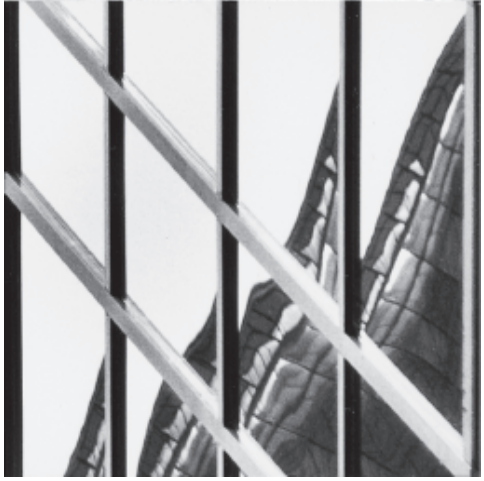

DEUTSCHES AKTIENINSTITUT

Internal Investigations bei Compliance-Verstößen

Praxisleitfaden für die Unternehmensleitung

WILLKIE FARR & GALLAGHER LLP

GDD GESELLSCHAFT FÜR DATENSCHUTZ UND DATENSICHERHEIT e.V.

FEIGEN · GRAF Rechtsanwälte

Deloitte.

Studien des Deutschen Aktieninstituts, Heft 48
Herausgegeben von Prof. Dr. Rüdiger von Rosen
Frankfurt am Main, August 2010

Herausgeber: Prof. Dr. Rüdiger von Rosen
Deutsches Aktieninstitut e.V. Tel. 0 69/9 29 15-0
Niedenau 13-19 Fax 0 69/9 29 15-12
60325 Frankfurt a. M. http://www.dai.de

Autoren:			
	Jan Bremer	0 69/9 29 15-36	bremer@dai.de
	Dr. Bernd Groß	0 69/7 70 19 6-0	gross@feigen-graf.de
	Uwe Heim	0 69/7 569 56-080	uheim@deloitte.de
	Rolf Hünermann	0 69/7 93 02-163	rhuenermann@willkie.com
	Andreas Jaspers	0 228/6 94 31-3	jaspers@gdd.de
	Michael Lorenz	0 69/7 569 56-036	mlorenz@deloitte.de
	Dr. Christian Rolf	0 69/7 93 02-151	crolf@willkie.com

1. Auflage, August 2010

ISBN 978-3-934579-62-0

Internal Investigations bei Compliance-Verstößen

Studien des Deutschen Aktieninstituts, Heft 48

Vorwort

Die Bedeutung von Compliance-Fragen für die Unternehmenspraxis nimmt stetig zu. Die wachsende Zahl von Medienberichten über Korruptionsfälle, Kartellvergehen oder andere Rechtsverstöße vor allem in internationalen Konzernen belegt dies. Die finanziellen Sanktionen, insbesondere Bußgelder, die aus einem Compliance-Verstoß resultieren, können sich für Unternehmen gerade in Krisenzeiten existenzbedrohend auswirken. Beispielhaft sind die von der EU-Kommission verhängten Kartellgeldbußen, die zuweilen eine dreistellige Millionenhöhe erreichen. Umso unverständlicher ist es, dass viele Unternehmen bislang unter anderem aus Aufwands- und Kostengründen mit dem Aufbau eines Compliance-Programms zögern. Zur Verhinderung folgenschwerer Rechtsverstöße ist ein funktionierendes Compliance-System essentiell.

Das Thema Compliance scheint noch immer einen besonders sensiblen Bereich zu berühren. Insgesamt dürften sich Vorstands- und Aufsichtsratsmitglieder noch zu wenig mit den damit verbundenen Fragen beschäftigen. Dabei geht es nicht nur um Kartellabsprachen und Korruptionsvorwürfe. Vielmehr ist die Einhaltung sämtlicher für das Unternehmen relevanter Rechtsvorschriften und vom Unternehmen selbst gesetzter interner Regeln Gegenstand der Compliance. International agierende Unternehmen stehen vor besonderen Herausforderungen, da grundsätzlich mehreren Rechtssystemen entsprochen werden muss. Problematisch in der Praxis ist dabei der Umgang mit ständig neuen nationalen und internationalen Rechtsvorschriften. Genannt sei nur beispielhaft die jüngste US-Gesetzgebung, der *Dodd–Frank Wall Street Reform and Consumer Protection Act,* wonach Mitarbeiter, die Compliance-Verstöße melden, unter gewissen Voraussetzungen signifikante Belohnungen staatlicherseits erhalten.

Neben der Präventivfunktion, die ein Compliance-System zu erfüllen hat, stellt sich für Unternehmen immer häufiger die Frage, wie mit Anhaltspunkten für oder Kenntniserlangung von Rechtsverstößen umzugehen ist. Welche konkreten Maßnahmen sollten auf Unternehmensebene ergriffen werden? Ein in Frage kommendes Management-Tool, das immer populärer wird, wenngleich nicht unumstritten ist, ist eine unternehmensinterne Sonderermittlung (*Internal Investigation*) zur Aufklärung der Vorwürfe. Letztere kann zum einen nötig sein, um Lücken im Compliance-System im Hinblick auf aufgedeckte Missstände zu schließen. Von einigen Rechtsordnungen wird die unternehmenseigene Aufklärung

aber auch explizit verlangt. Ferner kann eine *Internal Investigation* dem Erhalt bzw. der Wiederherstellung der Reputation der Gesellschaft förderlich sein. Gerade bei Kartellgeldbußen oder anderen Bußgeldverfahren kommt dem Gedanken des Vermögenserhalts besondere Bedeutung zu. Intern spielt die Wiederherstellung von Arbeitsmoral und Betriebsklima eine entscheidende Rolle. Überdies wird eine interne Aufklärung zwecks Kooperation mit Ermittlungsbehörden von vielen Jurisdiktionen mit Strafmilderung, manchmal gar Straffreiheit oder dem Erlass beziehungsweise der Reduzierung von Geldbußen „belohnt". Das Zurückgreifen auf die Erfahrung, das Know-how und die besonderen Hilfsmittel von externen Beratern wie Rechtsanwälten oder Wirtschaftsprüfern mag hier in vielen Fällen sinnvoll erscheinen.

Allerdings kann die Durchführung einer internen Untersuchung auch mit Problemen für das Unternehmen verbunden sein. Das gilt in der Konzernsituation insbesondere für grenzüberschreitende Untersuchungen (*Cross-Border Investigations*). Hier kann das grenzüberschreitende Moment zur Kollision von Rechtssystemen führen und die Gefahr bestehen, dass „von außen" in grundlegende nationale Rechtsprinzipien eingegriffen wird. Beispielhaft sind Untersuchungen, die im Ausland gegen die dort ansässige Tochtergesellschaft einer inländischen Konzernmutter geführt werden und sich dabei, wenn auch nur mittelbar, auch auf die Muttergesellschaft erstrecken.

Internal Investigations stellen sich für die meisten Unternehmen noch immer als Novum dar. Derzeit bestehen zahlreiche Unsicherheiten und Unklarheiten darüber, welche „Eingangstore" insbesondere das deutsche Recht für *Internal Investigations* vorsieht. Die Fragen beziehen sich vor allem darauf, wann es zweckmäßig oder angebracht ist, derartige Untersuchungen einzuleiten, wer diese vernünftigerweise vornimmt, wie eine *Internal Investigation* durchzuführen ist, welche rechtlichen Besonderheiten dabei zu beachten sind und wie schließlich mit den Ergebnissen verfahren werden sollte.

In Deutschland stecken *Internal Investigations* als Bestandteil von Compliance-Systemen trotz einiger in den Medien bekannt gewordener Fälle noch immer in den Kinderschuhen. Diese Studie will deshalb über das Instrument der *Internal Investigation* informieren und aufklären und Unternehmen eine Hilfestellung bei der Überlegung bieten, welcher Weg bei einem Compliance-Verstoß zweckmäßigerweise einzuschlagen ist. Angesichts einer sich ständig weiterentwickelnden Rechtspraxis und fort-

laufend neuer Gesetzesinitiativen versteht es sich dabei von selbst, dass sich diese Studie nur ausgewählten praxisrelevanten Rechtsfragen widmet und keinen Anspruch auf Vollständigkeit erheben kann. Die praxisrelevanten rechtlichen Spagatschritte, vor welchen die Unternehmen aufgrund der jüngsten Regulierungsinitiativen, vor allem bei der Korruptionsbekämpfung oder im Datenschutz, stehen, werden jedoch benannt.

Frankfurt am Main, im August 2010

Prof. Dr. Rüdiger von Rosen

Geschäftsführendes Vorstandsmitglied
Deutsches Aktieninstitut e.V.

Rolf Hünermann

Rechtsanwalt/Partner
Willkie Farr & Gallagher LLP

Inhaltsverzeichnis

Abkürzungsverzeichnis

AktG	Aktiengesetz
AO	Abgabenordnung
BAG	Bundesarbeitsgericht
BB	Betriebs-Berater
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGHSt	Entscheidungen des Bundesgerichtshofs in Strafsachen
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BMI	Bundesministerium des Inneren
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
CCZ	Corporate Compliance Zeitschrift
CR	Computer und Recht
DB	Der Betrieb
DOJ	United States Department of Justice
EStG	Einkommensteuergesetz
FCPA	Foreign Corrupt Practices Act
FG	Finanzgericht
GewO	Gewerbeordnung
GIACC	Global Infrastructure Anti-Corruption Centre
GmbHG	Gesetz betreffend die Gesellschaft mit beschränkter Haftung
GWB	Gesetz gegen Wettbewerbsbeschränkungen
ICC	International Chamber of Commerce
IntBestG	Gesetz zur Bekämpfung internationaler Bestechungen
KuR	Kommunikation und Recht
KWG	Kreditwesengesetz
LAG	Landesarbeitsgericht
LG	Landgericht
NJW	Neue Juristische Wochenschrift
NStZ	Neue Zeitschrift für Strafrecht
NYSE	New York Stock Exchange
NZA	Neue Zeitschrift für Arbeitsrecht
NZBau	Neue Zeitschrift für Baurecht
NZG	Neue Zeitschrift für Gesellschaftsrecht
OECD	Organisation for Economic Co-Operation and Development
OLG	Oberlandesgericht
OWiG	Gesetz gegen Ordnungswidrigkeiten
PACI	Partnering Against Corruption Initiative
RdA	Recht der Arbeit
RDV	Recht der Datenverarbeitung
SEA	Securities Exchange Act of 1934
SEC	United States Securities and Exchange Commission
SOX	Sarbanes-Oxley Act
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StV	Strafverteidiger
TKG	Telekommunikationsgesetz
USC	United States Code
USSG	United States Sentencing Guidelines
UWG	Gesetz gegen den unlauteren Wettbewerb
VOB/A	Verdingungsordnung für Bauleistungen, Teil A
VOL/A	Verdingungsordnung für Leistungen, Teil A
wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht
WM	Wertpapiermitteilungen
ZIP	Zeitschrift für Wirtschaftsrecht
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
ZPO	Zivilprozessordnung

1. Compliance und Internal Investigations

Compliance bedeutet im Allgemeinen die Übereinstimmung mit bzw. die Erfüllung von Rechtsvorgaben sowie Handlungs- und Verhaltensregeln, die für ein Unternehmen relevant sind.[1] So gesehen, handelt es sich hier nicht um ein inhaltliches Novum. Allerdings hat die Compliance in den vergangenen Jahren vor allem in großen Gesellschaften einen deutlich höheren Stellenwert erhalten, was sich teilweise in der Unternehmensorganisation durch die Etablierung von Compliance-Abteilungen und gegebenenfalls die Einsetzung eines Chief Compliance Officers (CCO) auf direkter Ebene unterhalb des Vorstands niedergeschlagen hat.

Der Aufbau bzw. die Existenz eines Compliance-Programms wird teilweise explizit in Gesetzen vorausgesetzt oder angeordnet, geht aber auch auf die Tendenz zu einer national wie international zu beobachtenden Ausweitung der Unternehmens- und Organhaftung zurück. Exemplarisch sind hier die weltweit einmalig hohen Bußgelder, die von der EU-Kommission gegen führende europäische Unternehmen wegen Verletzungen des Wettbewerbsrechts ausgesprochen wurden: Erst vor kurzem verhängte die EU-Kommission eine Geldstrafe von insgesamt 622 Millionen Euro gegen 17 Hersteller von Sanitäreinrichtungen wegen verbotener Preisabsprachen.[2] Fast zeitgleich wurden mehrere Stahlhersteller wegen eines Kartells mit einer Geldstrafe von 518 Millionen Euro belegt.[3] Auch die gegen die US-amerikanischen Unternehmen *Intel* und *Microsoft* festgesetzten Bußgelder wegen Missbrauchs einer marktbeherrschenden Stellung haben durchaus für Aufsehen gesorgt.[4]

---

1 Vgl. Arbeitskreis Externe und Interne Überwachung der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V. (AKEIÜ), DB 2010, 1509 ff. (1510).

2 Europäische Kommission, 23. Juni 2010, COMP/39092, Pressemitteilung der EU-Kommission vom 23. Juni 2010, abrufbar unter http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/790&format=HTML&aged=0&language=DE&guiLanguage=en.

3 Vgl. Börsen-Zeitung vom 1. Juli 2010, Ausgabe Nr. 123, S. 9.

4 Die Europäische Kommission hat im Jahre 2009 gegenüber dem weltweit größten Chiphersteller *Intel* ein Bußgeld von 1,06 Milliarden Euro festgesetzt; gegen *Microsoft* wurde im Februar 2008 eine Bußgeldsumme von 899 Millionen Euro verhängt; addiert man alle Bußgelder, die von der EU-Kommission gegen Microsoft verhängt wurden, kommt man sogar auf 1,7 Milliarden Euro.

Tabelle 1: Übersicht der insgesamt durch die Europäische Kommission in den Jahren 2006 bis 2010 verhängten Kartellgeldbußen[5]

Jahr	Betrag in Euro
2006	1.846.385.500
2007	3.338.427.700
2008	2.270.012.900
2009	1.623.384.400
2010	1.493.257.832
Gesamt	**10.571.468.332**

Tabelle 2: Die zehn höchsten Kartellgeldbußen seit 1969[6]

Jahr	Unternehmen	Fall	Betrag in Euro
2008	Saint Gobain	Autoglas	896.000.000
2009	E.ON	Gas	553.000.000
2009	GDF Suez	Gas	553.000.000
2007	ThyssenKrupp	Aufzüge	479.669.850
2001	F. Hoffmann-La Roche	Vitamine	462.000.000
2007	Siemens	Gasisolierte Schaltanlage	396.562.500
2008	Pilkington	Autoglas	370.000.000
2010	Ideal Standard	Badarmaturen	326.091.196
2008	Sasol	Kerzenwachs	318.200.000
2010	ArcelorMittal	Spannstahl	317.280.000

Zudem hat eine Reihe von höchstrichterlichen Urteilen dazu geführt, dass dem Bereich Compliance von Unternehmensseite erhöhte Aufmerksamkeit gewidmet wird. Im August 2008 hat der Bundesgerichtshof (BGH) entschieden, dass allein das Vorhalten sogenannter „schwarzer Kassen“

5 Die Beträge beziehen sich auf die von der Kommission ursprünglich verhängten Geldbußen ohne Anpassung durch nachfolgende Gerichtsurteile. Quelle: Europäische Kommission, Kartellstatistik, Stand 30. Juni 2010, abrufbar unter http://ec.europa.eu/competition/cartels/statistics/statistics.pdf.

6 Quelle: Europäische Kommission, Kartellstatistik, Stand 30. Juni 2010, a.a.O.

eine strafrechtliche Untreue darstellen kann.[7] Im Juli 2009 wurde vom BGH bestätigt, dass dem Verantwortlichen für die interne Revision bzw. auch dem Compliance-Beauftragten eine strafrechtliche Garantenstellung zukommen kann, nämlich dann, wenn dieser in dem Unternehmen eine zur Rechtstreue verpflichtende Position inne hat.[8] Dies könnte für weitere Einschnitte in der Compliance-Landschaft sorgen.

Internal Investigations dienen der Feststellung bzw. der Diagnose von Compliance-Verstößen. Mittelbar zielen sie darauf ab, das Compliance-System im Hinblick auf die aufgedeckten Verstöße anzupassen, um deren Wiederholung soweit wie möglich auszuschließen.

---

7 BGHSt 52, 323, abrufbar unter http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=34ce1b6cbcea156691cb94da2dd113a2&tnr=45994&tpos=1&anz=2.

8 BGH NJW 2009, 3173 ff. (3175).

2. Internal Investigations: Ursprung, Historie und Anreize

Internal Investigations haben ihren Ursprung in den USA. Eine Legaldefinition des Begriffs existiert nicht. Dennoch werden *Investigations*, wie sie im allgemeinen Sprachgebrauch bezeichnet werden, in vielen US-Vorschriften angeordnet oder als typischer Compliance-Bestandteil vorausgesetzt. Dies gilt insbesondere für die *US Federal Sentencing Guidelines (USSG)*, die u.a. für Unternehmen (*Organizations*) Vorschriften über Strafbemessungen für gesetzeswidriges Verhalten beinhalten. Für diese sind Geldstrafen bis in dreistelliger Millionenhöhe vorgesehen.[9]

Bereits in den einleitenden Vermerken zu Kapitel 8 der USSG wird jedoch explizit auf eine Möglichkeit zur Strafmilderung hingewiesen, sofern das betroffene Unternehmen die Tat selbst aufklärt, eine Anzeige bei der zuständigen Behörde vornimmt und daraufhin mit dieser umfänglich kooperiert.[10] Hierdurch wird ein besonderer Anreiz für die Aufklärung geschaffen.

Dies wird zusätzlich durch weitere Faktoren verstärkt: Nach dem sogenannten *Thompson-Memorandum*[11] aus dem Jahr 2003 kann eine Strafverfolgungsbehörde von einer Anklage absehen, wenn die juristische Person die Tat aufgeklärt, sie bei den Behörden angezeigt hat und zur Kooperation mit den Behörden bereit ist, das heißt insbesondere die Täter zu benennen, Zeugen zur Verfügung zu stellen und die Ergebnisse einer *Internal Investigation* zugänglich zu machen.[12] Der Grundsatz Strafmilderung bzw. Absehen von einer Anklage gegen Kooperation wird auch im nachfolgenden *McNulty-Memorandum*[13] aus dem Jahr 2006 sowie im *Filip-Memorandum*[14] von 2008 bekräftigt. Die genaue Klärung des Sachverhalts ist wesentliche Voraussetzung einer Einigung mit den US-

---

9 Vgl. Kapitel 8 der *USSG*.

10 Vgl. *Introductory Commentary to Chapter 8 of the USSG*, abrufbar unter http://www.ussc.gov/2009guid/8a1_1.htm, vgl. auch *Wagner*, CCZ 2009, 8 ff. (9).

11 Schreiben des Deputy Attorney General (Department of Justice) *Larry D. Thompson* vom 20.1.2003, *Principles of Federal Prosecution of Business Organizations („Thompson Memorandum")*, Abschnitt VI, abrufbar unter http://www.justice.gov/dag/cftf/corporate_guidelines.htm, vgl. auch *Wagner,* a.a.O. (9).

12 Vgl. *Wagner*, a.a.O.

13 Abrufbar unter http://www.justice.gov/dag/speeches/2006/mcnulty_memo.pdf

14 Abrufbar unter http://www.justice.gov/dag/readingroom/dag-memo-08282008.pdf.

Behörden.[15] Damit kann die Durchführung einer *Investigation* für das Unternehmen entscheidend zur Erlangung der Straffreiheit sein.[16] Den vorgenannten Memoranda vergleichbare Regelungen existieren auch auf Ebene der Einzelstaaten.[17]

Für börsennotierte Gesellschaften in den USA ist der *Seaboard Report*[18] der amerikanischen Börsenaufsicht *Securities and Exchange Commission* (*SEC*) sowie das ebenfalls von der *SEC* im Januar/März 2010 veröffentlichte *Enforcement Manual*[19] bedeutsam. Kriterien zur Bemessung einer Sanktion sind danach unter anderem Art und Dauer des Missstands, die Frage, wie dieser aufgeklärt wurde und welche Schritte die Gesellschaft unternommen hat, um das identifizierte Fehlverhalten für die Zukunft auszuschließen. Explizit wird danach gefragt, ob die Gesellschaft eine gründliche Aufarbeitung bzw. Untersuchung des Vorfalls vorgenommen hat. Diese wirkt sanktionsmildernd.

Hoheitliche Ermittlungen in einem Unternehmen stören regelmäßig Betriebsabläufe, binden Ressourcen und verursachen infolgedessen Kosten – von negativer Publicity und dadurch bedingten Reputationsschäden ganz zu schweigen. Zur Vermeidung dieser Auswirkungen kann eine *Internal Investigation* sinnvoll sein.

---

15 Vgl. Wybitul, BB 2009, 606.

16 Vgl. *Introductory Commentary to Chapter 8 of the USSG,* a.a.O., vgl. auch *Wagner*, a.a.O.

17 Nach den neuen Richtlinien des *District Attorney of the County of New York (DANY*) z.B. ist die Ermessensentscheidung über die Strafverfolgung von *Organizations* von einer Reihe von Faktoren abhängig. Ein Absehen von der Strafverfolgung kommt unter anderem dann in Betracht, wenn die Organisation ihr Fehlverhalten freiwillig und frühzeitig, das heißt ohne bereits erlassene Zwangsmaßnahmen offenbart, mit der Strafverfolgungsbehörde kooperiert und über ein Compliance-System verfügt, welches Abhilfemaßnahmen vorschreibt.

18 *„Report of Investigation Pursuant to Section 21 (a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions", Securities Exchange Act of 1934 Release No. 44969/October 23, 2001*, abrufbar unter http://www.sec.gov/litigation/investreport/34-44969.htm.

19 Abrufbar unter http://www.sec.gov/divisions/enforce/enforcementmanual.pdf.

3. Rechtliche Grundlagen für Internal Investigations

Trotz der vorgenannten Vorschriften existieren Normen, die Unternehmen unter gewissen Umständen explizit verpflichten, *Internal Investigations* durchzuführen, nur in wenigen Fällen. Allerdings gibt es zahlreiche Regelwerke auf internationaler und nationaler Ebene, die im Zusammenhang mit *Investigations* und Compliance-Verstößen diskutiert werden und – teilweise im Zusammenspiel mit weiteren Normen – eine *Investigation* aus Sicht eines Unternehmens vorteilhaft erscheinen lassen können.

3.1 Internationale Abkommen

3.1.1 OECD-Convention on Combating Bribery of Foreign Public Officials in International Business Transactions

Das OECD-Übereinkommen über die Bekämpfung der Bestechung ausländischer Amtsträger im internationalen Geschäftsverkehr[20] stammt aus dem Jahr 1997 und verpflichtet die Vertragsstaaten, die Bestechung ausländischer Amtsträger durch inländische Unternehmen unter Strafe zu stellen. Ziel der Konvention ist die Schaffung von transparenten und verzerrungsfreien Märkten durch lauteren Wettbewerb im internationalen Wirtschaftsverkehr.

Nach den auf Basis der Konvention erlassenen *OECD Recommendations of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions*[21] vom November 2009 sollen die Mitgliedstaaten Unternehmen dazu anhalten, Compliance-Programme zu errichten, um Bestechungen wirksam entgegenzuwirken. Hierzu sollen Initiativen sowohl im privaten als auch im öffentlichen Sektor dienen, um Auslandsbestechungen zu verhindern und, falls bereits geschehen, solche aufzuspüren; ferner sollen wirksame Maßnahmen zur Anzeige solcher Bestechungen untersucht und entsprechende *Reporting-Systeme* vorgehalten werden.[22]

---

20 Abrufbar unter http://www.oecd.org/dataoecd/4/18/38028044.pdf.

21 Abrufbar unter http://www.oecd.org/dataoecd/4/18/38028044.pdf, dort S. 19 ff.

22 Vgl. *General Provisions of Recommendations of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions*, Ziffer III. i) und iv) sowie Ziffer IX.

Zudem sind die Mitgliedstaaten nach Art. 3 der Konvention angewiesen, die Bestechungen ausländischer Amtsträger durch natürliche und juristische Personen mit „wirksamen, angemessenen und abschreckenden" Strafen bzw. Sanktionen zu bedrohen. Sofern eine Strafbarkeit juristischer Personen im respektiven nationalen Rechtssystem nicht existiert, wird in diesem Zusammenhang neben der Verhängung von Geldstrafen insbesondere auch die Einziehung der Erträge aus einer Bestechung oder die Beschlagnahme von Vermögensgegenständen mit entsprechendem Wert als geeignetes Mittel genannt.[23] Nach den Erläuterungen des Konventionstextes zählt hierzu zum Beispiel auch der Ausschluss von Ansprüchen auf öffentliche Hilfen sowie der zeitweise oder permanente Ausschluss von der Teilnahme an öffentlichen Ausschreibungen, die Anordnung der gerichtlichen Aufsicht über die Gesellschaft sowie gegebenenfalls gar eine Auflösungsverfügung oder Löschung der Gesellschaft.[24]

Gerade durch diese Maßnahmen werden Unternehmen empfindlich getroffen. Sofern in dem jeweiligen Vertragsstaat nationale Rechtsvorschriften existieren, die die Gewährung von Strafmilderungen bei Kooperation und/oder Aufklärung der Vorwürfe vorsieht, kann es sich für die Unternehmen daher lohnen, dem Bestechungsvorwurf intensiv nachzugehen und diesen aufzuklären.

3.1.2 United Nations Convention against Corruption

Die UN-Konvention aus dem Jahr 2005[25] zielt gleichermaßen auf die Bekämpfung der Korruption im öffentlichen wie im privaten Sektor ab und umfasst die Bereiche Korruptionsprävention, die Verpflichtung der Mitgliedstaaten zur Schaffung von Straftatbeständen, um eine große Bandbreite von korruptivem Verhalten zu sanktionieren, die internationale Kooperation der Vertragsstaaten sowie die *Asset Recovery*, das heißt die Abschöpfung oder Wiedererlangung des durch die Korruption Erlangten. Die Konvention verpflichtet die Vertragsstaaten darüber hinaus zur

---

23 Vgl. Art. 3 Abs. 2, 3 des OECD-Übereinkommens über die Bekämpfung der Bestechung ausländischer Amtsträger im Internationalen Geschäftsverkehr.

24 Vgl *Commentaries on the Convention*, Art. 3, Rz. 24: *„...exclusion from entitlement to public benefits or aid; temporary or permanent disqualification from participation in public procurement or from the practice of other commercial activities; placing under judicial supervision; and a judicial winding-up order."*, abrufbar unter http://www.oecd.org/dataoecd/4/18/38028044.pdf, S. 15.

25 Abrufbar unter http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf.

Schaffung von Maßnahmen, um die Kooperation zwischen Ermittlungsbehörden (*Law Enforcement Agencies*) und den „relevanten Privat-Institutionen“ zu erleichtern bzw. voranzutreiben. Ferner sollen die Mitgliedstaaten sicherstellen, dass Unternehmen – abhängig von ihrer Struktur und Größe – über ausreichende *Internal Auditing Controls* verfügen, um zur Prävention und zum Aufspüren von Korruptionsvorfällen beizutragen.[26] Je nach Umfang und Beschaffenheit des Vorfalls können *Internal Investigations* hier gewiss eine tragende Rolle spielen.

Art. 37 der Konvention verpflichtet die Mitgliedstaaten darüber hinaus zur Schaffung von Anreizen, um Personen zur Meldung von Korruptionsfällen, an denen sie selbst beteiligt waren, zu bewegen. Als Anreize werden eine mögliche Strafmilderung oder gar ein Absehen von der Strafverfolgung („Immunität“) genannt. Gerade aufgrund solcher Anreize drohen Unternehmen und ihre Organe durch Aussagen von Mitarbeitern, welche in das Visier der Ermittlungsbehörden geraten sind, belastet zu werden; hier kann eine *Internal Investigation* helfen, das Geschehen zu steuern, sofern sich Ermittlungen auch gegen das Unternehmen richten sollten.

3.2 Regelungen in den USA und Großbritannien

3.2.1 US Federal Sentencing Guidelines

In Kapitel 8 der *US Federal Sentencing Guidelines*[27] ist die Sanktionierung von Unternehmen geregelt (*Sentencing of Organizations*). Deren Strafmaß wird grundsätzlich anhand der folgenden strafverschärfenden und strafmildernden Faktoren bemessen:

Strafverschärfend wirken:

- Die Verstrickung in und die Tolerierung von kriminellem Verhalten,
- eine „negative Vorgeschichte“ des Unternehmens,
- das Nichtbefolgen einer gerichtlichen bzw. behördlichen Anordnung oder Verfügung,
- die Behinderung der Justiz (*Obstruction of Justice*).

---

26 Vgl. Art. 12 Nr. 2 (f) der Konvention
27 Abrufbar unter http://www.ussc.gov/2009guid/TABCON09.htm.

Strafmildernd wird berücksichtigt:

- Die Existenz eines effektiven Compliance- und Ethik-Programms und
- eine Selbstanzeige bzw. Kooperation zur Aufklärung des respektiven Vorfalls oder die Übernahme von Verantwortung dafür (*Self-Reporting, Cooperation or Acceptance of Responsibility*).

Hohe Bedeutung kommt einem effektiven Compliance- und Ethik-Programm zu, das mindestens die nachfolgenden sieben Punkte zu beinhalten hat:[28]

- Verfahrensweisen zur Prävention und Aufklärung strafbaren Verhaltens
- Die Unternehmensführung muss mit dem Inhalt und der Funktionsweise des Compliance-Programms vertraut sein und dessen Implementierung überwachen. Das Management muss sicherstellen, dass das Unternehmen über ein effektives Compliance-System verfügt. Es sind einzelne Führungskräfte zu benennen, die für das Programm verantwortlich sind und dem Management hierüber Bericht erstatten
- Keine Führungskraft im Management, deren Vergangenheit „im Widerspruch" zu einem effektiven Compliance-Programm steht
- Periodische Kommunikation und Bekanntmachung des Compliance-Systems auf allen Unternehmensebenen
- Gewährleistung des Unternehmens, dass das Compliance-Programm befolgt wird. Hierzu zählen ein *Monitoring* und ein *Auditing*, um kriminelles Verhalten aufzuspüren. Die Wirksamkeit des Compliance-Programms ist periodisch zu überprüfen. Ferner sind Reporting-Systeme einzurichten, die es Mitarbeitern gestatten, Verdachtsfälle auf Compliance-Verstöße anonym und ohne Befürchtungen persönlicher Nachteile zu berichten (*Whistleblower Hotline* oder Ombudsmann)
- Konsequente Durchsetzung des Compliance-Programms im gesamten Unternehmen und Schaffung angemessener Anreize hierfür. Zudem müssen angemessene Disziplinarmaßnahmen für kriminelles Verhalten und für das Unterlassen (*Failing*) vernünftiger Schritte zur Prävention und zum Aufspüren kriminellen Verhaltens etabliert werden

28 Detaillierte Darstellung in § 8 B 2.1. (b) USSG.

- Angemessene Reaktion auf kriminelles Verhalten, um zukünftiges Missverhalten zu verhindern; dies beinhaltet ein Anpassen des Compliance-Systems

Nach den *USSG* können empfindliche Geldbußen in dreistelligen Millionenbeträgen[29] verhängt werden, sodass sich für Unternehmen in der Regel eine Kooperation anbietet.

Nach der aktuellen Fassung der *USSG* kommt eine umfangreiche Reduzierung des Strafmaßes allerdings nicht in Betracht, sofern es sich um Compliance-Verstöße von Mitgliedern der oberen Führungsebene handelt (*High-Level Personnel*). Die die *USSG* erlassende *United States Sentencing Commission* hat allerdings vor kurzem eine eng begrenzte Ausnahme von diesem Grundsatz vorgeschlagen. Eine Sanktionsreduzierung käme danach beim Bestehen einer Meldepflicht des Compliance-Verantwortlichen gegenüber der jeweiligen Aufsichtsbehörde des Unternehmens (*Organization's Governing Authority*) maßgeblich dann in Frage, wenn der Verstoß intern aufgedeckt, sofort den zuständigen Behörden gemeldet wurde und keine für das Compliance- und Ethik-Programm verantwortliche Person darin verwickelt ist.[30]

3.2.2 Securities Exchange Act of 1934 (SEA)[31]

Nach Section 10 A (a) SEA müssen Wirtschaftsprüfungen bei Emittenten das Aufspüren von Missständen praktisch gewährleisten. Sofern eine Wirtschaftsprüfungsgesellschaft im Rahmen ihrer Tätigkeit auf Anhaltspunkte für Missstände oder Rechtsbrüche (*Illegal Acts*) stößt, hat sie einen vorgegebenen Ablauf einzuhalten. Zunächst ist die Wahrscheinlichkeit eines Rechtsverstoßes und dessen Auswirkung auf die Finanzbericht-

---

29 Siehe Ziffer 2 auf S. 16.

30 Abrufbar unter http://www.ussc.gov/2010guid/20100503_Reader_Friendly_Proposed_Amendments.pdf, dort S. 33: „...which allows an organization to receive the decrease if the organization meets four criteria: (1) the individual or individuals with operational responsibility for the compliance and ethics program have direct reporting obligations to the organization's governing authority or appropriate subgroup thereof; (2) the compliance and ethics program detected the offense before discovery outside the organization or before such discovery was reasonable likely; (3) the organization promptly reported the offense to the appropriate governmental authorities; and (4) no individual with operational responsibility for the compliance and ethics program participated in, condoned or was willfully ignorant of the offense."

31 Abrufbar unter http://www.law.uc.edu/CCL/34Act/index.html.

erstattung des Unternehmens zu eruieren; sodann ist das Audit Committee bzw. das gesamte *Board of Directors* zu verständigen, sofern ein Audit Committee nicht existiert.[32] Auf eine solche Meldung hin veranlasst das Unternehmen in der Praxis regelmäßig eine umfassende *Internal Investigation*,[33] um Reputationsschäden und möglichen Geldbußen entgegenzuwirken, sowie in den Genuss einer reduzierten Sanktion oder gegebenenfalls sogar Straffreiheit zu gelangen.

3.2.3 Foreign Corrupt Practices Act – FCPA

Diese in den USA bei weitem bedeutendste Anti-Korruptions-Bestimmung[34] stammt aus dem Jahr 1977. Das Gesetz ist in zwei Teile gegliedert, die *Anti-Bribery Provisions*, die Bestechungszahlungen an ausländische Amtsträger verbieten und die *Accounting Provisions*, die korruptives Verhalten, beispielsweise der Bildung schwarzer Kassen, im Vorfeld solcher Zahlungen durch ordnungsgemäße Rechnungslegung vorbeugen sollen. Innerhalb der *Accounting Provisions* sanktionieren die *Internal Control Provisions* das Unterlassen von Maßnahmen zur Aufdeckung korruptiven Verhaltens.

Das Gesetz hat einen extensiven Anwendungsbereich und enthält extraterritoriale Anknüpfungspunkte. Nach Ansicht des *United States Department of Justice (DOJ)* ist zur Anwendung der *Anti-Bribery Provisions* ein nur marginaler US-Bezug der Korruptionshandlung ausreichend, beispielsweise eine Überweisung oder ein Telefonanruf aus den USA, möglicherweise gar das Versenden einer E-Mail von einem amerikanischen Server.[35]

Hinzu kommt, dass der Begriff des ausländischen Amtsträgers als Bestechungsempfänger (*Foreign Official*) weit zu verstehen ist. Er umfasst nach der gesetzlichen Definition insbesondere jeden leitenden oder einfachen Mitarbeiter einer ausländischen Regierung, eines Ministeriums, einer Agentur, einer öffentlichen internationalen Organisation oder einer Person, die in einer amtlichen Eigenschaft für die vorgenannten Gremien

---

32 Vgl. Section 10 A (b) SEA
33 Vgl. *Wagner*, a.a.O. (9 f.).
34 Abrufbar unter http://www.justice.gov/criminal/fraud/fcpa/docs/fcpa-english.pdf.
35 Vgl. auch 15 USC § 78 dd-3 (a), *Grau*, *Meshulam*, *Blechschmidt*, BB 2010, 652 ff. (656).

tätig ist.[36] Darüber hinaus wurden in der Vergangenheit auch Mitarbeiter von staatlich beherrschten Unternehmen als *Foreign Officials* eingestuft.[37]

Von den Korruptionstatbeständen des FCPA wurden darüber hinaus auch Leistungen an Dritte erfasst, sofern der Leistende Grund zur Annahme hat, dass der Dritte zumindest einen Teil der Leistung an einen *Foreign Official* weiterleiten wird.[38] Ausreichend soll es dafür schon sein, wenn der Leistende Tatsachen ignoriert oder die vernünftigerweise gebotenen Erkundigungen über den Verbleib der Zahlungen nicht einholt.[39]

Emittenten bzw. Unternehmen mit einem geschäftlichen Bezug zu den USA drohen auch bei Verletzungen des deutschen Rechts Sanktionen nach dem FCPA, da sich die deutschen Wirtschaftsstraf- und Ordnungswidrigkeitstatbestände partiell mit denen der USA überschneiden. Dies gilt insbesondere hinsichtlich fehlerhafter Rechnungslegung (zum Beispiel unrichtige, unvollständige oder nicht rechtzeitige Bilanzierung) sowie im Hinblick auf Betrug, Untreue, Urkundsstraftaten und Bestechungsdelikte. Auf Letztere wird noch gesondert eingegangen.[40]

Die Schäden, die einem Unternehmen aufgrund von Korruptionsvorwürfen drohen, können gerade in den USA immens sein. Dies ist auf eine Kombination von Faktoren zurückzuführen. Hierzu zählt auch ein aus Verbrauchersicht lukratives Rechtssystem, das unter gewissen Umständen eine Geltendmachung von Strafschadensersatz auch im Wege von medienwirksam inszenierten Sammelklageverfahren ohne wirkliches Prozess- und Kostenrisiko ermöglicht. Vorzugswürdig erscheint es daher oftmals, eine interne Aufklärung und Kooperation mit eingeschalteten Ermittlungsbehörden zur Schadensbegrenzung und Sanktionsreduzierung nach den *USSG* vorzunehmen.[41]

---

36 Wortlaut 15 USC § 78 dd-1 (f) (1): „The term 'foreign official' means any officer or employee of a foreign government or any department, agency, or instrumentality thereof, or of a public international organization, or any person acting in an official capacity for or on behalf of any such government or department, agency, or instrumentality, or for or on behalf of any such public international organization." Vgl. auch *Grau, Meshulam, Blechschmidt*, a.a.O. (657).

37 *Grau*, *Meshulam*, *Blechschmidt*, a.a.O. (657).

38 Vgl. *Nietzer*, DAJV-NL 2/98, 43 ff. (44).

39 *Nietzer*, a.a.O. (S. 44).

40 Hinsichtlich weiterer Einzelheiten siehe Ziffer 6.4 auf S. 73.

41 Hinsichtlich weiterer Einzelheiten siehe Ziffer 3.2.1 auf S. 20.

3.2.4 Sarbanes-Oxley-Gesetz (SOX)

Mit Einführung des Sarbanes-Oxley-Gesetzes (*Sarbanes-Oxley-Act, SOX*)[42] hat der US-Gesetzgeber in den Jahren 2001 und 2002 auf die „Bilanzierungsskandale" amerikanischer Großunternehmen,[43] unter anderem hervorgerufen durch Insidergeschäfte, reagiert. Um Compliance-Verstößen wirksam zu begegnen, sieht *SOX* die Einrichtung von sogenannten – oft unternehmensextern betriebenen – Reporting-Systemen, beispielsweise *Whistleblowing-Hotlines,* vor, die es Mitarbeitern ermöglichen, Anhaltspunkte für Missstände oder Fehlverhalten anonym zu melden.[44] Hierdurch werden die Unternehmen mittelbar gezwungen, gemeldeten Missständen nachzugehen.

Dem Management wird ferner die Aufstellung eines *Internal Control Reports* abverlangt, der eine Bewertung des internen Kontrollsystems enthalten muss, welche wiederum durch den Jahresabschlussprüfer zu überprüfen ist. Beim internen Kontrollsystem handelt es sich um den „Kern" der Compliance. Dieser bedarf verständlicherweise einer regelmäßigen Überprüfung. Ein anerkanntes Mittel hierzu ist ein Compliance-Audit. Dessen Ziel ist es, vom Compliance-System vorgegebene Strukturen, Prozesse, Aktivitäten und Ziele einer systematischen Überprüfung durch unabhängige Experten zu unterziehen.[45] Die Definition klarer Anforderungen an die zu untersuchenden Strukturen und Abläufe ist eine wesentliche Voraussetzung für das Compliance-Audit, welches in der Regel erfolgt

- durch stichprobenartige *Walkthroughs*
- und nachfolgend durch stichprobenartige Überprüfung der aufgrund der Behebung von Schwachstellen implementierten Maßnahmen.[46]

Compliance-Audits und *Internal Investigations* sind demnach einander ähnlich. Allerdings sind *Investigations* nicht auf die ganzheitliche Überprüfung von Compliance-Systemen gerichtet, sondern beschränken sich auf die Aufklärung konkreter Rechtsverstöße, um deren Wiederholung durch Anpassung des Compliance-Systems auszuschließen. Der Aufga-

---

42 Abrufbar unter http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3763.ENR:.
43 Z.B. Enron, WorldCom.
44 Z.B. Sec. 301 (4) SOX, vgl. auch Sec. 806 SOX.
45 Vgl. *Menzies*, S. 184.
46 Vgl. für beides *Menzies*, a.a.O.

benbereich einer *Internal Investigation* ist daher im Vergleich zum Compliance-Audit enger umrissen.

Über die vorskizzierte OECD-Konvention hinaus haben FCPA und SOX unübersehbar auch die nationalen Gesetzgeber in ihren legislativen Bemühungen zur Korruptionsbekämpfung inspiriert. Derzeit besteht eine Tendenz zu einer immer restriktiveren Gesetzgebung.

3.2.5 Dodd-Frank Act

Mit dem *Dodd-Frank Wall Street Reform and Consumer Protection Act*,[47] der am 21. Juli 2010 in Kraft getreten ist, hat der US-Gesetzgeber auf Missstände reagiert, die die zurückliegende Finanzmarktkrise offenbart hat. Das Gesetz zielt unter anderem darauf ab, systemische Risiken frühzeitig zu erkennen und zu diesem Zweck auch die Transparenz der Unternehmen auszuweiten. Um letzteres zu erreichen, werden Mitarbeitern erhebliche finanzielle Anreize zur Meldung von Missständen gesetzt. Vereinfacht ausgedrückt sollen *Whistleblower*, die der *SEC* Compliance-Verstöße ihres Unternehmens melden, prozentual (zwischen zehn und 30 Prozent) an den Beträgen beteiligt werden, die die *SEC* aufgrund festgesetzter Geldstrafen vom Unternehmen erhält.[48] Aufgrund der hohen Geldbußen, die nach den *USSG* möglich sind und den Anforderungen des *SOX*, wonach *Whistleblower* anonym zu behandeln sind, ist davon auszugehen, dass von dieser Neuregelung massiv Gebrauch gemacht werden wird. Eine *Internal Investigation* kann deshalb zum einen sinnvoll sein, um entlastendes Material seitens des Unternehmens vorzubringen. Sofern sich der Verdacht erhärtet, kann durch eine unternehmensinterne Aufklärung zum anderen in Verhandlungen mit der *SEC* eine Sanktionsreduzierung erwirkt werden.

3.2.6 UK-Bribery Act 2010

Der im April dieses Jahres verabschiedete Bribery Act 2010,[49] der im April 2011 in Kraft treten wird, findet Anwendung auf jede Gesellschaft, die Geschäfte in Großbritannien tätigt („*...carries on a business, or part of a business, in any part of the United Kingdom*."), unabhängig vom Sitz

---

47 Abrufbar unter http://docs.house.gov/rules/finserv/111_hr4173_finsrvcr.pdf.
48 Vgl. Sec. 922 (b) (1) des Dodd-Frank-Act, abrufbar ebenda.
49 Abrufbar unter http://www.opsi.gov.uk/acts/acts2010/pdf/ukpga_20100023_en.pdf. Status: *Royal Assent* seit 8. April 2010.

dieser Gesellschaft. Das Gesetz reicht noch über den zuvor diskutierten FCPA hinaus, zumal es auch Bestechungen im privaten Bereich und damit Vorfälle erfasst, die keine Verbindung zu Amtsträgern bzw. *Government-* oder *Foreign Officials* aufweisen.

Dies stellt die Compliance-Systeme aller in Großbritannien tätigen Unternehmen vor neue Herausforderungen. Kritik wurde im Gesetzgebungsprozess vor allem daran geäußert, dass das Gesetz Verhalten kriminalisiere, welches bislang allenfalls zivil- oder wettbewerbsrechtliche Sanktionen nach sich ziehe.

Welche konkreten Maßnahmen das Gesetz Unternehmen im Hinblick auf ihre Compliance-Systeme und insbesondere interne Untersuchungen von Bestechungsvorfällen abverlangen wird, ist bislang nicht absehbar. Als einzige Maßnahme zur Exkulpation lässt das Gesetz *Adequate Procedures* im Compliance-System zur Verhinderung von Bestechungen ausreichen. Konkrete Ausführungsbestimmungen stehen derzeit noch aus. Eine Anpassung bestehender Compliance-Systeme, vor allem im Hinblick auf die sogenannte *Corporate Hospitality* (zum Beispiel die Bewirtungspraxis), wird sich wohl nicht vermeiden lassen.

3.2.7 NYSE: Listed Company Manual / Rules / Corporate Governance

Die Corporate Governance Standards des *New York Stock Exchange (NYSE) Listed Company Manual*,[50] des Leitfadens für die an der NYSE börsennotierten Unternehmen, verpflichten diese zur Implementierung und Veröffentlichung eines Verhaltenskodex für *Directors, Officers* und *Employees*. Der Kodex muss für den Fall der Verletzung bestimmter Verhaltensstandards umgehende und wirksame Gegenmaßnahmen vorsehen (*prompt and consistent action against violation of the code*).[51]

Die *NYSE-Rules*,[52] ein Regelwerk der NYSE zur Prävention und Bekämpfung betrügerischen Verhaltens, identifizieren bestimmte Vorfälle bzw. Missstände, bei denen sich eine Verpflichtung der gelisteten Unternehmen zur internen Untersuchung ergibt. Hierzu zählen Geschäfte, die eine Verletzung der Kapitalmarktgesetze oder des Insiderhandelsverbots möglich erscheinen lassen (*Violative Trades*). Die Vorgaben der *NYSE-Rules*

50 Abrufbar unter http://nysemanual.nyse.com/lcm/.
51 *NYSE Listed Company Manual*, Ziffer 303A.10.
52 Abrufbar unter http://nyserules.nyse.com/nyse/.

werden dabei durch Mitglieder-Rundschreiben (*Information Memoranda*) konkretisiert. Nach dem *NYSE Information Memorandum Nr. 06-6* vom 17.2.2006[53] ist bei Anhaltspunkten für *Violative Trades* eine *Internal Investigation* durchzuführen.

Im *NYSE Information Memorandum No. 05-65* vom 14. September 2005[54] weist die NYSE ausdrücklich darauf hin, dass sie bei Anhaltspunkten für Missstände eine Verpflichtung zunächst seitens der Unternehmen zur Kooperation und Offenlegung von Informationen sieht. Die Aussicht auf eine Sanktionsreduzierung bei umfassender Kooperation mit der *NYSE* wird hier besonders in den Vordergrund gestellt. Kategorien dabei sind die Bereitschaft, sich einem Missstand prompt zuzuwenden sowie die Fragen, ob, wann und welche Verfahrensweisen im Unternehmen etabliert wurden, um Fehlverhalten zu verhindern und wie sorgfältig das Unternehmen den Vorfall untersucht hat.[55] Einschneidende Sanktionen drohen demgegenüber dem Unternehmen, welches die Kooperation verweigert oder aber nachlässig oder unvollständig berichtet.[56]

Die Empfehlungen des *NYSE Corporate Accountability and Listing Standards Committee* zur Corporate Governance, denen das *NYSE Board of Directors* im August 2002 zugestimmt hat,[57] sowie die finalisierten *NYSE Corporate Governance Rules*[58] empfehlen den Unternehmen, die Compliance ernst zu nehmen und sich nachhaltig für die Befolgung gesetzlicher Vorschriften und Regularien einzusetzen. Als Mittel hierzu wird unter anderem auch die Einrichtung von *Reporting*-Systemen genannt, um illegales oder unethisches Verhalten innerhalb des Unternehmens anzuzeigen. Im Falle von Regelverstößen gelisteter Unternehmen kann die NYSE an diese einen sogenannten *Reprimand Letter* richten, der die Verstöße öffentlich macht. Zur Vermeidung von Rufschäden empfiehlt es sich für die Unternehmen daher in der Regel, den Vorwürfen aktiv nachzugehen, auch um entlastendes Material aufzufinden und vorzubringen.

---

53 Abrufbar unter http://apps.nyse.com/commdata/PubInfoMemos.nsf/AllPublishedInfoMemosNyseCom/85256FCB005E19E88525711700061566A/$FILE/Microsoft%20Word%20-%20Document%20in%2006-6.pdf.

54 Abrufbar unter http://apps.nyse.com/commdata/PubInfoMemos.nsf/AllPublishedInfoMemosNyseCom/85256FCB005E19E88525707C004C6DE0/$FILE/Microsoft%20Word%20-%20Document%20in%2005-65.pdf.

55 *NYSE Information Memorandum 05-65*, S. 5.

56 *NYSE Information Memorandum 05-65*, S. 6.

57 Abrufbar unter http://www.ecgi.org/codes/documents/corp_gov_pro_b.pdf.

58 Abrufbar unter http://www.ecgi.org/codes/documents/finalcorpgovrules.pdf, dort S. 16.

3.2.8 UK Anti-Korruptions-Compliance-Entwurfspapier

In Großbritannien hat eine Gruppe von *Senior Legal Officers* von über 85 Unternehmen, die im Financial Times 100 Index (FTSE100) notiert sind, ein Entwurfspapier zur Anti-Korruptions-Compliance vorgelegt,[59] welches neben der Implementierung eines Anti-Korruptions-Programms für das gesamte Unternehmen durch den Vorstand unter anderem einen Verhaltenskodex und die Sensibilisierung der Mitarbeiter empfiehlt, beispielsweise durch regelmäßige Schulungen. Der letzte Punkt dieses Entwurfpapiers empfiehlt den Unternehmen die Einrichtung eines *Whistleblowing*-Systems, um frühestmöglich über Compliance-Verstöße informiert zu sein. Im Falle einer Mitarbeiteranzeige über dieses System wird den Unternehmen empfohlen, den Verdachtsfall sorgfältig durch entsprechend qualifiziertes Personal untersuchen zu lassen und die Ergebnisse einer solchen Untersuchung gegebenenfalls dem anzeigenden Mitarbeiter zur Kenntnis zu geben.

3.3 Internationale Corporate-Governance-Empfehlungen

In den Empfehlungen des *Conference Board*[60] zur Corporate Governance[61] wird die Existenz und der regelmäßige Gebrauch von *Internal Investigations* vorausgesetzt. Die Empfehlungen sprechen explizit davon, dass *Internal Investigations* grundsätzlich von unabhängigen Ermittlern (vor allem Rechtsanwälten, aber auch Wirtschaftsprüfern) geführt werden sollten, sofern diese auch das Verhalten von *Company Executives* zum Gegenstand haben. Die unabhängigen Ermittler, die vom *Board* ernannt werden sollten, sollten dann auch direkt an das *Board* berichten. Bei ihrer Auswahl sollte darauf geachtet werden, dass es sich nicht um Anwaltsfirmen handelt, mit denen das Unternehmen regelmäßig zusammenarbeitet, da hier Zweifel an einer gründlichen und objektiven Untersuchung der Vorfälle bestehen, insbesondere dann, wenn die betreffende Kanzlei regelmäßig hohe Honorare bezieht.

---

59 Abrufbar unter http://www.justice.gov.uk/publications/docs/bach-letter-adequate-procedures-guidance.pdf.

60 Internationale unternehmensübergreifende Organisation zur Wirtschaftsförderung.

61 *The Conference Board: Commission on Public Trust and Private Enterprise – Findings and Recommendations, Part 2: Corporate Governance, Part 3: Audit and Accounting*, abrufbar unter http://www.ecgi.org/codes/documents/757.pdf.

Darüber hinaus können *Internal Investigations* aus den allgemeinen Sorgfaltspflichten eines *Board Members* bzw. *Directors* heraus entstehen. Aus der generellen *Duty of Care* haben Rechtsprechung und Literatur bei Verdachtsfällen die Pflicht des Vorstands/Boards entwickelt, den zugrunde liegenden Sachverhalt aufzuklären;[62] hieraus soll auch die Pflicht zur Durchführung einer *Internal Investigation* erfolgen.[63]

In den 2009 bereits in zweiter Auflage erschienenen *Principles for Countering Bribery* von *Transparency International*[64] wird ein effektives System der internen Kontrolle zur Bekämpfung von Bestechungen innerhalb des unternehmerischen Compliance-Systems vorausgesetzt, welches regelmäßig zu überprüfen und anzupassen ist. Zwar wird hier nicht explizit eine Empfehlung zur *Internal Investigation* bei Vorfällen ausgesprochen, die Mitarbeiter im Rahmen des *Whistleblowing* gemeldet haben, doch wird ebenso auf die Notwendigkeit hingewiesen, die Anti-Korruptions-Compliance zur „Chefsache“ zu machen. Zudem. Es wird ferner die Überlegung empfohlen, ob eine Überprüfung auch von einem „externen Blickwinkel“ aus sinnvoll sein kann.

Die *Rules of Conduct* der Internationalen Handelskammer (ICC)[65] enthalten ebenfalls an Unternehmen gerichtete Empfehlungen zur Korruptionsbekämpfung. Eine explizite Erwähnung von *Internal Investigations* als Mittel zur Aufklärung von und zum zukünftigen Ausschluss der hierdurch aufgedeckten Compliance-Verstöße findet sich hier nicht. Gleichwohl lassen die Empfehlungen der ICC zu *Independent Systems of Auditing* und zu einer laufenden Überprüfung der Compliance inklusive Anti-Korruptions-Verhaltensregeln durch das *Audit Committee* unternehmensinterne Ermittlungen zumindest als eine Option erscheinen.

Auch nach den *Business Principles for Countering Bribery* der *Partnering Against Corruption Initiative* (*PACI*) des *World Economic Forum*,[66] besteht eine explizite Empfehlung zu *Internal Investigations* bei Anhaltspunkten für Compliance-Verstöße nicht. Vielmehr wird im Allgemeinen auf die Notwendigkeit der Implementierung eines effektiven Anti-

---

62 Vgl. *Wagner*, a.a.O. (10) m.w.N.
63 *Wagner*, a.a.O. m.w.N.
64 Abrufbar unter http://www.transparency.org/publications/publications/other/business_principles_for_countering_bribery.
65 Abrufbar unter http://www.iccwbo.org/uploadedFiles/ICC/policy/anticorruption/Statements/ICC_Rules_of_Conduct_and_Recommendations%20_2005%20Revision.pdf.
66 Abrufbar unter http://www.weforum.org/pdf/paci/PACI_Principles.pdf.

Korruptions-Programms im Compliance-System, welches einer regelmäßigen Überprüfung bedarf, hingewiesen.

Praktische Empfehlungen zum Umgang mit einem Korruptionsverdacht oder evidenten Korruptionsfällen finden sich gerade im Zusammenhang mit internationalen Ausschreibungen von Infrastrukturprojekten auf der Webseite des *Global Infrastructure Anti Corruption Center (GIACC)*.[67] Hier spielen auch *Internal Investigations* eine Rolle. Im Kapitel *Dealing with Corruption*[68] wird das Instrument *Internal Investigations* zur Aufdeckung von hinreichend konkreten Verdachtsmomenten erkennbar vorausgesetzt. Unter anderem wird dem Unternehmen empfohlen, zunächst alle Fakten und Beweismittel zusammenzutragen. Eine solche Untersuchung sollte vor allem unvoreingenommen erfolgen. Kritisch setzt sich die Publikation im Anschluss mit dem *Reporting* von ermittelten Korruptionsvorfällen auseinander, da hier verschiedene Interessenkonflikte auftreten können.[69]

3.4 Anhaltspunkte für Internal Investigations im deutschen Recht und europäischen Kontext

3.4.1 Aktienrecht und Deutscher Corporate Governance Kodex

Nach § 91 Abs. 2 Aktiengesetz (AktG) hat der Vorstand einer Aktiengesellschaft geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, um Entwicklungen, die den Fortbestand der Gesellschaft gefährden, früh zu erkennen.

Die konkrete Ausgestaltung des Überwachungssystems ist von verschiedenen Faktoren, etwa der Größe und Branchenzugehörigkeit, des einzelnen Unternehmens abhängig. Sie lässt sich nicht unmittelbar dem Gesetz entnehmen, sondern ist dem Leitungsermessen des Vorstands im Einzelfall überlassen.[70]

---

67 Unabhängige Organisation, die Ressourcen und Dienstleistungen zur Vermeidung der Korruption im Infrastruktur- und Konstruktionssektor anbietet.

68 Abrufbar unter http://www.giaccentre.org/dealing_with_corruption.php.

69 Z.B. hinsichtlich einer möglichen Strafmilderung bei Kooperation mit den Ermittlungsbehörden bei gleichzeitiger Gefahr der Selbstbelastung mit einer weiteren Tat.

70 *Krieger/Sailer* in *Schmidt/Lutter*, AktG, 2008, § 91 Rn. 14.

Inwieweit der Aufbau eines Compliance-Systems, welches auch *Internal Investigations* beinhaltet, zu den zu ergreifenden Maßnahmen zur Risikofrüherkennung zählt, lässt sich daher nicht generell beantworten, sondern ist eine Frage des Einzelfalls. Zu beachten ist hier, dass der Vorstand nach der *Business Judgement Rule* einen Ermessensspielraum auch hinsichtlich der Frage genießt, wie eine Compliance-Organisation zu gestalten ist und welche Maßnahmen bei Compliance-Verstößen zu ergreifen sind.[71] Die Ausgestaltung des Compliance-Systems ist damit abhängig von der Größe, Struktur und Lage des Unternehmens, dem Risikopotential der Märkte, auf denen es tätig ist und der Art des Kapitalmarktzugangs.[72] Sofern beispielsweise ein (Zweit-)Listing in den USA besteht, sollte jedenfalls definiert werden, unter welchen Umständen und auf welche Weise eine *Internal Investigation* durchzuführen ist.

Nach § 76 Abs. 1 AktG hat der Vorstand die Gesellschaft unter eigener Verantwortung zu leiten. Nach § 93 Abs. 1 AktG haben Vorstandsmitglieder bei der Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Einigkeit besteht im Wesentlichen darüber, dass unter die Leitungskompetenz auch die Zuständigkeit für die Compliance fällt, zu der je nach den vorgenannten Umständen auch *Internal Investigations* zählen können.[73]

Nach deutschem Recht hat der Vorstand im Rahmen seiner Sorgfaltspflichten sicherzustellen, dass die Unternehmensangehörigen den ihnen übertragenen Aufgaben ordnungsgemäß nachkommen. Das Ausmaß dieser Überwachungspflicht hängt von den Umständen des Einzelfalls ab.[74] Bei Hinweisen auf Gesetzesverletzungen oder Unregelmäßigkeiten von Unternehmensangehörigen müssen Vorstandsmitglieder diesen Hinweisen unverzüglich nachgehen.[75] Einzelheiten sind hier zur Verletzung der Aufsichts- bzw. Überwachungspflicht bei Kartellverstößen herausgearbeitet worden. Hier können stichprobenartige, überraschende Prüfungen in regelmäßigen Abständen erforderlich sein,[76] sicherlich auch angesichts der Höhe einer sonst zu erwartenden Kartellgeldbuße. Eine zunehmende Bereitschaft zur Durchführung von *Internal Investigations* ist dabei si-

---

71 *Spindler* in Münchener Kommentar zum AktG, 3. Aufl., 2008, § 91 Rn. 36; vgl. auch *Fleischer*, AG 2003, 291 ff. (298).
72 *Spindler*, a.a.O.
73 Vgl. *Wagner*, a.a.O. (11 m.w.N.).
74 Vgl. *Fleischer*, AG 2003, 291 ff. (293).
75 *Fleischer*, a.a.O. (294).
76 *Fleischer,* a.a.O.

cherlich auch der rechtspolitischen Tendenz zur Verschärfung der Organhaftung geschuldet.[77]

Allerdings werden solche *Internal Investigations*, die von der Intensität ihres Eingriffs in das Unternehmensgeschehen her einem hoheitlichen Ermittlungsverfahren ähneln, beispielsweise durch Mitarbeiterbefragungen und Auswertungen umfangreicher Datensätze, normalerweise erst dann in Betracht zu ziehen sein, wenn eine anderweitige Aufklärung nicht in gleichem Maße erfolgversprechend ist.[78]

Ziffer 4.1.3 des Deutschen Corporate Governance Kodex („DCGK") unterstreicht die Verantwortlichkeit des Vorstands für die Compliance. Als „Katalysator" bei der Entscheidung für *Internal Investigations* können weitere Vorschriften des DCGK wirken. So informiert beispielsweise der Vorstand den Aufsichtsrat regelmäßig, zeitnah und umfassend unter anderem über alle Fragen der Compliance (Ziffer 3.4. Abs. 2 DCGK). Je komplexer und schwerwiegender der Verdacht eines Compliance-Verstoßes oder ein evidenter Compliance-Verstoß und je größer das Ausmaß des potentiellen Schadens für die Gesellschaft ist, desto eher wird der Vorstand eine umfassende Untersuchung anordnen.

Fraglich ist, ob auch der Aufsichtsrat zur Anordnung bzw. Durchführung einer *Internal Investigation* verpflichtet sein kann, etwa für den Fall, dass Compliance-Verstöße von Vorständen im Raum stehen. Zur Sorgfaltspflicht des Aufsichtsrats zählt es, sich mit Anhaltspunkten für Pflichtwidrigkeiten des Vorstands zu befassen. So muss der Aufsichtsrat bei ihm bekannt werdenden rechtswidrigen Maßnahmen des Vorstands einschreiten und ist verpflichtet, Schadensersatzansprüche der Gesellschaft gegen den Vorstand zu prüfen.[79] Neben der Rechtmäßigkeit hat der Aufsichtsrat auch die Ordnungs- und Zweckmäßigkeit der Geschäftsführung zu überwachen und muss sich einschalten, wenn das Verhalten des Vorstands

---

77 U.a. durch die geplante Verlängerung der Verjährungsfrist für die aktienrechtliche Organhaftung, vgl. Art. 5 des Referentenentwurfs eines „Gesetzes zur Restrukturierung und geordneten Abwicklung von Kreditinstituten, zur Errichtung eines Restrukturierungsfonds für Kreditinstitute und zur Verlängerung der Verjährungsfrist der aktienrechtlichen Organhaftung". Siehe dazu auch *Baums*, ILF Working Paper Series Nr. 119, Managerhaftung und Verjährungsfrist, abrufbar unter http://www.ilf-frankfurt.de/uploads/media/ILF_WP_119.pdf.

78 Zum Spannungsverhältnis zwischen Compliance und Mitarbeiterdatenschutz siehe Ziffer 3.4.5 auf S. 34.

79 *Drygala* in *Schmidt/Lutter*, AktG, 2008, § 116 Rn. 8 ff. und § 111 Rn. 11 ff.

nicht im Einklang mit den Vorgaben des Aktiengesetzes sowie der Gesellschaftssatzung und weiteren Normen steht, die sich auf die Gesellschaft beziehen.[80] Nach § 111 Abs. 2 AktG kann der Aufsichtsrat im Rahmen seines Einsichts- und Prüfungsrechts in die Unterlagen und die Vermögensverhältnisse der Gesellschaft Nachforschungen anstellen und unter anderem für bestimmte Aufgaben besondere Sachverständige hinzuziehen bzw. beauftragen.

Allerdings darf eine vollständige Delegation des Prüfungs- bzw. Überwachungsauftrags nicht erfolgen.[81] Zudem sind die Kompetenzverteilungen zwischen Vorstand und Aufsichtsrat zu beachten. Das heißt, dass in die eigenverantwortliche Leitung der Gesellschaft durch den Vorstand grundsätzlich nicht eingegriffen werden darf, weshalb unter anderem ein Herausgabeverlangen von Vorstandsprotokollen und auch die Befragung von Mitarbeitern durch den Aufsichtsrat höchst sensibel ist. Zumindest an der Zulässigkeit von Mitarbeiterbefragungen durch den Aufsichtsrat werden Zweifel geäußert.[82] Daher sollte bei der Anordnung von investigativen Maßnahmen durch den Aufsichtsrat Vorsicht geboten sein und eine solche Entscheidung mit der gebotenen Sorgfalt abgewogen werden.

3.4.2 Branchenspezifische Spezialregelungen der Risikofrüherkennung

Über die aktienrechtliche Pflicht zur Ergreifung von Maßnahmen zur Früherkennung von bestandsgefährdenden Risiken hinaus existieren branchenspezifische Spezialregelungen, beispielsweise im Hinblick auf Kreditinstitute und Wertpapierhandelsunternehmen. § 25a Kreditwesengesetz (KWG) adressiert explizit bestimmte organisatorische Pflichten, beispielsweise ein angemessenes Risikomanagement, welches die Errichtung eines internen Kontrollsystems und Prozesse zur Identifizierung und Beurteilung bestehender Risiken enthalten muss. Hierzu existieren auch umfangreiche Verwaltungsvorschriften, welche die Mindestanforderungen an das Risikomanagement in einem einheitlichen Rahmen zusammentragen, wie beispielsweise die von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) erlassenen Mindestanforderungen für das Risikomanagement (MaRisk).[83]

---

80 *Drygala*, a.a.O., § 111 Rn. 15, 16.

81 Vgl. *Drygala*, a.a.O. Rn. 28; vgl. auch *Habersack* in: MüKo „AktG“, 3. Aufl., 2008, § 111 Rn. 71 m.w.N.

82 Vgl. *Habersack*, a.a.O.

83 *Spindler* in MüKo „AktG“, 3. Aufl., 2008, § 91 Rn. 32; MaRisk abrufbar un-

Maßnahmen zur Risikofrüherkennung finden gleichfalls aufgrund der sogenannten Basel-II-Anforderungen statt. Danach müssen Banken in qualifizierter Weise das Risiko jeder Gesellschaft vor jeglicher Fremdmittelvergabe auf der Basis eines internen Rating-Systems einschätzen.[84] Vergleichbare Pflichten zur Risikofrüherkennung sind nach dem Wertpapierhandelsgesetz (WpHG) gegeben. Nach §§ 31 ff. WpHG sind Wertpapierhandelsunternehmen grundsätzlich zu einer anlegerschutzorientierten Organisation verpflichtet. § 33 WpHG normiert die ausdrückliche Pflicht zur Errichtung einer dauerhaften und wirksamen Compliance-Funktion (§ 33 Abs. 1 Nr. 1 WpHG). Dies wird gleichzeitig durch Verwaltungsvorschriften der BaFin konkretisiert. Maßgeblich sind hier die Mindestanforderungen an die Compliance (MaComp).[85]

3.4.3 Kartellrecht und Wettbewerbsrecht

Kartellrechtswidrige Absprachen zwischen Unternehmen werden sowohl von nationalen, als auch von internationalen Rechtsvorschriften empfindlich sanktioniert. Die von der EU-Kommission verhängten Bußgelder gelten dabei als die weltweit höchsten.[86] Nationale Rechtsvorschriften lassen es oftmals für ihre Anwendbarkeit ausreichen, dass sich ein Kartell auf einen inländischen Markt erstreckt, wenngleich die Kartellabsprache auch im Ausland getroffen worden ist. Diese extraterritoriale Rechtsanwendung stellt für viele Unternehmen ein unkalkulierbares Risiko dar, da unter anderem Geldbußen in ungeahnter Höhe drohen. Unabhängig davon droht beim Bekanntwerden von Preisabsprachen stets ein internationaler Reputationsverlust.

Einen spezifischen Anreiz für die Unternehmen zur Aufklärung und Offenlegung von Kartellverstößen und Zusammenarbeit mit den Kartellbehörden bilden die von der EU-Kommission erlassene Kronzeugenregelung für Kartellsachen[87] und die Bonusregelung des Bundeskartellamtes.[88]

---

ter http://www.bafin.de/nn_724304/SharedDocs/Veroeffentlichungen/DE/Service/Rundschreiben/2009/rs_0915_ba_marisk.html.

84 *Spindler*, a.a.O., Rn. 33.

85 Abrufbar unter http://www.bafin.de/nn_722758/SharedDocs/Veroeffentlichungen/DE/Service/Rundschreiben/2010/rs_1004_wa_macomp.html, siehe auch für die Versicherungswirtschaft die Regelung des § 64a VAG.

86 Vgl. Tabelle 1 und Tabelle 2 auf S. 13.

87 Mitteilung über den Erlass und die Ermäßigung von Geldbußen in Kartellsachen, Amtsblatt C298 vom 8. Dezember 2006, abrufbar unter http://europa.eu/legislation_summaries/competition/firms/l26119_de.htm.

88 Bekanntmachung Nr. 9/2006 über den Erlass und die Reduktion von Geld-

Nach der EU-Kronzeugenregelung gewährt die Kommission auf Antrag den vollständigen Erlass der Geldbuße, wenn ein Unternehmen als erstes Unternehmen Beweise für ein der EU-Kommission bis dato unbekanntes Kartell vorlegt oder im Falle der Kenntnis der Kommission entscheidende Beweise vorlegt, welche die Feststellung des Kartells ermöglichen.[89] Sofern ein Anspruch auf den vollständigen Erlass der Geldbuße nicht besteht, verspricht die Kommission im Rahmen der Kronzeugenregelung eine Ermäßigung, wenn der Kommission Beweise vorgelegt werden, die einen erheblichen Mehrwert darstellen.

Nach den Bonusregelungen des Bundeskartellamts kann einem Kartellbeteiligten das zu erwartende Bußgeld bis zur Hälfte reduziert oder gar ganz erlassen werden. Voraussetzung ist, dass der Beteiligte sich als erster an das Bundeskartellamt wendet, bevor dieses über ausreichende Beweismittel verfügt, um einen Durchsuchungsbeschluss zu erwirken oder die Tat nachzuweisen. Der Kartellbeteiligte muss die Beweismittel durch mündliche oder schriftliche Informationen erbringen und darf bei dem Kartell keine tragende Rolle gespielt haben. In beiden Fällen, sowohl auf europäischer als auch auf nationaler Ebene ist die uneingeschränkte Kooperation mit der Kommission bzw. der Kartellbehörde Voraussetzung, um in den Genuss der Sanktionsmilderung oder des vollständigen Sanktionserlasses zu gelangen.

Der empfindliche Sanktionsrahmen, den das Gesetz gegen Wettbewerbsbeschränkungen (GWB) für wettbewerbsverzerrendes Verhalten vorsieht, kann darüber hinaus zur Kooperation mit der Kartellbehörde motivieren: Neben einer Schadensersatzpflicht sieht das Gesetz eine Vorteilsabschöpfung durch die Kartellbehörde oder auch durch bestimmte rechtsfähige Verbände vor.[90] Das Gesetz gegen den unlauteren Wettbewerb (UWG) enthält vergleichbare Regelungen bei unlauteren geschäftlichen Handlungen, beispielsweise Täuschung, Irreführung oder Belästigung von Verbrauchern.[91]

---

bußen in: Kartellsachen – Bonusregelung – vom 7. März 2006, abrufbar unter http://www.bundeskartellamt.de/wDeutsch/download/pdf/Merkblaetter/Merkblaetter_deutsch/06_Bonusregelung.pdf.

89 *Langen*/*Bunte*, VO Nr. 1/2003 Rn. 56; EU-Kronzeugenregelung, Rn. 8 a)+b).

90 Vgl. §§ 33 Abs. 2, 34, 34a GWB

91 Vgl. §§ 8 Abs. 3 Nr. 2, 10 UWG

3.4.4 Vergaberecht

Gemäß § 97 Abs. 4 GWB muss ein Unternehmen gesetzestreu und zuverlässig sein, um für öffentliche Aufträge in Betracht zu kommen. Bestehen Zweifel an der Zuverlässigkeit, die sich etwa durch Einträge im Gewerbezentralregister manifestieren, kann das Unternehmen von Vergabeverfahren (Bieterverfahren) ausgeschlossen werden.[92] Darüber hinaus ist ein Unternehmen zwingend vom Vergabeverfahren auszuschließen, sofern eine dem Unternehmen zurechenbare Person rechtskräftig wegen Bestechung, Betrugs oder Geldwäsche verurteilt wurde.[93] In den Bundesländern Nordrhein-Westfalen und Berlin zum Beispiel existieren Vergabe-/Korruptionsregister, in denen die Daten von Gesellschaften, in denen Korruptionsfälle bekannt wurden, gespeichert werden. Die Registergesetze dieser Länder sehen vor, dass ein Eintrag schon dann erfolgen kann, wenn nach bestehender Beweislage vernünftige Zweifel am Vorliegen eines Korruptionsfalls nicht bestehen.[94]

Sofern allerdings das Unternehmen Maßnahmen ergreift, um die in der Vergangenheit geschehenen Missstände künftig auszuschließen und sozusagen eine „Selbstreinigung“ durchführt, kann nach der Rechtsprechung von Ausschlüssen von Vergabeverfahren abgesehen werden.[95] Als Teil einer geeigneten Maßnahme wird unter anderem die Aufklärung der Rechtsverstöße angesehen.[96]

---

92 § 8 Nr. 5 Abs. 1 c) VOB/A bzw. inhaltsgleich § 7 Nr. 5 c) VOL/A (jeweils Ausgabe 2006), abrufbar unter http://www.bmvbs.de/Anlage/original_982127/VOB-A_-Ausgabe-2006.pdf: „Von der Teilnahme am Wettbewerb dürfen Unternehmer (können Bewerber) ausgeschlossen werden, ... c) die nachweislich eine schwere Verfehlung begangen haben, die ihre Zuverlässigkeit als Bewerber in Frage stellt, ...“.

93 Vgl. *Moosmayer*, S. 13, m.w.N., vgl. auch Art. 45 Abs. 1 der Richtlinie 2004/18/EG über die Koordinierung der Verfahren zur Vergabe öffentlicher Bauaufträge, Lieferaufträge und Dienstleistungsaufträge.

94 Vgl. § 5 Abs. 2 Nr. 6 des Gesetzes zur Verbesserung der Korruptionsbekämpfung und zur Errichtung und Führung eines Vergaberegisters in Nordrhein-Westfalen; § 3 Abs. 2 Nr. 4 des Gesetzes zur Einrichtung und Führung eines Registers über korruptionsauffällige Unternehmen in Berlin (Korruptionsregistergesetz – KRG).

95 Vgl. *Moosmayer*, a.a.O. mit Verweis auf Ständige Rechtsprechung seit OLG Frankfurt WRP 1997, 203, zuletzt OLG Brandenburg NZBau 2008, 277.

96 *Moosmayer*, a.a.O.

3.4.5 Datenschutzrecht

Nach der derzeit geltenden Fassung des § 32 Bundesdatenschutzgesetz (BDSG) ist der Umgang mit Daten aus einem Beschäftigungsverhältnis einer besonderen Sensibilität unterworfen. § 32 BDSG erlaubt den Umgang mit personenbezogenen Beschäftigtendaten nur dann, wenn dies für die Entscheidung über die Begründung, Beendigung oder Durchführung eines Beschäftigungsverhältnisses „erforderlich" ist. Diese Regelung ist im Vorfeld heftig kritisiert worden, da sie unter anderem die Korruptionsbekämpfung erschwere und Unternehmen im Bereich Compliance veranlasse, zunächst abzuwarten, bis Klarheit darüber besteht, was erlaubt und was verboten ist.[97]

Inwieweit im Rahmen einer *Internal Investigation* beispielsweise Mitarbeiterbefragungen oder ein „Datenscreening" von den Grenzen des § 32 BDSG noch erfasst sind oder gegebenenfalls darüber hinaus gehen, lässt sich nicht generell, sondern nur für den Einzelfall beantworten und ist eine schwierige Abwägungsfrage.

Was „erforderlich" sein soll, ist laut Gesetzesbegründung anhand der von der Rechtsprechung entwickelten Grundsätze zum Datenschutz im Beschäftigtenverhältnis zu bestimmen.[98] Kriterien sind hier insbesondere die Grundsätze der Datenvermeidung und Datensparsamkeit und generell der Grundsatz der Verhältnismäßigkeit.[99] Auf Mitarbeiterebene ist unter anderem danach zu fragen, ob der Umgang mit personenbezogenen Daten die Geschäftsphäre, Privatsphäre oder Intimsphäre des Mitarbeiters tangiert. Während ein Eingriff in die Geschäftssphäre grundsätzlich durch ein berechtigtes Interesse des Arbeitgebers gerechtfertigt werden kann, scheinen Eingriffe in die Privatsphäre nur unter besonderen Umständen angemessen zu sein, sofern sich das Privatleben des Beschäftigten auf das Beschäftigungsverhältnis erstreckt. Ein Eingriff in die Intimsphäre hat grundsätzlich zu unterbleiben.[100]

Aus Sicht des Unternehmens ist insbesondere zu beachten, dass sein Interesse am Umgang mit personenbezogenen Daten die schutzwürdigen In-

---

97 Vgl. *Wybitul*, BB 2010, 1085 ff.

98 Vgl. Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss) zum Regierungsentwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften (BT-Drs. 13/657), vgl. auch *Wybitul*, a.a.O., 1085.

99 *Wybitul*, a.a.O., 1086 f.

100 Vgl. auch *Wybitul*, a.a.O., 1087.

teressen der von der Maßnahme betroffenen Mitarbeiter überwiegen muss.[101] Nicht selten stehen Unternehmen, d.h. insbesondere die Geschäftsleitung, hier vor einem Dilemma: Entweder kann ein nicht adäquat gemanagter Compliance-Verstoß oder aber, bei einem intensiven Umgang mit Mitarbeiterdaten, ein Verstoß gegen datenschutzrechtliche Bestimmungen entstehen, der sich schlimmstenfalls zu einem Datenskandal entwickelt. Auch die derzeit geplanten Änderungen im Zusammenhang mit der Einführung des Beschäftigtendatenschutzgesetzes in Form des § 32d Abs. 3 BDSG[102] und § 32e Abs. 3 BDSG[103] scheinen keine weitere Rechtssicherheit zu bringen.

---

101 *Hauschka/Salvenmoser*, „Korruption, Datenschutz und Compliance", NJW 2010, 331 ff. (335).

102 Referentenentwurf des § 32d BDSG (Stand: 7. Juli 2010):

„(3) Der Arbeitgeber darf Beschäftigtendaten auch verarbeiten und nutzen, soweit dies erforderlich und nach Art und Ausmaß nicht unverhältnismäßig ist, um die Verletzung von Pflichten, die sich aus dem Beschäftigungsverhältnis ergeben (Pflichtverletzungen), Ordnungswidrigkeiten oder Straftaten durch den Beschäftigten im Beschäftigungsverhältnis zu verhindern oder aufzudecken. Entsprechende Anforderungen ergeben sich z.B. für die Kreditwirtschaft unter anderem aus dem Kreditwesengesetz und dem Geldwäschegesetz."

Erlaubte Zweckänderung aus der Entwurfsbegründung: „Absatz 3 stellt eine Grundlage für die Korruptionsbekämpfung und die Durchsetzung von Compliance-Anforderungen dar. Compliance bedeutet in diesem Zusammenhang die Einhaltung aller relevanten Gesetze, Verordnungen, Richtlinien und Selbstverpflichtungen durch ein Unternehmen als Ganzes."

103 Referentenentwurf des § 32e BDSG (Stand: 7. Juli 2010):

„Der Arbeitgeber darf Beschäftigtendaten zur Verhinderung oder Aufdeckung von Pflichtverletzungen, von Ordnungswidrigkeiten oder von Straftaten ohne Kenntnis des Beschäftigten nur erheben, wenn

1. tatsächliche Anhaltspunkte bestehen, die den Verdacht begründen, dass der Beschäftigte im Beschäftigungsverhältnis
   a. eine schwerwiegende Pflichtverletzung,
   b. eine Ordnungswidrigkeit oder
   c. eine Straftat begangen hat,

   die den Arbeitgeber zu einer fristlosen Kündigung aus wichtigem Grund berechtigen würde,
2. die Erhebung, erforderlich ist, um diese aufzudecken oder um weitere schwerwiegende Pflichtverletzungen oder weitere Ordnungswidrigkeiten und Straftaten zu verhindern und
3. Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Der Arbeitgeber darf die nach Satz 1 erhobenen Daten nur für Zwecke, für die sie erhoben wurden, verarbeiten und nutzen. Die den Verdacht begründenden tatsächlichen Anhaltspunkte sind vor der Datenerhebung zu dokumentieren. Der Beschäftigte ist über die Erhebung, Verarbeitung oder Nutzung zu benachrichtigen, sobald deren Zweck durch die Benachrichtigung nicht gefährdet wird."

Zwar heißt es im Zusammenhang mit den geplanten Regelungen für den Beschäftigtendatenschutz im Eckpunktepapier des Bundesministeriums des Inneren (BMI) vom 31. März 2010:[104]

> „Die Korruptionsbekämpfung und die Durchsetzung von Compliance-Anforderungen sollten aufgrund klarer gesetzlicher Grundlagen erfolgen können. Der Arbeitgeber soll grundsätzlich vorhandene Beschäftigungsdaten verwenden dürfen, soweit dies erforderlich und verhältnismäßig ist, um die Begehung von Vertragsverletzungen zu seinen Lasten, Ordnungswidrigkeiten oder Straftaten durch den Beschäftigten im Beschäftigungsverhältnis zu verhindern oder aufzudecken. Nur wenn ein konkreter Verdacht gegenüber einem Beschäftigten besteht, soll der Arbeitgeber zusätzliche Daten unter erhöhten Voraussetzungen erheben dürfen."

Gleichwohl sind die derzeit diskutierten Entwürfe noch nicht zielführend. Die Rechtsunsicherheit des Balanceakts zwischen Compliance-Anforderungen und Datenschutz wird den Unternehmen aufgebürdet. In diesem Zusammenhang müssen vom Gesetzgeber klare Regelungen getroffen werden, damit der Vorstand sich nicht zwischen dem Risiko eines Compliance-Korruptionsfalls oder eines Datenschutzskandals entscheiden muss. Zu einer derartigen *Loose-Loose*-Situation darf es nicht kommen.

3.4.6 Steuer- und Abgabenrecht

Im Steuerrecht bestehen allgemein- und spezialgesetzliche Mitwirkungspflichten des Steuerpflichtigen zur Aufklärung von Steuersachverhalten. Nach der allgemeinen Mitwirkungspflicht des § 90 Abs. 1 Abgabenordnung (AO) sind die Beteiligten in einem Steuerverfahren zur Mitwirkung bei der Ermittlung des Sachverhalts verpflichtet. Dieser Pflicht wird vor allem durch wahrheitsgemäße und vollständige Offenlegung der für die Besteuerung erheblichen Tatsachen nachgekommen. Im Falle der Unrichtigkeit oder Unvollständigkeit einer Erklärung ist vom Steuerpflichtigen eine Berichtigung vorzunehmen.[105] Sofern es sich um Sachverhalte mit Auslandsbezug handelt, existiert eine gesteigerte Mitwirkungspflicht gegenüber den deutschen Steuerbehörden: Hier haben die Beteiligten die betreffenden Sachverhalte selbst aufzuklären und die erforderlichen Be-

---

104 Abrufbar unter http://www.bmi.bund.de/cae/servlet/contentblob/941830/publicationFile/60604/eckpunkte_an_datenschutz.pdf.

105 Vgl. § 153 AO.

weismittel zu beschaffen, wobei sie alle für sie bestehenden rechtlichen und tatsächlichen Möglichkeiten auszuschöpfen haben.[106]

Grundsätzlich müssen die Beteiligten bis zur Grenze des Zumutbaren an der Sachverhaltsaufklärung mitwirken.[107] Dabei können auch *Internal Investigations* eine Rolle spielen. Allerdings ist auch hier der Grundsatz der Verhältnismäßigkeit zu beachten.[108] Der staatlicherseits zu erwartende Nutzen aus der Mitwirkung darf in keinem Missverhältnis zum zeitlichen, persönlichen und finanziellen Aufwand des Betroffenen stehen. Wenn man davon ausgeht, dass es für den (Steuer-)Auskunftspflichtigen unzumutbar sein soll, zum Zweck der Auskunftserteilung zunächst – auf eigene Kosten – Nachforschungen anzustellen[109], wäre erst recht die Mandatierung externer Berater auf eigene Kosten unter Verhältnismäßigkeitsgesichtspunkten als nicht zumutbar anzusehen. Dies steht auch mit dem Wortlaut von § 90 AO in Einklang, wonach grundsätzlich nur ein Beteiligter selbst bzw. sein Bevollmächtigter, respektive Verwalter, nach § 34 AO mitwirkungspflichtig ist.[110]

3.4.7 Ordnungswidrigkeitsrecht, Straf- und Strafprozessrecht

§ 130 des Gesetzes gegen Ordnungswidrigkeiten (OWiG) gibt dem Inhaber eines Betriebs die Schaffung von Aufsichtsstrukturen zur Verhinderung von Verstößen gegen ihn treffende Pflichten auf. Sofern entsprechende Compliance-Strukturen nicht geschaffen werden, kann gegen den Betriebsinhaber und darüber hinaus auch gegen den Betrieb als solchen ein Bußgeld verhängt werden.[111]

§ 130 OWiG kommt in der Praxis eine ständig wachsende Bedeutung zu. Das hängt auch damit zusammen, dass nach deutschem Recht eine Strafbarkeit juristischer Personen, anders als beispielsweise in den USA oder Großbritannien, nicht existiert und über die Zurechnungsnorm § 30 OWiG auch Sanktionen gegen juristische Personen ermöglicht werden.

---

106 Vgl. § 90 Abs. 2 AO.
107 Vgl. *Söhn* in *Hübschmann/Hepp/Spitaler*, AO, 2009, § 90 Rn. 72.
108 *Söhn*, a.a.O. Rn. 92 ff.
109 *Söhn*, a.a.O. Rn. 119.
110 *Seer*, a.a.O. Rn. 10.
111 Vgl. § 30 OWiG; vgl. *Göhler*, „Gesetz über Ordnungswidrigkeiten“, 14. Aufl., 2006, § 130 Rn. 3.

Ob und unter welchen Umständen § 130 OWiG zur Errichtung eines umfassenden Compliance-Systems verpflichtet, welches auch *Internal Investigations* beinhaltet, lässt sich nicht eindeutig beantworten. Mindestens ist der Gefahr betriebstypischer Zuwiderhandlungen effektiv zu begegnen.[112] Hier werden Kernmerkmale der Compliance-Organisation berührt, wie die Personalauswahl, die Schulung des Personals in Compliance-relevanten Themen, ein funktionierendes Kontroll- und Aufsichtswesen sowie die sorgfältige Auswahl und Überwachung von Aufsichtspersonen.[113]

Aufsichtspflichten können aus einer Reihe von Vorschriften resultieren. Dazu zählen Spezialnormen, Gerichtsentscheide zur Konkretisierung von Sorgfaltspflichten sowie der allgemeine Grundsatz, dass bestimmte Lebenssachverhalte die Verantwortung für das Verhalten anderer Personen begründen.[114]

Die vom Betriebsinhaber zu treffenden Maßnahmen werden dabei jedoch immer verhältnismäßig sein müssen. Gerade wenn es um die Aufklärung eines Fehlverhaltens von Mitarbeitern geht, ist häufig der sensible Bereich des Datenschutzes tangiert.[115] Die ergriffenen Maßnahmen dürfen hier nicht über das Ziel hinausschießen; spiegelbildlich dazu dürfen dem Betriebsinhaber keine Maßnahmen abverlangt werden, die weder geeignet noch für ihn objektiv zumutbar sind.[116] Hierbei ist auch die Eigenverantwortung der Betriebsangehörigen zu beachten.[117] Es gilt der Grundsatz: je höher qualifiziert der Mitarbeiter ist, desto geringer ist die Kontrollpflicht und umgekehrt.[118]

Auch wenn ein Unternehmensstrafrecht in Deutschland nicht existiert, können Strafverfahren beispielsweise gegen Vorstände, Betriebsleiter, Aufsichtsräte oder auch einfache Mitarbeiter nachteilige Wirkungen auf das Unternehmen haben.

---

112 In diesem Zusammenhang sind auch die schwierigen Rechtsfragen zu sehen, die sich aus Konzernstrukturen ergeben, vgl. *Schneider,* NZG 2009, 1321 ff.

113 Vgl. *Hauschka*, § 25 Rn. 79.

114 Vgl. *Bohnert*, OWiG, 2. Aufl., 2007, § 130 Rn. 17.

115 Siehe vorstehend Ziffer 3.4.5 auf S. 38.

116 Vgl. *Bohnert*, OWiG, 2. Auf. 2007, § 130, Rn. 19, 20.

117 *Wieser*, OWiG, 88. AL, Dezember 2007, § 130, Rn. 6.1.

118 Vgl. *König* in *Göhler,* Gesetz über Ordnungswidrigkeiten, 15. Aufl., 2009, § 130, Rn. 12.

Bei Wirtschaftsstrafverfahren findet häufig eine Kooperation der Unternehmensseite mit der Staatsanwaltschaft statt. Ziel ist der Abschluss eines sogenannten *Deals*, das heißt Reduktion des Strafmaßes bzw. Einstellung des Verfahrens gegen eine Geldbuße. In der Regel wird sich die Staatsanwaltschaft für eine Kooperation bei der Aufklärung der Straftat erkenntlich zeigen. Darüber hinaus kommt es zu einem zügigen Verfahrensabschluss, was dem Unternehmen die Ressourcenbindung durch Zeugenaussagen von Mitarbeitern und Vorlagepflicht von Dokumenten etc., wodurch evtl. die Gefahr der Aufdeckung und Ahndung weiterer Rechtsverstöße besteht, erspart. Zum anderen bleibt gerade bei einer Verfahrenseinstellung gegen Auflagen nach § 153a StPO eine öffentliche Hauptverhandlung aus, wodurch Negativschlagzeilen vermieden bzw. begrenzt werden können.

Auch in Deutschland stellt sich die Frage nach *Internal Investigations* typischerweise im internationalen Geschäftsverkehr im Zusammenhang mit Korruptionsdelikten, vor allem mit der Bestechung von Amtsträgern.[119]

Ein wichtiger Anreiz zur Schaffung von Kontrollmechanismen zur Prävention strafrechtlichen bzw. ordnungswidrigen Verhaltens auf der Unternehmensebene ist die in den letzten Jahren ausgeweitete Rechtsprechung des BGH zur Abschöpfung des durch die Tat Erlangten (Verfall). So hat die höchstrichterliche Rechtsprechung zunächst bestätigt, dass die Abschöpfung nach dem sogenannten „Bruttoprinzip“ vorzunehmen ist, das heißt des gesamten Erlöses aus der Tat ohne Abzug eigener Aufwendungen, zum Beispiel eines Einkaufspreises, etc.[120] Da es sich beim Verfall nicht um eine Strafe oder strafähnliche Maßnahme handelt, sondern um eine Maßnahme eigener Art, müsse zudem der Verfall auch gegen begünstigte Dritte und beispielsweise juristische Personen angeordnet werden, und zwar auch dann, wenn der Dritte bzw. das respektive Organ der juristischen Person keine Straftat begangen hat.[121]

---

119 Dazu detailliert Ziffer 7.2.3 auf S. 105.

120 Vgl. *Taschke* in *Semler/Peltzer* „Arbeitshandbuch für Vorstandsmitglieder“, 2005, § 10 Rn. 246.

121 Vgl. *Taschke*, a.a.O., vgl. auch *Seidel* in *Hauschka*, § 25 Rn. 106.

4. Typische Auslöser für eine Internal Investigation

Für das Bekanntwerden bzw. den Verdacht von Compliance-Verstößen, die das Management zur Durchführung einer *Internal Investigation* veranlassen, sind verschiedene Ursachen denkbar.

Von hoher Bedeutung für die Meldung von Missständen sind Reporting-Systeme, welche aus den Compliance-Systemen gerade international operierender Unternehmen heute nicht mehr wegzudenken sind. Reporting-Systeme ermöglichen es Mitarbeitern, Missstände anonym zu melden. Im Wesentlichen sind zwei Formen denkbar, sogenannte *Whistleblowing-Hotlines* und der Ombudsmann. *Whistleblowing-Hotlines* werden teilweise über externe Dienstleister betrieben, um die Anonymität des Hinweisgebers zu wahren, teilweise sind sie aber auch unternehmensintern bei der Compliance-Organisation angesiedelt.[122] Beim Ombudsmann handelt es sich i.d.R. um einen externen Rechtsanwalt, der vom Unternehmen beauftragt wird, Mitarbeitern und Dritten als Anlaufstelle für Hinweise oder Beschwerden zur Verfügung zu stehen. Im amerikanischen Recht wird die Einrichtung von Reporting-Systemen explizit vorgeschrieben.[123] Sie nehmen in der Praxis zur Aufdeckung von Compliance-Verstößen einen wichtigen Stellenwert ein.

Vergleichbar effektiv sind gesetzliche Kronzeugenregelungen.[124] Sofern ein Mitarbeiter sich selbst strafbar macht, ist damit zu rechnen, dass die Inanspruchnahme einer Sanktionsreduzierung gegen umfassende Kooperation mit den Ermittlungsbehörden zu seiner Verteidigungsstrategie zählen wird. Hierdurch können Missstände im Unternehmen offenbart werden, die eine *Internal Investigation* auslösen können, um auch seitens des Unternehmens durch Kooperation mit den Ermittlungsbehörden eine mögliche Sanktionsreduzierung zu erwirken, zum Beispiel sofern es um ein Kartell geht.[125] Gerade im Kartellrecht sind auch Anzeigen von Wettbewerbern oder Vertragspartnern eine Ursache, auf Grund derer die Kartellbehörden auf ein Unternehmen aufmerksam werden.

Auch ist denkbar, dass ein Mitarbeiter seine Kenntnisse über einen Compliance-Verstoß direkt der Presse gegenüber offenbart. In einer sol-

---

122 Vgl. *Moosmayer*, S.54.
123 Vgl. Sec. 301 SOX, s.o. Ziffer 3.2.4 auf S. 25.
124 zu § 46b StGB siehe Ziffer 6.7 auf S. 72.
125 Hinsichtlich weiterer Einzelheiten verweisen wir vorstehend auf die Ziffer 3.4.3 auf S. 35.

chen Situation wird die Unternehmenskommunikation vor eine besondere Herausforderung gestellt, da bei einer Pressekampagne ein besonders großer Reputationsverlust droht.

Ermittlungsbehörden können darüber hinaus aufgrund gesetzlicher Meldepflichten auf Compliance-Verstöße in einem Unternehmen aufmerksam werden. So hat beispielsweise ein Steuerprüfer im Rahmen einer Außenprüfung der Finanzbehörde Meldung zu erstatten, wenn er auf Anhaltspunkte für eine Straftat stößt.[126]

Vermehrt dürfte es zu einem Anfangsverdacht auch im Zusammenhang mit arbeitsgerichtlichen Verfahren kommen, bei denen es um die Beendigung des Arbeitsverhältnisses eines vermeintlichen Einzeltäters geht. So hat beispielsweise das Arbeitsgericht München[127] die verhaltensbedingte Kündigung eines Arbeitnehmers für treuwidrig gehalten, der dabei mitgewirkt hatte, Gelder aus dem regulären Zahlungskreislauf in „schwarze Kassen“ umzuleiten. Das Unternehmen treffe, so das Gericht, wegen der systematischen Ermöglichung und Billigung schwarzer Kassen eine erhebliche Mitverantwortung, die dem Mitarbeiter dann letztlich nicht mehr zu Last gelegt werden könnte. Aus Sicht des überführten Täters liegt es also nahe, im Prozess möglichst systematische und unternehmensweite Compliance-Verstöße zu behaupten, um die eigene Situation zu verbessern, frei nach dem Motto: „Die anderen waren noch schlimmer“, „Ich war nur ein Rädchen im Getriebe“ oder „Die wussten alles“. Der letzte Einwand wird im Kündigungsschutzverfahren schon deshalb meist erhoben, um zu argumentieren, dass der Ausspruch der Kündigung seitens des Arbeitgebers nicht innerhalb von zwei Wochen nach Kenntnisnahme der Vorwürfe erfolgte und die Kündigung deshalb unwirksam ist.[128]

Die extraterritoriale Anwendung etwa von Korruptionsgesetzen – beispielsweise des US-amerikanischen *FCPA* – kann ebenfalls Ursache für das Erfordernis einer *Internal Investigation* bei einem deutschen Unternehmen (einschließlich etwaiger ausländischer Tochtergesellschaften) sein.

---

126 Vgl. § 10 Allgemeine Verwaltungsvorschrift für die Betriebsprüfung - Betriebsprüfungsordnung - (BpO 2000).

127 2. Oktober 2008, NZA-RR 2009, 134ff; dazu genauer Ziffer 7.2.1 auf S. 102.

128 Zur Zweiwochenfrist nach § 626 Abs. 2 BGB siehe Ziffer 7.2.2 auf S. 104.

Sobald das *DOJ* und die *SEC* getrennt oder (üblicherweise) gemeinsam einen *FCPA*-Fall untersuchen und Anhaltspunkte für eine Beteiligung an korruptiven Zahlungen bestehen, können deutsche Gesellschaften in Ermittlungstätigkeiten der US-Behörden einbezogen werden. Es ist etwa denkbar, dass eine bestimmte (deutsche) Tochtergesellschaft im Zusammenhang mit einem bestimmten Projekt in einem Drittland näher untersucht werden soll (anders ausgedrückt Gegenstand einer *Internal Investigation* sein soll). Wenn sich das Unternehmen im Stadium der freiwilligen informellen Kooperation durchaus weigern könnte, entsprechende Untersuchungsmaßnahmen durchzuführen, wird es im Zweifel dennoch zustimmen, um sich die Chance zu erhalten, dass dann entweder überhaupt keine Anklage erhoben wird oder im Rahmen sogenannter *Settlement Negotiations*, quasi Vergleichsverhandlungen, eine spürbare Sanktionsminimierung erzielt wird.

Denkbar ist auch, dass eine geforderte *Internal Investigation* Gegenstand einer *Subpoena* (lateinisch: unter Strafe) ist. Hierbei handelt es sich um ein im amerikanischen Beweisrecht eingesetztes Zwangsmittel, mit dem Beteiligte und Dritte zur Auskunft in oder gelegentlich vor einem Prozess verpflichtet werden.

Schließlich kann ein aufgrund unternehmensinterner Meldepflichten gemeldeter Compliance-Verstoß eine *Internal Investigation* rechtfertigen. Gerade in Konzernen existieren im Regelfall konzerninterne Berichtspflichten, die wesentlicher Bestandteil des Compliance-Systems sind. Einfach ausgedrückt ist dort definiert, wer wem wann was berichten muss. Da der Gesetzgeber für die Definition von Berichtspflichten bei Compliance-Verstößen innerhalb eines Unternehmens oder Konzerns[129] keine bindenden Vorgaben gemacht hat, sollte sich das Berichtswesen vor allem an praktischen Gesichtspunkten orientieren.

Die Berichtspflichten sollten anhand folgender Fragen definiert werden:

- Handelt es sich bei dem Compliance-Verstoß um einen Verdachtsfall oder ist der Verstoß evident?
- Kann der Compliance-Verstoß im Rahmen der periodischen Regelberichtserstattung behandelt werden oder rechtfertigt bzw. erfordert er eine sofortige Berichterstattung?

---

129 Zu den in diesem Zusammenhang schwierigen Rechtsfragen vgl. *Schneider* NZG 2009, 1321.

- Wem gegenüber muss eine sofortige Berichterstattung erfolgen?
  (hier unter Annahme einer Konzernstruktur)
  - **Auf der Ebene der Tochtergesellschaft**:
    Compliance Officer der Tochtergesellschaft (**CO**),
    Geschäftsführer der Tochtergesellschaft (**BL**)
  - **Auf Konzernebene**:
    Chief Compliance Officer (**CCO**),
    Compliance Committee (**CC**),
    Vorstand (**VO**)
  - **Auf Gesellschafterebene**:
    Audit Committee des Aufsichtsrats (**AC**)

Um einerseits sicherzustellen, dass den verschiedenen Stellen im Unternehmen die wesentlichen Informationen zur Verfügung gestellt werden und andererseits zu verhindern, dass in der Konzernhierarchie weiter oben angesiedelte Stellen mit unwesentlichen Informationen überflutet werden, bietet sich die Einführung eines Eskalationsmodells an.

Tabelle 3: Schematisches Beispiel für ein Eskalationsmodell bei der Compliance-Berichterstattung (Berichtsempfänger)

		Verdachtsfall	Evidenter Verstoß
Geringes Schadensrisiko	**Regelberichterstattung**	CO	CO, BL CCO
	Ad-hoc-Berichterstattung		CO, BL
Mittleres Schadensrisiko	**Regelberichterstattung**	CO, BL CCO, CC	CO, BL CCO, CC, VO AC
	Ad-hoc-Berichterstattung	CO, BL CCO	CO, BL CCO, CC
Hohes Schadensrisiko	**Regelberichterstattung**	CO, BL CCO, CC, VO AC	CO, BL CCO, CC, VO AC
	Ad-hoc-Berichterstattung	CO, BL CCO, CC	CO, BL CCO, CC, VO AC

Die tatsächliche Ausgestaltung des Berichtswesens muss sich dabei naturgemäß an den Gegebenheiten im Unternehmen orientieren.

5. Beispielhafter Ablauf einer Internal Investigation

Die Erfahrung zeigt, dass die Aufklärung von Compliance-Verstößen in den meisten Fällen ein zeitkritischer Prozess ist. Je größer die Zeitspanne zwischen der Entdeckung eines verdächtigen Sachverhalts im Unternehmen und dessen Untersuchung ist, desto größer ist die Gefahr von Verschleierungshandlungen durch den oder die Täter, also die Gefahr, dass belastende Daten und Dokumente vernichtet werden. Außerdem besteht die Möglichkeit, dass Informationen in Form von Gerüchten reputationsschädlich nach außen dringen oder arbeitsrechtlich relevante Fristen verstreichen.[130]

Das Bekanntwerden eines Verdachtsfalls oder sogar eines offensichtlichen Verstoßes bedeutet für den „normalen" Geschäftsprozess immer eine Ausnahmesituation. Übereiliges Handeln im Sinne eines blinden Aktionismus ist genauso fehl am Platze wie eine zu zögerliche Herangehensweise. Kritischer Erfolgsfaktor in einer solchen Situation ist, wie ein Unternehmen in den ersten Stunden agiert.

Bewährt hat sich für solche Fälle die Erarbeitung eines Notfallplans, gerade auch für den Fall, dass die Ermittlungsbehörden „vor der Tür stehen". Dieser dient dem Zweck, dass alle notwendigen Maßnahmen von den jeweils zuständigen Personen in einer definierten und koordinierten Art und Weise ergriffen werden und zudem alle Informationsfäden bei einem zentralen Verantwortlichen zusammenlaufen. Die Aufstellung eines Notfallplans erfordert einen relativ geringen Zeitaufwand, kann im Ernstfall aber entscheidend für den erfolgreichen Umgang mit einem Compliance-Verstoß sein.

Um dem Leser eine Hilfestellung für die Entwicklung eines solchen Notfallplans oder Anregungen für einen bereits bestehenden Plan zu geben, sind die nachstehenden Ausführungen in Anlehnung an einen möglichen Notfallplan ausgestaltet.

5.1 Maßnahmen im Vorfeld

Die wesentlichen Weichen im Umgang mit einem Compliance-Verstoß sollten idealerweise bereits im Vorfeld gestellt worden sein. Wie anfangs beschrieben, entspricht ein solcher Fall nicht dem normalen Geschäftsab-

---

130 Zur Zweiwochenfrist siehe Ziffer 7.2.2, S. 104.

lauf, und es besteht das Risiko, dass durch Missverständnisse und unkoordiniertes Handeln kontraproduktive Aktionen durchgeführt oder wichtige Untersuchungshandlungen und Sicherungsmaßnahmen unterlassen werden.

Das „Wer (Zuständigkeit und Kommunikationswege) macht wann (Art der Umstände) was“ bei Compliance-Verstöße sollte daher in Form eines Notfallplans festgehalten werden. Der Plan muss dabei nicht notwendigerweise für jedes denkbare Szenario voll ausgearbeitete Handlungsanweisungen enthalten, es sollten aber zumindest relevante Eckpunkte geklärt sein. Für gewöhnlich ist es zielführend, die Komponenten eines Notfallplans im Vorfeld, gegebenenfalls mit externen Dienstleistern, abzustimmen, um ein Gefühl für die Praxisrelevanz der einzelnen Maßnahmen zu bekommen.

Im Folgenden sind die Eckpunkte aufgeführt, die ein Notfallplan auf jeden Fall enthalten sollte.

5.1.1 Verdachtsfall oder offenbarer Verstoß

Bei der Untersuchung von Compliance-Verstößen sind grundsätzlich zwei Szenarien denkbar: Der Verdachtsfall und der Fall eines evidenten Verstoßes. Der Umgang mit diesen beiden (Arten von) Szenarien sollte bereits im Vorfeld geregelt worden sein.

In einem Verdachtsfall gibt es berechtigten Grund zur Annahme, dass ein Mitarbeiter in einen Compliance-Verstoß verwickelt sein könnte. Auslöser für einen Verdachtsfall können beispielsweise ein anonymer Hinweis oder Unregelmäßigkeiten in den vom betreffenden Mitarbeiter durchgeführten Transaktionen sein. Bevor eine offene Investigation gegen den oder die Mitarbeiter initiiert wird, sollte das Unternehmen Folgendes berücksichtigen:

- Unabhängig vom Ergebnis der *Internal Investigation* wird das Vertrauensverhältnis mit dem Mitarbeiter fast zwangsläufig nachhaltig geschädigt. Gleiches gilt für den Leumund des Mitarbeiters.
- Investigative Maßnahmen können das Arbeitsklima im Unternehmen schädigen.
- Wird eine offene Investigation angestoßen, verliert das Unternehmen mit großer Wahrscheinlichkeit die Informationshoheit, das heißt es ist davon auszugehen, dass Informationen über den möglichen Compli-

ance-Verstoß nach außen und damit auch an die Presse oder an die Staatsanwaltschaft dringen.

Rechtfertigt der Grad des Verdachts bzw. der drohende Schaden die Durchführung einer *Internal Investigation,* so kann es zweckmäßig sein, einen verdeckten Ansatz zu wählen. Praktisch bedeutet dies, dass die die Untersuchung durchführenden Personen entweder von vornherein nicht im Unternehmen in Erscheinung treten (beispielsweise, wenn die Untersuchung sich auf elektronische Daten beschränkt) oder aber, dass die *Internal Investigation* unter einer entsprechenden Legende durchgeführt wird (Beratungsprojekt, Internal Audit etc.). Wie vorstehend dargelegt, handelt es sich bei derartigen Konstellationen allerdings um datenschutzrechtlich sensible Untersuchungen, die gegebenenfalls auch strafrechtlich relevant werden können.[131] In diesem Zusammenhang sollte daher unter allen Umständen der Datenschutzbeauftragte involviert sein und vor Durchführung einer Ermittlungstätigkeit Rechtsrat eingeholt werden.

5.1.2 Benennung verantwortlicher Stellen

Liegt ein konkreter Verdacht auf einen Compliance-Verstoß vor, sollte keine Zeit auf die Klärung von Zuständigkeiten verwendet werden. Die verantwortliche Stelle sowie die einzuhaltenden Kommunikationswege sollten daher bereits im Vorfeld definiert worden sein. Je nach Unternehmen bieten sich hierfür die Compliance-Abteilung, die interne Revision oder die Rechtsabteilung an.

In der Praxis ist immer wieder zu beobachten, dass die entsprechenden Verantwortlichkeiten in der Vergangenheit zwar definiert worden sind, die im Notfallplan enthaltenen Angaben aber nicht mehr den aktuellen Gegebenheiten im Unternehmen entsprechen. Um einem unnötigen Zeitverlust vorzubeugen, sind die Daten der verantwortlichen Ansprechpartner daher in regelmäßigen Abständen auf den neuesten Stand zu bringen.

5.1.3 Durchführung erster Beweissicherungsmaßnahmen

Entscheidend für eine spätere Investigation ist im ersten Schritt die Sicherung des relevanten Daten-/Beweismaterials. Es sollte der verantwort-

---

131 Die geplanten § 32d Abs. 3 und § 32e Abs. 3 BDSG erleichtern eine Einschätzung nicht.

lichen Stelle bekannt sein, welche Formen relevanter Datenspeicherung im Unternehmen vorhanden sind (Computerfestplatten, Mail- und Fileserver, CDs und DVDs, Solid-State-Speicher wie USB-Sticks und Flash-Karten, Buchhaltungs- und Vertragsmanagementsysteme etc.), wann und in welcher Form eventuelle Backup- und Lösch-Zyklen erfolgen sowie welche Prozesse bei der Datensicherung einzuhalten sind. Entscheidend für eine mögliche Gerichtsverwertbarkeit von aus elektronischen Daten gewonnenen Informationen ist die sogenannte Revisionssicherheit. Das bedeutet, dass die zu verwendenden Daten ab dem Zeitpunkt der Sicherung entweder nicht mehr veränderbar dürfen oder aber dass jegliche Veränderung der Daten zweifelsfrei nachvollziehbar sein muss.[132]

5.1.4 Entzug von Benutzerrechten

Ebenfalls bei der verantwortlichen Stelle bekannt sein sollte die Person oder Abteilung, die die Übersicht über die Zugangsberechtigungen der IT-Systeme aller Mitarbeiter hat. Ob im (Verdachts-) Fall eines Compliance-Verstoßes sofort alle Zugangsberechtigungen entzogen werden sollten, hängt vor allem davon ab, ob die *Internal Investigation* offen oder verdeckt durchgeführt wird. Grundsätzlich sollte sich das Unternehmen über das Verdunklungs- und weitere Schädigungspotential im Klaren sein, wenn entsprechende Berechtigungen nicht entzogen werden.

Besonders hervorgehoben werden soll an dieser Stelle der Fall, dass Mitarbeiter Zugriff auf das Firmennetzwerk über einen Online-Zugang haben. Da Fernzugänge Verdunklungshandlungen auch dann erlauben, wenn sich der Mitarbeiter nicht auf dem Betriebsgelände befindet, ist hier das Risiko von Verschleierungshandlungen besonders groß. Der Entzug der Benutzerrechte sollte in diesem Fall sehr zeitnah erfolgen.

Arbeitsrechtlich ist die Abkopplung von den EDV-Systemen unproblematisch, wenn die Privatnutzung der dienstlichen EDV untersagt ist. Das gilt auch bei bloß geduldeter Privatnutzung. Zweifelhaft könnte die Sperrung der EDV allenfalls bei ausdrücklich erlaubter Privatnutzung sein. Im Idealfall ist die Sperrung auch bei erlaubter Privatnutzung vorbehalten und beim Missbrauch somit zulässig. Aber auch wenn dieser Vorbehalt fehlt, bleibt die Abkopplung in Missbrauchsfällen zulässig, da sich der Mitar-

---

132 Dies gilt gleichermaßen in *Cross-Border Investigations*, die etwa durch die *SEC* oder das *DOJ* initiiert wurden. Zur lückenlosen Dokumentation siehe Ziffer 5.2.6 auf S. 61.

beiter trotz Anspruchs auf Privatnutzung selbst nicht vertragstreu verhält. Man kann ohne weiteres annehmen, dass das Unternehmen die Privatnutzung stets nur unter der Bedingung gestattet, dass der Mitarbeiter weder die Betriebstätigkeit stört noch das EDV-System gefährdet und über die Nutzung des Systems nicht versucht, missbräuchliche Handlungen zu verschleiern. Bei ausdrücklicher vertraglicher Regelung des Anspruchs auf Privatnutzung ist (meist im Wiederholungsfall) außerdem an eine verhaltensbedingte Änderungskündigung zu denken, um den Anspruch auf Privatnutzung endgültig zu beseitigen, freilich nur, wenn der Missbrauch selbst nicht bereits eine Beendigungskündigung begründet.

5.1.5 Durchführung der Internal Investigation

Schlussendlich muss die Entscheidung über die operative Durchführung der *Internal Investigation* getroffen werden. Unabhängig davon, ob eine *Internal Investigation* intern oder von eigens mandatierten externen Beratern durchgeführt wird, spielt auch hier der Zeitfaktor eine entscheidende Rolle. Sollten die Umstände es erfordern, externe Kräfte heranzuziehen, ist es häufig zielführend, sich bereits im Vorfeld einen Überblick über in Frage kommende Anbieter verschafft zu haben und diese kennenzulernen. Gegebenenfalls sollten Rahmenverträge abgeschlossen werden, damit kein zeitaufwendiger Ausschreibungsprozess durchgeführt werden muss und um zu verhindern, dass aufgrund einer erforderlichen schnellen Auftragsvergabe nicht der ideale Partner gefunden werden kann.

Eine Vergabe der *Internal Investigation* an interne Kräfte bietet dem Unternehmen Kostenvorteile. Darüber hinaus kann die bessere Kenntnis über die Struktur des Unternehmens einen Vorteil bei der *Internal Investigation* bedeuten. Wichtig bei der Vergabe von *Internal Investigations* an interne Kräfte ist es, die Unabhängigkeit der Verantwortlichen zweifelsfrei sicherzustellen. Die Geschäftsleitung kann beispielsweise ungeeignet sein, eine Untersuchung zu leiten, wenn einzelne oder sogar alle Geschäftsleiter, beispielsweise aus persönlichen Gründen, ein Motiv haben, die Untersuchung in eine bestimmte Richtung zu beeinflussen. Die Verantwortung für die *Internal Investigation* an den Aufsichtsrat oder einen Gesellschafter zu übergeben, ist möglicherweise in diesem Fall die bessere Wahl.

Andererseits kann mit der Durchführung der *Internal Investigation* durch interne Kräfte eine Ressourcenbindung verbunden sein, die betriebliche

Abläufe verzögert oder hemmt. Je nach Umfang, Ausmaß und Gegenstand des in Rede stehenden Compliance-Verstoßes sollte daher sorgfältig abgewogen werden, ob die unternehmenseigene Aufklärung einer Mandatierung externer Berater vorzuziehen ist. Die Sicherstellung und Auswertung umfangreicher Datensätze kann im Extremfall gegebenenfalls einem amerikanischen Discovery-Verfahren ähnlich sein.[133] Wie zuvor beschrieben, ist ein solches zivilprozessuales Verfahren, das der Auffindung von Beweismitteln in einem Prozess dient, nicht selten geeignet, betriebliche Abläufe erheblich zu beeinträchtigen und gegebenenfalls lahm zu legen.

Spezielle Forensik-Dienstleister, für welche die Aufklärung von Compliance-Verstößen Tagesgeschäft ist und die über Spezialisten und entsprechende Hilfsmittel verfügen, sind zudem häufig für Fachfragen die bessere Wahl und können kurzfristig größere Ressourcen stellen. Darüber hinaus können in Einzelfällen die Verschwiegenheitspflicht und der damit verbundene Beschlagnahmeschutz[134] gegenüber der Staatsanwaltschaft dem Unternehmen zum Vorteil gereichen.

Für das Unternehmen ist es vor allem aber dann notwendig, externe Dienstleister hinzuzuziehen, wenn die Unabhängigkeit der *Internal Investigation* explizit sichergestellt werden muss, etwa, wenn mit einer späteren behördlichen oder gerichtlichen Verhandlung zu rechnen ist. Im Hinblick auf einen Notfallplan für Compliance-Verstöße ist es daher vielfach sinnvoll, die externe Vergabe der *Internal Investigation* mit einem Eskalationsmodell zu verbinden. Beispielsweise könnte eine *Internal Investigation* so lange intern durchgeführt werden, wie ein bloßer Verdachtsfall vorliegt. Erhärtet sich der Verdacht, wird ein externer Dienstleister hinzugezogen, der das interne Team personell unterstützt, Spezialdienstleistungen (beispielsweise Datenrekonstruktion oder die Durchführung von

---

133 Dies muss ohne die Erhebung, Nutzung oder Verarbeitung personenbezogener Daten erfolgen, da ansonsten ein bußgeldbewehrter Verstoß gegen das BDSG vorliegt (§ 43 BDSG).

134 Bei extraterritorialen Konstellationen mit US-Bezug spielt etwa das *Attorney-Client-Privilege* eine maßgebliche Rolle. Unterliegen Dokumente dem *Attorney-Client-Privilege* (etwa Schriftverkehr zwischen Anwalt und Mandant, der über die bloße Darstellung eines Sachverhalts hinausgeht und eine juristische Bewertung enthält), sind diese dem Zugriff durch Behörden entzogen. Daher muss selbst bei Untersuchungen, die durch US-Behörden gefordert werden, die aber außerhalb der USA stattfinden, stets darauf geachtet werden, die Anforderungen des US-Rechts an das *Attorney-Client-Privilege* sicherzustellen, um sich etwaigen Herausgabe- oder Beschlagnahmeverlangen widersetzen zu können.

Interviews) bereitstellt und die Verwaltung des Beweismaterials übernimmt.

Ein weiterer gangbarer Weg mag die frühzeitige Strafanzeige sein, also die Übergabe der Ermittlung an die Staatsanwaltschaft, vor allem vor dem Hintergrund, dass die Kooperation mit den Ermittlungsbehörden in der Regel honoriert wird. Allerdings müssen die Konsequenzen dieser Option auf das Sorgfältigste abgewogen werden: Für das Unternehmen bedeutet es im Wesentlichen, dass es nicht mehr Herr des Verfahrens ist. So geht die Möglichkeit verloren, Umfang und Verwendung der Ergebnisse der Ermittlung zu steuern. Der Informationsfluss nach außen kann nicht mehr reguliert werden und es ist mit einer längerfristigen Beeinträchtigung des Geschäftsbetriebs, beispielsweise durch die Beschlagnahme von Unterlagen, zu rechnen.

Grundsätzlich muss davon abgeraten werden, auf die Durchführung einer *Internal Investigation* insgesamt zu verzichten, sofern es sich bei dem in Rede stehenden Compliance-Verstoß um einen Sachverhalt handelt, der noch andauert bzw. noch in die Gegenwart ausstrahlt.[135] Ein „Unter-den-Teppich-Kehren“ kann für das Unternehmen hier schwerwiegende Folgen haben:

1. Die Nichtaufklärung eines Compliance-Verstoßes steht der Sorgfaltspflicht und Verantwortlichkeit von Vorstand und Aufsichtsrat bzw. Geschäftsführung (§§ 93, 116 AktG, 43 GmbHG) entgegen; die Organe laufen Gefahr eines Haftungsrisikos.

2. Entsteht im Unternehmen der Eindruck, dass Verstöße nicht geahndet werden, kann dies leicht als implizite Duldung wahrgenommen werden, was unter den Mitarbeitern eine „Selbstbedienungsmentalität“ hervorrufen kann und das zukünftige Risiko artverwandter Delikte stark erhöht.

3. Kommt der Sachverhalt ans Licht der Öffentlichkeit, ist der potentielle Reputationsschaden ungleich größer, wenn das Unternehmen versucht hat, den Vorgang zu verschleiern oder wenn auch nur dieser Anschein entsteht.

---

135 Anders bei bereits in der Vergangenheit abgeschlossenen Sachverhalten, siehe Ziffer 6.1 auf S. 62.

4. Eine Aufklärung des Vorfalls wird in aller Regel nötig sein, um daraus notwendige personelle Konsequenzen zur Abwehr bzw. Begrenzung weiterer Schäden zu ziehen.
5. Ein Unternehmen, das kriminelle Handlungen eines Mitarbeiters verschleiert, läuft Gefahr, sich gegenüber dem Mitarbeiter erpressbar zu machen.

5.1.6 Kommunikation

Wenn das Unternehmen keine geeignete Kommunikationsstrategie bei Compliance-Verstößen verfolgt, sind Rufschäden kaum vermeidbar. Ist ein Compliance-Verstoß an die Öffentlichkeit geraten, muss dem Unternehmen daran liegen, dadurch hervorgerufene Reputationsschäden zu begrenzen. Kern dieser Eindämmung ist eine klare Kommunikationsstrategie. Das Unternehmen muss tunlichst vermeiden, den Eindruck zu erwecken, das Ausmaß des Schadens nicht überblicken zu können oder, noch schlimmer, zu versuchen, dieses zu verschleiern. Die Erfahrung zeigt, dass besonders diese Fälle mediale Aufmerksamkeit erregen.

Im Idealfall ist der Compliance-Verstoß komplett aufgeklärt und entsprechende Folgemaßnahmen bereits eingeleitet, bevor die Information an die Öffentlichkeit getragen wird (sofern dies vor dem Hintergrund der Wesentlichkeit des Verstoßes notwendig ist). Dringt die Information aber vorher nach außen, ist der schnelle und professionelle Umgang mit den Medien gefragt. Notwendig ist eine klare Kommunikationsstrategie, die der Pressestelle und dem Vorstand vorliegt. In der Strategie sollte auch explizit geklärt sein, wer für einen solchen Fall überhaupt mit den Medien kommuniziert, denn nichts macht einen schlechteren Eindruck als widersprüchliche Informationen aus dem gleichen Unternehmen. Für das Ausarbeiten einer solchen Strategie ist es häufig sinnvoll, Kommunikationsberater einzubinden.

Ein weiterer Aspekt, der nicht vernachlässigt werden sollte, ist die unternehmensinterne Kommunikation. Erfahrungsgemäß funktioniert die „Gerüchteküche“ in den meisten Unternehmen sehr schnell und zuverlässig. Um einer Verunsicherung der Mitarbeiter entgegenzuwirken, sollte die Unternehmensführung frühzeitig Stellung beziehen, wenn ein Compliance-Verstoß im Unternehmen offenbar wurde.

5.2 Untersuchungsmaßnahmen

Unternehmen stehen heute bei der Untersuchung von Compliance-Verstößen eine Vielzahl von technischen Mitteln zur Verfügung, die es in der Vergangenheit nicht oder nicht in diesem Maße gegeben hat. Nichtsdestotrotz wird auch heute noch die überwiegende Mehrheit der *Internal Investigations* nicht ausschließlich am Computer durchgeführt: Compliance-Verstöße und deren Untersuchung bleiben *People Business*. Im Folgenden werden die wichtigsten Instrumente der *Internal Investigation* vorgestellt und weiterhin diskutiert, ob und inwieweit sie sich für verschiedene Untersuchungsumstände, vor allem der verdeckten Untersuchung, eignen.

Neben der professionellen Durchführung der geeigneten Untersuchungsmaßnahmen zeigt die Praxis, dass der Erfolg der *Internal Investigation* eines Compliance-Verstoßes auch maßgeblich vom Ausräumen einiger operativer „Stolpersteine“ abhängt. Erfahrungsgemäß ist es wichtig, folgende Punkte geklärt zu haben:

- Stehen die Unternehmensgremien mit dem nötigen Nachdruck hinter der *Internal Investigation*?
- Ist die Koordination zwischen internen und externen Parteien gewährleistet?
- Ist der Zugang zu allen relevanten Informationen geklärt (IT, physische Dokumente, Ansprechpartner)?
- Sind die Untersuchungen mit Datenschutzbeauftragtem und Betriebsrat koordiniert?

5.2.1 Gewinnung eines detaillierten Prozessverständnisses

Prozessanalysen haben den Sinn, das „wie“ eines Compliance-Verstoßes zu klären. Die in Frage kommenden Betriebsabläufe werden aufgenommen und einer kritischen Analyse unterzogen. Oftmals werden im Rahmen einer zufälligen Stichprobe ein oder mehrere Beispielvorgänge ausgewählt und hieran der Ablauf von Anfang bis Ende nachvollzogen. Ziel der Prozessanalyse ist es, potentiell kritische Schwachstellen zu identifizieren, um Ansatzpunkte für weitere Untersuchungshandlungen zu finden sowie aus dem Prozess heraus eindeutig zuzuordnende Merkmale der Ausnutzung der Schwachstelle im Sinne eines Compliance-Verstoßes zu finden. Diese können später als Basis für maschinelle Analysen (siehe 5.2.4) dienen.

Das Durchführen von Prozessanalysen ist in den meisten Fällen, auch im Rahmen einer verdeckten *Internal Investigation,* rechtlich unproblematisch.[136] Beispielsweise kann eine solche Analyse im Rahmen der Jahresabschlussprüfung oder eines Beratungsauftrages durchgeführt werden.

Prozessanalysen sind der Ausgangspunkt der meisten Untersuchungen, unabhängig davon, ob es sich um einen Verdachtsfall oder einen erwiesenen Verstoß handelt.

5.2.2 Informationsgewinnung durch Interviews

Das Führen von Interviews spielt in den meisten *Internal Investigations* eine zentrale Rolle. Grundsätzlich sind zwei Situationen zu unterscheiden: entweder dient das Interview nur der allgemeinen Informationsgewinnung (beispielsweise im Rahmen der Prozessanalyse) oder das Interview soll der direkten Überführung eines potentiellen Täters dienen.

Letztere Konstellation stellt durch ihren Konfrontationscharakter naturgemäß besondere Anforderungen an die Interviewführenden. Der befragte Mitarbeiter ist nach dem Arbeitsrecht seinem Arbeitgeber gegenüber verpflichtet, wahrheitsgemäße Angaben zu allen seine Tätigkeit betreffenden Fragen zu machen. Er hat drohende Risiken und Schäden von seinem Arbeitgeber abzuwenden und damit zu kooperieren.[137] Sofern gegen ihn ein Strafverfahren anhängig ist, wirft dies allerdings ein schwerwiegendes Dilemma auf, zumindest sofern sich der Mitarbeiter mit seinen Angaben selbst belasten würde.[138] Professionelle Gesprächsführung ist daher entsprechend wichtig und die entsprechende Fachkenntnis und Fallkenntnis der Interviewer unerlässlich.

Um eine gerichtliche Verwertbarkeit der im Rahmen eines Interviews gewonnenen Erkenntnisse zu gewährleisten, ist sicherzustellen, dass alle Gespräche von mindestens zwei möglichst unabhängigen Interviewern geführt werden. Weiterhin sollte das Gesprächsprotokoll vom Interviewten abgezeichnet werden, um Missverständnissen vorzubeugen. Eine Aufzeichnung des Gesprächs in Video- oder Audioform ohne das explizite Einverständnis aller Gesprächsteilnehmer ist nicht zulässig.

---

136 Natürlich nur, wenn keine personenbezogenen Daten erhoben werden.
137 Für weitere Einzelheiten verweisen wir auf Ziffer 6.1 auf S. 62.
138 Im Hinblick auf strafprozessuale Implikationen verweisen wir auf die nachstehenden Ausführungen unter Ziffer 6.9 auf S. 86.

Im Falle einer *Cross-Border Investigation*, etwa für die *SEC* oder das *DOJ*, wäre eine bloße Abschrift oder Tonbandaufzeichnung ohnehin kontraproduktiv, da in diesem Fall das sogenannte *Attorney-Client-Privilege* nicht greifen würden. Hiernach muss die Korrespondenz eine juristische Bewertung seitens des Anwalts enthalten. Ist dies nicht der Fall – etwa bei einer bloßen Abschrift eines Tonbandes – ist eine solche Dokumentation nicht vom *Attorney-Client-Privilege* umfasst. Dies hat zur Folge, dass diese Dokumente nicht vor einer Beschlagnahme bzw. vor einem entsprechenden Herausgabeverlangen seitens der US-Behörden geschützt wären.

5.2.3 Untersuchung physischer Dokumente

Auch im Zeitalter des „papierlosen Büros“ werden gewisse Dokumente wie beispielsweise Rechnungen und Verträge weiterhin in Papierform vorgehalten. Bei *Internal Investigations* nehmen Papierdokumente häufig die Rolle einer Vergleichsgesamtheit ein, das heißt elektronische Daten, insbesondere Buchhaltungsdaten, werden nach bestimmten Parametern analysiert[139] und verdächtige Transaktionen anhand ihrer Ursprungsdokumente nachvollzogen. Der Vorteil von Papierdokumenten liegt darin, dass sie in den meisten Fällen wesentlich aufwändiger zu fälschen sind, insbesondere im Hinblick auf verwendetes Papier, Layout und Unterschriften.

5.2.4 Computer-Forensik, Data Recovery, Untersuchung elektronischer Dokumente und Massendatenanalysen

Die gerichtsverwertbare Sicherung (Computer-Forensik) sowie die Wiederherstellung gelöschter Daten (*Data Recovery*) spielt für die darauf folgenden Untersuchungshandlungen eine entscheidende Rolle.

Die Sicherung der Daten ist zwingend der erste Schritt in der Untersuchung elektronischer Daten und gleichzeitig eine der häufigsten Fehlerquellen, die eine spätere Verwertung der Informationen erheblich einschränken können. In der Praxis ist es leider häufig zu beobachten, dass Datensicherungen durch dafür ungeschultes Personal mit unzureichender Ausrüstung durchgeführt werden und die gerichtliche Verwertbarkeit der Daten dadurch nachhaltig eingeschränkt wird. Wichtig ist beispielsweise, dass entsprechende Datenquellen nicht durch den Zugriff bei der Daten-

---

139 Hinsichtlich weiterer Einzelheiten verweisen wir auf Ziffer 5.2.4 auf S. 58.

sicherung verändert werden, was bei nicht-schreibgeschützten Datenmedien aber passiert, so nicht spezielle Hard- und/oder Software eingesetzt werden muss.

Bereits gelöschte Daten auf einer Festplatte können in der Regel zu einem großen Prozentsatz wiederhergestellt werden, sofern die Festplatte nicht mit spezieller Software bewusst überschrieben worden ist. Auch diese Verschleierungshandlung ist aber maschinell feststellbar.

Der größte Teil der Unternehmenskorrespondenz findet heute in elektronischer Form statt. Einen weiteren Eckpfeiler bei der *Internal Investigation* von Compliance-Verstößen bildet daher die Analyse des E-Mail-Verkehrs.

Die gesicherten E-Mail-Daten oder elektronischen Dokumente werden nach definierten Parametern gefiltert (beispielsweise einer Schlagwortliste, bestimmten semantischen Konstruktionen oder auch Auffälligkeiten, die im Rahmen einer grafischen Darstellung des E-Mail-Verkehrs identifiziert werden) und anschließend individuell untersucht, um Hinweise auf bzw. Nachweise von Compliance-Verstößen zu entdecken.[140] Rechtliche Hürden bestehen jedoch dann, wenn die Mitarbeiter ihr geschäftliches E-Mail-Account auch privat nutzen dürfen.[141]

Als Massendatenanalyse bezeichnet man schließlich die maschinelle Untersuchung größerer strukturierter Datenmengen auf Basis definierter Parameter oder logischer Konstrukte. Ein Anwendungsgebiet der Massendatenanalyse ist beispielsweise das *Screening* der Buchhaltungsdaten nach auffälligen Transaktionen, Buchungstexten oder anderen Indikatoren von Compliance-Verstößen. Das Vorgehen bei einer Massendatenanalyse lässt sich für gewöhnlich in drei Schritte unterteilen:

1. Generische Abfragen: Bereits im frühen Stadium einer *Internal Investigation* kann eine Analyse der Buchhaltungsdaten nach erfahrungsgemäß im Zusammenhang mit Compliance-Verstößen auftretenden Merkmalen erfolgen. Beispiele hierfür sind Lieferantenbankverbindungen, die der Bankverbindung eines Mitarbeiters entsprechen oder auch verdächtige Änderungen in Kreditorenstammdaten. Entschei-

140 Hinsichtlich etwaiger straf- und datenschutzrechtlicher Fragen siehe Ziffer 6.8.6 auf S. 82, zum Arbeitsrecht siehe Ziffer 7.2.3 auf S. 105.

141 Zum Datenschutz vgl. Punkt 3.4.5, zur strafrechtlichen Relevanz siehe Ziffer 6.8.6 auf S. 81..

dend bei dem Einsatz von generischen Abfragen ist das richtige Augenmaß. Schon aus datenschutzrechtlichen Gründen, aber auch um die Anzahl sogenannter *False Positives*, das heißt Transaktionen oder ähnliches, die zwar durch die Abfrage als auffällig eingestuft wurden, die sich aber als legitim herausstellen, gering zu halten, sollte vom pauschalen, undifferenzierten Einsatz von Abfragen abgesehen werden.

2. Ist die Prozessanalyse abgeschlossen und wurden kritische Schwachstellen identifiziert, werden maßgeschneiderte Abfragen entwickelt, die buchhalterische Spuren eines Ausnutzens dieser unternehmensindividuellen Schwachstellen identifizieren können.

3. Auswertung der Ergebnisse: Über den Erfolg einer Massendatenanalyse entscheidet nicht nur, ob potentielle Compliance-Verstöße durch die programmierten Abfragen identifiziert werden konnten. Entscheidend ist auch, ob die Abfragen so zielgerichtet gestaltet wurden, dass *False Positives* in einem handhabbaren Rahmen bleiben oder sogar ausgeschlossen werden können. Abfragen müssen also möglichst ein exklusives Merkmal eines Compliance-Verstoßes ansprechen. Sind auffällige Transaktionen identifiziert worden, kann diesen Vorgängen dann anhand der Originaldokumentation oder im Rahmen von Interviews weiter nachgegangen werden.

5.2.5 Hintergrundrecherche

Um gewonnene Informationen richtig auszulegen, ist häufig ein breiterer Kontext notwendig. Ein Lieferant wurde beispielsweise als auffällig identifiziert, weil er in der Lage scheint, marktunüblich hohe Preise durchzusetzen. Um qualitativ bewerten zu können, ob dies auf besonderes Verhandlungsgeschick oder aber auf einen möglichen Compliance-Verstoß hindeutet, sind zusätzliche Informationen notwendig. In diesem Beispiel sei der Geschäftsführer des Lieferanten der Ehepartner eines/r Mitarbeiters/in im Einkauf, womit aus einem auffälligen ein stark verdächtiger Sachverhalt wird.

Um diese Art von Informationen belastbar, gerichtsverwertbar und vor allem im Einklang mit der bestehenden Gesetzgebung zu erlangen, greifen Unternehmen zunehmend auf professionelle Recherche-Dienstleister zurück. Recherche-Dienstleister stellen vor allem Nachforschungen in öffentlich zugänglichen Quellen wie Handelsregistern, Medien, Auskunftei-

en etc. an. Besonders im internationalen Rahmen, beispielsweise bei Nachforschungen über potentielle ausländische Geschäftspartner, erweist sich das Beauftragen externer Dienstleister als sinnvoll, da Informationen über lokale Informationsquellen häufig schon vorhanden sind und der Dienstleister Personen mit den entsprechenden Sprachkenntnissen zur Verfügung stellen kann.

Bei der Vergabe eines Nachforschungsauftrags sollte im Vorfeld mit dem Dienstleister abgesprochen werden, ob es sich um eine offene oder verdeckte Investigation handelt, da einige Register und Auskunfteien die entsprechende Partei darüber in Kenntnis setzen müssen, dass Informationen über sie eingeholt wurden.

5.2.6 Anmerkungen zu Dokumentation von Internal Investigations

Bei der Dokumentation ist vor allem die spätere mögliche Gerichtsverwertbarkeit der Informationen zu beachten. Es ist daher essentiell, die lückenlose Dokumentation aller im Rahmen der *Internal Investigation* durchgeführten Untersuchungsschritte zu garantieren. Im Einzelnen ist dabei vor allem auf folgende Punkte zu achten:

- Dokumentation der Tätigkeiten: Alle durchgeführten Handlungen sollten in Form von Arbeitspapieren dokumentiert sein. Dazu gehören auch Kopien relevanter Dokumente und Dateien bzw. Verweise auf die entsprechenden Quellen.

- Dokumentation der Entscheidungen: Relevante Entscheidungen in Bezug auf die *Internal Investigation* sollten in Form von Memoranda festgehalten werden.

- Verwertbarkeit der Erkenntnisse: Alle im Laufe der *Internal Investigation* erlangten Erkenntnisse und Beweise sollten im Hinblick auf Verwertbarkeit vor Gericht geprüft werden.

Darüber hinaus hat es sich in der Praxis stark bewährt, komplexe sachliche Zusammenhänge wie beispielsweise Beziehungsgeflechte, den Zeitstrahl oder Transaktionsketten zur Veranschaulichung grafisch aufzuarbeiten. Zu diesem Zweck werden auf dem Markt verschiedene spezielle Softwarelösungen angeboten.

6. Internal Investigations aus strafrechtlicher Sicht

Für Unternehmen stellt sich aus strafrechtlicher Sicht die grundsätzliche Frage, ob und in welchem Umfang *Internal Investigations* zielführend sind. Bei den anzustellenden Überlegungen ist danach zu differenzieren, ob lediglich interne Verdachtsmomente vorliegen oder ob bereits ein Ermittlungsverfahren eingeleitet wurde.

6.1 Interne Verdachtsmomente

Es gibt eine Vielzahl von Konstellationen, in denen interne Verdachtsmomente für Straftaten vorliegen, allerdings (noch) nicht zu befürchten ist, dass die Ermittlungsbehörden hiervon Kenntnis haben. Dies kann beispielsweise der Fall sein, wenn die Unternehmensleitung – auf welchem Weg auch immer (*Whistleblowing-Hotline*, Ombudsmann, anonyme Schreiben) – Mitteilungen über angeblich strafbares Verhalten von Mitarbeitern erhält. Häufig ergeben sich auch aus gerichtlichen Auseinandersetzungen oder behördlichen Anfragen derartige Verdachtsmomente. In einem solchen Fall bestehen zwei Möglichkeiten: Das Unternehmen kann den Vorwürfen nachgehen oder diese auf sich beruhen lassen.

Sofern es sich um Vorwürfe handelt, die gänzlich in der Vergangenheit liegen und steuerrechtlich keine Pflicht zur Richtigstellung nach § 153 Abgabenordnung (AO) vorliegt, gibt es keine strafrechtliche Pflicht, diese Fälle aufzuklären. Auch § 130 OWiG verlangt lediglich ein besseres System für die Zukunft. An den (strafrechtlichen) Verfehlungen der Vergangenheit kann in diesem Fall ohnehin nichts mehr geändert werden. Liegen die Fälle in der Vergangenheit, so wird der Berater nicht verschweigen dürfen, dass unter Umständen erst die Aufklärung ein (steuer-)strafrechtliches Problem schafft, weil die Unternehmensleitung durch § 153 AO nach durchgeführter Aufklärung gezwungen ist, den Sachverhalt den Steuerbehörden mitzuteilen, soweit dieser steuerliche Auswirkungen hat.

Strahlen Verdachtsmomente der Vergangenheit in die Gegenwart aus oder dauern sie weiterhin an, gibt es hingegen eine Vielzahl von rechtlichen Gründen, den Dingen auf den Grund zu gehen. Zum einen besteht die Gefahr einer Ordnungswidrigkeit nach § 130 OWiG. Daneben laufen die Verantwortlichen des Unternehmens nunmehr Gefahr, dass man ihnen ihr Unterlassen als Beihilfehandlung zu einer Straftat auslegt. Dar-

über hinaus liegt auch der Vorwurf eigener Straftaten (beispielsweise Steuerhinterziehung) nicht mehr fern.

Das Unternehmen wird sich daher fragen, wie man die Sachverhalte aufklären kann.

Die Kunst liegt darin, zunächst ohne unverhältnismäßigen Aufwand und ohne eine vollständige Verunsicherung aller Mitarbeiter zu verursachen, eine Klärung der Vorwürfe und ihres Umfangs herbeizuführen. Hierzu ist es erforderlich, sich ein Bild über die Geschäftsabläufe zu machen. Alsdann ist zu untersuchen, wo die Gefahr von Straftaten bei derartigen Geschäften liegen kann. Es ist darauf zu achten, dass in diesen Fällen nicht ein unsinnig weites Feld untersucht wird, sondern sogenannte *Red Flags* identifiziert werden, also eine Liste mit potentiellen Anknüpfungspunkten erstellt wird. So gelten insbesondere im Gesetz zur Bekämpfung internationaler Bestechungen (IntBestG) strafrechtlich andere Regeln als bei rein nationalen Sachverhalten. In der Praxis kommt es jedoch häufig vor, dass im Rahmen von *Internal Investigations* auch Sachverhalte untersucht werden, die strafrechtlich offenkundig – weil verjährt – ohne Befund sind. Eine genaue Identifizierung des Untersuchungsgegenstands ist daher zur Vermeidung unnötigen Aufwands und übermäßiger interner Ressourcenbindungen sinnvoll.[142]

Sind die *Red Flags* und damit der Untersuchungsgegenstand sachgemäß definiert, so bietet es sich häufig an, leitende Mitarbeiter des jeweiligen Geschäftsbereichs zu den Vorkommnissen zu befragen. In vielen Fällen findet sich eine nachvollziehbare Erklärung, warum diese oder jene Gestaltung gewählt wurde.[143] Es kann – wenn auch selten – vorkommen, dass der betroffene Mitarbeiter bereits in einem solchen Gespräch, sei es aus tatsächlicher Reue oder völliger Verkennung der Situation *(„was glauben Sie eigentlich, wie man in diesem Land sonst Geschäfte machen soll", „alle anderen bestechen doch auch"* oder *„das haben wir schon immer so gemacht"*), die strafrechtlichen Verstöße mehr oder weniger offen einräumt, was die Untersuchung erheblich verkürzt.

---

142 In Untersuchungen, die von dem *DOJ* oder der *SEC* angestoßen wurden, hat man allerdings zuweilen keine Wahl, nach deutschem Recht längst verjährte Sachverhalte untersuchen zu müssen.

143 Ein typisches Problemfeld sind beispielsweise Kommissionszahlungen an ausländische Vertriebsvermittler (*Consultants*).

Sehr viel häufiger wird man in derartigen Gesprächen jedoch mit Erklärungen bzw. Erklärungsversuchen konfrontiert. Findet sich eine nachvollziehbare und strafrechtlich unproblematische Erklärung nicht, so macht es Sinn, eine vollständige Prüfung der betroffenen Geschäftsbereiche durchzuführen. Diese Prüfung sollte zunächst auf die Ausgangsgeschäfte beschränkt sein. Im Laufe der weiteren Untersuchungen wird dann im Regelfall – jedenfalls beim Einsatz qualifizierter Prüfer – schnell deutlich werden, wo die tatsächlichen Probleme des Falles liegen und welche Themen eher Randbereiche betreffen, die gegebenenfalls nicht einmal strafbar sind. Der Prüfungsgegenstand sollte dann anhand einer Prioritätenliste stets angepasst werden. Es ist hierbei wiederum darauf zu achten, dass keine Prüfungen „ins Blaue hinein" durchgeführt werden, indem beispielsweise Nebenpunkte zu stark gewichtet werden.

Die *Internal Investigation* sollte straff geführt und von einer nicht betroffenen Abteilung des Unternehmens eng begleitet werden. Leider hat es in jüngerer Zeit auch immer wieder *Internal Investigations* gegeben, deren Durchführung zu erheblichem Ärger bei dem untersuchten Unternehmen geführt hat, weil der Eindruck entstanden ist, Zweck der Prüfung sei ganz überwiegend, möglichst viele Prüfer über einen möglichst langen Zeitraum zu beschäftigen. Auch hier ist das Unternehmen gefordert, die Ziele der Untersuchung genau zu definieren und sich – gegebenenfalls unter Hinzuziehung unabhängiger Beratung – nicht von Schreckensszenarien (veranlasst beispielsweise durch *SEC* oder *DOJ*) einschüchtern zu lassen. Selbstredend müssen bei umfangreichen Untersuchungen größere Teams eingesetzt werden. Gerade dann ist es aber von entscheidender Wichtigkeit, dass die Koordination zwischen allen Beteiligten gewährleistet ist, damit keine Reibungsverluste entstehen. Es bietet sich beispielsweise an, die Untersuchung in Schwerpunktbereiche aufzuteilen, wobei es stets einen Leiter der Untersuchungen geben sollte, der über die notwendigen Aktenkenntnisse verfügen muss, um die Arbeit der einzelnen Teammitglieder synchronisieren zu können. Die Praxis zeigt hier zudem, dass es meist zielführender ist, wenn nicht ständig neue Mitglieder zu dem Untersuchungsteam stoßen.

Nicht selten stellt sich im Rahmen der Untersuchungen heraus, dass die ursprünglichen Vorwürfe überzogen oder bei genauerer Betrachtung gar unbegründet waren. Auch in diesen Fällen bringen die *Internal Investigations* regelmäßig einen erheblichen Mehrwert, weil Schwachstellen aufgedeckt und somit Abläufe besser organisiert werden und dadurch straf-

rechtliche Risiken weiter reduziert werden können. Man optimiert somit das Compliance-System.

Auch wenn das Ergebnis „(strafrechtliche) Verfehlungen konnten nicht festgestellt werden“ aus Sicht aller Beteiligten wünschenswert ist, enden leider nicht alle Untersuchungen mit diesem Befund. In einigen Fällen kommt es vor, dass sich die ursprünglichen Verdachtsmomente erhärten oder gar weitere Anhaltspunkte für Straftaten hinzukommen. Eine rechtliche Würdigung des Sachverhalts ist erforderlich. Es ist ratsam, dass die forensischen Prüfer den Sachverhalt ohne juristische Wertung ermitteln, das heißt, Hauptzweck der *Internal Investigation* ist die Zusammenstellung und Erfassung des Sachverhalts. Die juristische Bewertung erfolgt dann durch Juristen. Die strafrechtliche Prüfung sollte durch einen strafrechtlich versierten Unternehmensanwalt erfolgen, der die Untersuchungen bereits stets aus dem Blickwinkel des Strafrechtlers[144] begleitet. In dieser Funktion kann und muss er auch an Befragungen usw. teilnehmen. Keineswegs sollte jedoch die Leitung der Untersuchung bei ihm liegen.

Sobald die Ergebnisse der *Internal Investigation* und ihre Bewertung vorliegen, ist zu entscheiden, ob und gegebenenfalls in welchem Umfang diese den Strafverfolgungsbehörden mitzuteilen sind.

6.1.1 Einschaltung der Strafverfolgungsbehörden

Die Entscheidung über die Einschaltung der Behörden wird der Unternehmensleitung nur dann abgenommen, wenn die strafrechtlichen Verfehlungen auch steuerlichen Einfluss haben, weil in diesem Fall eine Berichtigung der Steuererklärungen erfolgen muss und die Steuerbehörden wiederum gehalten sind, bei schweren Wirtschaftsstraftaten[145] den Strafverfolgungsbehörden Mitteilung zu machen.

Fehlt es an einer steuerlichen Relevanz, ist die Entscheidung schwieriger. Im Ausgangspunkt besteht eine allgemeine Pflicht, Strafanzeige zu erstatten, nicht.[146] Lediglich bei bevorstehenden oder noch andauernden schwersten Straftaten (Mord, Raub etc.) ergibt sich aus §§ 138, 139 StGB eine Anzeigepflicht. In aller Regel sind diese Katalogtaten aber nicht Ge-

144 Im Hinblick auf die ebenso wichtige Begleitung durch einen arbeitsrechtlichen Berater verweisen wir auf 6.1.
145 Vgl. § 30 Abs. 4 Nr. 5 b AO.
146 Allg. Meinung, vgl. nur *Fischer,* StGB, 57. Aufl., 2010, § 138 Rn. 2.

genstand von *Internal Investigations*. Allerdings kann sich aus dem Untreuetatbestand (§ 266 StGB) die Pflicht ergeben, zivilrechtliche Ansprüche geltend zu machen, wenn die Unterlassung der Geltendmachung ihrerseits eine pflichtwidrige Vermögensschädigung im Sinne des § 266 StGB darstellen würde.

Im Rahmen der zivilrechtlichen Geltendmachung kann auch eine Strafanzeige geboten sein, weil denkbar ist, dass die Einschaltung der Strafverfolgungsbehörden die Durchsetzung zivilrechtlicher Ansprüche fördern kann, beispielsweise durch Akteneinsichtnahme nach Abschluss der staatsanwaltlichen Ermittlungen. Die Vermögensfürsorgepflicht zwingt den Vorstand eines Unternehmens, bzw. bei Ansprüchen gegen den Vorstand den Aufsichtsrat grundsätzlich dazu, entstandene Schäden möglichst umfassend zu kompensieren.[147] Es ist aber zu berücksichtigen, dass Vorstand und Aufsichtsrat einen weiten unternehmerischen Handlungsspielraum haben und nur eindeutig unvertretbare Handlungen den Anwendungsbereich des Untreuetatbestands eröffnen.[148] § 266 StGB schließt daher nicht aus, dass der Vorstand aus „übergeordneten Gründen“ von der Geltendmachung von Schadensersatzansprüchen absieht.[149] Entscheidend ist, dass der Vorstand sachgerecht und sorgfältig abwägt, welche Vor- und Nachteile mit der Geltendmachung von Schadensersatzansprüchen bzw. der Erstattung von Strafanzeigen verbunden sind.[150] Denkbare Gesichtspunkte sind hierbei unter anderem verbleibende Prozessrisiken, Kosten- und Bonitätsrisiken oder die Auswirkung auf andere Verfahren.

Als weiterer Gesichtspunkt bei der Abwägung der Frage, ob die Strafverfolgungsbehörden informiert werden sollen, wird auch stets zu berücksichtigen sein, wie dies durch die Öffentlichkeit aufgenommen wird. Zwar geht mit strafrechtlichen Ermittlungen zumeist eine Welle der öffentlichen Empörung einher, auf der anderen Seite zeigen zahlreiche Beispiele aber, dass eine rein interne Behandlung einer solchen Angelegenheit, auch wenn sie rechtlich zulässig und sachlich geboten war, im Nachhinein – wenn die Vorwürfe doch publik werden oder die Staatsanwaltschaft auf andere Weise Kenntnis erlangt – zu dem (in der Sache meist unzutreffenden) Vorwurf der Vertuschung führt.

---

147 BGHZ 135, 245, 253 (ARAG/Garmenbeck-Entscheidung).
148 BGHSt 46, 30; BGHSt 47, 187; BGHSt 47, 148; BGH NStZ 2006, 214.
149 *Hüffer*, AktG, 6. Aufl., 2010, § 93 Rn. 9.
150 Vgl. auch § 93 AktG.

In der Beratungspraxis lässt sich häufig feststellen, dass auf Seiten der Unternehmen eine große Zurückhaltung bei der Einschaltung von Strafverfolgungsbehörden besteht, weil deren Reaktion zumeist nicht verlässlich vorausgesagt werden kann. Allerdings lassen sich einige Grundprinzipien herausarbeiten, die die Entscheidung erleichtern:

6.1.2 Kooperation und Offenheit

In Fällen, in denen die Verfolgungsbehörden durch eigene Ermittlungen keine Anhaltspunkte für Straftaten haben, wird die freiwillige Herausgabe der Unterlagen von den Staatsanwaltschaften in aller Regel in hohem Maße honoriert. Während Staatsanwälte, die naturgemäß berufsbedingt misstrauisch sind, bei bereits bestehenden Ermittlungsmaßnahmen häufig eine gewisse Skepsis bezüglich der Kooperationsbereitschaft haben, ist in aller Regel davon auszugehen, dass die wirklich freiwillige Kooperation von den Staatsanwaltschaften als überraschend empfunden und als ernsthaftes Bemühen gewertet wird, die Verfehlungen auch tatsächlich abzustellen.

In vielen Fällen kann daher durch diese offene Herangehensweise jedenfalls eine öffentlichkeitswirksame Durchsuchung verhindert werden und die Verfahren können zügiger und geräuschloser zu einem für das Unternehmen befriedigenden Abschluss gebracht werden. Hier gilt jedoch die absolut zwingende Regel, dass man bei einer solchen Kooperation keine „halben Sachen“ machen kann. Nur wenn die zuständige Staatsanwaltschaft das Gefühl hat, dass sie den Vertretern des Unternehmens trauen kann, wird sie sich mit der Vorlage von Unterlagen durch das Unternehmen zufrieden geben. Wer nunmehr dieses Vertrauen missbraucht und nur selektierte Unterlagen überreicht, der läuft Gefahr, dass die Stimmung sehr schnell „kippt“ und die Staatsanwaltschaft die Sachverhaltsermittlung in die eigenen Hände nimmt.

Ganz generell ist es erforderlich, dass über den strafrechtlichen Unternehmensanwalt ein enger und offener Kontakt mit den Ermittlungsbehörden gepflegt wird, damit die erforderlichen Maßnahmen schnell und praktikabel umgesetzt werden können. Gerade bei zeitlichem Verzug kommt bei den Staatsanwaltschaften schnell der Verdacht auf, dass nicht ganz mit „offenen Karten“ gespielt wird. Für den Staatsanwalt ist ein zentraler Ansprechpartner, der insbesondere auch Entscheidungen treffen kann, daher von großer Bedeutung.

6.1.3 Strafprozessuale Probleme

Immer wieder können im Rahmen einer *Internal Investigation* auch strafprozessuale Probleme auftreten. So führt die Kooperation häufig dazu, dass die Ermittlungsbehörden mit ihren Wünschen über das hinausgehen, was sie mit ihren eigenen strafprozessualen Mitteln erreichen können. Hier wäre es äußerst kontraproduktiv, über jede Kleinigkeit einen prozessualen Diskurs mit der Staatsanwaltschaft anzustrengen. Allerdings sollte der Unternehmensanwalt dafür Sorge tragen, dass die Wünsche nicht zu weit gehen. An dieser Stelle ist mit einem weit verbreiteten Missverständnis unter strafrechtlich unerfahrenen Beratern aufzuräumen: Es ist keineswegs so, dass nur der Verzicht auf alle prozessualen Rechte und das Vorbringen berechtigter materieller Verteidigungsargumente sowie die vollständige Aufklärung des Falles und absolute Unterwerfung unter die Forderungen der Staatsanwaltschaft Kooperation bedeutet. Im Ergebnis soll Kooperation nicht heißen, dass auf sämtliche strafprozessualen Rechte im Vorfeld verzichtet wird. In diesem Zusammenhang die richtige Balance zu finden ist eine Herausforderung.

Ein weiteres Problem tritt immer dann auf, wenn die Staatsanwaltschaft die Herausgabe von Unterlagen begehrt, die das Unternehmen freiwillig (beispielsweise aus datenschutzrechtlichen Gründen) nicht herausgeben darf. Hier wird man in der Regel so verfahren, dass der Staatsanwaltschaft die Problematik dargelegt wird. Hält der zuständige Staatsanwalt die Unterlagen gleichwohl für unverzichtbar, kann er sich einen Beschlagnahmebeschluss beschaffen und das Unternehmen dann die Durchsuchung und Beschlagnahme durch freiwillige Herausgabe abwenden. Auch hier lassen sich durch eine offene und konstruktive Kooperation zahlreiche Probleme einvernehmlich lösen.

6.1.4 Keine ungefilterte Informationsweitergabe

Von einer Vorgehensweise, die – teilweise als Alternative zur eigenen Aufklärung – empfohlen wird, muss an dieser Stelle dringend abgeraten werden. Staatsanwaltschaften reagieren auf die Idee, ihnen ungefiltert und/oder ungeordnet irgendwelche unaufbereiteten Aktenberge zur Verfügung zu stellen, weil man interne Verdachtsmomente für mögliche Straftaten hat, meist mehr verärgert als erfreut. Staatsanwaltschaften sind keine Prüfgesellschaften und wollen in aller Regel auch nicht als solche missbraucht werden.

6.2 Bereits laufende Ermittlungen

Anders als bei lediglich internen Verdachtsmomenten stellt sich die Sachlage dar, wenn die Staatsanwaltschaft bereits aufgrund sonstiger Quellen Erkenntnisse von Straftaten hat und bereits ein strafrechtliches Ermittlungsverfahren eingeleitet wurde oder mit der Einleitung eines Ermittlungsverfahrens erkennbar zu rechnen ist. In diesem Fall stellt sich für das Unternehmen die Frage, inwieweit *Internal Investigations* überhaupt Sinn machen. Hat die Staatsanwaltschaft das Unternehmen bereits unter neuerdings immer wieder zu beobachtender medialer Begleitung durchsucht oder gar unter dem Motto „*Manchmal hilft ein Haftbefehl*“[151] Mitarbeiter zur Beförderung der Aufklärungsbereitschaft vorläufig festgenommen, dann wird das Unternehmen den zu beschreitenden Weg sorgfältig abzuwägen haben.

Kooperation, die grundsätzlich (fast) immer das beste Mittel der Verteidigung aus Sicht des Unternehmens darstellt, kann sich auch darauf beschränken, Unterlagen freiwillig herauszugeben und auf das Einlegen bestimmter Rechtsmittel zu verzichten. Selbstredend bleibt es jedem Unternehmen und jedem Beschuldigten in einem Strafverfahren unbenommen, sich gegen die Vorwürfe sachlich und mit den zur Verfügung stehenden prozessualen Mitteln zu verteidigen. Auch bleibt es dem Unternehmen weiterhin unbenommen, eine gemeinsame Verteidigung der Beschuldigten zu organisieren und die Verteidiger zu bezahlen, wenn es sich um Vorwürfe handelt, die die Mitarbeiter nicht eigennützig zu Lasten des Unternehmens begangen haben. Demgegenüber kommt es in der Praxis mittlerweile sogar vor, dass Staatsanwaltschaften einem Unternehmen bereits dann mangelnde Kooperationsbereitschaft vorwerfen, wenn das Unternehmen Mitarbeitern, die als Zeugen vernommen werden sollen, einen Zeugenbeistand zur Seite stellt oder wenn das Unternehmen sich weigert, Unterlagen herauszugeben, die mit dem Tatvorwurf nicht im Zusammenhang stehen. Solches Ansinnen muss seitens des Unternehmensanwalts stets entschieden zurückgewiesen werden.

Welche Vorgehensweise für das Unternehmen richtig ist, hängt wieder sehr stark von den Umständen des Einzelfalles ab:

---

151 Süddeutsche Zeitung vom 26. Mai 2010 als Überschrift eines Beitrags über die Arbeit der Staatsanwaltschaft München.

Relativ einfach ist die Beurteilung der Vorgehensweise dann, wenn sich die staatsanwaltschaftlichen Ermittlungen gegen einzelne Personen richten, die dem Unternehmen geschadet haben. In diesem Fall kommt eine Unternehmensverteidigung in aller Regel nicht in Betracht. Auch darf dem Beschuldigten hier regelmäßig kein Verteidiger gestellt werden. Das Unternehmen kann nun entscheiden, ob zusätzliche interne Untersuchungen des Falles Sinn machen, weil diese gegebenenfalls bei der Durchsetzung zivilrechtlicher Ansprüche helfen können. Zudem geht hier von internen Ermittlungen auch das starke Signal aus, dass das Unternehmen derartiges Fehlverhalten unter keinen Umständen duldet und stattdessen mit aller Härte hiergegen vorgeht. Zudem können durch *Internal Investigations* – wie gesagt – die Schwachstellen des Compliance-Systems identifiziert und für die Zukunft abgestellt werden. Die Gefahren sind hierbei überschaubar, weil solche Verstöße nur von einem überschaubaren Kreis von Mitarbeitern begangen werden und ein Übergreifen auf die Leitungsorgane oder gar ganze Unternehmensbereiche zumeist ausgeschlossen werden kann.

Ganz anders stellt sich die Sachlage bei strafrechtlichen Ermittlungen gegen eine Vielzahl von Mitarbeitern dar, die im (vermeintlichen) Unternehmensinteresse gehandelt haben. Klassisches Beispiel sind hier Bestechungsvorwürfe bei ausländischen Projekten. Es ist schlicht eine Tatsache, dass die heutige strenge Sichtweise in diesem Bereich noch vor wenigen Jahren nicht im Ansatz in den Köpfen der Verantwortlichen verankert war. Kein Wunder, wenn man bedenkt, dass vor 1999 im Ausland erbrachte sogenannte „nützliche Aufwendungen“ (sprich: Bestechungsgelder) steuerlich absetzbar waren.

In diesem Bereich trifft nun das heutige Unrechtsbewusstsein auf Sachverhalte, die wegen des späten Verjährungsbeginns der Korruptionsdelikte[152] teilweise fünf bis zehn Jahre zurückliegen. Häufig führt dies dazu, dass in die möglicherweise strafbaren Handlungen zahlreiche Mitarbeiter und sogar die aktuellen Leitungsorgane eines Unternehmens eingebunden waren.

Die Unternehmensleitung steht in einem solchen Fall vor dem Problem, dass die *Internal Investigation* mit ganz erheblichen Risiken einhergeht. Erfahrungsgemäß sind derartige Sachverhalte für Staatsanwaltschaften nur sehr schwer aufzuklären. Häufig ist es für die Ermittlungsbehörden

---

152 BGHSt 52, 300, 303.

unmöglich zu ermitteln, wer tatsächlich (End-)Empfänger der Bestechungsgelder war, wenn die Beschuldigten von ihrem Schweigerecht Gebrauch machen. Auch werden sich die Staatsanwaltschaften heute noch in vielen Ländern schwertun, wenn sie im Wege der Rechtshilfe zu ermitteln versuchen.

Der einfache Hinweis, der im Übrigen empirisch nicht belegt ist, die volle eigene Aufklärung würde sich später bei der Höhe der Unternehmensgeldbuße positiv auswirken, ist nicht unbedingt zielführend. Bei unterbliebener eigener Aufklärung sind häufig derartige Straftaten überhaupt nicht nachzuweisen. Hiermit soll nun in keiner Weise einer „Vogel-Strauß-Politik" das Wort geredet werden. Der Hinweis auf mögliche Risiken, die in dem konkreten Fall darin bestehen, die Tatsachen für eine (eigene) Verurteilung selbst zu liefern und das Ende der *Internal Investigation* nur als „Externer" zu erleben, gehört jedoch ebenfalls zu einer ausgewogenen anwaltlichen Beratung.

Im Ergebnis sind beim Verdacht „systemischer" Straftaten, die in der Vergangenheit begangen wurden, alle Gesichtspunkte, die für und gegen *Internal Investigations* und eine bedingungslose Kooperation sprechen, gegeneinander abzuwägen und am Ende diejenige Entscheidung zu treffen, die dem Wohle des Unternehmens am meisten dient. Wegen des beschriebenen Interessenkonflikts kann es im Übrigen Sinn machen, wenn nicht der Vorstand – soweit er an den vermeintlichen Taten beteiligt sein könnte –, sondern der Aufsichtsrat letztlich über die Durchführung einer *Internal Investigation* entscheidet und diese gegebenenfalls beauftragt. Allerdings sind hierbei die gesellschaftsrechtlichen Voraussetzungen zu beachten.[153] Auch die mandatierten Ermittler entgehen auf diese Weise einem Interessenkonflikt, der sich daraus ergibt, dass man das Verhalten des Mandanten zu untersuchen hat. Selbst wenn der Vorstand an den Straftaten nicht beteiligt war und von diesen keine Kenntnis hatte, zeigen zahlreiche prominente Beispiele, dass mit jeder aufgedeckten Verfehlung durch einzelne Mitarbeiter die Frage nach der Erfüllung der Aufsichtspflicht in der Vergangenheit immer drängender wird.

Kommt man nach gründlicher Abwägung zu dem Schluss, dass das beste Vorgehen eine Unternehmensverteidigung im klassischen Sinne ist, dann ist es dem Unternehmen natürlich unbenommen, sich auch gegen Korruptionsvorwürfe mit allen prozessual zulässigen Mitteln zu verteidigen.

---

153 Siehe bereits Ziffer 3.4.1 auf S. 31.

In diesem Fall kann eine *Internal Investigation* Sinn machen, um entlastende Gesichtspunkte zu ermitteln.

Um es deutlich zu sagen: Eine strafrechtliche Verpflichtung zur Aufklärung eigener Straftaten existiert nicht.

6.3 Kronzeugenregelung nach § 46b StGB

Trotz vielfältiger Kritik[154] ist am 1. September 2009 die Neuregelung der Strafzumessung bei Aufklärungs- und Präventionshilfe durch den Beschuldigten, die sogenannte „Kronzeugenregelung", in Kraft getreten.[155] Die Aufklärung des Kronzeugen muss sich auf eine der Katalogtaten des § 100a Abs. 2 der Strafprozessordnung (StPO) beziehen. Hierunter fallen auch Straftaten gegen den Wettbewerb und Bestechungsdelikte. Mit anderen Worten: Wer selbst eine besonders schwere Bestechung im geschäftlichen Verkehr begangen hat, kann eine Strafmilderung dadurch erreichen, dass er freiwillig sein Wissen über eine besonders schwere Bestechung im geschäftlichen Verkehr eines anderen den Strafverfolgungsbehörden offenbart. Hinzuweisen ist darauf, dass sich die Aufklärungshilfe nicht auf diejenige Tat beziehen muss, an der der Täter selbst beteiligt war, sondern auch andere Taten Dritter betreffen kann.

Im Ergebnis bedeutet diese Regelung eine ganz erhebliche Erhöhung des Risikos, dass Mitarbeiter eines Unternehmens gegenüber den Ermittlungsbehörden ihr Wissen offenbaren, um selbst möglichst milde (oder gar nicht) bestraft zu werden. War es bereits vor der Einführung des § 46b StGB gängige Praxis, dass Mitarbeiter – meist nach Festnahme – versucht haben, durch eine „Lebensbeichte", die die Belastung von Kollegen umfasste, eine mildere Bestrafung zu erlangen, so ist dies nun eine gesetzlich normierte und daher stets zu berücksichtigende Verteidigungsstrategie.

Es kommt hinzu, dass Mitarbeiter, die in Ländern und Branchen eingesetzt wurden, in denen eine hohe Korruptionsanfälligkeit besteht, früher zumeist mit der Unterstützung durch ihr Unternehmen rechnen konnten, wenn es zu Verdachtsfällen kam. Derzeit wird der Mitarbeiter hingegen eher damit rechnen müssen, dass sich das Unternehmen bereits bei Ver-

---

154 Vgl. nur *Salditt,* StV 2009, 375 ff.; *König,* NJW 2009, 2481 ff.

155 Zu den Eigenschaften des Aufklärungsgehilfen bzw. Kronzeugen siehe § 46b StGB

dachtsfällen von ihm distanziert, was die Bereitschaft der Mitarbeiter, gegebenenfalls durch Offenbarung der eigenen Kenntnisse eine milde Behandlung durch die Strafverfolgungsbehörden zu erlangen, deutlich erhöht.

Problematisch ist an der Kronzeugenregelung, dass sie nicht selten die Bereitschaft weckt, Dritte übermäßig oder gar falsch zu belasten, weil sich der Beschuldigte hierdurch einen Vorteil für sich selbst verspricht.

Im Zusammenhang mit *Internal Investigations* ist die neue Kronzeugenregelung in dreifacher Hinsicht relevant:

1. Weil durch die Regelung ein Anreiz geschaffen wird, sich den Strafverfolgungsbehörden zu offenbaren, steigt das Risiko weiter, dass Straftaten, die in einem (falsch verstandenen) Unternehmensinteresse begangen wurden, aufgeklärt werden, sodass ein „Unter-den-Teppich-Kehren“ immer riskanter wird.

2. Durch *Internal Investigations* kann jedoch auch dem Risiko entgegengewirkt werden, dass straffällige Mitarbeiter andere zu Unrecht belasten, um sich selbst zu entlasten. Oftmals können falsche Angaben durch die Ermittlungen widerlegt werden.

3. Von hohem Interesse ist letztlich, dass in § 46b StGB ganz klar die Intention des Gesetzgebers zum Ausdruck kommt, dass sich Aufklärungsarbeit lohnen muss. Entdeckt und offenbart ein Unternehmen selbst strafbare Handlungen aus der Vergangenheit, so werden sich die handelnden Personen auf § 46b StGB berufen können, wenn sie selbst diese Taten aufklären und den Verfolgungsbehörden offenbaren. Auch das Unternehmen selbst wird sich (beispielsweise im Rahmen einer Geldbuße nach § 30 OWiG) auf den hinter § 46b StGB stehenden Gedanken berufen können, wenn es aktive Aufklärungshilfe betreibt.

6.4 Strafrechtliche Verstöße als Anlass für Internal Investigations

Aus strafrechtlicher Sicht wird man bei typischen rechtlichen Verfehlungen zunächst an Korruptionsstraftaten denken. Allerdings ist dieser Begriff unscharf. Das deutsche Strafrecht kennt den Begriff der Korruptionsdelikte nicht. Gemeint sind hiermit die Bestechung und die Bestechlichkeit im geschäftlichen Verkehr (§§ 299 ff. StGB), die Vorteilsgewährung bzw. Bestechung von Amtsträgern (§§ 331 ff. StGB) sowie

Benachteiligung oder Begünstigung der Mitglieder von Betriebsräten oder vergleichbarer Gremien (§ 119 I Nr. 3 BetrVG). Darüber hinaus können jedoch eine Reihe von weiteren Straftaten Anlass für *Internal Investigations* sein.[156]

6.4.1 Bestechlichkeit und Bestechung im geschäftlichen Verkehr – § 299 StGB

Durch das Gesetz zur Bekämpfung von Korruption vom 13. August 1997[157] wurde § 299 StGB in das Strafgesetzbuch eingefügt. § 299 StGB stellt die Bestechung und Bestechlichkeit im geschäftlichen Verkehr unter Strafe. Die Norm entspricht im Wesentlichen dem aufgehobenen § 12 UWG („Schmieren"), dessen praktische Bedeutung allerdings sehr gering war. Gemäß § 299 Abs. 1 StGB macht sich strafbar, wer als Angestellter oder Beauftragter eines geschäftlichen Betriebs im geschäftlichen Verkehr einen Vorteil für sich oder einen Dritten als Gegenleistung für eine unlautere Bevorzugung fordert, annimmt oder sich versprechen lässt. § 299 Abs. 2 StGB regelt spiegelbildlich das Anbieten, Gewähren und Versprechen eines derartigen Vorteils.

Geschützt wird durch § 299 StGB, der in der Praxis in den letzten Jahren zunehmend an Bedeutung gewonnen hat, der freie Wettbewerb.[158] Vereinfacht ausgedrückt soll verhindert werden, dass wirtschaftliche Entscheidungen nicht anhand objektiver Kriterien erfolgen, sondern aufgrund persönlicher Vorteile gefällt werden. Vorteil ist hierbei alles, worauf der andere keinen durchsetzbaren Anspruch hat.[159] Eine Einschränkung erfolgt durch die Rechtsprechung bei sozialadäquaten Vorteilen, wobei die Beurteilung eine Gesamtbetrachtung des betroffenen Geschäftsbereichs, der Stellung und der Lebensumstände der Beteiligten berücksichtigt werden muss. Der teilweise diskutierte Ansatz, in bestimmten Branchen stehe bereits die Üblichkeit der Bestechung der Unlauterkeit entgegen, findet bei Strafverfolgungsbehörden (zu Recht) kein Gehör.

Erfasst werden sowohl materielle als auch immaterielle Vorteile. Die Begriffe geschäftlicher Betrieb und geschäftlicher Verkehr sind hierbei weit auszulegen. Erfasst werden allerdings nur Vorteilsgewährungen, die auf

---

156 Siehe nachstehend Ziffer 6.4.4 auf S. 78.
157 BGBl. I 2038.
158 *Fischer*, StGB, 57. Aufl., 2010, § 299 Rn. 2.
159 BGH wistra 2001, 260 ff.

einer (vorherigen) Unrechtsvereinbarung beruhen. Nachträgliche Belohnungen fallen nicht unter § 299 StGB, können aber – wenn das Geld aus der Firmenkasse stammt – den Tatbestand der Untreue (§ 266 StGB) begründen. Ebenfalls nicht erfasst sind Zahlungen, die im Zusammenhang mit der Abwicklung von Aufträgen stehen. Als Beispiel seien nur Fälle genannt, in denen der Bauherrenvertreter sich dafür vergüten lässt, dass er bei der Bauüberwachung keinen Ärger verursacht. Solche Konstellationen sind – weil es am Wettbewerb fehlt – von § 299 StGB nicht erfasst.

Von besonderer Bedeutung ist noch § 299 Abs. 3 StGB. Hiernach sind auch Schmiergeldzahlungen im Wettbewerb strafbar, wenn Zahlungen an einen Angestellten oder Beauftragten eines geschäftlichen Betriebes (im Ausland) geleistet werden, damit dieser den Leistenden beim Bezug von Waren oder Dienstleistungen in unlauterer Weise bevorzugt. Erst seit Einfügung des Absatzes 3 im Jahr 2002 schützt § 299 StGB auch den ausländischen Wettbewerb.[160]

6.4.2 Vorteilsannahme und -gewährung, Bestechung und Bestechlichkeit – §§ 331 ff. StGB, IntBestG

Bei (Korruptions-)Straftaten in Deutschland richtet sich die Strafbarkeit nach §§ 331 ff. StGB. Nach den §§ 331 ff. StGB ist bereits derjenige strafbar, der einem Amtsträger für eine Diensthandlung irgendeinen Vorteil gewährt; die Diensthandlung muss hierbei nicht pflichtwidrig sein (Vorteilsgewährung). Ist die Diensthandlung pflichtwidrig, so liegt eine Bestechung vor. Auch bei der Amtsträgerkorruption sind Drittvorteile erfasst. Ausgenommen sind auch hier sozialadäquate Vorteile, wie beispielsweise normale Bewirtung anlässlich einer Besprechung, wobei die Sozialadäquanz enger zu fassen ist als bei § 299 StGB.[161] Von den §§ 331 ff. StGB sind Vorteile erfasst, die vor, nach und während der Diensthandlung gewährt werden.

Amtsträger im Sinne des Gesetzes sind nach § 11 Abs. 1 Nr. 2 StGB vor allem Beamte oder Richter bzw. Personen, die in einem öffentlich-rechtlichen Amtsverhältnis stehen oder sonst Aufgaben der öffentlichen Verwaltung wahrnehmen. Nicht erfasst von § 11 Abs. 1 Nr. 2 StGB werden ausländische Amtsträger. Die Gewährung eines Vorteils an einen ausländischen Amtsträger ist nur dann strafbar, wenn ein Fall des § 334 StGB

160 BGHSt 52, 323, 329.
161 BGHSt 23, 228.

i.V.m. §§ 13 IntBestG gegeben ist. Über § 3 IntBestG[162] findet eine Erweiterung der Strafbarkeit für Taten, die ein Deutscher im Ausland begeht, statt. Die Regelung des IntBestG setzt jedoch (anders als bei deutschen Amtsträgern) voraus, dass ein Vorteil für eine künftige pflichtwidrige Diensthandlung gewährt wird, um sich oder einem Dritten einen Auftrag oder einen unbilligen Vorteil im internationalen Geschäftsverkehr zu verschaffen.[163]

Somit ist eine Strafbarkeit nach dem IntBestG an deutlich höhere Voraussetzungen geknüpft, als dies bei der Vorteilsgewährung an deutsche Amtsträger der Fall ist. Strafbar sind im Ausland nur Bestechungen (§ 334 StGB), die im internationalen geschäftlichen Verkehr geschehen, um einen unbilligen Vorteil zu erlangen. Die Vorteilsgewährung (§ 333 StGB) im Ausland ist hingegen nicht strafbar. Zahlungen an ausländische Amtsträger, die dazu dienen, Geschäftsabläufe zu beschleunigen, sind daher beispielsweise nach deutschem Recht nicht strafbar.

Dies wird sowohl von Staatsanwaltschaften als auch von internen Ermittlern häufig übersehen, was schnell zu einer Kriminalisierung von Handlungen führen kann, die jedenfalls nach deutschem Recht von der Strafbarkeit gerade ausgenommen sind. Hier ist es von besonderer Wichtigkeit, bei internationalen Sachverhalten stets die tatsächlichen straf- und steuerrechtlichen Rahmenbedingungen genau zu definieren, schon um „Panikmache“ zu verhindern. Es sei an dieser Stelle angemerkt, dass gerade dieser Punkt die staatsanwaltlichen Ermittler in der Praxis vor die größten Probleme stellt, weshalb gerade hier häufig der Versuch unternommen wird, den Unternehmen eine geständige Kooperation schmackhaft zu machen. Dies geschieht zumeist durch das Aufzeichnen von Drohszenarien, die eintreten sollen, wenn man den Sachverhalt (im Wege der Rechtshilfe) selbst ausermitteln würde. Hier kann es sich für das Unternehmen durchaus lohnen, die Risiken und Vorteile einer solchen Kooperation besonnen gegeneinander abzuwägen.

---

162 „Das deutsche Strafrecht gilt, unabhängig vom Recht des Tatorts, für folgende Taten, die von einem Deutschen im Ausland begangen werden: 1. Bestechung ausländischer Amtsträger im Zusammenhang mit internationalem geschäftlichen Verkehr (§§ 334 bis 336 StGB i.V.m § 1 IntBestG).“

163 *Tinkl*, wistra 2006, 126, 129.

6.4.3 § 266 StGB – Untreue („Schwarze Kassen")

Bei einer solchen Abwägung wird man allerdings auch zu berücksichtigen haben, dass wegen der oben genannten Beweisschwierigkeiten bei Korruptionsdelikten im Ausland zunehmend § 266 StGB (Untreue) als Auffangtatbestand fungiert. Zwar liegt nach dem Bundesgerichtshof dann keine Untreue vor, wenn eine Korruptionszahlung durch einen entsprechenden Vorteil kompensiert wird.[164] Bei der Bestimmung, welche Vorteile kompensationsfähig sind, ist die Rechtsprechung in den letzten Jahren freilich immer zurückhaltender gewesen.[165]

Noch deutlicher geht die Rechtsprechung mit Fällen um, in denen zunächst Gelder aus dem Buchungskreis der Gesellschaft transferiert werden, um hiermit später Zahlungen zu leisten, die in den Büchern nicht auftauchen sollen („Schwarze Kassen"). Bereits in der Entziehung der Gelder zur späteren (unkontrollierten) Verwendung soll hier der Vermögensschaden liegen.[166] Zudem soll eine (hypothetische) Einwilligung des Geschäftsherrn nicht in Betracht kommen.[167]

Allerdings hat das Bundesverfassungsgericht vor kurzem der restriktiven Rechtsprechung bei der Untreue Grenzen gesetzt und die Verurteilung von Vorstandsmitgliedern einer Hypothekenbank wegen Untreue aufgrund der Vergabe eines unzureichend besicherten Kredits aufgehoben. Zwar sei für einen Vermögensschaden auch eine bloße Vermögensgefährdung ausreichend, wie vom erstinstanzlichen Gericht angenommen, diese muss im Einzelfall jedoch konkret nachvollziehbar sein, woran es vorliegend fehlte. Eine Einschränkung der Strafbarkeit wegen Untreue durch die Bildung „Schwarzer Kassen" hat das Bundesverfassungsgericht hingegen nicht vorgenommen.[168]

Auf den Verwendungszweck der Mittel kommt es nicht an. Es ist strafrechtlich ohne Belang, ob der Täter vorhat, im (scheinbaren) Unternehmensinteresse zu handeln oder das Geld einsetzen will, um Aufträge für das Unternehmen zu erlangen. Es macht allenfalls bei der Strafzumes-

---

164 BGH NJW 1974, 1234.
165 Vgl. nur BGHSt 51, 100 ff.
166 Siehe BGH-Urteil vom August 2008, Ziffer 1. auf S. 11.
167 BGHSt 52, 323, 335.
168 Vgl. Pressemitteilung des Bundesverfassungsgerichts vom 11. August 2010, abrufbar unter http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-060.html.

sung einen (dann aber erheblichen) Unterschied, für welche Zwecke der Täter die Mittel verwendet hat.

Auch wenn man nicht davon sprechen kann, dass die Anlegung schwarzer Kassen bei Geschäften im Ausland allgemein üblich ist, fallen im Rahmen von staatsanwaltlichen Ermittlungen und *Internal Investigations* immer wieder Sachverhalte auf, in denen ausländische Gesellschaften (meist mit Geschäftssitz in Drittländern) nicht näher definierte Leistungen in Rechnung stellen, die die Gesellschaft dann ohne weitere Prüfung begleicht. Früher zeichneten sich derartige Leistungen durch schlechte Dokumentation, unzureichende oder fehlende vertragliche Grundlagen, fehlende Leistungsbeschreibungen und hohe Summen aus. All diese Merkmale dienen mittlerweile selbstredend als *Red Flags* bei einer *Internal Investigation*. Es darf in diesem Zusammenhang aber nicht übersehen werden, dass im Rahmen der vielfältigen Compliance-Maßnahmen mittlerweile die genannten äußeren Anzeichen nur noch selten auftreten, weshalb sich eine Prüfung zumeist nicht allein auf die (mittlerweile fast immer „saubere“) Dokumentation stützen kann.

6.4.4 Weitere Verstöße

Nur kurz werden nachstehend weitere Straftatbestände genannt, die häufig Gegenstand von *Internal Investigations* sind.

Hier ist zunächst § 263 StGB (Betrug) zu nennen. Einem Unternehmen kann ein großer wirtschaftlicher Schaden durch Betrügereien entstehen. Betrugshandlungen durch Mitarbeiter eines Unternehmens sind nicht selten. So treten immer wieder Fälle auf, bei denen über Scheinrechnungen Gelder aus dem Unternehmen geschleust werden, die sich alsdann der Rechnungssteller und Mitarbeiter des Unternehmens teilen. Hier sind *Internal Investigations* in mehrfacher Hinsicht weiterführend: Zum einen dienen sie der Beschleunigung der Aufklärung und der Durchsetzung zivilrechtlicher Ansprüche. Zum anderen werden auf diese Weise auch Schwachstellen aufgedeckt, durch deren Beseitigung viel Geld gespart werden kann.

Gegenstand von *Internal Investigations* können auch Verstöße gegen § 298 StGB (wettbewerbsbeschränkende Absprachen) sein. Waren derartige Absprachen noch bis vor kurzem allein Gegenstand kartellrechtlicher Verfahren, so haben mittlerweile auch Staatsanwaltschaften diese Norm für sich entdeckt.

Gleiches gilt für den Geheimnisverrat, der gemäß § 17 UWG strafbar ist. Nicht nur Schweizer Banken stehen vor dem Problem, dass mittlerweile durch die vollständige Digitalisierung aller wesentlichen Geschäftsgeheimnisse diese mit relativ geringem Aufwand und ohne großes Entdeckungsrisiko durch Mitarbeiter gesichtet werden können. Neben der deutschen Steuerfahndung gibt es eine Reihe von Akteuren, die sich für derartige Betriebsgeheimnisse interessieren, weshalb es einen Markt für solche Daten gibt. Auch hier können *Internal Investigations* für das Unternehmen bei der Aufklärung der Taten und der Geltendmachung von Schadensersatz- und Unterlassungsansprüchen sehr hilfreich sein.

Eine weitere Strafnorm, gegen die in der Praxis relativ häufig verstoßen wird, ist § 119 Abs. 1 Nr. 3 Betriebsverfassungsgesetz (BetrVG), die im Zusammenhang mit § 37 Abs. 1 BetrVG zu sehen ist, wonach das Betriebsratsamt ein Ehrenamt ist. Betriebsratsmitglieder müssen also praktisch unter Ausblendung ihres Amtes vergütet werden, eine besondere „Betriebsratsvergütung“ wäre rechtswidrig. Das kann das Unternehmen bei Betriebsräten, die nach mehrjähriger Wiederwahl über einen erheblichen Zeitraum freigestellt, also nur als Betriebsräte tätig sind, vor die schwierige Frage stellen, wie sich die Vergütung bemisst. Die strafrechtliche Relevanz überhöhter Vergütungen der Betriebsratsmitglieder ist auch Fachleuten erst im Rahmen der juristischen Aufbereitung bei einem großen Automobilhersteller bewusst geworden. Das Landgericht Braunschweig hat die diversen Leistungen an die Betriebsratsmitglieder sowohl als Untreue als auch als Verstoß gegen § 119 Abs. 1 Nr. 3 BetrVG angesehen.[169] Die Besonderheit besteht hier aber darin, dass jedenfalls § 119 Abs. 1 Nr. 3 BetrVG ein absolutes Antragsdelikt ist, das heißt, dass ein Strafantrag durch den Betriebsrat oder die Gewerkschaft gestellt werden muss.

6.4.5 Steuerrechtlich relevante Bestimmungen

Von zentraler Bedeutung im Zusammenhang mit *Internal Investigations* sind die Regelungen des Steuerrechts.

Korruptionsdelikte gehen in aller Regel mit Steuerhinterziehung gemäß § 370 AO einher. Der Grund hierfür liegt in der Neufassung des § 4 Abs. 5 Nr. 10 EStG im Jahre 1999. Zuvor waren jedenfalls im Ausland gezahlte „Schmiergelder“ so genannte „nützliche Aufwendungen“

169 LG Braunschweig, CCZ 2008, 32.

und als Betriebsausgaben steuerlich absetzbar. Nunmehr folgt aus § 4 Abs. 5 Nr. 10 EStG, dass die Zuwendung von Vorteilen, wenn diese als rechtswidrige Handlung den Tatbestand eines Strafgesetzes oder eines Gesetzes verwirklicht, das die Ahndung mit einer Geldbuße zulässt, nicht den Gewinn mindern darf.[170] Wenn „Schmiergeldzahlungen" gleichwohl steuerlich in Abzug gebracht werden, so ist die abgegebene Steuererklärung unrichtig.[171]

Ob hierin bereits eine Steuerhinterziehung liegt, kann im Einzelnen zweifelhaft sein, weil jedenfalls bei größeren Unternehmen in der Regel die Steuerabteilung keine Kenntnis davon haben dürfte, dass Zahlungen an etwa im Projektgeschäft häufig eingeschaltete Berater möglicherweise der Korruption dienen. Anders liegt der Fall jedoch dann, wenn die Geschäftsleitung Kenntnis von Schmiergeldzahlungen hat und die Steuererklärung unterzeichnet.

In allen Fällen, in denen die aktuellen Leitungsorgane keine (eigene) Steuerhinterziehung begangen haben, werden sie durch § 153 AO verpflichtet, die (Unternehmens-)Steuererklärung unverzüglich zu berichtigen, wenn vor Ablauf der Festsetzungsfrist erkannt wird, dass diese unrichtig ist. Kommt der Steuerpflichtige dieser Pflicht nicht nach, so macht er sich selbst gemäß § 370 AO strafbar.[172] Problematisch ist, dass § 153 AO nur dann eingreift, wenn der Steuerpflichtige die Unrichtigkeit der Erklärung tatsächlich erkennt. Bloßes „erkennen müssen" reicht nicht aus. Insoweit befinden sich die Leitungsorgane von Gesellschaften in einem gewissen Dilemma bei *Internal Investigations*. Wird der bloße Verdacht geäußert, dass gewisse in der Vergangenheit liegende Zahlungen korruptiver Natur waren, so löst allein der Verdacht noch nicht die Pflicht nach § 153 AO aus. Führen die *Internal Investigations* allerdings zu dem Ergebnis, dass sich die Zahlungen tatsächlich als Korruptionsdelikte erweisen, dann besteht die unmittelbare Pflicht, das zuständige Finanzamt hierüber in Kenntnis zu setzen, weil man sich ansonsten strafbar macht (§ 370 AO). Auf den ersten Blick könnte diese Konsequenz zu der Annahme verleiten, besser keine Untersuchungen durchzuführen.

---

170 Umstritten ist, ob in § 4 Abs. 5 Nr. 10 EStG auch Zuwendungen angesprochen sind, die gemäß § 266 StGB oder § 119 I Nr. 3 BetrVG strafbar sind. Vgl. hierzu *Graf/Link,* NJW 2009, 409 ff. m.w.N.

171 Gemäß § 4 Abs. 5 Nr. 10 S. 3 EStG besteht eine Mitteilungspflicht für die Finanzbehörde. Diese muss den Verdacht von Korruptionsstraftaten der Staatsanwaltschaft mitteilen.

172 FG Düsseldorf, EFG 89, 491.

Allerdings wäre dies in den meisten Fällen zu kurz gedacht. Grund hierfür ist, dass ein späterer Streit über die Frage, ob schon ein ausreichender Verdacht, der die Pflicht nach § 153 AO auslöst, vorlag oder nicht, in einem Ermittlungsverfahren zu führen wäre. Betrachtet man die jüngste restriktive Rechtsprechung des für Steuerstrafsachen zuständigen 1. Strafsenats des BGH, wonach für die Wirksamkeit einer Selbstanzeige eine vollständige Rückkehr zur Steuerehrlichkeit erforderlich ist und sogenannte „Teilselbstanzeigen" nicht mehr möglich sind,[173] so kann man den Staatsanwaltschaften kaum verdenken, wenn sie in derartige Diskussionen mit großer Zuversicht gehen. Es darf an dieser Stelle auch nicht übersehen werden, dass ein Untätigbleiben stets die Gefahr von Vorwürfen mit sich bringt, falls spätere weitere Verstöße entdeckt werden.

Entscheidet man sich dafür, den Vorfällen auf den Grund zu gehen, dann macht es Sinn, die Finanzbehörden möglichst früh über die Untersuchungen zu unterrichten, weil somit das Risiko vermieden werden kann, dass später die bereits angesprochenen Diskussionen darüber zu führen sind, ob die Meldung unverzüglich[174] erfolgte. Diese Unterrichtung sollte dann erfolgen, wenn die Verdachtsmomente sich zu einer gewissen Wahrscheinlichkeit verdichtet haben.

Es bietet sich an, das Finanzamt über den Verdacht und die geplanten Aufklärungsmaßnahmen zu unterrichten. Hierbei sollte allerdings von vornherein deutlich gemacht werden, dass man sich zu einer frühzeitigen Offenlegung entschlossen hat und aus Gründen äußerster Vorsicht alle Zahlungen mitteilt, die in irgendeiner Weise verdächtig erscheinen. In der Praxis gelingt es auf diese Weise zumeist, übertriebene Erwartungshaltungen bei den Finanzbehörden zu vermeiden. Zu beachten ist in derartigen Fällen zudem, dass in vielen Fällen durch die Nacherklärung gleichzeitig den Finanzbehörden offenbart wird, dass es früher zu Steuerhinterziehungen gekommen ist. Mit Eingang der Nacherklärung beim Finanzamt bzw. der Einleitung eines (Straf-)Verfahrens ist es den früheren Verantwortlichen zumeist verwehrt, eine Selbstanzeige nach § 371 AO zu erstatten. Gerade in Fällen, in denen die früheren Verantwortlichen aus dem Unternehmen ausgeschieden sind, wird es in aller Regel nicht zweckmäßig sein, diese vorab zu unterrichten, damit sie ei-

---

173 Vgl. nur das Urteil vom 20. Mai 2010 – 1 StR 577/09, vgl. auch *Joachim Jahn*, Frankfurter Allgemeine Zeitung Nr. 184 vom 11. August 2010, S. 19.

174 Das heißt „ohne schuldhaftes Verzögern".

gene Nacherklärungen abgeben können, weil das Risiko zu groß ist, dass hierdurch die gesamte Koordination des Verfahrens gefährdet wird.

Will man die früheren Verantwortlichen aber auch nicht einfach ihrem Schicksal überlassen, so hilft in der Praxis häufig die Aufnahme der Erklärung, dass die Nacherklärung auch für die früheren Verantwortlichen gelten soll. Zwar ist dies nach der reinen juristischen Lehre keine wirksame Selbstanzeige im Sinne des § 371 AO, gleichwohl wird diese Vorgehensweise von Finanzämtern häufig akzeptiert. Bei aktuellen Mitarbeitern des Unternehmens, die an der Steuerhinterziehung beteiligt waren, bietet es sich hingegen an, diese kurz vor der Kontaktaufnahme mit dem Finanzamt zu unterrichten, damit diese gleichzeitig eine Selbstanzeige abgeben können.

Entscheidet man sich dafür, die Finanzbehörden zu unterrichten, so darf auf keinen Fall übersehen werden, dass diese verpflichtet sind, die zuständige Staatsanwaltschaft über den Verdacht von Korruptionsstraftaten zu unterrichten.[175] Aus diesem Grund ist es zwingend erforderlich, kurz nach Mitteilung an die Finanzbehörden auch zur Staatsanwaltschaft Kontakt aufzunehmen und diese über die interne Verdachtslage und die geplante Vorgehensweise zu unterrichten. Auch wenn dies natürlich keine Garantie dafür bietet, dass die Staatsanwaltschaft keine eigenen Ermittlungshandlungen (etwa eine Durchsuchung) vornimmt, ist die Chance, dass diese unterbleiben oder zuvor abgestimmt werden, bei einem offenen Zugehen auf die Ermittlungsbehörden ungleich höher, als wenn man die Staatsanwaltschaft nicht selbst unterrichtet. Die immer wieder geäußerte Hoffnung, die Finanzbehörden würden es mit ihren Mitteilungspflichten nicht so genau nehmen, wird in aller Regel enttäuscht.

6.4.6 Datendelikte, Strafvereitelung

Wichtig ist bei der Durchführung von *Internal Investigations*, dass das Unternehmen selbst nicht den Rahmen des strafrechtlich Zulässigen überschreitet. Gefahren drohen hier insbesondere im Zusammenhang mit der Verwendung von Mitarbeiterdaten ohne Zustimmung der Mitarbeiter. Offenkundig besteht hier ein Widerspruch zwischen dem Interesse des Arbeitgebers und der Prüfteams an umfassender Information und dem Schutz des Arbeitnehmers. Diese Diskrepanz hat in jüngerer Zeit zu einigen so genannten „Datenskandalen“ geführt, an deren Ende diejenigen,

175 § 4 Abs. 5 Nr. 10 S. 2-4 EStG.

die Gesetzesverstöße im Unternehmen verhindern bzw. aufklären wollen, selbst – unter großer medialer Aufmerksamkeit – als „Gesetzesbrecher“ dastanden.

Keiner weiteren Erörterung bedarf in diesem Zusammenhang, dass das Ausspähen von Kontodaten, Krankenkassenunterlagen oder das (private) Abhören von Telefonen stets unzulässig ist. Neben der Gefahr eigener Straftaten im Zusammenhang mit Datendelikten ist im Rahmen von *Internal Investigations* auch stets darauf zu achten, dass diese bei laufenden Ermittlungsverfahren mit der Staatsanwaltschaft abgesprochen sind, weil ansonsten schnell der Vorwurf aufkommen kann, die eigenen Ermittlungen würden die staatsanwaltschaftlichen Ermittlungen behindern, was gegebenenfalls sogar den Vorwurf der Strafvereitelung mit sich bringt.

Dem Arbeitgeber ist es grundsätzlich gemäß § 206 StGB untersagt, E-Mails seiner Mitarbeiter durch Zugriff auf den E-Mail-Server einzusehen. Von § 206 StGB geschützt sind alle Daten (Verbindungsdaten und Inhalte), die im Zusammenhang mit dem Telekommunikationsvorgang stehen. Diese unterliegen dem Fernmeldegeheimnis (Art. 10 Abs. 1 GG). Eine Ausnahme besteht allerdings dann, wenn den Mitarbeitern die Privatnutzung des Internets untersagt ist. Die Ausnahme liegt darin begründet, dass die Weitergabe von auf dem E-Mail-Server des Unternehmens gespeicherten Informationen nur dann nach § 206 StGB strafbar ist, wenn die Informationen dem Weitergebenden als Inhaber oder Beschäftigten eines Unternehmens bekannt geworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt. Der Begriff des „geschäftsmäßigen Erbringens“ ist durch die Legaldefinition des § 3 Nr. 10 Telekommunikationsgesetz (TKG) als „das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht“ bestimmt. Das heißt, es gilt nach allgemeiner Ansicht das Fernmeldegeheimnis des § 88 TKG, weil der Arbeitgeber – willentlich oder auch nicht – zum Anbieter einer Telekommunikationsdienstleistung wird.

Wenn dienstliche E-Mails nicht von privaten getrennt werden können, verbietet das TKG sowohl die Kontrolle der Verbindungsdaten als auch die Untersuchung des Inhalts der E-Mails zum Zwecke einer *Internal Investigation*. Soweit vertreten wird, dass bei konkreten Verdachtsmomenten von Unregelmäßigkeiten in einem Unternehmen die Inhaltskontrolle zulässig sei und in diesem Zusammenhang auf den rechtfertigen-

den Notstand gemäß § 34 StGB zurückgegriffen wird,[176] ist dies wenig überzeugend. Nach verbreiteter Meinung[177] sollen bei § 206 StGB nämlich die Rechtfertigungsgründe Notwehr und rechtfertigender Notstand[178] ausscheiden. Grund sei die tatbestandlich engere Fassung von § 88 Abs. 3 Satz 3 TKG. Denn nur einer Anzeigepflicht nach § 138 StGB (schwerste Straftaten) solle Vorrang zukommen und damit einen Rechtfertigung darstellen können. Das bedeutet, dass beispielsweise beim Verdacht einer Straftat gemäß § 17 UWG (Verrat von Geschäfts- und Betriebsgeheimnissen) die Aufklärung dieses Vorwurfs den Verstoß gegen § 206 StGB nicht rechtfertigen kann.

Beim Bruch des Fernmeldegeheimnisses droht den Handelnden damit die Strafbarkeit wegen einer Verletzung des Post- oder Fernmeldegeheimnisses nach § 206 StGB.[179] Hat ein Arbeitnehmer zudem Daten auf dem von ihm genutzten Rechner mit einer Verschlüsselungssoftware oder einem Passwort gegenüber dem Arbeitgeber geschützt, sodass der Arbeitgeber es nicht mit einem Administratorpasswort überwinden kann, droht zudem die Strafbarkeit nach § 202a StGB wegen des Ausspähens von Daten.[180] Etwaige strafrechtliche Risiken müssen vor Zugriff auf E-Mails geklärt werden. Unklar ist auch, ob das Fernmeldegeheimnis greift, wenn die private Nutzung zwar nicht gestattet, aber doch geduldet ist bzw. der Missbrauch durch Mitarbeiter nicht sanktioniert wird. Richtigerweise wird der Arbeitgeber hierdurch noch nicht zum Anbieter einer Telekommunikationsdienstleistung, wenn die Privatnutzung unmissverständlich untersagt ist.[181]

Eine gewisse Erleichterung bietet der Beschluss des Verwaltungsgerichtshofs (VGH) Kassel vom 19. Mai 2009,[182] wonach das Fernmeldegeheimnis auch bei erlaubter privater Nutzung des E-Mail-Kontos nicht mehr greift, wenn die Nachricht beim Arbeitnehmer angekommen und der Kommuni-

---

176 *Behling*, BB 2010, 892, 893.

177 *Fischer*, StGB, 57. Aufl., 2010, § 206 Rn. 9; dazu auch; nach OLG Karlsruhe CR 2005, 288, 290 gilt § 34 StGB nur, wenn besondere Fallgestaltungen vorliegen, die den Rahmen von § 88 III 3 TKG sprengen.

178 *Fischer*, StGB, 57. Aufl., 2010, § 206 Rn. 9.

179 Arbeitsgericht Berlin, 18. Februar 2010, 35 Ca 12879/09.

180 Das normale Login-Passwort schützt die Daten vor dem Zugriff Dritter und nicht vor Zugriff des Arbeitgebers, sodass § 202a StGB ausscheidet: *Schuster* ZIS 2010, 68, 70.

181 Arbeitsgericht Düsseldorf, 29. Oktober 2007, 3 Ca 1455/07, Rn. 40.

182 6 A 2672/08 Z, KuR 2009, 748 ff.; im Anschluss an Bundesverfassungsgericht (16. Juni 2009, 2 BvR 902/06).

kationsübertragungsvorgang beendet ist. Offen ist allerdings, wann genau dies der Fall ist. Das ist sicher dann der Fall, wenn der Mitarbeiter selbst die E-Mail innerhalb seines Postfachs verschiebt. Streitig ist indes, ob der Übertragungsvorgang auch abgeschlossen ist, wenn die E-Mail nach Abruf durch den Mitarbeiter weiterhin auf dem Server gespeichert wird (wie etwa bei der Verwendung von IMAP). Obwohl einige Autoren[183] in dieser Konstellation vertreten, dass der Übertragungsvorgang noch läuft, erscheint plausibler, davon auszugehen, dass die Speicherung der E-Mail auf dem Server nur der Archivierung dient und nicht quasi der Aufrechterhaltung des Übertragungsvorgangs.[184] Umgekehrt dürfte der Übertragungsvorgang noch nicht beendet sein, wenn die E-Mail zwar auf dem Server des Arbeitgebers angekommen ist, aber „abgegriffen" wird, bevor der Mitarbeiter Gelegenheit hat, den Inhalt zur Kenntnis zu nehmen. All dies ist freilich durch Gerichtsentscheidungen noch nicht geklärt.

Um diese rechtlichen Risiken zu beherrschen, muss das E-Mail-System dokumentierbar von vornherein darauf justiert werden, im Ernstfall einer *Internal Investigation* standzuhalten. Das bedeutet: Entweder die Privatnutzung wird untersagt oder unter den Vorbehalt gestellt, dass sich der Arbeitgeber stichprobenartig vorbehält, E-Mails zu prüfen und im Fall einer *Internal Investigation* Geschäftspost vollständig durchzusehen. Sinnvoll sind auch Vorkehrungen, mit denen sich private E-Mails, die vom Firmen-E-Mail-Account verschickt werden, von geschäftlichen E-Mails leicht trennen lassen.

Abschließend sei im Zusammenhang mit der Erhebung personenbezogener Daten noch der Ordnungswidrigkeittatbestand des § 43 Abs. 2 BDSG erwähnt. Hiernach handelt unter anderem ordnungswidrig, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,
2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,
3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft [...].

---

183 Etwa *Rath/Karner*, KuR 2010, 469 ff. (472).
184 So *Nolte/Becker*, CR 2009, 126, 127 f.

Eine Sicherstellung der datenschutzrechtlichen Compliance bei einer *Internal Investigation* ist daher unabdingbar.

6.5 Einwirken auf Zeugen und Trüben von Erkenntnisquellen für die Staatsanwaltschaft

Staatsanwaltschaften stehen *Internal Investigations* jedenfalls dann teilweise kritisch gegenüber, wenn diese zeitgleich mit einem staatsanwaltschaftlichen Ermittlungsverfahren erfolgen. Weil die *Internal Investigations* häufig mit größerem Personaleinsatz und ohne bürokratische Hürden erfolgen, sind sie den staatsanwaltschaftlichen Ermittlungen bisweilen einige Schritte voraus. Andererseits hat die Staatsanwaltschaft jedoch ganz andere prozessuale Möglichkeiten als dies bei internen Ermittlern der Fall ist. Man denke nur an Durchsuchungsbeschlüsse und Haftbefehle. Bei nicht ausreichender Abstimmung zwischen privaten und staatlichen Ermittlern kann das Problem entstehen, dass potentielle Beschuldigte durch die internen Befragungen gewarnt werden und über den Umfang der Beweismittel Kenntnis erlangen, was sie gegebenenfalls für ihre Verteidigung nutzen können. Dies kann dazu führen, dass seitens der Staatsanwaltschaft der Vorwurf der Strafvereitelung (§ 258 StGB) erhoben wird. Dem ist allerdings entgegenzuhalten, dass der Bundesgerichtshof eindeutig entschieden hat, dass private Ermittlungen zulässig sind.[185] Gleichwohl muss die Problematik ernst genommen werden. Der Unternehmensanwalt sollte auch diesen Punkt konstruktiv mit der Staatsanwaltschaft erörtern.

6.6 Durchsuchungen

In vielen Fällen sind die Einleitung eines Ermittlungsverfahrens und eine damit gegebenenfalls verbundene Durchsuchung vorauszusehen. Auch in den Fällen, in denen ein Unternehmen freiwillig mit den Ermittlungsbehörden kooperiert, ist keineswegs ausgeschlossen, dass die Ermittlungsbehörden sich durch eine Durchsuchung ein eigenes Bild von der Faktenlage machen wollen. Keineswegs darf die Vorbereitung auf eine Durchsuchung darin bestehen, kritische Unterlagen zu vernichten oder zu versuchen, eine bessere Beweislage zu schaffen.[186] Jede Einwirkung auf die bestehenden Beweismittel ist aus strafprozessualer Sicht absolut kontrapro-

185 BGHSt 46, 1 ff.
186 Zur Vorbereitung von Durchsuchungen: *Feigen/Livonius*, ZIP 2004, 889 ff.

duktiv.[187] Entdeckt die Staatsanwaltschaft bei ihren Durchsuchungen derartige Vorgänge, so wird das unangenehme Konsequenzen haben.

Für den persönlich an den Maßnahmen beteiligten Beschuldigten kann ein solches Verhalten unmittelbar in die Untersuchungshaft führen. Der Haftgrund der Verdunkelungsgefahr ist bei Wirtschaftsstraftaten ohnehin an geringe Herausforderungen geknüpft, weil jedenfalls einige Oberlandesgerichte die Ansicht vertreten, dass Wirtschaftsstraftaten per se auf Verschleierung und Verdunkelung angelegt sind. Die Vernichtung von Unterlagen erfüllt daher immer den Haftgrund der Verdunkelungsgefahr.

Für das Unternehmen bedeutet ein solcher Vorfall zudem, dass die angekündigte Kooperationsbereitschaft von der Staatsanwaltschaft in hohem Maße kritisch betrachtet wird. Häufig wird die Staatsanwaltschaft unterstellen, dass die entdeckten Verdunkelungshandlungen nur die Spitze des Eisbergs sind und jegliches Vertrauen in die Zusammenarbeit wird massiv schwinden.

Es macht daher vielmehr Sinn, die Unterlagen, die mit den strafrechtlichen Vorwürfen in Zusammenhang stehen, zusammenzustellen und diese an einem zentralen Ort zu lagern, damit sie im Falle einer Durchsuchung schnell herausgegeben werden können. Ein weiterer Vorteil dieser Vorgehensweise liegt darin, dass von den Unterlagen Kopien angefertigt werden können, die dann für die hier interessierenden internen Untersuchungen des Sachverhalts verwendet werden können. Zwar ist es auch im Rahmen einer Durchsuchung durchaus möglich, einzelne Unterlagen vor der Herausgabe zu kopieren. Im Zweifelsfall wird die Staatsanwaltschaft sich jedoch nicht darauf einlassen, alle Unterlagen zu kopieren, weil dies oft einen unverhältnismäßigen Aufwand erfordert. So werden regelmäßig im Rahmen von Durchsuchungsmaßnahmen nur diejenigen Unterlagen kopiert, die für die Aufrechterhaltung des Geschäftsbetriebes erforderlich sind.

Bei der Durchsuchung sollte sichergestellt sein, dass ein Ansprechpartner im Unternehmen zur Verfügung steht. Aus den Durchsuchungsbeschlüssen geht hervor, ob es sich um eine Durchsuchung beim Beschuldigten oder um eine Durchsuchung bei Dritten handelt und was der Vorwurf ist. Weiterhin wird dort ausgeführt sein, welche Unterlagen herausverlangt werden. Es sollte dann ein in strafrechtlichen Dingen versierter Rechts-

187 Vgl. hierzu § 112 StPO.

anwalt hinzugezogen werden, um die Durchsuchung zu begleiten. In Wirtschaftsstrafsachen lehrt die Erfahrung, dass Durchsuchungsbeschlüsse meist gut vorbereitet sind, sodass eine Abwehr der Durchsuchungsmaßnahme in der Regel ausscheidet. Stattdessen gilt es alles zu tun, um die Durchsuchung im geordneten und kooperativen Rahmen ablaufen zu lassen. Die Praxis zeigt, dass bei einer kooperativen Verhaltensweise häufig erreicht werden kann, dass beispielsweise Kopien gefertigt werden, die Durchsuchung auf die wesentlichen Räumlichkeiten beschränkt und verhindert wird, dass spontane Vernehmungen durchgeführt werden. Gerade die Vermeidung von unnötigen Ausweitungen der Durchsuchung ist für ein Unternehmen von Interesse, weil bei derartigen Durchsuchungen nicht ausgeschlossen werden kann, dass es zu sogenannten „Zufallsfunden" kommt.

Es ist hier anzumerken, dass es immer mehr Staatsanwaltschaften gibt, die unter Kooperation auch den Verzicht auf sämtliche prozessuale Rechte verstehen. Ein solches Ansinnen ist jedoch im Interesse aller Beteiligten aufs Schärfste zurückzuweisen.

6.7 Befragung von Mitarbeitern

Dass Anwälte Zeugen und Mitbeschuldigte auch während eines laufenden Ermittlungsverfahrens befragen dürfen, ist mittlerweile höchstrichterlich geklärt[188] und in der Literatur weitestgehend unumstritten.[189] Ebenso offenkundig ist allerdings, dass dem Anwalt die Befugnis, Zeugen behördlich zu vernehmen, nicht zusteht.

Ob ein Mitarbeiter, gegen den strafrechtliche Ermittlungen eingeleitet wurden, verpflichtet ist, gegenüber privaten Ermittlern Aussagen zu tätigen, ist umstritten, weil hierdurch der Grundsatz des Selbstschutzes bzw. der Selbstbelastungsfreiheit (*nemo tenetur se ipsum accusare)*[190] verletzt werden könnte. Allerdings hat der VII. Zivilsenat des Bundesgerichtshofs bereits im Jahre 1964 ausgeführt, dass es einen übergeordneten Rechtssatz, der es verbietet, von einem Schuldner Auskünfte zu verlangen, wenn er sich dadurch einer strafbaren Handlung bezichtigen müsste,

188 BGHSt 46, 1 ff.
189 *Jahn*, StV 2009, 41 (43).
190 Das Recht, sich nicht selbst belasten zu müssen, ist ein übergeordneter Rechtsgrundsatz, der einfachgesetzlich in den §§ 136 und 55 StPO seine Ausprägung findet.

nicht gibt.[191] Die Rechtsprechung versteht den *Nemo-Tenetur*-Grundsatz bislang lediglich als Schutz vor staatlich veranlasstem Aussagezwang.[192]

Derzeit geht die wohl noch herrschende Meinung davon aus, dass der Grundsatz im Rahmen eines Arbeitsverhältnisses keine Anwendung findet.[193] Für den Mitarbeiter, der gleichzeitig gefährdeter Zeuge oder gar Beschuldigter in einem Strafverfahren ist, wirft dies ein schwerwiegendes Dilemma auf. Im Strafverfahren hat er das Recht, zu schweigen. Hiervon wird der Beschuldigte immer dann Gebrauch machen, wenn er zu der Auffassung gelangt, dass die Staatsanwaltschaft ohnehin nicht genug Beweismittel hat, um ihn einer Straftat zu überführen. In Wirtschaftsstrafverfahren wird sich der Beschuldigte allerdings zumeist zur Sache einlassen, um die Vorwürfe zu entkräften, was die hier angesprochene Problematik zu relativieren scheint. Allerdings wird die Einlassung zumeist in Form einer schriftlichen Stellungnahme erfolgen, und es gilt geradezu als Anfängerfehler, eine Einlassung vor Durchführung der Akteneinsicht abzugeben.

Da im Rahmen der *Internal Investigations* zumeist weder eine schriftliche Stellungnahme als ausreichend angesehen noch Akteneinsicht abgewartet wird, verbleibt es für den Beschuldigten bei der Problematik, dass seine strafprozessualen Rechte faktisch wertlos werden. Aus Gründen der Fairness macht es einen gewissen Sinn, den Mitarbeiter bei seiner Befragung wie einen Zeugen im Strafprozess zu behandeln. Das bedeutet, der Mitarbeiter muss aussagen und es besteht Wahrheitspflicht, allerdings wird ihm die Möglichkeit eingeräumt, zu Fragen, bei denen er sich selbst belasten müsste, die Aussage zu verweigern.

Eine andere Frage ist allerdings, ob eine Aussagepflicht nur gegenüber dem Arbeitgeber oder aber auch gegenüber privaten Ermittlungsteams besteht, die der Arbeitgeber beauftragt hat. Hier gehen vereinzelte Autoren davon aus, dass eine Aussagepflicht gegenüber privaten Ermittlern

---

191 BGHZ 41, 318, 323.

192 BVerfGE 56, 37, 49 ff.; Problematisch kann es allerdings sein, wenn Unterlagen von internen Ermittlern an die Ermittlungsbehörden weitergegeben werden, da hierdurch das Schweigerecht der Beschuldigten gegenüber staatlichen Behörden faktisch ausgehebelt werden könnte, vgl. *von Rosen*, BB 2009, 230 ff.

193 Siehe Ziffer 7.1.1 auf S. 93.

nicht bestehen soll.[194] In der Praxis lässt sich diese Problematik meist dahingehend lösen, dass ein Vertreter des Arbeitgebers zugegen ist.

Aus strafprozessualer Sicht von besonderer Bedeutung ist, dass die Befragungen nicht auf Täuschungen des Befragten oder anderen fraglichen Mitteln (z.B. Drohungen) beruhen. Zwar wird nicht einheitlich beurteilt, ob (absichtliche) Verletzungen der Rechte des Befragten in Extremfällen dazu führen können, dass die Ergebnisse der Befragung strafprozessual analog § 136a Abs. 2 S. 3 StPO unverwertbar sind.[195] Gleichwohl sollte man sich an die „Spielregeln" der fairen Vernehmung halten und Aussagen nicht durch unlautere Mittel erwirken. Auch lässt sich bei vielen Staatsanwaltschaften eine deutliche Sensibilisierung in diesem Punkt ausmachen, sodass keinesfalls damit gerechnet werden sollte, dass die Strafverfolgungsbehörden allzu raue Beweisgewinnungsmethoden mit Beifall belohnen werden. Aus diesem Grund ist auch besondere Vorsicht geboten, wenn Mitarbeiterbefragungen – etwa auf „Wunsch" von *SEC* oder *DOJ* – stattfinden und englischsprachige Anwälte ein Interview führen, die mit deutschen strafprozessualen Vorschriften naturgemäß nicht vertraut sind. Eine besondere Sensibilisierung der Ermittlungsteams ist hier gefragt.

Wird mit dem Arbeitnehmer ein (arbeits- und zivilrechtliches) Amnestieprogramm vereinbart, so muss dieser darauf hingewiesen werden, dass dieses die Strafverfolgungsbehörden nicht bindet.

Vor einer Befragung sollte der Mitarbeiter auch stets darauf hingewiesen werden, dass seine Aussagen der Staatsanwaltschaft zur Verfügung gestellt werden können. Immer wieder zu vernehmende Hinweise auf eine angebliche Beschlagnahmefreiheit sind rechtlich kaum überzeugend. Selbst wenn es so wäre, dass die Ergebnisse aus *Internal Investigations* nicht beschlagnahmefähig wären, so ist die Vorstellung, dass das kooperierende Unternehmen die Bitte nach Herausgabe der Protokolle ablehnt, aus praktischen Gesichtspunkten nahezu abwegig.

---

194 Zur grundsätzlichen Gefahr einer Aussagepflicht vgl. *von Rosen*, a.a.O. Vgl. auch *Wastl/Litzka/Pusch*, NStZ 2009, 68 ff.

195 Nach herrschender Meinung gilt § 136a StPO nicht bei einer Befragung durch Private, die ohne amtlichen Auftrag ermitteln, näheres unter *Meyer-Goßner*, StPO, 43. Aufl., 2010, § 136a Rn. 3.

6.8 Ordnungswidrigkeitsrecht

Gemäß § 130 OWiG handelt ordnungswidrig, wer als Inhaber eines Betriebes oder Unternehmens vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, wenn die Zuwiderhandlung durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre.

§ 130 OWiG kommt bei der Ahndung von unternehmensbezogenen Straftaten ein zweifacher Zweck zu. Zum einen können über § 130 i.V.m. § 9 OWiG die Leitungsorgane eines Unternehmens für Straftaten der Mitarbeiter verantwortlich gemacht werden, wenn Aufsichtspflichten verletzt wurden. Zum anderen stellt ein Verstoß gegen § 130 OWiG eine Ordnungswidrigkeit eines vertretungsberechtigten Organs der Gesellschaft dar, was Grundlage für eine Unternehmensgeldbuße gemäß § 30 OWiG ist.

§ 130 OWiG ist seitens der Staatsanwaltschaften erst in den letzten Jahren als wirksames Mittel im Kampf gegen unternehmensbezogene Straftaten entdeckt worden. Mittlerweile hat die Sanktionsnorm des § 30 OWiG über einen Verstoß nach § 130 OWiG eine derartige Bedeutung erlangt, dass beinahe bei jeder Straftat oder Ordnungswidrigkeit seitens der Staatsanwaltschaften oder Ordnungsbehörden der Vorwurf erhoben wird, die Verfehlungen hätten ihren Grund auch in mangelnder Aufsicht. Weil die praktische Anwendung des § 130 OWiG erst in jüngster Zeit weite Verbreitung findet und häufig eine einvernehmliche Lösung seitens der Unternehmen angestrebt wird, sind viele rechtliche Fragen in diesem Bereich noch vollkommen ungeklärt.

So ist keineswegs geklärt, wie die Aufsichtspflicht in Konzernen ausgestaltet ist und ob der Vorstand einer Konzernobergesellschaft Aufsichtspflichten in Bezug auf die Tochtergesellschaften hat.[196]

Auch die Tathandlung als solche ist weitestgehend unklar. Fest steht, dass sie im Unterlassen der erforderlichen Aufsichtsmaßnahmen liegt. Was jedoch erforderliche Aufsichtsmaßnahmen sind, lässt sich der Rechtsprechung nicht entnehmen. Vertreten wird in diesem Zusammenhang,

196 BGH v. 1. Dezember 1981 – KRB 3/79.

dass § 130 OWiG die Einführung einer Compliance-Organisation verlangen soll.[197] Selbst wenn man dies fordert, ist aber immer noch nichts über die Ausgestaltung dieser Organisation gesagt. Das Ausmaß der Aufsichtspflicht hängt von den Umständen des Einzelfalles ab. Zu berücksichtigen sind Größe und Organisation des Betriebes und des Geschäftsbereichs, in dem das Unternehmen tätig ist.[198] § 130 OWiG verlangt eine sorgfältige Auswahl der Mitarbeiter, eine sachgerechte Organisation, die Aufklärung und Instruktion der Mitarbeiter, die (stichprobenartige) Überwachung der Mitarbeiter und ein Einschreiten bei festgestellten Verstößen.

Für *Internal Investigations* bedeutet dies, dass § 130 OWiG das Unternehmen sicher nicht verpflichtet, verdachtsunabhängige Untersuchungen durchzuführen. Tritt jedoch ein Verdacht auf, so wird sich die Unternehmensleitung jedenfalls dann keinen Vorwurf gefallen lassen müssen, wenn sie externe Experten mit der Aufklärung der Vorwürfe beauftragt und anhand der Ergebnisse der Ermittlungen geeignete Maßnahmen trifft. In einem laufenden Verfahren werden die interne Aufarbeitung und die Verbesserung der internen Abläufe zudem in aller Regel strafmindernd wirken. Hinzu kommt noch ein weiterer Aspekt: Tritt ein Verstoß erstmalig auf, wird man sich stets damit verteidigen können, dass dies nicht vorhersehbar war. Wiederholt sich der Verstoß jedoch, so wird man mit dieser Verteidigungslinie nicht mehr durchdringen. Wurden die Vorfälle jedoch aufgearbeitet und geeignete Maßnahmen getroffen, so wird man bei neuen Verstößen wieder argumentieren können, dass diese nicht vorhersehbar waren.

---

197 S*chneider*, ZIP 2003, 645 (früher); kritisch hierzu: *Nell*, ZRP 2008, 149 ff., *Schneider*, NZG 2009, 1321 ff.

198 Die Diskussion, wann und welche Anforderungen an die Aufsichtspflicht im Sinne von § 130 OWiG zu stellen ist, ist sehr im Fluss. Erste Ideen, inwiefern in diesem Zusammenhang auf Kriterien des Aktien- und Konzernrechts sinnvoller Weise zurückgegriffen werden muss, beschreibt *Schneider*, NZG 2009, a.a.O.

7. Internal Investigations aus arbeitsrechtlicher Sicht

Bestechung, Bestechlichkeit und Mitwirkung bei Einrichtung und Unterhalt schwarzer Kassen sind – neben den vorstehend beschriebenen strafrechtlichen Sanktionen – auch arbeitsvertragliche Pflichtverletzungen.[199] Selbst dann, wenn strafrechtliche Sanktionen unterbleiben, bedeutet dies noch nicht, dass keine arbeitsvertragliche Pflichtverletzung vorliegt.

Die Durchsetzung arbeitsvertraglicher Sanktionen (Abmahnung/Kündigung) kann unabhängig von dem Vorliegen einer Pflichtverletzung dennoch schwierig sein.

7.1 Mitarbeiter in der Internal Investigation

Compliance-Verstöße sind letztlich auf das Verhalten von Arbeitnehmern und Führungskräften zurückzuführen, die damit im Zentrum der *Internal Investigation* stehen. Unter 5.2 sind die entscheidenden Aufklärungsmittel der *Internal Investigation* angesprochen. Aus arbeitsrechtlicher Sicht werfen Mitarbeiterinterviews, der Zugriff auf elektronische Dokumente (vor allem E-Mails) und eine etwaige Beteiligung der betrieblichen Interessenvertretung Fragen auf.

7.1.1 Teilnahmepflicht am Interview

Der Mitarbeiter kann im Rahmen einer *Internal Investigation* in eine schwierige Situation geraten. Er ist Zeuge etwaiger Compliance-Verstöße, möglicherweise aber auch deren Täter oder zumindest im näheren Umfeld der Täter. Im Zweifel wird ein Mitarbeiter wenig Neigung verspüren, an der Aufklärung aktiv mitzuwirken. Gleichwohl ist er arbeitsvertragsrechtlich grundsätzlich zur Teilnahme am Interview verpflichtet. Zählt die Auskunfts- oder Aufklärungspflicht zu seinen arbeitsvertraglichen Aufgaben, kann das Unternehmen die Teilnahme kraft Direktionsrecht[200] einfordern.[201] Das ist bei den Mitarbeitern der Fall, die im Compliance-Bereich arbeiten, nicht dagegen etwa bei Vertriebsmitarbeitern. Auch Mitarbeiter, die nicht im Compliance-Bereich arbeiten, sind indes ver-

---

199 BAG, NZA 2002, 232 (Leitsatz); *Kolbe*, NZA 2009, 228, 229; *Steinkühler/Kunze*, RdA 2009, 267 ff.

200 § 106 Gewerbeordnung (GewO).

201 *Maschmann*, Maschmann [Hrsg.], Corporate & Compliance im Arbeitsrecht, 2008, 170; *Rieble*, ZIP 2003, 1273, 1275; *Böhm*, WM 2009, 1923, 1924.

pflichtet, am Interview teilzunehmen. Stützen lässt sich dies entweder auf eine entsprechende Anwendung von § 666 BGB oder auf § 241 Abs. 2 BGB, wonach der Arbeitnehmer alles Zumutbare tun muss, um Schäden vom Unternehmen abzuwenden.[202] Dazu zählt auch die Teilnahme am Interview, die dazu dient, den für das Unternehmen potentiell gefährlichen Sachverhalt aufzuklären und damit das Unternehmen vor (weiteren) Schäden zu schützen.

7.1.2 Interview durch Dritte

Ob der Mitarbeiter zur Teilnahme und Kooperation verpflichtet ist, wenn die Befragung durch Dritte (etwa Anwälte) erfolgt, wird vereinzelt in Frage gestellt, da nebenvertragliche Kooperations- bzw. Auskunftspflichten, auf welche die Teilnahmepflicht meist gestützt wird, untrennbar mit dem zugrunde liegenden Arbeitsverhältnis verbunden sind und daher nur vom Arbeitgeber selbst eingefordert werden könnten.[203] Ein Problem wäre das indes nur, wenn die Untersuchung durch Dritte losgelöst von den Interessen des Unternehmens geführt würde. Das wird aber nur selten der Fall sein.

Selbst konzernweite Untersuchungen, für die letztlich eine ausländische Behörde oder ein Verfahren im Ausland den Anstoß gegeben hat, können im Interesse der deutschen Konzern(mutter)gesellschaft liegen. Auch ein zu Rate gezogener Dritter, der das Interview führt, handelt im (mittelbaren) Interesse des Unternehmens, sodass der Mitarbeiter auch in dieser Konstellation zur Teilnahme verpflichtet ist. Größere Probleme aus der Praxis sind hier nicht bekannt, da meist ein Vertreter des deutschen Unternehmens am Interview teilnimmt. Darauf wird man schon deshalb nicht verzichten, weil die Kooperationsbereitschaft eher niedrig sein wird, wenn ein Mitarbeiter im Interview nur „Fremden“ gegenüber sitzt. Das allein durch Dritte geführte Interview wäre oft praxisuntauglich.

---

202 *Rieble*, ZIP 2003, 1273, 1275; allgemein: LAG Hessen, 21. November 2007, 18 Sa 367/07 Rn. 67.

203 In diese Richtung: *Jahn*, StV 2009, 41, 45.

7.1.3 Pflicht zur Beantwortung einzelner Fragen und Selbstbelastungsfreiheit

Grundsätzlich muss der Mitarbeiter Fragen zu Vorgängen im Unternehmen beantworten.[204] Einigkeit hat sich dahin entwickelt, dass der Arbeitgeber diesen Auskunftsanspruch wiederum auf den Arbeitsvertrag stützen kann, wenn die Aufklärung zu den Aufgaben des Mitarbeiters zählt (Compliance-Mitarbeiter). Ist das nicht der Fall, kann der Arbeitgeber die Auskunft nach den Vorschriften über die Auskunfts- und Rechenschaftspflicht eines Beauftragten nach § 666 BGB verlangen, wenn der Mitarbeiter Auskunft über Angelegenheiten aus seinem unmittelbaren Arbeitsbereich geben soll.[205] Dagegen folgt die Auskunftspflicht aus Treu- und Glauben bzw. aus einer vertraglichen Nebenpflicht (§§ 242, 241 Abs. 2 BGB), soweit nicht der unmittelbare Arbeitsbereich betroffen ist.[206] Wird ein Mitarbeiter etwa zu Vorgängen befragt, die er gelegentlich einer Dienstreise mitbekommen hat, lässt sich das in der Regel nur auf §§ 242, 241 Abs. 2 BGB stützen. Diese Unterscheidung erscheint auf den ersten Blick wichtig, weil § 241 Abs. 2 BGB im Gegensatz zu § 666 BGB eine Interessenabwägung fordert und die Auskunft dem Mitarbeiter daher zumutbar sein muss.[207]

Unstreitig ist, dass ein Mitarbeiter generell zur Auskunft verpflichtet ist. Dennoch ist, wie bereits im strafrechtlichen Teil aufgezeigt, stark umstritten, ob er die Antwort auf einzelne Fragen mit dem Hinweis verweigern kann, dass er sich dadurch einer Straftat oder einer erheblichen Pflichtverletzung bezichtigen müsste, und zwar vor dem Hintergrund der Selbstbelastungsfreiheit (*Nemo-Tenetur*-Prinzip). Die Selbstbelastungsfreiheit folgt aus dem allgemeinen Persönlichkeitsrecht, wonach der Einzelne vom Staat grundsätzlich nicht in eine Konfliktlage gebracht werden darf, in der er sich strafbarer Handlungen und ähnlicher Verfehlungen bezichtigen müsste oder in Versuchung gerät, durch Falschaussagen ein neues Delikt zu begehen.[208] Wegen der Zwangslage, in die ein Mitarbeiter im Interview geraten kann (*Talk or Walk*), fragt sich, wieweit die Selbstbelastungsfreiheit auch im Verhältnis zum Arbeitgeber bei einer *Internal Investigation* greift.

---

204 *Reichold* in: Münchener Handbuch Arbeitsrecht, 3. Aufl., 2009, § 49 Rn. 7.
205 *Reichold*, a.a.O., Rn. 5. *Jahn*, a.a.O., 43.
206 *Reichold*, a.a.O., Rn. 6; *Göpfert/ Merten/Siegrist*, NJW 2008, 1703, 1705.
207 BAG, 7. September 1995, 8 AZR 828/93 Rn. 25.
208 BVerfG, 13. Oktober 2003, 2 BVR 1321/02.

Das Arbeitsrecht regelt ein solches Recht allerdings genauso wenig wie das allgemeine Zivilrecht. Die Selbstbelastungsfreiheit ist ein Abwehrrecht gegen staatliche Eingriffe und nicht gegen die Befragung durch einen (privaten) Arbeitgeber.[209] Strafprozessuale Normen gelten daher nicht entsprechend,[210] und die Selbstbelastungsfreiheit entlastet eine Partei grundsätzlich auch nicht von der Wahrheitspflicht im Zivilprozess.[211] Lediglich der Zeuge im Zivilprozess kann die Aussage verweigern,[212] und nur in Einzelfällen finden sich Bestimmungen, die der Zwangslage eines zur Auskunft Verpflichteten Rechnung tragen: Nach § 97 Abs. 1 Satz 3 der Insolvenzordnung (InsO) darf ein zur Auskunft verpflichteter Insolvenzschuldner Angaben zwar nicht verweigern, seine Antwort bleibt strafprozessual aber unverwertbar.[213]

Unterscheidet man nach Rechtsgrundlagen, wäre ein Auskunfts- bzw. Aussageverweigerungsrecht eher bei einer nebenvertraglichen Auskunftspflicht begründbar,[214] da das Interesse des Arbeitnehmers, sich nicht selbst zu bezichtigen, gegen das Informationsinteresse des Arbeitgebers abgewogen werden könnte.[215] Stützt man die Auskunftspflicht dagegen auf § 666 BGB, ist der Mitarbeiter auch bei drohender Selbstbezichtigung zur uneingeschränkten Auskunft verpflichtet.[216] In den hier zu Rede stehenden Fällen wird sich die Auskunftspflicht zwar meist auf § 666 BGB stützen lassen, weil der unmittelbare Aufgabenbereich des Mitarbeiters betroffen ist,[217] gleichwohl würde eine Unterscheidung nach der Anspruchsgrundlage (§ 666 oder § 241 Abs. 2 BGB?) den Interviewer in Grenzfällen vor kaum lösbare Bewertungsfragen stellen, vor allem wenn der Aufgabenbereich eines Mitarbeiters zu ungenau beschrieben ist. Der Interviewer stünde nämlich vor der schwierigen Aufgabe, beurteilen zu

---

209 *Maschmann*, a.a.O., 173, Fn. 177, siehe auch bereits strafrechtliche Erörterungen Punkt 6.2.1.

210 *Krey*, Zur Problematik privater Ermittlungen des durch eine Straftat Verletzten, 1994, 52.

211 BAG, 20. November 2003, 8 AZR 580/02.

212 Vgl. § 384 Nr. 2 Zivilprozessordnung (ZPO).

213 Ebenso: § 393 Abs. 2 S. 1 AO.

214 § 241 Abs. 2 BGB.

215 *Reichold*, a.a.O., Rn. 7.

216 BGHZ 41, 318, 322 f.; BGH, 30. November1989, 3 III ZR 112/88 unter III.; *Böhm,* WM 2009, 1923, 1924.

217 Interviews werden anhand der gesichteten geschäftlichen Unterlagen vorbereitet. Folglich werden Mitarbeiter befragt, die dazu etwas sagen können. Das sind in der Regel die Urheber und bei E-Mails die CC- oder BCC-Empfänger.

müssen, ob die Antwort auf die gestellte Frage den unmittelbaren Aufgabenbereich betrifft oder schon darüber hinausgeht.

Einen Ausweg bietet in diesem Zusammenhang eventuell eine Entscheidung des Landesarbeitsgerichts Hamm,[218] welche nicht nach Rechtsgrundlage unterscheidet, sondern das Problem auf der Ebene des Strafprozesses löst. Danach bleibt der Arbeitnehmer zur Auskunft verpflichtet, und der Selbstbelastungsfreiheit wird durch ein strafprozessuales Verwertungsverbot Rechnung getragen.[219] Diesen Ansatz verfolgt auch das Bundesverfassungsgericht,[220] um eine Konfliktlage eines privatrechtlichen Auskunftsschuldners zu lösen, der sich durch die zwangsweise durchsetzbare Auskunft selbst belasten müsste. Es scheint also einiges dafür zu sprechen, eine Konfliktfrage, wenn überhaupt, nur auf der Ebene des Strafprozesses zu lösen.[221]

Das BAG[222] hat die Selbstbelastungsfreiheit dahingehend anerkannt, dass Arbeitgeber die Kündigung nicht allein auf die Weigerung stützen konnte, an der Aufklärung einer etwaigen Straftat im privaten Bereich mitzuwirken. Für die Frage, ob der Mitarbeiter damit in dienstlichen Angelegenheiten ein Aussageverweigerungsrecht gegenüber dem Arbeitgeber hat, ist damit kaum etwas gewonnen, da es in der BAG-Entscheidung nicht um dienstliche Verfehlungen ging. Der Entscheidung des BAG mag man entnehmen, dass die Weigerung des Mitarbeiters, eine Frage zu beantworten, allein nicht ausreicht, um eine Kündigung zu begründen. Weigert sich der Mitarbeiter allerdings, unter Berufung auf eine mögliche Selbstbezichtigung, eine Frage zu beantworten, kann das umgekehrt einen Verdacht gegen ihn erst begründen, den das Unternehmen dann für weitere Ermittlungen zum Anlass nimmt.[223]

Zusammenfassend betrachtet ist die Rechtslage noch ungeklärt. In der Praxis kommt dieser Frage aber meist nicht die Bedeutung zu, die ihr die

---

218 LAG Hamm, 3. März 2009, Az.: 14 Sa 1689/08.

219 LAG Hamm, a.a.O., in diese Richtung auch: *Maschmann* a.a.O., 175; *de Fries*, Arbeitsstrafrecht im Umbruch (2009), 92; a.A. aber OLG Karlsruhe, 6. September 1988, 1 Ss 68/88; *Schaefer*, NJW-Spezial 2009, 120, 121.

220 BVerfG, 13. Januar 1981, 1 BVR 116/97; wobei die Berufung auf Selbstbelastungsfreiheit oft erfolglos blieb etwa in 2 BvR 1321/02 (13. Oktober 2003), 2 BvR 1316/04. (15. Oktober 2005) oder 2 BvR 467/08 (31. März 2008).

221 Das erkennen auch *Wastl*/*Litzka*/*Pusch*, NStZ 2009, 68, 76.

222 23. Oktober 2008, 2 AZR 483/07.

223 OLG München, 25. März 2009, Az. 7 U 4835/08, Rn. 53.

wissenschaftliche Diskussion derzeit zollt. Selbst wenn man sich auf den Standpunkt stellt, dass der Mitarbeiter die Auskunft auch bei drohender Selbstbezichtigung nicht verweigern darf, wäre die gerichtliche Durchsetzung und Vollstreckung, soweit überhaupt zulässig,[224] eines Auskunftsanspruchs im Rahmen einer *Internal Investigation* schon aus Zeitgründen kaum eine Option. Zudem wird der Mitarbeiter unter Umständen eher arbeitsrechtliche Unannehmlichkeiten bis hin zur Kündigung in Kauf nehmen und sich nach einer anderen Stelle umsehen, bevor er sich selbst als Täter überführt. Verweigert ein Mitarbeiter die Antwort auf eine Frage, muss daher in der Regel ein anderer Weg gefunden werden, um die „Mauer des Schweigens" zu durchbrechen.

7.1.4 Kronzeugenregelung und Amnestieprogramme

Um der Zwangslage eines Mitarbeiters Rechnung zu tragen und die Aussagebereitschaft herzustellen, kann man auf eine Kronzeugenregelung zurückgreifen, mit der das Unternehmen auf Strafanzeigen gegen den Mitarbeiter, das Arbeitsverhältnis beendende Maßnahmen oder Ersatzansprüche verzichtet, wenn der Mitarbeiter Angaben macht. Grundsätzlich sind solche Programme zulässig, wobei ein Vertrauensvorschuss des Mitarbeiters unverzichtbar ist, dass sich das Unternehmen an die Absprache hält. Die Vorteile für den Mitarbeiter müssen im Übrigen in einem angemessenen Verhältnis zur Wichtigkeit der Auskunft stehen. Das Unternehmen muss sich davon versprechen dürfen, dass Mitarbeiter nur so zu Aussagen bewegt werden können und damit Schaden vom Unternehmen abgewandt wird.

Mit einer Amnestieregelung „ins Blaue hinein" oder nach dem Gießkannenprinzip kann die Geschäftsleitung im schlimmsten Fall gesetzliche[225] oder anstellungsvertragliche Pflichten verletzen, wenn auf an sich durchsetzbare Ersatzansprüche gegen Täter verzichtet wird. Das kann im Extremfall zu einer Untreuehandlung führen.[226] Richtig eingesetzt hilft die Kronzeugenregelung, die Kooperationsbereitschaft bei den Mitarbeitern herzustellen. Wichtig ist aber umgekehrt, sich mit einem Verzicht auf

---

224 Ob die Auskunftspflicht vollstreckbar ist, ist streitig. Nach Ansicht von *Rieble*, ZIP 2003, 1273, 1280 scheitert die Vollstreckung an § 888 Abs. 3 ZPO; aus der Entscheidung des BGH vom 3. Juli 2008, I ZB 87/06, lässt sich aber schließen, dass § 888 Abs. 3 ZPO hier nicht greift, ebenso *Böhm*, a.a.O., 1923 ff. (1928).

225 Vgl. §§ 91, 93 AktG, 43 GmbHG.

226 *Maschmann*, a.a.O., 179 f.

Sanktionen gegen einzelne Täter den Weg zu einer umfassenden Kooperation mit den Strafverfolgungsbehörden nicht zu verbauen. Denn diese Kooperation kann gerade auch im Verhältnis zu deutschen Behörden im Hinblick auf § 130 OWiG dazu führen, dass das Unternehmen die finanziellen Lasten erheblich senken kann.

7.1.5 Whistleblowing als Instrument der Internal Investigation

In engem Zusammenhang mit der Kronzeugenregelung stehen Whistleblowing-Hotlines, die inzwischen Teil der meisten Compliance-Systeme sind. Auch während der *Internal Investigation* kann sich das Unternehmen dieser unternehmensinternen Informationsquelle bedienen und etwa die angesprochene Kronzeugenregelung davon abhängig machen, dass ein Mitarbeiter von sich aus mittels dieses Mediums zur Aufklärung von Compliance-Verstößen beiträgt. Die Notwendigkeit solcher Programme erklärt sich vor ihrem arbeitsrechtlichen Hintergrund. Die Rechtslage ist schwierig. Zunächst kann ein Mitarbeiter aus der arbeitsvertraglichen Rücksichtnahmepflicht[227] gehalten sein, ihm bekannt gewordene Verfehlungen zur Anzeige zu bringen, vor allem, wenn die Überwachung zu seinen Aufgaben zählt oder erhebliche Schäden drohen.[228] Hier gelten Zumutbarkeitsgesichtspunkte. So kann es etwa im Einzelfall unzumutbar sein, Familienangehörige, die im gleichen Betrieb arbeiten, beim Arbeitgeber zu „verpfeifen".[229] Generell wegsehen darf ein Arbeitnehmer also nicht, wenn ihm Compliance-Verstöße bekannt werden.

Umgekehrt können falsche, haltlose oder unfundierte Hinweise oder Anzeigen eines Mitarbeiters gegenüber Behörden oder anderen Stellen zur fristlosen Kündigung führen.[230] Zwar hat der Mitarbeiter ein (arbeitsvertraglich unbeschränkbares) staatsbürgerliches Recht zur Strafanzeige, und zwar auch gegen seinen eigenen Arbeitgeber.[231] Allerdings kann eine (Straf-)Anzeige trotzdem als Pflichtverletzung zu werten sein, wenn der Mitarbeiter leichtfertig falsche Angaben macht[232] oder die Anzeige un-

---

227 § 241 Abs. 2 BGB.
228 *Reichold*, a.a.O., § 49 Rn. 10.
229 LAG Hessen, 21. November 2007, 18 Sa 367/07.
230 LAG Hamm, NZA-RR 2004, 475, 476.
231 BVerfG, 2. Juli 2001, 1 BvR 2049; BAG, 7. Dezember 2006, NZA 2007, 502, 503.
232 BAG, 3. Juli 2003, NZA 2004, 427, 428.

verhältnismäßig ist,[233] auch wenn der Sachverhalt zutrifft. Der Arbeitnehmer ist, so das BAG, nach § 241 Abs. 2 BGB verpflichtet, auf die Interessen des Arbeitgebers auch in dieser Situation Rücksicht zu nehmen. Dazu zählt auch, Betriebsinterna, die unter Umständen nach § 17 UWG geschützt sind, zunächst nicht nach außen zu tragen, sondern sich um interne Klärung zu bemühen.[234] Davon darf der Mitarbeiter letztlich erst absehen, wenn eine solche Abhilfe nicht zu erwarten ist.[235] Der Mitarbeiter steht also unter Umständen vor der schwierigen Entscheidung, ob er einen Verstoß anzeigt und, wenn ja, gegenüber wem. Und selbst wenn seine Entscheidung richtig war, existiert in Deutschland kein ausdrücklicher Whistleblower-Schutz. Man kann daher sagen, dass die derzeitige Rechtslage die Whistleblower-Idee nicht fördert, sondern eher behindert.

Genau in diesem Konfliktfeld muss das Whistleblowing-System ansetzen. Es muss sicherstellen, dass Mitarbeiter – verlässliche – Strukturen vorfinden, in denen sie im Bedarfsfall Hinweise geben und, wenn sie den Mantel der Anonymität verlassen und ihre Identität offen legen, keine Repressalien zu erwarten haben. Das System muss gewährleisten, dass Mitarbeiter nicht aus Angst vor Repressalien schweigen. Aus Effektivitätsgesichtspunkten wird man zunächst auffordern, anonyme Hinweise zu geben und den Hinweisgeber nach Prüfung dann gegebenenfalls bitten, seine Identität offen zu legen, bevor er in den Genuss der Vorteile kommt. Studien zeigen, dass der „Glaubhaftigkeitsgehalt" einer Information bei fehlender Anonymität steigt.[236] Und auch im Hinblick auf datenschutzrechtliche Auskunftspflichten lässt sich die Anonymität nicht durchhalten.[237] Sinnvoll ist hier der Einsatz Dritter, bei welchen die Hinweise eingehen, geprüft und damit vorsortiert werden. Denn die Bereitschaft der Mitarbeiter, Hinweise zu geben, wird erhöht, wenn der Hinweis zunächst nicht an firmeneigene Stellen gegeben werden muss. Bei der Einrichtung der Hotline ist im Übrigen zu prüfen, ob der Betriebsrat zu beteiligen ist, weil die Steuerung des Verhaltens der Mitarbeiter insbe-

---

233 BAG, 3. Juli 2003, NZA 2004, 427 ff. (430); BAG, 7. Dezember 2006, NZA 2007, 502 ff. (504).

234 BAG, 3. Juli 2003, NZA 2004, 427 ff. (430).

235 BAG, ebenda, 430.

236 Dazu *Fritz*, Maschmann [Hrsg.] Corporate Compliance und Arbeitsrecht 2009, 134.

237 Dazu *Breinlinger/Krader*, RDV 2006, 60, 64 f.; Whistleblower-Hotlines, Arbeitsbericht der Ad-hoc-Arbeitsgruppe „Beschäftigtendatenschutz" des Düsseldorfer Kreises.

sondere bei Anzeigepflichten nach § 87 Abs. 1 Nr. 1 BetrVG, mitbestimmungspflichtig sein kann.

7.1.6 Anspruch des Mitarbeiters auf Rechtsbeistand

In der Praxis taucht immer wieder die Frage auf, ob Mitarbeiter bei Interviews ein Mitglied des Betriebsrats oder einen eigenen Rechtsbeistand hinzuziehen dürfen. Natürlich kann das Unternehmen dies erlauben. Vor allem, wenn der Betriebsrat dabei ist, kann das unter Umständen Hemmschwellen bei den Mitarbeitern abbauen und die Kooperationsbereitschaft fördern. Fraglich ist aber, ob Mitarbeiter darauf auch einen Anspruch haben.

§§ 81 Abs. 4 Satz 3, 82 Abs. 2 Satz 2, 83 Abs. 1 Satz 2 und 84 Abs. 1 Satz 2BetrVG sehen Einzelfälle vor, in denen ein Arbeitnehmer ein Mitglied des Betriebsrats bei Gesprächen hinzuziehen kann. Gerichte legen diese Bestimmungen eng aus,[238] sodass sich daraus für den Fall der *Internal Investigation* kein Anspruch des Mitarbeiters ableiten lässt. Da der Mitarbeiter grundsätzlich verpflichtet ist, am Interview teilzunehmen, kann es keinen generellen Anspruch auf Hinzuziehung eines Rechtsbeistands geben, denn die Erfüllung einer persönlichen Dienstpflicht hängt nicht davon ab, dass der Arbeitgeber die Teilnahme eines (betriebsfremden) Dritten zulässt.[239]

Nur in anderem Zusammenhang kann die Teilnahme eines Rechtsbeistands zulässig bzw. sogar notwendig sein, etwa bei der Anhörung des Mitarbeiters vor einer Verdachtskündigung,[240] wobei es nach Ansicht des Landesarbeitsgerichts Berlin-Brandenburg[241] ausreicht, dem Mitarbeiter Gelegenheit zu geben, sich über einen Rechtsanwalt zu äußern. Für die *Internal Investigation* lässt sich auch daraus nichts gewinnen. In erster Linie geht es hier nicht darum, dem Mitarbeiter die Gelegenheit zu geben, einen gegen ihn bestehenden Verdacht zu entkräften, sondern den Sachverhalt im Hinblick auf die Vermeidung von Konsequenzen für das Unternehmen aufzuklären. Im Vordergrund steht somit das Kontrollinteresse des Unternehmens, bei dem Rechtpositionen des Mitarbeiters nicht über-

238 Etwa BAG, 16. Oktober 2004, 1 ABR 53/03.
239 *Lange/Vogel*, DB 2010, 1066, 1067.
240 *Lange/Vogel*, DB 2010, 1066 ff. (1068); angedeutet auch bei BAG, 13. März 2008, AZR 961/06 Rn. 18.
241 6. November 2009, 6 Sa 1121/09.

wiegen können.[242] Das spricht gegen einen Anspruch des Mitarbeiters, bei der Befragung einen Rechtsanwalt hinzuzuziehen. In einem späteren Kündigungsprozess einschließlich einer darauf gerichteten Anhörung kann das anders sein.

7.2 Kündigung als arbeitsrechtliche Sanktion

Verletzen Mitarbeiter durch Schmiergeldzahlungen, Bildung schwarzer Kassen oder durch Betrugsfälle den Arbeitsvertrag, kommt als Sanktion meist eine verhaltensbedingte, gegebenenfalls sogar fristlose Kündigung des Anstellungsverhältnisses in Betracht.[243] Auf eine Abmahnung muss das Unternehmen dagegen zurückgreifen, wenn der Mitarbeiter nicht damit rechnen konnte, sein Verstoß würde sogleich zur Kündigung führen, was eine Einzelfallbetrachtung erfordert. Die Kündigung kann im Übrigen auch Teil der „Reparatur" sein: Was in den USA an der Tagesordnung ist, nämlich dass es von Behörden als Milderungstatbestand gewertet wird, wenn sich das Unternehmen von den „Tätern" trennt, wird zunehmend auch in deutschen Verfahren nach § 130 OWiG praktiziert. Auch hier kommt es häufiger vor, dass die Strafverfolgungsbehörden es als „Bonus" werten, wenn das Unternehmen die Mitarbeiter entlässt, die für die Compliance-Verstöße verantwortlich sind.

In der Praxis lauern allerdings Fallen. Zum einen stellt sich die Frage, wie weit sich Mitarbeiter darauf berufen können, im Interesse des Unternehmens gehandelt zu haben, als etwa Schmiergelder im Ausland gezahlt wurden. Zum anderen lässt sich die gründliche *Internal Investigation* nicht immer mit der Zweiwochenfrist in Einklang bringen, die nach § 626 Abs. 2 BGB zumindest für die fristlose Kündigung einzuhalten ist. Die Kündigung hat danach innerhalb von zwei Wochen nach Kenntnisnahme des zur Kündigung Berechtigten vom Kündigungsgrund zu erfolgen.

7.2.1 Kündigungsgrund

Relevant für die erste Frage ist die bereits erwähnte Entscheidung des Arbeitsgerichts München.[244] Der entlassene Mitarbeiter hatte sich darauf berufen, das Unternehmen habe durch die Bildung systematischer

---

242 *Maschmann*, a.a.O, 175.
243 LAG München, 19. März 2009, 3 Sa 25/09.
244 2. Oktober 2008, NZA-RR 2009, 134 ff.

schwarzer Kassen an der Entstehung des Kündigungsgrundes mitgewirkt, welcher dem Mitarbeiter zur Last gelegt wurde. Die Berufung darauf sei daher treuewidrig. Das Arbeitsgericht München hat diesen Einwand zugelassen. Folgt man dem, heißt das, je stärker das Organisationsverschulden des Unternehmens ist, desto schwieriger wird es, gegen einzelne Täter vorzugehen. Das Arbeitsgericht Berlin hat einen ähnlichen Einwand des Arbeitnehmers berücksichtigt, und zwar genau im umgekehrten Fall.[245] Diesmal wollte sich das Unternehmen von der Mitarbeiterin nicht wegen Compliance-Verstößen trennen, sondern wegen unzulässiger Maßnahmen, welche die Mitarbeiterin (Leiterin Korruptionsbekämpfung) zur Aufdeckung von Compliance-Verstößen ergriffen hatte. Nach Ansicht des Arbeitsgerichts ist eine Kündigung nur wirksam, wenn sich die Mitarbeiterin der Unrechtmäßigkeit der Compliance-Maßnahme bewusst war, zumal sie etwas getan hatte, was aus Sicht des Unternehmens zum damaligen Zeitpunkt gewünscht war.

Man mag all dem entgegenhalten, dass es bei Erfüllung von Straftatbeständen oder Vertragsverletzungen an sich nicht auf die Motivationslage ankommt. Solange der Mitarbeiter mindestens die Arbeitsvertragswidrigkeit erkennt, ist nicht entscheidend, ob er im (vermeintlichen) Unternehmensinteresse handelt. Die Bildung schwarzer Kassen bleibt Untreue, auch wenn das Unternehmen in der Vergangenheit Vorteile daraus zog.[246] Plausibel erscheint es, ein organisatorisches Mitverschulden des Unternehmens im Rahmen der Interessenabwägung zugunsten des Arbeitnehmers zu berücksichtigen, wenn der Arbeitgeber den Arbeitnehmer über einen erheblichen Zeitraum im System schwarzer Kassen oder Schmiergeldzahlungen „einsetzte“. In diesem Fall kann das Festhalten am Arbeitsverhältnis noch zumutbar sein. Es bleibt dann die Abmahnung.

In der Praxis muss man diesen Tendenzen in der Rechtsprechung Rechnung tragen. Das heißt: Nur eine angemessene Compliance-Organisation, aus der den Mitarbeitern klar wird, dass Verstöße nicht geduldet, sondern geahndet werden und welche Maßnahmen aus Compliance-Sicht zulässig sind, ebnet den Weg, im Verstoßfall angemessene Sanktionen gegen die Mitarbeiter zu ergreifen, die sich an die Regelungen nicht halten.

---

245 18. Mai 2010, 38 Ca 12879/09.
246 *Steinkühler/Kunze*, RdA 2009, 367, 369.

7.2.2 Kündigungsfrist

Soll der Anstellungsvertrag fristlos gekündigt werden, was bei den Mitarbeitern entscheidend ist, die entweder eine sehr lange Kündigungsfrist oder sogar einen Festvertrag haben (üblicherweise Geschäftsführer), kann das Unternehmen außerdem Gefahr laufen, die Zweiwochenfrist des § 626 Abs. 2 BGB zu versäumen. Gerichte lassen außerordentliche Kündigungen bei schwierig zu beurteilenden Sachverhalten daran gerne scheitern. Bei der Zweiwochenfrist handelt es sich um keine Handlungs-, sondern um eine Entscheidungsfrist, die erst zu laufen beginnt, wenn die für die Kündigung zuständigen Organe im Unternehmen eine zuverlässige und möglichst vollständige Kenntnis von den für die Kündigung maßgebenden Tatsachen haben und deshalb eine Entscheidung über die Zumutbarkeit der Fortsetzung des Anstellungsverhältnisses treffen können.

Neben der Ermittlung des Sachverhaltes gehören dazu – besonders im Fall der Verdachtskündigung – auch die Beweismittelsicherung und vor allem die Anhörung des betroffenen Mitarbeiters.[247] Das Unternehmen muss die Ermittlungen mit der gebotenen Eile führen. Das BAG billigt bei einfach gelagerten Fällen in der Regel eine Woche zu, um den Arbeitnehmer anzuhören.[248] Hinzu kommt bei Arbeitnehmern unterhalb der Ebene der leitenden Angestellten nach § 5 Abs. 3 BetrVG, dass innerhalb der Zweiwochenfrist das Anhörungsverfahren des Betriebsrats nach § 102 BetrVG durchzuführen ist. All das kann bei umfangreichen Massenuntersuchungen zu erheblichen Zeitproblemen führen, vor allem, wenn die Untersuchung durch ein dafür eingerichtetes Komitee durchgeführt wird. Die Delegation der Untersuchung auf dafür eingesetzte Stellen oder Dritte entlastet das Unternehmen nämlich nicht, dafür zu sorgen, dass die notwendigen Informationen in der gebotenen Eile bei der Geschäftsleitung bzw. der für die Kündigung zuständigen Stelle ankommen. Bei Überlastung der Ermittler hat das OLG München[249] jüngst sogar verlangt, gegebenenfalls weitere Berater hinzuziehen, was die Kosten der Ermittlungen natürlich erhöht.

Bei Einrichtung des Untersuchungsplans muss daher ein Mechanismus gefunden werden, wonach kündigungsrelevante Informationen zügig an

---

247 BAG, NZA 2006, 1211 ff. (1214); OLG München, 25. März 2009, 7 U 4835/08.
248 BAG, ebenda, 1214.
249 OLG München, 25. März 2009, 7 U 4835/08, Rn. 46.

die kündigungsbefugten Personen fließen. Alternativ kann das Unternehmen bei gleichzeitigen strafrechtlichen Ermittlungen gegen einen Mitarbeiter auch deren Ergebnis abwarten, um die Kündigung dann auf die strafrechtliche Anklageerhebung oder Verurteilung des Mitarbeiters zu stützen. Der Zeitpunkt darf nicht willkürlich gewählt sein, etwa wenn die Ermittlungen der Staatsanwaltschaft noch nicht abgeschlossen sind.[250]

7.2.3 Zugriff auf E-Mails

Im Rahmen einer *Internal Investigation* kommt dem Zugriff auf E-Mails und elektronisch gespeicherte Dokumente erhebliche Bedeutung zu, weil der Großteil der Geschäftspost im Unternehmen inzwischen meist elektronisch abgewickelt wird. Gleichwohl bewegt sich der Zugriff auf elektronische Dokumente in einem schwierigen rechtlichen Rahmen, der mangels handhabbarer gesetzlicher Regelungen derzeit mit Unsicherheiten belastet ist. Zu unterscheiden ist nach dienstlichen und privaten E-Mails

7.2.3.1 Zugriff auf dienstliche E-Mails

Beim Zugriff auf dienstliche E-Mails und elektronisch gespeicherte Geschäftspost ist das Einsichtsrecht des Arbeitgebers unbestritten.[251] Das betrifft gleichermaßen Verbindungsdaten und die Inhaltskontrolle von E-Mails. Die Kontrolle dienstlicher E-Mails und Geschäftspost hat auch keine telekommunikationsrechtliche Implikation. Es gilt dann nur die Begrenzung der Kontrolle nach dem Bundesdatenschutzgesetz (BDSG).[252] Bei einer *Internal Investigation*, die zur Aufklärung von Verfehlungen dient, dürfte indes in der Regel der nach § 32 Abs. 1 Satz 2 BDSG erforderliche Anfangsverdacht vorliegen, sodass sich die Datenerhebung auf § 32 BDSG stützen lässt. Erfolgt die Untersuchung zu präventiven Zwecken, kommt derzeit § 28 Abs. 1 Satz 1 Nr. 2 BDSG als Rechtsgrundlage in Betracht. Sofern der Verhältnismäßigkeitsgrundsatz gewahrt bleibt und die erhobenen Daten, die zu keinen „Treffern“ geführt haben, wieder gelöscht werden, sind Persönlichkeitsrechte der Mitarbeiter durch eine solche stichprobenartige Kontrolle der Geschäftspost nicht betroffen.[253] Nur ein permanentes Screening der gesamten E-Mail-Aktivität eines Mitarbeiters wäre als Dauerüberwachung unzulässig, weil sie zu einem un-

250 LAG München, 19. März 2009, 3 Sa 25/09.
251 *Wolf/Mulert*, BB 2008, 442, 443; *Ernst*, NZA 2002, 585 ff., (589).
252 *Löwisch*, BB 2009, 2753, 2754.
253 Vgl. BVerfG 17. Februar 2009, 2 BvR 1372/07, 2 BvR 1745/07 Rn. 17 ff.

zumutbaren ständigen Anpassungsdruck führt.[254] Einer nachträglichen anlassbezogenen Kontrolle der E-Mails steht das aber nicht entgegen.

7.2.3.2 Zugriff auf private E-Mails

Erheblich schwieriger ist die Situation, wenn sich im EDV-System auch private E-Mails der Mitarbeiter befinden, was an anderer Stelle bereits behandelt wurde.[255]

7.3 Aspekte der Mitbestimmung des Betriebsrats

Der betriebsverfassungsrechtliche Rahmen, in dem sich eine *Internal Investigation* bewegt, ist vielschichtig und muss sorgfältig geklärt werden. Es können Betriebsvereinbarungen vorhanden sein, die sich mit der Ermittlung von Compliance-Verstößen befassen, was etwa im EDV-Bereich oft der Fall ist. Davon muss man sich vor Beginn einer Untersuchung ein Bild machen und die Regelungen im Idealfall darauf justieren. Im Einzelnen gilt Folgendes:

7.3.1 Rechte bei der Befragung von Arbeitnehmern

Wie bereits dargestellt, haben Mitarbeiter keinen generellen Anspruch auf Teilnahme eines Betriebsratsmitglieds bei einer Befragung zu (mutmaßlichen) Compliance-Verstößen. Allerdings muss nach § 80 Abs. 1 Nr. 1 BetrVG der Betriebsrat die Einhaltung von Gesetzen überwachen, wozu er nach § 80 Abs. 2 BetrVG rechtzeitig und umfassend vom Arbeitgeber zu unterrichten ist. Dieses Informationsrecht wird bei systematischen Befragungen von Arbeitnehmern wohl ausgelöst.

§ 80 Abs. 2 BetrVG gibt dem Betriebsrat aber ausschließlich ein Informationsrecht und kein Mitbestimmungsrecht dahin, dass die Zustimmung des Betriebsrats eingeholt werden müsste. Da Teilnahme und Antworten zum Arbeits- und nicht zum Ordnungsverhalten des Mitarbeiters zählen, besteht nach Ansicht der Literatur auch kein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 jedenfalls beim „ob“ einer Befragung.[256] Sicher ist dies allerdings nicht. Das BAG hat in einer Entscheidung zum Personalvertretungsrecht bei ähnlicher Konstellation die Teilnahme an der Aufklärung von innerbetrieblichen Unregelmäßigkeiten dem Ordnungsverhalten zu-

---

254 BAG 14. Dezember 2004, 1 ABR 34/02; BAG 26. August 2008, 1 ABR 16/07.
255 Siehe Ziffer 6.4.6.
256 *Zimmer/Heymann*, BB 2010, 1853, 1854.

geschlagen, zumindest wenn die Teilnahme am Interview zu den Nebenpflichten des Mitarbeiters zählt.[257] Ein Mitbestimmungsrecht kommt danach zwar nicht beim „ob“ der Befragung in Betracht, wohl aber dann, wenn der Arbeitgeber allgemeine Regeln für die Befragung aufstellen will, etwa durch wen die Befragung durchgeführt wird oder wie mit dem Befragungsersuchen der Muttergesellschaft zu verfahren ist.[258]

7.3.2 Zugriff auf elektronische Dokumente

Setzt das Unternehmen technische Einrichtungen ein, mit denen das Verhalten der Mitarbeiter überwacht werden kann, was auf die meisten EDV-Systeme zutrifft, kann das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG ausgelöst werden.[259] Wenn der Arbeitgeber zur E-Mail-Auswertung das vorhandene EDV-System nutzt, zu dem der Betriebsrat zugestimmt hat, muss der Betriebsrat zwar nicht erneut mitbestimmen. Technisch wird sich eine Massenuntersuchung aber oft nur durch den Einsatz zusätzlicher Software durchführen lassen, deren Einrichtung auch dann mitbestimmungspflichtig ist, wenn sie auf dem vorhandenen System aufbaut. In diesem Fall muss der Betriebsrat beteiligt werden und hat ein Mitbestimmungsrecht.

7.3.3 Verhaltenskodex

Die Einführung und Änderung von Bestimmungen in Compliance-Verhaltenskodizes bedarf der Zustimmung des Betriebsrats nach § 87 Abs. 1 Nr. 1 BetrVG, wenn und soweit mit der entsprechenden Bestimmung des Kodex das Ordnungsverhalten der Mitarbeiter geregelt wird. Dazu kann auch die Verpflichtung zählen, über eine Whistleblowing-Hotline Hinweise zu geben.[260]

Nicht mitbestimmungspflichtig sind Bestimmungen, die ausschließlich gesetzliche Pflichten wiedergeben, wozu allerdings US-amerikanische Bestimmungen (zum Beispiel *SOX)* nicht zählen.[261] Es kann also sein, dass ein Kodex nur teilweise mitbestimmungspflichtig ist, was man natürlich umgekehrt dazu nutzen könnte, zu versuchen, ihn von vornherein mitbestimmungsfrei zu gestalten. Üblicherweise werden solche Richtlinien aber

---

257 Für § 75 Abs. 3 Nr. 15 BPersVG: 27. September 2005, 1 ABR 32/04.
258 Ebenda.
259 BAG, 27. Januar 2004, NZA 2004, 556.
260 *Reichold*, a.a.O, § 49 Rn. 11.
261 BAG, 22. Juli 2008 – 1 ABR 40/ 07.

„als Gesamtpaket“ verhandelt. Der Betriebsrat wird sich daher nicht darauf beschränken wollen, nur bei den tatsächlich mitbestimmten Punkten mitreden zu wollen. Dieser Punkt muss sorgfältig geprüft werden.

7.3.4 Timing

Soweit Mitbestimmungsrechte bestehen, ist die Einbindung des Betriebsrats unumgänglich. Der Interviewer kann aber in der Regel nicht erwarten, dass der Betriebsrat, oder genauer: die Betriebsratsmitglieder von Anfang an auf seiner Seite stehen. Vor allem unerfahrene Betriebsratsmitglieder werden auf die Ankündigung einer – womöglich umfangreichen – *Internal Investigation* zunächst genauso reagieren wie die Arbeitnehmer, die sie vertreten – nämlich mit Ablehnung.

Die zahlreichen Hinweise an die Unternehmen, den Betriebsrat frühzeitig und sofort einzubinden, helfen in der Praxis wenig, wenn der mit dem Anliegen des Arbeitgebers konfrontierte Betriebsrat überfordert ist und sich reflexartig gegen alles Weitere sperrt. Man muss sich daher genau überlegen, wann der Betriebsrat eingebunden wird, von wem und mit welcher Zielrichtung. Richtig eingebunden kann er helfen, Vertrauen bei den Mitarbeitern aufzubauen und deren Kooperationsbereitschaft zu fördern. Es bleibt aber stets ein gewisses Unkalkulierbarkeitsmoment.

8. Fazit

Adäquates Rechtsmanagement und Compliance gewinnen sowohl auf nationaler als auch auf internationaler Ebene ständig an Bedeutung. Dies ist zum großen Teil einer intensivierten Korruptionsbekämpfung geschuldet. Sowohl nationale Behörden als auch internationale Organisationen verhängen zur Abschreckung rechtswidrigen Verhaltens heute Sanktionen, die für Unternehmen existenzbedrohende Auswirkungen haben können. Die Verankerung entsprechender Anti-Korruptions-Maßnahmen in den Compliance-Systemen ist demnach unumgänglich.

Gleichzeitig ist sowohl in der nationalen Gesetzgebung als auch bei internationalen Abkommen die Tendenz zu beobachten, Unternehmen zu belohnen, die Compliance-Verstöße frühzeitig und freiwillig offenbaren und diese gründlich aufklären, um ihr Compliance-System anzupassen und vergleichbare Missstände für die Zukunft auszuschließen. Drohende Sanktionen können somit oftmals reduziert oder gar abgewandt werden.

Wenngleich *Internal Investigations* zur Aufklärung von Missständen vor diesem Hintergrund für Unternehmen grundsätzlich sinnvoll erscheinen, gibt es kein allgemeines Rezept, wie mit einem Compliance-Verstoß umzugehen ist. Es sind stets die konkreten Umstände entscheidend, und es gilt sorgfältig abzuwägen, ob eine *Internal Investigation* im Einzelfall sinnvoll ist und wie diese gegebenenfalls durchzuführen ist.

Gerade in datenschutz-, aber auch in steuerrechtlicher Hinsicht kann eine *Internal Investigation* manchmal unerwünschte Konsequenzen mit sich bringen. Wenn sich eine konzerninterne Untersuchung auf mehrere Gesellschaften in verschiedenen Ländern erstreckt, können zusätzliche Probleme entstehen, da Rechtsvorschriften verschiedener Jurisdiktionen miteinander kollidieren und schlimmstenfalls extraterritoriale Rechtsanwendungen zur Aushebelung nationaler Rechtsgrundsätze führen können.[262] Deshalb ist hier ein besonderes Fingerspitzengefühl der internen Ermittler gefragt. Eine *Internal Investigation* kann außerdem weiteres Fehlverhalten über die zu klärenden Sachverhalte hinaus aufdecken, wodurch zum Beispiel neue steuerrechtliche Meldepflichten entstehen. Sofern diesen dann nicht nachgekommen wird, droht möglicherweise die Verfolgung wegen einer Straftat oder Ordnungswidrigkeit.

---

262 Vgl. *von Rosen*, BB 2010, H. 12, I.

Wenn aufgrund eines Anfangsverdachts bereits die Ermittlungsbehörden tätig geworden sind, wird sich heute schon aus Reputationsgründen heraus kaum ein Unternehmen mehr erlauben können, sich einer Kooperation mit hoheitlichen Ermittlern zu entziehen. Gerade bei großen, börsennotierten Unternehmen würden sonst eine negative Pressekampagne und ein entsprechender Image- und Reputationsverlust provoziert, ganz zu schweigen von der Geltendmachung möglicher Schadensersatzansprüche zum Beispiel durch Aktionäre.

Sofern man sich nach sorgfältigem Abwägen aller Vor- und Nachteile für eine *Internal Investigation* entscheidet, ist an die Verhältnismäßigkeit der zu ergreifenden Maßnahmen zu denken. Bei Anhaltspunkten für Bagatellverstöße gegen die Compliance-Bestimmungen liegen beispielsweise umfangreiche Datenanalysen oder Mitarbeiterbefragungen vor dem Hintergrund der aufgezeigten Rechtsprobleme sicherlich nicht im Unternehmensinteresse. Es sollte also nicht mit „Kanonen auf Spatzen geschossen werden".

Simultan zur ständig wachsenden Bedeutung der Compliance und ihres *Enforcement* auf nationaler und internationaler Ebene ist zu erwarten, dass die Bedeutung des Instruments *Internal Investigation* weiter zunimmt. Daher ist es besonders wichtig, dass die derzeit bestehenden Rechtsunsicherheiten, die aus dem Spannungsverhältnis zwischen dem Interesse des Unternehmens an der Aufklärung von Compliance-Verstößen und den Rechten der Mitarbeiter resultieren, zügig geklärt werden.

Beim Thema Compliance ist Prävention das oberste Gebot, um potentielle Schäden zu begrenzen oder gar Flächenbrände zu verhindern. Im Unternehmen müssen daher Strukturen geschaffen werden, die bei etwaigen Compliance-Verstößen möglichst frühzeitig Alarm geben. Neben einer Sensibilisierung der Mitarbeiter, beispielsweise durch Schulungen, sollten vernünftige Compliance-Strukturen auch Reporting-Systeme vorsehen, die eine anonyme Meldung möglicher Missstände gestatten.

Wichtig ist in jedem Fall die Kommunikation einer *Zero-Tolerance-Guideline*. Die Unternehmensführung selbst sollte als Vorbild dienen und auf allen Unternehmensebenen klarmachen, dass korruptives, kartellrechtswidriges oder anderes Fehlverhalten auf keinen Fall geduldet wird. Durch effektive Präventivmaßnahmen lässt sich dann die Gefahr des Eintritts eines gravierenden Compliance-Verstoßes, der Anlass zu einer umfangreichen Untersuchung gibt, auf ein Minimum reduzieren.

9. Anhang: Frühwarnindikatoren und Maßnahmen[263]

Handlungsmuster	„Red Flags“	Maßnahmen zur Eingrenzung des Risikos
Gezielter Einkauf von Gütern bzw. Dienstleistungen zu überhöhten Preisen. Dabei wird auf die Einholung von Vergleichsangeboten bzw. auf die Durchführung von Ausschreibungen verzichtet. Überhöhte Angebote oder Abrechnungen werden akzeptiert, um im Gegenzug „Kick-back“-Zahlungen von dem begünstigten Lieferanten zu erhalten.	• Unklare, nicht nachvollziehbare und unvollständig dokumentierte Einkaufsentscheidungen; • Lieferanten suchen ausschließlich den persönlichen Kontakt zu bestimmten Einkaufsmitarbeitern; • Aufteilung der Bestellung (Splitting) zur Umgehung des Genehmigungsverfahrens.	• Einführung von Richtlinien und Verfahrensanweisungen im Einkaufsbereich; • Controlling der Einkaufspreise/ Durchführung von stichprobenartigen Prüfungen ohne konkreten Anlass; • Implementierung von Rahmenverträgen mit den wichtigsten Lieferanten (Abrufbestellungen).
Begünstigung von Kunden seitens eines Vertriebsmitarbeiters durch Verkauf von Gütern unter den üblichen Preisen oder überhöhte Rabattgewährung zur Generierung von „Kick-back“-Zahlungen.	• Erhöhte Rabatt- und Preisminderungsquoten einzelner Vertriebsmitarbeiter; • Auffällige Veränderungen der Leistungszahlen von Vertriebsmitarbeitern; • Signifikante Veränderung von Verkaufspreisen bzw. -konditionen nach dem Wechsel von Vertriebsmitarbeitern.	• Einführung von verbindlichen Vertriebskonditionen; • Implementierung eines Vier-Augen-Prinzips bei der Unterschreitung von Preisen bzw. bei der Gewährung von Rabatten jenseits definierter Grenzen; • Durchführung von Prüfungen ohne konkreten Anlass (Bildung relevanter Kennzahlen mittels analytischer Prüfprogramme).
Umleitung von Zahlungsströmen auf Drittkonten durch Anlage und Nutzung von fiktiven Lieferanten in Verbindung mit fingierten Einkaufsvorgängen.	• Lieferantendaten (Adress- bzw. Bankverbindungsdaten) stimmen mit den entsprechenden Daten von Mitarbeitern überein; • Zahlungen werden über Sammelkonten abgewickelt und somit nicht den Kreditoren zugeordnet.	• Regelmäßiges Controlling der Lieferanten und der Kreditorenstammdaten; • Einführung eines Standardprozesses zur Anlage von Kreditoren (Vier-Augen-Prinzip/ Funktionstrennung).
Abrechnung von überhöhten bzw. privat veranlassten Reise- bzw. Spesenaufwendungen.	• Erhöhtes Aufwandsvolumen für Reisekosten, Spesen etc.; • Belege gleichen Datums, jedoch von unterschiedlichen, weit entfernten Orten; • Bewirtungsrechnungen, Spesen- bzw. Geschenkquittungen ohne die erforderliche Freigabe.	• Implementierung von Plausibilisierungsroutinen und Abrechnungskontrollen; • Überprüfung von Genehmigungsprozessen auf deren Wirksamkeit und ordnungsgemäße Durchführung.

263 Quelle: Bundesverband der Deutschen Industrie e.V./KPMG AG Wirtschaftsprüfungsgesellschaft (Hrsg.), Sichere Geschäfte? Wirtschaftskriminalität – Risiken für mittelständische Unternehmen, BDI-Drucksache Nr. 421, 1. Aufl., Berlin 2009, S. 17.

10. Literaturverzeichnis

Arbeitskreis Externe und Interne Überwachung der Unternehmung der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V. (AKEIÜ), Compliance: 10 Thesen für die Unternehmenspraxis, in: Der Betrieb, Nr. 27/28, 2010, S. 1509 ff.

Baums, Theodor, Managerhaftung und Verjährungsfrist, Institute for Law and Finance Working Paper Series No. 119, Juli 2010

Behrling, Thorsten, Compliance versus Fernmeldegeheimnis, in: Betriebs-Berater, H. 15, 2010, S. 892 ff.

Böhm, Wolf-Tassilo, Strafrechtliche Verwertbarkeit der Auskünfte von Arbeitnehmern bei unternehmensinternen Untersuchungen, in: Wirtschaft und Wettbewerb, H. 41, 2009, S. 1923 ff.

Bohnert, Joachim, Ordnungswidrigkeitengesetz, 2. Aufl, München 2007.

Breinlinger, Astrid/Krader, Gabriela, Whistleblowing – Chancen und Risiken bei der Umsetzung von anonym nutzbaren Hinweisgebersystemen im Rahmen des Compliance-Management von Unternehmen, in: Recht der Datenverarbeitung, H. 1, 2006 S. 60 ff.

Drygala, Tim in: *Schmidt, Karsten/Lutter, Marcus*, Aktiengesetz Kommentar, Köln 2008.

Ernst, Stefan, Der Arbeitgeber, die E-Mail und das Internet, in: Neue Zeitschrift für Arbeitsrecht, H. 11, 2002, S. 585 ff.

Feigen, Hans/Livonius, Barbara, Wenn strafrechtliche Ermittlungen drohen, in: Zeitschrift für Wirtschaftsrecht 2004, S. 889 ff.

Fischer, Thomas, Kurzkommentar zum Strafgesetzbuch, 57. Aufl., München 2010.

Fleischer, Holger, Vorstandsverantwortlichkeit und Fehlverhalten von Unternehmensangehörigen – Von der Einzelüberwachung zur Errichtung einer Compliance-Organisation, in: Die Aktiengesellschaft, H. 5, 2003, S. 291 ff.

Fritz, Hans-Joachim, Whistleblowing – Denunziation oder Wettbewerbsvorteil?, in: *Maschmann* (Hrsg.), Corporate Compliance und Arbeitsrecht, Baden-Baden 2009, S. 111 ff.

Göhler, Erich, Kurzkommentar zum Ordnungswidrigkeitengesetz, 14. Aufl., München 2006

Göhler, Erich, Kurzkommentar zum Ordnungswidrigkeitengesetz, 15. Aufl., München 2009.

Graf, Walther/Link, Holger, Überhöhte Betriebsratsvergütung – kein neues Betätigungsfeld für Steuerfahnder, in: Neue Juristische Wochenschrift, H. 7, 2009, S. 409 ff.

Grau, Carsten/Meshulam, Deborah R./Blechschmidt, Vanessa, Der lange „Arm" des US-Foreign Corrupt Practices Act: Unerkannte Strafbarkeitsrisiken auch jenseits der eigentlichen Korruptionsdelikte, in: Betriebs-Berater, H. 12, 2010, S. 652 ff.

Habersack, Matthias/Goette, Wulf, Münchener Kommentar zum Aktiengesetz, 3. Aufl., München 2008.

Hauschka, Christoph E., Corporate Compliance – Handbuch der Haftungsvermeidung in Unternehmen, München 2007.

Hauschka, Christoph E./Salvenmoser, Steffen, Korruption, Datenschutz und Compliance, in: Neue Juristische Wochenschrift, H. 6, 2010, S. 331 ff.

Hübschmann, Walter/Hepp, Ernst/Spitaler, Armin, Kommentar zur Abgabenordnung und Finanzgerichtsordnung, 202. Lieferung, Köln 2009.

Hüffer, Uwe, Kurzkommentar zum Aktiengesetz, 6. Aufl., München 2010.

Jahn, Matthias, Ermittlungen in Sachen Siemens/SEC, in: Strafverteidiger, H. 11, 2009, S. 41 ff.

König, Stefan, Wieder da: Die große Kronzeugenregelung, in: Neue Juristische Wochenschrift, H. 34, 2009, S. 2481 ff.

Kolbe, Sebastian, Unkündbarkeit für Korruptionstäter, in: Neue Zeitschrift für Arbeitsrecht, H. 5, 2009, S. 228 ff.

Krey, Volker, Zur Problematik privater Ermittlungen des durch eine Straftat Verletzten, in: Schriften zum Strafrecht, H. 102, Berlin 1994.

Krieger, Gerd/Sailer, Viola in: *Schmidt, Karsten/Lutter, Marcus,* Aktiengesetz Kommentar, Köln 2008.

Lange, Niels/Vogel, Thius, Verdachtskündigung: Teilnahmerecht des Rechtsanwalts an der Anhörung, in: Der Betrieb, H. 19, 2010, S. 1066 ff.

Langen, Eugen/Bunte, Hermann-Josef, Kommentar zum deutschen und europäischen Kartellrecht, Bd. 2, 11. Aufl., München 2010.

Löwisch, Manfred, Telekommunikation, Arbeitsplatz, Überwachung, in: Der Betrieb, H. 42, 2009, S. 2189 ff.

Maschmann, Frank, Mitarbeiterkontrolle und private Ermittlungen, in: *Maschmann* (Hrsg.), Corporate Compliance und Arbeitsrecht, Baden-Baden 2009, S. 249 ff.

Menzies, Christof (Hrsg.), Sarbanes-Oxley und Corporate Compliance, Stuttgart, 2006

Meyer-Goßner, Lutz, Kurzkommentar zur Strafprozessordnung, 43. Aufl., München 2010.

Moosmayer, Klaus, Compliance – Praxisleitfaden für die Unternehmensführung, München 2010.

Nell, Mathias, Korruptionsbekämpfung ja – aber richtig!, in: Zeitschrift für Rechtspolitik, H. 5, 2008, S. 149.

Nietzer, Wolf, Die rechtliche Behandlung von Schmiergeldzahlungen in den USA („Foreign Corrupt Practices Act“) und Deutschland, Deutsch-Amerikanische Juristen-Vereinigung Newsletter 2/1998, S. 43 ff.

Nolte, Norbert/ Becker, Philipp, Anmerkungen zu VG Frankfurt, 6. November 2008, CR 2008, S. 127 ff.

Rath, Michael/Karner, Sophia, Internetnutzung am Arbeitsplatz, in: Kommunikation & Recht, 2010, S. 469 ff.

Reichhold, Hermann, Handbuch Arbeitsrecht, 3. Aufl., München 2009.

Rieble, Volker, Schuldrechtliche Zeugenpflicht von Mitarbeitern, in: Zeitschrift für Wirtschaftsrecht, H. 3, 2003, S. 127 ff.

Salditt, Franz, Allgemeine Honorierung besonderer Aufklärungshilfe, in: Strafverteidiger, H. 34, 2009, 375 ff.

Schaefer, Torsten, Selbstbelastungsschutz außerhalb des Strafverfahrens, in: Neue Juristische Wochenschrift-Spezial, 2010, S. 120.

Schmidt, Karsten/Lutter, Marcus, Aktiengesetz Kommentar, Köln 2008.

Schneider, Uwe H., Compliance als Aufgabe der Unternehmensleitung, in: ZIP Zeitschrift für Wirtschaftsrecht, H. 12, 2003, S. 645 ff.

Schneider, Uwe H., Compliance im Konzern, in: Neue Zeitschrift für Gesellschaftsrecht, H. 30, 2009, S. 1321 ff.

Semler, Johannes/Peltzer, Martin, Arbeitshandbuch für Vorstandsmitglieder, München 2005.

Spindler, Gerald, Münchener Kommentar zum Aktiengesetz, 3. Aufl., München 2008.

Steinkühler, Bernhard/Kunze, Kati, Schmiergelder, schwarze Kassen und ihre kündigungsrechtlichen Konsequenzen, in: Recht der Arbeit, H. 6, 2009, S. 367 ff.

Stephan, Hans Jürgen/Seidel, Jürgen, in: *Hauschka*, Corporate Compliance – Handbuch der Haftungsvermeidung in Unternehmen, München 2007.

Tinkl, Christina, Strafbarkeit von Bestechung nach dem europäischen Bestechungsgesetz und dem internationalen Bestechungsgesetz, in: Zeitschrift für Wirtschaft- und Steuerstrafrecht, H. 1, 2006, S. 126 ff.

von Rosen, Rüdiger, Rechtskollision durch grenzüberschreitende Sonderermittlungen, in: Betriebs-Berater, H. 6, 2009, S. 230 ff.

von Rosen, Rüdiger, US-Justiz ante portas?, in: Betriebs-Berater, H. 12, 2010, S. I.

Wagner, Jens, Internal Investigations und ihre Verankerung im Recht der AG, in: Corporate Compliance Zeitschrift, H. 1, 2009, S. 8 ff.

Wastl, Ulrich/Litzka, Philippe/Pusch, Martin, SEC-Ermittlungen in Deutschland – eine Umgehung rechtsstaatlicher Mindeststandards!, in: Neue Zeitschrift für Strafrecht, H. 2, 2009, S. 68 ff.

Wolf, Berlin/Mulert, Gerrit, Die Zulässigkeit der Überwachung von E-Mail Korrespondenz am Arbeitsplatz, in: Betriebs-Berater, H. 9, 2008, S. 442 ff.

Wybitul, Tim, Interne Ermittlungen auf Aufforderung von US-Behörden – ein Erfahrungsbericht, Betriebs-Berater, H. 12, 2009, S. 606 ff.

Wybitul, Tim, Wie viel Arbeitnehmerdatenschutz ist „erforderlich"?, in: Betriebs-Berater, H. 18, 2010, S. 1085 ff.

Zimmer, Mark/Heymann, Robert C. J., Beteiligungsrechte des Betriebsrats bei unternehmensinternen Ermittlungen, in: Betriebs-Berater, H. 31, 2010, S. 1853 ff.

Verzeichnis der verwendeten Internet-Seiten

Bundesanstalt für Finanzdienstleistungsaufsicht	http://www.bafin.de
Bundesgerichtshof	http://www.bundesgerichtshof.de
Bundeskartellamt	http://www.bundeskartellamt.de
Bundesministerium des Inneren	http://www.bmi.bund.de
Bundesverband der Deutschen Industrie e.V.	http://www.bdi.eu
Deutscher Bundestag	http://www.bundestag.de
Europäische Kommission	http://ec.europa.eu
Europäische Union	http://europa.eu
European Corporate Governance Institute	http://www.ecgi.org
Global Infrastructure Anti-Corruption Centre	http://www.giaccentre.org
International Chamber of Commerce	http://www.iccwbo.org
New York Stock Exchange	http://www.nyse.com
Organisation for Economic Co-operation and Development	http://www.oecd.org
Transparency International	http://www.transparency.org
UK Ministry of Justice	http://www.justice.gov.uk
UK Office of Public Sector Information	http://www.opsi.gov.uk
United Nations	http://www.un.org
United States Department of Justice	http://www.justice.gov
United States Securities and Exchange Commission	http://www.sec.gov
United States Sentencing Commission	http://www.ussc.gov
University of Cincinnati College of Law	http://www.law.uc.edu
World Economic Forum	http://www.weforum.org

DEUTSCHES AKTIENINSTITUT

Deutsches Aktieninstitut e.V.
Niedenau 13-19 60325 Frankfurt am Main
Tel. 0 69/9 29 15-0 Fax 0 69/9 29 15-12
E-Mail dai@dai.de Internet http://www.dai.de

ISBN 978-3-934579-62-0