystemen vergleichbar sind. Ein nachvertragliches Wettbewerbsverbot darf gem. §§ 23 Abs. 2, 24 AVG maximal zwei Jahre betragen und die zwingend zu zahlende Karenzentschädigung muss angemessen sein.

Indien gehört zu den Ländern mit den rigidesten Arbeitsgesetzen der Welt, die etwa die Schließung eines defizitären Betriebes sehr erschweren können. In der Praxis gelingt ein Personalabbau dann meistens ohne größere Schwierigkeiten, wenn sich der Arbeitgeber mit den Gewerkschaften auf einen Sozialplan einigt oder individuelle Absprachen mit den betroffenen Mitarbeitern schließt. Für Unternehmen mit 100 oder mehr Arbeitnehmern schreibt das Gesetz jedoch eine vorherige Genehmigung durch die zuständige Behörde vor. In der Praxis wird die Genehmigung für die Schließung eines Werkes allerdings nur sehr selten erteilt.

5 Unklare Regelungen und falsche Strukturen

Bei Geschäftsaktivitäten im Ausland ist besonderes Augenmerk auf die Ausgestaltung von Verträgen zu legen. Dies gilt sowohl für die „großen" Verträge wie Joint Venture-Verträge oder Gesellschaftsverträge als auch für die vermeintlich „kleineren, unwichtigeren" Verträge wie Liefer- oder Handelsvertreterverträge. Falsche oder nicht eindeutige Regelungen können erhebliche Nachteile für ein Unternehmen mit sich bringen, die im Nachhinein nur noch schwer zu beseitigen sind.

Im Rahmen eines **Joint Venture-Vertrags** ist stets auch eine angemessene Wettbewerbsklausel zu verhandeln. Dies gilt insbesondere dann, wenn die Mutterhäuser der Joint Venture-Partner im Kerngeschäft miteinander konkurrieren und strategische Konflikte

[52] *Binding, Thum*, aaO (FN 49).

daher vorprogrammiert sind. Der ausländische Investor, der regelmäßig Know-how und Technologien beisteuert, wird ein großes Interesse daran haben, dass der lokale Partner diese nicht zum Aufbau eines konkurrierenden Geschäfts nutzt. Insbesondere auch für die Zeit nach Beendigung des Joint Ventures ist daher bei entsprechender Verhandlungsmacht eine angemessene Regelung zu treffen. Das Wettbewerbsverbot ist dabei häufig so ausgestaltet, dass der lokale Partner weltweit nicht in Wettbewerb zu dem gemeinsamen Joint Venture treten darf, wohingegen der ausländische Partner außerhalb des betreffenden Landes frei bleibt, konkurrierende Tätigkeiten auszuüben.

In manchen asiatischen Rechtsordnungen besteht allerdings nur ein begrenzter Spielraum für die Vereinbarung eines durchsetzbaren Wettbewerbsverbots. Die für den Verstoß gegen das Wettbewerbsverbot regelmäßig vertraglich festgelegten Vertragsstrafen sind insbesondere in *Common Law*-Ländern nur dann durchsetzbar, wenn das Wettbewerbsverbot angemessen ist und die Höhe der Vertragsstrafe einer ehrlichen Schätzung des tatsächlich eingetretenen Schadens (sog. *genuine pre-estimate of actual damages,* sog. *liquidated damages*) entspricht.[53] Außerdem sollten Joint Venture-Verträge auch immer praktikable Regelungen zur Lösung von Pattsituationen enthalten. Viele Kooperationen scheitern letztlich daran, dass im Vorfeld nicht genügend Augenmerk auf die Entschärfung und Lösung von Konflikten gelegt wurde.

In **Indien** war in der Vergangenheit eine weitere Besonderheit zu beachten. Gemäß der Press Note No. 1 (2005)[54] galt die Regelung, dass ausländische Investoren, die ein weiteres Joint Venture (oder andere Kooperationsvereinbarungen) im gleichen Geschäftsfeld in Indien eingehen wollten, ein sog. *No Objection Certificate* (Unbedenklichkeitsbescheinigung) des bisherigen indischen Joint Venture-Partners benötigten. Mit dem Circular 1/2011 entfällt diese Pflicht für ausländische Investoren, sich eine solche Unbedenklichkeitsbescheinigung zu besorgen.

Bei Staaten des *Common Law*, unter anderem Indien und Singapur, gilt es ferner, die sog. *parol evidence rule* (Vermutung der Vollständigkeit und Richtigkeit einer Urkunde) zu berücksichtigen. Diese auf englischem Recht basierende Regelung wurde unter anderem in §§ 93, 94 des *Singapore Evidence Act* verankert und schreibt die Wortlautauslegung eines Schriftstückes vor. Im Gegensatz zum deutschen und anderen Zivilrechtssystemen, in denen der wirkliche Wille der Parteien zu erforschen ist, werden mit einigen Ausnahmen äußere Umstände, die dem Wortlaut des schriftlichen Vertrages widersprechen oder ihn abändern, nicht berücksichtigt. Auch deshalb sollten Verträge in diesen Ländern besonders umfassend und sorgfältig gestaltet werden.

Bei **Handelsvertreterverträgen** wird oftmals übersehen, dass der ansonsten zwingend vorgesehene Ausgleichsanspruch eines Handelsvertreters vertraglich ausgeschlossen werden kann, wenn der Handelsvertreter seine Tätigkeit für den Unternehmer außerhalb der Europäischen Gemeinschaft oder des EWR erbringt (§ 92c HGB). Dies ist beispielsweise der Fall, wenn ein in Deutschland ansässiges Unternehmen einen Handelsvertreter in

[53] Dunlop Pneumatic Tyre Co versus New Garage and Motor [1915] AC 79.

[54] Press Note 1 (2005 Series) vom 12. Januar 2005.

Singapur mit der Betreuung der Geschäfte im asiatisch-pazifischen Raum beauftragt. Das deutsche Unternehmen kann hierbei den gesetzlich vorgeschriebenen Ausgleichsanspruch des Handelsvertreters abbedingen und so eine Zahlung bei Beendigung des Vertragsverhältnisses vermeiden. Voraussetzung für diese Rechtsfolge ist allerdings eine hinreichend klare vertragliche Regelung und eine Prüfung, ob lokale Gesetze dem möglicherweise entgegenstehen.

Darüber hinaus sollte auch bei wirtschaftlich zusammenhängenden Verträgen darauf geachtet werden, dass diese konsequent ausgestaltet und aufeinander abgestimmt sind. Dies gilt insbesondere für die Rechtswahl und die Vereinbarung einer Schiedsklausel[55]. Zwar lässt sich aufgrund zwingenden Rechts nicht immer durchgehend eine Rechtsordnung für alle Verträge vereinbaren, insbesondere dann nicht, wenn nicht alle Verträge einen Bezug zu dem Land aufweisen, dessen Rechtsordnung gewünscht ist. Dennoch sollte in diesen Fällen, soweit möglich, zumindest eine einheitliche Schiedsklausel vereinbart werden. Dies gilt vor allem vor dem Hintergrund, dass sich eine Auseinandersetzung zwischen den Vertragsparteien über einen bestimmten Vertrag oftmals auch auf andere, wirtschaftlich zusammenhängende Verträge zwischen den gleichen Parteien oder mit den Parteien verbundene Unternehmen ausdehnt. Verfahren vor mehreren Schiedsgerichten in unterschiedlichen Ländern, womöglich noch in verschiedenen Verfahrenssprachen, erschweren die Lösung der Auseinandersetzung erheblich und verursachen hohe Kosten.

6 Durchsetzung von Rechten

Die Durchsetzung von Rechten ist in vielen Ländern, vor allem außerhalb Europas, immer noch schwierig. Die Rechtssysteme vieler Schwellenländer entsprechen noch nicht dem westlichen Standard, hinzu kommt oftmals eine Überlastung der örtlichen Gerichte und/oder eine mangelnde Qualifizierung der Richter. Recht bekommen ist hier vor allem eine Frage des praktischen Vorgehens und der ausreichenden (vertraglichen) Vorsorge.

6.1 Rechtswahl

Im globalen Wirtschaftsverkehr folgen Verträge heute oft anglo-amerikanischen Vorgaben. Ohne Zweifel bietet dies in vielen Fällen Vorteile und wird häufig auch nicht dispositiv sein. Deutsches Recht sollte aber nicht unreflektiert aufgegeben werden. Mit seiner umfassenden Kodifizierung bietet das deutsche Recht einen im internationalen Vergleich hervorragenden und für deutsche Unternehmen zudem vertrauten Rahmen.

Im Ausgangspunkt sollte man sich gründlich mit der Frage auseinandersetzen, ob das jeweilige lokale Recht einen verlässlichen Rahmen für den Vertragsgegenstand bietet oder

[55] *Li/Tang,* China News Report 2008, S. 124 ff.

Alternativen angezeigt sind. Verträge können in vielen asiatischen Ländern grundsätzlich auch einer anderen als der lokalen Rechtsordnung unterstellt werden. Hierbei ist jedoch zu beachten, dass eine solche Rechtswahl oftmals nur dann wirksam ist, wenn sie *bona fide*, also in „gutem Glauben" bzw. ohne betrügerische Absicht erfolgt. Insoweit ist grundsätzlich erforderlich, dass eine gewisse Beziehung zu der gewählten Rechtsordnung besteht. Bei Verträgen zwischen lokalen und ausländischen Parteien ist allerdings regelmäßig auch die Wahl einer „neutralen" Rechtsordnung zulässig, auch wenn keine der Parteien oder der Gegenstand des Verfahrens dem gewählten Rechts zuzuordnen ist.[56]

6.2 Prozessrisiken

Asiatische Geschäftspartner vertreten ihre Position regelmäßig mit allem Nachdruck und mit Raffinesse. Es bestehen im Vergleich zu Europa noch immer fundamentale Unterschiede in der Art der Verhandlungsführung, und selbst ein unterzeichneter Vertrag wird nicht selten wieder in Frage gestellt. Auch können sich ausländische Investoren bisweilen unakzeptablen Ansprüchen von Geschäftspartnern ausgesetzt sehen oder – aufgrund ihrer Geschäftsverbindung mit einem lokalen Partner – überraschend in einen Rechtstreit mit ihnen unbekannten Dritten involviert werden. Das Prozessrisiko ist in manchen asiatischen Ländern recht hoch und Streitigkeiten werden sich häufig nicht vermeiden lassen. Ausländischen Investoren ist anzuraten, Verhandlungsergebnisse bestmöglich zu dokumentieren und das *worst case scenario* eines späteren Rechtsstreits schon beim Geschäftsabschluss einzuplanen. Vertraglich fixierte Schadensersatzsummen in bestimmter Höhe (sog. *liquidated damages*) können ein wirksames Instrument zur Sicherung von Ansprüchen sein. In Joint Venture-Verträgen sollte einer möglichen vorzeitigen Beendigung der Kooperation durch Ausstiegsklauseln (sog. *exit clauses*) gebührende Beachtung geschenkt werden.

6.3 Gerichtssysteme

Viele asiatische Gerichtssysteme lassen noch immer zu wünschen übrig. Oft sind die Richter noch zu unerfahren, um die Komplexität moderner Geschäftsabläufe ausreichend würdigen zu können. Der Ausgang eines Gerichtsverfahrens ist immer ungewiss, aber für **China**[57] gilt dies wegen der fehlenden Tradition einer unabhängigen Gerichtsbarkeit wohl in besonderem Maße. Ohne Kenntnis der Umstände eines jeden Falles lassen sich nur schwer Schlussfolgerungen ziehen, doch gibt es leider zahlreiche Belege für Entscheidungen, die rational nicht nachvollziehbar sind oder in denen Gesetze widersprüchlich angewendet wurden. Nicht nur die Verteidigung gegen eine Klage, auch die gerichtliche Durchsetzung eines Anspruchs stellt sowohl für ausländische wie für einheimische Unternehmen oft ein erhebliches Problem dar. In China sollte der Kläger daher versuchen,

[56] *Reithmann/Martiny* aaO (FN 47) Rn. 64.

[57] *Glück/Semler*, RIW 2006, S. 436 ff.

sich die Regelungen zur örtlichen Zuständigkeit der chinesischen Gerichte zunutze zu machen, um beispielsweise den allgemeinen Gerichtsstand eines chinesischen Beklagten zu umgehen. Durch den vertraglich vorgesehenen Erfüllungsort lässt sich möglicherweise der grundsätzlich erforderliche Bezug einer Sache zum Gerichtsbezirk eines erfahrenen Gerichts (wie in Shanghai, Peking oder auch in Hong Kong) herstellen. Viele in China hergestellte Waren gelangen über Hong Kong in den Weltmarkt, so dass Beschlagnahmen und andere Maßnahmen einstweiligen Rechtsschutzes in der ehemaligen britischen Kolonie stets in Betracht gezogen werden sollten.

6.4 Schiedsverfahren

Bedenken hinsichtlich der Geschwindigkeit und Unparteilichkeit von asiatischen Gerichten bestehen nicht nur bei ausländischen Investoren, sondern sind manchmal auch in der lokalen Gesellschaft verbreitet. Die meisten Verträge zwischen lokalen und ausländischen Unternehmen enthalten deshalb Schiedsklauseln, die Streitigkeiten an Schiedsgerichte verweisen (und den Weg zu den ordentlichen Gerichten zunächst verschließen sollen). Den Parteien ist es grundsätzlich freigestellt, Vereinbarungen zur Schiedsgerichtsbarkeit zu treffen. Sie können hierzu Schiedsverfahren in oder außerhalb des jeweiligen Landes bestimmen und auch die vorherige Durchführung eines Vermittlungsverfahrens (sog. Mediation) vorsehen. In der Vergangenheit wurden auch wirksam vereinbarte Schiedsgerichtsklauseln bisweilen von chinesischen Gerichten für unwirksam erklärt.[58] In der Praxis sollten möglichst die Musterschiedsklauseln der Internationalen Handelskammer (ICC) in Paris oder anderer anerkannter Schiedsorganisationen verwendet werden. Überhaupt ist bei der Abfassung der Schiedsklauseln höchste Sorgfalt geboten.[59]

Trotz Vereinbarung einer Schiedsgerichtsbarkeit und dem damit verbundenen Ausschluss der ordentlichen Gerichte kann eine Intervention der ordentlichen Gerichte aber nicht immer vermieden werden. Insbesondere die indischen Gerichte haben in der Vergangenheit oftmals auch bei ausländischen Schiedsgerichtsverfahren Einfluss auf den Ausgang des Verfahrens genommen. In jüngster Vergangenheit hat der oberste Gerichtshof (*Supreme Court*) in **Indien** nun aber mit seiner Entscheidung vom 6. September 2012 in dem Verfahren *Baharat Aluminium Company vs. Kaiser Aluminium Technical Services Inc.* [60] die Interventionsmöglichkeiten indischer Gerichte in ausländischen Schiedsverfahren beschränkt. Das Gericht hat geurteilt, dass indische Gerichte nicht die Kompetenz

[58] Nach *Trappe*, SchiedsVZ 2006, 258, 263 mit Verweis auf Art. 58 Arbitration Law steht in China der Weg zum Gericht zur Klärung der Wirksamkeit der Schiedsvereinbarung stets offen. Ist am Schiedsort das Fehlen einer wirksamen Schiedsvereinbarung festgestellt worden, so ist diese Feststellung auch für das deutsche Exequaturgericht bindend, sofern sie anerkennungsfähig ist, vgl. hierzu *KG Berlin*, v. 18.5. 2006–20 Sch 13/04 (unveröffentlicht); *Kröll*, NJW 2007, 743, 749.

[59] http://www.iccwbo.org./uploadedFiles/TimeCost_E.pdf.

[60] http://judis.nic.in/supremecourt/disppdfjud.asp

besitzen, internationale Schiedsgerichtsverfahren zu überprüfen, sofern diese nicht in Indien stattfinden. Ausländische Schiedssprüche sind nur dann einer Überprüfung durch die indischen ordentlichen Gerichte unterworfen, sofern es um die Vollstreckung dieser ausländischen Schiedssprüche in Indien geht. Der indische Supreme Court hat damit seine frühere Rechtsprechung aufgegeben und die bis dahin bestehenden Zweifel an der Durchsetzbarkeit ausländischer Schiedssprüche in Indien zu einem großen Teil ausgeräumt. Auch in **China** gibt es im Bereich der Schiedsverfahren einige Veränderungen. Die *China International Economic and Trade Arbitration Commission (CIETAC)* – eine der am häufigsten gewählten Schiedsinstitution in China – hat im Mai 2012 ihre neuen Schiedsregeln in Kraft gesetzt. Hiermit erfolgt eine Annäherung an die moderne internationale Schiedspraxis. Im Besonderen wird die Rolle der beteiligten Parteien gestärkt und der Ermessensspielraum des Schiedsgerichts stärker eingeschränkt. Das Schiedsgericht wird angehalten stärker als zuvor auf die Besonderheiten des Einzelfalls und somit auf die Parteien einzugehen.[61]

Ein inländisches Schiedsurteil kann in den meisten Ländern Asiens durchgesetzt und vollstreckt werden.[62] Einwände gegen die Vollstreckung können nur unter ganz bestimmten Umständen geltend gemacht werden. Ein solches Vollstreckungshindernis stellt beispielsweise die Verletzung von Verfahrensvorschriften dar. Auch ist das Schiedsurteil dann nicht vollstreckbar, wenn der Streitgegenstand nicht schiedsgerichtsfähig war. Die Vollstreckung ausländischer Schiedsurteile richtet sich neben den jeweiligen lokalen Gesetzen vor allem nach den New Yorker und Genfer Abkommen zur gegenseitigen Anerkennung ausländischer Schiedssprüche, die sowohl Deutschland als auch eine Vielzahl der asiatischen Länder unterzeichnet haben. Ein in Einklang mit diesen internationalen Übereinkommen erlassenes ausländisches Schiedsurteil ist für die beteiligten Parteien bindend und wird von den lokalen Gerichten grundsätzlich anerkannt. Die im Schiedsverfahren obsiegende Partei muss bei dem sachlich und örtlich zuständigen Gericht im jeweiligen Land einen Antrag auf Vollstreckung des ausländischen Schiedsurteils stellen.

Die Vollstreckung ausländischer Gerichtsurteile ist im Vergleich zu Schiedsurteilen insbesondere in *Common Law*-Ländern wie Indien oder Singapur dagegen schwieriger. Für die Vollstreckung deutscher Gerichtsurteile muss oftmals ein eigenes Gerichtsverfahren angestrengt werden, in dem das deutsche Urteil mit gewissen Erleichterungen nochmals erstritten werden muss. Die Vereinbarung eines (in- oder ausländischen) Schiedsverfahrens ist auch vor diesem Hintergrund meist vorzugswürdig.

---

[61] *Pörnbacher/Knief*, BB 2012, S. 2967.

[62] Für China *Trappe*, SchiedsVZ 2006, 258, 268.

6.5 Investitionsschutz

Ausländische Investoren können – was oft nicht beachtet wird – Rechtsschutz möglicherweise auch aufgrund von Investitionsschutzabkommen erhalten.[63] Solche Investitionsschutzabkommen hat Deutschland mit mehreren asiatischen Ländern unterzeichnet, unter anderem mit Indien und China. Diese zwischenstaatlichen Verträge bieten ausländischen Investoren Schutz für den Fall diskriminierender Maßnahmen von Seiten staatlicher Behörden und erlauben es, Schadensersatz direkt vor internationalen Schiedsgerichten einzufordern. Streitigkeiten werden im Regelfall an das *International Centre for the Settlement of Investment Disputes* (ICSID) in Washington verwiesen (unter Umständen mit Vorrang auch vor ausschließlichen Zuständigkeitsklauseln in einem Vertrag). Die Besonderheit von Investitionsschutzabkommen besteht darin, dass der Gang zu einem Schiedsgericht auch dann möglich ist, wenn in den Vereinbarungen der Parteien selbst keine Schiedsklausel enthalten ist. Die Investitionsschutzabkommen enthalten ein Angebot des Vertragsstaates, sich auf ein Schiedsverfahren einzulassen, das von einem Investor – der selbst nicht Partei des Schutzabkommens ist – im Streitfall durch die Einreichung einer Schiedsklage stillschweigend angenommen wird.[64]

7 Erfahrungen aus der Transaktionsberatung

Im Vorfeld einer Akquisition oder eines Joint Ventures sollte in jedem Land regelmäßig eine ausführliche **Due Diligence** des Zielunternehmens bzw. des lokalen Partners durchgeführt werden. In *Common Law*-Ländern wie Indien oder Malaysia ist dies insbesondere schon deshalb erforderlich, weil dort das sog. *Caveat Emptor*-Prinzip gilt, nach welchem es im Verantwortungsbereich des Käufers liegt, den Kaufgegenstand vor dem Erwerb zu untersuchen. Die Due Diligence sollte dabei möglichst multidisziplinär ausgestaltet sein, also rechtliche, steuerliche, finanzielle und andere Aspekte abdecken. Die Schwerpunkte der rechtlichen Due Diligence liegen typischerweise in Bereichen wie *Corporate Compliance*, Grundbesitz, *Change-of-Control*- Klauseln, Rechtsstreitigkeiten und Verbindlichkeiten allgemein, Beziehungen mit verbundenen Unternehmen sowie im Bereich des Arbeitsrechts.

In vielen Schwellenländern stellt bereits die Due Diligence eines Zielunternehmens große Herausforderungen an den ausländischen Investor, wobei ein pragmatisches Vorgehen angezeigt ist. Viele wichtige Informationen sind bei privaten Unternehmen oft überhaupt nicht oder bestenfalls oberflächlich und unvollständig dokumentiert und nur

[63] Hierzu ausführlich *Wegen/Raible*, SchiedsVZ 2006, S. 225 ff.

[64] *Happ*, IStR 2006 Heft 19, S. 649; *Freudenberg*, Firmen im Ausland nicht schutzlos, Handelsblatt, 14. Juni 2006.

schwer zu erhalten. Bilanzen und juristische Dokumente entsprechen nicht immer internationalen Standards. Gespräche mit dem Management des Zielunternehmens, mit Firmenangehörigen und den lokalen Behörden sind deshalb häufig die wichtigste Quelle, um Informationen zu erlangen. Zugleich sollten sich Investoren aber nicht unkritisch auf die Äußerungen der lokalen Seite bei einer Transaktion verlassen, auch wenn ein staatliches Unternehmen beteiligt ist. Auch aus diesen Gründen dauern Due Diligence Untersuchungen in Asien meist deutlich länger als bei Targets im Westen. Das unübersichtliche Dickicht an Regularien erlaubt beispielsweise indischen Unternehmen eine Vielzahl an rechtlichen und steuerlichen Gestaltungsmöglichkeiten, die nur vor dem Hintergrund auch informeller Praktiken in Indien zu verstehen sind. M&A-Transaktionen müssen in vielen asiatischen Ländern grundsätzlich von einer oder mehreren zuständigen Behörden genehmigt werden. Die staatlichen Stellen haben so erheblichen Einfluss auf das Zustandekommen und auch den Inhalt eines M&A-Deals.

Die für eine M&A-Transaktion zu beachtenden Vorgaben divergieren in Asien sehr stark. In **China** gibt es eine Reihe spezifischer M&A-Regelungen für bestimmte Erwerbskonstellationen.[65] Die einschlägigen Regelungen sind jedoch nicht sehr übersichtlich und zudem stetem Wandel unterworfen. Nicht immer eindeutig ist, welche Rechtsvorschriften auf die Zielgesellschaft anwendbar sind, nachdem der ausländische Investor eingestiegen ist. Je nach Zielunternehmen und Beteiligungsart gibt es verschiedene Möglichkeiten, ein Unternehmen in China zu erwerben.[66] Ausländische Investoren sollten sich außerdem darüber im Klaren sein, dass eine Vielzahl von Zustimmungen und Genehmigungen erforderlich werden können, etwa solche von Aktionären, den Behörden und in einigen Fällen sogar von den Kreditgebern. In China bestehen üblicherweise bis zu einem gewissen Grad Unsicherheiten über das Vermögen und die Verbindlichkeiten der zur Übernahme ins Auge gefassten Gesellschaft. Ein ausländischer Investor sollte daher auch in Gespräche mit den Gläubigern des Zielunternehmens eintreten und diese in den Verhandlungsprozess einbeziehen, um sicher zu gehen, dass er einen richtigen Eindruck von der Vermögenssituation des Unternehmens erhält.

In einigen asiatischen Ländern muss der Kaufpreis grundsätzlich innerhalb eines bestimmten Zeitraumes nach dem Erwerb gezahlt werden, so dass die im internationalen Transaktionsgeschäft üblichen sog. *Earn-Out*-Regelungen, nach denen ein Teil des Kaufpreises von den Ergebnissen der Zielgesellschaft abhängig und auch erst nach Ablauf der jeweiligen Geschäftsjahre zur Zahlung fällig ist, nicht vereinbart werden können. Solche *Earn-Out*-Regelungen dienen dazu, den Verkäufer für einen Übergangszeitraum weiterhin an dem Unternehmen zu beteiligen, damit dieser die reibungslose Integration und Fortsetzung des Unternehmens unterstützt. Alternativen zu einer *Earn-Out*-Klausel sind die Verpflichtung des Verkäufers zu entgeltlichen Unterstützungsleistungen oder eine

---

[65] *Fischer*, Neue Verordnung für Übernahmen, ASIA BRIDGE, 10/2006, S. 35; *Ben QI*, China's New M&A Rules: A Revisionist's View, asialaw M&A Review, S. 23.

[66] *Tang/Ghaffar*, M&A-Transaktionsstrukturen in China – aktuelle Entwicklungen, Perspektiven, in: Lucks (Hrsg.), M&A in China 2006, S. 154.

Kaufpreisstundung, solange die im Anteilskaufvertrag festgelegten Gewährleistungsfristen laufen. Hierbei ist jedoch zu beachten, dass solche Darlehen beispielsweise in China zwingend über eine Bank abgewickelt werden müssen, da direkte Darlehen zwischen Gesellschaften unzulässig sind.

Weiterhin besteht regelmäßig ein Interesse des Erwerbers, das Management des Zielunternehmens zumindest für die Anfangszeit beibehalten zu können. Hierzu dienen *Lock in*-Klauseln. Ob diese jedoch auch im jeweiligen asiatischen Land durchgesetzt werden können, ist anhand des lokalen Arbeitsrechts, das beispielsweise in China auch auf Geschäftsführer Anwendung findet, genau zu prüfen. Möglicherweise steht der Wirksamkeit solcher Klauseln das örtliche Kündigungsrecht im Weg.

Eine wichtige Rolle spielen neben den materiellen Vermögenswerten und dem Management auch die Mitarbeiter der Zielgesellschaft, die den Wert eines Unternehmens aufgrund ihrer Expertise und ihres Know-hows erheblich mitbeeinflussen. Unerlässlich ist hier eine reibungslose Kommunikation und Information bereits während der Transaktion, um eventuell bestehende Unsicherheiten oder Missverständnisse auf Seiten der Arbeitnehmer zu beseitigen sowie die Schaffung von Anreizen, um wichtige Mitarbeiter nach der Transaktion zu halten. In vielen asiatischen Ländern sind die Interessen der Mitarbeiter gesetzlich zu beachten. Soweit z. B. in **China** die Arbeitnehmer der beteiligten Unternehmen gewerkschaftlich organisiert sind, sollten vor der Entscheidung über eine Fusion ihre Vertreter gehört und ihre Ansichten berücksichtigt werden. Kommt es in Folge der Übernahme zu Entlassungen, sind sowohl staatliche als auch lokale Vorschriften zu beachten. Regelmäßig werden an die zu entlassenden Arbeitnehmer Abfindungen zu zahlen sein. Bei der Übernahme eines chinesischen Unternehmens ist ein Sozialplan für die Arbeitnehmer aufzustellen und durch die Gewerkschaft genehmigen zu lassen. Bei der Fusion mehrerer ausländisch investierter Unternehmen besteht in China die Pflicht, sich um die Übernahme der gesamten Belegschaft oder eine sozialverträgliche Lösung zu bemühen. Auch bei Unternehmensübernahmen wird von den chinesischen Behörden oftmals auf ein solches Ergebnis hingewirkt.

8 Fazit

Wie die vorausgegangene Darstellung zeigt, spielen lokale rechtliche Besonderheiten bei der erfolgreichen Gestaltung von Projekten im Ausland, insbesondere in den Schwellenländern Asiens, eine große Rolle. So sollten im Vorfeld Investitionsbeschränkungen bzw. -verbote des Ziellandes untersucht werden, um Verluste, wie sie auch mancher deutsche Konzern bereits erlitten hat, zu vermeiden. Die Nichtberücksichtigung von ländereigenen Vorgaben oder Gepflogenheiten kann zum Scheitern des Projekts führen und sollte daher frühzeitig umfassend geprüft werden, um die Strukturen zu optimieren und damit den Erfolg zu sichern.

Sowohl in Deutschland als auch in vielen asiatischen Ländern steht Korruption unter strenger Strafe. Insgesamt hat die Korruptionsbekämpfung auch durch den Erlass des *UK Bribery Act* eine globale Dimension erreicht, die international agierende Unternehmen zum Handeln zwingt. Interne Richtlinien zur Korruptionsbekämpfung müssen überprüft und angepasst werden, um den gestiegenen internationalen Anforderungen zu genügen und nicht unwissentlich in Haftungsfallen zu laufen.

Rechtliche Aspekte von IT-Compliance

Michael Rath

Inhaltsverzeichnis

Zusammenfassung

Sowohl Corporate Governance (die verantwortungsvolle Steuerung des Unternehmens) als auch Corporate Compliance (die Umsetzung der hierzu notwendigen Kontrollmaßnahmen) sind heutzutage angesichts der stetig zunehmenden Komplexität von Geschäftsprozessen in einem Unternehmen ohne den Einsatz von Informationstechnologie (IT) nicht mehr vorstellbar. Corporate Governance und Compliance sind daher

M. Rath (✉)
Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: michael.rath@luther-lawfirm.com

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2_7, © Springer Fachmedien Wiesbaden 2013

untrennbar auch mit IT-Compliance verbunden, also dem verantwortungsvollen Umgang mit allen Aspekten der IT. IT-Compliance reicht dabei von der Einhaltung von Datenschutz und Datensicherheit (Vgl. dazu Kap. 8: *Bauer*, Datenschutzrechtliche Compliance im Unternehmen) über die Sicherstellung von IT-Security bis hin zur revisionssicheren elektronischen Archivierung. Dieser Beitrag soll einen ersten Überblick über die große Bandbreite der Anforderungen an IT-Compliance bieten.

1 Einleitung

Corporate Governance und Compliance sind wegen der stetig zunehmenden Komplexität von Geschäftsprozessen in einem Unternehmen untrennbar mit IT-Compliance verknüpft. Dabei sind die Sicherstellung von IT-Compliance und der Gedanke der Beherrschung von IT-spezifischen Risiken durch eine entsprechende Risikoidentifikation, Risikoanalyse, Risikobewertung und Risikosteuerung der im Unternehmen vorhandenen IT und der hieraus resultierenden Risiken nicht neu.[1] Vielmehr gehört es angesichts der stetig wachsenden Bedeutung der IT für ein Unternehmen schon seit geraumer Zeit zu der verantwortungsvollen Steuerung eines Unternehmens, auch im Hinblick auf die vorhandene (oder etwa neu anzuschaffende) Informationstechnologie die geltenden „Spielregeln" einzuhalten. Dies spiegelt sich auch in den entsprechenden Prüfungsstandards des IDW und den übrigen, nachfolgend kurz skizzierten Branchenstandards und Anforderungen wieder.

2 IT-Compliance als Aufgabe des Managements

IT-Compliance ist entgegen oftmals anzutreffender Praxis keine Aufgabe, die allein von der IT-Abteilung oder der Rechtsabteilung bewältigt werden kann. Zur Vermeidung einer (persönlichen) Haftung des Vorstandes oder des Geschäftsführers nach §§ 93 Abs. 2, 116 Abs. 1 AktG (analog), 43 GmbHG ist vielmehr gerade das Management aufgerufen, sich um die Einhaltung von IT-Compliance in den unterschiedlichen Fachbereichen zu bemühen. Gerade diese fachbereichsübergreifende Zusammenarbeit ist jedoch eine wesentliche Schwierigkeit bei der Erreichung von IT-Compliance.[2]

Die Verpflichtung der Geschäftsleitung zur Sicherstellung von IT-Compliance besteht auch ohne explizite Nennung im Gesetz. Denn nach § 93 Abs. 1 AktG haben die Vorstandsmitglieder bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften

[1] Siehe zu IT-Risiko und Chancenmanagement im Unternehmen den gleichnamigen Leitfaden der Bitkom, abrufbar unter http://www.bitkom.org/de/publikationen/38337_39864.aspx.

[2] Vgl. hierzu ausführlich *Rath/Sponholz*,: IT-Compliance, 2009, Kap. 1.6.

Geschäftsleiters anzuwenden.[3] Angesichts der Bedeutung von IT für das Funktionieren und den Fortbestand des Unternehmens gehört es damit auch zu den Pflichten eines gewissenhaften Geschäftsführers, das Unternehmen vor erkennbaren Gefahren zu schützen. Verletzt ein Vorstand diese Pflicht, haftet er dem Unternehmen nach § 93 Abs. 2 AktG. Danach kommt es sogar zu einer Beweislastumkehr zu Lasten des Vorstandes einer Aktiengesellschaft, denn den Geschäftsleiter trifft die Beweislast hinsichtlich der Anwendung der gebotenen Sorgfalt. Das Management muss also nachweisen können, dass auch im Zusammenhang mit der IT die erforderliche Sorgfalt Anwendung gefunden hat. Diese im Aktienrecht für Vorstände festgelegten Pflichten gelten kraft entsprechender Regelungen (etwa §§ 43 GmbHG, 347 HGB) auch für den Geschäftsführer einer GmbH oder die Geschäftsleitung von OHGs und KGs. Der Bedeutung der IT für das Unternehmen entspricht es, dass gemäß §§ 289, 317 HGB auch im Lagebericht der Gesellschaft Angaben zu den vorhandenen Risikofrüherkennungs- und IT-Systemen zu machen sind.

Obwohl mithin der primäre Adressatenkreis von Compliance die Unternehmensleitung ist, werden Vorstand, Aufsichtsrat und Geschäftsführer oft versuchen, die Aufgaben betreffend die Einhaltung von IT-Compliance (zumindest teilweise) zu delegieren. Leitende Mitarbeiter des Unternehmens haften jedoch auch dann, wenn IT-Compliance kraft Weisung oder arbeitsvertraglicher Regelung zum Bestandteil des Pflichtenkataloges des IT-Administrators, Datenschutzbeauftragten oder des CIO (IT-Leiter) gemacht werden.

3 Anforderungen von IT-Compliance

Die Schwierigkeit, die große Bandbreite der IT-Compliance-Anforderungen überschaubar darzustellen, liegt schon allein darin begründet, dass die einschlägigen Vorgaben in einer Vielzahl von Gesetzen, Richtlinien und gegebenenfalls sektorspezifischen Regelungen enthalten sind. Weltweit soll es schätzungsweise über 25.000 Compliance-Anforderungen (im weiteren Sinne) geben.[4] Auch wegen der oftmals völlig unterschiedlichen Zielrichtungen einschlägiger Normen ist es schwierig, die wirklich wesentlichen Eckpunkte von IT-Compliance zu benennen. Demgemäß sollen nachfolgend nur einzelne bedeutsame Aspekte von IT-Compliance hervorgehoben werden; die vorliegende Darstellung erhebt auch deshalb keinerlei Anspruch auf Vollständigkeit.[5] Die Einhaltung von IT-Compliance

[3] Vgl. allgemein zur Compliance als Aufgabe der Geschäftsleitung auch Kap. 1: *Vetter,* Compliance in der Unternehmerpraxis, Ziff. 2. und 3. und Kap. 2: *Wecker/Galla,* Pflichten der Geschäftsleitung & Aufbau einer Compliance Organisation, Ziff. 2.

[4] Vgl. bzgl. der Anforderungen von Solvency II etwa *Pfeifer*, VW 2005, 1558 ff.; bzgl. der Eigenkapitalvereinbarung Basel II siehe etwa *Duisberg/Ohrtmann*, ITRB 2005, 160 ff.

[5] IT-Compliance kann vielmehr beispielsweise auch im Arbeitsrecht Bedeutung erlangen, so etwa hinsichtlich der Mitspracherechte des Betriebsrates (§ 80 BetrVG) bei der Einführung von bestimmten IT-Systemen (insbesondere von Programmen mit Überwachungsfunktionen) sowie bei so scheinbar trivialen Aspekten wie der Einhaltung der Bildschirmarbeitsplatzverordnung.

wird zudem dadurch erschwert, dass aus ganz anderen Fachrichtungen, etwa dem Steuerrecht und der Wirtschaftsprüfung, weitere Anforderungen an die IT gestellt werden. Zudem gibt es neben den eher generischen gesetzlichen Regelungen in der Abgabenordnung (AO) und den Prüfungskatalogen der Wirtschaftsprüfer auch konkrete behördliche Vorgaben, etwa der Finanzverwaltung und der BaFin.

3.1 IT-gestütztes Informations- und Kontrollsystem (IKS)

Ein wesentlicher Aspekt von IT-Compliance ist zunächst die Einhaltung von gesetzlichen Anforderungen und Informations- sowie Dokumentationspflichten *mit Hilfe der IT*. Es ist mitnichten nur aus betriebswirtschaftlicher und unternehmerischer Sicht wünschenswert, dass die im Unternehmen vorhandenen IT-Systeme in der Lage sind, über die Identifikation bestandsgefährdender Entwicklungen hinaus sämtliche Geschäftsvorfälle dauerhaft zu erfassen. Vielmehr dient ein solches System auch der Zusammenführung aller für unternehmerische Entscheidungen wichtigen Informationen. Aus diesem Grund wird auch vom Gesetzgeber eine effektive Kontrolle über die Prozesse im Unternehmen und die Einhaltung einer so verstandenen IT-Governance gefordert.[6]

Die gesetzliche Verpflichtung zur Einführung eines solchen internen Kontrollsystems (IKS)[7] wurde bekanntlich bereits durch das am 1. Mai 1998 in Kraft getretene KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) eingeführt. § 91 Abs. 2 AktG bestimmt, dass der Vorstand geeignete Maßnahmen zu treffen und insbesondere ein Überwachungssystem einzurichten hat, damit etwaige den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden können. Ein zentraler Bestandteil ist dabei auch die Beurteilung der Angemessenheit und Wirksamkeit der IT-spezifischen Kontrollen als Teil des internen Kontrollsystems. Das interne Kontrollsystem dient so vor allem der Kontrolle von Fehlerrisiken.[8]

Daneben ist ein solches IKS aber auch deshalb erforderlich, um eine ausreichende Basis zur Unternehmenslenkung und zur Erfüllung von den einschlägigen gesetzlichen Berichts- und Dokumentationspflichten zu geben. Diese idealerweise in einem strukturierten „Business Information Warehouse" gesammelten Informationen bilden dann die Grundlage der sog. „Business Intelligence (BI)". Dieser Bestandteil von IT-Compliance wird daher teilweise auch als „Information Security Governance (ISG)" oder „Management Risk Controlling (MRC)" bezeichnet.

---

[6] Zu den künftigen Anforderungen von EURO-SOX siehe nachfolgend unter Ziff. 3.2.

[7] Zur Definition eines IKS siehe *Lösle/Maudrich*, DSWR 2006, 5 mit Hinweis auf IDW PS 260, Tz. 5.

[8] Fehlerrisiken setzen sich (übrigens nicht nur in der IT) zusammen aus „inhärenten Risiken" und den „Kontrollrisiken": Inhärente Risiken bezeichnen allgemein die Wahrscheinlichkeit für das Auftreten wesentlicher Fehler (etwa in der Rechnungslegung). Die Wahrscheinlichkeit dafür, dass wesentliche Fehler nicht rechtzeitig durch dieses interne Kontrollsystem aufgedeckt oder verhindert werden, wird allgemein als Kontrollrisiko bezeichnet. Vgl. dazu ausführlich *Rath/Sponholz*, IT-Compliance, 2009, Kap. 3.

3.2 SOX & Co.

Ähnliche Anforderungen an die Etablierung und Aufrechterhaltung von Kontroll- und Informationssystemen (und damit mittelbar auch an die IT) enthält auch der im Zusammenhang mit dem Thema Compliance stets zitierte Sarbanes Oxley Act (kurz: SOX oder SOA).[9] Auch andere amerikanische Vorgaben wie bspw. HIPAA, Tread Act oder DoD 5015.2, aber auch die Anforderungen von e-Discovery[10] können selbst für deutsche Firmen von Bedeutung sein, insbesondere wenn sie Niederlassungen in den USA haben. Hier hilft es wenig, dass die Vorgaben des Sarbanes Oxley Act per se nur für US-amerikanische börsennotierte Unternehmen und deren ausländischen Töchtern gelten. Denn in der Praxis ist die Tendenz feststellbar, dass auch in Verträgen mit deutschen Unternehmen, die gar nicht unmittelbar von SOX erfasst sind, die Einhaltung sämtlicher SOX-Vorgaben gefordert wird.

Section 404 SOX enthält – ähnlich wie das deutsche Recht – ebenfalls ausdrückliche Bestimmungen über Maßnahmen bezüglich der Errichtung eines internen Kontrollsystems (Management Assessment of Internal Controls). Section 404 fordert dabei u. a., dass ein effektives internes Kontrollsystem (IKS) zur Sicherstellung einer funktionsfähigen Berichterstattung eingerichtet wird. Ähnlich wie der Lagebericht deutscher Kapitalgesellschaften muss daher auch der Jahresbericht einer SEC-notierten Gesellschaft einen Bericht des Managements („Internal Control Report") über das dort vorhandene Kontrollsystem enthalten. Darin muss das Management u. a. Erklärungen hinsichtlich der Effizienz der eingerichteten Kontrollmaßnahmen abgeben, die dann auch gemäß Section 302 vom Vorstand im Rahmen der „Certification" zu bestätigen sind.[11]

Mit der 8. EU-Richtlinie (sog. EURO-SOX oder Prüferrichtlinie) haben zudem die internationalen Prüfungsstandards (ISA) europaweit verpflichtende Wirkung erhalten. Hierdurch werden u. a. auch strengere Anforderungen an die gesetzliche Abschlussprüfung bei Unternehmen öffentlichen Interesses (aus heutiger Sicht börsennotierte Unternehmen, Banken und Versicherungen, Energieversorger) gestellt. Neben neuen Regelungen für die Abschlussprüfer wird beispielsweise auch die Einführung eines Prüfungsausschusses verpflichtend, das gleichsam wie das „Audit Committee" im SOX die Aufgabe hat, die Abschlussprüfung sowie interne Kontrollsysteme und Risikomanagementsysteme zu überwachen. Dies kann daher auch die IT-Systeme des Unternehmens betreffen.

---

[9] Vgl. hierzu auch die Studie „Der Sarbanes-Oxley Act als Instrument der Corporate Governance" (Juli 2006) der Detecon International GmbH, abrufbar unter www.detecon.com/de/publikationen/studien.

[10] Siehe hierzu Deutlmoser/Filip, ZD-Beilage 6/2012; *Geercken/Holden/Rath/Surguy/Stretton*, CRi 2013, S. 44 ff., *Rath/Klug*, K&R 2008, 596 ff.

[11] Zur Konkretisierung dieser Vorgaben hat das Committee of Sponsoring Organisations of the Treadway Commission (COSO) ein Rahmenkonzept entwickelt, dessen Anwendung von der SEC empfohlen wird. Das Kontrollmodell CobiT (Control Objectives for Information and Related Technology) lehnt sich eng an dieses COSO-Modell an (vgl. dazu noch nachfolgend im Rahmen der IT-Standards).

Die Unternehmensleitung muss daher stets ausreichend über die tatsächlich im Unternehmen ablaufenden Prozesse informiert sein und diese kontrollieren. In einem großen Unternehmen kann aufgrund der Komplexität der dort in der Regel vorhandenen Prozesse ohnehin nur durch softwaregestützte Informationsmanagement-Prozesse und IT-gestützte Reportings sichergestellt werden, dass die unternehmerischen Entscheidungen auf der Grundlage angemessener Informationen getroffen werden. Es ist mithin im Rahmen des zuvor beschriebenen allgemeinen Risikomanagement auch notwendig, EDV-gestützte Maßnahmen zur Begleitung der Prozesse und zur Risikofrüherkennung zu etablieren und mit Hilfe der EDV auf ihre Brauchbarkeit hin zu kontrollieren.[12] Bei der Etablierung eines solchen „Governance, Risk and Compliance-Framework" helfen Enterprise-Content-Management (ECM)-Lösungen. Solche ECM-Programme werden inzwischen – gerade auch mit Blick auf eine gesetzeskonforme Archivierung – zahlreich angeboten und helfen dem Unternehmen, den Überblick über die vorhandenen Informationen zu behalten.

3.3 Audit der IT-Systeme

Angesichts der zuvor nur skizzierten Bedeutung von IT-Systemen für das Unternehmen versteht es sich fast von selbst, dass auch der Abschlussprüfer im Rahmen von (freiwilligen oder gesetzlich vorgeschriebenen) Jahresabschlussprüfungen gemäß § 317 Abs. 4 HGB die im Unternehmen vorhandenen Überwachungssysteme, also auch die dort etablierten Risikomanagement-Prozesse und zugehörigen Risikofrüherkennungs- und IT-Systeme zu beurteilen hat. So sind beispielsweise nach IDW PS 330 bei der Prüfung des IT-Systems Aufbau, Angemessenheit und Funktion des Risikomanagements zu beurteilen. Bei dieser Beurteilung hilft dem Prüfer u. a. die über 100 Fragen umfassende Checkliste zur Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PH 9.330.1).[13]

Die steigende Bedeutung der IT für Unternehmen verändert demgemäß (nicht nur aufgrund von EURO-SOX) auch die Arbeit des Abschlussprüfers. Die Beurteilung der Ordnungsmäßigkeit der Rechnungslegung erfolgt heutzutage im zunehmenden Maße neben der beleghaften Prüfungsmethode auch indirekt über die Ordnungsmäßigkeit der IT-gestützten Buchführungsprozesse und die Wirksamkeit der IT-bezogenen Kontrollen. Demgemäß berücksichtigt auch der Prüfungsstandard (PS) 260 des Institutes der Wirtschaftsprüfer (IDW) die Bedeutung der IT-Landschaft als wesentliche Komponente des IKS.

Die Frage, wann die Abschlussprüfung zwingend eine IT-Prüfung zu umfassen hat, richtet sich insbesondere nach der Wesentlichkeit des IT-Systems für die Rechnungslegung bzw. für die Beurteilung der Ordnungsmäßigkeit der Rechnungslegung, der Komplexität des eingesetzten IT-Systems sowie dem Grad der Integration der EDV-Lösung. Die

[12] Zum Risikomanagement siehe *Bier*, K&R 2005, 59 ff.; *Rath/Sponholz*, IT-Compliance, 2009, Kap. 6.

[13] Vgl. *Skopp/Greipl*, DSWR 2006, 2–4.

IT-Prüfung ist mittlerweile insbesondere bei mittelgroßen bis großen Unternehmen integraler Bestandteil einer Vielzahl von Jahresabschlussprüfungen und leistet für diese einen signifikanten Beitrag zur Erhöhung der Prüfungssicherheit.

Praxishinweis

Diverse IDW-Stellungnahmen konkretisieren die Anforderungen an die Rechnungslegung aus Sicht der Wirtschaftsprüfer, so insbesondere die IDW RS FAIT 1 (Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie) und die IDW RS FAIT 3 (Grundsätze ordnungsmäßiger Buchführung bei Einsatz elektronischer Archivierungsverfahren). Auch bezüglich der Auslagerung von E-Commerce-Systemen gibt es eine solche IDW Stellungnahme zur Rechnungslegung (Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce, IDW RS FAIT 2). IDW RS FAIT 4 (Anforderungen an die Ordnungsgemäßheit und Sicherheit IT-gestützter Konsolidierungsprozesse) konkretisiert nun die gesetzlichen Anforderungen der §§ 290–315 HGB und veranschaulicht die in IDW RS FAIT 1 dargelegten Ordnungsmäßigkeits- und Sicherheitsanforderungen der Abschlusserstellung im Konzern.

3.4 IT-Security

Die Unternehmensleitung ist daneben auch zur Etablierung effektiver IT-Sicherheitsmaßnahmen (sog. IT-Sicherheit oder IT-Security) und deren Kontrolle verpflichtet.[14] Diese Verpflichtung ergibt sich neben § 91 Abs. 2 AktG vor allem aus den allgemeinen Sorgfaltspflichten des Vorstandes, die in § 93 Abs. 1 AktG niedergelegt sind. Demgemäß ist die Unternehmensleitung auch zu einem angemessenen Risikomanagement hinsichtlich der vorhandenen IT-Systeme verpflichtet.

Die Verpflichtung zur Etablierung und Aufrechterhaltung von „IT-Sicherheit" als ein weiterer Bestandteil von IT-Compliance bedeutet, dass die IT-Systeme (und die darin enthaltenen ggf. sogar vertraulichen Informationen) gegen Angriffe von innen und außen geschützt werden müssen. Ergänzend kann man im Zusammenhang mit dem Begriff IT-Sicherheit auf eine Definition zurückgreifen, die im Zusammenhang mit der Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aufgestellt wurde: So heißt es in § 2 Abs. 2 BSIG, dass Sicherheit in der Informationstechnik die Einhaltung bestimmter Sicherheitsstandards bedeutet, welche die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen. Hierzu gehören Sicherheitsvorkehrungen in oder bei der Anwendung von informationstechnischen Systemen oder Komponenten. Eine Festlegung oder Vorauswahl bestimmter IT-Standards ist damit allerdings nicht verbunden. Es ist jedoch zu empfehlen, sich an den Best Practices anderer Unternehmen zu orientieren (vgl. dazu noch am Ende dieses Kapitels).

[14] Siehe zu den rechtlichen Verpflichtungen zur Gewährleistung von IT-Security und zur Einführung einer Notfallplanung im IT-Bereich *Steger*, CR 2007, 137 ff.; *Heckmann*, MMR 2006, 280 ff.; *Roth/Schneider*, ITRB 2005, 19 ff.

Zu den wichtigsten Eckpfeilern der IT-Sicherheit gehört es jedenfalls, im Unternehmen entsprechende Prozesse zum „IT-Sicherheitsmanagement“ zu etablieren und kontinuierlich zu betreiben sowie eine funktionierende Sicherheitsorganisation zu schaffen.[15] Zu den Aufgaben für den CIO bzw. den IT-Sicherheitsverantwortliche gehört es dabei auch, den Überblick über die abzusichernden Geschäftsprozesse zu bewahren und angemessene Sicherheitsmaßnahmen umzusetzen. So bieten beispielsweise die ISO 27001 und der „IT-Grundschutz“ des BSI bewährte Methoden und Vorgehensweisen, die dem Stand der Technik entsprechende IT-Sicherheitsmaßnahmen zu identifizieren und in der Praxis umzusetzen. Mit diesen Standards wird für die Sicherstellung von IT-Security eine Sammlung von IT-Sicherheitsmaßnahmen als auch eine entsprechende Methodik zur Auswahl und Anpassung geeigneter Maßnahmen zur Verfügung gestellt.

Allerdings kann es nicht zuletzt auch aus Kosten- und Ressourcengründen empfehlenswert sein, bei dem Versuch der Einhaltung von IT-Security eine „abgespeckte“ Version zu etablieren. So wird etwa in der Sparkassen-Finanzgruppe seit Jahren als Standard zur Informationssicherheit das Produkt „Sicherer IT-Betrieb“ nahezu flächendeckend bei mehr als 400 Unternehmen verwendet. Das Vorgehensmodell „Sicherer IT-Betrieb“ wurde vom SIZ[16] ursprünglich für den Einsatz bei Banken und Versicherungen in der Sparkassen-Finanzgruppe entwickelt, wurde aber inzwischen für den Einsatz außerhalb der Sparkassen-Finanzgruppe angepasst und wird mittlerweile nicht nur im Banken- und Versicherungssektor sondern auch in anderen Branchen erfolgreich eingesetzt. Der „Sichere IT-Betrieb“ stellt so einen risikoorientierten, ISO 27001/27002-konformen Ansatz, zur Verfügung. Dabei sind u. a. auch die relevanten IT-Compliance-Anforderungen der deutschen Gesetzgebung, der Wirtschaftsprüfer und aus CobiT berücksichtigt.[17]

Um belegen zu können, dass ein funktionsfähiges Informationssicherheits-Managementsystem etabliert und angemessene Sicherheitsmaßnahmen umgesetzt wurden, kann es sinnvoll sein, zusätzlich eine formale Zertifizierung anzustreben. Die erste internationale Norm für eine solche Zertifizierung des IT-Sicherheits-Managements ist ISO 27001. Das BSI hat für Behörden die Zertifizierung dieser abstrakten Vorgaben um die konkreten IT-Grundschutz-Empfehlungen erweitert. Eine derartige ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz umfasst sowohl eine Prüfung des IT-Sicherheitsmanagements als auch der konkreten IT-Sicherheitsmaßnahmen auf Basis von IT-Grundschutz.

Praxishinweis

Erste Maßnahmen im Bereich IT-Security beginnen mit so scheinbar trivialen Aspekten wie der Festlegung von Verantwortlichkeiten und Befugnissen der IT-User. Aber nur durch ein sorgfältig ausgearbeitetes Konzept für die Vergabe von Lese- und Editierrechten lässt sich erreichen, dass die jeweiligen betriebswesentlichen Informationen tatsächlich nur von den hierzu berechtigten Mitarbeitern gelesen und (über eine Ver-

[15] Siehe zu den wesentlichen Maßnahmen *Rath/Sponholz*, IT-Compliance, 2009, Kap. 10.

[16] SIZ ist das Informatikzentrum der Sparkassenorganisation GmbH (www.siz.de).

[17] Vgl. dazu *Rieger*, in: Rath/Sponholz (Hrsg.), IT-Compliance, 2009, Kap. 10.5.

sionskontrolle der in der Datenbank vorhandenen Dokumente) bearbeitet werden können. Zudem kann durch die Steuerung der Zugriffsberechtigungen die auch aus dem Blickwinkel des zuvor erörterten Risikomanagements erforderliche Funktionstrennung (sog. „Segregation of Duties, SOD") gewährleistet werden. Diese SOD sollte allerdings system- und plattformübergreifend ausgestaltet sein, weil sonst die eingerichteten Sicherheitsprozesse zu leicht umgangen werden können. Neben internen Sicherheitsrichtlinien ist ein weiterer unerlässlicher Bestandteil von IT-Security der Schutz der Systeme gegen Angriff von außen, insbesondere durch den Einsatz von systemadäquaten und aktuellen Firewalls, Virenschutz- und Anti-Spam-Software.

3.5 Elektronische Archivierung

IT-Compliance wird auch bei der elektronischen Archivierung von Dokumenten relevant. Kaufleute müssen bekanntlich nach Handelsrecht (§ 257 HGB), aber auch aus steuerrechtlichen Gründen (§ 147 AO) die von ihnen empfangenen und abgesendeten Handels- und Geschäftsbriefe aufbewahren.[18] Die Aufbewahrungsfrist für Handelsbriefe beträgt – von einer Reihe von Spezialnormen einmal abgesehen – nach § 257 Abs. 4 HGB (ebenso wie nach § 147 Abs. 3, 4 AO) grundsätzlich sechs, für Buchungsbelege, Jahresabschlüsse, etc. bis zu zehn Jahre. Da der Rechtsverkehr im Unternehmen heutzutage größtenteils elektronisch erfolgt, sind neben den vorgenannten Dokumenten selbstverständlich auch geschäftliche E-Mails, also elektronische Korrespondenz im Zusammenhang mit der Vorbereitung, dem Abschluss und der Durchführung des „Handelsgeschäftes" i. S. v. § 343 HGB, zu archivieren. Nach §§ 239 Abs. 4, 257 Abs. 3 HGB können solche (elektronischen) „Geschäftsbriefe" auch auf Datenträgern aufbewahrt werden, wenn dies den Grundsätzen ordnungsgemäßer Buchführung (GoB) und den Grundsätzen ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS) entspricht[19]. Hinzu kommt, dass im gesamten Aufbewahrungszeitraum die Unveränderbarkeit des Datenbestandes gewährleisten muss (§ 146 Abs. 4 AO). Auch im Falle eines Releasewechsels, eines Austauschs der Produktiv- oder E-Mail-Systeme oder gar eines vollständigen Wechsel des IT-Providers müssen daher die (unveränderten) Altdaten revisionssicher in das neue IT-System übertragen oder aber während der Aufbewahrungspflicht in zwei Systemen parallel verfügbar gehalten werden. Neben Authentizität und Integrität der Dokumente muss im Langzeitarchiv auch noch die Lesbarkeit garantiert werden. Dies führt in der Praxis oft zu einer kostenträchtigen redundanten Datenhaltung.[20] Problematisch ist hier zudem, dass die Rückwärtskompatibilität von Softwareprogrammen und Formaten zeitlich begrenzt ist. Um Dritten eine

[18] Siehe zur Aufbewahrungspflicht von E-Mails *Böhme*, K&R 2006, 176 ff.

[19] Schon länger ist angekündigt, dass die GoBS durch die neuen Vorgaben der „Grundsätze ordnungsgemäßer Buchführung beim IT-Einsatz" (GoBIT) abgelöst werden. Die aktuelle Fassung der GoBIT lag bei Drucklegung noch nicht vor.

[20] Siehe zu den Anforderungen an sog. „auswertbare Archive" auch Projekte wie Archisig und das Nachfolgeprojekt Transidoc [www.transidoc.de].

Prüfung der häufig unmittelbar aus den ERP-Systemen (Enterprise Ressource Planning) und Buchhaltungssystemen generierten Informationen zu ermöglichen, sollte die Archivierung idealerweise von Anfang an so erfolgen, dass die Dokumente periodengerecht den jeweiligen (Handels-) Geschäften zugeordnet werden können. Hierzu wird es in aller Regel notwendig sein, dass auch die Anlagen zu einer E-Mail aufbewahrt werden, da der in einer E-Mail verkörperte Handelsbrief ohne die zugehörigen Attachments regelmäßig nicht verständlich oder zur Dokumentation des Geschäftsvorfalles unzureichend wäre.

IT-Compliance bedeutet daher in diesem Zusammenhang, dass das Unternehmen zunächst eine interne Regelung für die Ablage und Archivierung von E-Mails vorsehen und auch praktizieren sollte.[21] Neben diesem E-Mail-Management sollte mit Blick auf die Unzulänglichkeiten der bereits angesprochenen ECM-Systeme und die Verfügbarkeit von unternehmensrelevanten Informationen eine Software vorhanden sein, mit der ggf. auch unstrukturiert vorliegende, geschäftsrelevante Informationen innerhalb einer angemessenen Zeit einem Projekt zugeordnet werden können. Dies gilt jedenfalls solange, bis E-Mails sog. Metadaten enthalten, die bspw. mit Hilfe der „Extensible Access Method (XAM)" oder einer anderen Methode eine strukturierte Auswertung der E-Mails erlauben.

3.6 Elektronische Prüfung/GDPdU

Beim Einsatz entsprechender Archivierungssysteme muss nach den vorstehenden Ausführungen u. a. sichergestellt sein, dass die Daten mit den Originalen übereinstimmen, dass diese innerhalb der Aufbewahrungsfrist verfügbar sind und in angemessener Frist lesbar und maschinell auswertbar gemacht werden können. Diese „Revisionssicherheit" und maschinelle Auswertbarkeit kann ggf. auch über eine direkte Verlinkung der Dokumente in das (produktive) Buchführungssystem erreicht werden, solange die Unveränderbarkeit gewährleistet ist. Sofern sich unter diesen E-Mails auch steuerrechtlich relevante Daten befinden, sollten allerdings diese E-Mails im Originalformat archiviert werden, auch wenn die Finanzverwaltung angesichts der unstrukturierten Daten in einer E-Mail insoweit kaum von ihrem Prüfungsrecht Gebrauch macht.[22]

Denn auch wenn integrierte ERP-Systeme heutzutage völlig neue Prozesslogiken aufweisen und die originäre Erfassung rechnungslegungsrelevanter Daten in operative Bereiche außerhalb der Buchführung verlagern, gelten auch für diese Systeme die allgemeinen Anforderungen an die Archivierung digitaler Unterlagen nach § 147 AO (insbesondere die GoBS), die vom Bundesfinanzministerium (BMF) durch die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)" aus dem Jahr 2001 konkretisiert wurden. Der Finanzverwaltung steht danach bereits seit dem 1. Januar 2002 bei Außen-

[21] Vgl. auch *Hauschka*, ZRP 2006, 258, 259.

[22] Allerdings werden E-Mails nicht in den GDPdU, sondern nur in den Q&A der Finanzverwaltung erwähnt. Für den Datenzugriff sind E-Mails wegen der fehlenden Datenstruktur zudem nur eingeschränkt geeignet.

prüfungen das Recht zu, nach Maßgabe der GDPdU auf alle digitalen steuerrelevanten Unternehmensdaten zuzugreifen. Danach sind die Unternehmen auf Anfrage des Steuerprüfers dazu verpflichtet, ihre steuerrelevanten Daten (also zumindest die Finanz-, Anlagen und Lohnbuchhaltung, wohl aber auch die ECM-Systeme) maschinell auswertbar zur Verfügung zu stellen.

Praxishinweis

Bei der Außenprüfung werden drei Arten des Datenzugriffs unterschieden: der unmittelbare Lesezugriff durch Verwendung der unternehmenseigenen Hard- und Software (Z1), der mittelbare Zugriff über Auswertungen des Unternehmens nach den Vorgaben des Prüfers (Z2) und die (ggf. nach dem Standard des BSI zusätzlich verschlüsselte) Datenüberlassung (Z3), wobei es für letztgenannten Datenzugriff durch den Betriebsprüfer ebenfalls Empfehlungen des Bundesfinanzministeriums gibt. Die Daten werden dann in der Regel in die Prüfsoftware „IDEA" oder „ACL" eingelesen. Unterstützt wird der Datenzugriff durch Makros, welche die Auswertung der beim Unternehmen vorhandenen Informationen erleichtern.[23] Ein Online-Zugriff auf die Datenbestände des Unternehmens ist der Finanzverwaltung jedoch (derzeit) nicht gestattet.

Das BMF hat die „Fragen und Antworten zum Datenzugriff der Finanzverwaltung" wiederholt aktualisiert und gibt viele Antworten (auf möglicherweise gar nicht gestellte Fragen) zu dem digitalen Datenzugriff, etwa bezüglich des Zugriffs des Prüfers auf das Intranet des Unternehmens. Trotz dieser Klärung einzelner Streitpunkte bleibt vor allem die Frage der Einordnung der im Unternehmen vorhandenen Daten als „steuerrelevant" von entscheidender Bedeutung[24]. Für eine solche steuerrechtliche Relevanz ist grundsätzlich keine steuerliche Auswirkung erforderlich; aus diesem Grund können ggf. auch freiwillig erstellte, digitale Aufzeichnungen (insbesondere für DMS-Systeme neu eingescannte Dokumente) oder gar Informationen zu Kostenstellen dem Datenzugriff der Finanzbehörden unterliegen. Aus dem Fragen- und Antwortenkatalog geht beispielsweise hervor, dass die steuerliche Außenprüfung auch den Zugriff auf ECM-Systeme umfasst. Daraus folgt, dass grundsätzlich auch eingescannte Dokumente als originär digitale Unterlagen anzusehen sind, mit der Folge, dass auch für ein ECM-System die in den GDPdU beschriebenen Zugriffsarten gelten. Hinzu kommt, dass nach Meinung der Finanzverwaltung elektronische Post im Originalformat (E-Mail-Format) archiviert werden muss. Firmen kommen damit nicht umhin, neben Langzeitformaten wie TIFF und PDF/A[25] auch das (proprietäre) Originalformat zu archivieren. Zudem ist die Frage, welche Dateiformate archivtauglich sind, noch nicht abschließend geklärt. In zahlreichen Unternehmen gilt seit Jahren das

[23] Bspw. AIS TaxAudit 2011 R 1 (Audit Information System der Fa. Audicon GmbH).

[24] Zur digitalen Archivierung steuerrelevanter Daten und Dokumente vgl. Beck-Folten, BC 2009, 157 ff.

[25] Zertifiziert nach ISO 19005-1:2005.

Format „TIFF-G4“[26] als Defacto-Standard, für farbige Vorlagen ist das Bildformat JPEG gebräuchlich.[27] Diese Formate bieten neben der (derzeitigen) Revisionssicherheit auch Möglichkeiten für die Auswertung strukturierter Inhalte, was eine Vollindizierung ermöglicht. Allerdings gibt es keine entsprechende ISO-Norm für eine gesetzeskonforme Archivierung mit diesen Formaten.

Auch in diesem Zusammenhang wird die Bedeutung des zuvor skizzierten User-Management nochmals deutlich: Dem Betriebsprüfer sollen schließlich nur diejenigen Teile der Dokumentationssammlung zur Verfügung gestellt werden, welche den Prüfungsbereich und die richtige Prüfungsperiode betreffen. Das EDV-System sollte daher (zumindest im Interesse des Unternehmens) von vornherein eine Trennung der steuerlich relevanten Daten von den übrigen archivierungspflichtigen Daten sowie eine Differenzierbarkeit nach Jahren und Steuerarten sowie Prüfungsarten ermöglichen.

3.7 Rechtskonforme IT-Systeme und Lizenzmanagement

Der Begriff IT-Compliance beschreibt daneben die Anforderungen, welche an die im Unternehmen vorhandenen IT-Systeme zu stellen sind. Dies bedeutet im Kern, dass auch die dort eingesetzten IT-Systeme wie Hardware und Software rechtskonform sein müssen. Rechtskonforme IT-Systeme sind aber beispielsweise nur solche, die ihrerseits über ausreichende „Lizenzen“ (also Nutzungsrechte) zum Betrieb der jeweiligen Software verfügen – einen gutgläubigen Erwerb von Rechten an einer Software gibt es nicht. Die Unternehmensleitung sollte daher durch ein „Software Asset Management“ (SAM) sicherstellen, dass die zum Betrieb der im Unternehmen vorhandenen Software erforderlichen Nutzungsrechte vorhanden sind[28]. Tut sie dies nicht, kann auch die Geschäftsführung unter Umständen haftbar gemacht werden:

So hat beispielsweise auch das OLG Karlsruhe in dem Urteil vom 23. April 2008 eine Haftung der Geschäftsleitung für das Vorhandensein von Softwarelizenzen bejaht.[29] In dem Unternehmen waren Computerprogramme installiert, ohne dass man sich um die dafür erforderlichen Lizenzen gekümmert hatte. Ein ehemaliger Angestellter meldete dies einem Software-Branchenverband, der die Informationen an die Kläger weitergab. Das Gericht verurteilte das Unternehmen und den Geschäftsführer, der keine Kontrollen vorgenommen oder angeordnet hatte, gesamtschuldnerisch zur Zahlung von insgesamt über 25.000,00 € zuzüglich Anwalts- und Gerichtskosten sowie Auskunft. Das Gericht stellte explizit fest, dass der Geschäftsführer als gesetzlicher Vertreter des Unternehmens Vorkehrungen gegen die Verletzung von Immaterialgüterrechten Dritter zu treffen habe.

---

[26] TIFF-G4-Dateien sind monochrome S/W-TIFFS.

[27] Weitere Formate sind der PDF/A-Standard und XPS (die Abkürzung steht für „XML Paper Specification“, entwickelt von Microsoft).

[28] Zu den Risiken eines fehlerhaften Lizenzmanagements vgl. Schrey/Krupna, CCZ 2012, 141 ff.

[29] OLG Karlsruhe v. 23.4.2008 – 6 U 180/06, CR 2009, 217 ff.

Der Geschäftsführer sei danach verpflichtet gewesen, im Rahmen des Zumutbaren und Erforderlichen Maßnahmen zu treffen, die eine Gefährdung der Urheberrechte Dritter ausschließen oder doch ernsthaft mindern. Er hätte mithin dafür Sorge tragen müssen, dass auf den Computern des Unternehmens nur lizenzierte Software genutzt wird.

Gerade aber nach einer Expansion, einer Fusion mit einem anderen Unternehmen oder einer Auslagerung von Betriebsteilen kann sich diese bei anfänglicher Lizenzierung der Software vermeintlich klare lizenzrechtliche Situation schnell anders darstellen. Denn der Erwerb einer „Unternehmenslizenz" bedeutet nicht, dass es keine weiteren Nutzungsbeschränkungen für die Software gibt. Das Gegenteil ist häufig der Fall: Oftmals gibt es (gerade auch bei den Standardprodukten) vielfältige Beschränkungen des zulässigen Nutzungsumfangs, etwa durch eine maximale Anzahl von „named user", „concurrent user" oder sonstigen Nutzungs- und Weitergabeverboten. Diese Einschränkungen gelten grundsätzlich auch beim Erwerb „gebrauchter Software"[30]. Durch die Etablierung eines Softwarelizenz-Managementsystems kann aber nicht nur eine (auch strafrechtlich relevante) Unterlizenzierung vermieden werden. Vielmehr kann oft auch eine kostenträchtige Überlizenzierung und so Kosteneinsparpotenziale identifiziert werden.[31]

4 IT-Compliance mit und durch IT-Standards

IT-Compliance insgesamt, aber vor allem aber die zuvor erörterte IT-Security, ist ohne die Einrichtung und Beachtung branchenüblicher und anerkannter IT-Standards nicht möglich.[32] Zudem füllen IT-Standards unbestimmte Rechtsbegriffe aus und legen Methoden zur Ermittlung und Sicherstellung des aktuellen Standes der Technik für IT-Leistungen fest. Dies bedeutet nicht, dass die Einhaltung von IT-Standards derzeit gesetzlich gefordert ist; im Falle des Schadenseintrittes wird jedoch die Frage gestellt werden, warum man sich nicht um die Einhaltung anerkannter Standards bemüht hat.

4.1 Die Suche nach dem passenden IT-Standard

Bei der Suche nach den für das jeweilige Unternehmen „richtigen" IT-Standards hat die Geschäftsleitung jedoch die Qual der Wahl. Zudem wird die Lesebegeisterung des IT-Anwenders auf eine harte Probe gestellt: So umfassen bspw. die allgemein anerkannten

[30] Zu den jüngeren Entwicklungen (8/2012) bzgl. des Erwerbs gebrauchter Software vgl. *Rath/Maiworm*, WRP 2012, 1051

[31] Laut einer Untersuchung von *Gartner* geben Unternehmen ohne ein effizientes Lizenzmanagementsystem bis zu 60 % zu viel für Software aus. Zu dem Projekt „Liberate" von IBM vgl. unter www.ibm.de.

[32] Wie schon zuvor gezeigt, geht auch § 2 Abs. 2 BSIG davon aus, dass Sicherheit in der Informationstechnik die Einhaltung bestimmter (Sicherheits-) Standards bedeutet.

Standards für IT-Sicherheit der ISO 27001-Familie und des BSI weit über 3.000 Seiten. Gerade die (im Bundesanzeiger-Verlag auch als Printversion erhältlichen) Grundschutz-Kataloge zeigen allerdings sehr anschaulich verschiedene Gefährdungslagen auf und geben Empfehlungen zur Risikominderung; das ebenfalls vom BSI angebotene „GS Tool" hilft bei der Erfassung und Auswertung.

Derzeit gibt es allerdings keinen übergreifenden, national oder international verbindlichen Standard für die Sicherstellung von IT-Compliance. Die Frage, welche Standards für das jeweilige Unternehmen und die betreffende Anwendung richtig sind, kann daher nicht pauschal beantwortet werden. Bei der Auswahl des richtigen Standards kommt es vielmehr auch auf die im Unternehmen und bei dem IT-Dienstleister bereits vorhandenen Prozesse und die Aktualität der einschlägigen Standards an.

4.2 Die Rechtsfolge der Einhaltung von IT-Standards und Best Practices aus der Finanzwelt

Es ist bereits zuvor angeklungen, dass die Vorgaben für IT-Compliance entweder in einer ganzen Reihe von Normen „versteckt" oder aber so wenig konkret sind, dass selbst bei deren gewissenhafter Umsetzung noch immer Zweifel bestehen, ob alle Vorgaben eingehalten sind. Auch die zuvor genannten, vermeintlich speziellen IT-Regelwerke enthalten im Ergebnis nur wenige eindeutige und belastbare Vorgaben zur Sicherstellung von IT-Compliance. Zudem entfalten IT-Standards – zumindest bislang – weder unmittelbare Rechtswirkung noch resultiert aus deren Anwendung eine (unwiderlegliche) Vermutung für die Rechtskonformität und damit die Einhaltung von IT-Compliance.

Weiterhin ist problematisch, dass es nur wenige wirklich konkrete Vorgaben an die IT gibt, welche überhaupt normativen Charakter haben, geschweige denn formalen Gesetzesrang einnehmen. Hierzu zählen beispielsweise beim IT-Outsourcing die bankenspezifischen Vorgaben der §§ 25 a KWG, 33 Abs. 2 WpHG, die für Banken und Finanzdienstleister durch spezifische Rundschreiben ergänzt werden (beispielsweise bezüglich des Outsourcing gemäß § 25 KWG das RS 11/2001 der BaFin) und das RS 11/2010 der BaFin, mit dem Mindestanforderungen für das Risikomanagement (MaRisk) aufgestellt werden.[33] In den derzeitigen Rahmenvorgaben werden Pflichten bezüglich der Ausgestaltung der Leitungs-, Steuerungs- und Kontrollprozesse als Bestandteile des internen Risikomanagement festgelegt[34]. So wird u. a. die Einhaltung der BSI-Standards für den IT-Grundschutz verlangt.[35] Mit den MaRisk werden im Ergebnis die Mindestanforde-

[33] In diesen MaRisk hat die BaFin zur Konkretisierung der Vorgaben des § 25 a Abs. 1 KWG die zuvor aufgestellten Mindestanforderungen an das Betreiben von Handelsgeschäften (MAH), die Mindestanforderungen an die Ausgestaltung der internen Revision (MaIR) und die Mindestanforderungen an das Kreditgeschäft (MaK) der Kreditinstitute konsolidiert und ergänzt.

[34] Für Ende 2012 wird eine vierte MaRisk-Novelle erwartet. Derzeit befindet sich ein Entwurf der MaRisk in der Fassung vom 26.04.2012 in der Konsultationsphase.

[35] Siehe AT 4.3.2 MaRisk; Modul BTR 4.

rungen definiert, die Finanzinstitute bei ihrem Risikomanagement umzusetzen haben. In den MaRisk wird zudem hervorgehoben, dass die operationellen Risiken inklusive der IT-Risiken integraler Bestandteil des Risikomanagements sind. Dies entspricht im Kern den zuvor aufgestellten Thesen und Vorgaben der IT-Compliance, weshalb die Anforderungen an die IT-Sicherheit von Banken nachfolgend nochmals etwas ausführlicher dargestellt werden sollen:

Explizit mit IT-Sicherheit beschäftigt sich beispielsweise Abschnitt AT 7.2 („Technisch-organisatorische Ausstattung") der MaRisk: Danach haben sich Umfang und Qualität der technisch-organisatorischen Ausstattung insbesondere an betriebsinternen Erfordernissen, den Geschäftsaktivitäten, der Risikostrategie sowie der Risikosituation zu orientieren. Die IT-Systeme und die zugehörigen IT-Prozesse müssen daher die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen. Für diese Zwecke ist bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen. Die Wahl der Standards ist zu begründen. Ihre Eignung ist regelmäßig von den fachlich und technisch zuständigen Stellen zu überprüfen. Neue IT-Systeme sowie Veränderungen an IT-Systemen sind vor ihrem Einsatz zu testen und von den fachlich und technisch zuständigen Stellen abzunehmen. Produktions- und Testumgebung sind dabei grundsätzlich voneinander zu trennen. Die Entwicklung und Änderung programmtechnischer Vorgaben (z. B. Bewertungsalgorithmen) haben unter Beteiligung aller fachlich und technisch zuständigen Stellen zu erfolgen. Die programmtechnische Umsetzung hat grundsätzlich durch eine vom Anwender unabhängige Stelle zu erfolgen.[36]

Die zunächst nur für Kreditinstitute einschlägigen Anforderungen der MaRisk können mit ihren unterschiedlichen Modulen als „Best Practice" auch in Unternehmen zur Anwendung kommen, die nicht zum Banken- und Finanzdienstleistungs-Sektor gehören. Denn auch interne Richtlinien und Verwaltungsvorschriften von eigentlich für das Unternehmen gar nicht zuständigen Behörden (wie etwa die IT-Richtlinie des BMI hinsichtlich des Einsatzes von IT-Systemen in den obersten Bundesbehörden) können wertvolle Ansatzpunkte für die Umsetzung von IT-Compliance im Unternehmen enthalten.

5 Das Damokles-Schwert der Haftung/Fazit

Die Palette der denkbaren Sanktionen bei Verstößen gegen IT-Compliance-Anforderungen reicht – je nach Zielrichtung und Charakter der verletzten Norm – neben den zuvor beschriebenen Folgen von drakonischen Maßnahmen wie Haft, Verhängung

[36] Weiterhin gibt es noch ergänzende Erläuterungen im Dokument „MaRisk – Regelungstext mit Erläuterungen". Hier wird ebenfalls auf die Auswahl von Standards zum IT-Sicherheitsmanagement eingegangen und auf die zuvor dargestellten BSI-Standards verwiesen.

von Geldbußen, Hausdurchsuchungen und Bußgeldverfahren wegen Aufsichtspflichtverletzung gegen geschäftsführende Organmitglieder über zivilrechtliche Ansprüche gegen Organe der Gesellschaft (§§ 91, 93, 116 AktG) bis hin zur Abschöpfung des „gesamten wirtschaftlichen Wertes" durch Verfall (§§ 73 StGB, 29 a OWiG) und Schadensersatzansprüchen von Wettbewerbern (etwa § 33 GWB). Daneben kann es zu steuerrechtlich unerwünschten Folgen (Abzugsverbot, Schätzung) wie auch zu negativen Folgen für das Rating des Unternehmens nach Basel II kommen. Bislang sind allerdings – zumindest in Deutschland – kaum Fälle mangelnder IT-Compliance bekannt geworden, bei denen dieses Sanktionsinstrumentarium mit aller Schärfe zur Anwendung kam.

Die vorstehend skizzierten IT-spezifischen Branchenkenntnisse sind naturgemäß nicht von jeder Geschäftsleitung zu erwarten. Es stellt jedoch auch kein Allheilmittel dar, sich auf den Sachverstand eines externen IT-Dienstleisters oder des CIO zu verlassen, denn eine vollständige Delegation der zuvor skizzierten Pflichten kann damit ebenso wenig erreicht werden wie mit der internen Aufgabenverlagerung und der Schaffung von Positionen eines CIO oder CSO. Dennoch wird gerade auch bei einer Auslagerung der IT-Systeme auf einen externen IT-Provider oftmals nur auf die Verbesserung der Kostenquote geschielt, anstatt bei dem Fremd-Outsourcing auch auf die notwendige „law compliance" zu achten.[37]

Trotz der komplexen Kombination aus Recht, Steuern und Technik müssen die im Unternehmen eingesetzten IT-Systeme den hohen Anforderungen von IT-Compliance genügen und dürfen nicht als zu vernachlässigende „Commodity" angesehen werden. Zu den Pflichten einer vorausschauenden Unternehmensleitung gehört es vielmehr, ein angemessenes Informations- und Risikomanagement zu etablieren und rechtskonforme IT-Systeme einzusetzen. Branchenübliche IT-Standards wie ISO, CobiT, ITIL und die IT-Grundschutz-Kataloge des BSI sowie die Best Practices aus dem Finanzdienstleistungssektor sind inzwischen allgemein anerkannt und helfen bei der Erfüllung der Anforderungen der IT-Compliance.

[37] Vgl. hierzu auch die Bitkom-Studie Compliance in IT-Outsourcing-Projekten (2007), abrufbar unter http://www.bitkom.org/files/documents/BITKOM-Leitfaden_Compliance.pdf.

6 Annex: IT-Compliance-Checkliste

	IT-Compliance-Bereich/Fragestellung	compliant	non compliant
		ja	nein/weiß nicht
1	Gibt es für Ihre IT ein Sicherheits- und Notfallkonzept? Erfolgt ein automatisches Backup/Spiegelung der Server Gibt es einen Masterplan für Systemabsturz und Recovery-Maßnahmen Redundante Server, USV für bestimmte Server		
2	Werden die Dokumentationspflichten eingehalten? Gibt es ein Verfahrensverzeichnis nach BDSG, eine schriftliche Dokumentation des ECM/DMS, und einer Data Retention Policy		
3	E-Mail und Internetnutzung Gibt es eine aktuelle IT-Richtlinie und E-Mail-Policy? Ist die private Nutzung der IT ausreichend geregelt? Gibt es eine Regelung bezüglich der Zugriffs-, Editier- und Löschrechte des Arbeitgebers? Gibt es Vorgaben bezüglich der Ablage von geschäftlichen E-Mails oder ein (softwaregestütztes) automatisches E-Mail-Management?		
4	Archivierung Gibt es ein Archivierungskonzept, dass die Einhaltung der Aufbewahrungsfristen sicherstellt? Ist die Revisionssicherheit des Archivierungssystems gewährleistet?		
5	Sind Ihre IT-Systeme oder Teile davon zertifiziert? Kommen IT-Standards bei Ihnen zum Einsatz? Wird ein Lizenzmanagement eingesetzt?		
6	IT-Security Werden die einschlägigen IT-Standards (etwa ISO 27001 oder BSI-Standards) eingehalten? Gibt es eine effektive Spam-Abwehr, einen aktuellen Virenfilter, effektive Firewalls?		
7	Beauftragung von IT-Dienstleistern Sind Ihre externen IT-Dienstleister auf die Einhaltung von IT-Compliance verpflichtet? Ist der Outsourcing-Vertrag auf aktuellem Stand? Gibt es einen Auftragsdatenverarbeitungsvertrag und pönalisierte SLA?		

Datenschutzrechtliche Compliance im Unternehmen

Silvia C. Bauer

Inhaltsverzeichnis

Zusammenfassung

Das Thema „Datenschutz" gerät immer mehr in den Fokus der Öffentlichkeit. Nicht nur die Verschärfung der Rechtslage innerhalb Deutschlands und die geplante Umsetzung einer europäischen Datenschutzgrundverordnung, die ganz Europa ein einheitliches Datenschutzniveau bringen soll, haben dazu beigetragen, sondern auch die stetige Sensibilisierung der Öffentlichkeit hinsichtlich des Umgangs mit ihren Daten. Neben der Forderung nach einer technisch ausgereiften und möglichst sicheren Datenverarbeitung hat sich auch verstärkt das Bewusstsein ausgebildet, dass Daten nicht beliebig für jeden Zweck verarbeitet und genutzt werden dürfen und den entsprechenden Aktivitäten von

S. C. Bauer (✉)
Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: silvia.c.bauer@luther-lawfirm.com

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2_8, © Springer Fachmedien Wiesbaden 2013

Unternehmen Grenzen zu setzen sind. Damit einhergehend sind die Anforderungen an Unternehmen, Daten im Einklang mit den gesetzlichen Vorgaben – also „compliant" – zu verarbeiten, gestiegen.

Unternehmen müssen die verschiedenen formalen Anforderungen der gesetzlichen Vorgaben wie Meldepflichten, Bestellung von Datenschutzbeauftragten oder Erstellung von Verfahrensverzeichnissen einhalten und daneben sicherstellen, dass auch der Umgang mit den Daten an sich innerhalb des Unternehmens den geltenden Rechtsvorschriften entspricht. Gerade in Hinblick auf den Umgang mit Arbeitnehmer- und Kundendaten haben die Skandale der jüngsten Zeit bedauerlicherweise erhebliche Defizite in deutschen Unternehmen aufgezeigt. Ein Unternehmen sollte daher den Datenschutz als Wettbewerbsvorteil begreifen, ihn zielgerichtet in seine organisatorischen Abläufe integrieren und entsprechende Strukturen etablieren. Thematisch auf den Datenschutz ausgerichtete Schulungen, Verhaltensregelungen und die Benennung von Verantwortlichen sollten daher wesentlicher Bestandteil einer Compliance-Organisation im Unternehmen sein.

1 Einleitung

Informationen sind sicher zu verarbeiten. Ein Unternehmen, das diesen Grundsatz missachtet, setzt sich erheblichen Risiken aus: Verstöße gegen entsprechende nationale oder internationale Vorgaben – insbesondere die Vorgaben des Sarbanes Oxley Acts[1], des EuroSOX, des KontraG oder bald auch des BilMoG[2] – können Schadenersatzansprüche, empfindliche Bußgelder oder sogar Freiheitsstrafen nach sich ziehen. Entgegen der früheren Praxis werden die deutschen Datenschutzaufsichtsbehörden immer stärker aktiv und verhängen Bußgelder, die sogar in Einzelfällen die Grenze von einer Million Euro überschritten haben. Daneben kann ein Sicherheitsleck in der eigenen IT-Infrastruktur oder der Verlust von Daten immense wirtschaftliche Auswirkungen haben.[3] Zudem sind Unternehmen als verantwortliche Stelle verpflichtet, bestimmte Datenpannen sowohl den Datenschutzaufsichtsbehörden als auch den Betroffenen, deren Daten unrechtmäßig Dritten zur Kenntnis gelangen, mitzuteilen. Der sorglose Umgang mit Daten wird daher nicht nur durch Sanktionen der Datenschutzaufsichtsbehörden, sondern auch durch eine negative Presse abgestraft und führt in der Regel zu einem immensen Vertrauensverlust bspw. bei Kunden oder Mitarbeitern, der auch den Verlust von Kunden und wirtschaftliche Nachteile zur Folge hat.

[1] Siehe dazu Kapitel *Rath*, Rechtliche Aspekte von IT-Compliance, Ziff 3.2.

[2] Siehe weiterführend zu den Anforderungen an eine entsprechende Compliance-Organisation *Bauer/Wesselmann*, WISU 8-9/08, 1128 ff.; *Bauer*, Datenschutzpraxis 9/2008, 2 ff.

[3] Siehe dazu bspw. die Ergebnisse aus der „Jahresstudie 2008: Kosten von Datenpannen" des Marktforschungsinstituts „The Ponemon Institute", das pro Datenpanne Kosten von 2,4 Mio. € ermittelt hat, abrufbar unter www.encryptionreports.com.

Datenschutz ist als Chance und Wettbewerbsvorteil zu begreifen; ein offener Umgang mit den Verarbeitungsvorgängen führt zu einer Kundenbindung der Altkunden und erleichtert den Gewinn von Neukunden.[4] Daneben haben datenschutzkonform aufgestellte Unternehmen regelmäßig bei der Vergabe von Aufträgen Vorteile gegenüber den weniger compliant aufgestellten Konkurrenten. Insbesondere im öffentlichen Bereich ist es erforderlich, nachweislich Daten vor dem Zugriff Dritter zu schützen; Zertifizierungen u. ä. werden daher immer mehr durchgeführt. Aus diesem Grund legen Unternehmen immer mehr Wert auf den Schutz ihrer Daten, die ordnungsgemäße Datenverarbeitung und die Sicherheit ihrer IT-Umgebung. Während in der Vergangenheit häufig die Informationstechnologie und deren Funktionalität als größter Risikofaktor in diesem Zusammenhang galt, setzt jetzt langsam ein Umdenken ein: Der Mensch und sein Umgang mit risikobehafteten Vorgängen rückt in den Vordergrund. Das Verantwortungsbewusstsein des Einzelnen bei dem Einsatz und der Nutzung von Informationstechnologie sowie der Verarbeitung von Daten soll geschärft werden. Ziel ist die Identifizierung, Minimierung oder sogar der völlige Ausschluss von datenschutzrechtlichen Risiken. Ein Unternehmen ist dabei maßgeblich auf seine Mitarbeiter angewiesen.

Datenschutzrechtliche Compliance hat deshalb – in enger Verzahnung mit der IT-Compliance – einerseits die Umsetzung von gesetzlich und auch tatsächlich erforderlichen organisatorischen und technischen Maßnahmen durch das Unternehmen zum Ziel; andererseits bezweckt sie die einzelnen Mitarbeiter in die Pflicht zu nehmen und ihnen ihre Verantwortung für einen datenschutzrechtlich korrekten Umgang mit Daten bewusst zu machen. Mitarbeiter sind so zu schulen, dass sie unter Wahrung der Persönlichkeitsrechte des Einzelnen gesetzeskonform Daten verarbeiten und nutzen.

Ziel dieses Abschnitts ist es daher nicht nur einen kurzen Überblick über die vom Unternehmen einzuhaltenden datenschutzrechtlichen Anforderungen zu geben, sondern darüber hinaus zu sensibilisieren, in welchen Bereichen die Mitwirkung der Mitarbeiter essentiell sein kann, um das Unternehmen in die Lage zu versetzen, die in Deutschland geltenden datenschutzrechtlichen Vorgaben umzusetzen und einzuhalten.

Dabei wird zunächst erläutert, wer im Unternehmen für den Datenschutz zuständig ist, wen welche Verantwortung trifft und welche Anforderungen das Unternehmen erfüllen muss. Daneben werden beispielhaft einzelne Maßnahmen vorgestellt, die das Unternehmen bei der Einführung seiner Datenschutzorganisation unterstützend ergreifen kann, um den Herausforderungen, die das Datenschutzrecht an ein Unternehmen stellt, gelassen gegenübertreten zu können.

2 Verantwortlichkeiten

Das deutsche Datenschutzrecht definiert in § 3 Abs. 7 BDSG (i. V. m. § 2 BDSG) als Verantwortliche die Personen oder Stellen,

[4] Vgl. *Bauer*, WISU 4/09, 504 ff.

- die personenbezogene Daten für sich selbst erheben, verarbeiten oder nutzen oder
- dies durch andere im Auftrag vornehmen lassen.

Eine verantwortliche Stelle hat dafür Sorge zu tragen, dass die durch sie oder ihren Auftragnehmer durchgeführten Datenverarbeitungsvorgänge rechtskonform erfolgen und sie bzw. ihr Auftragnehmer die datenschutzrechtlichen Vorgaben einhält. Verantwortlich ist dabei immer das Unternehmen als juristische Person und nicht etwa nur die Organisationseinheit innerhalb des Unternehmens, die tatsächlich die jeweilige Datenverarbeitung durchführt (bspw. das eigene Rechenzentrum).[5]

Daraus ergibt sich eine besondere Verantwortung der Geschäftsleitung, die in ihrem Unternehmen datenschutzrechtlich relevanten Vorgänge so zu organisieren, dass das Unternehmen insgesamt und speziell die jeweiligen Geschäftsbereiche bzw. Mitarbeiter datenschutzkonform agieren. Dabei sind – entgegen der bislang überwiegenden Praxis – nicht nur die IT-Abteilung oder der CIO einzubinden, sondern alle Geschäftsbereiche, in denen personenbezogene Daten verarbeitet werden. Dazu zählen insbesondere die Bereiche Human Resources, der Vertrieb, das Marketing, der Einkauf, die Buchführung sowie der Betriebsrat und der Betriebsarzt.

Nicht zuletzt hat die Geschäftsleitung sicherzustellen, dass auch Dritte, an die Daten übermittelt werden, den datenschutzrechtlichen Anforderungen Genüge tun. Dies gilt insbesondere, wenn diese Dritten ihren Sitz im Ausland haben und damit die Datenübermittlung und anschließende Verarbeitung speziellen Anforderungen unterliegt.

Eine besondere Verantwortung trifft auch den Datenschutzbeauftragten des Unternehmens: Sofern dieser nach den Vorgaben des BDSG von der Geschäftsleitung zu bestellen ist, hat er als unabhängige Instanz darauf hinzuwirken, dass das Unternehmen seine datenschutzrechtlichen Pflichten erfüllt (vgl. §§ 4f, 4g BDSG). Der Datenschutzbeauftragte gilt daher auch als verlängerter Arm der Datenschutzaufsichtsbehörden.

3 Haftung und Rechtsfolgen

3.1 Täterschaft

Wie auch im Rahmen der IT-Compliance[6] haften die Geschäftsleitung, der Datenschutzbeauftragte oder auch jeder einzelne Mitarbeiter für Verstöße gegen datenschutzrechtliche Bestimmungen bzw. unterlassene Kontrollen der datenschutzrelevanten Tätigkeiten. Die Haftung ergibt sich aus Gesetz bzw. aus entsprechenden Weisungen oder (arbeits-) vertraglichen Vereinbarungen. Verantwortlich ist jeweils derjenige, den die Pflicht,

[5] Vgl. *Dammann* in: Simitis, BDSG, 7. Aufl. 2011, § 3 Rn. 225 ff.; *Gola*, in: Gola/Schomerus, BDSG, 11. Aufl. 2012, § 3 Rn. 48.

[6] Vgl. dazu Kapitel *Rath*, Rechtliche Aspekte von IT-Compliance, Ziff. 2.

gegen die verstoßen wird, trifft.[7] Hat die Geschäftsleitung daher einer Person eine Pflicht übertragen, wie bspw. die Kontrolle der IT-Sicherheit, haftet diese Person für ihre Verstöße grundsätzlich selbst.[8]

3.2 Ansprüche des Betroffenen

Wird gegen eine Datenschutzbestimmung verstoßen bspw. durch unerlaubte Weitergabe von Gesundheitsdaten eines Arbeitnehmers an einen potentiellen neuen Arbeitgeber, der dadurch von der Einstellung absieht und ist dem Betroffenen dadurch ein Schaden entstanden, kann er entsprechende Ansprüche gegen den jeweiligen Täter geltend machen (u. a. gemäß § 7 BDSG, § 823 Abs. 1 und 2 BGB).

Die Praxis zeigt, dass den Betroffenen im Regelfall der Nachweis eines entsprechenden Schadens nur schwer gelingt und daher nur selten tatsächlich Ansprüche auf Schadenersatz geltend gemacht werden. Indes neigen Betroffene immer häufiger dazu, den Datenschutzaufsichtsbehörden vermeintliche Verstöße von Unternehmen zu melden. Die Konsequenz liegt auf der Hand: Die Datenschutzaufsichtsbehörden gehen entsprechenden Hinweisen regelmäßig nach, so dass sich ein Unternehmen in diesem Fall den Nachfragen bzw. Kontrollmaßnahmen der Behörde ausgesetzt sieht.

3.3 Sanktionen bei Verstößen

3.3.1 Ahndung als Ordnungswidrigkeit

Ein Verstoß gegen Datenschutzbestimmungen kann von den Datenschutzaufsichtsbehörden als Ordnungswidrigkeit mit Bußgeldern bis zu einer Höhe von 300.000,00 € geahndet werden (§ 43 BDSG). Die Datenschutzaufsichtsbehörden ahnden in der Regel jeden Verstoß einzeln; werden daher bspw. 100.000 Kundendaten unzulässigerweise an einen Dritten verkauft, werden die Bußgelder für die einzelnen Verstöße addiert, so das in der Summe ein höherer Betrag zusammenkommen kann. Jedenfalls soll die Geldbuße den wirtschaftlichen Vorteil, den der Täter aus der Tat zieht, überschreiten.

Sanktioniert werden zum einen Pflichtverstöße gegen **formelle Pflichten**, die gegenüber den **Datenschutzaufsichtsbehörden** oder auch allgemein erfüllt werden müssen, wie bspw.

- Verstöße gegen Meldepflichten
  (§ 43 Abs. 1 Nr. 1 i. V. m. § 4d, Abs. 1, § 4e Satz 2 BDSG),
- Verstöße gegen die Pflicht zur Auskunft
  (§ 43 Abs. 1 Nr. 10 i. V. m. § 38 BDSG),

[7] Vgl. *Ehmann* in: Simitis, BDSG, 7. Aufl. 2011, § 43, Rn. 22 ff.

[8] Vgl. bspw. für den Fall der Haftung bei fehlender Auskunftserteilung gegenüber einem Betroffenen durch einen Beauftragten: OLG Celle v. 14.6.1995 – 2 Ss (OWi) 185/95, RDV 1995, 244 f.

- Unterlassen der Bestellung des Datenschutzbeauftragten (§ 43 Abs. 1 Nr. 2 i. V. m. § 4f Abs. 1 BDSG),
- Unterlassen des Abschlusses eines schriftlichen Auftragsdatenverarbeitungsvertrages und der vorgeschriebenen Kontrollen des Auftragnehmers (§ 43 Abs. 1 Nr. 2b i. V. m. § 11 BDSG),
- Unterlassen der Benachrichtigungen nach § 42 a BDSG bei Datenschutzpannen (§ 43 Abs. 2 Nr. 7 i. V. m. § 42a BDSG).

Zum anderen können Pflichtverstöße gegen **formelle Pflichten**, die gegenüber dem **Betroffenen** erfüllt werden müssen, geahndet werden, wie bspw.

- Verstöße gegen Unterrichtungspflichten (§ 43 Abs. 1 Nr. 3 BDSG i. V. m. § 28 Abs. 4 Satz 2, 1. HS BDSG),
- Verstöße gegen die Pflicht zur Auskunft (§ 43 Abs. 1 Nr. 7a, 8a i. V. m. § 29 Abs. 6, § 34 BDSG),
- Verstöße gegen Benachrichtigungspflichten (§ 43 Abs. 1 Nr. 8 BDSG i. V. m. § 33 Abs. 1 BDSG).

Neben den Verstößen gegen formelle Pflichten werden auch Verstöße gegen **materielle Datenschutzvorschriften** sanktioniert. So werden bspw.

- die unzulässige Übermittlung, Nutzung, Verarbeitung von personenbezogenen Daten oder auch das unbefugte Bereithalten von Daten zum Abruf als Ordnungswidrigkeit geahndet (vgl. § 43 Abs. 1, Nr. 4, Nr. 6, § 43 Abs. 2 BDSG).

3.3.2 Ahndung als Straftat

Erfolgen die in § 43 Abs. 2 BDSG aufgeführten Handlungen, wie die unbefugte Verarbeitung von Daten gegen Entgelt oder mit Bereicherungsabsicht, kann dies als strafbare Handlung geahndet werden und eine Geldstrafe bzw. eine Freiheitsstrafe bis zu zwei Jahren Gefängnis nach sich ziehen (§ 44 BDSG).

3.3.3 Sonstige Maßnahmen

Neben den o. g. Sanktionen dürfen die Datenschutzaufsichtsbehörden die Ausführung der Vorschriften des BDSG im Unternehmen kontrollieren, Auskunft sowie – u. a. unter Verhängung von Zwangsgeld – die Umsetzung von Maßnahmen zur Beseitigung von festgestellten Mängeln technischer oder organisatorischer Maßnahmen verlangen (§ 38 i. V. m. § 43 BDSG). Bei der Durchführung von Kontrollen kann sich die Datenschutzaufsichtsbehörde im Übrigen bei einer Verweigerung des Zutritts mittels richterlichem Durchsuchungsbeschluss und polizeilicher Hilfe Zutritt zu dem Unternehmen verschaffen.

Daneben besteht gemäß § 42 a BDSG eine erweiterte Informationspflicht, der sogenannte Datenschutzpranger: Sofern

- besondere Arten von personenbezogenen Daten nach § 3 Abs. 9 BDSG (bspw. Gesundheitsdaten oder Daten betreffend die Religion, Rasse),
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten bzw. den Verdacht auf solche oder
- personenbezogene Daten betreffend Bank- oder Kreditkartenkonten

unrechtmäßig durch Dritte zur Kenntnis genommen werden oder unrechtmäßig übermittelt werden und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen Betroffener bestehen könnten, ist die verantwortliche Stelle verpflichtet, sowohl die jeweils zuständige Datenschutzaufsichtsbehörde als auch alle Betroffenen von den Verstößen, die sie begangen und erkannt hat, zu informieren. Erfordert die Unterrichtung der Betroffenen einen unverhältnismäßigen Aufwand, so kann die Information auch alternativ durch Anzeigen in zwei bundesweit erscheinenden Tageszeitungen erfolgen.

3.3.4 Verfolgung von Verstößen in der Praxis

In der Vergangenheit haben die Datenschutzaufsichtsbehörden Verstöße weniger mit Bußgeldern und Freiheitsstrafen geahndet, sondern den Schwerpunkt mehr in Richtung Kontrolle und anschließende Beseitigung der Mängel durch das Unternehmen gelegt.[9] Daher ist die Zahl der bis dato in diesem Zusammenhang bekannt gewordenen Entscheidungen als eher gering einzustufen.[10] Aufgrund der jüngsten Skandale beginnt sich dieses Bild jedoch zu wandeln: So wurde gegen ein Unternehmen eine Geldbuße von insgesamt 1,42 Mio. € verhängt; geahndet wurde dabei auch insbesondere der Verstoß der unterlassenen Bestellung von Datenschutzbeauftragten mit jeweils 10.000,00 €[11] oder die unbefugte Erstellung von Kundenprofilen mit 200.000,00 €.[12]

Insofern sollten Unternehmen künftig verstärkt damit rechnen, dass sich die Datenschutzaufsichtsbehörden nicht mehr auf eine Kontrolle und außergerichtliche Einigung beschränken. Infolgedessen besteht für Unternehmen ein erhöhter Handlungsbedarf: Während früher ein Verstoß anonym blieb, ist den Medien ein Datenschutzverstoß heute eine Schlagzeile wert. Daneben veröffentlichen viele Datenschutzaufsichtsbehörden nach

---

[9] Vgl. dazu etwa *Weichert*, NStZ 1999, 490.

[10] Siehe dazu m. w. N. *Bergmann/Möhrle/Herb*, BDSG, Loseblatt, Stand: Januar 2012, § 43, Rn. 114 oder auch beispielhaft den 23. Tätigkeitsbericht des hamburgischen Beauftragten für den Datenschutz und die Informationsfreiheit, S. 201, abrufbar unter: http://www.datenschutz-hamburg.de/uploads/media/23._Taetigkeitsbericht_Datenschutz_2010-2011.pdf.

[11] Vgl. die Pressemitteilung über den Beschluss des Innenministeriums Baden-Württemberg – Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich – vom 11.9.2008, abrufbar unter http://www.innenministerium.baden-wuerttemberg.de/fm7/2028/Lidl%20%20Bu%DFgeldverfahren%20abgeschlossen.470204.pdf.

[12] Vgl. den 23. Tätigkeitsbericht des hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, S. 185–187, abrufbar unter: http://www.datenschutz-hamburg.de/uploads/media/23._Taetigkeitsbericht_Datenschutz_2010-2011.pdf.

wie vor ihre Tätigkeitsberichte online, so dass einer Vielzahl von Interessierten einfach und schnell offen gelegt wird, welche Tätigkeiten die Behörden im Einzelnen entfaltet haben. Auch wenn Unternehmen nicht direkt benannt werden, ist wohl nicht auszuschließen, dass ein interessierter Leser durchaus Rückschlüsse auf das ein oder andere Unternehmen ziehen könnte.[13]

4 Anforderungen an das Unternehmen

Um datenschutzrechtlich konform Daten in Deutschland zu verarbeiten gilt es einerseits die gesetzlichen Formvorschriften zu beachten und andererseits die Datenverarbeitung an sich gesetzeskonform auszugestalten. Formelle Vorgaben sind direkt von dem Unternehmen zu erfüllen, während der gesetzeskonforme Umgang mit Daten der Mithilfe der Mitarbeiter in ihrer Funktion als datenverarbeitende Person bedarf. Nachfolgend soll kurz dargestellt werden, in welchen Bereichen Unternehmen entweder selbst oder durch ihre Mitarbeiter tätig werden müssen, um datenschutzrechtliche Compliance einzuhalten.

4.1 Formelle Anforderungen

Unternehmen haben formelle Anforderungen sowohl gegenüber den Datenschutzaufsichtsbehörden bzw. dem Datenschutzbeauftragten als auch gegenüber dem Betroffenen, also demjenigen, dessen Daten sie verarbeiten, zu erfüllen. Durch entsprechende Organisationsstrukturen im Unternehmen ist sicherzustellen, dass diese Anforderungen praktisch umgesetzt werden.

4.1.1 Meldung von Verfahren

Gemäß § 4d BDSG sind Unternehmen verpflichtet, vor Inbetriebnahme einer automatisierten Datenverarbeitung der zuständigen Datenschutzaufsichtsbehörde eine Meldung über dieses Verfahren zu machen.[14] Die Meldung muss bestimmte Angaben enthalten, die in § 4e BDSG aufgeführt sind:

- Name des Unternehmens;
- Inhaber, Vorstände, Geschäftsführer oder sonstige Vertretungsberechtigte;
- Anschrift des Unternehmens;

[13] Siehe etwa die Tätigkeitsberichte des hamburgischen Beauftragten für Datenschutz und Informationsfreiheit unter: http://www.datenschutz-hamburg.de/publikationen-taetigkeitsberichte/taetigkeitsberichte.html.

[14] Siehe dazu beispielhaft das Merkblatt zum Meldebogen des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein nebst entsprechender Meldeformulare unter: https://www.datenschutzzentrum.de/download/merkmeld.pdf.

- Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung;
- Beschreibung der von der Verarbeitung betroffenen Personengruppen und der betroffenen Daten oder Datenkategorien;
- Empfänger oder Empfängerkategorien der Daten (inklusive etwaiger Auftragsdatenverarbeiter);
- Regelfristen für die Löschung der Daten;
- die geplante Datenübermittlung in Drittstaaten (d. h. Länder, die kein den EU-Vorgaben entsprechendes Datenschutzniveau aufweisen, bspw. die USA oder Indien);
- eine allgemeine Beschreibung, die eine vorläufige Beurteilung ermöglicht, ob die ergriffenen technischen und organisatorischen Maßnahmen gemäß § 9 BDSG angemessen sind.

Erfolgt die Meldung nicht rechtzeitig, unvollständig, fehlerhaft oder gar nicht, gilt dies als Ordnungswidrigkeit gemäß § 43 Abs. 1 Nr. 1 BDSG.

Die Meldepflicht **entfällt** gemäß § 4d Abs. 2, 3 BDSG, sofern das Unternehmen

- einen Datenschutzbeauftragten bestellt hat oder
- höchstens neun Personen mit der Datenverarbeitung etc. beschäftigt sind, diese für eigene Zwecke des Unternehmens erfolgt, entweder die Einwilligung desjenigen, dessen Daten verarbeitet werden vorliegt oder die Verarbeitung für Zwecke der Erfüllung eines Vertrages oder vertragsähnlichen Vertrauensverhältnisses erfolgt.

Die Meldepflicht **besteht jedenfalls**, sofern das Unternehmen geschäftsmäßig (also dauerhaft und für wirtschaftliche Zwecke, bspw. Auskunfteien, Adressverlage, Kreditschutzorganisationen wie der SCHUFA)[15] Daten speichert für

- Zwecke der Übermittlung oder
- Zwecke der anonymisierten Übermittlung.

Praxishinweis

In der Regel haben Unternehmen Datenschutzbeauftragte bestellt. In diesem Fall ist die Meldung entbehrlich. Handelt es sich jedoch um eine meldepflichtige Auskunftei etc. oder ein Unternehmen, das keinen Datenschutzbeauftragten benötigt, sind Maßnahmen zu ergreifen, die dem Erfordernis der Meldung Rechnung tragen. Die Geschäftsleitung sollte daher zur Minimierung datenschutzrechtlicher Risiken entsprechende organisatorische Maßnahmen einleiten, wie bspw. einen Verantwortlichen in der IT-Abteilung benennen, der die Meldungen vorbereitet und durchführt.

[15] Siehe dazu *Gola*, in: Gola/Schomerus, BDSG, 11. Aufl. 2012, § 29 Rn. 4.

4.1.2 Erstellen von Verfahrensverzeichnissen

Unternehmen sind verpflichtet, Verfahrensverzeichnisse zu erstellen und ihrem Datenschutzbeauftragten zu übergeben. Die Verfahrensverzeichnisse enthalten Informationen über die einzelnen Datenverarbeitungsvorgänge im Unternehmen gemäß § 4e Abs. 1 Nr. 1–8 BDSG (siehe dazu bereits oben, Ziff. 4.1.1; Angaben zu den technischen und organisatorischen Maßnahmen sind jedoch entbehrlich) sowie die jeweils zugriffsberechtigten Personen. Ändern sich die Datenverarbeitungsvorgänge, sind die Verfahrensübersichten zu aktualisieren. Üblicherweise verwaltet der Datenschutzbeauftragte die Verfahrensverzeichnisse und stellt daraus eine Verfahrensübersicht zusammen. Diese gibt einen Überblick, welche Verfahren insgesamt im Unternehmen im Einsatz sind.

Der Datenschutzbeauftragte – respektive das Unternehmen, sofern kein Datenschutzbeauftragter zu bestellen ist – haben daneben ein öffentliches Verfahrensverzeichnis auf Antrag jedermann zur Verfügung zu stellen (§ 4g Abs. 2 BDSG). Das öffentliche Verfahrensverzeichnis wird häufig im Internet veröffentlicht, so dass Interessierte dieses leicht abrufen können. In der Regel enthält es nur allgemeine Angaben über die Datenverarbeitungsvorgänge im Unternehmen (bspw. von wem welche Daten verarbeitet werden und an wen diese übermittelt werden), die einen kurzen Überblick ermöglichen sollen.

Praxishinweis

Regelmäßig bestehen in Unternehmen erhebliche Defizite sowohl bei der Erstellung als auch bei der Übergabe der Verfahrensverzeichnisse an den Datenschutzbeauftragten. Dies birgt datenschutzrechtliche Risiken, da der Datenschutzbeauftragte gehalten ist, sowohl den Datenschutzaufsichtsbehörden als auch anderen Interessierten die in den Verfahrensverzeichnissen enthaltenen Informationen zur Verfügung zu stellen.

Um diese Defizite auszugleichen, empfiehlt sich die Einrichtung einer entsprechenden Datenschutzorganisationsstruktur: Die Geschäftsbereiche, die mit dem Verfahren in Berührung kommen, bspw. IT und Human Resources, sollten die erforderlichen Angaben proaktiv gemeinsam erarbeiten, in ein entsprechend zur Verfügung gestelltes Formular eintragen und dem Datenschutzbeauftragten übergeben. Dies setzt selbstverständlich voraus, dass Verantwortliche benannt werden, die sich der Thematik annehmen.

4.1.3 Vorabkontrolle

§ 4d Abs. 5, 6 BDSG sieht vor, dass der Datenschutzbeauftragte automatisierte Datenverarbeitungsverfahren vor deren Start zu kontrollieren hat, sofern die Datenverarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen nach sich ziehen kann.[16]

[16] Vgl. zur Durchführung der Vorabkontrolle: *Bergmann/Möhrle/Herb*, BDSG, Loseblatt, Stand: Januar 2012, § 4d, Rn. 46 ff.; *Ehmann*, Datenschutzpraxis, 01/09, 12 ff.

Insbesondere sind Vorabkontrollen durchzuführen, wenn

- besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG), also Daten betreffend die rassische/ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben verarbeitet werden bzw.
- Verarbeitungen durchgeführt werden, die der Bewertung der Persönlichkeit des Betroffenen dienen (insbesondere Fähigkeits-, Leistungs- und Verhaltenskontrollen).

In der Regel unterliegen daher bspw. Personalinformationssysteme, Videoüberwachungssysteme, Scoringdatenbanken der Vorabkontrolle.[17]

Die Vorabkontrolle **entfällt** grundsätzlich, wenn

- das automatisierte Verfahren aufgrund gesetzlicher Vorschriften durchgeführt werden muss,
- eine Einwilligung des jeweiligen Betroffenen vorliegt oder
- die Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder eines vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.

Praxishinweis

Selbst wenn die Vorabkontrolle aufgrund der oben genannten Ausnahmen nicht erforderlich sein sollte, empfiehlt sie sich im Regelfall, da so durch den Datenschutzbeauftragten eine Rechtmäßigkeitsprüfung erfolgt, die zumindest die Risiken einer unzulässigen Datenverarbeitung minimieren kann.

Das Unternehmen hat dem Datenschutzbeauftragten für Zwecke der Durchführung der Vorabkontrolle eine Verfahrensmeldung gemäß § 4e Satz 1 BDSG i. V. m. § 4g Abs. 2 BDSG zur Verfügung zu stellen (siehe dazu bereits oben unter Ziff. 4.1.2). Diese Meldung ist Grundlage der Vorabkontrolle.

Der Datenschutzbeauftragte hat bei Zweifeln an der Zulässigkeit der Datenverarbeitung die zuständige Aufsichtsbehörde zu kontaktieren (§ 4d Abs. 6 Satz 3 BDSG). Diese kann in diesem Fall u. a. gemäß § 38 Abs. 1, 3 BDSG Kontrollmaßnahmen im Unternehmen durchführen.

Praxishinweis

Der Datenschutzbeauftragte muss in Zweifelsfällen die Datenschutzaufsichtsbehörde benachrichtigen. Ist die Datenverarbeitung unzulässig, so haftet das Unternehmen als verantwortliche Stelle für diesen Verstoß gegen das Datenschutzrecht. Der regelmäßige Austausch zwischen den Beteiligten und der Wille, eine gemeinsame Lösung zu finden,

[17] Vgl. *Bergmann/Möhrle/Herb*, BDSG, Loseblatt, Stand: Januar 2012, § 4d, Rn. 36 ff.

sollten daher als eine dem Datenschutzmanagement immanente Zielsetzung erkannt und gefördert werden. Damit wird das Risiko des reglementierenden Eingriffs einer Behörde in das betriebliche Geschehen zumindest minimiert.

4.1.4 Bestellung von Datenschutzbeauftragten

Unternehmen, die eine Mindestanzahl von Personen mit der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten beschäftigen, sind grundsätzlich zur Bestellung eines Datenschutzbeauftragten verpflichtet, § 4f BDSG.[18] Ausnahmen bestehen daneben für bestimmte Arten von Datenverarbeitungen, bei deren Durchführung jedenfalls ein Datenschutzbeauftragter bestellt werden muss. Das Unterlassen der Bestellung kann als Ordnungswidrigkeit gemäß § 43 Abs. 1 Nr. 2 BDSG geahndet werden, wie bspw. in 2008 mit einem Bußgeld in Höhe von 10.000,00 €.[19]

Die Verpflichtung besteht **unabhängig von der Anzahl** der mit der Datenverarbeitung beschäftigten Personen, sofern das Unternehmen

- personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung erhebt, verarbeitet oder nutzt (bspw. Auskunfteien, Adressverlage, Markt- und Meinungsforschungsunternehmen; § 4f Abs. 1 S. 6 BDSG) oder
- automatisierte Datenverarbeitungsvorgänge durchführt, die eine Vorabkontrolle gemäß § 4d Abs. 5 BDSG verlangen (z. B. Systeme zur Bewertung der Kreditwürdigkeit, Einsatz von Videoüberwachung, Einführung von Personalinformationssystemen, die eine Persönlichkeitsüberwachung zulassen[20], § 4f Abs. 1 S. 6 BDSG).

Die Verpflichtung besteht **abhängig von der Anzahl** der mit der Datenverarbeitung beschäftigten Personen, sofern das Unternehmen

- mindestens zehn Personen wenigstens vorübergehend mit automatisierter Datenerhebung, -verarbeitung oder -nutzung beschäftigt (§ 4f Abs. 1 S. 4 BDSG) oder
- mindestens zwanzig Personen wenigstens vorübergehend mit nichtautomatisierter Datenerhebung, -verarbeitung oder -nutzung beschäftigt (§ 4f Abs. 1 S. 3 BDSG).

Als Personen zählen sämtliche Beschäftigte, die für das Unternehmen in einem „arbeitnehmerähnlichen Status" tätig werden, also neben den Arbeitnehmern auch Auszubildende, freie Mitarbeiter, Telearbeitnehmer oder auch an die IT des Unternehmens angebundene Handelsvertreter.[21]

---

[18] 20 Vgl. ausführlich *Gola/Klug*, NJW 2007, 118 ff. zu den seit 2006 geltenden Neuregelungen.

[19] Vgl. die Pressemitteilung über den Beschluss des Innenministerium Baden-Württemberg – Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich vom 11.9.2008, a. a. O.

[20] Vgl. *Bergmann/Möhrle/Herb*, BDSG, Loseblatt, Stand: Januar 2011, § 4d, Rn. 40; *Petri* in: Simitis, BDSG, 7. Aufl. 2011, § 4d, Rn. 33.

[21] Vgl. *Däuble*, in Däuble/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2010, § 4f, Rn. 15 ff.

Der Datenschutzbeauftragte ist spätestens **binnen eines Monats nach Eintreten der Voraussetzungen schriftlich** zu bestellen; zweckmäßig ist dabei die Festlegung der wichtigsten Aufgaben in der Bestellungsurkunde oder die Bezugnahme auf die Vorschriften der §§ 4f, 4g BDSG. Eine Anzeige der Bestellung gegenüber der Datenschutzaufsichtsbehörde ist nicht erforderlich.

Dem Unternehmen steht es frei, einen internen oder einen externen Datenschutzbeauftragten zu bestellen.[22] Bei der Bestellung eines internen Datenschutzbeauftragten ist zu beachten, dass dieser nach § 4f Abs. 3 BDSG einem besonderen Kündigungsschutz unterliegt, der dem von Betriebsräten ähnelt. Sein Arbeitsverhältnis darf nur dann gekündigt werden, wenn Tatsachen vorliegen, die das Unternehmen zu einer Kündigung aus wichtigem Grund berechtigen würden. Nach Abberufung als Datenschutzbeauftragter gilt der Kündigungsschutz für ein weiteres Jahr weiter. Die Bestellung selbst kann im Übrigen nur widerrufen werden, wenn ebenfalls nach § 626 BGB Gründe vorliegen, die eine Abberufung aus wichtigem Grund erlauben würden.[23] Im Ergebnis ist ein interner Datenschutzbeauftragter kaum kündbar. Insbesondere ist eine Bestellung nicht widerrufbar, nur weil aus bspw. wirtschaftlichen Gründen ein externer Datenschutzbeauftragter bestellt werden soll.[24]

Das Unternehmen ist im Übrigen verpflichtet, dem internen Datenschutzbeauftragten die nötigen Mittel zur Verfügung zu stellen, damit er seine Aufgaben erfüllen kann (bspw. Literatur, Büroausstattung) und ihn für die benötigte Zeit von anderen Aufgaben freizustellen. Ist der Datenschutzbeauftragte für viele Mitarbeiter zuständig oder betreut Unternehmen, die besonders sensible Daten verarbeiten (bspw. Pharmaunternehmen oder Adresshändler) wird dies in der Regel sehr zeitaufwändig sein.

Einen so genannten „Konzerndatenschutzbeauftragten", der sich für eine gesamte Konzerngruppe bestellen lässt, kennt das BDSG nicht. Diese Stellung ist organisatorischer Art; häufig wird der Konzerndatenschutzbeauftragte allerdings als interner Datenschutzbeauftragter von seinem Arbeitgeber bestellt und als externer Datenschutzbeauftragter für die weiteren Unternehmen der Konzerngruppe. Damit soll sichergestellt werden, dass in der Konzerngruppe ein einheitliches Datenschutzniveau herrscht und Synergien gebündelt werden.

Im Übrigen muss ein Datenschutzbeauftragter die nötige fachliche und sachliche Kompetenz sowie Zuverlässigkeit aufweisen, insbesondere sollte er sich im Datenschutzrecht und mit aktuellen Datenverarbeitungstechniken auskennen.[25] Dazu zählt auch eine regelmäßige Weiterbildung. Inzwischen bieten Unternehmen bzw. Verbände auch

---

[22] Vgl. zur Sinnhaftigkeit der Bestellung eines konzernweiten bzw. multinationalen Datenschutzbeauftragten, *Simitis*, in Simitis, BDSG,7. Aufl. 2011, § 4f Rn. 36 ff.

[23] Vgl. BAG v. 23.03.2011 – 10 AZR 562/09, NZA 2011, S. 1063.

[24] Vgl. LAG Berlin-Brandenburg v. 28.05.2009 – 5 Sa 425/09, 5 Sa 434/09, 5 Sa 425, 434/09, Folgeinstanz: BAG v. 23.3.2011 – 10 AZR 562/09, NZA 2011, S. 1063.

[25] Vgl. zum Berufsbild des Datenschutzbeauftragten: LG Ulm v. 31.10.1990 – 5 T 153/90, CR 1991, 103, mit Anm. *Ehmann*; *Koch*, in: Koch (Hrsg.), Der Betriebliche Datenschutzbeauftragte, 6. Aufl. 2006, S. 131 ff.; *Rudolf*, NZA 1996, 296 ff.; Berufsverband der Datenschutzbeauf-

Ausbildungen zum zertifizierten Datenschutzbeauftragten an.[26] Die Datenschutzaufsichtsbehörde ist in diesem Zusammenhang berechtigt, die Fachkunde und Zuverlässigkeit zu überprüfen und bei fehlenden Voraussetzungen den Widerruf der Bestellung zu verlangen, § 38 Abs. 5 Satz 3 BDSG.

Praxishinweis

Interne Datenschutzbeauftragte, die aus dem eigenen Unternehmen heraus rekrutiert werden, üben diese Tätigkeit neben ihrer üblichen Tätigkeit aus. Da der Datenschutzbeauftragte weisungsfrei und unabhängig als Kontrollorgan im Unternehmen agieren muss, sollte davon abgesehen werden, einen Mitarbeiter zu bestellen, der in Interessenkonflikte geraten könnte. Damit sollten insbesondere Mitglieder der Geschäftsführung, Rechtsabteilung oder Revision, Leiter der Abteilungen IT, Human Resources und Vertrieb nicht benannt werden. Dies kann auch für Mitarbeiter aus diesen Abteilungen gelten, da in der Konsequenz durch diese Mitarbeiter der Leiter kontrolliert werden müsste. Viele Unternehmen sehen inzwischen aufgrund des wirtschaftlichen Aufwands und der Unkündbarkeit davon ab, interne Datenschutzbeauftragte zu benennen. Da sich allerdings ein großer Markt für externe Datenschutzbeauftragte gebildet hat, die befristet bestellt werden können, bieten sich durchaus interessante Alternativen. Der externe Datenschutzbeauftragte hat jedoch häufig das Problem, nicht genügend im Unternehmen integriert zu sein. Daher ist es hier erforderlich, zumindest einen Datenschutzansprechpartner im Unternehmen zu benennen, der Auge und Ohr des Datenschutzbeauftragten ist und sicherstellt, dass die Informationsflüsse korrekt verlaufen.

4.1.5 Verpflichtung auf das Datengeheimnis

§ 5 BDSG sieht vor, dass Personen, die bei der Datenverarbeitung beschäftigt sind, mit Aufnahme ihrer Tätigkeit auf die Einhaltung des Datengeheimnisses zu verpflichten sind. Dazu zählt es, personenbezogene Daten nicht unbefugt zu erheben, zu verarbeiten oder zu nutzen. Ein Verstoß gegen diese Verpflichtung kann arbeitsrechtliche Sanktionen nach sich ziehen; daneben kann die unbefugte Verarbeitung von Daten sowohl für den Täter als auch für das Unternehmen als verantwortliche Stelle zu den oben unter Ziff. 3.2 und 3.3 benannten Konsequenzen führen.

Die Verpflichtung hat persönlich zu erfolgen und muss eine Belehrung über die damit einhergehenden Rechte und Pflichten beinhalten.[27] Zum Nachweis empfiehlt sich eine schriftliche Verpflichtung.[28] Unterbleibt die Belehrung, befindet sich der Beschäftigte ggf.

tragten Deutschland e. V.: Das Berufliche Leitbild der Datenschutzbeauftragten, abrufbar unter: https://www.bvdnet.de/dokumente/bvd_leitbild.pdf.

[26] Vgl. bspw. die Angebote der GDD, der DEKRA oder des TÜV Rheinland.

[27] Vgl. *Walz,* in: Simitis, BDSG, 7. Aufl. 2011, § 5 Rn. 28 f.

[28] Dieser kommt insbesondere zum Tragen, wenn dem Mitarbeiter wegen unbefugter Datenverarbeitung arbeitsrechtliche Konsequenzen drohen, vgl. zur Kündigung: LAG Köln v. 29.9.1982 – 5 Sa

in einem unvermeidbaren Verbotsirrtum und geht ggf. straflos aus.[29] Die Verpflichtung zur Einhaltung des Datengeheimnisses erstreckt sich über das Ende der Tätigkeit hinaus (§ 5 Satz 3 BDSG).

Der angesprochene Personenkreis ist weit zu fassen: Jeder, der faktisch die Möglichkeit hat, Zugang zu personenbezogenen Daten zu erlangen, ist zu verpflichten.[30] Damit sind nicht nur bspw. Mitarbeiter der Personalabteilung erfasst, sondern auch das Wartungs- oder sogar das Reinigungspersonal.[31]

Praxishinweis

Es ist organisatorisch sicherzustellen, dass die entsprechenden Erklärungen eingeholt und archiviert werden. Dabei ist nicht nur die Personalabteilung bspw. bei Einstellung eines Mitarbeiters aufgefordert, eine entsprechende Erklärung einzuholen; auch Abteilungen wie bspw. der Einkauf sollten angewiesen werden, bei bspw. Abschluss eines Wartungsvertrages oder bei der Beauftragung einer Reinigungsfirma Verpflichtungserklärungen von diesen zu verlangen.

4.1.6 Technische und organisatorische Maßnahmen

§ 9 BDSG sieht in Verbindung mit der Anlage 1 zu § 9 Satz 1 BDSG verschiedene technische und organisatorische Maßnahmen vor, die es seitens des Unternehmens einzuhalten gilt.[32] Die Maßnahmen betreffen die Bereiche der Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags-, und Verfügbarkeitskontrolle sowie die Einhaltung des Trennungsgebots, d. h. der Sicherstellung, dass die zu unterschiedlichen Zwecken erhobenen Daten getrennt verarbeitet werden. Daneben ist als Maßnahme des Zugangs, Zugriffs und der Weitergabe vom Gesetzgeber explizit der Einsatz von aktuellen Verschlüsselungsverfahren benannt, letzter Satz der Anlage zu § 9 Satz 1 BDSG.

In der Regel erfolgt die Umsetzung durch die IT-Abteilung, die die Einhaltung der Maßnahmen in Zusammenarbeit mit dem Datenschutzbeauftragten überwacht.

Selbstverständlich sollte jedes Unternehmen bereits aus Eigeninteresse heraus den höchstmöglichen Sicherheitsstandard anstreben. Da jedoch nicht jede Datenverarbeitung

514/82, DB 1983, 124 f.; LAG Chemnitz v. 14.7.1999 – 2 Sa 34/99, RDV 2000, 177; VG Frankfurt v. 22.8.2000 – 23 L 1642/00 (V), RDV 2000, 279 ff.; LAG Berlin v. 10.7.2003 – 16 Sa 545/03, RDV 2004, 129 f. LAG Köln v. 14.05.2010 – 4 Sa 1257/09, Gola/Schomerus, BDSG, 11. Aufl. 2012, § 5 Rn. 3.

[29] Vgl. *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2010, § 5, Rn. 15.

[30] Vgl. *Walz,* in: Simitis, BDSG, 7. Aufl. 2011, § 5 Rn. 13 ff.

[31] Vgl. *Walz,* in: Simitis, BDSG, 7. Aufl. 2011, § 5 Rn. 15; *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2010, § 5, Rn. 5; einschränkend: *Gola*, in: Gola/Schomerus, BDSG, 11. Aufl. 2012, § 5 Rn. 9.

[32] Praktische Tipps zur IT-Sicherheit sind bspw. bei dem Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein im Rahmen des IT-Magazins „backUP" unter https://www.datenschutzzentrum.de/backup-magazin/index.htm abrufbar.

gleich hohe Risiken für die Betroffenen nach zieht, sind nur die Maßnahmen zu ergreifen, deren Umsetzung einen im Verhältnis zu dem angestrebten Schutzzweck angemessenen Aufwand verursacht, § 9 Satz 2 BDSG. Aufwand wird dabei mit Kosten gleichgesetzt.[33] Ein Unternehmen, das bspw. im Rahmen medizinischer Forschung Gesundheitsdaten von Patienten verarbeitet wird strengere – und damit auch kostenintensivere – Maßnahmen ergreifen müssen als ein Unternehmen, das lediglich aus Telefonbüchern Adressen zusammenstellt und an Dritte verkauft. Dabei unterliegt nur der Umfang, aber nie die Umsetzung der Maßnahmen an sich der Verhältnismäßigkeitsprüfung. Fraglich ist daher nie das „Ob" der Umsetzung, sondern nur das „Wie". Die Maßnahmen unterliegen der Kontrolle der Datenschutzaufsichtsbehörden, die die Umsetzung kontrollieren, anordnen und untersagen dürfen. Daneben können sie bei Zuwiderhandlungen Zwangsgelder verhängen, § 38 Abs. 5 BDSG. (siehe dazu bereits Ziff. 3.3).

Praxishinweis

Unternehmen sollten vor Aufnahme der jeweiligen Datenverarbeitung eine Risikoanalyse durchführen, welche Datensicherungsmaßnahmen tatsächlich sinnvoll und wirtschaftlich angemessen umsetzbar sind. Die im IT-Grundschutzkatalog des Bundesamtes für Sicherheit und Informationstechnik (BSI) aufgezählten Grundsätze können dabei als Ausgangsbasis für die Umsetzung der mindestens notwendigen Datensicherungsmaßnahmen dienen.[34]

Setzen Unternehmen Auftragnehmer zur Durchführung ihrer Datenverarbeitung ein (so genannte „Datenverarbeitung im Auftrag" gemäß § 11 BDSG, bspw. bei Personalabrechnungen, Inanspruchnahme von Unternehmen zur Durchführung von Rechenzentrumsdienstleistungen siehe Ziff. 4.2.4) sollte der abzuschließende Auftragsdatenverarbeitungsvertrag eine entsprechende Verpflichtung des Auftragnehmers zur Umsetzung dieser Maßnahmen nebst geeigneten Kontrollmaßnahmen der Datenverarbeitungen zugunsten des Auftraggebers vorsehen. Seit dem 1.9.2009 haben sich die Unternehmen in ihrer Funktion als Auftraggeber vor Beginn der Auftragsdatenverarbeitung und sodann regelmäßig davon zu überzeugen, dass der Auftragnehmer ebenfalls die in § 9 BDSG und der Anlage zu § 9 Satz 1 BDSG geforderten Maßnahmen umsetzt, § 11 Abs. 2 BDSG. Das Unterlassen der Kontrollen gilt als Ordnungswidrigkeit, § 43 Abs. 1 Nr. 2b BDSG und kann mit einem Bußgeld bis zu 50,000.00 € bestraft werden. Unternehmen sollten daher Prozesse zur Prüfung der Auftragnehmer festlegen.

[33] Vgl. *Ernestus,* in: Simitis, BDSG, 7. Aufl. 2011, § 9 Rn. 23 ff.

[34] Vgl. dazu auch die von dem Bundesamt für Sicherheit und Informationstechnik (BSI) empfohlenen datenschutzrechtlichen Maßnahmen, die der Sicherheit dienen; die tabellarische Aufstellung der möglichen Maßnahmen abrufbar unter: http://www.bsi.de/gshb/bausteindatenschutz; Die Beschreibung der Maßnahmen bzw. die Maßnahmenkataloge sind abrufbar unter: http://www.bsi.de/gshb/deutsch.

4.2 Rechtskonforme Datenverarbeitung

4.2.1 Allgemeines

Ordnungsgemäße Datenverarbeitung im Unternehmen erfordert nicht nur die Erfüllung der formellen Anforderungen, die das BDSG dem für die Datenverarbeitung Verantwortlichen auferlegt – wesentlich ist auch die Einhaltung der so genannten „materiellen" Datenverarbeitungsvoraussetzungen: Das Erheben, Speichern, Verarbeiten und Nutzen von personenbezogenen Daten ist nur unter bestimmten Voraussetzungen erlaubt.

So sieht bspw. § 4 Abs. 1 BDSG vor, dass entweder eine Vorschrift des BDSG oder eine andere Rechtsvorschrift die Verarbeitung bzw. Nutzung erlauben/anordnen muss. Neben den gesetzlichen Erlaubnistatbeständen gelten auch Betriebsvereinbarungen als Rechtsvorschriften im Sinne des BDSG. Daher kann auch diese eine Datenverarbeitung legitimieren.[35] Alternativ kann von demjenigen, dessen Daten verarbeitet oder genutzt werden, eine freiwillige, bewusste und in der Regel schriftliche Einwilligung gemäß § 4a BDSG für die geplanten Zwecke der Datenerhebung etc. eingeholt werden.[36]

4.2.2 Gesetzliche Erlaubnistatbestände

Gesetzlich erlaubt ist eine Verarbeitung u. a. für eigene Geschäftszwecke, wenn es für die Begründung, Durchführung oder Änderung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit einem Betroffenen erforderlich ist. Dazu zählt bspw. die Erfüllung vertraglicher Zwecke, so etwa die Abwicklung von Kundenbestellungen auf der Basis von Kaufverträgen[37] oder auch die Erhebung von Daten im Rahmen der Vertragsanbahnung oder der Mitgliedschaft in einem Verein (vgl. § 28 Abs. 1 Satz 1 Nr. 1 BDSG).[38]

Mitunter setzen die gesetzlichen Erlaubnistatbestände für Datenverarbeitungen Wertungen im Einzelfall voraus: Erlaubt ist eine Datenverarbeitung bspw. dann, wenn die Interessen des Unternehmens an der Übermittlung von Daten höher zu werten sind als die

---

[35] Hier sollte darauf geachtet werden, dass das Datenschutzniveau des BDSGs nicht unterschritten wird; im Gegensatz zu den arbeitsrechtlichen Stimmen halten Datenschutzaufsichtsbehörden in der Regel Betriebsvereinbarungen, die Regelungen zu Lasten der Betroffenen vorsehen, als nicht wirksam. In diesem Fall stellen diese keine geeignete Rechtsgrundlage für den Umgang mit den Beschäftigtendaten dar.

[36] Vgl. bspw. zu den Voraussetzungen der Datenverarbeitung in Unternehmen: *Roßnagel*, in: Handbuch Datenschutzrecht, 2003, S. 485 ff.; *Tinnefeld/Ehmann/Gerling*, in: Einführung in das Datenschutzrecht, 4. Aufl. 2005, S. 539 ff.; vgl. ausführlich zu den Voraussetzungen einer wirksamen Einwilligung: *Bergmann/Möhrle/Herb*, BDSG, Loseblatt, Stand: Januar 2012, § 4a, Rn. 3a ff.

[37] Vgl. mit Bsp. zu einzelnen Vertragsverhältnissen: *Bergmann/Möhrle/Herb*, BDSG, Loseblatt, Stand: Januar 2012, § 28, Rn. 30 ff.

[38] Vgl. mit weiteren Bsp.: *Bergmann/Möhrle/Herb*, BDSG, Loseblatt, Stand: Januar 2012, § 28, Rn. 200 ff.

schutzwürdigen Interessen des Betroffenen am Unterlassen der Übermittlung (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG bzw. § 28 Abs. 2 Nr. 2 BDSG).[39]

§ 28 Abs. 3 BDSG regelt im Übrigen, unter welchen Voraussetzungen Kundendaten für Marketing-Zwecke genutzt werden dürfen. Während ein Unternehmen Bestandskunden zumindest per Post unter bestimmten Voraussetzungen Werbung zukommen lassen darf, ist bei Neukunden in der Regel eine freiwillige, bewusste und ausdrückliche Einwilligung erforderlich. Die Einwilligung ist schriftlich zu erteilen bzw. elektronisch.[40] Eine Ausnahme gilt, wenn die Daten allgemein zugänglichen Verzeichnissen, wie dem Telefonbuch, entnommen werden. Jedenfalls muss der Kunde über sein Recht zum Widerspruch belehrt werden.[41]

Besondere Regelungen bestehen im Übrigen für die Übermittlung von Daten an Auskunfteien, § 28a BDSG. Hier dürfen nur noch bestimmte Daten eingemeldet werden (bspw. Forderungen, die durch ein rechtskräftiges Urteil bestätigt wurden oder wenn der Kunde die Forderungen ausdrücklich anerkannt hat), um die Kunden zu schützen und dem Umstand Rechnung zu tragen, dass in der Vergangenheit unreflektiert Daten bspw. bereits im Fall einer ersten Mahnung an die SCHUFA gemeldet wurden und dies naturgemäß negative Konsequenzen für die jeweils Betroffenen nach sich gezogen hat.

Das gleiche Ziel verfolgen die expliziten Regelungen für Scoring (§ 28b BDSG), die insbesondere umfassende Informationspflichten vorsehen und für die geschäftsmäßige Datenverarbeitung, wie Adresshandel und Markt-und Meinungsforschung (§§ 29, 30, 30a BDSG). In letzteren Fällen sind vor allem die Widerspruchsrechte der Kunden erheblich gestärkt worden und es wurde hervorgehoben, dass die Anonymisierung von Daten vorzugswürdig ist.

Aufgrund der Skandale der Vergangenheit im Bereich des Arbeitnehmerdatenschutzes hat der Gesetzgeber eine spezielle Regelung für die Verarbeitung etc. von Beschäftigtendaten eingeführt, § 32 BDSG (siehe dazu unten unter Ziffer 4.2.3).

Neben den Regelungen des BDSG sind insbesondere im Bereich des Online-Handels etc. die datenschutzrechtlichen Vorgaben des Telemediengesetzes zu beachten: Danach dürfen bspw. Profile von Besuchern einer Webseite in pseudonymisierter Form erstellt werden oder Kundendaten nicht ohne weiteres für Werbezwecke genutzt werden. [42]

---

[39] Vgl. *Bergmann/Möhrle/Herb*, BDSG, Loseblatt, Stand: Januar 2012, § 28, Rn. 226 ff.

[40] In diesem Fall sind weitere Voraussetzungen zu beachten (bspw. Protokollierung, dauerhafte Abrufbarkeit); zusätzlich sind – sofern die Einwilligungen auf einer Webseite eingeholt werden, auf der Telemediendienste angeboten werden, die Anforderungen des Telemediengesetzes beachtlich. Telemediendienste sind bspw. Informationsseiten, Webshops, Newsletterdienste u. ä.

[41] Vgl. mit weiteren Bsp.: *Bergmann/Möhrle/Herb*, BDSG, Loseblatt, Stand: Januar 2012, § 28, Rn. 310 ff., Bauer, Datenschutz und Marketing, in: Oelschlaegel/Scholz (Hrsg.), Handbuch zum Versandhandelsrecht – E-Commerce, M-Commerce, Katalog, 2012; Drewes, ZD 2011, S.115;Roßnagel/Jandt, MMR 2011, S. 86.

[42] Vgl. bspw. die Empfehlungen des Unabhängigen Landeszentrum für Datenschutz, abrufbar unter: https://www.datenschutzzentrum.de/tracking/piwik/

4.2.3 Arbeitnehmerdatenschutz

Während auf der einen Seite die Mitarbeiter wesentlich zur Einhaltung datenschutzrechtlicher Compliance beitragen müssen, ist auf der anderen Seite das Unternehmen in seiner Funktion als Arbeitgeber gleichfalls angehalten, bestimmte Spielregeln zu beachten. Gerade die Skandale der Vergangenheit haben jedoch gezeigt, dass im Bereich des Arbeitnehmerdatenschutzes erheblicher Verbesserungsbedarf besteht. Insbesondere der Bereich der Arbeitnehmerüberwachung ist daher in die Kritik geraten: Ob heimliche Überwachung per Video oder GPRS, Kontrolle von E-Mails oder Telefonüberwachung, Gentests oder auch der Einsatz von Detektiven – die Möglichkeiten, Arbeitnehmer in ihren Persönlichkeitsrechten zu verletzen, sind vielfältig.[43] Auch wenn die Unternehmen durchaus berechtigte Interessen – wie die Prävention oder Bekämpfung von Wirtschaftskriminalität– verfolgen, sind ihren Tätigkeiten durch die geltenden Gesetze, wie dem BDSG, dem Telekommunikationsgesetz oder auch dem Grundgesetz deutliche Grenzen gesetzt.[44]

Ein erster Schritt in Richtung Schutz der Arbeitnehmer war die Einführung des § 32 BDSG in 2009, der die Erhebung, Verarbeitung etc. von Beschäftigtendaten u. a. erlaubt, wenn dies für Zwecke der Begründung, Durchführung oder Beendigung des Beschäftigtenverhältnisses erforderlich ist. Daneben dürfen personenbezogene Daten von Beschäftigten zur Aufdeckung von Straftaten genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung und Nutzung zur Aufdeckung der Straftat erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung etc. nicht überwiegt, § 32 Abs. 1 Satz 2 BDSG. Daneben darf Art und Ausmaß der Maßnahme im Hinblick auf den Anlass nicht unverhältnismäßig sein.

§ 32 BDSG war heftiger Kritik ausgesetzt, da er u. a. nach seinem Wortlaut präventive Maßnahmen, wie bspw. vorbeugende Maßnahmen zur Korruptionsbekämpfung nicht zulässt. Gleiches gilt für die Verfolgung von Ordnungswidrigkeiten etc.[45] Inzwischen ist weitgehend anerkannt, dass sich entsprechende Maßnahmen entweder über § 32 Abs. 1 Satz 1 BDSG rechtfertigen lassen, da sie als erforderlich erachtet werden, um zu prüfen, ob der Beschäftigte seinen arbeitsvertraglichen Pflichten nachkommt oder im Rahmen einer alternativen Argumentation über § 28 Abs. 1 Nr. 2 BDSG, da diese Daten für Zwecke

---

[43] Vgl. *Freckmann/Wahl,* BB 2008, 1904 ff.; weiterführend zum Arbeitnehmerdatenschutz: *Gola/Wronka*, in: Handbuch zum Arbeitnehmerdatenschutz, 5. Aufl. 2009, Rn. 48 ff.; *Oberwetter,* NZA 2008, 609 ff.

[44] Vgl. *Bauer*, Datenschutzpraxis 5/09, 1 ff.; *Bull,* ZRP 2008, 233 ff.; *Dann/Gastell*, NJW 2008, 2945 ff.; *Gola*, NZA 2007, 1139 ff.; siehe auch zum IT-Grundrecht und dem daraus resultierenden Schutz des Allgemeinen Persönlichkeitsrechts des Arbeitnehmers: BVerfG v. 27.2.2008–1 BvR 370/07 und 1 BvR 595/07, ZUM 2008, 301.

[45] Vgl. statt vieler aus jüngster Zeit: Albrecht/Maisch, DSB 3/2010, 11 ff.; Behling, BB 2010, 892 ff.; Beisenherz/Tinnefeld, DuD 2010, 221 ff.; Bierekoven, CR 2010, 203 ff., Forst, RDV 2010, 8 ff.; Kamp/Körffer, RDV 2010, 72 ff.; Kramer, DSB 5/2010, 14 ff.; Salvenmoser/Hauschka, NJW 2010, 331 ff.; vgl. auch die Beiträge von Däubler, Gläserne Belegschaften, 5. Aufl., Rdnr. 183; Gola/Wronka, Hdb. zum Arbeitnehmerdatenschutz, 5. Aufl., Rn. 847 ff.

neben dem Beschäftigtenverhältnis (bspw. Korruptionsbekämpfung, Verpflichtung des Arbeitgebers zur Einführung von Internen Kontrollsystemen, Haftung der Geschäftsführung bei Unterlassen von Kontrollen) genutzt werden und berechtigte Interessen des Arbeitgebers bestehen, hinter denen die schutzwürdigen Interessen des Betroffenen zurücktreten müssen. Gleichwohl müssen alle Maßnahmen verhältnismäßig sein, d. h. es muss das jeweils mildeste Mittel zur Erreichung des gewünschten Zwecks verwendet werden (bspw. erst anonyme Kontrollen, dann pseudonyme Kontrollen und bei Erhärtung von Verdachtsmomenten gezielte personenbezogene Kontrollen).[46] Dazu kommt, dass die Datenschutzaufsichtsbehörden einen eher konservativen Ansatz vertreten und der oben genannten Argumentation nicht zwingend folgen. Insofern bestehen durchaus Restrisiken.

Praxishinweis

Es empfehlen sich vor der Durchführung entsprechender Kontrollen sorgfältige Rechtmäßigkeitsprüfungen durch den Datenschutzbeauftragten im Einzelfall; dieser sollte kritisch prüfen, ob der Verhältnismäßigkeitsgrundsatz eingehalten wird. Daneben sollte ein Prozess festgelegt werden, wer wie wann welche Kontrollen vornimmt und wie im Einzelfall damit umzugehen ist. Dazu zählen auch Richtlinien zur Speicherung und Löschung der Daten. Besteht ein Betriebsrat, empfiehlt sich der Abschluss einer entsprechenden Betriebsvereinbarung, die in der Regel sogar zwingend abzuschließen ist, da Leistungs- und Verhaltenskontrollen mittels technischer Systeme erfolgen.

Über die Verhältnismäßigkeitsprüfungen des § 32 BDSG hinaus sind Sondervorschriften beachtlich, die auch vor Durchführung entsprechender Überwachungsmaßnahmen eine sorgfältige Rechtmäßigkeitsprüfung durch den Datenschutzbeauftragten bzw. eine entsprechende Person im Unternehmen voraussetzen. Bspw. sollte kritisch geprüft werden, ob

- die in § 6b BDSG vorgesehenen Vorgaben zur Videoüberwachung eingehalten werden;
- die in § 6c BDSG vor Einführung einer mobilen bspw. Chipkarte der Betroffene nicht nur über den Datenverarbeiter, sondern auch über die Funktionsweise, die Art der verarbeiteten Daten, seine Rechte auf Löschung etc. und ggf. Maßnahmen bei Verlust oder Zerstörung unterrichtet wird;
- die Kontrolle von E-Mails und Internetzugriffen der Mitarbeiter nicht gegen das Telekommunikationsgeheimnis nach §§ 88 ff. Telekommunikationsgesetz verstößt;
- Überwachungsmaßnahmen auf Grundlage konkreter Verdachtsmomente erfolgen und stets das mildeste Mittel zur Erreichung des jeweiligen Zwecks sind;
- die Einschaltung Dritter, wie bspw. Detekteien, auf Grundlage der erforderlichen Verträge erfolgt;
- besondere personenbezogene Daten nur in den engen rechtlich zulässigen Grenzen verarbeitet werden.

[46] Vgl. ausführlich zu der Thematik: Thüsing, Arbeitnehmerdatenschutz und Compliance, 2010.

Aufgrund der Defizite im Bereich des Arbeitnehmerdatenschutzrechts wird seit knapp zehn Jahren immer wieder die Einführung eines gesonderten Arbeitnehmerdatenschutzgesetzes verlangt. Der Gesetzgeber hat in 2009 einen Entwurf für ein Beschäftigtendatenschutzrecht vorgelegt, der heftig kritisiert[47] und mehrfach überarbeitet wurde.[48] Im November 2012 soll dieser Entwurf erneut diskutiert werden; gleichwohl wird keine Verabschiedung erwartet.

Dabei sind insbesondere die Entwicklungen auf europäischer Ebene von Relevanz: Die Europäische Kommission hat in 2012 entschieden, dass in Europa künftig eine einheitliche Datenschutzgrundverordnung gelten soll, die unmittelbar in den Mitgliedstaaten der Europäischen Union Anwendung finden wird. Ein erster Entwurf wurde vorgelegt und wird zurzeit durch die Gremien geprüft.[49] Zwar sieht der Entwurf ausdrücklich vor, dass die Regelung des Arbeitnehmerdatenschutzes den Mitgliedsstaaten überlassen bleiben soll; allerdings werden sich diese Regelungen an der Datenschutzgrundverordnung orientieren müssen, so dass spätestens mit der Einführung der Verordnung, die wohl für 2017 zu erwarten ist, eine Überarbeitung erforderlich wäre.

Insofern stellt sich zurzeit die Frage, ob eine Einführung des geplanten Beschäftigtendatenschutzrechts allein für die Zwischenzeit sinnvoll ist. Dabei ist auch zu berücksichtigen, dass Unternehmen ihre Prozesse umstrukturieren bzw. neue Prozesse einführen müssten, damit sie die Anforderungen der geplanten §§ 32–32m BDSG-Entwurf erfüllen können. Sowohl der Umgang mit Bewerberdaten als auch mit Beschäftigtendaten, insbesondere die Prozesse betreffend die Kontrolle von Bewerbern und Beschäftigten, die Information von Bewerbern und Beschäftigten sowie der Umgang mit Betriebsvereinbarungen wären anzupassen. Daneben ist zurzeit noch in der Diskussion, ob und in welchem Umfang Einwilligungen von Beschäftigten künftig noch möglich sein sollen.

Praxishinweis

Es empfiehlt sich für Unternehmen bereits jetzt, sich mit den kommenden Veränderungen auseinanderzusetzen und zumindest den Status-Quo des Datenschutzniveaus festzustellen. So können Defizite sowie Handlungsbedarf identifiziert und die Umsetzung der dann erforderlichen Prozesse beschleunigt werden.

---

[47] Vgl. Thüsing, RDV 2010, 147 ff., Tinnefeld/Petri/Brink, MMR 2010, 727, Forst NZA 2010, 1043.

[48] Vgl. BR-Drs. 535/10, BT-Drs. 17/4230, BT-Drs. 17/4853, Gesetzentwürfe SPD-Fraktion, BT-Drs. 17/69; Fraktion Bündnis 90/Die Grünen, BT-Drs. 17/121, BT-Drs. 17/4853 und Fraktion Die Linke, BT-Drs. 17/779.

[49] Vgl. Europäische Kommission, Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum Schutz des freien Datenverkehrs (Datenschutz-Grundverordnung – DS-GVO), Kom (2012) 11 endg.; siehe auch die negative Haltung der Bundesregierung vom 26.7.2010, RDV 2011, 157 und Stellungnahme des Bundesrates vom 11.2.2011 (BR-Drs. 707/10); vgl. auch Hornung, ZD 2012, 99, Wybitul/Fladung, BB 2012, 509.

4.2.4 Austausch von Daten

Grundlagen

Auch der Austausch von Daten zwischen verschiedenen Unternehmen bedarf einer Rechtsgrundlage: Die Übermittlung muss daher bspw. für die Durchführung des Vertrages mit dem Kunden erforderlich sein. Dies ist u. a. der Fall, wenn die Daten an einen Lieferanten für Zwecke der Auslieferung bestellter Ware übermittelt werden. Alternativ kann auch die Einwilligung des Betroffenen als Legitimation eingeholt werden.

Auftragsdatenverarbeitung

Ist der Empfänger der Daten als Auftragnehmer anzusehen, der im Sinne des § 11 BDSG im Rahmen einer Auftragsdatenverarbeitung tätig wird, bedarf es lediglich eines schriftlichen Auftragsdatenverarbeitungsvertrages, der die inhaltlichen Anforderungen des § 11 BDSG erfüllt. Dazu müssen u. a. die Zwecke der Datenverarbeitung, die übermittelten Daten, die vom Auftragnehmer umgesetzten technisch-organisatorischen Maßnahmen, Regelungen, wie der Auftragnehmer von dem Auftraggeber kontrolliert wird, welche Regelungen bei Vertragsbeendigung gelten sollen und ob Subunternehmer eingesetzt werden dürfen. Eine Auftragsdatenverarbeitung liegt u. a. vor, wenn der Auftragnehmer streng nach Weisung des Auftraggebers die Daten verarbeitet, die Daten Eigentum des Auftraggebers bleiben und der Auftragnehmer dem Auftraggeber lediglich einen Teil der Datenverarbeitung etc. abnimmt. Der Auftraggeber bleibt der „Herr der Daten" und damit für die Zulässigkeit der Datenverarbeitung gegenüber den Datenschutzaufsichtsbehörden und den Betroffenen verantwortlich. Daher obliegen ihm bestimmte Kontrollpflichten des Auftragnehmers, die er vor Beginn der Übergabe der Daten und sodann regelmäßig durchzuführen hat.

Verstöße gegen die Schriftform und das Unterlassen der Kontrollen können seit dem 1.9.2009 als Ordnungswidrigkeit geahndet werden.[50]

Praxishinweis

Es ist sorgfältig zu prüfen, ob das Unternehmen die erforderlichen Auftragsdatenverarbeitungsverträge abgeschlossen hat. Da die Regelung auch für Verträge gilt, die vor dem 1.9.2009 abgeschlossen wurden, besteht ein nicht unerhebliches Risiko, dass diese nicht in jedem Fall von der verantwortlichen Stelle abgeschlossen wurden bzw. nicht die inzwischen erforderlichen Regelungen beinhalten.

Daneben ist durch geeignete Prozesse sicherzustellen, dass der Auftraggeber sich von der Einhaltung der vertraglichen Vereinbarungen und der Umsetzung der technisch-organisatorischen Maßnahmen bei dem Auftragnehmer überzeugt; hier empfehlen sich Checklisten o. ä. sowie Kontrollbesuche. Alternativ wird auch häufig von Auftraggebern akzeptiert, dass der Auftragnehmer ein Zertifikat vorlegt, mittels dem eine neutrale Stelle (bspw. ein Wirtschaftsprüfer) die Einhaltung des Datenschutzes, der erforderlichen technisch-organisatorischen Maßnahmen etc. bestätigt.

[50] Vgl. Gaulke, DuD 2011, S. 417.

Übermittlung in unsichere Drittstaaten

Besonders kritisch ist daneben die Übermittlung von Daten in Länder, die kein angemessenes Datenschutzniveau aufweisen.[51] Dazu zählen Länder außerhalb des Europäischen Wirtschaftsraums und Länder, deren Datenschutzniveau nicht von der EU als angemessen anerkannt wurde; die EU hat bspw. Kanada, die Schweiz, Israel oder auch Argentinien als sichere Staaten anerkannt. Ansonsten ist die Übermittlung grundsätzlich verboten und nur in Ausnahmefällen gestattet ist, §§ 4b, 4c BDSG. Als Ausnahme gelten bspw. die Einwilligung des Betroffenen, die Teilnahme des Datenimporteurs mit Sitz in den USA am so genannten Safe-Harbor-Programm oder der Abschluss von so genannten EU-Standardvertragsklauseln zwischen Datenexporteur und -importeur.[52]

Praxishinweis

Nehmen amerikanische Unternehmen an dem Safe-Harbor-Programm teil, können sie mittels der Teilnahme nachweisen, dass sie ein angemessenes Datenschutzniveau einhalten. Erforderlich ist dazu eine Zertifizierung, die sie selbst vornehmen. Die deutschen Datenschutzaufsichtsbehörden verlangen – da sie diese Selbstzertifizierung anzweifeln – zusätzliche Garantien dieser Unternehmen. Vor einer Übermittlung sollte der Exporteur der Daten daher nachfragen, wie lange die Zertifizierung zurückliegt[53], ob der Datenimporteur die Grundsätze von Safe Harbor einhält und wie er seinen Informationspflichten gegenüber den Betroffenen nachkommt. Der Datenimporteur hat gemäß dem Notice-Princip der Grundsätze Privatpersonen darüber zu informieren, zu welchem Zweck personenbezogene Daten erhoben und verwendet werden, auf welchen Wegen etc. sich Betroffene mit Nachfragen und Beschwerden an den Datenimporteur wenden können und an welche Dritte die Daten weitergegeben werden. Der Datenexporteur muss dokumentieren, dass er die entsprechenden Informationen eingeholt hat und dies auf Verlangen den Datenschutzaufsichtsbehörden vorlegen. Andernfalls gilt die Safe-Harbor-Zertifizierung nicht als Legitimation des Transfers der Daten in die USA.[54]

Austausch von Daten in Konzerngruppen

Konzernunternehmen können sich im Übrigen nicht darauf berufen, dass sie Teil eines Konzerns sind und daher keine Rechtsgrundlage o. ä. für die Übermittlung erforderlich wäre. Alle Unternehmen gelten im Verhältnis zueinander als Dritte. Ein Konzernprivileg

[51] Vgl. Wybitul/Patzak, RDV 2011, S. 11.

[52] Siehe dazu bspw. *Gola*, in: Gola/Schomerus, BDSG, 11. Aufl. 2012, § 4c Rn. 10 ff.; hinsichtlich der Problematik der Nutzung von Clouds: Engels, K&R 2011, S. 548; vgl. zur internationalen Auftragsdatenverarbeitung: Scholz/Lutz, CR 2011, S. 424.

[53] Liegt die Zertifizierung mehr als sieben Jahre zurück, ist sie nicht mehr gültig.

[54] Siehe dazu: https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Pruefung_der_Selbst-Zertifizierung_des_Datenimporteuers/Beschluss_28_29_04_10neu.pdf.

besteht nicht. Daher müssen sie die Rechtsgrundlagen zum Austausch der Daten genauso schaffen, wie es im Verhältnis zu Unternehmen, die nicht der Konzerngruppe angehören, der Fall wäre.

Praxishinweis

Die Globalisierung fordert von vielen Unternehmen den internationalen Austausch von Daten im Konzernverbund. Gleichwohl ist dieser Austausch nur auf Basis einer Rechtsgrundlage zulässig. Insbesondere ist sorgfältig zu prüfen, ob eine Austausch von Arbeitnehmerdaten tatsächlich über § 32 BSDG oder ggf. über § 28 Abs. 1 Nr. 2 BDSG gerechtfertigt sein kann. Dies ist in der Regel nur in Ausnahmefällen zulässig (bspw. wenn ein internationaler Arbeitsvertrag geschlossen wurde, die Muttergesellschaft verbindliche Entscheidungen über bspw. die Gehälter der Arbeitnehmer trifft oder Outsourcing im Rahmen einer Auftragsdatenverarbeitung erfolgt ist). Die Zwecke der Übermittlung sind sorgfältig zu prüfen. Der Datenschutzbeauftragte sollte die Einführung von solchen internationalen HR-Systemen unbedingt begleiten; daneben ist die Einbindung des Betriebsrats erforderlich.

Dies gilt im Übrigen nicht nur für den Bereich von Arbeitnehmerdaten sondern auch von Kundendaten: Auch diese dürfen nicht ohne weiteres an Dritte bzw. andere Konzerngesellschaften übermittelt werden.

Daneben sind die datenschutzrechtlichen Vorgaben selbstverständlich auch zu beachten, wenn entsprechend dem neuesten Trend Daten im Rahmen des Cloud-Computings an einen Datenverarbeiter übermittelt werden. Ob und in welchem Umfang dies zulässig ist, wird zurzeit stark diskutiert. Erwartungsgemäß stellen sich die Datenschutzaufsichtsbehörden auf einen restriktiven Standpunkt und halten dieses Modell für nicht datenschutzkonform.[55]

4.2.5 Sonderfälle: Tracking-Tools und Social Media

Die Vorgaben des Telemediengesetzes erlauben nur begrenzt den Einsatz von Tracking-Tools, wie bspw. Google Analytics.[56] Google Inc. hat sich in Abstimmung mit dem Hamburgischen Datenschutzbeauftragten für Datenschutz und Informationssicherheit entschieden, die IP-Adressen der Nutzer zu anonymisieren, um den Webseiten- Betreibern eine datenschutzkonforme Nutzung des Tools zu ermöglichen. Um dem Datenschutz

[55] Siehe bspw. die Orientierungshilfe der Datenschutzaufsichtsbehörden: http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf, Wagner/Blaufuß, BB 2012, S. 1751.

[56] Vgl. den Beschluss des Düsseldorfer Kreises von Stralsund vom 26./27. November 2009, betreffend „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“, abrufbar bspw. unter: http://www.lfd.m-v.de/dschutz/beschlue/Analyse.pdf, a. a. O.; dazu auch ausführlich: Informationen des Unabhängigen Landeszentrum für Datenschutz, abrufbar unter https://www.datenschutzzentrum.de/tracking, insbesondere: https://www.datenschutzzentrum.de/tracking/20090123_GA_stellungnahme.pdf, siehe auch *Bauer,* Datenschutzpraxis 6/2009, 6.

gerecht zu werden, wurden daneben die nachfolgenden Voraussetzungen[57] vereinbart, die bei Einsatz des Tools von dem Webseiten-Betreiber zu beachten sind:[58]

- Abschluss eines Auftragsdatenverarbeitungsvertrags mit Google;[59]
- Hinweis sowohl auf die Nutzung des Tools als auch auf die bestehenden Widerspruchsmöglichkeiten gegen die Erfassung der Daten in der auf der Website abrufbaren Datenschutzerklärung des Webseiten-Betreibers; empfehlenswert sei ein Link auf die Seite http://tools.google.com/dlpage/gaoptout?hl=de;
- Verwendung des von Google zur Verfügung gestellten Anonymizers[60] und
- Löschung eventuell vorhandener Altdaten (d. h. von Daten, die nicht unter Beachtung dieser Vorgaben erhoben wurden).

Vorsicht ist auch bei dem Einsatz von Social Media geboten: Der „Gefällt-mir-Button" von Facebook oder der „1 +-Button" von Google werden aus Marketinggründen eingesetzt, obwohl sie datenschutzrechtlich kritisch sind. Nutzer können diese Buttons anklicken und damit zum Ausdruck bringen, dass ihnen die Webseite, der Inhalt etc. gefällt; neben erhöhtem Traffic führt dies zu einem positiven Image und liefert Erkenntnisse über die eigenen Nutzer. Da hier jedoch Daten an Facebook oder auch Google übermittelt werden, ohne dass der Nutzer dem widersprechen oder dies irgendwie verhindern kann, sehen die Datenschutzaufsichtsbehörden hier eine unzulässige Datennutzung. Das bloße Ansehen der Website kann bereits die entsprechende Datenübertragung auslösen und ermöglicht es Facebook, jedwedes Surfverhalten der Nutzer einer Webseite, die den Button enthält, aufzuzeichnen. Damit einhergehend kann auch eine Verknüpfung des Surfverhaltens von Nutzern außerhalb der besuchten Website erfolgen. In der Regel handelt es sich um die URL der Seite sowie die Angabe, ob dem Nutzer die Website gefällt oder nicht. Da das Verfahren letztlich nicht transparent ist und keiner genau weiß, was mit den Daten geschieht, sehen die Datenschutzaufsichtsbehörden darin eine Übermittlung von Daten ohne Rechtsgrundlage und haben deshalb bereits Bußgelder verhängt.[61]

---

[57] Vgl. die unter „http://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_Webseitenbetreiber_in_Hamburg.pdf" abrufbaren Hinweise des Hamburgischen Datenschutzbeauftragten für Datenschutz und Informationssicherheit.

[58] Vgl. zu den für Webseiten-Betreiber resultierenden Risiken: *Bauer,* Datenschutzpraxis 12/2011, 1.

[59] Abrufbar unter: http://www.google.de/intl/de/analytics/tos.pdf.

[60] S. dazu: http://code.google.com/intl/de/apis/analytics/docs/gaJS/gaJSApi_gat.html#_gat._anonymizIp.

[61] Siehe dazu die Entschließung des Düsseldorfer Kreises vom 8.12.2011: https://www.datenschutzzentrum.de/internet/20111208-DK-B-Soziale-Netzwerke.html, ausführliche Informationen zum Streit zwischen den Datenschutzaufsichtsbehörden und Facebook, siehe: https://www.datenschutzzentrum.de/facebook/; die IHK Schleswig-Holstein hat Klage gegen entsprechende Bußgeldbescheide vor dem VG Schleswig erhoben, die Entscheidung wird für Mitte 2013 erwartet. Bis dahin werden wohl keine weiteren Bußgeldbescheide erlassen. Weiterführend statt vieler: *Voigt/Alich*, NJW 2011, 3541, *Ernst,* NJOZ 2010, 1917.

Bei Nutzung der Tools ist daher in der Datenschutzerklärung ausführlich über das Tool zu belehren und es muss ein entsprechendes Widerspruchsrecht vorgesehen werden.[62] Empfehlenswert ist auch, eine 2-Klick-Variante vorzusehen: Der Button ist bei Aufruf einer Seite der Button zunächst deaktiviert und es wird erst nach dem Anklicken des Buttons eine Verbindung zu Facebook hergestellt.[63]

4.2.6 Einbindung der Mitarbeiter

Bereits aus diesen kurzen exemplarischen Beispielen ergibt sich, dass vielfältige Voraussetzungen zu beachten sind, die für jede Fachabteilung sehr unterschiedlich ausgestaltet sein können. Während die Personalabteilung die Verarbeitung von Mitarbeiterdaten ordnungsgemäß gestalten muss, hat die Marketingabteilung vornehmlich Kundendaten zu verwalten.

Das Unternehmen als für die Datenverarbeitung Verantwortlicher hat dafür Sorge zu tragen, dass in jeder Abteilung die vielfältigen materiellen Voraussetzungen erfüllt werden. Es muss sichergestellt sein, dass jeder Mitarbeiter Datenschutzrecht in seiner täglichen Praxis lebt und die Voraussetzungen kennt, unter denen er Daten verarbeiten darf. Damit einhergehend ist das Unternehmen gehalten, seine Mitarbeiter zu schulen und diese in die Lage zu versetzen, die gesetzlichen Anforderungen umzusetzen. Sofern das Unternehmen einen Datenschutzbeauftragten bestellt hat, ist dieser für die Durchführung entsprechender Schulungen verantwortlich.[64] Auch wenn damit nicht jede kriminelle Handlung, wie bspw. gerade in der jüngsten Vergangenheit der unbefugte Verkauf von Kundendaten an Dritte unterbunden werden kann, kann so zumindest das Risiko von Datenschutzverstößen aus Unwissenheit minimiert werden.

Praxishinweis

Mittels der Schulung sollen die Mitarbeiter für die Anforderungen des Datenschutzes sensibilisiert werden. Schulungsinhalte können bspw. im Rahmen einer Basisschulung folgende Kernfragen sein:

- Warum ist es notwendig, Datenschutzrecht zu beachten?
- Wann findet Datenschutzrecht überhaupt Anwendung und was sind personenbezogene Daten?
- Was ist unter einer automatisierten Datenverarbeitung und -nutzung zu verstehen?
- Unter welchen rechtlichen Voraussetzungen dürfen Daten verarbeitet werden?

[62] Vgl. dazu auch die Entscheidung des KG Berlin, Beschl. v. 29.4.2011 – 5 W 88/11, NJW-RR 2011, 1264: Ein Unterlassen der Belehrung ist nicht wettbewerbswidrig, da § 13 TMG keine markschützende Norm nach UWG ist.

[63] Vgl. zum Beispiel: www.hamburg.de/datenschutz/

[64] Siehe zu den verschiedenen Möglichkeiten der Schulung bereits Kapitel *Wecker/Galla*: Pflichten der Geschäftsleitung und Aufbau einer Compliance-Struktur, Ziff. 3.2.2.

- Wann und von wem muss eine Einwilligung in die Datenverarbeitung eingeholt werden und welchen Voraussetzungen unterliegt sie?
- Unter welchen Voraussetzungen darf das Unternehmen Daten für Marketingzwecke verarbeiten?
- Wann liegt eine Übermittlung von Daten vor und unter welchen Voraussetzungen dürfen Daten an wen übermittelt werden? Sind ggf. vertragliche Vereinbarungen abzuschließen?
- Welchen Voraussetzungen unterliegt eine Übermittlung ins Ausland, insbesondere in das außereuropäische Ausland?
- Welche Rechte hat ein Mitarbeiter, ein Kunde etc., dessen Daten durch das Unternehmen verarbeitet werden?
- Welche technischen und organisatorischen Maßnahmen sind für eine ordnungsgemäße Verarbeitung und Nutzung von Daten einzuhalten?
- In welchem Umfang dürfen Mitarbeiter die IT-Betriebsmittel (Smartphone, Laptop, iPad, PC, etc.) nutzen?
- Welche Vorgaben bestehen für die Nutzung von Social-Media?
- Welche Risiken bestehen bei einer unzulässigen Datenverarbeitung?

Neben der Grundlagenschulung empfiehlt sich eine bereichsspezifische Schulung der Mitarbeiter, bspw. sollten Mitarbeiter aus dem Personalbereich gezielt im Umgang mit Mitarbeiterdaten sensibilisiert werden, während Mitarbeiter im Bereich IT ausführlich im Bereich Umsetzung von technisch/organisatorischen Maßnahmen geschult werden sollten.

Mit Schulung allein ist es jedoch in der Regel nicht getan: Ein gelebtes Datenschutzmanagement setzt auch voraus, dass Mitarbeiter so in eine Datenschutzorganisation eingebunden und so für Datenschutzbelange sensibilisiert werden, dass sie selbstständig erkennen, wann bspw. eine Verarbeitung von Daten zu einem Risiko für das Unternehmen werden könnte und entsprechende Maßnahmen einleiten. In den wenigsten Unternehmen wird bspw. ein reger Austausch zwischen Datenschutzbeauftragten und Mitarbeitern gelebt. Üblicherweise wird der Datenschutz eher als „Hemmschuh“ oder „Erschwernis“ betrachtet und nicht als eine vom Unternehmen zu lösende Aufgabe, der es genauso wie der Bekämpfung von Korruption oder Diskriminierung zu begegnen gilt. Insofern sollte durch offene Kommunikation dafür Sorge getragen werden, dass die Akzeptanz des Datenschutzes im Unternehmen gestärkt wird, Mitarbeiter Verantwortung tragen, Vorgesetzte den entsprechenden Belangen wohlwollend gegenüberstehen und der Datenschutzbeauftragte Unterstützung erfährt. Nur dann wird eine Datenschutzorganisation entstehen, die dem Unternehmen tatsächlich einen Mehrwert bei der Umsetzung der datenschutzrechtlichen Aufgaben und Gesetze bietet.

4.3 Maßnahmen zur Sicherstellung von Datenschutzcompliance

Neben der Umsetzung der formalen gesetzlichen Vorgaben, der Sensibilisierung und Schulung von Mitarbeitern und Management bieten sich verschiedene Maßnahmen an, die das Unternehmen unterstützend einleiten kann, um Risiken im Bereich des Datenschutzes zu minimieren. Dazu zählen Maßnahmen der Ermittlung des datenschutzrechtlichen Status Quo im Unternehmen, Verpflichtungen der Mitarbeiter zum rechtskonformen Umgang mit Daten oder auch die Möglichkeit, Verstöße zu melden. Letztere Methode ist von besonderer Brisanz, da die Meldung von Verstößen gleichzeitig datenschutzrechtliche Risiken sowohl für den Melder als auch den Meldenden birgt, denen es bei der Einführung entsprechender Systeme – bspw. so genannter „Whistleblowing-Hotlines", die telefonisch oder online genutzt werden können – zu begegnen gilt.

4.3.1 Datenschutzaudit

Im Rahmen eines Datenschutzaudits werden die in einem Unternehmen bestehenden Datenschutzvorgänge – formeller und/oder materieller Art – überprüft. In der Regel erfolgt eine Bestandsaufnahme des „Ist-Zustands", der sich eine Gegenüberstellung mit dem „Soll-Zustand" anschließt, die schließlich in einer Darstellung des im Unternehmen festgestellten Verbesserungsbedarfs nebst anschließender Umsetzung der Verbesserungsvorschläge mündet. In der Praxis hat sich gezeigt, dass ein strukturiertes Datenschutzaudit – ähnlich wie Audits zur Prüfung der Umsetzung von SOX-Anforderungen – erheblich zur Verbesserung der Datenschutzorganisation im Unternehmen beitragen kann.

Eine gesetzliche Verpflichtung zur Durchführung eines Datenschutzaudits besteht indes nicht. § 9a BDSG, der den Gedanken eines formalisierten Audits aufgreift, definiert als Ziel eines Datenschutzaudits die „Verbesserung des Datenschutzes und der Datensicherheit". Das Datenschutzaudit gilt als Instrument der Selbstkontrolle von Unternehmen und soll einen datenschutzkonformen Umgang mit Daten fördern. § 9a BDSG sieht in diesem Zusammenhang allerdings nur die abstrakte Möglichkeit vor, Konzepte, Programme und Systeme auditieren zu lassen.[65] Zur Vereinfachung der Durchführung eines solchen Audits plante der Gesetzgeber die Einführung des Bundesdatenschutzauditgesetzes (§ 9a Satz 2 BDSG), dessen Entwurf zwar seit September 2007 vorliegt, der aber immer noch diskutiert wird und wohl eher als gescheitert zu betrachten ist.[66] Nach dem Gesetzentwurf können unabhängige Gutachter die Datenschutzkonzepte und technischen Einrichtungen des Unternehmens einer Prüfung unterziehen, bei deren Erfolg am Ende ein Siegel verliehen werden soll.[67]

---

[65] Siehe zu Pro und Kontra eines allgemeinen Datenschutzaudits: *Gola*, in: Gola/Schomerus, BDSG, 11. Aufl. 2012, § 9a Rn. 3 ff.

[66] Vgl. dazu die unter: https://www.datenschutzzentrum.de/bdsauditg/. Abrufbaren Materialien; *Hanloser,* MMR 2008, V ff.; der Entwurf des Datenschutzauditgesetzes sollte bis spätestens 2010 umgesetzt werden, dieses Vorhaben ist allerdings gescheitert; vgl. BR-Drucks. 4/09, abrufbar unter: http://dip21.bundestag.de/dip21/brd/2009/0004-09.pdf.

[67] Siehe zu einem möglichen Ablauf eines Audits: *Scholz* in: Simitis, BDSG, 7. Aufl. 2011, § 9a Rn. 23 ff.

In der Zwischenzeit hatte der Gesetzgeber als Alternative zu dem Datenschutzauditgesetz im Juli 2012 beschlossen, dass eine Stiftung Datenschutz bis Oktober 2012 eingerichtet und zügig tätig werden sollte.[68] Aufgabe der Datenschutzstiftung sollte die verstärkte Entwicklung von Datenschutzgütesiegeln sein, aber auch die Konzeption von Audits, mittels derer Unternehmen neutral einen „Daten-TÜV" durchführen lassen können, zählen. Unternehmen hätten dann – neben der Feststellung des status quo in ihrem Betrieb – eine offizielle Bestätigung der Datenschutzkonformität ihrer Prozesse erhalten. Ein solche neutrale Bestätigung kann gut als Marketing-Instrument genutzt werden, da die Unternehmen mit einer solchen Bestätigung um das Vertrauen ihrer Kunden werben können.

Allerdings ist noch offen, wie und mit welchen Mitteln die Stiftung ihre Arbeit aufnehmen soll. Im November 2012 haben sich die Datenschutzaufsichtsbehörden gegen die Stiftung ausgesprochen und ihre Mitwirkung verweigert, da diese wohl nicht die in sie gesetzten Erwartungen erfüllen könne und lediglich ein Feigenblatt sei. Insbesondere soll sie wohl lediglich Datenschutzsiegel entwickeln und nicht mehr die neutrale Auditierung vorgetrieben werden.[69]

Wollen Unternehmen ihre datenschutzrelevanten Prozesse auf Rechtskonformität geprüft haben, bietet ihnen zumindest der Gesetzgeber bislang keine entsprechenden Möglichkeiten. Sie müssen daher auf Eigeninitiative setzen. Zurzeit können sie lediglich ihre IT-Produkte auf Datenschutzkonformität hin prüfen lassen. Solche Prüfungen bietet bspw. das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein mit seinem Datenschutzgütesiegel an,[70] auf europäischer Ebene können Unternehmen ihre IT-Produkte durch das EuroPriSe-Siegel zertifizieren lassen.[71] Im behördlichen Bereich bestehen immerhin auf Landesebene verschiedene Verfahrensregelungen zur Durchführung von Behördenaudits.[72]

Praxishinweis

Neben dem Wettbewerbsvorteil, den ein Unternehmen gegenüber der Konkurrenz durch die Werbung mit einem datenschutzkonformen Produkt bzw. Verfahren sowie seinem Umgang mit Daten erlangen kann, führt ein Audit – selbst wenn es intern und nicht durch eine neutrale Stelle durchgeführt wird – regelmäßig zu einer veränderten Wahrnehmung des Datenschutzes in Unternehmen: Der Datenschutz und die Verant-

[68] Vgl. den angenommenen Antrag der FDP-Fraktion: http://dipbt.bundestag.de/dip21/btd/17/100/1710092.pdf.

[69] Vgl. dazu: http://www.spiegel.de/netzwelt/netzpolitik/verzicht-auf-mitarbeit-stiftung-datenschutz-ohne-datenschuetzer-a-866250.html.

[70] Vgl. https://www.datenschutzzentrum.de/guetesiegel/index.htm.

[71] Vgl. https://www.european-privacy-seal.eu/

[72] Vgl. u. a. § 11c BgfDSG; § 7b BremDSG; § 10a DSG NRW, § 4 Abs. 2 LDSG SH nebst den erforderlichen Ausführungsvorschriften in Schleswig-Holstein (Landesverordnung über ein Datenschutzaudit; GS Schl-H., S. 51, – Gl. Nr. 204-4-2 = RDV 2001, 203 nebst weiterführenden Hinweisen des ULD unter: https://www.datenschutzzentrum.de/audit/material.htm.

wortung des einzelnen Mitarbeiters für die von ihm verarbeiteten Daten sowie die aus einer Verletzung des Datenschutzes heraus resultierenden Risiken rücken mehr in den Fokus.

Daneben kann das Unternehmen Schwachstellen konkret identifizieren und eliminieren, im äußersten Fall die für die illegale Verarbeitung Verantwortlichen zur Rechenschaft ziehen.

Im Ergebnis empfiehlt sich die Durchführung eines Audits als Vorstufe zur Einführung einer funktionierenden Datenschutzorganisation. Es sollte zur Sicherstellung des Status Quo regelmäßig wiederholt werden.

4.3.2 Datenschutzrichtlinien und -kodizes

Ein Instrument, um Mitarbeiter in die Datenschutzorganisation einzubinden, ist die Einführung von so genannten „Datenschutzrichtlinien" oder „Datenschutzpolicies". In den Datenschutzrichtlinien, die von dem Datenschutzbeauftragten erstellt bzw. geprüft werden sollten, werden Mitarbeiter verpflichtet, bestimmte datenschutzrechtliche Pflichten zu erfüllen und u. a. das geltende Datenschutzrecht zu beachten.

Die zu regelnden Bereiche sind vielfältig: Von der allgemeinen Organisationsanweisung, in der der Umgang mit Daten geregelt wird, können Datenschutzrichtlinien auch speziellere Themen betreffen, bspw.

- den Umgang mit Passwörtern,
- die Nutzung von IT-Systemen,
- die Nutzung von Internet, E-Mail, Laptop, Smart-Phone, Telefon etc.,
- die Nutzung von Social-Media,
- den Umgang mit Telefax-Geräten,
- die Videoüberwachung,
- die Archivierung und Löschung von Daten oder auch
- Maßnahmen zur Erstellung von Verfahrensverzeichnissen.

Praxishinweis

Da diese Richtlinien regelmäßig mehrere Rechtsgebiete betreffen, empfiehlt sich die Prüfung nicht nur durch den Datenschutzbeauftragten, sondern auch eine Prüfung in arbeitsrechtlicher, IT- bzw. telekommunikationsrechtlicher Hinsicht.

Daneben können Verstöße gegen die Vorschriften in der Regel auch arbeitsrechtliche Konsequenzen nach sich ziehen, so dass sich neben der selbstverständlichen Abstimmung mit dem Management auch die Einbeziehung des Betriebsrats empfiehlt.

Nicht zuletzt sollte die Einhaltung von datenschutzrechtlichen Vorgaben auch ein wesentlicher Bestandteil eines Ethikkodizes oder Code of Conduct sein: Datenschutz ist Ausfluss des allgemeinen Persönlichkeitsrechts und Grundrechtsschutz. Unternehmen sind daher gehalten, sowohl die Persönlichkeitsrechte ihrer eigenen Mitarbeiter als auch die Persönlichkeitsrechte der Personen, deren Daten in ihrem Unternehmen

verarbeitet und genutzt werden, umfassend zu wahren. Verbindliche Richtlinien zu einem verantwortungsbewussten Umgang mit Daten sollten daher in keinem Code of Conduct fehlen.

§ 38a BDSG sieht darüber hinaus für Berufsverbände oder ähnliche Gruppierungen die Möglichkeit vor, den Datenschutzaufsichtsbehörden Kodizes zur Prüfung vorzulegen. Solche Verhaltenskodizes finden sich beispielsweise in dem Code of Conduct der Versicherungswirtschaft, dem „OBA" (Online Behavioural Advertising, dem Rahmenwerk zur Selbstregulierung von nutzungsbasierter Online-Werbung) oder auch dem Datenschutz-Kodex für Geodatendienste.[73] Regelmäßig sind solche Kodizes aber für Unternehmen nur dann von Interesse, wenn sie in entsprechenden Verbänden tätig sind oder kritische Datenverarbeitungen durchgeführt werden.

4.3.3 Whistleblowing-Hotlines

Viele Unternehmen haben inzwischen erkannt, dass sie auf Informationen aus dem eigenen Unternehmen angewiesen sind, sofern sie Missstände wie Korruption, Adresshandel, Betrug etc. erfolgreich und schnell aufdecken wollen. Daneben erfordert die Umsetzung der Vorgaben aus den nun immer häufiger auch in Deutschland eingeführten Ethikkodizes einen Kontrollmechanismus betreffend die Umsetzung der dort statuierten Regelungen. Eine schnelle Aufdeckung von Verstößen ist für Unternehmen nicht nur aus Eigeninteresse notwendig: Handelt es sich um Unternehmen, die selbst oder deren Muttergesellschaft an US-Börsen notiert sind, sind sie dazu sogar durch die Vorgaben des Sarbanes-Oxley-Acts[74], verpflichtet.

Ein Instrument zur Aufdeckung von Missständen sind die so genannten „Whistleblowing-Hotlines", die telefonisch oder online durch Unternehmen, häufig mit Unterstützung darauf spezialisierter Call-Center, Ombudsmänner und/oder Datenverarbeiter, betrieben werden.

„Whistleblowing" bedeutet übersetzt „in die Pfeife blasen, auf etwas aufmerksam machen". Daraus leitet sich bereits der Zweck dieser Hotlines ab: Mitarbeiter können über die Hotline das Fehlverhalten anderer anzeigen. Naturgemäß birgt eine solche Hotline die Gefahr der Denunziation Unschuldiger; sie weist jedoch auch datenschutzrechtlich eine erhebliche Brisanz auf: Während in den USA das Datenschutzrecht eher zurückhaltend ausgestaltet ist und daher wenig rechtliche Bedenken gegenüber der Erhebung, Speicherung und Verarbeitung von Daten des Meldenden und des Gemeldeten bestehen, gestaltet sich die Rechtslage in Europa anders. Der Schutz des Einzelnen und seiner Persönlichkeitsrechte vor dem Missbrauch seiner Daten durch bewusste Falschanzeigen oder auch die Möglichkeit der Rückverfolgung des Melders nebst damit für diesen einhergehenden Risiken wird im Vergleich zu den USA wesentlich höher gewertet. Die Interessen des Unternehmens an einer raschen Aufklärung der Missstände überwiegen aus europäisch

[73] Vgl. bspw. den Kodex für Geodatendienste: http://www.bitkom.org/files/documents/Datenschutz_Kodex.pdf.

[74] Abrufbar unter: http://www.legalarchiver.org/soa.htm.

geprägter datenschutzrechtlicher Sicht nicht automatisch die Interessen des Einzelnen und scheitern mitunter an den Datenschutzgesetzen der einzelnen europäischen Länder. Dies gilt insbesondere, wenn im Rahmen der Hotline ein umfassender Datenaustausch zwischen diversen Beteiligten mit Sitz innerhalb und außerhalb der EU stattfindet.

Um Unternehmen nicht in die unhaltbare Situation zu bringen, im Gebiet der EU eine Hotline auf Grundlage der SOX-Vorgaben betreiben zu müssen, die nach den jeweiligen europäischen Vorgaben verboten ist,[75] hat die Art. 29-Gruppe, die sich aus den Datenschutzbeauftragten der EU-Mitgliedstaaten zusammensetzt, eine Stellungnahme betreffend die datenschutzrechtliche Zulässigkeit des Betriebs einer solchen Hotline innerhalb des Gebiets der EU abgegeben.[76] Parallel haben auch andere Datenschutzaufsichtsbehörden in Europa entsprechende Empfehlungen bzw. sogar Registrierungs- oder Anzeigepflichten erlassen, die vor der Inbetriebnahme einer Hotline zu erfüllen sind.[77] Wesentliches Ziel sämtlicher Bestrebungen ist es dabei, sowohl den Gemeldeten als auch den Melder ausreichend zu schützen und einen unkontrollierten Datenfluss überflüssiger und diskriminierender Daten zu verhindern. Die Empfehlungen umfassen daher u. a. den Inhalt der Meldungen, den Umgang mit den Meldungen, die Zugriffsberechtigungen, die Meldebefugnisse, den Personenkreis, der gemeldet werden darf oder auch die bestehenden Informationspflichten gegenüber Mitarbeitern, Melder und Gemeldetem.[78]

Praxishinweis

Unabhängig von dem Imageschaden, den ein Verstoß von Unternehmen gegen datenschutzrechtliche Vorgaben nach sich zieht, scheuen sich die Datenschutzaufsichtsbehörden auch nicht Bußgelder zu verhängen und die Umsetzung ihrer Vorgaben bei Einführung einer Hotline zu kontrollieren. Insofern empfiehlt es sich vor Einführung einer entsprechenden Hotline sorgfältig zu prüfen, ob diese nach den jeweiligen landesspezifischen Vorgaben zulässig ist bzw. ob Registrierungs- oder Anzeigepflichten bestehen und die jeweiligen Datenströme rechtlich zulässig ausgestaltet sind.

[75] Vgl. bspw. die Entscheidungen der französischen Datenschutzaufsichtsbehörde CNIL, CNIL Entscheidung 2005-110 v. 26.5.2005 (Mc Donald's Gruppe Frankreich); CNIL Entscheidung 2005-111 v. 26.5.2005 (Exide Technologies) oder auch die Entscheidung des LAG Düsseldorf v. 14.11.2005 – 10 TaBV 46/05, BB 2006, 335 betreffend die Mitbestimmung bei Einführung einer Ethikrichtlinie im Fall Wal-Mart.

[76] Abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf.

[77] Vgl. bspw. CNIL-recommandations-whistleblowing-VA.pdf. oder die Empfehlungen des Düsseldorfer Kreises für den Betrieb von Hotlines in Deutschland, abrufbar unter: http://www.datenschutz-hamburg.de/news/detail/article/whistleblowing-hotlines-firmeninterne-warnsysteme-beschaeftigtendatenschutz.html.

[78] Vgl. dazu weitergehend: Wisskirchen/Körber/Bissels, BB 2006, 28 ff.; Breinlinger/Krader, RDV 2006, 1 ff.; Deiseroth/Derleder, ZRP 2008, 248; Bauer, Datenschutzpraxis 11/2012, S. 14.

5 Fazit

Während die formellen Voraussetzungen, die das deutsche Datenschutzrecht den Unternehmen auferlegt, relativ einfach umzusetzen sind, gestaltet sich die Einführung einer funktionsfähigen Datenschutzorganisation in der Regel etwas komplizierter. Alle Beteiligten sind über ihre eigene Verantwortung aufzuklären, in die Organisation einzubinden und so zu sensibilisieren, dass sie aus eigenem Antrieb für einen rechtskonformen Umgang mit Daten Sorge tragen.

Selbstverständlich obliegt dem Datenschutzbeauftragten als dem maßgeblichen Kontrollorgan im Unternehmen dabei eine wesentliche Verantwortung. Dazu bedarf er aber der Unterstützung des Managements. Nur dann, wenn auch das Management die Anforderungen des Datenschutzes nicht als „Hemmnis" sondern als notwendige Maßnahmen zur Wahrung der Rechte des Einzelnen und als Chance, sich gegenüber dem Wettbewerb wohltuend abzuheben begreift, wird eine Datenschutzorganisation mit Leben gefüllt.

Dabei sollte das Management nicht außer Acht lassen, dass Datenschutz ein wesentlicher Bestandteil von „Unternehmens-Compliance" ist und Verstöße gegen die entsprechenden gesetzlichen Vorgaben Haftungsfolgen sowohl für das Unternehmen als auch für das Management selbst nach sich ziehen können. Nicht vergessen werden darf weiterhin, dass der Datenschutz immer stärker in den Fokus der Öffentlichkeit gerät. Damit einhergehend registriert der Einzelne mit Interesse, wie mit seinen Daten bei welchem Unternehmen umgegangen wird. Unternehmen werden daher immer häufiger mit Anfragen und Ansprüchen von Betroffenen konfrontiert oder auch von Datenschutzaufsichtsbehörden kontrolliert. Eine funktionierende Datenschutzorganisation hilft, diesen Anforderungen gelassen entgegenzusehen.

IP-Compliance

Detlef Mäder

Inhaltsverzeichnis

Zusammenfassung

IP-Compliance betrifft den Bereich gewerblicher Schutzrechte (z. B. Marken, Patente, Geschmacksmuster, Gebrauchsmuster) und Urheberrechte sowie weitere Rechte geistigen Eigentums (z. B. Betriebsgeheimnisse und Know-how (Siehe ausführlich zum Begriff und Schutz von Know-how in *Wurzer, Alexander J., Know-how-Schutz als Teil des Compliance Managements, CCZ 2009, 49–56.*). Ein mögliches Haftungsrisiko für betroffene Unternehmen kann sich z. B. aus der Verletzung fremder Schutzrechte und daraus resultierender Unterlassungs-, Auskunfts-, Schadensersatz und Vernichtungsansprüche ergeben (*Kellenter, Wolfgang* in: Krieger/Schneider (Hrsg.), Handbuch Managerhaftung, 2. Aufl. 2010, § 23, Rn. 3 ff.). In der Praxis können insbesondere Unterlassungs- und Schadensersatzansprüche wegen Verletzung von IP-Rechten regelmäßig auch gegen die gesetzlichen Vertreter des verantwortlichen Unternehmens (Geschäftsführer und Vorstände) geltend gemacht werden (Vgl. dazu *Koch, Benjamin*, Ausgewählte Themen der IP-Compliance, CCZ 2010, 70, 72.). Zudem kann die Reputation des jeweiligen Unternehmens beschädigt werden. Darüber hinaus stellen IP-Rechte einen oft wesentlichen Vermögenswert des Unternehmens dar (Koch, CCZ 2010, 70.).

D. Mäder (✉)
Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: detlef.maeder@luther-lawfirm.com

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2_9, © Springer Fachmedien Wiesbaden 2013

1 „Best Practice“ für IP-Compliance

Zunächst sollte eine Analyse der bestehenden Schutzrechte durchgeführt werden. Nachdem eine Sichtung bzw. eine Inventur der vorhandenen Schutzrechte erfolgt ist, sollten diese hinsichtlich ihrer Relevanz bewertet und eine entsprechende Abstufung festgelegt werden, da naturgemäß nicht jedem Recht dieselbe Bedeutung und Wertigkeit innerhalb des Unternehmens zukommen wird. Unter Zugrundelegung der so gewonnenen Erkenntnisse kann eine unternehmensinterne IP-Richtlinie geschaffen sowie eine Stelle bestimmt werden, die in der Folgezeit für die Überwachung der Umsetzung und Einhaltung dieser Richtlinie zuständig ist.

2 IP-Richtlinie

Die unternehmensinterne IP-Richtlinie sollte sowohl Verfahren zum Schutz der im Unternehmen vorhandenen Rechte als auch Regelungen zur Meidung von Kollisionen und Konflikten mit Schutzrechten Dritter enthalten. Bezüglich Verfahren zum Schutz der vorhandenen Schutzrechte müssen konkrete Vorgehensweisen beschrieben und festgelegt werden, wie etwa die Durchführung von Marken- und Patentrecherchen im Vorfeld einer beabsichtigten Nutzung durch das Unternehmen. Dies wird in der Regel nötig sein, um Haftungsrisiken, die sich aus etwaigen Kollisionen mit Schutzrechten Dritter ergeben können, besser einzuschätzen und zu reduzieren. Je nach Eigenart und Relevanz des Schutzrechtes bieten sich zudem unterschiedliche Schutzstrategien an. Zu beachten ist insbesondere, dass sich häufig ein Konflikt aus dem Spannungsfeld zwischen dem frühzeitigen Schutz eines gewerblichen Schutzrechtes[1] und der damit zwingend einhergehenden frühzeitigen Offenlegung gegenüber Wettbewerbern ergeben kann. Zudem gilt es, den genauen Schutzumfang zu definieren, d. h. die geografische und inhaltliche Erstreckung des jeweiligen Schutzrechts.

Im Rahmen der IP-Richtlinie ist auch die Überwachung der bestehenden Schutzrechte und die entsprechende Marktbeobachtung zu regeln. Des Weiteren gilt es, den Bereich des Lizenzvertragsmanagements und der Verwaltung entsprechender vertraglicher Vereinbarungen festzulegen. Die IP-Richtlinie sollte außerdem Anweisungen für den Erwerb und die Lizenzierung fremder Schutzrechte enthalten. Zum einen empfiehlt es sich zur Vermeidung von Konflikten, vor der Nutzung eines Rechtes sicherzustellen, dass dieses ordnungsgemäß erworben oder lizenziert worden ist, zum anderen kann so gewährleistet werden, dass bei der Lizenzierung eigener bzw. fremder Schutzrechte Fristen und Lizenzgebührzahlungen eingehalten werden.

In der IP-Richtlinie sollten zudem Regelungen getroffen werden, die es ermöglichen, alle betroffenen Unternehmensbereiche wie etwa die Rechtsabteilung, die

[1] Siehe dazu *Lothert, Ralf-Wolfgang*, in: Hauschka, Corporate Compliance § 18, Rn 16.

Forschungs-/Entwicklungs- sowie die Marketing-Abteilung einzubinden und so frühzeitig Abstimmungen der einzelnen Bereiche untereinander zu erreichen.

Die spätere Implementierung und Überwachung der IP-Compliance setzt zunächst voraus, dass die Unternehmensleitung sich bereit erklärt, die geregelten Abläufe zu unterstützten, begleiten und nicht zuletzt auch zu überwachen. Darüber hinaus kann die effektive Umsetzung der Richtlinie auf Dauer aber nur umfassend sichergestellt werden, wenn Schulungen für die Mitarbeiter der betroffenen Unternehmensbereiche stattfinden und notwendige Anpassungen und Erneuerungen intern kommuniziert und umgesetzt werden können.

3 Unternehmenskommunikation und IP-Compliance

Auch im Bereich der Unternehmenskommunikation können sich Compliance-Fälle ergeben. Unternehmenskommunikation in diesem Sinne betrifft jedoch nicht nur die externe, sondern auch die interne Form der Kommunikation. Beispielhaft seien hier als mögliche zu betrachtende Anwendungen Interviews, Presseerklärungen, Kundenzeitschriften, Newsletter, das Internet, Mitarbeiterzeitschriften und das Intranet genannt, aber auch neuere Kommunikationsformen wie soziale Netzwerke, Corporate Blogs, Internet-Foren und Podcasts sind geeignet, potenzielle Risiken für die Compliance eines Unternehmens darzustellen.[2] Hier gilt es, Mitarbeiter anzuhalten, wie solche Kommunikationswege genutzt werden können und ein Bewusstsein dafür zu schaffen, welche Äußerungen problematisch sind.

Ansprüche im Zusammenhang mit der Unternehmenskommunikation können sich sowohl aus zivilrechtlichen und strafrechtlichen Normen, als auch aus dem Presse- und Wettbewerbsrecht ergeben.

Compliance-Maßnahmen im Bereich der Kommunikation können beispielsweise ebenfalls darin bestehen, die interne wie externe Kommunikation eines Unternehmens durch die Gestaltung einer Richtlinie zu regeln, auch wenn die Aufstellung von konkreten Anforderungen vor allem in Bereichen wie Marketing/Sales nur schwer möglich sein wird. In jedem Falle sollten auch Dritte, die bestimmungsgemäß mit dem Bereich der Unternehmenskommunikation in Berührung kommen wie Zulieferer oder Subunternehmer etc. entsprechenden in die Compliance-Richtlinie einbezogen werden.

[2] Rath/von Barby, in: Umnuß, Corporate Compliance Checklisten, 2. Aufl. 2012, Kap. 7, Rn 72, 76.

Kartellrechts-Compliance

Helmut Janssen

Inhaltsverzeichnis

H. Janssen (✉)
Avenue Louise 326, 1050 Brüssel, Belgien
E-Mail: helmut.janssen@luther-lawfirm.com

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2_10, © Springer Fachmedien Wiesbaden 2013

Zusammenfassung

Eine funktionierende Kartellrechts-Compliance vermeidet oder verringert im Wesentlichen folgende Risiken: Drastische Bußgelder gegen das Unternehmen und damit Wertminderung des Unternehmens, Bußgelder gegen Vorstand, Geschäftsführung und Mitarbeiter, Schadensersatzansprüche gegen Unternehmen und Mitarbeiter, Störung der betrieblichen Abläufe durch Ermittlungsverfahren, Strafverfolgung und Haftstrafen im In- und Ausland. Dabei ist eine Kartellrechts-Compliance in vielen Unternehmen ohne größeren organisatorischen Aufwand möglich. Oft genügen eine intelligente Organisation der Mitarbeiter, regelmäßige Schulungen sowie einige überschaubare Verhaltensregeln. Auch wenn bei einzelnen Unternehmen, je nach Größe und Branche, der Aufwand größer sein kann: er wird sich zum Schutz der Führung, der Mitarbeiter und der Eigentümer des Unternehmens stets lohnen. Zumindest muss die Kartellrechts-Compliance der Unternehmensleitung vor Augen führen, wo Risiken im eigenen Unternehmen liegen, wie sie zu bewerten sind und wie mit ihnen umgegangen werden kann.

1 Ziele der Kartellrechts-Compliance – Warum braucht man Kartellrechts-Compliance, und wer braucht sie?

Ziel kartellrechtlicher Compliance ist es, Nachteile für das Unternehmen, seine Mitarbeiter und seine Gesellschafter dadurch auszuschließen oder zu verringern, dass man Verstöße gegen das Kartellrecht vermeidet und im Fall von Verstößen richtig reagiert. Dazu werden zunächst jene Risikobereiche skizziert, die eine kartellrechtliche Compliance eingrenzen muss (dazu 2.). Danach werden die Nachteile beschrieben, die dem Unternehmen, seinen Managern, seinen Arbeitnehmern und seinen Gesellschaftern bei einem Verstoß gegen das Kartellrecht drohen (dazu 3.). Im Anschluss wird dargestellt, welche dieser Nachteile durch eine kartellrechtliche Compliance – ganz oder zum Teil – ausgeschlossen werden können (dazu 4.). Abschließend werden Bestandteile eines effektiven Compliance-Programms erläutert (dazu 5.).

2 Risikobereiche im Unternehmen – Was ist haftungsträchtig und verboten?

Um den Aufwand für die Kartellrechts-Compliance in ein vernünftiges Verhältnis zum Risiko zu setzen, wird man zunächst betrachten, ob bestimmte Bereiche ausgegrenzt werden können. So ist etwa zu fragen, ob das Unternehmen mit einem seiner Produkte oder Dienstleistungen Marktbeherrscher ist. Denn für einen Marktbeherrscher gelten strengere Regeln, wenn er einseitig (d. h. ohne Abstimmung mit seinen Wettbewerbern) zum Beispiel Preise festsetzt, Rabatte gewährt oder Vertriebsbindungen auferlegt. Auch gibt es Unternehmen, deren Wert nicht unwesentlich von der Wirksamkeit bestimmter Vertriebsvereinbarungen abhängt, zum Beispiel von einer geografischen Exklusivität oder einer langfristigen Alleinvertriebsvereinbarung. Während beim Marktbeherrscher die Compliance bereits im Prozess der Preis- und Konditionenbildung einsetzen muss, ist im Beispiel der Vertriebsbindungen eher das laufende Vertragsmanagement gefragt. In den meisten Fällen werden kritische Formen der Koordination mit Wettbewerbern Gegenstand der Kartellrechts-Compliance sein. Dies sind:

- klassische Kartellabsprachen mit Wettbewerbern. Also die Absprache von Preisen und Quoten und die Aufteilung von Gebieten und Kundengruppen;[1]
- der Austausch gewisser Informationen. So sind etwa Marktinformationssysteme problematisch, wenn sensible, genaue und aktuelle Daten in kurzen zeitlichen Abständen gemeldet und nicht hinreichend aggregiert und anonymisiert werden;[2]
- der Missbrauch einer marktbeherrschenden Stellung. Beispielsweise sind etablierte Telekommunikationsanbieter wegen überhöhter Preise im Ortsnetz oder der Erschwerung des Netzzugangs für Wettbewerber bebußt worden.[3] Microsoft macht seit vielen Jahren Schlagzeilen in der Tagespresse; [4]

---

[1] Vgl. *von Dietze/Janssen*, Kartellrecht in der anwaltlichen Praxis, 4. Aufl. München 2011, Rn. 147 ff.; Beispiele: Absprachen über Preise, Kundenzuordnungen und Liefermengen, Pressemitteilung des BKartA vom 19. Februar 2013 und Preisabsprachen für Water-Management-Produkte, Pressemitteilung der Kommission IP/12/704 vom 27. Juni 2012.

[2] Vgl. etwa Wirtschaftsvereinigung Stahl gegen Kommission, EuG v. 5.5.2001– Rs. T-16/98. *Zimmer*, in: Immenga/Mestmächer, GWB, 4. Aufl. 2007, § 1 Rn. 303 ff. Aktuelles Beispiel mit konkreten Hinweisen des BKartA zum „Standard für kartellrechtliche Gestaltung von Marktinformationssystemen im Bereich der Beschaffung von Rohmilch", Entscheidung B2–118/10 vom 12. Mai 2011, Fallbericht vom 29. Juni 2011; Fallbericht B2–118/10 vom 12. Mai 2011; Sektoruntersuchung Milch (B2–19/08) Endbericht Januar 2012 Rn. 129 ff.

[3] EG-Kommission vom 21. Mai 2003, ABl EG Nr. L 263/9 (Deutsche Telekom); aktuelles Beispiel ist die Geldbuße in Höhe von 127 Mio. € gegen Telekomunikacja Polska S.A., Pressemitteilung der Kommission IP/11/771 vom 22. Juni 2011.

[4] Microsoft gegen Kommission, EuG v. 17. September 2007– Rs. T 201/04 (Betriebssystem); Koppelung des Browsers „Internet Explorer" an das Windows-Betriebssystem; zuletzt Pressemitteilung der Kommission IP/12/1149 vom 24. Oktober 2012.

- der Aufruf zum Boykott. Ein aktuelleres Beispiel ist der Aufruf von Apothekerverbänden an ihre Mitglieder, von einem Pharmagroßhändler keine Produkte mehr zu beziehen, weil dieser eine Versandhandelsapotheke (DocMorris) übernommen hatte.[5] Ein anderes Beispiel ist die Aufforderung des Bundesverband Deutscher Milchviehhalter e. V. an die Milchbauern, Molkereien nicht zu beliefern, um einen einheitlichen Mindestpreis durchzusetzen.[6]

Es gibt noch andere Verbote, die im Weiteren nicht interessieren. So sind bei Unternehmenszusammenschlüssen die Fusionskontrollvorschriften einzuhalten. Wer ohne Genehmigung der Kartellbehörde den Zusammenschluss vollzieht oder Falschangaben im Verfahren macht, wird bebußt.[7]

Im Unternehmen bewegen sich vor allem Vorstände, Geschäftsführer und Vertriebsleiter in diesen Risikobereichen.

Das Risiko entdeckt zu werden, ist nicht zu unterschätzen. Kartelle werden in der Regel dadurch aufgedeckt, dass ein beteiligtes Unternehmen einen Kronzeugenantrag bei einer Kartellbehörde (oder bei mehreren) stellt, um auf diese Weise eine Geldbuße zu vermeiden oder zu verringern (der Bayer AG etwa hat die Europäische Kommission einen vollständigen Erlass der Buße in Höhe von 201 Mio. € gewährt[8]). Auslöser für einen solchen Kronzeugenantrag ist oft, dass ein Unternehmen verkauft wird und der neue Eigentümer eine Geldbuße zu Lasten dieses Unternehmens oder eine Haftung seiner Geschäftsführer ausschließen will. In jedem Mustervertrag für einen Unternehmenskauf dürfte heutzutage die Garantieerklärung des Verkäufers enthalten sein, die Zielgesellschaft habe das Kartellrecht befolgt. Überdies haben viele Kartellbehörden in den vergangenen Jahren Abteilungen eingerichtet, die selbst ermitteln und verfolgen (beim Bundeskartellamt die „Sonderkommission Kartellbekämpfung"), oft auch in Zusammenarbeit mit Behörden anderer Staaten.[9] Allein bei der Europäischen Kommission arbeiten 70 Inspektoren („Kartelljäger") in diesem Bereich.[10] Daneben erhöhen auch die

[5] Pressemitteilung des BKartA vom 2. Juli 2009; Bußgelder wurden verhängt.

[6] Pressemitteilung des BKartA vom 13. November 2008; Bußgelder wurden für den Wiederholungsfall angedroht.

[7] Praxis des Bundeskartellamts seit 2008; mehr als 4 Mio. € für Mars wegen Verstoßes gegen das Vollzugsverbot, Pressemitteilung des BKartA vom 15. Dezember 2008, 414.000 € für die Hauptgenossenschaft ZG Raiffeisen, Pressemitteilung des BKartA vom 28. Januar 2011; zur Falschinformation siehe Pressemitteilung vom 5. Oktober 2005 (INVISTA).

[8] Obgleich das Unternehmen als Wiederholungstäter dingfest gemacht worden war! Pressemitteilung der Kommission IP/07/1855 vom 5. Dezember 2007 (Chloropren-Kautschuk); aktueller Fall: Roto, der deutsche Hersteller von Fensterbeschlägen, erhielt einen vollständigen Erlass, Pressemitteilung der Kommission IP/12/313 vom 28. März 2012. Beispiel aus der Praxis des BKartA, Kartell der Hersteller von Automatiktüren, Pressemitteilung des BKartA vom 25. Juli 2012.

[9] Gegen Hersteller von Flachglas verhängte die Kommission eine Geldbuße in Höhe von 486,9 Mio. € nach eigenen Ermittlungen, die sie auf der Grundlage von Informationen durch mitgliedstaatliche Kartellbehörden eingeleitet hatte; vgl. Pressemitteilung der Kommission IP/07/1781 vom 28. November 2007.

[10] Die Kommission leitete das Verfahren gegen Autoglashersteller eigeninitiativ (auf Grund von Hinweisen eines anonymen Informanten) ein und schloss es im November 2008 mit der Verhängung

Untersuchung bestimmter Wirtschaftszweige durch die Wettbewerbsbehörden (sog. Sektoruntersuchung[11]), ein Wechsel des Geschäftsführers oder das unfreiwillige Ausscheiden eines Mitarbeiters das Entdeckungsrisiko für die Mitglieder eines Kartells; hinzu kommt in einigen Staaten neuerdings die Möglichkeit einer Belohnung für „Whistleblower".[12]

3 Drohende Nachteile – Was droht wem?

3.1 Drastische Bußgelder gegen Unternehmen

Kommission und Kartellamt können nach europäischem bzw. deutschem Recht jedem an einem Verstoß beteiligten Unternehmen Bußgelder bis zu 10 % des jeweiligen weltweiten Gesamtumsatzes auferlegen.[13] Gemeint ist damit in der Regel der Konzernumsatz der beteiligten Unternehmen, d. h. im Falle eines abhängigen Unternehmens kommt es auf die Umsätze der herrschenden Unternehmen sowie der von ihnen abhängigen Unternehmen an. Im Rekordjahr 2007 hat allein die Europäische Kommission Geldbußen über mehr als 3,3 Mrd. € verhängt. So entfiel zum Beispiel auf Saint-Gobain für seine Beteiligung am „Autoglaskartell" ein Bußgeld in Höhe von 896 Mio. €.[14] Bußgelder sind grundsätzlich nicht als Betriebsausgaben steuerlich abzugsfähig.[15] Dies gilt aber dann nicht, „soweit der wirtschaftliche Vorteil, der durch den Gesetzesverstoß erlangt wurde, abgeschöpft worden ist, wenn die Steuern vom Einkommen und Ertrag, die auf den wirtschaftlichen Vorteil entfallen, nicht abgezogen worden sind (Abb. 1, Tab. 1)."[16]

einer Geldbußen in Höhe von 1,3 Mrd. € ab; siehe Pressemitteilung der Kommission IP/08/1685 vom 12. November 2008.

[11] Die Kommission hat am 16. Januar 2008 zum ersten Mal im Rahmen einer Sektoruntersuchung unangekündigte Nachprüfungen in den Geschäftsräumen von Pharma-Herstellern durchgeführt, also ohne dass konkrete Indizien für einen Verstoß vorlagen; vgl. Pressemitteilung der Kommission IP/08/49 vom 16. Januar 2008.

[12] In Großbritannien und einigen weiteren Staaten besteht ein Belohnungssystem für Informanten, die zur Überführung von Kartellen beitragen; in den USA wurde die Einführung 2011 zunächst nur diskutiert, aber nicht beschlossen; zu Prämien für Whistleblower im Kartellrecht *Bueren,* ZWeR 2012, 310.

[13] § 81 Abs. 4 Satz 2 GWB, Art. 23 Abs. 2 VO 1/2003. Adressat des Verbotes und der Bußgeldvorschrift ist nach europäischem Recht das Unternehmen. Das Verhalten der natürlichen Person wird dem Unternehmen als eigenes schuldhaftes Handeln zugerechnet. Das deutsche Recht rechnet dem Unternehmen über § 30 OWiG das Handeln von Unternehmensangehörigen und über §§ 130, 30 OWiG die Aufsichtspflichtverletzung des gesetzlichen Vertreters zu.

[14] Pressemitteilung der Kommission IP/07/209 vom 21. Februar 2007; später auf 880 Mio. € reduziert.

[15] § 4 Abs. 5 Satz 1 Nr. 8 Satz 1 EStG.

[16] § 4 Abs. 5 Satz 1 Nr. 8 Satz 4 EStG. Die Finanzämter gehen bei Geldbußen durch die Europäische Kommission von der Regel aus, dass durch die Europäische Kommission verhängte Geldbußen keinen abschöpfenden sondern strafenden Charakter haben.

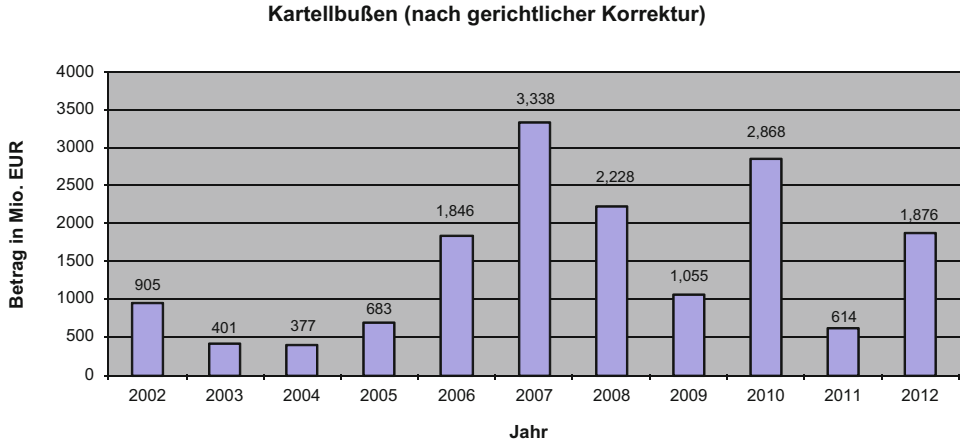


Abb. 1 Von der Europäischen Kommission verhängte Geldbußen (2002 bis 2012). (http://ec.europa.eu/competition/cartels/statistics/statistics.pdf)

3.2 Bußgelder gegen natürliche Personen – Vollstreckung in das Privatvermögen

Nach deutschem Recht können Bußgelder nicht nur gegen Unternehmen, sondern auch gegen natürliche Personen verhängt werden. Das Bundeskartellamt macht von dieser Befugnis regelmäßig Gebrauch. Die Europäische Kommission kann in aller Regel keine Bußgeldentscheidung gegen eine natürliche Person treffen.[17] Allerdings sind die deutschen Kartellbehörden befugt und verpflichtet, europäisches Recht durchzusetzen. Somit kann das Bundeskartellamt bei einem Verstoß gegen europäisches Kartellrecht nach den Vorschriften des OWiG auch gegen natürliche Personen Bußgelder festsetzen. Für den Betroffenen ist damit von entscheidender Bedeutung, ob ein Verfahren vom deutschen Kartellamt oder von der Europäischen Kommission geführt wird.

Die Höhe des Bußgeldes gegen eine natürliche Person ist auf 1 Mio. € für jeden einzelnen Verstoß begrenzt.[18] Für weniger gravierende Verstöße liegt die Obergrenze bei 100.000 €.[19] Bei klassischen Kartellen, also Absprachen über Preise, Gebiete, Quoten und Kundenaufteilung werden die Kartellbehörden praktisch immer von einem gravierenden Verstoß ausgehen. Einen weniger gravierenden Verstoß wird man in der Praxis wohl nur bei unvollständiger Anmeldung eines Unternehmenszusammenschlusses annehmen.

Versichern lässt sich das Risiko des Einzelnen in der Regel nicht. D&O-Versicherungen (Directors and Officers Liability Insurance) enthalten zumeist ausdrückliche Haftungsausschlüsse. Bußgelder sind auch nach den Allgemeinen Versicherungsbedingungen für

[17] Auch nach europäischem Recht könnte eine natürliche Person bebußt werden, wenn sie selber als „Unternehmen" im Sinne des EU-Kartellrechts zu qualifizieren wäre.

[18] § 81 Abs. 4 Satz 1 GWB.

[19] § 81 Abs. 4 Satz 5 GWB.

Tab. 1 Top Ten der bebußten Unternehmen bis Ende 2012 (nur Europäische Kommission [Stand 31. Mai 2013])[a]

Jahr	Unternehmen	Fall	Betrag in Euro
2008	Saint Gobain	Autoglas	880,000,000
2012	Philips	Fernseh- und Computerbildschirmröhren	705,296,000 davon 391.940.000 gesamtschuldnerisch mit LG Electronics
2012	LG Electronics	Fernseh- und Computerbildschirmröhren	687,537,000 davon 391.940.000 gesamtschuldnerisch mit Philips
2001	F. Hoffmann-La Roche AG	Vitamine	462,000,000
2007	Siemens AG	Gasisolierte Schaltanlagen	396,562,500
2008	Pilkington	Autoglas	357,000,000
2010	Ideal Standard	Badezimmerausstattungen	326,091,196
2009	E.ON	Gas	320,000,000
2009	GDF Suez	Gas	320,000,000
2007	ThyssenKrupp	Aufzüge und Fahrtreppen	319,779,900

[a]http://ec.europa.eu/competition/cartels/statistics/statistics.pdf. Nicht in dieser Aufstellung enthalten ist das von der Kommission (vgl. Pressemitteilung der Kommission IP/08/318 vom 27. Februar 2008) gegen Microsoft verhängte Zwangsgeld in Höhe von 899 Mio. €. Mit dieser Entscheidung hat die Kommission gezeigt, dass sie auch die Nichterfüllung von Auflagen, die sie in einer früheren Entscheidung gegen das Unternehmen festgelegt hatte, nicht hinnimmt. Der EuGH hat die Entscheidung grundsätzlich bestätigt, auch wenn er das Zwangsgeld auf 860 Mio. € gesenkt hat.

die Vermögensschaden-Haftpflichtversicherung von Aufsichtsräten, Vorständen und Geschäftsführern (AVB-AVG Stand Mai 2013) nicht vom Versicherungsschutz umfasst. Schließlich entfällt bei vorsätzlich begangenen Verstößen der Versicherungsschutz bereits auf Grund von § 81 Abs. 1 VVG.

Bußgeldpflichtig werden können Personen durch ihr eigenes Handeln (unmittelbar Handelnde und Beteiligte; dazu sogleich unter 3.3) oder durch die Verletzung ihrer Aufsichtspflicht (dazu 3.4).

3.3 Handelnde Personen

Über § 9 OWiG kann den unmittelbar handelnden Personen die Unternehmenseigenschaft der kartellrechtlichen Verbotsnorm zugerechnet werden. Dies sind in der Regel gesetzliche Vertreter und zu eigenverantwortlicher Aufgabenerledigung beauftragte Personen, etwa der Leiter einer Vertriebsabteilung oder einer Rechtsabteilung.[20] Zwischen mittelbarer Täterschaft, Anstiftung und Beihilfe unterscheidet das Ordnungswidrigkeitenrecht nicht. Bußgeldpflichtig können auch die „sonstigen Beteiligten" (§ 14 Abs. 1 Satz 2 OWiG) sein – demnach macht sich jeder bußgeldpflichtig, der den Handelnden „im Bewusstsein des Kartellrechtsverstoßes bei der Organisation eines Preiskartells unterstützt".[21] In seiner Praxis konzentriert sich das Bundeskartellamt auf die Entscheider im Unternehmen.

3.4 Aufsichtspflichtige

Gemäß § 130 OWiG kann ein Bußgeld auch gegen aufsichtspflichtige Personen verhängt werden. Dies setzt zum einen voraus, dass der Aufsichtspflichtige nicht bereits als Handelnder (§ 9 Abs. 2 OWiG) bebußt wird, und ihm zum anderen über § 9 OWiG die Unternehmenseigenschaft zugerechnet werden kann. Als Beispiel wird in der Literatur die Vorstandssekretärin genannt, für deren Handlung der Betriebsleiter im Sinne von § 9 Abs. 2 Nr. 1 OWiG aufsichtspflichtig ist.[22] Daneben ist erforderlich, dass der Aufsichtspflichtige vorsätzlich oder fahrlässig seine Aufsichtspflicht gegenüber der zu beaufsichtigenden Person dadurch verletzt, dass er schuldhaft unterlassen hat, die kartellrechtswidrige Handlung zu unterbinden. Einen solchen Verstoß könnte beispielsweise eine unterbliebene Unterrichtung des Mitarbeiters über die wesentlichen Verbote des Kartellrechts darstellen.

3.5 Haftstrafe und Geldstrafe

Unternehmensmitarbeitern, die sich an Kartellrechtsverstößen beteiligen, drohen Haft und Geldstrafen. Paradebeispiel für die Strafverfolgung von Wettbewerbsverstößen sind die USA. So mussten dort zwischen den Jahren 2003 und 2012 mehr als 250 Personen Haftstrafen antreten. Die durchschnittliche Dauer der verhängten Gefängnisstrafen betrug in den Jahren 2010 bis 2012 knapp 25 Monate. Unter den seit 1999 in US-Gefängnissen Inhaftierten befanden sich 31 Ausländer, darunter auch Deutsche. Die durchschnittliche

[20] *Klusmann*, in: Wiedemann (Hrsg.), Handbuch des Kartellrechts, 2. Aufl. 2008, § 55 Rn. 32, bezieht zum Beispiel auch sachbearbeitende Schreibkräfte in den Kreis dieser Personen ein, was in der Regel aber wohl den Begriff der „Eigenverantwortung" überdehnt und angesichts der Vermögensverhältnisse dieser Personen in der Regel für das Bundeskartellamt kaum interessant sein dürfte.

[21] *Dreher*, ZWeR 2004, 75, 83, 91.

[22] *Dreher*, ZWeR 2004, 75, 91.

Haftdauer bei Ausländern lag im Jahr 2011 bei 10 Monaten. Die USA drängen auch mit internationalen Haftbefehlen über Interpol auf die Auslieferung beschuldigter Personen. So hat Großbritannien den britischen Staatsbürger Ian Norris an die USA ausgeliefert, wo er inhaftiert wurde.[23] Für deutsche Staatsangehörige schließt zwar das Grundgesetz eine Auslieferung – zumindest in Länder außerhalb der Europäischen Union – aus.[24] Selbst ohne völkerrechtliches Auslieferungsabkommen kann ein deutscher Manager jedoch in die Lage geraten, Haft in den USA antreten zu müssen. Zum einen, wenn er sich dort zum Zeitpunkt der Verurteilung aufhält oder nach Verurteilung einreist. Zum anderen aber auch, falls ihn sein eigenes Unternehmen dazu bringt, sich zu stellen. Dies war im Jahr 2006 der Fall, als sieben koreanische Manager von Samsung ihre Teilnahme an einem Preiskartell gestanden und sich bereit erklärten, ihre Haft in den USA anzutreten.[25] Die strafrechtliche Verfolgung einzelner Personen wegen Verstößen gegen das Kartellrecht ist derzeit in 14 Ländern vorgesehen.[26]

In Deutschland drohen strafrechtliche Sanktionen demjenigen, der sich bei Ausschreibungen an wettbewerbswidrigen Absprachen beteiligt: Bis zu 5 Jahren Haft sind möglich (§ 298 StGB). Oft ist nicht bekannt, dass diese Strafvorschrift nicht nur öffentliche, sondern auch private Ausschreibungen schützt. Auch der Straftatbestand des Betruges (§ 263 StGB) kann bei Kartellrechtsverstößen erfüllt sein. Wegen Ausschreibungsbetruges (Submissionsabsprache) wurden zum Beispiel zweieinhalb Jahre Haft sowie eine Geldstrafe gegen den Vertreter eines Bauunternehmens verhängt, der bei der Vergabe von Aufträgen der Flughafen München GmbH (Bau des Franz-Josef-Strauss-Flughafens) an Preisabsprachen beteiligt war.[27]

3.6 Vorteilsabschöpfung

Durch die den Kartellbehörden eingeräumte Möglichkeit der Vorteilsabschöpfung kann sich der Ertrag und damit die Ausschüttung an die Gesellschafter mindern. Mindern kann sich folglich auch eine ertragsabhängige Tantieme für Mitglieder der Geschäftsleitung.

---

[23] Dem ging eine mehrjährige juristische Schlacht voraus, in der die Auslieferung zunächst daran scheiterte, dass das britische Recht zum Zeitpunkt der Tatbegehung einen Kartellrechtsverstoß nicht als Straftat qualifiziert hatte, im Ergebnis aber dann doch vollzogen wurde, weil Herrn Norris zudem die Straftat der „obstruction of justice" vorgeworfen werden konnte; siehe z. B. House of Lords, 12. März 2008, abrufbar unter www.publications.parliament.uk/pa/ld200708/ldjudgmt/jd080312/norris-1.htm und United States Court of Appeals for the Third Circuit, 15. März 2011, www.ca3.uscourts.gov/opinarch/104658np.pdf.

[24] Art. 16 Abs. 2 GG; das Auslieferungsverbot ist eingeschränkt bei einem Europäischen Haftbefehl.

[25] *Watson-Doig*, Crime and Competition. The Norris case and the future of competition enforcement, in: Competition Law Insight, 10. April 2006, S. 8, 9.

[26] Strafrechtliche Verfolgung ist vorgesehen in Australien, Frankreich, Griechenland, Großbritannien, Irland, Israel, Japan, Kanada, Korea, Norwegen, Nigeria (geplant), Mexico, Rumänien und den USA.

[27] BGH v. 11. Juli 2001–1 StR 576/00, NJW 2001, 3718: 300 Tagessätze à 300 €.

Hat ein Unternehmen durch einen schuldhaften Kartellrechtsverstoß einen wirtschaftlichen Vorteil erlangt, kann die Kartellbehörde die Abschöpfung dieses Vorteils anordnen und dem Unternehmen auferlegen, einen entsprechenden Geldbetrag zu zahlen.[28] Auch die Verbesserung der Marktposition eines Unternehmens stellt einen solchen wirtschaftlichen Vorteil dar.[29] Die Vorteilsabschöpfung ist subsidiär zur Geldbuße, soweit diese den wirtschaftlichen Vorteil abschöpft, und zu zivilrechtlichen Schadensersatzleistungen.[30]

3.7 Schadensersatz

Während bei der Bewertung von Risiken in Europa bis vor einigen Jahren ein etwaiges Bußgeld in der Regel mit dem höchsten Betrag ins Gewicht fiel, schlagen mittlerweile Schadensersatzansprüche (vermeintlicher) Kartellopfer in beachtlichem Maße zu Buche. Schadensersatzansprüche können die Höhe der Bußgelder sogar um ein Vielfaches übertreffen. Bislang richten sich in Deutschland Schadensersatzklagen gegen Unternehmen; Ansprüche gegen Mitarbeiter, die durch ihr Handeln den Kartellverstoß begangen haben, sollen nach deutschem Recht aber nicht auszuschließen sein.[31] In den USA sind kartellrechtliche Schadensersatzansprüche seit Langem ein fester Bestandteil des Rechtsschutzsystems. *Treble damages* (dreifacher Schadensersatz), *class actions* (Sammelklagen) und *pre-trial discovery* (die Möglichkeit, von der Gegenseite und von unbeteiligten Dritten umfassende Informationen zu allen Tatsachen einzufordern, die für den behaupteten Klageanspruch relevant sein können) fördern und erleichtern dort die Geltendmachung von Schadensersatzansprüchen.

In Europa ist ein starker Anstieg von Schadensersatzprozessen zu verzeichnen. Nach dem Urteil des Europäischen Gerichtshofes in der Sache Courage gegen Crehan[32] wäre das Kartellverbot nicht ausreichend wirkungsvoll, wenn nicht jedermann Schadensersatz für wettbewerbswidriges Verhalten erlangen könnte. Die Kommission hat sich auf die Fahnen geschrieben, die Ausübung des Rechts auf Erhebung von Schadenersatz wegen Wettbewerbsrechtsverletzungen (*private enforcement*) zu erleichtern. So hat sie 2005 ein Grünbuch zur privaten Kartellrechtsdurchsetzung veröffentlicht und im April 2008 ein Weißbuch folgen lassen. Am 11. Juni 2013 soll das Kollegium der Kommissare Legislativ-Maßnahmen beschließen. Seit einigen Jahren fördert die Kommission die Kartellrechtsdurchsetzung durch Private derweil dadurch, dass sie in ihre Pressemitteilungen über die Verhängung von Geldbußen immer den Hinweis aufnimmt, betroffene Personen oder Unternehmen könnten vor den Gerichten der Mitgliedstaaten Klage auf Schadenersatz erheben und sich zum Beweis, dass das Verhalten tatsächlich stattgefunden hat und

[28] § 34 GWB.

[29] *Bechtold*, GWB, 6. Aufl. 2010, § 34 Rn. 4.

[30] § 34 Abs. 2 GWB.

[31] So jedenfalls *Emmerich*, in: Immenga/Mestmäcker, GWB, 4. Aufl. 2007, § 33 Rn. 42.

[32] EuGH v. 20. September 2001– Rs. C-453/99.

rechtswidrig war, auf die veröffentlichte Entscheidung stützen. Außerdem hat sie, sozusagen, um mit gutem Beispiel voranzugehen, – in ihrer Eigenschaft als Nachfrager, nicht als Kartellbehörde – einen Schadensersatzprozess gegen die Mitglieder des Liftkartells begonnen.[33]

Erleichtert werden Klagen (sogenannte *follow-on* Klagen) auch dadurch, dass mittlerweile kein mitgliedstaatliches Gericht die rechtskräftige Feststellung eines Kartellrechtsverstoßes durch die Kartellbehörde eines anderen Mitgliedstaates in Frage stellen darf.[34] Außerdem können Anspruchsteller unter Umständen Auskünfte von Kartellbehörden erlangen, um ihre zivilrechtlichen Ansprüche leichter durchsetzen zu können; der Umfang des Auskunfts- und Akteneinsichtsrechts ist allerdings zur Zeit noch umstritten.[35]

In Deutschland sind mittlerweile mehrere Urteile ergangen, mit denen Schadensersatz zugesprochen wurde. Nach der Entscheidung „Durchschreibepapier" können nicht nur unmittelbare Abnehmer, sondern auch mittelbare Abnehmer Schadensersatz verlangen.[36] Auch in anderen EU-Mitgliedstaaten nehmen Schadensersatzprozesse auf Grund von Kartellverstößen stark zu.

3.8 Zivilrechtliche Unwirksamkeit

Vertragsbestimmungen, die gegen das Kartellrecht verstoßen, sind nichtig. Kaum jemand wird auf den Gedanken kommen, einen Kartellbruder auf Einhaltung einer rechtswidrigen Absprache zu verklagen. Abseits der Hardcore-Kartelle kann Compliance aber für sich genommen zulässige Kooperationsverträge mit Wettbewerbern oder wichtige Vertriebsverträge davor bewahren, ihren wirtschaftlichen Wert dadurch einzubüßen, dass zum Beispiel eine unzulässige Wettbewerbsbeschränkung den gesamten Vertrag oder wesentliche Teile undurchsetzbar macht. Die Nichtigkeit ermöglicht es etwa einer Partei, sich von einem unliebsamen Vertrag zu lösen oder zwingt zur Verhandlung neuer, ungünstigerer Konditionen. Compliance bezweckt in diesem Zusammenhang also nicht in erster Linie den Schutz vor Geldbußen, Strafen und Schadensersatz, sondern sichert die Wirksamkeit der für das Unternehmen wesentlichen Verträge.

---

[33] Pressemitteilung der Kommission IP/08/998 vom 24. Juni 2008. Der EuGH hat auf Grund einer Vorlagefrage durch das Zivilgericht entschieden, dass die Kommission einen solchen Schadensersatzanspruch geltend machen darf; Urteil vom 6. November 2012, Rechtssache C-199/11.

[34] Art. 16 Abs. 1 VO 1/2003.

[35] Siehe etwa *Janssen*, Einsicht in Kronzeugenakten – Was bedeutet das Pfleiderer-Urteil in der Praxis?; in: Schwerpunkte des Kartellrechts 2011, 19ff. AG Bonn v. 18. Januar 2012, WuW/E DE-R 3499– Pfleiderer II.

[36] BGH Urteil v. 28. Juni 2012 KZR75/10 („ORWI"), WuW/E DE-R 3431–3446.

3.9 Wertverlust des Unternehmens

Kartellrechtliche Compliance sichert den Unternehmenswert. Unternehmenskäufer und Investoren stellen in der Regel bereits in der Due Diligence Fragen zu möglichen Kartellverstößen und beziehen dies in die Kalkulation des Kaufpreises, zuweilen sogar in die Kaufentscheidung selbst ein. So groß wird das Risiko einer Minderung des Unternehmenswertes durch Kartellbußen angesehen, dass sich die Garantie des Verkäufers, die Zielgesellschaft habe das Kartellrecht eingehalten, heute in jedem Mustervertrag findet. Aber nicht nur der Käufer will keine Leichen im Keller. Das Risiko eines schlechteren Ratings – insbesondere bei Wiederholungstätern – und eines sinkenden Börsenkurses sind nicht von der Hand zu weisen. So verloren die Aktien von Kühne & Nagel 5 % und von Panalpina 2,5 % an Wert nachdem bekannt wurde, dass europäische und amerikanische Wettbewerbsbehörden diese Speditionsunternehmen durchsucht hatten;[37] der Kurs des Stahlunternehmens Voestalpine gab um mehrere Prozentpunkte nach, als die Presse berichtete, der Kronzeugenantrag des Unternehmens sei möglicherweise erfolglos.[38]

Kunden und Lieferanten können – möglicherweise zu Recht – dem überführten Unternehmen bei künftigen Verhandlungen die Angemessenheit des Preises in Abrede stellen oder sich für die Vergangenheit schadlos halten wollen.

Ein Kartellverstoß wird in der Öffentlichkeit heutzutage nicht mehr als unbeachtliches Kavaliersdelikt gesehen; den genannten Speditionsunternehmen sowie in jüngster Zeit den Mitgliedern des sogenannten „Schienenkartells" brachte ihr Erscheinen auf der Titelseite des Handelsblatts beachtliche Negativwerbung. Unternehmen, für die ein „sauberer Eindruck" in der Öffentlichkeit einen Wert darstellt, verlieren durch solche Schlagzeilen an Ansehen und müssen mit einigem PR-Aufwand gegensteuern.

3.10 Schadensersatz des Aufsichtsrats und des Vorstands an das Unternehmen

Gesellschaftsrechtliche Folgen eines Kartellverstoßes können insbesondere Aufsichtsrat und Vorstand in eine höchst diffizile Frontstellung gegeneinander bringen. Stellt das Bundeskartellamt fest, dass ein Vorstandsmitglied einen Verstoß selbst begangen oder seine Aufsichtspflicht verletzt hat, wird damit nämlich möglicherweise auch feststehen, dass diese Person ihren Anstellungsvertrag verletzt hat. Damit wird die Gesellschaft zum Schadensersatz berechtigt (§ 93 Abs. 2 AktG).[39] Der Aufsichtsrat muss dann nach den Grundsätzen der ARAG/ Garmenbeck-Entscheidung des BGH[40] „die Geltendmachung

[37] Handelsblatt vom 12. Oktober 2007, S. 1.

[38] http://diepresse.com/home/wirtschaft/boerse/677106/Kartellaffaere_Minikrise-bei-Voest.

[39] *Hauschka*, BB 2004, 1178 ff.

[40] BGH v. 21. April 1997– II ZR 175/95, BGHZ 235, 244 ff.

der Ansprüche gegen den Vorstand zumindest ernsthaft prüfen".[41] Sieht der Aufsichtsrat pflichtwidrig von einer Geltendmachung des Schadens gegen den Vorstand ab, macht er sich selbst Schadensersatzpflichtig (§ 116 i. V. m. § 93 Abs. 2 AktG).[42]

3.11 Arbeitsrechtliche Folgen

Begeht ein Arbeitnehmer einen Kartellrechtsverstoß, kann dies eine arbeitsvertragliche Pflichtwidrigkeit begründen. Dann steht dem Unternehmen das gesamte arbeitsrechtliche Instrumentarium von Verwarnung über Abmahnung und Versetzung bis zur Kündigung zur Verfügung. Das Arbeitsrecht richtet sich auch an Personen, die nicht von § 9 OWiG erfasst sind. In der Praxis sind diese arbeitsrechtlichen Fragen oft mit taktischen Aspekten in Einklang zu bringen, zum Beispiel mit der Überlegung, ob es sich das Unternehmen für eine effiziente Verteidigung leisten kann, auf die Kooperation dieses Arbeitnehmers zu verzichten.[43]

3.12 Hindernis bei der Vergabe von Aufträgen und für die Karriere

Ein formal nebensächlicher Aspekt kann sich für den Einzelnen in der Praxis erheblich auswirken: Verhängt das Bundeskartellamt gegen eine natürliche Person ein Bußgeld, wird dies im Gewerbezentralregister vermerkt.[44] Diese Person gilt dann nicht mehr als „zuverlässig" im gewerberechtlichen Sinne. In vielen Fällen müssen Unternehmen ihre gewerberechtliche Zuverlässigkeit nachweisen, und das gilt nicht immer für das Unternehmen abstrakt, sondern zuweilen auch für bestimmte Personen im Unternehmen. Diese Zuverlässigkeit aber kann eine Voraussetzung sein z. B. in einem Vergabeverfahren. Eine kartellrechtliche Bestrafung kann diese Person und damit das Unternehmen von der Vergabe möglicherweise ausschließen. Bei Bußgeldern über 300 € wird die Eintragung im Gewerbezentralregister nach fünf Jahren getilgt.[45] Ein persönliches Problem kann sich zudem für Manager börsennotierter Unternehmen ergeben. Für notierte Aktiengesellschaften gelten neben Corporate Governance-Regeln die Vorschriften des Börsengesetzes, gemäß denen die Börsenaufsichtsbehörde darauf hinzuwirken hat, dass kartellrechtliche Vorschriften eingehalten werden.[46] Die BaFin kann daher zum Beispiel darauf hinwirken,

---

[41] *Hauschka*, BB 2004, 1178 ff.

[42] BGH v. 21. April 1997– II ZR 175/95, BGHZ 235, 244 ff.; *Hefermehl/Spindler*, in: MüKo AktG, 3. Aufl. 2008, § 93 Rn. 124 ff.; ein Beispiel für eine straf- und aktienrechtliche Prüfung bietet das Schienenkartell, siehe Pressemitteilung vom 7. November 2012 auf www.thyssenkrupp.com.

[43] Für eine arbeitsrechtliche Pflicht, Verstöße dem Arbeitgeber offenzulegen *Rust/Abel,* ZWeR 2012, 521, 532.

[44] § 149 Abs. 2 Nr. 3 GewO.

[45] § 153 Abs. 1 Nr. 2 GewO.

[46] § 9 Börsengesetz.

dass am Kartell beteiligte Personen nicht in verantwortlicher Stellung in einem Unternehmen tätig sind oder werden. In Großbritannien können sowohl die Wettbewerbsbehörde (OFT) als auch das Gericht Personen verbieten, für mehrere Jahre als Geschäftsführer tätig zu werden (*disqualification order*).

3.13 Verfahrenskosten und Bindung von Mitarbeitern

Kartellverfahren können sich über mehrere Jahre erstrecken. Dies bedeutet nicht zu unterschätzende Belastungen für ein Unternehmen. So führt ein Bußgeldverfahren in der Regel dazu, dass sich Mitarbeiter für geraume Zeit nicht ihren eigentlichen Aufgaben widmen können, da sie eine erhebliche Menge an Informationen für das Verfahren zusammentragen müssen. Insbesondere für mittelständische Unternehmen mit einem verhältnismäßig kleinen Stamm nicht-operativer Mitarbeiter stellt dies eine große Belastung dar. Hinzu kommen die Kosten für externe Spezialisten, also Rechtsanwälte und zuweilen ökonomische Berater. Bei Verfahren in den USA oder anderen Staaten, in denen Kartellrecht Strafrecht ist, muss bedacht werden, dass während seiner Dauer die verdächtigten Manager längere Wartezeiten bei der Einreise einplanen müssen oder ohne vorherige Vereinbarung mit dem ermittelnden Staatsanwalt keine private oder geschäftliche Reise in die Vereinigten Staaten antreten können.

4 Kartellrechts-Compliance als Antwort – Was kann Compliance leisten?

4.1 Verstößen vorbeugen

Diese im vorherigen Abschnitt dargestellten Konsequenzen von Kartellrechtsverstößen für das Unternehmen, den Einzelnen und die Gesellschafter zeigen deutlich genug, dass es im ureignen Interesse aller Beteiligten liegt, Verstöße zu vermeiden. Kartellrechtliche Compliance muss daher zum Hauptzweck haben, durch organisatorische Maßnahmen Kartellrechtsverstößen vorzubeugen. Kein Verstoß bedeutet: Kein Bußgeld, kein Schadensersatz usw.

4.2 Vorbereitung auf den Ernstfall

Compliance muss auch vorbereiten, wie das Unternehmen reagieren soll, wenn es einen Verstoß erkennt oder es von Kartellbehörden damit konfrontiert wird. Festzulegen ist zum Beispiel, wie vorzugehen ist, wenn dem Unternehmen ein Fehlverhalten seiner Mitarbeiter bekannt wird: Wer berichtet an wen? Wer trifft letztlich die Entscheidung, ob eine Abstellung der Zuwiderhandlung ausreicht oder ob das Unternehmen darüber hinaus einen Kronzeugenantrag stellen sollte?

4.3 Aufsichtspflichtige enthaften

Kartellrechts-Compliance kann nach deutscher Rechtslage dazu dienen, die Unternehmensleitung vom Vorwurf einer Aufsichtspflichtverletzung zu entlasten. Aufsichtspflichtig gem. § 130 OWiG kann auch die Konzernmutter sein. Welche Anforderungen an die Geschäftsleiter und sonst verantwortlich Tätigen in den Obergesellschaften gestellt werden können, ist in der Literatur streitig.[47] Im Ergebnis wird eine konzernweite Compliance erforderlich sein, um das gesamte Management zu enthaften.

4.4 Geldbußen mindern

Das Bundeskartellamt hat in der Vergangenheit Compliance-Programme bei der Festsetzung der Höhe des Bußgeldes angeblich nicht berücksichtigt.[48] Die Kommission betrachtete zwar in einigen früheren Entscheidungen Compliance-Maßnahmen als mildernde Umstände,[49] doch hat sie inzwischen – etwa in ihrer Bußgeldentscheidung über das Aufzugskartell[50] – deutlich gemacht, dass sie solche Maßnahmen zukünftig nicht mehr berücksichtigen werde.[51]

Das britische OFT erkennt hingegen ausdrücklich als Bußgeld mindernd an, wenn das Unternehmen angemessene Schritte unternommen hat, um Verstöße zu vermeiden.[52] Auch die Sanktionsrichtlinien in den USA berücksichtigen wirksame Compliance-Programme als Bonusfaktor.[53]

---

[47] *Dreher*, Compliance Report, Heft 10, Oktober 2007, 3.

[48] *Pampel*, BB 2007, 1636.

[49] Europäische Kommission, 15. Juli 1992, ABl. L 233/27 ff. Rn. 24– VIHO/Parker Pen.

[50] Europäische Kommission, 21. Februar 2007.

[51] Vgl. Bolloré, EuG v. 26. April 2007– verbn. Rs. T -109/02 u.a; Danks Rørindustri, EuGH v. 28.6.2005– verb. Rs. C-189/02 P u. a. In einer öffentlichen Konsultation ist die Kommission von zahlreichen Teilnehmern dazu aufgerufen worden, Compliance-Programme als Bußgeld reduzierend zu behandeln; der Abschlussbericht der Kommission geht allerdings nicht auf diese Forderung ein; http://ec.europa.eu/competition/antitrust/legislation/regulations.html. Die im November 2011 von der Kommission veröffentlichte Broschüre „Compliance Matters" (Seite 20) hält die Existenz eines Compliance-Programms nicht für bußgeldmindernd.

[52] www.oft.gov.uk/shared_oft/business_leaflets/ca98_guidelines/oft423.pdf, Tz. 2.15.

[53] http://www.ussc.gov/Guidelines/2012_Guidelines/Manual_PDF/Chapter_8.pdf. Weitere rechtsvergleichende Hinweise bei *Voet van Vormizeele*, CCZ 2009, 41, 47.

5 Bestandteile eines effektiven Compliance-Programms – Wie muss Compliance organisiert sein?

5.1 Maßstab für Effizienz

Konkrete Feststellungen dazu, welchen Inhalt Compliance-Programme haben müssen, finden sich weder in der Praxis des BKartA noch der deutschen Gerichte, der Kommission oder des Gerichtshofs. So beschränkt sich die Kommission auf allgemeine Feststellungen.[54] Entscheidend ist, was das Unternehmen erreichen und welchen Aufwand es dafür in Kauf nehmen will.[55] In erster Linie wird Ziel die Haftungsvermeidung für das Unternehmen und das Führungspersonal sein. Dann ist die Aufsichtspflicht nach § 130 OWiG Ausgangspunkt für Vorschläge zum Inhalt und der Organisation der Kartellrechts-Compliance.[56] Denn das Führungspersonal kann mit einem effektiven Compliance-Programm nachweisen, dass es seiner Aufsichtspflicht nachgekommen ist, und auf diese Weise – anders als das Unternehmen (vgl. 4.4) – einer Geldbuße entgehen. Erforderlich aber auch ausreichend ist nach dem BGH das „realistisch Zumutbare"; „von starkem Misstrauen geprägte Aufsichtsmaßnahmen", die den Betriebsfrieden stören, können nicht verlangt werden.[57]

Das Compliance-Programm muss auf den Bedarf des jeweiligen Unternehmens zugeschnitten sein. Compliance-Maßnahmen sind von Unternehmen zu Unternehmen unterschiedlich und hängen von vielen Faktoren ab, wie zum Beispiel von der Größe des Unternehmens und vom Feld seiner Betätigung. Auch wird man festlegen müssen, in welchen Staaten das Unternehmen intensivere Compliance-Maßnahmen ergreifen muss und in welchen ein grobmaschigeres Vorgehen genügt.

Während es für bestimmte, vor allem große Unternehmen ratsam ist, ein ausgefeiltes, das heißt aber auch teures und personell aufwendiges Compliance-Programm aufzusetzen, bieten sich für kleinere Unternehmen schlankere Lösungen an. So schreibt die OFT in einem Merkblatt, dass kleinere Unternehmen möglicherweise kein formelles Compliance-Programm benötigen, sie aber dennoch sicherstellen müssten, dass ihre Mitarbeiter sich bewusst seien, wie wichtig die Einhaltung der kartellrechtlichen Regelungen sei und welche Konsequenzen sich aus einem Verstoß gegen die Wettbewerbsvorschriften ergeben

[54] *Pampel*, BB 2007, 1637, mit Verweis auf Kommission, 7. Dezember 1982, WuW/E EV 943, 946– National Panasonic, in der die Kommission sagt, es habe sich um ein „umfassendes, praktikables, detailliertes und sorgfältig abgewogenes Programm" gehandelt. Siehe auch die im November 2011 von der Kommission veröffentlichte Broschüre „Compliance Matters".

[55] Zur Bewertung von „Compliance Management Systemen" durch den Wirtschaftsprüfer hat das Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW) im März 2011 den Prüfstandard 980 verabschiedet.

[56] *Pampel*, BB 2007, 1637; *Dreher*, ZWeR 2004, 75, 93 f.

[57] BGH v. 11. März 1986 – KRB 7/85, WuW/E BGH 2262, 2264.

können.[58] Die Einsetzung eines Compliance-Beauftragten mag bereits einen wesentlichen Schritt zur Haftungsvermeidung darstellen.[59]

5.2 Kartellrechts-Compliance ist Chefsache

Nur wenn die Unternehmensleitung für Compliance eintritt, lohnt sich der Aufwand. Sie muss ihren Mitarbeitern deutlich zu verstehen geben, dass sie der Compliance einen angemessenen Stellenwert im Unternehmen gibt. Dies zeigt sich zum Beispiel dadurch, dass die wesentlichen Maßnahmen von der Unternehmensleitung angeordnet und kommuniziert werden. Delegiert sie diese Aufgaben zum Beispiel auf einen Compliance Officer, muss sichtbar werden, dass sie ihn stützt.

Dass die Mitglieder der Unternehmensleitung persönlich gefordert sind, ergibt sich aus den Urteilen zur Delegation von Aufsichtspflichten. Auch wenn danach die konkrete Durchführung von Instruktion, präventiver Kontrolle und repressiver Sanktionierung durch die Unternehmensleiter delegierbar ist, bleibt dem „Betriebsinhaber" im Sinne von § 130 OWiG beziehungsweise den bei juristischen Personen nach § 9 Abs. 1 OWiG verantwortlichen gesetzlichen Vertretern eine eigene „Oberaufsicht".[60]

5.3 Risikoanalyse

Im Vorfeld der Etablierung eines Compliance-Programms muss analysiert werden, in welchem Maße für das Unternehmen das Risiko von Kartellrechtsverstößen besteht. Bei einem erhöhten Risiko drängen sich verständlicherweise umfassendere Maßnahmen auf. Für die Analyse, ob und für welche Kartellrechtsverstöße das eigene Unternehmen anfällig ist, mögen folgende Fragen nützlich sein:[61]

- Ist das Unternehmen bereits einmal bebußt oder durchsucht worden?
- Sind Wettbewerber durchsucht oder bebußt worden?
- Gab es auf anderen Marktstufen (Lieferanten, Abnehmer) kartellrechtliche Ermittlungen?
- Hat mein Unternehmen eine marktbeherrschende Stellung auf einem der Märkte, auf dem es tätig ist? Nur dann ist ein Verstoß gegen das Missbrauchsverbot denkbar.
- Besteht für Mitarbeiter in den Bereichen Verkauf, Vertrieb, Marketing und Einkauf die Möglichkeit, ohne Kenntnis der Geschäftsführung mit Wettbewerbern wettbewerbs-

[58] Vgl. http://www.oft.gov.uk/shared_oft/business_leaflets/ca98_mini_guides/oft424.pdf.

[59] *Hauschka*, BB 2004, 1178 ff.

[60] *Dreher*, ZWeR 2004, 75, 94 f.; vgl. auch Kap. 1, 10 f.

[61] Vgl. http://www.oft.gov.uk/shared_oft/business_leaflets/ca98_mini_guides/oft424.pdf÷ *Kapp*, Kartellrecht in der Unternehmenspraxis, 2. Aufl. 2013, 279 ff.

widrige Vereinbarungen zu treffen, insbesondere Preiserhöhungen zu kommunizieren, Gebiete und Kundenkreise abzusprechen?
- Haben Angestellte, haben Führungskräfte regelmäßigen Kontakt mit Wettbewerbern? Auf welchen Foren trifft man sich (zum Beispiel in Verbänden)? Welche Informationen werden dort ausgetauscht?
- Ist die Branche durch einen starken Wettbewerb gekennzeichnet oder sind die Verhältnisse seit längerem unverändert?
- Sind viele oder wenige Wettbewerber in der Branche tätig?
- Wissen die Wettbewerber viel oder wenig über die geschäftlichen Tätigkeiten des jeweils anderen?
- Gibt es gemeinsame Marktinformationssysteme?
- Welche Kooperationen mit Wettbewerbern bestehen?

Die Risikoanalyse ist auch insoweit von Bedeutung, als unter bestimmten Voraussetzungen höhere Anforderungen an die Kartellrechts-Compliance zu stellen sind. Zum Beispiel dann, wenn konkrete Anhaltspunkte für den Verdacht bestehen, dass sich Unternehmensmitarbeiter an Kartellrechtsverstößen beteiligen oder in einer bestimmten Branche Submissionsabsprachen gehäuft vorkommen. Dann können z. B. häufigere Schulungen, Einzelgespräche oder gezielte Überwachung erforderlich werden.[62] Zur Risikoabschätzung gehört auch die Frage, ob Unternehmensmitarbeiter, die mit Aufgaben betraut werden sollen, die „zu kartellrechtsrelevantem Handeln führen", sorgfältig ausgewählt werden.[63]

5.4 Instruktion der Mitarbeiter

Ziel der Instruktion ist es, Kenntnisse über die kartellrechtlichen Verbote und ihren Zweck zu vermitteln. Die Hinweise müssen auf die Branche und die jeweilige Tätigkeit zugeschnitten sein. Nichtjuristen müssen sie verstehen können. Gerade die haftungsträchtigen Kernbeschränkungen lassen sich leicht erklären. Die Wertungen werden in der Regel von allen – zumindest abstrakt – geteilt. Typische Beispiele müssen gebracht und konkrete Handlungsanweisungen gegeben werden. Wer etwa an Treffen, auf denen wettbewerbswidrige Inhalte besprochen werden, teilnimmt, muss sich „offen vom Inhalt der Sitzungen distanzier[en]"[64] oder Umstände nachweisen, „aus denen sich eindeutig eine fehlende wettbewerbswidrige Einstellung bei der Teilnahme an Sitzungen ergibt".[65] Grenzfälle – oder Unklarheiten in der Rechtslage – müssen die Mitarbeiter nicht selbst entscheiden. Es geht nicht darum, Kartellrechtsspezialisten auszubilden oder unternehmerische Spielräume einzuengen. Im Kern geht es um eine Sensibilisierung der Mitarbeiter.

---

[62] *Dreher*, ZWeR 2004, 75, 95.

[63] KG v. 25. Juli 1980– Kart 26/79, WuW/E OLG 2330, 2332– Revisionsabteilung.

[64] Sarriò gegen Kommission, EuG v. 14. 5. 1998– Rs T – 334/94, Slg. 1998 II, 1439.

[65] Hüls gegen Kommission, EuGH v. 8.7.1999– Rs C – 199/92 P, Slg. 1999 I, 4287.

Für subjektive Unsicherheiten und objektive Zweifelsfälle muss organisatorisch gesichert sein, dass sich der betroffene Mitarbeiter an einen Zuständigen wenden kann. Allgemeine Hinweise nach dem Motto, bei Problemen die Rechtsabteilung einzuschalten oder das Kartellrecht zu beachten, sieht die Rechtsprechung als unzureichend für eine Enthaftung nach § 130 OWiG an.[66]

Das einfachste Mittel zur Durchführung von Instruktionen sind Mitarbeiterschulungen. Je nach Größe des Unternehmens und des betroffenen Personenkreises können sie als Präsenz-Schulungen oder elektronisch durchgeführt werden. Präsenz-Schulungen sind in fast jeder Hinsicht vorzugswürdig. Sie erlauben eine Interaktion und gewähren auch der Unternehmensleitung zuweilen einen überraschenden Einblick in die Gepflogenheiten ihrer Mitarbeiter. Die Mitarbeiter sollten im Vorfeld von Schulungen um ihre Fragen und Anmerkungen gebeten werden. Schriftliche Kartellrechts-Richtlinien können dies unterstützen, wobei man sich über die Lektüre von „Handbüchern", insbesondere durch Nicht-Juristen keine Illusionen machen sollte. Kurz gefasste Richtlinien helfen jedoch den Mitarbeitern, nach eigenem Belieben nachzulesen, und erlauben es der Unternehmensleitung, sich auf sie zu berufen.[67] Die wesentlichen Informationen passen oft auf ein personalausweisgroßes Format.[68] Die Teilnahme an einer Schulung und gegebenenfalls den Empfang und das Lesen der Richtlinien sollten die Mitarbeiter schriftlich bestätigen. Je nach Unternehmen, Branche und Personalfluktuation müssen die Schulungen nach längeren oders kürzeren Abständen wiederholt werden.

5.5 Motivation

Will die Unternehmensleitung eine Compliance-Kultur in ihrem Unternehmen durchsetzen, muss sie mit gutem Beispiel vorangehen. Dazu kann auch gehören, die Vergütungsanreize zu überdenken und neu festzusetzen. Eine einfache Maßnahme ist die Formulierung einer Compliance-Policy, an die sich alle im Unternehmen halten müssen. ThyssenKrupp reagierte auf für das Unternehmen teure Enthüllungen mit einer besonderen Form der Mitarbeitermotivation: Es setzte ein zeitlich befristetes Amnestieprogramm auf, dass Arbeitnehmer von Schadensersatzansprüchen des Unternehmens freistellt und sie vor Kündigungen schützt.[69]

5.6 Kontrolle

Bestandteil einer effektiven Kartellrechts-Compliance können auch regelmäßige Überwachungsmaßnahmen sein, um sicherzustellen, dass keine Kartellrechtsverstöße begangen

[66] KG v. 25. Juli 1980– Kart 26/79, WuW/E OLG 2230, 2232– Revisonsabteilung.

[67] Vgl. *Dreher*, ZWeR 2004, 75, 98.

[68] Siehe zum Beispiel die Do's & Don'ts im Kartellrecht auf www.luther-lawfirm.com.

[69] Pressemeldung vom 16. April 2013 auf www.thyssenkrupp.com.

werden. Hinzuweisen ist dabei zum einen auf die Auswahl eines Ansprechpartners für Zweifelsfragen, etwa in der Rechtsabteilung des Unternehmens. Dabei ist es wichtig, den Aufgaben- und Verantwortungsbereich dieses Ansprechpartners genau abzugrenzen, wobei die Oberaufsicht nach der Rechtsprechung immer bei der Geschäftsleitung bleibt.[70]

Zum anderen ist auf den Punkt „stichprobenhafte Prüfungen" hinzuweisen, den die Rechtsprechung bei verschiedenen Gelegenheiten behandelt hat. So stellte der BGH etwa fest: „Das Kammergericht geht zu Recht davon aus, dass der Betroffene die Revisionsabteilung so hätte organisieren müssen, dass sie in der Lage gewesen wäre, in allen Verkaufsbüros wenigstens stichprobenartige überraschende Prüfungen durchzuführen. Derartige Prüfungen sind erforderlich und regelmäßig auch geeignet, vorsätzliche Zuwiderhandlungen gegen gesetzliche Vorschriften und Anweisungen der Betriebsleitung zu verhindern, denn sie halten den Betriebsangehörigen vor Augen, dass solche Verstöße entdeckt und gegebenenfalls geahndet werden können. Für weitergehende Kontrollen musste der Betroffene im vorliegenden Fall nicht sorgen."[71]

5.7 Zuwiderhandlung abstellen

Stellt die Compliance-Organisation einen Verstoß fest, muss das Unternehmen sehr schnell die Schwere und das Risiko der Entdeckung bewerten. Entschließt sich das Unternehmen daraufhin, die Zuwiderhandlung abzustellen, muss es damit rechnen, dass die anderen beteiligten Unternehmen unruhig werden und eventuell selbst einen Kronzeugenantrag stellen. Dann beginnt ein Wettrennen zu den Kartellbehörden, denn für die Gewährung des Kronzeugenstatus gilt das Windhundprinzip.

5.8 Dokumentation

Die Instruktion und die Überwachungsmaßnahmen sollten dokumentiert werden. Dies ermöglicht eine frühzeitige und sachgerechte Reaktion der Unternehmensleitung und ihrer rechtlichen Berater. Werden zum Beispiel abgelehnte Avancen von Wettbewerbern dokumentiert, kann man sich bei Ermittlungen durch die Kartellbehörden leicht entlasten und somit den Aufwand des Verfahrens reduzieren.

Individuell zu beantworten ist die Frage, was genau und in welchem Umfang das Unternehmen dokumentieren soll. Dies gilt besonders für den Fall, dass ein Unternehmen bei der Kontrolle seiner Mitarbeiter Verstöße aufdeckt. Selbst wenn das Verhalten sofort abgestellt wird, nimmt die Dokumentation, sollte sie bei späteren Ermittlungen in die Hände der Wettbewerbsbehörden gelangen, dem Unternehmen wesentliche Verteidigungsmöglichkeiten.

---

[70] Vgl. *Dreher*, ZWeR 2004, 75, 99.

[71] BGH, Beschl. v. 24. März 1981– KRB 4/80, wistra 1982, 34.

Das Problem stellt sich mit aller Schärfe, da nach derzeitiger Rechtslage solche Dokumente beim Compliance-Officer oder beim Syndikus des Unternehmens nicht sicher vor Beschlagnahme sind: Nach der – im Urteil AKZO[72] bekräftigten – Rechtsprechung der europäischen Gerichte erfasst das *Legal Privilege* nicht die Korrespondenz mit einem Syndikusanwalt. Einzig die Korrespondenz mit unabhängigen unternehmensexternen Anwälten ist – ermittelt die Europäische Kommission – geschützt. Ermittelt hingegen das Bundeskartellamt, kommt es jedoch auf das deutsche Recht an, und die deutschen Gerichte beantworten die Frage, ob die Unterlagen eines Syndikusanwalts beschlagnahmefrei sind, uneinheitlich.[73] Sicher beschlagnahmefrei ist nach europäischem und deutschem Recht Anwaltskorrespondenz (Korrespondenz an Anwälte und von Anwälten) im Rahmen eines laufenden Straf- und Ordnungswidrigkeitenverfahrens. Nach europäischem Recht darf die Kommission nicht Einsicht nehmen in Dokumente des Unternehmens, die erstellt wurden, um damit zur Ausübung von Verteidigungsrechten Rechtsrat zu ersuchen. Dies gilt nach europäischem Recht selbst dann, wenn diese Dokumente dem Anwalt (noch) nicht übermittelt wurden.[74] In Deutschland wird die Beschlagnahmefreiheit restriktiver gehandhabt. Beschlagnahmefrei sind die Unterlagen hier nur dann, wenn sie sich im alleinigen Gewahrsam eines externen Rechtsanwalts befinden und auch das nur solange das Anwaltsprivileg zum Schutz der Dokumente vor dem Zugriff der Behörden nicht missbraucht wird.[75] Insbesondere Compliance-Officer, die kartellrechtlich bedenkliches Handeln von Mitarbeitern identifizieren und dokumentieren, müssen sich genau darüber informieren, ob und wie sie im Sinne des Unternehmens Notizen und Berichte verfassen.

5.9 Sanktion

Ebenfalls Bestandteil einer effektiven Kartellrechts-Compliance ist eine Sanktionierung von Kartellrechtsverstößen.[76] Denn nur so kann ein Unternehmen glaubwürdig zeigen, dass es einen Kartellrechtsverstoß nicht augenzwinkernd als Kavaliersdelikt durchgehen lässt. Eine Sanktionierung von Kartellrechtsverstößen erhöht insbesondere die Aufmerksamkeit und schreckt ab.

Treten Kartellrechtsverstöße trotz Compliance-Maßnahmen ein, kann es angezeigt sein, arbeitsrechtliche Konsequenzen gegen den betroffenen Mitarbeiter einzuleiten. Allerdings

[72] EuGH v. 14. September 2010, Rs. C-550/07, WuW/E EU-R 1763.

[73] *Schumacher*, Compliance Report, Heft 10, Oktober 2007, 12 f.

[74] EuGH, Urteil vom 14. September 2010– Akzo – C-550/07.

[75] So zumindest LG Mannheim, Beschluss vom 3. Juli 2012, Az. 24 Qs 1/12 und 2/12. Nach LG Hamburg, Beschluss vom 15. Oktober 2012, Az. 608 Qs 18/10 besteht kein Beschlagnahmeverbot für Ergebnisse, die eine Anwaltskanzlei bei unternehmensinternen Ermittlungen zusammengetragen hat.

[76] *Dreher*, ZWeR 2004, 75, 100.

kann der Rechtsprechung keine Verpflichtung entnommen werden, Unternehmensmitarbeitern ohne weiteren Anlass für den Fall eines Kartellrechtsverstoßes arbeitsrechtliche Sanktionen anzudrohen.[77]

5.10 Krisenmanagement

Keine organisatorische Vorkehrung kann Verstöße ausschließen. Eine gute Compliance-Organisation entdeckt unvorhergesehene Regelwidrigkeiten jedoch früher oder später. Für diesen Fall muss die Unternehmensleitung sich zumindest ihre wesentlichen Reaktionen vorab überlegen. Wie will man bei einem Verstoß reagieren? Man kann sicherlich keine allgemein richtige Antwort geben. Aber zumindest sollte klar sein, dass ein solcher Fall höchste Priorität genießt, wer in der Geschäftsleitung sich um die Vorbereitung einer Entscheidung kümmert und was man dokumentiert. Zum Standard gehört auch ein Notfallplan für den Fall, dass Kartellbehörden das Unternehmen durchsuchen.[78]

[77] BGH, v. 24. März 1981– KRB 4/80, wistra 1982, 34.

[78] *Kapp*, Kartellbehörde durchsucht Geschäftsräume – Was ist zu beachten? Compliance Report, Heft 10, Oktober 2007, 3–5.

Compliance in der arbeitsrechtlichen Praxis

Katrin Süßbrich und Eva Rütz

Inhaltsverzeichnis

K. Süßbrich (✉) · E. Rütz
Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: katrin.suessbrich@luther-lawfirm.com

E. Rütz
E-Mail: eva.ruetz@luther-lawfirm.com

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2_11, © Springer Fachmedien Wiesbaden 2013

Zusammenfassung

Die in den letzten Jahren steigende Zahl medienpräsenter Korruptions-, Datenüberwachungs- und Veruntreuungsskandale zeigt die Notwendigkeit funktionierender Compliance-Systeme auch und gerade unter arbeitsrechtlichen Gesichtspunkten mehr denn je. Denn bei einer Verletzung arbeitsrechtlicher Vorschriften drohen empfindliche (materielle und immaterielle) Schäden sowohl für das Unternehmen als auch für die persönlich haftenden Organe. Nicht umsonst definierte ein amerikanischer Anwalt im Juve-Branchenblatt Compliance als „die Kunst der Unternehmensjuristen, dem Vorstand den Knast zu ersparen" (*Hauschka*, ZRP 2006, 258). Auch wenn es seit dem Inkrafttreten des Allgemeinen Gleichbehandlungsgesetzes (AGG) im Jahr 2006 glücklicherweise nicht zu der vielfach befürchteten Flut von Schadensersatz- und Entschädigungsklagen gekommen ist und vor dem Hintergrund der deutschen Rechtsprechungspraxis insbesondere Entschädigungssummen nach amerikanischem oder britischem „Vorbild" bisher ausgeblieben sind (die Deutsche Bank wurde 2006 von einem Londoner Gericht zur Zahlung von Schadensersatz in Höhe von 1,2 Mio. € an ein Mobbingopfer verurteilt), sind Organisationsmaßnahmen, die bereits im Vorfeld möglicher Rechtsverletzungen ansetzen, für den Arbeitgeber unerlässlich. Dabei sollten die Handlungs- und Organisationspflichten des Arbeitgebers indes nicht alleiniger Beweggrund für die Einführung von Compliance-Systemen sein. Vielmehr muss mit Blick auf die Zukunft des Unternehmens auch das Interesse an der Vermeidung von Imageschäden als tragender Aspekt hinzukommen. Denn Reputationsverluste führen neben einer Verminderung der Unternehmensattraktivität für gute Bewerber auch zu einem Rückgang der Mitarbeitermotivation und damit der Leistungsfähigkeit des Unternehmens insgesamt (*Müller-Bonanni/Sagan*, BB-Special 2008, 28, 29). Ein weiterer, sicherlich ebenso wichtiger Aspekt ist im Bereich der innerbetrieblichen Transparenz und Aufklärung zu sehen. Compliance-Systeme dienen auch dem ordnungsgemäßen Umgang mit dem Verdacht unrechtmäßigen oder pflichtwidrigen Verhaltens der Arbeitnehmer. Eine auf der Grundlage wirksamer Compliance-Systeme erfolgte Dokumentation der Verdachtsmomente und des Untersuchungsgangs bieten deshalb die Grundlage für arbeitsrechtliche Maßnahmen und Sanktionen (*Müller-Bonanni/Sagan*, a.a.O.).

Funktionierende Compliance-Systeme erwachsen allerdings nicht aus dem Nichts. Sie bedürfen vielmehr einer verbindlichen Einführung im Unternehmen, die je nach Größe und (Personal-) Struktur des Unternehmens unterschiedlich ausgestaltet werden kann und sollte.

Compliance ist also nicht Selbstzweck, sondern dient der Vermeidung von Haftungsrisiken, zur Imagepflege und als Basis für arbeitsrechtliche Maßnahmen. Vor diesem Hintergrund sollen die Problemfelder und haftungsrechtlichen „Minengebiete" im Zusammenhang mit Compliance unter arbeitsrechtlichen Gesichtspunkten beleuchtet werden (1.). Im Anschluss daran werden die Möglichkeiten zur verbindlichen Einführung wirksamer Compliance-Systeme im Unternehmen am Beispiel von Ethik-

richtlinien sowie damit zusammenhängende Einzelfragen dargestellt (2. und 3.). Den Abschluss bilden die Informationserfassung im Rahmen der Compliance am Sonderfall des Whistleblowings (4.) und die bei Compliance-Verstößen zu ergreifenden arbeitgeberseitigen Maßnahmen (5.).

1 Arbeitsrechtliche Vorschriften mit Haftungsrisiko

1.1 „Klassischer" Arbeitsschutz

Dem Arbeitgeber obliegen in Bezug auf seine Arbeitnehmer unabdingbare Fürsorgepflichten. Hierzu zählt insbesondere die Verpflichtung, die Arbeitnehmer an ihrem Arbeitsplatz und bei der Arbeitsleistung vor gesundheitlichen Gefahren zu schützen (§§ 618, 619 BGB, 62 HGB). Eine Konkretisierung dieser aus dem Arbeitsverhältnis selbst erwachsenden Fürsorgepflicht erfolgt inzwischen durch eine Vielzahl von öffentlich-rechtlichen Schutzvorschriften.

Die Beachtung der Arbeitsschutzbestimmungen und die damit verbundene Verhütung von Arbeitsunfällen und Betriebskrankheiten sind deshalb an erster Stelle zu nennen, weil Pflichtverletzungen des Arbeitgebers in diesem Bereich zu Personen- und Sachschäden in erheblichem Umfang führen können. Verletzt der Arbeitgeber dabei vorsätzlich oder grob fahrlässig seine Pflichten, kann ihn die Berufsgenossenschaft z. B. in die Regresspflicht nehmen (§ 110 Abs. 1 Satz 1 SGB VII).

Zu den wichtigsten gesetzlichen Arbeitsschutzvorschriften – eines der ältesten Arbeitsrechtsthemen schlechthin – zählt insbesondere das Arbeitsschutzgesetz (ArbSchG). Des Weiteren sind neben den Beschäftigungsverboten für bestimmte Personengruppen (z. B. im Mutterschutzgesetz (MuSchG), Jugendarbeitsschutzgesetz (JArbSchG) und in der Kinderarbeitsschutzverordnung (KindArbSchV)) das Arbeitssicherheitsgesetz (ASiG) mit seiner Verpflichtung zur Bestellung von Betriebsärzten und Fachkräften für Arbeitssicherheit[1] sowie die von den Berufsgenossenschaften erlassenen Arbeitsschutz- und Unfallverhütungsvorschriften zu beachten. Im Einzelfall sind daneben besondere Vorschriften, z. B. die Bildschirmarbeitsverordnung für Bildschirmarbeitsplätze (BildscharbV), zu berücksichtigen, deren Verletzung mit Bußgeld sanktioniert ist.

In den Bereich des Arbeitsschutzes fällt schließlich auch das Arbeitszeitgesetz (ArbZG). § 3 ArbZG sieht vor, dass die werktägliche Arbeitszeit acht Stunden nicht überschreiten darf. Die Arbeitszeit kann indes auf bis zu zehn Stunden verlängert werden, wenn innerhalb von sechs Kalendermonaten oder 24 Wochen im Durchschnitt wieder acht Stunden erreicht werden. Daneben sind die gesetzlich vorgegebenen Pausen (30 bis 45 min. bei einer

[1] Diese Pflicht trifft gemäß §§ 1, 2, 5 ASiG nur Unternehmen, bei denen dies u. a. aufgrund ihrer Betriebsart, der Zahl der Beschäftigten, Zusammensetzung der Arbeitnehmerschaft und Betriebsorganisation erforderlich ist. Die konkretisierende behördliche Anordnung ergeht auf der Grundlage des § 12 ASiG.

Arbeitszeit über sechs Stunden) und Ruhezeiten (grundsätzlich elf Stunden) zu beachten. Verletzungen der arbeitszeitrechtlichen Vorschriften werden als Ordnungswidrigkeiten mit einer Geldbuße von bis zu 15.000,00 € geahndet, wobei diese Geldbuße für jeden einzelnen Verstoß – ggf. auch wiederholt – verhängt werden kann. Im Falle einer beharrlichen Wiederholung oder einer Gefährdung der Gesundheit oder Arbeitskraft eines Arbeitnehmers liegt sogar eine Straftat vor (§ 23 ArbZG).

1.2 Sozialversicherung

Bedeutende finanzielle Haftungsrisiken für den Arbeitgeber ergeben sich insbesondere im Bereich der Sozialversicherung. Schuldner der Sozialversicherungsabgaben (Beiträge zur gesetzlichen Kranken-, Pflege-, Renten- und Arbeitslosenversicherung) ist alleine der Arbeitgeber, wobei sich die Schuldnerstellung ausdrücklich auf den Gesamtsozialversicherungsbeitrag und damit gerade nicht nur auf den Arbeitgeberanteil erstreckt (§ 28e Abs. 1 Satz 1 SGB IV). Der Arbeitgeber hat mithin unbedingt die ordnungsgemäße Abführung aller Sozialversicherungsabgaben sicherzustellen. Hinzu kommt, dass dem Arbeitgeber zwar gegen den Arbeitnehmer ein Ausgleichsanspruch in Höhe des auf den Arbeitnehmer entfallenden Beitragsteils zusteht. Dieser Anspruch kann indes nur durch Abzug vom Arbeitsentgelt und insbesondere nur bei den nächsten drei Lohn- oder Gehaltszahlungen, also für maximal drei Monate, durchgesetzt werden (§ 28g Satz 3 SGB IV).

Die nicht rechtzeitige oder nicht vollständige Erfüllung dieser Pflicht fällt nach § 266a des Strafgesetzbuchs (StGB) darüber hinaus unter den Straftatbestand des sog. „Sozialversicherungsbetrugs". Als „Täter" sieht das StGB insoweit den Arbeitgeber an. Persönlich sind damit aber die Organe der Gesellschaften in der Pflicht (§ 14 Abs. 1 StGB).[2] Die Vorschrift des § 266a Abs. 1 StGB ist daneben als Schutzgesetz im Sinne des § 823 Abs. 2 BGB zugunsten der Sozialversicherungsträger anerkannt und führt auf diesem Wege auch zu zivilrechtlichen Schadensersatzpflichten.[3]

In diesem Zusammenhang spielt auch die Problematik der Scheinselbstständigkeit eine entscheidende Rolle. Scheinselbstständigkeit liegt vor, wenn ein Vertragsverhältnis zwar als selbstständiger Dienst- oder Werkvertrag bezeichnet und behandelt wird, tatsächlich aber nichtselbstständige Arbeit in einem Arbeitsverhältnis geleistet wird.[4] Denn der Arbeitgeber muss bei der für den Einzug der Sozialversicherungsabgaben zuständigen Stelle jeden bei ihm Beschäftigten melden. Beschäftigt i. d. S. ist indes nur derjenige, der nicht selbstständige Arbeit verrichtet (§ 7 Abs. 1 SGB IV). Die Abgrenzung zwischen selbstständiger und nicht selbstständiger Arbeit ist in vielen Fällen schwierig und bedarf einer

[2] Zur Verantwortung eines GmbH-Geschäftsführers in der finanziellen Krise der Gesellschaft etwa: BGH v. 9.1.2001 – VI ZR 407/99, NJW 2001, 969 ff.; zuletzt bestätigt durch BGH v. 16.2.2012 – IX ZR 218/10, MDR 2012, 660 f.

[3] BGH v. 25.9.2006 – II ZR 108/05, ZIP 2006, 2127 f. v. 21.1.1997 – VI ZR 338/95, BGHZ 134, 304 ff.

[4] *Umnuß/Dworschak/Scheele*, in: Umnuß, Corporate Compliance Checklisten, 2012, 1. Kapitel, Rn. 144.

umfassenden Abwägung aller Umstände des Einzelfalls. In Zweifelsfällen sollte das Statusfeststellungsverfahren bei der Deutschen Rentenversicherung Bund gemäß § 7a Abs. 1 Satz 1 SGB IV durchgeführt werden. Denn Scheinselbstständige, die nach außen wie selbstständig tätige Unternehmer auftreten, faktisch jedoch weisungsgebunden sind, gelten sozialversicherungsrechtlich als Beschäftigte.[5] Liegt eine Scheinselbstständigkeit vor, muss der Arbeitgeber jedoch mit Wirkung für die Vergangenheit – ggf. bis zum Ablauf der Verjährungsfrist von vier Jahren (bei Vorsatz gilt eine Verjährungsfrist von 30 Jahren!) (§ 25 Abs. 1 SGB IV)– die Gesamtsozialversicherungsbeiträge nachzahlen. Ein Erstattungsanspruch gegen den Arbeitnehmer besteht auch insoweit nur für die letzten drei Monate (§ 28g Satz 3 SGB IV). Hält man sich vor Augen, dass die Gesamtsozialversicherungsabgaben zur Zeit ca. 40 % der dem Arbeitnehmer gewährten Vergütung betragen und alleine durch die Beitragsbemessungsgrenze[6] gedeckelt sind, wird deutlich, welches (finanzielle) Haftungsrisiko sich hier verbirgt. Daneben tritt auch insoweit wieder die strafrechtliche Verantwortung gemäß § 266a StGB.[7]

1.3 AGG

Das Allgemeine Gleichbehandlungsgesetz (AGG) dürfte in den vergangenen Jahren das am häufigsten diskutierte Compliance-Thema in den Unternehmen gewesen sein. Eine Vielzahl von Unternehmen sind in dieser Zeit der in § 12 Abs. 1 und Abs. 2 AGG normierten Pflicht des Arbeitgebers nachgekommen, (vorbeugende) Maßnahmen zum Schutz der Arbeitnehmer vor Diskriminierungen zu treffen und haben ihre Mitarbeiter durch Personalschulungen oder E-Learning-Angebote zum AGG geschult. Darüber hinaus sind sog. „codes of conduct" (Ethikrichtlinien oder Verhaltenskodizes) und „Whistleblower-Hotlines" zumindest in großen Unternehmen vielfach schon gängige Praxis.[8] Das AGG schützt vor Diskriminierungen (das Gesetz verwendet insoweit den Begriff der „Benachteiligung") aus Gründen der Rasse oder ethnischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität. Dabei

---

[5] Vgl. auch *Pelz/Steffek,* in: Hauschka (Hrsg.), Corporate Compliance, 2007, § 19 D Rn. 33 m. w. N.

[6] Die Beitragsbemessungsgrenze im Jahr 2013 für die Rentenversicherung liegt in Ostdeutschland bei 58.800 € brutto p.a. (4.900 € brutto per Monat) bzw. in Westdeutschland bei 69.600 € brutto p.a. (5.800 € brutto per Monat). Für die Kranken- und Pflegeversicherung liegt sie im Jahr 2013 bundeseinheitlich bei 47.250 € brutto jährlich (3.937,50 € brutto monatlich).

[7] BGH v. 7.10.2009 – 1 StR 478/03, NStZ 2010, 337 f.; LG Ravensburg v. 26.9.2006 – 4 Ns 24 Js 22865/03, StV 2007, 412 ff.; *Wagner*, in: MüKo BGB, 5. Aufl. 2009, § 823, Rn. 405 ff.

[8] Zu der Frage, ob der Arbeitgeber durch die Implementierung von Ethikrichtlinien bereits seiner Pflicht aus § 12 Abs. 1 AGG genügt, vgl. zutreffend kritisch *Schneider/Sittard*, NZA 2007, 654 ff.; generell zu der Einführung von Ethikrichtlinien und der Einführung von Whistleblowing-Hotlines *Wiederholt/Walter*, BB 2011, 968 ff.; *Sieg*, in: Festschrift zum 70. Geburtstag von Herbert Bruchner, 859 ff.; *Simonet*, Die Implementierung interner Whistleblowingsysteme im Rahmen der Corporate Governance, 2012; *Schulz*, BB 2011, 629 ff.; *Fahrig,* Die Einführung eines Verhaltenskodexes und das Whistleblowing, 2010.

sieht das Gesetz fünf Formen der Benachteiligung vor. Die unmittelbare und die mittelbare Benachteiligung, die Belästigung und die sexuelle Belästigung sowie die Anweisung zur Benachteiligung. Nicht nur inhaltlich bietet das AGG mithin einen umfassenden Schutz für die Arbeitnehmer. Vielmehr ist auch der sachliche und persönliche Anwendungsbereich des arbeitsrechtlichen Teils des AGG weit gefasst. So sind insbesondere Diskriminierungen in Bezug auf Arbeitsbedingungen einschließlich Arbeitsentgelt und Entlassungsbedingungen, insbesondere in individual- und kollektivrechtlichen Vereinbarungen sowie Maßnahmen bei der Durchführung und Beendigung eines Beschäftigungsverhältnisses unzulässig (§ 2 Abs. 1 Nr. 2 AGG). In den persönlichen Schutzbereich des AGG fallen daneben nicht nur alle bereits beschäftigten Arbeitnehmerinnen und Arbeitnehmer, sondern insbesondere auch alle Bewerberinnen und Bewerber sowie die Auszubildenden. Organmitglieder sind hingegen „nur" geschützt, soweit es um die Bedingungen für den Zugang zur Erwerbstätigkeit sowie den beruflichen Aufstieg geht.

Liegt eine Benachteiligung im vorgenannten Sinne vor, haftet der Arbeitgeber gemäß § 15 AGG bei einem tatsächlich bezifferbaren Schaden auf Schadenersatz in unbegrenzter Höhe; wegen eines Schadens, der nicht Vermögensschaden ist (immaterieller Schaden; sog. „Schmerzensgeld"), muss der Arbeitgeber eine Entschädigung in Geld leisten. Diese ist nur für den Fall der Nichteinstellung eines Bewerbers auf drei Monatsgehälter beschränkt, wenn der Bewerber auch bei benachteiligungsfreier Auswahl nicht eingestellt worden wäre. Im Übrigen ist die Entschädigung unbegrenzt. Auch wenn – worauf eingangs bereits hingewiesen wurde – nicht zu erwarten ist, dass die deutschen Gerichte (z. B. bei einer Belästigung im Sinne des AGG) Entschädigungssummen nach amerikanischem oder britischem „Vorbild" zusprechen werden, liegt hierin doch ein beträchtliches Risiko für den Arbeitgeber. Dies gilt nicht zuletzt deshalb, weil das Gesetz in § 22 AGG eine wesentliche Beweiserleichterung für den jeweiligen Kläger vorsieht. Im ersten Schritt genügt für den Kläger nämlich bereits die Darlegung bloßer Indizien, die eine Benachteiligung wegen eines Diskriminierungsmerkmals vermuten lassen, um den Arbeitgeber in Bedrängnis zu bringen. Dieser muss im Anschluss beweisen, dass die Diskriminierung tatsächlich nicht stattgefunden hat.

Diese Beweislastumkehr wurde in der Vergangenheit zum sogenannten „AGG-Hopping" missbraucht: Dabei handelt es sich um Scheinbewerbungen, die gezielt auf Stellenanzeigen erfolgen, die unter Verstoß gegen § 11 AGG für ein bestimmtes Geschlecht oder eine bestimmte Altersgruppe ausgeschrieben sind. Die Bewerbung wird einzig mit der Intention einer späteren Schadensersatzforderung an den Arbeitgeber gerichtet. Dem AGG-Hopping wird in der Rechtsprechung mittlerweile mit dem Erfordernis einer „subjektiv ernsthaften Bewerbung" (Einwand der unzulässigen Rechtsausübung)[9] eine Grenze gesetzt. Dennoch ist bei der Gestaltung der Stellenanzeige besondere Vorsicht auf Seiten des Arbeitgebers geboten, muss er doch die „Nicht-Ernsthaftigkeit" einer Bewerbung nachweisen, was ihn regelmäßig vor Schwierigkeiten stellen wird.

[9] BAG v. 23.8.2012 – 8 AZR 285/11, Juris; LAG Hamm v. 22.5.2012 – 19 Sa 1658/11, Juris; Hessisches LAG v. 19.12.2011 – 16 Sa 965/11, AA 2012, 90; v. 8.7.2011 – 3 Sa 742/10, LAGE § 9 AGG Nr. 1.

1.4 Datenschutz

Gerade der Bereich des Datenschutzes hat im Arbeitsrecht in der letzten Zeit hohe Wellen geschlagen. Ob Telekom, Lidl oder Deutsche Bahn – die Skandale um den unbefugten Umgang mit Arbeitnehmerdaten haben in vielerlei Hinsicht die Aufmerksamkeit auf sich gezogen und die Diskussion um den Datenschutz in Unternehmen verschärft.

Mit Hilfe von EDV-Anlagen werden mittlerweile in jedem Unternehmen personenbezogene Daten erhoben, verarbeitet oder gespeichert. Dabei kommt im Zuge der täglichen Email- und Internetnutzung auch dem internationalen Datentransfer immer mehr Bedeutung zu. In diesem Zusammenhang ist zu berücksichtigen, dass der Datentransfer in sog. unsichere Drittländer, zu denen nach Auffassung der EU-Kommission insbesondere auch die USA gehören, ohne ausreichende Sicherstellung eines angemessenen Datenschutzniveaus durch Vereinbarung der Daten austauschenden Unternehmen oder durch Einwilligungserklärung des Arbeitnehmers mit einer Geldbuße von bis zu 300.000 € geahndet werden kann (§ 43 Abs. 3 Bundesdatenschutzgesetz (BDSG) n. F.).[10] Für den Fall vorsätzlichen und auf die Erzielung von Entgelt gerichteten Handelns sieht das Gesetz für bestimmte Fälle auch eine Freiheitsstrafe vor (§ 44 Abs. 1 BDSG).

Wird den Arbeitnehmern die private Nutzung von Telekommunikationseinrichtungen gestattet (vor allem Telefon, Email und Internet), ist umstritten, ob neben den Vorschriften des BDSG auch die Vorgaben des Telekommunikationsgesetzes (TKG) zu berücksichtigen sind und damit das Fernmeldegeheimnis des § 88 TKG durch den Arbeitgeber zu beachten ist. Verschiedene Landesarbeitsgerichte vertreten die Auffassung, dies sei nicht der Fall, weil der Arbeitgeber nicht allein dadurch zum Dienstanbieter i. S. d. § 3 Nr. 6 TKG werde, dass er seinen Beschäftigten gestatte, einen dienstlichen E-Mail-Account auch privat zu nutzen.[11] Allerdings steht eine Beantwortung der Streitfrage durch das BAG noch aus, so dass das Risiko verbleibt, dass der Arbeitgeber auch die Vorgaben des § 88 TKG zu beachten hat. Die Verletzung des Fernmeldegeheimnisses ist straf- und bußgeldbewehrt, vgl. §§ 148f. TKG.

Sonderfall: Due Diligence Prüfung

Ein datenschutzrechtliches Sonderproblem ergibt sich in der Praxis bei Unternehmensveräußerungen:

Interessiert sich ein potenzieller Käufer für ein zum Verkauf stehendes Unternehmen, so sind aussagekräftige Informationen hinsichtlich möglicher wirtschaftlicher und rechtlicher Risiken für ihn von großer Bedeutung. Zu diesem Zweck führen Rechtsanwalts- oder Wirtschaftsprüferkanzleien eine Prüfung des anvisierten Unternehmens durch – eine sogenannte „Due Diligence". Davon umfasst ist neben zahlreichen anderen Aspekten auch eine Analyse der Personalstruktur und -qualität. Die in diesem Zusammenhang erhobenen Daten fallen in den Anwendungsbereich des BDSG, wenn personenbezogene Daten unter

[10] Vgl. auch *Mengel/Hagemeister,* BB 2006, 2466, 2469 m. w. N.

[11] LAG Berlin-Brandenburg v. 16.2.2011 – 4 Sa 2132/10, NZA-RR 2011, 342 ff.; LAG Niedersachsen v. 31.5.2010 – 12 Sa 875/09, NZA-RR 2010, 406 ff.

Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden, oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden.[12] Dabei kommt es entscheidend darauf an, ob der Verwender einen Bezug zwischen dem Datensatz und der Person herstellen kann. Durch eine Pseudonymisierung (Name oder Identifikationsmerkmal wird durch Pseudonym ersetzt) und Anonymisierung (Vernichtung des Personenbezugs durch Datenänderung) der Daten kann dieser Personenbezug beseitigt werden, so dass der Anwendungsbereich des BDSG nicht eröffnet ist.[13] Die Praxis zeigt indes, dass vor dem Hintergrund der bei Unternehmenskäufen meist sehr engen Zeitschiene viele Dokumente „ungeschwärzt" in den Datenräumen zur Verfügung gestellt werden.

Bei einer Eröffnung des Anwendungsbereichs des BDSG ist die *Übermittlung* von Daten ein gesetzlicher Unterfall der Daten*verarbeitung.* Dabei gilt jede Weitergabe der Daten durch die verantwortliche Stelle als Übermittlung, selbst wenn es sich um Unternehmen eines gemeinsamen Konzerns handelt.

Neu eingeführt wurde im Rahmen der BDSG-Novelle im Jahr 2009 der § 32 BDSG n. F. Diese Vorschrift regelt den Umgang mit personenbezogenen Daten für Zwecke des Beschäftigungsverhältnisses und lässt Abweichungen von dem in § 4 BDSG normierten grundsätzlichen Verbot der Datenerhebung, -verarbeitung und –nutzung zu.[14] Soll die Übermittlung zulässig sein, muss das BDSG oder ein anderes Gesetz dies jedoch ausdrücklich erlauben oder der Betroffene muss aus freien Stücken dazu einwilligen (§ 4 Abs. 1 i. V. m. § 4a BDSG). Tarifverträge und Betriebsvereinbarungen sind wegen ihrer normativen Wirkung als sonstige Rechtsvorschriften i. S. d. § 4 BDSG anerkannt[15], so dass auch eine dort getroffene Regelung die Übermittlung erlauben kann. Bei Betriebsvereinbarungen ist dies allerdings nur zulässig, soweit damit kein Eingriff in das Allgemeine Persönlichkeitsrecht der Arbeitnehmer und damit in ein Grundrecht verbunden ist.[16] Dem Abschluss entsprechender Vereinbarungen steht in der Praxis jedoch häufig die Geheimhaltungspflicht über geführte Verhandlungen entgegen.

Auch „berechtigte Interessen" können eine Datenübermittlung rechtfertigen, wenn diese Interessen nicht anders als durch die Übermittlung der Daten gewahrt werden können und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder der Nutzung überwiegt (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Die im Einzelfall vorgenommene Interessenabwägung unterscheidet im Rahmen

---

[12] Vgl. *Braun/Wytibul*, BB 2008, 782.

[13] *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 3 Rn. 43 ff.

[14] Zur „kleinen Lösung" nach der BDSG-Novelle siehe *Straube/Klagges*, ArbRAktuell 2012, 328271.

[15] BAG v. 29.6.2004 – 1 ABR 21/03, NZA 2004, 1278 ff.; BAG v. 25.6.2002 – 9 AZR 405/00, BAGE 101, 357 ff.; BAG v. 27.5.1986 – 1 ABR 48/84, BAGE 52, 88 ff.; BAG v. 30.8.1995 – 1 ABR 4/95, BAGE 80, 366 ff.; *Kania*, in: ErfK, 13. Aufl. 2013, § 83 BetrVG, Rn. 11; *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 4, Rn. 7.

[16] *Straube/Klagges*, ArbRAktuell 2012, 328271.

der Erforderlichkeit zwischen der Art der übermittelten Daten und der Möglichkeit der Beschränkung der Datenübermittlung auf bestimmte Beschäftigungsgruppen.[17]

Werden Daten übermittelt, sind die Arbeitnehmer jedenfalls ausreichend zu informieren (§§ 33, 34 BDSG). Das beinhaltet vor der Datenersterfassung die Information über Datenerhebung, Zweckbestimmung, Verarbeitung, Nutzung und Übermittlung an Dritte. Darüber hinaus ist der Arbeitgeber nach der Erfassung verpflichtet, dem Arbeitnehmer kostenlos und schriftlich auf dessen Anfrage hin mitzuteilen, welche personenbezogenen Daten gespeichert sind, zu welchem Zweck die Speicherung erfolgt und an welche Personen und Stellen seine Daten weitergegeben werden. Vorsätzliche und fahrlässige Verstöße gegen die Benachrichtigungspflichten sind bußgeldbewehrt. Daneben drohen unter Umständen Schadensersatzansprüche nach § 823 Abs. 2 BGB.[18]Der Gegenstand häufiger Diskussionen war in den vergangenen Jahren der Entwurf des Beschäftigtendatenschutzgesetzes. Danach sollten auf der einen Seite Arbeitnehmer vor Bespitzelungen und Eingriffen in ihr Allgemeines Persönlichkeitsrecht geschützt werden und auf der anderen Seite sollte dem Arbeitgeber eine Grundlage an die Hand gegeben werden, um wirksam Compliance-Maßnahmen durchzusetzen und der Korruption vorzubeugen.[19] Geplant war v. a., die Möglichkeit der Arbeitnehmereinwilligungen einzuschränken und Betriebsvereinbarungen nicht mehr als Rechtsgrundlage für Abweichungen vom Datenschutzstandard zuzulassen.[20] Da ein Konsens nicht gefunden wurde, ist jedoch nicht damit zu rechnen, dass das Beschäftigtendatenschutzgesetz überhaupt verabschiedet werden wird.

1.5 Arbeitnehmerüberlassung

Der Arbeitnehmerüberlassung, d. h. die Überlassung eines Leiharbeitnehmers vom Arbeitgeber (Verleiher) auf einen Dritten (Entleiher) bei Übertragung des arbeitgeberseitigen Weisungsrechts, kommt insbesondere in großen Konzernen immer mehr Bedeutung zu. Durch die Novelle des Arbeitnehmerüberlassungsgesetzes (AÜG) im Jahr 2011 haben sich viele grundsätzliche Änderungen im Zusammenhang mit der Überlassung von Leiharbeitnehmern ergeben.

Grundsätzlich ist jede Arbeitnehmerüberlassung i. S. d. AÜG erlaubnispflichtig gemäß § 1 Abs. 1 Satz 1 AÜG. Nach der vorherigen Regelung im AÜG war der Anwendungsbereich des AÜG nur dann eröffnet, wenn eine sog. „gewerbsmäßige" Arbeitnehmerüberlassung vorlag. Gewerbsmäßig war die Arbeitnehmerüberlassung dann, wenn sie nicht nur gelegentlich erfolgt, sondern auf gewisse Dauer angelegt und auf Erzielung wirtschaftlicher Vorteile gerichtet war. Regelungen, die auf dem Prinzip der „bloßen Kostenerstattung" beruhten, unterfielen mangels Gewinnerzielungsabsicht nicht dem Anwendungsbereich des

[17] Vgl. *Braun/Wytibul*, BB 2008, 782.

[18] *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 33 Rn. 44 ff.

[19] Vgl. *Straube/Klagges*, ArbRAktuell 2012, 328271.

[20] Vgl. *Straube/Klagges*, ArbRAktuell 2012, 328271.

AÜG und waren dann auch nicht erlaubnispflichtig.[21] Heute ist eine Arbeitnehmerüberlassung jedoch bereits dann nach § 1 Abs. 1 Satz 1 AÜG erlaubnispflichtig, wenn sie „im Rahmen der wirtschaftlichen Tätigkeit" erfolgt.[22] Dadurch wurde der Anwendungsbereich der erlaubnispflichtigen Arbeitnehmerüberlassung extrem erweitert.

Auch das sog. Konzernprivileg[23] wurde wesentlich umgestaltet. Bisher galt, dass bei einer konzerninternen Arbeitnehmerüberlassung diese erlaubnisfrei ist, wenn sie lediglich vorübergehend erfolgt (vgl. § 1 Abs. 3 Nr. 2 AÜG a. F.). Nunmehr stellt § 1 Abs. 3 Nr. 2 AÜG n. F. entscheidend darauf ab, dass der jeweilige Arbeitnehmer nicht zum Zweck der Überlassung eingestellt und beschäftigt wird.

Zuletzt sollte das AÜG v. a. eine missbräuchliche Gestaltung der Arbeitnehmerüberlassung verhindern. In der Praxis wurden in der Vergangenheit vor dem Hintergrund der Erlaubnispflicht sowie des mit dem AÜG verbundenen sog. „Equal-Pay-Gebots" (Pflicht zur Vergütung der Leiharbeitnehmer entsprechend den Bedingungen im Entleiherbetrieb) vielfach Werk- oder Dienstverträge für den Einsatz betriebsfremder Arbeitnehmer geschlossen. Auch hatten konzerninterne Überlassungsgesellschaften für große öffentliche Aufmerksamkeit gesorgt, indem sie kürzlich entlassene Arbeitnehmer zu schlechteren (tariflichen) Bedingungen neu einstellten und als Leiharbeitnehmer an den bisherigen Arbeitgeber (zurück) überließen[24] („Schlecker-Fälle") – zur Umgehung des Equal-Pay-Gebots. Um dem einen Riegel vorzuschieben wurde in § 9 Nr. 2 AÜG n. F. die sog. „Drehtürklausel" eingefügt. Diese soll verhindern, dass durch die Anwendung eines Tarifvertrages vom zu beachtenden Equal-Pay-Grundsatz abgewichen werden kann, wenn der Leiharbeitnehmer innerhalb der letzten sechs Monate vor der Überlassung aus einem Arbeitsverhältnis mit dem Entleiher oder einem mit diesem verbundenen Konzernunternehmen ausgeschieden ist.[25] Wird diese Sechsmonatsgrenze unterschritten, gelten für den jeweiligen Arbeitnehmer uneingeschränkt die auch für die Stammbelegschaft geltenden Arbeitsbedingungen.[26]

Folge einer ohne die hierfür erforderliche Erlaubnis erfolgenden Arbeitnehmerüberlassung ist nicht nur die Begründung eines Arbeitsverhältnisses kraft Gesetzes zwischen Entleiher und Leiharbeitnehmer (vgl. §§ 9, 10 AÜG): der Entleiher ist damit für die Lohnzahlung nach den in seinem Betrieb geltenden Bestimmungen sowie für die Abführung der Sozialversicherungsbeiträge verantwortlich; daneben haftet er wie jeder andere Arbeitgeber auch für die Lohnsteuer (§ 42d Abs. 7 EStG). Darüber hinaus ist ein Verstoß gegen das AÜG auch als Ordnungswidrigkeit mit einem Bußgeld von bis zu 25.000,00 € je Verstoß (!) belegt (§ 16 Abs. 2 i. V. m. § 16 Abs. 1 Nr. 1 AÜG).

---

[21] *Rütz/Schreiner*, MedR 2012, 373, 374; *Oberthür*, ArbRB 2011, 146.

[22] BR-Drs. 847/10, v.31.12.2010S. 7; *Hamann*, NZA 2011, 70, 71; *Leuchten*, NZA 2011, 608, 609.

[23] Ausführlich zur Arbeitnehmerüberlassung im Konzern siehe *Lembke*, BB 2012, 2497 ff.

[24] *Oberthür*, ArbRB 2011, 146, 147,

[25] *Oberthür* aaO.

[26] *Oberthür* aaO.

Angesichts der vorstehenden Rechtsfolgen, insbesondere der Fiktion eines Arbeitsverhältnisses, ist vor dem Einsatz betriebsfremder Arbeitnehmer stets sorgfältig zu prüfen, ob nicht eine erlaubnispflichtige Arbeitnehmerüberlassung vorliegt.

1.6 Ausländerbeschäftigung

Die Beschäftigung eines Ausländers, der nicht (mehr) im Besitz eines gültigen Aufenthaltstitels ist, ist nach den Regelungen des Aufenthaltsgesetzes (AufenthG) sowie den Bestimmungen des Schwarzarbeitsbekämpfungsgesetzes (SchwarzArbG) mit Bußgeld von bis zu 500.000,00 € (§§ 98 Abs. 2a i. V. m. 4 Abs. 3 Satz 2 AufenthG) bzw. von bis zu 300.000,00 € (§ 8 Abs. 1 Nr. 2, Abs. 3 SchwarzArbG) bewehrt. Nach § 11 SchwarzArbG kommt sogar eine Freiheitsstrafe in Betracht. Daneben haftet der Arbeitgeber für die Kosten der Abschiebung (§ 66 Abs. 4 Nr. 1 AufenthG). Zu diesen Kosten gehören neben den erforderlichen Beförderungskosten auch die entstandenen Verwaltungskosten.

1.7 Betriebsverfassungsrecht

Die Öffentlichkeitswirkung des Arbeitsrechts und die Bedeutung der arbeitsrechtlichen Compliance wurden in der Vergangenheit nicht zuletzt vor dem Hintergrund der VW-Affäre um Lust- und Luxusreisen für Betriebsratsmitglieder unterstrichen. Auch –aber sicherlich nicht nur– mit Blick auf die strafrechtliche Relevanz der Begünstigung und Benachteiligung von Betriebsratsmitgliedern (§ 119 Abs. 1 Nr. 3 BetrVG) sowie die in diesen Fällen entstandenen Image-Schäden, ist verstärkt auf die Einhaltung der betriebsverfassungsrechtlichen Vorgaben zu achten.[27] Ferner führt die Missachtung der betriebsverfassungsrechtlichen Beteiligungsrechte im Regelfall zur Unwirksamkeit der arbeitgeberseitigen Maßnahme. So ist etwa jede Kündigung ohne Beteiligung des Betriebsrats unwirksam. Insgesamt ist es daher dringend erforderlich, den Bereich der betrieblichen Mitbestimmung genauestens im Auge zu behalten und die betrieblichen Vorgänge auf entsprechende Konformität zu überprüfen.

2 Die Implementierung von Compliance-Systemen am Beispiel der Einführung von Ethikrichtlinien

Angesichts der vorstehend zusammengefassten wesentlichen Haftungsrisiken im Arbeitsrecht sowie den in anderen Rechtsgebieten bestehenden Maßgaben, dürfte ausreichend Anlass zur Einführung und Verbesserung von Compliance-Systemen in Unternehmen jeder Größe gegeben sein.

[27] Vgl. auch *Mengel/Hagemeister,* BB 2006, 2466, 2469.

Von der Größe und Personalstruktur des Unternehmens hängt auch ab, welches Compliance-System konkret geeignet ist.

Grundsätzlich bestehen drei Möglichkeiten, um Compliance-Systeme verbindlich in das Unternehmen einzuführen:

1. Einführung kraft arbeitgeberseitigen Direktionsrechts
2. Einführung durch Individualvereinbarung
3. Einführung im Wege einer Betriebsvereinbarung

Im Folgenden werden die strukturellen Unterschiede der aufgezeigten Implementierungswege konkret am Beispiel der Einführung von Ethikrichtlinien erläutert.

Angelehnt an die in den USA verbreiteten sogenannten „codes of conduct" oder „codes of ethics" werden auch hierzulande vermehrt entsprechende Verhaltenskodizes bzw. Ethikrichtlinien eingeführt. In ihnen stellt die Unternehmensleitung Verhaltensstandards für die Arbeitnehmer auf. Nach den Regelungen der US-amerikanischen Börsenaufsicht (Securities Exchange Commission – kurz „SEC" genannt) sind die dort notierten Unternehmen zur Einführung und Veröffentlichung eines „Code of Business Conduct and Ethics" sogar verpflichtet.[28] Vor dem Hintergrund der Verschärfung der Sanktionen durch den Sarbanes-Oxley-Act wird man hieraus zumindest eine faktische Pflicht zur Einführung von Ethikrichtlinien auch in den deutschen Konzernunternehmen ableiten müssen. In diesen Fällen kommt es dann aber unvermeidbar zu Schnittstellen zwischen den zwingenden Vorgaben der SEC und dem national ebenfalls zwingenden Arbeitsrecht. Denn gerade große Unternehmen legen besonderen Wert auf eine einheitliche weltweite Ausgestaltung ihrer Ethikrichtlinien. Dieser Aufgabe muss sich die Compliance Abteilung oder der Compliance Officer stellen.

Die Regelungsdichte dieser Ethikrichtlinien variiert in der Praxis über die Benennung von Programmsätzen hinaus bis hin zu Vorschriften, die Liebesbeziehungen unter Mitarbeitern verbieten sollen. Typischer Inhalt solcher Ethikrichtlinien sind dabei: Verschwiegenheitsklauseln, Wertpapiertransaktionsklauseln zur Verhinderung von Insidergeschäften, Nebentätigkeitsklauseln, Regelungen zur Annahme von Geschenken, Verhalten in Geschäftsbeziehungen, sog. Whistleblowerklauseln (betreffen die Pflicht zur Anzeige von Pflichtverstößen anderer Arbeitnehmer und den Umgang mit den erhaltenen Informationen/ Informanten – siehe auch unten Ziff. 3.2, aber auch Regelungen zum allgemeinen Verhalten der Mitarbeiter am Arbeitsplatz, Regelungen zum privaten Umgang der Arbeitnehmer untereinander sowie dem Verbot verbaler Äußerungen etc.).[29]

Ob die Mitarbeiter sich an die in Ethikrichtlinien aufgeführten Verhaltensvorgaben halten müssen, hängt davon ab, ob der Arbeitgeber diese mit verbindlicher Wirkung für den einzelnen Arbeitnehmer in das Arbeitsverhältnis eingeführt hat. Je nachdem,

[28] Sec. 303A Nr. 10 des New York Stock Exchange's Listed Company Manual.

[29] Vgl. die Wal-Mart-Entscheidung zum "Flirtverbot": LAG Düsseldorf v. 14.11.2005 – 10 TaBV 46/05, NZA-RR 2006, 81 ff.; vgl. hierzu *Meyer*, NJW 2006, 3605, 3607 m. w. N.

welche Inhalte von einer entsprechenden Regelung umfasst werden, variieren auch die Voraussetzungen für die verbindliche Einführung.

2.1 Einführung kraft arbeitgeberseitigen Direktionsrechts

Unter dem Direktionsrecht ist das Recht des Arbeitgebers zu verstehen, die vom Arbeitnehmer geschuldete Arbeitsleistung näher zu konkretisieren, soweit diese nicht im Arbeitsvertrag oder durch Tarifvertrag bzw. Betriebsvereinbarung abschließend geregelt ist.[30] Anweisungen hinsichtlich des arbeitsbegleitenden Verhaltens oder inhaltlich korrespondierende abstrakt-generelle Richtlinien können über dieses arbeitgeberseitige Direktionsrecht, das in §§ 315 BGB, 106 Gewerbeordnung (GewO) normiert ist, verbindliche Geltung im Arbeitsverhältnis erlangen. Hierunter fallen etwa Regelungen zu Medienkontakten, zum sorgfältigen Umgang mit Arbeitgebereigentum, zur Nutzung der IT-Anlagen und zum ethisch korrekten Verhalten gegenüber Kunden und Lieferanten.

Aufgrund des Direktionsrechts kann der Arbeitgeber Inhalt, Ort und Zeit der Arbeitsleistung nach billigem Ermessen (vgl. § 315 BGB) näher bestimmen, soweit diese Arbeitsbedingungen nicht durch den Arbeitsvertrag, Bestimmungen einer Betriebsvereinbarung, eines anwendbaren Tarifvertrags oder gesetzliche Vorschriften festgelegt sind. Dies gilt ausdrücklich auch hinsichtlich der Ordnung und des Verhaltens der Arbeitnehmer im Betrieb. Ebenso können arbeitsvertragliche Nebenpflichten über das Direktionsrecht konkretisiert werden[31], das betrifft etwa die Pflicht zur Verschwiegenheit im Geschäftsverkehr, den Schutz von Betriebs- und Geschäftsgeheimnissen sowie das Verbot der Annahme von Geschenken.[32]

Aus Arbeitgebersicht ist die Einführung von Verhaltensvorgaben in Ethikrichtlinien durch einseitige Weisung die reizvollste Lösung. Wie sich aber bereits aus § 106 GewO ergibt, sind den Weisungen des Arbeitgebers zum Teil enge Grenzen gesetzt. Denn das Direktionsrecht kann nur dann greifen, wenn bereits bestehende vertragliche oder gesetzliche Haupt- oder Nebenpflichten konkretisiert werden sollen. Neue Pflichten können durch das Direktionsrecht ebenso wenig zum Gegenstand des Arbeitsverhältnisses gemacht werden wie Pflichten, die vom Arbeitsvertrag, einer Betriebsvereinbarung, einem Tarifvertrag oder gesetzlichen Vorschriften abweichen.

Unterteilt man darüber hinaus die in Ethikrichtlinien regelmäßig enthaltenen Verhaltensvorgaben in die folgenden drei Kategorien:

1. Regelungen mit ausschließlichem Tätigkeitsbezug,
2. Regelungen mit Bezug auf die Tätigkeit und das sonstige Verhalten und
3. Regelungen zum außerdienstlichen und privaten Verhalten,[33]

---

[30] *Künzl*, in: Ascheid/Preis/Schmidt, Kündigungsrecht, 4. Aufl. 2012, § 2, Rn. 50.

[31] *Maschmann,* Corporate Compliance und deutsches Arbeitsrecht, in: Maschmann (Hrsg.), Corporate Compliance und Arbeitsrecht – Mannheimer Arbeitsrechtstag 2009, 10.

[32] *Mengel/Hagemeister*, NZA 2007, 1386, 1387.

[33] Vgl. *Borgmann*, NZA 2003, 352, 353.

wird deutlich, dass zumindest Vorgaben zur dritten Kategorie nur in eng begrenzten Ausnahmefällen Gegenstand des Weisungsrechts sein können. Dies dürfte im Ergebnis nur dann möglich sein, wenn eine sich aus dem Arbeitsvertrag ergebende Nebenpflicht konkretisiert werden soll (z. B. Nebentätigkeitsverbote, Wertpapiertransaktionsklauseln mit Verboten für den Arbeitnehmer und seine Familienangehörigen oder das Verbot, außerdienstlich so viel Alkohol zu trinken, dass später die Arbeit beeinträchtigt wird).

Werden Verhaltensvorgaben in Form von Ethikrichtlinien durch Weisungsrecht des Arbeitgebers in das Arbeitsverhältnis eingeführt, ist aus Arbeitgebersicht darüber hinaus ein schriftliches Empfangsbekenntnis unverzichtbar. Grund dafür ist die Rechtsnatur der Weisungen: bei ihnen handelt es sich um empfangsbedürftige Willenserklärungen, die rechtssicher nur durchgesetzt werden können (Beweisbarkeit), wenn sie dem Arbeitnehmer nachweislich bekannt gemacht worden sind.[34]

2.2 Einführung durch Individualvereinbarung

Rechtssicherer ist die Umsetzung von Verhaltensvorgaben durch eine mit dem Arbeitnehmer getroffene Vereinbarung. Im Rahmen der Vertragsfreiheit sind auch deutlich weitergehende Vereinbarungen möglich, als dies dem Arbeitgeber einseitig kraft Direktionsrechts offen steht, wenngleich auch einer solchen Vereinbarung Grenzen gesetzt sind. Insbesondere darf sie nicht sittenwidrig (§ 138 BGB) sein oder gegen Treu und Glauben (§ 242 BGB) verstoßen. Hinzu kommt, dass vorformuliere Arbeitsvertragsbedingungen der Inhaltskontrolle nach §§ 305ff. BGB unterliegen.[35] Verhaltensvorgaben dürfen die Arbeitnehmer mithin v. a. nicht unangemessen benachteiligen. Dabei kann davon ausgegangen werden, dass die Anforderungen an die Rechtmäßigkeit steigen, je weiter die Verhaltensvorgaben von der eigentlichen Arbeitspflicht entfernt sind und auf das allgemeine Verhalten des Arbeitnehmers einwirken. Insbesondere Pflichten der unter der vorstehenden Ziff. 2.1 genannten zweiten und dritten Kategorie bedürfen mithin einer konkreten Begründung, um den Eingriff in die Privatsphäre zu rechtfertigen.[36]

Losgelöst hiervon ist zu berücksichtigen, dass die einzelvertragliche Einbeziehung von Verhaltensvorgaben in der Praxis wohl nur selten umfassend möglich sein wird. Zwar ist davon auszugehen, dass eine vertragliche Regelung bei Neueinstellungen noch problemlos umgesetzt werden kann. Im laufenden Arbeitsverhältnis besteht indes das Risiko, dass der Arbeitnehmer einer Einbeziehung in den Arbeitsvertrag nicht zustimmt – dies gilt insbesondere bei weitreichenden Vorgaben für den außerdienstlichen und privaten Bereich. In einem solchen Fall bliebe alleine die (wohl nur theoretische) Möglichkeit, die

[34] Vgl. hierzu *Borgmann*, NZA 2003, 352, 354.

[35] BAG v. 29.8.2012 – 10 AZR 385/11, zitiert nach Juris; v. 21.8.2012 – 3 AZR 698/10, DB 2012, 2894 ff.

[36] *Meyer*, NJW 2006, 3605, 3608.

Verhaltensvorgaben durch eine Änderungskündigung gemäß § 2 KSchG zum Inhalt des Arbeitsverhältnisses zu machen.

2.3 Einführung durch Betriebsvereinbarung

Schließlich können Verhaltensvorgaben in Betrieben mit Arbeitnehmervertretung auch durch Betriebsvereinbarung in das Arbeitsverhältnis eingeführt werden. Teilweise ist dies obligatorisch. Solch eine Umsetzung durch Betriebsvereinbarung ist immer dann zwingend erforderlich, wenn der Betriebsrat mit Blick auf den Regelungsgehalt der einzelnen Klausel des Verhaltenskodexes oder der Ethikrichtlinie ein Mitbestimmungsrecht hat. Richtigerweise sind Ethikrichtlinien weder allgemein mitbestimmungspflichtig noch pauschal mitbestimmungsfrei.[37]

Dreh- und Angelpunkt der mitbestimmungspflichtigen Tatbestände ist insoweit § 87 Abs. 1 Nr. 1 BetrVG. Hiernach sind die Maßnahmen des Arbeitgebers mitbestimmungspflichtig, die das Ordnungsverhalten der Arbeitnehmer im Betrieb betreffen. Darunter fallen z. B. Alkohol- oder Rauchverbote, Regelungen zur Einrichtung von sog. Chinese Walls bei Finanzunternehmen, Kleiderordnungen oder Vorgaben zur Nutzung von Email/Internet sowie Whistleblower-Hotlines, wobei bei letzteren zum Teil ein Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG hergeleitet wird.[38] Nicht mitbestimmungspflichtig sind hingegen Maßnahmen oder Regelungen, die das Arbeitsverhalten betreffen. Hierunter fallen alle arbeitgeberseitigen Maßnahmen, die bestimmen, welche Arbeiten und vor allem in welcher Art und Weise sie auszuführen sind.[39] Erst recht besteht kein Mitbestimmungsrecht des Betriebsrats bei Maßnahmen, die das außerdienstliche oder private Verhalten der Arbeitnehmer betreffen.

Will der Arbeitgeber umfassende Verhaltensvorgaben in seinem Unternehmen einführen, die neben mitbestimmungsfreien auch mitbestimmungspflichtige Regelungen enthalten, müssen zumindest die mitbestimmungspflichtigen Regelungen durch Betriebsvereinbarung umgesetzt werden. Ob daneben auch die mitbestimmungsfreien Regelungen freiwillig in die Betriebsvereinbarung aufgenommen werden oder insoweit auf die vorgenannten Möglichkeiten der Einführung kraft Direktionsrechts oder durch einzelvertragliche Regelung zurückgegriffen werden soll, ist eine Entscheidung des konkreten Einzelfalls und kann nicht abschließend bewertet werden.

Werden in Verhaltensrichtlinien rein informatorisch lediglich gesetzliche Vorgaben wiedergegeben, um diese für die Mitarbeiter noch einmal deutlich und vor allem laienverständlich darzulegen, so finden diese bereits kraft Gesetzes Anwendung auf das

---

[37] BAG v. 17.5.2011 – 1 ABR 121/09, AP Nr. 73 zu § 80 BetrVG; v. 22.7.2008 – 1 ABR 40/07, BAGE 127, 146 ff.; LAG Berlin-Brandenburg v. 15.12.2009 – 19 TaBV 1109/09, zitiert nach Juris; *Mengel/Hagemeister*, BB 2007, 1386, 1392.

[38] BAG v. 22.7.2008 – 1 ABR 40/07, BAGE 127, 146 ff.

[39] BAG v. 7.2.2012 – 1 ABR 63/10, NZA 2012, 685 ff.; v. 17.1.2012 – 1 ABR 45/10, NZA 2012, 687 ff.; *Fitting*, BetrVG, 15. Aufl. 2012, § 87 Rn. 65.

Arbeitsverhältnis und bedürfen keiner zusätzlichen Rechtsgrundlage.[40] Solche rein deklaratorischen bzw. informatorischen Regelungen unterliegen auch nicht der betrieblichen Mitbestimmung.

Der Vorteil der Einführung/Umsetzung per Betriebsvereinbarung liegt sicherlich darin, dass gemeinsam mit der Arbeitnehmervertretung eingeführte Ethikrichtlinien auf eine größere Akzeptanz bei den Arbeitnehmern selbst stoßen dürften. Auch hat der Arbeitgeber den Vorteil, dass er nur einen Ansprech- und Verhandlungspartner für die Ausgestaltung der Regelungen hat. Eine durch Betriebsvereinbarung eingeführte Richtlinie kann außerdem leichter wieder verändert werden als durch Arbeitsvertrag implementierte Regelungen. Insbesondere in großen Unternehmen empfiehlt sich daher oftmals eine Umsetzung kraft Betriebsvereinbarung. Dabei versteht sich von selbst, dass auch die in Betriebsvereinbarungen geregelten Verhaltensvorgaben an die gleichen Grenzen stoßen wie Individualvereinbarungen oder arbeitgeberseitige Weisungen: nämlich gegen zwingendes Recht, insbesondere die Grundrechte des Arbeitnehmers (z. B. Verbot der Liebesbeziehung zwischen Mitarbeitern) zu verstoßen.

3 Informationserfassung im Rahmen der Compliance/Sonderfall Whistleblowing

Unverzichtbar im Rahmen der Compliance ist die Informationserfassung. Ohne den Zugang zu compliance-relevanten Informationen kann der Arbeitgeber nicht feststellen, ob die Arbeitnehmer im konkreten Einzelfall einwandfrei den im Unternehmen eingeführten Verhaltensvorgaben entsprochen haben. Dabei sind nicht in erster Linie technische Informationen gefragt, sondern Erfahrungs- und Verhaltensberichte. Wichtigste Wissensträger sind deswegen die Mitarbeiter selbst.[41]

Um diese wertvollen Informationen zu erfassen, müssen Systeme eingeführt werden, die unterschiedlichsten Anforderungen gerecht werden. Hier ist es nicht immer einfach, den richtigen Weg der Informationsweitergabe durch Mitarbeiter zu finden. Vielfach findet sich der Arbeitgeber vor einer regelrechten Informationsbarriere.[42] Dabei spielen sowohl falsch verstandene Solidarität unter Mitarbeitern als auch die Angst davor, vom Mitwisser zum Mittäter zu werden, eine große Rolle.

3.1 Allgemeine Mitwirkungspflicht des Arbeitnehmers

Im Rahmen des Arbeitsverhältnisses und der arbeitnehmerseitigen Treuepflichten ist der Mitarbeiter grundsätzlich verpflichtet, dem Arbeitgeber Auskünfte zu erteilen. Hiervon

[40] *Müller-Bonanni/ Sagan*, BB-Special 2008, 28, 29.

[41] Vgl. auch *Göpfert/Merten/Siegrist,* NJW 2008, 1703 ff.

[42] Vgl. *Maschmann,* a.a.O. (Fn. 21), S. 12; *Hauschka,* DB 2006, 1143, 1146.

umfasst sind in erster Linie leistungsbezogene Auskünfte, etwa Angaben zu Art und Umfang der Leistung, dem Arbeitsbereich und Wahrnehmungen aus diesem.[43] Je weiter sich die Auskünfte inhaltlich vom eigentlichen Leistungsbereich des Mitarbeiters entfernen, desto größer muss das vom Arbeitgeber dargelegte berechtigte, billigenswerte und schutzwürdige Interesse an der Information sein, um eine Auskunftspflicht des Arbeitnehmers zu begründen. In die Abwägung zwischen dem Auskunftsinteresse des Arbeitgebers und dem Recht des Mitarbeiters, die Auskunft verweigern zu dürfen, ist das Persönlichkeitsrecht des Mitarbeiters einzubeziehen. Betrifft das Auskunftsersuchen des Arbeitgebers Wahrnehmungen, die der Mitarbeiter außerhalb seines Arbeitsbereichs gemacht hat, gilt der Grundsatz, dass der Mitarbeiter sich nicht selbst bezichtigen muss.[44] Zur Anzeigepflicht gegenüber Arbeitskollegen vgl. unten Ziff. 3.2.2.

3.2 Whistleblowing-Systeme

Viele größere Unternehmen haben zur Sicherstellung des Informationsflusses deshalb bereits sogenannte Whistleblowing-Systeme eingerichtet.[45] Beim Whistleblowing[46] wird ein Informationssystem errichtet, das dritten Personen (Mitarbeitern oder auch externen Personen, insbesondere Kunden) die Möglichkeit eröffnet, Hinweise zu Personen zu geben, deren Verhalten nicht im Einklang mit unternehmensinternen oder gesetzlichen Regelungen steht. Unter dem Gesichtspunkt der damit verbundenen Verarbeitung personenbezogener Daten, der Gefahr von Stigmatisierung, Missbrauchsmöglichkeiten, blinden Verdachtsfällen und den infolgedessen verursachten Eingriffen in die Persönlichkeitsrechte von Mitarbeitern gilt es, arbeits- und datenschutzrechtliche Maßgaben zu beachten. Für die Ausgestaltung eines solchen Hinweisgebersystems bestehen verschiedene Alternativen. So können Hotlines oder elektronische Hinweissysteme, aber auch externe oder interne Ombuds- bzw. Beschwerdestellen eingerichtet werden.

3.2.1 Datenschutz

Zum Umgang mit derartigen Systemen in datenschutzrechtlicher Hinsicht hat die sog. „Art. 29-Gruppe" – eine Kommission der Datenschutzbeauftragen der 25 EU-Mitgliedstaaten – am 1. Februar 2006 eine Stellungnahme mit Empfehlungen veröffentlicht. Die Gestaltungsvorschläge der Art. 29-Gruppe entsprechen im Wesentlichen

---

[43] BAG v. 18.1.1996 – 6 AZR 314/95, DB 1996, 2182 f.; v. 7.9.1995 – 8 AZR 828/93, NZA 1996, 637, 637.

[44] BAG v. 20.11.2003 – 8 AZR 580/02, NZA 2004, 489 ff.; BGH v. 23.2.1989 – IX ZR 236/86, NJW-RR 1989, 614 ff.; BVerfG, 13.1.1981 – 1 BvR 116/77, BVerfGE 56, 37; ausführlich dazu: *Göpfert/ Merten/ Siegrist,* NJW 2008, 1703 ff.; zur Auskunftspflicht im Rahmen von Compliance-Maßnahmen *Oberthür*, ArbRB 2011, 184 ff.

[45] Vgl. dazu Kapitel: *Bauer*, Datenschutzrechtliche Compliance im Unternehmen.

[46] Mit „whistleblower" werden im englischsprachigen Raum Informanten bezeichnet, die illegale oder unmoralische Taten anderer Personen enthüllen.

den Vorgaben des § 28 BDSG und können deshalb als Auslegungshilfe zu dieser Vorschrift herangezogen werden. Daneben bestehen mittlerweile auch gesonderte nationale Empfehlungen für den Betrieb von Whistleblowing-Hotlines.[47]

3.2.2 Meldepflicht vs. Treuepflicht

Losgelöst hiervon ist im Zusammenhang mit Regelungen zum Whistleblowing zu unterscheiden zwischen Vorschriften, die lediglich eine Meldeerwartung ausdrücken wollen und solchen, die eine Meldepflicht statuieren.[48] Während erstere problemlos möglich sind, sind bei der zweiten Variante Interessenkonflikte zwischen dem arbeitgeberseitigen Informationsinteresse und dem Recht auf informationelle Selbstbestimmung der Mitarbeiter voraussehbar. Diese bedürfen einer Abwägung im Einzelfall. Konkrete Maßgaben zu diesem Konflikt gibt es bisher noch nicht. Eine Pflicht zur Selbstanzeige soll jedenfalls grundsätzlich nicht statuierbar sein.[49] Nach der Rechtsprechung des BAG[50] kann der Arbeitnehmer je nach Stellung in der Betriebshierarchie, Ausmaß der Störung bzw. Gefahr und Umfang des vorauszusehenden Schadens jedoch zur Anzeige eigener Arbeitskollegen verpflichtet sein, wenn sich arbeitsvertragliche Rücksichtnahme- und Schadensabwendungspflichten im Zusammenhang mit der Arbeitsleistung oder im Hinblick auf die Überwachungs- und Kontrollpflicht gegenüber einem Dritten so verdichten, dass jede Nichtanzeige eine Pflichtverletzung darstellen würde.[51] Eine generelle Anzeigepflicht besteht dennoch nur bei der Gefahr des Eintritts von Personen- oder erheblichen Sachschäden.[52] Denn die Treupflicht des Arbeitnehmers zum Arbeitgeber wiegt am Ende doch schwerer als falsch verstandene Solidarität mit „kriminellen" Kollegen.

Die Rechtsprechung misst der Loyalität gegenüber dem Arbeitgeber generell einen hohen Stellenwert bei.[53] In der Vergangenheit hat das BAG insoweit entschieden, dass ein Arbeitnehmer, der illegale Praktiken des Arbeitgebers selbst und ohne vorherigen innerbetrieblichen Klärungsversuch direkt anzeigt, mit einer Kündigung rechnen muss.[54]

---

[47] Vgl. dazu Kapitel: *Bauer*, Datenschutzrechtliche Compliance im Unternehmen.; Stellungnahme abrufbar unter: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/spdocs/2006/wp11; dazu außerdem die Empfehlungen des Düsseldorfer Kreises für den Betrieb von Hotlines in Deutschland, abrufbar unter: http://www.hamburg.de/contentblob/254868/data/whistleblowing.pdf.

[48] Vgl. auch *Mahnhold,* NZA 2008, 737, 738.

[49] Vgl. *Schuster/Darsow,* NZA 2005, 273, 276; *Diller,* DB 2004, 313, 314; BGH v. 23.2.1989 – IX ZR 36/86, NJW-RR 1989, 614 f.; ausführlich dazu: *Göpfer/Merten/Siegrist,* NJW 2008, 1703 ff.

[50] BGH v. 23.2.1989 – IX ZR 236/86, BB 1989, 649; BAG v. 18.6.1970–1 AZR 520/69, AP Nr. 57 zu § 611 BGB Haftung des Arbeitnehmers; LAG Hamm v. 20.7.1994 – 18(2) Sa 2016/93, BB 1994, 2352.

[51] Ausführlich dazu siehe *Herbert/Oberrath*, NZA 2005, 193 ff.

[52] *Reinfeld*, in: Moll (Hrsg.), Münchener Anwaltshandbuch Arbeitsrecht, 3. Aufl. 2012, § 31 Rn. 2; LAG Hamm v. 29.7.1994 – 18(2) Sa 2016/93, BB 1994, 2352 (red. Leitsatz 1).

[53] BAG v. 3.7.2003 – 2 AZR 235/02, BAGE 107 36 ff.; LAG Frankfurt a. M. v. 14.2.1991 – 12 Sa 846/90, NZA 1992, 124 (Leitsatz 1–2).

[54] BAG v. 5.2.1959 – 2 AZR 60/56, AP Nr. 2 zu § 70 HGB.

Ausdrückliche Anzeigerechte für die Arbeitnehmer werden in Deutschland jedenfalls nur in bestimmten Bereichen statuiert. Hierzu zählen das Gefahrstoffrecht, das Arbeitssicherheitsrecht und das Antidiskriminierungsrecht.[55] Darüber hinaus haben die Bundesministerien für Arbeit und Soziales, für Ernährung, Landwirtschaft und Verbraucherschutz sowie das Bundesjustizministerium am 30. April 2008 eine Neufassung von § 612a BGB auf den Weg gebracht, die dem Arbeitnehmer unter bestimmten Voraussetzungen ein Anzeigerecht einräumen sollte. Diese Regelung ist jedoch bisher im Bundestag gescheitert. Der neue § 612a BGB sollte den bisher nach der Rechtsprechung[56] vorrangigen innerbetrieblichen Klärungsversuch entbehrlich machen. So hat das BAG bisher ausgeführt, dass „es eher zumutbar erscheint, vom Arbeitnehmer – auch wenn ein Vorgesetzter betroffen ist – vor einer Anzeigeerstattung einen Hinweis an den Arbeitgeber zu verlangen. Dies gilt insbesondere dann, wenn es sich um Pflichtwidrigkeiten handelt, die auch den Arbeitgeber selbst schädigen".[57] Sachgerecht erscheint dies jedenfalls dann, wenn Compliance Regelungen existieren, die auf eine innerbetriebliche Aufdeckung und Beseitigung gesetzeswidrigen Verhaltens von Mitarbeitern abzielen. Dieser Grundsatz gilt gleichwohl mit der Maßgabe, dass auf den vorherigen Klärungsversuch bei Unzumutbarkeit verzichtet werden kann.[58]

Im Juli vergangenen Jahres fällte der Europäische Gerichtshof für Menschenrechte (EGMR) eine viel beachtete Entscheidung. Geklagt hatte eine Pflegedienstmitarbeiterin von Vivantes, dem öffentlich-rechtlichen Betreiber einer großen Anzahl von Pflegeheimen.[59] Sie hatte gegen ihre Arbeitgeberin Strafanzeige wegen Mängeln in der institutionellen Pflege erstattet. Das Strafverfahren wurde mangels Tatverdacht eingestellt. Danach äußerte die Arbeitnehmerin ihre Empörung über die Pflegezustände polemisch auf einem Flugblatt. Daraufhin wurde sie fristlos gekündigt.

Das Arbeitsgericht[60] meinte, eine Kündigung sei nicht möglich, weil die Äußerungen durch die Meinungsfreiheit der Klägerin gedeckt sei. Das Landesarbeitsgericht[61] hob diese Entscheidung jedoch auf, weil die Arbeitnehmerin ihre Strafanzeige „leichtfertig" auf Tatsachen gegründet habe, die sie im Prozess nicht habe darlegen können. Damit habe sie nicht im Rahmen ihrer Verfassungsrechte gehandelt und ihre Loyalitätspflicht gegenüber ihrer Arbeitgeberin verletzt.

Der EGMR sah die Rechte der Arbeitnehmerin aus Art. 10 MRK (Meinungsäußerungsfreiheit) als verletzt an. Zwar seien wegen der Pflicht zur Loyalität und zur Diskretion

---

[55] § 21 Abs. 6 GefahrstoffVO; § 17 Abs. 2 ArbSchG.

[56] BAG v. 3.7.2003 – 2 AZR 235/02, NZA 2004, 427, 427.

[57] BAG a.a.O.

[58] Weitere Rspr. zum Thema: BVerfG v. 2.7.2001 – 1 BvR 2049/00, NZA 2001, 888 ff. LAG Rheinland-Pfalz v. 24.7.2007 – 7 Sa 451/07; LAG Berlin v. 28.3.2006 – 7 Sa 1884/05, LAGE § 626 BGB 2002 Nr. 7b.

[59] EGMR v.21.7.2011 „Heinisch" – 28274/08, NJW 2011, 3501 ff.

[60] ArbG Berlin v. 3.8.2005 – 39 Ca 4775/05, Juris.

[61] LAG Berlin v. 28.3.2006 – 7 Sa 1884/05, LAGE § 626 BGB 2002 Nr. 7b.

Hinweise in erster Linie gegenüber den Vorgesetzten oder anderen zuständigen Stellen oder Einrichtungen vorzubringen. Aber wenn dies eindeutig impraktikabel sei, dürfe als ultima ratio die Öffentlichkeit informiert werden.[62] Dabei maß der Gerichtshof insbesondere dem Aspekt des Handelns in gutem Glauben des „Whistleblowers" ein besonderes Gewicht zu. Diese Vorgaben des EGMR werden künftig auch die deutsche Rechtsprechung bei der Behandlung von sog. Whistleblowing-Fällen beeinflussen. Whistleblowing wird nur noch unter engen Voraussetzungen einen Verstoß gegen die Loyalitätspflicht gegenüber dem Arbeitgeber erfüllen, der dann zur Kündigung berechtigen könnte.

Hat der Arbeitgeber ein Whistleblowing-System eingeführt, kann er einem Arbeitnehmer natürlich nicht kündigen, wenn dieser das System vorschriftsgemäß zu einer Anzeige nutzt.[63]

3.2.3 Ombuds- und Beschwerdestellen

Unternehmen richten vermehrt auch externe Stellen ein, um Compliance-Verstößen vorzubeugen.[64] Dabei werden Ombudsmänner als Ansprechpartner für potenzielle Hinweisgeber eingesetzt. Sie stehen für gewöhnlich außerhalb der Unternehmenshierarchie und sind weitestgehend selbstständig sowie weisungsfrei. In der Praxis handelt es sich bei den Ombudsmännern häufig um Rechtsanwälte, die neben ihrer beruflichen Schweigepflicht den Informanten auch aufgrund ihrer unabhängigen Stellung Vertraulichkeit zusichern können. Als Schnittstelle zwischen Unternehmen und Informanten können sie zum einen dem Informanten weitestgehende Anonymität gegenüber dem Unternehmen garantieren und können zum anderen mithilfe seiner Informationen eigene Sachverhaltsaufklärung betreiben. Um ihrem Zweck gerecht werden zu können, müssen Ombudsstellen sachkundig besetzt und mit den erforderlichen Kompetenzen ausgestattet werden.

Besonderheiten im Zusammenhang mit externen Ombudsstellen sind insbesondere bei der Einhaltung der außerordentlichen Kündigungsfrist nach § 626 Abs. 2 BGB zu beachten.[65] Werden potenziell kündigungsrelevante Informationen im Rahmen der externen Ombudsstelle auf eine Person außerhalb des Unternehmens verlagert, kann dies grundsätzlich zu einer Wissenszurechnung aufgrund grob fahrlässiger (weil durch Organisationsfehler bedingte) Unkenntnis führen. Die Frist beginnt dann bereits zu laufen, wenn die Ombudsstelle die Information erhält. Führt diese dann noch eigene Ermittlungen durch und setzt den Kündigungsberechtigten erst im Anschluss in Kenntnis, ist die Zwei-Wochen-Frist längst vorüber.

---

[62] EGMR v.21.7.2011 „Heinisch" – 28274/08, NJW 2011, 3501 ff., Rn. 65.

[63] Damit würde er sich in Widerspruch zu seinem eigenen Verhalten setzen (sog. „venire contra factum proprium"- Grundsatz).

[64] *Bucher,* CCZ 2008, 148 ff.; *Hild*, AnwBl. 2010, 641 ff.; vgl. auch BAG v. 26.11.1987 – 2 AZR 312/87 (n.v.); zu den Einsichtsrechten bei unternehmensinternen Untersuchungen siehe *Schaefer/Klasen*, DB 2012, 1384 ff.

[65] Ausführlich dazu *Schimmelpfennig,* CCZ 2008, 161 ff.

Eine externe Stelle kann nur dann ohne Fristanrechnung eingeschaltet werden, wenn ein besonderes Bedürfnis zur Auslagerung dieser Untersuchungs- und Überwachungsaufgaben besteht. Das ist dann der Fall, wenn diese Art der Ermittlungen gerade deswegen effizienter ist, weil sie vom Arbeitgeber selbst so nicht durchgeführt werden können. Insbesondere gilt das für den Bereich der Wirtschaftskriminalität, wo ansonsten besondere Aufklärungsschwierigkeiten und Verschleierungsrisiken bestehen. Als Gegenbeispiel kann hier die Aufklärung von Vertragsverletzungen angeführt werden, die dem Arbeitgeber ohne Weiteres selbst möglich ist.[66]

3.2.4 Unternehmensinterner Compliance-Officer

Unabhängig von der Inanspruchnahme externer Ombudsstellen besteht jedoch auch eine Notwendigkeit der internen Compliance-Organisation. Wie diese auszugestalten ist, bleibt den Unternehmen ebenfalls selbst überlassen. Gesetzliche Vorgaben gibt es hierzu nicht. Eine häufig gewählte Möglichkeit besteht darin, die Stelle eines für Compliance-Fragen zuständigen Compliance-Officers zu schaffen. In größeren Unternehmen werden sogar ganze Compliance Abteilungen tätig. Zu beachten ist, dass den Compliance-Officer (oder auch Compliance-Beauftragten) ggf. auch eine persönliche strafrechtliche Verantwortung bei Compliance-Verstößen treffen kann.[67]

Aufgrund ihrer Aufgabe sollte die zentrale Compliance-Stelle in aller Regel auf der Stabsebene angesiedelt sein. Eine weitere Voraussetzung zur effektiven Wahrnehmung von Compliance-Befugnissen ist die fachliche Weisungsunabhängigkeit des Compliance-Officers. Der Compliance-Beauftragte sollte über ein unabhängiges Aufklärungs-, Verfolgungs-, Bearbeitungs-, Beratungs- und Entscheidungsrecht verfügen.[68] Die Kompetenzgrenze wird dort gezogen, wo die Aufgabenwahrnehmung von der Sachverhaltsermittlung und -bearbeitung in den Bereich der Anordnung von Abhilfemaßnahmen übergeht. Der operative Teil der Geschäftsführung muss in den Händen der letztverantwortlichen Geschäftsleitung bleiben.[69]

4 Maßnahmen bei Verstößen gegen das Compliance-System

Compliance verlangt dem Arbeitgeber nicht nur die Einführung der entsprechenden Verhaltensregeln ab, sondern auch deren effektive Kontrolle. Am Beispiel der Whistleblowing-Systeme heißt dies, dass sichergestellt werden muss, dass den entsprechenden Hinweisen auch tatsächlich nachgegangen wird.

---

[66] Vertiefend BAG v. 26.11.1987 – 2 AZR 312/87 (n. v.).

[67] BGH v. 17.7.2009 – 5 StR 394/08, BGHSt 54, 44 ff.; Anmerkung dazu *Schwarz*, wistra 2012, 13 ff. und *Raum*, CCZ 2012, 197 f.; eingehend zu den Berichtspflichten des Compliance-Officers siehe *Raus*, CCZ 2012, 96 ff.

[68] Vgl. die Funktionsbeschreibungen in § 33 WpHG, die auch außerhalb von Wertpapierdienstleistungsunternehmen nutzbar zu machen sind.

[69] Vgl. auch *Illing/Umnuß,* CCZ 2009, 1 ff.

In aller Regel werden insbesondere in Ethikrichtlinien bereits Sanktionen bis hin zur Kündigung für den Fall des Verstoßes gegen die Regelung angedroht sein. Zu beachten ist hier, dass auch die Ankündigung einer Sanktion in den Compliance-Regelungen regelmäßig nicht eine Abmahnung in der konkreten Situation des Verstoßes erspart. Die Anforderungen des Kündigungsschutzgesetzes an eine verhaltensbedingte Kündigung bleiben mithin unberührt. Auch kann keine Sanktionierung der bloßen Verweigerung der Kenntnisnahme oder der Anerkenntnis einer Richtlinie erfolgen, es sei denn der Arbeitgeber ist darauf angewiesen, dass der Mitarbeiter die Richtlinie offiziell anerkennt (beispielsweise dort, wo ausländisches Recht oder ein Geschäftspartner die Anerkennung verlangen).[70]

4.1 Verdachtskündigung

Häufig wird ein hundertprozentiger Nachweis eines Compliance-Verstoßes nicht möglich sein. Die gegenüber dem Mitarbeiter erhobenen Vorwürfe bleiben so im Verdachtsstadium stecken, ohne dass eine weitere Aufklärung möglich wäre. Da jedoch auch ein nicht nachgewiesener Verdacht das für die Zusammenarbeit nötige Vertrauensverhältnis zerstören kann, ist es in diesen Fällen möglich, eine Beendigung des Arbeitsverhältnisses auf der Grundlage einer sog. Verdachtskündigung herbeizuführen.

Eine Verdachtskündigung bedeutet aber auch immer gravierende Eingriffe in Rechte potenziell Unschuldiger. So liegt es auf der Hand, dass sie nicht bei jeder nur denkbaren Regelverletzung möglich ist. Eine Verdachtskündigung ist vielmehr an das Vorliegen des dringenden Verdachts einer strafbaren Handlung oder einer schwerwiegenden Verfehlung des Arbeitnehmers gebunden.[71] Dieser Verdacht muss auf objektiven Tatsachen gründen und so dringend sein, dass er geeignet ist, das Vertrauensverhältnis zwischen Arbeitnehmer und Arbeitgeber zu zerstören.[72] Als Ultima Ratio setzt die Verdachtskündigung außerdem voraus, dass der Arbeitgeber zuvor alle ihm zumutbaren Möglichkeiten der Sachverhaltsaufklärung ergriffen hat.[73] Insbesondere muss dem Arbeitnehmer die Gelegenheit zur Stellungnahme gegeben werden.[74]

Die Verdachtskündigung ist als außerordentliche und ordentliche Kündigung möglich.[75] Wird sie außerordentlich ausgesprochen, so ist zu beachten, dass die zur Erklärung der Kündigung maßgebliche Zwei-Wochen-Frist (§ 626 Abs. 2 BGB) zu dem Zeitpunkt

[70] *Maschmann,* a.a.O. (Fn. 21) S. 12.

[71] BAG v. 5.4.2001 –2 AZR 217/00, NJW 2001, 837 ff.; v. 12.8.1999 – 2 AZR 923/98, BAGE 92, 184 ff.; *Henssler*, in: MüKo BGB, 5. Aufl. 2009, § 626 Rn. 242.

[72] BAG v. 5.4.2001 – 2 AZR 217/00, NJW 2001, 837 ff.; v. 13.9.1995 – 2 AZR 587/94, NZA 1996, 81 ff.

[73] BAG v. 30.4.1987 – 2 AZR 283/86, NZA 1987, 699 f.; v. 11.4.1985 – 2 AZR 239/84, BAGE 49, 39 ff.

[74] BAG v. 10.2.2005 – 2 AZR 189/04, NZA 2005, 1056 ff.; v. 20.8.1997 – 2 AZR 620/96, NZA 1997, 1340 ff.; *Henssler*, in: MüKo BGB, 5. Aufl. 2009, § 626 Rn. 242.

[75] *Dörner*, in: Ascheid/Preis/Schmidt (Hrsg.), 3. Aufl. 2007, § 636 Rn. 368.

zu laufen beginnt, von dem an der Kündigungsberechtigte über eine zur Entscheidung ausreichende Tatsachengrundlage verfügt. Generell erfolgt dabei bei außerordentlichen Kündigungen eine Wissenszurechnung gesetzlicher bzw. rechtsgeschäftlicher Vertreter (oder Personen, die diesen gleichgestellt sind) zum Arbeitgeber. Auch hier ist der Tatsache Aufmerksamkeit zu schenken, dass Verzögerungen aufgrund von Organisationsfehlern zulasten des Arbeitgebers gehen.[76] Wichtig kann dies im Zusammenhang mit externen Ombudsstellen werden (vgl. oben Ziff. 3.2.3).

Hat der Arbeitgeber selbst an der Entstehung des Kündigungsgrundes mitgewirkt bzw. das dem Arbeitnehmer vorgeworfene Verhalten selbst initiiert oder geduldet, dann verstößt er mit einer Verdachtskündigung aus diesem Grund gegen das Verbot widersprüchlichen Verhaltens und die Kündigung ist treuwidrig.

4.2 Kronzeugen- und Amnestieregelungen

Die ursprünglich aus dem Strafprozessrecht stammende Kronzeugenregelung hat die Aufgabe, dem Täter einen Anreiz zur Aufklärung des Sachverhalts um den Preis der Strafmilderung zu geben. Mittlerweile findet diese Regelung auch in der arbeitsrechtlichen Praxis Anwendung, um die in manchen Fällen undurchdringlich scheinende „Mauer des Schweigens“[77] zu durchbrechen.

Das bedeutet ganz konkret, dass ein Kündigungs- oder Forderungsverzicht gegenüber dem Mitarbeiter erklärt wird, der etwas zur Sachverhaltsaufklärung beiträgt.[78] Voraussetzung ist allerdings eine Interessenabwägung, die ein dem Sanktionsinteresse überwiegendes Interesse des Gesellschaftswohls zum Ergebnis hat.[79] So wurde etwa dem Aufsichtsrat einer Aktiengesellschaft zugebilligt, von einer Schadensersatzklage gegen ein Vorstandsmitglied abzusehen, sofern gewichtige Gründe des Unternehmenswohls dem entgegenstehen. Im Gegensatz zu diesen im Einzelfall zulässigen Kronzeugenregelungen sind bedingungslose Amnestieregelungen unzulässig. Durch einen einseitigen Sanktionsverzicht ohne vom Arbeitnehmer zu erbringende Gegenleistung, verletzt die Geschäftsleitung ermessensfehlerhaft ihre Pflicht, sorgfältig und zum Wohl der Gesellschaft zu handeln.[80]

---

[76] BAG v. 26.11.1987 – 2 AZR 312/87 (n.v.).

[77] *Göpfert/Merten/Siegrist,* NJW 2008, 1703, 1703.

[78] Ein solcher Verzicht kann nur nachträglich erklärt werden. Ein Vorausverzicht wegen vorsätzlicher Schädigung ist nach § 276 Abs. 3 BGB unzulässig.

[79] BGH v. 21.4.1997 – II ZR 175/95, NJW 1997, 1926 f („ARAG/ Garmenbeck“).

[80] § 93 AktG, § 43 GmbHG.

5 Fazit

Wirksame Compliance-Systeme werden vor dem Hintergrund der zunehmenden Vereinheitlichung weltweiter Konzernvorgaben immer mehr an Bedeutung gewinnen. Dabei ist der Arbeitgeber gut beraten, frühzeitig zu überlegen, in welchem Umfang den Mitarbeitern Compliance-Pflichten auferlegt und wie diese konkret in das einzelne Arbeitsverhältnis eingeführt werden, um auch tatsächlich verbindliche Wirkung zu erlangen.

Wichtiger Bestandteil von Compliance-Systemen ist neben der Einführung von Verhaltensvorgaben durch Ethikrichtlinien oder Verhaltenskodizes auch die ständige Kontrolle der Einhaltung der Compliance Vorgaben. Zu diesem Zweck werden in vielen Unternehmen bereits sog. Compliance-Officer oder – mit zunehmender Größe des Unternehmens – ganze Compliance Abteilungen beschäftigt. Diese haben die Verantwortung für das jeweilige Compliance-System inne und berichten der Geschäftsleitung, agieren dabei aber grundsätzlich unabhängig und weisungsfrei.

An die damit in der Praxis bereits vielfach umgesetzten Compliance-Strukturen schließen sich weitere Fragen an. Dies gilt insbesondere für die Frage, in wessen Interesse z. B. der Compliance-Officer tätig wird. Ähnlich der Funktion eines Datenschutz- oder Strahlenschutzbeauftragten ist hier zu überlegen, inwieweit der Compliance-Officer im öffentlichen oder im betrieblichen Interesse tätig wird. Die Antwort auf diese Frage wird insbesondere für die Ausgestaltung seiner Unabhängigkeit von Bedeutung sein. Daneben ist von Fall zu Fall zu entscheiden, wie genau der Anstellungsvertrag eines Compliance-Officers ausgestaltet wird, um seiner Funktion gerecht zu werden. Wem etwa ist er unterstellt? Welche konkreten Regelungen sind in den Anstellungsvertrag aufzunehmen, ohne dass seine unabhängige Stellung beeinträchtigt wird?

Das Arbeitsrecht ist damit ein wesentliches Rechtsgebiet beim Thema Compliance. Es hat für den Aufbau einer Compliance-Organisation vor allem deshalb eine hervorgehobene Bedeutung, weil Compliance-Vorgaben – sobald die Rechtsstellung der Arbeitnehmer betroffen ist – nur über das Arbeitsrecht verbindlich in ein deutsches Unternehmen eingeführt werden können (vgl. oben 2.). Noch längst sind nicht alle Fragen hierzu geklärt. Ziel muss daher aus Arbeitgebersicht vorrangig sein, Sensibilität für das Thema Compliance unter arbeitsrechtlichen Gesichtspunkten zu entwickeln.

Tax Compliance

Christoph Kromer, Reinhard Pumpler und Katharina Henschel

Inhaltsverzeichnis

C. Kromer (✉) · K. Henschel
An der Welle 10, 60322 Frankfurt a. M., Deutschland
E-Mail: christoph.kromer@luther-lawfirm.com

R. Pumpler
Immofinanz AG, Wienerbergstr. 11, 1100 Wien, Deutschland
E-Mail: r.pumpler@immofinanz.com

K. Henschel
E-Mail: katharina.henschel@luther-lawfirm.com

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2_12, © Springer Fachmedien Wiesbaden 2013

Zusammenfassung

Tax Compliance im hier verstandenen Sinne als Summe der organisatorischen Maßnahmen eines Unternehmens, mit denen gewährleistet werden soll, dass sich die Geschäftsleitung wie auch die Mitarbeiter des Unternehmens und Konzerns rechtmäßig verhalten (1) ist in letzter Zeit zunehmend in die Schlagzeilen geraten. Dabei sind vor allem Banken durch Großrazzien der Steuerfahndung und Polizei aber auch durch imageschädigende materielle Klagen von Kunden in das Auge einer breiten Öffentlichkeit gerückt. (2) Es bleibt abzuwarten, inwieweit sich solche Schlagzeilen und Presseberichte aber auch damit verbundene Verhaftungen vom Mitarbeitern aus Steuerabteilungen und anderen Bereichen, Strafanzeigen gegen Vorstände, Steuernachzahlungen sowie Schadensersatz an Kunden auf die weitere geschäftliche Entwicklung betroffener Unternehmen im In- und Ausland auswirken.

Obgleich Tax Compliance aufgrund der Vielzahl vorhandener Rechts- und Strafvorschriften im In- und Ausland bei allen – nicht nur international agierenden – Unternehmen und Unternehmensgruppen an prominenter Stelle stehen sollte, ist der Befund in der Praxis ernüchternd. Nur eine geringe Zahl von Unternehmen weist eine vom Vorstand verabschiedete Steuerstrategie und darauf aufbauende Organisationsmaßnahmen auf, mit denen die tägliche Tax Compliance weltweit sichergestellt wird.

Dabei liegt die Notwendigkeit einer strukturierten und transparenten Tax Compliance-Organisation auf der Hand. Die Gesetzgeber und Finanzbehörden zahlreicher Staaten haben in den letzten Jahren massiv an einer Verschärfung aber gerade auch an der Anwendung gesetzlicher Regelungen zur Verfolgung nicht rechtmäßigen Verhaltens im Bereich der Erfüllung steuerlicher Pflichten bzw. gegen sog. aggressive Steuergestaltungen gearbeitet. Auch die Zusammenarbeit der Finanzverwaltungen über Staatengrenzen hinweg hat sich durch bilaterale bzw. multilaterale Regelungen auf EU-Ebene und seitens der OECD stark verbessert. Im Verhältnis zur Geschwindigkeit auf Seiten der Finanzverwaltungen haben die Unternehmen häufig nicht entsprechend nachgezogen. Der traditionell im angelsächsischen Raum verbreitete Begriff der „Tax Compliance“ als Umschreibung für alle Tätigkeiten im Zusammenhang mit der Erfüllung von Steuererklärungspflichten greift heutzutage deutlich zu kurz. Tax Compliance als Bestandteil der Compliance des Unternehmens geht weit über die korrekte und pünktliche Erfüllung von Steuererklärungspflichten hinaus. Hierzu sind insbesondere umfassende und weltweit greifende organisatorische Maßnahmen

erforderlich, die den ganzen Konzern und nicht nur die Steuerabteilung, aber auch außenstehende Adressaten wie Finanzverwaltungen, externe Steuerberater, Kunden und Öffentlichkeit sowie den Wirtschaftsprüfer überspannen.

Obwohl zahlreiche Unternehmen interne Compliance-Organisationen in den letzten Jahren eingezogen haben, verwundert es in zahlreichen Fällen, dass der „Bereich Steuern" dabei ausgeklammert bzw. unterstellt wird, dass die Steuerabteilung die Aufgabenstellung „Tax Compliance" alleine löst. Dabei gehören steuerliche Risiken als „Legalrisiken" zu den operationellen Risiken im Sinne von Basel II (3) bzw. darauf aufbauend nach deutschem Recht § 25 a KWG und MaRisk (4), für welche die Überwachungsverantwortung zumindest bei Kreditinstituten bei der Geschäftsleitung liegt. Entsprechend sind die Risiken auf der Ebene des gesamten (Kredit-)Instituts zu erfassen, unabhängig davon, in welcher Organisationseinheit die Risiken verursacht wurden (5). Es spricht wenig dagegen, dass dies bei Unternehmen sonstiger Wirtschaftsbranchen anders zu beurteilen wäre. Der steuerlichen Überwachung von Unternehmensprozessen kommt aus Managementsicht und aus Sicht von D&O-Versicherungen ebenfalls eine besondere Bedeutung zu, da Haftungen, welche ggf. Mängeln in der Tax Compliance zuzuordnen sind, häufig erst zeitverzögert im Nachhinein aufgrund von steuerlichen Betriebsprüfungen durch die Finanzämter auftreten. Zu diesem Zeitpunkt haben die versicherten Personen oft bereits das Unternehmen verlassen. Soweit Steuernachzahlungen mit Zeitverzögerung auftreten, sind auch erhebliche über den Marktzinsen liegende Steuerzinsen zusätzlich zu zahlen. Daneben können steuerliche Betriebsprüfungen auch zur Aufdeckung weitergehender Compliance-Verstöße in der Vergangenheit führen, z. B. durch die Aufdeckung von steuerlich nicht abzugsfähigen Schmiergeldern (6).

Insbesondere durch die bei großen Unternehmen grundsätzlich erfolgenden Überprüfungen und Nachforschungen seitens der Finanzverwaltungen mehrerer Staaten ergibt sich eine besondere Compliance-Verantwortung und ein besonderes Risikoprofil für den Bereich Steuern. Dabei ist auch zu beachten, dass nachträgliche Berichtigungen neben zusätzlichen Steuerzahlungen und zugehörenden Nebenleistungen (z. B. Zinsen oder Strafen) wiederum auch zu zusätzlichen Besteuerungen erfolgter Gewinnausschüttungen führen können.

Von daher werden wir im Folgenden ausgehend von einer begrifflichen und rechtlichen Präzisierung der „Tax Compliance" auch die möglichen Sanktionen und Risiken bei Verstößen aufzeigen. Wesentliche Schwerprunkte liegen bei der Organisation, Umsetzung und Integration der Tax Compliance in das unternehmensweite Compliance-Managementsystem. Abschließend werden Kriterien für die Beurteilung der Effizienz und Qualität eines Steuercompliance-Systems beschrieben.

(1) Vgl. Vetter, in: Wecker/van Laak, Compliance in der Unternehmerpraxis, 3. Aufl. Köln 2013, S. 33, Einleitung mit Verweis auf Bürkle, Kiethe, Schneider

(2) Deutsche Bank und HVB-Unicredit sind Beispiele: 1) Spiegel Online (www.spiegel.de) vom 28.04.2010 „Steuerfahnder durchsuchen Zentrale der Deutschen Bank", wonach mehr als 1.000 Beamte 230 Objekte der Deutschen Bank in Deutschland durchsuchen; 2) Frankfurter Rundschau Online (www.fronline.de) vom 13.12.2012 „Deutsche Bank im Visier"

und vom 12.12.2012 „Razzia bei der Deutschen Bank" mit Hinweisen auf strafrechtliche Ermittlungen gegen den Co-Vorstandschef Jürgen Fitschen und den Finanzvorstand Stefan Krause sowie Verhaftungen von 5 Bankangestellten; 3) Spiegel Online (www.spiegel.de) vom 29.11.2012 „Betrugsverdacht – Fahnder durchsuchen HypoVereinsbank" mit Verweis auf das Bundesfinanzministerium, welches von der „Geltendmachung ungerechtfertigter Steuererstattungsansprüche" spricht; 4) Das Finanzamt Wiesbaden hat der HVB vorgehalten „wider besseren Wissens" wiederholt falsche Bescheinigungen zur Abführung von Kapitalertragsteuern vorgelegt zu haben und damit „aktiv" an einem millionenschweren Steuerbetrug mitgewirkt zu haben (vgl.: manager magazin online, www.manager-magazin.de, vom 29.11.2012 mit Verweis auf Süddeutsche Zeitung); 5) Ferner: Urteil auf Schadensersatz gegen HVB-Unicredit wegen unvollständiger Aufklärung des Bankkunden über Risiken zu Medienfonds (o. V., Finanztest 10/2010); 6) o. V., „Der Fiskus spielt nicht mehr mit" in: JUVE Rechtsmarkt 12/2012, S. 64.

(3) Vgl.: Bas de Mik, Introduction to Tax Risk Management, in: Bakker/Kloosterhof, Tax Risk Management, Amsterdam, IBFD 2010, S. 15; Basel II: Revised Framework: Juni 2006, Para. 644, S. 144.

(4) BaFin-Rundschreiben 10/2010 (BA) – Mindestanforderungen an das Risikomanagement – MaRisk – idF vom 14. Dezember 2012 BA 54-FR 2210–2012/0002; gemäßAT2.2 Buchstabe d) gehören operationelle Risiken zu den wesentlichen Risiken.

(5) Ebd.

(6) In der Presse fanden insbesondere Schmiergeldaffären aus den DAX 30 bei den Unternehmen Siemens, MAN und Thyssen-Krupp besondere Beachtung. Dabei wurde auch über empfindliche Steuernachzahlungen berichtet. Vgl.: Hartmann, J., Wusste der Ex-MAN-Vorstand von Schmiergeld?, in: Die Welt online vom 15.08.2012: Demnach wird von kurzfristig fälligen Steuernachzahlungen über 500 Mio.€ für die MAN ausgegangen. Außerdem werden Schadensersatzklagen gegen Ex-Vorstände verschiedener Unternehmen angesprochen.

1 Definition und Eingrenzung des Begriffs „Tax Compliance"

In dem Beitrag „Compliance im Unternehmen" von Eberhard Vetter in diesem Buch wird der Begriff „Compliance" definiert als Pflicht, die für das Unternehmen geltenden Gesetze einzuhalten.

Der Begriff „Compliance" umfasst somit auch die Pflicht, Steuergesetze einzuhalten, die für das Unternehmen gelten. „Tax Compliance" stellt damit einen Teilbereich des Compliance-Systems eines Unternehmens dar. Dabei beinhaltet die Einhaltung der zu beachtenden Steuergesetze die Einhaltung der Steuerpflichten und die Erfüllung von Aufforderungen der Finanzverwaltung[1].

Tax Compliance stellt sich dabei – über die sich bereits aus den Gesetzen selbst ergebende Pflicht, diese einzuhalten hinaus – als Wertentscheidung eines Unternehmens dar, die Einhaltung der Pflichten ohne Ausnahme durch ein entsprechendes System sicherzustellen. Somit hat Tax Compliance einen formellen und materiellen Inhalt. Materiell umfasst

[1] Grützner/Jakob (Hrsg.), Compliance von A-Z, München 2010, „Tax Compliance".

Tax Compliance die Wertentscheidung zur Einhaltung der für das Unternehmen geltenden Vorschriften, formell bedeutet Tax Compliance die Einführung einer entsprechenden Organisationsstruktur, die in komplexen Strukturen die materiell geforderte Gesetzestreue sicherzustellen in der Lage ist.

Die Erfüllung der im Rahmen von Tax Compliance zu beachtenden Pflichten erfordert dabei entgegen einem immer noch weit verbreiteten Verständnis wesentlich mehr als die fristgerechte Abgabe von Steuererklärungen. Tax Compliance beinhaltet die Einhaltung aller steuerlichen und steuerstrafrechtlichen Regelungen, die für das Unternehmen gelten.

Der Begriff „Tax" als Bestandteil der Wortschöpfung „Tax Compliance" ist nach herrschender Meinung so zu interpretieren, dass sämtliche Steuern und Abgaben sowie alle steuerlichen Nebenleistungen wie Verzögerungsgelder, Verspätungszuschläge, Zinsen, Kostenzuschläge und Zwangszuschläge oder Zwangsgelder umfasst werden. Daneben wird auch die Einhaltung zollrechtlicher Vorschriften umfasst[2].

Die Pflicht zur Einhaltung der geltenden Gesetze in Rahmen von Tax Compliance betrifft alle unternehmerischen Organisationen und Einheiten, die Steuersubjekt sind, also Kapital- und Personengesellschaften, aber auch Vereine und Betriebe gewerblicher Art der öffentlichen Hand sowie steuerbefreite Einrichtungen.[3]

Inhaltlich hat Tax Compliance eine gestalterische, abwehrende und organisatorische Komponente:

Die gestalterische Komponente von Tax Compliance umfasst die Vermeidung von Steuern und die Steueroptimierung unter Anwendung der geltenden Steuergesetze[4]. Die abwehrende Komponente von Tax Compliance beinhaltet die Vermeidung von steuerrechtlichen und steuerstrafrechtlichen Risiken der Organe[5].

Somit bewegt sich Tax Compliance im Spannungsfeld von Risikominimierung und Steuerminimierung.

Organisatorisch bedeutet Tax Compliance die Einrichtung einer Organisation, die die Einhaltung der vom Unternehmen zu beachtenden Steuergesetze unter Einbeziehung der steuergestalterischen Möglichkeiten bei Vermeidung von Risiken für das Unternehmen und dessen Organe sicherstellt.

Systematisch ist Tax Compliance abzugrenzen von den Bereichen Tax Risk-Management und Corporate Goveranance.

Tax Risk-Management unterscheidet sich insofern von Tax Compliance als Tax Risk-Management Steuerrisiken evaluieren, aufdecken und vermeiden soll, während Tax

---

[2] Vgl.: Besch/Starck, in: Hauschka, Corporate Compliance, München 2010, § 34. Tax Compliance, Rz. 4, der auf alle Steuern, Zölle und Nebenleistungen i. S. v. § 3 AO nach deutschem Recht verweist; siehe auch auch Künstler/Seidel, in: Wecker/van Laak, Compliance in der Unternehmerpraxis, 2. Aufl. Köln 2009, S. 243.

[3] Ebd., § 34 Rz. 7.

[4] Schwedhelm, Tax Compliance – Mehr als ein Trend?, AnwBl 2/2009, S. 90 ff., S. 90; vgl. auch Künstler/Seidel, in: Wecker/van Laak, Compliance in der Unternehmerpraxis, 2. Aufl. Köln 2009, S. 244 f.

[5] Talaska, Tax Compliance in Unternehmen – Organhaftung, BB 2012, S. 1195 ff., S. 1195.

Compliance demgegenüber die Befolgung der für das Unternehmen relevanten Rechtsnormen zum Inhalt hat.[6] Wie dargestellt, umfasst die abwehrende Komponente von Tax Compliance jedoch die präventive Vermeidung von Risiken, so dass Tax Risk-Management integraler Bestandteil eines funktionierenden Tax Compliance-Systems ist.

Allerdings geht Tax Compliance insofern über bloßes steuerliches Risikomanagement hinaus, als Tax Compliance eine Grundentscheidung zur Gesetzestreue enthält, während Tax Risk Managment als Ziel eine Optimierung von Steuern ohne weitergehende Wertentscheidung umfasst.

Corporate Governance unterscheidet sich von Tax Compliance demgegenüber durch die Eingrenzung des Adressatenkreises der Vorschriften. So enthält der Deutsche Corporate Governance Kodex (DCGK)[7] unverbindliche Regelungen in Form von Empfehlungen, denen Vorstand und Aufsichtsrat insbesondere börsenorientierter Aktiengesellschaften folgen sollen (vgl. § 161 AktG)[8]. Corporate Governance-Vorschriften sind damit als Regelwerk für die Unternehmensleitung zu verstehen, während Tax Compliance erfordert, dass alle Mitarbeiter die für das Unternehmen geltenden steuerlichen Vorschriften einhalten.

Allerdings kann aus dem Corporate Governance Kodex eine Anweisung zur Compliance abgeleitet werden. In Tz. 4.1.2. des DCGK heißt es: „Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance)." Somit stellt sich Tax Compliance auch als Teilmenge der nach dem Corporate Governance Kodex zu befolgenden Vorschriften dar.

Die systematische Einordnung von Tax Compliance verdeutlicht, dass Tax Compliance Schnittmengen sowohl mit dem Bereich Tax Risk-Management als auch mit den Corporate Governance-Regeln aufweist.

Die entwickelte Definition von Tax Compliance als unternehmerische Wertentscheidung zur Einhaltung der Steuergesetze ohne Ausnahme durch die Einrichtung einer entsprechenden unternehmensinternen Organisation bedingt verschiedene Kernbausteine eines Tax Compliance-Systems.

Grundlage für eine Tax Compliance-Organisation ist die Integration einer in die Unternehmensstrategie eingebetteten Steuerstrategie, welche von der Unternehmensleitung zu verantworten ist. Hierzu gehört auch die Festlegung der Risikoneigung als Basis für die Festlegung des Risikomanagement-Systems. Weiterhin muss ein prozessbezogenes Regelwerk zur Verfügung gestellt werden, welches Mitarbeitern auf allen Hierarchieebenen Verhaltensregeln an die Hand gibt, die sicherstellen, dass alle rechtlichen Vorschriften eingehalten werden.

Wichtiger Standardbaustein einer funktionierenden Compliance-Organisation sind darüber hinaus sog. Whistleblower-Hotlines, die es Mitarbeitern ermöglichen, Compli-

[6] Besch/Starck, a. a. O., § 34. Tax Compliance, Rz. 9.

[7] BMJ- Bundesministerium der Justiz, Berlin, Erstfassung vom 26. Februar 2002, geltende Fassung vom 15. Mai 2012.

[8] Schwedhelm, Tax Compliance – Mehr als ein Trend?, AnwBl 2009, S. 90 ff, S. 90.

ance-Verstöße anzuzeigen[9]. Aus Steuersicht kann dies z. B. die Meldung von steuerlich nicht abziehbaren Schmiergeldern sein, um weitergehende strafrechtliche Folgen im Bereich der Steuerhinterziehung für das Unternehmen und nicht betroffene Mitarbeiter oder gesetzliche Vertreter zu vermeiden. Auch externe Berater – als verlängerte Werkbank bzw. Ansprechpartner von Finanzbehörden – sind in die Tax Compliance-Organisation zu integrieren und entsprechend zu überwachen. Zu den Kernbausteinen eines Compliance-Systems im Einzelnen vgl. die Ausführungen unter Ziff. VI.

2 Rechtliche Rahmenbedingungen und Prüfungsvorgaben

Rechtliche Rahmenbedingungen und Prüfungsvorgaben, die den Bereich Tax Compliance betreffen, ergeben sich aus unterschiedlichen Gesetzen und Vorschriften. Als Teilbereich von Corporate Compliance unterfällt der Bereich der Tax Compliance dabei grundsätzlich denselben Regelwerken wie der Bereich Corporate Compliance. Zudem sind die gesetzlichen Anforderungen an Risikomanagementsysteme in die Betrachtung einzubeziehen, da – wie oben dargestellt – Tax Risk-Management als integraler Bestandteil eines funktionierenden Tax Compliance-Systems anzusehen ist. Neben nationalen Gesetzen, die durch europarechtliche Vorgaben beeinflusst sind, sind auch internationale Regelwerke zu beachten. Insgesamt zeigt der folgende Überblick über die rechtlichen Rahmenbedingungen, dass in den letzten Jahren eine zunehmende Verschärfung der Anforderungen an Compliance- und Risk-Management-Systeme erfolgt ist, die sich voraussichtlich fortsetzen wird.

2.1 Nationale Vorgaben

Auf nationaler Ebene in Deutschland sind Regelungen zum Risikomanagement von Unternehmen insbesondere im HGB, AktG und GmbHG enthalten. In den letzten Jahren wurden die diesbezüglichen Anforderungen insbesondere durch europarechtlich beeinflusste Gesetze zunehmend verschärft. Darüber hinaus sind spezielle Vorschriften für Banken und Versicherungen, insbesondere die MaRisk, zu beachten.

In Deutschland bildete das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich – KontraG – für Aktiengesellschaften den Anfang einer Reihe von Gesetzen, die zu verschärften Anforderungen an das unternehmensinterne Risikomanagement führten. Mit dem KontraG wurde 1998 unter anderem die Einrichtung eines Risikofrüherkennungssystems verpflichtend eingeführt. Nach dem mit dem KontraG eingeführten § 91 Abs. 2

[9] Sog. Whistleblower-Hotlines sind Bestandteil des nach dem Sarbanes-Oxley Act aus dem Jahr 2002 für US-börsennotierte Unternehmen verpflichtend einzuführenden unternehmensinternen Kontrollsystems.

AktG hat der Vorstand geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.[10]

Als Reaktion auf die Holzmann-Pleite wurde im Jahr 2001 eine Regierungskommission eingesetzt, die unter anderem empfahl, einen Best-Practice-Code für deutsche Unternehmen zu erarbeiten. In der Folge wurde im Jahr 2002 die erste Version des Deutschen Corporate Governance Kodex (DCGK) veröffentlicht, der Empfehlungen zur Corporate Governance bei börsennotierten Gesellschaften enthält. Der Kodex beinhaltet Empfehlungen zur Best Practice und ist rechtlich nicht bindend. Dies ist vor dem Hintergrund, dass die Nichteinhaltung des Kodex somit folgenlos bleibt, stark kritisiert worden.[11]

Erhöhte Anforderungen an das Risikomanagement wurden aufgrund EU-rechtlicher Vorgaben durch das Bilanzrechtsmodernisierungsgesetz – BilMoG[12] – eingeführt, das mehrere EU-Richtlinien umsetzte[13]. Bis zum Inkrafttreten des BilMoG im Jahr 2009 lag der Fokus basierend auf den Regelungen des KontraG lediglich auf der Risikofrüherkennung.

Durch das BilMoG wurden erstmals gesetzliche Grundlagen für börsennotierte und kapitalmarktorientierte Unternehmen in Bezug auf die Anforderungen an interne Risikomanagement-, Kontroll- und Revisionssysteme geschaffen. Zudem wurden Publizitätspflichten eingeführt, wonach bei kapitalmarktorientierten Kapitalgesellschaften im Lagebericht das interne Kontroll- und Risikomanagementsystem zu beschreiben ist. Außerdem wurde eine Berichtspflicht des Abschlussprüfers über wesentliche Schwächen des internen Kontroll- und Risikofrüherkennungssystems bezüglich der Rechnungslegung eingeführt[14]. Dies bedeutet eine Erweiterung der Prüfungspflichten, da vor BilMoG lediglich eine allgemeine Berichtspflicht des Abschlussprüfers über das Nichtvorhandensein eines Risikofrüherkennungssystems bei Aktiengesellschaften bestand. Zudem wurden mit dem BilMoG die Aufgaben und Verantwortlichkeiten des Aufsichtsrats konkretisiert. Der Aufsichtsrat ist nun für die Überwachung der Wirksamkeit des internen Kontroll- und Risikomanagementsystems sowie der internen Revision zur Rechnungslegung für das Gesamtunternehmen verantwortlich[15]. Zwangsläufig wird er die Einrichtung des internen Kontroll- und Risikomanagementsystems an den Vorstand delegieren müssen und sich aber über dessen Funktionsfähigkeit regelmäßig informieren lassen. Außerdem muss er sich ein Bild davon machen, inwieweit das eingerichtete System „Good Practice-

[10] Vgl. zu den Anforderungen gem. § 91 Abs. 2 AktG Wecker/Galla in Kap. X, Tz. 2.8.1.

[11] Vgl. Theisen/Linn/Schoell, Die Berichterstattung des Aufsichtsrates im Wandel, Der Betrieb 2007, S. 2493; Kromer, Chapter 9- Germany, in: Tax Risk Management, Hrsg: Bakker/Kloosterhof, Amsterdam 2010, S. 259.

[12] BilMoG- Gesetz zur Modernisierung des Bilanzrechts vom 29.05.2009, BGBl. I 2009, S. 1102.

[13] Namentlich diente das BilMoG der Umsetzung der sog. Abschlussprüferrichtlinie (umgangssprachlich „Euro-Sox"; Richtlinie 2006/43/EG in Ergänzung durch die Richtlinie 2008/30/EG) sowie der sog. Abänderungsrichtlinie (Richtlinie 2006/46/EG) zu Einzel- und Konzernabschlüssen von Banken, Versicherungen und bestimmten anderen Unternehmensarten.

[14] §§ 289 Abs. 2 Nr. 2a u. Abs. 5, 315 Abs. 2 Nr. 5 HGB; § 171 Abs. 1 S. 2 AktG.

[15] § 107 Abs. 3 AktG.

Maßstäben“ genügt. Nach dem neu eingeführten § 107 Absatz 3 Satz 2 AktG kann der Aufsichtsrat hierzu einen Prüfungsausschuss bestellen, der sich unter anderem mit der Wirksamkeit des internen Kontrollsystems und des Risikomanagementsystems befasst. Sofern kein derartiger Prüfungsausschuss bestellt wird, nimmt der Gesamtaufsichtsrat diese Aufgaben wahr.[16] Modifikationen wurden durch das BilMoG auch im Hinblick auf die Erklärung zur Unternehmensführung vorgenommen. Nach § 289 a HGB haben insbesondere börsennotierte Aktiengesellschaften eine Erklärung zur Unternehmensführung abzugeben, in die eine Entsprechenserklärung zum DCGK gem. § 161 AktG aufzunehmen ist.

Insgesamt wurden durch das BilMoG damit deutlich klarere Verantwortlichkeiten, Haftungen und Maßstäbe für die Unternehmensführung eingeführt.

Weitergehende Spezialvorschriften bestehen für die Compliance von Banken und Versicherungen.

Nach AT 4.4.2 der neuen „Mindestanforderungen an das Risikomanagement“ – MaRisk – in der Fassung vom 14.12.2012 besteht eine Verpflichtung zur Einrichtung einer Compliance-Funktion. Bisher hatten die MaRisk in AT 2.2 bereits das Management der für das Institut wesentlichen Risiken gefordert. Die neue Fassung der MaRisk dient vor allem der Umsetzung der geplanten EU-Bankenrichtlinie CRD IV[17]. Die MaRisk, die erstmals am 20.12.2005 veröffentlicht wurden, konkretisieren § 25a KWG und dienen der Umsetzung der bankaufsichtsrechtlichen Überprüfungsprozesse für die in Basel II geregelten Eigenkapitalvorschriften in deutsches Recht.

Gemäß Basel II und den MaRisk sind bei einer Bank drei Gruppen von Risiken entscheidend. Neben Kreditausfallrisiken und Marktpreisrisiken sind operationelle Risiken zu berücksichtigen. Zu den operationellen Risiken zählen Legalrisiken, unter die auch steuerliche Risiken zu subsumieren sind. Den Vorstand bzw. die Geschäftsleitung trifft nach Basel II die Pflicht, die operationellen Risiken zu überwachen und zu steuern.

Weitergehende Anforderungen im Hinblick auf die Compliance von Wertpapierdienstleistungsinstituten ergeben sich aus den „Mindestanforderungen an Compliance und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 31ff. WpHG (MaComp)“ vom 7.6.2010. Das Rundschreiben der BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) konkretisiert die Verhaltens-, Organisations- und Transparenzpflichten des WpHG (Wertpapierhandelsgesetz), die Kredit- und Finanzdienstleistungsinstitute beachten müssen, wenn sie Wertpapierdienstleistungen gegenüber Kunden erbringen.

Aufgrund der Relevanz von in den letzten Jahren eingeführten Corporate Governance-Regeln und Compliance-Vorschriften wurden bereits bei zahlreichen Unternehmen Compliance-Management-Systeme etabliert. Für freiwillige Prüfungen derartiger Syste-

[16] Pampel/Glage, in Hauschka, Corporate Compliance (2010), § 5. Unternehmensrisiken und Risikomanagement, Rz. 14.

[17] Am 16. April 2013 hat das Europäische Parlament den Text zum CPD-IV-Maßnahmenpaket nach mehrmonatigen Trilog-Verhandlungen angenommen. Für ein Inkrafttreten ist die formale Annahme des Regelwerks durch den EU-Ministerrat erforderlich.

me hat das IDW einen Prüfungsstandard erlassen, der die Zugrundelegung einheitlicher Standards bei derartigen Prüfungen sicherstellen soll. Nach Prüfungsstandard IDW PS980 vom 11.3.2011 über die Grundsätze ordnungsgemäßer Prüfung von Compliance Management Systemen (CMS) ist ein bedeutender Bestandteil einer CMS-Prüfung auch die Tax Compliance. In Ziff. A3 des IDW PS980 werden als Prüfungsgebiete aus dem steuerlichen Bereich beispielhaft das Außensteuer- und Zollrecht genannt. Effektive CMS müssen daher auch in der Lage sein, den Bereich des Steuerrechts sowohl im Hinblick auf die Organisation von Abteilungen und Verantwortlichkeiten als auch bei der Anwendung von Steuergesetzen wirksam zu erfassen, damit eine Prüfung zu dem gewünschten Erfolg führt.[18] Es ist davon auszugehen, dass der Prüfungsstandard auch auf Prüfungen nach den Vorschriften für börsennotierte und kapitalmarktorientierte Unternehmen zu Aussagen über das Risikomanagementsystem übertragbar ist.

2.2 Internationale Vorgaben

Unter anderem als Reaktion auf die Unternehmenszusammenbrüche von Enron und Worldcom traten mit dem im Jahr 2002 erlassenen Sarbanes-Oxley Act (SOA) bedeutende Neuregelungen für die Finanzberichterstattung von US-börsennotierten Unternehmen in Kraft. Die Neuregelungen betrafen unter anderem unternehmensinterne Kontroll- und Überwachungssysteme sowie die Verantwortung der Unternehmensleitung, der Aufsichtsgremien und der Abschlussprüfer. Besondere Bedeutung kommt in diesem Zusammenhang den in Section 404 SOA enthaltenen Regelungen zu, nach denen das Management eines an der US-Börse gelisteten Unternehmens für die Einrichtung und Aufrechterhaltung eines angemessenen internen Kontrollsystems zur Finanzberichterstattung sowie für die jährliche Beurteilung und Berichterstattung über die Wirksamkeit dieses internen Kontrollsystems verantwortlich ist.[19]

Ähnliche Vorschriften enthält der am 15. Februar 2007 veröffentliche japanische Standard Naibutousei, auch J-SOX genannt. Dieser enthält Anforderungen für Unternehmen, die an der japanischen Börse gelistet sind.

Auf europäischer Ebene wurden teilweise vergleichbare Regelungen mit der sog. Abschlussprüferrichtlinie (Richtlinie 2006/43/EG) vom 17.5.2006 verabschiedet, die von den Mitgliedsstaaten bis zum 29.6.2008 in nationales Recht umzusetzen waren. In Deutschland ist die Umsetzung u. a. durch das BilMoG erfolgt. Allerdings ist festzustellen, dass die Umsetzungen in den einzelnen EU-Staaten beachtliche Unterschiede aufweisen.

Am 25. Mai 2011 hat die OECD-Ministerkonferenz eine Neufassung der erstmals im Jahr 1976 veröffentlichten Leitsätze verabschiedet. Dieses Regelwerk enthält Empfehlungen für ein verantwortungsvolles unternehmerisches Handeln. Mehrere OECD-Mitgliedstaaten sehen die Anwendung der OECD-Leitsätze als verbindlich an. Im

[18] Parsow, Verzahnung Tax, Krisenmanagement und Compliance, DB 2011, Heft 26/27, M1.

[19] Vgl. hierzu Pampel/Glage, a. a. O., § 5. Unternehmensrisiken und Risikomanagement, Rz. 11 ff.

Gegensatz zu anderen Verhaltenskodizes gehen die OECD-Leitsätze in einem eigenen Kapitel explizit auf die Besteuerung ein. Dieses Kapitel ist im Vergleich zur Vorgängerversion erheblich ausgeweitet worden.[20]

Im Wesentlichen beinhaltet Kapitel XI. der OECD-Leitsätze für multinationale Unternehmen folgende Kernpunkte, die nach dem Regelwerk beachtet werden sollen:

- Befolgung der Buchstaben und des Geistes der Steuergesetze und -vorschriften der Länder
- Transparenz und Kooperation
- Beachtung des Fremdvergleichsgrundsatzes bei der Festlegung von Verrechnungspreisen
- Einführung einer Risikomanagementstrategie im Steuerbereich.

Zwar handelt es sich bei den OECD-Leitsätzen aus deutscher Sicht lediglich um Grundsätze und Empfehlungen, deren Nichtbeachtung keine unmittelbaren rechtlichen Folgen hat. Insbesondere werden keine rechtlichen Sanktionen oder Kompensationen ausgelöst. Dennoch ist den OECD-Leitsätzen ein besonderes Gewicht beizumessen, da es sich um den einzigen multilateral anerkannten Kodex für multinationale Unternehmen handelt, den Regierungen untereinander vereinbart haben. Auch die deutsche Finanzverwaltung sieht deshalb die verabschiedeten Leitsätze als Unternehmensstandard an.

Bei Verstößen gegen die OECD-Leitsätze können bei den in den Teilnehmerstaaten eingerichteten Nationalen Kontaktstellen Beschwerden durch die Finanzverwaltungen und die Steuerpflichtigen eingereicht werden. Im Bereich der Besteuerung konnten bis zum Juni 2011 neun Beschwerdeverfahren verzeichnet werden, die vor allem in Entwicklungsländern tätige Rohstoffunternehmen mit Sitz im Ausland betrafen. Als Folge eines Beschwerdeverfahrens ist die Veröffentlichung von – unter Umständen auch sensiblen – Informationen in der Abschlusserklärung der Nationalen Kontaktstelle vorgesehen. Infolge eines Beschwerdeverfahrens drohen insbesondere Reputationsverluste für Unternehmen.

In einzelnen Staaten sind bei einem Verstoß gegen die OECD-Leitlinien direkte Sanktionen vorgesehen. In anderen Staaten erfolgt eine Koppelung der Vergabe von Investitionsschutzgarantien und Exportsubventionen an die explizite Bereitschaft, die OECD-Leitsätze zu befolgen (z. B. in den Niederlanden). In Deutschland bestehen momentan noch keine derartigen Mechanismen. Von verschiedenen Seiten wird jedoch eine Koppelung der Außenwirtschaftsförderung an die Einhaltung der Leitsätze gefordert, so dass Unternehmen möglicherweise zukünftig mit entsprechenden Restriktionen in Deutschland rechnen müssen, wenn sie die Kernpunkte der Tax Compliance des Kap. XI. der OECD-Richtlinien nicht umgesetzt haben.[21]

---

[20] Hardeck, Die Empfehlungen der OECD-Leitsätze für multinationale Unternehmen im Bereich der Besteuerung, IStR 2011, S. 933.

[21] Vgl. zum Ganzen: Hardeck, a. a. O., S. 933 ff.

2.3 Aktuelle Entwicklungen auf europäischer Ebene

Aktuell zeichnen sich auch auf europäischer Ebene weitere Neuerungen im Bereich der Tax Compliance ab. Am 06.12.2012 hat die EU-Kommission den „Aktionsplan zur Verstärkung der Bekämpfung von Steuerbetrug und Steuerhinterziehung" der EU (COM (2012) 722 final) vorgelegt. Der Aktionsplan enthält einen Maßnahmenkatalog für sofortige und künftige Maßnahmen, die den Mitgliedsstaaten helfen sollen, ihre Steuergrundlagen zu schützen. Laut Ziff. 4.1.3. des Aktionsplans ist die Entwicklung eines europäischen Kodex für die Steuerpflichtigen als kurzfristige Maßnahme für 2013 geplant. Der Kodex soll Erläuterungen bewährter Verfahren enthalten, durch die Zusammenarbeit und Vertrauen zwischen Steuerverwaltungen und Steuerpflichtigen verbessert werden, die Transparenz bezüglich der Rechte und Pflichten der Steuerpflichtigen erhöht und ein dienstleistungsorientiertes Konzept gefördert wird. Es finden sich Parallelen zu den OECD-Leitlinien.

2.4 Rechtspflicht zur Einrichtung eines Tax Compliance-Systems

Nach der einleitend vorgenommenen Einordung von Tax Compliance als Wertentscheidung eines Unternehmens, die Einhaltung der Pflichten ohne Ausnahme durch ein entsprechendes System sicherzustellen, stellt sich die Frage, ob eine Rechtspflicht zur Einrichtung eines entsprechenden Systems besteht. In der Literatur wird die Frage, ob sich eine Rechtspflicht zur Implementierung eines Tax Compliance-Systems ergibt, kontrovers diskutiert[22]. Dabei werden allerdings häufig nicht alle rechtlichen Grundlagen ausreichend beachtet.

Andererseits haben die internationalen Standardsetter mit Basel II, die EU, die Gesetzgeber in mehreren Staaten sowie die Finanzverwaltungen der OECD-Mitgliedstaaten bereits Fakten geschaffen, an denen zahlreiche Unternehmen, insbesondere kapitalmarktorientierte und außenwirtschaftsorientierte Unternehmen nicht mehr vorbei können. Jedenfalls im Bereich von Banken und Versicherungen ist nach der Neufassung der MaRisk die Einrichtung eines Compliance-Systems, welches auch die Verpflichtung zur Überwachung steuerlicher Risiken umfasst, vorgeschrieben. Ob dies auch für andere Unternehmen der Fall ist, kann dahingestellt bleiben, da eine verantwortungsvolle Unternehmensleitung zur Vermeidung der im folgenden Abschnitt beschriebenen Sanktionen und Haftungsrisiken und mit Blick auf die Anforderungen der D&O-Versicherungen jedenfalls die Einrichtung und den Nachweis einer entsprechendes Organisation aus Eigenschutz nicht mehr vermeiden kann.

[22] Gegen eine solche Pflicht z. B. Besch/Starck, a. a. O., § 34. Tax Compliance, Rz. 8 sowie Streck in Streck/Mack/Schwedhelm, Tax Compliance, Köln 2010, Kap. 1 A. V.; vgl. ebenfalls die Beiträge in diesem Buch von Wecker/Galla, Ziff. 2.6 und Vetter, Ziff. 2.2.

3 Sanktionen und Risiken bei Verstößen

3.1 Arten und Betroffene von Sanktionen und Risiken

Sanktionen und Risiken bei Verstößen gegen steuerliche Vorschriften können sich gegen das steuerpflichtige Unternehmen aber auch gegen dessen Vertreter oder Organe richten. Dabei sind die möglichen Sanktionen vielfältig und können zugleich in mehreren Ländern mit unterschiedlicher Auswirkung auftreten. In einzelnen Staaten (z. B. Großbritannien) können darüber hinaus – in Abhängigkeit von der Unternehmensgröße – Beschreibungen der Tax Compliance-Organisation von der Finanzverwaltung verlangt werden, um ggf. Organisationsverschulden einschätzen zu können. Auch in Deutschland kann dies prozessbezogen gelten, z. B. für die Systeme des Rechnungswesens[23].

Sanktionen und Risiken bei Verstößen gegen Tax Compliance-Regelungen können

- finanzieller Art durch Strafzahlungen, Schadensersatzleistungen oder Steuernachzahlungen mit/ohne Nebenleistungen sowie ungewisse Aufwendungen für Beratungs- und ggf. Gerichtskosten,
- strafrechtlicher Art durch Bußgelder oder Gefängnisstrafen,
- berufsrechtlicher Art bei Wirtschaftsprüfern oder Steuerberatern sowie
- nicht-materieller Art durch Reputationsverlust oder Ausschluss der Beteiligung an privaten oder öffentlichen Ausschreibungen sein.

Indien, Australien und Russland schließen beispielsweise Unternehmen von der Teilnahme an öffentlichen Ausschreibungen aus, wenn Steuererklärungen nicht rechtzeitig eingereicht oder Steuerzahlungen verspätet geleistet werden. Ungenügende Tax Compliance außerhalb rechtlicher Vorschriften kann imageschädigend wirken. So können sich Presseinformationen in Zeitschriften, die von Kapitalanlegern gelesen werden, über Verfahren zur Falschberatung bei vermeintlich steueroptimierten Bankprodukten, auf bestehende Kundenkontakte bzw. die Neukundengewinnung auswirken[24]. Sicherlich wäre in solchen Fällen eine verbindliche Auskunft im Vorhinein bei der Finanzbehörde – gerade auch bei befürchteter Ablehnung- die richtige Vorgehensweise gewesen.

Im Folgenden werden vorwiegend in Deutschland anwendbare Sanktionen vorgestellt. Andere Staaten können davon abweichende sowohl strengere als auch mildere Sanktionen vorsehen. Von daher ist es im Sinne einer funktionierenden Tax Compliance-Organisation unverzichtbar, dass alle möglicherweise zur Anwendung kommenden Sanktionen im

[23] Siehe: GoBS – Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme", BStBl. I 1995, S. 738 ff.; Anm.: Es ist geplant, die GoBS durch die GoBIT (Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz) künftig zu ersetzen.

[24] Bsp.: Urteil auf Schadensersatz gegen HVB-Unicredit wegen unvollständiger Aufklärung des Bankkunden über Risiken zu Medienfonds (vgl.: o. V., Finanztest 10/2010).

In- und Ausland bei Verstößen gegen Compliance-Vorschriften dem Unternehmen und seinen Mitarbeitern bekannt sind, um Schaden vom Unternehmen abzuwenden.

Sanktionen nach dem deutschen Steuerrecht können in steuerlichen Nebenleistungen, in Ordnungswidrigkeiten und Geldstrafen oder Freiheitsstrafen bestehen. Daneben können Organe (gesetzliche Vertreter oder Verfügungsberechtigte) bei Steuerhinterziehung oder Organisationsverschulden haften. Die Schwellen zum Steuerstrafrecht und zur Organhaftung aufgrund von Compliance-Verstößen liegen bei Umsatzsteuern und Lohnsteuern deutlich niedriger als bei Ertragsteuern. Über die Steuergesetze hinausgehende Haftungen können Mitarbeiter, Wirtschaftsprüfer, Steuerberater und Aufsichtsräte treffen. Steuerliche Nebenleistungen oder Geldstrafen können nicht als Aufwendungen steuerlich geltend gemacht werden.

3.2 Verspätungszuschläge und Säumniszuschläge

Ein *Verspätungszuschlag* kann von der Finanzverwaltung festgesetzt werden, wenn die Steuererklärung nicht oder nicht rechtzeitig eingereicht wird. Dabei steht das Verschulden durch einen Mitarbeiter oder einen Steuerberater dem eigenen Verschulden gleich. Die Entscheidung über die Festsetzung und die Höhe des Verspätungszuschlags steht im Ermessen der Finanzverwaltung. Er wird mit der Steuer festgesetzt und darf höchstens 10 % der festgesetzten Steuer sowie nicht mehr als 25.000 € betragen[25].

Ein *Säumniszuschlag* fällt bei einer um mehr als 3 Tage verspäteten Steuerzahlung an. Der Säumniszuschlag beträgt 1 % der zu entrichtenden Steuerschuld für jeden angefangenen Monat bis zur Zahlung des rückständigen Betrags[26].

Von besonderer Schwere sind verspätete Einreichungen von Lohnsteuer-Anmeldungen und Umsatzsteuer-Voranmeldungen, welche bei größeren Unternehmen monatlich einzureichen und abzuführen sind. Verspätete Einreichungen und Zahlungen, bei denen es um die Abführung von Dritten einbehaltener Steuern geht, können als fahrlässig eingestuft werden. Wiederholt verspätet eingereichte Anmeldungen und Zahlungen werden als grob fahrlässig bis vorsätzlich im Sinne strafrechtlicher Relevanz eingestuft. Materielle Nachzahlungen auf Grundlage jährlicher Erklärungen sind kritisch zu beurteilen. Die Erklärung und Zahlung der Steuern muss sich den einzelnen Voranmeldungsperioden zuordnen lassen und sollte entsprechend korrigiert werden.

3.3 Zinsen

Zinsen sind auf Steuerzahlungen durch Steuerpflichtige und auf Steuererstattungen durch die Finanzverwaltung zu entrichten. Zinsen fallen auch bei nachträglichen Steuerfestsetzungsänderungen, z. B. aufgrund einer Betriebsprüfung, an. Der Zinslauf beginnt 15

[25] § 152 AO.
[26] § 240 AO.

Monate nach dem Ende des relevanten Steuerjahrs und endet mit dem Tag an dem die Steuerfestsetzung wirksam wird[27]. Der Zinssatz beträgt 0,5 % der nachzuentrichtenden bzw. zu erstattenden Steuer pro Monat, d. h. 6 % p. a[28]. Aufgrund des weit über dem derzeitigen Marktzins liegenden Zinssatzes sind Zinszahlungen weitestgehend zu vermeiden. Von daher sollte bereits bei Bekanntwerden vorläufiger Feststellungen, die zu Nachzahlungszinsen führen, im Regelfall bereits eine entsprechend berichtigte Steuererklärung und Steuernachzahlung durch das Unternehmen ausgelöst werden. Auch in strittigen Fällen kann eine frühzeitige Zahlung zur Vermeidung weiterer Vermögensnachteile angezeigt sein. Mit einer solchen Zahlung ist zumindest in Deutschland keine Anerkennung der Verwaltungsposition verbunden.

Beispiel

Die X-GmbH muss aufgrund einer Betriebsprüfung Umsatzsteuern für die Jahre 2006–2008 1.000.000 € für das Jahr 2006, 500.000 € für das Jahr 2007 und 250.000 € für das Jahr 2008 nachzahlen. Das Finanzamt erlässt entsprechend berichtigte Steuerbescheide. Die Steuerfestsetzung wird zum 1. April 2013 wirksam. Entsprechend hat die X-GmbH neben den Steuernachzahlungen an Zinsen 570.000 € zu entrichten.

In Fällen der Steuerhinterziehung sind hinterzogene Steuern nach denselben Grundsätzen zu verzinsen, wobei der Zinslauf bereits mit dem Eintritt der Verkürzung der Steuern beginnt[29].

Beispiel

Die Y-GmbH reicht ihre Umsatzsteueranmeldung für den Monat September 2011 fristgerecht am 8. November 2011 ein und erhält aufgrund dessen eine Steuererstattung vom Finanzamt über 1.000.000 €. Im Rahmen einer Prüfung der Finanzverwaltung im Januar 2013 vertritt diese die Auffassung, dass anstelle einer Erstattung von 1.000.000 € eine Steuernachzahlung über 500.000 € zu entrichten sei. In Höhe von 1.500.000 € erkennt die Finanzverwaltung eine Steuerhinterziehung und verlangt hierauf 6 % bzw. 90.000 € an Hinterziehungszinsen für zwölf Monate[30].

---

[27] S. hierzu Künstler/Seidel, in: Wecker/van Laak, Compliance in der Unternehmerpraxis, 2. Aufl. Köln 2009, S. 250 f.

[28] §§ 233 a, 238 Abs. 1 AO; Besonderheiten sind gem. §§ 236, 237 AO bei Festsetzungsänderungen durch Gerichtsentscheid und in Fällen der Aussetzung der Vollziehung bei Rechtsbehelfen oder Anfechtungsklagen zu beachten.

[29] § 235 Abs. 1 u. 2 AO.

[30] Die Finanzverwaltung erkennt auch dann eine Steuerhinterziehung mit der Verpflichtung zur Zahlung von Hinterziehungszinsen, wenn die zu viel geltend gemachten Steuern im Rahmen einer später fristgerecht eingereichten Umsatzsteuer-Steuererklärung berichtigt werden. In diesem Fall läuft der Zinslauf vom Monat der Einreichung der Voranmeldung bis zur Festsetzung der Umsatzsteuer aufgrund Steuererklärung.

Soweit die Voraussetzungen für Zinsen auf Steuernachzahlungen und auf Hinterziehung für einzelne Monate gleichzeitig vorliegen, sind die Zinsen auf Steuernachzahlungen auf die Hinterziehungszinsen anrechenbar[31].

In Fällen der Steuerhinterziehung haftet neben dem Unternehmen als originärem Steuerschuldner auch jede Person, die eine Steuerhinterziehung begeht oder daran teilnimmt. Dies gilt sowohl für nachzuentrichtende Steuern als auch für Hinterziehungszinsen[32].

3.4 Zwangsgelder und Verzögerungsgelder

Die Finanzbehörde darf *Zwangsgelder* bis zu 25.000 € zur Erzwingung der Einreichung von Steuererklärungen oder anderer Handlungen, z. B. Erfüllung von Buchführungspflichten oder Aushändigung von Unterlagen, festsetzen. Die Finanzbehörde darf auch einen Dritten mit der Vornahme der Handlung auf Kosten des Steuerpflichtigen beauftragen soweit eine solche „Ersatzvornahme" möglich ist. Ein Zwangsgeld kann jeweils für jede Handlung der Nicht-Kooperation oder Verletzung von Mitwirkungspflichten festgesetzt werden[33].

Seit 2009 ist neben die Festsetzungsmöglichkeit von Zwangsgeldern das sog. „*Verzögerungsgeld*" getreten. Das Verzögerungsgeld kann zur Anwendung kommen, wenn der Steuerpflichtige innerhalb einer angemessenen Frist

- nicht seinen Pflichten zur Erteilung von Auskünften oder
- während einer Außenprüfung der Finanzverwaltung nicht seinen Mitwirkungspflichten zur Vorlage von Unterlagen oder zur Gewährung des Datenzugriffs oder
- bei Outsourcing oder Verlagerung der Buchführungssysteme ins Ausland nicht der Aufforderung zur Rückverlagerung seiner elektronischen Buchführung ins Inland folgt.

Das Verzögerungsgeld kann auch festgesetzt werden, wenn die elektronische Buchführung ohne Zustimmung (bzw. einzelne Teile davon) der Finanzverwaltung ins Ausland verlagert wurden.

Verzögerungsgelder können von der Finanzverwaltung anlassbezogen zwischen 2.500 € und 250.000 € festgesetzt werden[34]. Neben den steuerlichen Mitwirkungspflichten betrifft die Regelung vor allem Shared Service-Center im Ausland sowie Outsourcing-Verträge

[31] § 235 Abs. 4 AO; Anm.: In zahlreichen Ländern findet eine zu Deutschland vergleichbare Anrechnung nicht statt.

[32] § 71 AO; siehe auch Künstler/Seidel, in: Wecker/van Laak, Compliance in der Unternehmerpraxis, 2. Aufl. Köln 2009, S. 246.

[33] §§ 328–333 AO.

[34] § 146 Abs. 2b AO.

mit Dritten zu buchführungs- oder IT-bezogenen Tätigkeiten[35]. Hierbei ist auch an die verhältnismäßig langen Aufbewahrungspflichten und damit verbunden die Vorhaltung elektronischer Zugriffsrechte von 10 Jahren oder mehr z. B. bei nicht abgeschlossenen Betriebsprüfungen in Deutschland zu denken[36].

3.5 Schätzung von Besteuerungsgrundlagen

In Fällen unzureichender Kooperation von Steuerpflichtigen aus Sicht der Finanzverwaltung stellt die Schätzung von Besteuerungsgrundlagen die *ultima ratio* dar. Auch in Fällen von Verstößen gegen die Grundsätze ordnungsmäßiger Buchführung (GoB) oder anderer Verletzungen der gesetzlichen Buchführungs- und Aufbewahrungspflichten kann es zu Schätzungen kommen[37]. Die zunehmende Bedeutung des Datenzugriffs (digitale Betriebsprüfung)[38] und der damit verbundenen Überprüfung der Erfüllung der GoBS verlangen, dass der Steuerpflichtige nahezu alle IT-Systeme und zugehörigen Verfahrensdokumentationen vorhält. Soweit einzelne Teile oder noch nicht geprüfte Jahre archiviert wurden, ist dies mit der Finanzverwaltung abzustimmen und der Datenzugriff sicherzustellen, um den Verdacht unvollständiger Daten auszuräumen. Die Erfahrungen der letzten Jahre mit der zunehmend verbreiteten Anwendung der digitalen Betriebsprüfung haben gezeigt, dass Steuerpflichtige mit Mängeln beim Datenzugriff oder der elektronischen Aufbewahrung von Daten ein höheres Risiko haben, unerwartete Steuernachzahlungen bzw. in Einzelfällen sogar Steuerschätzungen zu realisieren.

Mit Blick auf das Ausland ist anzumerken, dass eine zunehmende Zahl von Ländern bereits aus Verstößen gegen Formvorschriften ein Recht zur Steuerschätzung ableiten.

3.6 Keine oder unzureichende Dokumentation von Verrechnungspreisen

Zahlreiche Staaten haben in den letzten Jahren Sanktionsvorschriften bei unzureichender Anfertigung von Dokumentationen konzerninterner Verrechnungspreise eingeführt. Dabei sehen mehrere Staaten auch sanktionsbewehrte Dokumentationspflichten für Verrechnungspreise zwischen inländischen Konzerngesellschaften vor, z. B. Großbritannien und Ungarn.

Deutschland hat in 2003 empfindliche Sanktionen eingeführt. Das Gesetz (§ 162 Abs. 2 und 3 AO) sieht bei Nichterfüllung folgende „Strafen“ vor[39]:

---

[35] Vgl. ausführlicher: Kromer, Germany – Chapter 9, in: Tax Risk Management, Hrsg. Bakker/Kloosterhof, Amsterdam 2010, S. 271 f.

[36] § 147 Abs. 3 AO.

[37] § 162 Abs. 1 und 2 AO.

[38] § 147 Abs. 6 AO.

[39] Vgl. auch Künstler/Seidel, in: Wecker/van Laak, Compliance in der Unternehmerpraxis, 2. Aufl. Köln 2009, S. 250.

a. Bei Nichtvorlage oder bei unzureichender Vorlage bzw. bei nicht zeitnaher Erstellung der Dokumentation kann die Finanzverwaltung die zutreffende Steuer schätzen (i. S. d. Umkehr der Beweislage). Soweit hierbei Spielräume zur Höhe ansetzbarer Verrechnungspreise gegeben sind, darf die Finanzverwaltung diese zu Lasten des Steuerpflichtigen mit Wirkung auf Ertragsteuern und Umsatzsteuer ausnutzen.
b. Bei Nichtvorlage oder unzureichender Vorlage der Verrechnungspreisdokumentation werden mind. 5 % und max. 10 % als Zuschlag auf die Mehrsteuern festgesetzt. Unabhängig davon werden selbstverständlich auch Zinsen auf nachzuzahlende Steuern aus früheren Jahren festgesetzt.
c. Bei verspäteter Vorlage verwertbarer Dokumentationen beträgt der Zuschlag bis zu 1 Mio. €, mindestens 100 € pro Tag der Fristüberschreitung. Dabei sieht das Gesetz kein Ermessen für eine Nichtfestsetzung im Anwendungsfall vor.
d. § 162 Abs. 4. S. 6 AO: Das Verschulden eines gesetzlichen Vertreters oder eines Erfüllungsgehilfen steht dem eigenen Verschulden gleich.

Es gibt nur wenige gesetzliche Regelungen im Steuerrecht, die derart empfindliche Strafen zur „Erzwingung" gesetzlicher Pflichten vorsehen. Insbesondere gilt dies auch für die explizite Managerhaftung nach (d), welche ggf. nicht von einer D&O-Versicherung abgedeckt wird. Ein Versicherungsausschluss dürfte häufig dann gelten, wenn das Management vorsätzlich oder fahrlässig die gesetzlichen Vorgaben nicht beachtet oder umgesetzt hat.

Eine Gegenberichtigung von Verrechnungspreisen im Ausland dürfte bei fehlender oder unzureichender Dokumentation der Verrechnungspreise ebenfalls kaum möglich sein.

3.7 Steuerhinterziehung und leichtfertige Steuerverkürzung

Die Verkürzung von Steuerzahlungen ist als Steuerhinterziehung und damit als Straftat definiert. Dafür ist es bereits ausreichend, wenn Steuern pflichtwidrig nicht rechtzeitig festgesetzt werden. Dies gilt damit auch bereits für (Vor-)Anmeldungen oder für unter dem Vorbehalt der Nachprüfung stehende Steuern[40]. Steuerhinterziehung kann mit Gefängnisstrafen bis zu 5 Jahren in besonders schweren Fällen bis zu 10 Jahren oder mit Geldstrafen bestraft werden. Jede natürliche Person kommt dabei als Täter oder Teilnehmer in Betracht.

Beispiel

Im Rahmen einer mehrfachen Übertragung eines Wirtschaftsguts über die Grenze fehlen Belege, die einen Vorsteuerabzug rechtfertigen. Auf Geheiß des Leiters Rechnungswesens bucht der zuständige Buchhalter die Anschaffung mit Vorsteuerschlüssel

[40] § 370 Abs. 4 AO.

ein und erstellt die Umsatzsteuer-Voranmeldung entsprechend. Im Rahmen der Jahreserklärung zur Umsatzsteuer erfolgt durch den Mitarbeiter der Steuerabteilung keine weitergehende Prüfung der in den Voranmeldungen geltend gemachten Vorsteuerabzüge. Die Steuererklärung wird von der Geschäftsführung unterschrieben. Neben dem Unternehmen als Steuerpflichtigem haften für die zu Unrecht erstattete Vorsteuer und damit verbundene Hinterziehungszinsen auch der Buchhalter und der Leiter Rechnungswesen nach § 71 AO. Aber auch der Mitarbeiter der Steuerabteilung sowie dessen Vorgesetzter können als mitwirkende Teilnehmer gesehen werden, da keine ausreichenden Kontrollen vorgenommen wurden. Daneben haftet die Geschäftsführung gem. § 69 AO. Alle vorgenannten Personen kommen daneben in strafrechtlicher Hinsicht als Täter oder Teilnehmer in Betracht. Täter oder Teilnehmer können in diesem Fall zusätzlich auch Geschäftspartner sein, die an Übertragungsvorgängen beteiligt waren.

Täter oder Teilnehmer an einer Steuerhinterziehung können durch „*Selbstanzeige*" unter bestimmten Voraussetzungen Straffreiheit erlangen. Solche Voraussetzungen sind insbesondere, dass die Tat noch nicht entdeckt wurde und noch keine Prüfungsanordnung bekannt gegeben wurde sowie noch kein Vertreter der Finanzbehörde zur steuerlichen Prüfung oder zur Ermittlung einer Steuerstraftat oder entsprechenden Ordnungswidrigkeit erschienen ist. Daneben darf noch keine Einleitung des Straf- oder Bußgeldverfahrens gegenüber dem Täter bekannt gegeben worden sein. Straffreiheit tritt zusätzlich nur ein, wenn der Täter oder andere an der Tat beteiligte Personen innerhalb der von der Finanzbehörde gesetzten Frist die hinterzogenen Steuern entrichten[41].

Das Gesetz sieht den Fall einer *leichtfertigen Steuerverkürzung* und damit eine Ordnungswidrigkeit für Fälle der nicht vorsätzlichen Steuerverkürzung vor. Leichtfertige Steuerverkürzungen können mit Geldbußen bis 50.000 € bestraft werden. Unter bestimmten Umständen ist eine bußgeldbefreiende Selbstanzeige in Fällen der leichtfertigen Steuerverkürzung noch solange möglich, als die Einleitung eines Straf- oder Bußgeldverfahrens wegen der Tat gegenüber dem Steuerpflichtigen noch nicht bekannt gegeben wurde.

Steuerhinterziehung sowie leichtfertige Steuerverkürzung sind aus Compliance-Sicht als Grenzen der Steuergestaltung und Steuerplanung zu sehen, die nicht übertreten werden dürfen[42].

3.8 Haftung

Geschäftsführer sowie gesetzliche Vertreter von Kapitalgesellschaften haften für Steuerschulden der Gesellschaft bei grob fahrlässiger oder vorsätzlicher Verletzung rechtlicher

[41] § 371 Abs. 1–3 AO.

[42] Gl. A.: Wulf, Tax Compliance als Feld steueranwaltlicher Tätigkeit, AnwBl 10/2010, S. 656.

Pflichten mit ihrem Privatvermögen[43]. Dies kann z. B. bei Zahlungsverzug gegeben sein. Die Haftung gilt aber auch noch nach dem Ausscheiden aus dem Unternehmen für nicht final festgesetzte Steuern, die aus zurückliegenden Perioden der Verantwortung resultieren. Von daher liegen funktionierende Überwachungssysteme wie Fristen- und Zahlungskontrollen auch im persönlichen Interesse der Geschäftsführung.

In Fällen der Steuerhinterziehung haften alle Teilnehmer an der Steuerhinterziehung für hinterzogene Steuern und Hinterziehungszinsen (Bsp. 3.7 zum Umfang der Haftung). Dies erfasst explizit auch die unrichtige oder nicht vorgenommene Verbuchung von Geschäftsvorfällen, z. B. Schwarzgeldumsätze, durch Personen, die daraus keinen persönlichen Vorteil erzielen[44].

Weitere Haftungsregelungen sind u. a. in Fällen der Betriebsübernahme beim Übernehmer, in Fällen der Lohnsteuer beim Arbeitgeber sowie in Fällen der Abführung von Umsatzsteuer und Kapitalertragsteuer zu beachten[45].

3.9 Zusätzliche Sanktionen im Bereich der Umsatzsteuer

Das Umsatzsteuergesetz sieht zusätzliche Bußgeld- und Strafvorschriften vor. So handelt ordnungswidrig, wer eine Rechnung nicht oder nicht rechtzeitig ausstellt, gegen die Aufbewahrungspflichten verstößt, bzw. einzureichende oder vorzulegende Unterlagen nicht oder nicht rechtzeitig erstellt[46].

In Fällen der Nichtentrichtung oder nicht vollständigen Entrichtung von in Rechnungen ausgewiesener Umsatzsteuern können Geldbußen bis zu 50.000 € festgesetzt werden. Werden solche Handlungen zusammen mit anderen Personen wiederholt begangen, sind neben Geldstrafen auch Haftstrafen bis zu 5 Jahren wegen banden- oder gewerbsmäßiger Schädigung des Umsatzsteueraufkommens möglich[47].

3.10 Folgen bei Erbringung unzulässiger Beratungsleistungen durch Wirtschaftsprüfer oder mit diesen verbundenen Unternehmen

Obwohl zahlreiche Länder im letzten Jahrzehnt die Regelungen zu erlaubten Beratungsleistungen durch den Wirtschaftsprüfer verschärft haben, trifft man in der Praxis immer wieder auf eine erhebliche Sorglosigkeit bei Vorständen, Aufsichtsräten und

[43] § 69 AO; vgl. hierzu auch Künstler/Seidel, in: Wecker/van Laak, Compliance in der Unternehmerpraxis, 2. Aufl. Köln 2009, S. 245 f.

[44] § 70–72 AO.

[45] § 75 AO, §§ 42 d und 44 Abs. 5 EStG, § 25d UStG; s. auch Künstler/Seidel, in: Wecker/van Laak, Compliance in der Unternehmerpraxis, 2. Aufl. Köln 2009, S. 251 f.

[46] Im Detail: § 26a UStG.

[47] §§ 26b, 26c UStG.

Bereichsleitern. Das Gesetz sieht hierfür in mehreren Fällen die Nichtigkeit des geprüften Jahresabschlusses vor, was insbesondere nach bereits erfolgter Hauptversammlung erhebliche Probleme bereiten dürfte. Die kammerrechtlichen Aufsichtsgremien zeigen verständlicherweise aus Selbstnutz wenig Interesse intensivere Überprüfungen vorzunehmen. Aus diesem Grund sind mehrere Länder (z. B. Italien, Frankreich, Türkei) soweit gegangen, dass Beratungsleistungen bei vorliegendem Prüfungsauftrag nahezu ausgeschlossen sind. Die EU diskutiert mit dem Barnier-Vorschlag ebenfalls ähnliche und sogar weitergehende Ansätze, um sämtliche Aspekte der Befangenheit im Rahmen der Prüfung auszuschließen.

Aus deutscher Sicht sind die Beachtung der §§ 319 und 319a HGB relevant. Danach darf der Wirtschaftsprüfer bei von ihm zu prüfenden Kapitalgesellschaften nicht an der Ermittlung oder Verbuchung von Zahlen mitwirken, die in den Jahresabschluss einfließen. Insoweit sind rechnungslegungsbezogene Beratungsleistungen durch den Wirtschaftsprüfer kritisch zu hinterfragen. Für kapitalmarktorientierte Unternehmen kommen weitergehende Beschränkungen hinzu: So dürfen Rechts- und Steuerberatungsleistungen nur erbracht werden, wenn sich diese nicht auf den zu prüfenden Abschluss unmittelbar auswirken. Dies dürfte aber im Regelfall bereits für die Erstellung von Steuerklärungen oder die Begleitung von Betriebsprüfungen gelten, da diese sich durch Steuernachzahlungen oder Steuererstattungen auf das Jahresergebnis auswirken können und dies im Vorhinein bei Auftragsannahme nur schwerlich ausschließbar sein dürfte[48]. M. a. W. was macht das Unternehmen, wenn es zu einer nicht unwesentlichen Steuernachbuchung für vergangene Jahre kommt: Einen zweiten Berater hinzuziehen, um den rechtlichen Regeln der Compliance zu entsprechen oder einen nichtigen Jahresabschluss riskieren, falls dies einem aufmerksamen oder streitbarem Aktionär bei Rückfragen zu den erbrachten Beratungsleistungen im Anhang des Jahresabschlusses auffällt?

Ebenfalls kritisch zu sehen ist die Beteiligung des Wirtschaftsprüfers oder mit diesem verbundener Unternehmen bei der Einführung oder Modifikation von Systemen, die zur Rechnungslegung gehören. Eine Beteiligung an Einführungen dürfte bereits für die Durchführung von Schulungen gelten[49]. Der Begriff „Rechnungslegungsinformationssystem" geht weiter als ein Buchführungssystem und erfasst damit auch alle Systeme, die Zahlen ermitteln, die in den Jahresabschluss eingehen. So sieht die amerikanische Börsenaufsicht SEC eine Einführungsbegleitung des Wirtschaftsprüfers bei Systemen zur Berechnung von Steuerrückstellungen oder latenten Steuern als unzulässig an.

[48] A. A.: Förschle/Schmidt, in: Beck'scher Bilanzkommentar, 7. Aufl., München 2010, § 319a Rz. 16,. Anm.: Bei den beiden Kommentatoren handelt es sich um Vertreter aus der großen Wirtschaftsprüfungsgesellschaft PWC, die in erheblichem Umfang steuerberatend tätig ist.

[49] Gl. A.: ebd., § 319 Rz. 23.

3.11 Folgen bei Beratungsfehlern, unzureichender Beratung und bei Verlagerung steuerlich relevanter Tätigkeiten an ausländische Konzerneinheiten oder Dritte

Grundsätzlich ist Schuldner von Steuerzahlungen der Steuerpflichtige. Dies gilt auch für Steuernachzahlungen oder gar Steuerhinterziehungen, die aus Beratungsfehlern oder unzureichender Beratung resultieren. Eine Abwälzung der Verantwortung ist regelmäßig nicht möglich. Im Einzelfall besteht die Möglichkeit den Berater in Regress zu nehmen, wobei in zahlreichen Fällen zu beachten ist, dass sich die Beraterhaftung aus dem abgeschlossenen Beratungsvertrag ergibt. Dabei wird insbesondere im Ausland häufig lediglich eine sehr geringe Haftung, z. B. das 2,5-fache des Auftragswerts, vereinbart. Dies kann auch gerade bei Verträgen mit Landesgesellschaften von vermeintlich sehr großen Wirtschaftsprüfungs- oder Steuerberatungsgesellschaften gelten. Von daher sollte jeder Beratungsauftrag unter besonderer Risikoabwägung abgeschlossen und regelmäßig auf ausreichende Haftung überprüft werden. In Einzelfällen kann aus Compliance-Sicht der Abschluss besonders zu versichernder Haftungssummen notwendig sein. Risiken aus Beratungsleistungen können in Einzelfällen, insbesondere bei Steuergestaltungen oder Reorganisationen durch die Einholung von verbindlichen Vorab-Zustimmungen, z. B. in Form einer verbindlichen Auskunft, drastisch reduziert werden. Leider wird hiervon in der Praxis nur beschränkt Gebrauch gemacht. Eine Kosten-Nutzung-Abwägung sollte aber sicherlich bei Verzicht auf eine verbindliche Auskunft erstellt und dokumentiert werden. Gleiches gilt für die Erstellung einer Begründung, warum eine verbindliche Auskunft nicht in Betracht kommt, z. B. wegen fehlender rechtlicher Möglichkeiten. Außerdem ist zu dokumentieren, was veranlasst wurde, um den Mangel auszugleichen oder zu begrenzen.

In den letzten Jahren haben die Unternehmen aus Kostengründen oder Gründen der organisatorischen Optimierung vermehrt Teile der Buchführung oder der Buchführungssysteme ins Ausland verlagert. Insbesondere die konzernweite Einführung von ERP-Systemen, z. B. von SAP oder Oracle, erfordert die Festlegung eines Standorts für den Betrieb der Server, der im In- oder Ausland belegen sein kann. Soweit Teile der Buchführung (z. B. Belegaufbewahrung oder Verbuchung) bzw. der Rechnungslegungssysteme im Ausland betrieben werden, ist vorab eine Zustimmung durch die deutsche Finanzverwaltung erforderlich. Dabei ist darzulegen, wie der Datenzugriff dauerhaft gewährleistet wird. Ferner ist zu beachten, dass die deutschen Aufbewahrungsfristen für steuerlich relevante Unterlagen mit 10 oder mehr Jahren zumeist weit über dem internationalen Durchschnitt liegen. Bei Nichterfüllung drohen neben materiellen Verzögerungsgeldern bis zu 250.000 € auch besondere Risiken bezüglich der Anerkennung der Ordnungsmäßigkeit der Buchführung und damit der Eröffnung von Schätzungsmöglichkeiten durch die deutsche Finanzverwaltung. Deshalb ist es zwingend erforderlich, dass in Verträgen mit konzerninternen Shared Service-Centern oder fremden Outsourcing-Firmen eine Sicherstellung der deutschen Aufbewahrungspflichten vereinbart wird, um alle rechtlichen Pflichten zu erfüllen und empfindliche Sanktionen und Risiken zu vermeiden.

4 Tax Compliance-Organisation und Integration in das Compliance-Managementsystem

Es gibt unterschiedliche Ansätze beim Aufbau von Tax Compliance-Strukturen, in jedem Fall ist eine klare Zuweisung der jeweiligen Verantwortung und Aufgaben erforderlich, ebenso eine eindeutige Regelung zu den Berichtsstrukturen.[50] Je nach dem vom Unternehmen gewählten Aufbau der Compliance Organisation ist Tax Compliance das Arbeitsergebnis verschiedener Abteilungen. Eine allgemeingültig richtige Organisationsstruktur im Zusammenhang mit Tax Compliance gibt es natürlich nicht. Entscheidend ist, dass der gewählte Weg zum Unternehmen und dessen steuerlichen Risiken passt.[51] Das Tax Compliance-System ist an das jeweilige Unternehmen anzupassen. Das System muss maßgeschneidert für das jeweilige Unternehmen angefertigt werden. Die Anforderungen sind insbesondere abhängig von

- der Größe des Unternehmens
- seiner Rechtsform
- seinem Unternehmenszweck
- der Branche
- dem Grad der Konzernierung und
- der internationalen Ausrichtung des Unternehmens.[52]

Wesentlich ist weiter die Aufstellung, Einordnung und Ressourcenzuordnung der (Tax)Compliance-Organisation als Zeichen oder Signal für den Wert von (Tax) Compliance, den das Unternehmen dieser Funktion beimisst. Die Erfahrungen der Unternehmenspraxis zeigen, dass die Compliance-Organisation mit dem glaubwürdigen Bekenntnis der Unternehmensspitze zur Compliance im Unternehmen steht und fällt.[53]

Bestehende Stabsabteilung vs. Compliance-Organisation Compliance Themen können einerseits von bereits bestehenden Stabsabteilungen mit übernommen werden, wie der Rechts-, Personal-, Revisions- und Steuerabteilung. Ebenso denkbar ist aber auch, dass die Compliance-Organisation als eine eigenständige Struktur aufgebaut wird, mit einer eigenen Stabsabteilung für Compliance sowie dezentralen Compliance Abteilungen verankert im operativen Tagesgeschäft, geführt von sog. Compliance-Officern oder Compliance-Beauftragten.[54] Wird der Organisationsweg über die bereits bestehenden Stabsstellen

[50] Vgl. Ehnert, in: Streck/Mack/Schwedhelm. Tax Compliance, Köln 2010, S. 66.

[51] Vgl. ebd.

[52] Kindl/Petsche, in: Althuber, Geschäftsführer und Vorstandshaftung im österreichischen Steuerrecht, 1. Aufl. 2012, S. 168.

[53] Vetter, in: Wecker/van Laak, Compliance in der Unternehmenspraxis, 3. Aufl., Köln 2013, Kap. X.

[54] Vgl. Ehnert, a. a. O., S. 66.

gewählt, bleibt die Tax Compliance originär bei der Steuerabteilung. Hinzu kommt der Abstimmungsaufwand insbesondere mit der Rechtsabteilung und der Internen Revision. Auch für den Fall einer eigenständigen Compliance-Struktur bleibt die Steuerabteilung für alle inhaltlichen Compliance-Themen primärer Ansprechpartner.[55]

Steuerstrategie als Grundlage Eine der Grundlagen für die Tax Compliance-Organisation ist eine – aus der Unternehmensstrategie abgeleitete – Steuerstrategie, die zumindest den Rahmen, die Zielsetzungen, das steuerliche Risikoprofil und die Aufgabenstellungen für die Steuerfunktion[56] vorzugeben hat.

Unternehmensorganisation Die Organisationsform des Unternehmens spielt ebenfalls eine wesentliche Rolle für die Ausgestaltung der Tax Compliance-Organisation. Unterschiedliche Organisationsformen des Unternehmens führen in aller Regel zu einer unterschiedlichen Ausgestaltung der Steuerfunktion und/oder der -abteilung. Diese unterschiedlichen Organisationsformen führen zu unterschiedlichen Risikomanagement- und Kontrollmaßnahmen.[57]

Grundsätzlich kann zwischen folgenden Organisationsgrundformen unterschieden werden:[58]

- Funktionale Organisation (Aufteilung nach Aufgaben und Funktionen)
- Divisionale Organisation (Aufteilung nach Geschäftsfeldern)
- Steuerartenorientierte Organisation (Aufteilung nach Steuerarten)
- Regionale Organisation (zentrale vs. dezentrale Organisation)
- Mischformen

Bei einer dezentral organisierten Managementfunktion gilt es Themen wie die fachliche Expertise der lokalen Kollegen, Weisungs- und Kompetenzabgrenzungen zwischen lokaler und zentraler Compliance-Funktion zu klären.[59]

Bei einer zentralen Tax Compliance-Organisation besteht ein erhöhter bzw. sehr hoher Kommunikations- und Abstimmungsbedarf mit den lokalen Einheiten, vor allem mit Kollegen in ausländischen Tochtergesellschaften. Je weiter weg die Konzernzentrale, desto höher ist die Wahrscheinlichkeit, dass Informationen „verloren“ gehen und notwendige Prozesse nicht oder nicht vollständig abgearbeitet werden.[60]

---

[55] Vgl. ebd., S. 66 f.

[56] Wesentlich ist die Steuerfunktion als Gesamtheit der Funktionsträger zu verstehen, die steuerrelevante Sachverhalte beeinflussen. Daher sind auch externe Berater, der Vorstand und der Aufsichtsrat Teile der Steuerfunktion.

[57] Kromer, Tax Risk Management – Steuerrisiken minimieren, Management Circle, Eschborn, 2010/2011.

[58] Ebd.

[59] Ebd.

[60] Ebd.

Tax Compliance Kultur Neben vielen einzelnen organisatorischen Maßnahmen, die ein effizientes Tax Compliance-Management voraussetzt, ist eine Compliance-Kultur erforderlich, die im Unternehmen breit verankert ist und sowohl von der Geschäftsleitung als auch den Mitarbeitern tatsächlich gelebt wird.[61] Es ist empfehlenswert, dass die Unternehmensleitung klärt, ob Steuern lediglich als Kostenfaktor oder als gesellschaftliche Verpflichtung aufgefasst werden.[62]

Tax-Compliance-Regeln (Tax Operating Manual) Ein in sich kohärentes und funktionierendes Compliance-System setzt voraus, dass für die betroffenen Bereiche eindeutige Richtlinien und transparente Strukturen bestehen. Sowohl die Verantwortlichkeiten als auch die Prozesse müssen aufeinander abgestimmt sein und sich nahtlos in einander fügen.[63] Zentraler Baustein einer Compliance-Organisation sind Richtlinien, die den Mitarbeitern verbindlich klare Regeln und Prozesse aufzeigen. Dazu zählen beispielsweise Checklisten, Fristenlisten, Verhaltensanweisungen, Dokumentationserfordernisse und Zuständigkeitsregeln.[64] Folgende Einzelrichtlinien können Teil eines Tax Operating Manual sein:[65]

- Richtlinie Informationsbedarf
- Richtlinie Steuerberechnung und Steuererklärung
- Fristenrichtlinie
- Richtlinie Tax-Risk-Management
- Richtlinie zur steuerlichen Verteidigung
- Berichtslinie

Um die Weitergabe der internen und externen Informationen zu gewährleisten, bedarf es einer unternehmensweiten, abteilungsübergreifenden Bündelung und Aktualisierung des Informationsmaterials sowie dessen permanenter Verfügbarkeit, damit keine für die Steuererhebung relevanten Informationen verloren gehen.[66]

Dokumentation Die Dokumentation und Beschreibung der Prozesse und Kontrollen ist Voraussetzung für die konsistente Anwendung als auch für die dauerhafte Beachtung sowie für die personenunabhängige Funktion eines Tax-Compliance-Systems.

---

[61] Vetter, in: Wecker/van Laak, Compliance in der Unternehmenspraxis, 3. Aufl., Köln 2013, Kap. X.

[62] Spengel/Matenaer, Tax Risk Management – Strategische, prozessuale und organisationale Einflussfaktoren, Ubg 10/2011, S. 803.

[63] Besch/Starck, a. a. O., § 34. Tax Compliance, Rz. 61.

[64] Kindl/Petsche, a. a. O., S. 165.

[65] Siehe im Detail Besch/Starck, a. a. O., § 34. Tax Compliance, Rz. 64 ff.

[66] Kindl/Petsche, a. a. O., S. 173.

Ressourcenausstattung der Steuerfunktion (Steuer-ERP-System) Die Ressourcenausstattung der Steuerfunktion bestimmt in einem hohen Ausmaß die Ausgestaltung des Tax-Compliance-Systems. Je höher das Ausmaß an internen und externen Ressourcen (externe Berater als „Sparringspartner", Second Opinion bei komplexen Steuersachverhalten) und je besser ausgebildet die Mitarbeiter der Steuerfunktion sind, desto geringer ist die Wahrscheinlichkeit, dass die Vorgaben des Tax-Compliance-Systems nicht erfüllt werden.

Die Erfassung sowie die Bewertung von steuerlichen Sachverhalten auf diversen Ebenen und Gesellschaften in einem Konzern werden mittels Excel-Tabellenkalkulation nicht mehr möglich sein. Es wird daher in der Praxis immer häufiger zur Optimierung der Bewirtschaftung der Steuerrisiken und anderer Tax Compliance Sachverhalte ein Steuer-ERP-System eingeführt.[67]

Klare Definition der Verantwortung Tax Compliance-Management ist eine der wesentlichen Herausforderungen für die Verantwortungsträger. Je nach Ausgestaltung der Organisationsstruktur ist entweder der Steuerchef oder ein Compliance-Officer unmittelbar für Tax-Compliance verantwortlich. In der Regel ist der Leiter der Steuerabteilung oder eine sonstige fachlich qualifizierte Person für Tax Compliance verantwortlich. Für den Fall, dass ein Compliance-Beauftragter oder Compliance-Officer installiert ist, muss dessen Zuständigkeit auch Tax Compliance umfassen, jedenfalls könnte er insoweit in die Tax Compliance eingebunden werden, als es um organisatorisches Themen geht;[68]. Es gilt daher zu klären wer für die inhaltliche Ausgestaltung des Tax Compliance-Managements verantwortlich ist. Dem Selbstverständnis der Steuerabteilung wird es eher entsprechen, wenn Tax Compliance als etwas Eigenständiges betrachtet wird und daher in der Steuerabteilung inkorporiert bleibt oder wird.[69] Ist hingegen das Thema Tax Compliance Teil der Zuständigkeit der allgemeinen Compliance-Implementierung und.-pflege, wird es zu einem Spannungsverhältnis zwischen Compliance- und Steuerabteilung kommen.[70]Die Stakeholder und insbesondere die externen Steuerberater sind von den Tax-Compliance-Maßnahmen in Kenntnis zu setzen, damit die Tax-Compliance Strategie einen dynamischen Rahmen für das Tax-Compliance Management bildet.

In eine Tax-Compliance-Struktur müssen auch andere Personen und Abteilungnen eingebunden werden. Mitarbeiter aus anderen Abteilungen sind für die vollständige Erfassung steuerrelevanter Informationen mitverantwortlich, weil in ihren Abteilungen die internen – für steuerliche Zwecke erforderlichen – Informationen generiert werden. Diese Informationen sind zeitnah an die entsprechende Mitarbeiter weiterzuleiten und

[67] Vgl. Pratter/Eichenberger Tax Risk Management im Konzern, Der Schweizer Treuhänder, 2012/5 S. 382.

[68] Kindl/Petsche, in: Althuber, Geschäftsführer und Vorstandshaftung im österreichischen Steuerrecht, S. 173.

[69] Vgl. Streck, in: Streck/Mack/Schwedhelm. Tax Compliance, S. 58.

[70] Vgl. ebd.

von diesen systematisch aufzubereiten, abzustimmen, zu kommunizieren und zu archivieren.[71] Nur im Zusammenwirken mit anderen Funktionsträgern wie den operativen Geschäftseinheiten und/oder der internen Revision kann sichergestellt werden, dass Compliance-Aufgaben tatsächlich erfüllt werden.[72]

5 Umfang und Umsetzung eines Tax Compliance-Managementsystems

5.1 Umfang

Im vorhergehenden Abschnitt wurde bereits darauf hingewiesen, dass der Umfang eines Tax Compliance-Managementsystems sich nach zahlreichen Faktoren richtet. Letztlich muss sich das Tax Compliance-Managementsystem nach der jeweiligen Konzernstruktur und dessen Risikoprofil einschließlich zu beachtender nationaler Unterschiede ausrichten. So wird die Überwachung steuerlicher Prozesse bei einem rein national agierenden Unternehmen z. B. der Bekleidungsbranche, weit weniger umfangreich sein als bei einem internationalen Sportbekleidungshersteller mit tiefer und grenzüberschreitender Wertschöpfungskette. Grundlegend ist aber in beiden Fällen eine ausformulierte und von der Konzernleitung verabschiedete Steuerstrategie. Außerdem fließt die Unternehmensorganisation in den Umfang der zu überwachenden Tätigkeiten und Prozesse mit ein. Wichtig ist auch das Bewusstsein auf Ebene der Unternehmensleitung und Aufsichtsgremien, dass es sich nicht um eine Pflichtübung sondern um einen Kernprozess handelt.

Als Adressaten und Beteiligte (Stakeholder) einer Tax Compliance-Organisation kommen primär in Betracht:

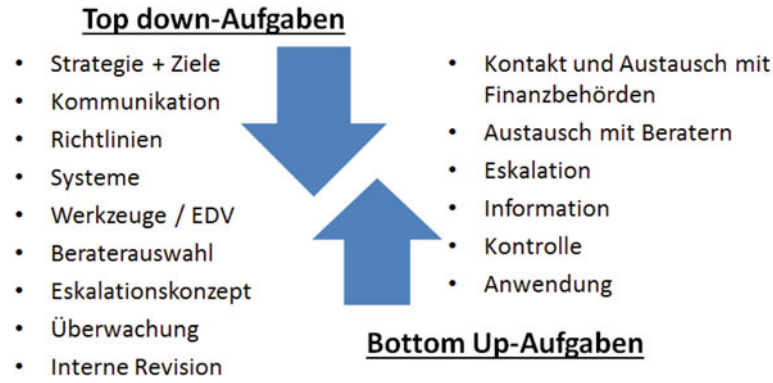
- Unternehmensleitung
- Aufsichtsrat
- Alle Mitarbeiter
- Wirtschaftsprüfer
- Externe Berater
- Steuer- und Zollverwaltungen
- Gesellschafter und Aktionäre
- Geldgeber, Lieferanten, Kunden und Analysten
- Öffentlichkeit

Die Umsetzung einer Tax Compliance-konformen Unternehmensorganisation konzentriert sich auf die in der folgenden Abbildung dargestellten Kernaufgaben. Grundsätzlich

[71] Ebd.

[72] Vgl. Pumpler, in: Zöchling, Tax Controlling in der Praxis, 1. Aufl. 2012, S. 71 f.

kann dabei zwischen einem Top down-Vorgehen und einem Bottom up-Vorgehen unterschieden werden. Für die Umsetzung einer Tax Compliance-Organisation kommt es auf beide Richtungen an:



5.2 Steuerstrategie und Festlegung von Zielen

Die Steuerstrategie ist ein Bestandteil der Unternehmensstrategie und wesentlicher Baustein eines Tax Control Frameworks, zu dem auch die Tax Compliance-Überwachung gehört. Verantwortlich für die Steuerstrategie ist die Unternehmens- oder Konzerngeschäftsleitung.

Die Steuerstrategie richtet sich sowohl an interne als auch an externe Adressaten (Stakeholder). Als interne Adressaten sind alle Mitarbeiter und der Aufsichtsrat anzusehen. Externe Adressaten sind Finanzverwaltungen, Wirtschaftsprüfer, Steuerberater, Aktionäre, Analysten, Presse und Kunden.

Quantitative und qualitative strategische Ziele für den Bereich „Tax" sind zu bezeichnen und ggf. zu beschreiben. Solche Ziele müssen auf die Unternehmensziele abgestimmt sein.

Quantitative Zielsetzungen für den Bereich „Tax" können z. B. in der Minimierung des steuerlichen Cash Flow liegen, wenn Cash Flow-Steuerung als Unternehmensziel gesetzt ist. Sind daneben Earnings per Share als Ziel gesetzt, so besteht die steuerliche Zielsetzung in der Maximierung der Nachsteuerrendite und des Unternehmenswerts durch Optimierung von Ertragsteuern im Einklang mit der Risikoneigung des Unternehmens oder Konzerns. Wird des Weiteren die Steigerung des Nachsteuerergebnisses oder Jahresüberschusses als Unternehmensziel verfolgt, so kommt der Steuerung der Effective Tax Rate (Konzernsteuerquote) und der darauf einwirkenden nicht-steuerlichen Einflussfaktoren eine besondere Bedeutung zu. Mit Blick auf die Erfüllung aller Rechtspflichten in quantitativer Hinsicht ist die Vermeidung von steuerlichen Nebenleistungen, Zuschlägen oder Schätzungen von Steuern verbunden.

Qualitative Ziele liegen daneben in der Erfüllung aller Rechtspflichten, der Effizienz der Steuerfunktion und zuzuordnender Beratungskosten, dem zeitgemäßen Einsatz von Technologie, der Vernetzung mit operativen Einheiten, der frühzeitigen Erfassung und Vermeidung bzw. Begrenzung steuerlicher Risiken, der Transparenz z. B. durch die Qualität und Nachvollziehbarkeit der Berichterstattung sowie der internen und externen Kommunikation[73]. Auch hierfür können (jährlich) überprüfbare Wertmaßstäbe angesetzt werden.

Bezüglich der Risikoneigung und deren Begrenzung können scharfe Grenzen gesetzt werden, wonach steuerliche Risiken z. B. maximal bestimmte Grenzen des Eigenkapitals, des Gesamtkapitals oder bestimmte Wertgrößen in Summe nicht übersteigen dürfen. Dies kann sowohl auf Konzernebene als auch auf Landes- oder Gesellschaftsebene bezogen werden. Solche Grenzen sind aufgrund der geltenden Vorschriften bei kapitalmarktorientierten Unternehmen und uneingeschränkt bei Finanzdienstleistern festzulegen und mit dem unternehmensweiten Risikomanagement abzustimmen.

Weitere wichtige Inhalte einer Steuerstrategie sind die Festlegung und Abgrenzung von Verantwortlichkeiten, insbesondere zwischen (Konzern-) Steuerabteilung, Bereichs- und Spartenleitungen, etc. sowie die Festlegung von Berichts- oder Informationspflichten. Hierzu gehört auch: Wer bearbeitet welche Prozesse und berichtet darüber an wen? Wer hat die Verantwortung für Anweisungen und Qualitätssicherung? Wer ist für die Ergebnisse verantwortlich?

Dabei lassen sich die Berichtslinien aufgabenbezogen folgendermaßen unterteilen:

Top down

- Konzernleitung
- Spartenleitung
- Bereichsleitung
- Steuerabteilung
- Compliance-Abteilung
- Einkauf
- Interne Revision

Bottom up

- Alle Mitarbeiter
- Im Besonderen:
  - Steuerabteilung
  - Rechnungswesen
  - HR/Personal
  - Vertrieb
  - Export/Import
  - IT
  - Externe Berater

[73] Pressenachrichten, wonach Apple und Amazon weltweit praktisch keine Steuern zahlen, sind aus Compliance-Sicht kontraproduktiv, da damit die Aufmerksamkeit der Finanzverwaltungen geweckt wird und auch in der Öffentlichkeit bei (potentiellen) Kunden der Eindruck erweckt wird, dass man keinen „Fair share" leistet. Insbesondere öffentliche Auftraggeber schließen solche Unternehmen dann bei Ausschreibungen eher aus. Kommen dann solche Meldungen auf, sollte man darauf vorbereitet sein und entsprechend nachvollziehbare Antworten parat haben.

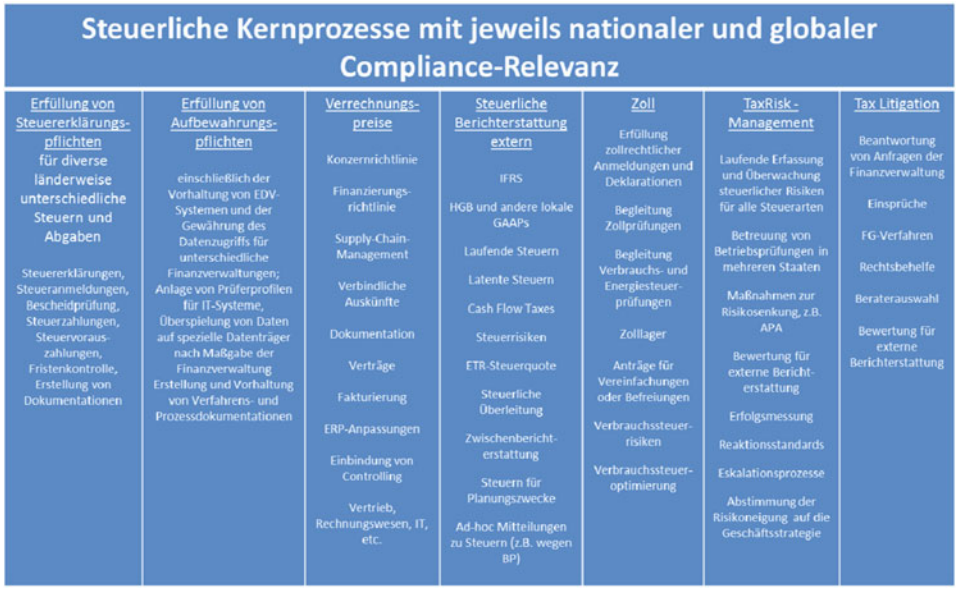
5.3 Kernprozesse der Tax Compliance und Bedeutung der Personalausstattung

Bei geringer Personalausstattung der Steuerabteilung besteht die Gefahr, dass die Erledigung der Pflichtprozesse, wie die Abgabe von Steuererklärungen, das Erfassen und Reduzieren von Risiken oder steuerlichen Ineffizienzen überlagert. Außerdem werden aus Zeitmangel u. U. Möglichkeiten der Steuerersparnis oder sinnvollen Steuergestaltung nicht oder nicht in gebotenem Maß genutzt. Letztlich muss der Konzernleitung und den Aufsichtsgremien jederzeit bewusst sein, dass die Arbeit nahezu aller Mitarbeiter der Unternehmensgruppe und die Verfügungsmöglichkeit über große Kapitalmittel zu einem Unternehmenserfolg oder Verlust führt, der erst nach Belastung mit Ertragsteuern zur Ausschüttung oder für Reinvestitionen in Wachstum genutzt werden kann. Es erstaunt insoweit immer wieder, dass je nach Besteuerungsquote für 50 bis 75 % des Unternehmenserfolgs oder Jahresüberschusses fast 100 % der Mitarbeiter und des Vorstands zuständig sind, während für 25 bis 50 % des Konzernerfolgs gerade mal 0 % bis maximal knapp 0,5 % der Mitarbeiter im Regelfall zuständig sind. Wenig beachtet wird auch häufig die Bedeutung der Steuerzahlungen für den Cash Flow: So stellen Steuerzahlungen im Regelfall eine der fünf größten Cash Flow-Positionen dar. Besonders materiell sind dabei die in der Bilanz und GuV im Hintergrund stehenden Umsatz- und Lohnsteuern[74]. Die verhältnismäßig kleine Gruppe der Steuerspezialisten ist daneben in internationalen oder großen Unternehmensgruppen, z. T. gemeinsam mit externen Beratern, zumeist für mehrere Tausend zu überwachende sowie zu bearbeitende Einzelvorgänge zuständig. Als Beispiel sei die Umsatzsteuer genannt. So sind bei 10 Gesellschaften für monatliche Voranmeldungen, Dauerfristverlängerungen, Umsatzsteuer-Erklärungen, Berichtigungen von Voranmeldungen oder Erklärungen im üblichen Rahmen, Zusammenfassenden Meldungen und Vergütungsanträge in 2–3 Ländern im Ausland ca. 220 Einreichungen und Zahlungsvorgänge in erheblicher Zahl anzustoßen bzw. zu überwachen. Dabei ist zu beachten, dass die Erklärungs- und Voranmeldungssystematik in den einzelnen Staaten stark voneinander abweicht. Dies gilt auch für die Strafen bei verspäteter Abgabe oder Zahlung. Ferner sind neben den in nahezu allen Staaten anzutreffenden Körperschaft- und Umsatzsteuern zahlreiche lokale Steuern (z. B. Gewerbesteuer), Verkehrs- und Substanzsteuern zu deklarieren und zu überwachen. Aufgrund der vorgenannten Befunde verwundert es in der Praxis, dass die Leistungen aber auch möglicherweise die Fehlleistungen von Steuerabteilungen häufig nicht erfasst und überwacht werden. Insoweit ist ein unbeachtetes Auftreten von Ineffizienzen oder Mehrsteuern bei fehlender Compliance-konformer Überwachung nicht auszuschließen.

---

[74] Vgl. zum Cash Tax-Management und zur Effizienz von Steuerabteilungen: Kromer/Walker, Strategisches Steuermanagement in Krisenzeiten in: Weber/Vater/Schmidt/Reinhard (Hrsg.)-Turnaround-Navigation in stürmischen Zeiten, Weinheim 2011, S. 739–755; Kromer/Walker, B.2.4. Steuern, in: Vater/Reinhard (Hrsg.) – Praxishandbuch Kostensenkungspläne, Weinheim 2012, S. 391–411.

Als Kernprozesse einer Tax Compliance-Überwachung sind zu nennen:



Wesentliche Faktoren für die Beurteilung der Qualität von Compliance-relevanten Prozessen sind Transparenz, Dokumentation, Unabhängigkeit von Einzelpersonen, Fristenkontrolle, Zugang und Aufbewahrung von Dokumenten und Daten sowie Vermeidung von Strafen, Zuschlägen oder Nebenleistungen. Je nach Unternehmens- oder Konzerngröße und der Anzahl, Häufigkeit sowie Komplexität der zu überwachenden Einzelprozesse ergibt sich auch die Anzahl der hierfür einzusetzenden Mitarbeiter und Aufwendungen. Die entsprechende Personalbedarfsermittlung im Verhältnis zu den anstehenden Aufgaben sollte dem Compliance Officer vorgelegt werden.

Es liegt auf der Hand, dass die großen Mengen von steuerlich relevanten Prozessen, Aufbewahrungspflichten und Informationen nur noch unter weitgehendem Einsatz qualifizierter State of the Art-Softwarelösungen risikosenkend und insbesondere Compliance-konform betrieben und gelöst werden können. Hierzu bedarf es in der Praxis strukturierter und jederzeit nachvollziehbarer Auswahlprozesse, die zunächst mit auf das konkrete Unternehmen abgestimmten Bedarfsanalysen beginnen müssen, da Fehlentscheidungen neben Erhöhung der Risiken erhebliche Kosten und Ressourcenbindung, abgesehen von Verstößen gegen IT-Compliance-Vorschriften, auslösen können.

Unabhängig davon sind Vorgaben und Sicherheitsvorschriften aus steuerlicher Sicht in konzernweite Richtlinien zur Anschaffung sowie Verwendung von IT und Software aufzunehmen, um Verstöße gegen steuerliche IT-Compliance-Standards der Finanzverwaltungen zu vermeiden.

5.4 Steuerliches Risikomanagement- und internes Kontrollsystem[75]

Für die vorstehend bezeichneten Kernprozesse ist die Einrichtung eines internen Risikomanagement- und Kontrollsystems (RMS/IKS) erforderlich. Grundsätzlich ist das RMS/IKS für Tax Compliance in ein weitergehendes steuerliches RMS/IKS zu integrieren.

Ein umfassendes steuerliches Risikomanagement umfasst grundsätzlich 5 Stufen:

- Festlegung von Sachverhalten und Prozessen mit Compliance- und Rechnungslegungswirkung
- Zuordnung von quantitativen und qualitativen Risiken zu Sachverhalten
- Maßnahmen und Tools zur Risikofrüherkennung
- Maßnahmen und Tools zum Risikomanagement
- Festlegung interner Kontrollen
- Festlegung interner Revisionskriterien.

Daneben ist festzulegen, ob ein Bottom Up-Ansatz oder ein Top Down-Ansatz für die Risikoaufnahme und Umsetzung verfolgt wird. Aus Vollständigkeitsgründen empfiehlt sich der Bottom Up-Ansatz, bei dem vom individuellen Sachverhalt ausgegangen wird. Geht man beispielsweise vom Tax Compliance- und rechnungslegungsrelevanten Sachverhalt „Umsatzsteuer-Voranmeldung" aus, kann man diesem sowohl finanzielle und bilanzielle Risiken (Verspätungszuschläge, unberechtigte Vorsteuerabzüge, fehlende Dokumentation oder Belege, fehlerhafte Ermittlung) als auch Reputationsrisiken und persönliche Organhaftung zuordnen. Maßnahmen der Risikofrüherkennung müssen sich auf rechtzeitige Fristmeldung und Zahlung, ungeregelte Zuständigkeit, Krankheit von Sachbearbeitern und unvollständige Dokumentation beziehen. Als Maßnahmen des Risikomanagements sind die klare Zuordnung der Zuständigkeit und Vertretung, die Einrichtung im Finanzbuchhaltungssystem mit Abnahme und Plausibilisierung sowie die Prüfung der Mitarbeiterqualifikation umzusetzen. Die Festlegung interner Kontrollen bezieht sich auf eine wirksame Fristenkontrolle, die Anwendung des 4-Augen-Prinzips und technische Plausibilisierung. Schließlich können als interne Revisionsmaßnahmen eine ERP-Systemverprobung, eine Ablaufprozesskontrolle und eine Prüfung mit der von den Finanzverwaltungen in Deutschland und Österreich eingesetzten Prüfsoftware IDEA oder ACL vorgeschlagen werden.

Insgesamt muss ein weltweites internes Risikomanagement- und Kontrollsystem für den Bereich Steuern (und analog Zoll) aus Compliance-Sicht die folgenden Bereiche abdecken:

---

[75] Kromer/Walker, Strategisches Steuermanagement in Krisenzeiten in: Weber/Vater/Schmidt/Reinhard (Hrsg.)- Turnaround-Navigation in stürmischen Zeiten, Weinheim 2011, S. 753 ff; Kromer/Walker, B.2.4. Steuern, in: Vater/Reinhard (Hrsg.) – Praxishandbuch Kostensenkungspläne, Weinheim 2012, S. 408 f.; Ausführlich: Kromer, Christoph, Germany, in: Corporate Tax Risk Management, IBFD Amsterdam 2010, Chapter 9.

1. Externe Berichterstattung im Jahresabschluss zu laufenden und latenten Ertragsteuern
2. Externe Zwischenberichterstattung und Steuerliches Forecasting
3. Laufende weltweite Steuerplanung für Zwecke der Dokumentation zur Verrechnung von Verlustvorträgen bei Ertragsteuern, für Zwecke der Steuerplanung zur Steueroptimierung bei materiellen Steuerarten, für das Liquiditätsmanagement (Cash Tax Planning) zu allen materiellen Steuern und zur Risikobegrenzung z. B. bei Zinsschranke und Änderungen der Unternehmensplanung
4. Erfassung, Gegenstand und Bewertung steuerlicher Risiken für alle Steuerarten
5. Erfassung aller steuerlichen Restriktionen mit Fristigkeit und Auswirkung, z. B. zur Aufdeckung stiller Reserven
6. Stand, Gegenstand und Bewertung aller offenen Rechtsbehelfe, Einwendungen von Finanzverwaltungen und Gerichtsverfahren
7. Stand und Fristüberwachung von Steuererklärungen und -veranlagungen für alle Steuerarten
8. Stand und Überwachung der Erfüllung von Aufbewahrungspflichten für alle offenen Veranlagungszeiträume für alle Steuerarten und Zolldeklarationen
9. Verrechnungspreismanagement und -dokumentation
10. Cash Tax Management
11. Steuerberatungskosten differenziert nach Steuerveranlagungs- und Steuerberatungstätigkeiten
12. Konsistenz mit anwendbaren Compliance- und Aufbewahrungsvorschriften – auch ggf. rein steuerlicher und zollrechtlicher Natur – in den Ansässigkeitsstaaten der Unternehmensgruppe und den konzernweiten Corporate Governance-Standards.

Auch zum steuerlichen Risikomanagement gilt, dass technische Lösungen die Umsetzung unterstützen und erheblich beschleunigen können. Als Vorteile global einsetzbarer Web-Lösungen mit dezentralem Benutzerzugang sind die Unabhängigkeit von einzelnen Individuen, zentrale Verfügbarkeit, die Überwachung aller Steuerarten, Transparenz, Dokumentation von Risiken und Kontrollen, Erleichterung interner und externer Prüfungen sowie erfahrungsgemäß auch Kostensenkungen durch Verringerung interner Rückfrage- und Abstimmprozesse zu nennen.

5.5 Kommunikation und Berichtswesen

Die Kommunikation steuerlicher Aufgabenstellungen, deren Implementierung und Überwachung sowie das steuerliche Berichtswesen liegen sinnvollerweise in der Verantwortung des Leiters Steuern. Dabei bedient er sich der Unterstützung aus der Unternehmensleitung für die Strategiefestlegung und den Rollout, der Internen Revision für die Überprüfung der zutreffenden Anwendung und des Compliance-Officer zur Abstimmung und für das Berichtswesen.

Die Anwendung aller Steuervorschriften mit Bedeutung für die Unternehmensgruppe ist dabei – wie bereits in vorherigen Abschnitten aufgeführt- durch Richtlinien mit Ver-

fahrensvorschriften als Kommunikation und soweit sinnvoll möglich durch Werkzeuge oder EDV-Lösungen für die tägliche Praxis umzusetzen. Dabei ist darauf zu achten, dass alle Mitarbeiter – zumindest alle potentiell Betroffenen – Zugriff auf die Richtlinien erhalten. Des Weiteren sollte in regelmäßigen Abständen oder bei relevanten Personalwechseln durch Stichproben überprüft werden, ob die Richtlinien und deren Standort bekannt sind. Hiermit wird auch die Einarbeitung bei Personalwechseln deutlich erleichtert und dadurch ansonsten möglicherweise auftretende Risiken vermieden.

Als Schnittstelle zwischen den Bereichen und Zuständigkeiten ist daneben von der Steuerabteilung ein Berichtswesen einzurichten, das aus den *laufenden Prozessen* heraus wichtige Informationen erfasst und an die verschiedenen Stakeholder übermittelt. Dabei sollte das Berichtswesen in übersichtliche und kurz gehaltene Zusammenfassungen für die Unternehmensleitung und entsprechende Adressaten münden, um so die z. B. nach MaRisk und Corporate Governance-Regeln erforderlichen Nachweise über ein laufendes Überwachungssystem zu erbringen:

Im Einzelnen sollten die wesentlichen Gliederungspunkte (Facts, Risks, Compliance, Opportunities) mindestens Aufschluss geben über:

1. Facts: Entwicklung wichtiger Kennzahlen auf Basis sinnvoller Vergleichszeiträume entsprechend anderer interner Reportings, z. B. Cash Taxes für alle materiellen Steuerarten einschließlich erwarteter Erstattungen, Steuerquote, latenter Steuern, GuV- und Rückstellungsentwicklung, Steuerplanung etc.
2. Risks: Entwicklung und Bewertung steuerlicher Risiken zwischen 2 Vergleichsstichtagen, Skizzierung wesentlicher Risiken, Beschreibung eingeleiteter Maßnahmen zur Reduktion, Informationen zum Stand von Betriebsprüfungen, Einfluss auf die externe Berichterstattung und den Cash Flow, Bewertung nach Maximalrisiko einschl. Zinsen etc.– und bei wahrscheinlichem Eintritt – Umkehreffekten, mögliche strafrechtliche Risiken oder Risiken aus persönlicher Haftung für Mitarbeiter oder Unternehmensleitung.[76]

[76] Berichtsvorschläge: Kromer, Unternehmensrisiken aus steuerlichen Sachverhalten, S. 23 ff., Seminar Tax Risk Management, Management Circle, Eschborn 2010/2011; Bakker/Kloosterhof (Hrsg.), Tax Risk Management, IBFD Amsterdam 2010, S. 54.

3. Compliance: Stand offener und abgegebener Erklärungen, anstehender Zahlungen, Dokumentationen, Umsetzungsbedarfe mit ggf. Aufwandsschätzung, Schwächen, Revisionsergebnisse.
4. Opportunities: Übersicht über Möglichkeiten zur Steueroptimierung mit entsprechender Berechnung einzusparender Steuern vs. Implementierungsaufwand und Risikobewertung.

6 Überwachung und Effizienzmessung

Tax Compliance-Management erfordert nicht nur die Etablierung von Informations- und Kontrollstandards, sondern auch deren unternehmensinterne Überwachung und Überprüfung.

Compliance-Management und -überwachung Allgemein umfasst das Management die systematische Erfassung und Bewertung von sowie die Steuerung von Reaktionen auf festgestellte Compliance-Themen bzw. Risiken. Hierbei ist der erste prozessuale Schritt die Identifikation und die Analyse der Themen und Risiken. Darüber hinaus beinhaltet Risikomanagement auch die Risikosteuerung, die wiederum die Risikovermeidung, -verminderung, -begrenzung, -überwälzung und -akzeptanz zum Gegenstand hat. Nach der Erfassung und der Steuerung der Risiken folgt als letzter Schritt idealtypisch für den Risikomanagementprozess die Kontrolle, die auch als Risiko-Monitoring bezeichnet wird.[77]

Eine laufende Risikoanalyse ist ein zentraler Bestandteil eines Tax Compliance-Systems und erfolgt regelmäßig als erster Schritt bei der Implementierung von Compliance-Systemen. Man könnte es als Due Diligence im eigenen Unternehmen bezeichnen. Wichtig ist jedoch, dass die Risikoanalyse laufend erfolgt und ständig fortentwickelt wird. Die laufende Risikoanalyse soll Steuerrisiken systematisch erfassen und bewerten sowie auf festgestellte Risiken reagieren. Entscheidend für den Erfolg eines jeden Tax Compliance-Systems ist die Identifizierung und Bewertung der individuellen steuerlichen Risiken eines Unternehmens. Das setzt voraus, dass innerhalb eines Unternehmens Prozesse eingeführt werden, die eine zeitnahe Erfassung der für die Bestandsaufnahme notwendigen Informationen ermöglichen. Materialien für eine Risikoanalyse liefern u. a. Tax Reviews, Tax Due Diligences sowie die Feststellungen steuerlicher Außenprüfungen der Vorjahre.[78]

Fokussierung auf kritische Sachverhalte Das Herausfiltern besonderer Sachverhalte dient jedenfalls der Kontrolle von Tax-Compliance Systemen. Es sind daher für eine schwer-

[77] Wolke, Risikomanagement, 2. Aufl. 2008 S. 4 f.

[78] Besch/Starck, a. a. O. § 34. Tax Compliance, Rz. 49.

punktmäßige Risikobearbeitung unternehmensspezifisch problematische Geschäftsvorfälle herauszufiltern.[79]

Internes Kontrollsystem Neben dem Risikomanagement dient das interne Kontrollsystem als Maßnahme zur Einhaltung gesetzlicher und unternehmensinterner Vorgaben sowie zur Abwehr von Schäden. Ein internes Kontrollsystem umfasst neben Weisungen auch Aktivitäten – wie beispielsweise Zutrittskontrollen – sowie Maßnahmen zum Schutz der materiellen und immateriellen Vermögenswerte. Folgende Prinzipien bilden die Grundlage eines internen Kontrollsystems: Prinzip der Transparenz, Prinzip der vier Augen, Prinzip der Funktionstrennung sowie das Prinzip der Mindestinformation. Das interne Kontrollsystem befasst sich also primär mit der prozessabhängigen Kontrolle und betrifft sowohl die Aufbau- und Ablauforganisation als auch Prozesse zur Risikosteuerung und zum Risikocontrolling. Demgegenüber ist die interne Revision insbesondere für die prozessunabhängige Prüfung und Beurteilung der Angemessenheit des internen Kontrollsystems verantwortlich.[80]

Interne Revision Die interne Revision soll in erster Linie die Unternehmensleitung in ihrer Kontrollfunktion im Rahmen der Steuerungsaufgabe unterstützen und folgende Funktionen erfüllen: Vertrauensfunktion, Präventivfunktion, und Informationsfunktion. Allgemein formuliert kommt der internen Revision die Aufgabe zu, Unternehmensvorgänge auf ihre Ordnungsmäßigkeit zu prüfen und Unwirtschaftlichkeit, Unregelmäßigkeiten oder Manipulationen aufzudecken.[81]

Andere Maßnahmen Zur Segmentierung des Unternehmens in verschiedene Vertraulichkeitsbereiche werden im Rahmen von Compliance-Maßnahmen sogenannte **Chinese Walls** eingerichtet. Als **Wall-Crossing** wird das Verfahren der Informationsweitergabe über eine Chinese Wall hinweg bezeichnet. Die **Watch-List** ist eine streng vertrauliche Liste, die alle Compliance-relevanten Informationen beinhaltet. **Whistleblowing und Whistleblowing-Hotlines** stellen weitere Compliance-Maßnahmen dar. Whistleblowing ist die (anonyme) Meldung eines Verstoßes gegen unternehmensinterne Verhaltensregeln oder gesetzliche Bestimmungen im Unternehmen. Das **Mission Statement** dient der ausdrücklichen Bekenntnis der Unternehmensführung zu den zuvor formulierten Zielen und den Strategien zur Erreichung dieser Ziele. Nach innen verdeutlicht die Unternehmensführung die Ernsthaftigkeit von Compliance-Programmen und den damit verbundenen Vorgaben bei gleichzeitiger Kommunikation der Compliance nach außen. Der **Code of Conduct** enthält unternehmensinterne Richtlinien, welche die rechtlichen Anforderungen an das Unternehmen und seine Mitarbeiter darstellen. Darüber hinaus wird insbesondere

[79] Ehlers, Tax Compliance, NWB Nr. 18 (2012) S. 1537.

[80] Petsche, in: Petsche/Mair, Handbuch Compliance, 1. Auflage 2010, S. 8 f.

[81] A. a. O., S. 9.

den Mitarbeitern verdeutlicht bzw. signalisiert, welches Verhalten in speziellen Situationen von ihnen erwartet wird. Neben Erklärungen zum rechtlich geforderten Verhalten sind darin auch Erklärungen zum Unternehmens- und Verfahrensablauf enthalten.[82]

Bei größeren Organisationen ist auch eine regelmäßige Tax Compliance-Berichterstattung durch den zuständigen Abteilungsleiter für Steuern vorzusehen. Dieser hat über allfällige Compliance-Verstöße, Meldungen durch Mitarbeiter, Anfragen von Mitarbeitern, Verbesserungs- und Überarbeitungsvorschläge und Erfolge durch die Tax Compliance zu berichten.[83]

Plausibilitätsprüfungen mithilfe EDV-gestützter Software Das frühzeitige Erkennen von Fehlerquellen hilft, Risiken zu vermeiden oder zumindest gut vorbereitet zu sein auf Auseinandersetzungen mit der Finanzverwaltung. Die heutigen Datenmengen und qualitativen Ansprüche übersteigen zunehmend die Möglichkeit einer manuellen Prüfung. Ziel der EDV-gestützten Plausibilitätsprüfungen ist es darum, Massendaten zielgerichtet auf Warnsignale zu filtern und zu analysieren.[84]

Auswahl und Ausbildung der Mitarbeiter Die Auswahl geeigneter Mitarbeiter und umfassende Einschulungen, Trainings und klare Kommunikationsstrukturen sind wesentliche Bausteine eines Überwachungs- und Kontrollsystems.

Fehlermanagement Ein heikles Thema im Zusammenhang mit Compliance ist das Verhalten beim Auftreten von Fehlern (Fehlermanagement). Mitarbeitern muss ein offener und transparenter Umgang mit Fehlern zugestanden werden. Mitarbeiter sind zu ermutigen, allfällige Probleme oder Fehler ehestmöglich zu melden, um rasch reagieren zu können, Schadensminimierung zu betreiben und allfällige schwerwiegendere Konsequenzen zu vermeiden.[85]

Abhängig von der Compliance-Struktur ist die Einbeziehung des Compliance-Officers bzw. der Compliance-Struktur für den Leiter Steuern als Verantwortlicher für Tax Compliance auch für die Effizienzmessung des Tax Compliance-Systems zielführend und zweckmäßig. Die Anwendung von Unternehmensstandards im Bereich der Compliance-Dokumentation stellt die wesentliche Grundlage für die Effizienzmessung dar. Damit ist gewährleistet, dass die unternehmensweiten Standards auch für den Steuerprozess gelten. Die Effizienzmessung eines Tax Compliance-Systems kann mittels (IT-gestützten) Kennzahlensystemen durchgeführt werden. Bspw. können Kennzahlen, wie z. B. „maximales Steuerrisiko/Eigenkapital" sein und „maximale Cash Tax Belastung/Cash-Flow" gemessen werden. Die Steuerabteilung sollte verpflichtend regelmäßig solche Kennzahlen berechnen und in einem Kennzahlensystem abbilden. Dies ermöglicht es, jederzeit die

[82] A. a. O., S. 10 f.

[83] Ebd.

[84] Ehlers, Tax Compliance, NWB Nr. 18 (2012), S. 1540.

[85] Ebd., S. 166.

Effizienz des Systems zu kontrollieren. Auch die Dokumentation des Veranlagungsstands (offen, in Bearbeitung, abgegeben, Bescheidprüfung, Rechtsmittel, etc.) in einem übersichtlichen Compliance-Tool ermöglicht eine Effizienzmessung des Compliance-Systems. Dabei sollten auch Verspätungszuschläge und andere Nebenleistungen verbindlich aufgeführt werden. Der regelmäßige Austausch mit spezialisierten externen Beratern kann eine hilfreiche Ergänzung im Effizienzmessungsprozess sein.

Compliance in Unternehmen der öffentlichen Hand

Robert Nagelschmitz und Bastian Ohl

Inhaltsverzeichnis

Nachfolgend wird insoweit von „öffentlichen Unternehmen" gesprochen.

Der Autor Robert Nagelschmitz ist derzeit Referent für Beteiligungsführung im Bundesministerium der Verteidigung und war davor in verschiedenen Beteiligungsunternehmen des Bundes tätig, zuletzt als Justitiar und Compliance-Manager der BwFuhrparkService GmbH.

R. Nagelschmitz (✉)
Auf dem Hügel 34, 53347 Alfter, Deutschland
E-Mail: robert.nagelschmitz@berlin.de

B. Ohl
Anna-Schneider-Steig 22, 50678 Köln, Deutschland
E-Mail: bastian.ohl@luther-lawfirm.com

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2_13,

Zusammenfassung

Der Aufbau eines umfassenden und effektiven Compliance-Management-Systems ist in öffentlichen Unternehmen aufgrund ihrer exponierten öffentlichen Stellung unverzichtbar. Hiervon profitieren die Gesellschaftsorgane und die Gesellschafter gleichermaßen. Auch Public Corporate Governance Kodizes sind ein probates Mittel zur Optimierung des Compliance-Managements in öffentlichen Unternehmen. Gerade im kommunalen Bereich sind sie eine wertvolle, praxisrelevante Handreichung für Gesellschaftsvertreter und Gremienmitglieder. Zudem schaffen sie eine größere Transparenz in der öffentlichen Beteiligungsverwaltung und können auf diesem Wege die gesellschaftliche Akzeptanz der öffentlichen Unternehmenstätigkeit stärken.

1 Compliance-Anforderungen in öffentlichen Unternehmen

In öffentlichen Unternehmen kommt der Einhaltung von Compliance-Vorschriften eine ebenso große Bedeutung zu, wie in privaten Unternehmen. Die Leitungsorgane eines öffentlichen Unternehmens haben jedoch – ergänzend zu den für alle Unternehmen geltenden allgemeinen gesellschaftsrechtlichen und strafrechtlichen Vorschriften – in der Regel noch eine Vielzahl öffentlich-rechtlicher Regelungen, insbesondere das Gemeindewirtschaftsrecht des jeweiligen Bundeslandes bzw. das Haushaltsrecht des Bundes (Haushaltsgrundsätzegesetz, Bundeshaushaltsordnung etc.), zu beachten. Erschwerend kommt hinzu, dass diese öffentlich-rechtlichen Vorschriften nicht immer mit den gesellschaftsrechtlichen Grundsätzen des GmbH- oder Aktienrechts im Einklang stehen. Dies zeigt sich insbesondere im Aufsichtsrat öffentlicher Unternehmen, wo der allgemeine gesellschaftsrechtliche Grundsatz der Weisungsfreiheit der Aufsichtsratsmitglieder mit den landesrechtlichen Weisungsbefugnissen der Gemeindevertretungen bzw. der Pflicht der vom Bund in ein Gremium entsandten Vertreter, zur Wahrung der Bundesinteressen, kollidiert.[1]

Darüber hinaus schlägt ein Verstoß gegen die Grundsätze einer ordnungsgemäßen Compliance in öffentlichen Unternehmen mitunter höhere Wellen in der Presse, als eine vergleichbare Verfehlung in einem privaten Unternehmen. Bürger und Steuerzahler sehen öffentliche Unternehmen, auch wenn diese in privatrechtlicher Form organisiert sind, grundsätzlich als Teil der öffentlichen Hand an und empfinden wirtschaftliche Fehlentscheidungen der Geschäftsführung als Verschwendung „ihrer" Steuergelder und Abgaben.[2] Verletzt die wirtschaftliche Fehlentscheidung neben den Grundsätzen ordnungsgemäßer Unternehmensführung auch noch (straf-)gesetzliche Vorschriften, entsteht schnell der Eindruck von „Vetternwirtschaft". Compliance-Verstöße in öffentlichen

[1] Vgl. hierzu näher unten 2.1

[2] Dies gilt insbesondere, wenn die öffentliche Hand die Unternehmen mit Steuergeldern, bspw. in Form von Bürgschaften oder Gesellschafterdarlehen absichert.

Unternehmen können deshalb im schlimmsten Fall das Vertrauen der Bürger in die Rechtstreue staatlicher Institutionen massiv erschüttern.[3]

2 Die Gesellschaftsorgane im Spannungsfeld zwischen den Interessen der Gesellschaft und den Interessen des kommunalen Gesellschafters

In privat-rechtlichen organisierten öffentlichen Unternehmen sind die Gesellschaftsorgane grundsätzlich dem Wohl der Gesellschaft und nicht den finanziellen und öffentlichen Interessen ihrer (kommunalen) Gesellschafter verpflichtet.

Die meisten Gemeindeordnungen und Kommunalverfassungen enthalten zwar die Vorgabe, dass der Unternehmensgegenstand auf einen öffentlichen Zweck ausgerichtet sein muss.[4] Als öffentlicher Zweck können jedoch regelmäßig nicht die Förderung der örtlichen Gemeinschaft[5] oder die finanzielle Unterstützung von öffentlichen Aufgaben, die nicht auf das Unternehmen selbst übertragen wurden, aufgenommen werden. Gerade in diesen Bereichen liegen jedoch in der Regel die Interessen und „Begehrlichkeiten" der kommunalen Gesellschafter.

In öffentlichen Unternehmen mit privater Beteiligung wird dieses Spannungsfeld noch vergrößert, da die Geschäftsführung die Interessen des kommunalen Gesellschafters und des privaten Gesellschafters berücksichtigen muss.

2.1 Konflikte zwischen Kommunalrecht und Gesellschaftsrecht

2.1.1 Zulässigkeit von Weisungen an Aufsichtsratsmitglieder

Einer der umstrittensten und am meisten diskutierten Konflikte zwischen Kommunalrecht und Gesellschaftsrecht ist, ob die kommunalen Gesellschafter eines öffentlichen Unternehmens den von ihnen bestellten, bzw. entsandten, Aufsichtsratsmitgliedern Weisungen erteilen dürfen.[6] Nach dem gesetzlichen Leitbild des Aktienrechts sind Aufsichtsratsmitglieder grundsätzlich nicht an Weisungen der Gesellschafter gebunden, auch wenn sie von diesen entsandt oder auf deren Vorschlag gewählt wurden. Sie üben ihr Amt unabhängig aus. Das Kommunalrecht weicht von diesem Grundsatz teilweise ab. So fordert § 108 Abs. 5 Nr. 2 GO NRW[7] ausdrücklich, dass sich eine Kommune nur dann an öffentlichen

[3] Vgl. *Ohrtmann,* in: Compliance – Anforderungen an rechtskonformes Verhalten öffentlicher Unternehmen, 1. Aufl. 2009, S. 29.

[4] Vgl. exemplarisch § 108 Abs. 1 Nr. 7 GO NRW.

[5] Bspw. von Sportvereinen und sonstigen sozialen und kulturellen Einrichtungen.

[6] Vgl. *Heidel*, NZG 2012, 54; *E. Vetter*, GmbHR 2011, S. 459; BVerwG, Urteil vom 31. August 2011, Az. 8 C 16.10; VGH Kassel, Urteil vom 9. Februar 2012, Az. 8 A 2043/10, NVwZ-RR 2012, 566.

[7] Gemeindeordnung für das Land Nordrhein-Westfalen.

Unternehmen in der Rechtsform der GmbH beteiligen darf, wenn im Gesellschaftsvertrag sichergestellt ist, dass „*der Rat den von der Gemeinde bestellten oder auf Vorschlag der Gemeinde gewählten Mitgliedern des Aufsichtsrats Weisungen erteilen kann, soweit die Bestellung eines Aufsichtsrates gesetzlich nicht vorgeschrieben ist*."

Bei der Beurteilung dieser Frage muss in der Praxis zunächst zwischen öffentlichen Unternehmen mit einem obligatorischen Aufsichtsrat und solchen mit einem fakultativen Aufsichtsrat unterschieden werden. Ist die Einrichtung eines Aufsichtsrats gesetzlich zwingend, wie bspw. in der Aktiengesellschaft oder bei mitbestimmten Unternehmen, ist die Erteilung von Weisungen an Aufsichtsratsmitglieder unzulässig.[8] Dies berücksichtigen auch die Gemeindeordnungen der Länder.

Anders kann sich die Situation nach der Rechtsprechung des Bundesverwaltungsgerichts[9] in öffentlichen Unternehmen mit einem fakultativen Aufsichtsrat, bspw. nach § 52 GmbHG, darstellen. Gemäß § 52 Abs. 1 GmbHG finden die dort genannten aktienrechtlichen Vorschriften auf einen fakultativen Aufsichtsrat nur dann Anwendung, wenn der Gesellschaftsvertrag nicht eine abweichende Regelung vorsieht. In dem vom Bundesverwaltungsgericht entschiedenen Fall enthielt der Gesellschaftsvertrag einen pauschalen Ausschluss der aktienrechtlichen Vorschriften, ohne jedoch selbst ein ausdrückliches Weisungsrecht der kommunalen Gesellschafter vorzusehen. Im Wege der Vertragsauslegung kam das Bundesverwaltungsgericht zu dem Schluss, dass:

> mit den kommunalrechtlichen Vorschriften ein Regelungssystem vorhanden [ist], auf das als Auslegungshilfe für den Gesellschaftsvertrag zurückgegriffen werden kann. Da sich die Gemeinde gemäß § 108 Abs. 5 Nr. 2 *GONRW* nur dann an einer GmbH mit einem fakultativen Aufsichtsrat beteiligen darf, wenn durch die Ausgestaltung des Gesellschaftsvertrages sichergestellt ist, dass der Rat den von der Gemeinde bestellten oder auf Vorschlag der Gemeinde gewählten Mitgliedern des Aufsichtsrats Weisungen erteilen kann, ist davon auszugehen, dass die Gesellschafter die gesellschaftsrechtlichen Voraussetzungen für eine Relevanz dieser Weisungen im Gesellschaftsvertrag schaffen wollten. Deshalb ist der Ausschluss der Vorschriften des Aktiengesetzes durch den Gesellschaftsvertrag dahin auszulegen, dass stattdessen ein Weisungsrecht des Beklagten gegenüber den Klägern für die Wahrnehmung ihrer Rechte als Mitglieder des Aufsichtsrats bestehen soll.

Die Rechtsprechung des Bundesverwaltungsgerichts ist sowohl in der Literatur[10] als auch von anderen Verwaltungsgerichten[11] kritisiert worden. Neben dem allgemeinen Vorrang des Gesellschaftsrechts als Bundesrecht vor landesrechtlichen Regelungen wurde insbesondere eingewandt, dass es nicht den Anforderungen an eine gute Corporate Governance genügt, wenn die Überwachungskompetenz des Aufsichtsrats vollkommen der Satzungsautonomie der Gesellschafter unterworfen wird.[12]

---

[8] Allgemeine Meinung, vgl. *Habersack*, in: Münchener Kommentar, AktG, 3. Aufl. 2008, § 111 Rn 136 ff.

[9] BVerwG, Urteil vom 31. August 2011, Az. 8 C 16.10.

[10] Vgl. exemplarisch *E. Vetter*, GmbHR 2011, S. 449.

[11] VGH Kassel, Urteil vom 9. Februar 2012, Az. 8 A 2043/10, NVwZ-RR 2012, 566.

[12] Vgl. *E. Vetter*, GmbHR 2011, S. 459.

In der **Unternehmenspraxis** sollten deshalb trotz der großzügigeren Rechtsprechung des Bundesverwaltungsgerichts die folgenden **Grundsätze für Weisungen an Aufsichtsratsmitglieder** berücksichtigt werden:

- Die kommunalen Gesellschafter dürfen grundsätzlich keine Weisungen an Aufsichtsratsmitglieder erteilen, die gegen das Unternehmensinteresse verstoßen und zu einem Schaden führen würden.
- Bei öffentlichen Unternehmen mit obligatorischem Aufsichtsrat (Aktiengesellschaften und mitbestimmte GmbHs) ist auf die Erteilung von Weisungen zu verzichten.
- Bei öffentlichen Unternehmen mit fakultativem Aufsichtsrat sollten Weisungsbefugnisse der Gemeinde an Aufsichtsratsmitglieder im Gesellschaftsvertrag geregelt und die Voraussetzungen für eine Weisung klar definiert werden (insbesondere keine Weisung gegen das Unternehmensinteresse).[13] Ein bloßer Ausschluss der aktienrechtlichen Vorschriften führt zu vermeidbaren Rechtsunsicherheiten.[14]

2.1.2 Vertraulichkeitspflichten der Aufsichtsratsmitglieder

Ein weiteres Spannungsfeld zwischen dem gesellschaftsrechtlichen Leitbild des Aufsichtsrats und den kommunalen Interessen liegt im Bereich der Vertraulichkeitspflichten der von der Kommune entsandten, bzw. gewählten, Aufsichtsratsmitglieder in öffentlichen Unternehmen.

Gemäß § 116 AktG Satz 2 AktG sind die Aufsichtsratsmitglieder „*insbesondere zur Verschwiegenheit über erhaltene vertrauliche Berichte und vertrauliche Beratungen verpflichtet*". Durch die Entsendung von Vertretern in den Aufsichtsrat soll jedoch sichergestellt werden, dass die demokratisch gewählten Ratsvertreter der Kommune über die Geschäfte der öffentlichen Unternehmen umfassend informiert werden. Aus diesem Grund sehen §§ 394 und 395 AktG Sonderregelungen für die Vertraulichkeitspflichten von Aufsichtsratsmitgliedern vor, die auf Veranlassung einer Gebietskörperschaft in den Aufsichtsrat gewählt oder entsandt worden sind. Sie unterliegen hinsichtlich der Berichte, die sie der Gebietskörperschaft zu erstatten haben, keiner Verschwiegenheitspflicht. Für vertrauliche Angaben und Geheimnisse der Gesellschaft, namentlich Betriebs- oder Geschäftsgeheimnisse, gilt dies allerdings nicht, wenn ihre Kenntnis für die Zwecke der Berichte nicht von Bedeutung ist.

In Gesellschaften mit fakultativem Aufsichtsrat, insbesondere in nicht mitbestimmten GmbHs, ist für die Anwendbarkeit der §§ 116, 394, 395 AktG danach zu differenzieren, ob der Gesellschaftsvertrag die Verschwiegenheitspflicht abbedingt.[15] Es obliegt grundsätzlich der Gestaltungsfreiheit der GmbH-Gesellschafter, ob sie im Gesellschaftsvertrag eigenständige Regelungen zur Abbedingung der Verschwiegenheitspflicht aufnehmen.[16]

---

[13] So auch VGH Kassel, Urteil vom 9. Februar 2012, Az. 8 A 2043/10, NVwZ-RR 2012, 569.

[14] Vgl. *Heidel*, NZG 2012, 54.

[15] Spindler, ZIP 2011, 692.

[16] Spindler, a. a. O. mit weiteren Nachweisen.

Enthält der Gesellschaftsvertrag keine Sonderregelungen zur Verschwiegenheitspflicht, gelten die genannten aktienrechtlichen Vorschriften über § 52 Abs. 1 GmbH im selben Umfang.[17]

Berichtspflicht

Die Lockerung der Verschwiegenheitspflichten der Aufsichtsratsmitglieder nach § 394 AktG setzt allerdings voraus, dass eine Berichts**pflicht** gegenüber der entsendenden Gebietskörperschaft besteht. Die Vorschrift des § 394 AktG statuiert insoweit keine Berichtspflicht, sondern nimmt auf eine anderweitig begründete Berichtspflicht Bezug und erlaubt es dem Aufsichtsratsmitglied lediglich, diese Pflicht zu erfüllen.

Die meisten Gemeindeordnungen der Länder enthalten eine gesetzliche Berichtspflicht der kommunalen Aufsichtsratsmitglieder an den Rat.[18] Sowohl der Adressat der Berichtspflicht als auch der Umfang (bspw. nur Angelegenheiten von besonderer Bedeutung[19]) richten sich nach der jeweiligen gesetzlichen Regelung. In der Praxis sollten die kommunalen Aufsichtsratsmitglieder bei der Erstattung ihrer Berichte deshalb strikt die für sie geltenden landesgesetzlichen Vorgaben einhalten.

Im Rahmen der Aktienrechtsnovelle 2012, die im Jahr 2013 in Kraft treten soll, wird § 394 AktG um einen neuen Satz 3 ergänzt werden. Dieser lautet[20]: „*Die Berichtspflicht nach Satz 1 kann auf Gesetz oder Rechtsgeschäft beruhen.*" Nach dem Willen der Bundesregierung soll eine Berichtspflicht i. S. v. § 394 Satz 1 AktG „*auch im Rahmen einer vertraglichen Vereinbarung, eines Auftrags oder einer Nebenabrede mit der Gebietskörperschaft begründet werden*" können.[21] Eine besondere Form der Abrede ist nach dem Gesetzeswortlaut nicht erforderlich. Im Sinne einer transparenten Unternehmensführung und zur Absicherung der kommunalen Gremienmitglieder sollte jedoch stets zumindest die Schriftform gewahrt werden.

[17] Spindler, a. a. O.

[18] So bspw. § 113 Abs. 5 Satz 1 GO NRW. Keine gesetzlichen Berichtspflichten bestehen bislang nur in Baden-Württemberg, Rheinland-Pfalz, Schleswig-Holstein und Thüringen.

[19] Als Angelegenheiten von besonderer Bedeutung sind bspw. nach § 113 Abs. 5 Satz 1 GO NRW i. V. m. § 41 Abs. 4 GO NRW anzusehen: Satzungsänderungen, Änderungen von Gesellschaftsverträgen, Eckdaten der Wirtschafts- und Finanzplanung, Eckdaten der Jahresrechnung, Verwendung von Bilanzgewinnen, Erhöhungen und Herabsetzungen des Stamm- bzw. Grundkapitals, wesentliche Umstrukturierungsmaßnahmen, Personalentscheidungen auf Vorstands- bzw. Geschäftsführerebene, erstmalige Beteiligungen und Veränderungen bestehender Beteiligungen an anderen juristischen Personen oder Personenvereinigungen.

[20] Stand: Gesetzentwurf der Bundesregierung nach Äußerung des Bundesrates und Gegenäußerung der Bundesregierung, in der am 29. November 2012 an den Rechtsausschuss überwiesenen Fassung.

[21] BT-Drucksache 17/8989, S. 21.

Umfang der Berichtspflicht

Der Zweck des Berichts liegt darin, der Gebietskörperschaft die für die Verwaltung der Beteiligung notwendigen Kenntnisse zu übermitteln und ihr sowie der Rechnungsprüfungsbehörde die haushaltsrechtliche Prüfung der wirtschaftlichen Betätigung zu ermöglichen. Dazu bedarf es auch solcher Informationen, die der Gebietskörperschaft die Möglichkeit planender und auf die Unternehmensziele einwirkender Tätigkeit verschaffen. Der Rahmen ist weit gespannt und umfasst alle Vorgänge, die wegen der mit ihnen verbundenen Chancen und Risiken von wesentlicher wirtschaftlicher Bedeutung sind. Nicht zu den Berichtszwecken gehören dagegen Details über den Geschäftsbetrieb, es sei denn, dass sie auch für die Verwaltung der Beteiligung erheblich sind.

Adressat der Berichtspflicht und Sicherstellung der Vertraulichkeit

Die §§ 394, 395 AktG schaffen nicht nur ein Informationsprivileg zugunsten der öffentlichen Hand, sondern wollen zugleich auch die berechtigten Interessen der Gesellschaft wahren. Daher ist eine Weitergabe vertraulicher Informationen durch ein Aufsichtsratsmitglied nur dann zulässig, wenn eine hinreichende Gewähr für die tatsächliche Wahrung der Vertraulichkeit besteht. Der Kreis der Empfänger muss daher so begrenzt sein, dass die Einhaltung der Verschwiegenheit in ähnlicher Weise wie beim Aufsichtsrat kontrollierbar bleibt. Eine Weitergabe von vertraulichen Informationen ist nur zulässig, wenn der Schutz der Vertraulichkeit nach Zusammensetzung und Arbeitsweise des mit der Prüfung betrauten Gremiums gesichert ist.

Um die Vertraulichkeit der Berichte der Aufsichtsratsmitglieder an die Kommune sicherzustellen, sieht § 395 AktG ergänzend eine Verschwiegenheitspflicht für diejenigen Personen vor, „*die damit betraut sind, die Beteiligungen einer Gebietskörperschaft zu verwalten oder für eine Gebietskörperschaft die Gesellschaft, die Betätigung der Gebietskörperschaft als Aktionär oder die Tätigkeit der auf Veranlassung der Gebietskörperschaft gewählten oder entsandten Aufsichtsratsmitglieder zu prüfen*".

2.1.3 Besonderheiten in kommunalen Aktiengesellschaften

Die Aktiengesellschaft ist eindeutig der Ausnahmefall unter den kommunalen Unternehmen. Die Gemeindeordnungen sehen in der Regel ein faktisches Verbot für Kommunen vor, sich an Aktiengesellschaften zu beteiligen oder neue Aktiengesellschaften zu gründen.[22] Bestehende kommunale Beteiligungen an Aktiengesellschaften genießen jedoch Bestandsschutz.

Die Regelungen des Aktienrechts sind auch auf öffentliche Unternehmen in Form der Aktiengesellschaft uneingeschränkt anwendbar. Landesrechtliche Abweichungen von den Vorschriften des Aktiengesetzes sind grundsätzlich unzulässig. Sie können das bundesgesetzliche Regime des Aktiengesetzes lediglich ergänzen, sofern die Ergänzungen nicht im

[22] Vgl. exemplarisch § 108 Abs. 4 GO NRW: „*Die Gemeinde darf unbeschadet des Absatzes 1 Unternehmen und Einrichtungen in der Rechtsform einer Aktiengesellschaft nur gründen, übernehmen, wesentlich erweitern oder sich daran beteiligen, wenn der öffentliche Zweck nicht ebenso gut in einer anderen Rechtsform erfüllt wird oder erfüllt werden kann.*"

Widerspruch zu den anerkannten aktienrechtlichen Grundsätzen stehen. Insbesondere können die kommunalen Gesellschafter den Vorstands- und Aufsichtsratsmitgliedern einer Aktiengesellschaft keine Weisungen erteilen.

2.2 Repräsentationsaufwendungen, Sponsoring und Spenden – Ein juristisches Minenfeld für die Geschäftsführung öffentlicher Unternehmen

In kommunalen Unternehmen wird die Geschäftsführung erfahrungsgemäß häufig damit konfrontiert, dass kommunale Gesellschaftervertreter an sie herantreten und um Sponsoringleistungen oder Spenden für öffentliche Einrichtungen bitten. Ebenso kommt es vor, dass die Geschäftsführung selbst an die kommunalen Gesellschafter herantritt und ihnen die Förderung örtlicher Projekte und öffentlicher Einrichtungen vorschlägt. Die Bandbreite ist schier unerschöpflich und reicht von Werbebanden auf dem Sportplatz des örtlichen Fußballvereins, über Spenden für die kommunale Musikschule oder die städtische Weihnachtsbeleuchtung bis hin zum Sponsoring von Stadtfesten, Weihnachtsmärkten und Sportvereinen.

All diese Leistungen wurden in der Vergangenheit meist von den Kommunen selbst erbracht. Aufgrund der angespannten finanziellen Lage greifen jedoch in vielen Kommunen haushaltsrechtliche Restriktionen, die dazu führen, dass die Kommunen solche freiwilligen Leistungen zurückfahren müssen. Viele öffentliche Unternehmen, insbesondere im Bereich der Stadtwerke, weisen dagegen Gewinne aus, da sie am Markt ausgezeichnet positioniert und etabliert sind. Für einen kommunalen Gesellschafter besteht deshalb die naheliegende Versuchung, die Gewinne des Unternehmens nicht vollständig an den allgemeinen Haushalt auszuschütten, sondern zumindest einen Teil vorab zur Förderung der örtlichen Gemeinschaft einzusetzen.

Die Geschäftsführung gerät in solchen Fällen in ein Spannungsfeld zwischen ihren gesetzlichen Pflichten, insbesondere ihrer Verpflichtung auf das Gesellschaftsinteresse, auf der einen Seite und den Forderungen ihres Allein-, oder Mehrheitsgesellschafters auf der anderen Seite. **Bei allen Zuwendungen an Gesellschafter sollten auch im Bereich Spenden und Sponsoring stets die steuerrechtlichen Risiken einer möglichen verdeckten Gewinnausschüttung bedacht werden**.[23]

2.2.1 Grundsätze für Sponsoring

Unter Sponsoring versteht man die Zuwendung von Geld oder geldwerten Leistungen, die neben dem Motiv zur Förderung des Empfängers auch andere Interessen verfolgen. Dem

[23] Unter einer verdeckten Gewinnausschüttung i. S. d § 8 Abs. 3 Satz 2 KStG ist bei einer Kapitalgesellschaft eine Vermögensminderung (verhinderte Vermögensmehrung) zu verstehen, die durch das Gesellschaftsverhältnis veranlasst ist, sich auf die Höhe des Einkommens auswirkt und in keinem Zusammenhang mit einer offenen Ausschüttung steht. Vgl. BFH DStR 2009, 217.

Sponsor kommt es in der Regel darauf an, sich in der Öffentlichkeit über das gesponserte Projekt zu profilieren.[24]

Die Geschäftsführung muss bei Sponsoringmaßnahmen darauf achten, dass diese mit dem Gesellschaftszweck vereinbar sind. Je enger der Unternehmensgegenstand gefasst ist, desto geringer wird in der Regel der Ermessensspielraum der Geschäftsführung. Zudem ist für jede Maßnahme die wirtschaftliche Angemessenheit der erhaltenen Gegenleistung zu beachten. Der Werbeeffekt muss im Verhältnis zum wirtschaftlichen Wert der Zuwendung stehen.

Bei Sponsoringmaßnahmen, die unmittelbar oder mittelbar dem kommunalen Gesellschafter, bzw. einem Organmitglied (bspw. den Aufsichtsratsmitgliedern) zugutekommen, können strafrechtliche Risiken auftreten. Besonders praxisrelevant ist in diesem Zusammenhang der Straftatbestand der Vorteilsgewährung gemäß § 334 StGB, auf den unten näher eingegangen wird.

2.2.2 Grundsätze für Spenden

Ein noch höheres Risikopotenzial als bei Sponsoring und Werbung liegt für die Geschäftsführung kommunaler Unternehmen im Bereich von Spenden, insbesondere für öffentliche Einrichtungen oder Vereine. Die Leistung des Unternehmens erfolgt bei einer Spende grundsätzlich ohne Gegenleistung. Es fehlt deshalb grundsätzlich ein Bezug zur indirekten Förderung der Unternehmensziele, wie er bei Sponsoringmaßnahmen regelmäßig gegeben ist.

Die Entscheidung darüber, ob und an wen Spenden des Unternehmens erfolgen sollen, darf durch die Geschäftsführung nur unter Berücksichtigung der nachfolgenden Kriterien erfolgen, die kumulativ erfüllt sein müssen[25]:

- Nähe der Zuwendung zum Unternehmensgegenstand (bspw. Förderung wissenschaftlicher und ökologischer Forschungsvorhaben sowie kulturelle und soziale Förderung im unmittelbaren regionalen Einzugsgebiet des Unternehmens),
- Angemessenheit der Höhe der Zuwendung im Hinblick auf die Ertrags-und Vermögenslage des Unternehmens (nicht mehr als 5 % des ausgeschütteten Jahresgewinns nach Steuern),
- Innergesellschaftliche Transparenz der Zuwendungshöhe, des Zuwendungszwecks und des Adressatenkreises der Zuwendung,
- Ausschaltung unsachlicher Motive, namentlich persönlicher Präferenzen bei der Auswahl der Empfänger und der Höhe der Begünstigung.

Um die innergesellschaftliche Transparenz und die sachliche, zweckgemäße Auswahl der Empfänger sicherzustellen, empfiehlt sich **in der Unternehmenspraxis** der Erlass einer

[24] Vgl. *P. Glauben*, LKRZ 2008, 81 (84).

[25] Säcker, BB 2009, S. 282.

Spenden- und Sponsoringrichtlinie für die Geschäftsführung durch die Gesellschafter[26]. In einer solchen Richtlinie kann ein jährliches Budget für Spenden und Sponsoring festgelegt werden, dass die Ertragslage der Gesellschaft berücksichtigt.

Zudem sollte der Empfängerkreis so definiert werden, dass ausschließlich nichtstaatliche und nicht-kommunale gemeinnützige Einrichtungen begünstigt werden können.[27] Es sollte sich hierbei um Einrichtungen aus den Bereichen Kunst, Wissenschaft, Sozialwesen oder Sport handeln. Reine Unterhaltungsveranstaltungen sollten wenn überhaupt nur äußerst zurückhaltend gefördert werden.[28] Die Entscheidung sollte nicht durch ein einzelnes Mitglied der Geschäftsführung, sondern durch eine unternehmensinterne Kommission, bzw. einen Ausschuss erfolgen.

Rechtlich hochproblematisch sind generell Spenden an Einrichtungen, an denen der kommunale Gesellschafter selbst beteiligt ist und an Vereine oder Organisationen, in denen Gesellschaftervertreter oder Organmitglieder des Unternehmens tätig sind. Hier sind die Grenzen zu den strafrechtlichen Vorteilsgewährungs- und Korruptionstatbeständen fließend (s. u. 2.4.3). Sie sollten deshalb im Sinne einer guten Unternehmensführung vermieden werden.

2.2.3 Besonderheiten für Sponsoring und Spenden bei öffentlichen Unternehmen in Monopolbereichen der Daseinsvorsorge

Insbesondere im Bereich der Wasserversorgung und Abwasserbeseitigung bestehen auch heute noch rechtlich anerkannte und gewollte Monopolstrukturen. Anders als im liberalisierten Energiesektor haben die Verbraucher nicht die Wahl, ihren Wasserversorger oder ihr Abwasserbeseitigungsunternehmen selbst zu wählen und ggf. den Anbieter zu wechseln. In der Rechtsprechung wurden deshalb teilweise besondere Restriktionen bei Sponsoring- und Werbeleistungen für in diesen Bereichen tätige öffentliche Unternehmen aufgestellt.

So haben das VG Dresden[29] und das OVG Bautzen[30] kürzlich entschieden, dass ein kommunales Wasserversorgungsunternehmen grundsätzlich keinerlei Werbe- oder Sponsoringmaßnahmen veranlassen dürfe. Zur Begründung haben die Gerichte u. a. angeführt, dass ein Wasserversorger weder Konkurrenz durch andere Wasseranbieter befürchten, noch um die Gunst potenzieller Kunden werben müsse. Es sei nicht ersichtlich, inwiefern die Aufgabenerfüllung des Unternehmens (kommunale Wasserversorgung) durch Bandenwerbung oder den Abdruck des Unternehmenslogos als Sponsor in Programmheften sowie auf Eintrittskarten für kulturelle Veranstaltung gefördert werde. Erst recht dürfe das Unternehmen keine Spenden tätigen, da in diesem Fall keinerlei Gegenleistung vorliege. Das VG Dresden hat seine Rechtsauffassung wie folgt zusammengefasst: „*Es gibt in der*

[26] Vgl. den Entwurf einer Vorstandsrichtlinie bei *Säcker,* DB 2009, S. 282.

[27] Vgl. *Säcker*, DB 2009, S. 282.

[28] Vgl. *Säcker*, DB 2009, S. 282.

[29] VG Dresden, BeckRS 2010, 52568.

[30] OVG Bautzen, Beschluss vom 18. Januar 2011, Az. 4 B 270/10, LKV 2011, 225.

demokratischen Ordnung keinen vernünftigen Grund, dass sich staatlich Bedienstete – einschließlich der leitenden Angestellten öffentlicher Unternehmen – mit öffentlichen Mitteln als Mäzene gerieren."

Es handelt sich, soweit ersichtlich, um die ersten zu dieser Thematik ergangenen gerichtlichen Entscheidungen. Insbesondere in Sachsen haben jedoch bereits weitere kommunale Aufsichtsbehörden entsprechende Unterlassungsverfügungen gegen kommunale Wasserversorgungsunternehmen erlassen. So wurden beispielsweise im Februar 2011 den Wasserwerken Zwickau von der Landesdirektion Chemnitz alle künftigen Sponsoringmaßnahmen untersagt. Das Sponsoring- und Spendenvolumen betrug in diesem Fall lediglich 0,2 % des Gesamtumsatzes.[31] Vergleichbare Fälle aus anderen Bundesländern sind aktuell allerdings noch nicht bekannt geworden.

In der juristischen Fachliteratur wird die Thematik bisher nur sehr sporadisch diskutiert. Sponsoringmaßnahmen durch kommunale Unternehmen der Daseinsvorsorge werden in diesem Zusammenhang als „*bedenklich*" bezeichnet.[32] Die Unternehmen hätten eine präzise Aufgabe zu erfüllen, zu der Kulturförderung grundsätzlich nicht gehöre. Gleiches gelte auch für privatrechtliche Unternehmen der öffentlichen Hand. Diese seien an ihren Gesellschaftszweck gebunden.[33] Auch nach Auffassung von Transparency International sollen Sponsoringmaßnahmen durch kommunale Unternehmen der Daseinsvorsorge unzulässig sein. Deren Finanzierung erfolge durch Staatszuschüsse, Abgaben und Gebühren, welche nicht „*beliebig für Sponsoring ausgegeben werden dürfen*".[34]

Das OVG Bautzen hat seine Ergebnisse jedoch im konkreten Fall explizit auf den Unternehmensgegenstand zurückgeführt. Dieser umfasste ausdrücklich nur die Wasserversorgung und keine darüber hinausgehenden Wettbewerbstätigkeiten oder öffentlichen Förderaufgaben. Es ist somit nicht zwingend, hieraus ein generelles Verbot des Sponsorings im herrschaftlichen Monopolbereich abzuleiten.

Zudem gehen die Urteile des OVG Bautzen und des VG Dresden an den tatsächlichen wirtschaftlichen Gegebenheiten in der Wasserversorgung vorbei. So stehen auch kommunale Wasserversorger beispielsweise mit Herstellern von Trinkwasser in Flaschen im Wettbewerb. Sie können deswegen durchaus ein sinnvolles und schutzwürdiges Interesse daran haben, ihre Kunden, etwa durch Werbemaßnahmen, davon zu überzeugen, anstelle von Trinkwasser aus Flaschen Trinkwasser aus dem Wasserhahn zu benutzen.[35] Die Aussagen des OVG, wonach Wasserversorger generell keinem Wettbewerb ausgesetzt seien, sind deshalb in dieser Pauschalität nicht haltbar.

Darüber hinaus wird auch im Bereich der Wasserversorgung derzeit eine Vielzahl auslaufender Konzessionsverträge durch die Kommunen neu vergeben, ohne dass hierbei eine Garantie für den bisherigen Versorger besteht, bei der Neuvergabe wieder berück-

---

[31] Vgl. Zwickauer Freie Presse vom 23. Februar 2011.

[32] Vgl. *Caspar/Neubauer*, LKV 2011, 200.

[33] Vgl. *Caspar/Neubauer*, a. a. O.

[34] Vgl. Potsdamer Neueste Nachrichten vom 14. April 2011.

[35] Vgl. Kommentar des Fachverband Sponsoring (FASPO) vom 7. März 2011.

sichtigt zu werden. Die kommunalen Wasserversorger haben unter diesem Aspekt ein schützenswertes Interesse, sich gegenüber privatwirtschaftlichen Konkurrenten um die Neuvergabe der Konzession am Markt positionieren zu können. Auch den Tarifkunden entstehen durch maßvolle Sponsoringmaßnahmen und gemeinnützige Spenden des kommunalen Wasserversorgungsunternehmens keine finanziellen Nachteile, **wenn und soweit die betreffenden Ausgaben bei der Festsetzung der Tarife nicht berücksichtigt werden**.

Ein generelles Sponsoringverbot für öffentliche Unternehmen in Monopolbereichen ist insbesondere dann abzulehnen, wenn der Unternehmensgegenstand auch Dienstleistungen und Arbeiten für andere Versorgungsunternehmen oder sonstige wettbewerbliche Tätigkeiten umfasst. In diesen Bereichen konkurrieren die öffentlichen Unternehmen mit privaten Konkurrenten und haben ein schützenswertes Interesse daran, sich durch Sponsoringmaßnahmen und Werbung am Markt darzustellen.

Da für Wasserversorgungsunternehmen weder ein gesetzliches Verbot von Sponsoringmaßnahmen und Spenden existiert, noch sonstige sachlich oder rechtlich überzeugende Gründe für ein pauschales Verbot vorliegen, ist den Entscheidungen des OVG Bautzen und des LG Dresden nicht ohne weiteres zuzustimmen.

2.2.4 Repräsentationsaufwendungen

Die Geschäftsführung eines öffentlichen Unternehmens darf generell Repräsentationsaufwendungen tätigen. Sie muss den kommunalrechtlichen Grundsatz der wirtschaftlichen und sparsamen Haushaltsführung und die wirtschaftliche Ertragskraft sowie das Marktumfeld des Unternehmens beachten.

Verlässt die Geschäftsführung bei Repräsentationsaufwendungen die sich hieraus ergebenden Grenzen der Sozialadäquanz und entsteht dadurch der Gesellschaft ein Schaden, kommen eine Strafbarkeit wegen Untreue nach § 266 Abs. 1 Alt. 2 StGB und Schadensersatzpflichten gemäß § 43 Abs. 2 GmbHG in Betracht.

Zivilrechtliche Haftung nach § 43 Abs. 2 GmbHG

Die Billigung einer geplanten oder bereits durchgeführten Geschäftsführungsmaßnahme durch die Gesellschafterversammlung schließt die Haftung des Geschäftsführers aus § 43 Abs. 2 GmbHG aus.

Generell reicht jede Entscheidung der Gesellschafterversammlung über die fragliche Geschäftsführungsmaßnahme aus. Eine formale Bezeichnung als Billigungsbeschluss ist nicht notwendig. Ob auch ein stillschweigendes Einverständnis einen solchen Haftungsausschluss zu begründen vermag, ist umstritten. Zumindest muss die stillschweigende Billigung die Qualität eines konkludenten Gesellschafterbeschlusses haben. Eine bloße unverbindliche Kenntnisnahme der Gesellschafterversammlung genügt nicht.

Ebenfalls nicht ausgeschlossen wird die Haftung des Geschäftsführers aus § 43 Abs. 2 GmbHG, wenn die Gesellschafterversammlung ihn zu einer rechtswidrigen Maßnahmen anweist. Begründet wird dies damit, dass die Gesellschafter nicht die erforderlichen Befugnisse haben, um den Geschäftsführer von der Pflicht zur Einhaltung zwingenden Rechts zu entbinden.

Strafrechtliche Untreue nach § 266 Abs. 1 Alt. 2 StGB

Im Bereich der strafrechtlichen Untreue zu Lasten der Gesellschaft gemäß § 266 Abs. 1 Alt. 2 StGB liegt grundsätzlich keine strafbare pflichtwidrige Handlung vor, wenn der Inhaber des zu betreuenden Vermögens eingewilligt hat. Ein Beschluss der Gesellschafterversammlung, durch den die entsprechende Geschäftsführungsmaßnahme angeordnet wird, lässt somit die strafrechtliche Verantwortlichkeit des Geschäftsführers in den meisten Konstellationen entfallen. Anders ist dies allerdings bei offensichtlich rechtswidrigen Weisungen der Gesellschafterversammlung.

Auch ohne ausdrückliche Ermächtigung der Gesellschafterversammlung im Einzelfall werden jedem Unternehmen, auch wenn sich sämtliche Anteile in kommunaler Hand befinden, sozialadäquate Aufwendungen für „Repräsentation" zugestanden. Ein abstrakter Rahmen für die Höhe derartiger Ausgaben existiert jedoch nicht.

Das OLG Hamm[36] hat den Fall einer kommunalen Stadtwerke-GmbH entschieden, deren Geschäftsführer über einen Zeitraum von 3 Jahren rund 56.000 € p. a. für Spirituosen aufgewendet hat und zudem etwa 500 Kunstwerke zur Ausstattung der Geschäftsräume angeschafft hatte. In diesem Fall lag die strafbare Untreue auf der Hand. Das OLG Hamm hat in diesem Fall jedoch grundlegende Ausführungen dazu gemacht, dass zur Bestimmung der „Verhältnismäßigkeit" von Repräsentationsaufwendungen *„der öffentliche Zweck der Gesellschaft und die sich aus der GO NRW ergebenden Wirtschaftsgrundsätze"* besonders zu beachten sind. Bei der Verwaltung öffentlicher Gelder und Gebühren gelten besonders strenge Sorgfaltsanforderungen. Dem hat sich die Kommentarliteratur angeschlossen.[37]

Sonderprobleme bei Zuwendungen an Amtsträger

Zuwendungen an Amtsträger können nach §§ 331 und 333 StGB als Vorteilsannahme, bzw. als Vorteilsgewährung strafbar sein. Dies setzt voraus, dass dem Amtsträger für seine Dienstausübung ein Vorteil für sich oder einen Dritten angeboten, versprochen oder gewährt wird, bzw. der Amtsträger einen solchen Vorteil fordert, sich versprechen lässt, oder annimmt.

Amtsträger sind nach § 11 Satz 1 Nr. 2 b) und c) StGB alle Personen, die in einem öffentlich-rechtlichen Amtsverhältnis stehen oder sonst dazu bestellt sind, bei einer Behörde oder einer sonstigen Stelle oder in deren Auftrag Aufgaben der öffentlichen Verwaltung wahrzunehmen. Auf die zur Aufgabenerfüllung gewählte Organisationsform kommt es hierbei nicht an. Als sonstige Stellen gelten insbesondere rechtsfähige Anstalten öffentlichen Rechts und Eigen- bzw. Regiebetriebe.

Auch juristische Personen des Privatrechts (wie GmbHs und AGs) können sonstige Stellen sein, wenn bei ihnen Merkmale vorliegen, die eine Gleichstellung mit Behörden rechtfertigen.[38] Bei Beteiligungen von Privaten ist dies nicht der Fall, wenn der private Mitgesellschafter zumindest über eine Sperrminorität für wesentliche unternehmerische

[36] OLG Hamm, NStZ 1986, 119.

[37] Vgl. Fischer, StGB, 60. Aufl. 2013, § 266 Rn. 121 ff.

[38] Vgl. *Fischer*, 60. Aufl. 2013, § 11 Rn. 19 ff.

Entscheidungen verfügt.[39] Letztlich muss eine Einzelfallabwägung für jedes öffentliche Unternehmen getroffen werden. Als **Orientierung für die Praxis** können die folgenden Beispiele aus der Rechtsprechung herangezogen werden, die als öffentliche Verwaltung i. S. v. § 11 Satz 1 Nr. 2 c) StGB eingestuft wurden[40]:

- Öffentliche Sparkassen,
- Versorgungswerke,
- In städtischem Alleinbesitz stehende GmbH, deren wesentliche Geschäftstätigkeit die Fernwärmeversorgung der Einwohner ist,
- GmbH zur Abfallbeseitigung, deren Alleingesellschafter ein Landkreis ist,
- Im städtischen Alleinbesitz stehende AG, die im Stadtgebiet den ÖPNV allein betreibt.

Vertreter der kommunalen Anteilseigner in den Gesellschaftsgremien sind nicht nur Gesellschaftervertreter, sondern in vielen Fällen auch Amtsträger. Dies gilt insbesondere für kommunale Eigengesellschaften, an denen keine privaten Mitgesellschafter mehrheitlich oder mit Sperrminoritäten beteiligt sind.[41] Zuwendungen der Gesellschaft an diese Gremienmitglieder müssen somit grundsätzlich an den gesetzlichen Regelungen, den einschlägigen Verwaltungsvorschriften und den Compliance-Richtlinien der Gesellschaft gemessen werden. Demnach sind generell nur sozialadäquate Zuwendungen zulässig. Sozialadäquat sind solche Leistungen, die der Höflichkeit oder Gefälligkeit entsprechen und sowohl sozial üblich als unter Gesichtspunkten des Rechtsschutzes allgemein gebilligt sind.[42]

Bei der Beurteilung der Sozialadäquanz kann auf die „*Verwaltungsvorschrift zu § 59 LBG NRW*[43]*/42 BeamtStG*[44]“ vom 16. März 2011 zurückgegriffen werden. Unter Ziff. 8 werden dort zur Sozialadäquanz die folgenden Ausführungen gemacht (Hervorhebungen hinzugefügt):

> Die Annahme von nach allgemeiner Auffassung nicht zu beanstandenden **geringwertigen Aufmerksamkeiten (z. B. Massenwerbeartikel wie Kugelschreiber, Kalender, Schreibblocks)** sowie den Geschenken aus dem Kreis der Mitarbeiterinnen und Mitarbeiter der Beamtin oder des Beamten (z. B. aus Anlass eines Geburtstages oder Dienstjubiläums) im herkömmlichen Umfang kann allgemein als stillschweigend genehmigt angesehen werden.
> Als stillschweigend genehmigt angesehen werden kann auch eine **übliche und angemessene Bewirtung bei allgemeinen Veranstaltungen**, an denen die Beamtin oder der Beamte im Rahmen ihres und seines Amtes, in dienstlichem Auftrag oder mit Rücksicht auf die ihr oder ihm durch das Amt auferlegten gesellschaftlichen Verpflichtungen teilnimmt, **z. B.** Einführung und Verabschiedung von Amtspersonen, offizielle Empfänge, gesellschaftliche

[39] BGH, NSZ 2006, 210.

[40] Vgl. die Auflistung bei *Fischer*, StGB, 60. Aufl. 2013, § 11 Rn 22b.

[41] Vgl. *Fischer*, StGB, 60. Aufl. 2013, § 11 Rn. 23a.

[42] Vgl. *Fischer*, StGB, 60. Aufl. 2013, § 331 Rn. 25 ff.

[43] Landesbeamtengesetz NRW.

[44] Beamtenstatusgesetz.

> Veranstaltungen, die der Pflege dienstlicher Interessen dienen, Jubiläen, Grundsteinlegungen, Richtfeste, Einweihungen, Eröffnungen von Ausstellungen, Betriebsbesichtigungen sowie **Sitzungen von Organen wirtschaftlicher Unternehmungen, an denen die öffentliche Hand beteiligt ist**.
>
> Als stillschweigend genehmigt kann auch die Teilnahme an Bewirtungen aus Anlass oder bei Gelegenheit dienstlicher Handlungen, Besprechungen, Besichtigungen oder dergleichen angesehen werden, **wenn die Bewirtungen üblich und angemessen sind und wenn sie ihren Grund in den Regeln des Verkehrs und der Höflichkeit haben, denen sich auch eine Beamtin oder ein Beamter nicht entziehen kann, ohne gegen gesellschaftliche Formen zu verstoßen.**

Geht die Geschäftsführung über das sozialadäquate Maß hinaus, kann sie sich bei schwerwiegenderen Verstößen einer Vorteilsgewährung nach § 333 StGB strafbar machen.

Eine übliche und angemessene Bewirtung kommunaler Anteilseignervertreter und Gremienmitglieder bei Gesellschafterversammlungen, Aufsichtsratssitzungen und vergleichbaren Veranstaltungen ist allerdings nach den oben aufgeführten Richtlinien grundsätzlich rechtlich unbedenklich. In Zweifelsfällen ist stets die vorherige Genehmigung der dienstvorgesetzten Stelle des Amtsträgers einzuholen.

Gleiches gilt für die Annahme von Vorteilen durch Mitarbeiter öffentlicher Unternehmen, welche nach den oben dargestellten Kriterien als Amtsträger einzustufen sind.

2.2.5 Handlungsempfehlungen zu Repräsentationsaufwendungen für die kommunale Unternehmerpraxis

- Der Geschäftsführer sollte für Maßnahmen, die nicht zweifelsfrei eine zulässige Repräsentationsaufwendung darstellen, bzw. bereits von den internen Compliance-Richtlinien gedeckt sind, stets einen Gesellschafterbeschluss einholen. So können zivilrechtliche Schadensersatzansprüche der Gesellschaft vermieden und strafrechtliche Risiken (bspw. einer Untreue gemäß § 266 StGB) verringert werden.
- Der Gesellschafterbeschluss muss rechtmäßig sein und unter Beachtung der Formanforderungen der Satzung gefasst werden. Zum Zwecke einer besseren Nachweisbarkeit sollte grundsätzlich ein schriftlicher Gesellschafterbeschluss eingeholt werden. Falls dies im konkreten Einzelfall ad hoc nicht möglich ist, sollte stets nachträglich ein schriftlicher Billigungsbeschluss eingeholt werden.
- Die Gesellschafter können, bspw. in einer internen Compliance-Richtlinie, ein jährliches Budget für Einladungen und Bewirtungen festlegen, bis zu dessen Überschreitung der Geschäftsführer nicht stets einen separaten Beschluss einholen muss. Die Höhe eines solchen Budgets sollte angesichts des kommunalrechtlichen Grundsatzes der wirtschaftlichen und sparsamen Haushaltsführung jedoch möglichst niedrig bemessen werden und die Ertragskraft des Unternehmens berücksichtigen.
- Zusätzlich kann in der Compliance-Richtlinie auch eine allgemeine Wertgrenze für Repräsentationsaufwendungen festgelegt werden. Unter Berücksichtigung der maßgeblichen Rechtsprechung und Kommentarliteratur, sollte diese Wertgrenze jedoch maximal bei 25,00 € pro Geschenk oder Bewirtung liegen.

- Persönliche Zuwendungen an kommunale Gremienvertreter, die über das sozialadäquate Maß hinausgehen, dürfen aufgrund deren Amtsträgerstellung grundsätzlich nicht erfolgen. Dies gilt unabhängig von Gesellschafterbeschlüssen und Compliance-Richtlinien, da diese eine Strafbarkeit wegen Vorteilsgewährung grundsätzlich nicht ausschließen können.

3 Besondere Compliance-Anforderungen in Beteiligungsunternehmen des Bundes

Auch öffentliche Unternehmen des Bundes oder mit Bundesbeteiligung haben neben den für alle (privaten) Gesellschaften geltenden Rechtsnormen eine große Zahl öffentlich-rechtlicher Vorschriften zu beachten. Hierunter fallen etwa das Haushaltsrecht, das Vergaberecht und ggf. das öffentliche Preisrecht.

Wie bei den öffentlichen Unternehmen im kommunalen Bereich bestehen auch bei Bundesbeteiligungen häufig widerstreitende Interessenlagen. Einerseits ist der Bund als Gesellschafter (und oft zugleich Auftraggeber) primär an der Erfüllung der öffentlichen Aufgabe interessiert, die zum Gegenstand und Zweck des Unternehmens gemacht wurde. Andererseits – insbesondere im Fall der Beteiligung gewerblicher oder industrieller Partner – existiert ein eher kaufmännisch/betriebswirtschaftlich geprägtes Interesse am Wohl des Unternehmens, das sich insbesondere im erzielten Jahresüberschuss zeigt.

Ebenso wie die kommunalen Unternehmen stehen auch die öffentlichen Unternehmen des Bundes bzw. mit Bundesbeteiligung unter verschärfter Beobachtung und Kritik der Öffentlichkeit, aber auch des Haushaltsausschusses des Deutschen Bundestages und des Bundesrechnungshofes.

Insoweit ergeben sich bei den öffentlichen Unternehmen des Bundes unter Compliance-Gesichtspunkten weitgehend dieselben Besonderheiten wie bei kommunalen Gesellschaften, so dass grundsätzlich auf die Ausführungen unter II. verwiesen werden kann. Im Folgenden sollen deshalb lediglich einige bundesspezifische Regelungen zu den oben behandelten Themenbereichen erwähnt werden.

3.1 Konflikt zwischen öffentlichem (Bundes-)Recht und Gesellschaftsrecht

Hinsichtlich der Zulässigkeit von Weisungen an vom Bund in einen Aufsichtsrat entsandte oder gewählte Vertreter und des Konfliktfeldes zwischen Verschwiegenheitspflicht und deren Lockerung gemäß § 394 AktG wird im Übrigen auf die Ausführungen zum PCGK des Bundes verwiesen (s. unten. 4.1).

3.2 Repräsentationsaufwendungen, Sponsoring, Spenden, Geschenke

Zu diesem oben bereits ausführlich abgehandelten Themenkomplex sind an dieser Stelle lediglich einige Regularien des Bundes zu erwähnen, die – soweit sie nicht unmittelbar auch für öffentliche Unternehmen des Bundes gelten – zumindest als Orientierungshilfe dienen können, was bei Bundesunternehmen zulässig ist und was nicht:

- Hier ist zunächst die Allgemeine Verwaltungsvorschrift zur Förderung der Tätigkeit des Bundes durch Leistungen Privater (Sponsoring, Spenden und sonstige Schenkungen) vom 07.07.2003[45] und die dazu ergangenen Durchführungsbestimmungen für den Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg)[46] zu nennen.
- Des Weiteren wird auf die Richtlinie der Bundesregierung zur Korruptionsprävention vom 30.07.2004 mit den (sehr anschaulichen) Anlagen „V*erhaltenskodex gegen Korruption*“ und „*Leitfaden für Vorgesetzte und Behördenleitungen*“ sowie den Empfehlungen des Bundesministeriums des Inneren[47] und auf die Durchführungsbestimmungen für den Geschäftsbereich des BMVg[48] aufmerksam gemacht, die als Hilfsmittel für die tägliche Compliance-Praxis in öffentlichen Unternehmen des Bundes herangezogen werden können.

4 Public Corporate Governance Kodex

Im Gegensatz zum Deutschen Corporate Governance Kodex für börsennotierte Aktiengesellschaften gibt es keinen einheitlichen Public Corporate Governance Kodex, der für alle öffentlichen Unternehmen gilt.

Der Bund hat für seine nicht börsennotierten Beteiligungsunternehmen am 1. Juli 2009 den Public Corporate Governance Kodex des Bundes („**PCGK**“) erlassen. Diesem Vorbild sind in der Zwischenzeit viele Kommunen gefolgt. In diesem Kreis sind nicht nur die meisten Großstädte und die Stadtstaaten zu finden, sondern zunehmend auch mittelgroße und kleine Städte. Der Trend geht klar zum kommunalen Corporate Governance Kodex.[49] Viele Kommunen orientieren sich hierbei jedoch stark am Public Corporate Governance Kodex des Bundes[50], den wir nachfolgend vorab in seinen Grundzügen darstellen.

---

[45] VMBl 2004, S. 24.

[46] VMBl 2011, S. 37.

[47] VMBl 2006, S. 19.

[48] VMBl 2006, S. 29.

[49] Einen aktuellen Überblick über bereits verabschiedete Public Corporate Governance Kodizes findet man im Internet unter www.publicgovernance.de.

[50] Vgl. bspw. den Entwurf eines Public Corporate Governance Kodex des Städte- und Gemeindebundes NRW für nordrhein-westfälische Kommunen, hierzu *Brandt-Schwabedissen*, Städte- und Gemeinderat 11/2010, S. 12.

4.1 Public Corporate Governance Kodex des Bundes

Der Public Corporate Governance Kodex des Bundes (PCGK) ist Teil A der „*Grundsätze guter Unternehmens- und Beteiligungsführung im Bereich des Bundes*“[51], der zentralen Leitlinien für die Steuerung der (nicht börsennotierten) Unternehmen mit Bundesbeteiligung.[52]

Der PCGK richtet sich primär an alle Unternehmen in der Rechtsform einer juristischen Person des Privatrechts, an denen der Bund eine Mehrheitsbeteiligung hält, so dass die Beachtung des PCGK auch durchgesetzt werden kann.[53] Die Beachtung des PCGK hat das beteiligungsführende Bundesministerium durch Verankerung im Regelwerk des Unternehmens in der Weise sicherzustellen, dass Vorstand/Geschäftsführung und Aufsichtsrat/Verwaltungsrat jährlich eine sog. **Entsprechenserklärung** abzugeben haben, in der Abweichungen von den Empfehlungen des PCGK nachvollziehbar begründet werden (entsprechend dem aktienrechtlichen Grundsatz „comply or explain“). Die Erklärung ist dauerhaft öffentlich zugänglich zu machen, etwa auf der Internetseite des Unternehmens oder im Bundesanzeiger.[54]

Leitbild für den PCGK war der für börsennotierte Unternehmen geltende Deutsche Corporate Governance Kodex (DCGK), aus welchem weite Teile wörtlich übernommen wurden.

Seine **Ziele**[55] sind,

- Unternehmensführung und Unternehmensüberwachung transparenter und nachvollziehbarer zu machen und zu deren Zusammenarbeit zu verbessern;
- die Rolle des Bundes als Anteilseigner klarer zu fassen und eine bessere und wirtschaftlichere Erfüllung der vom Bund mit der Beteiligung verfolgten Ziele zu gewährleisten;
- das Bewusstsein für eine gute Corporate Governance zu erhöhen; und
- das öffentliche Vertrauen in Unternehmen mit Bundesbeteiligung und den Bund als deren Gesellschafter zu stärken.

---

[51] Zu finden auf der Homepage des Bundesfinanzministeriums (www.bundesfinanzministerium.de) unter „Themen/Bundesvermögen/Public Corporate Governance Kodex“.

[52] Weitere Bestandteile dieses Kompendiums sind die (überarbeiteten) „Hinweise für gute Beteiligungsführung bei Bundesunternehmen“ (Teil B) sowie die „Berufungsrichtlinien“ (Teil C) für die Berufung der Mitglieder von Aufsichts- bzw. Verwaltungsräten sowie Vorständen bzw. Geschäftsführern in Unternehmen mit Bundesbeteiligung. Als Anlagen zu Teil B sind u. a. Muster/Formulierungshilfen für einen GmbH-Gesellschaftsvertrag, eine Geschäftsordnung für einen GmbH-Aufsichtsrat, eine Geschäftsordnung für die Geschäftsleitung und einen Geschäftsführeranstellungsvertrag enthalten, die auf den Regelungen des PCGK und den „Hinweisen für gute Beteiligungsführung . . . “ basieren.

[53] Bei Minderheitsbeteiligungen wird seine Beachtung empfohlen. Dies ist letztendlich allerdings nicht durchsetzbar.

[54] PCGK Ziff. 1.4.

[55] Vgl. PCGK Ziff. 1.1.

Der Kodex gibt für die bei Bundesbeteiligungen vorherrschenden Unternehmensrechtsformen GmbH und AG **verbindliche gesetzliche Bestimmungen** wieder und **national wie international anerkannte Standards** in Form von Empfehlungen und Anregungen vor:

- Von den **Empfehlungen** („soll"-Regelungen) dürfen Unternehmen zwar abweichen, müssen dies aber in der Entsprechenserklärung offenlegen.
- Von den enthaltenen **Anregungen** („sollte"-Regelungen) kann ohne Offenlegung abgewichen werden.
- Die darüber hinaus an den Text der wesentlichen Bestimmungen angehängten **Anmerkungen** sind explizit[56] (auch an der „blasseren" Schriftfarbe erkennbar) nicht Bestandteil des PCGK, sondern erläutern und verdeutlichen dessen Empfehlungen und Anregungen.

Thematisch ist der PCGK im Anschluss an die Präambel in die Kapitel *„Anteilseigner und Anteilseignerversammlung", „Zusammenwirken zwischen Geschäftsleitung und Überwachungsorgan", „Geschäftsleitung", „Überwachungsorgan", „Transparenz"* sowie *„Rechnungslegung und Abschlussprüfung"* untergliedert. Da die GmbH im Bereich der Bundesbeteiligungen die häufigste Gesellschaftsform ist, wird im Folgenden im Wesentlichen auf die GmbH-spezifischen Regelungen eingegangen.

4.1.1 Pflichten und Aufgaben von Anteilseignern und Anteilseignerversammlung

Erwähnenswert bei den Regelungen des PCGK zur Rolle des Bundes als Gesellschafter ist zunächst der in den Anmerkungen enthaltene Hinweis darauf, dass in **Unternehmen mit einer Minderheitsbeteiligung des Bundes** die **Wahrnehmung von gesetzlich normierten Minderheitsrechten zur Wahrung der Bundesinteressen** geboten sein kann.

Hinsichtlich der **Bestellung und der Abberufung von Mitgliedern der Geschäftsführung und des Aufsichtsrates** einer GmbH raten die Anmerkungen dazu, diese **Befugnisse nicht auf andere Organe zu übertragen,** soweit sie kraft Gesetzes der Gesellschafterversammlung zustehen.

Da das GmbH-Gesetz keine § 120 Abs. 2 AktG entsprechende gesetzliche **Regelung zur Entlastung der Mitglieder des Aufsichtsrates** enthält, empfehlen die Anmerkungen hier, eine solche Regelung in die Satzung der Gesellschaft aufzunehmen.

Im Zusammenhang mit den Grundlagenzuständigkeiten der Gesellschafterversammlung bei einer GmbH enthalten die Anmerkungen den Hinweis, dass der **unternehmerische Freiraum der Geschäftsführung** (auch) einer besseren und wirtschaftlicheren Erfüllung der vom Bund verfolgten Beteiligungsziele dienen soll, so dass trotz des entsprechenden in § 37 Abs. 1 GmbHG normierten Rechts zu **Einzelweisungen der Gesellschafterversammlung** an die Geschäftsführung, solche Weisungen **nicht die Regel** sein sollen.

[56] Vgl. PCGK Ziff. 1.2.

4.1.2 Zusammenwirken von Geschäftsleitung und Überwachungsorgan

In diesem Kapitel findet ein wesentliches Ziel des PCGK, die Verbesserung der Zusammenarbeit zwischen Geschäftsführung und Aufsichtsrat, seinen Niederschlag.

Grundsätze

Ziffer 3.1.1. PCGK weist auf die Verpflichtung zur **Beachtung der im Kodex festgelegten Transparenz-, Offenlegungs- und Vertraulichkeitsgebote** hin, die **Vertrauen** als Grundlage für ein enges Zusammenwirken dieser beiden Organe zum Wohle des Unternehmens **schaffen** soll.

Lediglich in den Anmerkungen zu dieser Regelung wird das für eine Bundesbeteiligung vorausgesetzte Interesse erwähnt, hierdurch bedeutsame Bundesaufgaben zu erfüllen, welches sich in Unternehmensgegenstand und Unternehmenszweck widerspiegelt. Dieses **Bundesinteresse** wird damit **zur Leitlinie der (Zusammen-) Arbeit beider Organe erhoben**.

Zustimmungsbedürftige Geschäfte

In Ziff. 3.1.2 PCGK werden die **„Geschäfte von grundlegender Bedeutung"** näher definiert, die im Gesellschaftsvertrag oder durch Entscheidung des Aufsichtsrates unter dessen Zustimmungsvorbehalt gestellt werden. In diesem Zusammenhang ist anzumerken, dass in einigen Gesellschaftsverträgen ein Teil dieser Geschäfte zusätzlich oder stattdessen unter dem Zustimmungsvorbehalt der Gesellschafterversammlung steht. Auch hier findet sich der Hinweis, dass die **Eigenverantwortlichkeit der Geschäftsführung** bei der Festlegung der zustimmungsbedürftigen Geschäfte gewährleistet bleiben muss.

Berichterstattung

Ziffer 3.1.3 PCGK beschreibt die Anforderungen an **Turnus, Aktualität und Umfang der Berichtspflicht der Geschäftsführung** an den Aufsichtsrat unter **Verweis auf** § **90 AktG**. Lediglich bei kleineren, wirtschaftlich unbedeutenderen Gesellschaften darf von dieser Regelung abgewichen werden. Gegenstand der Berichterstattung ist neben der Unternehmensplanung sowie den Abweichungen hiervon, Geschäftsentwicklung, Risikolage bzw. Risikomanagement und wirtschaftlichem Umfeld des Unternehmens auch die **Compliance**, die nach den Anmerkungen **alle Maßnahmen** umfasst, **die gewährleisten sollen, dass das Unternehmen, die Geschäftsleitung und auch die Mitarbeiter im Einklang mit Recht und Gesetz handeln**.

Als **Regelfrist für** den unbestimmten Rechtsbegriff der „rechtzeitigen" **Übersendung von Unterlagen an den Aufsichtsrat** und seine Ausschüsse werden **14 (Kalender-)Tage** vor der jeweiligen Sitzung genannt.

Hinzuweisen ist auch darauf, dass die ausreichende Versorgung des Aufsichtsrates mit Informationen eine gemeinsame Aufgabe von Geschäftsführung und Aufsichtsrat ist. Dabei hat das Überwachungsorgan auf eine rechtzeitige und ordnungsgemäße Berichterstattung der Geschäftsführung hinzuwirken. In den Anmerkungen wird in diesem Zusammenhang auf die Rechte des Aufsichtsrates zur Anforderung von Einzel-/

Sonderberichten (§ 90 Abs. 3 AktG) sowie die Einsichtnahme- und Prüfungsrechte gem. § 111 Abs. 2 AktG verwiesen.

Vertraulichkeit

Ziffer 3.2.1 PCGK unterstreicht die grundlegende Bedeutung der **offenen Diskussion** innerhalb von Geschäftsführung und Aufsichtsrat und zwischen diesen beiden Gesellschaftsorganen für eine gute Unternehmensführung. Diese Offenheit bedingt jedoch im Gegenzug die Wahrung **größtmöglicher Vertraulichkeit** über die Inhalte der Diskussionen.

Zur Problematik des Spannungsfeldes zwischen der Verschwiegenheitspflicht von Aufsichtsratsmitgliedern einerseits und bestehenden Berichtspflichten gegenüber der entsendenden Gebietskörperschaft andererseits wird auf die oben gemachten Ausführungen für den kommunalen Bereich verwiesen.[57]

Für den Bereich der Gesellschaften mit Bundesbeteiligung stellen die „*Hinweise für gute Beteiligungsführung bei Bundesunternehmen*" das Erfordernis von schriftlichen Abreden mit den auf Veranlassung des Bundes in das Gremium entsandten oder gewählten Mitgliedern dar.[58] Mit diesen Erklärungen[59] verpflichten sich die künftigen Aufsichtsratsmitglieder u. a. dazu, „*neben den Gesellschaftsinteressen auch die besonderen Interessen des Bundes zu berücksichtigen und die erforderlichen Berichte unverzüglich nach den jeweiligen Sitzungen dem Beteiligungsreferat zuzuleiten.*"

Beamtinnen und Beamten des Bundes, für die sich eine Berichtspflicht i. S. d. § 394 AktG aus der Folgepflicht des § 62 Bundesbeamtengesetz herleiten lässt, wird in Rn. 76 der Hinweise für gute Beteiligungsführung explizit erläutert, dass sie „*im Außenverhältnis*" Weisungen der entsendenden Dienststelle nicht zu folgen haben, wenn sie damit dem Unternehmenswohl zuwider handeln und folglich gegen ihre Pflichten als Aufsichtsratsmitglied verstoßen oder wenn sie sich durch Befolgen der Weisung strafbar machen würden.

Verantwortlichkeit

Geschäftsführung und Aufsichtsrat haben grundsätzlich die Regeln ordnungsgemäßer Unternehmensführung zu beachten und haften bei schuldhafter Verletzung ihrer daraus erwachsenen Pflichten dem Unternehmen auf Schadensersatz (Ziff. 3.3.1 PCGK). Die Anmerkungen erläutern, dass zu den vorgenannten Regeln auch die aktuellen betriebswirtschaftlichen Erkenntnisse und Erfahrungen im Bereich der Unternehmensführung und -überwachung sowie die Grundsätze des PCGK gehören.

Unter Ziff. 3.3.2 PCGK wird die mit dem Gesetz zur Angemessenheit der Vorstandsvergütung in § 93 Abs. 2 Satz 3 AktG eingeflossene Regelung zum **Mindestselbstbehalt**

---

[57] S. o. 2.1.2.

[58] Siehe dort Rn. 75 ff.

[59] Muster siehe Anlagen 1 und 2 zu den „Berufungsrichtlinien".

beim Abschluss einer Vermögenshaftpflichtversicherung für Geschäftsführungs- und Aufsichtsratsmitglieder (sog. **D&O-Versicherung**) wiedergegeben, die grundsätzlich nur für den Bereich der AG verbindlich ist. Durch die Aufnahme einer entsprechenden Anwendungsempfehlung wird sie jedoch auch für Unternehmen in anderer Rechtsform zum Grundsatz erhoben. Da die Satzungen der Bundesgesellschaften, die Anstellungsverträge der Geschäftsführer und die D&O-Versicherungsverträge bis 2009 keine Selbstbehalt-Regelungen enthielten, wird diese Empfehlung wohl nur nach und nach umgesetzt werden, nämlich wenn Satzungsänderungen anstehen und Geschäftsführerverträge neu abgeschlossen oder verlängert werden. Für Aufsichtsräte in öffentlichen Unternehmen ist in vielen Fällen die Festlegung eines Selbstbehalts in der D&O-Versicherung nicht geboten, weil sie keine Vergütung für ihre Aufsichtsratstätigkeit erhalten, sondern lediglich einen Aufwendungsersatz.

Kreditgewährung

Zur Vermeidung von Interessenkonflikten empfiehlt Ziff. 3.4 PCGK den Unternehmen, grundsätzlich **keine Kredite an Mitglieder der Geschäftsführung oder des Aufsichtsrats** sowie deren Angehörige zu geben. Hier geht der PCGK sogar über die entsprechende Regelung des DCGK hinaus, der eine Kreditgewährung mit Zustimmung des Aufsichtsrates zulässt.[60]

4.1.3 Geschäftsleitung

Aufgaben und Zuständigkeiten

Unter Ziff. 4.1 legt der PCGK zunächst dar, dass die **Geschäftsführung** auf der Grundlage ihrer **originären Verantwortung für die** an Unternehmensgegenstand und –zweck gebundene **Leitung des Unternehmens** die strategische Ausrichtung des Unternehmens entwickelt, mit dem Aufsichtsrat abstimmt und für ihre Umsetzung sorgt. Die Anmerkungen weisen darauf hin, dass – anders als beim Vorstand einer AG – den Geschäftsführern einer GmbH Weisungen erteilt werden können. Neben der Zulässigkeit von Gesellschafterweisungen – wovon, wie oben bereits ausgeführt[61], nur unter Beachtung des unternehmerischen Freiraums der Geschäftsführung Gebrauch gemacht werden sollte – wird auch die Möglichkeit erwähnt, in der Satzung festzulegen, dass auch der Aufsichtsrat der Geschäftsführung gegenüber zur Erteilung von Weisungen berechtigt werden kann. Auch insoweit empfehlen die Anmerkungen jedoch, im Interesse der klaren Trennung der Verantwortlichkeiten zwischen Geschäftsführung und Überwachungsorgan, eher einen Zustimmungsvorbehalt für den Aufsichtsrat zu installieren.

Weiterhin werden in diesem Kapitel die grundsätzliche Compliance-Verantwortung der Geschäftsführung sowie ihre Verpflichtung zur Schaffung eines angemessenen Risikomanagements und -controllings festgeschrieben. Die Einrichtung eines Überwachungssystems i. S. v. § 91 Abs. 2 AktG zur frühzeitigen Erkennung bestandsgefährdender

[60] S. Ziff. 3.9 DCGK (www.corporate-governance-code.de).

[61] S. o. Ziff. 4.1.1.

Risiken wird in den Anmerkungen wegen seiner großen Bedeutung für alle Unternehmen mit Bundesbeteiligung (unabhängig von ihrer Rechtsform) für verpflichtend erklärt.

Zusammensetzung

Hinsichtlich der Zusammensetzung der Geschäftsführung betont Ziff. 4.2 PCGK die Bedeutung des „Vier-Augen-Prinzips", das auch bei Gesellschaften, die ausnahmsweise nur einen Geschäftsführer haben, durch geeignete Maßnahmen sicherzustellen ist.

Vergütung

In Bezug auf die Vergütung entspricht Ziff. 4.3 PCGK den Bestimmungen des Gesetzes über die angemessene Vorstandsvergütung (VorstAG) vom 31.07.2009[62], das neben der Festlegung und Überprüfung der Vorstandsvergütung durch den Aufsichtsrat u. a. die Nachhaltigkeit und die Ausgestaltung als Bonus-Malus-System bei variablen Gehaltsbestandteilen, die Begrenzung von Zahlungen an vorzeitig ausscheidende Vorstandsmitglieder und die Pflicht zur detaillierten Veröffentlichung von Vorstandsgehältern zum Gegenstand hat. Auch in diesem Zusammenhang ist darauf hinzuweisen, dass diese Regelungen aufgrund der Laufzeit bestehender Geschäftsführerverträge erst umgesetzt werden kann, wenn diese Verträge verlängert oder neu abgeschlossen werden bzw. wenn sich der betreffende Geschäftsführer freiwillig den neuen Bestimmungen unterwirft.

Interessenkonflikte

Zu diesem Stichwort wird in Ziff. 4.4. PCGK neben der Verpflichtung der Geschäftsführung gegenüber dem Unternehmenszweck das umfassende Wettbewerbsverbot für die Geschäftsführung, das Verbot der Vorteilsgewährung oder –annahme bzw. des Forderns von Vorteilen im Zusammenhang mit ihrer Tätigkeit sowie das Verbot des Verfolgens eigener Interessen bei seinen Entscheidungen dargestellt.

Gemäß Ziff. 4.4.3 PCGK ist jeder Geschäftsführer verpflichtet, Interessenkonflikte unverzüglich dem Aufsichtsrat und den anderen Geschäftsführern zu offenbaren.

Geschäfte zwischen Unternehmen und Geschäftsführern bzw. deren Angehörigen (wer zum Kreis dieser Angehörigen gehört, ist in § 138 Abs. 1 Insolvenzordnung definiert) müssen branchenüblichen Standards entsprechen, wesentliche Geschäfte dieser Art bedürfen darüber hinaus der Zustimmung des Aufsichtsrates. Die Anmerkungen stufen solche Geschäfte generell als bedenklich ein und empfehlen deshalb, sie zu unterlassen.

Um Interessenkonflikten im Zusammenhang mit Nebentätigkeiten bereits im Vorfeld entgegen zu wirken, empfehlen die Anmerkungen, die Rahmenbedingungen hierzu mit den Geschäftsführern vertraglich zu regeln. Darüber hinaus bedürfen ihre Nebentätigkeiten der Zustimmung des Aufsichtsrates.

[62] BGBl I, S. 2509.

4.1.4 Überwachungsorgan

Die Bestimmungen des Kodex zum Überwachungsorgan (Ziff. 5 PCGK), in der Regel ein Aufsichtsrat, haben einen erheblichen Umfang und unterstreichen damit die Bedeutung dieses Organs für ein Bundesunternehmen.

Aufgaben und Zuständigkeiten

Hier wird zunächst die zentrale Aufgabe des Aufsichtsrates, die Beratung und Überwachung der Geschäftsführung bei der Unternehmensführung, näher definiert, beschrieben und erläutert und dem Aufsichtsrat und seinen Ausschüssen eine regelmäßige Effizienzprüfung empfohlen (Ziff. 5.1.1 PCGK).

Die Erläuterungen stellen darüber hinaus klar, dass bei einer GmbH ohne Aufsichtsrat die Gesellschafter gem. § 46 Nr. 6 GmbHG für die Überwachung der Geschäftsführung verantwortlich sind und allein die Bestellung eines Aufsichtsrates die Gesellschafter nicht von einer solchen Überwachungspflicht befreit.

Ziffer 5.1.2 PCGK befasst sich mit der Bestellung der Geschäftsführungsmitglieder, die bei Erstbestellung nicht länger als drei Jahre, bei Wiederbestellung nicht länger als fünf Jahre dauern soll.

Die Anmerkungen stellen klar, dass bei einer GmbH (soweit nicht das Mitbestimmungsgesetz greift) das Recht zur Bestellung und Anstellung von Geschäftsführern grundsätzlich nicht – wie bei der AG – beim Aufsichtsrat liegt, sondern gem. § 46 Nr. 5 GmbHG der Gesellschafterversammlung zusteht. Soweit diese Rechte gem. §§ 45, 52 GmbHG per Satzung dem Aufsichtsrat übertragen werden, soll die Entscheidung dem Plenum und nicht einem Ausschuss vorbehalten bleiben.

Für den Fall des Widerrufs einer Geschäftsführerbestellung, die bei einer GmbH unbeschadet etwaiger Ansprüche aus dem Anstellungsvertrag jederzeit möglich ist (§ 38 Abs. 1 GmbHG), regen die Anmerkungen an, dass wegen der Zweiwochenfrist des § 626 Abs. 2 BGB dann auch unverzüglich die Möglichkeit einer Beendigung des Anstellungsvertrages zu prüfen ist. Gerade wegen der oft zeitaufwändigen Abstimmungs- und Mitzeichnungserfordernisse auf Seiten des Bundes als Gesellschafter ist dies ein wichtiger Hinweis.

Ziffer 5.1.3–5.1.8 PCGK enthalten Regelungen in Bezug auf die innere Ordnung des Aufsichtsrates. Hinsichtlich der Umsetzung dieser Regelungen ist zunächst auf die als Anhang zu den Hinweisen für gute Beteiligungsführung abgedruckten §§ 8 – 11 des Muster-Gesellschaftsvertrages (Anlage 2) sowie auf das Muster einer Geschäftsordnung für Aufsichtsräte (Anlage 3) zu verweisen.

Ergänzend dazu ist zu erwähnen, dass gem. Ziff. 5.1.4 PCGK weder dem Vorsitzenden noch anderen Einzelmitgliedern des Aufsichtsrates das Recht eingeräumt werden soll, allein anstelle des Plenums zu entscheiden.

Weiter wird angemerkt, dass die Einrichtung eines Prüfungsausschusses (vgl. Ziff. 5.1.7 PCGK) wegen seiner besonderen Bedeutung auch bei Unternehmen gerechtfertigt sein kann, bei denen aufgrund der Größe des Aufsichtsrates eine Ausschussbildung ansonsten nicht geboten ist.

Zusammensetzung
Im Hinblick auf die Zusammensetzung des Aufsichtsrates unterstreicht Ziff. 5.2.1 PCGK die Notwendigkeit einer ausreichenden persönlichen und fachlichen Qualifikation sowie der für die Wahrnehmung des Mandats notwendigen terminlichen Freiräume. Insoweit ist die Beschränkung auf in der Regel nicht mehr als drei Aufsichtsratsmandate zu beachten sowie die Pflicht, im Bericht des Aufsichtsrates zu erwähnen, wenn ein Mitglied an weniger als der Hälfte der Sitzungen eines Geschäftsjahres in vollem Umfang teilgenommen hat.

Die ebenfalls geforderte gleichberechtigte Berücksichtigung von Frauen wird für vom Bund zu besetzende Mandate durch das Bundesgremienbesetzungsgesetz v. 24.06.1994 (BGBl I S. 1406, 1413) umgesetzt.

Vergütung
In Bezug auf die durch den Gesellschaftsvertrag oder die Gesellschafterversammlung festzulegende Aufsichtsratsvergütung erläutern die Anmerkungen, dass sich deren Höhe nach der wirtschaftlichen Bedeutung und Lage der Gesellschaft, der erforderlichen Qualifikation, dem zeitlichen Aufwand sowie den mit dem Mandat verbundenen Risiken richtet und – wie auch die Geschäftsführervergütung – regelmäßig auf Angemessenheit zu überprüfen ist.

Interessenkonflikte
Auch Aufsichtsratsmitglieder sind dem Unternehmenszweck verpflichtet und dürfen bei ihren Entscheidungen keinerlei eigene Interessen verfolgen (Ziff. 5.4 PCGK). Der PCGK konforme Umgang mit Interessenkonflikten der Aufsichtsratsmitglieder findet seinen Niederschlag etwa in den Regelungen des § 10 Abs. 4 des Muster-Gesellschaftsvertrages sowie des § 4 Abs. 4–6 der Muster-Geschäftsordnung für Aufsichtsräte. Die Anmerkungen stellen dem gegenüber klar, dass allein die Möglichkeit künftiger Interessenkonflikte einer Bestellung zum Aufsichtsrat nicht entgegensteht.

4.1.5 Transparenz
Kapitel 6 des PCGK enthält die Bestimmungen für den Inhalt und die Veröffentlichung des von Geschäftsführung und Aufsichtsrat gemeinsam jährlich zu erstattenden Corporate Governance Berichts, der neben der Entsprechenserklärung zum PCGK insbesondere die individualisierte und aufgeschlüsselte Vergütung der Geschäftsführer (soweit aufgrund Einverständniserklärung oder vertraglicher Vereinbarung zulässig) und Aufsichtsratsmitglieder zu enthalten hat (vgl. auch § 16 des Muster-Gesellschaftsvertrages).

4.1.6 Rechnungslegung und Abschlussprüfung
Das letzte Kapitel des PCGK (Ziff. 7.) befasst sich mit dem Jahresabschluss der Unternehmen mit Bundesbeteiligung und dessen Prüfung, die gem. § 65 Abs. 1 BHO in entsprechender Anwendung der für große Handelsgesellschaften geltenden Vorschriften des Dritten Buches des HGB zu erfolgen haben. Dies ist durch eine entsprechende Regelung im Gesellschaftsvertrag vorzusehen (s. § 15 Muster-Gesellschaftsvertrag). Im

Jahresabschluss ist ebenfalls die aufgeschlüsselte Vergütung der einzelnen Mitglieder der Geschäftsführung und des Aufsichtsrates auszuweisen.

Im Zusammenhang mit der Wahl bzw. Bestellung des Abschlussprüfers ist darauf zu achten, dass diese so rechtzeitig in die Wege geleitet wird, dass der Beteiligungsführung genügend Zeit bleibt, um das gemäß § 68 Abs. 1 Satz 2 BHO erforderliche Einvernehmen des Bundesrechnungshofes herbeizuführen (s. Anmerkungen zu Ziff. 7.2.2 PCGK).

Vor der Wahl bzw. Bestellung des Abschlussprüfers durch den Gesellschafter und der Beauftragung durch den Vorsitzenden des Aufsichtsrates hat dieser die in Ziff. 7.2.1 PCGK näher beschriebene Unabhängigkeitserklärung abzugeben. Ferner soll mit dem Abschlussprüfer gemäß Ziff. 7.2.3 PCGK vereinbart werden, dass er den Aufsichtsrat über wesentliche Feststellungen und Vorkommnisse im Verlauf der Prüfung unverzüglich unterrichtet sowie eine festgestellte Unrichtigkeit der Entsprechenserklärung zum PCGK ebenfalls berichtet oder in seinem Abschlussbericht vermerkt.

4.2 Kommunale Corporate Governance Kodizes

Für die Kommunen in Nordrhein-Westfalen hat eine Arbeitsgruppe der kommunalen Spitzenverbände gemeinsam mit Vertretern der zuständigen Landesministerien im Jahr 2010 Regelungen für einen nordrhein-westfälischen Public Corporate Governance Kodex erarbeitet („**PCGK NRW**“).[63] Er sieht vor, dass Geschäftsführung und Aufsichtsrat des öffentlichen Unternehmens einmal jährlich eine Entsprechenserklärung gegenüber der Verwaltung der Kommune abgeben und hierin etwaige Abweichungen vom PCGK NRW erläutern. Dies entspricht dem aus dem Aktienrecht bekannten Prinzip des „comply or explain“. Um die Einhaltung der Kodexvorgaben zu sichern, empfiehlt der Städte- und Gemeindebund NRW, den PCGK im jeweiligen Stadt- oder Gemeinderat beschließen zu lassen und die Verwaltung dazu anzuweisen, die Umsetzung des Kodex in allen kommunalen Beteiligungsgesellschaften sicherzustellen. Soweit möglich sollen hierzu die Gesellschaftsverträge und Geschäftsordnungen angepasst werden.[64]

Der PCGK NRW orientiert sich an der in kommunalen Beteiligungsunternehmen vorherrschenden Rechtsform der GmbH mit fakultativem Aufsichtsrat und wird deshalb nachfolgend als für die meisten kommunalen Unternehmen anwendbares Muster vorgestellt. Der PCGK NRW differenziert grundsätzlich nach Pflichten und Aufgaben der Gesellschafter, des Aufsichtsrates und der Geschäftsführung.

4.2.1 Pflichten und Aufgaben der Gesellschafter

Der PCGK NRW sieht zur Transparenzsteigerung vor, dass die Jahresabschlüsse der von der Kommune beherrschten Unternehmen bereits vor ihrer Feststellung in der Gesellschafterversammlung in einer öffentlichen Ratssitzung beraten werden sollen. Sofern das

[63] Vgl. *Brandt-Schwabedissen*, Städte- und Gemeinderat 11/2010, S. 12.

[64] Vgl. *Brandt-Schwabedissen*, a. a. O., S. 13.

beherrschte Unternehmen Verlustabdeckungsleistungen der Kommune erhält, soll auch der Wirtschaftsplan vorab im Rat erörtert werden.

Die Unternehmensdarstellungen im städtischen Beteiligungsbericht sollen gemäß Ziff. 1.4.3 PCGK NRW in angemessener Form (bspw. auf der kommunalen Homepage) im Internet veröffentlicht werden.

4.2.2 Pflichten und Aufgaben des Aufsichtsrats

Sach- und Fachkompetenz der Aufsichtsratsmitglieder

Für von der Kommune entsandte Aufsichtsratsmitglieder gelten grundsätzlich dieselben Anforderungen an die persönliche Sach- und Fachkompetenz der Organmitglieder, wie in privatwirtschaftlichen Unternehmen. Die Entsendung der Aufsichtsratsmitglieder sollte deshalb nicht anhand ihrer Funktionen oder Ämter (bspw. alle Fraktionsvorsitzenden), sondern allein nach ihrer fachlichen Qualifikation erfolgen. Das entspricht nicht nur dem kommunalen Interesse an einer möglichst effizienten Kontrolle der Beteiligungsgesellschaft durch den Aufsichtsrat, sondern schützt auch die entsandten Aufsichtsratsmitglieder selbst.

Interessenkonflikte

Der PCGK NRW stellt ausdrücklich klar, dass kein Aufsichtsratsmitglied bei seinen Entscheidungen persönliche Interessen verfolgen darf und stets die besonderen Interessen der Kommune berücksichtigen soll (Ziff. 2.9.1 und 2.9.2). Besteht ein Interessenkonflikt des Aufsichtsratsmitglieds, ist dieser dem Aufsichtsrat umgehend offenzulegen. Der Aufsichtsrat soll die Gesellschafterversammlung in einem Bericht über die aufgetretenen Interessenkonflikte und ihre Behandlung informieren.

Darüber hinaus soll die Gesellschaft keine Dienst- oder Werkverträge mit aktuellen und ehemaligen (binnen drei Jahren ab Mandatsende) Aufsichtsratsmitgliedern oder deren Angehörigen abschließen. Liegt ein wichtiger Grund für den Vertragsabschluss vor, kann dieser ausnahmsweise erfolgen, wenn zuvor das Aufsichtsratsplenum zustimmt (Ziff. 2.9.3 und 2.9.4 PCGK NRW).

Vertraulichkeit

Der Aufsichtsrat kann seine Aufgaben nur dann effektiv erfüllen, wenn er vertrauensvoll mit der Geschäftsführung zusammenarbeitet und von dieser zeitnah und umfangreich informiert wird. Eine vertrauensvolle Zusammenarbeit zwischen Geschäftsführung und Aufsichtsrat setzt voraus, dass insbesondere die von der Kommune entsandten Aufsichtsratsmitglieder ihre gesetzlichen Verschwiegenheitspflichten einhalten und nur an den jeweiligen Stadt- und Gemeinderat berichten. Auch bei aufsichtsratsinternen Beratungen ist das notwendige Maß an Offenheit und Kooperation nur gesichert, wenn die Aufsichtsratsmitglieder nicht befürchten müssen, dass ihre im Vertrauen gemachten Aussagen umgehend ihren Weg in die Öffentlichkeit finden.

Ziffer 2.10 PCGK NRW betont deshalb, dass die Aufsichtsratsmitglieder an Dritte nur in Ausnahmefällen und nur dann berichten dürfen, wenn die Vertraulichkeit gewahrt ist.

Speziell das „*Durchstecken*“ von vertraulichen Informationen an Pressevertreter aus politischen Erwägungen oder ein öffentlicher Wahlkampf anhand von im Aufsichtsrat gewonnenen Informationen sollten deshalb zwingend unterlassen werden. Die Aufsichtsratsmitglieder werden von der Kommune allein zur Wahrung der kommunalen Interessen entsandt und nicht zur Munitionierung mit Informationen für politische Auseinandersetzungen.

4.2.3 Pflichten und Aufgaben der Geschäftsführung

Die Mitglieder der Geschäftsführung sind dem Unternehmensinteresse verpflichtet und dürfen bei ihren Entscheidungen keine persönlichen Interessen verfolgen (Ziff. 3.4.3 PCGK NRW). Anders als bei den Aufsichtsratsmitgliedern (Ziff. 2.9.1 PCGK NRW) ist die Geschäftsführung nicht dazu verpflichtet, die besonderen Interessen der Kommune zu verfolgen. Dies gilt insbesondere bei öffentlichen Unternehmen, an denen neben der Kommune auch noch private Gesellschafter beteiligt sind.

Interessenkonflikte der Geschäftsführer sind ebenso zu behandeln, wie bei Aufsichtsratsmitgliedern (s. o.). In Ziff. 3.4.2. PCGK NRW wird nochmals die gesetzliche Verpflichtung der Geschäftsführung klargestellt, weder Dritten ungerechtfertigte Vorteile zu gewähren noch Zuwendungen oder sonstige Vorteile von Dritten zu fordern.

Aspekte einer Korruptionsprävention

André Große Vorholt

Inhaltsverzeichnis

Zusammenfassung

In den vergangenen 10 Jahren haben sich die Maßnahmen zur Korruptionsbekämpfung im Unternehmen zunehmend professionalisiert. Die Entwicklung in diesem Bereich wird mutmaßlich anhalten. NGOs, gesetzlich wie TI, gesetzliche Maßnahmen wie der BBA und vor allem das in den Unternehmen zunehmend steigende Bewusstsein über die Bedeutung, die Notwendigkeit und die Berechtigung einer effektiven Korrupti-

A. Große Vorholt (✉)
Karlstraße 10–12, 80333 München, Deutschland
E-Mail: andre.groszevorholt@luther-lawfirm.com

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2_14, © Springer Fachmedien Wiesbaden 2013

onsbekämpfung, steigt. Die Entwicklung einzelner Maßnahmen wie die Aufnahme korruptionsverhütender Vertragsinhalte, Prüfprogramme und personalpolitische Steuerungsmaßnahmen wird vermutlich weiter dynamisch bleiben und auch für die Zukunft die Entwicklung neuer Steuerungsmittel erwarten lassen.

1 Einleitung

Korruptionsbekämpfung steht fast immer im Mittelpunkt der Compliance-Bestrebungen der großen Mehrzahl der Unternehmen.

In seiner Bedeutung für die unternehmensinterne Compliance wird dieser Bereich wohl nur von branchenspezifischen Risikobereichen (wie z. B. Geldwäschebekämpfung im Bereich von Banken und Projektentwicklern oder Spezialrisiken wie FSK-Beschränkungen im Medienbereich o. ä.) und der Anti-Kartell-Compliance erreicht.

Dieser Befund hat gute Gründe: Ein Blick in die aktuelle Wirtschaftspresse zeigt, dass Korruptionsprobleme sich keineswegs nur in der Vergangenheit vollständig oder weitgehend abgeschlossene Fälle wie die Siemens-Verfahren, Ferrostaal oder den EvoBus-Skandal beschränken. Vielmehr belegen u. a. aktuelle Berichte über Verdachtsfälle bei der BayernLB, EADS, angeblich korruptive Zuwendungen an Kassenärzte oder im Zusammenhang mit dem Bezug von Arzneimitteln oder mit Organtransplantationen, dass der Handlungsbedarf für Unternehmen unverändert hoch ist – und sei es nur, um sich und die eigenen Mitarbeiter vor (ggf. unberechtigten) Verdachtsmomenten wirksam zu schützen.

Neben der eigentlichen strafrechtlichen Sanktionierung haben Korruptionsfälle auch erhebliche vorstrafrechtliche Konsequenzen, die die Unternehmen nicht selten härter treffen als die unmittelbaren strafverfahrensrechtlichen Sanktionen wie Geldbußen oder Verfallsanordnungen. Neben diesen Sanktionen drohen den Unternehmen Gewerberegistereinträge, Vergabesperren, der Entzug von eine besondere Zuverlässigkeit voraussetzenden Befugnis (etwa im Außenwirtschaftsrecht) und ähnliche Sanktionen.

Zunehmend macht sich auch bemerkbar, dass die Compliance-Bemühungen der letzten Jahre dazu geführt haben, dass die Unternehmen sich auch vor (vermeintlich) unzuverlässigen Geschäftspartnern schützen wollen um nicht direkt oder mittelbar für Rechtsverletzungen von Geschäftspartnern einstehen zu müssen. Da Unternehmen zunehmend dazu übergehen, als „non-compliant" eingestufte Geschäftspartner zu meiden, droht insbesondere kleinen und mittelständischen Unternehmen der Verlust von bestehenden oder möglichen Geschäftsbeziehungen[1].

[1] So enthalten etwa zahlreiche Fragebögen im Rahmen von Vertragspartnerprüfungen die Frage nach „Auffälligkeiten" bei bestehenden und insbesondere bei neuen Geschäftspartnern. Erscheint ein Vertragspartner im Rahmen einer solchen Prüfung als „vorbelastet", wird der Geschäftskontakt mit ihm u. U. alleine aus diesem Grund nicht fortgeführt.

Schließlich: Da Korruptionstaten ihren Charakter als Kavaliersdelikt verloren haben – wenn sie ihn denn je hatten –, ist die Beschädigung des guten Rufes und der Marke der betroffenen Unternehmen ist eine so unvermeidliche wie ihn vielen Fällen in wirtschaftlicher Hinsicht schmerzhafte Konsequenz von Korruptionsfällen.

Diese Entwicklung wird sich fortsetzen: NGOs, allen voran Transparency International („TI"), sind – trotz der offensichtlichen Schwächen, die ihren Bewertungsmethoden immanent sind, eine feste Größe in der öffentlichen Wahrnehmung geworden. Sie können – trotz mancher Defizite, die ihre Analysen und ihre Facharbeit im Einzelfall aufweisen mag – für sich in Anspruch nehmen, die Bedeutung einer wirksamen Anti-Korruptions-Compliance in das Bewusstsein der Öffentlichkeit gebracht zu haben. Sie bestimmen über die öffentliche Meinung und eigene Beiträge die Compliance-Programme von Unternehmen aktiv mit[2]. Die durch diese NGOs initiierte öffentliche Diskussion wird auch zunehmend qualifiziert und nüchtern geführt – hat aber nichts an ihrer Intesität verloren und übt erheblichen Druck auf Unternehmen aus, die sich gegen Vorwürfe korruptiver Verhaltensweisen ihrer Mitarbeiter wehren müssen.

Dieser Druck macht vor den Entscheidungsträgern selbst nicht halt. Darauf, dass Korruptionsdelikte im vermeintlichen „Interesse des Unternehmens" begangen werden, sie also gleichsam einen altruistischen Charakter haben, kann sich niemand (mehr) berufen. Manager, Geschäftsführer und Vorstände, die sich wenigstens einigermaßen schlüssigen und „harten" Verdachtsmomenten ausgesetzt sehen, sind in der Wirtschaftspraxis selbst ohne eine gerichtliche Verurteilung immer schwerer zu halten. Selbst Ikonen ihrer jeweiligen Märkte wie etwa die Formel 1-Legende Bernie Ecclestone scheinen in Ansehung des Drucks, die die Compliance-Officer der Automobilhersteller, die in der Formel 1-Rennserie beteiligt sind, ausüben, möglicherweise nicht mehr haltbar zu sein, sollte eine Anklage gegen ihn zugelassen werden[3]. Die persönlichen Konsequenzen für Manager beschränken sich freilich nicht auf die – gestiegenen – eigenen Strafbarkeitsrisiken[4] oder den Verlust ihrer unternehmensinternen Position: Unternehmen waren und sind rechtlich verpflichtet, Schadensersatzansprüche, die ihnen im Zusammenhang mit strafrechtlichen Verfehlungen ihrer Mitarbeiter zustehen, auch durchzusetzen[5]. Die Tatsache, dass derart gravierende persönliche Konsequenzen drohen, sorgt zusätzlich dafür, dass die wirksame Umsetzung von Anti-Korruptionsmaßnahmen in Unternehmen durch Führungskräfte als wichtige eigene Aufgabe verstanden wird.

---

[2] Am Beispiel des Corruption Perception Index („CPI") von TI: Der CPI dürfte aktiv in das Compliance-Programm wohl nahezu jedes international agierenden Unternehmens integriert sein und als Orientierungshilfe für die Intensität der jeweils zu wählenden lokalen Anti-Korruptionsmaßnahmen dienen.

[3] So etwa Sport Bild vom 30. Dezember 2012.

[4] Vgl. hierzu etwa BGH NJW 2009, 3137 „Compliance-Officer".

[5] Vgl. BGHZ 135, 244– „ARAG/Garmenbeck"; vgl. hierzu Große Vorholt, Wirtschaftsstrafrecht, 2. Aufl., S. 125 ff. m. w. N.

In der Unternehmenspraxis hat die Korruptionsbekämpfung in den letzten Jahren erhebliche Fortschritte gemacht. Dies gilt nicht nur in Großunternehmen und keineswegs nur bei Unternehmen, die der vermeintlich „scharfen" Überwachung durch die Securities Exchange Commission („SEC") unterliegen. Auch von der SEC nicht betroffene mittelständische Unternehmen haben erkannt, dass und wie wichtig eine wirksame Anti-Korruptionsbekämpfung – in ihrem eigenen Interesse – geworden ist. Unternehmen aller Größenordnungen gehen daher inzwischen dazu über, auf ihre Größe und ihr Risikoprofil angemessene Anti-Korruptionsprogramme zu entwickeln und zu implementieren[6].

2 Zentrale Korruptionsstraftatbestände aus Unternehmenssicht

Die nachstehende Darstellung der aus Unternehmenssicht relevanten Korruptionsstraftatbestände beschränkt sich, der Zielsetzung des Beitrages entsprechend, auf zentrale Aspekte des durch Unternehmen zu beachtenden Rechtsrahmens. Im Rahmen der Umsetzung der Compliance-Organisation des jeweiligen Unternehmens ist eine genaue Bestimmung des durch das Unternehmen zu beachtenden Rechtsrahmens und der im jeweiligen Einzelfall bestehenden Risikobereiche unabdingbar[7].

Bereits in geographischer Hinsicht ist naturgemäß zu prüfen, ob ausländische Rechtsordnungen möglicherweise einen Anwendungsanspruch erheben[8].

Darüber hinaus wird gerade im Zusammenhang mit Korruptionsdelikten häufig unterschätzt, dass und in welchem Umfang durch jeweils anwendbaren Rechtsrahmen auch Begleitdelikte zu Korruptionsstraftatbeständen verwirklicht werden können. So sorgen beispielsweise „kick-back-Vereinbarungen" bzw. „finders fee" -Vereinbarungen in einigen Branchen für schwierige juristische Probleme und strafrechtliche Risiken für die jeweiligen Entscheidungsträger: So ist etwa verkammerten Berufen wie Steuerberatern, Rechtsanwälten oder Ärzten durch ihre jeweiligen Berufsordnungen[9] standesrechtlich untersagt, für die Vermittlung von Mandaten bzw. Aufträgen Honorare zu entrichten oder anzunehmen. Diese berufsrechtlichen Untersagungen entsprechen zudem der in diesen Fällen regelmäßig anwendbaren Wertung des § 675 BGB, der normiert, dass im Zusammenhang mit dem Auftrag erlangte Vorteile an den Geschäftsherren herauszugeben sind. Werden derartige Vorteile verschwiegen, kommt eine Strafbarkeit der Beteiligten etwa wegen Betruges oder Untreue selbst dann in Betracht, wenn Korruptionsstraftatbe-

[6] Vgl. zu den insoweit sinnvollen und gebotenen Schritten grundlegend Moosmayer, Compliance, 2. Aufl. 2012.

[7] Vgl. Moosmayer, Fn. 5.

[8] Dies kann sehr schnell der Fall sein. Das deutsche Recht (vgl. §§ 3, 9, 12 StGB) lässt es bereits ausreichen, wenn ein Teilakt der tatbestandsmäßigen Handlung einen Inlandsbezug aufweist. Das britische Recht lässt sogar substantielle geschäftliche Aktivitäten auf britischem Boden ausreichen.

[9] Vgl. etwa § 49b Abs. 3 BRAO für Rechtsanwälte bzw. § 2 Abs. 3 BerufsO Stb.

stände aus Rechtsgründen nicht verwirklicht sind[10]. Vergleichbare Probleme stellen sich aber – für die Verkehrsteilnehmer nicht selten überraschend – durchaus auch in anderen Wirtschaftsbereichen[11].

2.1 Deutsches Recht

2.1.1 Korruption im Inland

Die „klassischen" Korruptionsstraftatbestände des deutschen Rechtes beziehen sich auf korruptive Zuwendungen an Amtsträger und Richter (§§ 331 ff. StGB) bzw. auf korruptive Zuwendungen im geschäftlichen Verkehr (§§ 299 ff. StGB)[12].

In diesen Straftatbeständen wird die strafrechtlich relevante Zuwendung von Vorteilen an die genannten Adressatenkreise unter Strafe gestellt. Der Vorteilsbegriff des deutschen Rechts ist dabei denkbar weit. Unter einem Vorteil wird grundsätzlich jede Zuwendung oder Leistung verstanden, auf die der Empfänger keinen rechtlichen Anspruch hat und die seine wirtschaftliche, rechtliche oder auch nur persönliche Lage objektiv verbessert[13].

Von wenigen, für die Praxis irrelevanten, Fallkonstellationen abgesehen sind zudem diese wie auch die sonstigen Straftatbestände des deutschen Rechtes Spiegelbilddelikte. Hieraus folgt, dass strafbar stets sowohl derjenige Beteiligte ist (aktive Korruption), der eine korruptive Zuwendung anbietet, verspricht oder gewährt wie auch der Beteiligte (passive Korruption), der den Vorteil fordert, sich versprechen lässt oder annimmt[14].

---

[10] So wird etwa die Reichweite der „Kassenarztentscheidung" des Bundesgerichtshofes – BGH NJH 2012, 2530 ff. m. E. überschätzt. Mitarbeiter bei Stellen der öffentlichen Verwaltung, insbesondere von Universitätskliniken, fallen ohnehin in den Anwendungsbereich der §§ 331 ff. StGB, angestellte Ärzte in privaten Einrichtungen in denjenigen des § 299 StGB. Aber selbst niedergelassene Ärzte können sich im Falle einer fehlenden Weitergabe von Rabatten der Arzneimittelhersteller unter bestimmten Voraussetzungen gemäß §§ 263, 266 StGB strafbar machen.

[11] So hat etwa die Staatsanwaltschaft München I vor einiger Zeit Ermittlungen im Medienbereich geführt. Aus Sicht der Staatsanwaltschaft begründete die seinerzeit existierende Praxis der Gewährung von Mengenrabatten durch Medienunternehmen die Fernsehsender an Mediaagenturen als „Belohnung" dafür, dass die Agenturen für ihre Werbekunden Werbeplätze buchten, im Falle einer nicht Offenlegung der erhaltenen Rabatte den Anfangsverdacht u. a. der Bestechung bzw. Bestechlichkeit im geschäftlichen Verkehr. Vergleichbare Rechtsfragen dürften sich in bestimmten Fallkonstellationen auch in bisher noch nicht betroffenen Branchen stellen – so darf man mit Spannung auf eine erste staatsanwaltschaftliche Überprüfung von „Finders Fee" -Praktiken in einigen Beratungsbranchen, warten.

[12] Vgl. zu den im Rahmen dieser Tatbestände bestehenden Auslegungsproblemen instruktiv die Kommentierungen bei Schönke/Schröder-Perron, 28. Aufl. 2010 bzw. Fischer, StGB, 60. Aufl. 2013.

[13] Vgl. BGHSt 53, 6 ff. – „EnBW" m. w. N.

[14] Was unter Verfolgungsaspekten von erheblicher Bedeutung ist. Der Dienstherr des bestochenen Arbeitnehmers ist typischerweise die Partei, die die wirtschaftlichen Folgen von korruptiven Vorgängen zu tragen hat – und sorgt schon zur Sicherung eigener zivilrechtlicher Ansprüche dafür, dass Aufklärung betrieben wird wenn die Straftat entdeckt wird.

Das deutsche Strafrecht differenziert damit im Rahmen der in der Praxis wichtigsten Korruptionsstraftatbestände zwischen Zuwendungen an Amtsträger[15] einerseits und der Zuwendung von Vorteilen an Mitarbeiter und Beauftragte geschäftlicher Betriebe andererseits.

Eine strukturelle Ähnlichkeit besteht zwischen der Bestechung und Bestechlichkeit (von Amtsträgern) und der Bestechung bzw. Bestechlichkeit im geschäftlichen Verkehr auch insoweit, als strafbar stets solche Vorteilszuwendungen sind, durch die eine rechtswidrige Diensthandlung (bei Amtsträgern) bzw. eine unlautere Bevorzugung (im geschäftlichen Verkehr) angestrebt wird. Diese durch eine Unrechtsabrede im engeren Sinne, einem „quid pro quo" von Vorteilszuwendung als Gegenleistung für eine Bevorzugungshandlung, geprägten Tatbild dürfte das Verständnis von „Korruption" im Rechtsverkehr entsprechen.

Allerdings sanktioniert das deutsche Strafrecht (vgl. §§ 331, 333 StGB) im Falle der Zuwendung von Vorteilen an Amtsträger nicht nur die „Belohnung" einer konkreten Gegenleistung – sondern bereits eine Vorteilszuwendung „im Zusammenhang mit der Dienstausübung". Anders als im Bereich des geschäftlichen Verkehrs ist es also im Falle der Zuwendung von Vorteilen an Amtsträger bereits strafbar, wenn durch die Vorteilszuwendung zwar keine konkrete Diensthandlung beeinflusst werden soll sofern die Vorteilszuwendung geeignet ist, auf die künftige Dienstausübung des Vorteilsempfängers in noch nicht konkretisierter Form Einfluss nehmen zu können. Nach der Rechtsprechung des Bundesgerichtshofes ist es insoweit für eine Korruptionsstraftat bereits ausreichend, wenn „der Wille des Vorteilsgebers auf ein generelles Wohlwollen (des Amtsträgers) bezogen auf künftige Fachentscheidungen gerichtet ist, das bei Gelegenheit aktiviert werden kann"[16].

Ein Straftatbestand des Nebenstrafrechtes, der gerade in der jüngeren Vergangenheit an Bedeutung gewonnen hat, ist § 119 BetrVG (Betriebsratsbegünstigung)[17]. Daneben kennt das deutsche Kern- und Nebenstrafrecht zahlreiche weitere Korruptionsstraftatbestände (vgl. etwa §§ 108e StGB – Abgeordnetenbestechung), die allerdings eine eher untergeordnete Bedeutung erhalten haben[18].

---

[15] Und der Zuwendung von Vorteilen an Richter, die wegen ihrer richterlichen Unabhängigkeit keine Amtsträger sind, im Hinblick auf Zuwendungen aber behandelt werden wie diese (wenngleich diese Fallgruppe in der Praxis so gut wie keine Rolle spielt).

[16] Vgl. Urteil vom 14.10.2008, BGH 1 StR 260/08, BGHSt 53,6 – „EnBW".

[17] Von einer ausführlichen Darstellung der im Zusammenhang mit § 119 BetrVG gegebenen Praxisprobleme muss an dieser Stelle abgesehen werden. Allerdings dürfte gegen § 119 BetrVG in zahlreichen Unternehmen massiv verstoßen werden. Denn bereits Sondervorteile für Betriebsräte, die nicht in gleicher Form sonstigen Mitarbeitern zu Gute kommen (so z. B. pauschalierte Überstundenvergütungen o. ä.) sind grundsätzlich vom Tatbestand des § 119 BetrVG erfasst. Diese rücken – wie zuletzt die Ermittlungen im Zusammenhang mit den Betriebsräten von Opel oder die aktuellen Berichte über angebliche Luxusreisen von Betriebsräten von ThyssenKrupp gezeigt haben – auch zunehmend in das Interesse der Ermittlungsbehörden. Unternehmen sind daher gut beraten, Ihre jeweiligen „Vergütungspakete" für Betriebsräte rechtlich zu prüfen. Vgl. hierzu Rieble/Klebeck, Strafrechtliche Risiken der Betriebsratsarbeit, NZA 2006, 758.

[18] Vgl. zu weiteren Tatbeständen etwa Greeve in Hauschka (Corporate Compliance, 2. Aufl. 2010), § 25.

2.1.2 Auslandssachverhalte und Korruption im Zusammenhang mit ausländischen Amtsträgern

Sofern das deutsche Recht anwendbar ist[19], stellt es auch Bestechungshandlungen im ausländischen geschäftlichen Verkehr unter Strafe, § 299 Abs. 3 StGB.

Im Hinblick auf ausländische Amtsträger, Richter und weitere vergleichbare Personengruppen stellt das Gesetz über die Bekämpfung der Bestechung ausländischer Amtsträger im internationalen Geschäftsverkehr („IntBestG") ihren deutschen Pendants grundsätzlich gleich.

Im Hinblick auf die Bestechung von EU-Beamten stellt das EU-Bestechungsgesetz („EU-BestG") ebenfalls EU-Beamte und vergleichbare Personengruppen deutschen Amtsträgern gleich.

Allerdings gibt es einen wichtigen normativen Unterschied zwischen dem EU-BestG und dem IntBestG einerseits und den Bestimmungen des StGB andererseits: Das EU-BestG und IntBestG erklären im Hinblick auf die Strafbarkeit ausländischer Amtsträger bzw. von EU-Beamten lediglich die Vorschriften über die Bestechung und Bestechlichkeit, nicht aber die Vorschriften über die Vorteilsgewährung und Vorteilsannahme für anwendbar. Hieraus folgt, dass – anders als bei deutschen Amtsträgern – eine Strafbarkeit nach dem EU-BestG und dem IntBestG nur dann in Betracht kommt, wenn eine Unrechtsabrede im engeren Sinne feststellbar ist. Eine Zuwendung lediglich „im Zusammenhang mit der Dienstausübung" wäre nicht tatbestandsmäßig.

In der Praxis ist es typischerweise so, dass neben der Erfüllung eines Korruptionsstraftatbestandes weitere Straftatbestände verwirklicht werden. Die in der Praxis wohl häufigsten Delikte sind[20]:

- Untreue (§ 266 StGB)
- Betrug (§ 263 StGB)
- Urkundsdelikte (§§ 267 ff. StGB)
- Submissionsbetrug (§ 298 StGB)
- Steuerhinterziehung (§ 370 AO)
- Verrat von Geschäfts- und Betriebsgeheimnissen (§ 17 UWG)

Von besonderer praktischer Bedeutung sind allerdings die mit dem in § 4 Abs. 5 Nr. 10 EStG normierten Betriebsausgabenabzugsverbot verbundenen Probleme.

Danach ist der (steuerliche) Betriebsausgabenabzug bereits dann zu versagen, wenn die vermeintliche Betriebsausgabe als korruptive Vorteilszuwendung zu qualifizieren ist. Wird dieses Betriebsausgabenabzugsverbot verletzt, mindert also der Steuerpflichtige

[19] In Sachverhaltskonstellationen, in denen die eigentliche Bestechungshandlung im Ausland liegt, es aber einen wie auch immer gearteten Inlandsbezug, so etwa einen Transfer von Bestechungsgeldern von einem deutschen Konto, die Einbindung von Staatsabteilungen aus Deutschland o. ä. gibt, ist die Anwendbarkeit deutschen Strafrechtes gegeben, §§ 3, 9 StGB.

[20] Eine Darstellung der denkbaren Fallkonstellationen würde den Rahmen dieses Beitrages sprengen. Vgl. daher bitte zu weiterführenden Hinweisen Greeve in Hauschka, a. a. O.

(rechtswidrigerweise) seinen steuerbaren Gewinn (oder vergrößert er seinen Verlustvortrag), verkürzt er den durch ihn zu erfüllenden Steueranspruch und begeht hierdurch eine Steuerhinterziehung gemäß § 370 AO. Eine besondere praktische Bedeutung erhält diese Vorschrift dadurch, dass „Verdächtige" im Rahmen von Betriebsprüfungen zwischenzeitlich systematisch einer regelmäßigen Kontrolle unterzogen werden. Stellen die Finanzbehörden dabei – etwa im Rahmen von Betriebsprüfungen – entsprechende Verdachtsmomente auf Korruptionsstraftaten fest, sind sie rechtlich verpflichtet, die entsprechenden Verdachtsmomente an die zuständige Staatsanwaltschaft zu melden, die von Amts wegen den entstandenen Tatverdacht zu überprüfen hat.

Die Tatsache, dass auf diese Weise strafrechtliche Risiken für den Geschäftsführer einer Kapitalgesellschaft entstehen können, der an der (ursprünglichen) Korruptionsstraftat nicht beteiligt gewesen ist, führt in der Praxis zudem zunehmend dazu, dass im Falle eines Wechsels der vertretungsberechtigten Organe einer Kapitalgesellschaft auch die jeweiligen Amtsnachfolger prüfen lassen, ob es Hinweise auf Verletzungen dieses Betriebsausgabenabzugsverbotes gibt. Denn auch der Amtsnachfolger ist rechtlich verpflichtet, als unrichtig erkannte Steuererklärungen einer durch ihn geführten Kapitalgesellschaft unverzüglich zu berichtigen, § 153 AO. Verletzt er diese Pflicht, begeht er seinerseits eine Steuerhinterziehung.

2.2 Ausländische Rechtsordnungen

2.2.1 FCPA und British Bribery Act 2010 („BBA")

Neben dem FCPA[21] gewinnt in letzter Zeit der BBA an praktischer Bedeutung.

Der BBA hat in zahlreichen Punkten für Unruhe, fast schon für Aufregung, in Unternehmen gesorgt[22]. Der BBA enthält neben drakonischen Sanktionsandrohungen Anwendungsvorschriften, die über die vergleichbaren Bestimmungen im deutschen Recht hinausgehen[23].

---

[21] Auch von einer ausführlichen Darstellung des FCPA wird an dieser Stelle abgesehen. Der FCPA entspricht in weiten Bereichen dem deutschen IntBestG soweit es um Zuwendungsverbote an ausländische Amtsträger geht. Er enthält daneben aber eine Vielzahl an Ausführungs-, Buchhaltungs- und Verwaltungsvorschriften. Vgl. zur Literatur etwa Rübenstahl, NZWiSt 2012, 401, Schwarz, CCZ 2011, 59, Kohen, Hollend CCZ 2008, 7, jeweils mit weiteren Nachweisen.

[22] Mit Recht kritisch Moosmayer, NJW 2012, 3013 ff. Der BBA und die durch das britische Justizministerium erlassenen Auslegungshilfen sind ganz generell davon geprägt, dass sie die „proportionality" der zu schaffenden Compliance-Maßnahmen betonen. Die Normadressaten sollen also – bei aller Ernsthaftigkeit der mit dem BBA verfolgten Ziele – gerade nicht überfordert werden. Einige der in diesem Zusammenhang gemachten Beispiele sind zudem für deutsche Verhältnisse deutlich zu großzügig.

[23] Vgl. zu Auslegungsfragen den durch das britische Justizministerium erlassenen Leitfaden „Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing" und den „Quick start guide", http://www.justice.gov.uk/.

Der BBA verlangt zunächst für die Anwendbarkeit britischen Rechts nur noch einen relevanten Geschäftsbezug zu Großbritannien, nicht aber eine in Großbritannien ansässige Firma oder dort eine handelnde Person[24].

Vor allem ermöglicht der BBA aber die Sanktionierung von Unternehmen, wenn lediglich eine dem Unternehmen „nahestehende Person" eine korruptive Zuwendung an einen Amtsträger oder im Geschäftsverkehr leistet. Eine in diesem Sinne sehr weitgehend verstandenen – auch strafrechtlichen – Verantwortung können Unternehmen nur entgehen, wenn sie geeignete Maßnahmen – „adequate procedures" – zur Korruptionsbekämpfung eingeleitet haben.

Das britische Justizministerium hat zum besseren Verständnis und zur besseren Orientierung dieser „adequate procedures" sechs Prinzipien entwickelt, nämlich:

- Proportionate procedures
- Top-level commitment
- Risk Assessment
- Due Diligence
- Communication (including training)
- Monitoring and review.

Die Geltung und das Verständnis dieser „six principles" wird durch das Justizministerium in einem eigens hierzu erlassenen Leitfaden erläutert[25]. Dieser Leitfaden und die Umsetzung dieser Organisationsinhalte durch die Unternehmen führen zunehmend zu einer Standardisierung von best practice-Maßnahmen in Compliance-Programmen. Dies gilt insbesondere für die Umsetzung von Vertragspartnerprüfungen (3rd party due diligence), eine an die Vorgaben der „six principles" angelehnten Ergänzung von Anti-Korruptionsrichtlinien und Compliance-Programmen sowie eine an diesen orientierte Optimierung von HR-Prozessen.

3 Strafrechtliche Geschäftsherrenhaftung

Die strafrechtlichen Risiken für Entscheidungsträger im Unternehmen haben sich nicht nur durch die verschärfte Auslegung von Korruptionsstraftatbeständen selbst und einen verschärften regulatorischen Rahmen ergeben.

Auch die Rechtsprechung zur strafrechtlichen Geschäftsherrenhaftung hat im Rahmen zahlreicher Entscheidungen dafür gesorgt, dass die Verantwortungsposition der Entscheidungsträger selbst wesentlich verschärft wurde. Der Bundesgerichtshof vertritt in ständiger Rechtsprechung die Rechtsauffassung, dass die geschäftsleitenden Organe des

[24] Vgl. Section 7 BBA.

[25] Vgl. "Quick Start", Fußnote 23.

Unternehmens nach dem Grundsatz der Generalverantwortung und Allzuständigkeit der Geschäftsleitung dafür verantwortlich sind, dass das Unternehmen rechtstreu handelt und von seinem Betrieb keine Gefahren für Rechtsgüter der Allgemeinheit oder Dritter ausgehen[26]. Im Rahmen der Mauerschützen-Rechtsprechung hat der BGH zudem verdeutlicht, dass die Kontrolle über „regelhafte Abläufe" im Unternehmen eine Tatherrschaft kraft Weisungsmacht (der geschäftsleitenden Organe) vermitteln kann[27].

Selbst für den Fall, dass Entscheidungsträger in Unternehmen strafrechtlich nicht zur Verantwortung gezogen werden können, bestehen für sie bußgeldrechtliche Risiken. Denn § 130 Ordnungswidrigkeitengesetz („OWiG") sieht vor, dass ein Entscheidungsträger zur Verantwortung gezogen werden kann, der vorsätzlich oder fahrlässig Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in einem Betrieb oder Unternehmen unternehmensbezogene Pflichtverletzungen zu verhindern und die mit Strafe oder Geldbuße bedroht sind, wenn die gebotenen Aufsichtsmaßnahmen die Begehung der Straftat oder Ordnungswidrigkeit wesentlich erschwert hätten.

Da § 130 OWiG – anders als die große Mehrzahl wirtschaftsstrafrechtlicher Tatbestände – nicht nur im Falle einer vorsätzlichen, sondern auch einer fahrlässigen Begehung tatbestandsmäßig verwirklicht werden kann und die Ausübung einer gehörigen Aufsicht die Begehung einer unternehmensbezogenen Straftat oder Ordnungswidrigkeit nicht verhindert, sondern nur „wesentlich erschwert" haben muss, ist eine Tatbestandsmäßigkeit im Sinne des § 130 OWiG sehr schnell gegeben. Hieraus folgt, dass eine Sanktionierung von Entscheidungsträgern für im Unternehmen begangene Straftaten durch die Rechtsprechung (vor allem im Bereich von Straftaten) und die konsequente Ausnutzung des ohnehin schon bestehenden gesetzlichen Rahmens (§ 130 OWiG) wesentlich gestiegen ist.

Es kommt hinzu, dass die Staatsanwaltschaften in der Praxis deutlich stärker als in der Vergangenheit auf der Verhängung von Unternehmensgeldbußen (§ 30 OWiG) bestehen, durch die zugleich der aus möglichen Korruptionsstraftaten generierte Gewinn (§ 17 OWiG) abgeschöpft werden soll.

4 Compliance-Maßnahmen

4.1 Risikoanalyse

Compliance-Maßnahmen müssen dem Risikoprofil des jeweiligen Unternehmens gerecht werden. Um eine sachgerechte Compliance aufzubauen, muss das Unternehmen daher

[26] BGHSt 37, 106 ff.; vgl. auch zu Einzelheiten und verweisende weitere Literatur meine Ausführungen in Wirtschaftsstrafrecht, 2. Aufl., S 11 ff., dort auch mit einer Erläuterung der Entscheidungen „Lederspray", „Mauerschützen", „Time-sharing" und jeweils weiteren Nachweisen auf Rechtsprechung und Literatur.

[27] BGHSt 40, 218, 236 f.; vgl. hierzu meine Ausführungen in Wirtschaftsstrafrecht, S. 7 ff. mit Nachweisen auf weiterführende Rechtsprechung und Literatur.

zunächst analysieren, ob und in welchen Bereichen es für mögliche Compliance-Verstöße anfällig ist. Naturgemäß wird ein Unternehmen, das im preislich umkämpften Einzelhandel tätig ist, andere Compliance-Akzente setzen (müssen) als ein Unternehmen, das – wie z. B. die Deutsche Bahn AG – als Auftraggeber großer Projekte geschäftsmodellbedingt besonders anfällig für wirtschaftliche Schäden durch passive Korruption ist[28].

Ein international operierendes Unternehmen wiederum wird andere Compliance-Schwerpunkte setzen als ein Unternehmen, das hauptsächlich im Inland operiert.

Schließlich müssen Unternehmen geschäftsmodellbedingt auch den Inhalt ihrer jeweiligen Compliance-Vorgaben unterschiedlich ausgestalten[29]. Unternehmen, die überwiegend oder ausschließlich im privaten Geschäftsverkehr tätig sind, dürfen hingegen großzügigere Zuwendungen im Sinne von klassischen Hospitality-Zuwendungen gestatten, je weniger die jeweiligen Ansprechpartner der jeweiligen Geschäftspartner durch derartige Zuwendungen beeinflusst werden können (was von der internen Position, der wirtschaftlichen Bedeutung der Geschäftsbeziehung, den genauen Umständen der Zuwendung, dem Volumen des Geschäftes usw. abhängt). Hieraus folgt: Zwar sind Unternehmen gut beraten, sich an Marktstandards zu orientieren, die sich ggf. in ihrer jeweiligen Branche und bei Unternehmen gleicher Größenordnung herausgebildet haben – dies schützt jedenfalls vor dem denkbaren Vorwurf, man habe zumutbare und verkehrsübliche Korruptionsbekämpfungsmaßnahmen außer Acht gelassen. Eine individuelle Risikobeurteilung ist aber unersetzlich[30]. Dies vorangestellt werden wichtige Compliance-Maßnahmen wie folgt vorgestellt:

4.2 Organisation

Die Rechtsprechung zur strafrechtlichen Geschäftsherrenhaftung und zu § 130 OWiG erzwingt ebenso wie die ggf. anwendbaren ausländischen Rechtsordnungen eine sachgerechte Organisation und ggf. Delegation von Organisations- und Aufsichtspflichten. Auch diese – rechtliche zwingende – Compliance-Organisation muss an die jeweiligen Erfordernisse angepasst sein. Hieraus folgt ausdrücklich nicht, dass auch mittelständische und kleinere Unternehmen eine eigene Compliance-Abteilung aufbauen und unterhalten müssen. Es ist durchaus zulässig und üblich, dass Unternehmen Compliance-Funktionen in bereits vorhandene Abteilungen integrieren[31].

---

[28] Nämlich dann, wenn die durch das Unternehmen ausgelösten Vergabeprozesse in korruptiver Weise beeinflusst und dadurch wirtschaftlich unattraktive Angebote angenommen werden.

[29] So muss ein Unternehmen, dessen Mitarbeiter überwiegend mit Amtsträgern in Kontakt kommen, den rigiden Zuwendungsverboten der öffentlichen Hand Rechnung tragen.

[30] Vgl. hierzu Moosmayer, Compliance, passim.

[31] Eine derartige Verknüpfung von Compliance-Aufgaben mit bereits vorhandenen Stabsabteilungen oder operativ tätigen Abteilungen bewirkt zudem zusätzlich eine bessere Kommunikation von Compliance-Belangen und entsprechenden internen Vorgaben im Unternehmen.

Die durch das Unternehmen zu schaffende Compliance-Organisation muss damit dem Risikoprofil, der Größe und der Innenorganisation des Unternehmens angemessen sein. Die internen Organisations- und Delegationsvorgaben müssen klar und verständlich sein.

4.3 Richtlinien und Schulungen

Unverzichtbarer Kernbestandteil einer unternehmensinternen Korruptionsbekämpfung ist die Schaffung von Korruptionsrichtlinien.

Bei der Abfassung der Anti-Korruptionsrichtlinien sollte darauf geachtet werden, dass – soweit anwendbar – Kommunikationserfordernissen vor allem ausländischer Rechtsordnungen Rechnung getragen wird[32].

Im Rahmen der Umsetzung von Anti-Korruptionsrichtlinien stellen sich typischerweise verschiedene Gestaltungsfragen. Die wohl bedeutsamste – und stets kritische – Entscheidung im Rahmen der Gestaltung von Anti-Korruptionsrichtlinien ist die Frage nach Zuwendungswerten (im Sinne einer Setzung von Wertgrenzen für die Gewährung und die Annahme von Geschenken, Bewirtungen und sonstigen Vorteilen).

Will das Unternehmen nicht Zuwendungen an Geschäftspartner generell verbieten, ist es darauf angewiesen, im Rahmen einer abstrakt–generellen Regelung festzulegen, in welchem Rahmen die Adressaten der Richtlinie Zuwendungen vornehmen dürfen. Diese Frage führt – sowohl im Bereich von Amtsträgern wie im Rahmen des geschäftlichen Verkehrs – zu schwierigen Abgrenzungsproblemen, die der Bundesgerichtshof in der „EnBW-Entscheidung“[33] wie folgt und sehr anschaulich beschreibt:

> [. . .] Das bedeutet auch, dass die Strafbestimmung der Vorteilsgewährung nicht schon dadurch uneinwendbar wird, das eine (angestrebte) Unrechtsvereinbarung in sozial adäquate Handlungen – wie die Durchführung eines für sich gesehen in strafrechtlicher Hinsicht gänzlich unverdächtigen Sponsoringkonzepts – eingebunden wird. Auch in diesem Fall ist maßgeblich, wie sich das Vorgehen aufgrund der gesamten Umstände, unter denen es geschieht, darstellt.
> Der Senat ist sich bewusst, dass das Merkmal der Unrechtsvereinbarung nach der hier vorgenommenen Auslegung im Randbereich kaum scharfe Konturen aufweist; dies kann zu Beweisschwierigkeiten führen und räumt dem Tatrichter eine beträchtliche Entscheidungsmacht ein. Diese Auslegung trägt jedoch dem Willen des Gesetzgebers Rechnung. In ihr spiegelt sich der Kompromisscharakter der durch das Korruptionsbekämpfungsgesetz der vom 13.08.1997 reformierten Regelung wieder, die über die alte Rechtslage hinausgeht aber nach dem weitergehenden Vorschlag des Bundesrates zurückbleibt, die Strafbarkeit allein an die Amtsbezogenheit der Vorteilszuwendung zu knüpfen (siehe oben aa). Inwieweit ein

[32] So wird etwa im Zusammenhang mit dem British Bribery Act („BBA“) eine „Speak up“-Policy, also die Aufforderung an Mitarbeiter, potentiell korruptive Verhaltensweisen Dritter zu melden, als „best practice“ angesehen. Aber auch aus deutsch-rechtlicher Sicht muss z. B. verdeutlicht werden, dass Verstöße gegen die Richtlinie sanktioniert werden – ansonsten setzt sich die geschaffene Compliance Glaubwürdigkeitsvorwürfen aus.

[33] BGHSt 53, 6 ff. – „EnBW“.

derartiger Vorschlag in Verbindung mit einer weitgehenden Transparenz gewährleistenden Anzeige- oder Genehmigungslösung (vgl. den Vorschlag von T. Schäfer/Liesching, ZRP 2008, 173, 175 f.) sachgerechter gewesen wäre, hat der Senat indessen nicht zu entscheiden.

Diese angedeutete Kritik des BGH an der Tatbestandsgestaltung des Gesetzgebers im Hinblick auf den Straftatbestand der Vorteilsgewährung (Zuwendung an Amtsträger ohne konkrete Gegenleistung) verdeutlicht die Schwierigkeiten der Unternehmen, die „im Randbereich kaum scharfen Konturen" und die Probleme, korruptive Zuwendungen in einem eigentlich zulässigen „sozialadäquaten Gewand" zuverlässig auszuschließen.

Vergleichbare Anwendungsprobleme ergeben sich typischerweise im geschäftlichen Verkehr soweit es darum geht, in Anti-Korruptionsrichtlinien zulässige und verständliche Entscheidungshilfen und Wertmaßstäbe dafür zu normieren, was als Zuwendung zulässig sein soll (Art der Zuwendung, Wert der Zuwendung).

Diese Probleme werden in der Praxis regelmäßig wie folgt gelöst:

Im Bereich von Amtsträgern erlassen Behörden regelmäßig Anti-Korruptionsrichtlinien, denen zu entnehmen ist, ob und ggf. in welchem Umfang die jeweiligen Amtsträger Zuwendungen annehmen dürfen. Soweit nicht die Annahme jeglicher Vorteile gänzlich verboten wird, gestatten die jeweiligen Dienstherren Amtsträgern in Deutschland in aller Regel allenfalls die Annahme geringfügiger Vorteile. Um dieser Situation Rechnung zu tragen, werden in Korruptionsrechtlinien für den Bereich von Amtsträgern in aller Regel folgende Regelungen vorgesehen:

- Entweder ein komplettes Verbot der Gewährung von Vorteilen (Geschenke, Bewirtungen usw.) oder
- Berechtigung zur Gewährung von Vorteilen lediglich dann, wenn eine entsprechende Genehmigung des Dienstherren (in Form einer Pauschalgenehmigung oder Einzelfallgenehmigung) vorliegt oder
- wenn eine interne Stelle, regelmäßig der Compliance-Officer eine entsprechende Zuwendung genehmigt hat (was das Unternehmen in die Lage versetzt, über einen Compliance-Experten die Zulässigkeit der Zuwendung zu prüfen bevor sie erfolgt).

Im Bereich des Geschäftsverkehrs wird in der Praxis intensiv und in Teilen sehr kontrovers über die Frage diskutiert, ob Unternehmen in ihren Richtlinien „harte"[34] Wertgrenzen als Zuwendungsgrenze oder „weiche" Wertgrenzen vorgesehen werden sollen.

Für starre oder harte Wertgrenzen spricht, dass von ihnen eine deutlich größere Verhaltenssteuerung ausgeht. Der Mitarbeiter als Adressat weiß, dass und bis zu welcher Grenze er Zuwendungen gewähren darf.

[34] Eine „starre" Wertgrenze unterscheidet sich von einer flexiblen Wertgrenze dadurch, dass im ersten Falle Zuwendungen oberhalb eines bestimmten Grenzwertes (z. B. 30,00 €, 50,00 € oder 100,00 €) gänzlich untersagt werden während „weiche" Wertgrenzen den Mitarbeitern lediglich als Orientierungshilfe dienen sollen, die Frage des Zuwendungsverbotes aber nicht von der Einhaltung der Wertgrenze selbst sondern davon abhängig gemacht wird, ob die Zuwendung mit dem Ziel einer Verhaltensbeeinflussung des Empfängers erfolgt.

Gleichwohl sind sie nach der Überzeugung des Unterzeichners nicht zu empfehlen. Zum einen können sie nicht ausschließen, dass mit Zuwendungen, die wertmäßig unterhalb der gewählten Wertgrenze liegen, effektiv bestochen wird[35]. Zudem sind diese Wertgrenzen nicht oder nur sehr schwer praktikabel zu machen. Denn sie verhindern entweder zulässige und im Sinne der Geschäftsförderung auch sinnvolle Zuwendungen oder sind so hoch angesetzt, dass von ihnen keine effektive Präventionswirkung mehr ausgeht[36].

Bei der Ausgestaltung von Anti-Korruptionsrichtlinien ist es auch sinnvoll, sich mit den entsprechenden Vorschlägen der öffentlichen Verwaltung oder von Interessengruppen wie den S 20 auseinander zu setzen[37].

Unverzichtbar im Sinne einer sachgerechten Instruktion ist die Durchführung von Schulungen. Die Praxis zeigt, dass derartige Schulungen durch die Mitarbeiter regelmäßig sehr gut angenommen werden. Jedenfalls für höhere Hierarchieebenen ist zu empfehlen, dass Präsenzschulungen durchgeführt werden, die im Vergleich zu Online-Trainingsmaßnahmen den Vorteil bieten, dass sie eine Diskussion über mögliche Anwendungsprobleme ermöglichen und zugleich die Chance bieten, den Zuhörerkreis „automatisch" als wichtiges Transportmittel für Compliance-Botschaften im Unternehmen zu nutzen.

4.4 Vertragspartnerprüfungen (3rd Party-Due diligence)

Spätestens nach der Einführung des BBA wird man Vertragspartnerprüfungen als Praxisstandard bezeichnen dürfen[38].

Im Rahmen von Vertragspartnerprüfungen werden die Stammdaten des Vertragspartners[39] geprüft. Im Anschluss daran wird ein auf die jeweilige Risikosituation abgestimmte Due diligence durchgeführt, die die Beantwortung von Compliance-Fragebögen, Prüfung von Unterlagen bis hin zur Einziehung von Informationen über den (potentiellen) Vertragspartner beinhalten kann.

---

[35] Vgl. insoweit den sehr instruktiven Bericht über Korruptionsfälle bei Philips: http://www.faz.net/aktuell/wirtschaft/wirtschaftskriminalitaet-kleine-geschenke-von-philips-1356887.html.

[36] So wäre etwa ein Geschäftsführer in einem Unternehmen mit einer Wertgrenze von 30,00 € daran gehindert, Zuwendungen vorzunehmen, die diesen Wert überschreiten – obwohl dies von den Ansprechpartnern, mit denen er seiner Hierarchieebene entsprechend umgeht, möglicherweise erwartet wird und auch nicht damit zu rechnen ist, dass diese in irgendeiner Weise durch Zuwendungen oder Einladungen beeinflusst werden.

[37] Vgl. etwa: http://www.s20.eu/leitfaden_d_250711.pdfx.

[38] Allerdings ist der Umfang der durchgeführten Vertragspartnerprüfungen in der Praxis sehr uneinheitlich und reicht von der Überprüfung wesentlicher Kundendaten bis hin zu umfangreichen Fragebögen, die durch die Vertragspartner ausgefüllt werden müssen.

[39] So z. B. Registerauszüge, Gründungsunterlagen.

4.5 Liquiditätskontrolle

Eine wirksame Kontrolle der im Unternehmen verfügbaren Liquidität ist schon zur Vermeidung der Bildung schwarzer Kassen zwingend erforderlich. Gerade im Rahmen der Bekämpfung von Korruption mit hohen und mittleren Beträgen ist die eine wirksame unternehmensinterne Liquiditätskontrolle ein zentraler Bestandteil einer effektiven Korruptionsbekämpfung.

4.6 Vertragsgestaltung

Zunehmend werden auch Compliance-bezogene vertragliche Verpflichtungen üblich. Über Compliance-Klauseln versuchen Unternehmen, auch ihre Geschäftspartner zur Beachtung der für sie wesentlichen Compliance-Vorgaben anzuhalten.

4.7 Compliance-Bezug von Vergütungskomponenten

Um einer wirksamen Compliance-Struktur auch tatsächlich Geltung zu verlangen, gehen einige Unternehmen dazu über, die Vergütung von Führungskräften jedenfalls teilweise von der Einhaltung von Compliance-Zielen abhängig zu machen. Verallgemeinerungsfähige Marktstandards sind allerdings nach dem Eindruck des Verf. in diesem Punkt noch nicht feststellbar.

4.8 Hinweisgebersysteme und Ombudsmannfunktionen

Unternehmen gehen zunehmend dazu über, interne Hinweisgebersysteme einzurichten oder externe Ombudsmänner, zumeist Rechtsanwälte, zu bestellen.

Diese Einrichtungen sind eine sinnvolle Ergänzung zu den vorstehend beschriebenen Compliance-Maßnahmen.

EDV-gestützte Hinweisgebersysteme sind zumeist so konstruiert, dass potentielle Hinweisgeber sich per E-Mail an das Unternehmen wenden können, insoweit aber die Möglichkeit haben, mit dem Unternehmen anonym zu korrespondieren. Diese Systeme haben den Vorzug, dass die Hemmschwelle, Kontakt mit dem Hinweisgebersystem aufzunehmen, vergleichsweise gering ist.

Alternativ oder kumulativ gehen zahlreiche Unternehmen dazu über, externe Rechtsanwälte als Ombudsmänner zu bestellen. Diese haben – im Falle einer entsprechenden konstruierten Mandatsvereinbarung – die Möglichkeit, den Hinweisgebern unter dem Schutz der anwaltlichen Vertraulichkeit die Möglichkeit zu offerieren, einen persönlichen Kontakt zum Ombudsmann aufzunehmen. Aus Unternehmenssicht hat ein derartiges

System den Vorteil, dass das Unternehmen über den Ombudsmann eine bessere Möglichkeit zur Sachverhaltsermittlung und vor allem zur Prüfung der Glaubwürdigkeit des Hinweisgebers erhält.

In der Praxis hat sich gezeigt, dass Ombudsmannsysteme eine wichtige Rolle im Bereich des Schutzes der Unternehmen in – vor allem Fällen passiver Korruption – spielen können[40].

4.9 Kontrollmaßnahmen

Eine wirksame Compliance lebt naturgemäß von routinemäßigen und außerplanmäßigen Kontrollmaßnahmen. Auch diese müssen auf die bestehende Compliance-Organisation und die Binnenorganisation bzw. das Geschäftsmodell des jeweiligen Unternehmens ausgerichtet werden.

Daneben sollten Unternehmen typische „neuralgische" Unternehmensbereiche überprüfen. In Betracht kommen insoweit etwa die Überprüfung von Beraterverträgen, kritischen Buchhaltungskonten – insbesondere von solchen, die Spesen oder unkörperliche Leistungen (Beraterverträge und sonstige nicht inventarisierbare Leistungen) betreffen.

[40] Der Verfasser ist Ombudsmann verschiedener Unternehmen. Nach seinen Erfahrungen ist die Quote gezielter Falschmeldungen bisher nicht signifikant; allerdings kommen derartige Versuche eines Missbrauchs von Ombudsmannsystemen vereinzelt vor. Die Erfahrung zeigt aber, dass vor allem Fälle passiver Korruption unter Benachteiligung von Dienstleistern und Lieferanten eher an ein Ombudsmannsystem als in sonstiger Form an das Unternehmen kommuniziert werden. Entsprechendes gilt wenn Hinweise durch Mitarbeiter erfolgen, die Repressionen fürchten.

Praxistipps Unternehmenskrise

Reinhard Willemsen

Inhaltsverzeichnis

Zusammenfassung

Die Krise eines Unternehmens an der Grenze zur Insolvenzantragspflicht birgt eine Vielzahl von Fallstricken. Im schlimmsten Fall macht sich der handelnde Geschäftsführer oder faktische Geschäftsführer strafbar bzw. zivilrechtlich haftbar sowohl gegenüber den Gläubigern des Unternehmens als auch dem Insolvenzverwalter. Krisenmanagement bedeutet, auch für den Ernstfall der Insolvenz gerüstet zu sein und im Vorfeld die richtigen Maßnahmen zur richtigen Zeit zu treffen.

R. Willemsen (✉)
Karlstraße 10–12, 80333 München, Deutschland
E-Mail: reinhard.willemsen@luther-lawfirm.com

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2_15, © Springer Fachmedien Wiesbaden 2013

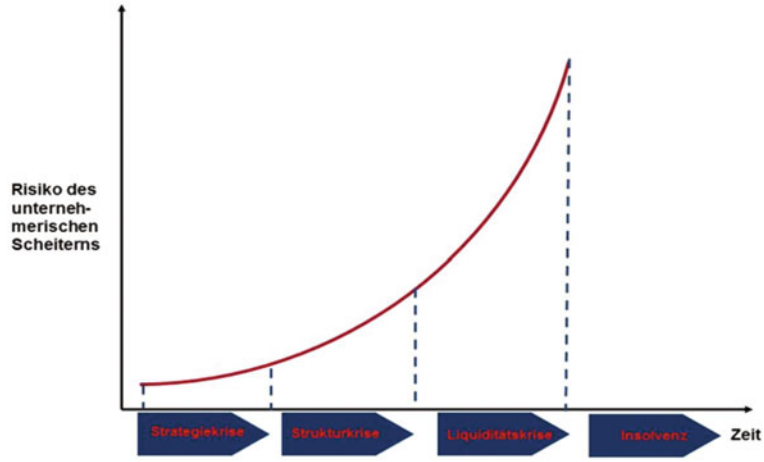


Abb. 1 Krisenstadien

1 Einleitung

Die Krise eines Unternehmens ist in aller Regel ein schleichender Prozess, der sich über Monate teilweise sogar Jahre hinzieht (Abb. 1).

Von der strategischen über die Strukturkrise bis zur Liquiditätskrise und Insolvenz gibt es eine Vielzahl von Entscheidungen, die entweder eine Sanierung des Unternehmens erlauben oder direkt in die Insolvenz führen. Erst im Nachhinein stellt sich in vielen Fällen heraus, dass eine Entscheidung, die bereits Monate oder Jahre zuvor getroffen wurde, letztlich zur Insolvenz geführt hat.

Neben der Existenz des Unternehmens steht in der Unternehmenskrise auch die Haftung des Unternehmers/Geschäftsführers auf dem Spiel[1]. Dabei ist – grob gesprochen – zwischen zivilrechtlichen und strafrechtlichen Ansprüchen zu unterscheiden. Während zivilrechtliche Ansprüche noch durch Versicherungen oder Haftungsübernahmen Dritter (beispielsweise des Gesellschafters) abgefedert werden können, trifft die strafrechtliche Verantwortung den handelnden Geschäftsführer oder – in der Praxis gar nicht so selten – den faktischen Geschäftsführer alleine, ohne dass dieser die Möglichkeit hat sich vor dieser Haftung zu schützen, es sei denn ein funktionierendes (dokumentiertes!) Krisenmanagement gibt ihm die Möglichkeit rechtzeitig die entsprechenden Schritte einzuleiten.

[1] *Willemsen*, in: Umnuss (Hrsg.) Corporate Compliance Checklisten, 2. Aufl. München 2012, Kap. 6. Rz. 2.

2 Krisenstadien

Die Krise eines Unternehmens vollzieht sich wie bereits dargestellt nicht auf einmal, sondern umfasst verschiedene Krisenstadien. In jedem dieser Stadien treffen den Geschäftsführer andere Pflichten zur Vermeidung seiner Haftung, wobei die für eine Entscheidung verbleibende Zeit exponentiell abnimmt, während das Haftungsrisiko im gleichen Maße zunimmt.

2.1 Strategische Krise

Von einer strategischen Krise spricht man, wenn die Ausrichtung des Unternehmens im Hinblick auf Marktteilnehmer, Produkte, Standorte, Mitarbeiter etc. nicht mehr stimmt. In der strategischen Krise gibt es zunächst noch keine Auswirkungen auf das Ergebnis. Dieses wird schleichend schlechter. Eine „harte" Pflicht des Geschäftsführers bereits an dieser Stelle einzugreifen gibt es nicht. Insbesondere sind an eine Unterlassung eines solchen Eingriffs keine straf- oder zivilrechtlichen Konsequenzen geknüpft. Trotzdem ist einem Geschäftsleiter anzuraten, bereits in diesem frühen Stadium gegenzusteuern. Voraussetzung hierfür ist, dass er eine Strategiekrise erkennt. Anhaltspunkte für eine solche Strategiekrise sind:

- Zunehmender Preisdruck
- Verlust von Alleinstellungsmerkmalen
- Abwanderung wichtiger Mitarbeiter
- ganz allgemein Veralten von Produktionsstandorten und Maschinen
- nachlassende Qualifikation der Mitarbeiter – Überalterung der Belegschaft
- Verlust wichtiger Kunden an neue Konkurrenten
- drohender Ablauf wichtiger Patente/Geschmacksmuster
- das Management kümmert sich nicht um neue Marketingideen, unternehmerische Entscheidungen werden aus persönlichen Differenzen (mehrere Familienstämme) oder angeblichem Zeitmangel immer wieder verschoben.

In dieser Situation ist eigentlich noch ausreichend Zeit vorhanden, um eine positive Veränderung herbeizuführen. Das Problem liegt – wie gesagt – darin, die Strategiekrise zu erkennen. Der Geschäftsführer/Unternehmer sollte daher permanent folgende Regeln beachten:

- ständige Überprüfung sämtlicher Geschäftsfelder
- Beobachtung von Branche und Konkurrenten
- Beschränkung auf das Kerngeschäft
- Frühzeitige Kooperation mit andern (größeren, stärkeren) Unternehmen suchen, um Synergien zu nutzen

- Produktbereich identifizieren, die für den Erfolg des Unternehmens relevant sind und ständig neue Produkte entwickeln, auch wenn ein Produkt gerade „läuft“

2.2 Struktur oder Erfolgskrise

Strategie- und Strukturkrise gehen ineinander über und sind nur schwer voneinander abzugrenzen. In der Strukturkrise sind schon erste Auswirkungen im Ergebnis erkennbar. Unternehmensziele werden nicht mehr vollständig erreicht, der Jahresüberschuss erreicht nicht die prognostizierten Höhen, die Umsätze werden geringer, ohne dass dies jedoch schon besorgniserregende Umfänge annimmt.

Spätestens in dieser Situation sollte die Geschäftsführung handeln, um noch einen echten Einfluss auf die weitere Entwicklung nehmen zu können.

Signale der Erfolgskrise sind:

- Verlust von Stammkunden
- Absatzrückgang und anwachsen der Außenstände
- Häufigere Kundenbeschwerden
- Nichteinhaltung vereinbarter Liefertermine
- fehlende Auslastung der Produktion und Qualitätsprobleme
- Umsatzrückgang und Gewinneinbruch
- Verschlechterung des Betriebsklimas und erhöhte Fluktuation

Spätestens jetzt sind die Maßnahmen nach 2.1 zu ergreifen

Wird hier nicht gegengesteuert kommt es zur:

2.3 Liquiditätskrise

Hierbei verstärken sich sämtliche Anzeichen der Erfolgskrise, zusätzlich kommt es zu erheblichen Liquiditätsengpässen. Hinzu kommt häufig, dass zuverlässige Zahlen nicht mehr erhältlich sind, weil entweder entsprechende Mitarbeiter fehlen oder diese „Brandherde“ löschen müssen, so dass sie ihren eigentlichen Aufgaben nicht mehr nachkommen können.

In dieser Situation helfen nur noch drastische Mittel. Möglicherweise unter Zuhilfenahme eines externen Beraters sind sämtliche – wesentliche – Gläubiger an einen Tisch zu holen, um eine Sanierung zu ermöglichen. Im Vorfeld zu einem solchen Treffen sollte ein Sanierungsplan erstellt werden, aus dem sich eine mindestens kurz- und mittelfristige Erholung der Situation (bei angenommener Zustimmung der Gläubiger) ergibt. Inhalt der Sanierungsvereinbarung können Stundungen, Teilverzichte, Verlagerungen etc. sein. In der Regel ist eine Sanierungsvereinbarung, der sämtliche wesentliche Stakeholder zugestimmt haben, eine Voraussetzung für die Vergabe neuer Darlehen[2].

[2] *Häuser,* in Schimanski/Bunte/Lwowski, Bankrechtshandbuch, 4. Aufl. 2011, § 85 Rz. 15.

Je nach vorhandener Liquidität schlägt die Liquiditätskrise sehr schnell in ein Insolvenzszenario um, jedenfalls dann, wenn nicht massiv gegengesteuert wird.

3 Insolvenzszenario

Verstärken sich die Anzeichen der Liquiditätskrise und gelingt es nicht, durch einen Sanierungsplan Handlungsfreiheit zu gewinnen, dann gerät die Gesellschaft in ein Insolvenzszenario. Ist dieses Stadium erreicht, hängt die Haftung des Leitungsorgans im Wesentlichen von der Rechtsform der Gesellschaft ab. Die Haftungsfolgen für eine Kapitalgesellschaft sind deutlich strenger als die einer echten Personengesellschaft. Insolvenzantragspflichten mit der strafrechtlichen Konsequenz bei Nichtbefolgung treffen nur das Leitungsorgan einer Kapitalgesellschaft (wozu auch „kapitalistische" Personengesellschaften zählen, also solche, bei denen kein persönlich haftender Gesellschafter eine natürliche Person ist). Aber auch für Personengesellschaften gibt es Haftungsrisiken bei Insolvenzreife.

3.1 Kapitalgesellschaften

Liegt ein verpflichtender Insolvenzantragsgrund vor, so ist das Leitungsorgan einer Kapitalgesellschaft verpflichtet, Antrag auf Eröffnung des Insolvenzverfahrens zu stellen. (§ 15 a InsO). Unterbleibt ein solcher Antrag, machen sich die Mitglieder des Leitungsorgans (Geschäftsführung oder Vorstand) strafbar (§ 15a Abs. 4 InsO).

Zwingende Antragsgründe sind Zahlungsunfähigkeit und Überschuldung. Zahlungsunfähigkeit liegt nach der Rechtsprechung des BGH[3] in der Regel vor, wenn ein Schuldner nicht in der Lage ist, innerhalb von 21 Tagen mindestens 90 % seiner am Prüfungsstichtag fälligen Verbindlichkeiten zu decken.

Hierzu ist ein Status zu erstellen, in dem die fälligen Verbindlichkeiten aufzuführen sind, die noch auf dem Konto befindlichen Barmittel (bzw. nicht ausgeschöpfte und ungekündigte Kreditlinien) sowie die in den nächsten 21 Tagen voraussichtlich eingehenden liquiden Mittel[4].

Nach wie vor ungeklärt ist die Frage, ob die innerhalb der 21-Tagesfrist zusätzlich fällig werdenden Verbindlichkeiten in diese Kalkulation einzubeziehen sind oder nicht[5].

In jedem Fall gehört zu einer heutigen Compliance-Ansprüchen genügenden Vorsorge die Einrichtung eines Controllings, das Liquiditätsengpässe rechtzeitig anzeigt und der Ge-

[3] St. Rspr. Seit BGH Urt. v. 24. Mai 2005, IX ZR 123/04 BGHZ 163, 134 ff.

[4] Willemsen/Rechel, Kommentar zum ESUG, Frankfurt 2012 § 17 Rz. 2.

[5] Zum Meinungsstand: Willemsen/Rechel, Kommentar zum ESUG, Frankfurt 2012 § 17 Rz. 3 ff.

schäftsleitung die Möglichkeit gibt, die vorbeschriebenen Berechnungen – falls notwendig auch täglich – durchführen zu können.

Neben der Zahlungsunfähigkeit ist auch die Überschuldung ein zwingender Insolvenzantragsgrund. Allerdings kann Überschuldung nach der geltenden Fassung des § 19 InsO nur vorliegen, wenn die Gesellschaft eine negative Fortbestehensprognose hat. Die Befristung dieses Überschuldungsbegriffs auf den 31. Dezember 2013 ist mittlerweile entfallen[6]. Vereinfacht gesprochen ist eine Fortbestehensprognose eine Prognose über die zukünftige Zahlungsfähigkeit[7]. Auch eine solche Prognose setzt ein funktionierendes Controlling und eine integrierte Vermögens- Finanz- und Ertragsrechnung voraus.

Kann eine positive Fortbestehensprognose nicht gestellt werden, so ist ein Überschuldungsstatus auf der Basis von Zerschlagungswerten zu erstellen. Übersteigen hiernach die Verbindlichkeiten das Vermögen der Gesellschaft, so liegt Überschuldung und damit ein zwingender Insolvenzantragsgrund vor.

Der Insolvenzantrag muss nach den Änderungen der Insolvenzordnung durch das ESUG gewisse Mindestangaben enthalten, wobei diese teilweise nur bei bestimmten Größenkategorien erforderlich sind[8]. Da die o. g. Strafbarkeit auch dann vorliegt, wenn der Insolvenzantrag „nicht richtig" gestellt wird, ist es in jedem Falle ratsam, die in § 13 InsO genannten Unterlagen dem Insolvenzantrag beizufügen.

3.2 Alle Gesellschaftsformen und Einzelkaufleute

Während die Insolvenzantrags*pflichten* nur Kapitalgesellschaften und deren Geschäftsleiter treffen, gibt es eine Reihe weiterer potentieller Straftatbestände, die in jeder Gesellschaftsform verwirklicht werden kann.

Hierzu gehören sämtliche Tatbestände der §§ 283ff. StGB, aber auch Untreue, (Eingehungs)betrug, Vorenthaltung von Sozialversicherungsbeiträgen etc.

Da die meisten dieser Tatbestände, insbesondere der §§ 283ff. StGB an das Vorliegen eines Insolvenzantragsgrundes anknüpfen, ist auch für Personengesellschaften (für die eigentlich die Insolvenzantragstellung nicht verpflichtend ist) ein Controlling unerlässlich, was zuverlässig die Insolvenzgefahr anzeigt.

Insgesamt erfordert ein funktionierendes Compliance-System eine integrierte Vermögens- Finanz- und Ertragsplanung, die jederzeit ein zuverlässiges Bild der finanziellen Situation des Unternehmens erlaubt.

---

[6] Pressemitteilung des BMJ vom 9. November 2012 http://www.bmj.de/SharedDocs/Pressemitteilungen/DE/2012/20121109_Rechtsbehelfsbelehrung.html.

[7] *Willemsen,* in: Umnuss (Hrsg.), Corporate Compliance-Checklisten, 2. Aufl. München 2011, Kap. 6. Rz. 14.

[8] Willemsen/Rechel, Kommentar zum ESUG, Frankfurt 2012 § 13 Rz. 1, 6 f.

Literatur

ALBRECHT, FLORIAN/MAISCH, MICHAEL MARC; Bluttests und Verhaltensanalysen bei Bewerbern, DSB 03/2010, S. 11–18.

ALTMEPPEN, HOLGER; Die Auswirkungen des KonTraG auf die GmbH, ZGR 1999, S. 291–313.

ASCHEID, REINER/PREIS, ULRICH/SCHMIDT, INGRID; Kündigungsrecht Kommentar, 4. Auflage, München 2012.

ASSMANN, HEINZ-DIETER; Das künftige deutsche Insiderrecht, AG 1994, S. 237–258.

AX, ROLF/GROßE, THOMAS/MELCHIOR, JÜRGEN; Abgabenordnung und Finanzgerichtsordnung, 20. Auflage, Stuttgart 2010.

BACHMANN, GREGOR; Compliance – Rechtsgrundlagen und offene Fragen, Gesellschaftsrecht in der Diskussion 2007, S. 65–73.

BANNENBERG, BRITTA/SCHAUPENSTEINER, WOLFGANG; Korruption in Deutschland: Portrait einer Wachstumsbranche, 3. Auflage, München 2007.

BAUER, SILVIA C./WESSELMANN, CARSTEN; EuroSox und Compliance Organisation, WISU 8–9/08, S. 1128–1131.

BAUER, SILVIA C.; EuroSOX und Datenschutz – Vorhandenes Know-How des Datenschutzbeauftragten gezielt nutzen, Datenschutzpraxis 9/2008, S. 2–3.

BAUER, SILVIA C.; Datenschutz und Korruption, Datenschutzpraxis 5/2009, S. 6–7.

BAUER, SILVIA C.; Datenschutz im Unternehmen, WISU 4/09, S. 504–508.

BAUER, SILVIA C.; Google Analytics – datenschutzrechtlich zulässig oder nicht?, Datenschutz Praxis 06/2009, S. 6–7.

BAUER, SILVIA C.; Google Analytics: Endlich eine Lösung!?, Datenschutz Praxis 12/2011, S. 8–9.

BAUER, SILVIA C.; Whistleblowing-Systeme rechtskonform gestalten, Datenschutz Praxis 11/2012, S. 14–16.

BAUMBACH, ADOLF/HUECK, ALFRED; GmbHG Kommentar, 20. Auflage, Düsseldorf u. a. 2013.

BECHTOLD, RAINER; GWB: Kartellgesetz, Gesetz gegen Wettbewerbsbeschränkungen, 5. Auflage, München 2008.

BECHTOLD, RAINER; Kartellgesetz. Gesetz gegen Wettbewerbsbeschränkungen, Kommentar. 6. Auflage, München 2010.

BEHLING, TORSTEN B.; Compliance versus Fernmeldegeheimnis, BB 2010, S. 892–896.

BEISENHERZ, GERHARD/TINNEFELD, MARIE-THERES, Sozialdatenschutz – eine Frage des Beschäftigtendatenschutzes?, DuD 2010, S. 221–224.

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2, © Springer Fachmedien Wiesbaden 2013

BERENS, WOLFGANG/BRAUNER, HANS U./STRAUCH, JOACHIM; Due Diligence bei Unternehmensakquisitionen, 6. Auflage, Stuttgart 2011.
BERG, CAI; Korruption in Unternehmen und Risikomanagement nach § 91 II AktG, AG 2007, S. 271–278.
BERGMANN, LUTZ/MÖHRLE, ROLAND/HERB, ARMIN; Datenschutzrecht, Kommentar Bundesdatenschutzgesetz, Loseblatt, Stuttgart, u. a., Stand: 2012.
BERGMOSER, ULRICH/THEUSINGER, INGO/GUSHORST, KLAUS-PETER; Corporate Compliance – Grundlagen und Umsetzung; BB-Special 2008, Nr. 5, S. 1–11.
BERWANGER, JÖRG/KULLMANN, STEFAN; Interne Revision – Wesen, Aufgaben und rechtliche Verankerung, Wiesbaden 2008.
BESEN, MARC/GRONEMEYER, ACHIM; Kartellrechtliche Risiken bei Unternehmenskäufen – Informationsaustausch und Clean Team, CCZ 2009, S. 67–70.
BIENECK, KLAUS; Handbuch des Außenwirtschaftsrechts mit Kriegswaffenkontrollrecht, 2. Auflage, Köln 2005.
BIER, SASCHA: Risk – Management zur Haftungsminimierung im E-Business, K&R 2005, S. 59–64.
BIEREKOVEN, CHRISTIANE; Korruptionsbekämpfung vs. Datenschutz nach der BDSG-Novelle, CR 2010, S. 203–208.
BINDING, JÖRG/THUM, KAI; Aktuelle Entwicklungen im Arbeitsrecht der VR China, RdA 2008, S. 347–357.
BIRNFELD, MARION; Compliance in der Vergaberechtspraxis, CCZ 2010, S. 133–138.
BÖHME, MARTIN; Die Aufbewahrungspflicht von E-Mails, K&R 2006, S. 176–178.
BOHNERT, JOACHIM; Kommentar zum Ordnungswidrigkeitengesetz, 3. Auflage, Berlin 2010.
BORGMANN, BERND; Ethikrichtlinien und Arbeitsrecht, NZA 2003, S. 352–357.
BRANDT-SCHWABEDISSEN, ANETTE; Selbstverpflichtung führt eher zum Erfolg; Städte- und Gemeinderat 11/2010, S. 12–16.
BRAUN, MARTIN/WYBITUL TIM; Übermittlung von Arbeitnehmerdaten bei der Due Diligence – Rechtliche Anforderungen und Gestaltungsmöglichkeiten, BB 2008, S. 782–786.
BREINLINGER, ASTRID/KRADER, GABRIELA; Whistleblowing – Chancen und Risiken bei der Umsetzung von anonym nutzbaren Hinweisgebern im Rahmen des Compliance – Managements von Unternehmen, RDV 2006, S. 60–70.
BREMER, JÜRGEN; GmbH-Praxis GmbH-Beratung, GmbHR 2000, S. 176–180.
BUCHERT, RAINER; Der externe Ombudsmann – ein Erfahrungsbericht, CCZ 2008, S. 148–152.
BUCHTA, JENS; Haftung und Verantwortlichkeit des Vorstands einer Aktiengesellschaft – Eine Bestandsaufnahme, DB 2006, S. 1939–1943.
BUCK-HEEB, PETRA; Informationsorganisation im Kapitalmarktrecht – Compliance zwischen Informationsmanagement und Wissenorganisationspflichten, CCZ 2009, S. 18–25.
BUEREN, ECKART; Prämien für Whistleblower im Kartellvollzug, ZWeR 2012, 310.
BULL, HANS PETER; Neue Bewegung im Datenschutz – Missbrauchsbekämpfung oder Ausbau bereichsspezifischer Regelungen? ZRP 2008, S. 233–236.
BÜRKLE, JÜRGEN: Corporate Compliance – Pflicht oder Kür für den Vorstand der AG?, BB 2005, S. 565–570.
BÜRKLE, JÜRGEN: Corporate Compliance als Standard guter Unternehmensführung des Deutschen Corporate Governance Kodex, BB 2007, S. 1797–1801.
BÜSSOW, THOMAS/TAETZNER, TOBIAS; Sarbanes-Oxley Act Section 404: Internes Kontrollsystem zur Sicherstellung einer effektiven Finanzberichterstattung im Steuerbereich von Unternehmen – Pflicht oder Kür?, BB 2005, S. 2437–2445.
BUSEKIST VON, KONSTANTIN/SCHLITT, CHRISTIAN; Der IDW PS 980 und die allgemeinen rechtlichen Mindestanforderungen an ein wirksames Compliance Management System (2), CCZ 2012, S. 86–95.
CASPAR, CHRISTA/NEUBAUER, REINHARD; Korruptionsprävention in kommunalen Verwaltungen, LKV 2011, S. 200–208.

CASPER, MATTHIAS; Der Compliancebeauftragte – unternehmensinternes Aktienamt, Unternehmensbeauftragter oder einfacher Angestellter?, Festschrift Karsten Schmidt 2009, S. 199–216.
COHEN, JOEL M./HOLLAND, MICHAEL P.; Fünf Punkte, die ausländische Unternehmen über den United States Foreign Corrupt Practices Act (FCPA) wissen sollten, CCZ 2008, S. 7–11.
DANN, MATTHIAS/GASTELL, ROLAND; Geheime Mitarbeiterkontrollen: Straf- und arbeitsrechtliche Risiken bei unternehmensinterner Aufklärung, NJW 2008, S. 2945–2949.
DÄUBLER, WOLFGANG/KLEBE, THOMAS/WEDDE, PETER/WEICHERT, THILO; Bundesdatenschutzgesetz, Basiskommentar, 3. Auflage, Frankfurt am Main 2010.
DÄUBLER, WOLFGANG; Gläserne Belegschaften, 5. Auflage, Frankfurt 2010.
DÄUBLER, WOLFGANG/WANG; QIAN; Bestandsschutz des Arbeitsverhältnisses in der Volksrepublik China, RdA 2008, S. 141–146.
DEISEROTH, DIETER/DERLEDER, PETER; Whistleblower und Denunziatoren, ZRP 2008, S. 248–251.
DEISTER, JOCHEN/GEIER, ANTON/REW, PAUL; Business as usual? Die Leitlinien zum UK Bribery Act 2010 sind veröffentlicht, CCZ 2011, S. 81–89.
DEUTLMOSER, RALF/FILIP, ALEXANDER; Europäischer Datenschutz und US-amerikanische (e-) Discovery – Pflichten, ZD-Beilage 2012, S. 1–23.
DICKINSON, STEVE M./VIETZ, NADJA; Das neue GmbH-Recht der Volksrepublik China, GmbHR 2006, S. 245–249.
VON DIETZE, PHILIPP/JANSSEN, HELMUT; Kartellrecht in der anwaltlichen Praxis, 4. Auflage, München 2011.
DILLER, MARTIN: Der Arbeitnehmer als Informant, Handlanger und Zeuge im Prozess der Arbeitgebers gegen Dritte, DB 2004, S. 313–319.
DÖSER, WULF HEINRICH; Vertragsgestaltung im internationalen Wirtschaftsrecht, München 2001.
DREHER, MEINRAD; Die persönliche Verantwortung von Geschäftsleitern nach außen und in die innergesellschaftliche Aufgabenteilung, ZGR 1992, S. 22–63.
DREHER, MEINRAD; Kartellrechtscompliance – Voraussetzungen und Rechtsfolgen unternehmens- oder verbandsinterner Maßnahmen zur Einhaltung des Kartellrechts, ZWeR 2004, S. 75–105.
DREHER, MEINRAD; Die Aufsichtspflicht zur Vermeidung von Kartellverstößen, Compliance Report 10/2007, S. 2 f.
DREHER, MEINRAD; Die Vorstandsverantwortung im Geflecht von Risikomanagement, Compliance und interner Revision, Festschrift Hüffer 2010, S. 161–178.
DREHER, MEINRAD/SCHAAF, MARTIN; Versicherungsunternehmensrecht und Risikomanagement, WM 2008, S. 1765–1773.
DRESKY VON, BRIGITTA; Newcomer Myanmar, Unternehmer Edition, 11/2012, S. 52–54.
DREWES, STEFAN; Werbliche Nutzung von Daten – Die Implosion der BDSG-Novelle und Auswirkungen der EuGH-Rechtsprechung, ZD 2012, S. 115–119.
DRYGALA, TIM/DRYGALA, ANJA; Wer braucht ein Frühwarnsystem?, ZIP 2000, S. 297–305.
DUISBERG, ALEXANDER/ORTHMANN, JAN-PETER; Basel II und seine Auswirkungen auf die IT-Infrastruktur der Banken, ITRB 2005, S. 160–161.
EHLERS, HARALD; Tax Compliance; NWB 2012, S. 1535–1543.
EHMANN, EUGEN; Vorabkontrolle – wann ist sie nötig?, Datenschutzpraxis, 01/09, S. 12–13.
EISELE, DIETER; Insiderrecht und Compliance, WM 1993, S. 1021–1026.
ENGELHARDT, CLEMENS; Gesellschafterbeschluss zur Durchführung einer Due Diligence, GmbHR 2009, S. 237–243.
ENGELS, THOMAS; Datenschutz in der Cloud – ist hierbei immer eine Auftragsdatenverarbeitung anzunehmen?, K&R 2011, S. 548–551.

ERNST, STEFAN; Social Plugins – Der „Like-Button" als datenschutzrechtliches Problem, NJOZ 2010, S. 1917.
FAHRIG, STEPHAN; Die Einführung eines Verhaltenskodexes und das Whistleblowing, Baden-Baden 2010.
FIETZ, EIKE/WEIDLICH, THOMAS; Schwarze Schafe oder weiße Ritter?, RiW 2005, S. 423–429.
FITTING, KARL; Betriebsverfassungsgesetz Kommentar, 15. Auflage, München 2012.
FISCHER, THOMAS; Strafgesetzbuch: STGB, 59. Auflage, München 2012.
FLEISCHER, HOLGER; Vorstandsverantwortlichkeit und Fehlverhalten von Unternehmensangehörigen – Von einer Einzelüberwachung zur Errichtung einer Compliance-Organisation, AG 2003, S. 291–300.
FLEISCHER, HOLGER; Konzernleitung und Leitungssorgfalt der Vorstandsmitglieder im Unternehmensverbund, DB 2005, S. 759–766.
FLEISCHER, HOLGER; Corporate Compliance im aktienrechtlichen Unternehmensverbund, CCZ 2008, S. 1–6.
FLEISCHER, HOLGER; Zum Grundsatz der Gesamtverantwortung im Aktienrecht, NZG 2003, S. 449–460.
FLEISCHER, HOLGER; Zur Leitungsaufgabe des Vorstands im Aktienrecht, ZIP 2003, S. 1–11.
FLEISCHER, HOLGER; Handbuch des Vorstandsrechts, 1. Auflage, Bonn 2006.
FOERSTE, ULRICH/VON WESTPHALEN, FRIEDRICH GRAF; Produkthaftungshandbuch, 2. Auflage, München 1997.
FORST, GERRIT; Blutproben vor der Einstellung? – Zur Zulässigkeit von Blutentnahmen und –Untersuchungen bei Arbeitsplatzbewerbern, RDV 2010, S. 8–10.
FRECKMANN, ANKE/WAHL, SABINE; Überwachung am Arbeitsplatz – Was ist legitim? Wo setzt das Recht Grenzen? BB 2008, S. 1904–1908.
GAULKE, MARKUS; Prüfung der Einhaltung der technischen und organisatorischen Maßnahmen bei Auftragsdatenverarbeitungen, DuD 2011, S. 417–420.
GEERCKEN, KARL/HOLDEN, KELLY/RATH, MICHAEL/STRETTON, TRACEY; Cross Border E-Discovery, CRi 2013, S. 65–74.
GEUENICH, MARCUS/KIESEL, HANNO; Tax Compliance bei Unternehmen – einschlägige Risiken und Folgerungen für die Praxis, BB 2012, S. 155–162.
GILDEGGEN, RAINER/WILBURGER, ANDREAS; Internationale Handelsgeschäfte, 4. Auflage, München 2012.
GLAUBEN, PAUL J.; Gesetzliche Neuregelungen von Spenden sowie Sponsor Leistungen an Kommunen und strafrechtliche Auswirkungen, LKRZ 2008, S. 81–86.
GLÜCK, ULRIKE/SEMLER, FRANZ-JÖRG; Rechtschutz deutscher Unternehmen in China, RIW 2006, S. 436–442.
GOETTE, WULF; Organisationspflichten in Kapitalgesellschaften zwischen Rechtspflicht und Opportunität, ZHR 175 (2011), S. 388–398.
GOLA, PETER; Datenschutz bei der Kontrolle „mobiler" Arbeitnehmer – Zulässigkeit und Transparenz, NZA 2007, S. 1139–1144.
GOLA, PETER/SCHOMERUS, RUDOLF; BDSG Bundesdatenschutzgesetz, Kommentar, 11. Auflage, München 2012.
GOLA, PETER/KLUG, CHRISTOPH; Neuregelungen zur Bestellung betrieblicher Datenschutzbeauftragter, NJW 2007, S. 118–122.
GOLA, PETER/WRONKA, GEORG; Handbuch zum Arbeitnehmerdatenschutz, 5. Auflage, Frechen-Königsdorf 2009.
GÖPFERT, BURKARD/MERTEN, FRANK/SIEGRIST, CAROLIN; Mitarbeiter als „Wissensträger" – Ein Beitrag zur aktuellen Compliance-Diskussion, NJW 2008, S. 1703–1709.

GÖTZE, CORNELIUS; Auskunftserteilung durch GmbH-Geschäftsführer im Rahmen der Due Diligence beim Beteiligungserwerb, ZGR 1999, S. 202–233.
GRAN, ANDREAS; Abläufe bei Mergers & Acquisitions, NJW 2008, S. 1409–1415.
GROßE VORHOLT, ANDRE; Wirtschaftsstrafrecht, 2. Auflage, München 2006.
GRUNDMEIER, CHARLOTTE; Rechtspflicht zur Compliance im Konzern, 1. Auflage, Köln 2011.
GRÜTZNER, THOMAS/JAKOB, ALEXANDER; Compliance von A-Z, 1. Auflage, München 2010.
HAGENKÖTTER, ANDREAS; Die Digitale Steuerprüfung – Neue Formen des Datenzugriffs der Finanzverwaltung seit 1.1.2002, NJW 2002, S. 1977–1983.
HAMANN, WOLFGANG; Kurswechsel bei der Arbeitnehmerüberlassung?, NZA 2011, S. 70–77.
HANLOSER, STEFAN; Gesetz zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften – Regierungsentwurf, MMR 2/2009, V–VI.
HAPP, RICHARD; Beilegung von Steuerstreitigkeiten zwischen Investoren und ausländischen Staaten durch Schiedsgerichte, IStR 2006, S. 649–655.
HASSELBACH, KAI; Die Weitergabe von Insiderinformationen bei M&A – Transaktionen mit börsennotierten Aktiengesellschaften – Unter Berücksichtigung des Gesetztes zur Verbesserung des Anlegeschutzes vom 28.10.2004, NZG 2004, S. 1087–1095.
HARDECK, INGA; Die Empfehlungen der OECD-Leitsätze für multinationale Unternehmen im Bereich der Besteuerung, IStR 2011, S. 933–939.
HAUSCHKA, CHRISTOPH E.; Der Compliance-Beauftragte im Kartellrecht – Absicherungsstrategien für mittelständische Unternehmen und deren Organe, BB 2004, S. 1178–1182.
HAUSCHKA, CHRISTOPH E.; Compliance am Beispiel der Korruptionsbekämpfung, ZIP 2004, S. 877–883.
HAUSCHKA, CHRISTOPH E.; Corporate Compliance – Unternehmensorganisatorische Ansätze zur Erfüllung der Pflichten von Vorständen und Geschäftsführern, AG 2004, S. 461–475.
HAUSCHKA, CHRISTOPH E.; Der Compliance-Beauftragte im Kartellrecht, BB 2004, S. 1178–1182.
HAUSCHKA, CHRISTOPH E.; Von Compliance zu Best Practice, ZRP 2006, S. 258–261.
HAUSCHKA, CHRISTOPH E.; Die Voraussetzungen für ein effektives Compliance System i. S. von § 317 Abs. 4 HGB, DB 2006, S. 1143–1146.
HAUSCHKA, CHRISTOPH E. (*HRSG.*); Corporate Compliance, 2. Auflage, München 2010.
HAUSCHKA, CHRISTOPH E.; Compliance – Praktische Erfahrungen und Thesen, Gesellschaftsrecht in der Diskussion 2007, S. 51–59.
HAUSCHKA, CHRISTOPH E./GREEVE, GINA; Compliance in der Korruptionsprävention – was müssen, was sollen, was können die Unternehmen tun?, BB 2007, S. 165–173.
HECKMANN, DIRK; Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen, MMR 2006, S. 280–285.
HEIDEL, THOMAS; Aktienrecht und Kapitalmarktrecht, 3. Auflage, Hamburg 2011.
HEIDEL, THOMAS; Zur Weisungsgebundenheit von Aufsichtsratsmitgliedern bei Beteiligung von Gebietskörperschaften und Alleinaktionären, NZG 2012, S. 48–54.
HENSSLER, MARTIN/BRAUN, AXEL, Arbeitsrecht in Europa, 3. Auflage, Köln 2011.
HERBERT, MANFRED/OBERRATH, JÖRG-DIETER; Schweigen ist Gold? Rechtliche Vorgaben für den Umgang des Arbeitnehmers mit seiner Kenntnis über Rechtsverstöße im Betrieb, NZA 2005, S. 193–199.
HETZER, WOLFGANG; Verbandsstrafe in Europa, EuZW 2007, S. 75–80.
HILD, ECKART C.; Outsourcing von Compliance-Funktionen: Anwalt als Ombudsmann, AnwBl. 2010, S. 641–643.
HOFFMANN-BECKING, MICHAEL; Münchener Handbuch des Gesellschaftsrechts AG, 3. Auflage, München 2007.
HOFFMANN-BECKING, MICHAEL; Zur rechtlichen Organisation der Zusammenarbeit im Vorstand der AG, ZGR 1998, S. 497–519.

HÖLTERS, WOLFGANG; Handbuch des Unternehmens- und Beteiligungskaufs, 6. Auflage, Köln 2005.
HOPSON, MARK D./KOEHLER, KRISTIN GRAHAM; Effektive Compliance – Programme im Sinne der United States Federal Sentencing Guidelines, CCZ 2008, S. 208–213.
HORNUNG, GERRIT; Eine Datenschutz-Grundverordnung für Europa?, ZD 2012, S. 99–106.
HUBER, ERICH/SEER, ROMAN; Steuerverwaltung im 21. Jahrhundert: Risikomanagement und Compliance, StuW 2007, S. 355–371.
HÜFFER, UWE; Die leistungsbezogene Verantwortung des Aufsichtsrats, NZG 2007, S. 47–54.
HÜFFER, UWE; Compliance im Innen- und Außenrecht der Unternehmen, Festschrift G.H. Roth 2011, S. 299–308.
HÜFFER, UWE; Aktiengesetz, 10. Auflage, Bad Dürkheim/Mannheim 2012.
HUGGER, HEINER/RÖHRICH, RAIMUND; Der neue UK Bribary Act und seine Geltung für deutsche Unternehmen, BB 2010, S. 2643–2647.
ILLING, DIANA/UMNUß, KARSTEN; Die arbeitsrechtliche Stellung des Compliance Managers– insbesondere Weisungsunterworfenheit und Reportingpflichten, CCZ 2009, S. 1–8.
IMMENGA, ULRICH; Compliance als Rechtspflicht nach Aktienrecht und Sarbanes-Oxley-Act, Festschrift Schwark 2009, S. 199–218.
IMMENGA,ULRICH/MESTMÄCKER, ERNST-JOACHIM, Wettbewerbsrecht. GWB. Kommentar, 4. Auflage, München, 2007.
IMMENGA, ULRICH/MESTMÄCKER, ERNST-JOACHIM; Wettbewerbsrecht Band 2: GWB, 4. Auflage, München 2011.
ITZEN, UTA; Richtungswechsel, Bestandsaufnahme, Prävention: Das Gerüst einer erfolgreichen Compliance-Strategie, BB-Special 2008, Nr. 5, S. 12–16.
JANSSEN, HELMUT; Einsicht in Kronzeugenakten – Was bedeutet das Pfleiderer – Urteil in der Praxis?; in : Schwerpunkte des Kartellrechts 2011, 19 ff.
KAMP, MAIKE/KÖRFER BARBARA; Auswirkungen des § 32 BDSG auf die Aufgabenerfüllung und die strafrechtliche Verantwortung des Compliance Officers, RDV 2010, S. 72–76.
KAPP, THOMAS; Kartellrecht in der Unternehmenspraxis – was Unternehmer und Manager wissen müssen, Wiesbaden 2005.
KAPP, THOMAS; Kartellbehörde durchsucht Geschäftsräume – Was ist zu beachten?, Compliance Report Oktober, Heft 10, 2007, S. 3–5.
KAPPEL, JAN/EHLING, JAN; Wie viel Strafe ist genug? – Deutsche Unternehmen zwischen UK Bribary Act, FCBA und StGB, BB 2011, S. 2115–2121.
KIETHE, KURT; Vermeidung der Haftung von geschäftsführenden Organen durch Corporate Compliance, GmbHR 2007, S. 393–400.
KINDLER, PETER; Pflichtverletzung und Schaden bei der Vorstandshaftung wegen unzureichender Compliance, Festschrift G.H. Roth 2011, S. 367–378.
KINZL, ULRICH-PETER; Wie angemessen muss „angemessene Information" als Grundlage für Vorstandsentscheidungen sein?, DB 2004, S. 1653–1654.
KLASEN, EVELYN/SCHAEFER, SANDRA; Einsichtsrechte von Arbeitnehmern und Beteiligten bei unternehmensinternen Untersuchungen, DB 2012, S. 1384–1387.
KLEIN, FRANZ; Abgabenordnung: AO, 11. Auflage, München 2012.
KLINDT, THOMAS/PELZ, CHRISTIAN/THEUSINGER, INGO; Compliance im Spiegel der Rechtsprechung, NJW 2010, S. 2385–2391.
KOCH, BENJAMIN; Ausgewählte Themen der IP-Compliance; CCZ 2010, S. 70–73.
KOCH, HANS-DIETRICH (*HRSG.*); Der betriebliche Datenschutzbeauftragte – Aufgaben, Voraussetzungen, Anforderungen, 6. Auflage, Frechen 2006.
KOCH, JENS; Der kartellrechtliche Sanktionsdurchgriff im Unternehmensverbund, ZHR 171 (2007), S. 554–580.

KOCH, JENS; Compliance-Pflichten im Unternehmensverbund?, WM 2009, S. 1013–1020.
KÖRBER, THORSTEN; Geschäftsleitung der Zielgesellschaft und Due Diligence bei Paketerwerb und Unternehmenskauf, NZG 2002, S. 263–272.
KORT, MICHAEL; Verhaltensstandardisierung durch Corporate Compliance, NZG 2008, S. 81–86.
KORT, MICHAEL; Ethik-Richtlinien im Spannungsfeld zwischen US-amerikanischer Compliance und deutschem Konzernbetriebsverfassungsrecht, NJW 2009, S. 129–133.
KORT, MICHAEL; Compliance-Pflichten von Vorstandsmitgliedern und Aufsichtsratsmitgliedern, Festschrift Hopt 2010, S. 983–1004.
KRAMER, PHILIPP, Dix in Hamburg: „§ 32 BDSG ist ein Baustellenschild", DSB 05/2010, S. 14–16.
KREMER, THOMAS/KLAHOLD CHRISTOPH; Compliance-Programme in Industriekonzernen, ZGR 2010, S. 113–143.
KRIEGER, GERD (*HRSG.*)/SCHNEIDER, UWE H.(*HRSG.*); Handbuch Managerhaftung – Risikobereiche und Haftungsfolgen für Vorstand, Geschäftsführer und Aufsichtsrat, 2. Auflage, Köln 2010.
KRÖLL, STEFAN; Die Entwicklung des Rechts der Schiedsgerichtsbarkeit 2005/2006, NJW 2007, S. 743–749.
LACKNER, KARL/KÜHL, KRISTIAN; Strafgesetzbuch: Kommentar; 27. Auflage, München 2011.
LEISCH, FRANZ CLEMENS/LOHNER, ANDREAS; Compliance-Risiken im Transaktionsgeschäft, M&A-Review, S. 133–136.
LEMBKE, MARK; Arbeitnehmerüberlassung im Konzern, BB 2012, S. 2497–2505.
LEUCHTEN, ALEXIUS; Das neue Recht der Leiharbeit, NZA 2011, S. 608–612.
LI, GUANG/FRIK, ROMAN; Das neue Arbeitsvertragsgesetz Chinas, NZA 2008, S. 86–91.
LIESE JENS; Much Adoe About Nothing? oder: Ist der Vorstand einer AG verpflichtet, eine Compliance-Organisation zu implementieren?, BB-Special 2008, Nr. 5, S. 17–22.
LIESE JENS; Die Offenlegung vertraulicher Verträge in Due Diligence-Verfahren, DB 2010, S. 1806–1811.
LIESE JENS; Compliance in Due Diligence-Fragelisten, BB Special 4/2010, S. 27–30.
LINSMEIER, PETRA/BALSSEN, JAN; Die Kommission macht Ernst: Erstmals Durchsuchungen wegen Gun Jumping, BB 2008, S. 741–748.
LÖSLE, ALF-CHRISTIAN/MAUDRICH, ARMIN HANS; Die Prüfung des internen Kontrollsystems, DSWR 2006, S. 5–8.
LÖSLER, THOMAS; Das moderne Verständnis von Compliance im Finanzmarktrecht, NZG 2005, S. 104–108.
LÖSLER, THOMAS; Spannungen zwischen der Effizienz der internen Compliance und möglichen Reporting-Pflichten des Compliance-Officers, WM 2007, S. 676–683.
LUTTER, MARCUS; Haftung und Haftungsfreiräume des GmbH-Geschäftsführers – 10 Gebote an den Geschäftsführer; GmbHR 2000, S. 301–312.
LUTTER, MARCUS; Konzernphilosophie vs. konzernweite Compliance und konzernweites Risikomanagement, Festschrift Goette 2011, S. 289–298.
LUTTER, MARCUS/HOMMELHOFF PETER; GmbH-Gesetz, 18. Auflage, Köln 2012.
MAHNHOLD, THILO; „Global Whistle" oder „deutsche Pfeife" – Whistleblowing-Systeme im Jurisdiktionskonflikt, NZA 2008, S. 737–743.
MASCHMANN, FRANK (*HRSG.*); Corporate Compliance und Arbeitsrecht – Mannheimer Arbeitsrechtstag 2009,
MENGEL, ANJA; Arbeitsrechtliche Besonderheiten der Implementierung von Compliance Programmen in internationalen Konzernen, CCZ 2008, S. 85–91.
MENGEL, ANJA/HAGEMEISTER, VOLKER; Compliance und Arbeitsrecht, BB 2006, S. 2466–2471.
MENGEL, ANJA/HAGEMEISTER, VOLKER; Compliance und arbeitsrechtliche Implementierung im Unternehmen, BB 2007, S. 1386–1392.

MEYER, UWE; Ethikrichtlinien internationaler Unternehmen und deutsches Arbeitsrecht, NJW 2006, S. 3605–3609.
MOLL, WILHELM; Münchener Anwaltshandbuch Arbeitsrecht, 3. Auflage, München 2012.
MOOSMAYER, KLAUS; Compliance – Praxisleitfaden für Unternehmen, 2. Auflage, München 2012.
MOOSMAYER, KLAUS; Modethema oder Pflichtprogramm guter Unternehmensführung? – Zehn Thesen zu Compliance, NJW 2012, S. 3013–3017.
MÜLLER-BONANNI, THOMAS/SAGAN, ADAM; Arbeitsrechtliche Aspekte der Compliance, BB-Special 2008, Nr. 5, S. 28–32.
OBERTHÜR, NATHALIE; Die Neuregelung des AÜG, ArbRB 2011, S. 146–149.
OBERTHÜR, NATHALIE; Auskunftspflicht des Arbeitnehmers im Rahmen von Compliance-Maßnahmen, ArbRB 2011, S. 184–186.
OBERWETTER, CHRISTIAN; Arbeitnehmerrechte bei Lidl, Aldi & Co., NZA 2008, S. 609–913.
OELSCHLÄGEL, KAY/SCHOLZ, JOCHEN; Handbuch Versandhandelsrecht – E-Commerce, M-Commerce, Katalog, 1. Auflage, Köln 2012.
OHRTMANN, NICOLA; Compliance – Anforderungen an ein rechtskonformes Verhalten öffentlicher Unternehmen, 2009.
OLBING, KLAUS; Tax Compliance in der Krise, AG 2010, S. 583–584.
PALANDT, OTTO; Bürgerliches Gesetzbuch: BGB, 71. Auflage, München 2012.
PAMPEL, GUNNAR; Die Bedeutung von Compliance-Programmen im Kartellordnungswidrigkeitenrecht, BB 2007, S. 1636–1639.
PARSOW, CHRISTIAN; Verzahnung Tax, Krisenmanagement und Compliance, DB 2011, Heft 26/27, M1.
PEEMÖLLER, VOLKER H./REINEL-NEUMANN, BIRGIT; Corporate Governance und Corporate Compliance im Akquisitionsprozess, BB 2009, S. 206–210.
PETRAK, LARS/SCHNEIDER, JULIA; Compliance und Steuern: Praxistipps zur Vermeidung wirtschaftlicher Risiken, BC 2008, S. 11–16.
PFAR, MICHAEL/REHLING, STEFFEN; Besteuerung deutscher Investitionen in Indonesien, IStR 2011, S. 828–835.
PFEIFER, UWE; Solvency II – ein Thema für die IT?, VW 2005, S. 1558.
PIETZKE, RUDOLF; Die Verantwortung für Risikomanagement und Compliance im mehrköpfigen Vorstand, CCZ 2010, S. 45–53.
PÖRNBACHER, KARL/MARK, JONAS; Auswirkungen des UK Bribery Act 2010 auf deutsche Unternehmen, NZG 2010, S. 1372–1375.
PÖRNBACHER, KARL/KNIEF, INKEN; Novelle der CIETAC-Schiedsordnung – neue Perspektiven in der Streitschlichtung zwischen deutschen und chinesischen Unternehmen, BB 2012, S. 2967–2969.
POWILLEIT, SIMONE; Compliance im Unternehmen: Rechtliches Risikomanagement als Wertschöpfungsfaktor, GWR 2010, S. 28–32.
PRATTER, KIRSTEN/EICHENBERGER, O.; Tax Risk Management im Konzern, Der Schweizer Treuhänder, Heft 5/2012, S. 376 ff.
PREUSSNER, JOACHIM; Risikomanagement im Schnittpunkt von Bankaufsichtsrecht und Gesellschaftsrecht, NZG 2004, S. 57–61.
PROSS, ACHIM/CZAKERT, ERNST; Die Bedeutung von rechtzeitigen, gezielten und umfassenden Informationen zur Bekämpfung aggressiver Steuerplanung, IStR 2011, S. 277–278.
RATH, MICHAEL/SPONHOLZ, RAINER; IT-Compliance, Berlin 2009.
RATH, MICHAEL/KLUG, SASKIA; e-Discovery in Germany?, K&R 2008, S. 596–600.
RATH, MICHAEL/MAIWORM, CHRISTOPH; Weg frei für Second-Hand Software?; WRP 2012, S. 1051–1055.

RAUM, ROLF; Strafrechtliche Pflichten von Compliance-Beauftragten, CCZ 2012, S. 197–198.
RAUS, NADJA/LÜTZELER, MARTIN; Berichtspflicht des Compliance Officers – zwischen interner Eskalation und externer Anzeige, CCZ 2012, S. 96–101.
REICHERT, JOCHEM/OTT, NICOLAS; Non Compliance in der AG – Vorstandspflichten im Zusammenhang mit der Vermeidung, Aufklärung und Sanktionierung von Rechtsverstößen, ZIP 2009, S. 2173–2178.
REITHMANN, CHRISTOPH/MARTINY, DIETER; Internationales Vertragsrecht, 7. Auflage, Köln 2009.
RIEBLE, VOLKER/KLEBECK, ULF; Strafrechtliche Risiken der Betriebsratsarbeit, NZA 2006, S. 758–769.
RINGLEB, HENRIK-MICHAEL/KREMER, THOMAS/LUTTER, MARCUS/WERDER, AXEL VON(*HRSG.*); Kommentar zum Deutschen Corporate Governance Kodex, 4. Auflage, München 2010.
RITTMEISTER, MAXIMILIAN; Due Diligence und Geheimhaltungspflichten beim Unternehmenskauf – Die Zulässigkeit der Gestattung einer Due Diligence durch den Vorstand oder die Geschäftsführer der Zielgesellschaft, NZG 2004, S. 1032–1037.
RODEWALD, JÖRG/UNGER, ULRIKE; Corporate Compliance – Organisatorische Vorkehrungen zur Vermeidung von Haftungsfällen der Geschäftsleitung, BB 2006, S. 113–117.
RODEWALD, JÖRG/UNGER, ULRIKE; Kommunikation und Krisenmanagement im Gefüge der Corporate Compliance-Organisation, BB 2007, S. 1629–1634.
ROSBACH, THORSTEN; Ethik in einem Wirtschaftsunternehmen – nützlich oder überflüssige Förmelei?, CCZ 2008, S. 101–104.
ROßNAGEL, ALEXANDER (*HRSG.*); Handbuch Datenschutzrecht, München 2003.
ROßNAGEL, ALEXANDER/JANDT, SILKE; Rechtskonformes Direktmarketing – Gestaltungsanforderungen und neue Strategien für Unternehmen, MMR 2011, S. 69–91.
ROTH, GÜNTER H./ALTMEPPEN, HOLGER; GmbHG Kommentar, 7. Auflage, Innsbruck/Passau 2012.
ROTH, BIRGIT/SCHNEIDER, UWE K.; IT-Sicherheit und Haftung, ITRB 2005, S. 19–22.
ROWEDDER, HEINZ/SCHMIDT-LEITHOFF, CHRISTIAN; GmbHG, 4. Auflage, München 2002.
RÜBENSTAHL, MARKUS; Der Foreign Corrupt Practices Act (FCPA) der USA, NZWiST 2012, S. 401–407.
RUDOLF, INGE; Aufgaben und Stellung des betrieblichen Datenschutzbeauftragten, NZA 1996, S. 296–301.
RUST, ULRICH/ABEL, MALTE; Unternehmensinterne Untersuchungen im Spannungsverhältnis zwischen Unternehmens-, Arbeits- und Straf(prozess)recht, ZWeR 2012, 521
SÄCKER, FRANZ; Gesetzliche und satzungsmäßige Grenzen für Spenden und Sponsoring Maßnahmen in der Kapitalgesellschaft, BB 2009, S. 282–286.
SALVENMOSER, STEFFEN/HAUSCHKA, CHRISTOPH E.; Korruption, Datenschutz und Compliance, NJW 2010, S. 331–335.
SCHEEL, THOMAS; Haftung, Beck'sches Steuer- und Bilanzrechtslexikon, Edition 3/12, München 2012.
SCHEMMEL, ALEXANDER/HACKER, PHILIPP; Korruptionsamnestie – Eine neue Vokabel im nachhaltigen Kampf gegen Korruption, ZRP 2009, S. 4–6.
SCHIMMELPFENNIG, HANS-CHRISTOPH; Die externe Ombudsstelle – Risiko für die Wirksamkeit außerordentlicher Kündigungen, CCZ 2008, S. 161–166.
SCHLÜTER, MARKUS; Grundzüge des thailändischen Investitionsrechts, RiW 2011, S. 207–213.
SCHMIDT, KARSTEN/LUTTER MARCUS; Aktiengesetz Kommentar, 2. Auflage, Köln 2010.
SCHNEIDER, DAVID/SITTARD, ULRICH; Ethikrichtlinien als Präventionsmaßnahmen i. S. des § 12 AGG?, NZA 2007, S. 654–657.
SCHNEIDER SVEN/SCNEIDER UWE H.; Vorstandshaftung im Konzern, AG 2005, S. 57–66.
SCHNEIDER, UWE H.; Compliance als Aufgabe der Unternehmensleitung, ZIP 2003, S. 645–650.

SCHNEIDER, UWE H.; Compliance im Konzern, NZG 2009, S. 1321–1328.
SCHNEIDER, UWE H./SCHNEIDER, SVEN H.; Konzern-Compliance als Aufgabe der Konzernleitung, ZIP 2007, S. 2061–2065.
SCHOLZ, FRANZ; GmbHG, 11. Auflage, Köln 2012.
SCHOLZ, MATTHIAS/LUTZ, HOLGER; Standardvertragsklausel für Auftragsverarbeiter und § 11 BDSG, CR 2011, S. 424–428.
SCHÖNKE, ADOLF/SCHRÖDER, HORST (*HRSG.)*; Strafgesetzbuch Kommentar, 28. Auflage, München 2010.
SCHREINER, PAUL/RÜTZ, EVA-MARIA; Arbeitnehmerüberlassung bei Kooperationsvereinbarungen im Gesundheitswerden, MedR 2012, S. 373–377.
SCHREY, JOACHIM/KRUPNA, KARSTEN; Softwarelizenzmanagement – Ein unterschätztes Compliance – Risiko, CCZ 2012, S. 141–143.
SCHUMACHER, ANKE; Legal Privilege – auch bei Syndikusanwälten?, in: Compliance Report Heft 10/2007, S. 12 ff.
SCHULZ, MIKE; Compliance – Internes Whistleblowing, BB 2011, S. 629–634.
SCHUSTER, DORIS-MARIA/DARSOW, INGEBJÖRG; Einführung von Ethikrichtlinien durch Direktionsrecht, NZA 2005, S. 273–277.
SCHWARZ, ALEXANDRA; Die strafrechtliche Haftung des Compliance-Beauftragten, wistra 2012, S. 13–18.
SCHWARZ, BENNO, FCPA Compliance Monitorships – US Marotte oder Flavor of the New Times? Praktische Erfahrungen mit FCPA Compliance Monitorships, CCZ 2011, S. 59–63.
SCHWEDHELM, ROLF; Tax Compliance – mehr als ein Trend, AnwBl. 2009, S. 90.
SCHWINTOWSKI, HANS-PETER; Gesellschafsrechtliche Anforderungen an Vorstandshaftung und Corporate Governance durch das neue System der kartellrechtlichen Legalausnahme, NZG 2005, S. 200–203.
SEDEMUND, JAN; Der Verfall von Unternehmensvermögen bei Schmiergeldzahlungen durch die Geschäftsleitung von Organgesellschaften, DB 2003, S. 323–329.
SEER, ROMAN; Die Rolle des Steuerberaters in einer elektronischen Finanzverwaltung, DStR 2008, S. 1553–1560.
SEMLER, JOHANNES/PELTZER, MARTIN; Arbeitshandbuch für Vorstandsmitglieder, München 2005.
SEMLER, JOHANNES/VOLHARD, RÜDIGER; Arbeitshandbuch für Unternehmensübernahmen; Band 1/2, München 2003.
SIEG, RAINER; Arbeitnehmer im Banne von Compliance – Programmen – zwischen Zivilcourage und Denunziantentum, Festschrift zum 70.Geburtstag von Herbert Bruchner, S. 859–874.
SIMITIS, SPIROS (*HRSG.*); NomosKommentar zum Bundesdatenschutzgesetz, 7. Auflage, Baden-Baden 2011.
SIMONET, MICHAEL, Die Implementierung interner Whistleblowingsysteme im Rahmen der Corporate Governance, Berlin 2012.
SKOPP, HANNS R./GREIPL, DIETER; Die Prüfung des IT-Systems durch den Abschlussprüfer, DSWR 2006, S. 2–4.
SPENGEL, CHRISTOPH/MATENAER, SEBASTIAN; Tax Risk Management – Strategische, prozessuale und organisationale Einflussfaktoren; Ubg 10/2011, S. 798–811.
SPINDLER, GERALD; Compliance in der multinationalen Bankengruppe, WM 2008, S. 905–918.
SPINDLER, GERALD/STILZ, EBERHARD; Kommentar zum Aktiengesetz, 2. Auflage, Göttingen/Stuttgart 2010.
STEGER, UDO; Rechtliche Verpflichtungen zur Notfallplanung im IT-Bereich, CR 2007, S. 137–143.
STRAUBE, GUNNAR/KLAGGES, RHEA-CHRISTINA; Beschäftigtendatenschutzgesetz: Wiedervorlage in vier Jahren?, ArbRAktuell 2012, 328271.

STRECK, MICHAEL/BINNEWIES, BURKHARD; Tax Compliance, DStR 2009, S. 229–234.
STRECK, MICHAEL/MACK, ALEXANDRA/SCHWEDHELM, ROLF; Tax Compliance, 1. Auflage, Köln 2010.
TALASKA, PETER; Tax Compliance in Unternehmen – Organhaftung, BB 2012, S. 1195–1200.
THÜSING, GREGOR; Arbeitnehmerdatenschutz und Compliance, 1. Auflage, München 2010.
THÜSING, GREGOR; Licht und Schatten im Entwurf des neuen Bundesdatenschutzgesetzes, RDV 2010, S. 147–149.
TINNEFELD, MARIE-THERES/EHMANN, EUGEN/GERLING, RAINER W.; Einführung in das Datenschutzrecht, 4. Auflage, München 2005.
TINNEFELD, MARIE-THERES/PETRI, THOMAS/BRINK, STEFAN; Aktuelle Fragen um ein Beschäftigtendatenschutzgesetz, MMR 2010, S. 727–735.
TIPKE, KLAUS/KRUSE, HEINRICH WILHELM/SEER, ROMAN; Abgabenordnung/Finanzgerichtsordnung, Loseblatt, Stand Sept 2009, Köln.
TRAPPE, JOHANNES; Zur Schiedsgerichtsbarkeit der CIETAC, SchiedsVZ 2006, S. 258–270.
UMNUß, KARSTEN; Corporate Compliance Checklisten, Rechtliche Risiken im Unternehmen erkennen und vermeiden, 2. Auflage, München 2012.
VATER, HENDRIK/REINHARD, HARTMUT; Praxishandbuch Kostensenkungspläne, 1. Auflage, Weinheim 2012.
VEIL, RÜDIGER; Krisenbewältigung durch Gesellschaftsrecht, ZGR 2006, S. 374–397.
VERSE, DIRK A.; Compliance im Konzern, ZHR 175(2011), S. 401–424.
VETTER, EBERHARD; Die Änderungen 2007 des Deutschen Corporate Governance Kodex, DB 2007, S. 1963–1968.
VETTER, EBERHARD; Zur Compliance-Verantwortung des Vorstands und zu den Compliance-Aufgaben des Aufsichtsrats, Festschrift Friedrich Graf von Westphalen, 2010, S. 719–739.
VETTER, EBERHARD; Der Prüfungsausschuss in der AG nach dem BilMoG, ZGR 2010, S. 751–793.
VETTER, EBERHARD; Zur Compliance-Verantwortung des Aufsichtsrats in eigenen Angelegenheiten, Liber Amicorum Martin Winter 2011, S. 701–733.
VETTER, EBERHARD; Corporate Governance in der GmbH – Aufgaben des Aufsichtsrats der GmbH, GmbHR 2011, S. 449–459.
VOET VAN VORMIZEELE, PHILIPP; Kartellrechtliche Compliance – Programme im Rahmen der Bußgeldbemessung *de lege lata* und *de lege ferenda*, CCZ 2009, S. 41–49.
VOIGT, PAUL/ALICH, STEFAN; Facebook-Like-Button und Co. – Datenschutzrechtliche Verantwortlichkeit der Webseitenbetreiber, NJW 2011, S. 3541–3544.
WAGNER, AXEL-MICHAEL/BLAUFUSS, HENNING; Datenexport als juristische Herausforderung: Cloud Computing, BB 2012, S. 1751.
WEBER, JÜRGEN/VATER, HENRIK/SCHMIDT, WALTER/REINHARD, HARTMUT; Turnaround – Navigation in stürmischen Zeiten, 1. Auflage, Weinheim 2011.
WEGEN, GERHARD/RAIBLE, MARTIN; Unterschätzt die deutsche Wirtschaft die Wirksamkeit des völkerrechtlichen Investitionsschutzes?, SchiedsVZ 2006, S. 225–236.
WEGNER, CHRISTOF/EHRLICH, WOLFGANG/WEITH, NILS; Grundzüge der Exportkontrolle, 2006.
WEICHERT, THILO; Datenschutzstrafrecht – ein zahnloser Tiger?, NStZ 1999, S. 490–496.
WEIDLICH, THOMAS/FIETZ, EIKE H.; Schmiergeldzahlungen in Asien – Rechtliche Risiken für deutsche Mitarbeiter in Singapur und Hongkong, RiW 2005, S. 362–370.
WERNER, RÜDIGER; Sorgfaltspflichten des Geschäftsführers bei Unternehmensakquisitionen, GmbHR 2007, S. 678–682.
WESTERMANN, HARM PETER; Gesellschafter- und Geschäftsführerpflichten im Vorfeld der Insolvenz nach gegenwärtigem und künftigem Recht, DZWir 2006, S. 485–494.
WIEDEMANN, GERHARD; Handbuch des Kartellrechts. 2. Auflage, München 2008.

WIEDERHOLT, NORBERT/WALTER, ANDREAS; Compliance – Anforderungen an die Unternehmensorganisationspflichten, BB 2011, S. 968–972.
WILLEMSEN, REINHARD/RECHEL, JANINE; Kommentar zum ESUG, Frankfurt 2012.
WINTER, MARTIN; Die Verantwortlichkeit des Aufsichtsrats für „Corporate Compliance", Festschrift Hüffer 2010, S. 1103–1128.
WOLFFGANG, HANS-MICHAEL/NATZEL, JULIA; Fortentwicklung des Zollrechts durch Sicherheitsänderungen und Modernisierten Zollkodex, EuZW 2008, S. 39–44.
WOLKE, THOMAS; Risikomanagement, 2. Auflage, 2008.
WULF, MARTIN; Tax Compliance als Fels steueranwaltlicher Tätigkeit, AnwBl 2010, S. 656–659.
WURZER, ALEXANDER J.; Know-how-Schutz als Teil des Compliance-Managements, CCZ 2009, S. 49–56.
WYBITUL, TIM/FLADUNG, ARMIN; EU-Datenschutz-Grundordnung – Überblick und arbeitsrechtliche Betrachtung des Entwurfs, BB 2012, S. 509–515.
WYBITUL, TIM/PATZAK, ANDREA; Neue Anforderungen beim grenzüberschreitenden Datenverkehr, RDV 2011, S. 11–18.
YANG, HONGGUANG; Das IT-Vorgehensmodell in der GoBS-Verfahrensdokumentation, VW 2012, S. 1132.
ZIEGLER, OLAF; Due Diligence im Spannungsfeld zur Geheimhaltungspflicht von Geschäftsführern und Gesellschaftern, DStR 2000, S. 249–255.
ZÖCHLING, HANS; Tax Controlling in der Praxis (f. Österreich), 1. Auflage, Wien 2012.

Sachverzeichnis

G. Wecker, B. Ohl (Hrsg.), *Compliance in der Unternehmerpraxis*,
DOI 10.1007/978-3-658-00893-2, © Springer Fachmedien Wiesbaden 2013