

**Ausgabe 6
März 2009**



FACHHOCHSCHULE DÜSSELDORF
UNIVERSITY OF APPLIED SCIENCES DÜSSELDORF

Forschungsberichte

des Fachbereichs Wirtschaft der Fachhochschule Düsseldorf

Felicitas G. Albers

Compliance der Compliance: Elektronische Analyseverfahren
personenbezogener Daten zur Prävention und Aufdeckung
geschäftsschädigender Handlungen in Unternehmen

Diskurs aus Anlass des sogenannten ‚Datenskandals‘ der Deutsche
Bahn AG



Compliance der Compliance:

Elektronische Analyseverfahren personenbezogener Daten zur Prävention und Aufdeckung geschäftsschädigender Handlungen in Unternehmen

Diskurs aus Anlass des sogenannten ‚Datenskandals‘ der Deutsche Bahn AG

Felicitas G. Albers

Fachbereich Wirtschaft
Fachhochschule Düsseldorf¹
Universitätsstraße Geb. 23.32
40225 Düsseldorf
felicitas.albers@fh-duesseldorf.de

Abstract: Im Rahmen einer umfassenden betrieblichen "Compliance", also der Gewährleistung einer gesetzestreu und regelkonformen, ordnungsgemäßen Unternehmensführung, ist durch geeignete Kontrollen sicher zu stellen, dass Gesetzesverstöße und regelwidriges Verhalten im Unternehmen sowie aus ihnen resultierende Schäden vermieden werden. Dabei kommen IT-gestützte Verfahren zum Einsatz, die ihrerseits den Anforderungen der Compliance, insbesondere hinsichtlich Datenschutz- und Mitbestimmungsrecht, genügen müssen. Die Abhandlung versteht sich als Diskussionsbeitrag im Zusammenhang mit dem sogenannten "Datenskandal" der Deutsche Bahn AG 2009 und seiner Erörterung in der deutschen Öffentlichkeit.

1. Sachverhalt: Umfassender Abgleich von Mitarbeiterdaten im Rahmen der Korruptionsbekämpfung

1.1 Compliance als Aufgabe der Unternehmensführung

Im Rahmen einer umfassenden betrieblichen ‚**Compliance**‘, also der Gewährleistung einer gesetzestreu und regelkonformen, ordnungsgemäßen Unternehmensführung², ist durch geeignete Maßnahmen sicher zu stellen, dass Gesetzesverstöße und regelwidriges Verhalten im bzw. durch das Unternehmen sowie aus ihnen resultierende Schäden vermieden werden.

Im Folgenden liegt das besondere Augenmerk auf geschäftsschädigenden Handlungen, die strafbar sind bzw. als Ordnungswidrigkeiten gelten. Als für diese Fragen zuständige betriebliche Einheit kann der Stabsbereich ‚Interne Revision‘ gelten, der auch Ansprechpartner im Rahmen der Abschlussprüfung durch externe Wirtschaftsprüfer ist.³ Aufgaben der Internen Revision im Rahmen des betrieblichen Risikomanagements sind die Sicherstellung der

- ‚Zuverlässigkeit und Integrität von Daten des Rechnungswesens und anderen betrieblichen Informationen,
- Effektivität und Effizienz von Geschäftsprozessen,

¹ Prof. Dr. rer.pol. Felicitas G. Albers vertritt das Lehrgebiet Betriebswirtschaftslehre, insbes. Organisation und Datenverarbeitung. Die Verfasserin dankt Prof. Dr. Heidemarie Hofmeister, Prof. Dr. Dirk Kalmring und Prof. Dr. Peter J. Lipperheide für den kollegialen Gedankenaustausch zum behandelten Thema.

² Der Deutsche Corporate Governance Kodex definiert ‚Compliance‘ als ‚Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien‘; DCGK 2008, 4.1.3

³ vgl.: Lück/Henke 2004, Sp. 1278 ff.; Bäcker 2002; IIR 1

- Sicherung des Betriebsvermögens,
- Einhaltung von Gesetzen, Verordnungen und Verträgen.⁴

Desweiteren verdienen auch Abweichungen von unternehmensinternen Leitlinien und Grundsätzen erörtert zu werden, z.B. bezüglich der Kommunikationskultur eines Unternehmens und der Transparenz gegenüber Leitungsorganen und Gremien, die, wenn auch nicht illegal, den Grundsätzen einer guten **Corporate Governance** widersprechen, was in der vorliegenden Untersuchung aber nicht erfolgt.⁵

Bei der Bekämpfung illegalen Verhaltens im Unternehmen steht das **Fehlverhalten von Unternehmensangehörigen aller Hierarchiestufen einschließlich der Geschäftsleitung** im Vordergrund.

Ausweislich einer Studie⁶ der Wirtschaftsprüfungsgesellschaft KPMG Deutsche Treuhand – Gesellschaft AG zur betrügerischen Geschäftsschädigung (,fraud‘)

- handelte es sich in 89 % der untersuchten Fälle um Mitarbeiter des geschädigten Unternehmens,
- waren 60 % der Täter Mitglieder des oberen Managements,
- waren 26 % der Täter Mitglieder des mittleren Managements,
- arbeiteten die internen Täter zumeist in der Finanzabteilung einschließlich Controlling und Rechnungswesen sowie im Vertriebsbereich,
- waren auch die Vorsitzenden der Unternehmensleitungen in Teilen betroffen.

Ein Segment der auch als ‚**dolose Handlungen**‘ bezeichneten Geschäftsschädigungen bildet die **Korruption**, definiert ‚*als Missbrauch eines öffentlichen Amtes, einer Funktion in der Wirtschaft oder eines politischen Mandats, begangen auf Veranlassung oder aus eigener Initiative zur Erlangung eines Vorteils für sich oder einen Dritten mit Eintritt oder in Erwartung des Eintritts eines Schadens oder Nachteils für die Allgemeinheit (...) oder für ein Unternehmen (...)*.‘⁷ Klassische Korruptionsdelikte sind Bestechung und Bestechlichkeit sowie Vorteilsgewährung und Vorteilsnahme. Es handelt sich dabei sowohl um Straftatbestände⁸ als auch um die Missachtung eines der Prinzipien des von den Vereinten Nationen begründeten **Global Compact**⁹ zur weltweiten Förderung des gesellschaftlichen Engagements von Unternehmen.

Selbstverständlich gelten die zuvor getroffenen Überlegungen zur Compliance gleichermaßen für die allgemeine Geschäftstätigkeit eines Unternehmens wie auch –und hier liegt in der aktuellen Diskussion die Problematik– für die Maßnahmen, die zur Aufdeckung und Vermeidung geschäftsschädigenden Verhaltens getroffen werden. Der Zweck heiligt natürlich keineswegs die Mittel.

1.2 Verantwortung der Unternehmensleitung

Im Rahmen ihrer Verantwortung und zur Abwendung potentieller Schadenersatzansprüche gegen das Unternehmen oder Mitglieder seiner Führungsorgane ist die Unternehmensleitung gehalten, geeignete Kontroll- und Prüfungsmaßnahmen zur Sicherstellung einer ordnungsgemäßen Geschäftstätigkeit durchzuführen.

Entsprechend heißt es im Deutschen Corporate Governance Kodex: ‚*Vorstand und Aufsichtsrat beachten die Regeln ordnungsgemäßer Unternehmensführung. Verletzen sie die Sorgfalt eines*

⁴ IIA 2007, 2120.A1, S. 13

⁵ vgl. v. Werder 2004, Sp. 160 ff.; Schwarz 2005

⁶ KPMG 2007, S. 5

⁷ BMI 2004

⁸ § 299 StGB; §§ 331 – 335 StGB

⁹ Prinzip 10 des Global Compact lautet: ‚Unternehmen sollen gegen alle Arten der Korruption eintreten, einschließlich Erpressung und Bestechung.‘ GC 2005

ordentlichen und gewissenhaften Geschäftsleiters bzw. Aufsichtsratsmitglieds schuldhaft, so haften sie der Gesellschaft gegenüber auf Schadensersatz. Bei unternehmerischen Entscheidungen liegt keine Pflichtverletzung vor, wenn das Mitglied von Vorstand oder Aufsichtsrat vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln (Business Judgement Rule).¹⁰

1.2.1 Haftung bei Organisationsverschulden im Allgemeinen

Vorbeugung, geschäftsprozessbegleitende Kontrolle und Revision abgeschlossener Geschäftsprozesse mit dem Ziel der Eindämmung geschäftsschädigenden Verhaltens gehören im Rahmen des **Organisationsverschuldens**¹¹ zu den haftungsrelevanten Verantwortlichkeiten der Unternehmensleitung.¹² Im Falle der nachzuweisenden schuldhaften Verletzung ihrer Organisationspflicht sind Schadenersatzansprüche des geschädigten Unternehmens gegen die Mitglieder der Unternehmensleitung, Leitende Angestellte und ggf. auch Mitarbeiter in Betracht zu ziehen.

1.2.2 Haftung von Vorstand, Aufsichtsrat und Abschlussprüfer bei Aktiengesellschaften¹³

Im Rahmen seiner autonomen Leitungskompetenz¹⁴ obliegt es dem **Vorstand** einer Aktiengesellschaft ,geeignete Maßnahmen zu treffen, insbesondere ein **Überwachungssystem** einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden‘.¹⁵ Dies schließt die Verhinderung bzw. Aufdeckung geschäftsschädigender Handlungen ein. Werden solche Maßnahmen schuldhaft nicht getroffen, sind die Vorstandsmitglieder dem Unternehmen in der Regel als Gesamtschuldner zum Schadensersatz verpflichtet¹⁶. Zur Implementierung von Überwachungssystemen gehört ,nach einer starken Meinung im juristischen Schrifttum‘ auch ,das Ergreifen entsprechender IT-Sicherheitsmaßnahmen‘.¹⁷ Das Überwachungssystem ist Gegenstand der Regelberichterstattung des Vorstandes gegenüber dem Aufsichtsrat.¹⁸ Sollten Mängel des Überwachungssystems offenbar oder geschäftsschädigende Handlungen erheblichen Ausmaßes entdeckt werden, hat der Vorstand durch eine Sofortmeldung¹⁹ den Aufsichtsrat zu unterrichten.

Dem **Aufsichtsrat** obliegt die Überwachung des Vorstandes.²⁰ Im hier diskutierten Sachverhalt beinhaltet dies die Frage, ob der Vorstand funktionsfähige und hinreichende Sicherheits- und Kontrollvorgänge, d. h. ein geeignetes Überwachungssystem eingerichtet hat²¹.

Der **Abschlussprüfer** börsennotierter Aktiengesellschaften hat im Rahmen seiner Prüfungstätigkeit zu beurteilen, ,ob der Vorstand die ihm obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann‘.²² Dabei hat er

¹⁰ DCGK 2008, Ziff. 3.8

¹¹ Das Organisationsverschulden umfasst das Auswahl-, Anordnungs- und Überwachungsverschulden im Rahmen der Verkehrssicherungspflicht der Unternehmensleitung. Vgl. Palandt/Sprau 2009, § 823 RdNr. 50

¹² §§823 i.v.m. 831 BGB

¹³ ,In das GmbHG ist keine entsprechende Regelung aufgenommen worden. Der Gesetzgeber geht davon aus, dass für GmbH's je nach ihrer Größe, Komplexität, ihrer Struktur usw. nichts anderes gilt und dass die Neuregelung des § 91 Abs. 2 AktG Ausstrahlungswirkung auf den Pflichtenrahmen der Geschäftsführer auch anderer Gesellschaftsformen hat‘. Lück 1998, S. 1925 ff.; vgl. auch KPMG 2004, S.9

¹⁴ § 76 Abs. 1 AktG

¹⁵ § 91 Abs. 2 AktG

¹⁶ § 93 Abs. 2 und 3 AktG

¹⁷ Becker/Hoeren 2007, S. 100; Batou 2004, S. 305 f.

¹⁸ § 90 AktG

¹⁹ § 90 Abs. 1 Satz 3 AktG

²⁰ § 111 Abs. 1 AktG

²¹ Lück 1998, S. 1925 ff.

²² § 317 Abs. 4 HGB; vgl. auch Prüfungsstandard IDW PS 210, S. 1422 ff., sowie den, für an der US-amerikanischen Börse gelistete Unternehmen einschlägigen, Sarbanes-Oxley-Act SOX 2002

über die im Rahmen der gebotenen ‚kritischen Grundhaltung‘²³ und die ‚berufsübliche Skepsis‘ hinaus im Verdachtsfall im Rahmen von Unterschlagungsprüfungen ‚besonderes Misstrauen‘ an den Tag zu legen.²⁴

1.3 Potentielle Tätergruppen regelwidrigen Verhaltens

Grundsätzlich kommen als Tätergruppen bei Wirtschaftsstraftaten zulasten von Unternehmen unternehmensexterne oder –interne Personen in Betracht. Zu den externen gehören insbesondere Lieferanten, Kunden und Wettbewerber.

In den Fällen, die eine Mitwirkung von Unternehmensangehörigen erfordern, bieten die Mitglieder der Geschäftsleitung, die sonstigen Führungskräfte sowie die Mitarbeiter Ermittlungsansätze und ggf. Anhaltspunkte für entsprechende Verstöße. Dass dabei auch Arbeitnehmervertreter in Erscheinung treten können, zeigen die Fälle der Volkswagen AG²⁵ und der Siemens AG.²⁶

Das Profil potentieller Täter gilt für Unternehmen wie für Behörden gleichermaßen. Die Bundesregierung gibt in der Richtlinie zur Korruptionsprävention in der Bundesverwaltung²⁷ Hinweise zum ‚Aufspüren von Korruptionssignalen im Rahmen der Dienst- und Fachaufsicht‘ und nennt folgende, die Bediensteten betreffenden ‚neutrale Indikatoren‘ als ‚Anzeichen für Korruption‘ und ‚Warnsignale‘:

- *‚auffallender und unerklärlich hoher Lebensstandard; aufwändiger Lebensstil; Vorzeigen von Statussymbolen;*
- *auffällige private Kontakte zwischen Beschäftigten und Dritten (z. B. Einladungen, Nebentätigkeiten, Berater- oder Gutachterverträge, Kapitalbeteiligungen); (...)*
- *Ausübung von Nebentätigkeiten ohne entsprechende Genehmigung bzw. Anzeige; (...)*
- *Inanspruchnahme von Vergünstigungen Dritter (Sonderkonditionen beim Einkauf, Freihalten in Restaurants, Einladungen zu privaten oder geschäftlichen Veranstaltungen von „Verwaltungskunden“);*
- *auffallende Großzügigkeit von Unternehmen (z. B. Sponsoring).‘*

Der Prüfungsstandard IDW PS 210 nennt bezüglich der durch den Abschlussprüfer vorzunehmenden Risikobeurteilung u.a. als ‚eine Motivation für eine Unterschlagung‘, dass ‚eine Person wesentlich über ihre Verhältnisse lebt‘.²⁸ ‚Geschäfte mit nahestehenden Personen‘ können Indizien für ein erhöhtes Missbrauchsrisiko sein.²⁹

Die Identifikation solcher oder ähnlicher, Geschäftsleitung, Führungskräfte und Mitarbeiter betreffende Frühwarnindikatoren findet sich in der internationalen Fachliteratur gleichermaßen und basiert offenkundig auf Erfahrungswissen aus der einschlägigen Deliktforschung.³⁰

²³ IDW PS 210, Tz. 14, S. 1425

²⁴ IDW PS 210, Tz. 15, S. 1425 und die dort angegebenen Literatur; vgl. hinsichtlich der Vorgehensweise zur Berücksichtigung von Verstößen IWP 2006, S. 1976 ff.

²⁵ vgl. z.B.: Grill/Schneyink 2005

²⁶ vgl. z.B. den sog. ‚Siemens-Skandal‘ STERN 24. November 2008

²⁷ RLK 2004, Anlage 2 Leitfaden für Vorgesetzte und Behördenleitungen, II, 1.1

²⁸ IDW PS 210, Tz. 24, S. 1426

²⁹ IDW PS 210, Tz. 35 u. 37, S. 1428

³⁰ vgl. z.B. Wells 2001, S. 4; ACFE 2008; PWC AG 29. Januar 2009

1.4 Der Fall der Deutschen Bahn AG als Ausgangspunkt der aktuellen öffentlichen Debatte über IT-gestützte Maßnahmen der Compliance

Die nachfolgend chronologisch genannten Vorgänge im Rahmen des sog. ‚Datenskandals‘ der Deutsche Bahn AG geben aktuellen Anlass zur Erörterung der Notwendigkeit und der IT-gestützten Möglichkeiten des Erkennens und Vermeidens geschäftsschädigender Handlungen.

Zur Erkennung geeigneter Indikatoren z.B. von Korruptionsvorgängen, auch als Bestandteil sog. Frühwarnsysteme bzw. interner Kontrollsysteme (IKS) im Rahmen des Risikomanagements, setzt die Wirtschaftspraxis automatisierte Verfahren der Informationsverarbeitung mit dem Ziel ein, rechtswidriges Verhalten beteiligter Marktpartner zu erkennen, zu vermeiden bzw. aufzuklären.³¹

Aktuell wird dies anhand des nachfolgend skizzierten Falles der Deutsche Bahn AG in der deutschen Öffentlichkeit diskutiert. Die Sensibilisierung im Hinblick auf diesen ‚Datenskandal‘ ist angesichts vorgelagerter Fälle bei der Lidl Dienstleistung GmbH & Co. KG³² und der Telekom AG³³ besonders hoch, gleichwohl die dort dabei im Vordergrund stehenden Maßnahmen der versteckten Videoüberwachung und detektivischen Mitarbeiterbeobachtung im Falle Lidl sowie der Telefonüberwachung im Falle der Telekom völlig andere Sachverhalte darstellen als ein IT-gestützter Datenabgleich, wie er –neben anderen hier nicht weiter erörterten Maßnahmen– im Falle des nachfolgend chronologisch rekapitulierten sog. ‚Datenskandals‘ der Deutsche Bahn AG in der öffentlichen Berichterstattung zu beobachten gewesen ist. Der Medientenor sei hier exemplarisch anhand einiger Schlagzeilen wiedergegeben:

- *‚Bahn-Spitzelskandal. Mitarbeiter unter Generalverdacht‘³⁴*
- *‚173.000 Mitarbeiter in der Spitzel-Falle‘³⁵*
- *‚Massenbespitzelung der Mitarbeiter. Rasterfahndung bei der Bahn‘³⁶*
- *‚Spitzelaffäre "Babylon": Bahn überprüfte heimlich 173. 000 Mitarbeiter‘³⁷*
- *‚Deutsche Bahn: Spitzel-Affäre‘³⁸*
- *‚Der Datenskandal wird für Bahn-Chef Mehdorn zum Showdown‘³⁹*

Festzustellen ist, dass die Berichterstattung der Medien zu diesem Fall nahezu ausschließlich die mitbestimmungsrechtliche und datenschutzrechtliche Dimension der betroffenen Mitarbeiter einschließlich ggf. betroffener Ehepartner zum Gegenstand hat. Gleichmaßen ist natürlich die datenschutzrechtliche Würdigung der möglicherweise betroffenen Lieferanten angezeigt.

20.01.2009 Im Vorgriff auf einen am 22.1.2009 erscheinenden Bericht im Wochenmagazin ‚STERN‘ verweist die Deutsche Bahn AG auf ihr berechtigtes Interesse zur Bekämpfung von Wirtschaftskriminalität. *‚Bei den Ermittlungen durch die DB ging es beispielsweise darum, ob Top- Führungskräfte und deren Ehepartner Beteiligungen an Firmen halten oder Nebentätigkeiten ausüben, die nicht der DB offen gelegt wurden.‘⁴⁰*

³¹ Zur Prüfung des Risikomanagement durch die Interne Revision siehe IIR 2

³² vgl. o.V. STERN 2009

³³ vgl. o.V. SPIEGEL 2008

³⁴ Röhrig 2009

³⁵ o.V. Süddeutsche 2009

³⁶ Rother 2009

³⁷ o.V. Handelsblatt 2009

³⁸ o.V. WELT 2009

³⁹ Böhmer 2009

⁴⁰ DB AG 20. Januar 2009

21.01.2009 Vorabbericht stern.de: ‚Daten-Skandal. Bahn bespitzelt eigene Mitarbeiter‘⁴¹

‚Im Kampf gegen Korruption‘ habe die Deutsche Bahn durch ihre Konzernrevision die Detektei Network Deutschland GmbH beauftragt, ‚mehr als 1000 Mitarbeiter‘, darunter ‚ein Großteil des oberen Managements‘ und deren Ehepartner ‚ausforschen‘ zu lassen. Im Einzelnen wirft der Bericht des Wochenmagazins ‚STERN‘ der Deutsche Bahn AG vor:

- **2002:** Projekt ‚Babylon‘ zur Prüfung, inwieweit Verbindungen zwischen Mitarbeitern und Lieferanten bestünden mittels ‚Rasterfahndung‘ zum Datenabgleich von Adress-, Bankdaten und Telefonnummern
- **2003:** Projekt ‚Eichhörnchen‘ zur Prüfung, inwiefern Top-Manager oder deren Ehepartner außerhalb der Deutsche Bahn AG ‚wirtschaftlich engagiert‘ seien. Die fraglichen Daten seien der Detektei per CD zur Verfügung gestellt worden.

28.01.2009 DB-Stellungnahme zur Sitzung des Verkehrsausschusses des deutschen Bundestages

- ‚DB-Mitarbeiter haben im Kampf gegen Wirtschaftskriminalität keine strafrechtlich relevanten Taten begangen.
- Entgegen vielfacher Behauptung ist der Abgleich von Mitarbeiter- und Lieferantendaten – das sogenannte Screening – rechtlich nicht zu beanstanden – unabhängig von der Zahl der überprüften Mitarbeiter. Der Berliner Datenschutzbeauftragte bejaht grundsätzlich die Vorgehensweise des Screening im Rahmen der Korruptionsbekämpfung.
- Ein solches Verfahren ist der DB von ihrer Wirtschaftsprüfungsgesellschaft empfohlen worden.
- Zwischen dem Berliner Datenschutzbeauftragten und der DB ist unverändert umstritten, ob es aufgrund der fehlenden Benachrichtigung der Mitarbeiter in diesem Zusammenhang zu einer reinen Ordnungswidrigkeit gekommen ist.⁴²

06.02.2009 Erklärung des Vorstandsvorsitzenden der DB AG im Konzernbetriebsrat

‚Der Vorstand der DB AG bedauert, dass es in der Vergangenheit bei den Mitarbeiterüberprüfungen zu Verstößen gekommen ist und kein Gremium der Arbeitnehmerinteressenvertretung informiert war. Er entschuldigt sich dafür bei seinen Mitarbeitern.‘⁴³

10.02.2009 Zwischenbericht der Deutsche Bahn AG⁴⁴

Die Deutsche Bahn AG bestätigt den Abgleich von Mitarbeiter- und Lieferantendaten in den Jahren 1998, 2002/03 und 2005/06.

‚Die maschinelle Datenanalyse bezog sich stets auf drei Merkmale:

- Gleicher **Name**
- Gleiche **Adresse**
- Gleiche **Bankverbindung** (Bankleitzahl und Kontonummer)

Grundlage waren die **Personalstammdaten** und die **Kreditorenstammdaten** (Lieferanten). Andere Merkmale wurden nicht abgeglichen.⁴⁵

Die Deutsche Bahn AG räumt folgende Fehler bei der Durchführung von Compliance Maßnahmen ein:

- ‚Beim maschinellen **Screening** wurde eine unangemessen hohe Zahl von Mitarbeitern einbezogen; der Grundsatz der Verhältnismäßigkeit war nicht gewahrt.

⁴¹ Gatzke/Güßgen/Röhrig 2009

⁴² DB AG 28.Januar 2009

⁴³ DB AG 6.Februar 2009

⁴⁴ DB AG 12.Februar 2009

⁴⁵ DB AG 12.Februar 2009, S. 16

- Außerdem fehlte die notwendige **Einbindung** des betrieblichen Datenschutzbeauftragten und der Arbeitnehmervertreter; die Mitarbeiter wurden nicht informiert.
- Bei den **Ermittlungen** zur Aufklärung von Verdachtsfällen können wir nicht ausschließen, dass beauftragte externe Dienstleister beim Einholen von Informationen - teilweise mit Kenntnis und Billigung von Mitarbeitern der DB AG - gegen Gesetze verstoßen haben.⁴⁶

In Anlage 1 dieses Zwischenberichtes befindet sich ein Geschäftsschreiben, in dem die Wirtschaftsprüfungsgesellschaft Pricewaterhouse Coopers AG auf den International Standard on Auditing 240 (ISA 240) zur Verantwortung des Abschlussprüfers bei Verstößen hinweist, der in seiner Anlage 2 als Reaktionsmöglichkeiten auf ‚mögliche falsche Angaben im Jahresabschluss aufgrund von Vermögensschädigungen‘ nennt:⁴⁷

- ‚IT-gestützter Abgleich der Liste der Verkäufer mit einer Liste der Mitarbeiter zur Identifikation von Übereinstimmungen von Adressen oder Telefonnummern
- IT-gestützte Durchsuchung der Aufzeichnung für die Lohnbuchhaltung zur Identifikation doppelter Adressen, Personal- und Steuernummern sowie Bankkonten.

*Der Abgleich von Mitarbeiterstammdaten und Lieferantenstammdaten kann grobe Fälle im Einkaufsbereich leicht aufdecken. Diese Fälle wären anderweitig nur schwer zu entdecken. Die Methode ist schnell und vergleichsweise kostengünstig. Alle benötigten Daten liegen im Unternehmen vor. In Abhängigkeit von der Risikobeurteilung kann es deshalb sinnvoll sein, diesen Datenabgleich unter Beachtung gesetzlicher Regelungen durchzuführen.*⁴⁸

16.02.2009 Gespräch über den Arbeitnehmerdatenschutz unter Leitung des Bundesinnenministers

*Das Bundesdatenschutzgesetz trifft zwar allgemeine Regelungen auch zum Schutz von Daten im Arbeitsverhältnis. Diese werden aber teilweise als nicht ausreichend erachtet. Deshalb ist ein Gedankenaustausch wichtig, ob und in welchen Bereichen weiterer Handlungsbedarf zum Schutz der Daten von Arbeitnehmern besteht und welche konkreten Umsetzungsmöglichkeiten, gegebenenfalls im Bundesdatenschutzgesetz, in Betracht kommen.*⁴⁹

Zusammenfassend lässt sich also feststellen, dass die Deutsche Bahn AG in ihrem Zwischenbericht Fehler bei der Durchführung von Compliance Maßnahmen einräumt. Gleichwohl ist der ursprüngliche Zweck dieser Maßnahmen im Sinne der Compliance notwendiger Weise zu verfolgen. Es stellt sich somit die Frage nach geeigneten Verfahren, die grundsätzlich diesen Zweck mit rechtmäßigen und - auch im Hinblick auf einen im politischen Raum diskutierten umfassenden Arbeitnehmerdatenschutz-legitimen Mitteln erreichen lassen.⁵⁰

⁴⁶ DB AG 12.Februar 2009, S. 13

⁴⁷ ISA 240, Anlage 2, S. 53: 'The Auditors responsibility to consider fraud in an audit of financial statements'

⁴⁸ DB AG 12.Februar 2009, Anlage 1, S. 2/2

⁴⁹ BIM 11.Februar 2009

⁵⁰ Dass dieser Fall auch aus berufsständischer Sicht der Internen Revision Anlass zu Überlegungen gibt, zeigt die Stellungnahme, die das Deutsche Institut für Interne Revision e.V. auf seiner Homepage ‚aus aktuellem Anlass‘ formuliert: ‚Das DIIR beobachtet aufmerksam die aktuelle Medienberichterstattung über die Deutsche Bahn AG zum Thema Datenerhebung und -analyse. Eine Berichterstattung im Sinne eines Generalverdachts, der sich gegen den gesamten Berufsstand der Internen Revision richten würde, lässt sich nach Auffassung des DIIR derzeit nicht erkennen. Das DIIR wird Aussagen zum Thema Datenerhebung und -analyse weiterhin kritisch verfolgen.‘ DIIR 2009

2. Elektronische Recherche- und Analyseverfahren

Im Rahmen sog. betrieblicher ‚**business intelligence**‘ Anwendungen sind in der Betriebswirtschaftslehre und Wirtschaftsinformatik automatisierte Verfahren geläufig, die das Recherche- und Analysepotential betrieblicher Datenbestände z.T. unter Anwendung mathematisch-statistischer Verfahren auszuschöpfen suchen, um so unternehmerische Entscheidungen durch geeignete Führungsinformationen zu unterstützen.⁵¹ Bei den betrieblichen Datenbeständen handelt es sich um Geschäftsdaten, die im Rahmen kaufmännischer IT-Anwendungen (z.B. sog. Enterprise-Resource-Planning Systeme; ERP-Systeme⁵²) benötigt bzw. generiert werden. Dazu zählen auch kunden-, lieferanten- und mitarbeiterbezogene Daten. Denkbar ist auch die Einbeziehung öffentlich zugänglicher Informationsquellen wie z.B. elektronischer Telefonbücher oder anderer Verzeichnisse.

Unter die elektronischen Recherche- und Analyseverfahren fallen sowohl turnusmäßige Auswertungen als auch ad-hoc Analysen z.B. auch durch Einsatz von Abfragesprachen bei relationalen Datenbanken. Solche Verfahren sind in unterschiedlichen betrieblichen Aufgabenfeldern einsetzbar:

- im **Marketing**, zur Identifikation von Kundenprofilen und zum Ausbau der Kundenbindung,
- im **Controlling**, zur Durchführung von Soll-/Ist-Abweichungsanalysen und zur Identifikation von Ertragssteigerungs- und Kostensenkungspotentialen,
- in der internen und externen **Prüfung** zur Gewährleistung der Ordnungsmäßigkeit betrieblicher Geschäftstätigkeit. So nennt der Standard ISA 240 als ein Beispiel einer Prüfungsprozedur ‚performing computer-assisted techniques, such as datamining⁵³ to test for anomalies in a population‘⁵⁴.

Auch die **Finanzverwaltungen** nutzen im Rahmen der digitalen Betriebsprüfung die Unternehmens-IT entsprechend der Abgabenordnung⁵⁵ und den ‚Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen‘ (GDPdU)⁵⁶.

In der Wirtschaftsinformatik sind ‚programmierte Kontrollen‘ als **organisatorische IT-Sicherheitsmaßnahmen** geläufig. Im Sinne eines **Validierungsverfahrens** werden im Rahmen einer Ausschlussprüfung als unzulässig definierte Sachverhalte (z.B. Identität von Kontonummern eines Mitarbeiters und der Kontonummer eines Lieferanten) identifiziert.⁵⁷ Im hier insbesondere diskutierten Fall des Abgleiches von Mitarbeiterdaten zur Vermeidung und Aufklärung betrügerischer Geschäftsschädigung durch Mitglieder von Geschäftsleitung, Management oder Mitarbeitern sind in der Wirtschaftspraxis vielfältige **elektronische Werkzeuge** im Einsatz.

Exemplarisch und einer heuristischen Recherche im Internet entnommen, sei hier auf das **Dienstleistungs- und Produktangebot** der Audicon GmbH⁵⁸ hingewiesen.

‚Die Audicon Information Suite (...) verbindet umfassende Auswertungsmöglichkeiten mit den Vorteilen einer relationalen Datenbank. Damit sind Sie in der Lage sowohl ad hoc als auch kontinuierlich selbst größte Datenmengen innerhalb kürzester Zeit flächendeckend zu analysieren – und das unabhängig von den Quellsystemen. Durch die kontinuierliche, automatisierte Überwachung Ihrer Unternehmensdaten wird die Hemmschwelle der potenziellen Täter erhöht und somit das Risiko der

⁵¹ vgl. zu solchen Management-intendierten, datenbankbasierten Anwendungen Albers/Rüschbaum 2002, S. 114 ff.

⁵² ERP-Systeme sind Standardanwendungssoftwarelösungen, die betrieblichen Funktionsbereiche unterstützen, wie z.B. das Rechnungswesen, das Controlling, den Vertrieb, das Personalwesen, die Produktion. Vgl. z.B. Albers/Rüschbaum 2002, S. 108 ff.

⁵³ Data mining ist ein IT-gestütztes Analyseverfahren, das unter Anwendung mathematisch-statistischer Verfahren zunächst unbekannte Beziehungsmuster, Regelmäßigkeiten, Auffälligkeiten in den zugrunde liegenden Datenbeständen feststellt und abbildet. Vgl. Albers/Rüschbaum 2002, S. 119

⁵⁴ ISA 240, Anlage 2, S. 50

⁵⁵ §§ 146, 147 AO

⁵⁶ GDPdU 2001

⁵⁷ vgl. Stahlknecht/Hasenkamp 2005, S. 484 f.

⁵⁸ Audicon 2009a

Wirtschaftskriminalität gesenkt. (...) Dezentral gehaltene **Datenmengen** können innerhalb kürzester Zeit zusammengeführt, **abgeglichen** und **Gemeinsamkeiten** und **Auffälligkeiten** festgestellt werden.

*IDEA ist die ideale Unterstützung für die einfache und **flexible Massendatenanalyse** und überprüft Ihre Daten zu 100%. Auffälligkeiten sind sofort erkennbar, für Detailanalysen und die Weiterverarbeitung der Daten stehen Ihnen umfangreiche Funktionen zur Verfügung. Typische Prüfungshandlungen sind z. B. die Ermittlung von gleichen Bankverbindungen zwischen Kreditoren- und Personalstammdaten, die Ermittlung von Unterschlagungen im Zahlungsverkehr oder Änderungen von Bankverbindungen. Außerdem können mit IDEA Finanzdaten (Zusammenarbeit Mitarbeiter – Kunde/Lieferant), Telefondaten (Anruferverhalten) und Logfiles (PC) ausgewertet werden.*⁵⁹

Unter dem Schlagwort ‚**digital analysis**‘⁶⁰ werden IT-gestützte Verfahren verstanden, die unter Anwendung mathematisch-statistischer Methoden Konsistenz- und Plausibilitätsprüfungen von elektronisch gespeicherten Daten durchführen. Ein in der betriebswirtschaftlichen Forensik (‚forensic accounting‘) angewandtes Prinzip ist das nach Frank Benford benannte Gesetz⁶¹ über die Verteilung führender Ziffern in Datenbeständen.⁶²

2.1 Datenschutzrechtliche Relevanz

Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze der Bundesrepublik Deutschland kodifizieren das nach dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983⁶³ definierte Recht auf informationelle Selbstbestimmung als ‚Befugnis, über die Preisgabe und Verwendung der eigenen persönlichen Daten zu bestimmen‘.⁶⁴ Nachfolgend wird die datenschutzrechtliche Relevanz elektronischer Recherche- und Analyseverfahren, wie sie zur Vorbeugung und Aufklärung illegaler Handlungen von Mitgliedern der Geschäftsleitungen, Managern und Mitarbeitern Anwendung finden, erörtert.⁶⁵

2.1.1 Personenbezogene Daten

Sind **personenbezogene Daten**, also ‚Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener)‘⁶⁶ Gegenstand elektronischer Recherche- und Analyseverfahren, so ist deren Erhebung, Speicherung, Verarbeitung oder Übermittlung grundsätzlich nicht zulässig.

Es liegt in der Natur elektronischer Recherche- und Analyseverfahren, dass sie bei Verarbeitung personenbezogener Daten als Verfahrensergebnis neue personenbezogene Daten generieren, deren Speicherung, Verarbeitung und Übermittlung wiederum grundsätzlich nicht zulässig ist.

⁵⁹ Audicon 2009b

⁶⁰ vgl.: Ettredge/Srivastava 1998

⁶¹ Diekmann 2004 und die dort zitierte Literatur: Benford 1938, S. 551f.; Berton 1995; Carslow 1988, S. 321ff.; Drake/Nigrini 2000, S. 127ff.

⁶² vgl. z.B.: Bhattacharya/Kumar 2008, S. 150 ff.

⁶³ NJW 1984, S. 419 ff.; vgl. Geis/Helfrich 2007, S. XI f.

⁶⁴ Geis/Helfrich 2007, S. XI f. und die dort angegebenen Literatur; das am 27. Februar 2008 verkündete Urteil des BVerfG zur Online-Durchsuchung definiert das ‚Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme‘. Es ist im hier erörterten Zusammenhang insofern nicht einschlägig, als dass es sich auf Fälle bezieht, in denen ‚der Betroffene das System als eigenes nutzt‘. BVerfG 2008, Ziff. 206, siehe Kommentar Hoeren 2008, S. 366

⁶⁵ vgl. grundlegend auch ‚Baustein Datenschutz‘ im IT-Grundschutz-Katalog BSI 2008

⁶⁶ § 3 Abs. 1 BDSG

Nur die Existenz substantiierter **Erlaubnistatbestände** ermöglicht die rechtmäßige Durchführung solcher Verfahren. Erlaubnistatbestände sind⁶⁷:

- **Einwilligung der Betroffenen**⁶⁸

Es ist gängige Praxis, im Rahmen von Vertragsverhältnissen durch sog. Datenschutzklauseln diese Zustimmung z.B. des Kunden für den Geltungsbereich des Kaufvertrages oder auch im Rahmen von Kundenkartenvereinbarungen insgesamt einzuholen.⁶⁹

- **Zweckbestimmung** eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses⁷⁰

- **Berechtigtes Interesse** der datenverarbeitenden Stelle⁷¹

Die Vermeidung und Aufklärung von Straftaten kommt als Beispiel für das berechtigte Interesse von Unternehmen in Betracht, diesem Zweck dienende Speicherung, Verarbeitung und Übertragung von Daten durchzuführen.

- **Gesetzliche Verpflichtung** bzw. Erlaubnis⁷²

Die Datenübertragungsverordnung (DÜV) bezüglich der Meldung von Mitarbeiterdaten an die Sozialversicherungsträger ist ein Beispiel für eine solche gesetzliche Verpflichtung von Unternehmen zur Übertragung personenbezogener Daten.

2.1.2. Anonymisierte und pseudonymisierte personenbezogene Daten

Die Verarbeitung **anonymisierter**⁷³ bzw. **pseudonymisierter**⁷⁴ **Daten** wird seitens des Gesetzgebers im Sinne der **Datenvermeidung und der Datensparsamkeit** ausdrücklich gefordert.⁷⁵ Damit ist der Datenabgleich nicht personalisierter Stammdaten unterschiedlicher Personenkreise (Mitarbeiter, Lieferanten, Kunden) zunächst datenschutzrechtlich grundsätzlich insofern ohne Belang, als dass die Betroffenen nicht bestimmt sind. Durch die Wiederherstellung des Personenbezugs und damit der Bestimmbarkeit der Betroffenen werden diese Daten zu personalisierten personenbezogenen Daten.

2.1.3 Daten juristischer Personen

Daten juristischer Personen, also z.B. Firmendaten von Lieferanten, sind datenschutzrechtlich nur indirekt insofern relevant, als dass sie unmittelbare Rückschlüsse auf personenbezogene Daten zulassen.⁷⁶

⁶⁷ vgl. Geis/Helfrich 2007, S. XXIII ff.

⁶⁸ § 4 Abs. 1 BDSG

⁶⁹ Handelt es sich dabei um eine für eine Vielzahl von Verträgen vorformulierte Klausel im Sinne Allgemeiner Geschäftsbedingungen ist auf deren Wirksamkeit gemäß §§ 305 ff. BGB zu achten.

⁷⁰ § 28 Abs. 1 S. 1 BDSG

⁷¹ § 28 Abs. 1 S. 2

⁷² § 4 Abs. 1 BDSG

⁷³ § 3 Abs. 6 BDSG

⁷⁴ § 3 Abs. 6a BDSG

⁷⁵ § 3a S. 2 BDSG

⁷⁶ § 3 Abs. 1 BDSG

2.1.4 Auslagerung der Verarbeitung personenbezogener Daten

Im Falle der Auslagerung der Datenverarbeitung personenbezogener Daten an ein anderes Unternehmen bzw. einen externen Mitarbeiter (z.B. Berater, Spezialisten, eine Detektei usw.) ist zu unterscheiden⁷⁷:

- **Auftragsdatenverarbeitung** gemäß § 11 BDSG erfolgt den Weisungen des Auftraggebers entsprechend.⁷⁸ Hier bleibt der Auftraggeber für die Einhaltung der Vorschriften des BDSG verantwortlich, der Auftragnehmer ist grundsätzlich nicht ‚Dritter‘.⁷⁹

Der Auftraggeber verantwortet die gebotene **Sorgfalt bei der Auswahl**⁸⁰ des Auftragnehmers im Hinblick auf dessen Eignung. Der **Auftrag ist schriftlich** und dezidiert zu erteilen.⁸¹ Der Auftragnehmer darf die personenbezogenen Daten **nur im Rahmen der Weisungen**⁸² verarbeiten.

- **Funktionsübertragung** an einen ‚Dritten‘⁸³ i.V.m. der im Sinne von Bekanntgeben⁸⁴ erfolgten Übermittlung personenbezogener Daten an einen Dienstleister. Er ist neben dem die Funktion Übertragenden weitere verantwortliche Stelle⁸⁵ und muss aus eigenem Recht einen Erlaubnistatbestand für die Verarbeitung personenbezogener Daten nachweisen.

Werden Maßnahmen im Rahmen der Compliance ausgelagert, ergibt sich insofern eine besondere Gefahrenlage im Hinblick auf die Auswahl des Auftragnehmers, als dass bei der Erfüllung dieses Auftrages potentiell auch kompromittierende personenbezogene Daten generiert werden. Die Möglichkeit des Auftragnehmers, diese unzulässig und ggf. auch kriminell zu verwenden, kann erhebliche Rechtsverstöße provozieren und intensiviert die Schützwürdigkeit personenbezogener Daten.⁸⁶

2.1.5 Rechte der Betroffenen

Die Rechte der von der Verarbeitung personenbezogener Daten Betroffenen umfassen:

- Benachrichtigung durch die verantwortliche Stelle bei erstmaliger Speicherung sowie Übermittlung⁸⁷
- Auskunft auf Verlangen des Betroffenen⁸⁸
- Berichtigung, Löschung und Sperrung von Daten⁸⁹.

Das BDSG schließt für Auskunft sowie für die Berichtigung, Löschung und Sperrung einen durch Rechtsgeschäft vereinbarten Verzicht der Betroffenen aus.⁹⁰

⁷⁷ Geis/Helfrich 2007, S. XXIX

⁷⁸ § 11 Abs. 3, S. 1 BDSG

⁷⁹ § 3 Abs. 8, S. 3 BDSG

⁸⁰ § 11 Abs. 2, S. 1 BDSG

⁸¹ § 11 Abs. 3, S. 1 BDSG

⁸² § 11 Abs. 2, S. 1 BDSG

⁸³ § 3 Abs. 8, S. 3 BDSG

⁸⁴ § 3 Abs. 4, S. 3 BDSG

⁸⁵ § 3 Abs. 7 BDSG

⁸⁶ Dies dürfte auch neben der datenschutzrechtlichen Anspruchsgrundlage im Rahmen der allgemeinen Fürsorgepflicht gegenüber den Mitarbeitern geboten sein.

⁸⁷ § 33 BDSG

⁸⁸ § 34 BDSG

⁸⁹ § 35 BDSG

⁹⁰ § 6 BDSG

2.1.6 Beteiligung des betrieblichen Beauftragten für den Datenschutz

Im Rahmen seiner Überwachungsaufgabe ist der betriebliche Beauftragte für den Datenschutz ‚rechtzeitig zu unterrichten‘ über ‚Vorhaben der automatisierten Verarbeitung personenbezogener Daten‘.⁹¹ Dabei ist das Vorhaben umfassend inhaltlich zu kennzeichnen im Hinblick auf die Zweckbestimmung, die betroffenen Personengruppen, die für die personenbezogene Verarbeitung verantwortliche Stelle und die verantwortlichen Personen.⁹²

2.2 Betriebsverfassungsrechtliche Relevanz bei der Verarbeitung von Mitarbeiterdaten

Auch unter dem Gesichtspunkt der im Betriebsverfassungsgesetz geregelten Mitbestimmung der Arbeitnehmervertretung sind elektronische Recherche- und Analyseverfahren, wie sie zur Vorbeugung und Aufklärung illegaler Handlungen von Mitgliedern der Geschäftsleitungen, Managern und Mitarbeitern Anwendung finden, auf ihre Rechtskonformität zu prüfen. Insbesondere relevant sind dabei die Bestimmungen hinsichtlich

- der Überwachungsaufgaben des Betriebsrates⁹³,
- des Rechtes des Betriebsrates auf rechtzeitige und umfassende Unterrichtung⁹⁴,
- der Mitbestimmungsrechte des Betriebsrates im Rahmen der Verhaltens- und Leistungskontrolle⁹⁵.

Die Überwachungsaufgaben des Betriebsrates beziehen sich auf die Durchführung der ‚zugunsten der Arbeitnehmer geltenden Gesetze (...)‘⁹⁶ und damit auch auf die im hier diskutierten Zusammenhang erörterten Bestimmungen der Datenschutzgesetze. Entsprechend ist der Betriebsrat ‚rechtzeitig und umfassend zu unterrichten‘. Zusätzlich hat der Betriebsrat grundsätzlich immer dann ein Mitbestimmungsrecht, wenn die zur Debatte stehenden elektronischen Recherche- und Analyseverfahren eine Verhaltens- und Leistungskontrolle von Arbeitnehmern ermöglichen.⁹⁷

2.3 Relevanz des DCGK⁹⁸ hinsichtlich Maßnahmen der Compliance

Da die hier diskutierten Recherche- und Analyseverfahren als Maßnahmen der Compliance zur Aufdeckung geschäftsschädigender Handlungen betrachtet werden, erweist sich der Deutsche Corporate Governance Kodex insofern als einschlägig, als dass er für das Zusammenwirken von Vorstand und Aufsichtsrat empfiehlt: ‚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.‘⁹⁹ Hieraus ergibt sich somit eine vom Aufsichtsrat näher festzulegende Informationspflicht des Vorstandes, wobei die Zeitnähe auch vor dem Hintergrund der Sicherstellung des Recherche- und Analyseziels zu bemessen sein wird.

⁹¹ § 4g Abs. 1, S. 4 BDSG

⁹² §§ 4e S. 1, 4g Abs. 2, S. 1 BDSG

⁹³ § 80 Abs. 1 Nr. 1 BetrVG

⁹⁴ § 80 Abs. 2 S. 1 BetrVG

⁹⁵ § 87 Abs. 1 Nr. 6 BetrVG

⁹⁶ § 80 Abs. 1 Nr. 1 BetrVG

⁹⁷ § 87 Abs. 1 Nr. 6 BetrVG

⁹⁸ Der von der Regierungskommission DCGK veröffentlichte Deutsche Corporate Governance Kodex ist insofern relevant, als dass Vorstand und Aufsichtsrat börsennotierter Aktiengesellschaften eine Entsprechungserklärung abzugeben und diese den Aktionären dauerhaft zugänglich zu machen haben. § 161 AktG; DCGK 2008

⁹⁹ DCGK 2008, Ziff. 3.4

2.4 Verhältnismäßigkeit

Der allgemeine Rechtsgrundsatz der Verhältnismäßigkeit gebietet eine angemessene Relation zwischen dem angestrebten Recherche- und Analyseergebnis und dem dazu betriebenen Aufwand sowie den dabei in Kauf genommenen Beeinträchtigungen.¹⁰⁰ ‚Der Grundsatz der Verhältnismäßigkeit verlangt‘, dass eine entsprechende Maßnahme

- ‚geeignet‘ (,der erstrebte Zweck wird gefördert‘),
- ‚erforderlich‘ (,kein anderes, gleich wirksames und das Persönlichkeitsrecht weniger einschränkendes Mittel‘ steht zur Verfügung) und
- ‚unter Berücksichtigung der gewährleisteten Freiheitsrechte **angemessen** ist, um den erstrebten Zweck zu erreichen‘ (,im engeren Sinne verhältnismäßig (...); es bedarf einer Gesamtabwägung der Intensität des Eingriffs und des Gewichtes der ihn rechtfertigenden Gründe‘ sind.¹⁰¹

3 Fiktive Fallgestaltung zur rechtskonformen Durchführung IT-gestützter Recherche- und Analyseverfahren

Die bisherigen Ausführungen haben den Zielkonflikt zwischen der unternehmerischen Kontroll- und Überwachungspflicht einerseits und den Rechten der Betroffenen aus Sicht des Datenschutzes und der Mitbestimmung andererseits aufgezeigt. Nunmehr soll der Versuch unternommen werden, in einigen Grundzügen darzulegen, wie beiden Intentionen in der Durchführung eines entsprechenden Praxisprojektes gleichermaßen Rechnung getragen und so das scheinbare Dilemma gelöst werden kann.

Im Rahmen ihrer Kontroll- und Überwachungspflicht ist es Aufgabe der Unternehmensleitung, Verfahren und Systeme zu implementieren, die u.a. geeignet sind, Verstöße gegen gesetzliche Regelungen und dolose Handlungen von Mitgliedern der Unternehmensleitung, des Managements sowie von Mitarbeitern zu verhindern und aufzudecken. Dazu wird die Unternehmensleitung i.d.R. die Interne Revision beauftragen. Im Rahmen seiner vom Aufsichtsrat näher geregelten Informationspflicht informiert der Vorstand den Aufsichtsrat über Maßnahmen der Compliance. IT-gestützte Verfahren zum Abgleich von Datenbeständen im Hinblick auf als relevant erkannte Merkmale und deren Ausprägungen ggf. unter Anwendung mathematisch-statistischer Methoden bieten eine wirkungsvolle und wirtschaftliche Möglichkeit zur Identifikation von Normabweichungen und von Anhaltspunkten verdächtiger Sachverhalte.

Phasen eines solchen Recherche- und Analyseverfahrens sind:

Phase 1: Festlegung des Recherche- und Analysezweckes

Phase 2: Identifikation geeigneter Indikatoren

Phase 3: Definition der abzugleichenden Datenbestände

Phase 4: Bereitstellung eines geeigneten Softwaretools bzw. Einsatz einer geeigneten Abfragesprache

Phase 5: Extraktion anonymisierter bzw. pseudonymisierter Daten aus den betrieblichen Datenbeständen

Phase 6: Durchführung des Datenabgleiches¹⁰²

¹⁰⁰ vgl. DB AG 12. Februar 2009, S. 13: ‚Beim maschinellen Screening wurde eine unangemessen hohe Zahl von Mitarbeitern einbezogen; der Grundsatz der Verhältnismäßigkeit war nicht gewahrt.‘

¹⁰¹ BAG 2008; Rz. 18 ff. und die dort angegebenen Entscheidungen.

Phase 7: ggf. Reduktion der Schnittmenge im Ausschlussverfahren durch Anwendung weiterer Indikatoren

Phase 8: Personalisierung der generierten Verdachtsfälle

Phase 9: Klärung der Verdachtsfälle

Zur Wahrung des informationellen Selbstbestimmungsrechtes der Betroffenen und der Mitbestimmungsrechte der Arbeitnehmervertretungen sollten diese Verfahren insbesondere gekennzeichnet sein durch:

- Weitgehende Verwendung anonymisierter und pseudonymisierter Daten
- Einbeziehung des betrieblichen Datenschutzbeauftragten
- Personalisierung nur der ermittelten Verdachtsfälle unter Einbezug des Betriebsrates
- Sorgfältige Vertragsgestaltung und schriftliche Weisung bei Auftragsdatenverarbeitung durch externe Dienstleister
- Sorgfältiger Umgang mit der Datenübermittlung bei Funktionsübertragung an externe Dienstleister
- Benachrichtigung Betroffener
- Stakeholdermangement zur konsensorientierten Problemlösung
- Generelle vertragliche Regelungen

Mit der weitgehenden **Verwendung anonymisierter bzw. pseudonymisierter Daten** wird ein wesentlicher Beitrag zur Datenvermeidung im Sinne des BDSG¹⁰³ geleistet. So stellt der Abgleich von nicht personalisierten Dateien, z.B. Kontonummern und Bankleitzahlen von Mitarbeitern einerseits und von Lieferanten andererseits mit dem Ziel der Ermittlung der Schnittmenge von Fällen, die sowohl in der mitarbeiterbezogenen als auch in der lieferantenbezogenen Datei enthalten sind, nach diesseitiger Auffassung eine Vorgehensweise dar, die unter **Einbeziehung des betrieblichen Datenschutzbeauftragten** ausgeführt, datenschutzrechtlich nicht zu beanstanden ist. Methodisch-technisch setzt dies die Extraktion ausgewählter Datenfelder aus betrieblichen Datenbeständen voraus, also keine separate Erhebung ‚neuer‘ Daten. Im vorgenannten Beispiel wären dies die Datenfelder ‚Kontonummer‘ und ‚Bankleitzahl‘ aus den Stammdatensätzen der Mitarbeiter und der Lieferanten (Kreditoren). Andere personenidentifizierende Datenfelder wie Name, Personalnummer sind hingegen nicht Gegenstand des Datenabgleiches.

Der in diesem Zusammenhang häufig geäußerte **Vorwurf des Generalverdacht**, im genannten Beispiel gegenüber allen Mitarbeitern und Lieferanten, geht insofern fehl, als dass die Daten **ohne Ansehen der Person** einem ‚diskreten‘ technischen Verfahren unterzogen werden, dessen Ergebnis die Selektion von Verdachtsfällen ist. Es kann sogar argumentiert werden, dass durch eine vorgelagerte Selektion der Datenbestände, z.B. im Hinblick auf die Zugehörigkeit von Mitarbeitern zu bestimmten Abteilungen, ein weiterer datenschutzrechtlich relevanter Sachverhalt geschaffen würde und die Abteilungszugehörigkeit verdachtsverstärkend oder –mindernd wäre. Der begründete Verdacht ist aber eben nicht Ausgangspunkt und Impuls des Selektionsverfahrens, sondern sein erklärtes Ziel. Ein solcher Datenabgleich mit dem Ziel der Identifikation von Verdachtsfällen setzt empirische Erkenntnisse und Plausibilitäten über solche Merkmale und deren Ausprägungen (Indikatoren; ‚red flags‘) voraus, die signifikant sind im Hinblick auf den Analysegegenstand. Es liegt in der Natur der Sache, dass der gewählte Recherche- und Analyseansatz an Erfolgsaussicht verliert, wenn er dem Kreis der potentiellen Täter bekannt wird. Die Schaffung von Transparenz über ein solches Verfahren über das rechtlich gebotene Maß hinausgehend ist also nur insoweit angezeigt, als dass dadurch der Recherche- und Analyseerfolg und damit der berechtigte Zweck des Vorhabens nicht gefährdet ist.

¹⁰² Beim Einsatz von Abfragesprachen relationaler Datenbanken führt der Abgleich ggf. unmittelbar zu einer personalisierten Auflistung der in der Schnittmenge enthaltenen Datensätze, d.h. die Phasen 6 und 8 fallen zusammen.

¹⁰³ § 3a S. 2 BDSG

Ist die Anzahl der in der Schnittmenge vorliegenden abgeglichenen Daten > 0 , d.h. werden tatsächlich Verdachtsfälle aufgrund von Merkmalsentsprechungen identifiziert, so ist diese, typischerweise kleine Datenmenge datenschutzrechtlich einschlägig. Mit dem Abgleich wurde zunächst ein neues Datum generiert, im Beispiel das der Identität von Kontodaten der untersuchten Personengruppen. Auch wenn zunächst personell nicht zuzuordnen, bleibt eine solche Personalisierung zwingende Voraussetzung um den geschaffenen Verdacht weitergehend zu prüfen. Spätestens ab diesem Punkt (Phase 8) des Verfahrens wird die **Beteiligung des Betriebsrates** zu erfolgen haben. Für die generierten Verdachtsfälle

Aufgrund mangelnder technischer Voraussetzungen und um den Kreis der eingeweihten eigenen Mitarbeiter möglichst klein zu halten, werden ggf. externe Dienstleister mit der Durchführung der Recherche- und Analyseverfahren betraut. Insbesondere die externe Vergabe der Extraktion anonymisierter bzw. pseudonymisierter Daten, der Durchführung des Datenabgleichs und der Personalisierung der Verdachtsfälle erfordert datenschutzrechtlich ein detailliertes und formalisiertes Auftragsverhältnis. Wird dabei das Konstrukt der ‚Datenverarbeitung im Auftrag‘ gewählt, bleibt die Auftrag gebende Stelle verantwortlich für die weisungsgemäße Dienstleistung des Externen. Findet eine ‚Funktionsübertragung‘ statt, ist der Dienstleister für eigene Zwecke tätiger ‚Dritter‘. Seine Erlaubnistatbestände zur Verarbeitung der ihm übermittelten Daten sind aus dem Vertragsverhältnis mit dem Auftraggeber abzuleiten. Die Erlaubnistatbestände für die Übermittlung sind seitens des Auftraggebers nachzuweisen.

Die **Benachrichtigung der Betroffenen** ist grundsätzlich spätestens mit der Phase 8 (Personalisierung der generierten Verdachtsfälle) angezeigt. Sofern der Recherche- und Analysezweck dadurch nicht gefährdet wird, ist über die rechtlichen Vorgaben hinaus die Schaffung von Transparenz durch frühestmögliche Einbindung relevanter Organe, Gremien und Stellen ein wirkungsvolles Instrument, die innerbetriebliche und externe Akzeptanz für solche Maßnahmen zu fördern. Ein solches, die Anspruchsgruppen des Vorhabens berücksichtigendes **Stakeholdermanagement** mit dem Ziel der konsensorientierten Problemlösung, ist als wesentlicher Erfolgsfaktor des Projektmanagements anzusehen. Auch ist zu erwägen über erforderliche Compliance-Maßnahmen projektunabhängige, **generelle vertragliche Regelungen** durch Vereinbarungen mit dem Betriebsrat sowie den Mitarbeitern zu schaffen.

Zusammenfassend vertritt die Verfasserin mit den hier vorgelegten Ausführungen die Auffassung, dass ein **automatisierter Datenabgleich** auch von großen Mengen **nicht personalisierter Daten** mit dem Ziel der **Identifikation von Verdachtsfällen**, grundsätzlich sowohl hinsichtlich des BDSG und des BetrVG als auch unter dem Gesichtspunkt der Verhältnismäßigkeit nicht zu beanstanden ist. Die Angemessenheit im Hinblick auf die generierten und zu personalisierenden Verdachtsfälle bleibt im Einzelfall zu prüfen. Mit der Personalisierung der Verdachtsfälle erfordern die genannten Normen im Weiteren ein Verfahren mit hohem Organisations- und Formalisierungsgrad unter Beteiligung von Mitgliedern betrieblicher Aufsichts- und Überwachungsgremien, der Arbeitnehmervertretung sowie der Betroffenen.

Literatur- und Quellenverzeichnis

- [Albers/Rüschbaum 2002] Albers, Felicitas; Rüschbaum, Ferdinand: Wirtschaftsinformatik. Informationssysteme im Unternehmen. Stuttgart 2002.
- [ACFE 2008] Association of Certified Fraud Examiners (ACFE): Spotlight on Detecting and Preventing Billing Schemes, Fraud Examiner Newsletter Article, May 2008, <http://www.acfe.com/newsletters/fraud-examiner.asp?copy=may08-spotlight>, Abrufdatum 11.02.2009.
- [Audicon 2008a] Audicon GmbH: http://www.audicon.net/loesungen/continuous_monitoring/index.php, Stuttgart Abrufdatum 17.2.2009.
- [Audicon 2008b] Audicon GmbH: http://www.audicon.net/loesungen/wirtschaftskriminalitaet/audicon_Themensheets_Wirtschaftskriminalitaet.pdf, Stuttgart Abrufdatum 17.2.2009
- [Bäcker 2002] Bäcker, Ingo: Dolose Handlungen – Forensische Prüfungen und Kriminalitätsprävention als Pflichtaufgaben für die Interne Revision, Wien 2002.

- [Barton 2004] Barton, Dirk-Michael: Risikomanagement und IT-Sicherheit. Kommunikation Recht, 7. Jg. 2004, S. 305 - 312
- [Becker/Hoeren 2007] Becker, Jörg; Hoeren, Thomas: IT-Sicherheit – rechtliche Vorgaben und Implikationen für die Systemgestaltung. HMD – Praxis der Wirtschaftsinformatik. 43. Heft 258 2007, S. 98 - 108
- [Benford 1938] Benford, Frank: The Law of Anomalous Numbers. Proceedings of the American Philosophical Society 78 Jg. 1938, S. 551-572.
- [Berton 1995] Berton, Lee: He's got their Number. Scholar Uses Math to Foil Financial Fraud. Wall Street Journal, 10. July 1995.
- [Bhattacharya/Kumar 2008] Bhattacharya, Sukanto; Kumar, Kuldeep: Forensic Accounting and Benford's Law. IEEE Signal Processing Magazin, 25. Jg. März 2008, S. 150 – 152, Manuskript, Abrufdatum 17.2.2009: ftp://140.98.193.215/Magazines/sp/toieee/Mar2k8/InTheSpotlight_Mar2k8_FIN/InTheSpotlight_v6_FIN.pdf.
- [Böhmer 2009] Böhmer, Reinhold: Uhu, Thymian und Traviata: Der Datenskandal wird für Bahn-Chef Mehdorn zum Showdown. 4.2.2009 wiwo.de.
- [BIM 11.2.2009] Bundesministerium des Innern: Verlautbarung des Bundesinnenministers Schäuble, Pressemitteilung des BIM vom 11.2.2009; http://www.bmi.bund.de/cln_012/nn_662928/Internet/Content/Nachrichten/Pressemitteilungen/2009/01/Arbeitnehmerdatenschutz.html, Abrufdatum 17.2.2009.
- [BIM 2009] Bundesministerium des Innern: Abrufdatum 16.2.2009 http://www.bmi.bund.de/cln_012/nn_122688/sid_B938F6AF04CC7A695984A3417EE9C92A/Internet/Content/Commun/Lexikon/K/Korruption_und_Korruptionspraevention_Id_93284_de.html.
- [BVG 1983] Bundesverfassungsgericht: Volkszählungsurteil 15. Dezember 1983, NJW 1984, S. 419 ff.
- [Carslow 1988] Carslow, C.: Anomalies in Income Numbers. Evidence of Goal Oriented Behavior. The Accounting Review 63. Jg. 1988, S. 321-327.
- [DB AG 20.1.2009] Deutsche Bahn AG: DB und Berliner Datenschutzbeauftragter analysieren Arbeit der Network GmbH. Presseinformation, Berlin 20. Januar 2009.
- [DB AG 28.1.2009] Deutsche Bahn AG: DB-Stellungnahme zur Sitzung des Verkehrsausschusses. Datenabgleich hat nichts mit Ausspähung zu tun und ist rechtlich nicht zu beanstanden. Presseinformation, Berlin 28. Januar 2009.
- [DB AG 6.2.2009] Deutsche Bahn AG: Presseinformation, Berlin 6. Februar 2009.
- [DB AG 12.2.2009] Deutsche Bahn AG: Zwischenbericht des Vorstandes und des Chief Compliance Officer: Überprüfung der Ordnungsmäßigkeit von Maßnahmen der Korruptionsbekämpfung in den Jahren 1998-2007, Abrufdatum 12.2.2009: http://www.deutschebahn.com/site/shared/de/dateianhaenge/presse/zwischenbericht_090210.pdf.
- [Diekmann 2004] Diekmann, Andreas: Not the First Digit! Using Benford's Law to Detect Fraudulent Scientific Data. Manuskript, ETH Zürich, 2004.
- [DIIR 2009] Deutsches Institut für Interne Revision e.V.: homepage Abrufdatum 6.3.2009 <http://www.diir-2009.de/>
- [Drake/Nigrini 2000] Drake, Philip D.; Nigrini, Mark J.: Computer Assisted Analytic Procedures Using Benford's Law. Journal of Accounting Education 18. Jg. 2000, S. 127-146.
- [Ettredge/Srivastava 1998] Ettredge, Michael L.; Srivastava, Rajendra P.: Using Digital Analysis to Enhance Data Integrity. Manuskript University of Kansas, Juni 1998, Abrufdatum 17.2.2009: <http://www.eyecarat.ku.edu/publications/PDF%20Files%20of%20Papers%20by%20RPS/19.%20Digital%20Analysis%20Paper%20by%20E&S.pdf>.
- [Gatzke/Güßgen/Röhrig 2009] Gatzke, Marcus; Güßgen, Florian; Röhrig, Johannes : Daten-Skandal. Bahn bespitzelte eigene Mitarbeiter. Abrufdatum 16.2.2009: www.stern.de/wirtschaft/unternehmen/unternehmen/652179.html.
- [Geis/Helfrich 2007] Geis, Ivo; Helfrich, Marcus: Einführung. In: Datenschutzrecht, München 2007.
- [Grill/Schneyink 2005] Grill, Markus; Schneyink, Doris: Der VW-Skandal. Magazin stern 23.7.2005, zitiert nach <http://www.stern.de/wirtschaft/unternehmen/VW-Skandal-Die-Wolfsburg/542982.html?p=2&postid=2>, Abrufdatum 17.2.2009.
- [Grochla/Weber/Albers/Verhahn 1983] Grochla, E.; Weber, H.; Albers, F.; Verhahn, Th.: Ein betriebliches Informationssystem – Notwendigkeit und Ansatzpunkte für eine Neuorientierung. Angewandte Informatik Heft 5 /1983, S. 187 - 194.
- [Hoeren 2008] Hoeren, Thomas: Was ist das ‚Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme‘? MMR Multimedia und Recht, Heft 6 /2008, S. 365 f.
- [IDW 2006] Institut der Wirtschaftsprüfer in Deutschland e.V. (Hrsg.): WP-Handbuch 2006 Wirtschaftsprüfung, Rechnungslegung, Beratung. Band 1, 13. Aufl. Düsseldorf 2006.
- [KPMG 2007] KPMG Deutsche Treuhand – Gesellschaft Aktiengesellschaft Wirtschaftsprüfungsgesellschaft: Profile of a Fraudster. Studie 2007, S. 5 http://www.kpmg.de/docs/070420_Profile_of_a_Fraudster.pdf.
- [KPMG 2004] KPMG: Audit Committee Quaterly III/2004, S.9.
- [Lück/Henke 2004] Lück, Wolfgang; Henke, Michael: Risikomanagement und Interne Revision. In: Handwörterbuch Unternehmensführung und Organisation, 4. Aufl., hrsg. von Georg Schreyögg und Axel v. Werder, Stuttgart 2004, Sp. 1278 - 1288.
- [Lück 1998] Lück, Wolfgang: Der Umgang mit unternehmerischen Risiken durch ein Risikomanagementsystem und durch ein Überwachungssystem.. Der Betrieb, Heft 39, 25.9.1998, S. 1925 – 1930, zitiert aus DB-online Archiv, Abrufdatum 12.2.2009 http://www.der-betrieb.de/psdb/fn/db/sfn/bp/SH/ad0d1232627b431e2afb44431fbb89/bt_0/flg/1/cn/doc/strucid//ct//dh/0/bstruc/113/delcode/0/id/981925A/noautoiplogin/0/nops/0/oldpw/0/x/6/y/11/p1/p2/index.html#top.
- [o.V. Handelsblatt 2009] o.V.: handelsblatt.com 28.1.2009.
- [o.V. STERN 2009] o.V.: Mitarbeiterüberwachung: Der Lidl-Skandal; Abrufdatum 17.2.2009: <http://www.stern.de/wirtschaft/unternehmen/unternehmen/Mitarbeiter%FCberwachung-Der-Lidl-Skandal/614772.html>.
- [o.V. STERN 2008] o.V.: Siemens-Skandal: Gewerkschafter Schlesky muss in Haft. Magazin stern, 24. 11. 2008, zitiert nach: <http://www.stern.de/wirtschaft/unternehmen/unternehmen/Siemens-Skandal-Gewerkschafter-Schlesky-Haft/646695.html>, Abrufdatum 17.2.2009.
- [Palandt/Sprau 2009] Palandt, Otto/Sprau: BGB. Kommentar. 68. Aufl. München 2009

- [PWC AG 2009] Pricewaterhouse Coopers AG Wirtschaftsprüfungsgesellschaft: Datenscreening. Geschäftsschreiben an die Deutsche Bahn AG, 29. Januar 2009. In: Deutsche Bahn AG: Zwischenbericht: Überprüfung der Ordnungsmäßigkeit von Maßnahmen der Korruptionsbekämpfung in den Jahren 1998-2007, Anlage 1, 10.2.2009, http://www.deutschebahn.com/site/shared/de/dateianhaenge/presse/zwischenbericht_090210.pdf.
- [Röhrig 2009] Röhrig, Johannes: Kommentar 28.1.2009, www.stern.de.
- [Rother 2009] Rother, Michael: Kommentar 28.1.2009, taz.de.
- [Schwarz 2005] Schwarz, Sebastian Henner: Regulierung durch Corporate Governance Kodizes. Diss. Jur. Fak. Humboldt-Universität zu Berlin, 2005.
- [o.V. SPIEGEL 2008] o.V.: Abhöraffaire. Telekom bespitzelt Aufsichtsräte, Manager und Journalisten. Spiegel-online 24. Mai 2008, <http://www.spiegel.de/wirtschaft/0,1518,555148,00.html>, Abrufdatum 17.2.2009.
- [Stahlknecht/Hasenkamp 2005] Stahlknecht, Peter; Hasenkamp, Ulrich: Einführung in die Wirtschaftsinformatik, 11. Aufl., Berlin u.a. 2005.
- [o.V. Süddeutsche 2009] o.V.: sueddeutsche.de, 28.1.2009.
- [Wells 2001] Wells, Joseph T.: Enemies Within. Asset misappropriation comes in many forms. Journal of Accountancy, December 2001, S. 4; Abrufdatum 11.02.2009: <http://www.journalofaccountancy.com/Issues/2001/Dec/EnemiesWithin.htm?action=p>.
- [o.V. WELT 2009] o.V.: welt.online, 3.2.2009.
- [v. Werder 2004] Werder, Axel v.: Corporate Governance (Unternehmensverfassung). In: Handwörterbuch Unternehmensführung und Organisation, 4. Aufl., hrsg. von Georg Schreyögg und Axel v. Werder, Stuttgart 2004, Sp. 160 – 170.

Normen und Urteile

- [AO] Abgabenordnung
- [AktG] Aktiengesetz
- [BAG 2008] Bundesarbeitsgericht: Videoüberwachung im Betrieb - Beachtung des Persönlichkeitsrechts der Arbeitnehmer - Grundsatz der Verhältnismäßigkeit – Einigungsstellenspruch; 26.8.2008, 1 ABR 16/07; <http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=en&Datum=2008&nr=12998&pos=1&anz=296#druck>
- [BVerfG 1983] Volkszählungsurteil 15. Dezember 1983, NJW 1984, S. 419 ff.
- [BVerfG 2008] Urteil zur Online-Durchsuchung BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html
- [BetrV] Betriebsverfassungsgesetz
- [BGB] Bürgerliches Gesetzbuch
- [BDSG] Bundesdatenschutzgesetz
- [BSI 2008] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge, Übergreifende Aspekte, Baustein Datenschutz (B 1.5); <http://www.bsi.de/gshb/baustein-datenschutz/dokumente/b01005.pdf>
- [DCGK 2008] Deutscher Corporate Governance Kodex http://www.corporate-governance-code.de/ger/download/D_Kodex%202008_markiert.pdf
- [GC 2005] Global compact Büro, Vereinte Nationen: <http://www.unglobalcompact.org/Languages/german/de-gc-flyer-05.pdf>
- [GDPdU 2001] Die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU). BMF-Schreiben vom 16. Juli 2001 - IV D 2 - S 0316 - 136/01 - http://www.bundesfinanzministerium.de/nr_314/DE/BMF_Startseite/Aktuelles/BMF_Schreiben/Veroeffentlichungen_zu_Steuerarten/abgabenordnung/006.templateId=raw.property=publicationFile.pdf
- [GmbHG] GmbH-Gesetz
- [HGB] Handelsgesetzbuch
- [IDW210] IDW PS 210 'Zur Aufdeckung von Unregelmäßigkeiten im Rahmen der Abschlussprüfung', Die Wirtschaftsprüfung Heft 22/2006, S. 1422 ff.
- [IIA 2007] The Institute of Internal Auditors: Standards für die berufliche Praxis der Internen Revision, Florida 2007; http://www.diiir-2009.de/fileadmin/downloads/fachwissen/IIA_Standards.pdf
- [IIR 1] Deutsches Institut für Interne Revision e.V. (IIR): Revisionsstandard Nr. 1: Zusammenarbeit von Interner Revision und Abschlussprüfer; http://www.diiir-2009.de/fileadmin/downloads/fachwissen/Revisionsstandard_Nr_1.pdf
- [IIR 2] Deutsches Institut für Interne Revision e.V. (IIR): Revisionsstandard Nr. 2: Prüfung des Risikomanagement durch die Interne Revision, ohne Datum; http://www.diiir-2009.de/fileadmin/downloads/fachwissen/Revisionsstandard_Nr_2.pdf
- [IIR 3] Deutsches Institut für Interne Revision e.V. (IIR): Revisionsstandard Nr. 3: Qualitätsmanagement in der Internen Revision, 12. August 2002; http://www.diiir-2009.de/fileadmin/downloads/fachwissen/Revisionsstandard_Nr_3.pdf
- [ISA240] International Standard of Auditing (UK and Ireland) 240.
- [RLK 2004] Richtlinie der Bundesregierung zur Korruptionsprävention in der Bundesverwaltung Vom 30. Juli 2004; Anlage 2 Leitfaden für Vorgesetzte und Behördenleitungen, II, 1.1, Abrufdatum 14.2.2009: http://www.bmi.bund.de/nr_122688/Internet/Content/Common/Anlagen/Lexikon/Richtlinie_korruptionspraevention_30072004de.templateId=raw.property=publicationFile.pdf/Richtlinie_korruptionspraevention_30072004de.pdf
- [SOX 2002] Sarbanes-Oxley-Act 2002, <http://www.sec.gov/about/laws/soa2002.pdf>.
- [StGB] Strafgesetzbuch

