sofia

Sonderforschungsgruppe
Institutionenanalyse

Das Spannungsfeld zwischen Datenschutz-Anforderungen und dem Aufbau und Betrieb eines internen Kontrollsystems

Die Zulässigkeit von automatischen Datenanalysen
aus der Sicht eines IT-Dienstleistungsunternehmens

Diplomarbeit

Julian Schenten

sofia-Studien 10-2, Darmstadt 2010

ISBN: 978-3-933795-99-0

Sofia-Studien
zur Institutionenanalyse
Nr. 10-2

ISSN 1439-6874
ISBN 978-3-933795-99-0

Das Spannungsfeld zwischen Datenschutz - Anforderungen und dem Aufbau und Betrieb eines internen Kontrollsystems

Die Zulässigkeit von automatischen Datenanalysen aus der Sicht eines IT-Dienstleistungsunternehmens

Diplomarbeit von
Julian Schenten

Diplomarbeit im Studiengang Informationsrecht · Hochschule Darmstadt

Vorgelegt am 31. Mai 2010

Referent: Prof. Dr. Martin Führ

Korreferent: Prof. Dr. Thomas Wilmer

Themenvorschlag „Das Spannungsfeld zwischen Datenschutzbestimmungen und dem Aufbau und Betrieb eines internen Kontrollsystems“ von Hubertus Gottschalk

Vorwort aus aktuellem Anlass

Die vorliegende Arbeit beschreibt das Spannungsfeld zwischen Datenschutzanforderungen und dem Aufbau und Betrieb eines internen Kontrollsystems unter besonderer Berücksichtigung der datenschutzrechtlichen Norm § 32 BDSG in der Fassung vom 1. September 2009. Möglicherweise aufgrund der massiven Kritik an der Formulierung dieser Vorschrift hat die aktuelle Regierungskoalition aus Union und FDP in Berlin am 25. August 2010 – und damit nicht einmal ein Jahr nach Inkrafttreten der Norm – einen neuen Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes beschlossen.[1] Dessen § 32d lautet nunmehr wie folgt:

> (1) Der Arbeitgeber darf Beschäftigtendaten verarbeiten und nutzen, soweit
>
> (...) dies erforderlich ist zur Erfüllung der Zwecke, für die die Daten erhoben worden sind, oder zur Erfüllung anderer Zwecke, für die der Arbeitgeber sie nach den Vorschriften dieses Unterabschnitts hätte erheben dürfen und dies nach Art und Ausmaß im Hinblick auf den Zweck verhältnismäßig ist. (...)
>
> (3) Der Arbeitgeber darf zur Aufdeckung von Straftaten oder anderen schwerwiegenden Pflichtverletzungen durch Beschäftigte im Beschäftigungsverhältnis, insbesondere zur Aufdeckung von Straftaten nach den §§ 266, 299, 331 bis 334 des StGB, einen automatisierten Abgleich von Beschäftigtendaten in anonymisierter oder pseudonymisierter Form mit von ihm geführten Dateien durchführen. Ergibt sich ein Verdachtsfall, dürfen die Daten personalisiert werden (...)

Damit regelt der Entwurf explizit die auch den Schwerpunkt der vorliegenden Arbeit bildende Frage der Zulässigkeit von automatisierten Datenanalysen zur Aufdeckung von Rechtsverstößen.[2] Die vorliegende Untersuchung hat ungeachtet dessen eine ungebrochen praktische Relevanz, da zum einen auch unter dem eventuell zukünftigen Regime von § 32d BDSG-E der Nachweis der Verhältnismäßigkeit der Analyse der maßgebliche Faktor ist (siehe hierzu ausführlich die Abschnitte 4.2 und 4.3). Aus Unternehmenssicht können demnach nur mit äußerster Vorsicht gestaltete Datenanalysemaßnahmen in Betracht kommen. Zeitgleich setzt die Rechtsprechung weiterhin strenge Standards bezüglich interner Kontrollsysteme, wie etwa ein kürzlich veröffentlichtes Urteil des OLG Jena[3] zeigt. Das im Folgenden untersuchte Spannungsverhältnis wird somit aktuell bleiben.

Julian Schenten, Oktober 2010

---

1 Der Entwurfstext ist unter http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_Beschaeftigtendatenschutz.pdf?__blob=publicationFile abrufbar (Stand: 25.10.2010).

2 Die an die Analyse anschließenden Ermittlungsmaßnahmen sind von § 32 e BDSG-E erfasst.

3 *OLG Jena*, Urt. v. 12.08.2009 – 7 U 244/07 (nicht rechtkräftig), NZG 2010, 226.

Inhaltsverzeichnis III

Abkürzungsverzeichnis VI

1 Einleitung 1

1.1 Problemlage 1

1.2 Ziel der Arbeit und Eingrenzung des Themas 4

1.3 Methodisches Vorgehen 6

1.4 Aufbau der Arbeit 6

1.5 Glossar 7

1.5.1 Corporate Governance und Compliance 7

1.5.2 Internes Kontrollsystem 7

1.5.3 Fraud, Wirtschaftsdelikt, Straftat 8

1.5.4 Datenverarbeitende Stelle, Konzernleitung, Vorstand, Arbeitgeber 8

1.5.5 Arbeitnehmer, Beschäftigter, Betroffener 9

1.5.6 Personenbezogene Daten und der Umgang mit ihnen 9

2 Gesetzliche und andere Anforderungen an Unternehmen zur Errichtung interner Kontrollsysteme 11

2.1 Anforderungen aus dem deutschen Wirtschafts- und Gesellschaftsrecht, unter Berücksichtigung der europäischen Vorgaben 11

2.1.1 Überwachungspflicht und Haftung des Vorstands nach dem Aktiengesetz 11

2.1.1.1 Organisationspflicht des Vorstands: Errichtung eines Überwachungssystems 11

2.1.1.2 Sorgfaltspflicht und Verantwortung der Vorstandsmitglieder 14

2.1.1.3 Haftung des Vorstands 15

2.1.2 Überwachungspflicht und Haftung des Aufsichtsrates nach dem Aktiengesetz 17

2.1.2.1 Überwachung der Wirksamkeit des internen Kontrollsystems 17

2.1.2.2 Überprüfung von Konzernabschluss und –lagebericht 18

2.1.2.3 Haftung des Aufsichtsrates 19

2.1.3 Erklärung zum Deutschen Corporate Governance Index 20

2.1.3.1 Der Deutsche Corporate Governance Kodex 20

2.1.3.2 Auswirkungen für die Organe der Gesellschaft 21

2.1.4 Erwartungen an das Interne Kontrollsystem aus handelsrechtlicher Sicht 23

2.1.4.1 Konzernlagebericht 23

2.1.4.2 Feststellungen im Prüfungsbericht zur Wirksamkeit des Überwachungssystems 24

2.1.5 Branchenbezogene Spezialvorschriften mit Ausstrahlungswirkung auf andere Wirtschaftszweige 26

2.1.5.1 Technische Schutzmaßnahmen, § 109 TKG 26

2.1.5.2 Spezialvorschriften des KWG i.V.m. MaRisk 27

2.1.5.3 Basel II 28

2.1.5.4 Organisationspflichten, § 33 WpHG 28

2.2 Ordnungswidrigkeit der Verletzung von Aufsichtspflichten 29

2.3 Der Sarbanes-Oxley Act: Erweiterte Offenlegung von Unternehmensdaten und interne Kontrollsysteme 30
2.3.1 Anwendungsbereich 32
2.3.2 Pflichten der Geschäftsführung 33
2.3.2.1 Organisationspflichten 33
2.3.2.1.1 Disclosure controls and procedures 34
2.3.2.1.2 Internal control over financial reporting 34
2.3.2.2 Jahresabschlussbericht und Bestätigungserklärung 35
2.3.2.2.1 Beurteilungspflichten im Jahresabschlussbericht 35
2.3.2.2.2 Bestätigungserklärung nach sec. 302 SOA 36
a) Inhalt der Bestätigungserklärung 36
b) Mögliche Rechtsfolge bei unwahrer Bestätigungserklärung 37
2.3.2.2.3 Bestätigungserklärung nach sec. 906 SOA 38
2.3.3 Abschlussprüferbericht 38
2.4 Zusammenfassende Anforderungen an das interne Kontrollsystem 39
3 Datenschutzrechtliche Vorgaben 43
3.1 Anwendbarkeit bereichsspezifischer Regelungen aus TKG und TMG 43
3.2 Anwendbarkeit des BDSG 44
3.3 Grundsätze des Datenschutzrechts 44
3.4 Ermächtigungsgrundlagen für die Verwendung personenbezogener Beschäftigtendaten 46
3.4.1 Einwilligung des betroffenen Beschäftigten 47
3.4.2 Betriebsvereinbarung 49
3.4.3 Erhebung, Verarbeitung und Nutzung personenbezogener Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses im Allgemeinen, § 32 Abs. 1 Satz 1 BDSG 51
3.4.3.1 Die Ermächtigungsgrundlagen im Einzelnen 52
3.4.3.1.1 Begründung des Beschäftigungsverhältnisses 52
3.4.3.1.2 Durchführung des Beschäftigungsverhältnisses 53
3.4.3.1.3 Beendigung des Beschäftigungsverhältnisses 54
3.4.3.2 Erforderlichkeit 54
3.4.3.2.1 Der datenschutzrechtliche Begriff der Erforderlichkeit 55
3.4.3.2.2 Anknüpfungspunkt für die Erforderlichkeit 57
3.4.4 Erhebung, Verarbeitung und Nutzung personenbezogener Beschäftigtendaten gemäß § 32 BDSG im Besonderen zur Aufdeckung und Prävention von Straftaten und anderen Rechtsverstößen 58
3.4.4.1 Anwendung von § 32 Abs. 1 Satz 2 BDSG zur Aufdeckung von Straftaten 58
3.4.4.1.1 Aufdeckung 59
3.4.4.1.2 Straftat im Beschäftigungsverhältnis 59
3.4.4.1.3 Tatsächliche zu dokumentierende Anhaltspunkte, die den Verdacht einer Straftat begründen 60
3.4.4.1.4 Verhältnismäßigkeit 62
a) Geeignetheit 63
b) Erforderlichkeit 63
c) Angemessenheit 64
i. Rechte der Arbeitnehmer 64
ii. Rechte der Arbeitgeber 65
iii. Praktische Konkordanz 66

3.4.4.2 Anwendung von § 32 Abs. 1 Satz 1 BDSG zur Prävention von Straftaten 67
3.4.4.3 Würdigung 68
3.4.5 Datenerhebung und –speicherung für eigene Geschäftszwecke 71

4 Unternehmensinterne Kontroll-Maßnahmen und ihre Beurteilung nach deutschem Datenschutzrecht 72

4.1 Grundlegende organisatorische Kontroll-Maßnahmen des Anti-Fraud-Managements ... 73
4.2 Präventive Datenanalysen 76
4.2.1 Beschreibung des Vorgangs: Abgleich von Mitarbeiter- und Lieferantendaten zur Aufdeckung von Fraud 76
4.2.2 Datenschutzrechtliche Überprüfung 79
4.2.2.1 Zulässigkeit der Verwendung der Lieferantendaten 79
4.2.2.2 Zulässigkeit der Verwendung der Beschäftigtendaten 79
4.2.2.2.1 Ermächtigungsgrundlage 80
4.2.2.2.2 Verhältnismäßigkeit 81
a) Geeignetheit 81
b) Erforderlichkeit 81
c) Angemessenheit 83
i. Praktische Konkordanz 84
ii. Würdigung des Urteils vom ArbG Berlin zur Massendatenanalyse der Bahn AG 88
iii. Würdigung der Vorgaben aus der jüngeren Rechtsprechung des BVerfG 90
iv. Würdigung der Vorgaben des europäischen Gemeinschaftsrechts 94
4.2.3 Rechte der Arbeitnehmervertretung 97
4.2.4 Schlussfolgerungen 99
4.3 Aufdeckung bereits begangener Straftaten 101
4.3.1 Beschreibung des Vorgangs: Weiterverfolgung der Verdachtsmomente, welche durch die in Abschnitt 4.2.1 beschriebene Datenanalyse gewonnen wurden 101
4.3.2 Rechtliche Überprüfung 102
4.3.2.1 Arbeitsvertrag, Hausrecht und Direktionsrecht des Arbeitgebers 102
4.3.2.2 Datenschutzrechtliche Überprüfung 104
4.3.2.2.1 Aufdeckung 105
4.3.2.2.2 Straftat im Beschäftigungsverhältnis 105
4.3.2.2.3 Tatsächliche zu dokumentierende Anhaltspunkte, die den Verdacht einer Straftat begründen 106
4.3.2.2.4 Verhältnismäßigkeit 107
4.3.2.3 Rechte der Arbeitnehmervertretung 109
4.3.2.4 Schlussfolgerungen 110

5 Zusammenfassung und Handlungsempfehlung 112

5.1 Zusammenfassung 112
5.2 Handlungsempfehlung 114

6 Literatur- und Quellenverzeichnis 117

Abkürzungsverzeichnis

a.A.	anderer Ansicht
a.a.O.	am angegebenen Ort
a.F.	alte Fassung
ABlEG	Amtsblatts der Europäischen Gemeinschaft
ABlEU	Amtsblatts der Europäischen Union
Abs.	Absatz
AFM	Anti Fraud Management
AG	Aktiengesellschaft
AGG	Allgemeines Gleichheitsgesetz
AktG	Aktiengesetz
Alt.	Alternative
Anm.	Anmerkung
APR	Allgemeines Persönlichkeitsrecht
ArbG	Arbeitsgericht
Art.	Artikel
AT	allgemeiner Teil
Aufl.	Auflage
BaFin	Bundesamt für Finanzdienstleistungsaufsicht
BAG	Bundesarbeitsgericht
BB	Betriebs-Berater
BC	Zeitschrift für Bilanzierung, Rechnungswesen und Controlling
Bd.	Band
BDSG	Bundesdatenschutzgesetz
bearb. v.	bearbeitet von
BeckOK	Beck Online-Kommentar
Beschl.	Beschluss
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGH	Bundesgerichtshof
BilMoG	Bilanzrechtsmodernisierungsgesetz

BKA	Bundeskriminalamt
BKR	Zeitschrift für Bank und Kapitalmarktrecht
BLZ	Bankleitzahl
BT-Drucks.	Bundestags-Drucksache
BvD	Berufsverband der Deutschen Datenschützer e.V.
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
bzw.	beziehungsweise
CCZ	Corporate Compliance Zeitschrift
CEO	Chief Executive Officer
CFO	Chief Financial Officer
COSO	Committee of Sponsoring Organizations of the Threadway Commission
CR	Computer und Recht
CuA	Computer und Arbeit
d.h.	das heißt
DB	Der Betrieb
DCGK	Deutscher Corporate Governance Kodex
DCP	Disclosure Controls and Procedures
dies.	dieselben
DIIR	Deutsches Institut für interne Revision e.V.
DIN	Deutsches Institut für Normung
DSB	Datenschutzberater
DStR	Deutsches Steuerrecht
DStZ	Deutsche Steuerzeitung
DuD	Zeitschrift für Datenschutz und Datensicherheit
e.V.	eingetragener Verein
EDV	elektronische Datenverarbeitung
EGBGB	Einführungsgesetz zum BGB
ErfKomm	Erfurter Kommentar zum Arbeitsrecht
etc.	et cetera
EVÜ	Europäisches Schuldvertragsübereinkommen

EWG	Europäische Währungsgemeinschaft
f.	folgende (Einzahl)
FAZ	Frankfurter Allgemeine Zeitung
ff.	folgende (Mehrzahl)
GDD	Gesellschaft für Datenschutz und Datensicherheit e.V.
gemäß	gemäß
GewO	Gewerbeordnung
GG	Grundgesetz
GmbH	Gesellschaft mit beschränkter Haftung
GPS	Global Positioning System
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
h.M.	herrschende Meinung
HGB	Handelsgesetzbuch
Hrsg.	Herausgeber
hrsg. v.	herausgegeben von
i.d.R.	in der Regel
i.e.S.	im engeren Sinne
i.S.d. / v.	Im Sinne des / von
i.V.m.	in Verbindung mit
ICFR	Internal Control over Financial Reporting
IDW	Institut der Wirtschaftsprüfer
IEC	International Electrotechnical Commission
IKS	Internes Kontrollsystem
ISBR	Informationelles Selbstbestimmungsrecht = Recht auf informationelle Selbstbestimmung
ISO	International Standards Organisation
IT	Informationstechnologie
jurisPR-ITR	Juris Praxisreport IT-Recht
K&R	Kommunikation & Recht
KK-StPO	Karlsruher Kommentar zur StPO
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

KWG	Kreditwesengesetz
L.	législation
LAG	Landesarbeitsgericht
LG	Landgericht
Lit.	Buchstabe
m.w.N.	mit weiteren Nachweisen
MaRisk	Mindestanforderungen an das Risikomanagement
MiFID	Markets in Financial instruments Directive
Mio.	Millionen
MMR	Multimedia und Recht
MünchKomm	Münchner Kommentar
NJOZ	Neue Juristische Online-Zeitschrift
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NZA	Neue Zeitschrift für Arbeitsrecht
NZG	Neue Zeitschrift für Gesellschaftsrecht
o. Fußn.	oben Fußnote
OLG	Oberlandesgericht
OWiG	Ordnungswidrigkeitengesetz
PCAOB	Public Company Accounting Oversight Board
PS	Prüfstandard
Rn.	Randnummer
RDV	Recht der Datenverarbeitung
RFID	Radio Frequency Identification
Rspr.	Rechtsprechung
S.	je nach Zusammenhang: Seite oder Satz
SEA	Secureties Exchange Act
SEC	Secureties and Exchange Commission
sec.	section
SOA	Sarbanes-Oxley Act
sog.	so genannt(e)
st. Rspr.	ständige Rechtsprechung
StGB	Strafgesetzbuch

StPO	Strafprozessordnung
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TransPuG	Transparenz- und Publizitätsgesetz
u.a.	unter anderem
U.S.A.	United States of America
Urt.	Urteil
v.	vom
VAG	Versicherungsaufsichtsgesetz
VG	Verwaltungsgericht
vgl.	vergleiche
VO	Verordnung
vorauss.	voraussichtlich
WP	Working Paper = Arbeitspapier
WpHG	Wertpapierhandelsgesetz
z.B.	zum Beispiel
Zif.	Ziffer
ZIS	Zeitschrift für internationale Strafrechtsdogmatik
ZRFC	Zeitschrift Risk, Fraud und Compliance

1
Einleitung

1.1
Problemlage

Die Wirtschaftskriminalität stieg in den letzten Jahren offenbar signifikant an. Laut einer Studie aus dem Jahre 2009 waren zwischen den Jahren 2007 und 2009 61 % aller deutschen Großunternehmen von Wirtschaftsdelikten wie Betrug, Unterschlagung und Korruption betroffen.[4] Dies deckt sich mit den Ergebnissen einer Untersuchung des Bundeskriminalamts für das Jahr 2008, wonach die Zahl der polizeilich bekannt gewordenen Korruptionsfälle im Bereich der Privatwirtschaft stark anstieg.[5] Allein im Jahr 2009 soll sich der durch aufgedeckte Delikte verursachte finanzielle Schaden auf 5,57 Millionen EUR pro geschädigtes Unternehmen belaufen haben.[6] Hinzu kommen die im Rahmen der Aufdeckung der Delikte entstehenden Kosten, welche im Durchschnitt bei 830.000 EUR pro Unternehmen liegen, und die mittelbaren Schäden wie Rufschädigungen oder der Rückgang des Aktienkurses bei börsennotierten Unternehmen.[7] Alleine diese Zahlen belegen den Handlungsbedarf aufseiten der betroffenen Unternehmen, der hinsichtlich der Verhinderung von Wirtschaftsdelikten besteht.

Daneben existiert eine Reihe von gesetzlichen Vorschriften, aus denen sich Pflichten für die Unternehmen ergeben, Straftaten und andere Rechtsverstöße innerhalb des Betriebs zu verhindern. Ein Geschäftsinhaber begeht nach § 130 Abs. 1 OWiG eine Ordnungswidrigkeit, wenn innerhalb des Unternehmens Straftaten oder bußgeldbewehrte Verstöße begangen werden, die er bei Beachtung seiner Aufsichtspflicht hätte verhindern können. Ferner verpflichtet § 91 Abs. 2 AktG Vorstände deutscher Aktiengesellschaften, Überwachungssysteme einzurichten, die geeignet sind, den Fortbestand der Gesellschaft gefährdende Risiken frühzeitig zu erkennen. Neben dem Vorstand ist in diesem Zusammenhang auch der Aufsichtsrat einem erhöhten Haftungsrisiko ausgesetzt, wenn entsprechende Kontrollmaßnahmen nicht ergriffen werden. Handelsrechtliche Vorschriften ergänzen diese Anforderungen.

---

4 *PWC/Martin Luther Universität Halle-Wittenberg*, Wirtschaftskriminalität 2009, S. 11. Im Vergleichszeitraum zwischen den Jahren 2005 und 2007 lag die Quote noch bei 49%.

5 *BKA*, Korruption - Bundeslagebild 2008, Pressefreie Kurzfassung, S. 16.

6 *PWC/Martin Luther Universität Halle-Wittenberg, 2009* (o. Fußn. 4), S. 12. Die vorangegangene Studie von 2007 bezifferte den Gesamtschaden auf geschätzte 6 Milliarden EUR. Alle diese Summen stellen ferner die Untergrenze für den zu schätzenden Gesamtschaden dar, da etwa die durch unaufgedeckte Delikte entstandenen Einbußen nicht kalkulierbar sind.

7 PWC/Martin Luther Universität Halle-Wittenberg, 2009 a.a.O., S. 13 f.

Überdies wurden als Reaktion auf die großen Unternehmensskandale um Bilanzfälschungen in den Jahren 2001 und 2002 in den U.S.A.[8] umfangreiche Regelungen verabschiedet, welche das Ziel haben, den Anteilseignern der Gesellschaften Schutz zu gewähren. Im Juli 2002 trat der Sarbanes-Oxley Act in Kraft, ein U.S. Bundesgesetz, welches auch für ausländische, an U.S.-Börsen notierte Unternehmen Anwendung findet und welches durch ein erhöhtes Haftungsrisiko aufseiten des Vorstands betroffener Betriebe eine umfassende Transparenz der Jahresabschlussprüfungen bewirkte.

Auch auf EU-Ebene wurden verschiedene Richtlinien verabschiedet, welche denselben Zweck verfolgen[9] und mittlerweile größtenteils in deutsches Recht umgesetzt wurden. Verschärfend kommt hinzu, dass sowohl nach deutschem, als auch nach amerikanischem Recht, der Wirtschaftsprüfer im Rahmen der Jahresabschlussprüfung zu bestätigen hat, ob die vom Vorstand ergriffenen Maßnahmen zur Verhinderung von Straftaten und anderen Verstößen mit Mängeln behaftet sind, bzw. ob sie wirksam arbeiten.

Alle diese Maßnahmen verweisen auf die zwei zentralen Begriffe *Corporate Governance* und *Compliance*.[10] Um den Anforderungen aus Corporate Governance und Compliance, die sich unter anderem aus den oben genannten Vorschriften ergeben, gerecht zu werden, sind Unternehmen zum Aufbau von *internen Kontrollsystemen* (IKS) gezwungen, mit deren Hilfe sie selbstständig oder unter Zuhilfenahme professioneller Dienstleistungsunternehmen, Gefahren für die Gesellschaft zu verhindern suchen. Teil des IKS ist das unternehmensweit durchzuführende *Anti Fraud Management* (AFM). Unter AFM wird die Gesamtheit der Maßnahmen zur Vorbeugung, Aufdeckung und Reaktion im Zusammenhang mit wirtschaftskriminellen Handlungen verstanden. Dabei spielt die Bekämpfung der eingangs erwähnten Wirtschaftsdelikte wie Korruption, Insidergeschäfte und Unterschlagung, welche unter dem Begriff *Fraud* zusammengefasst werden, eine herausragende Rolle.

Um diesen auch strafrechtlich relevanten Handlungen Einhalt zu gebieten, sind die Unternehmen im Rahmen ihrer internen Überwachungsmaßnahmen gegebenenfalls zur Kontrolle der Arbeitnehmer verpflichtet, etwa durch Befragungen der Angestellten, offene oder verdeckte Videoüberwachung, eine Überprüfung der Telefon- und E-Mail-Korrespondenz oder die automatisierte Analyse größerer Datenbestände,[11] beispielsweise um verdächtige, auf einen Missbrauch hindeutende Kontobewegungen zu erfassen. Dabei ist zwischen Handlungen zur Prävention und Handlungen zur Aufdeckung von Missbrauchsfällen (*Fraud-Prevention* bzw. -*Detection)* zu unterscheiden. Insgesamt

---

8 Übersicht unter http://www.heise.de/newsticker/meldung/Hintergrund-Bilanzskandale-in-den-USA-64933.html (Stand: 21.02.2010).

9 Etwa die sog. Abschlussprüfer-, Änderungs-, Banken- und Kapitaladäquanzrichtlinien.

10 Siehe Definition in Abschnitt 1.5.1.

11 Sog. „*Massenscreenings*". Der Begriff bezeichnet den systematischen Abgleich großer Datensätze mittels EDV.

sind die genannten Maßnahmen nötig, weil die meisten aufgedeckten Fälle von Fraud auf unternehmensinterne Täter zurückzuführen sind.[12]

Unter anderem[13] löste die Durchführung dieser Maßnahmen jedoch in der jüngeren Vergangenheit zahlreiche sog. „*Datenskandale*" aus, verursacht durch prominente Unternehmen wie *Lidl*[14], *Edeka*[15], *Deutsche Telekom*[16], *Deutsche Bank*[17] und *Deutsche Bahn*[18]. Um Korruption und andere strafbare Handlungen seitens der Arbeitnehmer erfolgreich zu bekämpfen, wurden offenbar Verletzungen des Persönlichkeitsrechts der Arbeitnehmer sowie des Datenschutzrechts in Kauf genommen.

Das Bundesdatenschutzgesetz (BDSG) findet gemäß § 1 Abs. 2 BDSG Anwendung, sobald personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Ferner ist eine Datenerhebung, -verarbeitung und -nutzung nach dem BDSG grundsätzlich verboten, es sei denn, der Betroffene hat dem zugestimmt oder ein Gesetz enthält einen Erlaubnistatbestand. Mit der Novellierung des BDSG zum 01. September 2009 hat sich die Lage für die Unternehmen nach einer verbreiteten Auffassung noch weiter zugespitzt: Der neue § 32 BDSG regelt als Spezialnorm die Datenverwendung in Beschäftigungsverhältnissen und hat wegen seiner sprachlichen Unbestimmtheit, insbesondere im Hinblick auf die Zulässigkeit präventiver Maßnahmen zur Verhinderung von Straftaten und anderen Rechtsverstößen, viel Kritik aus der juristischen Literatur erfahren.[19] Ein Urteil[20] des ArbG Berlin vom 18. Februar 2010, wel-

---

12 *KPMG*, Wirtschaftskriminalität in Deutschland, 2010, S. 20.

13 Andere Ursachen waren z.B. sog. "Datenpannen", bei denen Datenträger mit großen Datensätzen von Kunden verloren gingen, oder die umfassend angelegte Bespitzelung von hochrangigen Vertretern des Betriebsrats, um Kontakte zu Journalisten aufzudecken.

14 http://www.heise.de/newsticker/meldung/Datenschutzverletzungen-Lidl-faellt-als-Wiederholungstaeter-auf-192822.html (Stand: 21.02.2010).

15 http://www.heise.de/newsticker/meldung/Mitarbeiter-Bespitzelung-im-Handel-Auch-Edeka-und-Plus-im-Visier-195390.html (Stand: 21.02.2010).

16 http://www.heise.de/newsticker/meldung/Nach-neuer-Telekom-Datenpanne-Kritik-an-Konzernfuehrung-waechst-210873.html (Stand: 21.02.2010).

17 http://www.heise.de/newsticker/meldung/Datenschutz-Affaere-im-Machtzirkel-der-Deutschen-Bank-220081.html (Stand: 21.02.2010).

18 http://www.heise.de/newsticker/meldung/Bericht-Datenschuetzer-wirft-Bahn-Gesetzesverstoesse-vor-212222.html (Stand: 21.02.2010).

19 *Albrecht*, jurisPR-ITR 20/2009, Anm. 2, S. 2 ff.; *Barton*, RDV 2009, 200 (201 f.); *Bierekoven*, CR 2010, 203 (208); *Deutsch/Diller*, DB 2009, 1462 (1465); *Erfurth*, NJOZ 2009, 2914 (2919 f.); *Grentzenberg/Schreibauer/Schuppert*, K&R 2009, 535 (538 ff.); *Thüsing*, NZA 2009, 865 (868); *Vogel/Glas*, DB 2009, 1747 (1750 f.); Stellungnahme des *Deutschen Anwaltvereins*, Nr. 2/2010 zum Arbeitnehmerdatenschutz, http://anwaltverein.de/interessenvertretung/stellungnahmen+2 (Stand: 23.03.2010); vgl. ferner die Pressemitteilung von *Transparency International Deutschland e.V.* v. 30.06.2009, http://www.transparency.de/09-06-30_Datenschutz.1438.0.html (Stand: 15.12.2009).

20 *ArbG Berlin*, Urt. v. 18. Februar 2010, Aktenzeichen 38 Ca 12879/09, nicht rechtskräftig, http://www.gerichtsentscheidungen.berlin-brandenburg.de/jportal/portal/t/d4p/bs/10/page/sammlung.psml;jsessionid=5EDBD74815B5C37A8DB8E34D44BFE9C0.jp95_2?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnum-

ches sich mit den in der Öffentlichkeit hitzig diskutierten Massendatenanalysen der *Bahn AG*[21] befasst, kann in diesem Zusammenhang jedoch als erste Orientierungshilfe herangezogen werden.

Schließlich sind die Rechte der Arbeitnehmervertretung zu beachten, da etwa die Einführung und Anwendung von technischen Überwachungseinrichtungen gemäß § 87 Abs. 1 Satz 1 Nr. 6 BetrVG ein Mitbestimmungsrecht des Betriebsrats auslösen.

1.2
Ziel der Arbeit und Eingrenzung des Themas

Dem Konflikt, der aus den Anforderungen des deutschen Datenschutzrechts und des deutschen und internationalen Kapital- und Wirtschaftsrechts erwächst, widmet sich die vorliegende Arbeit. Im Mittelpunkt steht folgende Frage:

> Welche Maßnahmen kann und muss ein deutscher, auch in den U.S.A. operierender und börsennotierter IT-Dienstleistungskonzern in der Rechtsform einer Aktiengesellschaft durchführen, um sowohl den deutschen und amerikanischen Anforderungen an Corporate Governance und Compliance als auch den Bestimmungen des deutschen Datenschutzrechts gerecht zu werden?

Die bereits existierenden Checklisten zur bestmöglichen Errichtung eines durchsetzungsfähigen IKS[22] lassen den Arbeitnehmerdatenschutz zumeist völlig außer Acht. Daher ist das Ziel dieser Arbeit, eine umfassende Abwägung durchzuführen zwischen den Interessen der Unternehmen auf der einen Seite, insbesondere die Erhaltung des eingerichteten und ausgeübten Gewerbebetriebs sowie die damit verbundenen Pflichten, und den schutzwürdigen Interessen des Arbeitnehmers auf der anderen Seite, nämlich die Wahrung seiner grundrechtlich geschützten Persönlichkeitsrechte. Diese Abwägung geschieht anhand einer beispielhaft durchgeführten datenschutzrechtlichen Überprüfung einer automatischen Datenanalyse zur Verhinderung von Wirtschaftsdelikten. Im Ergebnis soll dem Leser eine Anleitung an die Hand gegeben werden, mit deren Befolgung er beiden entgegenstehenden Interessen zur Genüge Rechnung trägt.

Ausgangspunkt für die Überlegungen ist die Situation eines weltweit operierenden Dienstleistungskonzerns mit Mitarbeitern im sechsstelligen Bereich und Umsätzen im Milliardenbereich. Die Eingrenzung auf einen in Deutschland und den U.S.A. börsennotierten Konzern bietet sich an, da sich in diesem Zusammenhang die Analyse der aus deutscher Sicht meist diskutierten Vorschrif-

---

ber=1&numberofresults=1&fromdoctodoc=yes&doc.id=KARE600029371&doc.part=L&doc.price=0.0#focuspoint (Stand: 22.05.2010).

21 Eine ausführliche Chronik der Ereignisse gibt *Albers*, Compliance der Compliance, S. 5 ff., http://fhdd.opus.hbz-nrw.de/volltexte/2009/508/ (Stand: 27.04.2010).

22 *Hauschka/Greeve*, BB 2007, 165 (169) m.w.N.

ten zu Corporate Governance und Compliance aus dem deutschen Aktiengesetz und dem amerikanischen Sarbanes-Oxley Act empfiehlt. Die thematische Ausrichtung auf einen Konzern ist der Tatsache geschuldet, dass die Wahrscheinlichkeit von Wirtschaftsdelikten mit der Größe des Unternehmens steigt.[23] Die Darstellung der aktuellen Situation für Gesellschaften mit beschränkter Haftung wird vollständig ausgelassen.

Aus der Fokussierung auf ein Unternehmen aus der IT-Branche folgt, dass prinzipiell für das Thema dieser Arbeit relevante Spezialvorschriften aus anderen Wirtschaftszweigen lediglich auf eventuelle Ausstrahlungswirkungen hin untersucht werden. Ferner waren einer Studie aus dem Jahre 2007 zufolge immerhin rund 40% der deutschen Unternehmen aus den Bereichen (Tele)-Kommunikation und Technologie Opfer von wirtschaftskriminellen Handlungen.[24]

Bei der Beurteilung, welche Kontroll-Maßnahmen für die Praxis des IT-Dienstleistungskonzerns relevant und daher Gegenstand der Untersuchung sind, erscheint es bei der weiteren Eingrenzung des Untersuchungsgegenstandes sinnvoll, auf die Sicht des Abschlussprüfers abzustellen. Dieser hat nach verschiedenen, im Verlauf der Arbeit noch im Detail zu klärenden Vorschriften, insbesondere aus dem Handelsgesetzbuch und dem Sarbanes-Oxley Act, die Wirksamkeit des IKS zu bestätigen. Lediglich jene Kontrollmaßnahmen, die im Hinblick auf die Feststellung des Abschlussprüfers relevant sind, sind Teil der Untersuchung. Aus diesem Grund wird etwa nicht Gegenstand der Arbeit sein, ob die Maßnahmen zur Aufdeckung unrechtmäßiger Nutzungen der vom Arbeitgeber bereitgestellten Kommunikationsmittel rechtmäßig sind. Dagegen stehen Kontrollmaßnahmen im Bereich des Finanz- und Rechnungswesens im Vordergrund der Untersuchung, insbesondere da dieser Unternehmenszweig in den letzten Jahren einer steigenden Zahl von Wirtschaftsdelikten ausgesetzt war.[25] Ein besonderer Fokus wird auf die Frage der datenschutzrechtlichen Zulässigkeit von verdachtsunabhängigen Datenanalysen gesetzt, welche sowohl zur Verhinderung als auch zur Aufdeckung von Straftaten geeignet sind. Welche arbeits-, zivil- und/oder strafrechtlichen Sanktionen dem Arbeitgeber gegen den von ihm beschäftigten und der Tat überführten Täter eines Wirtschaftsdelikts zustehen, ist nicht Gegenstand der Betrachtung.

---

23 PWC/Martin Luther Universität Halle-Wittenberg, Wirtschaftskriminalität 2007, S. 10.
24 PWC/Martin Luther Universität Halle-Wittenberg, 2007 a.a.O., S. 14.
25 *KPMG,* 2010 (o. Fußn. 12), S. 9.

1.3
Methodisches Vorgehen

Methodisch bedient sich die Arbeit zunächst der theoretischen juristischen Analyse. Die wesentlichen Anforderungen aus den Bereichen Datenschutz und Corporate Governance und Compliance werden durch eine Auswertung der einschlägigen Gesetzesmaterialien und der zu den Themenkomplexen ergangenen Rechtsprechung und Literatur zusammengetragen. Praxisbezug erhält die Arbeit durch die Berücksichtigung von Studien zur Wirtschaftskriminalität, welche von Unternehmensberatungs- bzw. Wirtschaftsprüfungsgesellschaften wie PWC und KMPG herausgegeben wurden. Die Beschreibung eines automatisierten Datenabgleichs entstand in Zusammenarbeit mit Fachleuten aus der IT-Praxis.

Abschnitt 1.5 enthält ein Glossar mit den für die vorliegende Arbeit wichtigsten Begriffsbestimmungen. Darüber hinaus finden sich im gesamten Verlauf der Arbeit vereinzelte Definitionen von Fachbegriffen, für welche eine Erläuterung zum Zeitpunkt der Einführung des Begriffs genügt. Alle erläuterten Begriffe werden im Anschluss an ihre Definition gemäß dieser verwendet.

Die Einleitungen der einzelnen Abschnitte enthalten jeweils weitere Details zum konkreten methodischen Vorgehen.

1.4
Aufbau der Arbeit

Zunächst sind in Abschnitt 2 die wesentlichen gesetzlichen Anforderungen zur Errichtung IKS und in Abschnitt 3 die entgegenstehenden Vorgaben aus dem BDSG vorzustellen. Im Vordergrund der Arbeit steht die Frage nach der Zulässigkeit verdachtsunabhängiger Datenanalysen. In Abschnitt 3 werden die zur Klärung dieser Frage notwendigen datenschutzrechtlichen Grundsätze im Beschäftigungsverhältnis erst einmal umfassend erläutert. Im nachfolgenden Abschnitt 4 wird dargestellt, welche Maßnahmen die Unternehmensleitung im Rahmen ihrer Pflichten durchzuführen hat. Die zuvor gewonnen Erkenntnisse bezüglich der datenschutzrechtlichen Vorgaben werden auf ausgewählte Kontroll-Maßnahmen angewandt. Deren Vereinbarkeit mit dem deutschen Datenschutzrecht wird diskutiert. Im Rahmen der datenschutzrechtlichen Beurteilung wird zudem jeweils ein kurzer Überblick über die einschlägigen Beteiligungsrechte der Arbeitnehmervertretung gegeben. Im letzten Abschnitt 5 folgt schließlich eine Zusammenfassung der durch die Untersuchung gewonnenen Erkenntnisse. Ferner wird eine Handlungsempfehlung gegeben, wie sich verdachtsunabhängige Datenanalysen gestalten lassen, ohne dass es zu unzulässigen Eingriffen in die Persönlichkeitsrechte der Arbeitnehmer kommt. Diese Empfehlung lässt sich entsprechend auf andere Maßnahmen anwenden.

1.5
Glossar

Nachfolgend sollen die für die vorliegende Arbeit wesentlichsten Begriffe erläutert werden. Dies ist insbesondere im Hinblick auf die spezielle Terminologie des BDSG erforderlich. Die Abfolge der Definitionen orientiert sich nach deren sinnhaften Zusammenhängen.

1.5.1
Corporate Governance und Compliance

Während eine exakte Übersetzung von Corporate Governance ins Deutsche nicht ohne Weiteres möglich ist, existiert eine Reihe von Definitionen, wofür der Begriff inhaltlich steht.[26] Nach einem eher allgemeinen Verständnis verbirgt sich dahinter die „Unternehmensverfassung", welche den Ordnungsrahmen für die Leitung und Überwachung eines Unternehmens darstellt.[27] Etwas konkreter ausformuliert steht Corporate Governance für eine verantwortliche und auf langfristige Wertschöpfung zielende Unternehmensführung sowie Unternehmenskontrolle, welche die Rechte, Pflichten und Verantwortlichkeiten aller Gesellschaftsorgane, Anteilseigner und Mitarbeiter beachtet.[28] In engem sachlichen Zusammenhang[29] zur Corporate Governance steht der Begriff der Compliance, bzw. auf das gesamte Unternehmen oder den Konzern bezogen, Corporate Compliance, worunter man im Allgemeinen sämtliche organisatorischen Maßnahmen zusammenfasst, mit denen ein Unternehmen innerbetrieblich gewährleistet, dass die geltenden Gebote und Verbote auch beachtet werden.[30] Ziel der Compliance ist die Vermeidung von durch Mitarbeiter oder Organe der Gesellschaft begangenen Regelverstößen, welche negative wirtschaftliche Konsequenzen für das Unternehmen haben können.[31]

1.5.2
Internes Kontrollsystem

Eine universelle Definition des Begriffs ist nicht möglich, da jedes Unternehmen ein für seine konkrete Situation angemessenes Modell des IKS zu wählen hat. Welches dies im Falle des betrachteten Konzerns ist, soll in Abschnitt 2 untersucht werden.

---

26 *Knapp*, Interne Revision und Corporate Governance, S. 57 ff.
27 *Hauschka*, in: *Hauschka* (Hrsg.), Corporate Compliance, § 1, Rn. 1.
28 *Knapp* (o. Fußn. 26), S. 59.
29 Zur Abgrenzung der Begriffe siehe *Hauschka* in: *Hauschka* (o. Fußn. 27), Rn. 3 f.
30 *Wybitul*, BB 2009, 1582.
31 *Hauschka* in: *Hauschka* (o. Fußn. 27), Rn. 4.

1.5.3
Fraud, Wirtschaftsdelikt, Straftat

Ausgangspunkt für die vorliegende Untersuchung sind die zuletzt[32] gehäuft aufgetretenen Fälle von Betrug, Insiderhandel, Korruption, Unterschlagungen und Kartellverstößen. Im Allgemeinen werden diese und andere rechtswidrige Handlungen unter dem Begriff Fraud zusammengefasst, der eine vorsätzliche Handlung einer oder mehrerer Personen bezeichnet, die darauf abzielt, ungerechtfertigte oder rechtswidrige Vorteile zu erlangen.[33] Nicht alle Fälle von Fraud erfüllen zugleich den Tatbestand einer Straftat, sondern stellen zum Teil auch lediglich Vertragsverletzungen oder etwa Ordnungswidrigkeiten dar. Wo das Vorliegen der Tatbestandserfüllung einer Straftat i.S.d. StGB von Bedeutung ist, soll im Speziellen darauf eingegangen werden. Im Übrigen werden die Begriffe Fraud, Missbrauch, Wirtschaftsdelikt und Wirtschaftsstraftat gleichbedeutend verwendet.

1.5.4
Datenverarbeitende Stelle, Konzernleitung, Vorstand, Arbeitgeber

Zunächst handelt es sich bei dem der vorliegenden Untersuchung zugrunde liegenden Konzern um ein privatwirtschaftliches Unternehmen in der Gesellschaftsform der Aktiengesellschaft. Somit stellt der Konzern eine nichtöffentliche Stelle i.S.v. § 2 Abs. 4 BDSG dar,[34] woraus sich i.V.m. § 1 Abs. 2 Nr. 3 BDSG die allgemeine Anwendbarkeit des BDSG ergibt. Bei der Frage der Zulässigkeit von Maßnahmen mit datenschutzrechtlichen Implikationen kommt es zumeist auf eine Abwägung der Interessen des Betroffenen und der datenverarbeitenden Stelle an. Der Einfachheit halber werden die Interessen der datenverarbeitenden Stelle mit jenen der Konzernleitung gleichgestellt. Ferner hat der Großteil der in Abschnitt 2 dargestellten Vorschriften gemeinsam, dass sie den Vorstand als geschäftsführendes Organ des Konzerns verpflichten. Dieser führt die erwähnten Kontrollmaßnahmen naturgemäß nicht selbst aus, sondern delegiert seine Pflichten an das ihm unterstellte Aufsichtspersonal. Eine dahingehende Unterscheidung, wer konkret eine Handlung vollzieht, wird im Verlauf der Arbeit nicht gemacht. In den folgenden Ausführungen werden die Begriffe Vorstand, Konzern- bzw. Unternehmensleitung und Arbeitgeber gleichbedeutend verwendet.

---

32 Vergleiche etwa die Nachweise in den Fußn. 8 und 181.

33 *Menzies* (Hrsg.), Sarbanes-Oxley und Corporate Compliance, S. 94; in der Literatur wird ebenfalls oftmals von dolosen Handlungen gesprochen.

34 Hierbei handelt es sich um natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie keine öffentlichen Stellen des Bundes, der Länder oder Vereinigungen des privaten Rechts von öffentlichen Stellen i.S.v. § 2 BDSG darstellen.

1.5.5
Arbeitnehmer, Beschäftigter, Betroffener

Der Beschäftigtenbegriff des BDSG, der nicht mit jenem aus dem Sozialversicherungsrecht gleichzusetzen ist,[35] wird als Orientierungspunkt herangezogen. Das Gesetz listet in § 3 Abs. 11 BDSG als unter den Beschäftigtenbegriff fallende Personen insbesondere Arbeitnehmerinnen und Arbeitnehmer, Auszubildende, Bewerberinnen und Bewerber vor Begründung des Arbeitsverhältnisses, Personen, deren Beschäftigungsverhältnis beendet ist sowie Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind.[36] Hiervon sind Organmitglieder wie Vorstände oder Geschäftsführer abzugrenzen, welche keine Erwähnung in der Norm finden.[37] Sofern personenbezogene Daten von einer der von der Norm genannten Personengruppen verwendet werden, sind diese gleichzeitig Betroffene i.S.d. § 3 Abs. 1 BDSG. Die Begriffe Betroffener, Beschäftigter, Arbeitnehmer und Unternehmensangestellte sind für die folgenden Ausführungen gleichbedeutend.

1.5.6
Personenbezogene Daten und der Umgang mit ihnen

Bei Personenbezogenen Daten handelt es sich gemäß § 3 Abs. 1 BDSG um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Als Beispiele kommen Name, Geburtsdatum, Wohnadresse, Versicherungsnummer, Kontonummer, Ausweis-Nummern oder Videoaufnahmen eines Betroffenen in Betracht. Dabei ist der Personenbezug eines Datums relativ. Entscheidend ist, ob die verantwortliche Stelle über die entsprechenden Kenntnisse, Mittel oder Möglichkeiten verfügt, ohne unverhältnismäßigen Aufwand einen Personenbezug herzustellen.[38] Derselbe Maßstab gilt für pseudonymisierte Daten, bei welchen gemäß § 3 Abs. 6a BDSG der Name und andere Identifikationsmerkmale durch ein Kennzeichen ersetzt werden, zu dem Zweck die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. Kann die verantwortliche Stelle

---

35 BT-Drucks. 16/13657, S. 17.

36 Die letzte Kategorie umfasst damit auch die verbreitete Gruppe der sog. freien Mitarbeiter, *Däubler*, in: *Däubler/Klebe/Wedde/Weichert* (Hrsg.), BDSG, § 32 Rn. 4.

37 Damit fallen diese Personen nicht unter den Beschäftigtenbegriff, mit allen daraus folgenden Konsequenzen, *Salvenmoser/Hauschka*, NJW 2010, 331 (333). Gleiches gilt für Leiharbeitnehmer, da diese in keinem Beschäftigungsverhältnis mit der entleihenden Stelle stehen, sondern Arbeitnehmer der Unternehmen zur Vermittlung von Leiharbeitnehmern sind, *Gola/Schomerus* (Hrsg.), BDSG, § 32 Rn. 5.

38 *Gola/Wronka*, Handbuch zum Arbeitnehmerdatenschutz, Rn. 180; a.A. *Weichert,* in: *Däubler/Klebe/Wedde/Weichert* (o. Fußn. 36), § 3 Rn. 13, nach dem ein objektiver Maßstab angelegt werden muss und es bereits ausreicht, dass irgendeine andere, als die verantwortliche Stelle, den Personenbezug herstellen kann.

das Pseudonym dem Betroffenen direkt oder indirekt wieder zuordnen, handelt es sich hierbei ebenfalls um personenbezogene Daten.[39]

Ein Personenbezug ist jedoch regelmäßig bei aggregierten oder anonymisierten Daten zu verneinen, soweit die Möglichkeit zur Reidentifizierung einer Person ausgeschlossen ist. Dies ist gemäß § 3 Abs. 6 BDSG gewährleistet, wenn die personenbezogenen Daten derart verändert wurden, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

In der Terminologie des BDSG finden sich bezüglich der Handhabung von personenbezogenen Daten die Begriffe erheben[40], verarbeiten[41] und nutzen[42]. Als Oberbegriff für den Umgang mit Daten wird im Rahmen der vorliegenden Arbeit der Terminus *Verwendung* gebraucht.

[39] Weichert, in: Däubler/Klebe/Wedde/Weichert a.a.O., § 3 Rn. 51.

[40] Der Begriff bezeichnet das Beschaffen von Daten über den Betroffenen, § 3 Abs. 3 BDSG.

[41] Der Begriff bezeichnet das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten, § 3 Abs. 4 BDSG.

[42] Der Begriff bezeichnet jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt, § 3 Abs. 5 BDSG.

2
Gesetzliche und andere Anforderungen an Unternehmen zur Errichtung interner Kontrollsysteme

Wegen den zahlreichen in Frage kommenden Regelungen des deutschen und internationalen Wirtschaftrechts aus dem Bereich der Corporate Governance und Compliance, deren umfassende Darstellung den Rahmen einer Diplomarbeit bei weitem übersteigen würde, soll hier nur auf die in der Praxis relevantesten Vorschriften eingegangen werden.

2.1
Anforderungen aus dem deutschen Wirtschafts- und Gesellschaftsrecht, unter Berücksichtigung der europäischen Vorgaben

Aus deutscher Sicht enthalten insbesondere das Aktiengesetz (AktG) und das Handelsgesetzbuch (HGB) Anforderungen bezüglich der Errichtung interner Kontrollsysteme. Diese dienen überwiegend der Umsetzung verschiedener EU-Richtlinien. Wegen inhaltlichen Überschneidungen und Analogien zwischen aktien- und handelsrechtlichen Vorschriften ist eine klar getrennte Darstellung der Normen nicht immer möglich. Darüber hinaus sind entsprechende branchenbezogene Spezialvorschriften auf eventuelle Ausstrahlungswirkungen auf andere Wirtschaftszweige hin zu untersuchen.

2.1.1
Überwachungspflicht und Haftung des Vorstands nach dem Aktiengesetz

Aus § 76 Abs. 1 AktG ergibt sich eine Leitungspflicht für den Vorstand einer Aktiengesellschaft (AG). Diese Pflicht wird in § 91 Abs. 2 AktG dahingehend konkretisiert, dass der Vorstand Maßnahmen zum Schutz der Gesellschaft zu ergreifen hat. Dabei unterliegen die Handlungen der Vorstandsmitglieder der allgemeinen Sorgfaltspflicht und Verantwortlichkeit aus § 93 AktG.

2.1.1.1
Organisationspflicht des Vorstands: Errichtung eines Überwachungssystems

Gemäß § 91 Abs. 2 AktG hat der Vorstand geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Die Norm trat 1998 als Teil des KonTraG in Kraft,[43] welches vor dem Hintergrund zahlreicher Unternehmenskrisen und der sich immer stärker globalisierenden Kapitalmärkte zum Schutz der Anteilseigner der Gesellschaften die Haftung von

[43] Gesetz zur Kontrolle und Transparenz im Unternehmensbereich v. 27.04.1998, BGBl. 1998 I S. 786.

Vorständen, Aufsichtsräten und Wirtschaftsprüfern erweiterte.[44] Zweck der Vorschrift ist die Sicherstellung eines Organisationsstandards, der die rechtzeitige Erkennung bestandsgefährdender Entwicklungen erlaubt.[45] Diese Überwachungs- und Organisationspflicht bezieht sich überdies auf den gesamten Konzern.[46] Jedoch ist fraglich, welche Anforderungen an ein derartiges Überwachungssystem zu stellen sind, weshalb die Tatbestandsmerkmale der Norm im Einzelnen zu untersuchen sind.

Zunächst ist zu klären, welche Entwicklungen als den Fortbestand der Gesellschaft gefährdend zu qualifizieren sind. Die Gesetzesbegründung nennt in diesem Zusammenhang risikobehaftete Geschäfte, Unrichtigkeiten in der Rechnungslegung sowie Verstöße gegen gesetzliche Vorschriften, die sich wesentlich auf die Finanz-, Vermögens- oder Ertragslage der Gesellschaft auswirken.[47] Da auf den Fortbestand der Gesellschaft abgestellt wird, können nur solche Entwicklungen gemeint sein, die ein Insolvenzrisiko für das Unternehmen darstellen oder zumindest erhöhen, nicht jedoch bereits solche Veränderungen, die die Rentabilität der Gesellschaft beeinträchtigen, auch wenn diese auf lange Sicht ebenfalls das Ende des Unternehmens bedeuten könnten.[48] In der Praxis ist diese Unterscheidung jedoch unerheblich, da diejenigen Gefährdungen, die zwar kein Insolvenz-Risiko bedeuten, aber dennoch schädlich für das Unternehmen sind, vom Vorstand auf Grund seiner Sorgfaltspflicht aus § 93 Abs. 1 Satz 1 AktG zu beseitigen sind.[49] Wegen des zu erwartenden immensen Reputationsschadens im Zusammenhang mit Fällen von Korruption, könnte sich daher aus § 91 Abs. 2 AktG die Pflicht zur Verhinderung von derartigen Delikten innerhalb des Unternehmens ergeben.[50]

Die Geeignetheit der jeweiligen Maßnahme orientiert sich insbesondere an der Größe, Branche, Struktur und dem Kapitalmarktzugang des jeweiligen Unternehmens.[51] Vorherige Verdachtsmomente und Auffälligkeiten, also auf Fraud hindeutende Indikatoren wie Differenzen in der Rechnungslegung,[52] spielen ebenso eine Rolle und können etwa eine ständige Kontrolle zweckdienlicher als Stichproben erscheinen lassen.[53] Dabei handelt der Vorstand bei der Wahl der Maßnahmen grundsätzlich im Rahmen seines in § 93 Abs. 1 Satz 2 AktG kodifizierten Ermessens. In jedem Fall haben jene aber dazu geeignet zu sein, bestandsgefährdende Entwicklungen frühzeitig zu erkennen,

---

44 BT-Drucks. 13/9712, S. 11.
45 *Hüffer*, AktG, § 91 Rn. 1.
46 BT-Drucks. 13/9712, S. 15.
47 BT-Drucks. 13/9712, S. 15.
48 *Blasche*, CCZ 2009, 62 (63); *Spindler*, in: MünchKomm-AktG, § 91 Rn. 21.
49 *Spindler*, in: MünchKomm-AktG a.a.O., § 91 Rn. 22; siehe ferner Abschnitt 2.1.1.2.
50 So auch *Barton*, RDV 2009, 200 (201).
51 BT-Drucks. 13/9712, S. 15.
52 Siehe hierzu Abschnitt 4.1.
53 *Spindler*, in: MünchKomm-AktG (o. Fußn. 48), § 91 Rn. 19.

d.h. zu einem Zeitpunkt, an dem noch Gegenmaßnahmen zur Sicherung des Fortbestands der Gesellschaft ergriffen werden können.[54]

Im Allgemeinen besteht jedoch keine gesetzliche Verpflichtung, ein bestimmtes Frühwarnsystem oder darüber hinaus ein bestimmtes Risikomanagementsystem einzurichten,[55] da das zu installierende Überwachungssystem lediglich beispielhaft genannt wird („insbesondere"), womit prinzipiell jede andere Maßnahme, die den Zweck der Norm erreicht, genauso geeignet ist.[56] Ein bestimmtes Model vorauszusetzen, würde ferner dem Leitungsermessen des Vorstands und der ihm durch Art. 14 GG zustehenden Organisationsfreiheit entgegenstehen.[57]

In der Literatur bestehen zwei gegensätzliche Auffassungen über die Anforderungen an das Überwachungssystem. Das juristische Schrifttum legt § 91 Abs. 2 AktG eng aus und verlangt ein System der unternehmensinternen Kontrolle, welches zwar die Ergreifung geeigneter Maßnahmen zur Früherkennung vorsieht, das daneben zu implementierende, unternehmensinterne Überwachungssystem jedoch dahingehend versteht, dass lediglich die zu treffenden *Maßnahmen* auf ihre Funktionalität hin überwacht werden, also etwa ob Innenrevision und Controlling eine zeitnahe Meldung an den Vorstand zulassen.[58] Davon abzugrenzen sei ein Risikomanagement-System mit den Schwerpunkten Risikoidentifikation, -bewertung und -steuerung.[59]

Das betriebswirtschaftliche Schrifttum dagegen sieht in der Norm die Grundlage zur verpflichtenden Implementierung eines umfassenden Risikomanagementsystems, bestehend aus einem Frühwarnsystem, einem internen Überwachungssystem – bezogen auf die Überwachung von *Risiken* – und dem Controlling.[60] Ein solches System muss nach dem Mindeststandard der betriebswirtschaftlichen Lehre die Risikoidentifikation und -analyse, die Bewertung und Kommunikation des Risikos sowie die jeweiligen Bewältigungsmaßnahmen enthalten.[61]

---

54 BT-Drucks. 13/9712, S. 15.

55 Zu beachten ist allerdings, dass die Gerichte zum Teil bestimmte Qualitätsanforderungen an das interne Kontrollsystem stellen, vgl. etwa *LG München I*, Urt. v. 5.4.2007 – 5 HKO 15964/96, NZG 2008, 319 (320) wonach die Errichtung einer Organisation mit engmaschigem Berichtswesen, in der erkannte Risiken vom Sachbearbeiter bis zur Unternehmensleitung reibungslos kommuniziert werden können und zwar mit entsprechender Dokumentation, verlangt wird, um den Anforderungen aus § 91 Abs. 2 AktG zu entsprechen.

56 *Spindler*, in: MünchKomm-AktG (o. Fußn. 48), § 91 Rn. 16; *Hüffer* (o. Fußn. 45), § 91 Rn. 1, 9.

57 *Spindler*, in: MünchKomm-AktG a.a.O., § 91 Rn. 27.

58 *Blasche* (o. Fußn. 48), S. 63 f.; *Hüffer* (o. Fußn. 45), § 91 Rn. 8 m.w.N.

59 *Pampel/Krolak*, in: *Hauschka* (o. Fußn. 27), S. 330.

60 *Lorenz*, in: *Romeike* (Hrsg.), Rechtliche Grundlagen des Risikomanagements, S. 7.

61 *Kort*, NZG 2008, 81 (82). Da vom Vorstand verursachte Verstöße gegen gesetzliche Vorschriften ebenfalls bestandsgefährdend sein können (siehe BT-Drucks. 13/9712, S. 15), ließe sich aus § 91 Abs. 2 AktG darüber hinaus die Pflicht zu einer umfassenden Compliance-Organisation ableiten. Dem ist jedoch insoweit nicht zuzustimmen, als auch hier der Ermessensspielraum des Vorstands gilt und die Einhaltung des geltenden Rechts seitens des Unter-

Nach der Begründung des Gesetzgebers hat der Vorstand jedenfalls für ein angemessenes Risikomanagement und eine angemessene interne Revision zu sorgen.[62] Selbst wenn man dies dahingehend versteht, dass der Vorstand nicht zur Einrichtung eines umfassenden Risikomanagementsystems verpflichtet ist, so muss er doch gemäß § 76 Abs. 1 AktG angemessen mit potentiellen Risiken umgehen.

2.1.1.2
Sorgfaltspflicht und Verantwortung der Vorstandsmitglieder

Überdies hat der Vorstand gemäß § 93 Abs. 1 Satz 1 AktG bei der Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden, wobei gemäß Satz 2 der Norm eine Verletzung dieser Pflicht nicht vorliegt, wenn das Vorstandsmitglied bei der unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln.

Vor diesem Hintergrund gilt es grundsätzlich, nicht nur die erwerbswirtschaftlichen Interessen der Gesellschaft zu berücksichtigen, sondern ebenso jene der Anteilseigner sowie das Wohl der Arbeitnehmer und der Allgemeinheit.[63] Zu beachten sind ferner Pflichten, die sich aus der Anwendbarkeit ausländischen Rechts ergeben, insbesondere aus den amerikanischen Vorschriften des Kapitalmarktes mit extraterritorialer Geltung.[64]

Die Anforderungen an die Sorgfaltspflicht orientieren sich erneut an der Art und Größe des Unternehmens, der Marktstellung oder der Beschäftigtenzahl.[65] Maßstab soll der selbstständige Leiter eines Unternehmens sein, der, ähnlich einem Treuhänder, fremden Vermögensinteressen verpflichtet ist.[66]

Ob die Installation eines bestimmten betriebswirtschaftlichen Risikofrühwarn- und Überwachungssystems gemäß § 91 Abs. 2 AktG den Ansprüchen genügt, ist nicht endgültig geklärt.[67] Auch der Einfluss des Deutschen Corporate Governance Kodex auf die Konkretisierung der Sorgfaltspflicht ist umstritten.[68] Anknüpfungspunkt für das Vorliegen der Sorgfalt ist gemäß § 93 Abs. 1 Satz 2 AktG das Handeln auf Grundlage angemessener Informationen. Hat ein Konzern, der wegen seiner Größe und der daraus resultierenden Anonymität einem ständigen Risiko ausgesetzt ist, kein wirksames Risikomanagementsystem implementiert, ist bei unternehmensbezogenen Risikoentscheidungen al-

---

nehmens und des Vorstands ohnehin eine Selbstverständlichkeit darstellt, *Spindler*, in: MünchKomm-AktG (o. Fußn. 48), § 91 Rn. 36.

62 BT-Drucks. 13/9712, S. 15.

63 *Spindler*, in: MünchKomm-AktG (o. Fußn. 48), § 93 Rn. 21.

64 *Spindler*, in: MünchKomm-AktG a.a.O., § 93 Rn. 21; siehe Abschnitt 2.3.

65 *Spindler*, in: MünchKomm-AktG a.a.O., § 93 Rn. 24.

66 *Hüffer* (o. Fußn. 45), § 93 Rn. 4.

67 Einen Überblick über den Meinungsstand gibt *Spindler*, in: MünchKomm-AktG (o. Fußn. 48), § 93 Rn. 29 m.w.N.

68 Siehe Abschnitt 2.1.3.

lerdings zu bezweifeln, ob diese „vernünftigerweise" auf der Grundlage „angemessener Information" gefällt wurden.[69] Daneben wird von einem dem Unternehmensinteresse verschriebenen Geschäftsleiter die Einrichtung eines Systems, welches Risiken frühzeitig erkennt und abwendet, allein deshalb zu fordern sein, da das Abwarten auf den Risikoeintritt die Gesellschaft in der Regel nur schädigen kann.[70]

2.1.1.3
Haftung des Vorstands

Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft gemäß § 93 Abs. 2 AktG zum Ersatz des daraus entstandenen Schadens verpflichtet, wenn sie vorsätzlich oder fahrlässig gehandelt haben oder den zu führenden Entlastungsbeweis nicht erbringen können.[71] Im Falle einer geltend gemachten Pflichtverletzung liegt es also am Vorstand, zu beweisen, dass er seiner Sorgfaltspflicht nachgekommen ist. Dabei haftet der Vorstand als Gesamtschuldner. Die Zuteilung bestimmter Ressorts an einzelne Vorstandsmitglieder ist zwar möglich, die übrigen Vorstandsmitglieder trifft jedoch zumindest eine Überwachungspflicht gegenüber dem zuständigen Mitglied, deren Nichtbefolgung gegebenenfalls zu einer Haftung führt, in den meisten Fällen aber zumindest personelle Konsequenzen hat.[72]

Zwar stellt ein mangelhaftes Risikomanagementsystem per se keinen Schaden dar,[73] jedoch kann es zu schädigenden unternehmerischen Fehlentscheidungen führen.[74] Nach dem BGH kommt eine Schadensersatzpflicht in Betracht,

> „wenn die Grenzen, in denen sich ein von Verantwortungsbewusstsein getragenes, ausschließlich am Unternehmenswohl orientiertes, auf sorgfältiger Ermittlung der Entscheidungsgrundlagen beruhendes unternehmerisches Handeln bewegen muss, deutlich überschritten sind, oder die Bereitschaft, unternehmerische Risiken einzugehen, in unverantwortlicher Weise überspannt worden ist, oder das Verhalten des Vorstands aus anderen Gründen als pflichtwidrig gelten muss."[75]

---

69 *Preußner*, NZG 2008, 574 (575).
70 *Lorenz*, in: *Romeike* (o. Fußn. 60), S. 12.
71 *Spindler*, in: MünchKomm-AktG, § 93 Rn. 216; *Hüffer*, AktG, § 93 Rn. 11.
72 Siehe etwa *LG Berlin*, Urt. v. 03.07.2002 - 2 O 358/01 (nicht rechtskräftig), BKR 2002, 969 (970); *VG Frankfurt/Main*, Urt. v. 08.07.2004 - 1 E 7363/03, Pressemitteilung, http://www.vg-frankfurt.justiz.hessen.de/irj/VG_Frankfurt_am_Main_Internet?rid=HMdJ_15/VG_Frankfurt_am_Main_Internet/sub/5c3/5c33c229-7428-b11f-3efe-f97ccf4e69f2,,,11111111-2222-3333-4444-100000005003%26overview=true.htm. (Stand: 13.03.2010); zu den weiteren Voraussetzungen der persönlichen Haftung bei einer mehrgliedrigen Geschäftsleitung siehe *Rehbinder*, in: *Hilty/Drexl/Nordemann*, Schutz von Kreativität und Wettbewerb, S. 523 f.
73 Allerdings stellt dies einen wichtigen Grund für eine fristlose Kündigung des verantwortlichen Vorstandsmitglieds dar, siehe *LG Berlin* a.a.O., S. 970.
74 *Lorenz*, in: *Romeike*, Rechtliche Grundlagen des Risikomanagements, S. 22.
75 *BGH*, Urt. v. 21.04.1997 – II ZR 175/95 (ARAG/Garmenbeck), NJW 1997, 1926 (1928).

Der damit im Rahmen der sog. Business Judgement Rule[76] eingeräumte Spielraum sei überschritten, wenn

> „aus der Sicht eines ordentlichen und gewissenhaften Geschäftsleiters das hohe Risiko eines Schadens unabweisbar ist und keine vernünftigen wirtschaftlichen Gründe dafür sprechen, es dennoch einzugehen."[77]

Bei der Haftung nach § 93 Abs. 2 AktG handelt es sich um eine Binnenhaftung der Vorstandsmitglieder. Die Anleger können gemäß § 147 AktG durchsetzen, dass der Schaden zugunsten der Gesellschaft geltend gemacht wird.

Eine Außenhaftung gegenüber den Anlegern ist an dieser Stelle nicht vorgesehen. Die Anleger können jedoch in Ausnahmefällen bei einer sittenwidrigen vorsätzlichen Schädigung gemäß § 826 BGB oder der Verletzung von Schutzgesetzen i.S.v. § 823 Abs. 2 BGB durch den Vorstand eine persönliche Entschädigung verlangen.[78] Ein solches Schutzgesetz stellt etwa § 400 AktG dar,[79] auf dessen Grundlage es im Verlauf des zurückliegen Jahrzehntes zu einer Reihe bemerkenswerter BGH-Entscheidungen hinsichtlich der persönlichen Haftung von Gesellschaftsorganen kam. So kann etwa ein Schadensersatzanspruch vonseiten der Aktionäre wegen falscher Ad-hoc-Mitteilungen gegeben sein,[80] wobei auf Grund der drohenden „uferlosen Ausweitung" der Haftung die Fragen der haftungsbegründenen Kausalität und des Umfangs des Schadensersatzes immer im Vordergrund zu stehen haben.[81] Darüber hinaus kommt auch die zuvor wenig beachtete strafrechtliche Verantwortlichkeit von Vorstands- und Aufsichtsratesmitgliedern durchaus zur Anwendung.[82]

Auch wenn nicht ausdrücklich auf die Vorstandshaftung bezogen, so ist in diesem Zusammenhang schließlich noch ein Urteil des BGH aus dem Jahre 2009 zu erwähnen, in welchem das Gericht eine Rechtspflicht zur Kontrolle der Mitarbeiter eines Unternehmens, ob von diesen unternehmensbezogene Straftaten oder Gesetzesverstöße begangen worden sein könnten, auch auf

---

[76] Nach der aus dem angelsächsischen Rechtsraum stammenden Business Judgement Rule dürfen Entscheidungen der Geschäftsleitung grundsätzlich keiner richterlichen Kontrolle unterliegen, da andernfalls Entscheidungen, die zwar im Unternehmensinteresse liegen, jedoch mit einem gewissen Restrisiko verbunden sind, nicht mehr getroffen würden. Der Vorstand ist allerdings selbstverständlich gehalten, nicht gegen allgemeine Treuepflichten, Informationspflichten, die Satzung oder andere Gesetze zu verstoßen, BT Drucks. 15/5092, S. 11.

[77] *BGH*, Urt. v. 21.03.2005 – II ZR 54/03, NZG 2005, 562 (563); siehe ferner *Sieg/Zeidler*, in: *Hauschka*, Corporate Compliance, § 3 Rn. 4-6 m.w.N.; *Meier-Greve*, BB 2009, 2555 (2557 ff.)

[78] *Nicklisch*, Die Auswirkungen des Sarbanes-Oxley Act auf die deutsche Corporate Governance, S. 174 f.

[79] *Schaal*, in: *Erbs/Kohlhaas*, Strafrechtliche Nebengesetze, § 400 AktG Rn. 3.

[80] *BGH*, Urt. v. 19.07.2004 – II ZR 402/02 (Informatec), NJW 2004, 2971; *BGH*, Urt. v. 09.05.2005 – II ZR 287/02, NJW 2005, 2450.

[81] Siehe zu den BGH-Entscheidungen ComROAD I – VIII *Möllers*, NZG 2008, 413; *Longino*, DStR 2008, 2068.

[82] *BGH*, Urt. v. 16.12.2004 – 1 StR 420/03 (Fall Haffa/EM.TV); siehe auch zur vom BGH bestätigten Vorinstanz *Kiethe*, NStZ 2004, 73 (76). Die an die Brüder Haffa verhängten Geldbußen betrugen 1,2 Millionen bzw. 240.000 EUR.

einen leitenden Angestellten erstreckt. Das Urteil bestätigt die strafrechtliche Haftung des Compliance-Beauftragten, wenn dieser nicht seiner Aufgabe der Verhinderung sämtlicher unternehmensbezogenen Rechtsverstöße und insbesondere Straftaten nachkommt.[83]

2.1.2
Überwachungspflicht und Haftung des Aufsichtsrates nach dem Aktiengesetz

Gemäß § 111 Abs. 1 AktG hat der Aufsichtsrat die Geschäftsführung zu überwachen. Im Vordergrund steht die Aufsicht darüber, dass der Vorstand seiner Pflicht zur Bestandssicherung der Gesellschaft aus § 76 Abs. 1 AktG[84] i.V.m. § 91 Abs. 2 AktG nachkommt. Diese Überwachungsaufgabe wird durch § 107 Abs. 3 Satz 2 AktG weiter konkretisiert. Verstöße werden durch § 116 AktG sanktioniert.

2.1.2.1
Überwachung der Wirksamkeit des internen Kontrollsystems

Nach § 107 Abs. 3 Satz 1 AktG kann der Aufsichtsrat zur Erfüllung seiner Aufgaben Ausschüsse bestellen. Im Rahmen des BilMoG[85] wurde § 107 Abs. 3 AktG ein neuer Satz 2 hinzugefügt, wonach der Aufsichtsrat insbesondere einen Prüfungsausschuss bestellen kann, der sich mit der Überwachung des Rechnungslegungsprozesses sowie der Wirksamkeit des internen Kontrollsystems, des Risikomanagementsystems und des Revisionssystems befasst.

Neben der Möglichkeit zur Bildung eines Prüfungsausschusses stellt die Norm klar, dass die Überwachung jener Systeme der Kontrollpflicht des Aufsichtsrates unterliegt. Die Einrichtung eines Prüfungsausschusses ändert ebenfalls nichts an der vollumfänglichen Verantwortlichkeit des Aufsichtsrates.[86]

Der Gesetzesentwurf beschreibt die vorzunehmende „Überwachung des internen Kontrollsystems, des zum internen Kontrollsystem gehörenden internen Revisionssystems und des Risikomanagementsystems (als) umfassend angelegt“[87] und weist deutlich auf die Prüfung des vom Vorstand eingerichteten Risikofrüherkennungssystems nach § 91 Abs. 2 AktG im Hinblick auf mögliche Erweiterungen oder Verbesserungen hin.[88] Laut *Hüffer* ist die Einrichtung des Prüfungsausschusses zu diesem Zweck bei börsennotierten Unternehmen oh-

---

83 *BGH*, Urt. v. 17.07.2009 – 5 StR 394/08, NJW 2009, 3173 (3175); siehe zur Garantenpflicht des Compliance-Beauftragten kritisch *Kamp/Körffer*, RDV 2010, 72.
84 *Hüffer* (o. Fußn. 45), § 111 Rn. 6.
85 Gesetz zur Modernisierung des Bilanzrechts (Bilanzrechtsmodernisierungsgesetz) v. 25.05.2009, BGBl. 2009 I S. 1102.
86 BT-Drucks. 16/10067, S. 102.
87 BT-Drucks. 16/10067, S. 102.
88 BT-Drucks. 16/10067, S. 103.

nehin gängige Praxis bzw. dringend zu empfehlen.[89] Darüber hinaus verlangt § 324 Abs. 1 HGB von kapitalmarktorientierten Kapitalgesellschaften[90], also auch von börsennotierten Gesellschaften, dass diese einen Prüfungsausschuss einrichten, der sich insbesondere mit den in § 107 Abs. 3 Satz 2 AktG beschriebenen Aufgaben befasst.[91] Ferner befreit ein Prüfungsausschuss auf Konzernebene die Tochtergesellschaften nicht von der Pflicht, eigene Prüfungsausschüsse einzurichten.[92]

Da die Gesetzesbegründung mit solchem Nachdruck die Überwachungspflichten des Aufsichtsrates bzw. des Prüfungsausschusses betont, ist im Ergebnis von einer Intensivierung der ohnehin vorhandenen Aufsichtspflicht im Hinblick auf das IKS auszugehen. Die Prüfung des reinen Vorhandenseins eines Früherkennungssystems reicht danach nicht mehr aus, hingegen wird die Prüfung auf dessen Wirksamkeit[93] hin verlangt.[94]

2.1.2.2
Überprüfung von Konzernabschluss und –lagebericht

Nach § 171 Abs. 1 AktG hat der Aufsichtsrat insbesondere den Jahresabschluss und bei Mutterunternehmen[95] auch den Konzernabschluss und den Konzernlagebericht[96] zu prüfen. Hierbei wird er vom Abschlussprüfer unterstützt. Ebenfalls durch das BilMoG in Umsetzung von Art. 42 Abs. 1 Lit. b) und c)[97] der Abschlussprüferrichtlinie[98] neu eingeführt wurde die Forderung, dass der Abschlussprüfer die wesentlichen Ergebnisse seiner Prüfung, insbe-

---

89 *Hüffer* (o. Fußn. 45), § 107 Rn. 16a.

90 Nach der Definition in § 264d HGB ist eine Gesellschaft kapitalmarktorientiert, wenn sie einen organisierten Markt im Sinn des § 2 Abs. 5 WpHG durch von ihr ausgegebene Wertpapiere im Sinn des § 2 Abs. 1 S. 1 WpHG in Anspruch nimmt oder die Zulassung solcher Wertpapiere zum Handel an einem organisierten Markt beantragt hat.

91 Diese Verbindlichkeit besteht zumindest sofern kein Aufsichtsrat existiert, dem gemäß § 100 Abs. 5 AktG mindestens ein unabhängiges Mitglied angehört, das über Sachverstand auf den Gebieten der Rechnungslegung oder Abschlussprüfung verfügt.

92 *Wolf*, DStR 2009, 920 (921) m.w.N.

93 BT-Drucks. 16/10067, S. 102.

94 *Preußner* (o. Fußn. 69), S. 575; zur Vertiefung der Pflichten des Prüfungsausschusses und den weiteren Aufgaben des Aufsichtsrates im Zusammenhang mit dem Jahresabschlussbericht siehe *Lanfermann/Röhricht*, BB 2009, 887.

95 Siehe § 290 Abs. 1 HGB.

96 Siehe hierzu sogleich Abschnitt 2.1.4.1.

97 Nach der Vorschrift haben die Mitgliedstaaten sicherzustellen, dass die Abschlussprüfer oder die Prüfungsgesellschaften, die die Abschlussprüfung von Unternehmen von öffentlichem Interesse durchführen, b) den Prüfungsausschuss jährlich über die von ihnen gegenüber dem geprüften Unternehmen erbrachten zusätzlichen Leistungen informieren und c) mit dem Prüfungsausschuss die Risiken für ihre Unabhängigkeit sowie die von ihnen gemäß Artikel 22 der Abschlussprüferrichtlinie ergriffenen Schutzmaßnahmen zur Minderung dieser Risiken erörtern.

98 Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates v. 17.05.2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates, ABlEU Nr. L 157 v. 09.06.2006 S. 87.

sondere wesentliche Schwächen des internen Kontroll- und des Risikomanagementsystems bezogen auf den Rechnungslegungsprozess, dem Aufsichtsrat zu berichten hat.[99]

Die Norm hat hauptsächlich Auswirkungen auf eine mögliche Haftung des Aufsichtsrates, wenn dieser trotz der Mitteilung des Prüfers über Mängel des Kontrollsystems keine Maßnahmen zur Beseitigung der Mängel ergreift.

2.1.2.3
Haftung des Aufsichtsrates

Für die Sorgfaltspflicht und Verantwortlichkeit der Aufsichtsratesmitglieder gilt nach § 116 AktG der für den Vorstand einschlägige § 93 AktG sinngemäß, wobei dieser Verweis nicht dahingehend verstanden werden darf, dass Aufsichtsrat und Vorstand dieselben Pflichten treffen. So tritt im Falle des Aufsichtsrates nach h.M. die Überwachungspflicht in den Vordergrund.[100] Die Anforderungen an die Sorgfaltspflicht können sich nach der Zuständigkeit des jeweiligen Aufsichtsratesmitglieds sowie nach der Art und Größe des Unternehmens bemessen.[101] Über eine sinngemäße Anwendung von § 93 Abs. 2 bis Abs. 4 AktG ist der Aufsichtsrat ebenfalls zum Ersatz des durch eine Pflichtverletzung, etwa der unterlassenen Prüfung des Risikomanagementsystems auf seine Wirksamkeit hin, entstandenen Schadens verpflichtet.

Auch für den Aufsichtsrat gilt ein unternehmerischer Ermessensspielraum, sofern er auf der Grundlage unternehmerischer Entscheidungen die Tätigkeit des Vorstands im Sinne einer präventiven Kontrolle mitgestaltet und etwa von Zustimmungsvorbehalten i.S.d. § 111 Abs. 4 Satz 2 AktG Gebrauch macht. Dieser Spielraum ist bei Maßnahmen im Rahmen einer nachträglichen Überwachung jedoch weitestgehend eingegrenzt[102] und damit auch bei der Beurteilung der Wirksamkeit eines bereits implementierten Risikomanagementsystems.

Der bisherigen Rechtsprechung sind nur wenige konkretisierende Ausführungen zu der Frage zu entnehmen, wann ein Verstoß gegen die Sorgfaltspflichten und damit eine Haftung des Aufsichtsrates vorliegt. Dies soll beispielsweise dann der Fall sein, wenn der Aufsichtsrat ohne sich hinreichend zu informieren und die darauf aufbauende Chancen- und Risikoabschätzung seine Zustimmung zu nachteiligen Geschäften erteilt[103] und weiterhin wenn er

---

[99] Zur Abschlussprüfung siehe Abschnitt 2.1.4.

[100] *Hüffer*, AktG, § 116 Rn. 2 m.w.N.

[101] *Hüffer*, AktG, § 116 Rn. 3.

[102] So trifft den Aufsichtsrat etwa die Pflicht zur Prüfung des Vorliegens von Schadensersatzansprüchen und ihrer Geltendmachung gegen den Vorstand, siehe *BGH*, Urt. v. 21.04.1997 – II ZR 175/95 (ARAG/Garmenbeck), NJW 1997, 1926 (1928).

[103] *BGH*, *Urt.* v. 11.12.2006 – II ZR 243/05, NZG 2007, 187. Das Urteil bezog sich zwar auf die Pflichten eines fakultativen Aufsichtsrates einer GmbH, jedoch sind die gemachten Vorgaben genauso vom Aufsichtsrat einer AG zu berücksichtigen, siehe etwa *Liebscher*, LMK 2007, 220409.

trotz Hinweisen auf unkorrekte oder unseriöse Geschäfte des Vorstands mit existenzbedrohender Bedeutung keine Nachforschungen über dessen Praktiken anstellt.[104] Als wegweisend dürfte ein Urteil des OLG Düsseldorf aus dem Jahre 2008 zu werten sein, in welchem das Gericht einem Aktionär einen Schadensersatzanspruch gegen einen ehemaligen Aufsichtsratesvorsitzenden zugebilligt hat, da dieser die „augenfällige" widerrechtliche Verwendung der Anlegergelder durch den Vorstand bei einer sorgfältigen Wahrnehmung seiner Kontrollpflichten hätte erkennen müssen.[105] Das Gericht schafft damit die Grundlage für eine persönliche Haftung eines Aufsichtsratesmitglieds auf Grund von § 826 BGB wegen eines strafbaren oder sittenwidrigen Verhaltens des Vorstands.

2.1.3
Erklärung zum Deutschen Corporate Governance Index

Vorstand und Aufsichtsrat einer börsennotierten Gesellschaft haben des Weiteren gemäß § 161 Abs. 1 AktG jährlich zu erklären, dass den vom Bundesministerium der Justiz bekannt gemachten Empfehlungen der Regierungskommission Deutscher Corporate Governance Kodex entsprochen wurde und wird oder welche Empfehlungen nicht angewendet wurden oder werden und warum nicht. Diese sog. Entsprechenserklärung ist nach Abs. 2 der Norm auf der Internetseite der Gesellschaft dauerhaft öffentlich zugänglich zu machen. Die Erklärung ist in Bezug auf die Anforderungen an das IKS von Interesse, da der Kodex zum einen Vorschriften zum Risikomanagement enthält und damit Rückschlüsse auf die Auslegung von § 91 Abs. 2 AktG zulässt. Zum anderen könnte er eine Ausstrahlungswirkung auf die Konkretisierung der Sorgfaltspflicht nach § 93 AktG haben.[106]

2.1.3.1
Der Deutsche Corporate Governance Kodex

Zweck des Deutschen Corporate Governance Kodex (DCGK)[107] ist ausweislich seiner Präambel, die wesentlichen gesetzlichen Vorschriften zur Leitung und Überwachung deutscher, börsennotierter Gesellschaften darzustellen. Daneben enthält er national und international anerkannte Standards verantwortungsvoller Unternehmensführung und soll aufseiten der Anteilseigner und der Öffentlichkeit zu mehr Vertrauen durch Transparenz führen. Der DCGK beinhaltet Empfehlungen, deren Nichtbefolgung in der Erklärung gemäß § 161 AktG anzuzeigen, wenn auch nicht zu begründen[108] ist. Daneben ent-

---

[104] *LG Bielefeld*, Urt. v. 16.11.1999 – 15 O 91/98 (nicht rechtskräftig), BB 1999, 2630 (2632).
[105] *OLG Düsseldorf*, Urt. v. 23.06.2008 – 9 U 22/08, NZG 2008, 713. Die zu zahlende Summe betrug knapp 40.000€.
[106] *OLG Schleswig*, Urt. v. 19. 9. 2002 - 5 U 164/01 (nicht rechtskräftig), NZG 2003, 176 (179).
[107] In der zuletzt geänderten Fassung vom 18.06.2009 abrufbar unter http://www.corporate-governance-code.de/ger/kodex/index.html (Stand: 01.03.2010).
[108] BT-Drucks 14/8769, S. 21.

hält der DCGK Anregungen, von welchen ohne Offenlegung abgewichen werden kann.

Der Vorstand ist entsprechend Zif. 4.1.3 DCGK zur Compliance verpflichtet, indem er für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und auf deren Beachtung durch die Konzernunternehmen hinzuwirken hat. Nach Zif. 4.1.4. DCGK sorgt er ferner für ein angemessenes Risikomanagement und Risikocontrolling im Unternehmen und informiert gemäß Zif. 3.4 DCGK den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen insbesondere der Risikolage, des Risikomanagements und der Compliance. Bei den genannten Vorschriften handelt es sich lediglich um eine Darstellung geltenden Rechts, deren Befolgung nicht Gegenstand der Erklärung aus § 161 AktG ist.

Dagegen empfiehlt Zif. 5.2 DCGK, dass der Aufsichtsratesvorsitzende mit dem Vorstand regelmäßig Kontakt hält und mit ihm die Strategie, die Geschäftsentwicklung und das Risikomanagement des Unternehmens berät. Weiterhin empfiehlt Zif. 5.3.2 DCGK, dass der Aufsichtsrat einen Prüfungsausschuss einrichtet, der sich insbesondere mit Fragen des Risikomanagements, der Compliance und der erforderlichen Unabhängigkeit des Abschlussprüfers befasst.

2.1.3.2
Auswirkungen für die Organe der Gesellschaft

Zunächst ist die Einhaltung des DCGK weder Voraussetzung für eine Börsennotierung des Unternehmens, noch unterliegt sie der Kontrolle durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) oder wird vom Abschlussprüfer überprüft.[109]

Im Zusammenhang mit den möglichen Auswirkungen des DCGK stellt sich vorab grundsätzlich die Frage nach seiner Rechtsnatur. Zumindest die Empfehlungen haben Normcharakter, da sie zu befolgen sind, jedoch sind sie keine Rechtsnormen, da sie von einer überwiegend aus Vertretern der Wirtschaft zusammengesetzten Kommission[110] erarbeitet wurden und daher kein Akt staatlicher Rechtsetzung sind.[111] Damit kommt den Empfehlungen ein „Geltungsanspruch mit Ausstiegsklausel" (*Hüffer*) zu[112], da ein Abweichen von den Normen denkbar ist. Wegen dieser Möglichkeit wird auch eine Konkretisierungswirkung der Sorgfaltspflicht aus § 93 AktG durch den DCGK abgelehnt, da ein derartiger Effekt jedenfalls für Gesellschaften, die sich dem DCGK nicht unterworfen haben, ausgeschlossen ist.[113]

---

[109] *Romeike*, in: *Romeike* (o. Fußn. 60), S. 59.
[110] http://www.corporate-governance-code.de/ger/mitglieder/index.html (Stand: 01.03.2010).
[111] *Hüffer* (o. Fußn. 45), § 161 Rn. 3.
[112] *Hüffer* a.a.O., § 161 Rn. 3.
[113] *Spindler*, in: MünchKomm-AktG (o. Fußn. 48), § 93, Rn. 31.

Eine solche Wirkung haben die Empfehlungen aber dann, wenn sie in die Geschäftsordnung oder Satzung der Gesellschaft überführt werden,[114] denn in diesem Fall gehören sie zu den internen Verhaltenspflichten der Gesellschaft und ein Verstoß kann einen Haftungszwang nach §§ 93, 116 AktG auslösen.[115]

Bezüglich der Auslegung von § 91 Abs. 2 AktG stellt der DCGK klar, dass der Vorstand zumindest für ein angemessenes Risikomanagement und Risikocontrolling im Unternehmen zu sorgen hat. Den Rückschluss auf die aktienrechtliche Norm lässt die Gesetzesbegründung zum DCGK zu, da es sich bei der relevanten Zif. 4.1.4 DCGK weder um eine Empfehlung, noch um eine Anregung, sondern um die Darstellung geltenden Rechts handelt.[116] Im Umkehrschluss verlangt das Kontrollsystem demnach neben dem schon vorher bekannten angemessenen internen Risikomanagement und der internen Revision[117] ein angemessenes Risikocontrolling.

In Bezug auf den Prüfungsausschuss, den der Aufsichtsrat insbesondere zur Überprüfung der Wirksamkeit des IKS einberufen kann, findet eine Konkretisierung statt. Während § 107 Abs. 2 Satz 3 AktG lediglich vorsieht, dass ein solcher Ausschuss bestellt werden kann, enthält Zif. 5.3.2 DCGK eine dahingehende Empfehlung, mit der Konsequenz, dass ein Abweichen zumindest anzuzeigen ist.

Letztlich kann den erweiterten Anforderungen durch den DCGK wegen der beschriebenen fraglichen Rechtsnatur der Empfehlungen, die im Übrigen auch verfassungsrechtliche Bedenken hervorrufen,[118] bestenfalls eine Indizwirkung zukommen.[119]

Eine gesetzliche Flankierung des DCGK besteht jedoch durch die Entsprechenserklärung aus § 161 AktG. Auch wenn diese dem DCGK laut der Begründung des Gesetzgebers lediglich einen „besonderen Nachdruck" verleihen soll,[120] stellt eine unterbliebene oder mangelhafte Entsprechenserklärung einen Verstoß gegen § 161 AktG dar, der bei einem nachweisbaren Schaden gemäß § 93 AktG eine Schadensersatzpflicht des unrechtmäßig handelnden Organs auslöst. Wird die Entsprechenserklärung nicht befolgt, kann dies weiterhin Konsequenzen für unternehmensinterne Entscheidungen nach sich ziehen.[121]

---

[114] *Spindler*, in: MünchKomm-AktG a.a.O., § 93 Rn. 31.
[115] *Romeike*, in: *Romeike* (o. Fußn. 60), S. 60.
[116] BT-Drucks. 14/8769, S. 21.
[117] BT-Drucks. 13/9712, S. 15.
[118] *Hüffer* (o. Fußn. 45), § 161 Rn. 4; *Schmidt*, BB 2009, 1295 m.w.N.
[119] *Schmidt* a.a.O., 1295.
[120] BT-Drucks. 14/8769, S. 21.
[121] Befolgt der Aufsichtsrat die Entsprechenserklärung über die Einhaltung von Empfehlungen nicht, die gleichzeitig Grundlage eines Hauptversammlungsbeschlusses sind, kann dies etwa Auswirkungen auf die Wirksamkeit des Beschlusses haben, vgl. *Vetter*, NZG 2008, 121 (126).

2.1.4
Erwartungen an das Interne Kontrollsystem aus handelsrechtlicher Sicht

Das HGB enthält einige an den Vorstand von Gesellschaftern oder den Wirtschaftsprüfer gerichtete Vorschriften, die sich auf das IKS beziehen. Die wichtigsten Regelungen sollen nachfolgend kurz dargestellt werden.

2.1.4.1
Konzernlagebericht

Der Lagebericht ist Teil des Jahresabschlussberichts größerer Kapitalgesellschaften. In Umsetzung von Art. 46a Abs. 1 Lit. c)[122] der Abänderungsrichtlinie[123] wurde im Rahmen des BilMoG der Umfang des durch den Vorstand abzugebenden Konzernlageberichts erweitert. Gemäß § 315 Abs. 2 Nr. 5 HGB hat der Bericht die wesentlichen Merkmale des internen Kontroll- und des Risikomanagementsystems im Hinblick auf den Konzernrechnungslegungsprozess zu enthalten, sofern es sich bei dem Mutterunternehmen oder einem der in den Konzernabschluss einbezogenen Tochterunternehmen um eine kapitalmarktorientierte Gesellschaft[124] handelt.

Dabei soll das IKS insbesondere die Grundsätze, Verfahren und Maßnahmen zur Sicherung der Wirksamkeit, Wirtschaftlichkeit und Ordnungsmäßigkeit der Rechnungslegung und zur Sicherung der Einhaltung der maßgeblichen rechtlichen Vorschriften umfassen.[125] Laut der Gesetzesbegründung ergibt sich hieraus jedoch keine Pflicht, ein bestimmtes bzw. überhaupt ein internes Kontroll- und Risikomanagementsystem im Hinblick auf den Rechnungslegungsprozess zu installieren. Die vorhandenen Systeme sind im Lagebericht lediglich derart zu beschreiben, dass sich die Abschlussadressaten ein Bild von den wesentlichen Merkmalen machen können. Einschätzungen zur Wirksamkeit des Systems sind ebenfalls nicht mit anzugeben. Allerdings ist anzuzeigen, falls ein entsprechendes internes Kontroll- und Risikomanagementsystem nicht besteht.[126]

---

[122] Art. 46a Abs. 1, „Eine Gesellschaft, deren Wertpapiere zum Handel an einem geregelten Markt (…) zugelassen sind, nimmt eine Erklärung zur Unternehmensführung in ihren Lagebericht auf. Diese Erklärung bildet einen gesonderten Abschnitt im Lagebericht und enthält zumindest die folgenden Angaben: (…) c) eine Beschreibung der wichtigsten Merkmale des internen Kontroll- und des Risikomanagementsystems der Gesellschaft im Hinblick auf den Rechnungslegungsprozess."

[123] Richtlinie 2006/46/EG des Europäischen Parlaments und des Rates v. 14.06.2006 zur Änderung der Richtlinien des Rates 78/660/EWG über den Jahresabschluss von Gesellschaften bestimmter Rechtsformen, 83/349/EWG über den konsolidierten Abschluss, 86/635/EWG über den Jahresabschluss und den konsolidierten Abschluss von Banken und anderen Finanzinstituten und 91/674/EWG über den Jahresabschluss und den konsolidierten Abschluss von Versicherungsunternehmen, ABlEU Nr. L 224 v. 16.08.2006 S. 1.

[124] Siehe § 264d HGB (o. Fußn. 90).

[125] BT-Drucks. 16/10067, S. 77.

[126] BT-Drucks. 16/10067, S. 76.

Gemäß § 315 Abs. 1 Satz 5 HGB ist im Konzernlagebericht die voraussichtliche Entwicklung der Gesellschaft mit ihren wesentlichen Chancen und Risiken zu beurteilen und zu erläutern. Ferner haben die gesetzlichen Vertreter einer kapitalmarktorientierten Gesellschaft zu versichern, dass der im Lagebericht beschriebene Geschäftsverlauf einschließlich des Geschäftsergebnisses und der Lage der Kapitalgesellschaft nach ihrem bestem Wissen so dargestellt ist, dass ein den tatsächlichen Verhältnissen entsprechendes Bild vermittelt wird und die wesentlichen Risiken beschrieben sind.

2.1.4.2
Feststellungen im Prüfungsbericht zur Wirksamkeit des Überwachungssystems

Aus § 316 HGB ergibt sich die Pflicht, den Jahresabschluss und den Konzernlagebericht durch einen Wirtschaftsprüfer prüfen zu lassen. Das nach § 91 Abs. 2 AktG einzurichtende Überwachungssystem ist gemäß § 317 Abs. 4 HGB ebenfalls Gegenstand der Überprüfung. Nach der in Folge des KonTraG eingeführten[127] und zuletzt durch das TransPuG geänderten[128] Norm ist bei einer börsennotierten AG im Rahmen der Prüfung des Jahresabschlusses zu beurteilen, ob der Vorstand die ihm nach § 91 Abs. 2 AktG obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann. In diesem Zusammenhang ist des Weiteren der Prüfungsstandard 340 des Instituts der Wirtschaftsprüfer (IDW PS 340) zu beachten. Dieser enthält im Wesentlichen Vorgaben über Art und Umfang der vorzunehmenden Prüfung.[129]

Laut der Begründung des Gesetzgebers ist durch die Abschlussprüfung gemäß § 317 Abs. 4 HGB festzustellen, ob ein angemessenes internes Risikomanagementsystem und eine angemessene interne Revision vorhanden sind.[130] Dabei ist nicht nur zu prüfen, ob ein Überwachungssystem nach § 91 Abs. 2 AktG eingerichtet wurde, sondern darüber hinaus, ob dieses in der konkreten Situation der Gesellschaft geeignet ist, mögliche Risiken frühzeitig und in effizienter Weise zu erkennen.[131]

---

[127] Siehe o. Fußn. 43.

[128] Gesetz zur weiteren Reform des Aktien- und Bilanzrechts, zu Transparenz und Publizität (Transparenz- und Publizitätsgesetz) v. 19.07.2002, BGBl. 2002 I S. 2681.

[129] *Ebke*, in: MünchKomm-HGB, § 317 Rn. 83.

[130] BT-Drucks 13/9712, S. 27.

[131] *Morck*, in: *Koller/Roth/Morck* (Hrsg.), HGB, § 317 Rn. 5; grundsätzlich nicht Gegenstand der Prüfung ist demgegenüber, ob der Vorstand in konkreten Fällen das Risiko frühzeitig erkannt und geeignete Gegenmaßnahmen ergriffen hat, siehe *Ebke* (o. Fußn. 129), § 317 Rn. 82; allerdings kann die angemessene Reaktion des Vorstands in der Prüfungspraxis dennoch von Interesse für die Prüfung sein, siehe *Lorenz*, in: *Romeike* (o. Fußn. 60), S. 9.

Der IDW PS 340 enthält konkretisierende Angaben bezüglich der Anforderungen an das Risikomanagementsystem.[132] Hiernach hat der Wirtschaftsprüfer folgende Elemente auf ihr Vorhandensein bzw. ihre Effizienz hin zu prüfen:[133] Vorhandensein eines Risikofrüherkennungssystems, Festlegung der Risikofelder, Risikoerkennung und -analyse, Risikokommunikation, Zuordnung von Verantwortlichkeiten und Aufgaben, Überwachungssystem[134], Dokumentation[135].

Da davon auszugehen ist, dass der Abschlussprüfer zumindest die Erfüllung dieser Mindestanforderungen überprüft, lässt § 317 Abs. 4 HGB i.V.m. IDW PS 340 insofern Rückschlüsse auf die Anforderungen an das Früherkennungs- und Überwachungssystem nach § 91 Abs. 2 AktG zu.[136] Daher empfiehlt sich für Unternehmen das Vorhandensein dieser Standards in effizienter Form zu gewährleisten, um eine Prüfung durch den Wirtschaftsprüfer mit positivem Ausgang wahrscheinlicher zu machen.[137]

Weiterhin kann der Prüfer von den gesetzlichen Vertretern der Gesellschaft laut § 320 Abs. 2 Satz 1 HGB alle Aufklärungen und Nachweise verlangen, die für eine sorgfältige Prüfung notwendig sind. Unter den Begriff der Notwendigkeit fällt dabei alles, was „der Klarstellung und Erläuterung des Jahresabschlusses, der Buchführung und des Lageberichts oder sonstiger Gegenstände der Abschlussprüfung sachdienlich ist."[138] Aus § 321 Abs. 2 Satz 2 HGB geht ferner hervor, dass im Prüfungsbericht auch über schwerwiegende Verstöße zu berichten ist, selbst wenn sie keinen Einfluss auf den Jahresabschlussbericht haben.[139] Daher ergibt sich aus den beiden vorgenannten Normen etwa auch die Pflicht des Wirtschaftsprüfers, zur Aufdeckung von Scheingeschäften Abgleiche der Kontonummern von Angestellten des Unternehmens mit jenen von geschäftlichen Vertragspartnern durchzuführen.[140] Diese Missbrauchsfälle haben zwar eher in seltenen Fällen Einfluss auf den Jahresabschluss, müssen aber dennoch Teil einer sorgfältigen Prüfung sein, da die Gefahr solcher Wirtschaftsdelikte allgemein bekannt ist.[141] Darüber hinaus hat der Prüfer allein

[132] Überblick bei *Hopt/Merkt*, in: *Baumbach/Hopt* (Hrsg.), HGB, § 317 Rn. 10; zur umstrittenen Verbindlichkeit des IDW PS 340 *Ebke* a.a.O., § 323 Rn. 31.
[133] Jeweils mit weiteren Erläuterungen *Blasche* (o. Fußn. 48), S. 65 ff.
[134] Im Vordergrund steht die Überwachung der im Rahmen des Risikomanagements ergriffenen Maßnahmen.
[135] Hiermit ist die Dokumentation der ergriffenen Maßnahmen gemeint.
[136] *Ebke* (o. Fußn. 129), § 317 Rn. 82; *Morck*, in: *Koller/Roth/Morck* (o. Fußn. 131), § 317 Rn. 5.
[137] Das Prüfungsergebnis ist schließlich gemäß § 321 Abs. 4 HGB in einem besonderen Teil des Prüfungsberichts darzustellen, in welchem auch auf Verbesserungsvorschläge hinsichtlich des internen Überwachungssystems einzugehen ist.
[138] *Aßmus*, MMR 2009, 599 (600) m.w.N.
[139] *Salvenmoser/Hauschka* (o. Fußn. 37), S. 322.
[140] Zu den datenschutzrechtlichen Implikationen, die mit der Herausgabe der Kontostammdaten des Unternehmens an den Abschlussprüfer verbunden sind, *Aßmus* (o. Fußn. 138), S. 600 ff.
[141] Die Wahrscheinlichkeit solcher Abgleiche im Rahmen der Abschlussprüfung wird durch den ebenfalls vom Prüfer zu berücksichtigenden Standard IDW PS 210 zur Aufdeckung von Unregelmäßigkeiten verdeutlicht, welcher Indikatoren für Fraud nennt und Abfragen bekannter

wegen einer möglichen Haftung aus § 323 HGB ein gesteigertes Interesse an der Aufdeckung von Wirtschaftsdelikten jeglicher Art.[142]

Da der Abschlussprüfer beim erhöhten Aufkommen derartiger Fälle zu der Einschätzung gelangen könnte, dass das nach § 91 Abs. 2 AktG eingerichtete Überwachungssystem ineffizient ist, hat das Unternehmen ein Interesse an der Verhinderung solcher Scheingeschäfte, was mit der eigenständigen Durchführung derartiger Abgleiche zu erreichen wäre.

2.1.5
Branchenbezogene Spezialvorschriften mit Ausstrahlungswirkung auf andere Wirtschaftszweige

Für einige Wirtschaftszweige mit besonders hohem Risikopotential gelten Sondervorschriften in Bezug auf die Organisationspflichten der leitenden Organe. Auch wenn die sich hieraus ergebenen Anforderungen auf die Besonderheiten regulierter Wirtschaftszweige zugeschnitten sind, können sie für die Auslegung der aktienrechtlichen Vorschriften von Bedeutung sein. Die in diesem Zusammenhang wichtigsten Regelungen aus dem Telekommunikationsgesetz (TKG), dem Kreditwesengesetz (KWG), der Baseler Eigenkapitalvereinbarung von 2004 (Basel II) sowie dem Wertpapierhandelsgesetz (WpHG) sollen nachfolgend kurz dargestellt werden.[143]

2.1.5.1
Technische Schutzmaßnahmen, § 109 TKG

Gemäß § 109 Abs. 1 TKG haben Anbieter von Telekommunikationsdiensten angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten sowie der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu treffen. Die Norm verpflichtet dazu, ein IT-Sicherheitskonzept zu erstellen, welches etwa die Auswahl und Etablierung einer geeigneten Organisationsstruktur für die IT-Sicherheit sowie eine Risiko- und Schwachstellenanalyse zu umfassen hat.[144]

Das IT-Risikomanagement mit seinem Ziel, Verfügbarkeit, Integrität und Vertraulichkeit der IT-Systeme zu gewährleisten, ist letztlich ebenfalls ein Teil des nach § 91 Abs. 2 AktG einzuführenden Überwachungssystems[145] und ver-

---

Missbrauchsmuster, ebenfalls durch automatische Datenanalysen, verlangt, siehe hierzu *Bantleon/Thomann/Bühner*, DStR 2007, 1987 (1981); *Berndt/Jeker*, BB 2007, 2615 (2620).

[142] So sollen Abschlussprüfer im Zusammenhang mit lückenhaften Prüfungen zuletzt „vermehrt" in Regress genommen worden sein, *Berndt/Jeker* a.a.O., S. 2621.

[143] Die versicherungsrechtliche Vorschrift § 64 VAG zur Geschäftsorganisation enthält zwar Details bezüglich des einzurichtenden Risikomanagementsystems, stimmt inhaltlich jedoch größtenteils mit § 25a KWG überein. Es gelten also die Ausführungen zu § 25a KWG entsprechend. Siehe zu § 64 VAG auch *Kort* (o. Fußn. 61), S. 83.

[144] *Bock*, in: *Geppert/Piepenbrock/Schütz* u.a. (Hrsg.), TKG, § 109 Rn. 50.

[145] *Bock*, in: *Geppert/Piepenbrock/Schütz* a.a.O., § 109 Rn. 52.

pflichtet alle Unternehmen, die Anbieter von Telekommunikationsdiensten im Sinne des TKG sind.[146]

2.1.5.2 Spezialvorschriften des KWG i.V.m. MaRisk

Laut § 25a KWG muss ein (Kredit-) Institut eine ordnungsgemäße Geschäftsorganisation gewährleisten, welche insbesondere ein angemessenes und wirksames Risikomanagement umfasst. Jenes Risikomanagement hat im Wesentlichen die Einrichtung interner Kontrollverfahren mit einem IKS und einer internen Revision zu beinhalten, wobei das IKS insbesondere klar abgegrenzte Verantwortungsbereiche sowie Prozesse zur Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation der Risiken umfasst.

Darüber hinaus veröffentlicht die BaFin zur Konkretisierung dieser Vorschrift regelmäßig Rundschreiben zu den Mindestanforderungen an das Risikomanagement[147] (MaRisk), bei denen es sich allerdings nur um unverbindliche Verlautbarungen handelt.[148]

Normadressaten sind gemäß § 1 KWG, wegen der besonderen Risiken des Finanzsektors,[149] Kredit- und Finanzdienstleistungsinstitute. Bei solchen Unternehmen können und müssen die Vorschriften ohne weiteres zur Konkretisierung der Pflichten aus § 91 Abs. 2 AktG herangezogen werden.[150] Das VG Frankfurt hat § 25a KWG darüber hinaus im Zusammenhang mit einer branchenfremden Versicherungsgesellschaft angewandt und sieht insoweit sogar eine rechtliche Entsprechung zwischen § 25a KWG und § 91 Abs. 2 AktG.[151] Von einer Pflicht zur Beachtung der Vorgaben aufseiten von Unternehmen anderer Branchen kann jedoch nicht gesprochen werden,[152] zumal der Vorstand einer AG bei der Ausgestaltung seiner Organisationspflicht einen Ermessensspielraum hat. Zumindest die im allgemeinen Teil der MaRisk unter AT 4 enthaltenen „Allgemeinen Anforderungen an das Risikomanagement“ können aber als unverbindliches Model auch für Nicht-Kreditinstitute eine Auslegungshilfe für § 91 Abs. 2 AktG sein.[153]

---

[146] Hierbei handelt es sich nach § 3 Nr. 24 TKG um alle Anbieter von Diensten, die in der Regel gegen Entgelt erbracht werden und die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdiensten in Rundfunknetzen. Hierunter fallen nach h.M. auch Arbeitgeber, die ihren Angestellten die private Nutzung von Telefon, Internet und E-Mail erlauben.

[147] In der zuletzt am 14.08.2009 aktualisierten Fassung abrufbar unter http://www.bafin.de/cln_161/nn_724304/SharedDocs/Veroeffentlichungen/DE/Service/Rundschreiben/2009/rs__0915__ba__marisk.html (Stand: 03.03.2010)

[148] *Binder*, in: *Romeike* (o. Fußn. 60), S. 136.

[149] *Spindler*, in: MünchKomm-AktG (o. Fußn. 48), § 91 Rn. 31.

[150] *LG Berlin* (o. Fußn. 72), S. 970; *Hüffer* (o. Fußn. 45), § 91 Rn. 8 m.w.N.

[151] *VG Frankfurt/Main* (o. Fußn. 72).

[152] *Blasche* (o. Fußn. 48), S. 64.

[153] *Spindler*, in: MünchKomm-AktG (o. Fußn. 48), § 91 Rn 32.

Zu beachten ist ferner § 25c KWG, wonach die Institute im Rahmen ihrer ordnungsgemäßen Geschäftsorganisation für interne Sicherungsmaßnahmen zu sorgen haben. Dabei sollen die Institute insbesondere Datenverarbeitungsanlagen einrichten, um Geschäftsbeziehungen und einzelne Transaktionen im Zahlungsverkehr zu erkennen, die aufgrund der Erfahrungen des Instituts über die Methoden der Geldwäsche, der Terrorismusfinanzierung und betrügerischer Handlungen zum Nachteil der Institute, als zweifelhaft oder ungewöhnlich erscheinen. Dabei sind unter „betrügerischen Handlungen" neben dem Betrug i.S.v. § 263 StGB sämtliche Handlungen von Unternehmensinternen wie –externen zu verstehen, die das Institut schädigen können.[154] Zur Erfüllung dieser Pflicht erlaubt die Norm die Erhebung, Verarbeitung und Nutzung personenbezogener Daten.

2.1.5.3
Basel II

Das durch den Baseler Ausschuss für Bankenaufsicht erarbeitete Regelwerk stellte zunächst einen internationalen Standard dar und ist mittlerweile über die Banken-[155] und die Kapitaladäquanzrichtlinie[156] auch in Deutschland umgesetzt.[157]

Zwar bezieht sich Basel II zunächst auf Eigenkapitalvorschriften von Kreditinstituten bzw. die Fähigkeit der Finanzsysteme der Banken, Risiken zu erkennen und zu verhindern. Auswirkungen des Regelwerks auf Firmenkunden der Banken aller Wirtschaftszweige sind jedoch zu erwarten, da die Kreditinstitute ihre Risiko- und Eigenkapitalkosten auf jenen Kunden abwälzen werden, die höhere Ausfallkosten verursachen.[158] Ein effektives Risikomanagementsystem wirkt sich somit positiv auf die Kreditvergabe aus.[159]

2.1.5.4
Organisationspflichten, § 33 WpHG

Mit einem Verweis auf § 25a KWG verlangt § 33 Abs. 1 WpHG die Einhaltung derselben organisatorischen Pflichten für Wertpapierdienstleistungsunternehmen, wie sie auch für Kreditinstitute gelten. Darüber hinaus fordert § 33 Abs. 1 Satz 2 Nr. 1 WpHG in Umsetzung der Richtlinie über Märkte für

---

[154] *Salvenmoser/Hauschka* (o. Fußn. 37), S. 331.
[155] Richtlinie 2006/48/EG des Europäischen Parlaments v. 14.06.2006 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute (Neufassung), ABlEU Nr. L 177 v. 30.06.2006, S. 1.
[156] Richtlinie 2006/49/EG des Rates vom 14.06.2006 über die angemessene Eigenkapitalausstattung von Wertpapierfirmen und Kreditinstituten (Neufassung), ABlEU Nr. L 177 v. 30.06.2006, S. 201.
[157] Gesetz zur Umsetzung der neu gefassten Bankenrichtlinie und der neu gefassten Kapitaladäquanzrichtlinie v. 17.11.2006, BGBl. 2006 I S. 2606.
[158] *Menzies* (o. Fußn. 33), S. 13.
[159] *Bitkom/DIN*, Kompass der IT-Sicherheitsstandards, S. 40, http://www.bitkom.org/files/documents/Kompass_der_IT-Sicherheitsstandards_haftung_(2).pdf (Stand: 22.05.2010)

Finanzinstrumente (MiFID)[160] insbesondere eine dauerhafte und wirksame Compliance-Funktion einzurichten. Wegen der starken inhaltlichen Übereinstimmungen mit dem bereits branchenfremd angewandten § 25a KWG ist eine Ausstrahlungswirkung von § 33 WpHG und damit auch die Pflicht zur Einrichtung einer Compliance-Funktion, ebenfalls denkbar.[161]

2.2
Ordnungswidrigkeit der Verletzung von Aufsichtspflichten

Unterlässt der Inhaber eines Unternehmens fahrlässig oder vorsätzlich seine zur Verhinderung von Zuwiderhandlungen erforderlichen Aufsichtspflichten, handelt er im Falle von betriebsbezogenen Verstößen, die mit Strafe oder Geldbuße bedroht sind, gemäß § 130 Abs. 1 OWiG ordnungswidrig.[162]

Beim Inhaber des Unternehmens handelt es sich im Falle einer Gesellschaft um den Geschäftsführer bzw. den Vorstand als das geschäftsführende Organ.[163] Da die Verletzung der Aufsichtspflicht jedoch eine betriebsbezogene Ordnungswidrigkeit darstellt, kann sich die Sanktion im Falle eines Verstoßes wegen der Durchgriffsmöglichkeit nach § 30 OWiG gegebenenfalls gegen die gesamte Gesellschaft als juristische Person und nicht gegen den Vorstand oder das einzelne, schuldhaft handelnde Mitglied[164] richten.[165] Tatbestandsvoraussetzungen der Vorschrift sind das Vorliegen der Verletzung der Aufsichtspflicht sowie das Vorhandensein einer bußgeldbewehrten Zuwiderhandlung.[166]

Welche Handlungen zur Abwendung von Zuwiderhandlungen geeignet sind, oder wie der Inhaber des Unternehmens seiner Aufsichtspflicht und damit seiner Sorgfaltspflicht adäquat nachkommt, ist jeweils im Einzelfall zu bestimmen.[167] Entsprechend § 130 Abs. 1 Satz 3 OWiG spielt insbesondere die De-

---

[160] Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates vom 21. April 2004 über Märkte für Finanzinstrumente, zur Änderung der Richtlinien 85/611/EWG und 93/6/EWG des Rates und der Richtlinie 2000/12/EG des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 93/22/EWG des Rates, *ABlEG Nr. L 145 v. 30.4.2004, S. 1.*

[161] Siehe ferner zum Konflikt zwischen dem BDSG und § 33b WpHG zur Verhinderung von Insidergeschäften *Karg*, CuA 11/2009, S. 13.

[162] § 130 Abs. 1 OWiG: 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, handelt ordnungswidrig, wenn eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre. Zu den erforderlichen Aufsichtsmaßnahmen gehören auch die Bestellung, sorgfältige Auswahl und Überwachung von Aufsichtspersonen.

[163] *Süßmann*, in: *Park*, Kapitalmarkstrafrecht, Teil 4, T1 § 130 OWiG Rn. 1.

[164] Zur Haftung des Unternehmensinhabers selbst auf Grund von § 130 OWiG siehe *Rehbinder*, in: *Hilty/Drexl/Nordemann*, Schutz von Kreativität und Wettbewerb, S. 521 f.

[165] *Rogall*, in: *Senge*, KK-OWiG, § 130 Rn. 6.

[166] *Bohnert*, OWiG, § 130 Rn. 16.

[167] *Bohnert* a.a.O., § 130 Rn. 19; bis auf wenige Ausnahmen, etwa die Notwendigkeit einer fünf Personen starken Revisionsabteilung bei mehr als 5000 Beschäftigten, hat die Rechtsprechung

legation von Verantwortung und die damit verbundene sorgfältige Auswahl des Aufsichtspersonals eine herausragende Rolle.[168] Im Bereich der börsennotierten Aktiengesellschaft ist das nach § 91 Abs. 2 AktG zu implementierende System zur Bestandssicherung, unter Berücksichtigung der konkretisierenden Anforderungen aus anderen Vorschriften, der Maßstab.

Unter einer betriebsbezogenen Zuwiderhandlung ist die Begehung einer Straftat oder Ordnungswidrigkeit durch jemand anderen als den Vorstand zu verstehen.[169] Gemeint sind Verstöße gegen öffentlich rechtliche Pflichten, etwa des Kartellrechts, nicht jedoch gegen das Unternehmen gewandte Delikte, wie Diebstähle oder Sachbeschädigungen.[170]

Die Rechtsfolge der Aufsichtspflichtverletzung ist gemäß § 130 Abs. 3 OWiG eine Geldbuße, die bei Vorliegen einer Straftat die Höhe von bis zu einer Millionen Euro erreicht. Teile der Literatur leiten aus § 130 OWiG die Pflicht zur Einrichtung einer umfassenden Compliance-Organisation ab.[171] Da die Ordnungswidrigkeit wegen einer Aufsichtspflichtverletzung bei bußgeldbewehrten Verstößen aus einer Vielzahl verschiedenster Rechtsgebiete entstammen kann (z. B. Kartellrecht, Kapitalmarktrecht, Umweltrecht, Arbeitsstrafrecht und auch Datenschutzrecht), lässt sich zumindest von einer mittelbaren Pflicht zur Implementierung einer solchen Organisation sprechen.[172]

In besonders risikogefährdeten Bereichen, etwa im Anwendungsfeld des Kartellrechts, wird jedenfalls eine strengere, über Stichproben hinausgehende Kontrolle bis hin zur intensiven Überwachung der Angestellten zu fordern sein.[173] In diesen Fällen trifft den Vorstand weiterhin eine gesteigerte Aufsichtspflicht.[174] Im Ergebnis hat der Betriebsinhaber sämtliche Maßnahmen zur Verhinderung von Wirtschaftsdelikten zu ergreifen, die möglich, geeignet, erforderlich sowie zumutbar sind, um diese zu verhindern.[175]

2.3
Der Sarbanes-Oxley Act: Erweiterte Offenlegung von Unternehmensdaten und interne Kontrollsysteme

Der Sarbanes-Oxley Act of 2002 (SOA)[176] ist ein amerikanisches Bundesgesetz, welches in Folge zahlreicher Unternehmenskrisen verabschiedet wurde, zu deren Ursachen Bilanzfälschungen, Täuschungen der Kapitalanleger und andere

bisher keine allgemeingültigen Regeln aufgestellt, *Hauschka/Greeve* (o. Fußn. 22), S. 166 m.w.N.

[168] *Rogall,* in: *Senge* (o. Fußn. 165), § 130 Rn. 5.
[169] *Bohnert* (o. Fußn. 166), § 130 Rn. 25.
[170] *Bohnert* a.a.O., § 130 Rn. 31.
[171] *Schmidt* (o. Fußn. 119), S. 1296; ähnlich *Kort* (o. Fußn. 61), S. 83.
[172] *Wecker/Galler*, in: *Wecker/Van Laak* (Hrsg.), Compliance in der Unternehmerpraxis, S. 37.
[173] *Rogall,* in: *Senge* (o. Fußn. 165) § 130 Rn. 58.
[174] *Rogall,* in: *Senge* a.a.O., § 130 Rn. 64.
[175] *Hauschka/Greeve* (o. Fußn. 22), S. 166 m.w.N.
[176] Am 30.07.2002 in Kraft getreten.

Wirtschaftsdelikte gehörten. Ziel des SOA ist der Schutz der Anleger durch eine detailliertere und verlässlichere Offenlegung von Unternehmensdaten. Die äußerst umfangreichen Forderungen des SOA, insbesondere im Hinblick auf das einzurichtende IKS, mit zum Teil scharfer Strafandrohung im Falle von Verstößen, haben betroffene deutsche Gesellschaften mit einer U.S.-Börsennotierung[177] zunächst vor große Herausforderungen mit vor allem hohem finanziellem Aufwand gestellt.[178] In den Jahren seit Inkrafttreten des SOA haben die Gesetzgeber der EG[179] und Deutschlands jedoch durch diverse Novellierungen des hiesigen Rechts einen Standard entwickelt, der der „Strenge" des SOA in kaum etwas nachsteht. In diesem Zusammenhang ist vor allem das BilMoG von großer Bedeutung, welches insbesondere den Begriff des „internen Kontroll- und Risikomanagementsystems im Hinblick auf den Rechnungslegungsprozess" etabliert hat.[180]

Ein Großteil der Regelungen des SOA bedurfte einer Ausgestaltung durch die U.S.-Börsenaufsichtsbehörde Securities and Exchange Commission (SEC), welche verbindliche Verordnungen, sog. *Final Rules*, zur Anwendung des Gesetzes beschloss. Die SEC ist ebenfalls die ermittelnde Behörde, wenn U.S.-börsennotierte Unternehmen gegen den SOA oder andere Börsengesetze verstoßen.[181] Ferner enthalten die allgemeinen Regelungen des Securities Exchange Act 1934 (SEA) und die diesen konkretisierenden *Final Exchange Rules* weitere, für die vorliegenden Arbeit relevante Vorschriften und Definitionen zur Auslegung des SOA.[182]

Im Folgenden soll auf die wichtigsten Regelungen des SOA mit den entsprechenden begleitenden Verordnungen und anderen Vorschriften eingegangen werden. Zunächst sind der örtliche und persönliche Anwendungsbereich des Gesetzes zu klären. Darauf folgt eine Darstellung der sich aus sec. 302 SOA, sec. 404 SOA und sec. 906 SOA ergebenen Organisationspflichten sowie den

---

[177] Neben dem SOA hat auch der Foreign Corrupt Practices Act große Bedeutung für ausländische Unternehmen, die an U.S.-Börsen notiert sind. Dieser wendet sich konkret gegen Korruption und verlangt in diesem Zusammenhang ebenfalls eine spezielle Buchführung und Kontrollen, welche allerdings hinter den Anforderungen der sec. 404 SOA-Kontrollen zurückbleiben und daher nicht Gegenstand der vorliegenden Betrachtung sind, siehe hierzu *Menzies* (o. Fußn. 33), S. 24 ff.

[178] So hat die SAP AG für die Implementierung des internen Finanzkontrollsystems nach sec. 404 SOA einen Zeitraum von drei Jahren benötigt, mit internen Umsetzungsaufwendungen von ca. 17.000 Mannstunden und unter Zuhilfenahme externer Spezialisten für ca. 11 Mio. EUR, *Brandt/Mucic* in: *Wagenhofer* (Hrsg.), Controlling und Corporate Governance-Anforderungen, S. 228.

[179] Siehe zur Entwicklung im Bereich der Corporate Governance und Compliance in Europa *Menzies* (o. Fußn. 33), S. 35 ff.

[180] Drucks 16/10067, S. 39.

[181] *Neundorf,* in: *Hauschka* (o. Fußn. 27), § 27, Rn. 16; siehe ferner das aktuelle Beispiel im Fall *Daimler AG* von diesem März http://www.finanznachrichten.de/nachrichten-2010-03/16454508-update2-daimler-zahlt-in-us-korruptionsstreit-185-mio-usd-kreise-015.htm (Stand: 24.03.2010)

[182] Daneben kann der im Rahmen dieser Arbeit nicht behandelte Securities Act 1933 eine Rolle spielen.

den einzelnen Vorstandsmitgliedern zugewiesenen, zivil- und strafrechtlichen Verantwortlichkeiten für die Finanzberichterstattung. Für deutsche Unternehmen im Anwendungsbereich des SOA wird nachfolgend der Begriff Emittent verwendet.

2.3.1
Anwendungsbereich

Der SOA richtet sich zumeist[183] an sog. *issuers*. Hierbei handelt es sich nach der Definition in sec. 2 (7) SOA im Wesentlichen um Gesellschaften, deren Aktien gemäß sec. 12 SEA an der New York Stock Exchange, der American Stock Exchange oder der Nasdaq registriert sind sowie um Gesellschaften, die ihre Wertpapiere öffentlich in den U.S.A. anbieten, ohne börsennotiert zu sein und damit gemäß sec. 15 (d) SEA Berichte bei der SEC einzureichen haben.[184]

Der erste Fall betrifft neben börsennotierten Gesellschaften auch Unternehmen, die wegen einer Berührung des *Interstate Commerce*[185] und zusätzlich einem Kapital von mehr als 10 Mio. U.S.-Dollar sowie Wertpapieren mit 500 oder mehr Inhabern, einer Registrierungspflicht nach sec. 12 g SEA unterliegen.[186]

Daraus ergibt sich, verkürzt dargestellt, eine Anwendbarkeit des SOA für deutsche Unternehmen zum einen, wenn diese an einer U.S.-Börse notiert sind,[187] zum anderen, wenn eine Berührung des Interstate Commerce mit den weiteren genannten Voraussetzungen vorliegt und zusätzlich die Bedingung[188] erfüllt ist, dass mindestens 300 der 500 Wertpapierinhaber ihren Sitz in den U.S.A. haben. Schließlich findet der SOA Anwendung, wenn das Unternehmen seine Aktien öffentlich in den U.S.A. anbietet und deshalb registrierungspflichtig ist.[189] Der SOA hat daneben Auswirkungen auf die Tochterunternehmen der Emittenten, sei es durch ihre Einbindung in das zu errichtende IKS oder durch ihre Jahresabschlussprüfung nach Standards des SOA.[190]

---

[183] Die Normen des SOA haben unterschiedliche Adressaten.
[184] *Carl*, in: *Spahlinger/Wegen* (Hrsg.), Internationales Gesellschaftsrecht in der Praxis, Rn. 1625.
[185] Definition in sec. 3 (a) (17) SEA.
[186] *Block*, BKR 2003, 774 (775).
[187] Im Jahre 2006 waren 17 deutsche Unternehmen an der NYSE gelistet: Allianz, Altana, BASF, Bayer, DaimlerChrysler, Deutsche Bank, Deutsche Telekom, E.ON, Epcos, Fresenius Medical Care, Infineon, Pfeiffer Vacuum, SAP, Schering, SGL Carbon und Siemens. GPC Biotech und Aixtron sind an der Nasdaq gelistet, Bannenberg, in: Wabnitz/Janovsky (Hrsg.), Handbuch des Wirtschafts- und Steuerrechts, Kapitel 10, Rn. 142 dort Fußn. 270. Große Unternehmen wie Allianz, Bayer, Infenion und jüngst die Deutsche Telekom verlassen die NYSE jedoch aufgrund der mit dem Listing verbundenen immensen Kosten, weshalb im Jahr 2011 nur noch sechs deutsche Unternehmen an der Wall Street vertreten sein werden, FAZ v. 22.04.2010, S. 22.
[188] Sec. 12 (g) (3) SEA i.V.m. Exchange Act Rule 12g3-2 (a), (b).
[189] *Block* (o. Fußn. 189), S. 775.
[190] *Carl*, in: *Spahlinger/Wegen* (o. Fußn. 184), Rn. 1626.

Es steht im Ermessen der SEC, Ausnahmeregelungen für ausländische Unternehmen zu erlassen. So gelten etwa für sog. *foreign private issuers* eingeschränkte Anforderungen. Laut Exchange Act Rule 3b-4 (c) handelt es sich bei jedem ausländischen, privaten Emittenten um einen *foreign private issuer*, außer die beiden nachfolgenden Bedingungen liegen vor:

- Über 50% der Anteile befinden sich in Händen von US-Anlegern, und
- entweder die Mehrheit des Managements oder des Vorstands sind in den USA beheimatet, oder über 50% der Vermögensgegenstände des Emittenten sind in den USA gelegen, oder das Unternehmen wird überwiegend in den USA verwaltet.[191]

Nach dieser Definition ist also davon auszugehen, dass es sich bei den meisten an einer U.S.-Börse notierten, deutschen Unternehmen um *foreign private issuers* handelt.

2.3.2
Pflichten der Geschäftsführung

Der SOA gibt eine Reihe von Organisationspflichten vor, wonach die Geschäftsleitung bzw. der Vorstand der Emittenten insbesondere im Bereich der Finanzen effektive IKS zu errichten haben. Im Jahresabschlussbericht, der bei der SEC eingereicht wird, hat der Vorstand zu bestätigen, dass er den entsprechenden Forderungen nachgekommen ist. Diesem Bericht ist ferner eine Bestätigungserklärung beizulegen, in welcher der Vorstand die Richtigkeit des Berichts beeidet. Schließlich attestiert der Abschlussprüfer die Korrektheit der gemachten Angaben.

2.3.2.1 Organisationspflichten

Zur Konkretisierung der größtenteils vagen Vorgaben aus sec. 302 SOA[192] und sec. 404 SOA hat die SEC Final Rules erlassen, die am 29. August 2002[193] bzw. am 14. August 2003[194] in Kraft getreten sind. Diese werden wiederum von ebenfalls neu eingefügten Exchange Act Rules im SEA gesetzlich flankiert. Hiernach haben die Emittenten zunächst *disclosure controls and procedures* einzurichten, welche aus sec. 302 SOA abgeleitet werden und die Offenlegung von Informationen sowie ein effizientes Informationsmanagement zum Ziel haben. Darüber hinaus ist eine *internal control over financial reporting* zu

[191] *Flägel*, NZG 2008, 576 (577).
[192] Sec. 302 (a) (4) (A), (B) SOA etwa weist den Unterzeichnern des Berichts lediglich ihre Verantwortlichkeit über die Einrichtung und Aufrechterhaltung interner Kontrollen zu, welche die Bekanntgabe wesentlicher Informationen im Zusammenhang mit dem Emittenten gewährleisten.
[193] *Final Rule* v. 28.08.2002, Release No. 33-8124, http://www.sec.gov/rules/final/33-8124.htm (Stand: 08.03.2010).
[194] *Final Rule* v. 5.06.2003, Release No. 33-8238, http://www.sec.gov/rules/final/33-8238.htm (Stand: 08.03.2010).

implementieren, welche sich aus sec. 404 SOA ableiten lässt und auf die interne Kontrolle des Finanzwesens abzielt.

2.3.2.1.1 Disclosure controls and procedures

Diese vom Emittenten einzurichtenden Offenlegungskontrollen und -verfahren beinhalten nach ihrer Definition[195] Kontrollen und andere Verfahren, welche gewährleisten, dass die im Rahmen des bei der SEC einzureichenden Jahresabschlussberichts offen zu legenden Informationen in der vorgegebenen Zeit dokumentiert, verarbeitet, zusammengefasst und berichtet werden. Die Informationen sind ferner anzusammeln und dem Management, insbesondere dem *principle* bzw. *chief executive officer* (CEO) und dem *financial executive officer* (CFO)[196] derart mitzuteilen, dass diese in angemessener Zeit Entscheidungen über eine erforderliche Offenlegung treffen können. Dies gilt ausweislich der Begründung der SEC auch für deutsche Unternehmen.[197] Die SEC verlangt keine speziellen Verfahren bei der Umsetzung ihrer Vorgaben, vielmehr soll sich dies nach der konkreten Situation des Emittenten richten.[198]

2.3.2.1.2 Internal control over financial reporting

Laut der Definition[199] der internen Kontrolle über die Finanzberichterstattung verlangt diese ein unter der Aufsicht von CEO und CFO entwickeltes, den Vorstand und weiteres leitendes Personal verpflichtendes Verfahren, welches eine hinreichend verlässliche Finanzberichterstattung sicherstellt und die Vorbereitung der externen Rechnungslegung im Einklang mit den allgemeinen Grundsätzen ordnungsgemäßer Buchführung[200] gewährleistet. Effektiv sind die Verfahren, wenn sie

- sicherstellen, dass die gesammelten Informationen angemessen detailliert und ordentlich die Geschäftsvorgänge und die Verwendung der Vermögenswerte des Emittenten wiedergeben; und
- gewährleisten, dass zum einen die Geschäftsvorgänge hinreichend dokumentiert werden, damit die Rechnungslegung in Übereinstimmung mit den allgemeinen Grundsätzen der ordentlichen Buchfüh-

[195] Exchange Act Rule 13a-15 (e).
[196] Nach h.M. handelt es sich im deutschen Gesellschaftsrecht beim CEO um den Vorstandsvorsitzenden und beim CFO um den Finanzvorstand, zur Diskussion siehe *Nicklisch* (o. Fußn. 78), S. 171 ff.
[197] *Final Rule* 33-8124 (o. Fußn. 193), dort Abschnitt II B. 1. a).
[198] *Final Rule* 33-8124 a.a.O., dort Abschnitt II B. 3. 7. Absatz.
[199] Exchange Act Rule 13a-15 (f).
[200] Die SEC nennt in diesem Zusammenhang § 319 der Codification of Statements on Auditing Standards oder vergleichbare, vom Public Company Accounting Oversight Board (PCAOB) anerkannte Regeln, siehe *Final Rule* v. 05.06.2003 (o. Fußn. 194), dort Abschnitt II. A. 1. 1. Absatz.

rung möglich ist, und dass zum anderen Einnahmen und Ausgaben nur mit Zustimmung der Geschäftsleitung getätigt werden; und

– gewährleisten, dass unautorisierte Akquisitionen, oder die Verwendung oder Veräußerung von Vermögenswerten mit erheblichen Auswirkungen auf die Rechnungslegung verhindert oder rechtzeitig aufgedeckt werden.

2.3.2.2 Jahresabschlussbericht und Bestätigungserklärung

Im Nachfolgenden werden die aus Emittentensicht problematischsten Regelungen des SOA, welche erhebliche Sanktionen nach sich ziehen können, dargestellt.

2.3.2.2.1 Beurteilungspflichten im Jahresabschlussbericht

Am Ende jedes Geschäftsjahres haben der CEO und der CFO zusammen mit der Geschäftsleitung die Effektivität der disclosure controls and procedures[201] (DCP) und der internal control over financial reporting[202] (ICFR) zu beurteilen. Letztere Beurteilung soll auf einem passenden, von Experten anerkannten Kontrollregelwerk beruhen. Als Beispiel nennt die SEC[203] in diesem Zusammenhang die von der *Committee of Sponsoring Organizations of the Treadway Commission* zusammengetragenen Anforderungen an Kontrollsysteme (COSO).[204] Die Beurteilung hat ferner etwa Ausführungen darüber zu enthalten, ob die ICFR im zurückliegenden Jahr Veränderungen ausgesetzt waren, die die Kontrolle erheblich beeinträchtigt haben oder eine Beeinträchtigung mit hinreichender Sicherheit wahrscheinlich machen.[205]

Die Beurteilung ist Teil des bei der SEC einzureichenden Jahresabschlussberichts, dessen Inhalt sich für alle foreign private issuers[206] an dem von der SEC für die Jahresabschlussprüfung herausgegeben Formular Form 20-F orientiert.[207] Dem Abschlussbericht sind detaillierte Erklärungen zu den DCP und der ICFR anzuhängen,[208] worin ebenfalls der in sec. 404 SOA geforderte *internal control report* umfasst ist. Die Richtigkeit der gemachten Angaben ist in der Bestätigungserklärung zu zertifizieren.[209]

---

[201] Exchange Act Rule 13a-15 (b).
[202] Exchange Act Rule 13a-15 (c).
[203] *Final Rule* v. 05.06.2003 (o. Fußn. 194), dort Abschnitt II.B.3.a.
[204] Mit Anwendungsbeispiel auf sec. 404 SOA *Wolf*, BC 2003, 268 (269 f.).
[205] Exchange Act Rule 13a-15 (d).
[206] Außer Kanada, *Nicklisch* (o. Fußn. 78), S. 163.
[207] Form 20-F, http://www.sec.gov/about/forms/form20-f.pdf (Stand. 10.03.2010).
[208] Form 20-F, Item 15.
[209] Siehe die nachfolgenden Abschnitte bezüglich der konkret zu machenden Angaben.

2.3.2.2.2 Bestätigungserklärung nach sec. 302 SOA

Der Inhalt der sog. zivilrechtlichen Bestätigungserklärung nach sec. 302 SOA sowie die Pflicht, diese Angaben wahrheitsgetreu zu machen, bestand bereits vor Erlass des SOA. Auch die mögliche Haftung ist keine Neuerung, wohl aber die erweiterte Verantwortung von CEO und CFO.[210]

a) Inhalt der Bestätigungserklärung

Auf Grundlage von sec. 302 SOA hat die SEC Regelungen erlassen, die den CEO und den CFO der Emittenten verpflichten, die Richtigkeit des Jahresabschlussberichts persönlich, schriftlich zu bestätigen. Diese von den beiden Vorstandsmitgliedern unterschriebene Bestätigungserklärung ist als Anhang zum Jahresabschlussbericht bei der SEC mit einzureichen.[211] Der Inhalt der Erklärung ist von der SEC verbindlich vorgegeben.[212] CEO und CFO haben danach im Wesentlichen jeweils folgende Angaben zu machen:

- Sie haben den Jahresabschlussbericht gemäß Form 20-F überprüft;
- Nach ihrer Kenntnis enthält der Bericht weder falsche Angaben zu wesentlichen Einzelheiten, noch fehlen wesentliche Einzelheiten, deren Berichtigung oder Mitteilung erforderlich sind, um eine Irreführung zu vermeiden;[213]
- Nach ihrer Kenntnis geben die hier eingereichte Rechnungslegung und die anderen Informationen zu Finanzen die finanzielle Lage, die Geschäftsergebnisse und den Cash Flow des Unternehmens im Berichtszeitraum in allen wesentlichen Punkten wahrheitsgetreu wieder;
- Sie bestätigen die Verantwortlichkeit für die Errichtung und Aufrechterhaltung der DCP und der ICFR. Ferner bestätigt das Vorstandsmitglied, dass es
    - effektive DCP entwickelt hat oder unter seiner Beaufsichtigung entwickeln ließ, welche sicherstellen, dass die wesentlichen unternehmensbezogenen Informationen, inklusive aller Informationen über die Tochtergesellschaften, intern an die Geschäftsleitung weitergeleitet werden;
    - effektive[214] ICFR entwickelt hat oder unter seiner Beaufsichtigung entwickeln ließ;

[210] *Nicklisch* (o. Fußn. 78), S. 165.
[211] Exchange Act Rule 13a-14 (a).
[212] Form 20-F, Certifications, S. 65 ff.
[213] *Block* (o. Fußn. 189), S. 776.
[214] Zur Effektivität siehe Abschnitt 2.3.2.1.2.

- die Effektivität der DCP zum Ende des Berichtszeitraums beurteilt und die jeweiligen Schlussfolgerungen dem vorliegenden Bericht beigefügt hat;
- jegliche Änderung der ICFR im Berichtszeitraum, die die Kontrolle erheblich beeinträchtigt hat oder eine Beeinträchtigung mit hinreichender Sicherheit wahrscheinlich macht, durch den vorliegenden Bericht offen legt;

– Zusammen mit dem (den) anderen verantwortlichen Vorstandsmitglied(ern) hat das Vorstandsmitglied dem Abschlussprüfer und dem *audit committee*[215] seine Beurteilung darzulegen bezüglich

- aller erheblichen Mängel und wesentlichen Schwächen in der Entwicklung oder Durchführung der ICFR, die mit hinreichender Wahrscheinlichkeit die Fähigkeit des Unternehmens beeinträchtigen, Finanzinformationen zu dokumentieren, zu verarbeiten, zusammenzufassen und zu berichten; sowie
- jeglicher Täuschung oder jedes Betrugs, bei dem Management oder andere Angestellte mit Einfluss auf die ICFR beteiligt sind.

b) Mögliche Rechtsfolge bei unwahrer Bestätigungserklärung

Eine wahrheitswidrige oder irreführende Bestätigungserklärung nach sec. 302 SOA kann zivilrechtliche Folgen haben. Gemäß sec. 18a SEA kann der Unterzeichner einer nicht wahrheitsgemäßen oder irreführenden Bestätigungserklärung von jeder Person in Anspruch genommen werden, die im Vertrauen auf die Erklärung Wertpapiere zu einem Preis, der von der Erklärung beeinflusst wurde, gekauft oder verkauft hat und der damit ein Schaden entstanden ist. Die Vorschrift richtet sich an alle betroffenen Anleger. Zwar kann sich der Unterzeichner exkulpieren, wenn er beweisen kann, dass er im guten Glauben gehandelt hat und keine Kenntnis von der Mangelhaftigkeit der Erklärung hatte. Da die Unterzeichner im Rahmen des Abschlussberichts jedoch vielfach bestätigen müssen, dass sie die Verantwortung für die Implementierung der Kontrollen übernommen und diese auf etwaige Schwachstellen hin überprüft haben, erscheint eine Exkulpation nahezu undenkbar.[216]

Daneben können die Unterzeichner einer unwahren Bestätigungserklärung gemäß sec. 10b SEA und Exchange Act Rule 10b-5 wegen manipulativen und betrügerischen Verhaltens von Anlegern oder der SEC selbst in Anspruch genommen werden.[217] Der Vorteil gegenüber dem Anspruch aus sec. 18a SEA

[215] Im deutschen Gesellschaftsrecht handelt es sich hierbei um den gegebenenfalls nach § 107 Abs. 3 S. 2 AktG einberufenen Prüfungsausschuss.
[216] *Nicklisch* (o. Fußn. 78), S. 166.
[217] Die SEC hat darüber hinaus einen Klageanspruch nach sec. 13 (a) und Sec. 15 (d) SEA, *Final Rule* v. 28.08.2002 (o. Fußn. 193), dort Abschnitt II B. 6.

besteht hier aus Gläubigersicht darin, dass die Anleger wegen der sog. *fraud-on-the-market theory* nicht zu beweisen haben, dass der Kauf oder Verkauf von Wertpapieren nur aufgrund der Annahme getätigt wurde, dass die Erklärung der Unterzeichner der Wahrheit entspricht.[218]

2.3.2.2.3
Bestätigungserklärung nach sec. 906 SOA

Über sec. 906 SOA wurde weiterhin im U.S. Strafgesetzbuch[219] der neue § 1350 eingefügt, welcher verlangt, dass CEO und CFO in einer weiteren strafrechtlichen Bestätigungserklärung beurkunden, dass der Jahresabschlussbericht mit den Regelungen des SEA übereinstimmt sowie dass der Bericht nach ihrer Kenntnis die finanzielle Lage des Emittenten in allen wesentlichen Punkten wahrheitsgetreu wiedergibt. Diese Erklärung ist ebenso im Anhang des Jahresabschlussberichts mit einzureichen.[220]

Bei Verstößen drohen empfindliche Geld- und Haftstrafen, welche den CEO und den CFO persönlich treffen. Wird die Bestätigungserklärung abgegeben, obwohl der Unterzeichner weiß, dass der Jahresabschluss nicht den gesetzlichen Anforderungen entspricht, kann dies mit einer Geldstrafe bis zu einer Millionen U.S. Dollar oder einer Haftstrafe bis zu 10 Jahren sanktioniert werden oder beides.[221] Bei einem wissentlichen und willentlichen Verstoß, droht sogar eine fünf Millionen U.S. Dollar hohe Geldstrafe oder ein Freiheitsentzug bis zu 20 Jahren oder beides.[222]

2.3.3
Abschlussprüferbericht

Schließlich verlangt sec. 404 (b),[223] dass dem Jahresbericht ein weiteres Dokument angehängt wird, in dem der Abschlussprüfer des Emittenten, der zudem ein registrierter und unabhängiger Wirtschaftsprüfer sein muss,[224] die Einschätzungen des CEO und des CFO bezüglich der Effektivität der ICFR überprüft, Mängel seinerseits evaluiert und die Erklärung gegebenenfalls at-

[218] *Nicklisch* (o. Fußn. 78), S. 167 m.w.N; auch die für deutsche Verhältnisse ungewöhnlich hohen Prozesskosten in den U.S.A. können als „Haftungsrisiko" qualifiziert werden.
[219] United States Code, Title 18 – Crimes and criminal procedure.
[220] Exchange Act Rule 13a-14 (b).
[221] Siehe 18 US Code 1350 (c) (1).
[222] Siehe 18 US Code 1350 (c) (2).
[223] Vgl. auch Form 20-F (o. Fußn. 207), Item 15 c).
[224] Definition in sec. 2 (a) (12) SOA.

testiert.[225] Diese Überprüfung hat mit den vom PCAOB entwickelten Standards übereinzustimmen.[226]

Dadurch entsteht eine mit der in Deutschland vergleichbaren Situation,[227] wobei der Prüfer im Rahmen der Abschlussprüfung nach dem SOA die Standards der PCAOB nicht zur Konkretisierung gesetzlicher Vorgaben heranzieht, sondern an diese gebunden ist. Daher empfiehlt sich für Emittenten, ihr IKS an den Anforderungen des *Auditing Standards No.* 5[228] auszurichten, da dieser der Prüfung der ICFR zugrunde gelegt wird.[229]

2.4
Zusammenfassende Anforderungen an das interne Kontrollsystem

Aus dem Vorangegangenen ergibt sich zunächst allgemein die Pflicht des Vorstands dafür Sorge zu tragen, dass die Gesellschaft vor bestandsgefährdenden Entwicklungen geschützt wird. Hierzu sind nach h.M. eine angemessene interne Revision und ein angemessenes Risikomanagementsystem zu implementieren. Konkret erfordern etwa die umfangreichen Offenlegungspflichten durch den SOA sowie eingeschränkt auch durch das BilMoG[230], eine detaillierte Dokumentation sämtlicher Vorgänge mit potentiellem Einfluss auf die Rechnungslegung. Enthüllt der Abschlussprüferbericht erhebliche Differenzen im Jahresabschluss oder Mängel der internen Kontrollen, drohen strikte Sanktionen wegen unwahren oder irreführenden Bestätigungserklärungen im Rahmen des SOA. Auch deutsche Gerichte sprechen empfindliche Haft- und Geldstrafen im Zusammenhang mit Anlegerbetrug aufgrund falscher Offenlegungen aus.[231] Daneben drohen Geldbußen in Millionenhöhe bei einer Verletzung der Aufsichtspflichten gemäß § 130 OWiG.

Das „ob" und das „wie" der Kontrolle liegt vollkommen im Ermessen des Vorstands und hat sich an der konkreten Situation der Gesellschaft, etwa an ihrer Art, Größe oder dem Kapitalmarktzugang zu orientieren. Der Vorstand handelt zumindest gemäß § 93 AktG seiner Sorgfaltspflicht entsprechend, wenn er seine unternehmerischen Entscheidungen aufgrund angemessener Information zum Wohle der Gesellschaft trifft.

---

[225] Der Abschlussprüfer muss etwa „*significant deficiencies*" (Ziff. 80) und „material weaknesses" (Ziff. 90 ff.) der Kontrollen beurteilen, siehe *Auditing Standard No. 5*, http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5.aspx#wrappingup (Stand: 11.03.2010).

[226] Release No. 33-8222 v. 25.04.2003, http://www.sec.gov/rules/other/33-8222.htm (Stand: 11.03.2010);

[227] Siehe Abschnitt 2.1.4.2.

[228] *Auditing Standard No. 5 (*o. Fußn. 225).

[229] *Menzies* (o. Fußn. 33), S. 19.

[230] Siehe sogleich Tabelle 1.

[231] Siehe etwa *BGH*, Urt. v. 16.12.2004 – 1 StR 420/03, NJW 2005, 445, hier wurde eine Millionenstrafe an ehemalige Vorstände eines Medienunternehmens aufgrund von 400 AktG verhängt. Das *LG München I,* Urt. v. 21.11.2002 – 6 KLs 305 Js 34066/02, NStZ 2004, 291 verhängte eine Freiheitsstrafe von 7 Jahren wegen schwerem Kursbetrug.

Kriterium	BilMoG	Sarbanes-Oxley Act
Explizite Forderung zur Einrichtung eines IKS	Nein / im Falle einer Nichteinrichtung ist Negativerklärung notwendig	Ja / gesetzliche Verpflichtung seitens des CEO und CFO
Effektivitätsüberwachung/-überprüfung	Überwachung durch Prüfungsausschuss (sofern eingerichtet) oder Aufsichtsrat	Überprüfung durch CEO und CFO
Berichterstattung durch Abschlussprüfer	Ja / über wesentliche Schwächen des internen Kontroll- und Risikomanagementsystems bezogen auf den (Konzern-) Rechnungslegungsprozess	Ja /über bedeutsame Kontrollmängel und über wesentliche Kontrollschwächen
Offenlegungspflicht/ -umfang	Ja / wesentliche Merkmale des internen Kontroll- und Risikomanagementsystems im Hinblick auf den (Konzern-) Rechnungslegungsprozess	Ja / Bestätigung der CEO- und CFO-Verantwortung zur Einrichtung der ICFR, Aussagen zur Effektivität, Aussagen zum umgesetzten Rahmenwerk sowie eine Bestätigung über das Testat des Abschlussprüfers hinsichtlich der Effektivität der ICFR

Tabelle 1: Gegenüberstellung der Anforderungen nach BilMoG und Sarbanes-Oxley Act[232]

Bei einem den Ausgangspunkt für diese Arbeit bildenden, weltweit operierenden Konzern mit Mitarbeitern im sechsstelligen Bereich und Umsätzen im Milliardenbereich, mit aus der Börsennotierung in Deutschland und den U.S.A. resultierendem, erschöpfenden Kapitalmarktzugang hat der Vorstand von einem erhöhten Missbrauchsrisiko auszugehen. Bekannte Fälle um Korruptionsskandale, wie jene der *Siemens AG* und aktuell der *Daimler AG*, haben ferner bewiesen, dass die mit Wirtschaftsdelikten verbundenen unmittelbaren und mittelbaren Schäden das Wohl der Gesellschaft erheblich zu beeinträchtigen vermögen. Daher ist vorliegend die strengst mögliche Interpretation von § 91 Abs. 2 AktG und den verwandten Vorschriften anzunehmen, womit der Sorgfaltspflicht entsprechend ein umfassendes, nachweislich wirksames IKS zu fordern ist.[233]

[232] *Wolf* (o. Fußn 92), S. 924.

[233] Dies gilt umso mehr vor dem Hintergrund zunehmend auftretender, sektorspezifischer konkreter Organisationspflichten zur Errichtung von internen Kontroll- und Risikomanagementsystemen.

Im Allgemeinen ist das IKS bzw. das Risikomanagementsystem nach dem LG Berlin so auszugestalten, dass auf einer ersten Stufe die Früherkennung bestandsgefährdender Entwicklungen durch geeignete Maßnahmen gewährleistet ist und auf einer zweiten Stufe die eingeleiteten Maßnahmen überwacht werden.[234] Der SOA empfiehlt zur Erreichung dieses Ziels die Anwendung des COSO-Modells, welches die fünf Komponenten Kontrollumfeld, Risikobeurteilung, Kontrollaktivitäten, Information und Kommunikation sowie Überwachung umfasst. Zur Risikobeurteilung gehört die Identifizierung, Analyse, Einschätzung und Steuerung von Risiken.[235] Der allgemeine Teil der MaRisk[236] stellt ebenfalls mit Gestaltungshinweisen eine gute erste Orientierungshilfe für die Implementierung des Risikomanagementsystems dar.[237]

Nach einer überwiegenden Meinung hat sich der Vorstand bei der Architektur des Systems an den Anforderungen des Abschlussprüfers zu orientieren. Dieser prüft gemäß IDW PS 340 neben dem Vorhandensein eines Risikofrüherkennungssystems, ob folgende Maßnahmen erfolgt sind: Festlegung der Risikofelder, Risikoerkennung und -analyse, Risikokommunikation, Zuordnung von Verantwortlichkeiten und Aufgaben, Überwachungssystem, Dokumentation.

---

[234] *LG Berlin* (o. Fußn. 72), S. 970; *Hüffer* (o. Fußn. 45), § 91 Rn. 6-8.

[235] Siehe zum COSO-Modell *Menzies* (o. Fußn. 33), S. 6 f. und allgemein zur Implementierung von Risikomanagementsystemen *Pampel/Glage,* in: *Hauschka* (o. Fußn. 27), § 5.

[236] MaRisk, AT 4 Allgemeine Anforderungen an das Risikomanagement, siehe Abschnitt 2.1.5.2.

[237] IT-Dienstleistungsunternehmen können ferner auf weitere nationale und internationale Standards zurückgreifen. Zu nennen ist in diesem Zusammenhang insbesondere die vom Technischen Gemeinschaftskomitee „Information Technology" der Internationalen Normenorganisationen ISO und IEC entwickelte ISO/IEC 27001, welche einen internationalen Standard für Informationssicherheits- und Managementsysteme darstellt und dabei sogar über die Anforderungen des SOA hinaus geht, siehe www.jtc1sc27.din.de (Stand: 14.03.2010) und *Russenberger*, Einhaltung der Anforderungen aus dem Sarbanes-Oxley Act mit Hilfe der Standards ISO/IEC 27001 & 27002, Diplomarbeit, http://www.russenberger.com/uni/SOX%20and%20ISO%202700x%20-%20public%20version.pdf, (Stand: 15.03.2010). Zu erwähnen ist auch der zum Deutschen Institut für Normung e.V. (DIN) gehörende Arbeitsausschuss „IT-Sicherheitsverfahren" des Normenausschusses Informationstechnik „*NIA-27*", http://www.nia.din.de/cmd?level=tpl-rubrik&languageid=de&cmsrubid=nia27 (Stand: 14.03.2010). Ferner spielt das bereits vorgestellte IT-Risikomanagement eine herausragende Rolle, siehe Abschnitt 2.1.5.1.

Um diesen Anforderungen gerecht zu werden, ist ein konzernweit organisiertes Anti Fraud Management durchzuführen. Zum AFM gehören die drei wesentlichen Elemente Vermeidung, Entdeckung und Reaktion im Hinblick auf Fälle von Wirtschaftskriminalität.[238] In diesem Rahmen ist es Aufgabe des AFM, sämtliche Abläufe und Prozesse innerhalb des Unternehmens auf Risikogefährdungen hin zu analysieren. In besonders sensiblen Hochrisikobereichen sind entsprechende präventive Maßnahmen zur Verhinderung von Fraud zu ergreifen. Hierzu gehören organisatorische Vorkehrungen wie die Einhaltung des sog. Vier-Augen-Prinzips oder Jobrotationen in empfindlichen Bereichen. Wo diese Methoden alleine nicht weiterhelfen, sind intensivere Mittel wie die Einrichtung anonymer Whistleblowing-Hotlines, Videoüberwachung oder automatische Datenanalysen zur Verhinderung und Bekämpfung von Wirtschaftsdelikten einzusetzen.[239] Einige dieser Maßnahmen erfordern zugleich den Zugriff auf personenbezogene Daten, womit der Anwendungsbereich des BDSG grundsätzlich eröffnet ist.

[238] *KPMG,* Anti Fraud Management, 2006, S.11.
[239] Eine umfassende Darstellung der AFM-Maßnahmen erfolgt sogleich in Abschnitt 4.

3
Datenschutzrechtliche Vorgaben

Das vom Vorstand des Unternehmens einzurichtende IKS erfordert in vielen Fällen den Umgang mit personenbezogenen Daten der Arbeitnehmer. Diese unterliegen im Bereich der Überwachung der elektronischen Kommunikation der Beschäftigten dem besonderen Schutz bereichsspezifischer Datenschutzvorschriften aus dem TMG und dem TKG. Ansonsten fällt, in Ermangelung einer Spezialregelung, der Umgang mit personenbezogenen Arbeitnehmerdaten in den Anwendungsbereich des BDSG. Im Folgenden sollen die wesentlichen datenschutzrechtlichen Implikationen dargestellt werden, mit denen sich der Vorstand beim Aufbau und Betrieb des Kontrollsystems konfrontiert sieht. Besondere Aufmerksamkeit wird dabei der neuen Norm § 32 BDSG gewidmet, welche den Datenschutz in Beschäftigungsverhältnissen regelt. Nach der letzten größeren Novellierung des BDSG im Jahre 2001, welche in großen Teilen der Umsetzung der Datenschutzrichtlinie[240] diente, wurde der § 32 im Zuge der BDSG-Novelle II neu in das Gesetz eingefügt und trat zum 1. September 2009 in Kraft.[241] Viele Kritiker sehen in der Vorschrift jedoch lediglich einen Akt von Symbolpolitik, mit der sich die scheidende Bundesregierung auf überhastete Weise gegen die sich häufenden sog. Datenschutzskandale positionieren wollte.[242]

3.1
Anwendbarkeit bereichsspezifischer Regelungen aus TKG und TMG

Sektorspezifische, den Datenschutz betreffende Regelungen gehen dem BDSG vor. Vor allem im Bereich der Überwachung der Telefon- und E-Mail-Kommunikation spielen die Vorschriften des TKG, bzw. bei der Überwachung der Internetnutzung der Beschäftigten die Vorschriften des TMG, eine herausragende Rolle. Jene Überwachungsmaßnahmen, die insbesondere auf den Zugriff auf geschäftliche E-Mails gerichtet sind, dienen jedoch mehr der Feststellung, ob die Beschäftigten ihren arbeitsvertraglich geschuldeten Pflichten nachkommen. Für die Risiken, gegen welche sich das IKS wendet, haben derartige Praktiken kaum eine Relevanz.[243]

Daher soll lediglich kurz umrissen werden, dass sich die Anwendbarkeit der genannten Normen danach richtet, ob der Arbeitnehmer die private Nutzung der Kommunikationsmittel gestattet hat oder nicht. Ist dies der Fall, so ist der

[240] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24.05.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABlEG Nr. L 281 v. 23.11.1995, S. 31.
[241] Gesetz zur Änderung datenschutzrechtlicher Vorschriften v. 14.8.2009, BGBl. I S. 2814.
[242] Für eine Auswahl der kritischen Stimmen aus dem juristischen Schrifttum siehe o. Fußn. 19.
[243] Auch wenn nicht auszuschließen ist, dass Wirtschaftsdelikte durch eine Überwachung oder Überprüfung der Kommunikation der Beschäftigten aufgedeckt werden.

Arbeitgeber etwa bei der Gestattung privater E-Mail-Nutzung nach h.M. Diensteanbieter i.S.d § 3 Nr. 6 TKG[244] und hat insbesondere das Fernmeldegeheimnis nach § 88 TKG zu beachten, womit ihm der Zugang zum Inhalt und den näheren Umständen der Kommunikation seiner Beschäftigten verwehrt ist.[245] Inhaltskontrollen von privaten E-Mails sind damit ausgeschlossen und auch die Überprüfung dienstlicher Korrespondenz gestaltet sich schwierig, wenn sich private und dienstliche E-Mails nicht eindeutig voneinander trennen lassen.[246]

Ist die private Nutzung der Kommunikationsmittel verboten, kommen die Regelungen des TKG nicht zur Anwendung. Stattdessen richtet sich die Zulässigkeit von Kontrollen nach den allgemeinen Vorschriften des BDSG.[247]

3.2
Anwendbarkeit des BDSG

Das BDSG findet entsprechend § 1 Abs. 3 BDSG Anwendung, soweit keine anderen Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind. Zweck des BDSG ist gemäß § 1 Abs. 1 BDSG, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten durch die speichernde oder verantwortliche Stelle[248] in seinem Persönlichkeitsrecht beeinträchtigt wird. Nach § 1 Abs. 2 Nr. 3 BDSG gilt dies ebenfalls für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen.

3.3
Grundsätze des Datenschutzrechts

Auch wenn ein Erlaubnistatbestand die Verwendung personenbezogener Beschäftigtendaten grundsätzlich gestattet,[249] sind einige allgemeine Grundsätze immer zu beachten. Diese Grundsätze des Datenschutzrechts, welche nachfolgend kurz dargestellt werden, sind von erheblicher Bedeutung für die Beurteilung der Zulässigkeit von Datenverwendungen und spielen insbesondere bei der stets durchzuführenden Prüfung der Verhältnismäßigkeit eine herausragende Rolle.

Zunächst schreibt § 3a BDSG vor, dass die Verwendung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sich an dem Ziel auszurichten haben, so wenig personenbezogene Daten wie

---

[244] *Heldmann*, DB 2010, 1235 (1239) m.w.N.
[245] *Wedde*, in: *Däubler/Klebe/Wedde/Weichert* (o. Fußn. 36), § 32 Rn. 115.
[246] *Wellhörner/Beyers*, BB 2009, 2310.
[247] *Wellhörner/Beyers* a.a.O., S. 2311.
[248] Verantwortliche Stelle ist gemäß § 3 Abs. 7 BDSG jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Die ebenfalls im BDSG auftretenden Begriffe der „speichernden" oder der „verarbeitenden" Stelle sind gleichbedeutend.
[249] Siehe sogleich Abschnitt 3.4.

möglich zu erheben, zu verarbeiten oder zu nutzen. Diesem Grundsatz der **Datenvermeidung** und **Datensparsamkeit** kann insbesondere durch eine Pseudonymisierung oder Anonymisierung der Daten nachgekommen werden, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert. Auch eine automatische unverzügliche Löschung nicht mehr gebrauchter Daten dient diesem Zweck.[250]

Laut § 5 BDSG sind die bei der Datenverarbeitung beschäftigten Personen nicht öffentlicher Stellen auf das **Datengeheimnis** zu verpflichten. Hiernach ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Verstöße gegen § 5 BDSG, etwa die unerlaubte Weitergabe der Daten innerhalb der verantwortlichen Stelle,[251] sind bußgeldbewehrt und können gemäß § 43 Abs. 2 i.V.m. § 44 Abs. 1 BDSG eine Freiheitsstrafe nach sich ziehen.

Die Rechte des Betroffenen auf Auskunft, Berichtigung, Löschung oder Sperrung seiner personenbezogenen Daten sind gemäß § 6 Abs. 1 BDSG unabdingbar.[252] Hiermit wird dem bedeutsamen Grundsatz der **Transparenz** Rechnung getragen.[253] Diesem verfassungsrechtlich vorgegebenen Prinzip,[254] wonach der Betroffene grundsätzlich zu wissen hat, wer welche Daten über ihn verwendet, ist auch die **Benachrichtigungspflicht** geschuldet. Werden Daten des Beschäftigten ohne dessen Kenntnis erstmalig gespeichert, so ist er gemäß § 33 Abs. 1 S 1 BDSG zu benachrichtigen. In Abs. 2 der Norm sind allerdings einige Fälle gelistet, in denen keine Benachrichtigungspflicht besteht. Eine Ausnahme besteht etwa gemäß § 33 Abs. 2 Satz 1 Nr. 7b BDSG, wenn die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde und das Interesse an der Benachrichtigung nicht überwiegt. Daten, die der Arbeitgeber im Zusammenhang mit der Aufdeckung von einem Korruptionsverdacht gespeichert hat, sind demnach solange nicht mitzuteilen[255], wie die Gefahr einer möglichen Verschleierung der Tat besteht. Verstöße gegen § 33 BDSG sind ebenfalls bußgeldbewehrt.

Bezüglich der Erhebung der Daten gilt gemäß § 4 Abs. 2 BDSG der Grundsatz der **Direkterhebung** beim Betroffenen. Das Gebot der **Zweckbindung** von erhobenen Daten wird durch § 4 Abs. 1 BDSG gewährleistet. Dieser enthält ein Verbot mit Erlaubnisvorbehalt, wonach selbst rechtmäßig gespeicherte Daten grundsätzlich nur für den mit der Speicherung verfolgten Zweck verwendet

[250] *Weichert,* in: *Däubler/Klebe/Wedde/Weichert* (o. Fußn. 36), § 3a Rn. 3.
[251] *Klebe,* in: *Däubler/Klebe/Wedde/Weichert* (o. Fußn. 36), § 5 Rn. 9.
[252] Vgl. im Einzelnen die §§ 19, 34, 20, 35 BDSG.
[253] *Gola/Wronka* (o. Fußn. 38), Rn. 176.
[254] *BVerfG*, Urt. v. 15.12.1983, 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1 (Volkszählungsurteil).
[255] *Gola/Wronka* (o. Fußn. 38), Rn. 371.

werden dürfen.[256] Weitere Einzelheiten hierzu werden im nachfolgenden Abschnitt 3.4 behandelt.

Nach § 9 BDSG hat die verantwortliche Stelle die **technischen und organisatorischen Maßnahmen** zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG, insbesondere die in der Anlage zum BDSG genannten Anforderungen, zu gewährleisten. Im Rahmen dieser Datensicherungspflichten ist entsprechend der Anlage zu § 9 Satz 1 BDSG bei der automatisierten Verarbeitung oder Nutzung personenbezogener Daten im Wesentlichen die Vornahme von Zutritts-, Zugangs-, Zugriffs- und Verfügbarkeitskontrollen sicherzustellen.

Verfahren automatisierter Datenverarbeitung sind schließlich vor der Inbetriebnahme durch eine nicht öffentliche, verantwortliche Stelle gemäß § 4d Abs. 2 BDSG dem betrieblichen **Datenschutzbeauftragten** zu melden.[257] Dieser überwacht gemäß § 4g Abs. 1 Satz 4 Nr. 1 BDSG die ordnungsgemäße Durchführung der Programme.

3.4
Ermächtigungsgrundlagen für die Verwendung personenbezogener Beschäftigtendaten

Gemäß § 4 Abs. 1 BDSG ist die Verwendung personenbezogener Daten nur zulässig, soweit das BDSG selbst oder eine andere Rechtsvorschrift dies gestattet[258] oder der Betroffene eingewilligt hat. Demnach ist eine Verwendung der Arbeitnehmerdaten durch das Unternehmen zu den genannten Kontroll-Zwecken grundsätzlich rechtswidrig, es sei denn, eine der anschließend dargestellten Ermächtigungsgrundlagen besteht.

Die in Abschnitt 2 vorgestellten aktien-, handels- und ordnungswidrigkeitsrechtlichen Regelungen, die die Unternehmensleitung zur Durchführung von Kontrollen der Beschäftigten zwingen, stellen keine Erlaubnistatbestände für Datenverwendungen dar.[259] Die Zulässigkeit der Verwendung personenbezogener Daten im Arbeitsverhältnis bemisst sich grundsätzlich nach den bereichsspezifischen Vorschriften bzw. den Erlaubnistatbeständen aus § 32 BDSG und hilfsweise aus § 28 BDSG. Daneben besteht die Möglichkeit eine Betriebsvereinbarung abzuschließen, welche den Handlungsrahmen der Un-

[256] *Gola/Wronka* (o. Fußn. 38), Rn. 142.

[257] Existiert kein Datenschutzbeauftragter (die Voraussetzungen hierzu enthält § 4f BDSG), so ist gemäß § 4d Abs. 1 BDSG die zuständige Aufsichtsbehörde zu unterrichten.

[258] Die Datenübertragungsverordnung (DÜV) bezüglich der Meldung von Mitarbeiterdaten an die Sozialversicherungsträger stellt gar eine gesetzliche Verpflichtung zur Datenverwendung dar. Der BGH erklärte ferner die Meinungsfreiheit als Erlaubnistatbestand für die Generierung personenbezogener Daten einer Lehrerin auf einer Internetplattform, *BGH* Urt. v. 23.06.2009 – VI ZR 196/08, NJW 2009, 2888 (spickmich.de).

[259] *Gola/Wronka* (o. Fußn. 38), Rn. 852; lediglich der für das Kreditwesen einschlägige § 25c KWG beinhaltet eine konkrete Ermächtigung zur Verwendung personenbezogener Daten zum Zweck der Missbrauchsbekämpfung.

ternehmensleitung abschließend regelt .Die Einwilligung des Betroffenen spielt in der Praxis allenfalls eine untergeordnete Rolle.

3.4.1
Einwilligung des betroffenen Beschäftigten

Die Einwilligung ist gemäß § 4a Abs. 1 Satz 1 BDSG nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Der Arbeitgeber hat den Arbeitnehmer weiterhin gemäß Satz 2 auf den vorgesehenen Zweck der Verwendung der Daten und soweit erforderlich oder auf Verlangen, auf die Konsequenzen einer unterbleibenden Einwilligung hinzuweisen. Obwohl nicht ausdrücklich im Gesetz erwähnt, hat die Information auch Auskünfte darüber zu enthalten, welche Daten genau verwendet werden, wer verantwortliche Stelle ist und wie man diese erreicht sowie ob die Daten an Dritte übermittelt werden und wenn ja, um welche Stellen es sich dabei handelt.[260] Damit stellt die Einwilligung in Datenverwendungen im Rahmen von internen Ermittlungen alleine deshalb kein probates Mittel dar, weil die umfassende Belehrung des Beschäftigen über die Zwecke der Verwendung Rückschlüsse auf die i.d.R. unter Verschluss gehaltenen unternehmensinternen Arbeitsprozesse zur Verhinderung und Aufdeckung von Straftaten zulassen kann.[261]

Schließlich verlangt Satz 3 der Norm für die Einwilligung grundsätzlich die Schriftform,[262] von der nur in Ausnahmefällen abgewichen werden darf.[263] Sollte die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie gemäß Satz 4 besonders hervorzuheben. So soll verhindert werden, dass die Einwilligung dem Betroffenen einfach „untergejubelt" wird, sondern er sie ganz bewusst abgibt – oder eben nicht.

Schwierigkeiten bereitet im Arbeitsverhältnis insbesondere das Tatbestandsmerkmal der Freiwilligkeit gemäß § 4a Abs. 1 Satz 1 BDSG. Anhaltspunkte für das Vorliegen einer freien Entscheidung liefern Art. 2 lit. h) sowie Art. 7 lit. a) der Datenschutzrichtlinie[264], wonach diese „ohne Zwang", bzw. „ohne jeden Zweifel" zu sein hat.

Im Arbeitsverhältnis in dem der Arbeitgeber dem Arbeitnehmer als ungleich stärkerer Vertragsteil gegenübersteht und der Arbeitnehmer vermutlich alleine aufgrund vorstellbarer negativer Konsequenzen einer ausbleibenden Einwilligung eine solche erteilen wird, werden an eine tatsächlich freiwillige Einwilli-

---

[260] *Weichert,* in: *Däubler/Klebe/Wedde/Weichert* (o. Fußn. 36), § 4a Rn. 8.
[261] *Vogel/Glas*, DB 2009, 1747 (1748).
[262] § 126 BGB: Ist durch Gesetz schriftliche Form vorgeschrieben, so muss die Urkunde von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden. Eine Ausweichmöglichkeit stellt die elektronische Form gemäß § 126a BGB dar, soweit das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist.
[263] *Gola/Wronka* (o. Fußn. 38), Rn. 268 f.
[264] Richtlinie 95/46/EG (o. Fußn. 240).

gung erhöhte Anforderungen gestellt. Neben der Angst des Arbeitnehmers vor einer Kündigung, können auch Befürchtungen, sich verdächtig zu machen, eine Rolle spielen, wenn in Datenverwendungen im Zusammenhang mit internen Ermittlungen nicht eingewilligt wird.[265]

Wird die Einwilligung dem Arbeitnehmer von einer wirtschaftlichen Machtposition[266] aus aufgezwängt oder durch eine arglistige Täuschung erschlichen, so ist sie jedenfalls rechtsmissbräuchlich und damit unwirksam, da sie nicht den freien Willen des Betroffenen abbildet.[267] Rechtsmissbräuchlich ist die Einwilligung weiterhin, wenn sie gegen zwingende Schutzvorschriften verstößt oder der Arbeitgeber durch sie versucht, zwingendes Recht zu umgehen, um an Informationen zu gelangen, die ihm etwa nach den sozial- oder arbeitsrechtlichen Grundsätzen nicht zustehen.[268] Eine Unwirksamkeit nach § 134 BGB ist die Folge.[269]

Letztendlich kann eine Einwilligung dem Arbeitgeber nur dann eine gegenüber den bereichsspezifischen Ermächtigungsgrundlagen oder den Erlaubnistatbeständen aus den §§ 32, 28 BDSG erweiterte Informationsbefugnis gestatten, wenn der Arbeitnehmer ohne drohende Sanktionen die Einwilligung auch ablehnen oder eine erteilte Erlaubnis frei widerrufen kann.[270] Dieser Nachweis wird in der Praxis regelmäßig schwer zu erbringen sein. Das nach h.M. in diesem Zusammenhang bestehende Widerrufsrecht[271] stellt zudem ein weiteres Problem für das Unternehmen dar: Basiert eine unternehmensinterne Datenschutzarchitektur alleine auf der Grundlage von Einwilligungen der Betroffenen, so haben vermehrte Widerrufserklärungen die Schwierigkeit zur Folge, dass die Datensätze jener Arbeitnehmer von den anderen Datensätzen zu filtern und getrennt zu verwenden sind.[272]

Im Ergebnis ist eine arbeitnehmerseitige Einwilligung in die Verwendung seiner personenbezogenen Daten zum Zweck der Bekämpfung von Wirtschaftsdelikten – trotz ihrer ausdrücklichen Erwähnung in der Gesetzesbegründung zu § 32 BDSG[273] – nicht geeignet, diese Maßnahmen zu legitimieren. Die Einwilligung wäre im Hinblick auf die neue Spezialnorm zur Verwendung von Beschäftigtendaten überdies als irreführend anzusehen, da § 32 BDSG dem Arbeitgeber die Verwendung der Daten unter bestimmten Voraussetzungen ohnehin gestattet und durch eine zusätzlich abzugebende Einwilligung beim

---

[265] *Vogel/Glas* (o. Fußn. 261), S. 1748.
[266] *BGH*, Urt. v. 16.07.2008 - VIII ZR 348/06, NJW 2008, 3055 (3056).
[267] *Gola/Wronka* (o. Fußn. 38), Rn. 260.
[268] Bezogen auf das Fragerecht des Arbeitgebers *Gola/Wronka* (o. Fußn. 38), Rn. 262.
[269] Gemäß § 134 BGB ist ein Rechtsgeschäft, das gegen ein gesetzliches Verbot verstößt, nichtig, wenn sich nicht aus dem Gesetz ein anderes ergibt.
[270] *Gola/Wronka* (o. Fußn. 38), Rn. 261.
[271] *Gola/Wronka* (o. Fußn. 38), Rn. 280 f.*; Weichert,* in: *Däubler/Klebe/Wedde/Weichert* (o. Fußn. 36), § 4a, Rn. 35 m.w.N.
[272] *Schmidl*, DuD 2007, 756 (758); *Olbers*, BB 2010, 844 (847).
[273] BT-Drucks. 16/13657, S. 20.

Arbeitnehmer der Eindruck entstehen könnte, er hätte auch ein Widerspruchsrecht gegenüber der gesetzlichen Ermächtigung.[274] Nach der Artikel 29-Datenschutzgruppe ist die Einwilligung folglich nur dann nicht irreführend, wenn der Arbeitnehmer eine „echte Wahl" hat.[275]

3.4.2 Betriebsvereinbarung

Auch die Betriebsvereinbarung, eine für die ganze Belegschaft geltende Vereinbarung zwischen dem Arbeitgeber und dem Betriebsrat, kann eine vorrangige Erlaubnisnorm i.S.v. § 4 Abs. 1 BDSG darstellen.[276] Betriebsvereinbarungen gelten gemäß § 77 Abs. 4 BetrVG unmittelbar und zwingend und haben ferner eine normative Wirkung.[277] In einem bereits einige Jahre zurückliegenden Beschluss, hat das BAG festgestellt, dass der weite Begriff der anderen Rechtsvorschrift aus § 4 Abs. 1 BDSG „auch Rechtsvorschriften im Range unterhalb des Gesetzesrechtes" umfasst und diese damit verbindliche Regelungen zum Datenschutz treffen können, auch da das BDSG als subsidiäre Regelung des Datenschutzes hinter die bereichsspezifischen Vorschriften zurücktritt.[278] Die Wirkung der Betriebsvereinbarung wird ferner dadurch deutlich, dass der Rahmen der zulässigen Datenverwendung nicht einmal über eine Einwilligung des Arbeitnehmers ausgedehnt werden kann, soweit die Vereinbarung eine abschließende Aufzählung von zur Verwendung freigegebenen Daten enthält.[279] Generell kann in der Betriebsvereinbarung auch eine Erlaubnisnorm zur Datenverwendung zum Zwecke der Kontrollen und internen Ermittlungen gesehen werden.[280] Zusätzlich hat das BAG im bereits erwähnten Beschluss aus dem Jahre 1986 anerkannt, dass sich Betriebsvereinbarungen, abweichend vom BDSG, auch negativ auf die Arbeitnehmer auswirken können, sofern dies im Rahmen der Regelungskompetenz der Betriebspartner und unter Berücksichtigung der Grundsätze des Persönlichkeitsschutzes der Arbeitnehmer geschieht. Hierzu führte das Gericht aus:

> „(Betriebsvereinbarungen) sind nicht darauf beschränkt, nur unbestimmte Rechtsbegriffe des BDSG unter Berücksichtigung der betrieblichen Besonderheiten näher zu konkretisieren oder den Datenschutz der Arbeitnehmer zu verstärken. Der Datenschutz nach dem BDSG ist gegenüber den (…) anderen Rechtsvorschriften nicht unabdingbarer Mindeststandard, der durch (…) Betriebsvereinbarungen nur zugunsten der Arbeitnehmer verbessert werden könnte. (…) Soweit in der Literatur geltend gemacht wird, durch eine (…) Be-

[274] *Gola/Wronka* (o. Fußn. 38), Rn. 271 ff.
[275] *Artikel 29-Datenschutzgruppe*, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, S. 28.
[276] *Gola/Wronka* (o. Fußn. 38), Rn. 242.
[277] *Werner,* in: *Rolfs/Giesen/Kreikebohm* u.a. (Hrsg.), BeckOK, BetrVG, § 77 Rn. 11.
[278] *BAG*, Beschl. v. 27.05.1986 - 1 ABR 48/84, NZA 1986, 643 (646).
[279] *Gola/Wronka* (o. Fußn. 38), Rn. 256.
[280] *Wybitul* (o. Fußn. 30), 1584 unter Hinweis auf *BAG*, Beschl. v. 26.08.2008 - 1 ABR 16/07, NZA 2008, 1187.

> triebsvereinbarung dürfe der Datenschutz der Arbeitnehmer nicht verschlechtert werden (…) vermag der Senat dem daher nicht zu folgen."[281]

Zwar hat der zitierte Beschluss in der Literatur viel Kritik erfahren.[282] So wird etwa vertreten, dass die Argumentation des BAG seit Erlass der Datenschutzrichtlinie[283] im Jahre 1994 nicht mehr tragbar sei, da diese in Erwägungsgrund 12 festschreibt, dass die in der Richtlinie formulierten Schutzprinzipien für alle Verarbeitungen personenbezogener Daten im Anwendungsbereich des Gemeinschaftsrechts gelten, womit eine Abweichung von diesen Prinzipien unzulässig sei.[284] Auch dürfen Arbeitgeber und Betriebsrat wegen ihres Auftrags aus § 75 Abs. 2 BetrVG, die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern, Eingriffe in das Persönlichkeitsrecht der Arbeitnehmer nur dann billigen, wenn diese als Ergebnis einer umfassenden Interessenabwägung das letzte verbliebene Mittel sind und die Persönlichkeitsrechte „maximal gewahrt" bleiben,[285] weshalb Fälle, in denen die Rechtmäßigkeit von grundsätzlich unzulässigen Datenverwendungen alleine auf einer Betriebsvereinbarung beruht, „kaum denkbar" sind.[286]

Grundsätzlich besteht jedoch die Möglichkeit innerhalb einer Betriebsvereinbarung Regelungen zu formulieren, die einerseits den Kontrollbedürfnissen des Arbeitgebers nach einer effektiven Überwachung gerecht werden und andererseits nicht so weit vom Wortlaut des BDSG abweichen, das hierin eine Verletzung des Persönlichkeitsrechts der Beschäftigten bestehen würde.[287] Dabei ist dem verfassungsrechtlich verbürgten Bestimmtheitsgrundsatz Rechnung zu tragen, indem die Vereinbarung etwa konkrete Vorgaben enthält, um welche Arten von personenbezogenen Daten es sich handelt, diesen ist ein hinreichend bestimmter Verwendungszweck zuzuordnen, ferner sind die technischen und organisatorischen Datenschutzmaßnahmen darzustellen sowie die Rechte der Arbeitnehmer, die Kontrollmöglichkeiten des Betriebsrats und des Datenschutzbeauftragten.[288]

---

[281] *BAG* (o. Fußn. 278) S. 646; dieser Ansicht sind gefolgt *LAG Düsseldorf*, Beschl. v. 04.11.1988 –17 (6) TaBV 114/88, NZA 1989, 146 (148); *Kania,* in: Erfkomm, § 87 BetrVG Rn. 61; *Blomeyer,* in: *Richardi/Wlotzke* (Hrsg.), Münchner Handbuch zum Arbeitsrecht, § 99 Rn. 95.

[282] Einen Überblick über den Meinungsstand geben *Brandt*, DuD 2010, 213 (214f) m.w.N.; *Gola/Wronka* (o. Fußn. 38), Rn. 245 f m.w.N.

[283] Richtlinie 95/46/EG (o. Fußn. 240).

[284] *Brandt* (o. Fußn. 282), S. 215; *Trittin/Fischer*, NZA 2009, 343 (344).

[285] *Wedde*, in: *Däubler/Klebe/Wedde/Weichert* (o. Fußn. 36), § 32 Rn. 117.

[286] *Gola/Wronka* (o. Fußn. 38), Rn. 264; ablehnend auch *Mengel*, Compliance und Arbeitsrecht, S. 202, welche die Einführung von Whistleblowing-Systemen auf Grundlage einer Betriebsvereinbarung ausschließt.

[287] *Wybitul* (o. Fußn. 30), S. 1585.

[288] *Wybitul* a.a.O., S. 1585, siehe zu den Anforderungen Abschnitt 3.3.

3.4.3
Erhebung, Verarbeitung und Nutzung personenbezogener Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses im Allgemeinen, § 32 Abs. 1 Satz 1 BDSG

Besteht keine bereichsspezifische Erlaubnisnorm zur Verwendung der Beschäftigtendaten, ist der mit der BDSG-Novelle II neu eingeführte § 32 BDSG als Spezialnorm für die Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses einschlägig. Diese nachfolgend untersuchte Regelung unterscheidet in ihrem Abs. 1 Satz 1 zwischen der Datenverwendung zur Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses. Abs. 1 Satz 2 enthält überdies eine Sondervorschrift hinsichtlich der Verwendung personenbezogener Beschäftigtendaten zur Aufdeckung von Straftaten. Wegen der zentralen Bedeutung der Regelung für diese Arbeit soll sie zunächst im originalen Wortlaut wiedergeben werden:

> § 32 BDSG
> Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses
>
> (1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.
>
> (2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden. (…)

Laut dem Gesetzgeber stellt § 32 BDSG keine abschließende Regelung dar.[289] Die Norm enthalte nur „eine allgemeine Regelung zum Schutz personenbezogener Daten von Beschäftigten, die die von der Rechtsprechung erarbeiteten Grundsätze des Datenschutzes im Beschäftigungsverhältnis nicht ändern, sondern lediglich zusammenfassen und ein Arbeitnehmerdatenschutzgesetz weder entbehrlich machen noch inhaltlich präjudizieren soll."[290] Neu ist lediglich die Pflicht zur Dokumentation von Verdachtsfällen gemäß Abs. 1 Satz 2.[291]

[289] BT-Drucks. 16/12011, S. 53.
[290] BT-Drucks. 16/13657, S. 20.
[291] *Polenz*, DuD 2010, 561 (563).

Eine der Transparenz der Norm geschuldete Änderung sieht darüber hinaus Abs. 2 vor, wonach die im Folgenden erläuterten Grundsätze im Umgang mit personenbezogenen Beschäftigtendaten auch dann anwendbar sind, wenn es sich um nicht automatisierte Daten handelt. Damit fallen Befragungen oder Beobachtungen durch den Arbeitgeber[292], die Einsichtnahme in personenbezogene Daten der Beschäftigten in sozialen Online-Netzwerken[293], schriftlich geführte Akten oder handschriftliche Notizen im Zusammenhang mit dem Beschäftigungsverhältnis in den Anwendungsbereich der Vorschrift.

Im Folgenden wird zunächst dargestellt, welche Befugnisse § 32 Abs. 1 Satz 1 BDSG dem Arbeitgeber im Allgemeinen erteilt. Im anschließenden Abschnitt 3.4.4 wird untersucht, welche Befugnisse Satz 2 im Besonderen hinsichtlich der geschilderten, durchzuführenden Kontrollen erteilt. Wegen des systematischen Zusammenhangs wird an letztgenannter Stelle auch die Zulässigkeit von Datenverwendungen zur Verhinderung von Straftaten und Rechtsverstößen erörtert, obwohl diese präventiven Handlungen im Anwendungsbereich von Satz 1 liegen.

3.4.3.1
Die Ermächtigungsgrundlagen im Einzelnen

In der Praxis gilt es jeweils zu klären, ob eine bestimmte Maßnahme des Arbeitgebers durch einen der Verwendungszwecke der Norm gedeckt ist. In einem nächsten Schritt ist zu klären, ob die jeweilige Maßnahme zur Erreichung dieses Zwecks erforderlich ist.[294] Als Grundlage für diese Beurteilung gelten folgende Ausführungen.

3.4.3.1.1
Begründung des Beschäftigungsverhältnisses

Für Zwecke des Beschäftigungsverhältnisses erlaubt § 32 Abs. 1 Satz 1 Alt. 1 BDSG zunächst die Erhebung, Verarbeitung und Speicherung personenbezogener Daten eines Beschäftigten, wenn dies für die Entscheidung über die Begründung des Beschäftigungsverhältnisses erforderlich ist. Dies umfasst etwa Daten, die im Rahmen von Fragen nach den fachlichen Fähigkeiten, Kenntnissen und Erfahrungen des Bewerbers gewonnen werden.[295] Weiterhin darf sich der Arbeitgeber im Rahmen seines allgemein anerkannten Fragerechts nach weiteren Tatsachen erkundigen, an deren Kenntnis er ein schutzwürdiges Interesse hat. So hat der Bewerber Mitteilungspflichten hinsichtlich Tatsachen, die die Durchführung des Arbeitsvertrags unmöglich oder unzumutbar machen, etwa wenn ihn ein Wettbewerbsverbot an der Aufnahme der

[292] *Deutsch/Diller*, DB 2009, 1462.
[293] *Albrecht*, jurisPR-ITR 20/2009, Anm. 2, S. 2 m.w.N.
[294] Siehe Abschnitt 3.4.3.2.
[295] BT-Drucks 16/13657, S. 21 unter Hinweis auf *BAG*, Urt. v. 06.06.1984, NZA 1984, 321; *BAG*, Urt. v. 07.06.1984, NZA 1985, 57; *BAG*, Urt. v. 07.09.1995, NZA 1996, 637.

Tätigkeit hindert.[296] Ferner darf der Arbeitgeber sich nach Vorstrafen erkundigen, sofern diese einschlägig sind.[297] Er darf dementsprechend einen Interessenten für eine leitende Position im Einkauf danach fragen, ob er je wegen eines Vorwurfs der Korruption verurteilt wurde, nicht jedoch nach eventuell begangenen Verkehrsdelikten.

Kommt es nicht zu einer Einstellung dürfen Bewerberdaten schließlich nur so lange in gesperrter Form aufbewahrt werden, bis das Risiko von Rechtsstreitigkeiten etwa aufgrund von § 15 AGG auszuschließen ist, und sind daraufhin unverzüglich zu löschen.[298]

3.4.3.1.2 Durchführung des Beschäftigungsverhältnisses

Nach § 32 Abs. 1 Satz 1 Alt. 2 BDSG ist die Erhebung, Verarbeitung und Speicherung personenbezogener Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses weiterhin erlaubt, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Als Beispiele einer zulässigen Verwendung von Beschäftigtendaten nennt der Gesetzgeber[299] Datenerhebungen, die es dem Arbeitgeber ermöglichen, seinen vertraglichen Pflichten gegenüber dem Beschäftigten hinsichtlich Personalverwaltung, Lohn- oder Gehaltsabrechnungen nachzukommen, also die Erhebung aller Daten, die zum „üblichen Geschäft"[300] von Personalabteilungen gehören. Hierzu zählen Daten wie Name, Anschrift, Geschlecht, Familienstand, Ausbildung, Betriebs-Eintrittsdatum, Entgelt, Kontoverbindung, Krankenkassenzugehörigkeit.[301]

Die Ermächtigung zur Datenverwendung gilt selbstverständlich auch für die Wahrnehmung der sich aus dem Arbeitsverhältnis ergebenen Rechte des Arbeitgebers. So erfasst der Erlaubnistatbestand auch Datenverwendungen im Zusammenhang mit der Ausübung des Weisungsrechts des Arbeitgebers oder mit Kontrollen der Leistung und des Verhaltens der Beschäftigten. Ebenfalls gerechtfertigt kann der Einsatz von technischen Mitteln wie RFID[302] sowie die Speicherung biometrischer Daten, etwa dem Fingerabdruck oder dem Abbild der Iris, sein, wenn dies für die Handhabung sensibler Sicherheitsbereiche erforderlich ist.[303] Speichert der Arbeitgeber Fingerabdrücke jedoch lediglich im

---

[296] *Däubler,* in: *Däubler/Klebe/Wedde/Weichert* (o. Fußn. 36), § 32 Rn. 18.
[297] *Däubler*, in: *Däubler/Klebe/Wedde/Weichert* a.a.O., § 32 Rn. 35.
[298] *Wank*, in: Erfkomm (o. Fußn. 281), § 32 BDSG Rn. 15.
[299] BT-Drucks. 16/13657, S. 21 unter Hinweis auf *BAG*, Urt. v. 22.10.1986, DB 1987, 1048; *BAG*, Urt. v. 07.09.1995, NZA 1996, 637.
[300] *Schaar*, Pressemitteilung, http://www.bfdi.bund.de/DE/Themen/Arbeit/Arbeitnehmerdatenschutz/Artikel/ArbeitnehmerDSAb010909.html?nn=647266 (Stand: 19.03.2010).
[301] *Däubler,* in: *Däubler/Klebe/Wedde/Weichert* (o. Fußn. 36), § 32 Rn. 68.
[302] *Däubler*, in: *Däubler/Klebe/Wedde/Weichert* a.a.O., § 32 Rn. 89 ff.
[303] *Däubler*, in: *Däubler/Klebe/Wedde/Weichert* a.a.O., § 32 Rn. 84-88.

Hinblick auf potentielle Straftaten in der Zukunft, liegt ein unzulässiger Fall von Vorratsdatenspeicherung vor.[304]

Aufschlussreich im Bezug auf das Arbeitsverhalten der Beschäftigten ist ferner die Überwachung von deren Internetnutzung oder elektronischer Kommunikation, was, unter Beachtung der besonderen Vorschriften aus bereichsspezifischen Regelungen des TKG und des TMG, im Rahmen der zur Durchführung des Beschäftigungsverhältnisses liegenden Rechte des Arbeitgebers ebenfalls zulässig sein kann.[305] Gleiches gilt für die unter engen Voraussetzungen mögliche Videoüberwachung. Das Ahnden von Vertragsbrüchen, die nicht strafrechtlich relevant sind, also etwa Verstöße gegen das Wettbewerbsverbot, oder die Verschwiegenheitspflicht, kann ebenso erforderlich für die Durchführung des Beschäftigungsverhältnisses sein.[306]

Mit den letztgenannten Handlungen des Arbeitgebers in direkter Beziehung stehen die Maßnahmen zur Verhinderung von Straftaten und anderen Rechtsverstößen, die im Zusammenhang mit dem Beschäftigungsverhältnis stehen. Deren Zulässigkeit ist ebenfalls an § 32 Abs. 1 Satz 1 Alt. 2 BDSG zu messen.[307] Weitere Ausführungen hierzu erfolgen in Abschnitt 3.4.4.2.

3.4.3.1.3
Beendigung des Beschäftigungsverhältnisses

Die 3. Alternative von § 32 Abs. 1 Satz 1 BDSG erlaubt schließlich die Erhebung, Verarbeitung und Speicherung personenbezogener Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses, wenn dies für die Beendigung des Beschäftigungsverhältnisses erforderlich ist. Im Vordergrund stehen hier Datenverwendungen im Zusammenhang mit Abmahnungen, Kündigungen oder der Abwicklung eines Beschäftigungsverhältnisses.[308] Umfasst sind ebenfalls Maßnahmen gegenüber ehemaligen Beschäftigten, etwa hinsichtlich ihrer Betriebsrente.[309]

3.4.3.2
Erforderlichkeit

Zentrale Voraussetzung für die Zulässigkeit der Erhebung, Verarbeitung und Speicherung personenbezogener Daten eines Beschäftigten nach § 32 Abs. 1 Satz 1 BDSG ist die Erforderlichkeit der jeweiligen Maßnahme.

---

[304] *Gola/Wronka* (o. Fußn. 38), Rn. 819 ff.
[305] *Wellhörner/Byers* (o. Fußn. 246), 2311 f.
[306] *Thüsing*, NZA 2009, 865 (868).
[307] BT-Drucks. 16/13657, S. 21.
[308] BT-Drucks. 16/13657, S. 21.
[309] *Erfurth*, NJOZ 2009, 2914 (2917); die genannten Handlungen erhalten eine zusätzliche Rechtfertigung durch eine Öffnung des Beschäftigtenbegriffs für Personen, deren Beschäftigungsverhältnis beendet ist, gemäß § 3 Abs. 11 Nr. 7 BDSG.

3.4.3.2.1 Der datenschutzrechtliche Begriff der Erforderlichkeit

Das Kriterium der Erforderlichkeit ist Teil des verfassungsrechtlichen Prinzips der Verhältnismäßigkeit. Hiernach ist eine Maßnahme nur dann zulässig, wenn sie einen legitimen Zweck durch ein legitimes Mittel verfolgt und dieses Mittel weiterhin geeignet sowie darüber hinaus notwendig bzw. erforderlich ist, den Zweck zu erreichen. Erforderlichkeit bedeutet in diesem Zusammenhang, dass kein gleich geeignetes, jedoch weniger belastendes Mittel zur Verfügung steht. Im letzten Schritt der Verhältnismäßigkeitsprüfung ist zu untersuchen, ob das angewandte Mittel im Hinblick auf den angestrebten Zweck angemessen, d.h. verhältnismäßig i.e.S. ist.

Zur Feststellung, ob eine konkrete Datenverwendung durch den Arbeitnehmer als erforderlich einzustufen ist, ist eine Interessenabwägung durchzuführen. Zwar muss eine Datenverwendung dem Wortlaut von § 32 Abs. 1 Satz 1 BDSG nach lediglich erforderlich sein und darüber hinaus sind keine weiteren Anhaltspunkte gegeben, wann diese Erforderlichkeit zu bejahen ist. Jedoch kann zur Auslegung dieses Kriteriums § 28 Abs. 1 Satz 1 Nr. 2 BDSG in der Fassung von vor der Novellierung herangezogen werden. Diese Norm stellte eine der Ermächtigungsgrundlagen für Datenverwendungen in Beschäftigungsverhältnissen dar und der Rückgriff auf sie ist insofern einleuchtend, als die neue Regelung zum Datenschutz in Beschäftigungsverhältnissen die bisherige Rechtslage nicht ändern soll.[310]

Nach dieser war die Verwendung von personenbezogenen Daten für die Erfüllung eigener Geschäftszwecke zulässig, soweit dies zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich war und kein Grund zu der Annahme bestand, dass das schutzwürdige Interesse des Betroffenen an einem Ausschluss der Verwendung überwiegt. Es stehen also die schutzwürdigen Interessen[311] des Beschäftigten den berechtigten Interessen des Arbeitgebers gegenüber.[312] Die Interessenabwägung ist daher eine Abwägung zwischen dem allgemeinen Persönlichkeitsrecht (APR) aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und dessen speziellen Ausprägungen[313] auf der Arbeitnehmerseite und der Berufsfreiheit aus Art. 12 GG bzw. dem Recht am Eigentum aus Art. 14 GG auf der Arbeitgeberseite.[314]

---

[310] BT-Drucks. 16/13657, S. 20.

[311] Das BDSG verwendet auch häufig den gleichbedeutenden Begriff „schutzwürdige Bedürfnisse".

[312] Zum selben Ergebnis, dass § 32 Abs. 1 S. 1 BDSG entgegen des Wortlauts eine Interessenabwägung verlangt, kommen *Erfurth* (o. Fußn. 309), S. 2918 f.; *Schmidt*, RDV 2009, 193 (198).

[313] Weitere Einzelheiten hierzu enthält Abschnitt 3.4.4.1.4.c)i.

[314] Es wird ferner vertreten, dass dem Arbeitgeber auf der Grundlage der Informationsfreiheit aus Art. 5 Abs. 1 S. 1 GG ein Recht zur Verwendung der Beschäftigtendaten zusteht, vgl. *Däubler*, Gläserne Belegschaften?, 2002, Rn. 114, der dies jedoch ablehnt.

Zwar sind die Grundrechte in erster Linie Abwehrrechte des Bürgers gegen den Staat. Dennoch kommen sie vorliegend zum Tragen, da sie nach h.M. eine mittelbare Drittwirkung auf das Zivilrecht ausstrahlen.[315] Das objektive Wertsystem der Grundrechte gibt verbindliche Regeln für die Auslegung privatrechtlicher Normen vor.[316] Insbesondere Generalklauseln, wie „erforderlich" sowie „berechtigte" oder „schutzwürdige" Interessen, sind hiernach verfassungskonform auszulegen.

Im Bereich des Datenschutzrechts ist zu verlangen, dass eine Datenverwendung zur Erfüllung des legitimen Vertragszwecks benötigt wird, da die berechtigten Interessen des Arbeitgebers auf eine andere Weise nicht oder nicht angemessen gewahrt werden können.[317] Die reine „Nützlichkeit" einer Datenverwendung wird den Anforderungen an die Erforderlichkeit also nicht gerecht.[318] Eine Unverzichtbarkeit der jeweiligen Maßnahme kann indessen ebenfalls nicht vorausgesetzt werden, da dies einerseits den Handlungsspielraum des Arbeitgebers zu sehr einschränken würde und andererseits selbst eine unverzichtbare Maßnahme in Ausnahmefällen einen zu intensiven Eingriff in die Persönlichkeitsrechte der Arbeitnehmer darstellen kann.[319]

Als berechtigtes Interesse des Arbeitgebers kann jedes, durch die konkrete Sachlage gerechtfertigtes, tatsächliches Interesse zu werten sein.[320] Insoweit ist ein subjektiver Maßstab anzulegen, da der Arbeitgeber – und nicht etwa die Aufsichtsbehörde oder ein Gericht – zu entscheiden hat, ob die Nutzung eines Datums seinem „unternehmerischen Konzept" entsprechend geboten ist.[321] Er kann sich innerhalb seines Entscheidungsspielraums bei der Ausübung seiner grundrechtlich geschützten Unternehmerfreiheit daher ebenfalls von wirtschaftlichen Erwägungen leiten lassen.[322] Insofern kann eine elektronische Arbeitszeiterfassung gerechtfertigt sein, obwohl weniger einschneidende Mittel, etwa Kontrollen durch Aufsichtspersonal, verfügbar wären.[323]

Die Grenze der unternehmerischen Entscheidungsfreiheit bilden die der Datenverwendung entgegenstehenden, schutzwürdigen Interessen der Beschäftigten. Diese sind verletzt, wenn die Maßnahmen des Arbeitgebers in die Intim-, Privat- oder Sozialsphäre der Beschäftigten eingreifen, oder negative wirtschaftliche oder berufliche Auswirkungen nach sich ziehen können.[324] Sind Eingriffe in das Persönlichkeitsrecht der Beschäftigten unter objektiven Maßstäben unabdingbar, hat der Arbeitgeber diese so zurückhaltend wie

[315] *Pieroth/Schlink*, Grundrechte Staatsrecht II, Rn. 181.
[316] *BVerfG*, Urt. v. 15.01.1958 – 1 BvR 400/51, BVerfGE 7, 198 (205) (Lüth).
[317] *Gola/Schomerus* (o. Fußn. 37), § 32 Rn. 12 f.
[318] *Gola/Schomerus* a.a.O., § 32 Rn. 12.
[319] *Erfurth* (o. Fußn. 309), S. 2919.
[320] *Gola/Schomerus* (o. Fußn. 37), § 28 Rn. 24.
[321] *Deutsch/Diller* (o. Fußn. 321), S. 1463; dies kritisierend *Albrecht* (o. Fußn. 293), S. 3.
[322] *Gola/Schomerus* (o. Fußn. 37), § 32 Rn. 12.
[323] *Gola/Schomerus* a.a.O., § 32 Rn. 13.
[324] *Gola/Schomerus* a.a.O., § 28 Rn. 26.

möglich zu gestalten.[325] Dabei sind bei der Beurteilung der Rechtmäßigkeit einer Maßnahme immer auch die allgemeinen Grundsätze des Datenschutzrechts zu beachten.[326]

Im Ergebnis ist eine Verwendung personenbezogener Beschäftigtendaten durch den Arbeitnehmer zulässig, wenn in der konkreten Situation und unter Berücksichtigung der entgegenstehenden Interessen, die andersartige Beschaffung oder der Verzicht auf die Information zur Erreichung des verfolgten Zwecks nicht sinnvoll oder unzumutbar wäre.[327]

3.4.3.2.2
Anknüpfungspunkt für die Erforderlichkeit

Anknüpfungspunkt für die Erforderlichkeit, ist der jeweils verfolgte Zweck einer Maßnahme, d.h. die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses.

Von diesen übergeordneten Kategorien von Zwecken, sind jedoch die im Einzelfall konkret verfolgten Zwecke einer Maßnahme des Arbeitgebers abzugrenzen. Wird etwa das Dienstfahrzeug eines Angestellten im Außendienst mit einem Empfänger bestückt, der eine Positionsbestimmung über GPS zulässt, so dient dies zunächst dem konkreten Zweck, dass der Arbeitgeber darüber informiert werden möchte, ob der Beschäftigte Privatfahrten mit seinem Dienstfahrzeug tätigt, damit dieses Verhalten gegebenenfalls unterbunden werden kann. Daneben dient die Maßnahme aber auch dem übergeordneten Zweck der Durchführung des Beschäftigungsverhältnisses gemäß § 32 Abs. 1 Satz 1 Alt. 2 BDSG. Dieser übergeordnete Zweck hat ebenfalls der Anknüpfungspunkt für die Erforderlichkeit zu sein. Demnach muss gefragt werden, ob das Bestücken des Dienstwagens mit einem GPS-Sender zur Durchführung des Beschäftigungsverhältnisses erforderlich ist. Denn würde man als Anknüpfungspunkt den konkreten, vom Arbeitgeber selbst festzulegenden Zweck wählen und fragen, ob die Maßnahme erforderlich ist, um Privatfahrten des Beschäftigten aufzudecken und zu verhindern, würde eine entsprechend enge Zwecksetzung praktisch jede Datenverwendung durch den Arbeitgeber erlauben.[328]

[325] *Wedde,* in: *Däubler/Klebe/Wedde/Weichert* (o. Fußn. 36), § 32 Rn. 91.
[326] Siehe Abschnitt 3.3.
[327] *Gola/Schomerus* (o. Fußn. 37), § 28 Rn. 15.
[328] *Erfurth* (o. Fußn. 309), S. 2918.

3.4.4
Erhebung, Verarbeitung und Nutzung personenbezogener Beschäftigtendaten gemäß § 32 BDSG im Besonderen zur Aufdeckung und Prävention von Straftaten und anderen Rechtsverstößen

Mit § 32 Abs. 1 Satz 2 BDSG hat der Gesetzgeber eine Spezialvorschrift geschaffen, welche die Verwendung personenbezogener Beschäftigtendaten zum Zweck der Aufdeckung von Straftaten, die der Beschäftigte im Zusammenhang mit dem Beschäftigungsverhältnis begangen hat, regelt.

Der Inhalt der Norm orientiert sich an der Rechtsprechung des BAG zur Videoüberwachung[329] und der Wortlaut an § 100 Abs. 3 Satz 1 TKG, der die Zulässigkeit von Maßnahmen zur Aufdeckung rechtswidriger Inanspruchnahmen von Telekommunikationsnetzen und –diensten regelt.[330]

Nicht von § 32 Abs. 1 Satz 2 BDSG umfasst sollen Maßnahmen zur Prävention von Straftaten sein. Diese fallen in den Anwendungsbereich von Satz 1 der Norm.[331] In der Praxis sind die Übergänge zwischen Präventions- und Aufdeckungsmaßnahmen allerdings fließend.[332] Vor allem diese Kontroverse steht aus Sicht der juristischen Literatur im Mittelpunkt der Kritik an § 32 BDSG.[333] Im Vordergrund steht dabei die Befürchtung, dass die Vorschrift die Erfüllung von Pflichten der Unternehmensleitung im Zusammenhang mit den in Abschnitt 2 beschriebenen Anforderungen aus Corporate Governance und Compliance wesentlich erschwert. Diese Sichtweise soll in den folgenden Ausführungen widerlegt werden.

3.4.4.1
Anwendung von § 32 Abs. 1 Satz 2 BDSG zur Aufdeckung von Straftaten

Wegen der zentralen Bedeutung von § 32 Abs. 1 Satz 2 BDSG für diese Arbeit, sind die Tatbestandsmerkmale der Vorschrift im Einzelnen zu untersuchen. Dies ist umso wichtiger, als die Norm[334] eine Fülle von unbestimmten Rechtsbegriffen enthält.

---

[329] *BAG* , Urt. v. 27.03.2003 - 2 AZR 51/02, NZA 2003, 1193; *BAG*, Beschl. v. 26.08.2008 - 1 ABR 16/07, NZA 2008, 1187.

[330] BT-Drucks. 16/13657, S. 21.

[331] BT-Drucks. 16/13657, S. 21.

[332] *Schmidt* (o. Fußn. 312), S. 196; *Erfurth* (o. Fußn. 309), S. 2921; ähnlich *Gola/Wronka* (o. Fußn. 38), Rn. 401

[333] Siehe insbesondere die in Fußn. 19 genannten Beiträge.

[334] § 32 Abs. 1 S. 2 BDSG: Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu *dokumentierende tatsächliche Anhaltspunkte* den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung *erforderlich* ist und das *schutzwürdige Interesse* des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht *unverhältnismäßig* sind.

3.4.4.1.1 Aufdeckung

Zu Recht ist nach einer Ansicht der Vorgang der Aufdeckung der Straftat dahingehend auszulegen, dass er an die Aufrechterhaltung und Weiterverfolgung von Verdachtsmomenten anknüpft.[335] Danach würde die Zulässigkeit der Generierung von Verdachtsmomenten – und damit auch die Rechtmäßigkeit verdachtsunabhängiger präventiver Ermittlungen – unter Satz 1 der Norm fallen und lediglich die Verfolgung der gewonnenen Verdachtsmomente den erhöhten Anforderungen von Satz 2 unterliegen.[336]

Begründet wird dies damit, dass der Gesetzgeber ausweislich der Gesetzesbegründung zu § 32 BDSG die geltende Rechtslage, nach der verdachtsunabhängige Ermittlungsmaßnahmen unter sorgfältiger Güterabwägung der schutzwürdigen Interessen und Rechte des Arbeitgebers und des Arbeitnehmers gestattet sind[337], nicht ändern möchte und präventive Maßnahmen zur Verhinderung von Straftaten in den Regelungsbereich von Satz 1 fallen sollen.[338]

3.4.4.1.2 Straftat im Beschäftigungsverhältnis

Die Norm findet lediglich bei Straftaten Anwendung, die von Beschäftigten im Zusammenhang mit dem Beschäftigungsverhältnis begangen wurden. Der reine Zusammenhang mit dem Beschäftigungsverhältnis ist dabei ausreichend, ein unmittelbarer Bezug zur vertraglich geschuldeten Leistungspflicht wird dagegen nicht verlangt.[339] Als Arten von Straftaten im Beschäftigungsverhältnis kommen also etwa Diebstahl von Betriebseigentum, Korruption,[340] Betrug, Unterschlagungen und Untreue in Betracht. Die vom Wortlaut verlangte Straftat schließt die Aufdeckung von anderen Rechtsverstößen als Straftaten, etwa Ordnungswidrigkeiten, im Rahmen von Satz 2 aus.[341] Hierin besteht eine Abwendung von den Vorlagen zur Norm, denn sowohl ein vom Gesetzgeber zi-

---

[335] *Schmidt* (o. Fußn. 312), S. 195 ff.

[336] *Schmidt* a.a.O., S. 196; im Ergebnis auch *Gola/Wronka* (o. Fußn. 38), Rn. 857; siehe hierzu noch Abschnitt 3.4.4.3.

[337] *ArbG Berlin* (o. Fußn. 20), Abs.-Nr. 21-23; *Diller*, BB 2009, 438 (440); *Kock/Franke* (o. Fußn. 400), S. 648; *Zikesch/Reimer*, DuD 2010, 96; wohl auch *ArbG Dessau-Roßlau*, Beschl. v. 17.06.2009 – 1 BV 1/09, BeckRS 2009, 69201, dort Abschnitt B.II.2., welches zwar zu entscheiden hatte, ob dem örtlichen Betriebsrat Mitbestimmungsrechte bezüglich eines konzernweit durchgeführten Mitarbeiterscreenings zustehen, womit die Zulässigkeit der Maßnahme nicht zur Frage stand. Dennoch stellte das Gericht fest, dass „lediglich zwei verschiedene Listen mit Namen, Kontonummern und Bankleitzahlen gegeneinander abgeglichen (wurden), um Übereinstimmungen zu finden, die auch bei einem manuellen Abgleich feststellbar gewesen wären."

[338] BT-Drucks. 16/13657, S. 20f.

[339] *Wank*, in: Erfkomm (o. Fußn. 281), § 32 BDSG Rn. 28; *Deutsch/Diller* (o. Fußn. 321), S. 1464.

[340] BT-Drucks. 16/13657, S. 21.

[341] Obwohl Straftaten und Ordnungswidrigkeiten an anderer Stelle gleichwertig behandelt werden, vgl. § 35 Abs. 2 S. 2 Nr. 2 BDSG.

tiertes BAG Urteil zur verdeckten Videoüberwachung sah die Überwachung im Einzelfall bei strafbaren Handlungen „und anderen schweren Verfehlungen" als zulässig an[342] und auch der als Vorlage für den Wortlaut von Satz 2 dienende[343] § 100 Abs. 3 Satz 1 TKG erlaubt ein Vorgehen gegen „sonstige rechtswidrige Inanspruchnahmen" von Telekommunikationsdiensten.[344]

Damit ist jedoch nicht gesagt, dass keinerlei Beschäftigtendaten zur Verfolgung von Ordnungswidrigkeiten oder unterstrafrechtlichen Compliance-Verstößen verwendet werden dürften. Die Zulässigkeit von Maßnahmen zur Aufdeckung derartiger Vergehen ist stattdessen an Satz 1 der Norm zu messen.[345] Obwohl dem Wortlaut von Satz 1 nach alleine das Kriterium der Erforderlichkeit für die Beurteilung der Rechtmäßigkeit einer Maßnahme einschlägig ist, bedeutet dies auch nicht, dass die Verfolgung strafrechtlich irrelevanter Vergehen intensiver in die Persönlichkeitsrechte der Beschäftigten eingreifen dürfe, als dies bei der Verfolgung von Straftaten gemäß Satz 2 erlaubt wäre.[346] Vielmehr sind die Anforderungen aus Satz 2 analog anzuwenden.[347] Andernfalls würde dies nämlich zu dem widersprüchlichen Ergebnis führen, dass eine Ordnungswidrigkeit oder ein geringfügiger Compliance-Verstoß effektiver aufzudecken wären, als eine schwerwiegende Straftat.[348] Dem Wortlaut nach gelten bei strafrechtlichen Verstößen lediglich höhere Anforderungen an die Interessenabwägung, da Maßnahmen zur Aufdeckung einer Straftat zumeist besonders intensiv in das APR eingreifen[349] und zwar insoweit, als die Bezichtigung einer Straftat die soziale Anerkennung des Beschuldigten stärker angreift, als etwa die Bezichtigung einer geringfügigen Vertragsverletzung.[350]

3.4.4.1.3 Tatsächliche zu dokumentierende Anhaltspunkte, die den Verdacht einer Straftat begründen

Die Voraussetzung der tatsächlichen zu dokumentierenden Anhaltspunkte, die den Verdacht einer Straftat begründen, verhindert verdachtslose Eingriffe in

[342] *BAG* , Urt. v. 27.03.2003 - 2 AZR 51/02, NZA 2003, 1193 (1195); Vgl. auch Hinweis bei *Hanloser*, MMR 2009, 594 (597).
[343] BT-Drucks. 16/13657, S. 21.
[344] *Erfurth* (o. Fußn. 309), S. 2921.
[345] *Albrecht* (o. Fußn. 293), S. 3; *Gola/Schomerus* (o. Fußn. 37), § 32 Rn. 29; *Hanloser* (o. Fußn. 342), S. 597; a.A. *Wank*, in: Erfkomm (o. Fußn. 281), § 32 BDSG Rn. 28; *Heldmann* (o. Fußn. 244), S. 1238, die die Zulässigkeit von Maßnahmen zur Aufdeckung unterstrafrechtlicher Verstöße an § 28 Abs. 1 Nr. 2 BDSG messen.
[346] *Gola/Schomerus* a.a.O., § 32 Rn. 29.
[347] Grentzenberg/Schreibauer/Schuppert, K&R 2009, 535 (539).
[348] *Schmidt* (o. Fußn. 312), S. 195 f.; ähnlich *Deutsch/Diller* (o. Fußn. 321), S. 1464.
[349] BT-Drucks. 16/13657, S. 21.
[350] *Schmidt* (o. Fußn. 312), S. 197.

die Persönlichkeitsrechte der Beschäftigten „ins Blaue hinein“[351]. Die Formulierung erinnert an den strafprozessrechtlichen Begriff des Anfangsverdachts gemäß § 152 Abs. 2 StPO.[352] Dieser soll erbracht sein, wenn Indizien, beurteilt im Rahmen eines gewissen Erfahrungswertes, zumindest auf eine Straftat hindeuten.[353] Auch § 100 Abs. 3 Satz 1 TKG, welcher für Ermittlungsmaßnahmen ebenfalls auf das Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte für einen Missbrauch abstellt, wird analog der strafprozessrechtlichen Grundsätze dahingehend ausgelegt, dass Tatsachen vorzuliegen haben, die einen Missbrauch als möglich erscheinen lassen.[354] Überdies wird ebenfalls vertreten, der von § 32 BDSG geforderte Verdacht müsse auf Grund seiner Formulierung unterhalb der für § 152 Abs. 2 StPO maßgeblichen Schwelle liegen.[355]

Dennoch spricht vieles[356] für eine restriktive Auslegung der Vorschrift, zumal sie auf Entscheidungen des BAG zur verdeckten Videoüberwachung basiert, in denen die Gerichte die Überwachungsmaßnahmen nur dann als zulässig erachteten, wenn alle anderen, die Arbeitnehmerrechte weniger belastenden Möglichkeiten zur Aufdeckung von Straftaten erschöpft waren.[357] Im Umkehrschluss ergibt dies jedoch, dass sich die Strenge der Anforderungen an die tatsächlichen, einen Verdacht begründenden Anhaltspunkte, aus einer im Einzelfall vorzunehmenden Verhältnismäßigkeitsprüfung ergibt, welche die schutzwürdigen Interessen der Beschäftigten zwar besonders berücksichtigt, jedoch auch die schützenswerten Interessen des Arbeitgebers beachtet. So können je nach Sachverhalt bereits Anzeigen aus einem Whistleblowing-

[351] *Schaar*, Interview mit der Zeitschrift WirtschaftsWoche , S. 3, http://www.wiwo.de/unternehmen-maerkte/pendel-am-anschlag-406957/ (Stand: 26.03.2010)

[352] *Brandt*, CuA 11/2009, S. 9; *Erfurth* (o. Fußn. 309), S. 2920; *Hanloser* (o. Fußn. 342), S. 597; *Olbers* (o. Fußn. 272), S. 846.

[353] *Pfeiffer*, StPO, § 152 Rn. 1a; siehe weiterhin Abschnitt 4.3.2.2.3.

[354] *Fetzer*, in: *Arndt/Fetzer/Scherer* (Hrsg.), TKG, § 100 Rn. 13; *Wittern*, in: BeckTKG-Komm, § 100 Rn. 9, der konkrete Anhaltspunkte fordert, die einen Tatverdacht zumindest nahelegen, wozu jedoch schon ein ungewöhnliches Telefonierverhalten zählen könne; siehe aber auch *Wedde,* in: *Däubler/Klebe/Wedde/Weichert* (o. Fußn. 36), § 32 Rn. 127, der unter Hinweis auf *Fetzer* Maßnahmen zur Aufdeckung von Straftaten erst dann als gerechtfertigt erachtet, wenn ein hinreichender Verdacht einer Straftat vorliegt, der zumindest ansatzweise auf Tatsachen gestützt ist, selbst wenn ausreichende Tatsachengrundlagen noch nicht vorliegen.

[355] *Salvenmoser/Hauschka* (o. Fußn. 37), S. 333.

[356] Die Norm wurde ja gerade wegen der öffentlichkeitswirksamen Verfehlungen mancher Unternehmen im Hinblick auf den Arbeitnehmerdatenschutz in das Gesetz eingefügt, BT-Drucks. 16/13657, S. 20.

[357] *Wedde,* in: *Däubler/Klebe/Wedde/Weichert* (o. Fußn. 36), § 32 Rn. 129.

Programm einen hinreichenden Tatverdacht liefern.[358] Zumeist wird der Verdacht jedoch das Ergebnis präventiver Ermittlungsmethoden sein.[359]

Die den Verdacht begründenden Indizien oder Tatsachen sind schließlich durch den Arbeitgeber zu dokumentieren. Hierzu gehören etwa die schriftliche oder elektronische Fixierung des Schadens, des Verdächtigtenkreises und der Indizien, warum die jeweils überwachte Person verdächtig ist.[360] Die Dokumentationspflicht dient vor allem der Rechtfertigung dem Betroffenen gegenüber.[361] Dabei ist zu gewährleisten, dass die Speicherung dauerhaft und jederzeit abrufbar ist.[362] Lässt sich der Verdacht nicht erhärten, sind die dokumentierten Daten gemäß § 35 Abs. 2 Satz 2 Nr. 3 BDSG unverzüglich zu löschen.[363]

3.4.4.1.4 Verhältnismäßigkeit

Die Erhebung, Verarbeitung und Nutzung der personenbezogenen Beschäftigtendaten hat erforderlich zur Aufdeckung der Straftat zu sein. Ferner dürfen das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Datenverwendung nicht überwiegen und insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sein. Diese Anforderungen an Aufdeckungsmaßnahmen kommen einer ausführlichen Verhältnismäßigkeitsprüfung gleich[364], was insoweit nicht verwundert, als sich auch nach ständiger Rechtsprechung des BAG das zulässige Maß einer Beschränkung des APR der Arbeitnehmer nach dem Grundsatz der Verhältnismäßigkeit bestimmt.[365] Die in der Gesetzesbegründung zu § 32 BDSG zitierten und vom BAG aufgestellten, allgemein anwendbaren Grundsätze zur Verhältnismäßigkeit von heimlichen Videoüberwachungen sollen nachfolgend näher erläutert werden.[366]

---

[358] So auch *Hanloser* (o. Fußn. 342), S. 597; *Gola/Wronka* (o. Fußn. 38), Rn. 402; a.A. *Albrecht* (o. Fußn. 293), S. 4, der hierin zwar einen bloßen, unsubstantiierten Verdacht sieht, letztlich aber ebenfalls vom Erfordernis eines Anfangsverdachts spricht, der sich per Definition aus einer Whistleblowing-Meldung ergeben kann.

[359] *Gola/Wronka* (o. Fußn. 38), Rn. 857; Siehe hierzu sogleich 3.4.4.2.

[360] *Wank*, in: Erfkomm (o. Fußn. 281), § 32 BDSG Rn. 29.

[361] *Gola/Schomerus* (o. Fußn. 37), § 32 Rn. 28.

[362] *Wedde,* in: *Däubler/Klebe/Wedde/Weichert* (o. Fußn. 36), § 32 Rn. 127.

[363] *Erfurth* (o. Fußn. 309), S. 2920; nach einer anderen Ansicht sollten auch Verdachtsfälle, die nicht erhärtet werden konnten, dokumentiert werden Dies hätte zwar die Aufrechterhaltung unbegründeter Verdachtsmomente zur Folge, die datenverarbeitende Stelle könne andernfalls jedoch ihre Einhaltung der Dokumentationspflicht nicht beweisen, *Deutsch/Diller* (o. Fußn. 321), S. 1464.

[364] So auch *Albrecht* (o. Fußn. 293), S. 4.

[365] *BAG*, Beschl. v. 26.08.2008 - 1 ABR 16/07, NZA 2008, 1187 (1189), m.w.N.

[366] Dabei wird zur Konzentration auf die tatsächlichen Anforderungen bewusst auf Stimmen aus der Literatur verzichtet. Der aktuelle Meinungsstand ist jedoch bei der Anwendung der hier aufgestellten Regeln in Abschnitt 4 eingearbeitet.

a) Geeignetheit

Dogmatisch ist an erster Stelle der Verhältnismäßigkeitsprüfung und vor der Analyse der Geeignetheit zu untersuchen, ob ein legitimes Mittel eingesetzt wird, um einen legitimen Zweck zu verfolgen. Die Aufdeckung begangener Straftaten ist ohne Frage ein legitimer Zweck.[367] Grundsätzlich kann in der verdeckten Überwachung von Arbeitnehmern auch ein legitimes Mittel gesehen werden. Ob das Mittel darüber hinaus legal ist, wird erst die abgeschlossene Prüfung der Verhältnismäßigkeit zeigen können.

Auch wenn das Kriterium der Geeignetheit nicht im Wortlaut der Norm genannt wird, hat jede Maßnahme zur Erreichung des angestrebten Zwecks geeignet zu sein. Hierbei steht dem Arbeitgeber ein gewisser Beurteilungsspielraum zu.[368] Entscheidend ist, ob die jeweilige Maßnahme die Identifizierung des Täters, dessen Ergreifung und damit die Verhinderung weiterer Straftaten zumindest fördert.[369]

b) Erforderlichkeit

Die Maßnahme hat weiterhin notwendig für die Aufdeckung der Straftat zu sein. Diese Voraussetzung ist erfüllt, wenn alle weniger intensiv in die Persönlichkeitsrechte der Beschäftigten eingreifenden Maßnahmen zur Aufklärung des Verdachts erschöpft sind und die heimliche Überwachung praktisch das letzte verbleibende Mittel darstellt.[370] Auch hier steht dem Arbeitgeber ein bestimmter Beurteilungsspielraum zu, ob ein gleichermaßen effektives, jedoch die Arbeitnehmerrechte weniger belastendes Mittel zur Verfügung steht.[371]

Insbesondere eine verstärkte Kontrolle durch Aufsichtspersonal oder eine offene Videoüberwachung sind zur Aufdeckung von heimlich begangenen Straftaten wenig Erfolg versprechend, da „ein auf Heimlichkeit angelegtes Verhalten (des Täters) seiner Natur nach nicht durch offen angekündigte Beobachtung entdeckt werden“ kann.[372] Auch Taschen- und Personenkontrollen sind nicht geeignet, das gleiche Resultat wie eine verdeckte Überwachung zu erzielen.[373] Stellt man sich den Fall vor, dass ein Beschäftigter geheime, auf einem winzigen Datenträger gespeicherte Dokumente entwendet hat, so würde dies im Zweifelsfall nicht durch eine Taschenkontrolle oder etwa ein Abtasten der Oberbekleidung aufgedeckt werden können. Vielmehr wäre

[367] *BAG* (o. Fußn. 365), S. 1190.
[368] *BAG* a.a.O., S. 1190.
[369] *BAG* a.a.O., S. 1190.
[370] *BAG* (o. Fußn. 342), S. 1195.
[371] *BAG* (o. Fußn. 365), S. 1191.
[372] *BAG* (o. Fußn. 342), S. 1195.
[373] *BAG* (o. Fußn. 365), S. 1191.

hierzu eine „Leibesvisitation“[374] nötig, die jedoch im Einzelfall wegen des nötigen Eingriffs in die Intimsphäre des Beschäftigten noch intensiver dessen Persönlichkeitsrechte beeinträchtigen würde, als die verdeckte Videoüberwachung.

Die Verdeckte Überwachung des Personals darf trotz allem nur das letzte verbleibende Mittel sein. Bevor diese Maßnahme ergriffen wird, sind alle weniger einschneidenden Mittel zur Aufdeckung der Tat anzuwenden, wobei hinsichtlich der Schwere der Straftat auch die Frage nach der Zumutbarkeit der milderen Maßnahmen zu stellen ist.

c) Angemessenheit

Schließlich hat das angewandte Mittel im Hinblick auf den verfolgten Zweck angemessen, d.h. verhältnismäßig i.e.S. zu sein. In diesem Teil der Verhältnismäßigkeitsprüfung ist eine umfassende Güterabwägung zwischen den entgegenstehenden Interessen von Arbeitgeber und Arbeitnehmer durchzuführen, welche ebenfalls die Vorgaben aus § 32 Abs. 1 Satz 2 BDSG umfasst. Danach dürfen der Aufdeckungsmaßnahme kein überwiegendes schutzwürdiges Interesse des Betroffenen entgegenstehen und insbesondere Art und Ausmaß der Maßnahme im Hinblick auf den Anlass nicht unverhältnismäßig sein. Zwar würdigt Satz 2 die berechtigten Interessen des Arbeitgebers mit keinem Wort. Ungeachtet dessen sind nach ständiger Rechtsprechung des BAG[375] und vor dem Hintergrund, dass die geltende Rechtslage durch die Norm nicht verändert werden soll, die Arbeitnehmerrechte mit den Interessen des Arbeitgebers unter Beachtung der Gesamtumstände im Wege der praktischen Konkordanz[376] in Ausgleich zu bringen.

i. Rechte der Arbeitnehmer

In der Formulierung des § 32 Abs. 1 Satz 2 BDSG ist von schutzwürdigen Interessen der Beschäftigten, die am Ausschluss der Datenverwendung überwiegen, die Rede. Die Arbeitnehmer werden durch das grundrechtlich verbürgte APR geschützt. Aus diesem, auch im Arbeitsverhältnis zu beachtenden Recht[377], werden das Recht am eigenen Bild und das Recht auf informationelle Selbstbestimmung (ISBR) abgeleitet. Eingriffe in das Recht am eigenen Bild liegen insbesondere vor, wenn von dem Betroffenen gegen seinen Willen oder ohne dessen Zustimmung Bilder oder Videoaufnahmen angefertigt werden.

[374] Der Begriff wird ebenfalls durch das Gericht aufgegriffen, jedoch wird nur festgestellt, dass die zu verhandelnde Betriebsvereinbarung eben keine „Leibesvisitationen“ vorsieht, vgl. *BAG* a.a.O., S. 1191.

[375] *BAG* (o. Fußn. 342), S. 1194; *BAG* (o. Fußn. 365), S. 1190 m.w.N.

[376] Anders formuliert, sollen zwei konfligierende Grundrechte in einen nach beiden Seiten hin schonendsten Ausgleich gebracht werden, *Schulze-Fielitz*, in: *Dreier* (Hrsg.), GG, Art. 2 II Rn. 35.

[377] *BAG* (o. Fußn. 342), S. 1194.

Das vom Bundesverfassungsgericht im sog. Volkszählungsurteil entwickelte ISBR hebt den Datenschutz in den Rang eines Grundrechts und gewährleistet vor dem Hintergrund der Bedingungen der modernen Datenverarbeitung, die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[378]

Nach dem sich aus dem APR ergebenen, umfassenden Selbstbestimmungsrecht obliegt es also grundsätzlich dem Arbeitnehmer, selbst zu entscheiden, ob Videoaufnahmen von ihm gemacht oder Daten über ihn elektronisch verarbeitet werden dürfen, auch da diese Handlungen negative Auswirkungen auf ihn haben können.[379] Insbesondere die Möglichkeiten moderner Datenverarbeitungen mit unbegrenzter Speicherdauer sind geeignet, einen psychischen Anpassungsdruck auf den Betroffenen auszuüben und somit seine freie Entfaltung der Persönlichkeit zu hemmen.[380] Demgemäß schützt das APR vor einer lückenlosen technischen Überwachung am Arbeitsplatz.[381] Diese Rechte hat der Arbeitgeber ferner im Zusammenhang mit seiner Pflicht aus § 75 Abs. 2 BetrVG zu beachten.[382] Das APR der Beschäftigten findet jedoch seine Schranken in den überwiegenden schutzwürdigen Interessen des Arbeitgebers.[383]

ii. Rechte der Arbeitgeber

Für den Arbeitgeber streiten das Recht am Betriebseigentum aus Art. 14 Abs. 1 Satz 1 GG und das Recht auf unternehmerische Betätigungsfreiheit aus Art. 12 Abs. 1 GG.[384] Diese Rechte gestatten ihm grundsätzlich die Vornahme von Maßnahmen zum Schutz seines Eigentums, wobei ihm ein gewisser unternehmerischer Handlungsspielraum zusteht. Die Aufdeckung von Straftaten im Beschäftigungsverhältnis ist weiterhin ein rechtlich schützenswertes Ziel und kann sich neben dem Eigeninteresse der Aufklärung auch aus gesetzlichen Vorgaben ergeben, die den Arbeitgeber zur Verhinderung bestimmter Straftaten verpflichten.[385] Dabei hat er sowohl ein berechtigtes schützenswertes Interesse an der repressiven Aufklärung von Straftaten, als auch an der präventiven Verhinderung von weiteren Vergehen.[386]

[378] *BVerfGE* 65, 1 (o. Fußn. 254).
[379] *BAG* (o. Fußn. 365), S. 1189.
[380] *BAG* a.a.O., S. 1189; *BAG* (o. Fußn. 342), S. 1194.
[381] *BAG* (o. Fußn. 342), S. 1194.
[382] Siehe Abschnitt 3.4.2.
[383] *BAG* (o. Fußn. 342), S. 1194.
[384] *BAG* a.a.O., S. 1195.
[385] *BAG* (o. Fußn. 365), S. 1190.
[386] *BAG* a.a.O., S. 1190.

iii. Praktische Konkordanz

Die entgegenstehenden Interessen sind sodann mit Hilfe einer Güterabwägung in Ausgleich zu bringen. Maßgeblich sind auf die Intensität des Eingriffs in Form der verdeckten Überwachung und das Gewicht der ihn rechtfertigen Gründe abzustellen.[387] Zur Beurteilung der Schwere des Eingriffs ist insbesondere von Bedeutung, wie viele Personen wie intensiv den Beeinträchtigungen ausgesetzt sind, ob beispielsweise auch die Intim- oder Privatsphäre betroffen ist,[388] ob die Betroffenen anonym bleiben, welche zusätzlichen Informationen durch die Überwachung gewonnen werden können und mit welchen negativen Konsequenzen zu rechnen sein kann.[389] Ferner maßgeblich sind die Dauer und Art der Überwachungsmaßnahmen sowie ob der Betroffene einen Grund für sie geliefert hat, etwa durch einen Rechtsverstoß,[390] oder im Gegensatz dazu eine wahllose, allgemeine (Verhaltens-) Kontrolle der Beschäftigten stattfindet.[391]

Ist ein konkreter Verdacht auf eine Straftat gegeben, muss eine Aufklärung vor dem Hintergrund der schutzwürdigen Interessen des Arbeitgebers jedoch möglich sein. Sind alle milderen Mittel ausgeschöpft, kann die verdeckte Überwachung sogar als eine Handlung aus Notwehr oder einer notwehrähnlichen Situation[392] heraus gewertet werden. Der unangreifbare, absolute Kernbereich privater Lebensgestaltung der Arbeitnehmer wird zudem nicht verletzt, wenn sich die Überwachung auf den Arbeitsplatz begrenzt.[393] Die Überwachung aufgrund eines „räumlich und funktional konkretisierten Verdachts“ ermöglicht ferner, unschuldige Personen aus dem engen Kreis der Verdächtigten auszuschließen.[394] Im Ergebnis ist

> „die heimliche Videoüberwachung eines Arbeitnehmers zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die verdeckte Video-Überwachung praktisch das einzig verbleibende Mittel darstellt und insgesamt nicht unverhältnismäßig ist.“[395]

Schlussfolgerungen zu den Ausführungen dieses Abschnitts erfolgen sogleich in Abschnitt 3.4.4.3 im Rahmen einer Würdigung des § 32 BDSG insgesamt.

---

[387] *BAG* a.a.O., S. 1190.
[388] *BAG* (o. Fußn. 342), S. 1195.
[389] *BAG* (o. Fußn. 365), S. 1190.
[390] *BAG* a.a.O., S. 1190.
[391] *BAG* (o. Fußn. 342), S. 1195.
[392] *BAG* a.a.O., S. 1195).
[393] *BAG* (o. Fußn. 365), S. 1189.
[394] *BAG* (o. Fußn. 342), S. 1195.
[395] *BAG* a.a.O., S. 1195

3.4.4.2 Anwendung von § 32 Abs. 1 Satz 1 BDSG zur Prävention von Straftaten

Verdachtsunabhängige Maßnahmen im Zusammenhang mit Compliance geschehen i.d.R. zur Prävention von Straftaten.[396] Die Zulässigkeit solcher und anderer präventiver Ermittlungshandlungen zur Verhinderung von Straftaten und anderen Rechtsverstößen ist zwar grundsätzlich an § 32 Abs. 1 Satz 1 BDSG zu messen, da sie laut der Gesetzesbegründung im Rahmen der Durchführung des Beschäftigungsverhältnisses erlaubt sind.[397] Jedoch darf nicht zugelassen werden, dass gerade in Fällen ohne Vorliegen eines konkreten Verdachts für präventive Ermittlungen die strengen Anforderungen aus Satz 2 nicht gelten sollen.[398] Andernfalls müsste der Arbeitgeber für Datenverwendungen im Rahmen der Verhinderung von Straftaten gemäß Satz 1 lediglich die Erforderlichkeit der jeweiligen Maßnahme nachweisen, womit der von § 32 BDSG angestrebte Schutz der Beschäftigten vor zu weit gehenden Eingriffen in deren Persönlichkeitsrechte, nahezu ausgehöhlt würde. Eine ausschließlich an Satz 1 gemessene Beurteilung präventiver Maßnahmen wäre also gleichbedeutend mit der Umgehung der Gesetzeslage und damit unzulässig.

Daher sind Präventionsmaßnahmen vielmehr im systematischen Zusammenhang mit Satz 2 zu lesen. Dies bedeutet nicht, dass alle Tatbestandsmerkmale der Norm einschlägig wären. So können etwa bei verdachtsunabhängigen, präventiven Maßnahmen gerade keine tatsächlichen Anhaltspunkte, die den Verdacht einer Straftat begründen, vorliegen. Jedoch sind die Präventionsmaßnahmen der gleichen soeben dargestellten Verhältnismäßigkeitsprüfung zu unterziehen.[399] Dies gilt umso mehr, als der Übergang zwischen präventivem und restriktivem Handeln fließend ist und der Arbeitgeber sich auch bei scheinbar offensichtlich präventiven Maßnahmen, nur unter Beachtung der erhöhten Anforderungen aus Satz 2 in rechtlicher Sicherheit wähnen kann. Die Sorge vor in Zukunft erschwerten verdachtsunabhängigen Ermittlungsmethoden ist gleichwohl unbegründet. Schon vor der Einführung von § 32 BDSG hatten derartige Handlungen einer Verhältnismäßigkeitsprüfung bedurft[400] und es sei an dieser Stelle erneut auf den Willen des Gesetzgebers hingewiesen, dass eine Veränderung der Rechtslage nicht beabsichtigt ist.

Eine ausführliche Prüfung der Verhältnismäßigkeit am Fallbeispiel einer präventiven Datenanalyse erfolgt unter Abschnitt 4.2.2.

---

[396] *Wybitul* (o. Fußn. 30), S. 1583; *Erfurth* (o. Fußn. 309), S. 2921.
[397] BT-Drucks. 16/13657, S. 21; *Albrecht* (o. Fußn. 293), S. 3; *Gola/Wronka* (o. Fußn. 38), Rn. 401, 853 ff.; *Heldmann* (o. Fußn. 244), S. 1237; *Schmidt* (o. Fußn. 312), S. 197; im Ergebnis auch *Zikesch/Reimer* (o. Fußn. 337), S. 96.
[398] *Erfurth* (o. Fußn. 309), S. 2921.
[399] *Thüsing* (o. Fußn. 306), S. 868; *Gola/Schomerus* (o. Fußn. 37), § 32 Rn. 25; ähnlich *Schmidt* (o. Fußn. 312), S. 198; a.A. *Vogel/Glas* (o. Fußn. 261), S. 1751.
[400] Siehe bereits die Nachweise in Fußn 337.

3.4.4.3 Würdigung

Die Einordnung von präventiven Ermittlungsmethoden unter Satz 1 und damit die Feststellung deren grundsätzlicher Zulässigkeit, hat im Wortlaut des § 32 BDSG keine Erwähnung gefunden, weshalb sich diesbezüglich auch noch keine h.M. in der Literatur durchgesetzt hat. Eine diese Zuordnung ablehnende Auffassung hätte allerdings zur Folge, dass präventive und somit auch verdachtsunabhängige Ermittlungen an Satz 2 zu messen wären, womit derartige Maßnahmen wegen des offensichtlichen Fehlens tatsächlicher den Verdacht begründender Anhaltspunkte fortan allgemein unzulässig wären. Dies würde den Vorschriften aus den Bereichen Corporate Governance und Compliance, welche die Vornahme verdachtsunabhängiger Datenanalysen zur Verhinderung von Fraud etwa in der Rechnungslegung in vielen Fällen unumgänglich machen, ad absurdum führen.[401] Daneben wäre diese Auslegung – dies kann nicht oft genug wiederholt werden – nicht mit dem Grundgedanken von § 32 BDSG vereinbar, nämlich die geltende Rechtslage und damit die grundsätzliche Zulässigkeit der in Frage stehenden Ermittlungen zur Generierung von Verdachtsmomenten bei nachgewiesener Verhältnismäßigkeit[402], nicht zu ändern.

Die historische Auslegung von § 32 BDSG lässt wegen der ausdrücklichen Zuordnung präventiver Ermittlungsmethoden zur Verhinderung von Straftaten[403] zu Satz 1 der Norm keinen anderen Schluss zu, als die Annahme der grundsätzlichen Rechtmäßigkeit verdachtsunabhängiger Maßnahmen. Zum gleichen Ergebnis gelangt man, wenn man die dem Anbieter von Telekommunikationsdienstleistungen gemäß § 100 Abs. 3 TKG im Rahmen der Missbrauchsbekämpfung zur Verfügung stehenden Mittel betrachtet.[404] Aus Satz 1 jener Vorschrift ist der Wortlaut von § 32 Abs. 1 Satz 2 BDSG entliehen;[405] welche Rechte dem Anbieter konkret zustehen, ergibt jedoch erst die Gesamtschau von Abs. 3 der TKG-Norm.[406] Hiernach darf der Anbieter etwa den Gesamtbestand der in den letzten 6 Monaten gesammelten Verbindungsdaten, in pseudonymisierter Form und unter Beachtung der Verhältnismäßigkeit, durch die Anwendung von bestimmten Suchfiltern nach konkreten, auf einen Missbrauch hindeutenden Indizien rastern.[407] Diese Befugnis spricht für die Wertung, dass § 32 BDSG ebenfalls verdachtsunabhängige Ermittlungen zur Generierung von Verdachtsfällen zulässt.[408] Auch aus der Rechtsprechung des

[401] *Gola/Schomerus* (o. Fußn. 37), § 32 Rn. 26.
[402] Siehe bereits die Nachweise in Fußn. 337.
[403] BT-Drucks. 16/13657, S. 21.
[404] *Schmidt* (o. Fußn. 312), S. 197.
[405] BT-Drucks. 16/13657, S. 21.
[406] *Schmidt* (o. Fußn. 312), S. 197.
[407] *Fetzer*, in: *Arndt/Fetzer/Scherer* (o. Fußn. 354), § 100 Rn. 16 f.; *Wittern*, in: BeckTKG-Komm, (o. Fußn. 354), § 100 Rn. 11.
[408] *Schmidt* (o. Fußn. 312), S. 197

BAG, nach welcher sich die Regelung laut dem Gesetzgeber inhaltlich orientiert,[409] ergibt sich lediglich, dass selbst intensivste Eingriffe in das Persönlichkeitsrecht der Arbeitnehmer – denn hierum handelt es sich bei der den genannten Entscheidungen zugrunde liegenden verdeckten Videoüberwachung und der damit verbundenen Gefahr der Erstellung von Verhaltensprofilen schlussendlich – als letztes Mittel zur Bekämpfung von Straftaten zulässig sein können.[410]

Ein Verbot automatischer Datenabgleiche zur Generierung von Verdachtsfällen, welche unter Beachtung der Verhältnismäßigkeit mit vergleichsweise niedriger Intensität in die Arbeitnehmerrechte eingreifen, kann demzufolge nicht beabsichtigt worden sein. Daher ist *Schmidt* zuzustimmen, der den Begriff der Aufdeckung an die Aufrechterhaltung und Weiterverfolgung von Verdachtsfällen knüpft. Datenverwendungen in diesem Zusammenhang sind danach an § 32 Abs. 1 Satz 2 BDSG zu messen und etwa unzulässig, falls sich ein Verdacht als unbegründet herausstellt.[411] Bei der Perpetuierung von Verdachtsfällen erscheinen die erhöhten Anforderungen von Satz 2 ferner gerechtfertigt, da hier die soziale Anerkennung des Betroffenen einer erheblichen Gefahr ausgesetzt wird und er bei der Überführung einer Straftat mit harten arbeitsrechtlichen Konsequenzen zu rechnen hat.[412] Von präventiven Datenanalysen geht eine solche Gefahr jedoch nicht aus. Die Generierung von Verdachtsfällen unterliegt dementsprechend den Voraussetzungen von § 32 Abs. 1 Satz 1 BDSG, wobei wegen des systematischen Zusammenhangs zu Satz 2 zumindest eine umfassende Verhältnismäßigkeitsprüfung präventiver Mechanismen zur Missbrauchsbekämpfung zu verlangen ist.[413]

Der Anwendungs-Konflikt ließe sich überdies ganz einfach lösen, indem man sich den zumeist fließenden Übergang zwischen präventivem und restriktivem Handeln zunutze macht. So kann eine Datenanalyse als Maßnahme zur Verhinderung von Straftaten starten und an einem gewissen Punkt in eine Aufdeckungsmaßnahme übergehen. Somit wäre der Abgleich zweier pseudonymisierter Listen mit Kontodaten zur Aufdeckung von Scheingeschäften an Satz 1 zu messen und müsste lediglich dem Grundsatz der Verhältnismäßigkeit entsprechen. Will man die Ergebnisse des Abgleichs reidentifizieren, gerät man in den Bereich der Aufdeckung von Straftaten, womit Satz 2 einschlägig wird. Da die auf legale Weise erlangte pseudonyme Information jedoch bereits ein Indiz für eine Straftat darstellt, steht einer Weiterverfolgung des Verdachts auf Grundlage von Satz 2 nichts im Wege.[414]

---

[409] BT-Drucks. 16/13657, S. 21.
[410] *BAG* (o. Fußn. 342), S. 1195.
[411] *Schmidt* (o. Fußn. 312), S. 197.
[412] Etwa kann eine fristlose Kündigung gerechtfertigt sein, *Albrecht* (o. Fußn. 293), S. 3.
[413] *Thüsing* (o. Fußn. 306), S. 868; *Gola/Schomerus* (o. Fußn. 37), § 32 Rn. 25; ähnlich *Schmidt* (o. Fußn. 312), S. 198; a.A. *Vogel/Glas* (o. Fußn. 261), S. 1751.
[414] Eine umfassende Anwendung dieser Grundsätze anhand eines Praxisbeispiels erfolgt in den Abschnitten 4.2 und 4.3.

Innerhalb der Anwendung von § 32 BDSG ist zu beachten, dass einerseits nicht jede Maßnahme gleich intensiv in die Arbeitnehmerrechte eingreift und sich unter Berücksichtigung einiger grundlegender Prinzipien des Datenschutzrechts weniger belastend gestalten lassen. Andererseits ist zu berücksichtigen, dass laut der Gesetzesbegründung bei der Beurteilung der Verhältnismäßigkeit einer Überwachungsmaßnahme insbesondere der Art und Schwere der Straftat und der Intensität des Verdachts Rechnung zu tragen sind.[415] Dies bedeutet allerdings nicht, dass der Arbeitgeber nicht etwa auch dem konkreten Verdacht des Diebstahls von an sich unerheblichen Arbeitsmaterialien, wie Druckerpatronen, durch systematische Datenauswertungen nachgehen dürfte.[416]

Kritiker des § 32 BDSG monieren, dass die Norm aufgrund der vielen unbestimmten Rechtsbegriffe eine Einzelfallentscheidung für jeden gesonderten Sachverhalt unumgänglich macht.[417] Der umgekehrte Fall, wenn nämlich der Gesetzgeber im Rahmen des angekündigten,[418] umfassenden Arbeitnehmerdatenschutzgesetzes, die Zulässigkeit jeder möglichen Form von Datenerhebungen durch Gesetz bestimmte, würde einen flexiblen Umgang mit personenbezogenen Beschäftigtendaten in der Praxis allerdings zusätzlich erschweren. Denn im Anwendungsbereich des Datenschutzrechts, wie in nahezu keinem anderen Rechtsgebiet, entstehen mit der Zeit immer neuere Technologien, die die Auswertung von Daten ermöglichen und ein zu konkreter Gesetzestext könnte dieser Entwicklung nicht standhalten. Schon vor der Novelle war vor jeder Datenverwendung eine Interessenabwägung durchzuführen, welche mal mehr und mal weniger eindeutig für das überwiegende Interesse einer Partei sprach. Und auch unter der aktuellen Rechtslage ist von den Unternehmen zu verlangen, dass vor jeder Maßnahme eine umfassende Abwägung der entgegenstehenden Interessen und insbesondere eine Prüfung der Verhältnismäßigkeit einer jeden Maßnahme vorgenommen werden. Daneben besteht die Möglichkeit, Fallgruppen für oftmals auftretende Abwägungsfragen zu bilden, was zur Reduzierung des bemängelten Mehraufwandes beiträgt.

[415] BT-Drucks. 16/13657, S. 21.
[416] *Gola/Schomerus* (o. Fußn. 37), § 32 Rn. 27.
[417] *BvD*, DuD 2010, 254.
[418] BT-Drucks. 16/13657, S. 18; http://www.heise.de/newsticker/meldung/Innenministerium-macht-Vorstoss-zu-Arbeitnehmer-Datenschutzgesetz-996923.html (Stand: 12.05.2010).

3.4.5
Datenerhebung und –speicherung für eigene Geschäftszwecke

§ 32 BDSG als Spezialnorm verdrängt für Zwecke des Beschäftigungsverhältnisses die Anwendbarkeit von § 28 BDSG als allgemeinen Erlaubnistatbestand zur Datenerhebung und –speicherung für eigene Geschäftszwecke von nichtöffentlichen Stellen. Lediglich für andere Zwecke können auch im Verhältnis zwischen Arbeitgeber und Arbeitnehmer die allgemeinen Erlaubnistatbestände des BDSG herangezogen werden.[419] So bleibt § 28 Abs. 1 Satz 1 Nr. 2 BDSG, wonach Datenverwendungen zulässig sind, soweit sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich sind und keine überwiegenden schutzwürdigen Interessen des Betroffenen bestehen, in bestimmten Fällen weiterhin anwendbar.

Ein Anwendungsfall der Norm sind etwa Datenverwendungen im Zusammenhang mit Veröffentlichungen in Werkszeitungen, da diese für keine der in § 32 Abs. 1 Satz 1 BDSG genannten Phasen des Beschäftigungsverhältnisses erforderlich sind.[420] Auf keinen Fall ist in § 28 Abs. 1 Satz 1 Nr. 2 BDSG aber eine gleichberechtigte Anwendungsalternative zu § 32 BDSG zu sehen: Eine beschäftigungsbezogene Datenverwendung, die durch § 32 BDSG nicht gerechtfertigt ist, kann nicht durch § 28 Abs. 1 Satz 1 Nr. 2 BDSG legitimiert werden, seine Anwendung ist gesperrt.[421] Insbesondere kann jene Norm nicht zur Rechtfertigung präventiver Maßnahmen zur Verhinderung von Rechtsverstößen herangezogen werden.[422]

Für die vorliegende Arbeit kann § 28 Abs. 1 Satz 1 Nr. 2 BDSG in jenen Fällen relevant sein, in welchen der Arbeitgeber Im Rahmen der Missbrauchsbekämpfung etwa personenbezogene Daten eines Lieferanten oder Kunden verwenden möchte. Die neben der oben genannten wenigen weiteren Ausnahmen, in welchen § 28 BGDSG im Beschäftigungsverhältnis weiterhin eingreift, etwa beim Umgang mit besonderen Arten von personenbezogenen Daten,[423] sind dagegen nicht Gegenstand der Betrachtung.[424]

---

[419] BT-Drucks. 16/13657, S. 21.
[420] *Gola/Wronka* (o. Fußn. 38), Rn. 407.
[421] *Gola/Wronka* a.a.O., Rn. 404 f.
[422] *Wedde,* in: *Däubler/Klebe/Wedde/Weichert* (o. Fußn. 36), § 28 Rn. 47; a.A. *Vogel/Glas* (o. Fußn. 261), S. 1751.
[423] Definition in § 3 Abs. 9 BDSG.
[424] Vgl. hierzu *Gola/Wronka* (o. Fußn. 38), Rn. 404 ff.; *Erfurth* (o. Fußn. 309), S. 2922 ff.; *Gola/Schomerus* (o. Fußn. 37), § 32 Rn. 31-42.

4
Unternehmensinterne Kontroll-Maßnahmen und ihre Beurteilung nach deutschem Datenschutzrecht

Wie bereits ausführlich dargestellt, ist die Unternehmensleitung der AG verpflichtet, ein IKS zu installieren. Im Rahmen des damit zusammenhängenden AFM ist zwischen Maßnahmen zur Vermeidung, Entdeckung und Reaktion in Bezug auf wirtschaftskriminelle Handlungen zu unterscheiden.[425] Insbesondere die beiden erstgenannten Tätigkeitsfelder sind von Interesse für diese Arbeit.[426]

In den Bereich der Aufdeckung von Wirtschaftskriminalität fallen etwa Ermittlungsmethoden wie die Durchsuchung des Arbeitsplatzes eines Verdächtigten oder die Befragung von Kollegen aus dessen näherem Umfeld.[427] Im Rahmen ihrer Vermeidung ist eine Reihe von Maßnahmen zu ergreifen, die bereits erheblich zur Prävention von Rechtsverstößen im Unternehmen beitragen, wegen ihrer meist rein organisatorischen Natur jedoch keinerlei datenschutzrechtliche Implikationen hervorrufen. Gleichwohl sind diese Vorkehrungen von großer Bedeutung für die datenschutzrechtliche Beurteilung von AFM-Maßnahmen in Hochrisikobereichen, in denen etwa auch Analysen von personenbezogenen Beschäftigtendaten durchzuführen sind. Das Vorhandensein der nachfolgend unter 4.1 kurz geschilderten, grundlegenden Maßnahmen des AFM fließt in die Verhältnismäßigkeitsprüfung von datenschutzrechtlich relevanten Tätigkeiten mit ein, denn nur wenn alle milderen Mittel ausgeschöpft sind, darf in zulässiger Weise in die Persönlichkeitsrechte der Arbeitnehmer eingegriffen werden.[428]

Zu den AFM-Maßnahmen mit datenschutzrechtlichen Implikationen gehören insbesondere Hinweisgebersysteme, in denen Mitarbeiter Kollegen melden können, die sie eines Missbrauchs verdächtigen (z.B. sog. Whistleblowing-Hotlines),[429] die offene oder verdeckte Videoüberwachung,[430] die Überwachung der Kommunikation der Beschäftigten[431] sowie die automatisierte Analyse großer Datenbestände zum Zweck der Missbrauchsaufdeckung. Zwei ausgewählte Maßnahmen werden in den folgenden Abschnitten einer datenschutzrechtlichen Prüfung unterzogen. Lediglich Abschnitt 4.2., der sich mit der Zulässigkeit präventiver Datenanalysen befasst, enthält dabei eine umfassende Verhältnismäßigkeitsprüfung mit Berücksichtigung der Vorgaben des

[425] *KPMG,* 2006 (o. Fußn. 238), S. 11.
[426] Welche arbeits-, zivil- und oder strafrechtlichen Sanktionen dem Arbeitgeber gegen den in seinem Unternehmen angestellten Täter eines Wirtschaftsdelikts hat, sind nicht Gegenstand der Betrachtung.
[427] Siehe hierzu sogleich Abschnitt 4.3.1.
[428] Siehe bereits Abschnitt 3.4.3.2.
[429] Siehe hierzu *Mahnhold*, NZA 2008, 737 ff.; *Mengel* (o. Fußn. 286), S. 199-204.
[430] Siehe hierzu *Forst*, RDV 2009, 204ff.
[431] Siehe hierzu *Dann/Gastell*, NJW 2008, 2945 ff.; *Wellhörner/Byers* (o. Fußn. 246), S. 2310 ff.

BVerfG und des europäischen Gemeinschaftsrechts. Die dort gewonnenen Grundsätze lassen sich jedoch zumeist auf den anschließenden Abschnitt 4.3. anwenden, welcher sich mit der rechtlichen Beurteilung von Aufdeckungsmaßnahmen, die an die Datenanalyse anschließen, befasst.

Neben den Vorschriften des Datenschutzrechts hat der Arbeitgeber im Rahmen von Kontrollmaßnahmen auch die einschlägigen kollektivrechtlichen Voraussetzungen zu beachten. Diese ergeben sich im Wesentlichen aus dem BetrVG und gewähren dem (Konzern-)Betriebsrat der Gesellschaft verschiedene Mitwirkungs- und Mitbestimmungsrechte. Daher soll in diesem Abschnitt im Rahmen der rechtlichen Beurteilung der dargestellten AFM-Maßnahmen ebenfalls ein kurzer Überblick über die entsprechenden Beteiligungsrechte der Arbeitnehmervertretung gegeben werden.

4.1
Grundlegende organisatorische Kontroll-Maßnahmen des Anti-Fraud-Managements

Zunächst sind fundamentale kaufmännische Grundsätze anzuwenden, wie die Dokumentations- und Nachweispflicht für Zahlungsvorgänge und deren Prüfung durch eine unabhängige Stelle im Unternehmen sowie die Trennung von potentiell mit Interessenkonflikten behafteten Funktionen.[432] Daneben sind Ethik-Richtlinien bzw. sog. *Codes of Conduct* unternehmensweit einzuführen, welche eine unterste Stufe der Fraud-Prevention darstellen.[433] Diese sind dazu gedacht, der gesamten Unternehmensbelegschaft positive Werte wie Integrität, Vertrauen und Verantwortung zu vermitteln. Daneben enthalten sie oftmals die für das jeweilige Unternehmen einschlägigen, von den Mitarbeitern zu beachtenden, gesetzlichen Regelungen, beispielsweise aus den Bereichen Datenschutz-, Umwelt-, Arbeits- oder Kartellrecht.

Bewerber für eine Position im Unternehmen sind auf eventuell begangene Wirtschaftsdelikte in der Vergangenheit hin zu befragen.[434] Mitarbeiter sind im Umgang mit dem geltenden Recht zu schulen und auch über die Schulungen hinaus hat ein fortdauerndes Beratungsangebot zu dieser Thematik zu bestehen.[435] Im Vordergrund steht die Vermittlung dessen, wie schnell etwa ein Fall von Korruption durch das beiläufige Annehmen von Geschenken vorliegt. Daneben ist das Personal dahingehend auszubilden, dass auf einen Missbrauch hindeutende Warnsignale (sog. *Red Flags*)[436], schnellstmöglich er-

[432] *Hauschka/Greeve* (o. Fußn. 22), S. 167.
[433] *Odenthal*, Kriminalität am Arbeitsplatz, S. 46-48.
[434] Hierbei handelt es sich zwar ebenfalls um einen datenschutzrechtlich relevanten Vorgang, das sog. Fragerecht des Arbeitgebers ist aber allgemein anerkannt, siehe hierzu schon Abschnitt 3.4.3.1.1.
[435] *Lampert*, in: *Hauschka* (o. Fußn. 27), § 9, Rn. 32.
[436] In Betracht kommen mangelnde Dokumentation von Vorgängen, Umgehung von Unterschriftenregelungen, stillschweigende Duldung von Fehlverhalten usw., siehe hierzu den ausführli-

kannt werden.[437] Darüber hinaus ist jedem Mitarbeiter ein Compliance-Handbuch auszuhändigen. Eine Verankerung der Compliance im Arbeitsvertrag kann die Ausgangsposition des Arbeitgebers bei späteren arbeitsrechtlichen Streitigkeiten erheblich verbessern.[438]

Zu den wichtigsten grundlegenden Kontrollprinzipien gehören weiterhin folgende Organisationsmaßnahmen: [439]

- Das *Vier-Augen-Prinzip* als Mittel der Funktionstrennung gewährleistet, dass einer alleine keine risikoreichen Entscheidungen treffen kann, sondern eine weitere Person immer eine Zustimmung erteilen muss;
- Nach dem *Need-to-know-Prinzip* darf jeder Mitarbeiter nur so viele Befugnisse sowie lediglich Zugang zu solchen Informationen erhalten, die zur Durchführung seiner Tätigkeit tatsächlich erforderlich sind. Ansonsten haben strikte interne Informationsbarrieren zu gelten;
- Klare Regelungen der Genehmigungsbefugnisse mit expliziter Formulierung von Aufsichtspflichten der Vorgesetzten tragen zu transparenten Verantwortlichkeiten bei;
- *Jobrotationen* in sensiblen Bereichen alle 2-3 Jahre verhindern, dass Angestellte zu Wirtschaftsdelikten verführt werden;
- Für Mitarbeiter im Bereich des Einkaufs sind *Wertgrenzen* zu definieren;
- Alle genannten Maßnahmen können keine hinreichende Abschreckungswirkung entfalten, wenn nicht klar kommuniziert wird, dass jeglicher Regelverstoß geahndet und sanktioniert wird (*Zero Tolerance* Politik).[440]

Bei den genannten Maßnahmen handelt es sich keineswegs um eine abschließende Liste,[441] wie die nachfolgende Abbildung, die zwar speziell auf die Prä-

---

chen Beispielkatalog für entsprechende Indikatoren bei *Greeve*, in: *Hauschka* (o. Fußn. 27), § 24, Rn. 71 f.

[437] Hierbei kommt ein dreistufiges Schulungssystem in Betracht: Jedem Angestellten wird das für das Unternehmen im Allgemeinen und für ihn im Speziellen einschlägige geltende Recht vermittelt. Beim Aufsichtspersonal kommen Einweisungen hinzu, wie auf Wirtschaftsdelikte hindeutende Warnsignale effektiv erkannt werden können. Beim vorrangig mit der Bekämpfung von Fraud befassten Personal schließlich, z.B. Mitarbeitern der internen Revision, steht die systematische Schulung etwa im Umgang mit spezieller Prüfsoftware im Vordergrund, siehe hierzu *KPMG*, 2006 (o. Fußn. 238), S. 17 f.

[438] *Klindt*, NJW 2006, 3999 (3400).

[439] Zu alledem *KPMG,* 2006 (o. Fußn. 238), 19 f.; *Odenthal* (o. Fußn. 433), S. 35 ff.

[440] Kritisch hierzu *Hauschka/Greeve* (o. Fußn. 22), S. 171.

[441] Auch die Mitteilung, dass die Möglichkeit anonymer Whistleblowing-Meldungen besteht, hat abschreckende Wirkung, ganz gleich ob die Möglichkeit tatsächlich besteht, oder nicht. Ferner in Betracht kommen spezifische Unterschriftenregelungen, Anreiz- und Bestrafungssysteme etc., siehe hierzu *Greeve*, in: *Hauschka* (o. Fußn. 27), § 24, Rn. 68; siehe ferner die *Richtlinie der Bundesregierung zur Korruptionsprävention in der Bundesverwaltung* v. 30.07.2004, http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_30072004_O4634140151.htm (Stand: 23.05.2010).

vention von Korruption zugeschnitten, jedoch auf die Verhinderung sämtlicher Wirtschaftsdelikte übertragbar ist, verdeutlicht. Auch reicht die Berücksichtigung dieser Prinzipien alleine nicht aus.[442] Vielmehr hat die Unternehmensleitung ausführlich zu dokumentieren, dass alle grundlegenden Präventionsmaßnahmen ergriffen wurden. Erst wenn dies geschehen ist und es dennoch zu Fällen von Fraud kommt, können grundrechtsintensive Methoden zur Prävention zulässig sein.

Risikopotential → Unternehmensgröße ↓ ↓ ↓	Unternehmerischer Normalfall (Stufe I)	Gefährdete Branche/Tätigkeit etc. (Stufe II)	Bereits konkrete Vorfälle (Stufe III)
alle Unternehmen, auch Kleinbetriebe	- auf Korruptionsthemen bezogene(s) Risikoanalyse und Commitment der Geschäftsleitung - nachweisbare Vermittlung von erforderlichen Fach- bzw. Rechtskenntnissen - Einhaltung kaufmännischer Grundsätze - Dokumentations- und Nachweispflichten, Funktionstrennung, Regelungen zu Nebentätigkeiten, Beteiligungen, Berater- und Beiratstätigkeit, Spenden, Sponsoring, Kontoeröffnung, Geschenken, Bewirtungen, Privatgeschäften mit Geschäftspartnern - regelmäßige Durchführung von Stichproben - Einschreiten der Leitung bei konkretem Verdacht - Streben nach Transparenz im Unternehmen	*ergänzend:* - Branchenrisikoanalyse (etwa Handelsrisiken, Auslandsrisiken, gefährdete Branche und Tätigkeit) - Commitment und Kommunikation auf Ergebnis der Risikoanalyse bezogen - Jobrotation in gefährdeten Bereichen - Einbeziehung von Spezialisten - Geschäftsanweisung/Rundschreiben zu betriebsspezifischen Korruptionsthemen - Personalauswahl mit „besonderer Sorgfalt" - Eingehen auf und Umgang mit Lobbyismus - lückenlose Zuständigkeitsregelung - Ethikklauseln in Verträgen	*ergänzend:* - fallbezogene Analyse und Beseitigung der Ursachen - unternehmensinterne Verlautbarung zu beiden Punkten - Zero Tolerance Policy - Versuch der Einführung einer generellen Mitteilungspflicht - Bestellung interner Beauftragter zur Überwachung - Ethikklauseln in Verträgen
mittelständisch geprägte Unternehmen	*ergänzend:* - Existenz einer Abteilung Revision/Controlling - durch diese regelmäßig Prüfung gängiger Indikatorenlisten (auffälliger Lebensstandard, Bevorzugung oder Sonderkonditionen, mangelhafte Dokumentation von Geschäftsvorfällen, unnötige Dienstreisen, Kompetenzüberschreitung etc.) - belastbares Commitment der Leitung - konsequent praktiziertes Vier-Augen-Prinzip - Regelungen zu Beschaffung und Investitionen - Zuständigkeitsregelung und Dokumentation	*ergänzend:* - Risikoprüfung durch Revision/Controlling - Zuschnitt auf spezielle Risikofelder (etwa Kundenveranstaltungen, Kickback-Geschäfte, Nachtragsforderungen, Hochrisikoländer etc.) - individuelle Risikoanpassung in Arbeitsverträgen, Stellenbeschreibungen etc. - anwaltliche Gutachten zu Sonderthemen - verstärkter Organisationsrahmen (Verhaltenskodex, Ethik-Management-System etc.) - Eingehen auf und Umgang mit Lobbyismus - interner Ansprechpartner - Ethikklauseln in Verträgen	*ergänzend:* - Bestandsaufnahme systematisiert und professionalisiert - dazu Beratungsunternehmen - Commitment der Mitarbeiter kontrolliert (Tests, interaktive Schulungen) - überraschende Geschäftsprüfungen - Bestellung eines Compliance-Beauftragten
Großunternehmen, Konzerne	*ergänzend:* - systematische Risikoerkennung durch Revision/Controlling (gezielte Korruptionsprüfungen) - Commitment in Geschäftsanweisung oder Rundschreiben, Face-to-Face-Schulung und ergänzend e-Learning - vollständige Trennung aller Handlungs- von Überwachungsfunktionen im Unternehmen - Existenz eines Bereichs Unternehmenssicherheit/Werkschutz - Bestellung interner Beauftragter	*ergänzend:* - Systematisierung und Professionalisierung bzgl. Prüfungsvorbereitung und Ablauf - sofortige Kommunikation besonderer Gefahrenpotentiale - Nutzung des unternehmensinternen Intranet - Korruptionsbeauftragter oder externer Ombudsmann - Eingehen auf und Umgang mit Lobbyismus - Ethikklauseln in Verträgen	*ergänzend:* - professionelle Ermittlung (Täterprofile, Berater) - Einführung einer permanenten Compliance-Organisation (beobachtet, informiert und schult Mitarbeiter) - anonyme Whistleblower-Hotline (vorzugsweise zu einer externen Anwaltskanzlei)

Abbildung 1: Checkliste zur Korruptionsprävention,[443] welche die jeweiligen Handlungsempfehlungen nach der Größe des Unternehmens und seiner Gefährdungslage definiert

[442] Siehe zur Verbreitung der genannten Maßnahmen in deutschen Großunternehmen *PWC/Martin Luther Universität Halle-Wittenberg* (o. Fußn. 4), S. 56.
[443] *Hauschka/Greeve* (o. Fußn. 22), S. 173.

4.2
Präventive Datenanalysen

Die genannten organisatorischen Maßnahmen alleine sind in Hochrisikobereichen nicht geeignet, ein erfolgreiches AFM zu gewährleisten. In diesen, für Wirtschaftskriminalität besonders anfälligen Unternehmenssektoren – laut einer Studie handelt es sich hierbei um das Finanz- und Rechnungswesen, den Vertrieb sowie das Kreditgeschäft und die IT[444] – sind darüber hinaus stichprobenartige Kontrollen durchzuführen.[445] In diesen wird überprüft, ob es zu heimlichen Fällen von Missbrauch gekommen ist. Die Analyse im Rahmen des AFM ergibt für die einzelnen sensiblen Unternehmensbereiche besonders wahrscheinliche Missbrauchsszenarien. Im Finanz- und Rechnungswesen kommen beispielhaft folgende, in Tabelle 2 dargestellte, Szenarien in Betracht:

Szenario	Test zur Aufdeckung
Fiktive Buchungen für Vertuschungsaktionen	Suche nach Buchungen ohne Belegnummer oder ohne Buchungstext
Lieferanten werden mehrfach ausgezahlt	Suche nach Doppelrechnungen und Doppelzahlungen
Mitarbeiter treten als Lieferanten auf	Abgleich von Mitarbeiter- und Lieferantendaten
Vollmachten werden bei Zahlungs- oder Bestellvorgängen umgangen	Suche nach gesplitteten Zahlungen oder Bestellungen

Tabelle 2: Missbrauchsszenarien und Prüfungsmöglichkeiten[446]

Nachfolgend wird exemplarisch eine präventive Datenanalyse-Maßnahme zur Klärung, ob Mitarbeiter als Lieferanten auftreten, auf ihre Vereinbarkeit mit dem deutschen Datenschutzrecht hin überprüft.

4.2.1
Beschreibung des Vorgangs: Abgleich von Mitarbeiter- und Lieferantendaten zur Aufdeckung von Fraud

Eine in der Unternehmenspraxis häufige Form des Missbrauchs stellt das Auftreten von Mitarbeitern als Lieferanten dar. Sie stellen dem Unternehmen fingierte Rechnungen, für die keine Gegenleistung erbracht wird und lassen sich die unrechtmäßigen Gelder für die angeblichen Aufträge auf das eigene Kon-

[444] *KPMG*, 2010 (o. Fußn 12), S. 9.
[445] *Hauschka/Greeve* (o. Fußn. 22), S. 167; *Lampert*, in: *Hauschka* (o. Fußn. 27), § 9, Rn. 33.
[446] Die Beispiele entstammen *Odenthal* (o. Fußn. 433), S. 108, 112.

to überweisen. Dabei beauftragen sich die Täter zumeist selbst oder haben einen Komplizen, der den Scheinauftrag erteilt bzw. genehmigt. Dieses Szenario ist deshalb verbreitet, da der Missbrauch sich leicht vertuschen lässt. Insbesondere gilt dies für den Verkauf immaterieller Leistungen. Bietet der Täter dem Unternehmen etwa Beratungsleistungen an, so lässt sich der Nachweis, ob die Leistung tatsächlich erbracht wurde, für einen erfahrenen Mitarbeiter, der die entsprechenden Bestätigungsvorgänge kennt, leicht fälschen.

Einer Studie aus dem Jahre 2009 nach handelte es sich bei etwas mehr als der Hälfte der im Berichtszeitraum aufgedeckten Fälle von Wirtschaftskriminalität bei deutschen Unternehmen um einen internen Täter, d.h. um einen Mitarbeiter.[447] Daneben existiert eine nur geringe Wahrscheinlichkeit, dass ein Arbeitnehmer gleichzeitig in einem Lieferantenverhältnis zu seinem Arbeitgeber steht. Daher bietet sich die Suche nach sog. Daten-Dubletten an, bei welchen auf Arbeitnehmer- und Lieferantenseite die gleichen Namen, Anschriften und/oder Kontonummern erscheinen.[448]

Bevor es zu der eigentlichen Datenanalyse kommt, sind einige Vorüberlegungen zu treffen. Der Kreis der von der Überprüfung betroffenen Personen ist so weit wie möglich einzugrenzen. Für das erläuterte Szenario kommen auf der Arbeitnehmerseite zunächst nur alle Bestellberechtigten in Betracht. Dieser Personenkreis ließe sich weiter einschränken, indem lediglich Mitarbeiter mit einer Bestellvollmacht bis zu einer bestimmten erheblichen Wertgrenze von beispielsweise 5000 EUR in die Untersuchung mit einfließen.

Ferner muss das Mitbestimmungsrecht des Betriebsrats beachtet werden, da es sich bei der angestrebten Datenanalyse um eine technische Einrichtung i.S.d. BetrVG handelt.[449] Darüber hinaus ist dem Grundsatz der Transparenz von Datenverwendungen Rechnung zu tragen.[450] Auch wenn das BDSG keine konkrete Pflicht zur Information der Betroffenen enthält,[451] ist diese von großer Bedeutung für die Verhältnismäßigkeit der Maßnahme, da dem Betroffenen nur so die Möglichkeit zu Einwendungen bzw. einem effektiven vorherigen Rechtschutz gegeben wird.[452] Ebenfalls kann die Maßnahme wegen des zu erwartenden Abschreckungseffekts nur dann eine präventive Wirkung entfalten und zukünftige Scheingeschäfte verhindern, wenn die Betroffenen eine Kenntnis von ihr haben.[453] Eine allgemeine Ankündigung von präventiven Analysen im Vorfeld der Maßnahme erfüllt grundsätzlich das Erfordernis der

[447] *PWC/Martin Luther Universität Halle-Wittenberg* (o. Fußn. 4), S. 44.
[448] *Kock/Franke* (o. Fußn. 400), S. 647; nach *Salvenmoser/Hauschka* (o. Fußn. 37), S. 332, drängt sich der Abgleich geradezu auf.
[449] Siehe hierzu Abschnitt 4.2.3.
[450] Siehe zu den Grundsätzen des Datenschutzrechts Abschnitt 3.3.
[451] So schreibt § 4 Abs. 3 BDSG lediglich vor, dass der Betroffene zum Zeitpunkt der Erhebung über jenen Vorgang zu unterrichten ist. Bei der Analyse werden jedoch keine neuen Daten erhoben.
[452] *Kock/Franke* (o. Fußn. 400), S. 650.
[453] *Brandt* (o. Fußn. 352), S. 8; *Gola/Wronka* (o. Fußn. 38), Rn. 860.

Transparenz.[454] Diese Ankündigung kann in Form einer Betriebsvereinbarung geschehen.[455] Dabei ist zu gewährleisten, dass jedem potenziell von der Analyse betroffenen Beschäftigten eine Kenntnisnahme der Vereinbarung ermöglicht wird. Denkbar wäre etwa, das Dokument über das konzerninterne Intranet zugänglich zu machen, da davon auszugehen ist, dass jeder Betroffene im Bereich der Finanzbuchhaltung auch über einen eigenen Computer mit Zugang zu der Vereinbarung verfügt. Überdies hat die Betriebsvereinbarung auch angemessen genaue Angaben darüber zu enthalten, wann die geplante Analyse stattfindet. Etwa könnte vereinbart werden, dass in einem Zeitraum von einem Jahr vier stichprobenartige unangekündigte Untersuchen erfolgen dürfen. Schließlich ist der betriebliche Datenschutzbeauftragte vor der Durchführung der Analyse zu benachrichtigen, damit dieser den ordnungsgemäßen Ablauf überwachen kann.

Die darauf folgende Datenanalyse lässt sich in drei Schritte unterteilen:

1. Schritt: Der eingegrenzte Personenkreis wird in den Stammdaten[456] des Unternehmens erfasst. Der mit der Vorbereitung der Analyse betraute Mitarbeiter A verschlüsselt die Personalnummern und Bankdaten (BLZ und Kontonummer) der betroffenen Mitarbeiter. Die Lieferantennummern und Bankdaten der Lieferanten werden mit demselben Schlüssel (Key) verschlüsselt.[457] Die Verschlüsselungsfunktion hat dabei zu gewährleisten, dass vor der Verschlüsselung übereinstimmende Daten auch nach der Verschlüsselung noch übereinstimmen, damit die Daten im Anschluss verglichen werden können.

2. Schritt: Die Daten werden an den organisatorisch getrennt arbeitenden Analysten B weitergegeben.[458] Für ihn handelt es sich um anonyme Daten, da er nicht über den Entschlüsselungs-Key verfügt.[459] Er hat daher keine Möglichkeit, Rückschlüsse auf die hinter den verschlüsselten Daten stehenden Personen zu ziehen. B führt einen Abgleich zwischen den Bankdaten durch.[460] Als „Treffer"[461] erhält B jene Datensätze, in denen Kontonummern und BLZ übereinstimmen. Die entsprechenden Personal- und Lieferantennummern werden erfasst. Auch diese Daten sind wegen ihrer Verschlüsselung für B

---

[454] *Gola/Wronka* a.a.O., Rn. 860.
[455] *Kock/Franke* (o. Fußn. 400), S. 650.
[456] Hierbei handelt es sich um die vom Arbeitgeber bei der Einstellung erhobenen Daten wie Name, Anschrift, Telefon- und Kontonummer, Schulabschluss etc., *Gola/Wronka* (o. Fußn. 38), Rn. 487.
[457] A erhält also folgende zwei Tabellen:
Tabelle 1: Personalnummer, BLZ_M, Kontonummer_M (M=Mitarbeiterdaten),
Tabelle 2: Lieferantennummer, BLZ_L, Kontonummer_L (L=Lieferantendaten).
[458] Hierbei handelt es sich im keine Übermittlung i.S.v. § 3 Abs. 4 S. 2 Nr. 3 BDSG, da B kein Dritter i.S.d. BDSG ist (vgl. § 3 Abs. 8 BDSG).
[459] Gleichwohl handelt es sich nicht um anonymisierte Daten i.S.v. § 3 Abs. 6 BDSG, da maßgeblich ist, ob die verantwortliche Stelle zur Reidentifikation der Daten fähig ist.
[460] Er vergleicht also (BLZ_M, Kontonummer_M) mit (BLZ_L, Kontonummer_L).
[461] (BLZ_M=BLZ_L) UND (Kontonummer_M=Kontonummer_L).

anonym. Alle Daten der nicht betroffenen Mitarbeiter werden umgehend gelöscht.

3. Schritt: Die Treffer werden wieder an A übermittelt. Unter Anwesenheit eines Vertreters des Betriebsrats[462] entschlüsselt A die Daten und deckt die Identitäten der verdächtigten Mitarbeiter auf, womit der Übergang in den restriktiven Teil der Analyse vollzogen wäre.

4.2.2
Datenschutzrechtliche Überprüfung

Bei dem geschilderten Vorgang werden Lieferantendaten sowie personenbezogene und nicht personenbezogene Beschäftigtendaten verwendet. Bei der nachfolgenden Beurteilung der Datenanalyse fließen die in Abschnitt 3.4.4.1.4 dargelegten Grundsätze des BAG zur verdeckten Videoüberwachung sowie die Ausführungen des ArbG Berlin zu den Datenanalysen der *Bahn AG,* die themenverwandte neuere Rechtsprechung des BVerfG und die vorhandenen Vorgaben des europäischen Gemeinschaftsrechts mit ein.

4.2.2.1
Zulässigkeit der Verwendung der Lieferantendaten

Die Verwendung der Lieferantendaten ist zunächst datenschutzrechtlich unbedenklich, da diese gewerblichen Informationen keine personenbezogenen Daten darstellen.[463] Selbst wenn die Lieferantendaten auf eine hinter dem Betrieb stehende, natürliche Person „durchschlagen"[464] (z.B. „Hi-Fi-Profi Peter Zwegat"), ist eine Verwendung der Daten entweder zur Wahrung der berechtigten Interessen des Arbeitgebers gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG, oder, wegen der allgemeinen Zugänglichkeit der Daten, etwa im Rahmen des Internetauftritts des Lieferanten, gemäß Nr. 3 der genannten Norm, gerechtfertigt. Ferner lässt sich die Ermächtigung zur Nutzung der Daten wirksam im Rahmen der AGB vereinbaren. Vertiefende Ausführungen zu diesem Themenkomplex sind für das Ziel der vorliegenden Arbeit nicht von Relevanz.

4.2.2.2
Zulässigkeit der Verwendung der Beschäftigtendaten

Bereits die in Schritt 1 skizzierte Verwendung der Beschäftigtendaten erscheint trotz der Nutzung nicht personenbezogener Daten vor dem Hintergrund von § 32 BDSG rechtlich bedenklich. Auch wenn eine Pseudonymisie-

---

[462] Personenbezogene Beschäftigtendaten sollten wegen des Mitbestimmungsrechts nur im Beisein eines Mitglieds des Betriebsrats verwendet werden, siehe bereits oben sowie Abschnitt 4.2.3.

[463] Nur natürliche Personen können sich auf den Schutz durch das BDSG berufen, siehe Abschnitt 1.5.6. Eine andere Rechtslage findet sich etwa in Österreich, wo auch juristische Personen dem Schutzbereich des dortigen Datenschutzgesetzes unterfallen.

[464] *Weichert,* in: *Däubler/Klebe/Wedde/Weichert* (o. Fußn. 36), § 3 Rn. 9.

rung der Daten vollzogen wird, gelingt dies regelmäßig nicht, ohne einen vorherigen Zugriff auf die im Stammdatenbestand vorhandenen Klardaten zu Namen und Kontoverbindungen der betroffenen Personen. Dieser Vorgang bedarf einer datenschutzrechtlichen Ermächtigung.

4.2.2.2.1 Ermächtigungsgrundlage

Die vorliegend verwendeten Daten hat der Arbeitgeber zur Wahrnehmung seiner organisatorischen Pflichten, z.B. Gehaltauszahlungen, erhoben. Eine Verwendung der Daten zur Generierung von Verdachtsmomenten für begangene, strafrechtlich relevante Handlungen ist durch den ursprünglichen Zweck nicht gedeckt und benötigt daher eine neue Rechtfertigung.[465] Eine Einwilligung der Arbeitnehmer zur Nutzung der Daten für Präventionshandlungen liegt in der Praxis – und auch im hier gewählten Beispiel – regelmäßig nicht vor[466] und würde ohnehin auf beträchtliche Vorbehalte stoßen.[467] Auch eine Betriebsvereinbarung alleine stellt keine rechtssichere Ermächtigungsgrundlage dar.[468] Damit ist die Zulässigkeit des Datenabgleichs an den Anforderungen aus § 32 BDSG zu messen.

Für Datenverwendungen zum Zweck der Prävention von Straftaten und anderen Rechtsverstößen ist § 32 Abs. 1 Satz 1 BDSG einschlägig.[469] Trotz des fließenden Übergangs in den Bereich der Aufdeckung bereits begangener Straftaten, handelt es sich bei dem geschilderten Vorgang zunächst grundsätzlich um eine präventive Maßnahme[470], da ohne einen konkreten Verdacht nach Missbrauchsfällen gesucht wird. Die von der Analyse ausgehende Abschreckungswirkung fällt ebenfalls in den Bereich der Prävention. Die beschriebenen Schritte 1 und 2 der Analyse sind dementsprechend an § 32 Abs. 1 Satz 1 BDSG zu messen. Erst im 3. Schritt kommt es zu einer Reidentifizierung der pseudonymen Daten. Da nun personenbezogene Beschäftigtendaten zur Aufdeckung von Straftaten verwendet werden sollen, ist hierfür § 32 Abs. 1 Satz 2 BDSG einschlägig,[471] die entsprechende datenschutzrechtliche Überprüfung erfolgt in Abschnitt 4.3.2.2. Die weiteren Ausführungen des vorliegen-

---

[465] *Wank*, in: Erfkomm (o. Fußn. 281), § 32 BDSG Rn. 16.
[466] *Bierekoven,* CR 2010, 203 (205); *Bisges,* MMR 2009*,* XX; *Kock/Franke* (o. Fußn. 400), S. 648.
[467] Siehe Abschnitt 3.4.1
[468] Gleichwohl die Vereinbarung Bedeutung für die später zu prüfende Verhältnismäßigkeit der Maßnahme hat, siehe ferner Abschnitt 3.4.2
[469] Siehe Abschnitt 3.4.4.2.
[470] So auch *Kock/Franke* (o. Fußn. 400), S. 647; *Salvenmoser/Hauschka* (o. Fußn. 37), S. 332; wohl auch *Gola/Wronka* (o. Fußn. 38), Rn. 857 f.; a.A. *Bierekoven* (o. Fußn. 466), S. 206, welche unter Anwendung von § 32 Abs. 1 S. 2 BDSG zwar zurecht darauf hinweist, dass es sich bei den Treffern der Analyse um Indizien einer bereits begangenen Straftat handelt, jedoch insoweit verkennt, dass bei der Datenanalyse das Fehlen konkreter Verdachtsmomente gerade im Vordergrund steht, was eine Anwendung von S. 2 unmöglich macht.
[471] Siehe zu dieser Abgrenzung bereits Abschnitt 3.4.4.3.

den Abschnitts beziehen sich zwar auf den präventiven Teil der Datenanalyse, lassen sich zumeist aber auch auf den restriktiven Teil anwenden, da in beiden Fällen eine Prüfung der Verhältnismäßigkeit durchzuführen ist.

4.2.2.2.2 Verhältnismäßigkeit

Über das Vorhandensein der von § 32 Abs. 1 Satz 1 BDSG geforderten Erforderlichkeit der Analyse hinaus, ist, wegen des systematischen Zusammenhangs zu Satz 2, eine Verhältnismäßigkeitsprüfung der Maßnahme mit einer umfassenden Interessenabwägung durchzuführen. Dies ist ebenfalls ständige Rechtsprechung des BAG zur Zulässigkeit von Eingriffen in das Persönlichkeitsrecht der Arbeitnehmer.

a) Geeignetheit

Die Verhinderung von Straftaten stellt einen nicht nur zweifellos legitimen Zweck für die Datenverwendung dar, darüber hinaus besteht sogar die gesetzliche Verpflichtung dazu.[472] Auch das Mittel der automatisierten Datenanalyse ist grundsätzlich legitim.

Die Maßnahme ist darüber hinaus geeignet, den angestrebten Zweck zu erfüllen. Auch wenn ein durchschnittlich findiger Täter Sorge dafür tragen wird, dass die Konten seines Beschäftigten- und seines Lieferantendaseins eben nicht identisch sind, belegen die im Zusammenhang mit den vieldiskutierten Datenanalysen der *Bahn AG* veröffentlichten Zahlen, dass das beschriebene Verfahren objektiv geeignet ist, Verdachtsfälle von Wirtschaftsdelikten zu generieren.[473] Eine Geeignetheit ergibt sich weiterhin aus der Tatsache, dass der Wirtschaftsprüfer im Rahmen der Abschlussprüfung denselben Abgleich zur Aufdeckung von Missbrauchsfällen durchführt.[474]

b) Erforderlichkeit

Erforderlich ist die Präventionshandlung, wenn dem Arbeitgeber kein milderes, jedoch gleichermaßen geeignetes Mittel zur Verfügung steht.[475] Weniger intensive Mittel stellen etwa die in Abschnitt 4.1 beschriebenen organisatorischen Kontroll-Mechanismen des AFM dar. Diese sind jedoch, wie nachfolgend dargestellt, nicht in gleicher Weise zur Erreichung des angestrebten Zwecks geeignet. Die folgenden Ausführungen sollen keineswegs ein generell schlechtes Menschenbild zeichnen.[476] Allerdings zeigen die zahlreichen Fälle

[472] Siehe Abschnitt 2.
[473] *Kock/Franke* (o. Fußn. 400), S. 648.
[474] *Aßmus* (o. Fußn. 138), S. 600.
[475] Siehe bereits Abschnitt 3.4.3.2.
[476] Siehe zur Person des Wirtschaftsstraftäters und einer Motivanalyse *PWC/Hochschule Pforzheim*, Wirtschaftskriminalität, 2009, S. 22 ff.

von Fraud in der Praxis[477], dass die Unternehmen auf eventuell vorhandene, kriminelle Energien vonseiten der Angestellten vorbereitet sein müssen.

Das reine Vorhandensein eines allgemeinen, unternehmensweiten Verhaltenskodexes, wird kaum zur Prävention von Rechtsverstößen beitragen.[478] Auch schützt eine noch so akribische Bewerberauswahl nicht davor, sich bei der Einstellung ausgerechnet für das „schwarze Schaf" zu entscheiden. Compliance-Schulungen vermögen vielleicht unbeabsichtigte, strafrechtlich relevante Handlungen, etwa das unbewusste Entgegennehmen von Geschenken, zu vermeiden. Vorsätzliche Betrugsfälle, wie das Vortäuschen der Lieferanteneigenschaft eines Mitarbeiters, können so jedoch nicht verhindert werden. Wertgrenzen kann ohne Aufwand ausgewichen werden, indem die Bestellberechtigten höherwertige Bestellungen in mehrere Einzeltransaktionen aufsplitten. Das Vier-Augen-Prinzip lässt sich ebenfalls leicht umgehen: Ein zwischen den sich gegenüberstehenden Beschäftigten entstandenes Vertrauensverhältnis kann bereits dazu führen, dass über Nichteinhaltungen des Rechts oder der innerbetrieblichen Weisungen, anfangs noch im Bagatellbereich und im weiteren Verlauf mit sinkender Hemmschwelle, großzügig hinweg gesehen wird. Dem kann auch mit einer frequentierten Jobrotation und eventuell der Einbeziehung weiterer Genehmigungsinstanzen (Sechs- oder auch Acht-Augen-Prinzip) nur bedingt nachgekommen werden. Ferner kommt eine Aufstockung des Kontrollpersonals in Betracht. Jedoch ist hier dem BAG zuzustimmen, welches anerkennt, dass offene Kontrollen kaum geeignet sind, ein auf Heimlichkeit angelegtes Verhalten aufzudecken.[479] Diese geringen Erfolgschancen in Verbindung mit den durch weiteres Personal entstehenden Kosten erlauben es dem Arbeitgeber, eine die Persönlichkeitsrechte der Arbeitnehmer intensiver beeinträchtigende Maßnahme zu ergreifen, da wirtschaftliche Erwägungen bei der Wahl der Instrumente durchaus legitim sind.[480] Im Übrigen müsste vom Wachpersonal verlangt werden, den Beschäftigten permanent „über die Schulter zu schauen", was wegen des dadurch entstehenden Überwachungsdrucks ebenfalls einen erheblichen Eingriff in die Rechte der Beschäftigten darstellen würde.

Die Datenanalyse besticht mit dem relativ geringen Aufwand an Kosten und Mann-Stunden. Daneben erfüllt sie eine doppelte Präventions-Funktion: Zum einen generiert sie Verdachtsmomente und gestattet ein gezieltes Vorgehen gegen einzelne potentielle Täter. Zum anderen strahlt die Ankündigung von geplanten Analysen, etwa im Rahmen einer Betriebsvereinbarung, eine Abschreckungswirkung aus. Überdies ermöglicht sie ein repressives Vorgehen gegen Mitarbeiter, die bereits Straftaten verübt haben. Zudem ist keinesfalls

[477] Siehe hierzu Abschnitt 1.1.
[478] Richtlinien können Korruption nicht verhindern, vielmehr sind begleitende Maßnahmen nötig, *Herb*, in: *Hauschka* (o. Fußn. 27), § 18, Rn. 24.
[479] *BAG* (o. Fußn. 342), S. 1195.
[480] *Gola/Schomerus* (o. Fußn. 37), § 32 Rn. 12.

eine wohl stets unzulässige[481] Vollkontrolle der Beschäftigten angestrebt bzw. handelt es sich nicht um eine lückenlose technische Überwachung.[482] Dies ergibt sich aus der weit reichenden personellen Eingrenzung der Betroffenen sowie aus den lediglich stichprobenartig angestrebten Prüfungen. Diese Form der Kontrolle ist nicht nur allgemein anerkannt, zur Erfüllung der Aufsichtspflichten gemäß § 130 Abs. 1 OWiG werden sie von den Gerichten sogar als erforderlich angesehen.[483] Sie haben regelmäßig, innerhalb angemessener Zeitabstände und unangekündigt stattzufinden.[484] Auch diese Grundsätze sprechen für eine Verhältnismäßigkeit der vorliegenden Maßnahme.

Zur weiteren Verringerung der Eingriffsintensität wäre eventuell ein dem 1. Schritt vorgezogener weiterer Filter denkbar. In diesem könnte der Verschlüsselungs-Key nach der Verschlüsselung der Mitarbeiter- und der Lieferantendaten automatisch vernichtet werden. Erst wenn der Abgleich mit den dann tatsächlich anonymisierten Daten zu einer nicht unerheblichen Zahl von Treffern führen würde, dürfte der Vorgang mit pseudonymisierten Daten wiederholt werden. Möglich wäre auch, zunächst einen Abgleich zwischen den BLZ von Personal und Lieferanten durchzuführen, da es sich hierbei um keine personenbezogenen Daten handelt. Lediglich die aus dieser Prüfung hervorgehenden Treffer würden weiter behandelt werden. Somit würde man den Personenkreis für die Analyse der personenbezogenen Kontodaten im 2. Schritt noch weiter eingrenzen. Jedoch ist zu beachten, dass der aus § 3a BDSG folgende Grundsatz der Anonymisierung und der Pseudonymisierung selbst unter dem Vorbehalt der Verhältnismäßigkeit steht und seine Befolgung nicht verlangt werden kann, wenn dies einen unverhältnismäßigen Aufwand für den Arbeitgeber bedeuten würde.

Da, wie dargestellt, kein gleichermaßen geeignetes, jedoch weniger intensives Mittel ersichtlich ist, sind automatisierte Datenanalysen personenbezogener Beschäftigtendaten zur Erreichung des definierten Zwecks erforderlich.

c) Angemessenheit

Die Analyse ist auch angemessen und damit verhältnismäßig i.e.S. Dies ergibt zunächst die Beurteilung der Angemessenheit des angewandten Mittels im Verhältnis zum verfolgten Zweck. In anderen Branchen bestehen ausdrückliche gesetzliche Ermächtigungen für die Nutzung von personenbezogenen Beschäftigtendaten zur Missbrauchsaufdeckung.[485] Im Hinblick auf § 25c KWG ist dies zwar auf das enorme Missbrauchsrisiko zurückzuführen, welches all-

[481] *Bierekoven* (o. Fußn. 466), S. 207; *Bisges* (o. Fußn. 466), S. XXII; *Gola/Wronka* (o. Fußn. 38), Rn. 859; *Kock/Franke* (o. Fußn. 400), S. 648; *Schneider*, NZG 2009, 1321 (1326); *Steinkühler*, BB 2009, 1294 (1295); a.A. scheinbar *Diller* (o. Fußn. 402), 439.
[482] *BAG* (o. Fußn. 342), S. 1194.
[483] *BGH*, wistra 1982, 34 (35).
[484] *Bock*, ZIS 2009, 68 (78) m.w.N.
[485] Siehe hierzu Abschnitt 2.1.5.2.

gemein im Bankensektor besteht;[486] bei einem den Ausgangspunkt für diese Arbeit bildenden Unternehmen mit beschriebener Größe und Kapitalmarktzugang, ist das Risiko allerdings kaum geringer. Es leuchtet daher nicht ein, warum für ein Institut i.S.d. KWG und einen Konzern der IT-Branche zwar nahezu identische Corporate Governance und Compliance Anforderungen gelten, jedoch nur ersteres Unternehmen über die nötigen Mittel verfügt, diesen Ansprüchen gerecht zu werden. Damit muss die Maßnahme im Gesamtkontext betrachtet verhältnismäßig sein. Zu demselben Ergebnis führt eine Güterabwägung der sich entgegenstehenden Interessen.

i. Praktische Konkordanz

Das **berechtigte Interesse des Arbeitgebers** ist im vorliegenden Fall höher zu bewerten als die schutzwürdigen Bedürfnisse der Arbeitnehmer. Zunächst existiert eine Fülle von gesetzlichen Verpflichtungen, die den Arbeitgeber zur Vornahme von Präventionshandlungen zwingen und bei der Beurteilung der Verhältnismäßigkeit zu berücksichtigen sind. Dies gilt im Übrigen für die amerikanischen Vorschriften des SOA[487] grundsätzlich genauso, wie auch für die deutschen handels-, aktien- und ordnungswidrigkeitsrechtlichen Regelungen[488]. Zwar hat das BAG in einem jüngeren Beschluss die Ansicht vertreten, dass es sich bei den im SOA enthaltenen Pflichten zur Implementierung von Verhaltenskodexes um keine die Mitbestimmungsrechte des Betriebsrats gemäß § 87 Abs. 1 BetrVG ausschließende gesetzlichen Regelungen handelt.[489] In Rechtsprechung und Literatur besteht darüber hinaus keine Einigkeit darüber, ob ausländische Vorschriften in einem in Deutschland geführten Rechtsstreit durch ein deutsches Gericht entsprechend einer Eingriffsnorm i.S.v. Art. 34 EGBGB anzuwenden sind, nur weil die Normen eine am Verfahren beteiligte Partei zu bestimmten Handlungen oder Unterlassungen verpflichten.[490] Zur Umgehung dieses Problems haben jedoch zumindest der BGH und verschiedene Oberlandesgerichte schon auf den sog. „sachrechtlichen Ansatz"

[486] Einer Erhebung von 2007 nach, sollen im Bereich der Finanzdienstleistungen 70% der deutschen Unternehmen im Berichtszeitraum Opfer von Wirtschaftskriminalität gewesen sein, *PWC/Martin Luther Universität Halle-Wittenberg* (o. Fußn. 23), S. 14.

[487] Siehe Abschnitt 2.3.

[488] Siehe Abschnitte 2.1 und 2.2.

[489] *BAG*, Beschl. v. 22.07.2008 – 1 ABR 40/07, NZA 2008, 1248 (1254).

[490] Siehe hierzu *Heldrich*, in: *Palandt*, 68. Aufl., Art. 34 EGBGB Rn. 5; *Magnus,* in: *Staudinger*, Art. 34 EGBGB Rn. 113 ff; *Pfeiffer/Weller*, in: *Spindler/Schuster*, Recht der elektronischen Medien, Art. 34 EGBGB Rn. 2 ff.; mit den entsprechenden Nachweisen aus der Rechtsprechung *Fetsch*, Eingriffsnormen und EG-Vertrag, S. 18; *Mahnhold* (o. Fußn. 429), S. 742. Weiterhin steht zu erwarten, dass die Sonderanknüpfung ausländischer Eingriffsnormen bei der Auslegung vertraglicher Schuldverhältnisse durch die am 17.12.2009 in Kraft getretene Rom I-VO zukünftig eine wichtigere Rolle spielen wird. Die VO löst die bis zu diesem Zeitpunkt geltende EVÜ ab – und damit auch Art. 34 EGBGB – und enthält in ihrem Art. 9 erstmals eine konkrete Regelung zu Eingriffsnormen, siehe hierzu Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17. Juni 2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I) Verordnung v. 17.06.2008, ABlEU Nr. L 177 v. 04.07.2008, S. 6; *Thorn*, in: *Palandt*, 69. Aufl., (IPR) Rom I 9, Rn. 1, 11 ff.

zurückgegriffen, indem die Gerichte die ausländische Norm zwar nicht konkret angewandt, deren Auswirkungen jedoch als Faktum akzeptiert und in die Auslegung deutschen materiellen Rechts mit einfließen lassen haben.[491] Auf diese Weise können die Anforderungen des SOA ganz unproblematisch Einfluss auf die Beurteilung der berechtigten Interessen des Arbeitgebers an Kontrollmaßnahmen haben, so wie es für die deutschen Vorschriften[492] der Fall ist. Der Arbeitgeber hat bei unterlassenen Kontrollen also mit verschiedenen straf-, zivil- und arbeitsrechtlichen Haftungsfolgen zu rechnen.[493] Zur Grundlage für das berechtigte Interesse kommen die, durch verschiedene Studien belegte, hohe, mit der Größe des Unternehmens steigende, Wahrscheinlichkeit des Auftretens von Wirtschaftsdelikten[494] und die damit verbundenen Schäden und Folgeschäden hinzu. Der unmittelbare Schaden ergibt sich ganz konkret daraus, dass das Unternehmen im beschriebenen Szenario Geldmittel für eine Leistung aufwendet, die entweder gar nicht oder zumindest mit minderer Qualität erbracht wird, als dies nach einer objektiven und transparenten Auftragserteilung an einen „echten" Lieferanten der Fall gewesen wäre. Mittelbare Schäden entstehen durch Bußgelder die etwa von der SEC und anderen Behörden ausgesprochen werden, ferner im Zusammenhang mit dem Reputations- und dem damit verbundenen Vertrauensverlust[495] des Unternehmens, wenn der Missbrauch bekannt wird sowie mit den Kosten, die in die Aufdeckung der Tat investiert werden. Wegen der drohenden negativen Auswirkungen hat der Arbeitgeber vor dem Hintergrund der alljährlichen Überprüfung der Konzernrechnungslegung durch den Abschlussprüfer also ein gesteigertes, schützenswertes Interesse an einer Rechnungslegung ohne auf Missbrauch hindeutende Auffälligkeiten. Ein berechtigtes Interesse besteht ferner, da der von der erläuterten Analyse betroffene Bereich der Finanzbuchhaltung besonders anfällig für Missbrauch ist. Dies belegen im Rahmen des AFM durchgeführte Risikoanalysen sowie Fälle, in denen das Risiko sich bereits realisiert hat.[496] Auch die Art des mit der Analyse zu verhindern gesuchten Delikts gehört zu den mit Abstand am häufigsten auftretenden Formen von Wirtschaftsdelikten.[497] Insgesamt ist das berechtigte Interesse des Arbeitgebers an der Datenanalyse damit zu bejahen.

---

[491] *Mahnhold* a.a.O., S. 742 m.w.N.

[492] *BAG* (o. Fußn. 365), S. 1190; *Gola/Wronka* (o. Fußn. 38), Rn. 852.

[493] Die Strafrechtlichen Risiken ergeben sich insbesondere aus dem SOA, bei einem fehlenden oder grob fehlerhaften Risikomanagementsystem besteht ferner eine zivilrechtliche Binnenhaftung der Gesellschaft gegenüber und laut dem *LG Berlin* (o. Fußn. 72), S. 970 ein außerordentlicher Kündigungsgrund.

[494] Siehe Abschnitt 1.1.

[495] Dies betrifft zum einen die Kunden der Gesellschaft und zwar Geschäftskunden gleichermaßen wie Verbraucher, aber auch deren Anteilseigner, die sich bei einem öffentlich werden des Sachverhalts die Frage stellen müssen, ob sie sich nicht besser andernorts wirtschaftlich beteiligen. Sinkende Aktienkurse sind somit häufig die Folge.

[496] *KPMG,* 2010 (o. Fußn. 12), S. 9.

[497] Betrug, Untreue und Unterschlagung sind mit 41% die aktuell am meisten verbreiteten Fälle von Fraud, *PWC/Martin Luther Universität Halle-Wittenberg,* 2009 (o. Fußn. 4), S. 19.

Die **schutzwürdigen Interessen des Arbeitnehmers** stehen der Datenanalyse im konkreten Fall nicht entgegen. Zwar darf der Betroffene gemäß den von der Rechtsprechung entwickelten Grundsätzen prinzipiell selbst entscheiden, wer wann welche Daten über ihn zu welchen Zwecken verarbeitet. Dieses Recht findet seine Grenzen jedoch im berechtigten Interesse des Arbeitgebers. Dieser hat im beschriebenen Beispiel ein Verfahren gewählt, welches zwar einen Eingriff in das Persönlichkeitsrecht der Beschäftigten darstellt, dies jedoch mit einer möglichst geringen Intensität. Die vom BAG zur verdeckten Videoüberwachung aufgestellten Grundsätze sind erfüllt. Zunächst wurde der Kreis der Betroffenen größtmöglich eingegrenzt. Von einer ausufernden Analyse, wie sie die *Bahn AG* durchgeführt hat und welche jeden „Gleisarbeiter oder das Reinigungspersonal"[498] mit einbezog, kann keine Rede sein. Würde es sich um derartige flächendeckende Rasterfahndungen handeln, würde ein schützenswertes Interesse der Beschäftigten am Ausschluss der Maßnahme zu bejahen sein.[499] Eingriffe in die Intimsphäre und damit in den unantastbaren Kernbereich[500] des Persönlichkeitsrechts, sind ebenfalls auszuschließen. Diese Beurteilung basiert auf der im Zivilrecht entwickelten *Sphärentheorie*, auf welche im Rahmen der Verhältnismäßigkeitsprüfung zur Bestimmung der Intensität von Eingriffen in das APR zurückgegriffen werden kann.[501] Hiernach lassen sich Eingriffe mit steigender Intensität entweder der Sozial-, der Privat- oder der Intimsphäre zuordnen, wobei der Persönlichkeitsschutz im Arbeitsverhältnis in die Sozialsphäre fällt[502], welche den niedrigsten Schutz genießt. Im Anwendungsbereich der automatisierten Datenverarbeitung und damit des ISBR hat das BVerfG eine Anwendbarkeit der Theorie jedoch insoweit verneint[503], als es für den Schutz vor Datenverwendungen nicht darauf ankommen könne, welcher Sphäre die Daten zuzuordnen sind.[504] Hierzu führt das Gericht aus, dass durch die gegenwärtigen „Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten (…) ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen (kann); insoweit (gebe) es unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum mehr."[505] Trotz der im vorliegenden Fall fehlenden Anwendbarkeit der Sphärentheorie, liegt in der Verwendung der Kontodaten gleichwohl ein geringerer Eingriff in die Persön-

[498] *Kock/Franke* (o. Fußn. 400), S. 648.
[499] *Deutsch/Diller* (o. Fußn. 321), S. 1464.
[500] In diese Sphäre fallen etwa Tagebucheinträge oder Informationen über sexuelle Vorlieben des Betroffenen, *Lang*, in: BeckOK, GG, Art. 2 Rn. 40; jedoch können bei Vorliegen absolut außergewöhnlicher Umstände und zum Schutz elementarer Arbeitgeberinteressen selbst Eingriffe in diese Sphäre angemessen sein, *Wybitul*, BB 2010, 1085 (1088), *Schmidt,* in: Erfkomm (o. Fußn. 281), Art. 2 GG Rn. 63.
[501] *Dreier*, in: *Dreier* (o. Fuß. 376), Art. 2 I Rn. 60 f.; *Lang*, in: BeckOK a.a.O., Art. 2 Rn. 36aa, 37bb m.w.N.
[502] *Lang*, in: BeckOK a.a.O., Art. 2 Rn. 44.
[503] *BVerfGE* 65, 1 (o. Fußn. 254), S. 45.
[504] *Dreier*, in: *Dreier* (o. Fuß. 376), Art. 2 I Rn. 61.
[505] *BVerfGE* 65, 1 (o. Fußn. 254), S. 45

lichkeitsrechte der Beschäftigten vor, als dies etwa bei einer Nutzung von Krankendaten der Fall wäre. Schließlich bestehen die Kontonummer und die BLZ lediglich aus bis zu zehnstelligen Zahlenkombinationen und Zahlen stehen „im Zweifel mehr als alle anderen Datenformen für Anonymität, Neutralität und Sachlichkeit" (*Aßmus*).[506]

Ferner erhält der Arbeitgeber durch die Analyse keinerlei überschüssige, dem Zweck der Überprüfung nicht dienliche Informationen, da zum Beispiel keineswegs der Kontostand oder einzelne Kontobewegungen der Beschäftigten abgefragt werden.[507] Insoweit ist die Datenanalyse auch weitaus weniger eingriffsintensiv, als die vom BAG unter bestimmten Voraussetzungen als zulässig befundene heimliche Videoüberwachung, bei welcher sich etwa schnell Rückschlüsse auf das Verhalten der Beschäftigten ziehen lassen und ein genereller Überwachungs- und Anpassungsdruck besteht, da die Beschäftigten bei Kenntnis des Vorhandenseins der Videoanlage immer damit rechnen müssen, dass diese zur Zeit in Betrieb ist.[508] Auch ist die Beeinträchtigung der Betroffenen durch die Datenanalyse nur von kurzer Dauer, da der automatische Suchlauf, verglichen mit der sich im Extremfall über Wochen erstreckenden Videoüberwachung, bei entsprechender Leistungsfähigkeit der EDV abhängig von der Datenmenge zumeist innerhalb Sekunden oder Minuten geschieht. Wegen der Konzentration auf den Hochrisikobereich Finanzbuchhaltung und der hohen Wahrscheinlichkeit von Fällen, in denen sich das Risiko bereits realisiert hat, lässt sich ebenfalls vom Vorliegen eines zumindest räumlich und funktional begrenzten Verdachts sprechen, im Gegensatz zu einer wahllosen, allgemeinen Kontrolle.[509] Diesbezüglich ist noch zu erwähnen, dass das BAG die Ansicht vertritt, dass Kassendifferenzen bereits einen hinreichend konkreten Anlass für gezielte Überwachungsmaßnahmen liefern.[510] Nach dieser Auffassung können ebenfalls unerklärliche Differenzen in der Rechnungslegung die beschriebene Datenanalyse rechtfertigen. Schließlich wird dem Grundsatz der Datensparsamkeit Rechnung getragen. Durch die Verschlüsselung der Daten und die organisatorische Trennung von Analysten und demjenigen, der die Daten verschlüsselt, ist nach der hier vertretenen Auffassung zumindest eine pseudonyme Datenverwendung gewährleistet.[511] Auch eine eventuelle Verletzung anderer datenschutzrechtlicher Prinzipien, wie dem Grundsatz der Direkterhebung[512] oder der Transparenz[513], ist nicht ersichtlich.

Alle genannten, die Analyse rechtfertigenden Gründe, sind vom Arbeitgeber jedoch sorgfältig zu dokumentieren.

---

[506] *Aßmus* (o. Fußn. 138), S. 603.
[507] Hinweis schon bei *Diller* (o. Fußn. 402), S. 440.
[508] *BAG* (o. Fußn. 365), S. 1191.
[509] *BAG* (o. Fußn. 342), S. 1195.
[510] *BAG* a.a.O., S. 1194.
[511] So auch *Bierekoven* (o. Fußn. 466), S. 207.
[512] Für die vorliegende Analyse wurden keine neuen Daten erhoben.
[513] Siehe zu den Grundsätzen des Datenschutzrechts Abschnitt 3.3.

ii. Würdigung des Urteils vom ArbG Berlin zur Massendatenanalyse der Bahn AG

In dem Urteil hat das ArbG Berlin[514] über eine Klage der Compliance-Beauftragten der *Bahn AG* entschieden, in welcher sie sich gegen ihre Kündigung im Zusammenhang mit den durchgeführten Massendatenanalysen gewendet hat. Der Konzern wirft der Klägerin im Wesentlichen vor, dass sie unter Verletzung von Datenschutzbestimmungen und anderen rechtlichen Vorgaben, unzulässige Maßnahmen zur Überwachung der Mitarbeiter angeordnet habe.[515] Zunächst bejaht das Gericht vor dem Hintergrund der Forderungen nach effektiver Compliance vonseiten der Anteilseigner der Unternehmen, des Gesetzgebers, des Steuerfahnders, des Wirtschaftsprüfers und der Finanzverwaltungen allgemein, der Vertragspartner etc.[516] die prinzipielle Notwendigkeit von Maßnahmen zur Bekämpfung von Korruption und anderen Wirtschaftsdelikten. Daraufhin konstatiert es die in diesem Zusammenhang oftmalige Erforderlichkeit der Verwendung personenbezogener Beschäftigtendaten, etwa im Rahmen des Abgleichs von Kontodaten und Wohnanschriften der Angestellten mit den entsprechenden Daten der Lieferanten, da es einem gängigen Muster entspräche, dass Mitarbeiter Scheingeschäfte über Verwandte abwickeln.[517] Eine solche, dem BDSG unterliegende Datennutzung sei rechtmäßig, wenn ein Rechtfertigungsgrund vorliege.[518]

Die Verwendung der Daten zur Erfüllung eigener Geschäftszwecke hatte gemäß § 28 Abs. 1 Nr. 2 BDSG a.F. zur Wahrung der berechtigten Interessen des Arbeitgebers erforderlich zu sein und es durfte kein Grund zu der Annahme bestehen, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Datenverwendung überwiegt. Das berechtigte Interesse bejaht das Gericht aufgrund der genannten Forderungen nach Compliance, wegen des potentiellen, durch Wirtschaftsdelikte verursachten Schadens sowie der möglichen Folgeschäden und gegebenenfalls noch infolge von Risikoanalysen, die belegen, dass das Unternehmen für das in Frage stehende Korruptionsmuster besonders anfällig ist, bzw. aufgrund von Fällen, in welchen dieses Risiko sich bereits realisiert hat.[519] Davon abgesehen, dürften zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäftigten erhoben, verarbeitet oder genutzt werden, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und

[514] *ArbG Berlin* (o. Fußn. 20).
[515] *ArbG Berlin* a.a.O., Abs.-Nr. 15.
[516] *ArbG Berlin* a.a.O., Abs.-Nr. 17.
[517] *ArbG Berlin* a.a.O., Abs.-Nr. 18.
[518] *ArbG Berlin* a.a.O., Abs.-Nr. 20.
[519] *ArbG Berlin* a.a.O., Abs.-Nr. 21 f.

Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Das Gericht erläutert, dass dieser Wortlaut zwar dem neuen § 32 BDSG entstamme, dass diese Maßstäbe allerdings schon zur damaligen Rechtslage galten, da „(d)urch die BDSG-Reform doch nur positiviert (wurde), was bereits immer schon geltendes Recht war."[520] Daraus folge wiederum, dass zur Aufdeckung von Straftaten durchaus Beschäftigtendaten auf die beschriebene Weise verwendet werden dürften und die beklagte *Bahn AG* es zumindest versäumt habe, darzulegen, wieso die Datenverwendung im konkreten Fall unzulässig gewesen sein sollte.[521]

Mit dem Hinweis auf die vom Gesetzgeber nicht gewollte Veränderung der Rechtslage, äußert sich das Gericht auch zu dem in der Literatur geführten Streit über die Auslegung von § 32 BDSG. Zwar ist das Urteil wegen der bevorstehenden Berufung[522] vor dem Landesarbeitsgericht noch nicht rechtskräftig. Selbst wenn das Berufungsgericht unter Berücksichtigung weiterer Ausführungen der *Bahn AG* eine Unzulässigkeit der erfolgten Datenanalysen feststellen sollte, ist jedoch zu beachten, dass die *Bahn AG* in den Jahren 2002 und 2003 rund 173.000 und im Jahre 2005 220.000 ihrer 237.000 Mitarbeiterstammdaten mit denen ihrer 80.000 Lieferanten verdachtsunabhängig abgeglichen hat.[523] Diese Zahlen mögen für eine Unverhältnismäßigkeit der konkreten Maßnahme sprechen, da keinerlei Eingrenzung des Betroffenenkreises oder auch nur Pseudonymisierungen vorgenommen wurden. Daraus ließen sich aber keine Rückschlüsse über die Zulässigkeit einer mit Bedacht entwickelten, die Persönlichkeitsrechte der Arbeitnehmer in möglichst geringer Art und Weise verletzenden, Datenanalyse ziehen. Daneben erlaubt das Urteil des ArbG Berlin die Einschätzung, dass die deutschen Gerichte bei der datenschutzrechtlichen Beurteilung von Datenanalysemaßnahmen im Rahmen der Prüfung von § 32 BDSG auch den Willen des Gesetzgebers berücksichtigen werden, der eine Änderung der Rechtslage nicht beabsichtigte,[524] womit präventive Datenanalysen gemäß der alten Rechtslage unter Beachtung der Verhältnismäßigkeit zulässig sind.

Die Entscheidung kann zwar nicht dahingehend herangezogen werden, dass sämtliche Datenanalyse-Maßnahmen zur Missbrauchsbekämpfung datenschutzrechtlich zulässig sind, weil hier lediglich die Ansicht dreier Einzelrichter wiedergegeben wird und auf die Details der konkreten Maßnahme mangels entsprechendem Beklagtenvortrag nicht eingegangen werden konnte. Da die Berufungsinstanz sowie Beurteilungen der Sachlage durch andere Gerichte, noch ausstehen, kann das Urteil insofern nur als Orientierungshilfe oder bestenfalls als Indiz für eine sich in Zukunft noch zu festigende Ansicht zu werten

[520] *ArbG Berlin* a.a.O., Abs.-Nr. 23.
[521] *ArbG Berlin* a.a.O., Abs.-Nr. 23.
[522] http://www.sueddeutsche.de/wirtschaft/59/505261/text/ (Stand: 18.04.2010).
[523] *Kock/Franke* (o. Fußn. 400), S. 648.
[524] Siehe Abschnitt 3.4.3.

sein. Es kann allerdings ebenfalls nicht dahingehend herangezogen werden, dass die entsprechenden Kontrollmaßnahmen einzustellen sind.

iii. Würdigung der Vorgaben aus der jüngeren Rechtsprechung des BVerfG

Zu der Einschätzung, dass die beschriebene Datenanalyse einen zulässigen Eingriff in die Persönlichkeitsrechte der Beschäftigten darstellt, gelangt man auch, wenn man die Entscheidungen des BVerfG jüngeren Datums mit inhaltlichen Parallelen berücksichtigt. Zwar bezieht sich die im Folgenden dargestellte Rechtsprechung auf staatliche Datenerhebungen und -nutzungen, womit sich die aufgestellten Grundsätze, wegen des im Arbeitsverhältnis andersartigen Über- und Unterordnungsverhältnisses, nicht in jeder Beziehung auf die vorliegenden Untersuchungen beziehen lassen. Allerdings gibt das BVerfG eine Reihe wichtiger Hinweise, die für die Frage der Zulässigkeit arbeitgeberseitiger Maßnahmen hilfreich sein können.

Der Beschluss zur präventiven polizeilichen Rasterfahndung aus dem Jahre 2006[525] hat zunächst hohe Hürden für die in Frage stehende Ermittlungsmaßnahme aufgestellt. Als Voraussetzung für die Zulässigkeit präventiver Rasterfahndungen sah das Gericht eine allgemeine Gefährdungslage, wie sie etwa nach den Anschlägen vom 11. September 2001 bestand, als nicht ausreichend an und verlangte vielmehr das Vorliegen weiterer Tatsachen,[526] aus denen sich eine konkrete Gefahr für hochrangige Rechtsgüter wie den Bestand des Bundes oder für Leib, Leben und Freiheit einer Person ergeben.[527] Allerdings handelte es sich bei den durchgeführten Ermittlungen auch um äußerst intensive Eingriffe in das ISBR der Betroffenen. Im Rahmen der dem Beschluss zugrunde liegenden Rasterfahndung ließen sich die Polizeibehörden personenbezogene Daten von öffentlichen und nicht öffentlichen Stellen übermitteln. Die dadurch gewonnenen „Massendaten" wurden per Datenanalyse abgeglichen, mit dem Ziel an eine Schnittmenge von Personen zu gelangen, auf welche bestimmte, vorher festgelegte Merkmale zutrafen.[528] Im Fokus standen insbesondere die Merkmale Student oder ehemaliger Student eines bestimmten Alters, islamische Religionszugehörigkeit, Geburtsland oder Nationalität.[529] Zusammen mit anderen Abgleichsdaten, wie etwa Inhaberschaften von Fluglizenzen, sollen im Laufe der Maßnahme die Daten zu zwischen 200.000 und 300.000 Personen gesammelt worden sein.[530] All dies geschah in verdeckter Form. Beurteilt man die hohe Intensität des Eingriffs, die sich aus dem Ausmaß der Datensammlung sowie aus der Art der gesammelten Daten ergibt, vor dem Hintergrund der Rechtsgüter, die mit der Maßnahme geschützt wer-

[525] *BVerfG*, Beschl. v. 04.04.2006 - 1 BvR 518/02, BVerfGE 115, 320 (Rasterfahndung II).
[526] *BVerfG* a.a.O., S. 364 f., Rn. 147.
[527] *BVerfG* a.a.O., S. 346, Rn. 91.
[528] *BVerfG* a.a.O., S. 321, Rn. 2.
[529] *BVerfG* a.a.O., S. 323, Rn. 8.
[530] *BVerfG* a.a.O., S. 324, Rn. 9.

den sollten, so erscheinen die Anforderungen des Gerichts zwar streng, aber gerechtfertigt. Verschärfend kommt hinzu, dass die dem Beschluss zugrunde liegende „Sammelwut" staatlicher Stellen daran erinnert, dass das BVerfG das ISBR gerade aus der Motivation heraus entwickelt hat, diesem staatlichen Handeln Einhalt zu gebieten.[531] Für die vorliegende, in Abschnitt 4.2.1 beschriebene Maßnahme stellt der Beschluss indessen dieselben Regeln auf, die bereits durch die behandelten Entscheidungen des BAG bekannt sind. Nach den Ausführungen des Gerichts hinge die Zulässigkeit einer Ermittlungsmaßnahme insgesamt davon ab, wie viele Grundrechtsträger Beeinträchtigungen welcher Intensität ausgesetzt sind und ob etwa die betroffenen Personen Anlass zu der Maßnahme gegeben haben.[532] Für die Beurteilung der individuellen Beeinträchtigung sei maßgeblich, ob der Betroffene anonym bleibt, welche Informationen über ihn gewonnen werden – wobei auch Verknüpfungsmöglichkeiten mit anderen Daten berücksichtigt werden müssten – und welche Konsequenzen die Maßnahme für ihn haben könnte.[533] Hier kann auf das oben Gesagte verwiesen werden, wonach bei dem geschilderten Abgleich der Personal- und Lieferantendaten eine hinreichende Eingrenzung des Kreises der von der Analyse Betroffenen vollzogen wurde, keinerlei überschüssige Informationen gewonnen werden und mit pseudonymisierten Daten gearbeitet wurde. In der Verwendung von Kontodaten ist weiterhin kein derart intensiver Grundrechtseingriff zu erblicken, wie in der Nutzung von den speziell schützenswerten besonderen Arten von personenbezogenen Daten, etwa der Religionszugehörigkeit. Auch die drohenden Konsequenzen stehen in keinem Verhältnis: Die Bezichtigung als Terrorist mit den aus den Medien bekannten Folgen der Denunziation sowie den undurchsichtigen, monatelangen Verhören unter Ausschluss der Öffentlichkeit, greift weitaus stärker in die Rechte der Betroffenen ein, als die Reaktion auf Verdachtsfälle einer vorgetäuschten Lieferanteneigenschaft im Unternehmen. Ferner sei das ISBR verletzt, wenn der Einzelne nicht mit hinreichender Sicherheit überschauen könne, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind und er das Wissen möglicher Kommunikationspartner nicht einigermaßen abschätzen könne.[534] Diese Gefahr besteht vorliegend in keiner Weise, da keine Übermittlung der Daten des Betroffenen an dritte Stellen stattfindet, sondern der Arbeitgeber lediglich die bereits vorliegenden, beim Arbeitnehmer erhobenen Daten nutzt.[535] Im Ergebnis stellt sich lediglich die Frage, ob die Betroffenen vorliegend Anlass zu der Maßnahme gegeben haben. Hier kann nur auf Risikoanalysen und Fälle verwiesen wer-

[531] *BVerfGE* 65, 1 (o. Fußn. 254).
[532] *BVerfGE* 115, 320 (o. Fußn. 525), S. 346, Rn. 94.
[533] *BVerfG* a.a.O., S. 346, Rn. 94.
[534] *BVerfG* a.a.O., S. 342, Rn. 69.
[535] Ob er die Daten für andere Zwecke, als ursprünglich bei der Erhebung angegeben nutzen darf, ist dagegen durch die Verhältnismäßigkeitsprüfung im Rahmen von § 32 Abs. 1 BDSG zu klären.

den, in welchen sich das Risiko bereits realisiert hat. Sind derartige Fälle dokumentiert, haben zumindest Mitarbeiter gleichen Ranges den Anlass geliefert. Schließlich findet sich in dem Beschluss der Hinweis darauf, dass die Heimlichkeit der Maßnahme ihre Intensität erhöht.[536] Auf die Heimlichkeit kommt es für die vorliegende Datenanalyse jedoch gar nicht an, da diese Maßnahme über eine Betriebsvereinbarung bereits angekündigt wurde.

Daneben wurde der Aspekt der Heimlichkeit von Aufdeckungsmaßnahmen in einem Beschluss aus dem Jahre 2009[537] zur Abfrage von Kreditkartendaten im strafrechtlichen Ermittlungsverfahren weiter konkretisiert. Hier erkennt das Gericht an, dass manche Maßnahmen nur verdeckt zum Erfolg führen können, womit sich auch aus der Heimlichkeit einer Datenanalyse nicht automatisch deren Unzulässigkeit ergebe.[538] Dieser Beschluss ist für die vorliegende Arbeit von besonders großer Bedeutung. Im zugrunde liegenden Sachverhalt hatte eine Staatsanwaltschaft, mit dem Ziel der Identifizierung von Nutzern kinderpornographischer Angebote, ein Kreditinstitut dazu veranlasst, den eigenen Kundenstamm an Kreditkartenbesitzern nach Zahlungsanweisungen innerhalb eines bestimmten Zeitraumes, mit einem bestimmten Betrag, auf ein bestimmtes philippinisches Konto zu durchsuchen. Lediglich die Treffer wurden an die Staatsanwaltschaft übermittelt. Das BVerfG sah diesen Vorgang nicht nur als zulässig an, es verneinte darüber hinaus einen Eingriff in das ISBR derjenigen Kreditkarteninhaber, die zwar Teil der Analyse waren, deren Daten mangels einer Übereinstimmung mit den Suchparametern jedoch nicht an die Behörde übermittelt wurden.[539] Für die Annahme eines Eingriffs genüge es nicht, „dass die Daten bei den Unternehmen in einen maschinellen Suchlauf mit eingestellt wurden, da ihre Daten anonym und spurenlos aus diesem Suchlauf ausgeschieden wurden und nicht im Zusammenhang mit dieser Ermittlungsmaßnahme behördlich zur Kenntnis genommen wurden".[540] Durch die genaue Eingrenzung der Suchparameter, könne weiterhin mit hinreichender Wahrscheinlichkeit sichergestellt werden, dass es sich bei den übermittelten Personen um Straftäter handelt.[541] Daneben nennt das Gericht als maßgebliche Faktoren für die Beurteilung der Eingriffsintensität die Verdachtslosigkeit einer Maßnahme sowie die große Streubreite in Bezug auf den überprüften Personenkreis und verneint im vorliegenden Falle beides.[542] Die aufgestellten Grundsätze lassen sich materiell problemlos auf den Abgleich der Mitarbeiter- und Lieferantendaten im Rahmen des IKS übertragen.

---

[536] *BVerfGE* 115, 320 (o. Fußn. 525), S. 352, Rn. 113.
[537] *BVerfG*, Beschl. v. 17.02.2009 - 2 BvR 1372, 1745/07, http://www.bundesverfassungsgericht.de/entscheidungen/rk20090217_2bvr137207.html (Stand: 23.05.2010).
[538] *BVerfG*, a.a.O. Abs.-Nr. 28.
[539] *BVerfG,* a.a.O. Abs.-Nr. 19 m.w.N.
[540] *BVerfG,* a.a.O. Abs.-Nr. 19 m.w.N
[541] *BVerfG,* a.a.O. Abs.-Nr. 14 m.w.N.
[542] *BVerfG,* a.a.O. Abs.-Nr. 29 m.w.N

Demnach läge bei denjenigen, von der Analyse betroffenen Beschäftigten, die keinen Treffer erzeugen, nicht einmal ein Eingriff in das ISBR vor, da auch deren Daten „anonym und spurenlos" aus dem Suchlauf ausscheiden. Die Streubreite der Maßnahme ist ebenfalls gering, da von allen für das Unternehmen tätigen Personen lediglich die Beschäftigten im Bereich der Finanzbuchhaltung betroffenen sind und von jenen Personen wiederum nur diejenigen, die über eine Bestellberichtigung verfügen.[543] Damit sind die Suchparameter auch hinreichend konkret, so dass sich, wegen der geringen Wahrscheinlichkeit der parallelen Arbeitnehmer- und Lieferanteneigenschaft der durch die Analyse aufgedeckten Mitarbeiter, bei diesen Personen ebenfalls von einer hinreichenden Wahrscheinlichkeit des Vorliegens einer Straftat sprechen lässt. Nun ließe sich argumentieren, dass die Interessenlage, die dem Beschluss zugrunde lag, eine andere war. Dort war das übergeordnete Ziel die Bekämpfung von Kinderpornographie, vorliegend ist das Ziel die Sicherung des Fortbestands des Unternehmens und die Vermeidung von finanziellen Schäden. Jedoch sind auch die möglichen Konsequenzen im Rahmen von Ermittlungen zur Bekämpfung von Kinderpornographie weitaus tiefgreifender.[544] Daher wäre der weniger intensive Kontodatenabgleich bei analoger Anwendung des Beschlusses zulässig.

Die strengen Anforderungen, die das BVerfG an die Zulässigkeit von heimlichen Online-Durchsuchungen durch die Strafverfolgungsbehörden gestellt hat, sind für die in Abschnitt 4.2 beschriebene Maßnahme hingegen nicht relevant. In dem Urteil von 2008[545] hat das Gericht aus Art. 1 Abs. 1 GG i.V.m. Art. 2 Abs. 1 GG das Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme abgeleitet. Die vom BVerfG grundsätzlich unter den Richtervorbehalt gestellte heimliche Infiltration etwa eines Personalcomputers stellt vor dem Hintergrund der vermehrten Nutzung elektronischer oder digitaler Kommunikationsmittel und deren Vordringen in nahezu alle Lebensbereiche[546] unbestritten einen besonders intensiven Eingriff in die Persönlichkeitsrechte des Betroffenen dar. Der Abgleich der Kontodaten von Mitarbeitern und Lieferanten ergibt demgegenüber lediglich eine einzige zutreffende Aussage: Nämlich die gleichzeitige Eigenschaft- oder Nichteigenschaft der Mitarbeiter als Lieferanten. Keineswegs ist damit der Zugriff auf informationstechnische Systeme der Beschäftigten verbunden. Dies wäre erst der Fall, wenn im Rahmen der Missbrauchsbekämpfung tatsächlich auf die Computer der Angestellten zugegriffen würde und nicht lediglich auf deren Kontodaten, die auf einem vom Mitarbeitercomputer phy-

[543] Und auch dieser Personenkreis kann, wie dargestellt, noch weiter auf Bestellberechtigte mit erheblichen Wertgrenzen beschränkt werden.
[544] *BVerfGE* 115, 320 (o. Fußn. 525), S. 346, Rn. 94
[545] *BVerfG*, Urt. v. 27.02.2008 – 1 BvR 370/07 und 1 BvR 595/0, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html (Stand: 20.04.2010).
[546] *BVerfG* a.a.O., Abs.-Nr. 220.

sisch getrennten Server in einer zentralen Datei gespeichert vorliegen. Das dem Urteil zugrunde liegende Ausspähen der Festplatte des Computers einer Person sowie das Mitverfolgen von deren Onlineaktivitäten, ermöglicht hingegen die Erstellung umfassender Persönlichkeitsprofile und ist unter datenschutz- und vor allem verfassungsrechtlichen Gesichtspunkten prinzipiell unzulässig und kann nur bei Vorliegen einer konkreten Gefahr für ein überragend wichtiges Rechtsgut und nur ausnahmsweise statthaft sein.

Schließlich bietet auch das lang erwartete Urteil zur Vorratsdatenspeichung vom 2. März 2010[547] wenig Neues für die Beurteilung der vorliegenden Datenanalyse. Lediglich die vom Gericht aufgestellten Anforderungen an eine zukünftige gesetzliche Regelung zur Datenspeicherung auf Vorrat können hilfreich sein. Diese hat dem Grundsatz der Transparenz Rechnung zu tragen[548] sowie eine ausreichende Datensicherheit[549] und einen effektiven Rechtsschutz zu gewährleisten.[550] Transparenz und Rechtsschutz wird vorliegend durch die abgeschlossene Betriebsvereinbarung sichergestellt. Das Erfordernis der Datensicherheit gehört daneben zu den Grundprinzipien des BDSG und sollte bereits im Zusammenhang mit den nach § 9 BDSG zu treffenden technischen und organisatorischen Maßnahmen erfüllt sein. Für präventive Zugriffe auf die Daten werden Anhaltspunkte für konkrete Gefahren eines überragend wichtigen Rechtsguts gefordert,[551] insoweit kann auf die Ausführungen am Anfang dieses Abschnitts zum Beschluss über die Rasterfahndungen verwiesen werden.[552]

Zusammenfassend lässt sich sagen, dass der Abgleich der Mitarbeiter- und Lieferantenkontodaten in der beschriebenen Form auch unter Berücksichtigung der neueren Rechtsprechung des BVerfG angemessen ist.

iv. Würdigung der Vorgaben des europäischen Gemeinschaftsrechts

In ihrer Stellungnahme zum Datenschutz im Beschäftigungsverhältnis stellt die Artikel 29-Datenschutzgruppe auch einige Regeln über den Umgang mit personenbezogenen Beschäftigtendaten zur Überwachung und Kontrolle auf.[553] Diese nachfolgend dargestellten Grundsätze haben, wegen der rein beratenden Funktion der Artikel 29-Datenschutzgruppe,[554] zwar keinerlei bindende

---

[547] *BVerfG*, Urt. v. 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08 und 1 BvR 586/08, http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html (Stand: 20.04.2010).
[548] *BVerfG* a.a.O., Abs.-Nr. 242.
[549] *BVerfG* a.a.O., Abs.-Nr. 220.
[550] *BVerfG* a.a.O., Abs.-Nr. 239.
[551] *BVerfG* a.a.O., Abs.-Nr. 231.
[552] Für bereits begangene Straftaten reicht ein durch bestimmte Tatsachen begründeter Verdacht einer schweren Straftat, wobei dem Gesetzgeber bei der Beurteilung des Vorliegens einer „schweren Straftat" ein weiträumiger Beurteilungsspielraum zusteht, *BVerfG* a.a.O., Abs.-Nr. 228.
[553] *Artikel 29-Datenschutzgruppe* (o. Fußn. 275), S. 29 f.
[554] *Artikel 29-Datenschutzgruppe* a.a.O., S. 1.

Wirkung, jedoch können sie als Orientierungshilfen herangezogen werden, um die Zulässigkeit arbeitgeberseitiger Handlungen einzuschätzen.

> „Jede Überwachung muss, um den Anforderungen von Artikel 6 zu genügen, und insbesondere, wenn sie sich auf Artikel 7 Buchstabe f der Richtlinie 95/46/EG stützt, eine angemessene Reaktion eines Arbeitgebers auf die Risiken sein, mit denen er konfrontiert ist, wobei der legitime Anspruch auf Schutz der Privatsphäre und andere Interessen der Beschäftigten zu berücksichtigen sind."[555]

Der genannte Art. 7 Lit. f) der Richtlinie[556] erlaubt Datenverarbeitungen, die zur Wahrung des berechtigten Interesses der verantwortlichen Stelle erforderlich sind und welchen keine überwiegenden, schutzwürdigen Interessen des Betroffenen entgegenstehen. Maßgeblich für die Beurteilung der Zulässigkeit von Kontrollen ist also erneut eine Interessenabwägung. Die hohe Wahrscheinlichkeit von Missbrauchsfällen im Bereich der Finanz- und Rechnungslegung sowie der drohende Verstoß gegen gesetzliche Compliance-Pflichten, wenn keine geeigneten Maßnahmen zur Verhinderung von Fraud ergriffen wurden, stellen ein erhebliches Risiko dar. Die beschriebene, in ihrer Eingriffsintensität möglichst gering gehaltene, Datenanalyse zur Verhinderung solcher Fälle, stellt auch eine demgegenüber angemessene Reaktion dar. Ebenfalls sind die Interessen der Beschäftigten berücksichtigt worden, da nur eine sehr geringe Zahl der Belegschaft tatsächlich betroffen ist und der Abgleich einer Kontonummer überdies einen vergleichsweise geringen Eingriff in die Persönlichkeitsrechte des Einzelnen darstellt.

> „Alle personenbezogenen Daten, die im Laufe der Überwachung vorgehalten oder verwendet werden, müssen den Zwecken der Kontrolle entsprechen und dafür erheblich sein und dürfen nicht darüber hinaus gehen. Jede Überwachung muss so ausgeführt werden, dass das Eindringen in die Privatsphäre auf ein Mindestmaß beschränkt wird. Sie muss auf den Risikobereich ausgerichtet sein und unter Beachtung der Datenschutzvorschriften (…) erfolgen."[557]

Auch die hier aufgestellten Kriterien sind erfüllt. Die Nutzung der Konto- und Personalnummern der Beschäftigten ist vollkommen auf den Risikobereich ausgerichtet und zur Erreichung des angestrebten Zweckes unerlässlich.[558] Weiterhin greift die Maßnahme so gering wie möglich in die Rechte der Betroffenen ein und auch den einschlägigen Datenschutzvorschriften, also § 32 BDSG oder etwa den allgemeinen Grundsätze des Datenschutzrechts, wurde zur Genüge Rechnung getragen.

> „Eine Überwachung (…) muss den Transparenzanforderungen von Artikel 10 genügen. Die Beschäftigten müssen über die Existenz der Überwachungsmaßnahmen informiert werden und über die Zwecke, für die personenbezo-

[555] *Artikel 29-Datenschutzgruppe* a.a.O., S. 29.
[556] Richtlinie 95/46/EG (o. Fußn. 240).
[557] *Artikel 29-Datenschutzgruppe* (o. Fußn. 275), S. 30.
[558] Siehe Abschnitt 4.2.2.2.2.

> gene Daten verarbeitet werden, und sie müssen darüber hinaus die Informationen erhalten, die erforderlich sind, um eine Verarbeitung nach Treu und Glauben zu garantieren."[559]

Art. 10, genau wie seine deutsche Umsetzung im Rahmen des § 4 Abs. 3 BDSG, sieht eine Informationspflicht zum Zeitpunkt der Erhebung eines Datums vor. Vorliegend werden jedoch keine neuen Daten erhoben. Dennoch wird durch die abzuschließende Betriebsvereinbarung sichergestellt, dass die Betroffenen Kenntnis von der geplanten Maßnahme und den dafür verwendeten Daten erhalten, womit insgesamt die Transparenz gewahrt ist.

Daneben existiert eine weitere Stellungnahme der Artikel 29-Datenschutzgruppe, welche sich speziell mit der Konfliktlage zwischen Corporate Governance- und Compliance-Anforderungen und den europäischen Datenschutzbestimmungen befasst.[560] Hintergrund sind die von sec. 806 SOA verlangten Maßnahmen zum Schutz von sog. *Whistleblowern*, also Mitarbeitern, die auf Wirtschaftsdelikte hindeutende Auffälligkeiten melden. Die damit zusammenhängende Möglichkeit der anonymen Anschuldigungen von Arbeitskollegen ist mit dem europäischen Datenschutzgrundsatz der Transparenz grundsätzlich nicht vereinbar. Im Ergebnis erkennt die Arbeitsgruppe jedoch an, dass ein solches Meldesystem die Unternehmensführung „insbesondere in Bezug auf Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung und Vorschriften über die Bekämpfung von Korruption und Banken- und Finanzkriminalität und Strafrecht" erheblich unterstützen könne.[561] Die Umsetzung des Systems müsse allerdings im Einklang mit der Datenschutzrichtlinie[562] geschehen, d.h. den Schutz der personenbezogenen Daten des Hinweisgebers und auch der beschuldigten Person gewährleisten.[563] Im Vordergrund stünden dabei die Rechte der beschuldigten Person auf Mitteilung, Zugang, Berichtigung und Löschung der Daten. Auch diesbezüglich erkennt die Gruppe an, dass jene Rechte in Einzelfällen und nach einer Abwägung der entgegenstehenden Interessen, beschränkt werden könnten, „um ein Gleichgewicht zwischen dem Recht auf Schutz der Privatsphäre und den Interessen des Systems herzustellen," solange die Beschränkungen restriktiv gehandhabt würden und lediglich dann gälten, wenn sie für die Erreichung des verfolgten Ziels erforderlich sind.[564]

Bei der vorliegenden Datenanalyse stehen sich, verglichen mit der Stellungnahme, die identischen berechtigten Interessen der Daten verarbeitenden Stel-

---

[559] *Artikel 29-Datenschutzgruppe* (o. Fußn. 275), S. 30.
[560] *Artikel 29-Datenschutzgruppe*, Stellungnahme 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität.
[561] *Artikel 29-Datenschutzgruppe* a.a.O., S. 19 f.
[562] Richtlinie 95/46/EG (o. Fußn. 240).
[563] *Artikel 29-Datenschutzgruppe* (o. Fußn. 560), S. 20.
[564] *Artikel 29-Datenschutzgruppe*, a.a.O. S. 20.

le und fast deckungsgleiche schutzwürdige Bedürfnisse des Betroffenen gegenüber. Die Artikel 29-Datenschutzgruppe verlangt also nicht mehr, als dass mit der Analyse verbundene Beeinträchtigungen der Betroffenenrechte erforderlich sind und der Vorgang so transparent wie möglich gestaltet wird, damit sich die Eingriffsintensität auf ein Minimum reduziert. Dass diese Forderungen hinreichend berücksichtigt wurden, ist bereits ausführlich erläutert worden.[565]

Nach einer Abwägung der Interessen von Arbeitgeber und Arbeitnehmer und der Würdigung des Urteils des ArbG Berlin, der einschlägigen Judikate des BVerfG sowie der Vorgaben des europäischen Gemeinschaftsrechts, gelangt man zu dem Ergebnis, dass der Mitarbeiter-Lieferanten-Abgleich auch angemessen i.e.S. und damit insgesamt verhältnismäßig gemäß § 32 Abs. 1 Satz 1 BDSG ist.

4.2.3
Rechte der Arbeitnehmervertretung

Ferner ist zu beachten, dass dem Betriebsrat hinsichtlich der Einführung und Anwendung der Datenanalysesoftware ein Mitbestimmungsrecht zusteht. Dies ergibt sich aus § 87 Abs. 1 Nr. 6 BetrVG, wonach die „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen" mitbestimmungspflichtig sind.[566] Nach h.M. fällt hierunter auch allgemein eine Datenauswertung[567], bei welcher verhaltensbezogene Daten „sortiert, zusammengestellt oder miteinander in Beziehung gesetzt" *(Kania)* werden, um Rückschlüsse auf das Verhalten der Beschäftigten ziehen zu können.[568] Bei dem zur Analyse verwendeten EDV-Programm handelt es sich zunächst um eine technische Einrichtung.[569] Diese ist weiterhin offensichtlich dazu bestimmt, die Arbeitnehmer zu überwachen, so dass es nicht einmal auf die nach h.M. von der Norm lediglich geforderte objektive Geeignetheit zur Überwachung ankommt.[570] Im

[565] Die weiteren Ausführungen der Stellungnahme sind eher für Datenverwendungen im Rahmen der Aufdeckung bereits begangener Straftaten relevant und finden im entsprechenden Abschnitt 4.3. der vorliegenden Arbeit Erwähnung.

[566] Da § 87 Abs. 1 Nr. 6 BetrVG nach überwiegender Meinung einschlägig ist, kommt es auf die in der Literatur diskutierte zusätzliche Anwendbarkeit von Nr. 1 der Norm insoweit nicht an, als dies keine zusätzlichen Rechte des Betriebsrats auslösen würde, siehe zur Diskussion *Diller* (o. Fußn. 402), S. 438; *Kock/Franke* (o. Fußn. 400), S. 649; *Steinkühler* (o. Fußn. 481), S. 1294.

[567] Laut dem BAG ergibt sich bereits aus der reinen Möglichkeit zur Datenauswertung ein Mitbestimmungsrecht, siehe *BAG*, Beschl. v. 14.09.1984 - 1 ABR 23/82, NJW 1985, 450.

[568] *Gola/Wronka* (o. Fußn. 38), Rn. 1773; *Kania,* in: Erfkomm (o. Fußn. 281), § 87 BetrVG Rn. 49 m.w.N; *Steinkühler* a.a.O., S. 1294.

[569] Jeweils m.w.N. zur Rechtsprechung *Gola/Wronka* a.a.O., Rn. 1770; *Kania,* in: Erfkomm a.a.O., § 87 BetrVG Rn. 62; *Kock/Franke* (o. Fußn. 400), S. 649; *Richardi*, in: *Richardi* (Hrsg.), BetrVG, § 87 Rn. 495; *Steinkühler* a.a.O., S. 1294; *Werner,* in: *Rolfs/Giesen/Kreikebohm (*o Fußn 277), § 87 Rn. 95; a.A. *Diller* (o. Fußn. 402), S. 438.

[570] Siehe hierzu *Blomeyer,* in: *Richardi/Wlotzke* (o. Fußn. 281),§ 99 Rn. 95; *Kania,* in: Erfkomm a.a.O., § 87 BetrVG Rn. 55; *Richardi*, in: *Richardi* a.a.O., § 87 Rn. 501; *Werner,* in: *Rolfs/Giesen/Kreikebohm* a.a.O., § 87 Rn. 92.

Fokus der Überwachung liegt überdies das Verhalten der Beschäftigten. Hierunter wird jedes vom Arbeitnehmer individuell gesteuerte Tun oder Unterlassen verstanden.[571] Daher enthält die mit der Datenanalyse gewonnene Information, ob ein Mitarbeiter Scheingeschäfte tätigt, eine Aussage über dessen vorliegend rechtswidrige Handlungen und damit auch sein Verhalten.[572] Selbst wenn man davon ausginge, dass die gewonnene Information alleine noch keine definitiven Rückschlüsse auf das Verhalten zuließe, da hierfür etwa zunächst weitere Beweissicherungen nötig wären, so genügt doch für die Erfüllung des Tatbestandsmerkmals, dass das Programm diese neue Information eigenständig generiert hat.[573] Darüber hinaus wird gefordert, dass sich die gewonnenen Daten wieder den einzelnen Arbeitnehmern zuordnen lassen.[574] Dies ist wegen der vorliegenden umkehrbaren Pseudonymisierung der Daten ebenfalls gegeben.

Im Hinblick auf den Konzern stellt sich zudem die Frage, auf welcher Ebene der Arbeitnehmervertretung das Mitbestimmungsrecht gemäß § 87 Abs. 1 Nr. 6 BetrVG entsteht. Prinzipiell ist der von den Arbeitnehmern unmittelbar gewählte örtliche Betriebsrat berechtigt.[575] Gemäß § 58 Abs. 1 BetrVG ist jedoch der Konzernbetriebsrat für die Behandlung von Angelegenheiten zuständig, die den Konzern oder mehrere Konzernunternehmen betreffen und nicht durch die einzelnen Gesamtbetriebsräte innerhalb ihrer Unternehmen geregelt werden können.[576] Voraussetzung für die Zuständigkeit des Konzernbetriebsrats ist das Vorliegen objektiv zwingender Gründe rechtlicher oder technischer Natur, die eine unternehmensübergreifende Regelung erfordern.[577] Damit reicht das bloße Interesse des Arbeitgebers an einer zentralisierten Organisation nicht aus.[578] An Stelle dessen ist auf die konkrete Situation des Konzerns und seiner einzelnen Unternehmen, den Inhalt der geplanten Regelung und insbesondere deren Ziel abzustellen.[579] Lässt sich dieses nur durch eine konzernübergreifende Regelung erreichen, ist der Konzernbetriebsrat zuständig.[580] Da die Mitbestimmungsrechte vorliegend durch arbeitgeberseitige Bestrebungen zur Verhinderung von Betrugsfällen entstehen und jene Missbrauchsbekämpfung nur bei einem konsequenten Vorgehen auf der ge-

---

[571] *Kania,* in: Erfkomm a.a.O., § 87 BetrVG Rn. 50; *Richardi*, in: *Richardi* a.a.O., § 87 Rn. 494.
[572] *Steinkühler* (o. Fußn. 481), S.1294; *Kock/Franke* (o. Fußn. 400), S. 649.
[573] *Kock/Francke* a.a.O., S. 649 m.w.N.
[574] *Blomeyer,* in: *Richardi/Wlotzke* (o. Fußn. 281),§ 99 Rn. 95; *Kania,* in: Erfkomm (o. Fußn. 281), § 87 BetrVG Rn. 53; *Kock/Francke* a.a.O., S. 649; *Werner,* in: *Rolfs/Giesen/Kreikebohm (*o. Fußn 277), § 87 Rn. 95.
[575] *Kock/Franke* a.a.O., S. 649; *Trittin/Fischer* (o. Fuß. 284), S. 344.
[576] Laut der Parallelvorschrift § 50 BetrVG ist der Gesamtbetriebsrat für die Behandlung von Angelegenheiten zuständig, die das Gesamtunternehmen oder mehrere Betriebe betreffen und nicht durch die einzelnen Betriebsräte innerhalb ihrer Betriebe geregelt werden können.
[577] *Trittin/Fischer* (o. Fuß. 284), S. 344.
[578] *Kock/Franke* (o. Fußn. 400), S. 649; *Trittin/Fischer* a.a.O., 344.
[579] *Kock/Francke* a.a.O., S. 649.
[580] *BAG*, Beschl. v. 20.12.1995 – 7 ABR 8/95, NZA 1996, 945; *Kock/Francke* a.a.O., S. 649.

samten Konzernebene gelingen kann, ist im Konzernbetriebsrat die zuständige Arbeitnehmervertretung zu sehen.[581]

Aus der Anwendbarkeit von § 87 Abs. 1 Nr. 6 BetrVG folgt die Pflicht des Arbeitgebers, vor Inbetriebnahme der technischen Einrichtung die Zustimmung des Konzernbetriebsrats einzuholen.[582] Das Mitbestimmungsrecht erstreckt sich aber auch auf die konkrete Ausgestaltung der Kontrolle.[583] Dies alles ist aus Gründen der Rechtssicherheit in Form einer Betriebsvereinbarung zu regeln,[584] da grundrechtsrelevante Eingriffe geplant sind.[585]

Schließlich ist noch zu erwähnen, dass durch technische Überwachungseinrichtungen gewonnene Erkenntnisse, welche ohne Mitwirkung des Betriebsrats entstanden sind, keinem prinzipiellen Beweisverwertungsverbot unterliegen. Ein Verwertungsverbot besteht nur, wenn der entsprechende Beweis unter Verletzung des APR zustande kam.[586] Eine unterbliebene Mitbestimmung stellt per se jedoch keine solche Verletzung dar.[587]

4.2.4 Schlussfolgerungen

Die datenschutzrechtliche Untersuchung und insbesondere die Prüfung der Verhältnismäßigkeit präventiver Datenanalysen, bei denen die Kontodaten von Mitarbeitern des Unternehmens mit jenen der Lieferanten abgeglichen werden, hat ergeben, dass derartige Maßnahmen auch aufgrund der neuen Rechtslage nicht per se unzulässig sind.

Das ArbG Berlin bestätigt diese Ansicht. Auch aus der Rechtsprechung des BVerfG lässt sich kein Verbot verdachtsunabhängiger Datenanalysen entnehmen. Die Judikate geben vielmehr eine Reihe von Anforderungen an präventive Ermittlungen vor, die bei der Gestaltung entsprechender Maßnahmen zu beachten und dokumentieren sind. Gleiches gilt für die Vorgaben der Artikel 29-Datenschutzgruppe.[588] Demnach ist folgendes Ergebnis festzuhalten:

> Präventive Datenanalysen, bei denen mit dem Ziel der Verhinderung von Wirtschaftsdelikten Abgleiche der Kontodaten von Mitarbeitern des Unter-

[581] *Kock/Francke* a.a.O., S. 650; im Ergebnis auch *ArbG Dessau-Roßlau* (o. Fußn. 337).
[582] *Werner,* in: *Rolfs/Giesen/Kreikebohm (*o. Fußn 277), § 87 Rn. 1.
[583] *Kania,* in: Erfkomm (o. Fußn. 281), § 87 BetrVG Rn. 58; *Werner,* in: *Rolfs/Giesen/Kreikebohm* a.a.O., § 87 Rn. 96.
[584] Werner, in: Rolfs/Giesen/Kreikebohm a.a.O., § 87 Rn. 9.
[585] Siehe hierzu Abschnitt 3.4.2.
[586] *BAG* (o. Fußn. 342), S. 1196.
[587] *BAG* a.a.O., S. 1196.
[588] Stärkungen des Arbeitnehmerdatenschutzes auf gemeinschaftsrechtlicher Ebene, welche die Bekämpfung von Fraud erschweren könnten, sind darüber hinaus vorerst nicht zu erwarten. Zwar hat die EU-Kommission mit einer Umfrage zur Notwendigkeit einer speziellen Richtlinie zum Arbeitnehmerdatenschutz aus dem Jahre 2001 signalisiert, dass die Verabschiedung einer solchen Richtlinie nicht unwahrscheinlich ist. Allerdings wurde diese Notwendigkeit innerhalb der Mitgliedstaaten unterschiedlich bewertet und es liegt auch bis heute kein Entwurf zu einer entsprechenden Richtlinie vor, siehe *Gola/Wronka* (o. Fußn. 38), Rn. 57

> nehmens mit dessen Lieferanten durchgeführt werden, sind bei Einhaltung der erläuterten Grundsätze der Verhältnismäßigkeit und der Transparenz auch unter den neuen Voraussetzungen des § 32 Abs. 1 BDSG zulässig.[589]

Selbst wenn man die Auffassung vertritt, dass es sich bei der beschriebenen Datenanalyse um keine reine Präventionsmaßnahme handelt, da sie zur Aufdeckung von bereits begangenen Straftaten geeignet ist[590], gelangt man zum selben Ergebnis ihrer Rechtmäßigkeit. Bis zur Generierung der Verdachtsfälle in Form von pseudonymisierten Daten-Dubletten liegt ein ausschließlich präventives Handeln vor. Es kann jedoch der Standpunkt vertreten werden, dass durch die Reidentifizierung der Daten der Prozess der Aufdeckung einer Straftat beginnt.[591] Wenn man bereits diesen Schritt 3 der beschriebenen Analyse an § 32 Abs. 1 Satz 2 BDSG misst, kommt man jedoch ebenfalls zu dem Ergebnis der Zulässigkeit des Vorgangs, wie im nachfolgenden Abschnitt 4.3. darlegt wird.

Im Ergebnis stimmt selbst der Bundesdatenschutzbeauftragte Peter Schaar dieser Auslegung von § 32 BDSG zu: „Grundsätzlich geht es ja (bei verdachtsunabhängigen Datenanalysen) darum, Auffälligkeiten, also Muster, zu erkennen, ohne dass man im ersten Schritt den direkten Rückschluss auf Personen braucht. Eine Mustererkennung mit anonymisierten[592] Daten ist weiterhin möglich. Und wenn man bei einer solchen Auswertung Anhaltspunkte gewinnt, dass bezogen auf konkrete Geschäftsvorgänge Rechtsverstöße erfolgt sind, ist die Herstellung eines Personenbezugs auch legitim und legal. Es muss aber zuvor eine Gefährdungsanalyse stattfinden, es müssen Schwachstellen analysiert werden. Der Kreis der in die Analyse einbezogenen Personen muss möglichst klein gehalten werden."[593]

---

[589] Diese Ansicht wird ebenfalls vertreten durch *ArbG Berlin* (o. Fußn. 20), Abs.-Nr. 21-23; *Bierekoven* (o. Fußn. 466), S. 208; *Brandt* (o. Fußn. 352), S. 8; *Heldmann* (o. Fußn. 244), S. 1238; *Salvenmoser/Hauschka* (o. Fußn. 37), S. 333; *Schmidt* (o. Fußn. 312), S. 198 f.; *Zikesch/Reimer* (o. Fußn. 337), S. 98; wohl auch *Gola/Wronka* (o. Fußn. 38), Rn. 857-859; *Kramer/Gliss,* DSB 4/2010, S. 13; *Thüsing* (o. Fußn. 306), S. 868; a.A. *Schneider* (o. Fußn. 481), S. 1326; *Däubler*, Gläserne Belegschaften?, 2009, S. 229, welcher aber von einer Beurteilung nach S. 2 ausgeht und auch nach alter Rechtslage für eine generelle Unzulässigkeit verdachtsunabhängiger Datenanalysen ist.

[590] *Bierekoven* (o. Fußn. 466), S. 206.

[591] *Brandt* (o. Fußn. 352), S. 9.

[592] Gemeint muss eine Verwendung pseudonymer Daten sein, da bei nach der Legaldefinition anonymen Daten eine Reidentifizierung ausgeschlossen ist.

[593] *Schaar* (o. Fußn. 351), S. 3.

4.3
Aufdeckung bereits begangener Straftaten

Nachfolgend werden die an die präventive Datenanalyse anschließenden Ermittlungsmaßnahmen und deren (datenschutz-)rechtliche Implikationen behandelt. Die rechtliche Bewertung konzentriert sich dabei auf neue Aspekte, die nicht bereits im Rahmen von Abschnitt 4.2 behandelt wurden. Im Hinblick auf die Verhältnismäßigkeitsprüfung, insbesondere in Bezug auf die sich bei der Datenverwendung gegenüberstehenden Interessen, kann zumeist auf das in Abschnitt 4.2.2.2.2 Gesagte verwiesen werden.

4.3.1
Beschreibung des Vorgangs: Weiterverfolgung der Verdachtsmomente, welche durch die in Abschnitt 4.2.1 beschriebene Datenanalyse gewonnen wurden

Die Ergebnisliste der Datenanalyse enthält einige Treffer, welche Übereinstimmungen zwischen den Kontodaten von Mitarbeitern und Lieferanten anzeigen. Jene pseudonymen Daten-Dubletten werden im 3. Schritt der Analyse zu personenbezogenen Daten entschlüsselt. Im Laufe der darauf folgenden internen Ermittlungsmaßnahmen *(Investigations*[594]*)* wird zunächst der Verdacht innerhalb des Buchungssystems weiterverfolgt, z.B. wird nach weiteren, vom Verdächtigten erteilten Aufträgen gesucht. (Personal-)Akten und Unterlagen in elektronischer sowie in Papierform werden gesichtet, die Mitarbeiter in seinem näheren Umfeld werden vernommen, seine Räumlichkeiten bzw. sein Arbeitsplatz oder Schreibtisch werden durchsucht, Unterlagen und sonstige Gegenstände beschlagnahmt und gegebenenfalls seine elektronische Korrespondenz ausgewertet.[595] Diese Maßnahmen sind unter anderem von taktischen Erwägungen geprägt. Insbesondere der durch den Missbrauch entstandene finanzielle Schaden, die im Einzelfall gegebenen Aufklärungsmöglichkeiten und damit zusammenhängende Gelegenheiten zur Beweissicherung sowie eventuelle arbeitsrechtliche Hindernisse, wie Kündigungsfristen, sind zu berücksichtigende Parameter. Hiernach entscheidet sich, wie im konkreten Fall vorgegangen wird, ob etwa der Sachverhalt intern zu lösen oder an die Strafverfolgungsbehörden abzugeben ist.[596] Die Maßnahmen sollten ebenfalls geschehen bevor der verdächtigte Mitarbeiter selbst angehört wird, da andernfalls die Gefahr der Verschleierung der vorgeworfenen Tat bestünde. Denkbar wäre, die genannten Handlungen zu arbeitsfreien Zei-

[594] *Mengel/Ullrich*, NZA 2006, 240 (241), die als „klassischen" Fall von Investigations die Aufdeckung struktureller und langjährig bestehender Missstände im Hinblick auf bilanz-, aufsichts- und insiderrechtliche Fragen verstehen.

[595] Siehe zu den weiteren möglichen Ermittlungsmaßnahmen im Arbeitsumfeld des Verdächtigten *Odenthal* (o. Fußn. 433), S. 155 ff.

[596] Siehe hierzu auch Abschnitt 4.3.2.4; siehe ferner *Klengel/Mückenberger*, CCZ 2009, 81 (87).

ten durchzuführen, wenn der Verdächtigte abwesend ist.[597] In jedem Fall sollte der Arbeitgeber jedoch allein wegen drohender Sanktionen oder Beweisverwertungsverbote sicherstellen, dass alle Aufdeckungsmaßnahmen nur im Bereich des rechtlich zulässigen erfolgen.[598]

4.3.2
Rechtliche Überprüfung

Vor der Beurteilung dieser Aufdeckungsmaßnahmen unter datenschutzrechtlichen Gesichtspunkten stellt sich zunächst die Frage, welche rechtliche Grundlage dem Arbeitgeber die Durchsuchung des Arbeitsplatzes bzw. des Schreibtisches des Verdächtigten und die Beschlagnahme seiner Unterlagen gestattet.

4.3.2.1
Arbeitsvertrag, Hausrecht und Direktionsrecht des Arbeitgebers

Zunächst gilt für alle Akten und Unterlagen ohne Personenbezug, dass der Arbeitgeber bezüglich dieser dienstlichen Dokumente ein uneingeschränktes, vom Arbeitnehmer als Besitzdiener nicht begrenzbares, Einsichtsrecht hat und zwar gilt dies für Dokumente in nicht elektronischer wie in elektronischer Form.[599] Da die meisten Dokumente jedoch zumindest eine Unterschrift oder eventuell personenbezogene Kontaktdaten enthalten werden, lässt sich eine Anwendbarkeit des BDSG nur selten umgehen.[600]

Die Weichen für solche Ermittlungen sollten daher bereits bei Abschluss des Arbeitsvertrags oder im Rahmen einer Betriebsvereinbarung gestellt werden. Diese Rechtsinstitute stellen eine vertragliche Ermächtigung für Ermittlungshandlungen dar und gewährleisten, dass der Arbeitgeber bei Vorliegen von Verdachtsfällen schnell reagieren kann. In Verbindung mit § 242 BGB kann sich aus dem Arbeitsvertrag darüber hinaus eine Duldungspflicht der Handlungen ergeben, wenn „dringende sachliche Gründe" entsprechende Maßnahmen erfordern.[601] Daneben hat der Arbeitnehmer die Ermittlungen im Rahmen seiner arbeitsvertraglichen Nebenpflichten grundsätzlich zu dulden.[602]

Eine Rechtfertigung für die Ermittlungshandlungen ist weiterhin im Hausrecht zu sehen, welches gemäß Art. 13 GG verfassungsrechtlichen Schutz genießt und sich ebenfalls auf Betriebs- und Geschäftsräume erstreckt.[603] Es steht dem Arbeitgeber als Eigentümer oder Besitzer der Betriebsräumlichkeiten gemäß

---

[597] *Odenthal* (o. Fußn. 433), S. 156.
[598] *Klengel/Mückenberger* (o. Fußn. 596), S. 81 f.; *Mengel/Ullrich* (o. Fußn. 594), S. 241.
[599] *Mengel/Ullrich* a.a.O., S. 241.
[600] Siehe hierzu sogleich Abschnitt 4.3.2.2.
[601] Im Hinblick auf Torkontrollen mit Leibesvisitationen *Schmidt*, in: Erfkomm (o. Fußn. 281), Art. 2 GG Rn. 100.
[602] *Mengel* (o. Fußn. 286); S. 109.
[603] *BVerfG,* Beschl. v. 13.10.1971 – 1 BvR 280/66 (Betriebsbetretungsrecht), BVerfGE 32, 54 (68) Rn. 48.

§§ 858 ff., 903, 1004 BGB zu[604] und erlaubt ihm, den Aufenthalt der Arbeitnehmer in den Räumlichkeiten an bestimmte Bedingungen zu knüpfen.[605] Die Inaugenscheinnahme des Arbeitsplatzes bzw. Schreibtisches durch den Arbeitgeber oder von ihm beauftragte Dritte, ist daher ohne Kenntnis oder Zustimmung des betroffenen Beschäftigten zulässig.[606]

In engem sachlichen Zusammenhang mit dem Hausrecht steht das Direktionsrecht des Arbeitgebers aus §§ 106 GewO, 315 BGB. Dieses gestattet ihm jedoch lediglich, bereits vorhandene vertragliche Verpflichtungen näher zu konkretisieren.[607] Sind also entsprechende Duldungspflichten allgemein vereinbart, jedoch nicht abschließend durch Arbeitsvertrag, Betriebsvereinbarungen oder gesetzliche Vorschriften geregelt, kann der Arbeitgeber gemäß § 106 Satz 1 GewO „nach billigem Ermessen" von seinem Direktionsrecht Gebrauch machen.[608] Ein Handeln nach billigem Ermessen liegt vor, wenn er die wesentlichen Umstände des Einzelfalls abgewogen und beiderseitige Interessen angemessen berücksichtigt hat.[609] Sind diese Voraussetzungen erfüllt, lässt sich etwa auch die Befragung von Mitarbeitern im Umfeld der Verdächtigten durch das Direktionsrecht rechtfertigen, da diesen grundsätzlich die Weisung erteilt werden kann, an der Untersuchung mitzuwirken.[610] Die vorzunehmende, nachfolgend lediglich kurz angerissene[611] Abwägung, sollte sicherlich auch vor Ermittlungen, welche auf Ermächtigungen durch den Arbeitsvertrag bzw. eine Betriebsvereinbarung gestützt sind, durchgeführt werden.

Vorliegend bewegt sich der Arbeitnehmer im Bereich der Geschäftsräume innerhalb der Sphäre des Arbeitgebers. Dieser hat damit nicht nur die Möglichkeit, die genannten Ermittlungen durchzuführen. Er ist darüber hinaus aufgrund der in Abschnitt 2 vorgestellten gesetzlichen Anforderungen verpflichtet, auf Verdachtsfälle von Wirtschaftsdelikten zu reagieren. Aufseiten der Interessen des Arbeitnehmers ist zu fragen, wie privat sein Büro oder Schreibtisch ist, wobei grundsätzlich davon ausgegangen werden kann, dass der Mitarbeiter an seinem Arbeitsplatz nur geschäftliche – und damit in die Sphäre des Arbeitgebers fallende – Unterlagen aufbewahrt. Somit überwiegen die schutzwürdigen Interessen des Arbeitgebers. Etwas anderes gilt natürlich für den Dienst-Computer, welcher zumeist ebenfalls für private Zwecke ge-

[604] *BGH*, Urt. v. 20.01.2006 – V ZR 134/05, NJW 2006, 1054.
[605] *Müller-Glöge*, in: MünchKomm-BGB, § 611 Rn. 1022.
[606] *Klengel/Mückenberger* (o. Fußn. 596), S. 85.
[607] *Mengel/Hagemeister*, BB 2007, 1386 (1387) m.w.N.
[608] In diesem Fall kann sogar die Einführung eines Whistleblowing-Systems über das Direktionsrecht erfolgen, wenn darin die Konkretisierung von bereits im Arbeitsvertrag vorhandenen Compliance-Pflichten zu erblicken ist, siehe *Mengel* (o. Fußn. 286); S. 203.
[609] *BAG*, Urt. v. 17.12.1997 - 5 AZR 332/96, NZA 1998, 555 (557); *Mengel/Hagemeister* (o. Fußn. 607), S. 1388 m.w.N.
[610] Zu den weiteren Voraussetzungen *Mengel/Ullrich* (o. Fußn. 594), S. 243 m.w.N.; zu den datenschutzrechtlichen Implikationen siehe den nachfolgenden Abschnitt.
[611] Daneben kann auf die ausführliche Güterabwägung in Abschnitt 4.2.2.2.2 verwiesen werden.

nutzt wird. Zwar ist die Einsichtnahme nicht passwortgeschützter dienstlicher Dateien grundsätzlich zulässig.[612] Wegen der Gefahr einer Strafbarkeit nach § 202a StGB aufgrund eines unzulässigen Ausspähens von Daten sollte eine Auswertung des Computers des Verdächtigten im Rahmen der Ermittlung allerdings mit äußerster Sorgfalt durchgeführt werden.[613] Gleiches gilt wegen der möglichen Verletzung des grundrechtlich geschützten Fernmeldegeheimnisses gemäß Art. 10 GG für die Auswertung seiner E-Mail-Kommunikation, es sei denn, es wurde eindeutig vereinbart, dass eine Privatnutzung der Telekommunikationsmittel im Betrieb verboten ist.[614]

Im Ergebnis bleibt festzuhalten, dass auch eine Durchsuchung des Arbeitsplatzes des Verdächtigten durch den Arbeitgeber ausschließlich im Rahmen der Verhältnismäßigkeit zulässig ist, was angesichts des vorliegenden hinreichend konkreten Verdachts einer Straftat[615] jedoch der Fall ist.

4.3.2.2
Datenschutzrechtliche Überprüfung

Ganz offenkundig an die Voraussetzungen des BDSG gebunden sind die Reidentifizierung der pseudonymen Daten-Dubletten sowie im Bereich der Verwendung personenbezogener Beschäftigtendaten die Weiterverfolgung des Verdachts innerhalb der elektronischen Buchungssysteme und die Auswertung elektronischer Unterlagen und (Personal-)Akten. Durch die gemäß § 32 Abs. 2 BDSG geänderte Rechtslage, wonach auch nicht automatisierte Datenverwendungen den Anforderungen des BDSG unterfallen[616], sind, soweit Daten mit Personenbezug betroffen sind, die Befragungen der Kollegen des Verdächtigten[617] sowie die Überprüfung von Akten und Unterlagen in Papierform, ebenfalls an § 32 Abs. 1 BDSG zu messen. Im Hinblick auf die eventuell vorzunehmende Einsicht in die vom Persönlichkeitsrecht geschützten Personalakten soll lediglich aufgezeigt werden, dass Eingriffe bei einem überwiegenden schutzwürdigen Interesse des Arbeitgebers auch im Rahmen von Investigations gerechtfertigt sein können.[618] Darüber hinaus soll auf die jeweilige Rechtsprechung und Literatur zum Personalaktenrecht[619] verwiesen werden.

---

[612] *Klengel/Mückenberger* (o. Fußn. 596), S. 85.
[613] Jedoch wird auch die Ansicht vertreten, dass in Ausnahmefällen, etwa dem Vorliegen des Verdachts der Begehung einer Straftat, die Überprüfung des privat genutzten Computers zulässig sein kann, vgl. *Mengel/Ullrich* (o. Fußn. 594), S. 242.
[614] Siehe hierzu Abschnitt 3.1.
[615] Siehe hierzu Abschnitt 4.3.2.2.3.
[616] Siehe Abschnitt 3.4.3.
[617] *Wybitul* (o. Fußn. 30), S. 1584.
[618] *Mengel/Ullrich* (o. Fußn. 594), S. 242; *Klengel/Mückenberger* (o. Fußn. 596), S. 86.
[619] *BAG*, Urt. v. 04.04.1990 – 5 AZR 299/89, NZA 1990, 933; *Gola/Wronka* (o. Fußn. 38), Rn. 98ff. m.w.N; *Mengel* (o. Fußn. 286); S. 114 f.

Vorliegend handelt es sich um Maßnahmen zur Aufdeckung bereits begangener Straftaten. Die Maßnahmen sind also nur zulässig, soweit sie den Ansprüchen aus § 32 Abs. 1 S. 2 BDSG gerecht werden.[620]

4.3.2.2.1
Aufdeckung

Wie bereits dargelegt[621] handelt es sich bei einer Ermittlungsmaßnahme um die Aufdeckung einer Straftat gemäß § 32 Abs. 1 Satz 2 BDSG, wenn sie an die Perpetuierung und Weiterverfolgung von Verdachtsmomenten anknüpft, welche etwa aus präventiven Ermittlungsmaßnahmen hervorgegangen sind. Dies ist vorliegend der Fall, da lediglich die aus der Datenanalyse aus 4.2 gewonnenen Verdachtsmomente aufrechterhalten werden.

4.3.2.2.2
Straftat im Beschäftigungsverhältnis

Dem Verdächtigten ist eine Straftat im Beschäftigungsverhältnis zur Last zu legen. Die präventive Datenanalyse betraf nur einen genau festgelegten Kreis der Unternehmensangestellten im Einkaufsbereich. Damit handelt es sich beim Verdächtigten, dessen Identität erst mit jener Analyse festgestellt wurde, um einen Beschäftigten i.S.v. § 3 Nr. 11 BDSG. Bei der ihm vorgeworfenen Tat handelt es sich ferner um eine Straftat. Korruption in der Privatwirtschaft fällt vorrangig in den Anwendungsbereich der §§ 299, 300 StGB,[622] welche die Bestechlichkeit und Bestechung im geschäftlichen Verkehr, bzw. besonders schwere Fälle solcher Handlungen sanktionieren. Der gegenwärtige Fall des unwahren Auftretens als Lieferant und die damit verbundene rechtswidrige Erlangung von Vermögensvorteilen spricht jedoch eher für eine Strafbarkeit wegen Betrugs, § 263 StGB oder aufgrund von Untreue, § 266 StGB. Jedenfalls lässt sich der Missbrauch einem Straftatbestand des StGB zuordnen.

Im Ergebnis handelt es sich also um eine Straftat im Beschäftigungsverhältnis. Darüber hinaus liegt sogar eine von § 32 Abs. 1 Satz 2 BDSG nicht einmal geforderte Straftat mit unmittelbarem Bezug zur vertraglich geschuldeten Leistungspflicht vor, da der Verdächtigte seine Stellung im Einkauf missbraucht und das Unternehmen schädigende Aufträge erteilt hat.[623]

[620] Siehe hierzu schon Abschnitt 3.4.4.1.
[621] Siehe Abschnitt 3.4.4.1.1
[622] *Zimmer/Stetter*, BB 2006, 1445 (1446).
[623] Siehe auch Abschnitt 3.4.4.1.2.

4.3.2.2.3
Tatsächliche zu dokumentierende Anhaltspunkte, die den Verdacht einer Straftat begründen

Fraglich ist darüber hinaus, ob ein hinreichend konkreter Verdacht vorliegt, der die internen Ermittlungsmaßnahmen rechtfertigt. Wie bereits dargestellt[624], empfiehlt sich im Hinblick auf die Auslegung dieses Tatbestandsmerkmals der Rückgriff auf strafprozessrechtliche Grundsätze, welche im Zusammenhang mit dem von § 152 Abs. 2 StPO für das Einschreiten der Staatsanwaltschaft geforderten Anfangsverdacht einer Straftat aufgestellt wurden. Ein solcher Anfangsverdacht ist gemäß § 152 Abs. 2 StPO bei Vorliegen „zureichende(r) tatsächliche(r) Anhaltspunkte" für eine „verfolgbare Straftat" gegeben. Dabei ist eine Straftat verfolgbar, soweit keine Verfahrenshindernisse bestehen oder die Strafklage verbraucht ist.[625] Für die Qualifizierung als zureichend tatsächliche Anhaltspunkte genügt es, wenn die gewonnen Tatsachen unter Heranziehung eines gewissen Erfahrungssatzes zumindest Indizien für ein strafrechtlich relevantes Handeln bilden, auch wenn sie selbst noch nicht den Tatbestand einer Strafnorm erfüllen oder ein rechtswidriges Verhalten darstellen.[626] Es muss lediglich „nach kriminalistischer Erfahrung die Möglichkeit (bestehen), dass eine verfolgbare Straftat vorliegt."[627] Der Verdacht hat auch nicht dringend zu sein oder hinreichenden Anlass für eine Anklage zu geben.[628] Bei der Frage, ob ein Anfangsverdacht vorliegt, steht der Staatsanwaltschaft ferner ein Beurteilungsspielraum zu.[629] Jedoch zwingen schon „entferntere Verdachtsgründe, die es nach kriminalistischer Erfahrung als möglich erscheinen lassen, dass eine verfolgbare Straftat vorliegt" zur Aufnahme von Ermittlungen.[630] Bloße Vermutungen genügen hingegen nicht, jemandem eine Straftat zur Last zu legen.[631] Darüber hinaus sind zunächst alle plausiblen Sachverhaltsalternativen zu Prüfen und die konkrete Ermittlungsmaßnahme darf auch nicht unverhältnismäßig sein.[632] Im Hinblick auf den Adressatenkreis von § 32 BDSG ist jedoch auch zu berücksichtigen, dass die verantwortliche Stelle zumeist aus einer „kriminalistischen Laienper-

[624] Siehe Abschnitt 3.4.4.1.3.
[625] *Pfeiffer* (o. Fußn. 353), §. 152 Rn. 3; *Schoreit*, in: KK-StPO, § 152 Rn. 28.
[626] *Pfeiffer* a.a.O., § 152 Rn. 1a.
[627] *BGH*, Urt. v. 21.04.1988 – III ZR 255/86, NJW 1989, 96 (97).
[628] *Schoreit,* in: KK-StPO, § 152 Rn. 30; *Pfeiffer* (o. Fußn. 353), §. 152 Rn. 1a.
[629] *BGH*, Urt. v. 18.06.1970 – III ZR 95/68, NJW 1970, 1543 (1544); *BGH* (o. Fußn. 627), S 97.
[630] *BVerfG*, Beschl. v. 18.01.1994 – BvR 1912/93, NJW 1994, 783 (784).
[631] *BVerfG*, Urt. v. 20.02.2001 – 2 BvR 1444/00, BVerfGE 103, 142 (163) (Wohnungsdurchsuchung), Rn. 64; *OLG Hamburg*, Beschl. v. 08.02.1984 – 1 Ws 26/84, NJW 1984, 1635 (1636).
[632] *BVerfG*, Beschl. v. 03.07.2006 – 2 BvR 230/04, Pressemitteilung Nr. 63/2006 v. 12.07.2006, http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg06-063.html (Stand 10.05.2010).

spektive“[633] heraus handelt und die Anforderungen an den Verdacht i.S.d. Norm daher nicht allzu streng sein dürfen.[634]

Die vorliegenden internen Ermittlungen basieren auf der durch die Analyse bewiesenen Tatsache, dass ein Angestellter zugleich in einem Lieferantenverhältnis zum Unternehmen steht. Sie gehen also über eine bloße Vermutung hinaus. Es werden nicht etwa alle Büros der Angestellten im Einkauf durchsucht, weil das pauschale Risiko von Scheingeschäften bestünde. An Stelle dessen wird einem konkreten Verdacht, der eine konkrete Person bzw. Personen betrifft, nachgegangen. Dieser Verdacht ergibt sich aus der Auswertung der Ergebnisse der Datenanalyse und der Erfahrung, dass Mitarbeiter eines Unternehmens in den seltensten Fällen auch Lieferanten des gleichen Unternehmens sind, womit die Wahrscheinlichkeit eines Missbrauchs sehr groß ist. Die Übereinstimmung bei der Datenanalyse stellt zwar per se keine rechtswidrige oder gar strafrechtlich relevante Handlung dar, wohl aber ein Indiz für das Vorliegen einer Straftat. Nichtsdestotrotz ist vor der Ermittlung zu prüfen, ob es neben Missbrauch auch noch andere Gründe für die übereinstimmenden Kontodaten geben könnte. Systemfehler, Eingabefehler bei der Einstellung der Kontodaten oder die tatsächlich gleichzeitige Eigenschaft als Angestellter und als Lieferant, ohne dass diese Position für Missbrauch genutzt wurde, kommen etwa in Betracht.

Sind diese Alternativen jedoch ausgeschlossen, bestehen die von § 32 Abs. 1 Satz 2 BDSG geforderten tatsächlichen Anhaltspunkte, die den Verdacht einer Straftat begründen.[635] Ein Vorhalten des positiven Ergebnisses der Datenanalyse stellt weiterhin eine Dokumentation des Verdachts i. S. d. Norm dar.

4.3.2.2.4 Verhältnismäßigkeit

Grundsätzlich müsste jede einzelne Maßnahme zur Aufdeckung der Straftat einzeln auf ihre Verhältnismäßigkeit hin geprüft werden. Da dies jedoch im begrenzten Rahmen der vorliegenden Arbeit nicht ausführlich geschehen kann, werden die Reidentifizierung, die weiteren Nachforschungen im elektronischen Buchungssystem, die Durchsuchung des Arbeitsplatzes, die Beschlagnahme von Unterlagen mit Personenbezug und die Befragung von Kollegen des Verdächtigten[636] nachfolgend einheitlich behandelt. Diese Datenverwendungen haben erforderlich zur Aufdeckung der Straftat zu sein. Ferner dürfen das schutzwürdige Interesse des Beschäftigten an dem Aus-

[633] *Hanloser* (o. Fußn. 342), S. 597; auch des *ArbG Berlin* hält der klagenden Compliance-Beauftragten zugute, dass sie keine Juristin ist (o. Fußn. 20), Abs.-Nr.16, 22.
[634] Siehe auch *Salvenmoser/Hauschka* (o. Fußn. 37), S. 333, nach deren Auffassung eine Anwendung der strafprozessrechtlichen Grundsätze zu weit gehend wäre.
[635] *Bierekoven* (o. Fußn. 466), S.; im Ergebnis auch *Gola/Wronka* (o. Fußn. 38), Rn. 857.
[636] Siehe zu einigen der genannten Maßnahmen im Einzelnen *Klengel/Mückenberger* (o. Fußn. 596), S. 82 ff.; *Mengel* (o. Fußn. 286); S. 109ff.

schluss der Datenverwendung nicht überwiegen und insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sein.

Die im Rahmen der Ermittlungen angewandten Methoden stellen allesamt geeignete Maßnahmen zur Aufklärung der Straftat dar. Mildere, jedoch gleichermaßen effektive Mittel sind ebenfalls nicht ersichtlich. Die reine Befragung des Verdächtigten etwa stellt kein geeignetes Mittel dar. Es stünde zu erwarten, dass der Verdächtigte, der offensichtlich ein Interesse daran hat, dass seine Taten nicht aufgedeckt werden, im persönlichen Gespräch zunächst alle Vorwürfe leugnen und anschließend damit beginnen würde, seine Tat zu verschleiern, indem er etwa den Verdacht erhärtende Daten löscht oder Unterlagen vernichtet. Aus diesem Grund entfällt laut der Artikel 29-Datenschutzgruppe auch die Benachrichtigungspflicht[637], die dem Verdächtigten gemäß § 33 Abs. 1 BDSG grundsätzlich zustünde. Damit wäre dieses Mittel für den Arbeitgeber unzumutbar. Daneben stellen die gewählten Ermittlungsmethoden vergleichsweise geringe Eingriffe in das Persönlichkeitsrecht der Betroffenen dar, da mit den internen Ermittlungen keineswegs die Einsicht in private Angelegenheiten verbunden ist, sondern der Arbeitgeber sich ausschließlich in der ihm zugeordneten Arbeitssphäre bewegt. Im Übrigen sind selbst Ermittlungen im privaten Umfeld des Verdächtigten, etwa durch die Beauftragung eines Privatdetektivs, als letztes verbleibendes Mittel zur Aufdeckung von Straftaten im Beschäftigungsverhältnis von der Rechtsprechung als zulässig anerkannt.[638]

Die weiteren Grundsätze, die im Rahmen dieser Verhältnismäßigkeitsprüfung zu beachten sind, wurden bereits in Abschnitt 3.4.4.1.4 ausführlich dargestellt.[639] Nach allem Gesagten bestehen am berechtigten Interesse des Arbeitgebers an der Aufdeckung der Straftat vor dem Hintergrund seiner gesetzlichen Pflichten, aber auch wegen des Eigeninteresses an der Bekämpfung von Vermögensschäden, keine Zweifel. Die Aufklärung stellt laut dem BAG[640] im Gegenteil sogar ein rechtlich schützenswertes Ziel dar und auch die Artikel 29-Datenschutzgruppe erkennt das dahingehende berechtigte Interesse des Arbeitgebers, trotz eventuell entgegenstehender Rechte der Betroffenen, an.[641] Darüber hinaus sind keine schutzwürdigen Interessen des Betroffenen am Ausschluss der Datenverwendung ersichtlich. Abgesehen von dem mit dem Zugriff auf elektronische personenbezogene Daten grundsätzlich verbundenen Eingriff in sein ISBR, bestehen keine weitergehenden Verletzungen des APR,

---

637 *Artikel 29-Datenschutzgruppe,* (o. Fußn. 560), S. 15.

638 *Gola/Wronka* (o. Fußn. 38), Rn. 665; *Klengel/Mückenberger* (o. Fußn. 596), S. 86 welche die Persönlichkeitsrechte des Verdächtigten gar nicht tangiert sehen und die Grenzen der Untersuchungen lediglich in den Rechten der betroffenen Dritten erblicken.

639 Ferner kann auch hier auf die Verhältnismäßigkeitsprüfung mit Güterabwägung im Rahmen der datenschutzrechtlichen Überprüfung der präventiven Datenanalyse in Abschnitt 4.2.2.2.2 verwiesen werden.

640 *BAG* (o. Fußn. 365), S. 1190.

641 *Artikel 29-Datenschutzgruppe* (o. Fußn. 560), S. 10.

da weder Video- noch Tonaufnahmen von ihm verwendet werden und auch seine Privatsphäre nicht tangiert wird.[642] Eventuelle Eingriffe wären jedoch gerechtfertigt, da insbesondere nicht jenes Interesse des Betroffenen schutzwürdig sein kann, dass seine Straftat nicht aufgedeckt wird.[643] Sein schutzwürdiges Interesse kann also nur dann überwiegen, wenn es eine andere plausible Erklärung für die Übereinstimmung der Kontodaten gibt. Wie bereits dargestellt, ist diese Möglichkeit ohnehin vor der Durchführung weiterer Ermittlungen auszuschließen, um überhaupt den erforderlichen Anfangsverdacht feststellen zu können.[644] Sind diese Alternativen allerdings ausgeschlossen, sind die genannten Maßnahmen verhältnismäßig. Insbesondere sind die Maßnahmen nicht nach Art und Ausmaß im Hinblick auf den Anlass der Datenverwendung unverhältnismäßig, d.h. auch die Schwere der Straftat und die Intensität des Verdachts[645] sprechen für die Verhältnismäßigkeit. Die vorliegende Betrugsart stellt keinesfalls ein Kavaliersdelikt dar und kann bei gehäuftem Auftreten ernsthafte Auswirkungen auf die Rechnungslegung des Unternehmens haben, mit den bekannten Folgen. Wie bereits dargelegt, geschehen alle Handlungen ebenfalls auf der Grundlage eines hinreichenden Verdachts. Damit überwiegen die Interessen des Arbeitgebers.

Die Ermittlungsmaßnahmen sind insgesamt verhältnismäßig i.S.v. § 32 Abs. 1 Satz 2 BDSG und damit zulässig.

4.3.2.3
Rechte der Arbeitnehmervertretung

Auch bei den vorliegenden Maßnahmen im Zusammenhang mit den Investigations sind die Rechte des Betriebsrats zu berücksichtigen. Die Auswertung von Dokumenten, die den Anwendungsbereich des BDSG eröffnen, löst etwa gemäß § 80 Abs. 2 i.V.m. § 80 Abs. 1 Nr. 1 BetrVG eine Pflicht zur Benachrichtigung des Betriebsrats aus, damit dieser seinem Auftrag zur Überwachung der Einhaltung der für die Beschäftigten geltenden Gesetze nachkommen kann.[646] Sind private Dokumente Gegenstand der Untersuchung, können darüber hinaus gemäß § 87 Abs. 1 Nr. 1 BetrVG sogar Mitbestimmungsrechte entstehen.[647] Gleiches gilt gemäß § 87 Abs. 1 Nr. 6 BetrVG für die elektronische Auswertung dienstlicher Unterlagen, wenn dies mit einer eigens dafür

[642] Zu beachten sind ferner strafbewährte Schutzvorschriften des StGB wie das Recht auf persönliche Freiheit des Verdächtigten aus § 239 StGB, siehe *Odenthal* (o. Fußn. 433), S. 162 f.
[643] *Diller* (o. Fußn. 402), S. 439; *Olbers* (o. Fußn. 272), S. 846; *Schmidt*, DuD 2010, 207 (211).
[644] Ferner wird die Ansicht vertreten, dass auch eine Feststellung der Unschuld erst im Laufe der späteren Auswertung der Daten in Kauf genommen werden kann, womit die schutzwürdigen Interessen des Arbeitnehmers am Ausschluss der Datenverarbeitung nicht überwiegen, siehe *Diller* a.a.O., S. 439; *Olbers* a.a.O., S. 846.
[645] BT-Drucks. 16/13657, S. 21.
[646] *Kania,* in: Erfkomm (o. Fußn. 281), § 80 BetrVG Rn. 3; *Mengel/Ullrich* (o. Fußn. 594), S. 244; *Thüsing,* in: *Richardi* (o. Fußn. 569), § 80 Rn. 8;
[647] *Mengel/Ullrich* a.a.O., S. 244.

eingerichteten Datenbank erfolgt.[648] Befragungen von Mitarbeitern lösen mindestens Informations- und zum Teil auch Mitbestimmungsrechte aus.[649] Um das derzeit verfügbare Maß an Rechtssicherheit auszuschöpfen, empfiehlt sich daher auch hier der Abschluss einer Betriebsvereinbarung. In jener sollte genau festlegt werden, welche Befugnisse dem Arbeitgeber bei Vorliegen des Verdachts einer Straftat zustehen und insbesondere auch, wo sich am Arbeitsplatz des Angestellten private bzw. geschäftliche Inhalte befinden, sei es auf der Festplatte des dienstlichen Computers[650], sei es in einer Schreibtischschublade. Die Betriebsvereinbarung muss sowohl den Interessen des Arbeitgebers an der Erfüllung seiner Pflichten aus Corporate Governance und Compliance, als auch den Persönlichkeitsrechten des Arbeitnehmers gerecht werden.

4.3.2.4 Schlussfolgerungen

Entgegen der Frage der Zulässigkeit von präventiven Mechanismen wie der beschriebenen Datenanalyse, erscheint eine Prüfung der Rechtmäßigkeit von Maßnahmen zur Aufdeckung von Straftaten vergleichsweise eindeutig. Das maßgebliche Kriterium stellt hier das Vorliegen des hinreichenden Verdachts dar. Ist dieser jedoch gegeben,[651] hat eine Abwägung der entgegenstehenden Interessen im Zweifel für den Arbeitgeber auszufallen.

Über die genannten Ermittlungsmaßnahmen hinausgehenden Handlungen kann entgegen gehalten werden, dass dem Arbeitgeber auch die Möglichkeit der Anzeige bleibt, mit der Folge, dass die Strafverfolgungsbehörden die Straftat aufklären. Diese haben weiterreichende Befugnisse als die unternehmensinternen Ermittler. Aus diesem Grund sind auch die strengen Anforderungen an die Verhältnismäßigkeitsprüfung gemäß § 32 Abs. 1 Satz 2 BDSG gerechtfertigt, da die verantwortliche Stelle ihre Fälle von Wirtschaftdelikten bei Auftreten erster Verdachtsmomente ebenso umgehend an die Behörden abgeben könnte. Der Arbeitgeber hat also zu entscheiden, ob er die erweiterten Ermittlungsbefugnisse der Behörden nutzen möchte, was zwar zu einer schnelleren Klärung des Sachverhalts führen kann, diesen jedoch auch automatisch öffentlich macht, womit die beschriebenen Vertrauens- und Reputationsverluste die Folge sein können. Oder ob er den Fall eigenständig klärt, sich damit angesichts zu beachtender arbeits-, persönlichkeits-, kollektiv- sowie datenschutzrechtlicher Bestimmungen in das „juristische Minenfeld“[652] interner Er-

[648] *Olbers* (o. Fußn. 272), S. 846.
[649] *Mengel/Ullrich* (o. Fußn. 594), S. 244f; *Olbers* a.a.O., S. 846; überdies kann hinsichtlich der Mitbestimmungsrechte auf die weiteren Ausführungen in Abschnitt 4.2.3 verwiesen werden.
[650] Siehe zur Zulässigkeit der Kontrolle von Mitarbeiter-E-Mails *Dann/Gastell* (o. Fußn. 431), S. 2995; *Wellhörner/Byers* (o. Fußn. 246), S. 2310;
[651] In Betracht kommen etwa auch Whistleblowing-Meldungen, siehe *Hanloser* (o. Fußn. 342), S. 597; *Gola/Wronka* (o. Fußn. 38), Rn. 402.
[652] *Odenthal* (o. Fußn. 433), S. 158.

mittlungen begibt und es etwa bei arbeits- und zivilrechtlichen Sanktionen gegen den Verdächtigten belässt. Auch hier spielen die eingangs erwähnten taktischen Überlegungen wieder eine Rolle.[653] Eine Anzeigepflicht gemäß § 138 StGB besteht jedenfalls nicht.[654]

Es empfiehlt sich der Abschluss einer Konzernbetriebsvereinbarung. Diese dient auch der Dokumentation, dass der Arbeitgeber die dem Arbeitnehmer im Zusammenhang mit der Nutzung der vorhandenen Kommunikationsmittel zustehenden Rechte beachtet. Ferner ist, wie bereits dargestellt, der den Ermittlungen zugrunde liegende Verdacht zu dokumentieren und natürlich auch, dass alle Alternativen, die einen Missbrauch ausschließen könnten, nicht zutreffend sind.

[653] Zu alledem *Klengel/Mückenberger* (o. Fußn. 596), S. 87.
[654] *Hohmann*, in: MünchKomm-StGB, § 138 Rn. 7

5
Zusammenfassung und Handlungsempfehlung

Zu Beginn der vorliegenden Arbeit wurde die Kernfrage gestellt, welche Maßnahmen ein deutscher, auch in den U.S.A. operierender und börsennotierter IT-Dienstleistungskonzern in der Rechtsform einer Aktiengesellschaft durchführen kann und muss, um sowohl den deutschen und amerikanischen Anforderungen an Corporate Governance und Compliance als auch den Bestimmungen des deutschen Datenschutzrechts gerecht zu werden. Die Erkenntnisse, die diesbezüglich im Rahmen der Untersuchung gewonnen werden konnten, lassen sich in vier Thesen zusammenfassen (5.1.). Darauf folgt unter 5.2. eine Handlungsempfehlung, wie den Interessen des Unternehmens an der Durchführung verdachtsunabhängiger Datenanalysen auf der einen und den Persönlichkeitsrechten der betroffenen Beschäftigten auf der anderen Seite hinreichend Rechnung getragen werden kann.

5.1
Zusammenfassung

1. These: Von einem Konzern mit beschriebener Größe und Kapitalmarktzugang ist die strengst mögliche Interpretation von § 91 Abs. 2 AktG anzunehmen, womit ein umfassendes, nachweislich wirksames IKS bzw. Risikomanagementsystem zu implementieren ist, welches vor bestandsgefährdenden Entwicklungen schützt. Zwei verschiedene Faktoren verpflichten den Konzern: Zunächst existiert eine Fülle von gesetzlichen Anforderungen, welche wie das AktG und der SOA die Errichtung entsprechender Kontrollsysteme explizit fordern oder wie § 130 OWiG dem Normadressat zur Abwendung von Sanktionen keine andere Wahl als die Implementierung entsprechender Systeme lassen. Mängel des Risikomanagementsystems werden straf-, zivil- und arbeitsrechtlich geahndet. Der zweite Faktor ist das erhebliche, mit der Größe des Unternehmens steigende Risiko von Wirtschaftsdelikten, welche durch Mitarbeiter des Unternehmens begangen werden. Die von diesen Delikten ausgehenden mittelbaren und unmittelbaren Schäden sind immens. Verhindern lassen sich diese Fälle von Fraud nur durch ein ganzheitliches IKS.

2. These: Der Vorstand hat sich bei der Architektur des Systems an den Anforderungen des Abschlussprüfers zu orientieren, denn darin spiegeln sich die Anforderungen, die zu beachten sind. Danach muss das IKS insbesondere folgende Funktionen umfassen: Festlegung der Risikofelder, Risikoerkennung und –analyse, Risikokommunikation, Zuordnung von Verantwortlichkeiten und Aufgaben, Überwachung der ergriffenen Maßnahmen, Dokumentation des IKS. Im Rahmen des kontinuierlich durchzuführenden AFM sind Methoden zur Vermeidung, Entdeckung und Reaktion im Hinblick auf Fälle von Wirtschaftskriminalität anzuwenden. Im Bereich der präventiven Maßnahmen sind neben der Einhaltung grundlegender organisatorischer Prinzipien in Hochrisi-

kobereichen auch verdachtslose Datenanalysen durchzuführen, in welchen der Bestand der Beschäftigtendaten des Unternehmens auf typische Missbrauchsszenarien hin untersucht wird. Eines dieser verbreiteten Delikte ist die Abwicklung von Scheingeschäften durch Beschäftigte des Unternehmens, indem diese gleichzeitig als Lieferanten auftreten.

3. These: Werden personenbezogene Daten der Beschäftigten verwendet, richtet sich die Zulässigkeit der Datenverwendung nach § 32 BDSG. Präventive Maßnahmen zur Verhinderung von Straftaten und damit auch verdachtsunabhängige Ermittlungen werden durch § 32 Abs. 1 Satz 1 BDSG geregelt. Danach dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. § 32 Abs. 1 Satz 2 BDSG betrifft Maßnahmen zur Aufdeckung von Straftaten, wobei der Begriff der Aufdeckung an die Aufrechterhaltung und Weiterverfolgung von Verdachtsmomenten anknüpft. Nach Satz 2 dürfen personenbezogene Daten eines Beschäftigten nur dann zur Aufdeckung von Straftaten erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Datenverwendung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Datenverwendung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Im Ergebnis sind Datenverwendungen zur Prävention oder Aufdeckung von Straftaten unabhängig von der konkreten Ermächtigungsgrundlage nur zulässig, wenn eine umfassende Verhältnismäßigkeitsprüfung zu diesem Ergebnis führt. Die Maßnahme hat demnach erforderlich zur Erreichung des verfolgten Ziels und darüber hinaus auch angemessen zu sein. Überdies verbietet der verfassungsrechtlich vorgegebene Grundsatz der Transparenz die heimliche Vornahme von datenschutzrechtlich relevanten Maßnahmen, die zur Verletzung der Persönlichkeitsrechte der Betroffenen geeignet sind.

Damit führt § 32 BDSG bis auf zwei Ausnahmen zu keiner Veränderung der Rechtslage. Diese bestehen in der Erweiterung des Anwendungsbereichs des BDSG gemäß Abs. 2 der Norm auf personenbezogene Daten, die keine automatisierten Dateien darstellen und in der Pflicht gemäß Abs. 1 Satz 2 der Norm zur Dokumentation von Anhaltspunkten, die den Verdacht einer Straftat begründen.

4. These: Präventive Datenanalysen, bei welchen mit dem Ziel der Verhinderung von Wirtschaftsdelikten Abgleiche der Kontodaten von Mitarbeitern des Unternehmens mit dessen Lieferanten durchgeführt werden, sind bei Einhaltung der erläuterten Grundsätze der Verhältnismäßigkeit und der Transparenz auch unter den neuen Voraussetzungen des § 32 Abs. 1 BDSG zulässig. Die Rechtmäßigkeit des verdachtsunabhängigen Abgleichs pseudonymisierter

Kontodaten richtet sich bis einschließlich der Generierung der pseudonymisierten Verdachtsfälle zunächst nach § 32 Abs. 1 Satz 1 BDSG und ist folglich zulässig, sofern dem Gebot der Verhältnismäßigkeit hinreichend Rechnung getragen wurde. Mit der Reidentifizierung der Daten beginnt der Prozess der Aufdeckung einer Straftat, womit § 32 Abs. 1 Satz 2 BDSG eingreift. Bei den durch die Analyse generierten Verdachtsfällen handelt es sich um die von Satz 2 verlangten, zu dokumentierenden tatsächlichen Anhaltspunkte, die den Verdacht einer Straftat begründen, wodurch die Weiterverfolgung des Verdachts unter Wahrung der Verhältnismäßigkeit und der besonderen Berücksichtigung der Interessen des Betroffenen, zulässig ist.

5.2
Handlungsempfehlung

Letzte Rechtssicherheit kann es im Hinblick auf verdachtsunabhängige automatisierte Datenanalysen zur Verhinderung von Wirtschaftsdelikten wegen des Mangels an obergerichtlicher arbeitsrechtlicher Rechtsprechung zur Problematik vorerst nicht geben. Nach einer Würdigung des Urteils des ArbG Berlin und der Rechtsprechung des BVerfG lautet die derzeit mögliche Empfehlung, dass entsprechende Kontrollen vorerst nicht einzuschränken sind, solange kein Urteil mit gegenteiligem Ergebnis ersichtlich ist. Parallel muss jedoch die Rechtsprechung zur Thematik beobachtet werden.

Ferner empfiehlt es sich für die Unternehmen, umfassend zu dokumentieren, dass das Risiko, gegen welches sich die Analyse wendet, tatsächlich oder mit sehr hoher Wahrscheinlichkeit besteht. Der pauschale Verweis auf allgemein zugängliche Studien wird hierfür i.d.R. nicht ausreichend sein. Darüber hinaus sollen alle weiteren Anstrengungen im Rahmen des Risiko- und Anti-Fraud-Managements dokumentiert werden, denn datenschutzrechtlich bedenkliche Eingriffe können nur dann gerechtfertigt sein, wenn alle zumutbaren milderen Maßnahmen nicht den erhofften Erfolg bringen könnten. Überdies ist die Datensicherheit der durch die Analyse gewonnenen sensiblen Verdachtsmomente gegenüber dem Zugriff Dritter zu gewährleisten. Und schließlich sind alle anfallenden Daten, die für die Missbrauchsbekämpfung unbrauchbar sind, unverzüglich zu löschen.

Die Maßnahmen sind am Kriterium des Übermaßverbots zu messen. Insbesondere ist der Grundsatz der Datensparsamkeit zu beachten, d.h. es dürfen immer nur so viele personenbezogene Daten wie nötig verwendet werden und wo immer möglich, sollte anonymisierten oder pseudonymisierten Daten Vorrang gegeben werden. Daneben ist eine Betriebsvereinbarung abzuschließen[655], womit automatisch die Transparenz der Datenverwendung garantiert wird. Neben einer Beteiligung des Betriebsrats ist in jedem Fall auch der be-

[655] Diese Notwendigkeit besteht grundsätzlich bei allen datenschutzrechtlich relevanten Compliance-Konzepten, *Albrecht* (o. Fußn. 293), S. 4.

triebliche Datenschutzbeauftragte in das Verfahren einzubinden. Möglich ist darüber hinaus eine Absprache mit der zuständigen Datenschutzaufsichtsbehörde.

Im Folgenden soll ein in 8 Phasen unterteilter Ablauf einer Datenanalyse aufgezeigt werden, der alle im Verlauf der vorliegenden Arbeit behandelten Grundsätze und Vorgaben hinreichend beachtet.[656] Zu jeder Phase findet sich eine kurze Erläuterung mit Verweisen auf die entsprechenden Abschnitte.

Dokumentation und Festlegung von Analyseanlass und -zweck

Der Anlass des Datenabgleichs (z.B. das Ergebnis einer Risikoanalyse oder das Auftreten von auf Missbrauch hindeutenden Indikatoren) ist umfassend zu dokumentieren.

Der Zweck muss so definiert werden, dass er das Mittel der Datenanalyse rechtfertigt. Daher ist das Risiko bzw. das Ziel, gegen das bzw. für das die Analyse eingesetzt wird, ausführlich zu beschreiben.

Die Frage nach der Verhältnismäßigkeit der Maßnahme muss stets im Vordergrund stehen. Die konkrete Analyse muss erforderlich zur Erreichung des angestrebten Zwecks und darüber hinaus auch angemessen sein.

Die diesbezüglichen Vorgaben aus der Rechtsprechung sind einzuhalten (siehe S. 64-66 und 86 f.).

Absprache mit Betriebsrat und betrieblichem Datenschutzbeauftragten, Abschluss einer Betriebsvereinbarung

Der Datenschutzbeauftragte ist in die Planung mit einzubeziehen (siehe S. 46). Der Betriebsrat ist wegen seines Mitbestimmungsrechts im Falle der Verwertung personenbezogener Daten am Verfahren zu beteiligen (siehe Abschnitt 4.2.3).

Datenanalysen sind niemals heimlich durchzuführen. Der Grundsatz der Transparenz muss gewahrt sein. Die abzuschließende Betriebsvereinbarung erfüllt dieses Erfordernis. Für die Vereinbarung gilt die Beachtung des Bestimmtheitsgrundsatzes (siehe S. 45, 49 f. und 77 f.).

Definition der abzugleichenden Datenbestände mit größtmöglicher Eingrenzung des Betroffenenkreises

Dem Grundsatz der Datensparsamkeit entsprechend haben anonymisierte Daten immer Vorrang. Ist eine Verwendung personenbezogener Daten unausweislich, kann eine Nutzung in pseudonymisierter Form zulässig sein. Der Kreis der von der Analyse Betroffenen ist durch die Wahl geeigneter Indikatoren größtmöglich einzugrenzen (siehe Abschnitt 1.5.6 sowie S. 44 f., 77 und 83).

[656] Siehe auch *Albers*, ZRFC 2009, 150 (156); *DIIR/GDD*, Datenauswertungen und personenbezogene Datenanalyse, S. 18 ff.; *Wybitul* (o. Fußn. 500), S. 1089.

Bereitstellung eines geeigneten Softwaretools

Der Grundsatz der Datensicherheit verpflichtet zur Vertraulichkeit und Integrität der verwendeten personenbezogenen Daten in allen Phasen der Analyse. Über geeignete Verfahren zur Authentifikation ist lediglich berechtigten, auf das Datengeheimnis verpflichteten Personen Zugang zu gewähren.

Das Analysetool muss einerseits eine unverzügliche Löschung der für die weiteren Ermittlungen unbrauchbaren Daten und andererseits eine Dokumentation der generierten Verdachtsfälle gewährleisten (siehe S. 45 f., 62 und 78 f.).

Überprüfung der die Analyse rechtfertigenden Dokumentation

Vor Beginn der Datenanalyse ist sicherzustellen, dass sämtliche die Analyse rechtfertigende Gründe hinreichend dokumentiert sind. Dies umfasst eine sorgfältig durchgeführte Interessenabwägung; Risikoanalysen; Fälle, in welchen sich das Risiko zuvor realisiert hat; die bereits erfolgte Vornahme von weniger intensiven Mitteln im Rahmen des AFM (siehe Abschnitt 4.1), ggf. der Nachweis, dass diese nicht zum Erfolg geführt haben etc. (siehe S. 84 f.).

Extraktion anonymisierter bzw. pseudonymisierter Daten aus den betrieblichen Datenbeständen und Durchführung des Datenabgleichs

Auch die eigentliche Analyse ist hinsichtlich einer eventuell später durchzuführenden Rekonstruktion zu dokumentieren. Es empfiehlt sich die Anwesenheit eines Mitglieds der Arbeitnehmervertretung.

Dokumentation der Ergebnisse

Die Ergebnisse des Abgleichs sind zu dokumentieren. Hieraus kann sich der für die anschließenden Aufdeckungsmaßnahmen erforderliche Anfangsverdacht ergeben (siehe S. 62 und Abschnitt 4.3.2.2.3).

Personalisierung und Klärung der Verdachtsfälle

Spätestens in dieser Phase sind wegen der Verwendung personenbezogener Daten ein Mitglied des Betriebsrats und bestenfalls auch der Datenschutzbeauftragte hinzuzuziehen (siehe bezüglich der anschließenden Aufdeckungsmaßnahmen Abschnitt 4.3).

6
Literatur- und Quellenverzeichnis

Albers, Felicitas G. (2009 a): Compliance der Compliance – Elektronische Analyseverfahren personenbezogener Daten zur Prävention und Aufdeckung geschäftsschädigender Handlungen im Unternehmen, in: Forschungsberichte des Fachbereichs Wirtschaft der Fachhochschule Düsseldorf (Hrsg.), Ausgabe 6, März, http://fhdd.opus.hbz-nrw.de/volltexte/2009/508/ (Stand: 27.04.2010).

– (2009 b): Compliance elektronischer Analyseverfahren personenbezogener Daten – Zielkonflikt zwischen berechtigtem Analyseinteresse und informationeller Selbstbestimmung, ZRFC 4, 150-156.

Albrecht, Florian (2009): Datenschutz im Arbeitsverhältnis: Die Neuregelung des § 32 BDSG, jurisPR-ITR 20, Anm. 2.

Arndt, Hans-Wolfgang*/Fetzer,* Thomas*/Scherer,* Joachim (Hrsg.) (2008): Telekommunikationsgesetz – Kommentar, Berlin (zitiert: *Bearbeiter*, in: *Arndt/Fetzer/Scherer*).

Artikel 29-Datenschutzgruppe (2001): Stellungnahme 8 zur Verarbeitung personenbezogener Daten von Beschäftigten v. 13.09.2001, WP 48.

– (2006): Stellungnahme 1 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität v. 01.02.2006, WP 117.

Aßmus, Ubbo (2009): Jahresabschlussprüfung: Datenschutzrechtliche Aspekte bei der Weitergabe von Mitarbeiterdaten, MMR 9, 599-603.

Bantleon, Ulrich/*Thomann,* Detlef/*Bühner*, Andreas (2007): Die Neufassung des IDW Prüfungsstandards: „Zur Aufdeckung von Unregelmäßigkeiten im Rahmen der Abschlussprüfung (IDW PS 210)" und dessen Auswirkungen auf die Unternehmensorganisation, DStR 44, 1978-1983.

Barton, Dirk-M. (2009): Risiko-/Compliance-Management und Arbeitnehmerdatenschutz – eine nach wie vor unbefriedigende Kollisionslage – Anmerkung zu § 32 BDSG, RDV 5, 200-204.

Berndt, Thomas*/Jeker,* Marc (2007): Fraud detection im Rahmen der Abschlussprüfung, BB 48, 2615-2621.

Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (2010): Eine Frage der Erforderlichkeit – Zwischenruf von Praktikern zum § 32 BDSG, DuD 4, 254-256.

Bierekoven, Christiane (2010): Korruptionsbekämpfung vs. Datenschutz nach der BDSG-Novelle, CR 3, 203-208.

Bisges, Marcel (2009): Rasterfahndung im Unternehmen zur Aufdeckung von Korruptionskriminalität, MMR 4, XX-XXII.

Bitkom/DIN (Hrsg.) (2009): Kompass der IT-Sicherheitsstandards – Leitfaden und Nachschlagewerk, 4. Aufl., http://www.bitkom.org/files/documents/Kompass_der_IT-Sicherheitsstandards_haftung_(2).pdf (Stand: 22.05.2010).

BKA (Hrsg.) (2009): Korruption - Bundeslagebild 2008, Pressefreie Kurzfassung, http://www.prohonore.de/BKA-Korruption-2008.pdf (Stand: 24.05.2010).

Blasche, Sebastian (2009): Die Mindestanforderungen an ein Risikofrüherkennungs- und Überwachungssystem nach § 91 Abs. 2 AktG, CCZ 2, 62-67.

Block, Ulrich (2003): Neue Regelungen zur Corporate Governance gemäß Sarbanes-Oxley Act, BKR 19, 774-787.

Bock, Dennis (2009): Strafrechtliche Aspekte der Compliance-Diskussion: § 130 OWiG als zentrale Norm der criminal Compliance, ZIS 2, 68-81.

Bohnert, Joachim (2007): Kommentar zum Ordnungswidrigkeitengesetz, 2. Aufl., München.

Brandt, Jochen (2009): Compliance – Interessenvertretung im Spannungsfeld, CuA 11, 6-9.

– (2010): Betriebsvereinbarungen als datenschutzrechtliche „Öffnungsklauseln"?, DuD 4, 213-215.

*Bundesanstalt für Finanzdienstleistungen (*Hrsg.) (2009): Mindestanforderungen an das Risikomanagement – MaRisk*,* Rundschreiben 15, http://www.bafin.de/cln_161/nn_724304/SharedDocs/Veroeffentlichungen/DE/Service/Rundschreiben/2009/rs__0915__ba__marisk.html (Stand. 03.03.2010).

Dann, Matthias*/Gastell*, Roland (2008): Geheime Mitarbeiterkontrollen: Straf- und arbeitsrechtliche Risiken bei unternehmensinterner Aufklärung, NJW 41, 2945-2949.

Däubler, Wolfgang (2002): Gläserne Belegschaften? Datenschutz in Betrieb und Dienststelle, 4. Aufl., Frankfurt am Main.

– (2010): Gläserne Belegschaften? Das Handbuch zum Arbeitnehmerdatenschutz, 5. Aufl., Frankfurt am Main.

Däubler, Wolfgang/*Klebe,* Thomas/*Wedde*, Peter/*Weichert*, Thilo (Hrsg.) (2010): Bundesdatenschutzgesetz – Kompaktkommentar zum BDSG, Frankfurt am Main (zitiert: *Bearbeiter*, in: *Däubler/Klebe/Wedde/Weichert*).

Deutsch, Markus/*Diller,* Martin (2009): Die geplante Neuregelung des Arbeitnehmerdatenschutzes in § 32 BDSG, DB 27, 1462-1465.

Deutscher Anwaltverein (2010): Stellungnahme, Nr. 2 zum Arbeitnehmerdatenschutz, http://anwaltverein.de/interessenvertretung/stellungnahmen+2 (Stand: 23.03.2010).

DIIR/GDD (Hrsg.) (2009): Datenauswertungen und personenbezogene Datenanalyse: Beispiel für den praktischen Umgang im Revisionsumfeld, http://www.diir.de/fileadmin/fachwissen/downloads/09DIIRDatenanalyseWeb.pdf (Stand: 25.05.2010).

Diller, Martin (2009): „Konten-Ausspäh-Skandal" bei der Deutschen Bahn: Wo ist das Problem?, BB 9, 438-440.

Dreier, Horst (Hrsg.) (1996): Grundgesetz – Kommentar, Bd. I, Tübingen (*zitiert*: Bearbeiter in: *Dreier*).

Epping, Volker/*Hillgruber*, Christian (2010): Beck'scher Online-Kommentar – Grundgesetz, Edition 6, Stand: 01.02.2010, München (zitiert: *Bearbeiter,* in: *BeckOK GG).*

Erbs/Kohlhaas (2009): Strafrechtliche Nebengesetze, hrsg. v. *Ambs*, Friedrich, Bd. I, 177. Aufl., München, (zitiert: *Bearbeiter*, in: *Erbs/Kohlhaas).*

Erfurth, René (2009): Der „neue" Arbeitnehmerdatenschutz im BDSG, NJOZ 34, 2914-2926.

Fetsch, Johannis (2002): Eingriffsnormen und EG-Vertrag, Tübingen.

Finanznachrichten.de (2010): Daimler zahlt in US-Korruptionsstreit 185 Mio USD – Kreise, *Kendall*, Brent (Verfasser), 24.03., http://www.finanznachrichten.de/nachrichten-2010-03/16454508-update2-daimler-zahlt-in-us-korruptionsstreit-185-mio-usd-kreise-015.htm (Stand: 24.03.2010).

Flägel, Peter (2008): Deregistrierung von „Foreign Private Issuers" in den USA., NZG 15, 576-579.

Forst, Gerrit (2009): Videoüberwachung am Arbeitsplatz und der neue § 32 BDSG, RDV 5, 204-211.

Frankfurter Allgemeine Zeitung (2010): Hohe Kosten vertreiben Telekom von Wall Street, o.V., 22.04., S. 22.

Geppert, Martin*/Piepenbrock,* Hermann-Josef*/Schütz,* Raimund u.a. (Hrsg.) (2006): Beck'scher TKG-Kommentar, 3. Aufl., München. (zitiert: *Bearbeiter*, in: *Geppert/Piepenbrock /Schütz).*

Gola/Schomerus (2010): Bearb. v. *Gola*, Peter/*Klug*, Christoph/*Körffer*, Barbara, Bundesdatenschutzgesetz – Kommentar, 10. Aufl., München.

Gola, Peter*/Wronka,* Georg (2010): Handbuch zum Arbeitnehmerdatenschutz – Rechtsfragen und Handlungshilfen unter Berücksichtigung der BDSG-Novellen, 5. Aufl., Heidelberg, München, Landsberg, Frechen, Hamburg.

Grentzenberg, Verena*/Schreibauer*, Markus*/Schuppert,* Stefan (2009): Die Datenschutz-Novelle (Teil II): Ein Überblick zum „Gesetz zur Änderung datenschutzrechtlicher Vorschriften", K&R 9, 535-543.

Hanloser, Stefan (2009): Die BDSG-Novelle II: Neuregelungen zum Kunden- und Arbeitnehmerdatenschutz, MMR 9, 594-599.

Hannich, Rolf (Hrsg.) (2008): Karlsruher Kommentar zur StPO, 6. Aufl., München (zitiert: *Bearbeiter*, in: *KK-StPO).*

Hauschka, Christoph E. (Hrsg.) (2010): Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen, 2. Aufl., München (zitiert: *Bearbeiter*, in: *Hauschka).*

Hauschka, Christoph E*./Greeve*, Gina (2007): Compliance in der Korruptionsprävention – was müssen, was sollen, was können die Unternehmen tun?, BB 4, 165-173.

Heldmann, Sebastian (2010): Betrugs- und Korruptionsbekämpfung zur Herstellung von Compliance; Arbeits- und datenschutzrechtliche Sicht, DB 22, 1235-1239.

Heise-Online (2007): Hintergrund: Bilanzskandale in den U.S.A., *Kuri*, Jürgen (Verfasser), 22.07., http://www.heise.de/newsticker/meldung/Hintergrund-Bilanzskandale-in-den-USA-64933.html (Stand: 21.02.2010).

– (2008 a): Mitarbeiter-Bespitzelung im Handel: Auch Edeka und Plus im Visier, *Ziegler*, Peter-Michael (Verfasser), 02.04., http://www.heise.de/newsticker/meldung/Mitarbeiter-Bespitzelung-im-Handel-Auch-Edeka-und-Plus-im-Visier-195390.html (Stand: 21.02.2010).

– (2008 b): Datenschutzverletzungen: Lidl fällt als Wiederholungstäter auf, *Ziegler*, Peter-Michael (Verfasser), 26.03., http://www.heise.de/newsticker/meldung/Datenschutzverletzungen-Lidl-faellt-als-Wiederholungstaeter-auf-192822.html (Stand: 21.02.2010).

– (2008 c): Nach neuer Telekom-Panne: Kritik an Konzernführung wächst, *Murphy*, Martin (Verfasser), 13.10, http://www.heise.de/newsticker/meldung/Nach-neuer-Telekom-Datenpanne-Kritik-an-Konzernfuehrung-waechst-210873.html (Stand: 21.02.2010).

– (2009 a): Datenschutzaffäre im Machtzirkel der Deutschen Bank, *Ziegler*, Peter-Michael (Verfasser), 26.05., http://www.heise.de/newsticker/meldung/Datenschutz-Affaere-im-Machtzirkel-der-Deutschen-Bank-220081.html (Stand: 21.02.2010).

– (2009 b): Bericht: Datenschützer wirft Bahn Gesetzesverstöße vor, *Wilkens*, Andreas (Verfasser), 09.04., http://www.heise.de/newsticker/meldung/Bericht-Datenschuetzer-wirft-Bahn-Gesetzesverstoesse-vor-212222.html (Stand: 21.02.2010).

Hilty, Reto M./*Drexl,* Josef/*Nordemann*, Wilhelm (Hrsg.) (2009): Schutz von Kreativität und Wettbewerb. Festschrift für Ulrich Loewenheim zum 75. Geburtstag, München (zitiert: *Bearbeiter*, in: *Hilty/Drexl/Nordemann*).

Hopt, Klaus J./*Merkt*, Hanno/*Baumbach*, Adolf (Hrsg.) (2010): Handelsgesetzbuch 34. Aufl., München (zitiert: *Bearbeiter* in: *Baumbach/Hopt).*

*Hüffer,*Uwe (Hrsg.) (2008): Aktiengesetz, 8. Aufl., München.

Institut der Wirtschaftsprüfer (Hrsg.) (2002): IDW Prüfungsstandard: Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB – IDW PS 340, Stand: 11.09

Kamp, Meike/*Körffer*, Barbara (2010): Auswirkungen des § 32 BDSG auf die Aufgabenerfüllung und die strafrechtliche Verantwortung des Compliance Officers, RDV 2, 72-76.

Karg, Moritz (2009): Compliance und Datenschutz, CuA 11, 13-15.

Kiethe, Kurt (2004): Strafrechtlicher Anlegerschutz durch § 400 I Nr. 1 AktG – Zugleich Besprechung von LG München I, Urteil vom 8. 4. 2003 – 4 KLs 305 Js 52373/00 (EM.TV), NStZ 2, 73-77.

Klengel, Detlef/*Mückenberger*, Ole (2009): Internal Investigations – typische Rechts- und Praxisprobleme unternehmensinterner Ermittlungen, CCZ 3, 81-87.

Klindt, Thomas (2006): Nicht-börsliches Compliance-Management als zukünftige Aufgabe der Inhouse-Juristen, NJW 47, 3999-3400.

Knapp, Eckhard (2005): Interne Revision und Corporate Governance – Aufgaben und Entwicklungen für die Überwachung, Berlin.

Kock, Martin*/Francke*, Julia (2009): Mitarbeiterkontrolle durch systematischen Datenabgleich zur Korruptionsbekämpfung, NZA 12, 646-651.

Koller, Ingo*/Roth*, Wulf-Henning*/Morck*, Winfried (Hrsg.) (2007): Handelsgesetzbuch, 6. Aufl., München (zitiert: *Bearbeiter*, in: *Koller/Roth/Morck)*

Kort, Michael (2008): Verhaltensstandardisierung durch Corporate Compliance, NZG 3, 81-86,

KPMG (2006): Anti Fraud Management – Best Practice der Prävention gegen Wirtschaftskriminalität, http://www.kpmg.ch/docs/20060801_Anti_Fraud_Management_Best_Practice_der_Praevention_gegen_Wirtschaftskriminalitaet_deutsch.pdf (Stand: 25.05.2010).

– (2010): Wirtschaftskriminalität in Deutschland – Fokus Mittelstand, http://www.kpmg.de/docs/20091220_Wirtschaftskriminalitaet.pdf (Stand: 25.05.2010).

Kramer, Philipp*/Gliss*, Hans (2010): Arbeitnehmerdatenschutz: Abgleich von Kontodaten für zulässig erklärt, DSB 4, 13-14.

Lanfermann, Georg*/Röhricht*, Victoria (2009): Pflichten des Prüfungsausschusses nach dem BilMoG, BB 17, 887-891.

Liebscher, Thomas (2007): BGH – Haftung des fakultativen Aufsichtsrates einer GmbH bei sorgfaltswidriger Zustimmung zu nachteiligen Geschäften – Anmerkung zu BGH, Urteil vom 11.12.2006 – II ZR 243/05, LMK 4, 220409.

Longino, Marcus (2008): Haftung des Emittenten für fehlerhafte Informationen, DStR 43, 2068-2075.

Mahnhold, Thilo (2008): „Global Whistle" oder „deutsche Pfeife" – Whistleblowing-Systeme im Juridiktionskonflikt, NZA 13, 737-743.

Meier-Greve, Daniel (2009): Vorstandshaftung wegen mangelhafter Corporate Compliance, BB 48, 2555-2560.

Mengel, Anja (2009): Compliance und Arbeitsrecht – Implementierung, Durchsetzung, Organisation, München.

Mengel, Anja*/Hagemeister*, Volker (2007): Compliance und arbeitsrechtliche Implementierung im Unternehmen, BB 25, 1386-1393.

Mengel, Anja*/Ullrich*, Thilo (2006): Arbeitsrechtliche Aspekte unternehmensinterner Investigations, NZA 5, 240-246.

Menzies, Christof (Hrsg.) (2006), Sarbanes-Oxley und Corporate Compliance – Nachhaltigkeit, Optimierung, Integration, Stuttgart.

Möllers, Thomas M. J. (2008): Konkrete Kausalität, Preiskausalität und uferlose Haftungsausdehnung – ComROAD I – VIII, NZG 11, 413-416.

Müller-Glöge, Rudi/*Preis*, Ulrich/*Schmidt*, Ingrid (Hrsg.) (2010): Erfurter Kommentar zum Arbeitsrecht, 10. Aufl., München (zitiert: *Bearbeiter*, in: *ErfKomm).*

Münchner Kommentar zum Aktiengesetz (2008): Hrsg. v. *Goette*, Wulf/*Habersack*, Mathias, Bd. II, 3. Aufl., München (zitiert: *Bearbeiter*, in: *MünchKomm-AktG).*

Münchner Kommentar zum Bürgerlichen Gesetzbuch (2009): Hrsg. v. *Henssler*, Martin, Bd. IV, 5. Aufl., München (zitiert: *Bearbeiter*, in: *MünchKomm-BGB).*

Münchner Kommentar zum Handelsgesetzbuch (2008): Hrsg. *v. Schmidt,* Karsten, Bd. IV, 2. Aufl., München (zitiert: *Bearbeiter*, in: *MünchKomm-HGB).*

Münchner Kommentar zum Strafgesetzbuch (2005): Bearb. v. *Bosch,* Nikolaus/*Classen,* Dieter/*Erb,* Volker u.a., Bd. II/II, München, (zitiert: *Bearbeiter*, in: *MünchKomm-StGB).*

Nicklisch, Anette Christina (2007): Die Auswirkungen des Sarbanes-Oxley Act auf die deutsche Corporate Governance – ein Beitrag zur Amerikanisierung des deutschen Aktienwesens, Berlin.

Odenthal, Roger (2005), Kriminalität am Arbeitsplatz – Korruption und Unterschlagung durch Mitarbeiter erkennen und verhindern, Wiesbaden.

Olbers, Lucie Anne Mary (2010): Korruptionsbekämpfung durch die Weltbank – Datenschutzrechtliche Aspekte der Kooperation eines betroffenen Unternehmens, BB 15, 844-848.

Palandt (2007): Kommentar zum Bürgerlichen Gesetzbuch, bearb. v. *Bassenge,* Peter/*Brudermüller*, Gerd/*Diederichsen*, Uwe u.a., 67. Aufl., München (zitiert: *Bearbeiter*, in: *Palandt,* 67. Aufl.)

– (2010): dies., 69. Aufl., München (zitiert: *Bearbeiter*, in: *Palandt,* 69. Aufl.).

Park, Tido (Hrsg.) (2008): Kapitalmarkstrafrecht – Handkommentar, Teil 4, T1, Aufl. 2, Baden-Baden (zitiert: *Bearbeiter*, in: *Park).*

PCAOB (Hrsg.) (2007): Auditing Standard No. 5 – An audit of internal control over financial reporting that is integrated with an audit of financial statements, 15.11., http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5.aspx#wrappingup (Stand*:* 11.03.2010).

Pfeiffer, Gerd (Hrsg.) (2005): Strafprozessordnung – Kommentar, München.

Pieroth, Bodo/*Schlink*, Bernhard (2006): Grundrechte – Staatsrecht II, 22. Aufl., Heidelberg.

Polenz, Sven (2009): Fehlverhaltenskontrolle am Arbeitsplatz, DuD 9, 561-563.

Preußner, Joachim (2008): Risikomanagement und Compliance in der aktienrechtlichen Verantwortung des Aufsichtsrates unter Berücksichtigung des Gesetzes zur Modernisierung des Bilanzrechts, NZG 15, 574-576.

PWC/Hochschule Pforzheim (2009): Wirtschaftskriminalität – Eine Analyse der Motivstrukturen, http://www.pwc.de/fileserver/RepositoryItem/Wirtschaftskriminalitaet_Feb09.pdf?itemId=9112227 (Stand: 25.05.2010).

PWC/Martin Luther Universität Halle-Wittenberg (2007): Wirtschaftskriminalität – Sicherheitslage der deutschen Wirtschaft, http://www.pwc.de/fileserver/RepositoryItem/studie_wikri_2007.pdf?itemId=3169192 (Stand: 25.05.2010).

– (2009): Wirtschaftskriminalität – Sicherheitslage in deutschen Großunternehmen, http://www.pwc.de/fileserver/RepositoryItem/Studie-Wirtschaftskriminal-09.pdf?itemId=13277911 (Stand: 25.05.2010).

Richardi, Reinhard (Hrsg.) (2010): Betriebsverfassungsgesetz mit Wahlordnung – Kommentar, 12. Aufl., München (zitiert: *Bearbeiter*, in: *Richardi).*

Richardi, Reinhard/*Wlotzke*, Otfried (Hrsg.)(2000): Münchner Handbuch zum Arbeitsrecht, 2. Aufl., München (zitiert: *Bearbeiter*, in: *Richardi/Wlotzke).*

Rolfs, Christian/*Giesen,* Richard/*Kreikebohm*, Ralf u.a. (Hrsg.) (2009):Beck'scher Onlinekommentar zum Arbeitsrecht, Stand: 01.12., Edition 14, München (zitiert*: Bearbeiter*, in: *Rolfs/Giesen/Kreikebohm).*

Romeike, Franz (Hrsg.) (2008): Rechtliche Grundlagen des Risikomanagements – Haftungs- und Strafvermeidung für Corporate Compliance, Berlin (zitiert: *Bearbeiter*, in: *Romeike).*

Russenberger, Daniel (2007): Einhaltung der Anforderungen aus dem Sarbanes-Oxley Act mit Hilfe der Standards ISO/IEC 27001 & 27002, Diplomarbeit, http://www.russenberger.com/uni/SOX%20and%20ISO%202700x%20-%20public%20version.pdf (Stand: 15.03.2010).

Salvenmoser; Steffen/*Hauschka*, Christopf E. (2010): Korruption, Datenschutz und Compliance, NJW 6, 331-335.

Schaar, Peter (2009 a): Pressemitteilung, http://www.bfdi.bund.de/DE/Themen/Arbeit/Arbeitnehmerdatenschutz/Artikel/ArbeitnehmerDSAb010909.html?nn=647266 (Stand: 19.03.2010*).*

– (2009 b) in: *Schumacher*, Harald: Korruption – Pendel am Anschlag, Interview mit der Zeitschrift WirtschaftsWoche v. 29.08.2009 http://www.wiwo.de/unternehmen-maerkte/pendel-am-anschlag-406957/ (Stand: 26.03.2010).

Schmidl, Michael (2007): Die Subsidiarität der Einwilligung im Arbeitsverhältnis, DuD 10, 756-761.

Schmidt, Bernd (2009 a): Arbeitnehmerdatenschutz gemäß § 32 BDSG – Eine Neuregelung (fast) ohne Veränderung der Rechtslage, RDV 5, 193-200.

– (2009 b): Vertrauen ist gut, Compliance ist besser! – Anforderungen an die Datenverarbeitung im Rahmen der Compliance-Überwachung, BB 24, 1295-1299.

– (2010): Beschäftigtendatenschutz in § 32 BDSG – Perspektiven einer vorläufigen Regelung, DuD 4, 207-212.

Schneider, Uwe H. (2008): Compliance im Konzern, NZG 34, 1321-1326.

Senge, Lothar (2006): Karlsruher Kommentar zum Ordnungswidrigkeitengesetz, 3. Aufl., München (zitiert: *Bearbeiter*, in: *Senge).*

Spahlinger, Andreas*/Wegen*, Gerhard (Hrsg.) (2005): Internationales Gesellschaftsrecht in der Praxis – Kollisions- und Sachrecht wesentlicher Fälle mit Auslandsberührung, München *(*zitiert: *Bearbeiter*, in: *Spahlinger/Wegen).*

Spindler, Gerald*/Schuster*, Fabian (Hrsg.) (2008): Recht der elektronischen Medien – Kommentar, München (zitiert: *Bearbeiter*, in: *Spindler/Schuster).*

*Staudinger (*2002): Kommentar zum Bürgerlichen Gesetzbuch, 13. Bearb., Berlin (zitiert: *Bearbeiter*, in: *Staudinger).*

Steinkühler, Bernhard (2009): BB-Forum: Kein Datenproblem bei der Deutschen Bahn AG? Mitnichten!, BB 24, 1295-1295.

Sueddeutsche.de (2010): Urteil gegen Deutsche Bahn: Zu Unrecht gefeuert, *Ott,* Klaus*/Kuhr,* Daniela (Verfasser), 08.03., http://www.sueddeutsche.de/wirtschaft/urteil-gegen-deutsche-bahn-zu-unrecht-gefeuert-1.13522 (Stand: 18.04.2010).

Thüsing, Gregor (2009): Datenschutz im Arbeitsverhältnis – Kritische Gedanken zum neuen § 32 BDSG, NZA 16, 865-870.

Transparency International Deutschland e.V. (2009): Pressemitteilung v. 30.06., http://www.transparency.de/09-06-30_Datenschutz.1438.0.html (Stand: 15.12.2009).

Trittin, Wolfgang/*Fischer*, Esther D. (2009): Datenschutz und Mitbestimmung – Konzernweite Personaldatenverarbeitung und die Zuständigkeit der Arbeitnehmervertretung, NZA 7, 343-346.

Vetter, Eberhard (2008): Der Deutsche Corporate Governance Kodex nur ein zahnloser Tiger? – Zur Bedeutung von § 161 AktG für Beschlüsse der Hauptversammlung, NZG 4, 121-126,

Vogel, Florian/*Glas*, Vera (2009): Datenschutzrechtliche Probleme unternehmensinterner Ermittlungen, DB 33, 1747-1754.

Wabnitz, Heinz-Bernd/*Janovsky*, Thomas (Hrsg.) (2007): Handbuch des Wirtschafts- und Steuerstrafrechts, 3. Aufl., München (zitiert: *Bearbeiter*, in: *Wabnitz/Janovsky).*

Wagenhofer, Alfred (Hrsg.) (2009), Controlling und Corporate Governance-Anforderungen – Konzepte, Maßnahmen, Umsetzungen, Berlin (zitiert: *Bearbeiter*, in: *Wagenhofer).*

Wecker, Gregor/*Van Laak,* Hendrik (Hrsg.) (2009): Compliance in der Unternehmerpraxis – Grundlagen, Organisation und Umsetzung, 2. Aufl., Wiesbaden (zitiert: *Bearbeiter*, in: *Wecker/Van Laak).*

Wellhörner, Astrid/*Beyers*, Philipp (2009): Datenschutz im Betrieb – Alltägliche Herausforderung für den Arbeitgeber?! BB 43, 2310-2316.

Wolf, Klaus (2003): Qualitative Verbesserung der Finanzberichterstattung – Spezifische Anforderungen des Sarbanes-Oxley Act, BC 12, 268-272.

– (2009): Zur Anforderung eines internen Kontroll- und Risikomanagementsystems im Hinblick auf den (Konzern-) Rechnungslegungsprozess gemäß BilMoG, DStR 18, 920-925.

Wybitul, Tim (2009): Das neune Bundesdatenschutzgesetz: Verschärfte Regeln für Compliance und interne Ermittlungen, BB 30, 1582-1585.

– (2010): Wie viel Arbeitnehmerdatenschutz ist „erforderlich"?, BB 18, 1085-1089.

Zikesch, Phillip /*Reimer*, Bernd (2010): Datenschutz und präventive Korruptionsbekämpfung – kein Zielkonflikt, DuD 2, 96-98

Zimmer, Mark/*Stetter*, Sabine (2006): Korruption und Arbeitsrecht, BB 26, 1445-1452.