COMPLIANCE UND DATENSCHUTZ

DER FALL DEUTSCHE BAHN AG

von

cand. Wirtsch.-Ing. Christina Katherina Tobescu

Ass. jur. Stefan Holzner, LL.M.

Die hier vorgelegte Untersuchung beruht auf eigenen Recherchen der Bearbeiter und zwar nach bestem Wissen und Gewissen. Der Fall Deutsch Bahn AG ist nur exemplarisch, um das Grundproblem Compliance und Datenschutz aufzuarbeiten.

Inhaltsverzeichnis

LITERATURVERZEICHNIS

Adam, Dirk: Die Begrenzung der Aufsichtspflichten in der Vorschrift des § 130 OWiG, in: Wistra 2003, S. 285-292.

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

Beckschulze, Martin: Internet-, Intranet- und E-Mail-Einsatz am Arbeitsplatz, in: BB 2007, S. 1526-1535.

Beckschulze, Martin/ Henkel, Wolfram: Der Einfluss des Internets auf das Arbeitsrecht, in: DB 2001, S. 1491-1506.

Bergmann, Lutz/ Möhrle, Roland/ Herb, Armin: Datenschutzrecht, Loseblattsammlung, Boorberg Verlag, Stuttgart.

Biermann, Kai: Nur Ordnungswidrigkeiten, in: Zeit Online, 04.02.2009, abrufbar unter http://www.zeit.de/online/2009/06/bahn-datenskandal-folgen (Stand: 01.09.2009).

Bisges, Marcel: Rasterfahndung im Unternehmen zur Aufdeckung von Korruptionskriminalität, in: MMR 2009, Heft 4, S. XX-XXII.

Brouwer, Tobias: Compliance im Wirtschaftsverband, in: CCZ 2009, S. 161-168.

Bürkle, Jürgen: Corporate Compliance als Standard guter Unternehmensführung des Deutschen Corporate Governance Kodex, in: BB 2007, S. 1797-1801.

Bürkle, Jürgen: Corporate Compliance – Pflicht oder Kür für den Vorstand der AG? In: BB 2005, S. 565-570.

Bürkle, Jürgen: Weitergabe von Informationen über Fehlverhalten in Unternehmen (Whistleblowing) und Steuerung auftretender Probleme durch ein Compliance-System, in: DB 2004, S. 2158-2161.

Bürkle, Jürgen: Compliance in Versicherungsunternehmen: Ja, aber wie?, in: VW 2004, S. 830-833.

Bussmann, Kai-D./ Matschke, Sebastian: Die Zukunft der unternehmerischen Haftung bei Compliance-Verstößen, in: CCZ 2009, S. 132-138.

Campos Nave, José A./ Bonenberger, Saskia: Korruptionsaffären, Corporate Compliance und Sofortmaßnahmen für den Krisenfall, in: BB 2008, 734-741.

Däubler, Wolfgang: Internet und Arbeitsrecht, 3. Auflage 2004, Bund-Verlag, Frankfurt.

Däubler, Wolfgang/ Klebe, Thomas/ Wedde, Peter/ Weichert, Thilo (Hrsg.): Bundesdatenschutzgesetz, Basiskommentar zum BDSG, 2. Auflage 2007, Bund-Verlag, Frankfurt [zitiert: *Bearbeiter*, in: Basiskommentar zum BDSG].

Deutsche Bahn AG: Kurzprofil Deutsche Bahn AG, abrufbar unter: http://www.deutschebahn.com/site/bahn/de/unternehmen/presse/themendienst/konzern/bilanz__pk__2008.html (Stand: 01.09.2009).

Deutsche Bahn AG: Zwischenbericht Überprüfung der Ordnungsmäßigkeit von-Maßnahmen der Korruptionsbekämpfung in den Jahren 1998-2007, 2009, abrufbar unter: http://www.deutschebahn.com/site/shared/de/dateianhaenge/presse/zwischenbericht__090210.pdf (Stand: 01.09.2009).

Deutsche Bahn AG: Compliance Bericht der Deutschen Bahn (2006/2007), abrufbar unter: http://www.deutschebahn.com/site/shared/de/dateianhaenge/berichte/compliance__bericht06__07.pdf (Stand: 01.09.2009).

Deutsche Bahn AG (2005): Korruptionsbericht 2005. Erfolge konsequenter Compliance-Arbeit, abrufbar unter: http://www.deutschebahn.com/site/shared/de/dateianhaenge/berichte/DB_Korruptionsbericht_2005.pdf (Stand: 01.06.2009).

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

Diller, Martin: "Konten-Ausspäh-Skandal" bei der Deutschen Bahn: Wo ist das Problem?, in: BB 2009, S. 438-440.

Dünwell, Franz Josef (Hrsg.): Betriebsverfassungsgesetz, Handkommentar, 2. Auflage 2006, Baden-Baden [zitiert: *Bearbeiter*, in: Dünwell, Betriebsverfassungsgesetz Handkommentar].

Erfurter Kommentar zum Arbeitsrecht, Hrsg. v. Müller-Glöge, Rudi / Preis, Ulrich / Schmidt, Ingrid, 10. Aufl. 2010, Beck, München [zitiert: *Bearbeiter*, in: Erfurter Kommentar zum Arbeitsrecht].

Fitting, Karl/ Engels, Gerd/ Schmitdt, Ingrid/ Trebinger, Yvone/ Linsemaier, Wolfgang: Betriebsverfassungsgesetz, Handkommentar, 24. Aufl. 2008, Franz Vahlen Verlag, München.

Fleischer, Holger: Vorstandsverantwortlichkeit und Fehlverhalten von Unternehmensangehörigen - Von der Einzelüberwachung zur Errichtung einer Compliance-Organisation, in: AG 2003, S. 291-300.

Gliss, Hans/ Kramer, Philipp: Mitarbeiter kontrollieren, in: Personal 2009, S. 51-54.

Gola, Peter: Datenschutz und Multimedia am Arbeitsplatz, 2. Aufl. 2008, Datakontext, Frechen.

Gola, Peter/ Schomerus, Rudolf: Bundesdatenschutzgesetz, Kommentar, 9. Aufl. 2007, Beck, München.

Gola, Peter/ Klug, Christoph: Die Entwicklung des Datenschutzrechts in den Jahren 2008/2009, in: NJW 2009, S. 2577-2583.

Gola, Peter/ Wronka, Georg: Handbuch zum Arbeitnehmerdatenschutz. Rechtsfragen und Handlungshilfen für die betriebliche Praxis, 4. Aufl. 2008, Datakontext, Frechen.

Grosjean, Sascha: Überwachung von Arbeitnehmern – Befugnisse des Arbeitgebers und mögliche Beweisverwertungsverbote, in: DB 2003, S. 2650-2654.

Grundei, Jens/ Talaulicar, Till: Corporate Compliance, in: WiSt 2009, S. 73-77.

Hampel, Volker: Handlungsempfehlungen beim Datenabgleich zur Aufdeckung wirtschaftskrimineller Handlungen durch die Interne Revision, in: ZIR 2009, S. 99-102.

Hauschka, Christoph E. (Hrsg.): Corporate Compliance: Handbuch der Haftungsvermeidung im Unternehmen, 1. Auflage 2007, Beck, München.

Hauschka, Christoph E.: Die Voraussetzungen für ein effektives Compliance System i. S. von § 317 Abs. 4 HGB, in: DB 2006, S. 1143-1146.

Hauschka, Christoph E.: Corporate Compliance - Unternehmensorganisatorische Ansätze zur Erfüllung der Pflichten von Vorständen und Geschäftsführern, in: AG 2004, S. 461-475.

Hauschka, Christoph E.: Compliance am Beispiel der Korruptionsbekämpfung. Eine Erwiderung aus der Praxis auf Uwe H. Schneiders Vorschläge, ZIP 2003, 645, in: ZIP 2004, S. 877-883.

Hauschka, Christoph E.: Compliance, Compliance-Manager, Compliance-Programme: Eine geeignete Reaktion auf gestiegene Haftungsrisiken für Unternehmen und Management?, in: NJW 2004, S. 257-261.

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

Illing, Diana/ Umnuß, Karsten: Die arbeitsrechtliche Stellung des Compliance Managers – insbesondere Weisungsunterworfenheit und Reportingpflichten, in: CCZ 2009, S. 1-8.

Karlsruher Kommentar zum Gesetz über Ordnungswidrigkeiten: Hrsg. v. Senge, Lothar, 3. Aufl. 2006, Beck, München [zitiert: *Bearbeiter*, in: KK-OWiG].

Kiethe, Kurt: Vermeidung der Haftung von geschäftsführenden Organen durch Corporate Compliance, in: GmbHR, 2007, S. 393-400.

Klengel, Detlef, W./ Mückenberger, Ole: Internal Investigations – typische Rechts- und Praxisprobleme unternehmensinterner Ermittlungen, in: CCZ 2009, S. 81-87.

Kock, Martin/ Franke, Julia: Mitarbeiterkontrolle durch systematischen Datenabgleich zur Korruptionsbekämpfung, in: NZA 2009, S. 646-651.

Kollmer, Franz (Hrsg.)*:* Arbeitsschutzgesetze, 1. Aufl. 2005, München [zitiert: *Bearbeiter*, in: Kollmer, Arbeitsschutzgesetze].

Kort, Michael: Verhaltensstandardisierung durch Corporate Compliance, in: NZG 2008, S. 81-86.

Lampert, Thomas: Gestiegenes Unternehmensrisiko Kartellrecht – Risikoreduzierung durch Competition-Compliance-Programme, in: BB 2002, S. 2237-2243.

Lelley, Jan Tibor: Ein Arbeitnehmerdatenschutzgesetz – zwingend notwendig oder Hyperaktivismus?, in: GmbHR 2009, R 209-R210.

Leyendecker, Hans: Korruption als Vorwand, in: Sueddeutsche.de v. 04.06.2009, abrufbar unter: http://www.sueddeutsche.de/wirtschaft/350/470894/text/ (Stand: 17. 08. 2009).

Liese, Jens: Much Adoe About Nothing? Oder: Ist der Vorstand einer Aktiengesellschaft verpflichtet, eine Compliance-Organisation zu implementieren? In: BB-Special zu Heft 25, 2008, S. 17-22.

Lösler, Thomas: Spannungen zwischen der Effizienz der internen Compliance und möglichen Reporting-Pflichten des Compliance Officers, in: WM 2007, S. 676-683.

Lösler, Thomas: Das moderne Verständnis von Compliance im Finanzmarktrecht, in: NZG 2005, S. 104-108.

Löwisch, Manfred: Fernmeldegeheimnis und Datenschutz bei der Mitarbeiterkontrolle, in: DB 2009, S. 2782-2787.

Lücke, Oliver: Vorstand der AG, in: Beck´sches Mandatshandbuch, 2004, Beck, München.

Lunk, Stefan: Prozessuale Verwertungsverbote im Arbeitsrecht, in: NZA 2009, S. 457-464.

Mahnhold, Thilo: „Global Whistle“ oder „deutsche Pfeife“ – Whistleblowing-Systeme im Jurisdiktionskonflikt, in: NZA 2008, S. 737-743.

Maurer, Hartmut: Staatsrecht 1, 5. Aufl. 2007, Beck, München.

Mengel, Anja: Compliance und Arbeitsrecht, 2009, Beck, München.

Mengel, Anja: Compliance und arbeitsrechtliche Implementierung im Unternehmen, in: BB 2007, S. 1386-1393.

Mengel, Anja: Kontrolle der E-mail- und Internetkommunikation am Arbeitsplatz. Wege durch einen juristischen Irrgarten, in: BB 2004, S. 2014-2012.

Mengel, Anja/ Ulrich, Thilo: „Mitarbeiter-Screenings“ zur internen Korruptionsbekämpfung, in: ArbRB 2009, S. 110-113.

Mengel, Anja/ Ulrich, Thilo: Arbeitsrechtliche Aspekte unternehmensinterner Investigations, in: NZA 2006, S. 240-246.

Menzies, Christof/ Tüller, Jörg/ Martin, Alan: Compliance Mangement, in: ZFO 2008, S. 136-142.

Moos, Flemming: Datenschutz ist, was man daraus macht, in: BB 2009 Heft 34, M1.

Münchener Kommentar zum Aktiengesetz: Hrsg. v. Kropff, Bruno/ Semler, Johannes, 3. Aufl. 2008, Beck, München [zitiert: *Bearbeiter*, in: MK-AktG].

Oberwetter, Christian: Überwachung und Ausspähung am Arbeitsplatz – alles ohne Entschädigung?, in: NZA 2009, S. 1120-1123.

Ott, Klaus: EX-Manager kommen mit Bewährung davon – Siemens muss 38 Millionen Euro zahlen, in: Sueddeutsche.de v. 14.05.2007, Online: http://www.sueddeutsche.de/wirtschaft/78/348913/text/ (Stand: 24.08.2009).

Pahlke, Anne-Kathrin: Risikomanagement nach KonTraG – Überwachungspflichten und Haftungsrisiken für den Aufsichtsrat, in: NJW 2002, S. 1680-1688.

Pampel, Gunnar: Die Bedeutung von Compliance-Programmen im Kartellordnungswidrigkeitenrecht, in: BB 2007, S. 1636-1640.

Pieroth, Bodo/ Schlink, Bernhard: Grundrechte Staatsrecht 2, 23. Aufl. 2007, C.F. Müller, Heidelberg.

Puppe, Ingeborg: Was ist Anstiftung? – Zugleich eine Besprechung von BGH, Urteil vom 11.10.2005 – 1 StR 250/ 05, in: NStZ 2006, S. 424-426.

Richardi, Reinhard (Hrsg.): Betriebsverfassungsgesetz, 11. Aufl. 2008, Beck, München.

Ringleb, Henrik-Michael/ Kremer, Thomas/; Lutter, Marcus/; v. Werder, Alex (2008): Kommentar zum Deutschen Corporate Governance Kodex, 3. Aufl. 2008, Beck, München.

Rodewald, Jörg/ Unger, Ulrike: Kommunikation und Krisenmanagement im Gefüge der Corporate Compliance-Organisation, in: BB 2007, S. 1629-1635.

Rodewald, Jörg/ Unger, Ulrike: Corporate Compliance – Organisatorische Vorkehrungen zur Vermeidung von Haftungsfällen der Geschäftsleitung, in: BB 2006, S. 113-117.

Röh, Lars: Compliance nach der MiFID - zwischen höherer Effizienz und mehr Bürokratie, in: BB 2008, S. 398-410.

Roßnagel, Alexander (Hrsg.), Datenschutz in der betrieblichen Datenverarbeitung, in: Handbuch Datenschutzrecht, 2002, Beck, München [zitiert: *Bearbeiter*, in Roßnagel, Handbuch Datenschutzrecht].

Sachs, Michael (Hrsg.): Grundgesetz, Kommentar, 5. Aufl. 2009, Beck, München [zitiert: Bearbeiter, in: Sachs, Grundgesetz].

Schaefer, Torsten: Rasterfahndung „light“ – Abfrage von Kreditkartendaten, in: NJW-Spezial 2009, S. 280.

Schaffland, Hans-Jürgen/ Wiltfang, Noeme: Bundesdatenschutzgesetz Kommentar, Loseblattsammlung, Erich Schmidt Verlag, Berlin.

Scherp, Dirk/ Stief, Alexander: Compliance – Sonderuntersuchungen in Banken und der Datenschutz, in: BKR 2009, S. 404-410.

Schmidt, Bernd: Vertrauen ist gut, Compliance ist besser! – Anforderungen an die Datenverarbeitung im Rahmen der Compliance-Überwachung, in: BB 2009, S. 1295-1299.

ders.: Arbeitnehmerdatenschutz gemäß § 32 BDSG – Eine Neuregelung (fast) ohne Veränderung der Rechtslage, in: RDV 2009, 193-200.

Schnalbel, Christopf: Das „Mikado-Prinzip“, in: DuD 2007, S. 426-430.

Schneider, Jochen: Handbuch des EDV-Rechts, 4. Auflage 2009, Otto Schmidt Verlag, Köln.

Schneider, Uwe H.: Compliance im Konzern, in: NZG 2009, 1321.

Schneider, Uwe H./ Nowak, Claudia: Sind die Einrichtung einer Whistleblowing-Stelle und der Schutz des Whistleblowers Teil guter Corporate Compliance?, in: Festschrift für Peter Kreutz, Hrsg. v. Hönn/ Oetker/ Raab, S. 855-865, 2010, Luchterhand.

Schneider, Uwe H./ Schneider, Sven H.: Konzern-Compliance als Aufgabe der Konzernleitung, in: ZIP 2007, S. 2061-2065.

Schneider, Uwe H.: Compliance als Aufgabe der Unternehmensleitung, in: ZIP 2003, S. 645-650.

Schwenn, Kerstin: Langsam zog sich die Schlinge zu, in: FAZ v. 31. 03. 2009, S. 3.

Sendler, Horst: Unmittelbare Drittwirkung der Grundrechte durch die Hintertür?, in: NJW 1994, 709.

Simitis, Spiros (Hrsg.): Kommentar zum Datenschutzgesetz, 6. Aufl. 2006, Nomos Verlagsgesellschaft, Baden-Baden [zitiert: *Bearbeiter*, in: Simitis, Bundesdatenschutzgesetz].

Spindler, Gerald: Compliance in der multinationalen Bankengruppe, in: WM 2008, S. 905-918.

Steinkühler, Bernhard: BB-Forum: Kein Datenproblem bei der Deutschen Bahn? Mitnichten!, in: BB 2009, S. 1294-1295.

Thüsing, Gregor: Datenschutz im Arbeitsverhältnis – Kritische Gedanken zum neuen § 32 BDSG, in: NZA 2009, S. 865-870.

Vogel, Florian/ Glas, Vera: Datenschutzrechtliche Probleme unternehmensinterner Ermittlungen, in: DB 2009, S. 1747-1754.

v. Pelchrzim, Gero (2009): Whistleblowing und der strafrechtliche Geheimnisschutz nach § 17 UWG, in: CCZ 2009, S. 25-29.

v. Steinau-Steinrück, Robert/ Glanz, Peter: Grenzen der Mitarbeiterüberwachung, in: NJW-Spezial 2008, S. 402-403.

Vogt, Volker: Compliance und Investigations – Zehn Fragen aus Sicht der arbeitsrechtlichen Praxis, in: NJOZ 2009, 4206.

Wagner, Jens: „Internal Investigations“ und ihre Verankerung im Recht der AG, in: CCZ 2009, S. 8-17.

Wybitul, Tim: Das neue Bundesdatenschutzgesetz: Verschärfte Regeln für Compliance und interne Ermittlungen, in: BB 2009, S. 1582-1585.

ABKÜRZUNGSVERZEICHNIS

Abs.	Absatz
AG	Die Aktiengesellschaft (Zeitschrift)
AktG	Aktiengesetz
AP	Arbeitsrechtliche Praxis (Zeitschrift)
ArbRB	Der Arbeits-Rechts-Berater (Zeitschrift)
AuA	Arbeit und Arbeitsrecht (Zeitschrift)
Aufl.	Auflage
BAG	Bundesarbeitsgericht
BB	Betriebsberater (Zeitschrift)
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
Beschl.	Beschluss
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
CCZ	Corporate Compliance Zeitschrift
DB	Der Betrieb (Zeitschrift)
DUD	Datenschutz und Datensicherheit (Zeitschrift)
FAZ	Frankfurter Allgemeine Zeitung
GDL	Gewerkschaft Deutscher Lokomotivführer
GG	Grundgesetz
GmbHR	GmbH Rundschau (Zeitschrift)
HGB	Handelsgesetzbuch

Hrsg.	Herausgeber
Kap.	Kapitel
MMR	Multimedia und Recht (Zeitschrift)
NJOZ	Neue juristische Online Zeitschrift
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NStZ	Neue Zeitschrift für Strafrecht
NZA	Neue Zeitschrift für Arbeitsrecht
NZG	Neue Zeitschrift für Gesellschaftsrecht
o. Fußn.	obere Fußnote
OWiG	Gesetz über Ordnungswidrigkeiten
Rn.	Randnummer
StGB	Strafgesetzbuch
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
Urt.	Urteil
v.	von / vom
VW	Versicherungswirtschaft (Zeitschrift)
WiSt	Wirtschaftswissenschaftliches Studium (Zeitschrift)
Wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht
WM	Zeitschrift für Wirtschafts- und Bankrecht
WpHG	Wertpapierhandelsgesetz
ZFO	Zeitschrift Führung und Organisation
ZIP	Zeitschrift für Wirtschaftsrecht und Insolvenzpraxis
ZIR	Zeitschrift interne Revision

A. EINLEITUNG

Presseberichten zufolge soll die *Deutsche Bahn AG* (im Folgenden einfach *Bahn*) über Jahre hinweg Mitarbeiterdaten abgeglichen, betrieblich E-Mails kontrolliert sowie Mitarbeiter mit Hilfe von Detekteien überwacht haben.[1] Dabei soll es u.a. in größerem Umfang zu Abgleichen diverser Mitarbeiterdaten, wie etwa Kontodaten, mit Daten von Zulieferern u.ä. gekommen sein (sog. *Screening*[2]).

Ziel dieser Arbeit ist es zu untersuchen, ob dabei die – insbesondere datenschutzbezogenen – Rechte von Arbeitnehmern der *Bahn* missachtet wurden oder ob die *Bahn* lediglich im Rahmen ihrer Aufsichtspflichten als Arbeitgeber handelte. Mit dem Zusammentreffen von Compliance-Pflichten von Unternehmen und den von entsprechenden Compliance-Maßnahmen, wie etwa *internal investigations*, betroffenen Rechten Dritter, also regelmäßig der Arbeitnehmer, kommt es zu neuen, bisher wenig beleuchteten und daher noch ungeklärten Rechtsfragen im Bereich der Compliance und des Datenschutzes. Es mag auf den ersten Blick den Anschein haben, dass Compliance-Pflichten und der Datenschutz zueinander in einem unüberbrückbaren Widerspruch stehen. Dies jedoch – soviel sei vorweggenommen – ist nicht der Fall, auch wenn es durchaus diverse „Reibungspunkte“ zwischen den verschiedenen Interessen gibt. Diese Arbeit kann möglicherweise dazu beitragen, die Problemfelder und Kollisionspunkte aufzuzeigen.

Zunächst soll der so genannte „Datenskandal“ bei der *Bahn* soweit möglich dargestellt werden. Dabei ist zu berücksichtigen, dass die Informationen dazu überwiegend der Tagespresse entnommen werden mussten; in geringem Umfang konnten durch Auswertung von Eigenberichten der *Bahn* entsprechende Schlüsse gezogen werden. Daher ist eine Analyse nur immer so weit möglich, wie auch die Informationen über den Sachverhalt verfügbar waren. Im Anschluss daran wird geklärt, was zunächst unter Compliance zu verstehen ist, welche Pflichten und Rechte sich daraus für Unternehmen ergeben und wie eine effektive Compliance-Organisation aussehen kann. Anschließend soll die Effektivität der Compliance-Organisation bei der *Bahn* untersucht werden. Dazu werden die

[1] *Biermann*, Zeit online v. 04.09.2009.
[2] Bei einem sog. Screening vergleicht der Arbeitgeber computergestützt systematisch die erfassten Stammdaten der Arbeitnehmer, wie etwa Kontonummern, Adressen, etc., mit denen von Vertragspartnern wie etwa Zulieferern.

Compliance-Strukturen der *Bahn*, sofern entsprechende Informationen zu erheben waren, dargestellt und im Anschluss mit den Empfehlungen zur Einrichtung und Ausgestaltung von Compliance-Organisationen aus der Literatur verglichen.

Der zweite Teil der Arbeit befasst sich mit den Rechten und Pflichten, die Arbeitnehmern sowie Arbeitgebern durch das Bundesdatenschutzgesetz (BDSG) eingeräumt werden. Hierbei sollen die rechtlichen Aspekte beim Datenabgleich, den E-Mail-Kontrollen sowie der Zusammenarbeit mit externen Dienstleistern getrennt untersucht werden.

Nach einem Fazit werden zum Schluss noch die wichtigsten Neuerungen des Bundesdatenschutzgesetzes (BDSG) im Arbeitsverhältnis dargestellt und ihre möglichen Auswirkungen aufgezeigt.

B. DARSTELLUNG DES SACHVERHALTS

Laut einem Zwischenbericht der *Bahn* vom 10. Februar 2009 habe das Unternehmen seine Mitarbeiter insgesamt fünfmal einem sogenannten Datenabgleich unterzogen. Dabei sollen Namen, Adressen und Kontonummern maschinell mit denen von Lieferanten des Unternehmens verglichen worden sein. Von den Abgleichen seien im Jahr 1998 eine nicht mehr rekonstruierbare Anzahl an Mitarbeitern betroffen gewesen, 2002/2003 sollen 173.000 Mitarbeiter und in den Jahren 2005/2006 sogar 188.602 Personalstammdatensätze überprüft worden sein.[3] Des Weiteren wurden laut Bericht die Datensätze von knapp 800 Führungskräften des Unternehmens zweimal untersucht, wohl in den Jahren 2003/ 2004 sowie 2005/ 2006.[4] Weiterhin räumte der neue Vorstandsvorsitzende der *Bahn – Dr. Rüdiger Grube* – ein, dass teilweise auch die Angehörigen von Mitarbeitern in die Abgleiche einbezogen worden wären.[5]

Nach Erkenntnissen von Sonderermittlern, die vom Aufsichtsrat der *Bahn* eingesetzt wurden, sollen zudem E-Mails von Mitarbeitern gezielt nach Kontakten zu Journalisten und Kritikern der *Bahn* durchsucht worden sein. So sollen im Jahr 2005 E-Mails nach bestimmten Namen oder Internetdomänen ohne Wissen der betroffenen Mitarbeiter durchsucht und bei Auffinden bestimmter Begriffe automatisch an eine interne Kontrollinstanz weitergeleitet worden sein. Dabei soll es jedoch nur in konkreten Verdachtsfällen zu detaillierten Inhaltskontrollen der E-Mails gekommen sein.[6] Darüber hinaus sollen während des Tarifkonflikts mit den Lokführern im Jahr 2007 auch E-Mails der Gewerkschaft *GDL* mit der Begründung abgefangen worden sein, dass durch die Masse der versandten E-Mails ein Server zusammengebrochen sei.[7]

Weiterhin äußerte sich der Vorstand dahingehend, dass er nicht über die konrete Vorgehensweise der Compliance-Abteilung informiert gewesen sei, sondern lediglich über die ermittelten Ergebnisse.[8] Hier stellt sich die Frage, welche Be-

---

[3] *Deutsche Bahn AG*, Zwischenbericht „Überprüfung der Ordnungsmäßigkeit von Maßnahmen der Korruptionsbekämpfung in den Jahren 1998-2007“, 2009, S. 17 ff.
[4] FAZ v. 12.02.2009, S.1 f.
[5] Pressekonferenz v. 13.05.2009 mit *Dr. Rüdiger Grube*, Vorstandsvorsitzender der Deutschen Bahn, Berlin, S. 2.
[6] FAZ v. 28.03.2009, S. 1.
[7] *Schwenn*, FAZ v. 31.03.2009, S. 3.
[8] FAZ v. 20.02.2009, S. 17.

fugnisse die Compliance-Abteilung hatte und damit auch, ob mögliche Verletzungen des Datenschutzrechts auch dem Vorstand oder ausschließlich dem Compliance-Officer zuzurechnen sind.

Auch über die Arbeitsweise von externen Dienstleistern, die im Zusammenhang mit den Datenabgleichen eingeschaltet wurden, sei dem Vorstand der *Bahn* nichts bekannt gewesen. Dabei handele es sich vor allem um zwei Unternehmen, die Firma *Argen GmbH* sowie die *Network Deutschland GmbH*. Nachfolgend sollen daher auch Sachverhalte in Bezug auf die Zusammenarbeit der *Bahn* mit externen Dienstleistern bei Durchführung von Compliance-Maßnahmen dargestellt werden.

Der *Bahn* sollen Hinweise auf Verstöße bei der Ausführung und Abrechnung von Leistungen vorgelegen haben. Im Rahmen der internen Untersuchungen habe das Unternehmen eine Rechtsanwaltskanzlei beauftragt, die ihrerseits die Firma *Argen* eingeschaltet habe, um Kontobewegungsdaten der verdächtigten Bahn-Mitarbeiter sowie einer weiteren in den Fall verwickelten Firma zu ermitteln. Zudem sei die Firma *Argen* von einem Ombudsmann, der Hinweise auf Scheckzahlungen an Bahn-Mitarbeiter erhalten hatte, beauftragt gewesen, die Kontobewegungsdaten des betroffenen Bahn-Mitarbeiters zu recherchieren.[9]

Im Rahmen von sieben Projekten, die in Zusammenarbeit mit der Firma *Network* stattfanden, sollen Informationen über Kraftfahrzeughalter, Immobilien, Verwandtschaftsbeziehungen und ähnlichem beschafft und der *Bahn* zugänglich gemacht worden sein.[10]

Im Jahr 2002 seien die Büroräume von vier Bahn-Mitarbeitern, die aufgrund eines anonymen Hinweises in den Verdacht der Vorteilsannahme gerieten, in Zusammenarbeit der Konzernrevision mit der Firma *Network* durchsucht und Firmenrechner der Mitarbeiter sichergestellt und ausgewertet worden. Auf den Rechnern hätten sich auch private Dateien über Kontobewegungen, Reisetätigkeiten und Familienverhältnisse befunden, die, soweit sie in Verbindung mit den Vorwürfen standen, ebenfalls ausgewertet wurden. Des Weiteren sollen die von

[9] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 36.
[10] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 27.

den Bahn-Mitarbeitern mit ihren dienstlichen PCs besuchten Internetseiten überprüft worden sein.[11]

Im Jahr 2003 trat der Verdacht auf, dass es sich bei einem US-amerikanischen Unternehmen, mit dem die *Bahn* kooperieren wollte, um eine Scheinfirma handele. Diese sei daraufhin durch die *Network Deutschland GmbH* überprüft worden und der daraus resultierende Bericht soll auch den Verlauf von Geldbewegungen eines der Konten der verdächtigten US-Firma enthalten haben. Nach Angaben der Konzernrevision wurde dieser Bericht jedoch zurückgewiesen, da die Recherche solcher Daten von der *Bahn* nicht beauftragt worden sei.[12]

Daneben sollen vier weitere externe Dienstleister, die bislang noch nicht benannt wurden, beauftragt worden sein, die Vermögensverhältnisse von Bahn-Mitarbeitern im In- und Ausland aufzuklären. Zusätzlich sollten diese in Verdachtsfällen sogenannte Nähebeziehungen zwischen Mitarbeitern der *Bahn* und Auftragnehmern ermitteln. Außerdem sollte dem Verdacht nachgegangen werden, Bahn-Mitarbeiter würden nicht genehmigten Nebentätigkeiten nachgehen.[13]

[11] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 30.
[12] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 34.
[13] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 36.

C. COMPLIANCE IM UNTERNEHMEN

Fraglich im Fall der *Bahn* ist, ob sich das Unternehmen bei seinem Bemühen, Korruption durch Compliance-Maßnahmen zu verhindern, rechtmäßig verhalten hat. Dazu soll zunächst geklärt werden, was der Begriff der Compliance umfasst und welche Funktionen Compliance erfüllt. Im Anschluss wird geprüft, welche Gesetze und Regeln einer Compliance-Organisation zugrunde liegen und wie eine solche Organisation aussehen sollte. Des Weiteren wird dargestellt, welche Aufgaben dem Compliance-Officer zufallen und welche Stellung er im Unternehmen einnehmen sollte, um den Anforderungen seiner Arbeit gerecht werden zu können. Im Anschluss wird die Compliance-Struktur bei der *Bahn* dargestellt und der Frage nachgegangen, ob sie ordnungsgemäß eingerichtet wurde und das Unternehmen rechtmäßig gehandelt hat.

I. Begriff der Compliance

Der Begriff Compliance wurde aus dem angloamerikanischen übernommen und bedeutet im engen Sinne zunächst lediglich, dass sich ein Unternehmen selbst, sowie alle seine Organe und Mitarbeiter an die Gesetze halten.[14] Damit ist zunächst keine eigenständige Funktion con Compliance zu erkennen, denn es ist in einem Rechtsstaat üblich, dass Unternehmen und deren Organe im Rahmen des rechtlich erlaubten agieren.

Dennoch umfasst der Begriff inhaltlich weitere Aspekte. Compliance geht über schlichte Gesetzes- und Normentreue hinaus und beinhaltet zudem die Einhaltung von weiteren nationalen und internationalen Standards, wie etwa die Befolgung der Prinzipien des Corporate Governance.[15] Compliance beschreibt weiterhin die persönlichen Verhaltenspflichten der Organmitglieder und Mitarbeiter, die Organisationspflichten der geschäftsführenden Organe, sowie deren Deliktverhinderungs- und Schadensabwehrpflicht.[16] Prägnanter formuliert es *Kiethe*,

[14] *Hauschka*, ZIP 2004, 877.
[15] *Kort*, NZG 2008, 81, 82.
[16] *Uwe H. Schneider/Sven H. Schneider*, ZIP 2007, 2061, 2062.

der Corporate Compliance als „Haftungsvermeidung durch bestmögliche Organisation des Unternehmens“ beschreibt.[17]

In Deutschland existiert der Begriff, der ohne Übersetzung übernommen wurde, seit etwa Mitte der 90er Jahre.[18] Zu seiner Durchsetzung in Deutschland hat auch die „ARAG/Garmenbeck“-Entscheidung des *BGH* beigetragen. Dort heißt es, dass der Aufsichtsrat Schadensersatzansprüche gegen den Vorstand zu verfolgen hat, falls er nach Prüfung des Sachverhaltes zu dem Schluss kommt, dass diese Ansprüche durchsetzbar sind.[19] Durch diese Entscheidung wird der Aufsichtsrat bei Kenntnis entsprechender Sachverhalte praktisch zum Handeln gezwungen. Von daher muss es schon originäres Interesse der handelnden Organe eines Unternehmens sein, durch eine effektive Compliance-Organisation auf die Einhaltung des gesetzlich Gebotenen und Erlaubten hinzuwirken, um dadurch eventuelle Haftungsansprüche nicht nur gegen das Unternehmen sondern auch eine persönliche Haftung zu vermeiden.

Weiter verstärkt wurde die Tendenz, Organe durch Einführung neuer Regelungen stärker in Haftung zu nehmen, etwa mit dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (1998), dem Transparenz- und Publizitätsgesetz (2002), dem Deutschen Corporate Governance Kodex (zuletzt 2007 geändert) sowie dem Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (2005).[20]

Um sich vor künftigen Haftungsansprüchen zu schützen, ist neben dem Vorstand auch der Aufsichtsrat gehalten, entsprechend sorgfältig seinen Aufgaben nachzukommen.

II. Funktionen von Compliance

Seit einigen Jahren werden Unternehmen, die gegen geltendes Recht verstoßen, mit erheblich empfindlicheren Bußgeldern belegt als früher. Im Jahr 2001 hat die Europäische Kommission allein wegen Kartellverstößen Bußgelder in Höhe von

[17] *Kiethe*, GmbHR 2007, 393.
[18] *Hauschka*, in: Hauschka (Hrsg.), Corporate Compliance, § 1 Rn. 1.
[19] *BGH*, Urt. v. 21.04.1997 – II ZR 175/95, NJW 1997, 1926 f.
[20] *Hauschka*, in: Hauschka (Hrsg.), Corporate Compliance, § 1 Rn. 19.

1,836 Mrd. Euro gegen 56 Unternehmen verhängt.[21] Darüber hinaus laufen Unternehmen, die gegen geltendes Recht verstoßen, Gefahr, von öffentlichen Ausschreibungen sowie teilweise auch von privaten Aufträgen ausgeschlossen zu werden. Rechtliche Sanktionen können darüber hinaus auch die Organmitglieder persönlich treffen.[22]

Weitere Ge- und Verbote ergeben sich für Unternehmen aus dem Gesellschafts-, Insolvenz-, Umwelt-, Produkthaftungs-, Datenschutz-, Steuer-, und dem Arbeitsrecht. Des Weiteren können noch rechtliche Sondergebiete hinzukommen, die sich aus dem besonderen Tätigkeitsbereich des Unternehmens ergeben.[23]

Indes genügt oft schon der Vorwurf der Verwirklichung entsprechender Ordnungswidrigkeiten oder Strafdelikte, um für ein Unternehmen beachtliche Aufwendungen in Gestalt von Beratungs- und Verfahrenskosten hervorzurufen. Hinzu kommt neben dem zeitlichen Aufwand, den das Management in solchen Fällen erbringen muss, noch ein enormer Ansehensverlust durch negative Schlagzeilen in der Presse.[24] Denn nach wie vor gilt: Der über viele Jahre hinweg kontinuierlich erworbene „Gute Ruf“ eines Unternehmens kann innerhalb weniger Stunden dauerhaft geschädigt werden. Nicht zuletzt ist die Gefahr einer Rufschädigung größer denn je, weil es über die heute üblichen Verbreitungskanäle möglich ist, erste bekannt gewordene Informationen über Unternehmens- bzw. Organverfehlungen binnen Minuten weltweit zu verbreiten. Und oftmals reicht bereits ein erster „böser Anschein“ aus, Schaden am Unternehmensimage oder am Anlegervertrauen und damit am Aktienkurs zu erzeugen, ganz gleich in welcher Richtung sich der anfängliche Sachverhalt später noch entwickeln mag.

Somit kann durch eine effektive Compliance-Struktur sowohl das Vertrauen von Geschäftspartnern als auch der Öffentlichkeit in das Unternehmen gesteigert werden,[25] da Regelverstöße durch Compliance-Maßnahmen zwar nicht absolut vermieden werden können, eine effektive Compliance-Organisation das Risiko jedoch zumindest deutlich verringern kann.[26] Die Einrichtung einer Compliance-Organisation kann dabei verschiedene Funktionen erfüllen. Zuvörderst erfüllt sie

[21] *Lampert*, BB 2002, 2237.
[22] *Grundei/Talaulicar*, WiSt 2009, 73.
[23] *Hauschka*, AG 2004, 461, 472.
[24] *Bürkle*, BB 2005, 565, 566.
[25] *Uwe H. Schneider*, ZIP 2003, 645, 648.
[26] *Bürkle*, BB 2005, 565, 566.

eine Informations- und Beratungsfunktion.[27] Alle Organmitglieder und Mitarbeiter werden über geltendes Recht, interne Regeln im Unternehmen und über mögliche Gefahren aufgeklärt.

III. Rechtspflicht zur Compliance

Die *Bahn* ist eine nicht börsennotierte Aktiengesellschaft, deren 100-prozentiger Anteilseigner der Bund ist. Dennoch sollen die folgenden Ausführungen auf die Rechtsform der Aktiengesellschaft bezogen werden.[28]

Die Pflicht zur Einrichtung einer Compliance-Organisation ist nicht ausdrücklich gesetzlich normiert.[29] Verpflichtungen für die Einrichtung einer Compliance-Organisation können allerdings aus den allgemeinen Vorstandspflichten, den §§ 76 Abs. 1, 93 Abs. 1 AktG, sowie aus § 130 Abs. 1 Satz 1 OWiG entnommen werden.[30] Für Aktiengesellschaften wird häufig auch § 91 Abs. 2 AktG herangezogen.[31] Des Weiteren existieren entsprechende Empfehlungen im Deutschen Corporate Governance Kodex (DCGK).[32]

In der Literatur sind die Ansichten zu der Frage, ob jedes Unternehmen der Pflicht zur Einrichtung einer Compliance-Organisation unterliegt, geteilt. So gibt es eine Ansicht, nach der etwa Kleinunternehmer, die über alle Einzelheiten in ihrem Betrieb informiert sind und die Einhaltung der Gesetzestreue selbst organisieren können, nicht zwangsläufig eine eigene Compliance-Organisation einrichten müssen.[33] Teilweise wird dem Vorstand innerhalb der Business Judgement Rule ein Ermessensspielraum eingeräumt, in dessen Rahmen auch die Entscheidung zur Einrichtung einer Compliance-Organisation fällt.[34] Andere leiten eine gesetzliche Verpflichtung im Wege der Rechtsanalogie aus Einzelvorschrif-

---

[27] *Lösler*, NZG 2005, 104, 105.
[28] Zur Compliance im Wirtschaftsverband *Brouwer*, CCZ 2009, 161.
[29] *Uwe H. Schneider/Sven H. Schneider*, ZIP 2007, 2061, 2062.
[30] *Uwe H. Schneider*, NZG 2009, 1321, 1322.
[31] *Wagner*, CCZ 2009, 8, 12.
[32] Die aktuelle Version des Deutschen Corporate Governance Kodex ist abrufbar unter http://www.corporate-governance-code.de/ger/kodex/index.html.
[33] Hauschka, ZIP 2004, 877, 878, sowie *ders.*, in: Hauschka (Hrsg.), Corporate Compliance, § 1 Rn. 22 vertritt die Ansicht, dass auch in größeren Unternehmen den Leitungsorganen die Einrichtung solcher Organisationen frei stünde, soweit sich diese selbst kompetent und hinreichend informiert fühlten, um die Einhaltung der Gesetze in ihrem Unternehmen selbst zu überwachen. Ebenfalls verneinend *Lücke*, in: Vorstand der AG, § 3 Rn. 15.
[34] *Spindler*, in: MK-AktG, § 91, Rn. 37.

ten ab[35] oder sehen es als Teil der Überwachungssorgfalt der Vorstandsmitglieder.[36] Beachtet werden muss allerdings, dass Vorstände, die sich gegen die Einrichtung einer Compliance-Organisation entscheiden, auch die uneingeschränkten Konsequenzen dieser Entscheidung zu tragen haben. Je nach Art des Rechtsverstoßes, der ohne eine entsprechende Compliance-Organisation auftreten kann, können die daraus entstehenden Konsequenzen Unternehmen und ihre Organe hart treffen. Daher hat sich die ursprüngliche und vereinzelte Sichtweise einiger Unternehmensführer, Compliance mehr als „Kür" denn als „Pflicht" guter Unternehmensführung anzusehen, inzwischen gewandelt.[37]

1. Pflichten des Vorstandes

Zwar ist umstritten, ob eine Pflicht zur Einrichtung einer Compliance-Organisation besteht. Unstreitig ist jedoch, dass es sich bei der Entscheidung darüber um eine Leitungsaufgabe handelt, die in den Aufgabenbereich des Vorstandes fällt.[38]

Der Vorstand kann auf zwei Wegen zur Verantwortung gezogen werden. Zum einen können ihm persönliche Verfehlungen zur Last gelegt werden. Zum anderen kann ihm unter Umständen das Fehlverhalten von nachgeordneten Mitarbeitern zugerechnet werden. Der Vorwurf in diesem Fall lautet, dass der Vorstand bei seinen Personalentscheidungen seinen Auswahl-, Einweisungs- oder Überwachungspflichten nicht oder nicht in hinreichendem Maße nachgekommen sei.[39]

Die *Auswahlpflichten* hängen von der Art der den Mitarbeitern übertragenen Aufgaben ab und können daher kaum allgemein formuliert werden. Bei der Betrachtung typischer Profile wirtschaftskrimineller Täter stellt sich allerdings heraus, dass dies häufig junge Männer mit guter Ausbildung, ausgeprägter Entscheidungsfreude und hochgradiger Karriere- und Erfolgsorientierung sind.[40] Da viele Menschen ohne kriminelle Absichten diese Eigenschaften ebenfalls aufwei-

[35] *Uwe H. Schneider*, ZIP 2003, 645, 649.
[36] *Fleischer*, AG 2003, 291, 299.
[37] *Campos Nave/Bonenberg*, BB 2008, 734; *Lösler*, WM 2007, 676, 679.
[38] *Uwe H. Schneider*, ZIP 2003, 645, 647; *Spindler*, in: MK-AktG, § 76 Rn. 17.
[39] *Fleischer*, AG 2003, 291.
[40] *Grundei/Talaulicar*, WiSt 2009, 73, 75.

sen, können sie nicht als Anhaltspunkte für die Auswahl von Mitarbeitern dienen.

Die *Einweisungspflichten* beziehen sich auf die Einführung der Mitarbeiter in ihre konkrete Aufgabe. Dafür müssen sie auf die unternehmensinternen Regeln sowie die Gefahren, die sich aus ihrer Tätigkeit ergeben, hingewiesen werden. Hierzu zählen auch typische Rechtsverletzungen, die in Zusammenhang mit ihren Tätigkeiten in Betracht kommen können.[41]

Die *Überwachungspflichten* des Vorstandes hängen ebenfalls vom Einzellfall ab, näheres dazu findet sich im Kapitel „Überwachung". Der Vorstand hat nach § 76 AktG die Geschäfte der Gesellschaft in eigener Verantwortung zu leiten. Somit ist Ausgangspunkt jeglicher Haftung des Vorstandes einer AG § 93 Abs. 1 AktG.[42] Nach § 93 Abs. 1 Satz 1 AktG haben die Vorstände bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Verletzen Mitglieder des Vorstandes ihre Aufsichtspflichten vorsätzlich oder fahrlässig, sind sie nach § 93 Abs. 2 Satz 1 AktG der Gesellschaft zum Ersatz des daraus entstandenen Schadens verpflichtet.[43]

Demgegenüber liegt nach § 93 Abs. 1 Satz 2 AktG keine Pflichtverletzung vor, wenn der Vorstand bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Informationen zum Wohle der Gesellschaft zu handeln. Eine unternehmerische Entscheidung liegt dann nicht vor, wenn kraft Gesetzes, Satzung, Geschäftsordnung, Vertrag oder rechtmäßiger Weisung *kein Beurteilungsspielraum* bei der Entscheidungsfindung gegeben war.[44] Aus dieser Regelung wird ersichtlich, dass Voraussetzung für die Vermeidung von Pflichtverletzungen bei unternehmerischen Entscheidungen ein umfassender Informationsstand der zur Entscheidung zuständigen Organe ist.[45]

Im Rahmen der Compliance-Pflichten schuldet der Vorstand angemessene und verhältnismäßige Maßnahmen. Das bedeutet, dass sich die Pflicht des Vorstandes nicht in der bloßen Überwachung einzelner Bereiche im Unternehmen erschöpft. Vielmehr müssen die wesentlichen rechtlich und wirtschaftlich kriti-

[41] *Fleischer*, AG 2003, 291, 293; *Lösler*, WM 2007, 676, 681.
[42] *Kiethe*, GmbHR 2007, 393, 395.
[43] *Spindler*, in: MK-AktG, § 93 Rn. 12.
[44] *Hauschka*, in: Hauschka (Hrsg.), Corporate Compliance, § 1 Rn. 29.
[45] *Kiethe*, GmbHR 2007, 393, 395.

schen Bereiche im Unternehmen beobachtet werden.[46] Verfügt jedoch ein Unternehmen über mehr Mitarbeiter, die für Compliance-Aufgaben zuständig sind als Mitarbeiter, die in der Forschungsabteilung oder im Vertrieb tätig sind, ist dies nicht mehr angemessen.[47] Ein Compliance-System, das sich auf besonders risikoreiche Bereiche konzentriert, weist gegenüber einem flächendeckenden System eine höhere Effektivität und Akzeptanz auf und spart zudem Kosten.[48]

Im Deutschen Corporate Governance Kodex, in der Fassung von 2007, wird erstmals der Begriff Compliance ausdrücklich verwendet. Ziffer 4.1.3 DCGK wurde gegenüber der vorherigen Fassung wie folgt geändert:

> „Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin *(Compliance)*."[49]

Diese Regelung ist zunächst lediglich eine Beschreibung der gegebenen Rechtslage, denn an sich stellt der Hinweis, dass der Vorstand für die Einhaltung der gesetzlichen Bestimmungen Sorge zu tragen hat, eine Selbstverständlichkeit[50] bzw. eine „Binsenweisheit"[51] dar.

Der DCGK definiert Compliance als übergeordneten Begriff, der die Einhaltung sowohl externer als auch interner Vorgaben umfasst. Hierbei umfasst die Leitungsverantwortung des Vorstandes eine *Organisations- und Legalitätspflicht*.[52]

a) LEGALITÄTSPFLICHT

Legalitätspflicht soll in diesem Zusammenhang bedeuten, dass der Vorstand die Verantwortung für das rechtmäßige Verhalten und für die Erfüllung öffentlich-rechtlicher Pflichten der Gesellschaft sowohl intern als auch gegenüber Dritten trägt.[53] Die Legalitätspflicht ist nicht gleichzusetzen mit dem Begriff Compliance, da dieser weitergehend ist. Während Legalitätspflicht tatsächlich Gesetzes-

---

[46] *Bürkle*, BB 2007, 1797, 1798.
[47] *Uwe H. Schneider/Sven H. Schneider*, ZIP 2007, 2061.
[48] *Bürkle*, BB 2007, 1797, 1798.
[49] Hervorhebungen durch die Verfasser.
[50] *Ringleb/Kremer/Lutter/*v. *Werder*, in: Kommentar zum Deutschen Corporate Governance Kodex, Rn. 615.
[51] Begriff bei *Uwe H. Schneider*, ZIP 2003, 645, 646.
[52] *Bürkle*, BB 2007, 1797, 1798.
[53] *Bürkle*, BB 2005, 565, 567; a.A. dagegen *Brouwer*, CCZ 2009, 161, 162, nach dem Compliance vor allem der Vorbeugung und Begrenzung von Unternehmensschäden dienen soll und die Rechtstreue als solche gerade nicht zu den Hauptaufgaben gehöre.

treue meint, umfasst Compliance auch eine Unternehmensorganisation, die präventiv und risikominimierend ausgestaltet ist.[54]

b) ORGANISATIONSPFLICHT

Ein Organisationsverschulden liegt vor, wenn Maßnahmen zur rechtmäßigen Organisation, einschließlich ordnungsmäßiger interner Entscheidungsprozesse, gänzlich fehlen oder unzureichend sind. Organisationsverschulden bezieht sich somit regelmäßig auf das Unterlassen einer gebotenen Unternehmensorganisation.[55]

Nach § 91 Abs. 2 AktG hat der Vorstand geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen rechtzeitig erkannt werden können. Welche Maßnahmen hierbei konkret getroffen werden müssen, ist aus dem Gesetz jedoch nicht abzuleiten. Für diese Norm relevant sind indes nur die Risiken, die für das Unternehmen letztlich bestandsgefährdend sein können.[56] Zu der Frage, ob diese Vorschrift den Vorstand zur Einrichtung eines umfassenden Risikomanagementsystems verpflichtet, werden verschiedene Ansichten vertreten. So gibt es insbesondere aus dem Bereich der Betriebswirtschaftslehre Befürworter eines umfassenden Risikomanagementsystems, wohingegen im rechtswissenschaftlichen Schrifttum eher zurückhaltende Ansichten vertreten werden.[57]

Weiterhin legen die Zurechnungsnormen des § 9 OWiG sowie des § 130 OWiG eine Organisation des Unternehmens nahe, bei der Gesetzesverstöße minimiert werden, so dass auch Haftungsfolgen aus Organisationsverschulden reduziert werden.[58]

Die Verpflichtung zur Einrichtung einer Compliance-Organisation ergibt sich somit mittelbar aus § 130 OWiG.[59] Danach hat die Unternehmensleitung die Aufsichtsmaßnahmen zu treffen, die erforderlich sind zu verhindern, dass aus

---

[54] *Lücke*, in: Beck´sches Mandatshandbuch, Vorstand der AG, § 3 Rn. 12.
[55] *Bürkle*, BB 2005, 565, 567.
[56] *Liese*, BB Special zu Heft 25/2008, 17, 19.
[57] *Pahlke*, NJW 2002, 1680. 1681.
[58] *Ringleb/Kremer/Lutter/*v. *Werder*, in: Kommentar zum Deutschen Corporate Governance Kodex, Rn. 625.
[59] *Uwe H. Schneider*, ZIP 2003, 645, 649.

dem Unternehmen heraus Straftaten begangen werden.[60] Grenzen bilden dabei die Zumutbarkeit und praktische Durchführbarkeit.[61]

2. Pflichten des Aufsichtsrates

Nicht nur den Vorstand, auch den Aufsichtsrat trifft zunächst die Pflicht, sich rechtmäßig zu verhalten und interne sowie externe Regeln einzuhalten. Daneben muss der Aufsichtsrat zur Erfüllung seiner Pflicht, den Vorstand zu überwachen und zu beraten, prüfen, ob dieser ebenfalls die verbindlichen Bestimmungen einhält.[62] Neben dieser Rechtmäßigkeitsprüfung muss der Aufsichtsrat prüfen, ob der Vorstand seinen Pflichten ordnungsgemäß, wirtschaftlich und zweckmäßig nachkommt. Hierbei bedeutet ordnungsgemäß ein Handeln unter Beachtung betriebswirtschaftlicher Erkenntnisse und Erfahrungen. Wirtschaftlich meint die Sicherung der Liquidität, Finanzierung und Ertragskraft des Unternehmens, zweckmäßig zielt auf eine dauerhafte Rentabilität des Unternehmens.[63]

Der Deutsche Corporate Govenance Kodex formuliert die Aufgaben des Aufsichtsrates in der geänderten Fassung in Ziffer 5.3.2 DCGK wie folgt:

> „Der Aufsichtsrat soll einen Prüfungsausschuss (Audit Committee) einrichten, der sich insbesondere mit Fragen der Rechnungslegung, des Risikomanagements und der *Compliance*, der erforderlichen Unabhängigkeit des Abschlussprüfers, der Erteilung des Prüfungsauftrags an den Abschlussprüfer, der Bestimmung von Prüfungsschwerpunkten und der Honorarvereinbarung befasst."[64]

Somit muss der vom Aufsichtsrat gebildete Prüfungsausschuss beurteilen, ob die vom Vorstand eingerichtete Compliance-Organsation den rechtlichen Anforderungen und der Risikolage des Unternehmens genügt. In der Regel muss der Prüfungsausschuss sich weder mit Details der Organisation noch mit allen einzelnen Verstößen befassen.[65] Der Prüfungsausschuss befasst sich lediglich mit den wichtigsten Fällen, wie beispielsweise solchen, die zu erheblichen Reputationsschäden führen können.[66]

---

[60] *Hauschka/Greeve*, BB 2007, 165, 166.
[61] *Liese*, BB Special zu Heft 25/2008, 17, 19.
[62] *Bürkle*, BB 2007, 1797, 1800.
[63] *Pahlke*, NJW 2002, 1680. 1684f.
[64] Hervorhebungen durch die Verfasser.
[65] *Ringleb/ Kremer/ Lutter/* v. *Werder*, in: Kommentar zum Deutschen Corporate Governance Kodex, Rn. 629.
[66] *Kort*, NZG 2008, 81, 84.

3. Zusammenarbeit von Vorstand und Aufsichtsrat

Auch für die Zusammenarbeit von Vorstand und Aufsichtsrat gab es eine Neuregelung im Kodex in Ziffer 3.4 Abs. 2 DCGK:

> „Der Vorstand informiert den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und der *Compliance*. Er geht auf Abweichungen des Geschäftsverlaufs von den aufgestellten Plänen und Zielen unter Angabe von Gründen ein.“[67]

Die Informationsversorgung des Aufsichtsrates ist eine gemeinsame Pflicht von Vorstand und Aufsichtsrat und sollte regelmäßig – bei Bedarf auch direkt – geschehen. Wichtig für den Aufsichtsrat ist, dass er über aktuelle rechtliche Entwicklungen, wie beispielsweise wichtige Gesetzesänderungen, richtungsweisende Gerichtsurteile oder Anordnungen von maßgeblichen Aufsichtsbehörden, welche die Planung und Entwicklung des Unternehmens stark beeinflussen können, informiert ist.[68]

IV. Organisation eines effektiven Compliance-Systems

Die Ausgestaltung einer Compliance-Organisation hängt im Einzelnen von der Branche, der Größe, der nationalen und internationalen Ausrichtung des Unternehmens sowie von weiteren Faktoren ab.[69] Dennoch lassen sich einige Grundpflichten festhalten, die eine Compliance-Organisation leisten sollte, um ihren Zweck zu erfüllen.

Konkrete gesetzliche Vorgaben darüber, wie eine Compliance-Organisation ausgestaltet werden soll, gibt es nicht. Compliance-Programme entstammen ursprünglich vor allem aus dem Kartellordnungswidrigkeitenrecht. Daher wurden die Inhalte dieser Programme in Anlehnung an die Praxis des Bundeskartellamts und der Gerichte zur Aufsichtspflicht nach § 130 OWiG entwickelt. Weitere Anhaltspunkte ergeben sich aus dem Kapitalmarktrecht, sowie aus sektorspezifischen Vorgaben mit Ausstrahlwirkung.[70] Auch die Betrachtung ausländischer Rechtsordnungen hilft bei der Entwicklung von

---

[67] Hervorhebungen durch die Verfasser.
[68] *Bürkle*, BB 2007, 1797, 1800.
[69] *Uwe H. Schneider*, ZIP 2003, 645, 649.
[70] *Kort*, NZG 2008, 81, 82 f.

Rechtsordnungen hilft bei der Entwicklung von Compliance-Programmen weiter.[71]

Eine Compliance-Organisation umfasst die Identifikation, Analyse und Steuerung der Risiken im Unternehmen und die Überwachung der Effektivität der Maßnahmen.[72] Die erforderlichen Maßnahmen lassen sich unterteilen in Anweisung, vorbeugende Kontrolle sowie repressive Sanktionierung.[73]

1. Aufgabenzuweisung

Im ersten Schritt kann bei mehreren Vorstandsmitgliedern ein Verantwortungsbereich einem Vorstandsmitglied zugewiesen werden. Durch diese horizontale Aufgabenzuweisung können die anderen Vorstandsmitglieder entlastet werden.[74] Weiterhin können Compliance-Aufgaben vertikal an sachgerecht ausgewählte Mitarbeiter delegiert werden.[75] Die Verantwortungsbereiche und Kompetenzen sind bei der Delegation sorgfältig gegeneinander abzugrenzen, damit es nicht zu Überschneidungen kommt und letztlich jeder darauf vertraut, dass sich ein Kollege um die Erfüllung von Pflichten kümmert.[76]

Ein vollständiger Übergang der Pflichten des Vorstandes ist indes nicht möglich, da die Überwachungspflicht eine Leitungsaufgabe darstellt und somit nach § 76 Abs. 1 AktG nicht übertragbar ist.[77] Daher bringt die Delegation von Compliance-Aufgaben zwar eine deutliche Haftungsentlastung für den Vorstand, befreit ihn jedoch nicht von seiner Aufsichtspflicht.[78]

Der Vorstand kann sich auch der durch § 130 Abs. 1 OWiG auferlegten Pflicht zur Aufsicht nicht entziehen. Daher wird der Vorstand sich auch bei der Delegation von Einzelaufgaben regelmäßig ein Bild von der Gesamtsituation im Unternehmen machen müssen. Die Delegation wird ohnehin dort eingeschränkt sein, wo ein Verdacht gegen Mitarbeiter in Führungspositionen auftritt oder wo der Vorstand selbst über Konsequenzen entscheiden muss sowie in Situationen, die

[71] *Hauschka*, DB 2006, 1143 ff.; speziell für die USA *Uwe H. Schneider*, ZIP 2003, 645, 648.
[72] *Lampert*, in: Hauschka (Hrsg.), Corporate Compliance, § 9 Rn. 2.
[73] *Pampel*, BB 2007, 1636, 1637.
[74] *Rodewald/Unger*, BB 2006, 113, 115.
[75] *Liese*, BB Special zu Heft 25/2008, 17, 21.
[76] *Bussmann/Matschke*, CCZ 2009, 132, 136.
[77] *Wagner*, CCZ 2009, 8, 14.
[78] *Hauschka*, NJW 2004, 257, 260.

das Gesamtunternehmen betreffen.[79] Innerhalb dieser Rahmen ist die Zuweisung von Aufsichtsaufgaben an entsprechend qualifizierte und gewissenhaft ausgesuchte Mitarbeiter möglich.

2. Aufstellen von Standards

Um eine Compliance-Organisation aufstellen zu können, müssen zunächst die Standards erarbeitet werden, an denen sich die Mitarbeiter orientieren können.

Grundvoraussetzung ist zunächst die Identifikation von unternehmensspezifischen Risiken. Diese sind abhängig von der Unternehmensgröße, der Unternehmensstruktur oder der Branche. Auch die Analyse bereits erfolgter Verstöße kann helfen, Risiken zu identifizieren. Des Weiteren ist das Aufdecken von solchen Risiken relevant, die bei einem potentiellen Verstoß zu besonders hohen Schäden führen.[80]

Sind die Standards im Unternehmen aufgestellt, sollten sich die Leitungsorgane öffentlich zu diesen und zur Rechtstreue allgemein bekennen.[81] Dieses Bekenntnis erhöht die Motivation der Mitarbeiter, ebenfalls sämtliche Rechtspflichten einzuhalten, erheblich.[82] Die Unternehmensstandards sollten allen Mitarbeitern zugänglich sein und ihnen eine wichtige Orientierungshilfe in Zweifelsfragen bieten. Daher müssen klare Aussagen zu sensiblen Bereichen wie Bestechung oder Vorteilsannahme gemacht werden.[83]

Da die Standards gerade bei Zweifelsfragen weiter helfen sollen, muss darauf geachtet werden, dass der Umfang des Regelwerkes nicht zu groß wird. Mit steigendem Umfang nimmt auch die Wahrscheinlichkeit ab, dass die Mitarbeiter alle Regeln zur Kenntnis nehmen und verinnerlichen können. Anwendungsbeispiele sind sinnvoll, wenn diese relevant und realistisch sind. Standards wie auch Beispiele sollten stets klar formuliert sein.[84]

---

[79] *Wagner*, CCZ 2009, 8, 14.
[80] *Lampert*, in: Hauschka (Hrsg.), Corporate Compliance, § 9 Rn. 8.
[81] Nach *Uwe H. Schneider*, NZG 2009, 1321, 1326 darf „Compliance nicht nur ein Papierprogramm“ darstellen.
[82] *Liese*, BB Special zu Heft 25/2008, 17, 21.
[83] *Bürkle*, VW 2004, 830, 831.
[84] *Grundei/Talaulicar*, WiSt 2009, Heft 2, 73, 75.

3. Schulungen und Trainingsprogramme

Oftmals werden Verstöße gegen geltende Gesetze aus Unwissenheit begangen. Daher sollte es Ziel einer Compliance-Organisation sein, bei den Mitarbeitern ein Bewusstsein für unternehmensspezifische Gefahren zu schaffen.[85] Den Mitarbeitern sollen im Wesentlichen gesetzliche Pflichten, Gebote und Verbote sowie zu erwartende Sanktionen bei Verstößen näher gebracht werden.[86]

Der Schulungserfolg kann häufig noch dadurch gesteigert werden, dass zumindest am Anfang einer Schulungsreihe auf externe Ausbilder zurückgegriffen wird, da diese oft von den Mitarbeitern besser akzeptiert werden.[87] Auch der Einsatz von unterschiedlichen Lernmaterialien ist Erfolg versprechend. Die Schulungen sollten auf die jeweiligen Mitarbeiter und ihre individuelle Arbeitssituation abgestimmt sein.[88] Den Schulungen sollte daher angemessene Aufmerksamkeit zugewandt werden, da das Verhalten der Mitarbeiter nur beeinflusst werden kann, wenn ihnen die Regelungen, nach denen sie sich richten sollen, bekannt sind und sie die Verhaltensmaßgaben auch verinnerlicht haben.[89] Es sollte sichergestellt sein, dass Mitarbeiter die Schulungen tatsächlich besuchen und neu in das Unternehmen eintretende Mitarbeiter automatisch und frühzeitig in diesen Prozess eingebunden werden.[90]

4. Kontrolle und Überwachung

Die Einrichtung einer Compliance-Organisation allein ist nicht ausreichend, um sicher zu stellen, dass alle Mitarbeiter rechtstreu handeln. Umgangssprachlich wird die Situation fehlender Aufsicht mit dem Ausdruck „Gelegenheit macht Diebe“ umschrieben.[91] Die Einhaltung der Regeln muss daher auch regelmäßig überwacht werden.[92] Sinnvoll ist es daher, in regelmäßigen zeitlichen Abständen Mitarbeiter zu befragen und Geschäftsvorgänge zu prüfen.[93]

---

[85] *Lampert*, in: Hauschka (Hrsg.), Corporate Compliance, § 9 Rn. 26.
[86] *Uwe H. Schneider*, ZIP 2003, 645, 649.
[87] *Lampert*, in: Hauschka (Hrsg.), Corporate Compliance, § 9 Rn. 27.
[88] *Menzies/Tüller/Martin*, ZFO 2008, 136, 140.
[89] *Rodewald/Unger*, BB 2007, 1629, 1630.
[90] *Menzies/Tüller/Martin*, ZFO 2008, 136, 140.
[91] *Grundei/Talaulicar*, BB 2009, 73, 75.
[92] *Bussmann/Matschke*, CCZ 2009, 132, 135.
[93] *Lampert*, in: Hauschka (Hrsg.), Corporate Compliance, § 9 Rn. 33.

Der *BGH* hat dazu allgemein festgestellt, dass die Maßnahmen, die ein Unternehmer ergreifen muss, um durch Überwachung sicher zu stellen, dass in seinem Betrieb geltendes Recht befolgt wird, von den Umständen des jeweiligen Einzelfalles abhängen.[94] Es sind dazu jedoch auch stichprobenartige, überraschende Prüfungen notwendig – aber regelmäßig auch ausreichend – um vorsätzliche Verstöße gegen Vorschriften zu verhindern. Zweck der Überwachung ist, dass den Mitarbeitern vor Augen gehalten wird, dass Verstöße entdeckt werden können. Andere Anforderungen sind freilich zu stellen wenn abzusehen ist, dass diese Maßnahmen nicht ausreichen, um ihren Zweck zu erfüllen, etwa weil der Umfang der Überprüfungen zu gering ist. Ist dies der Fall, sollten auch überraschend durchgeführte Geschäftsprüfungen abgehalten werden.[95]

Aus der Spruchpraxis der Gerichte lassen sich auch über allgemeine Erwägungen hinaus weitere Anhaltspunkte für die Überwachungspflicht entnehmen und nach insgesamt fünf Pflichten differenzieren.[96] Dazu gehört die Pflicht, bei Verdachtsmomenten unverzüglich einzuschreiten. Außerdem muss das Unternehmen so organisiert werden, dass Pflichtverletzungen vermieden werden. Ferner muss der Vorstand laufend Kontrollen durchführen. Des Weiteren können gesteigerte Überwachungspflichten erforderlich werden, wenn es in der Vergangenheit bereits zu Verstößen gekommen ist.[97] Bei größeren oder komplex organisierten Unternehmen sowie bei besonderen Gefahren kann es notwendig sein, Aufsichtspersonen auf verschiedenen Ebenen unterhalb der Leitungsebene zu bestellen.[98] So kann der Vorstand entlastet werden, behält jedoch die Aufsichtspflicht über die von ihm eingesetzten Aufsichtspersonen.[99]

Insgesamt werden keine Maßnahmen verlangt, die nicht durchführbar oder beispielsweise aus Kostengründen nicht zumutbar sind.[100] Außerdem soll weder das Vertrauensverhältnis zwischen Arbeitgeber und Arbeitnehmer überspannt noch das Betriebsklima zerstört oder die Würde der Betriebsangehörigen durch übertriebene Maßnamen verletzt wird.[101]

---

[94] *BGH*, Urt. v. 25.6.1985 – KRB 2/85 (KG), NStZ 1986, 34.
[95] *BHG*, Urt. v. 25.6.1985 – KRB 2/85 (KG), NStZ 1986, 34.
[96] *Fleischer*, AG 2003, 291, 294 ff.
[97] *Fleischer*, AG 2003, 291, 294 f.
[98] *Hauschka*, ZIP 2004, 877, 881.
[99] *Rogall*, in: KK-OWiG, § 130 Rn. 66.
[100] *Adam*, Wistra 2003, 285, 288.
[101] *Rogall*, in: KK-OWiG, § 130 Rn. 49.

5. Helpline und Whistleblowing

Eine telefonische Beratungsstelle – auch „Helpline“ oder „Whistleblower-Hotline“ genannt – soll aus Sicht der Mitarbeiter zwei Zwecke erfüllen. Zum einen sollen die Mitarbeiter bei konkreten rechtlichen Fragen oder Problemen in Zusammenhang mit ihrer Tätigkeit die Möglichkeit haben, sich beraten zu lassen. Zum anderen soll Mitarbeitern, denen Unregelmäßigkeiten auffallen, ein Ansprechpartner sowohl unabhängig von ihrem direkten Vorgesetzten als auch unabhängig vom Unternehmen selbst angeboten werden. Aus Sicht des Unternehmens besteht der Vorteil, dass so den Mitarbeitern auch in kritischen Situationen eine sofortige Anlaufstelle zur Verfügung steht. Des Weiteren erhöht sich die Entdeckungsgefahr für unrechtmäßige Praktiken, wenn auch anonyme Hinweise verfolgt werden.[102] Dadurch kann eine abschreckende Wirkung erzielt werden, da sich potenzielle Täter weniger durch drohende strenge Strafen abschrecken lassen, als von der Furcht, entdeckt zu werden.[103]

Die Funktion eines Ansprechpartners bei Unregelmäßigkeiten, auch „Whistleblowing“ genannt, ist nicht unumstritten. Amerikanische und ausländische Unternehmen, die an US-Börsen notiert sind, sind nach Section 301 (4) des Sarbanes-Oxley Act 2002[104] dazu verpflichtet, ihren Mitarbeitern Gelegenheit zu geben, vertrauliche bzw. anonyme Hinweise weiter zu geben.[105]

In Deutschland gehört es an sich schon zu den arbeitsvertraglichen Nebenpflichten des Arbeitnehmers, den Arbeitgeber über alle wichtigen Vorkommnisse im Betrieb in Kenntnis zu setzten, vor allem um Schäden des Unternehmens zu verhindern.[106] Von daher wird die Schaffung einer Whistleblowing-Stelle zwar als *Good Practice* zur Ausgestaltung der Compliance-Organisation eines Unternehmens anerkannt; sie soll allerdings keinen notwendigen Bestandteil einer angemessenen Compliance-Organisation darstellen.[107]

Das Problem bei der Einrichtung von Whistleblowing-Hotlines besteht darin, dass damit mittelbar die Förderung von „Denunziantentum“ verbunden ist. Tatsächlich ist es wichtig klarzustellen, dass sich Mitarbeiter durch das „Anschwär-

[102] *Bürkle*, DB 2004, 2158, 2161.
[103] *Bussmann/Matschke*, CCZ 2009, 132, 135.
[104] Sarbanes-Oxley Act of 2002, H.R. 3763.
[105] *v. Pelchrzim*, CCZ 2008, 25.
[106] *Mengel*, Compliance und Arbeitsrecht, Kap. 1 Rn. 25.
[107] *Uwe H. Schneider/Nowak*, in: FS Kreutz, S. 865.

zen“ von Kollegen nicht besser stellen können oder das System dazu missbrauchen können, unliebsame Konkurrenten loszuwerden. Aus diesem Grund ist es auch nicht zumutbar, wenn für Denunziationen eine Belohnung gewährt wird.[108] Außerdem wird befürchtet, dass Whistleblowing sich von einer außergewöhnlichen Tat, die im Regelfall mit vielen Bedenken und Zweifeln bei den Betroffenen einhergeht, zu einem alltäglichen Vorgang wandelt, welcher als Mittel zur Unternehmensführung dient.[109]

Wesentlich für das Unternehmensklima ist bereits, wie ein Whistleblowing-System eingeführt wird. Solche Systeme können entweder als Möglichkeit zur Informationsweitergabe eingerichtet werden oder als Pflicht für die Mitarbeiter, Informationen weiter zu geben. Ein gezieltes Fördern von Anzeigen, insbesondere unabhängig vom Schweregrad der Tat, könnte sich tatsächlich zu einem Problem für das Unternehmensklima entwickeln und kann den Arbeitnehmern nicht per Direktionsrecht auferlegt werden.[110] Das bloße zur Verfügung stellen von Ansprechpartnern hingegen gilt als unproblematisch.[111]

Kernelement beider Funktionen einer Helpline ist die Gewährleistung der Anonymität. Nur so besteht die Möglichkeit, dass Mitarbeiter, die sich bereits in einer mit Zweifel behafteten Situation befinden, mit Angst vor Konsequenzen oder Reputationsverlust die Hotline annehmen. Dabei ist zu berücksichtigen, dass die Mitarbeiter insbesondere vor dem Hintergrund Zweifel haben können ihre Beobachtungen weiter zu leiten, weil es für Hinweisgeber nur schwer einzuschätzen ist, ob es sich bei einer beobachteten Handlung bereits um ein Vergehen handelt oder diese noch ordnungsgemäß war.[112] Es ist auch möglich, dass es sich bei dem Beschuldigten um einen Vorgesetzten handelt, so dass der Hinweisgeber fürchten müsste, dass seine Meldung Konsequenzen für ihn selbst oder seine weitere Tätigkeit hat. Daher sollte den Mitarbeitern klar sein, dass ein berechtigter Hinweis keine Auswirkungen auf sie selbst oder ihre Stellung im Unternehmen hat.[113]

Der Ansprechpartner kann sowohl ein Mitarbeiter aus dem Unternehmen als auch eine Person von außerhalb sein. Mögliche Hemmschwellen können bei

[108] *Rogall*, in: KK-OWiG, § 130 Rn. 49.
[109] *Mahnhold*, NZA 2008, 737.
[110] *Mengel*, Compliance und Arbeitsrecht, Kap. 1 Rn. 25.
[111] *Mahnhold*, NZA 2008, 737, 743.
[112] *v. Pelchrzim*, CCZ 2008, 25, 26.
[113] *Rodewald/Unger*, BB 2007, 1629, 1630.

manchen Mitarbeitern eventuell weiter gesenkt werden, wenn die Helpline zu einem externen Rechtsanwalt führt, da dieser einer besonderen berufsrechtlich begründeten Schweigepflicht unterliegt.[114] Jedoch ist die Weitergabe der Kenntnisse dann mit zeitlichen Verzögerungen verbunden, da der Anwalt diese erst mal einschätzen und dann weiterleiten muss. Demgegenüber kennt sich ein Compliance-Officer besser mit unternehmensinternen Abläufen aus und genießt bei den Mitarbeitern möglicherweise mehr Vertrauen als ein unbekannter externer Ansprechpartner.[115]

6. Sanktionen

Für die Organe der Unternehmensleitung besteht eine Rechtspflicht zu Handeln, wenn ihnen Unregelmäßigkeiten bekannt werden. Das Unterlassen von entsprechenden Maßnahmen kann dann eine Haftung der Unternehmensleitung begründen, so dass sich aus jeder Kontrollpflicht auch eine Handlungspflicht ergibt.[116]

Zugleich können Compliance-Organisationen dauerhaft nur dann effektiv sein, wenn Verstöße nicht folgenlos bleiben.[117] Verstöße müssen organisatorische und gegebenenfalls auch personelle Konsequenzen haben. Diese müssen von Beginn an angedroht werden, um eine abschreckende Wirkung entfalten zu können.[118] Die Androhung von Sanktionen verleiht einer Compliance-Organisation zusätzlichen Nachdruck, stärkt ihre Glaubwürdigkeit und dient der Abschreckung.[119]

In Bezug auf den Inhalt von Sanktionen wird zum Teil eine „Zero Tolerance"-Politik vertreten. Das bedeutet, dass Mitarbeiter, die gegen geltende Vorschriften verstoßen, unmittelbar gekündigt werden. Dieses Vorgehen ist sicherlich schwierig für den einzelnen Mitarbeiter, wird jedoch dadurch relativiert, dass dieser auf Grund von Schulungen und angebotenen Beratungen, sowie Hilfestellungen durch das Unternehmen in der Lage ist, rechtswidriges Handeln im Vorfeld zu erkennen und sich entsprechend zu verhalten.[120] Darüber hinaus kann das Bagatellisieren oder das Unterlassen von Maßnahmen als Indiz dafür gewertet werden, dass der Vorstand die Gesetzesübertretung billigt oder ihr zumindest gleich-

[114] *Lampert*, in: Hauschka (Hrsg.), Corporate Compliance, § 9 Rn. 34.
[115] *Bürkle*, DB 2004, 2158, 2160.
[116] *Hauschka*, ZIP 2004, 877, 881.
[117] *Mengel/Hagemeister*, BB 2007, 1386, 1392; *Vogt*, NJOZ 2009, 4206, 4209.
[118] *Hauschka*, DB 2006, 1143, 1145.
[119] *Pampel*, BB 2007, 1636, 1638.
[120] *Lampert*, in: Hauschka (Hrsg.), Corporate Compliance, § 9 Rn. 32.

gültig begegnet.[121] Dadurch würde ein Compliance-System letztlich ausgehöhlt werden.

7. Dokumentation

Schließlich sind die eingerichteten Informations- und Kontrollsysteme, wie zum Beispiel Berichtssysteme, Gesprächsprotokolle und sonstige Maßnahmen hinreichend genau zu dokumentieren.[122] Dies ist für Unternehmen zwingend, die den Ausführungsbestimmungen des Sarbanes Oxley Act unterliegen. Art. 404, 406 und 407 Sarbanes Oxley Act verlangen einen *internal control report*, der in den Geschäftsbericht des Unternehmens aufzunehmen ist.[123]

Unternehmen die nicht dem Sarbanes-Oxley Act unterliegen sollten ebenfalls auf eine sorgfältige Dokumentation achten. Bei möglichen, später festgestellten Verstößen kann so der Entlastungsbeweis geführt werden und möglicherweise eine Haftungsbeschränkung erwirkt werden.[124] Daher sollte auch das Unterlassen einer Handlung genau dokumentiert werden, falls eine Pflicht zum Handeln bestehen könnte.[125] Weiterhin ist zu beachten, dass größere Zeiträume vergehen können, bis es zu möglichen Haftungsprozessen kommt, so dass es schwierig sein kann, Entscheidungen und Maßnahmen ohne Dokumentation zu rekonstruieren. Daher kann mit einem Compliance-System ohne hinreichende Dokumentation nur bedingt eine Haftungsbeschränkung erreicht werden.[126]

Darüber hinaus kann das Erfordernis zur Dokumentation, insbesondere von Gründen für getroffene Entscheidungen, dazu führen, dass diese intensiver reflektiert werden und es dadurch zu einer Verbesserung der Qualität der Entscheidungsfindung kommt.[127]

---

[121] *Bussmann/Matschke*, CCZ 2009, 132, 136.
[122] *Rodewald/Unger*, BB 2006, 113, 115.
[123] *Uwe H. Schneider*, ZIP 2003, 645, 650.
[124] *Lampert*, in: Hauschka (Hrsg.), Corporate Compliance, § 9 Rn. 33.
[125] *Rodewald/Unger*, BB 2006, 113, 115.
[126] *Hauschka*, DB 2006, 1143, 1146.
[127] *Rodewald/Unger*, BB 2006, 113, 115.

V. Stellung des Compliance-Officers

Im Fall der *Bahn* wurde ausgesagt, dass der Vorstand über das Vorgehen des Compliance-Officers bei der Überprüfung der Mitarbeiter nicht informiert gewesen sei. Fraglich ist, wie weit die Befugnisse eines Compliance-Officers typischerweise reichen und welche Stellung dieser im Unternehmen haben sollte. Hierbei ist vor allem zu klären, ob der Compliance-Officer weisungsgebunden ist und welche Berichtspflichten ihm auferlegt wurden.

Da der Arbeitsvertrag des Compliance-Officers der *Bahn* nicht öffentlich einsehbar ist, soll davon ausgegangen werden, dass diesem so viele Kompetenzen eingeräumt wurden, wie für seine Arbeit *sinnvollerweise* notwendig wäre. Welche Kompetenzen das im Einzelnen sind, wird im Folgenden untersucht.

1. Aufgaben eines Compliance-Officers

Der Compliance-Officer hat eine Schnittstellen- und Steuerungsfunktion im Unternehmen inne.[128] Ihm kommt die Aufgabe zu, die Unternehmensleitung in compliancerelevanten Fragen zu unterstützen und zu beraten. Er berichtet in festgelegten zeitlichen Abständen oder bei Bedarf auch ad hoc über wesentliche rechtliche Vorfälle im Unternehmen sowie über anstehende rechtliche Veränderungen im Unternehmensumfeld.[129] Hierbei hat er ein jederzeitiges Vortragsrecht beim Vorstand.[130] Der Compliance-Officer bewertet die Informationen im Vorfeld und gibt der Geschäftsleitung nur die relevanten Fakten weiter. Dabei kann er der Geschäftsleitung auch eigene Vorschläge für Maßnahmen unterbreiten, die sich durch das Auswerten der Informationen ergeben können.[131]

Der Compliance-Officer sorgt außerdem für Schulung und Information der Mitarbeiter. Diese Aufgabe muss er nicht zwangsläufig selbst erledigen, er kann sie auch externen Dienstleistern oder anderen Mitarbeitern aus der Compliance-Organisation zuweisen.[132]

---

[128] *Bürkle*, in: Hauschka (Hrsg.), Corporate Compliance, § 8 Rn. 10.
[129] *Rodewald/Unger*, BB 2007, 1629, 1632; *Bürkle*, in: Hauschka (Hrsg.), Corporate Compliance, § 8 Rn. 12.
[130] *Lösler*, WM 2007, 676, 681.
[131] *Rodewald/Unger*, BB 2007, 1629, 1632.
[132] *Bürkle*, in: Hauschka (Hrsg.), Corporate Compliance, § 8 Rn. 13.

2. Tätigkeitsvoraussetzungen

Wie schon im Zusammenhang mit der Pflicht zur Einrichtung einer Compliance-Organisation und deren Ausgestaltung erwähnt, gibt es außer im Wertpapierhandelsgesetz keine konkreten Vorgaben für die Ausgestaltung von Compliance-Systemen. Nach § 33 WpHG muss Compliance drei wichtige Kriterien erfüllen: Sie muss dauerhaft, wirksam und unabhängig sein.[133]

Die Kriterien Dauerhaftigkeit und Wirksamkeit sind durch institutionell geeignete Organisationsverfügungen und Arbeitsanweisungen im Unternehmen verankert. Zu diesem Zweck hat das Unternehmen sicher zu gehen, dass der Compliance-Officer über ausreichende Fachkenntnisse verfügt, und ihm in ausreichendem Maß Mittel und Kompetenzen zustehen.[134] Dazu gehören auch Zutritts-, Einsichts- und Auskunftsrechte zu allen Abteilungen und geschäftlichen Obliegenheiten.[135] Die Unabhängigkeit umfasst mehrere Aspekte, wie etwa den der finanziellen Unabhängigkeit, der Weisungsfreiheit und der organisatorischen Unabhängigkeit.[136]

Die Regelungen des Kapitalmarktrechts können indes nicht ohne weiteres auf andere Wirtschaftsbranchen angewendet werden.[137] Dennoch können sie einen Anhaltspunkt bieten. So sollte dem Compliance-Officer zumindest fachliche Weisungsfreiheit zugebilligt werden, da dieser in der Regel als einziger den Überblick über alle compliancerelevanten Vorgänge im Unternehmen hat[138]. Zu den Kompetenzen des Compliance-Officers sollten zudem auch alle Maßnahmen, die der Prävention oder Aufklärung von möglichen Straftaten und Ordnungswidrigkeiten dienen, gehören. Nicht in den Aufgabenbereich sollte allerdings das eigenständige Ergreifen von konkreten Abhilfemaßnahmen fallen, da dies zu weit in den Entscheidungs- und Leitungsbereich des Vorstandes eindringen würde.

---

[133] *Illing/Umnuß*, CCZ 2009, 1, 3.
[134] *Röh*, BB 2008, 398, 403.
[135] *Lösler*, NZG 2005, 104, 108.
[136] *Lösler*, NZG 2005, 104, 107.
[137] *Spindler*, WM 2008, 905, 908; eine ausführliche Begründung dazu findet sich auch bei *Illing/Umnuß*, CCZ 2009, 1, 3.
[138] *Illing/Umnuß*, CCZ 2009, 1, 4.

D. COMPLIANCE BEI DER BAHN

I. Aufgabenzuweisung

Der Vorstand der *Bahn* hat im Februar 2001 den Beschluss gefasst, eine zentrale Compliance-Organisation einzurichten. Dazu wurde direkt unterhalb der Ebene des Konzernvorstandes ein Lenkungskreis Compliance mit weitgehenden Befugnissen eingerichtet. Dieser konnte auch ohne Zustimmung oder Unterrichtung der Linienverantwortlichen tätig werden.[139] Maßnahmen bei Verdachtsfällen wurden in Zusammenarbeit mit der Konzernrevision ergriffen. Der Leiter der Konzernrevision berichtete dem Vorstandsvorsitzenden.[140]

Am 1. September 2007 wurde die Funktion des „Chief Compliance Officers" eingerichtet, der direkt dem Vorstandsvorsitzenden unterstellt ist und ihm berichtet.[141]

II. Aufstellung von Standards und Schulungen

Es wurden Verhaltensrichtlinien für den Bahn-Konzern erlassen. Diese wurden den Mitarbeitern und Führungskräften in Seminaren und Workshops, zu denen Experten aus der Justiz und der Wirtschaft hinzugezogen wurden, näher gebracht.[142]

III. Überwachung

Überwacht wurden die Arbeitnehmer bei der *Bahn* beispielsweise durch den Abgleich ihrer Personaldaten mit denen von Lieferanten oder mittels automatischer Durchsuchung ihrer E-Mails nach bestimmten Schlagwörtern.

IV. Whistleblowing und Sanktionen

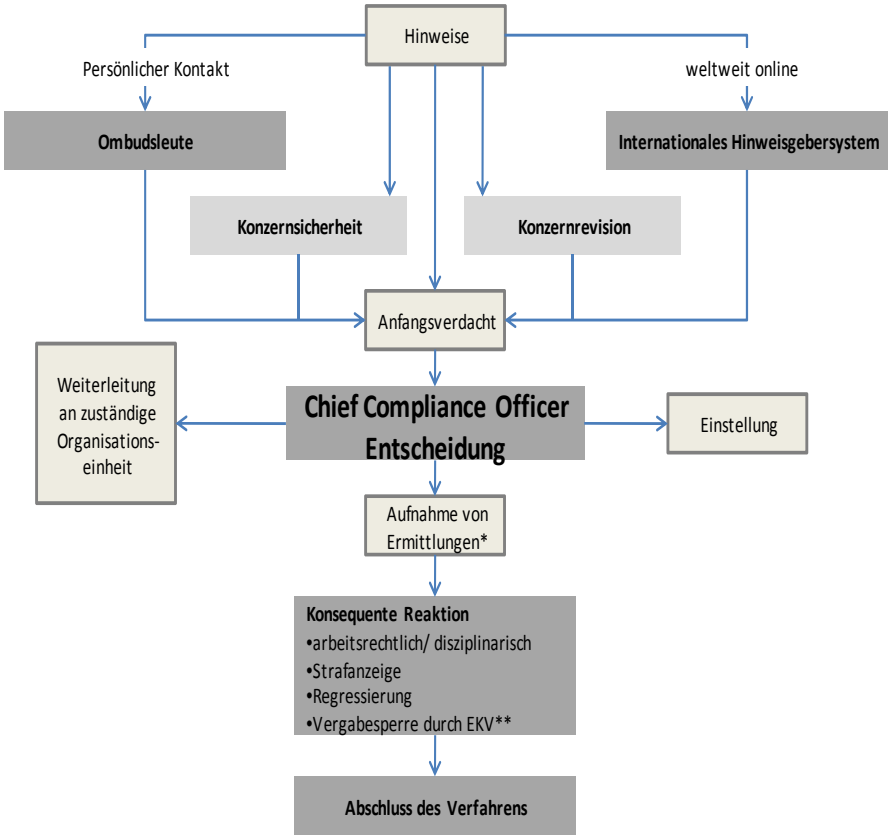
Hinweisgebern, denen Unregelmäßigkeiten auffallen, stehen bei der *Bahn* zwei externe Rechtsanwälte als unabhängige Ansprechpartner zur Verfügung.[143] Des

[139] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 5.
[140] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 14.
[141] *Deutsche Bahn AG*, Compliance Bericht 2006/2007, S. 6.
[142] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 6.
[143] *Deutsche Bahn AG*, in Compliance Bericht 2006/2007, S. 14.

Weiteren wurde ein weltweites elektronisches System für Hinweisgeber installiert. Hinweise können sowohl über dieses System als auch an die Anwälte anonym weitergeleitet werden.[144] Die eingehenden Hinweise wurden zwischen 2001 und 2007 dem Lenkungskreis Compliance zu weiteren Veranlassungen vorgelegt. Mittlerweile liegt die Entscheidung darüber, welche Hinweise weiter verfolg werden, beim Chief Compliance Officer.[145] Dieser entscheidet nun, ob eingehende Hinweise weiter verfolgt werden oder die Untersuchung eingestellt wird. Ermittlungen werden entweder intern oder extern geführt, beispielsweise durch hinzuzuziehende Rechtsanwaltskanzleien, Wirtschaftsprüfer, Wirtschaftsauskunftsteien.[146] Interne Ermittlungen bestehen je nach Fall aus Personalanfragen, Internetrecherchen, Buchhaltungs- und Vertragsrecherchen, Lieferantenüberprüfungen, Abfragen bei Wirtschaftsauskunfteien und Handelsregistern, Befragungen der Betroffenen unter Einbeziehung der Vorgesetzen und der Personalabteilung sowie zusätzlich bei Erhärtung des Verdachts auf Straftaten in der Analyse von gespeicherten Daten oder E-Mails der Betroffenen.[147] Die Ermittlungsaufgaben wurden in der Regel von der Konzernrevision übernommen.[148] Die Konzernrevision unterstützte auch den Prüfungsausschuss des Aufsichtsrates bei der Bewertung der Wirksamkeit des internen Kontrollsystems.[149]

Die nachfolgende Abbildung 1 stellt schematisch dar, wie Hinweisen bei der *Bahn* nachgegangen wird.

[144] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 6.
[145] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 12.
[146] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 11.
[147] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 12/13.
[148] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 6.
[149] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 15.



* Fallbezogene Unterstützung durch Konzernrevision, Konzernsicherheit und Rechtsabteilung; ** Entscheiderkreis Vergabesperre

Abbildung 1: Bereichsübergreifende Zusammenarbeit bei Anfangsverdacht bei der Deutschen Bahn AG[150]

Neben arbeitsrechtlichen Konsequenzen, wie beispielsweise Kündigungen oder Abmahnungen, wurde zusätzlich eine Sperrliste aufgestellt, auf der alle Unternehmen aufgeführt werden, die in Korruptionsfälle verwickelt waren und deswegen keine Aufträge mehr von der *Bahn* erhalten.[151]

V. Dokumentation

Alle Verdachtsfälle, die durch die Compliance-Organisation der *Bahn* bearbeitet werden, sind präzise zu dokumentieren.[152] Dies scheint allerdings nicht in der Form geschehen zu sein, denn die *Bahn* hat Schwierigkeiten bei der Aufklärung

[150] Quelle: *Deutsche Bahn AG*, Compliance Bericht 2006/2007, S. 15.
[151] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 6.
[152] *Deutsche Bahn AG*, Korruptionsbericht 2005, S. 7.

der „Datenaffäre“ eingeräumt, die sich aus teilweise nicht vorhandener oder teils nicht ausreichender Dokumentation ergeben.[153]

Hier zeigt einmal mehr der Nachteil unterlassener Dokumentation: Während eine unzulängliche Dokumentation auf der einen Seite dazu führen kann, dass getroffene oder unterlassene Entscheidungen nicht mehr nachvollzogen werden können, kann es auf der anderen Seite dazu führen, dass – möglicherweise zu weit reichende – Untersuchungen im Rahmen von Compliance-Maßnahmen nicht mehr zu rechtfertigen sind. Dadurch kann also gerade das Gegenteil dessen erreicht werden, das es zu erreichen gilt. Statt positiver Publicity für eine „schlagkräftige“ Compliance-Organisation zu generieren, wird gerade negative Publicity für das Unternehmen wegen einer möglicherweise unverhältnismäßigen und insgesamt über das Ziel hinausschießenden Tätigkeit der Compliance-Organisation erzeugt.

[153] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 10.

E. COMPLINANCE-MAßNAHMEN IN DER DATENAFFÄRE

Wie bereits aus dem Kapitel „Darstellung des Sachverhalts“ ersichtlich, gab es im Rahmen der Datenaffäre bei der *Bahn* unterschiedliche Sachverhalte. Für die weitere Untersuchung in dieser Arbeit ist es zunächst von Bedeutung, diejenigen Fälle, die auf konkrete Hinweise zurückzuführen sind von den Fällen zu trennen, die auf Mutmaßungen zurückgehen.

So wurden etwa Screenings ohne konkrete Hinweise auf bestimmte Personen durchgeführt und dienten allein der Überwachung der Mitarbeiter. Wieder anders sind demgegenüber die Fälle zu betrachten, bei denen konkrete Hinweise vorangingen, da in diesem Fall der Vorstand sogar verpflichtet gewesen sein könnte, zu handeln.

I. Ermittlungen bei Verdacht

Da der Vorstand generell für die Überwachung des Unternehmens zuständig ist, trifft ihn auch die Pflicht, Hinweisen auf Gesetzesverstöße oder sonstigen Unregemäßigkeiten im Unternehmen nachzugehen.[154] Die Pflicht zur Ermittlung von Sachverhalten endet dort, wo diese nicht mehr vom Unternehmensinteresse gedeckt ist, da der Vorstand sich bei seiner Tätigkeit vom Unternehmensinteresse leiten lassen muss.[155] Dies gilt auch für Ermittlungen, deren möglicher Nutzen außer Verhältnis zum erforderlichen Aufwand steht, um alle erforderlichen Informationen zu erhalten.

Im Fall der *Bahn* wurden Hinweise nach Bewertung durch den Compliance-Officer konsequent verfolgt. Das Auftragsvolumen allein für die Firma *Network* belief sich zwischen 1998 und 2007 auf insgesamt rund 800.000 Euro.[156] Darin enthalten sind jedoch sämtliche Tätigkeiten, die die Firma *Network Deutschland GmbH* für die *Bahn* ausführte.

Demgegenüber stehen Einnahmen von 30 Millionen Euro im Zeitraum 2001 bis 2007, die durch die Aufdeckung von Korruptionsfällen auf einem von der *Bahn* eigens dafür eingerichteten Konto verbucht werden konnten. Hinzu kommen

---

[154] *Fleischer*, AG 2003, 291, 294; *Wagner*, CCZ 2009, 8, 12.
[155] *Wagner*, CCZ 2009, 8, 17.
[156] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 26.

Beträge in zweistelligem Millionenbereich von betroffenen Firmen als Ausgleichszahlungen oder Verrechnungen an Wiedergutmachungen von Korruptionsschäden.[157] Somit sprechen zumindest die wirtschaftlichen Erfolge dafür, dass bei den Ermittlungen im Unternehmensinteresse gehandelt wurde. Weniger eindeutig ist, in wieweit die Beschaffung rechtlich fragwürdiger Daten im Unternehmensinteresse liegt.

In diesem Zusammenhang ist aus den vorhandenen Materialien nicht ersichtlich, ob die *Bahn* über die Arbeitsweise der externen Dienstleister informiert war, mit denen sie zusammengearbeitet hat. Auch ist nicht ersichtlich, welche Daten tatsächlich beschafft werden sollten. Lediglich in einem Fall wurden von externen Dienstleistern gesammelte Daten durch die *Bahn* als zu weitreichend und nicht in Auftrag gegeben zurückgewiesen.

II. Ermittlungen als Überwachungsmaßnahmen

Der Bundesgerichtshof sieht es als Zweck von Überprüfungen an, Mitarbeitern vor Augen zu halten, dass Verstöße entdeckt und geahndet werden können.[158] Da jedoch weder die Mitarbeiter selbst noch der Datenschutzbeauftragte oder Arbeitnehmervertreter über diese Überwachungsmaßnahmen informiert wurden,[159] konnten sie kaum eine abschreckende Wirkung entfalten.

Insgesamt wurden die Daten von annähernd 200.000 Bahn-Mitarbeitern überprüft. Die *Bahn* hat 240.000 Mitarbeiter, davon ca. 182.000 in Deutschland.[160] Somit wurde fast jeder Mitarbeiter der *Bahn* überprüft. Die *Bahn* selbst räumt ein, dass die Zahl der Überwachten Personen unverhältnismäßig hoch gewesen sei.[161]

---

[157] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 7.
[158] *BGH*, Urt. v. 25.6.1985 – KRB 2/85 (KG), NStZ 1986, 34.
[159] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 13.
[160] *Deutsche Bahn AG*, Homepage, http://www.deutschebahn.com/site/bahn/de/unternehmen/presse/themendienst/konzern/bilanz__pk__2008.html.
[161] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 13.

F. ZWISCHENERGEBNIS

Zunächst ist festzuhalten, dass bei der *Bahn* eine Compliance-Organisation existiert.

Die Aspekte, die für eine effektive Compliance-Organisation notwendig sind, wurden von der *Bahn* bei der Einrichtung ihrer Organisation berücksichtigt. So wurden Standards und Verhaltensrichtlinien aufgestellt, die den Mitarbeitern durch Schulungen näher gebracht werden. Schulungen werden auch in Zusammenarbeit mit externen Personen durchgeführt. Für Mitarbeiter, denen Unregelmäßigkeiten auffallen, gib es die Möglichkeit diese anonym in elektronischer Form oder telefonisch einem von zwei externen Rechtsanwälten zu melden. Solchen Hinweisen wird grundsätzlich nachgegangen, unabhängig davon ob diese anonym sind oder nicht. Regelverstöße werden konsequent geahndet. Als Sanktionsmöglichkeiten stehen arbeitsrechtliche oder disziplinarische Maßnahmen, Strafanzeigen oder bei Beteiligung von Unternehmen die Auftragsvergabesperre zur Verfügung. Die *Bahn* publiziert sowohl die Tatsache, dass Regelverstöße geahndet werden, wie auch die drohenden „Sanktionen“ durch das Unternehmen. Die Mitarbeiter, die mit Compliance-Angelegenheiten beschäftigt sind, sind gehalten, ihr Handeln sorgfältig zu dokumentieren. Zumindest in diesem Punkt scheinen bei der Umsetzung der Unternehmensvorgaben gewisse Unregelmäßigkeiten vorzuliegen, wie die *Bahn* eingeräumt hat.

Zu den Aufgaben des Compliance-Officers bei der *Bahn* gehört die Selektion der Hinweise, denen nachgegangen werden soll. Des Weiteren berichtet er direkt an den Vorstandsvorsitzenden und ist für Schulungen der Mitarbeiter sowie deren Befragung zuständig.

Anzumerken ist jedoch, dass das einzige Gebiet auf das sich die gesamte Compliance-Organisation der *Bahn* konzentriert, die Bekämpfung der Korruption im Unternehmen ist. Durch die Datenaffäre wird jedoch ersichtlich, dass sich Compliance im Unternehmen nicht ausschließlich auf Korruptionsbekämpfung beschränken sollte. Zumindest beim Datenschutz scheint es noch Probleme bei der *Bahn* zu geben.

Aus finanzieller Sicht war das Unternehmensinteresse der *Bahn* bei den Überwachungsmaßnahmen gewahrt. Nicht im Unternehmsinteresse kann es liegen, die

Beschaffung von Daten in Auftrag zu geben, die, wie die *Bahn* selbst einräumte, nicht oder nicht ohne weiters öffentlich zugänglich sind.[162]

Schließlich erscheint die Anzahl der Mitarbeiter, die im Rahmen von Datenabgleichen überprüft wurden, auch nach Ansicht der *Bahn*, unverhältnismäßig hoch.[163]

[162] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 27.
[163] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 13.

G. DATENABGLEICH

Das informationelle Selbstbestimmungsrecht aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG schützt die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[164] Die Verarbeitung von persönlichen Daten unterliegt daher zunächst den Bestimmungen des BDSG als gesetzlicher Schranke dieses Grundrechts.[165] Der Schutzbereich des BDSG ist jedoch begrenzt. Grund dafür ist zum einen, dass nach § 1 Abs. 3 Satz 1 BDSG das Gesetz gegenüber bereichsspezifischen Regelungen des Bundes, wie beispielsweise dem Telekommunikationsgesetz (TKG), subsidiär ist. Zum anderen fällt im Bereich der Privatwirtschaft lediglich die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, die dateigebunden oder automatisiert erfolgt, unter den Anwendungsbereich des BDSG.[166]
In dem hier dargestellten Sachverhalt ist fraglich, ob der Abgleich von Mitarbeiterdaten mit den Daten von Liefanten und Vertragspartnern der *Bahn* zulässig war. Nach § 43 Abs. 2 und Abs. 3 BDSG würde ein unzulässiger Datenabgleich eine Ordnungswidrigkeit darstellen.[167] Diese könnte mit einem Bußgeld von bis zu 250 000 Euro geahndet werden.

I. Erhebung von Daten

Im Rahmen der Privatwirtschaft fällt das Erheben von Daten in den Anwendungsbereich des BDSG, wenn dies zur Speicherung geschieht.[168] Nach § 4 Abs. 1 BDSG ist u.a. die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zulässig, wenn das BDSG selbst oder eine vorrangige Norm dies gestatten oder der Betroffene einwilligt. Nach der Legaldefinition in § 3 Abs. 3 BDSG ist unter Erheben das Beschaffen von Daten zu verstehen. Ein Erheben von Daten

[164] *BVerfG*, Urt. v. 15. 12. 1983 – 1 BvR 209/83, NJW 1984, 419.
[165] *Trittin/Fischer*, NZA 2009, 343.
[166] *Gola*, Datenschutz und Multimedia am Arbeitsplatz, Rn. 120.
[167] *Kock/Francke*, NZA 2009, 646, 651.
[168] *Gola*, Datenschutz und Multimedia am Arbeitsplatz, Rn. 121.

liegt damit dann vor, wenn die erhebende Stelle Kenntnis von den betreffenden Daten erhält.[169]

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Erheben von Daten für eigene Geschäftszwecke zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen dient. Bei Arbeits- oder Lieferantenverträgen dient die Zahlung der vertraglichen Vergütung – in der Regel per Überweisung auf ein Bankkonto – und die Möglichkeit der schriftlichen Kontaktaufnahme dem Vertragszweck.[170] Daher ist das Erheben von Konto- und Adressdaten bei solchen Verträgen grundsätzlich unproblematisch.

Darüber hinaus hat das *BAG* entschieden, dass durch die elektronische Verarbeitung der Personaldaten Verwaltungsvereinfachungen für den Arbeitgeber entstünden, die auf andere Weise nicht erreicht werden können.[171] Somit besteht ein berechtigtes Interesse des Arbeitgebers an der elektronischen Verarbeitung der o.g. Daten der Mitarbeiter, während die dadurch verursachte Beeinträchtigung des Arbeitnehmers lediglich geringfügig ist.

Entsprechend war die Erhebung und Speicherung der Arbeitnehmer- und Lieferantendaten bei der *Bahn* daher zulässig.

II. Verarbeitung von Daten

Die Verarbeitung von personenbezogenen Daten ist nach § 4 Abs. 1 BDSG zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Unter einer Verarbeitung ist nach der Legaldefinition in § 3 Abs. 4 Satz 1 BDSG jedes Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten zu verstehen.

Mögliche Rechtsgrundlagen für die Datenabgleiche der *Bahn* sollen im Folgenden dargestellt werden.

---

[169] *Dammann*, in: Simitis, Bundesdatenschutzgesetz, § 3 Rn. 102.
[170] *Bisges*, MMR 2009, Heft 4, S. XX.
[171] *BAG*, Urt. v. 22. 10. 1986 – 5 AZR 660/85, DB 1987, 1048, 1050.

1. Zulässigkeit nach BDSG

Nach § 27 Abs. 1 Satz 1 Nr.1 BDSG findet § 28 BDSG Anwendung, wenn es um die Nutzung und Verarbeitung personenbezogener Daten bei nicht-öffentlichen Stellen geht.

Die Zulässigkeit der Nutzung der Daten bestimmt sich nach § 28 BDSG. § 28 Abs. 1 BDSG enthält drei Zulässigkeitsvarianten, die grundsätzlich unabhängig voneinander die Zulässigkeit des Erhebens, Speicherns, Veränderns bzw. Nutzens von personenbezogenen Daten begründen können.[172]

Strittig jedoch ist, ob diese drei „Alternativen" tatsächlich alternativ angewendet werden können. Nach überwiegender Meinung wird dies verneint oder es wird zumindest gefordert, dass die Zulässigkeitsalternativen bei einem bestehenden Vertragsverhältnis eng auszulegen sind.[173] Das *BAG* hat dazu festgestellt, dass es nicht zulässig ist tiefer in die Privatsphäre des Arbeitnehmers vorzudringen, als es im Rahmen des Arbeitsverhältnisses unbedingt erforderlich ist.[174] Somit ist § 28 Abs. 1 Nr. 2 BDSG nicht im Sinne eines Auffangtatbestands zu verstehen, der es verarbeitenden Stellen ermöglicht, Daten zu nutzen, wenn § 28 Abs. 1 Satz 1 Nr. 1 BDSG dies ausschließt.[175]

a) ZULÄSSIGKEIT NACH § 28 ABS. 1 SATZ 1 NR. 1 BDSG

Stehen die verarbeitende Stelle und der Betroffene durch Vertrag oder durch vertragsähnliches Verhältnis in einer Rechtsbeziehung, begründet dies typischerweise die Anwendbarkeit des § 28 Abs. 1 Satz 1 Nr. 1 BDSG.[176] Die Art des Vertrages ist dabei irrelevant.[177] Voraussetzung ist jedoch, dass die Daten der Zweckbestimmung des Vertrages dienen.

Dem Wortlaut nach schließt § 28 Abs. 1 Satz 1 Nr. 1 BDSG dabei jede Nutzung oder Verarbeitung ein, die die Erfüllung der Pflichten oder die Wahrnehmung

---

[172] *Gola*, in: Gola/Schomerus, Bundesdatenschutzgesetz, § 28 Rn. 8.
[173] *Wedde*, in: Basiskommentar zum BDSG, § 28 Rn. 12; *Simitis*, in: Simitis, Bundesdatenschutzgesetz, § 28 Rn. 77; *Gola*, in: Gola/Schomerus, Bundesdatenschutzgesetz, § 28 Rn. 9; die Unabhängigkeit der Alternativen bejahend: *Schaffland/Wiltfang*, in: Bundesdatenschutzgesetz, § 28 Rn. 13.
[174] *BAG*, Urt. v. 22.10.1986 – 5 AZR 660/85, NJW 1987, 2459, 2461.
[175] *Simitis*, in: Bundesdatenschutzgesetz Kommentar, § 28 Rn. 134.
[176] *Wedde*, in: Basiskommentar zum BDSG, § 28 Rn. 9.
[177] *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 28 Rn. 17.

der Rechte aus dem Vertragsverhältnis unterstützt oder fördert.[178] Folglich wird für die Datenverarbeitung ein unmittelbarer sachlicher Zusammenhang zwischen Verwendung und Vertragszweck vorausgesetzt.[179]

Im Fall der *Bahn* war das Unternehmen mit seinen Arbeitnehmern durch Arbeitsverträge verbunden. Der Zweck eines Arbeitsvertrages besteht darin, Arbeitsleistung gegen Arbeitslohn zu tauschen.[180]

Im Einzelfall ist die Zulässigkeit der Datenverarbeitung an Hand der objektiv feststellbaren Erforderlichkeit zu messen.[181] Hierbei ist jedoch schwierig zu erkennen, welche Daten durch den Vertragszweck erfasst werden und somit erforderlich erhoben wurden. So wird einerseits argumentiert, dass sich der Zweck des Vertrages lediglich aus den Hauptleistungspflichten ergebe und nur die dafür erforderlichen Daten verarbeitet werden dürften.[182] Das würde bedeuten, dass Korruptionsbekämpfung als Zweck der Datennutzung ausscheidet. Dagegen wird eingewendet, dass der Vertragszweck des Arbeitsvertrags auch zur Ermittlung von gegen den Vertragsinhalt sprechendem Verhalten berechtige.[183] Korruptionsermittlungen wären somit mittels der erhobenen Daten möglich.

Grundsätzlich ist die Verwendung von Arbeitnehmerdaten im Rahmen eines bestehenden Arbeitsvertrags zu Zwecken der Verhaltens- und Leistungskontrolle nicht ausgeschlossen.[184] Objektive Informationen über Leistung und Verhalten von Arbeitnehmern sind nur durch Kotrollen zu erhalten.[185] Kontrollen im Rahmen von Arbeitsverträgen dürfen jedoch nicht in einem solchen Ausmaß erfolgen, das die Erstellung von Persönlichkeitsprofilen ermöglicht.[186]

Da sich meist eine rechtfertigende Zweckbestimmung für eine Datennutzung nicht unmittelbar aus dem Wortlaut des Vertrages ablesen lässt, gilt es, die Rechte und Pflichten der Parteien im Rahmen einer Interesseabwägung festzustel-

---

[178] *Wedde*, in: Basiskommentar zum BDSG, § 28 Rn. 13.
[179] *Simitis*, in: Bundesdatenschutzgesetz Kommentar, § 28 Rn. 79.
[180] *Schaffland/Wiltfang*, in: Bundesdatenschutzgesetz, § 28 Rn. 26.
[181] *Wedde*, in: Basiskommentar zum BDSG, § 28 Rn. 15.
[182] *Bisges*, MMR 2009, Heft 4, S. XX.
[183] *Gola*, in: Gola/Schomerus, Bundesdatenschutzgesetz, § 28 Rn. 14; a.A. *Bisges*, MMR 2009, Heft 4, S. XX, der die Kriminalitätsbekämpfung im Unternehmen nicht als Zweck des Arbeitsvertrags sieht; ebenso *Kock/Francke*, ArbRB 2009, 110, die Arbeitnehmerscreenings als Zweckänderung des Vertrages ansehen.
[184] *Wedde*, in: Basiskommentar zum BDSG, § 28 Rn. 40.
[185] *Schaffland/Wiltfang*, in: Bundesdatenschutzgesetz, § 28 Rn. 25.
[186] *Wedde*, in: Basiskommentar zum BDSG, § 28 Rn. 40

len.[187] Hierbei ist festzustellen, ob die Eingriffsintensität in das allgemeine Persönlichkeitsrecht angemessen und der Grundsatz der Verhältnismäßigkeit gewahrt wurde. Dies soll nachfolgend in den entsprechenden Kapiteln erörtert werden. Grundsätzlich wäre § 28 Abs. 1 Satz 1 Nr. 1 BDSG jedoch zur Rechtfertigung des Datenabgleichs geeignet.

b) Zulässigkeit nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG

Ohne Einwilligung des Betroffenen oder ohne Anwendbarkeit einer anderen Rechtsnorm ist die Nutzung von Daten nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig, soweit es „zur Wahrung berechtigter Interessen der verantwortlichen Stellen erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt".

Um zu prüfen, ob dies im Fall der *Bahn* gegeben war, sind zwei Prüfungsschritte notwendig: Zum einen muss die Verarbeitung der Daten erforderlich gewesen sein, um berechtigte Interessen der speichernden Stelle, hier also des Unternehmens, zu wahren.[188] Zum anderen dürfen die schutzwürdigen Interessen der Betroffenen, hier die der Arbeitnehmer, nicht überwiegen.[189]

Strittig ist indes, wann ein berechtigtes Interesse der speichernden Stelle vorliegt. In der Literatur wird, überwiegend an die Rechtsprechung angelehnt, argumentiert, dass ein berechtigtes Interesse sich aus jedem Zweck, dessen Verfolgung von gesundem Rechtsempfinden gebilligt wird, ergeben könne.[190] Ein berechtigtes Interesse kann somit jedes von der Rechtsordnung gebilligte Interesse sein.[191] Daneben wird die Ansicht vertreten, dass sich die Berechtigung des Interesses der verarbeitenden Stelle nur vor dem Hintergrund des BDSG und seiner Grundsätze beurteilen lasse.[192]

Berechtigte Interessen können beispielsweise die Abwehr von Gefahren für die öffentliche Sicherheit oder die Verfolgung von Straftaten sein.[193] Aber auch rein wirtschaftliche Interessen können als berechtigte Interessen angesehen wer-

[187] *Gola*, in: Gola/Schomerus, Bundesdatenschutzgesetz, § 28 Rn. 16.
[188] *Schneider*, in Handbuch des EDV-Rechts, Rn. 209.
[189] *Gola*, in: Gola/Schomerus, Bundesdatenschutzgesetz, § 28 Rn. 35.
[190] *Gola*, in: Gola/Schomerus, Bundesdatenschutzgesetz, § 28 Rn. 33.
[191] *Schaffland/Wiltfang*, in: Bundesdatenschutzgesetz, § 28 Rn. 85.
[192] *Simitis*, in: Simitis, Bundesdatenschutzgesetz, § 28 Rn. 138.
[193] *Gola/Wronka*, in: Handbuch zum Arbeitnehmerdatenschutz, Rn. 807.

den.[194] Bei diesen muss es sich aber um eigene Belange der verantwortlichen Stelle handeln.[195]

Offensichtlich und auch berechtigt ist das Interesse der *Bahn*, durch den Kontenabgleich Korruption im Unternehmen aufzudecken. Die Frage, ob ein schutzwürdiges Interesse der Arbeitnehmer überwiegt, ist strittig. Schutzwürdige Interessen der Betroffenen sind grundsätzlich anzunehmen, wenn es sich um Angaben über gesundheitliche Situationen, Sexualverhalten, religiöse, politische oder philosophische Einstellungen, arbeitsrechtliche Verhältnisse, Zugehörigkeit zu rassischen oder ethnischen Gruppen, zu Gewerkschaften oder die Begehung strafbarer Handlungen oder Ordnungswidrigkeiten handelt.[196] Im Fall der *Bahn* handelte es sich jedoch lediglich um Namen, Adressen und Kontodaten.

Daher wird zum einen die Ansicht vertreten, dass Arbeitnehmer, die Straftaten begangen haben, keine schutzwürdigen Interessen hätten,[197] und auch die, bei denen die Überprüfung ergebnislos bleibt, mangels Beeinträchtigung nicht schutzwürdig seien. Andererseits wird vertreten, dass nach einer solchen Argumentation der „gläserne Arbeitnehmer“ unvermeidbar sei, da so jegliche technische Überwachung begründbar wäre.[198]

Die Erlaubnisnorm erfordert eine Interessenabwägung, bei der der Grundsatz der Verhältnismäßigkeit gewahrt bleiben muss. Ob dies der Fall ist, wird nachfolgend in den Kapiteln zum allgemeinen Persönlichkeitsrecht und zur Verhältnismäßigkeit behandelt. Das Ergebnis dieser Prüfung ausgeblendet, wäre grundsätzlich auch § 28 Abs. 1 Nr. 2 BDSG zur Rechtfertigung des Datenabgleichs geeignet.

c) ZULÄSSIGKEIT NACH § 28 ABS. 1 SATZ 1 NR. 3 BDSG

Nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG ist die Nutzung personenbezogener Daten zulässig, wenn diese allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte. Allgemein zugänglich sind solche Daten, die geeignet

[194] *BGH*, Urt. v. 22.05.1984 – VI ZR 105/82, NJW 1984, 1886, 1887.
[195] *Simitis*, in: Simitis, Bundesdatenschutzgesetz, § 28 Rn. 140.
[196] *Neundorf*, in: Hauschka (Hrsg.), Corporate Compliance, § 27 Rn. 26.
[197] *Diller*, BB 2009, 438, 439; *Scherp/Stief*, BKR 2009, 404, 406.
[198] *Steinkühler*, BB 2009, 1294, 1295.

sind, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln.[199]

Da die von der *Bahn* verwendeten Daten nicht allgemein zugänglich sind, scheidet diese Zulässigkeitsalternative schon im Vorfeld für den vorliegenden Fall aus.

2. Zulässigkeit durch andere Rechtsvorschriften

a) Tarifverträge oder Betriebsvereinbarung

Als Erlaubnisnorm für die Datenerhebung könnten weiter auch Tarifverträge oder Betriebsvereinbarungen in Betracht kommen. Diese können jedoch schon nicht als höherrangige Rechtsnorm im Sinne von § 1 Abs. 3 Satz 1 BDSG angesehen werden.[200] Die Subsidiarität des BDSG nach § 1 Abs. 3 BDSG tritt nur ein, wenn eine speziellere Norm inhaltlich einen Reglungsgegenstand des BDSG umfasst.[201] Bei Prüfung des BetrVG auf materielle Datenschutzregelungen ergibt sich, dass es lediglich zwei Stellen gibt, an denen datenschutzrechtliche Vorgaben gemacht werden. Zum einen in § 80 Abs. 1 Nr.1 BetrVG und zum anderen in § 87 Abs. 1 Satz 1 Nr. 6 BetrVG.

Nach § 80 Abs. 1 Nr. 1 BetrVG hat der Betriebsrat darüber zu wachen, dass zu Gunsten der Arbeitnehmer geltende Gesetze und auch Betriebsvereinbarungen eingehalten werden. Nach § 87 Abs. 1 Satz Nr. 6 BetrVG kommt dem Betriebsrat das Recht zu, bei Einführung und Anwendung von technischen Einrichtungen zur Überwachung von Arbeitnehmern mitzubestimmen. Beide Regelungen enthalten indes keine inhaltlichen Vorgaben für die Umsetzung des Datenschutzes. Daher wird das BDSG als höherrangige Norm nicht außer Kraft gesetzt.[202] Vielmehr werden die Mitbestimmungsrechte durch das BDSG eingeschränkt.[203]

Eine Betriebsvereinbarung kann jedoch eine Datenverarbeitung gemäß § 4 Abs. 1 BDSG legitimieren.[204] Hierbei ist der normative Teil von Tarifverträgen und Betriebsvereinbarungen wegen seiner unmittelbaren Außenwirkung als Rechts-

[199] *Simitis*, in: Simitis, Bundesdatenschutzgesetz, § 28 Rn. 189.
[200] *Gola*, in: Gola/Schomerus, Bundesdatenschutzgesetz, § 1 Rn. 23.
[201] *Weichert*, in: Basiskommentar zum BDSG, § 1 Rn. 13.
[202] *Weichert*, in Basiskommentar zum BDSG, § 4 Rn. 2.
[203] *Trittin/Fischer*, NZA 2009, 343, 345.
[204] *Weichert*, in: Basiskommentar zum BDSG, § 1 Rn. 12.

vorschrift zu behandeln.[205] Somit können Betriebsvereinbarungen als anderweitige Erlaubnisnormen nach § 4 Abs. 1 BDSG herangezogen werden.[206]

Eine Betriebsvereinbarung darf dabei die Schutzansprüche des § 75 Abs. 2 Satz 1 BetrVG, die freie Entfaltung der Persönlichkeit der Arbeitnehmer zu schützen und zu fördern, nicht unterschreiten.[207] Ferner darf nach überwiegender Ansicht auch der Schutzstandard des BDSG nicht durch eine Regelung in einer Betriebsvereinbarung unterschritten werden.[208]

Innerhalb dieses Rahmens jedoch hätte eine entsprechende Betriebsvereinbarung bei der *Bahn* als Erlaubnisgrundlage für das Abgleichen der Daten dienen können, wenn sie vor den Datenabgleichen ausgehandelt worden wäre.

b) COMPLIANCE

Wie bereits in Kapitel C III festgestellt, ist der Vorstand verpflichtet, das Unternehmen unter eigener Verantwortung zu führen. Daraus entstehen für den Vorstand diverse Aufsichtspflichten. Diese Pflichten könnten gegenüber dem BDSG vorrangig sein und so im Rahmen von Compliance-Maßnahmen das Recht begründen, Daten zu erheben, zu nutzen und zu verarbeiten.

Nach § 4 Abs. 1 BDSG ist das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten nur zulässig, soweit es das BDSG selbst oder eine andere Rechtsvorschrift erlaubt oder anordnet oder der Betroffene eingewilligt hat. Fraglich ist, ob Compliance im Sinne einer anderen Rechtsvorschrift als Erlaubnisgrundlage für die Datennutzung dienen könnte.

Als Rechtsvorschrift werden alle materiellen Rechtsnormen mit unmittelbarer Außenwirkung bezeichnet, folglich insbesondere Gesetze und Rechtsverordnungen, jedoch keine Erlasse und Verwaltungsvorschriften.[209] Nach § 1 Abs. 3 Satz 1 BDSG sind alle den Umgang mit personenbezogenen Daten regelnden Vorschriften des Bundesrechts vorrangig vor dem BDSG.[210] Für eine Vorrangigkeit

---

[205] *Walz*, in: Simitis, Bundesdatenschutzgesetz, § 4 Rn. 11.
[206] *Büllesbach*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 6.1 Rn. 89.
[207] *Steinkühler/Raif*, AuA 2009, 213, 214.
[208] *Trittin/Fischer*, NZA 2009, 343, 344; *Simitis*, in: Simitis, Bundesdatenschutzgesetz, § 4 Rn. 17; *Gola*, in: Gola/Schomerus, Bundesdatenschutzgesetz, § 4 Rn. 10; anders *BAG*, Beschl. v. 27.05.1986 – 1 ABR 48/84, NJW 1987, 674, 677; *Sassenberg/Bamberg*, DuD 2006, 226, 229 vertreten eine begrenzte Abdingbarkeit.
[209] *Walz*, in Simitis, Bundesdatenschutzgesetz, § 4 Rn. 9.
[210] *Gola*, in: Gola/Schomerus, Bundesdatenschutzgesetz, § 1 Rn. 23.

gegenüber dem BDSG genügt bereits ein mittelbarer datenschützender Charakter.[211]

Mittelbare Compliance-Regelungen ergeben sich für den Vorstand aus § 93 Abs. 1 AktG und § 130 OWiG, sowie für Vorstand und Aufsichtsrat aus dem Corporate Governance Kodex. Darüber hinaus ist für Unternehmen, die an der US Börse notiert sind, der US-amerikanische Sarbanes-Oxley Act relevant.

Weder § 93 Abs. 1 AktG noch § 130 OWiG erfassen einen inhaltlichen Regelungsgegenstand des BDSG. Allein aus der Aufgabe, ein Unternehmen unter eigener Verantwortung zu leiten, ergibt sich keine Befugnis zu einem Eingriff in die (Grund-)Rechte von Arbeitnehmern.[212]

Die Compliance-Aufgaben von Vorstand und Aufsichtsrat beschreibt der Deutschen Corporate Governance Kodex in den Ziffern 4.1.3, 5.3.2 sowie 3.4 Abs. 2 DCGK. Diese enthalten ebenfalls keine inhaltlichen Regelungsgegenstände des BDSG. Daher kann hier auch dahinstehen, welche Rechtsnatur der DCGK hat.

Eine ausländische Rechtsnorm, wie der US-amerikanische Sarbanes-Oxley Act, ist ebenfalls keine andere Rechtsvorschrift im Sinne von § 4 Abs. 1 BDSG.[213]

Somit können Compliance-Pflichten alleine nicht als Erlaubnisnorm herangezogen werden. Die Zulässigkeit von Compliance-Maßnahmen richtet sich nach den Vorgaben des BDSG.

3. Einwilligung des Betroffenen

Das Erfordernis einer Einwilligung der Mitarbeiter zur Verarbeitung und Nutzung ihrer Daten ist im Arbeitsverhältnis auf Grund der ungleichen Machtverhältnisse fragwürdig.[214] Da Arbeitnehmer regelmäßig auf ihren Arbeitsplatz angewiesen sind, werden sie der Speicherung oder Verarbeitung ihrer Daten wohl regelmäßig zustimmen.[215]

---

[211] *Schaffland/Wiltfang*, in: Bundesdatenschutzgesetz, § 1 Rn. 42.
[212] *Weichert*, in: Basiskommentar zum BDSG, § 4 Rn. 3.
[213] Hessischer Landtag, Vorlage der Landesregierung betreffend den Siebzehnten Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, 15.02.2005, LT-Drs. 16/3650, S. 21, abrufbar unter: http://starweb.hessen.de/cache/DRS/16/0/03650.pdf.
[214] *Trittin/Fischer*, NZA 2009, 343, 344.
[215] *Däubler*, in: Basiskommentar zum BDSG, § 4a Rn. 1.

Die Einwilligung des Betroffenen kommt außerdem nur dann in Frage, wenn Unternehmen über mehrere Datenverarbeitungsalternativen verfügen und bereit sind, die Verweigerung der Einwilligung durch den Betroffenen zu respektieren.[216] Hat die verantwortliche Stelle jedoch die Absicht, im Falle einer Verweigerung der Einwilligung auf ihre gesetzliche Verarbeitungserlaubnis zurückzugreifen, wird dem Betroffenen eine Wahlfreiheit vorgetäuscht, die dieser letztlich nicht hat.[217] Somit wird der Betroffene im Ergebnis in die Irre geführt.[218]

Auch im Fall der *Bahn* wäre das Einverständnis der Betroffenen nicht die optimale Rechtsgrundlage gewesen, insbesondere auf Grund der Vielzahl an Betroffenen. Jedoch hätte es grundsätzlich als Rechtsgrundlage für den Datenabgleich dienen können.

III. Weitergabe von Daten

Fraglich im Fall der *Bahn* ist ferner, ob die Weitergabe von Arbeitnehmer- und Lieferantendaten an die *Network Deutschland GmbH* zum Zwecke des Abgleichs rechtlich unbedenklich war.

Zunächst ist in diesem Fall die rechtliche Einordnung des Dienstleisters notwendig. Das BDSG unterscheidet zwischen der Übermittlung von Daten an Dritte und der Weitergabe von Daten im Rahmen einer Auftragsdatenverarbeitung. Eine Übermittlung liegt vor, wenn die verantwortliche Stelle Daten einem Dritten bekannt gibt.[219] Laut § 3 Abs. 8 Satz 3 BDSG sind „Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen“, keine Dritten. Das bedeutet, dass der Datentransfer zu und von einem Auftragsdatenverarbeiter nicht als Übermittlung im Sinne von § 3 Abs. 4 Satz 2 Nr. 3 BDSG aufgefasst wird.[220] Dies setzt jedoch voraus, dass der Dienstleister weisungsgebunden ist, und somit nicht über den Umgang mit den Daten eigenverantwortlich

[216] *Holznagel/Sonntag*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.8 Rn. 24.
[217] *Weichert*, in: Basiskommentar zum BDSG, § 4 Rn. 4.
[218] *Walz*, in: Simitis, Bundesdatenschutzgesetz, § 4 Rn. 7.
[219] *Dammann*, in: Simitis, Bundesdatenschutzgesetz, § 3 Rn. 229.
[220] *Gola/Wronka*, Handbuch zum Arbeitnehmerdatenschutz, Rn. 859.

entscheiden darf.[221] Wird dem Dienstleister ein inhaltlicher Ermessens- oder Bewertungsspielraum eingeräumt, so handelt es sich um eine Funktionsübertragung.[222]

Verantwortliche Stellen bleiben bei der Auftragsdatenverarbeitung auch dann verantwortlich, wenn sie selbst keine Daten verarbeiten, sondern dies in Auftrag gegeben haben.[223] Der Auftraggeber ist als „Herr der Daten" für die Beachtung der datenschutzrechtlichen Vorgaben für die von ihm veranlassten Verarbeitungen verantwortlich.[224] Werden Rechte missachtet, so kann der Betroffene Auskunft und gegebenenfalls Schadensersatzansprüche beim Auftraggeber geltend machen, nicht aber beim Auftragnehmer.[225] Daher sollte bei Einbeziehung externer Dienstleister die Einhaltung der relevanten Datenschutzbestimmungen durch den Auftragnehmer schriftlich zugesichert werden.[226] Ferner muss nach § 11 Abs. 2 Satz 2 BDSG Art und Umfang des Auftrags schriftlich festgehalten werden.[227] Verpflichtend für den Auftraggeber ist auch die sorgfältige Auswahl und Überprüfung der Datensicherung des Auftragnehmers.[228]

Im Fall der *Bahn* ist unklar, ob es im Rahmen der Zusammenarbeit mit der *Network Deutschland GmbH* eine schriftliche Auftragsvergabe gab. Ebenfalls nicht belegbar ist, ob die *Bahn* die Datensicherungsmaßnahmen der *Network Deutschland GmbH* überprüft hat.[229] Zumindest wurden bei der *Bahn* keine entsprechenden Unterlagen gefunden.[230] Über mögliche Konsequenzen einer mündlichen Auftragsvergabe entgegen § 11 Abs. 2 Satz 2 BDSG hat sich – soweit ersichtliche – bisher weder die Rechtsprechung noch die Literatur geäußert.[231]

IV. Allgemeines Persönlichkeitsrecht

[221] *Kock/Francke*, NZA 2009, 646, 651.
[222] *Gola*, in: Gola/Schomerus, Bundesdatenschutzgesetz, § 11 Rn. 9.
[223] *Dammann*, in Simitis, Bundesdatenschutzgesetz, §3 Rn. 227.
[224] *Gola*, in: Gola/Schomerus, Bundesdatenschutzgesetz, § 3 Rn. 50.
[225] *Hoeren*, in: Roßnagel, Handbuch Datenschutzrecht, 4.6 Rn. 100.
[226] *Hampel*, ZIR 2009, 99, 102.
[227] Vgl. nur *Hoeren*, in: Roßnagel, Handbuch Datenschutzrecht, 4.6 Rn. 108.
[228] *Walz*, in: Simitis, Bundesdatenschutzgesetz, § 11 Rn. 43.
[229] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 25.
[230] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 27.
[231] *Hoeren*, in: Roßnagel, Handbuch Datenschutzrecht, 4.6 Rn. 108

Mit Hilfe des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG wird die Befugnis des Einzelnen gesichert, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[232] Da dieses Recht jedoch nicht unbeschränkt ist, muss der Einzelne Einschränkungen hinnehmen, die dem überwiegenden Allgemeininteresse dienen.[233]

Zwar sind die Grundrechte Abwehrrechte des Bürgers gegen den Staat und finden daher unmittelbar grundsätzlich nur im Rahmen einer Staat-Bürger-Beziehung Anwendung. Jedoch besteht im arbeitsrechtlichen Schrifttum die Auffassung, der Schutz der Grundrechte müsse auch dann gewahrt sein, wenn der Grundrechtsträger sich in einem Verhältnis der Über- und Unterordnung befindet, das zwar nicht durch den Staat selbst, aber durch einen von ihm geschaffenen und tolerierten Machtträger bestimmt wird. Soweit arbeitsrechtliche Beziehungen in vergleichbarer Weise durch ein Über- und Unterordnungsverhältnis gekennzeichnet seien, müssten die Grundrechte daher auch im „Arbeitsleben" unmittelbar zur Anwendung kommen.[234]

Diese Ansicht wird durch § 75 Abs. 2 Satz 1 BetrVG gestützt, wonach die Betriebsparteien verpflichtet sind, die grundrechtlich geschützten Freiheitsrechte zu wahren.[235] Daher haben die Parteien insbesondere auch das Allgemeine Persönlichkeitsrecht zu beachten, da der einzelne Grundrechtsträger auch vor einer unverhältnismäßigen Grundrechtsbeschränkung durch privatautonome Regelungen bewahrt werden muss.[236] Die Frage, ob das allgemeine Persönlichkeitsrecht der Mitarbeiter durch die von der *Bahn* durchgeführten Screenings verletzt wurde, wird unterschiedlich beantwortet. So argumentiert *Diller* beispielsweise, dass das allgemeine Persönlichkeitsrecht in diesem Fall gar nicht berührt werde, da die Maßnahmen nicht den engeren Lebensbereich beträfen.[237]

Dem entgegen argumentiert *Steinkühler* mit Rückgriff auf eine Entscheidung des *BAG* zur Videoüberwachung[238], dass durch die Screenings beim Arbeitnehmer ein ständiger „Überwachungsdruck" entstehe und somit ein erheblicher Eingriff

---

[232] *Murswiek*, in: Sachs, Grundgesetz, Art. 2 Rn. 72.
[233] *Weichert*, in: Basiskommentar zum BDSG, Einführung Rn. 16.
[234] *Wiedemann*, in: Kollmer, Arbeitsschutzgesetz, Abschn. A Rn. 38 f.; *Sendler*, NJW 1994, 709.
[235] So auch *BAG*, Urt. v. 19.01.1999 – 1 AZR 499/98, NZA 1999, 546.
[236] *BAG*, Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278, 1279 f.
[237] *Diller*, BB 2009, 438, 439.
[238] *BAG*, Beschl. v. 14.12.2004 – 1 ARG 34/03, NZA 2005, 839.

in die Persönlichkeitssphäre der Mitarbeiter vorliege.[239] Bei der in Bezug genommenen Entscheidung des *BAG* ging es um die Überwachung von Arbeitnehmern durch Videokameras. Diese Kameras filmten die Angestellten zwar nicht durchgängig, jedoch war für den Arbeitnehmer nicht ersichtlich, wann er genau beobachtet wurde und wann nicht. Das *BAG* sah dies als einen erheblichen Eingriff in die Persönlichkeitsrechte der Mitarbeiter an, da diese jederzeit damit rechnen müssten, gefilmt zu werden, womit ein ständiger Überwachungsdruck entstünde.[240]

Als besonders erheblich wird darüber hinaus der Eingriff in die Persönlichkeitsrechte externer Dritter aufgefasst, da diese regelmäßig keinen zurechenbaren Anlass für eine Überwachungsmaßnahme geben.[241] Die Überwachung dieser Personen ist für die Korruptionsbekämpfung nicht notwendig, so dass eine Rechtfertigung dafür fehlt.[242]

Es mag zwar zutreffen, dass der Abgleich von Kontodaten nicht in den engeren Lebensbereich eingreift. Dennoch wird durch Überwachungsmaßnahmen regelmäßig in das allgemeine Persönlichkeitsrecht eingegriffen.[243] Zwar ist dies beispielsweise im Vergleich zur Videoüberwachung ein weniger einschneidender Eingriff. Dennoch liegt ein Eingriff vor.

Das Argument, es entstehe durch die Screenings ein „Überwachungsdruck“ beim Arbeitnehmer, kann nicht überzeugen. Im Fall der *Bahn* ist den Mitarbeitern nicht mitgeteilt worden, dass ihre Daten abgeglichen wurden. Somit ist fraglich, ob die Mitarbeiter einen „Überwachungsdruck“ verspürten, wenn sie nichts von der Überwachung mitbekamen.

Sind die Daten unbeteiligter Dritter betroffen, so sind im Allgemeinen höhere Anforderungen an eine Rechtfertigung zu stellen.[244] Im Fall der *Bahn* wären dies Personen, die auf Grund ihrer Stellung und Kompetenzen im Unternehmen schon von vornherein keine Möglichkeit hatten, entsprechende Straftaten zu begehen.[245] Nach dem vorliegenden Sachverhalt wären das beispielsweise Gleisarbeiter oder Reinigungskräfte. Fraglich ist, ob die Daten dieser Personen im Vorfeld

[239] *Steinkühler*, BB 2009, 1294, 1295.
[240] *BAG*, Beschl. v. 14.12.2004 – 1ARG 34/03, NZA 2005, 839.
[241] *Kock/Francke*, NZA 2009, 646, 648.
[242] *Steinkühler*, BB 2009, 1294, 1295.
[243] *Murswiek*, in: Sachs, Grundgesetz, Art. 2 Rn. 87.
[244] *BVerfG*, Urt. v. 3. 3. 2004 – 1 BvR 2378/98 u. 1 BvR 1084/99, NJW 2004, 999.1013.
[245] *Kock/Francke*, NZA 2009, 646, 648.

hätten aussortiert werden müssen.[246] Das *BVerfG* hat in einem Fall, in dem es um die Abfrage von Kreditkartendaten ging, entschieden, dass kein Eingriff in das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG vorliege, wenn Kreditkartendaten nur maschinell geprüft, mangels Übereinstimmung mit den Suchkriterien aber nicht als Treffer angezeigt und daher nicht weitergeleitet werden würden.[247] Es erfolge keine Beeinträchtigung der Rechte betroffener Personen, wenn der Datenabgleich maschinell und somit in erfolglosen Fällen anonym, spurenlos und ohne Erkenntnisinteresse bleibe. In dem Fall hatte die Staatsanwaltschaft im Rahmen von Ermittlungen Institute, die *Mastercard*- und *Visa*-Kreditkarten in Deutschland ausgeben, aufgefordert, Kreditkartenkonten anzugeben, die seit dem 01.03.2006 einen Betrag von 79,99 US-Dollar an eine philippinische Bank überwiesen hatten.[248] Da der Abgleich maschinell erfolgte, wurden nur die Konten verdächtiger Personen angezeigt. Nach Auffassung des *BVerfG* sei darin kein Eingriff in das informationelle Selbstbestimmungsrecht unbeteiligter Dritter zu sehen.[249]

Bei der *Bahn* wurden ausschließlich Daten von Bahn-Arbeitnehmern angezeigt, die eine Übereinstimmung mit Lieferantendaten ergeben hatten. Der o.g. Auffassung des *BVerfG* folgend, läge auch hier kein Eingriff in die Persönlichkeitsrechte Dritter vor. Jedoch gewährleistet das informationelle Selbstbestimmungsrecht dem Einzelnen nicht nur, über die Preisgabe seiner Daten zu bestimmen, sondern auch über deren Verwendung.[250] Damit stellt der Abgleich der Daten einen Eingriff in das informationelle Selbstbestimmungsrecht dar, unabhängig davon, ob die Daten eine Übereinstimmung ergeben und gesondert hervorgehoben werden oder nicht.

---

[246] *Steinkühler*, BB 2009, 1294, 1295; *Kock/Francke*, NZA 2009, 646, 646 bejahen dies, da die entsprechenden Personen keinen Anlass für eine derartige Kontrolle geben würden und diese Maßnahme somit als unzulässig anzusehen sei.
[247] *BVerfG*, Beschl. v. 17.02.2009 – 2 BvR 1372, 1745/07, NJW 2009, 1405.
[248] *BVerfG*, Beschl. v. 17.02.2009 – 2 BvR 1372, 1745/07, NJW 2009, 1405.
[249] *BVerfG*, Beschl. v. 17.02.2009 – 2 BvR 1372, 1745/07, NJW 2009, 1405.
[250] *BVerfG*, Urt. v. 15.12.1983 – 1 BvR 209/83, NJW 1984, 419.

V. Verhältnismäßigkeit

Kollidieren betriebliche Interessen des Arbeitgebers mit den Persönlichkeitsrechten des Arbeitnehmers, ist eine Güter- und Interessenabwägung notwendig.[251] Die Zulässigkeit eines Eingriffes in das allgemeine Persönlichkeitsrecht des Arbeitnehmers bestimmt sich nach dem Grundsatz der Verhältnismäßigkeit.[252] Denn der Arbeitgeber darf nur so weit in die Privatsphäre des Arbeitnehmers eindringen, wie es zum Zwecke des Arbeitsverhältnisses unbedingt erforderlich ist.[253] Daher muss eine Maßnahme geeignet, erforderlich und unter Berücksichtigung der Persönlichkeitsrechte des Betroffenen angemessen sein, um den verfolgten Zweck zu erreichen.[254]

Vorab muss bei der Prüfung der Verhältnismäßigkeit einer Maßnahme jedoch der damit angestrebte Zweck bestimmt werden. Der verfolgte Zweck muss ein legitimer sein, da sonst der Eingriff schon aus diesem Grunde rechtswidrig ist.[255] Der von der *Bahn* verfolgte Zweck war die Aufdeckung von Korruption im Unternehmen im Rahmen von Compliance-Maßnahmen. Dies stellt einen legitimen Zweck dar.

1. Geeignetheit

Geeignetheit bedeutet, dass die gewählten Maßnahmen den gewünschten Zweck fördern.[256]

Der Abgleich von Mitarbeiter- und Lieferantenkonten bei der *Bahn* war geeignet, um Rückschlüsse auf Betrugs- und Unterschlagungsdelikte zu liefern.

Bei dem Datenabgleich wurden die Daten nahezu aller Mitarbeiter verwendet. Viele dieser Arbeitnehmer hatten, wie bereits erwähnt, aus ihrer Tätigkeit heraus keine Möglichkeit, Täter einer Korruptionsstraftat zu werden. Beispielsweise sind Schaffner oder die Reinigungskräfte nicht an der Vergabe von Aufträgen beteiligt. Somit waren von dem Datenabgleich auch viele von vornherein unverdächtige Personen erfasst. Die Überprüfung von nicht verdächtigen Personen war nicht geeignet dem Zweck der Korruptionsbekämpfung zu dienen. Gegen die

[251] *BAG*, Urt. v. 18.11.1999 – 2 AZR 743/98, NZA 2000, 418, 420.
[252] *BAG*, Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278.
[253] *Kock/Francke*, NZA 2009, 646, 648.
[254] *Kock/Francke*, NZA 2009, 646, 648.
[255] *Maurer*, Staatsrecht 1, § 8 Rn. 56.
[256] *Pieroth/Schlink*, in: Grundrechte Staatsrecht 2, § 6 Rn. 283.

Verhältnismäßigkeit spricht somit, dass unverdächtige Personen nicht bereits im Vorfeld aussortiert wurden. Dies hätte zwar einen zusätzlichen Aufwand bedeutet, jedoch hätten Eingriffe in die Rechte unbeteiligter Personen reduziert werden können.[257] Damit sind die internen Untersuchungsmaßnahmen der *Bahn* zumindest in Bezug auf solche Mitarbeiter, die auf Grund ihrer Position im Unternehmen von vornherein nicht in Betracht kommen, Täter oder Teilnehmer einer Straftat zu Lasten des Unternehmens zu sein, ungeeignet und damit unverhältnismäßig. In Bezug auf die übrigen Mitarbeiter ist jedoch weiter zu prüfen, ob die Maßnahme erforderlich und angemessen ist.

2. Erforderlichkeit

Eine Maßnahme kann dann als erforderlich angesehen werden, wenn der Zweck nicht durch eine gleich wirksame, aber für den Betroffenen weniger beeinträchtigende Maßnahme erreicht werden kann.[258]

Bei dem Datenabgleich der *Bahn* wurde nur geringfügig in die Rechte der Arbeitnehmer eingegriffen. Eine mögliche alternative Maßnahme könnte die gezielte Überprüfung einzelner Geschäftsvorfälle oder Mitarbeiter darstellen. Möglicherweise auch begrenzt auf solche Vorfälle oder Mitarbeiter, zu denen sich bereits eine Art „Anfangsverdacht“ in Bezug auf die mögliche Beteiligung an einer Straftat zum Nachteil des Unternehmens ergeben hat.

Hierbei ist jedoch nicht ersichtlicht, dass die Eingriffsintensität in Bezug auf die bei dieser Überprüfung betroffenen Mitarbeiter geringer gewesen wäre. Jedoch wären dadurch weitaus weniger Arbeitnehmer betroffen worden. Damit wäre die Maßnahme aber möglicherweise auch weniger effektiv gewesen. Insgesamt kann die Maßnahme der *Bahn* daher noch als erforderlich angesehen werden.

3. Angemessenheit

Die Angemessenheit einer Überwachungsmaßnahme richtet sich maßgeblich nach ihrer Eingriffsintensität in die Persönlichkeitsrechte der Betroffenen.[259] Steht der angestrebte Erfolg außer Verhältnis zur Schwere des Eingriffs ist die

[257] Zustimmend *Steinkühler*, BB 2009, 1294, 1295; ablehnend dagegen *Diller*, BB 2009, 438, 440.
[258] *Pieroth/Schlink*, in: Grundrechte Staatsrecht 2, § 6 Rn. 285.
[259] *BAG*, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187.

Maßnahme nicht angemessen.[260] Zur Feststellung der Angemessenheit der Compliance-Maßnahmen bedarf es einer Gesamtabwägung der Eingriffsintensität und der den Eingriff rechtfertigenden Gründe, wobei die Grenze der Zumutbarkeit nicht überschritten werden darf.[261]

Im Arbeitsverhältnis muss sich der Arbeitgeber auf die Kontrollen beschränken, die am wenigsten in die Rechte der betroffenen Arbeitnehmer eingreifen.[262] Nach der Rechtsprechung ist ausschlaggebend, ob die Überwachung offen oder verdeckt stattfindet, welche Arten von Medien dabei verwendetet werden, ob eine verdächtige oder unverdächtige Person überwacht wird und ob der überwachte Ort öffentlich zugänglich ist oder nicht.[263] Weiteres Kriterium ist die Dauer der Überwachung.[264]

Gegen die Angemessenheit der Maßnahme spricht hier auch, dass sie verdeckt durchgeführt wurde. Das Gewicht des Eingriffs in die Grundrechte der Betroffenen wird durch eine heimlich durchgeführte Maßnahme, wie im vorliegenden Fall die Kontenscreenings der Mitarbeiter, erhöht, da diesen dadurch ein vorheriger Rechtsschutz faktisch verwehrt wird.[265]

Weiteres Kriterium für die Angemessenheit der Maßnahme ist, ob verdächtige oder unverdächtige Personen überwacht wurden. Nach der Ansicht des *BVerfG*, dass durch die Datenabgleiche schon kein Eingriff in die Persönlichkeitsrechte[266] von Arbeitnehmern vorläge, bei denen die Überprüfung ergebnislos blieb,[267] müsste die Verhältnismäßigkeit hier bejaht werden, weil somit ausschließlich in die Rechte verdächtiger Personen eingegriffen worden wäre. Da dieser Ansicht hier nicht gefolgt wird, da es sich beim Datenabgleich immer um einen Eingriff in das Recht auf informationelle Selbstbestimmung handelt,[268] ist die Verhältnismäßigkeit der Maßnahme der *Bahn* zu verneinen, weil die Anzahl der Betroffen, die unverdächtig in die Datenabgleiche einbezogen wurden, unangemessen hoch war.[269] Eine Art von Rasterfahndung, bei der die Daten der Arbeitnehmer

[260] *Schnabel*, DUD 2007, 427, 429.
[261] *BAG*, Beschl. v. 14.12.2004 – 1 ABR 34/03, NJOZ 2005, 2708, 2711.
[262] *Mengel*, Compliance und Arbeitsrecht, Kap. 4 Rn. 2.
[263] v. *Steinau-Steinrück/Glanz*, NJW-Spezial 2008, 402.
[264] *Mengel*, Compliance und Arbeitsrecht, Kap. 4 Rn. 2.
[265] *Kock/Francke*, NZA 2009, 646, 650.
[266] *BVerfG*, Beschl. v. 17.02.2009 – 2 BvR 1372, 1745/07, NJW 2009, 1405.
[267] *Diller*, BB 2009, 438, 440.
[268] Siehe dazu oben unter G. IV.
[269] So auch *Steinkühler*, BB 2009, 1294, 1295; *Kock/Francke*, NZA 2009, 646, 648.

unabhängig von der tatsächlichen Möglichkeit, auf Grund ihrer Stellung Einfluss auf Zahlungen nehmen zu können, verdachtsunabhängig abgeglichen werden, ist unverhältnismäßig.[270]

Dadurch ist die von der *Bahn* durchgeführte Maßnahme in ihrer Zweck-Mittel-Relation unangemessen.

Auch die permanente Überwachung von Arbeitnehmern wäre ein unverhältnismäßiger Eingriff in das Persönlichkeitsrecht der Arbeitnehmer und somit nicht zulässig.[271] Zwischen den Jahren 1998 und 2006 wurden bei der *Bahn* insgesamt fünf dieser Abgleiche mit teilweise unterschiedlichen Zielgruppen durchgeführt. Die zeitlichen Abstände der Kontrollen liegen jedoch angemessen weit auseinander, so dass durch die hier gewählte Häufigkeit der Wiederkehr der Maßnahme die Angemessenheit gewahrt bliebe.

VI. Betriebsrat

Fraglich ist, ob beim Vorgehen der *Bahn* die Mitbestimmungsrechte des Betriebsrates übergangen wurden. In Betracht kämen in diesem Fall Mitbestimmungsrechte nach § 87 Abs. 1 Nr. 1 und Nr. 6 BetrVG. Wirksamkeits- und Rechtmäßigkeitsvoraussetzung einer Datenverarbeitungsmaßnahme ist die Beachtung von Mitbestimmungsrechten des Betriebsrates durch den Arbeitgeber.[272]

1. Mitbestimmung bei Fragen der Betriebesordnung, § 87 Abs. 1 Nr. 1 BetrVG

Der Zweck der Regelung des § 87 Abs. 1 Nr. 1 BetrVG ist es, den Arbeitnehmern eine gleichberechtigte Teilhabe an der Gestaltung des betrieblichen Zusammenlebens zu gewähren.[273] Mitbestimmungstatbestand ist die Regelung des Zusammenlebens und Zusammenwirkens der Arbeitnehmer im Betrieb.[274] Die Mitbestimmung scheidet somit für alle Maßnahmen des Arbeitgebers aus, die nur das Verhältnis zwischen Arbeitnehmer und Arbeitgeber oder die Erbringung

[270] *Vogt*, NJOZ 2009, 4206, 4214; i.E. auch *Scherp/Stief*, BKR 2009, 404, 406.
[271] *Wank*, in: Erfurter Kommentar zum Arbeitsrecht, § 28 BDSG Rn. 13.
[272] *Wank*, in: Erfurter Kommentar zum Arbeitsrecht, § 28 BDSG Rn. 5.
[273] *Kothe*, in: Dünwell, Betriebsverfassungsgesetz Handkommentar, § 87 Rn. 30; sowie *BAG*, Urt. v. 23.07.1996 – 1 ARB 17/96, NZA 1997, 216, 217f.
[274] *Kania*, in: Erfurter Kommentar zum Arbeitsrecht, § 87 BetrVG, Rn. 18.

der Arbeitsleistung betreffen.[275] Hierzu zählen Regeln und Weisungen, die vom Arbeitnehmer bei der Erbringung der geschuldeten Arbeitsleistung zu beachten sind.[276] Dies gilt auch für generelle Anweisungen an alle Arbeitnehmer.[277]

Daher werden alle Kontrollregelungen, mit deren Hilfe eine Ordnung im Betrieb durchgesetzt werden soll, von den Mitbestimmungsrechten erfasst.[278] So hat das *BAG* beispielsweise entschieden, dass die generelle Einrichtung von Tor- und Taschenkontrollen dem Mitbestimmungsrecht unterliegt.[279] Anders hat das *BAG* für den Fall entschieden, dass die Arbeitsleistung der Arbeitnehmer selbst, beispielsweise durch verdeckte Testkunden, überwacht werden soll.[280] Hierbei entfällt ein Mitbestimmungsrecht schon allein deswegen, weil das Verhalten des Arbeitnehmers gerade nicht beeinflusst werden soll, sondern eine Bestandsaufnahme der Leistungen bezweckt wird.[281] Auch für den Fall, in dem die Ehrlichkeit einer Kassiererin durch heimliche Erhöhung vereinzelter Kassenbestände geprüft werden sollte, hat das *BAG* ein Mitbestimmungsrecht des Betriebsrates nach § 87 Abs. 1 Nr. 1 BetrVG verneint.[282] Zur Begründung wurde festgestellt, dass dieses Vorgehen lediglich das Arbeitsverhalten der Arbeitnehmerin betreffe.[283]

Im Fall der *Bahn* wurde mit dem Abgleichen von Daten keine Beeinflussung des Verhaltens der Arbeitnehmer im Betrieb bezweckt. Es sollten lediglich Betrugsfälle aufgedeckt werden. Es ist denkbar, dass sich Arbeitnehmer von geplanten Straftaten abschrecken lassen. Insbesondere wenn durch entdeckte Fälle ersichtlich wird, dass die Möglichkeit besteht, dass diese durch das Unternehmen aufgedeckt werden. Wenn jedoch vorrangig eine Veränderung des Verhaltens im Betrieb bezweckt worden wäre, hätten die Arbeitnehmer über solche Maßnahmen aufgeklärt werden müssen, damit diese eine abschreckende Wirkung hätten

---

[275] *Richardi*, in: Richardi, Betriebsverfassungsgesetz, § 87 Rn. 174.
[276] *Fitting/Engels/Schmidt/Trebinger/Linsenmaier*, Betriebsverfassungsgesetz, § 87 Rn. 64.
[277] *BAG*, Beschl. v. 08.06.1999, AP Nr. 31 zu § 87 BetrVG 1972 Ordnung des Betriebes.
[278] *Kania*, in: Erfurter Kommentar zum Arbeitsrecht, § 87 BetrVG, Rn. 20; ähnlich *BAG*, Beschl. v. 26.03.1991 – 1 ABR 26/90, NZA 1991, 729, das ein Mitbestimmungsrecht beim Einsatz von Privatdetektiven verneint, da dadurch kein Verhalten der Arbeitnehmer geregelt werde. Dem entgegen *FittingEngelsSchmidtTrebinger/Linsenmaier*, Betriebsverfassungsgesetz, § 87 Rn. 74, die ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG für alle Maßnahmen des Arbeitgebers befürworten, mit denen das Verhalten der Arbeitnehmer kontrolliert werden soll; zustimmend *Steinkühler*, BB 2009, 1294.
[279] *BAG*, Beschl. v. 26.05.1988 – 1 ABR 9/87, NZA 1988, 811, 812.
[280] *BAG*, Beschl. v. 18.04.2000 – 1 ABR 22/99, NZA 2000, 1176.
[281] *BAG*, Beschl. v. 18.04.2000 – 1 ABR 22/99, NZA 2000, 1176, 1177.
[282] *BAG*, Urt. v. 18.11.1999 – 2 AZR 743/98, NJW 2000, 1211.
[283] *BAG*, Urt. v. 18.11.1999 – 2 AZR 743/98, NJW 2000, 1211, 1214.

entfalten können. Daher entfällt ein Mitbestimmungsrecht des Betriebsrates nach § 87 Abs. 1 Nr. 1 BetrVG.[284]

2. Mitbestimmung bei der Arbeitnehmerüberwachung durch technische Einrichtungen nach § 87 Abs. 1 Nr. 6 BetrVG

Zweck des Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 BetrVG ist der präventive Persönlichkeitsschutz im Vorfeld der Gefährdung des Persönlichkeitsrechts.[285] Dadurch wird der in § 75 Abs. 2 BetrVG enthaltene Grundsatz konkretisieret, dass Arbeitgeber und Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern haben.[286] Der Arbeitnehmer soll hierdurch nicht vor jeglicher Überwachung geschützt werden, sondern nur vor den besonderen Gefahren von Überwachungsmethoden, die sich für das Persönlichkeitsrecht der Arbeitnehmer aus dem Einsatz von technischen Einrichtungen ergeben.[287] Mit Hilfe von technischen Mitteln kann eine sehr viel größere Menge an Daten gesammelt werden.[288] Dies kann praktisch andauernd und auch ohne die Wahrnehmung des Arbeitnehmers geschehen.[289]

Der Begriff der Überwachung i.S.v. § 87 Abs. 1 Nr. 6 BetrVG umfasst zunächst die Erhebung von Daten, beispielsweise durch Filmkameras, Abhörgeräte oder Stechuhren.[290] Darüber hinaus unterliegt nach der Rechtsprechung auch die Datenauswertung dem Mitbestimmungsrecht.[291] Hierbei müssen die auszuwertenden Daten nicht zwingend durch eine technische Einrichtung erhoben worden sein, damit der Mitbestimmungstatbestand gegeben ist.[292] Eine Auswertung liegt vor, wenn Daten so miteinander in Beziehung gesetzt werden, dass damit Aussagen über das Verhalten oder die Leistung von Arbeitnehmern ermöglicht wer-

---

[284] Zustimmend *Diller*, BB 2009, 438; Ablehnend *Steinkühler*, BB 2009, 1294.
[285] *Kothe*, in: Dünwell, Betriebsverfassungsgesetz Handkommentar, § 87 Rn. 66.
[286] *Trittin/Fischer*, NZA 2009, 343; *BAG*, Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278, 1279.
[287] *BAG*, Beschl. v. 30.08.1995 - 1 ABR 4/95, AP Nr. 29 zu § 87 BetrVG 1972 Überwachung.
[288] *Richardi*, in: Richardi, Betriebsverfassungsgesetz, § 87 Rn. 484.
[289] *BAG*, Beschl. v. 06.12.1983 - 1 ABR 43/81, AP Nr. 7 zu § 87 BetrVG 1972 Überwachung.
[290] *Kania*, in: Erfurter Kommentar zum Arbeitsrecht, § 87 BetrVG Rn. 48.
[291] *BAG*, Beschl. v. 14.09.1984 - 1 ABR 23/82, AP BetrVG 1972 § 87 Überwachung Nr. 9; *Kothe*, in: Dünwell, Betriebsverfassungsgesetz Handkommentar, § 87 Rn. 68; *Kania*, in Erfurter Kommentar zum Arbeitsrecht, § 87 BetrVG Rn. 49.
[292] *Richardi*, in: Richardi, Betriebsverfassungsgesetz, § 87 Rn. 490.

den.[293] Für die Überwachung des Verhaltens kommt es nicht darauf an, ob die Informationen für sich alleine schon eine sinnvolle Beurteilung ermöglichen. Auch Statusdaten, wie etwa Name oder Geburtstag, können durch Verknüpfung mit anderen Daten Aussagen über das Verhalten ermöglichen und damit von § 87 Abs. 1 Nr. 6 BetrVG erfasst werden.[294] Der Begriff des Verhaltens beschreibt ein vom Willen des Arbeitnehmers getragenes oder gesteuertes Tun oder Unterlassen, wobei es unerheblich ist in welchem Bereich es sich abspielt, ob bloß bei der Arbeitsleistung selbst oder sonst im Betrieb.[295]

Des Weiteren muss die technische Einrichtung zur Überwachung der Arbeitnehmer bestimmt sein, um unter das Mitbestimmungsrecht zu fallen.[296] Hierbei ist es unerheblich, ob diese tatsächlich dazu benutzt wird, Arbeitnehmer zu überwachen. Es genügt, dass damit Daten erhoben werden, die unmittelbar Rückschlüsse auf das Verhalten oder die Leistung der Arbeitnehmer ermöglichen.[297]

Im Fall der *Bahn* war der Zweck des Datenabgleichs von Mitarbeiterdaten und Lieferantendaten die Überwachung der Arbeitnehmer. Hilfsmittel waren Computer und entsprechende Software. Diese sind technische Hilfsmittel, so dass § 87 Abs. 1 Nr. 6 BetrVG anwendbar ist. Zwar wurden Daten verglichen, die weder leistungs- noch verhaltensbezogen waren. Jedoch ermöglichte der Datenabgleich Rückschlüsse auf eventuelle, durch Arbeitnehmer getätigte Scheingeschäfte mit der *Bahn* und folglich auf das, möglicherweise strafbare, Verhalten der Arbeitnehmer. Daher unterliegt das Abgleichen von Daten zum Zwecke der Korruptionsbekämpfung wohl der Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG.[298]

---

[293] *Kania*, in: Erfurter Kommentar zum Arbeitsrecht, § 87 BetrVG Rn. 49; *BAG*, Beschl. v. 14.09.1984 – 1 ABR 23/82, AP BetrVG 1972, § 87 Überwachung Nr. 9.

[294] *Fitting/Engels/Schmidt/Trebinger/Linsenmaier*, Betriebsverfassungsgesetz, § 87 Rn. 222.

[295] *Richardi*, in: Richardi, Betriebsverfassungsgesetz, § 87 Rn. 494.

[296] *Kothe*, in: Dünwell, Betriebsverfassungsgesetz Handkommentar, § 87 Rn. 71.

[297] *Richardi*, in: Richardi, Betriebsverfassungsgesetz, § 87 Rn. 505.

[298] Ablehnend *Diller*, BB 2009, 438 f, der in der Verwendung von Computer und Software keine technische Einrichtung sieht, da diese keine neue Möglichkeit der Überwachung schaffe, sondern diese lediglich beschleunige. Danach würde es sich beim Datenabgleich durch die Bahn um einen beschleunigten Vergleich zweier Listen handeln, der ebenso hätte von Hand durchgeführt werden können. Dem entgegnet *Steinkühler*, BB 2009, 1294 zutreffend, es handele sich hierbei sehr wohl um ein technisches Hilfsmittel und daher stehe dem Betriebsrat ein Mitbestimmungsrecht zu. Weiterhin sei grade der Zweck dieser Vorschrift, Arbeitnehmer vor den Möglichkeiten zu schützen, die sich durch die technischen Mittel zur Überwachung ergeben. Somit könne das Argument, dass es sich hierbei lediglich um eine Beschleunigung eines Vorganges handelt, der auch ohne Hilfsmittel möglich gewesen wäre, nicht dazu dienen Mitbestimmungsrechte auszuschließen.

VII. Informationspflichten

Unklar ist, in wieweit die Mitarbeiter der *Bahn* über die Datenabgleiche hätten informiert werden müssen. Nach § 33 Abs. 1 BDSG ist der Betroffene bei erstmaliger Speicherung seiner Daten über die Speicherung selbst, die Art der gespeicherten Daten sowie den Zweck der Speicherung durch die verantwortliche Stelle zu informieren.

Strittig ist hierbei, ob der Betroffene auch bei Änderungen bereits gespeicherter Daten zu informieren ist. So wird zum einen die Ansicht vertreten, dass dem Wortlaut entsprechend lediglich auf die erstmalige Speicherung von Daten abzustellen sei.[299] Es gibt jedoch auch Meinungen, nach denen der Betroffene erneut zu benachrichtigen sei, wenn eine neue Art von Daten erstmals gespeichert wird oder sich die Zweckbestimmung bereits gespeicherter Daten wesentlich ändert.[300] Zweck des § 33 Abs. 1 BDSG sei es, die Datenverarbeitung für den Betroffenen so transparent zu gestalten, dass dieser grundsätzlich Kenntnis davon hat, wer was wann und bei welcher Gelegenheit über ihn weiß.[301] Diese Transparenz erfordert indes eine erneute Benachrichtigung des Betroffenen bei Änderung der Zweckbestimmung, so dass hier der zweiten Ansicht gefolgt wird.

Nach § 33 Abs. 1 Satz 1 BDSG hätte die *Bahn* also die betroffenen Personen zu benachrichtigen gehabt, wenn personenbezogene Daten über sie gespeichert wurden.[302] Die Zahl der vom Datenabgleich betroffenen Arbeitnehmer ist sehr groß. Jedoch lag eine Speicherung von neuen Daten lediglich bei denjenigen vor, bei denen sich eine Übereinstimmung von Daten ergab. Somit könnte in diesem Fall von einer Unterrichtung zumindest der Personen abgesehen werden, deren Daten keine Übereinstimmungen aufwiesen. In den anderen Fällen hätten die Arbeitnehmer unterrichtet werden müssen.[303]

Darüber hinaus stellt die Nutzung von Kontodaten zum Datenabgleich im Rahmen der Compliance-Maßnahmen eine wesentliche Zweckänderung der Arbeit-

---

[299] *Schaffland/Wiltfang*, in: Bundesdatenschutzgesetz, § 33 Rn. 7.

[300] *Gola/Schomerus*, in: Bundesdatenschutzgesetz, § 33 Rn. 16; *Dix*, in: Simitis, Bundesdatenschutzgesetz, § 33 Rn. 11; ähnlich *Diller*, BB 2009, 438, 439, der bei Zweckänderung nur dann eine neue Benachrichtigungspflicht bejaht, wenn die Datennutzung eine neue Dimension erreicht und damit neue Gefährdungen bewirkt.

[301] *Dix*, in: Simitis, Bundesdatenschutzgesetz, § 33 Rn. 2.

[302] *Däubler*, in: Basiskommentar zum BDSG, § 33 Rn. 4; *Dix*, in: Simitis, Bundesdatenschutzgesetz, § 33 Rn. 9.

[303] *Dix*, in: Simitis, Bundesdatenschutzgesetz, § 33 Rn. 11; *Däubler*, in: Basiskommentar zum BDSG, § 33 Rn. 8.

nehmerdaten dar.[304] Folglich hätten alle betroffenen Arbeitnehmer über diese Zweckänderung informiert werden müssen.

Nach § 33 Abs. 2 Nr. 7b BDSG kann zwar von einer Unterrichtung der Betroffenen so lang abgesehen werden, wie die Information die Aufklärung von Unregelmäßigkeiten gefährden würde.[305] Eine vorzeitige Unterrichtung würde die Möglichkeit schaffen, Beweise zu vernichten und die Aufklärung zu verhindern.[306]

Nach Abschluss der internen Ermittlungen wäre es im Falle der *Bahn*, unabhängig von den rechtlichen Anforderungen, sinnvoll gewesen, alle Arbeitnehmer über die Compliance-Maßnahmen zu benachrichtigen. Denn die Information der Arbeitnehmer über unternehmensinterne Maßnahmen gegen Korruption kann durchaus eine Präventionswirkung entfalten.[307]

[304] *Kock/Francke*, ArbRB 2009, 110, 111; a.A. *Diller*, BB 2009, 438, 439.
[305] *Kock/Francke*, NZA 2009, 646, 650.
[306] *Mengel*, Compliance und Arbeitsrecht, Kap. 7 Rn. 44.
[307] *Kock/Francke*, NZA 2009, 646, 650.

H. E-MAIL

I. Kontrolle von E-Mails

Des Weiteren wurde publik, dass die *Bahn* im Jahr 2005 auch E-Mails von Mitarbeitern gezielt nach Kontakten zu Journalisten und Kritikern durchsucht hatte. Diese E-Mails wurden beim Auffinden bestimmter Namen oder Internetdomänen an interne Kontrollinstanzen weitergeleitet.[308]

Entscheidend für die Frage, ob die *Bahn* als Arbeitgeber dazu berechtigt war E-Mails von Arbeitnehmern zu kontrollieren, ist, ob den Bahn-Mitarbeitern die Privatnutzung des Internets erlaubt war.[309] Den Arbeitnehmern der *Bahn* war bis zum 18.12.2007 die private Nutzung von E-Mail und Internet untersagt. Seit dem 19.12.2007 gibt es eine Betriebsvereinbarung, welche die private Nutzung in geringfügigem Umfang erlaubt, wenn der Arbeitnehmer in die Nutzungsbedingungen einwilligt und den definierten Kontrollprozessen zustimmt.[310] Somit war zum hier gegenständlichen Zeitpunkt die private Nutzung des dienstlich zur Verfügung gestellten Zugangs zu Internet und E-Mail-Diensten untersagt.

Wenn die Kontrolle von E-Mails der Erfüllung oder Durchsetzung von Rechten und Pflichten aus dem Arbeitsvertrag dient, soll sie nach § 28 Abs.1 Satz 1 Nr. 1 BDSG zulässig sein.[311]

Darüber hinaus sind nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG Kontrollen zulässig, wenn sie zur Wahrung eines berechtigten Interesses erforderlich sind und die schutzwürdigen Interessen des Arbeitnehmers nicht überwiegen. Berechtigtes Interesse des Arbeitgebers ist vor allem die Feststellung, ob E-Mails tatsächlich nur dienstlich genutzt werden, um sein Eigentum zu schützen oder um arbeitszeitlichen oder inhaltlichen Missbrauch aufzudecken.[312] Die schutzwürdigen Interessen des Arbeitnehmers hängen von den Umständen des Einzelfalls ab und sind gegenüber den Interessen des Arbeitgebers abzuwägen.[313] Dabei zu berücksichtigen sind das Allgemeine Persönlichkeitsrecht des Arbeitnehmers, insbesondere das Recht am eigenen Wort, sowie das Recht auf informationelle Selbst-

[308] FAZ v. 28.03.2009, S. 1.
[309] *Dann/Gastell*, NJW 2008, 2945, 2947.
[310] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 13.
[311] *Schmidt*, BB 2009, 1297, 1298.
[312] *Mengel*, BB 2004, 2014, 2015.
[313] *Dann/Gastell*, NJW 2008, 2945, 2947.

bestimmung nach Art. 2 Abs. 1 GG und Art. 1 GG sowie das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG.[314]

Bereichsspezifische Vorschriften des TKG und des TMG sind nur dann anzuwenden, wenn die Nutzung von E-Mail und Internet aus einer ausdrücklichen oder konkludenten Genehmigung resultiert.[315] In diesem Fall war die private Nutzung nicht erlaubt, so dass TKG und TMG hier keine Anwendung finden.

a) Überwachung von Verbindungsdaten

Bislang gibt es noch keine höchstrichterliche Rechtsprechung zu der Frage, in welchem Umfang der Arbeitgeber E-Mails sowie die Nutzung des Internets kontrollieren darf.[316] Daher werden die bisher ergangene Rechtsprechung, sowie die in der Literatur entwickelten Grundsätze zur Nutzung dienstlicher Telefonate und Briefwechsel herangezogen.[317] Die E-Mail steht dem Telefongespräch, insbesondere bei eigener E-Mailadresse des Empfängers, näher als dem Brief.[318] Dafür spricht auch, dass der Absender eines Briefes im Gegensatz zum Versender einer E-Mail damit rechenden muss, dass dieser eventuell vom Sekretariat geöffnet oder von anderen Personen im Rahmen der Postbearbeitung zur Kenntnis genommen wird.[319] Dies kann jedoch je nach Firmenbrauch auch bei eingehenden E-Mails der Fall sein.

Überwiegend unstrittig ist, dass der Arbeitgeber, wenn ausschließlich die dienstlicher Nutzung des Internets erlaubt ist, die Verbindungsdaten, das bedeutet Datum, Uhrzeit und Datenvolumen von E-Mails, kontrollieren darf.[320] Dies wird mit Anlehnung an die Rechtsprechung zur Speicherung dienstlicher Telefondaten[321] begründet.[322]

Schwieriger zu beantworten ist die Frage, in wieweit dies auch für die Speicherung von Ziel- bzw. Absenderadressen von E-Mails gelten kann, da diese in der

---

[314] *Mengel*, BB 2004, 2014, 2016.
[315] *Gola/Wronka*, in: Handbuch zum Arbeitnehmerdatenschutz, Rn. 637; *Wolf/Mulert*, BB 2008, 442, 445; Schmidt, BB 2009, 1295, 1297; *Ernst*, NZA 2002, 585, 588; *Scherp/Stief*, BKR 2009, 404, 408.
[316] *Gola*, Datenschutz und Multimedia am Arbeitsplatz, Rn. 257.
[317] *Mengel*, BB 2004, 2014.
[318] *Däubler*, in: Internet und Arbeitsrecht, Rn. 249.
[319] *Ernst*, NZA 2002, 585, 589.
[320] *Wolf/Mulert*, BB 2008, 442; *Mengel*, BB 2004, 2014, 2016; *Ernst*, NZA 2002, 585, 590.
[321] *BAG*, Urt. v. 13.01.1987 – 1 AZR 267/85, NZA 1987, 515.
[322] *Mengel*, BB 2004, 2014, 2016; *Büllesbach*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 6.1 Rn. 82.

Regel den Namen des Empfängers bzw. Absenders, und bei dienstlichen Adressen auch den Namen des Unternehmens, beinhalten.[323] Die Rechtsprechung über die Zulässigkeit der Speicherung von Zielrufnummern bei Telefondaten kann nicht ohne weiteres herangezogen werden, da Zielrufnummern wesentlich anonymer sind.[324] Im Falle von dienstlichen Briefen ist es zulässig, dass der Arbeitgeber den Absender bzw. Adressaten erfasst und zur Akte nimmt.[325] Die überwiegende Meinung in der Literatur kommt daher zu dem Schluss, dass die Erfassung von Absendern bzw. Empfängern dienstlicher E-Mails zulässig ist.[326]

b) Inhaltskontrolle von E-Mails

Problematischer bei der Kontrolle von E-Mails ist die Frage, ob der Arbeitgeber neben den Verbindungsdaten auch den Inhalt der Nachrichten kontrollieren darf. Ist eine E-Mail eindeutig als privat gekennzeichnet, ist die Kenntnisnahme des Inhalts durch den Arbeitgeber nicht erlaubt.[327]

Anders ist dies bei den dienstlichen E-Mails. Folgt man der Ansicht, dass E-Mails wie dienstliche Telefonate zu behandeln sind, so haben Inhaltskontrollen die gleiche Eingriffswirkung in das Allgemeine Persönlichkeitsrecht der Arbeitnehmer wie das heimliche Mithören von Telefonaten.[328] Inhalte dürfen dann nur in Ausnahmefällen, beispielsweise bei konkretem Verdacht auf Straftaten oder Missbrauch, kontrolliert werden.[329]

Dagegen spricht jedoch, dass dem Absender einer E-Mail aufgrund unterschiedlicher Gewohnheiten in Unternehmen kein Vertrauensschutz zusteht, dass die E-Mail ausschließlich vom Empfänger gelesen wird.[330] E-Mails können beispielsweise wie Briefe oder Faxe zunächst durch das Sekretariat gesichtet oder ausgedruckt und zu den Akten genommen werden.[331] Darüber hinaus werden E-Mails auch im Rahmen des § 257 HGB und § 130 Abs. 1 BGB rechtlich wie Schrift-

[323] *Wolf/Mulert*, BB 2008, 442.
[324] *Ernst*, NZA 2002, 585, 590; *Wolf/Mulert*, BB 2008, 442, 443.
[325] *Mengel*, BB 2004, 2014, 2016.
[326] *Däubler*, in: Internet und Arbeitsrecht, Rn. 252; *Gola*/Wronka, in: Handbuch zum Arbeitnehmerdatenschutz, Rn. 688; *Lindemann/Simon*, BB 2001, 1950, 1952; *Mengel*, BB 2004, 2014, 2016; a.A. *Ernst*, NZA 2002, 585, 590, dieser geht von der Erfassung verkürzter E-Mailadressen aus und vertritt die Auffassung, dass diese sich nicht sinnvoll kürzen lassen und eine Erkennbarkeit bestehen bleibt.
[327] *Klenge/Mückenberger*, CCZ 2009, 81, 83.
[328] *Däubler*, in: Internet und Arbeitsrecht, Rn. 249.
[329] *Büllesbach*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 6.1 Rn. 82.
[330] *Gola*/Wronka, in: Handbuch zum Arbeitnehmerdatenschutz, Rn. 690.
[331] *Mengel*, BB 2004, 2014, 2017.

stücke behandelt.[332] Unter diesen Annahmen sollen dienstliche E-Mails wie Briefe zu behandeln sein.[333] Die Kenntnisnahme von Inhalten der Geschäftspost durch den Arbeitgeber ist indes zulässig, da sie als Teil der Arbeitsleistung aufgefasst werden und somit als Teil der Unternehmenskommunikation dem Unternehmen zustehen.[334]

Eine besondere Rechtfertigung ist in jedem Fall notwendig, wenn der Arbeitnehmer nicht über Zugriffe auf seine E-Mails informiert wird, dies also heimlich geschieht, da er in diesem Fall darauf vertrauen dürfen soll, dass seine E-Mails zumindest nicht ohne Rückfragen kontrolliert werden.[335] Der Arbeitnehmer soll sich bei der Gestaltung seiner E-Mails auf Kontrollen einstellen können.[336] Ein Hinweis über Kontrollen kann auch in einfacher und allgemeiner Form, wie beispielsweise im Rahmen der Betriebsvereinbarung geschehen.[337]

Bei der *Bahn* soll es eine entsprechende Betriebsvereinbarung gegeben haben, in der es hieß, dass die Verkehrsdaten samt Adress- und Betreffzeile protokolliert würden.[338] Ob auch Inhaltskontrollen vereinbart wurden, ist hingegen nicht bekannt. Inhaltliche Kontrollen von E-Mails wurden nach Angaben der *Bahn* erst bei konkretem Verdacht vorgenommen. Ein solcher Verdacht konnte dabei durch das Auffinden von Namen von Journalisten oder Kritikern der *Bahn* in der Adress- oder Betreffzeile entstehen. Das Vorgehen der *Bahn* war somit rechtlich nicht zu beanstanden.

II. Zurückhalten von E-Mails der Gewerkschaft

Neben der Kontrolle von E-Mails wurden im Jahr 2007 auch E-Mails der Gewerkschaft *GDL* mit der Begründung nicht weitergeleitet, dass ein Server durch die Masse der von der *GDL* verschickten E-Mails zusammengebrochen sei.[339]

Im Schrifttum ist umstritten, ob Gewerkschaften überhaupt E-Mails an die dienstlichen E-Mail-Adressen von Arbeitnehmern versenden dürfen.[340] Das *BAG*

[332] *Dann/Gastell*, NJW 2008, 2945, 2948.
[333] *Beckschulze*/ Henkel, DB 2001, 1491, 1494; *Grosjean*, DB 2003, 2650, 2652.
[334] *Klenge/Mückenberger*, CCZ 2009, 81, 83.
[335] *Lindemann/Simon*, BB 2001, 1950, 1952.
[336] *Gola*, Datenschutz und Multimedia am Arbeitsplatz, Rn. 257.
[337] *Lindemann/Simon*, BB 2001, 1950, 1952.
[338] *Schwenn*, FAZ v. 31.03.2009, S. 3.
[339] *Schwenn*, FAZ v. 31.03.2009, S. 3.

hat dazu entschieden, dass es Gewerkschaften grundsätzlich gestattet sei, E-Mails zu Werbe- und Informationszwecken an betriebliche E-Mail-Adressen von Beschäftigten zu versenden.[341] Dies gilt unabhängig davon, ob der Arbeitgeber die private Nutzung dienstlicher E-Mail-Konten erlaubt.

Eine Beschränkung der Ausübung der nach Art. 9 Abs. 3 GG geschützten Betätigungsfreiheit der Gewerkschaften kann nur ausnahmsweise durch gleichwertige Interessen des Arbeitgebers erfolgen.[342] Gleichwertige Interessen können Eigentumsstörungen oder Eingriffe in das Recht am eingerichteten und ausgeübten Gewerbebetrieb sein. Diese Eingriffe müssen aber der Gewerkschaft zurechenbar und jedenfalls geeignet sein, das Funktionieren des Betriebes oder den Gebrauch des Eigentums in spürbarer Weise zu beeinträchtigen.[343]

Dass die E-Mails Speicherplatz auf dem Server des Arbeitgebers benötigen und die Arbeitnehmer diese innerhalb ihrer Arbeitszeit lesen, führt nicht nachweislich zu nennenswerten Betriebsstörungen. Tatsächlich ist durch den benötigten elektronischen Speicher keine Beeinträchtigung ersichtlich.[344] Die Arbeitszeit wird allenfalls für wenige Minuten beansprucht. Eine rechtlich bedeutsame Belastung könnte nur angenommen werden, wenn dies über das sozialübliche Maß an Zeit hinausginge, das der Arbeitnehmer auch sonst mit privaten Gesprächen mit Kollegen oder sonstigen privaten Verrichtungen verbringen würde.[345] Darüber hinaus ist die benötigte Zeit nicht größer als die zum Lesen des Informations- und Werbematerials notwendige, das den Arbeitnehmern im Betrieb in Papierform überreicht wird.[346]

Den Interessen des Arbeitgebers stehen die Interessen der Gewerkschaft gegenüber. Zweifellos bietet die Informationsversendung mit Hilfe des Internets für die Gewerkschaften diverse Vorteile. So können die Gewerkschaftsmitglieder beispielsweise zeitnah und kostengünstig über Streiks, Versammlungen oder andere Ereignisse informiert werden. Es ist jedoch nicht zwingend notwendig auf einem Weg zu informieren, der in den eingerichteten und ausgeübten Betrieb des

---

[340] Bejahend *Däubler*, in: Internet und Arbeitsrecht, Rn. 527 ff.; ablehnend bei nicht erlaubter Privatnutzung des Internets *Gola*/Wronka, in: Handbuch zum Arbeitnehmerdatenschutz, Rn. 1789; zweifelnd *Beckschulze*/*Henkel*, DB 2001, 1491, 1501.
[341] *BAG*, Urt. v. 20.01.2009 – 1 AZR 515/08, NZA 2009, 615.
[342] *Däubler*, in: Internet und Arbeitsrecht, Rn. 528.
[343] *BAG*, Urt. v. 20.01.2009 – 1 AZR 515/08, NZA 2009, 615.
[344] *BAG*, Urt. v. 20.01.2009 – 1 AZR 515/08, NZA 2009, 615, 620.
[345] *BAG*, Urt. v. 20.01.2009 – 1 AZR 515/08, NZA 2009, 615, 618.
[346] *Däubler*, in: Internet und Arbeitsrecht, Rn. 528.

Arbeitgebers eingreift. So könnten Gewerkschaften beispielsweise auch die privaten E-Mail-Adressen der Arbeitnehmer oder die eigene Homepage zu Informationszwecken nutzen.[347]

Sollte tatsächlich ein Server der *Bahn* durch die Masse an E-Mails, die die Gewerkschaft versenden wollte ausgefallen sein, wäre dies eine Beeinträchtigung der Funktion des Betriebes gewesen. Da bei Ausfall eines Servers in der Regel auch der weitere E-Mail-Verkehr beeinträchtigt sein wird, kann der dadurch entstehende Schaden eventuell erheblich werden. Das muss der Arbeitgeber freilich nicht hinnehmen.

Die *Bahn* beschäftigt rund 240.000 Mitarbeiter, davon ca. 182.000 in Deutschland. Die betreffende E-Mail der Gewerkschaft war an 30.000 Mitarbeiter adressiert.[348] Das bedeutet, dass weniger als 17 Prozent der in Deutschland beschäftigten Mitarbeiter diese E-Mail der Gewerkschaft erhalten sollten. Es ist zwar nicht bekannt, wie groß diese E-Mail vom Datenvolumen her war. Unter der Annahme, dass es sich um eine durchschnittlich große E-Mail ohne Anhänge handelte, ist jedoch davon auszugehen, dass die tatsächliche zusätzliche Belastung der Server durch die Gewerkschafts-E-Mails relativ gering war. Daher scheint es überraschend, dass durch diese E-Mails ein Server ausgefallen sein sollte. Tatsächlich hat der neue Vorstandsvorsitzende der *Bahn – Dr. Rüdiger Grube* – in einer späteren Pressekonferenz eingeräumt, dass die betreffende E-Mail der *GDL* zunächst inhaltlich durchsucht und anschließend heimlich gelöscht wurde.[349]

Da diese E-Mail zu einem Zeitpunkt versandt wurde, zu dem Tarifverhandlungen geführt wurden, könnte es sich bei der E-Mail auch um einen rechtswidrigen Aufruf zum Streik gehandelt haben. Die *GDL* hatte unter anderem eine Erhöhung der Monatsentgelte um mindestens 31 Prozent sowie kürzere Arbeitszeiten und einen Jahresruhetagplan gefordert.[350]

---

[347] *Arnold/Wiese*, NZA 2009, 716, 719.
[348] *Schwenn*, FAZ v. 31.03.2009, S. 3.
[349] Pressekonferenz *Dr. Rüdiger Grube*, (siehe o. Fußn. 4), S. 3.
[350] *LAG Sachsen*, Urt. v. 02.11.2007 – 7 SaGa 19/07, NZA 2008, 59, 62.

I. ZUSAMMENARBEIT MIT EXTERNEN DIENSTLEISTERN

Viele Ermittlungen wurden im Auftrag der *Bahn* durch externe Dienstleister und Detekteien durchgeführt. Hierbei wurden zum Teil Daten ermittelt, die nicht ohne weiteres zugänglich sind, wie zum Beispiel Bankkontobewegungsdaten.[351] Im Rahmen dieser Arbeit soll nicht geklärt werden, wie die Daten beschafft wurden und welche Konsequenzen sich daraus für die Dienstleister ergeben. Hier soll vielmehr die Frage aufgeworfen werden, ob sich die *Bahn* als Auftraggeber die Rechtsverstöße der von ihr eingesetzten Dienstleister anrechnen lassen muss.

Arbeitgeber dürfen bei konkreten Verdachtsfällen von strafbaren Handlungen oder schweren Vertragsverletzungen grundsätzlich Detekteien zur Überwachung von Mitarbeitern einsetzen.[352] Da das Selbstbestimmungsrecht der Arbeitnehmer dadurch erheblich beeinträchtigt wird, dürfen solche Ermittlungsmethoden jedoch erst eingesetzt werden, wenn der Arbeitgeber alle zumutbaren Maßnahmen unternommen hat, den Verdacht auszuräumen.[353] Darüber hinaus muss der private Kernbereich des Arbeitnehmers unberührt bleiben.[354]

Im Fall der *Bahn* ist unklar, wie beispielsweise Kontobewegungsdaten beschafft wurden. Diese könnten Ergebnis von Bestechungen oder illegalem Eindringen in Computersysteme sein. Die *Bahn* selbst könnte dann bei möglichen Straftaten als Anstifter zur Tat im Sinne von § 26 StGB in Frage kommen.

Für den Nachweis einer Anstiftung wäre die Kenntnis der Vorgehensweise der Firma *Network Deutschland GmbH* bei der Datenbeschaffung notwendig. Darüber hinaus müsste es eine an den Täter gerichtete Aufforderung gegeben haben, die den Kern der Tat hätte kennzeichnen müssen und mitursächlich für den Tatentschluss hätte sein müssen.[355] Es ist jedoch nicht belegbar, welche Daten genau ermittelt werden sollten. So hat die *Bahn* zwar nach eigenen Angaben einen Bericht der *Network Deutschland GmbH* aus dem Jahr 2003, der Kontobewegungsdaten enthielt, zurückgewiesen, weil die Ermittlung dieser Daten nicht beauftragt worden sei.[356] Die Zusammenarbeit mit dem Unternehmen wurde jedoch nicht

[351] Pressekonferenz *Dr. Rüdiger Grube*, (siehe o. Fußn. 4), S. 3.
[352] *Lunk*, NZA 2009, 457, 461.
[353] *LAG Baden-Württemberg*, Urt. v. 25.10.2002 – 5 Sa 59/00, BeckRS 2009, 68144.
[354] *Lunk*, NZA 2009, 457, 461.
[355] *Puppe*, NStZ 2006, 424.
[356] *Deutsche Bahn AG*, Zwischenbericht, (siehe o. Fußn. 2), S. 34.

beendet. Daher ist davon auszugehen, dass die *Bahn* über zweifelhafte Vorgänge bei der *Network Deutschland GmbH* informiert war und diese zumindest billigend in Kauf genommen hat.

J. DATENSCHUTZ ALS COMPLIANCE-AUFGABE

Zu den Aufgaben der Compliance gehört nicht nur die Verhinderung und Aufdeckung von Korruption im Unternehmen, sondern auch die Vermeidung von Verstößen gegen geltendes Datenschutzrecht. Werden beispielsweise bei internen Untersuchungen die Vorgaben von Straf-, Arbeits- und Datenschutzrecht nicht beachtet, kann dies zu einem Image-Schaden für das Unternehmen führen.[357] Unsachgemäß gestaltete Ermittlungen können sowohl erhebliche rechtliche, teils sogar strafrechtliche, Risiken für Unternehmen und deren Verantwortliche bergen, als auch zu Beweisverwertungsverboten, dem Verfall von Schadensersatzansprüchen oder zur Unwirksamkeit von ausgesprochenen Kündigungen führen.[358]

Weitere Risiken begründen Mitarbeiter, die unsachgemäß mit Daten umgehen. Mögliche Folgen für Unternehmen ergeben sich aus den §§ 43 und 44 BDSG. So können von der zuständigen Aufsichtsbehörde Bußgelder zwischen 25.000 Euro und 250.000 Euro verhängt werden. Daneben drohen auch Haftstrafen, sowie Schadensersatzklagen Betroffener nach § 7 BDSG.

Um sicher zu stellen, dass die Datenschutzgesetze beachtet werden, muss ein Datenschutzbeauftragter bestellt werden, wenn mehr als neun Personen mit der elektronischen Verarbeitung personenbezogener Daten beschäftigt sind, § 4f Abs. 1 Satz 4 BDSG. Dieser muss sowohl über Kenntnisse im Datenschutzrecht, als auch über Verfahren und Techniken der Datenverarbeitung verfügen.[359] Darüber hinaus sollte die Person zuverlässig sein und keinen Interessenkonflikt unterliegen.[360]

Die nachfolgende Abbildung 2 veranschaulicht die fachlichen und charakteristischen Anforderungen an einen Datenschutzbeauftragten.

[357] *Dann/Gastell*, NJW 2008, 2945, 2949.
[358] *Klengel/ Mückenberger*, CCZ 2009, 81.
[359] *Gola*, in: Gola/Schomerus, Bundesdatenschutzgesetz, § 4 f, Rn. 20.
[360] *Neundorf*, in: Hauschka (Hrsg.), Corporate Compliance, § 27 Rn. 4.

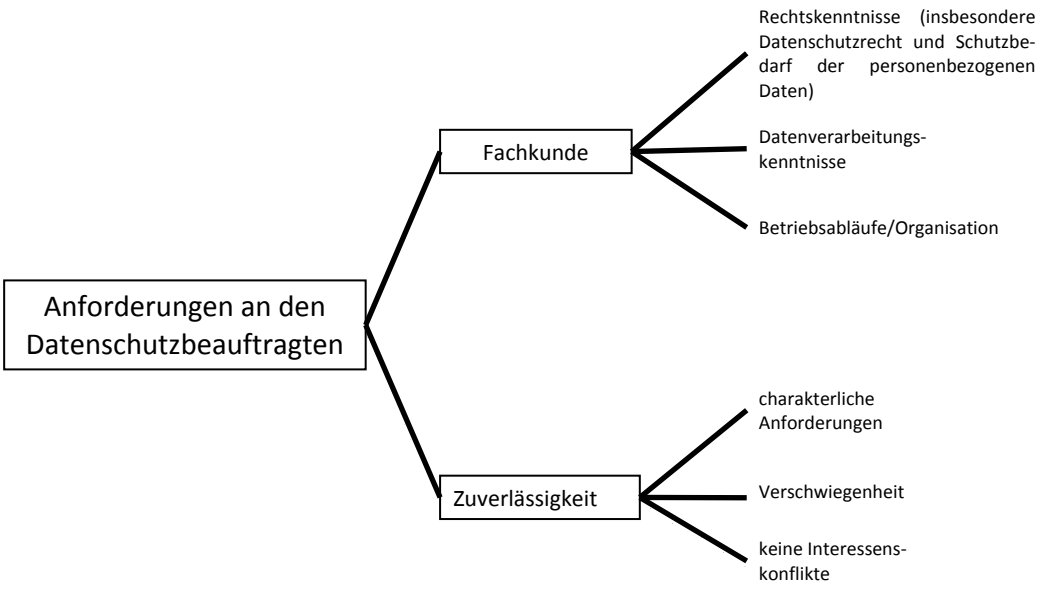


Abbildung 2: Anforderungen nach § 4 f Abs. 2 BDSG an den Datenschutzbeauftragten[361]

Alle Personen, die durch ihre Tätigkeit mit personenbezogenen Daten sind, sind nach § 5 BDSG auf das Datengeheimnis zu verpflichten, welches auch nach Beendigung ihrer Tätigkeit fortbesteht.[362]

Nach § 9 BDSG und Anhang sind Unternehmen außerdem verpflichtet, in eigener Verantwortung alle technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind und in einem angemessen Verhältnis zum angestrebten Schutzzweck stehen, um die Einhaltung der Datenschutzgesetze zu gewährleisten.[363]

Ferner können Unternehmen sogenannte Datenschutzauditierungen nach § 9a BDSG durchführen, um die Datensicherheit zu erhöhen.[364]

[361] Quelle: *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 4f Rn. 91.
[362] *Mengel*, Compliance und Arbeitsrecht, Kap. 7 Rn. 1.
[363] *Schaffland/Wiltfang*, in: Bundesdatenschutzgesetz, § 9 Rn. 1.
[364] *Neundorf*, in: Hauschka (Hrsg.), Corporate Compliance, § 27 Rn. 19.

K. FAZIT

I. Compliance

Viele der in der Literatur vorgeschlagene Maßnahmen für die Einrichtung einer effektiven Compliance-Organisation wurden bei der *Bahn* umgesetzt. Zu wenig Beachtung fand dabei jedoch der Datenschutz. Dieser ist allerdings Teil einer umfassenden Compliance und sollte dementsprechend umgesetzt werden.

Inzwischen wurde bekannt, dass die *Bahn* trotz des im Übrigen eingeschlagenen Sparkurses viel Geld in ihre Compliance-Struktur steckt und diese Aufgabe inzwischen direkt beim Vorstand angesiedelt ist.[365] Danach soll die Hauptaufgabe der Abteilung Compliance künftig in erster Linie in der Prävention, Beratung und Schulung liegen. Die Mitarbeiter bekämen klarere Vorgaben mittels neuer Betriebsvereinbarungen. Auch hat das Unternehmen das im Zusammenhang mit der Datenaffäre verhängte Bußgeld der Berliner Datenschutzbehörde in Höhe von 1,1 Millionen Euro akzeptiert.[366]

II. Datenabgleich

Der Datenabgleich bei der *Bahn* war grundsätzlich zulässig.[367] Eine denkbare Rechtfertigungsgrundlage ergibt sich aus § 28 Abs. 1 BDSG. Möglich wäre auch eine Betriebsvereinbarung oder die Einwilligung der Betroffenen gewesen. Dies hätte die *Bahn* jedoch im Vorfeld besorgen müssen. Auch wenn diese sog. Mitarbeiter-Screenings nur dann effektiv sind, wenn viele Daten verglichen werden, um so auf mögliche Parallelen zu stoßen,[368] waren die Maßnahmen der *Bahn* jedoch insoweit unverhältnismäßig, wie die Daten der Arbeitnehmer unabhängig von ihrer konkreten Möglichkeit, Einfluss auf Zahlungen zu nehmen, verdachtsunabhängig abgeglichen wurden. Hier wäre es erforderlich gewesen, im Vorfeld die Datensätze solcher Mitarbeiter von der Überprüfung auszuschließen, die denkunmöglich an einer Korruptionshandlung zu Lasten des Unternehmens hätten teilnehmen können.

---

[365] FAZ v. 24.11.2009, S. 13.
[366] FAZ v. 24.11.2009, S. 13.
[367] *Lelley*, GmbHR 2009, R 209 f.
[368] Dazu *Vogt*, NJOZ 2009, 4206, 4214.

Weder die Informationspflichten der Betroffenen noch die Mitbestimmungsrechte des Betriebsrates wurden allerdings beachtet. Darüber hinaus war die Anzahl der von der Maßnahme Betroffenen unverhältnismäßig hoch. Ein Verstoß gegen die Informationspflichten aus § 33 BDSG kann nach § 43 Abs. 1 Nr. 8 und Abs. 3 BDSG mit einer Geldbuße von bis zu 25.000 Euro geahndet werden. Strafbar nach § 44 BDSG sind nur vorsätzliche Verstöße, die gegen Entgelt oder in Bereicherungs- oder Schädigungsabsicht begangen wurden. Die Missachtung von Mitbestimmungsrechten des Betriebsrates kann indes zu einem Unterlassungsanspruch führen.[369]

III. E-Mail-Kontrolle und Verhinderung der Weiterleitung

Die *Bahn* durfte die dienstlichen E-Mails ihrer Mitarbeiter kontrollieren. Dieses Vorgehen ist sicherlich auch geeignet, um Geheimnisverrat im Unternehmen aufzudecken, jedoch ist es nicht förderlich für das Betriebsklima. So dürften Arbeitnehmer, die sich überwacht fühlen, einem größeren Anreiz unterliegen korrupt zu handeln und Informationen weiter zu geben als Arbeitnehmer, die sich ihrem Unternehmen verbunden fühlen. Daher wären Gespräche mit verdächtigen Arbeitnehmern und die Förderung eines guten Arbeitsklimas ebenfalls mögliche Mittel zur Verhinderung von Geheimnisverrat gewesen. Darüber hinaus kann es dem Ruf eines Unternehmens beachtlichen Schaden zufügen, wenn solche Maßnahmen in der Öffentlichkeit als „Ausspionieren von Kritikern“ aufgefasst werden.[370]

Eine abschließende Beurteilung der rechtlichen Lage bezüglich der gelöschten E-Mails der Gewerkschaft ist ohne Kenntnis des Inhalts nicht möglich. Es deutet jedoch alles darauf hin, dass die *Bahn* hier rechtswidrig und massiv in die Betätigungsfreiheit der Gewerkschaft eingegriffen hat.

[369] *Mengel*/*Ulrich*, NZA 2006, 240, 245.
[370] *Leyendecker*, sueddeutsche.de v. 04.06.2009.

IV. Zusammenarbeit mit Dienstleistern

Aus den öffentlichen Angaben der *Bahn* ist nicht ersichtlich, in wie weit die *Bahn* selbst die Beschaffung von nicht ohne weiteres zugänglichen Daten forciert hat. Klar ist jedoch, dass die *Bahn* darüber informiert war, dass die *Network Deutschland GmbH* auch Daten über Kontobewegungen beschafft hat. Dennoch hat die *Bahn* weiterhin mit dieser Firma zusammengearbeitet, so dass davon auszugehen ist, dass die *Bahn* solche Vorgänge zumindest billigend in Kauf genommen hat.

L. AUSBLICK

I. Allgemein

Spätestens seit dem Korruptionsfall *Siemens* ist die Frage nach der Haftung von Unternehmen und ihren Managern bei Straftaten ins Licht der öffentlichen Aufmerksamkeit gerückt. Der Fall *Siemens*, bei dem es um Schmiergelder in Millionenhöhe ging, führte zu einer Verurteilung des Unternehmens zur Zahlung von 38 Millionen Euro. Daneben wurden einige Manager zu Bewährungsstrafen und Bußgeldzahlungen verurteilt.[371] Das Unternehmen hat inzwischen auch gegen verschiedene ehemalige Mitglieder von Vorstand und Aufsichtsrat Schadensersatzansprüche geltend gemacht.

Jedem Manager dürfte seither bewusst sein, dass er bei Vernachlässigung seiner Aufsichtspflichten zur Rechenschaft gezogen werden kann. Bei näherer Betrachtung ist allerdings festzustellen, dass allgemeingültige Anhaltspunkte, was die Aufsichtspflichten konkret umfassen, fehlen.[372]

Gleichzeitig nehmen seit einiger Zeit auch die Berichte über Unternehmen zu, die in ihrem Bemühen, ihren Aufsichtspflichten nachzukommen, zu weit in die Privatsphäre ihrer Arbeitnehmer eindringen. Man denke da nur an die Medienberichte über den Lebensmitteldiscounter *Lidl*[373], die *Deutsche Telekom AG* oder die *Deutsche Bank AG*. Angesichts dieser Entwicklung werden Stimmen laut, die eine Reform des Datenschutzes und insbesondere ein Arbeitnehmerdatenschutzgesetz fordern.

II. § 32 BDSG n.F.

Im Zuge dieser Entwicklung entstand zwar kein neues Arbeitnehmerdatenschutzgesetz, jedoch § 32 BDSG n.F., der zum 01.09.2009 in Kraft getreten ist.[374] Dieser wird künftig § 28 Abs. 1 BDSG als gesetzliche Verarbeitungsbe-

[371] *Ott*, sueddeutsche.de v. 14.05.2007.
[372] *Bussmann/Matschke*, CCZ 2009, 132.
[373] *Lelley*, GmbHR 2009, R209.
[374] Neu eingefügt durch das Gesetz zur Änderung datenschutzrechtlicher Vorschriften, BGBl. I v. 19.08.2009, S. 2814.

fugnis im Arbeitsverhältnis als lex specialis vorgehen und damit zur wichtigsten Neuerung für den Umgang mit Arbeitnehmern.[375]

§ 32 Abs. 1 Satz 1 BDSG n.F. soll dabei den bisher lediglich aus der Rechtsprechung des *BVerfG* zum Allgemeinen Persönlichkeitsrecht hergeleiteten allgemeinen Grundsätzen zum Datenschutz in Beschäftigungsverhältnissen entsprechen.[376] Dem Wortlaut des neuen § 32 BDSG nach dürfen personenbezogene Daten eines Beschäftigten 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.[377]

Nicht näher bestimmt ist indes, was als *erforderlich* anzusehen ist. Werden die bisherigen Grundsätze zum Arbeitnehmerdatenschutz zu Grunde gelegt, ist die Datennutzung erforderlich, wenn berechtigte Interessen von Unternehmen auf andere Weise nicht oder nicht angemessen gewahrt werden können.[378] Somit kann durch die Erforderlichkeit im Prinzip nur die Verarbeitung von für den Zweck überflüssigen Daten verhindert werden.[379] Außerdem muss weiterhin das Verhältnismäßigkeitsprinzip beachtet werden.[380] Dies gilt nach § 32 Abs. 2 BDSG auch für solche Daten, die nicht in automatisierter Form vorliegen oder genutzt werden.[381]

Zum Zwecke der Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, § 32 Abs. 1 Satz 2 BDSG. Sollen interne Ermittlungen durchgeführt werden, sind Anhaltspunkte für mögliche Straftaten schon vor Beginn der Ermittlungen zu dokumentiert.[382] Daraus soll jedoch nicht folgen, dass § 32 Abs. 1 Satz 2 BDSG unternehmensinterne Ermittlungen insgesamt verhindere.[383] Weiterhin dürfen der Datenverwendung

[375] *Deutsch/Diller*, DB 2009, 1462.
[376] Begr. RegE in der Beschlussempfehlung des Innenausschusses, BT-Drs. 16/13657, S. 21.
[377] *Gola/Klug*, NJW 2009, 2577, 2580.
[378] *Wybitul*, BB 2009, 1582, 1583.
[379] *Deutsch/Diller*, DB 2009, 1462, 1463.
[380] *Gola/Klug*, NJW 2009, 2577, 2580.
[381] *Deutsch/Diller*, DB 2009, 1462.
[382] *Vogel/Glas*, DB 2009, 1747.
[383] *Schmidt*, RDV 2009, 193, 195 ff.; *Scherp/Stief*, BKR 2009, 404, 410.

keine überwiegenden schutzwürdigen Interessen des Betroffenen entgegenstehen und Art und Ausmaß der Verwendung dürfen im Hinblick auf den Anlass nicht unverhältnismäßig sein.[384] Grund für die Abwägung der Interessen an dieser Stelle sei die Tatsache, dass Maßnahmen zur Aufdeckung von Straftaten regelmäßig besonders intensiv in das allgemeine Persönlichkeitsrecht des von der Maßnahme Betroffenen eingriffen.[385]

Fraglich ist jedoch, wie das Verhältnis dieser Vorraussetzungen zu den allgemeinen arbeitsrechtlichen Grundsätzen ist. Denn Straftaten stellen regelmäßig auch eine Verletzung der Pflichten des dem Arbeitnehmerverhältnis zu Grunde liegenden Vertrages dar und betreffen damit auch die Durchführung des Beschäftigungsverhältnisses iSd § 32 Abs. 1 Satz 1 BDSG.[386] Offen ist daher, ob gegen solche Pflichtverletzungen nur unter den engeren Voraussetzungen des § 32 Abs. 1 Satz 2 BDSG vorgegangen werden darf.

Geänderte Regelungen gelten nun auch für die Auftragsdatenverarbeitung. § 11 Abs. 2 BDSG n.F. enthält erheblich umfangreichere Anforderungen an die erforderlichen Mindestinhalte von Auftragsdatenverarbeitungsverträgen.[387]

Da auch eine mangelnde Befolgung datenschutzrechtlicher Vorgaben kritisiert wurde,[388] gab es auch in diesem Bereich Neuerungen. So haben Aufsichtsbehörden nun die Möglichkeit, Maßnahmen zur Beseitigung von Datenschutzverstößen anzuordnen oder im Extremfall entsprechende Verarbeitungsverfahren ganz zu untersagen sowie die Möglichkeit der Gewinnabschöpfung.[389]

Kern des Problems ist allerdings nicht, dass es kein oder nur ein unzureichendes Datenschutzrecht gäbe, sondern viel mehr, dass das vorhandene Datenschutzrecht äußerst schwierig zu durchschauen ist.[390] Daneben fehlt es zur Zeit noch an beispielhafter Rechtsprechung, die Orientierung verschaffen könnte.[391] Festzuhalten bleibt daher, dass der Grad zwischen der Vernachlässigung von Aufsichtspflichten und zu weitgehenden Eingriffen in die Rechte von Arbeitnehmern schmal ist. Gleichzeitig ist die Rechtsunsicherheit umso größer. Zweifellos gibt

[384] *Gola/Klug*, NJW 2009, 2577, 2580.
[385] Begr. RegE in der Beschlussempfehlung des Innenausschusses, BT-Drs. 16/13657, S. 21.
[386] *Löwisch*, DB 2009, 2782, 2785.
[387] *Moos*, BB 2009, Heft 34, M1.
[388] *Kock/Francke*, NZA 2009, 646, 651.
[389] *Moos*, BB 2009, Heft 34, M1.
[390] *Lelley*, GmbHR 2009, R 209, R 210.
[391] *Thüsing*, NZA 2009, 865, 866.

es sowohl Gesetze zur Haftung von Unternehmen und Managern als auch zum Schutz der Arbeitnehmer vor zu weit reichenden Eingriffen in ihre Persönlichkeitsrechte. Jedoch wäre eine konkretere Formulierung der Rechte und Pflichten erstrebenswert.

Die Änderungen des BDSG können daher nicht zur Verbesserung der Situation beitragen.[392] Die Anforderungen sind weiter verschärft worden, die konkrete Anwendbarkeit der Normen im Alltag der Unternehmen indes nicht verbessert worden. Darüber hinaus müssen die Unternehmen erheblich mehr Vorgänge dokumentieren.[393] Daher ist zu erwarten, dass die Rechtsunsicherheit durch die Neuerungen noch weiter zunimmt.[394]

III. Gesetzgebung de lege ferenda

Die Regierungsparteien der 17. Legislaturperiode, CDU, CSU und FDP haben in ihrem Koalitionsvertrag vereinbart, den Arbeitnehmerdatenschutz zu verbessern, indem der Arbeitnehmerdatenschutz in einem eigenständigen Kapitel des Bundesdatenschutzgesetzes geregelt werden soll.[395] Zum Schutze der Arbeitnehmer sollen nur solche Daten erhoben werden dürfen, die für das Arbeitsverhältnis erforderlich sind, wobei gleichzeitig den Arbeitgebern verlässliche Regelungen im Kampf gegen die Korruption zur Verfügung gestellt werden sollen.[396]

Von der SPD-Bundestagsfraktion ist inzwischen ein Gesetzentwurf für ein Gesetz zum Datenschutz im Beschäftigungsverhältnis (Beschäftigtendatenschutzgesetz – BDatG) vorgelegt worden.[397] Darin wird wegen der Defizite der gesetzlichen Regelung des geltenden Datenschutzrechts die Notwendigkeit eines eigenständigen Beschäftigtendatenschutzgesetzes angemahnt.[398] Ziel ist es, die Unternehmen stärker als bisher zu verpflichten, die Persönlichkeitsrechte des einzel-

---

[392] Ähnlich *Barton*, RDV 2009, 200, 202, der „eine „Verschlimmbesserung" der gegenwärtigen Situation" sieht.
[393] *Gola/Klug*, NJW 2009, 2577, 2583.
[394] Zustimmend *Deutsch/Diller*, DB 2009, 1462, 1465; *Wybitul*, BB 2009, 1582, 1584; *Vogel/ Glas*, DB 2009, 1747, 1754.
[395] WACHSTUM. BILDUNG. ZUSAMMENHALT. Koalitionsvertrag zwischen CDU, CSU und FDP, S. 106.
[396] WACHSTUM. BILDUNG. ZUSAMMENHALT. Koalitionsvertrag zwischen CDU, CSU und FDP, S. 106.
[397] BT-Drs. 17/69 v. 25.11.2009.
[398] BT-Drs. 17/69, S. 1.

nen Arbeitnehmers zu beachten, indem in dem neuen Gesetz geregelt werde, welche Daten des Arbeitnehmers explizit durch den Arbeitgeber erhoben und verwendet werden dürfen.[399] Grundsätzlich sollen dies nur solche Daten sein, die der Arbeitgeber zur Erfüllung seiner Pflichten oder Wahrnehmung seiner Rechte notwendigerweise benötigt. Darüber hinausgehende Datenerhebung oder unzulässige Verwendung der Daten soll zu einem Anspruch des Arbeitnehmers auf Unterlassung und Schadensersatz führen, § 23 BDatG-E.[400] Darüber hinaus sollen in dem Gesetz auch solche Fragen wie etwa die Videoüberwachung am Arbeitsplatz oder die private Nutzung von Telefon, E-Mail und Internet am Arbeitsplatz geregelt werden.

Ein Beschäftigtendatenschutzgesetz hätte den Vorzug, dass die herrschenden Probleme, die insbesondere auf der immer weiter fortschreitenden Digitalisierung und Vernetzung von Arbeitnehmerdaten gründen spezifischen Lösungen zugeführt würden. Andererseits würde die Unübersichtlichkeit des geltenden Datenschutzrechts durch ein weiteres bereichsspezifisches Sonderrecht verkompliziert werden. Es bleibt daher abzuwarten, wie die weitere Entwicklung de lege ferenda aussehen wird. Vorzugswürdig erscheint es jedoch, das Datenschutzrecht insgesamt einer umfassenden Revision und Fortschreibung zu unterziehen, als ein weiteres Mal an neuer Stelle mit gesetzgeberischem Flickwerk aktuelle Unzulänglichkeiten lediglich vorübergehend auszubessern.

Die für die Herbstkonferenz 2009 der Justizministerinnen und Justizminister der Länder ursprünglich auf der Agenda stehende Frage der Einführung eines gesetzlich vorgeschriebenen Compliance-Systems wurde kurzfristig wieder von der Tagesordnung gestrichen.[401] Zu groß scheinen derzeit die Widersprüche zwischen den Anforderungen an eine effektive Compliance-Organisation und den Belangen des Datenschutzrechts. Jedoch widersprechen sich die Aufgaben des Datenschutzes und der Compliance nicht.[402] Vielmehr ist wesentlicher Bestandteil einer guten Compliance-Organisation, dass Rechte anderer beachtet werden und die Strukturen eines Unternehmens so geordnet werden, dass es nicht zu rechtswidrigen Eingriffen in die Rechte Dritter kommt. Zu diesen Rechten gehört

[399] BT-Drs. 17/69, S. 2.
[400] Einen immateriellen Entschädigungsanspruch von Arbeitnehmern wegen Persönlichkeitsrechtsverletzungen fordert auch *Oberwetter*, NZA 2009, 1120.
[401] FAZ v. 11.11.2009, S. 23.
[402] So i.E. auch *Uwe H. Schneider*, NZG 2009, 1321, 1326.

auch das informationelle Selbstbestimmungsrecht der Arbeitnehmer, einfachgesetzlich bisher im BDSG geschützt. Damit ist der Datenschutz Bestandteil der Compliance. Das Datenschutzrecht stellt eine Schranke für die Compliance-Pflichten dar.