CReport

Dennis Heinson/Bernd Schmidt

IT-gestützte Compliance-Systeme und Datenschutzrecht

Ein Überblick am Beispiel von OLAP und Data Mining

Als Bestandteil guter Corporate Governance ist die Geschäftsleitung verpflichtet Legalität der unternehmerischen Tätigkeit sicherzustellen, indem sie unternehmensorganisatorische Maßnahmen ergreift (Compliance). Insbesondere in komplexen Unternehmensstrukturen verbinden sich damit große Herausforderungen. So gilt es Compliance-Risiken zu erfassen, Maßnahmen zu ihrer Vermeidung zu treffen und den Compliance-Standard zu überwachen. Es liegt nahe hierfür IT-gestützte Verfahren unter Nutzung betrieblicher Datenbestände einzusetzen, denn sie bilden betriebliche Vorgänge aufgrund der mittlerweile allgegenwärtigen Nutzung von IT-Systemen in der Geschäftswelt umfassend ab. Durch Online Analytical Processing (OLAP) und Data Mining lassen sich betriebliche Datenbestände systematisch auswerten und Verdachtsfälle von Verstößen gegen Unternehmensrichtlinien, Verträge und Strafgesetze durch Beschäftigte ermitteln. IT kann auch der Steuerung der Un-

▷ Dennis Heinson, LL.M. (UCLA), ist Doktorand am Lehrstuhl von Prof. Dr. Alexander Roßnagel und Stipendiat an der Universität Kassel für das Center for Advanced Security Research Darmstadt (CASED). Dr. iur. Bernd Schmidt, LL.M. (UoA), ist Rechtsreferendar in Bremen, er promovierte am Lehrstuhl von Prof. Taeger an der Universität Oldenburg zum Thema ‚Compliance in Kapitalgesellschaften'.

ternehmensorganisation durch das Management dienen, so dass ihr Einsatz auch für die Organisation von Compliance hohen Wert haben kann. Hierbei gilt es die Lehren aus den Datenskandalen bei der Bahn, der Telekom und anderen Unternehmen zu ziehen und IT-gestützte Compliance-Systeme nur im Rahmen der datenschutzrechtlichen Zulässigkeit zu implementieren. Dieser Beitrag gibt einen Überblick über die rechtliche Notwendigkeit und die technischen Möglichkeiten IT-gestützter Maßnahmen, greift hieraus folgende rechtliche Fragestellungen auf und zeigt Möglichkeiten zur rechtskonformen Gestaltung eines IT-gestützten Compliance-Systems auf.

I. Compliance-Pflicht des Managements

Der Deutsche Corporate Governance Kodex (DCGK) definiert Compliance in Ziff. 4.1.2 als Einhaltung der gesetzlichen Bestimmungen und unternehmensinternen Richtlinien und geht für die Aktiengesellschaft von der Verantwortlichkeit des Vorstands aus. Bei Ziff. 4.1.2 DCGK handelt es sich um eine Informationsvorschrift ohne normativen Charakter, die lediglich bestehendes Gesetzesrecht darstellen soll. Zur Begründung von Rechtspflichten ist daher die zugrunde liegende gesetzliche Wertung heranzuziehen. Richtigerweise wird überwiegend angenommen, dass die Compliance-Verantwortung des Managements in seinen Sorgfaltspflichten angelegt ist.[1] Im Fall der Aktiengesellschaft findet sich eine solche Pflicht in § 93 Abs. 1, Satz 2 AktG, für die GmbH in § 43 Abs. 1 GmbHG und für die Genossenschaft in § 34 Abs. 1 Satz 1 GenG. Dies ist konsequent, da sich der intern zulässige Handlungsrahmen für die Geschäftsleitung aus ihrer allgemeinen Sorgfaltspflicht und spezielleren Ausprägungen hiervon ergibt, so dass auch eine Pflicht zur Herstellung von Compliance in Ermangelung einer spezielleren Vorschrift hierauf zurück zu führen ist.[2] Hiervon abweichend, in den rechtlichen Konsequenzen aber ähnlich, wird zur Begründung von Compliance-Pflichten zum einen auch auf einen verallgemeinerbaren Rechtsgedanken verwiesen, der seine Ausprägung in einer Vielzahl von Einzelvorschriften gefunden habe, wie in § 91 Abs. 2 AktG, § 130 OWiG, § 52a Abs. 2 BImSchG, § 53 KrW-/AbfG sowie § 14 Abs. 2 GeldwäscheG.[3] Zum andern wird vertreten, dass Compliance-Pflichten aus der Sorgfalt eines ordentlichen Kaufmanns gem. § 347 HGB abzuleiten seien.[4]

1. Vermeidung von Compliance-Schäden

Das Management hat bei der Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Aus dieser allgemeinen Umschreibung ergeben sich keine unmittelbaren Rückschlüsse auf die Compliance-Verantwortung des Managements, jedoch eine Gebot, die Kapitalgesellschaft nicht durch aktives Tun zu schädigen sowie Schädigungen durch Dritte abzuwenden und Vorteile der Gesellschaft zu wahren.[5] Nachteile für die Gesellschaft sind in diesem Zusammenhang in zwei Konstellationen denkbar. So können Unternehmen als Opfer von Rechtsverletzungen geschädigt werden, aber auch auf Täterseite an der Begehung von Rechtsverstößen beteiligt sein, woraus Sanktionen gegen das Unternehmen für zurechenbares Verhalten folgen können.[6] Auch kann es zu Gewinnabschöpfungen im Rahmen von Strafverfahren und börsenrechtlichen Maßnahmen, zu Auftragssperren durch die Aufnahme in schwarze Listen bei Korruptionsvorfällen[7] sowie zu Störungen im Betriebsablauf durch Ermittlungstätigkeit von Behörden und zu Reputationsschäden bei Geschäftspartnern und in der Öffentlichkeit durch eine negative mediale Präsenz kommen.[8] Vor dem Hintergrund hoher Schadenspotentiale aus einem schlechten Compliance-Standard ergibt sich für das Management im Rahmen seiner Sorgfaltspflicht das Gebot Maßnahmen zu ergreifen, um Transparenz der Compliance-Risiken herzustellen und ihr Auftreten sowie ihre Auswirkungen zu kontrollieren.

2. Legalitätspflicht

Die Wertung aus der Verantwortung für die Schadensabwehr wird verstärkt durch die Legalitätspflicht, die im deutschen Recht keine direkte Normierung erfahren hat, jedoch einer Vielzahl gesetzlicher Regelungen zugrunde liegt. So lässt sich auf § 130 OWiG verweisen, aus dem sich eine personalbezogene Aufsichtspflicht zur Vermeidung von Straftaten und Ordnungswidrigkeiten durch Unternehmensangehörige ergibt.[9] Der Vorrang des geltenden Rechts vor anderen Zielen und Interessen der Gesellschaft ergibt sich zudem aus § 396 Abs. 1 AktG.[10] Die Norm ermöglicht eine Auflösung der Gesellschaft bei gemeinwohlgefährdender und rechtswidriger Aktivität, woraus sich der Rückschluss auf die Legalitätspflicht ziehen lässt. Neben der Verantwortung zur Schadensabwehr wird die Compliance-Pflicht des Managements wesentlich durch den Grundsatz der Legalität geprägt. In Ergänzung zur Verantwortung des Managements für die Schadensabwehr erfordert die Legalitätspflicht, Compliance auch dann herzustellen, wenn dies in der unmittelbaren Konsequenz zunächst nachteilig für die Gesellschaft erscheint.

II. OLAP und Data Mining

Zur Gewinnung relevanter Daten aus IT-Systemen werden Verfahren aus den Bereichen OLAP und Data Mining angewendet.[11] Seit einiger Zeit werden sie in Unternehmen auch zu sog. Massenscreenings von Beschäftigtendaten zur Erfüllung von Compliance-Pflichten eingesetzt. Sie werden als Mittel gewählt, da sie durch technischen Fortschritt bei der eingesetzten Software wirtschaftlich attraktiv geworden sind, um große Datenbestände auszuwerten. Bei ihrem Einsatz stellt sich eine Vielzahl neuer Rechtsfragen, denn das Spektrum des

1 *Bürkle*, BB 2007, 1797 (1798); *Fleischer*, BB 2008, 1070 (1072); *Fleischer*, CCZ 2008, 1 (3); *Hauschka*, AG 2004, 461 (462); *Kort*, NZG 2008, S. 81 (83); *Nolte/Becker*, BB-Special 5/2008, 23; *Schmidt*, BB 2009, 1295; *Schneider/Schneider*, ZIP 2007, 2061 ff.; *Taeger* in Hoffmann/Kitz/Leible, IT-Compliance, 2009, S. 46 (47); *Vetter*, DB 2007, 1963 (1964).

2 Umfassend zur Begründung von Compliance-Pflichten *Schmidt*, Compliance in Kapitalgesellschaften, 2010.

3 *Schneider*, ZIP 2003, 645 (648 f.).

4 *Heldmann*, DB 2010, 1235.

5 BGHZ 21, 354 (357); *Fleischer* in Spindler/Stilz, AktG, § 93 Rz. 11; *Hopt* in GK, AktG, § 93 Rz. 72.

6 *Barton*, RDV 2009, 200 (201); *Hauschka*, BB 2004, 1178; *Lösler*, NZG 2005, 104; *Schneider*, ZIP 2003, 645 (648).

7 *Barton*, RDV 2009, 200 (201); *Kolbe*, NZA 2009, S. 228 (229); *Zimmer/Stetter*, BB 2006, 1445 f.

8 So auch *Brandt*, AiB 2009, 288; *Vetter* in Wecker/van Laak, Compliance in der Unternehmerpraxis, 2008, S. 29 (33); zur Bedrohung durch Korruption im Unternehmen *Wieland*, CCZ 2008, S. 15 (17); *Zimmer/Stetter* BB 2006, 1445 f.

9 So auch *Heldmann*, DB 2010, 1235.

10 *Fleischer* in Spindler/Stilz, AktG, § 93 Rz. 32; *Fleischer*, ZIP 2005, 141 (148); *Thole*, ZHR 2009, 504 (514 f.).

11 Zu den Begriffen s. *Düsing* in P. Chamoni/P. Gluchowski: Analytische Informationssysteme, 2008, S. 292, 295.

technisch Möglichen wird vom datenschutzrechtlich Zulässigen begrenzt. Jede Untersuchung muss ihrerseits mit dem Datenschutzrecht ‚compliant' sein. Was zu tun ist, um Verfahren datenschutzkonform zu gestalten, hängt von den eingesetzten Methoden und Algorithmen ab. Grundsätzlich lassen sich die in Unternehmen eingesetzten Verfahren in zwei Gruppen einteilen:

1. OLAP (Massendatenabgleiche)

OLAP-basierte Verfahren untersuchen Datensammlungen auf die Erfüllung von vordefinierten Hypothesen und erkennen so Übereinstimmungen mit erwarteten Mustern. Vor einem Screening werden dazu potentiell relevante Daten aus unterschiedlichen Unternehmensbereichen auf einen einzelnen dedizierten Server kopiert und dort analysiert.[12] Die eigentliche Untersuchung ist eine komplexe Form einer Datenbankabfrage mit optimierten Suchalgorithmen.[13] Die Abfragekriterien beim Aufspüren von Verstößen Beschäftigter (fraud patterns), drücken die Art und Weise aus, in der sich missbräuchliches Verhalten in Datensammlungen niederschlägt. In Abhängigkeit von der Formulierung der Abfrage wird stets eine eindeutige Antwort geliefert. Je genauer das Untersuchungsmuster definiert ist, desto höher kann der Beweiswert der ausgegebenen Daten ausfallen. Er kann vom Anfangsverdacht (red flag) bis zum eindeutigen Nachweis eines Verstoßes reichen. Nach der Untersuchung können die Daten wieder gelöscht werden oder verbleiben in einem Data Warehouse zur späteren Verwendung.[14] Ein denkbarer Anwendungsfall für OLAP ist der Abgleich von Kontodaten der Beschäftigten eines Unternehmens mit allen Kontodaten von Lieferanten. Übereinstimmungen können dann belegen, dass ein Kontoinhaber nicht nur ein Gehalt vom Unternehmen erhält, sondern auch der Empfänger weiterer Zahlungen ist. Auch nachträgliche Manipulationen in der Unternehmens-IT können mit dieser Methode aufgespürt werden, indem Relationen zwischen Datenbankeinträgen automatisiert auf ihre Schlüssigkeit überprüft werden.[15]

2. Data Mining

Data Mining geht über die einfache Suche nach definierten Mustern heraus. Als Form des maschinellen Lernens sind diese Verfahren eigenständig in der Lage unbekannte Muster zu entdecken. Neben Systemen, die Kaufempfehlungen für Kunden von Online-Shopsystemen geben können und dem Customer Relationship Management ist Data Mining besonders beim Aufspüren von Kreditkartenmissbrauch oder zur Aufdeckung von Geldwäsche (fraud detection) bereits großflächig im Einsatz.[16] Data Mining eignet sich auch dazu, eigenständig Abweichungen vom Normverhalten aufzuspüren (Abweichungsentdeckung) und somit mögliche fraud patterns zu erzeugen. Deshalb werden sie auch für das Aufspüren von Verstößen durch Beschäftigte eingesetzt. Data Mining vollzieht sich in vier Schritten:[17]

(1.) Fokussierung: Hier werden Erkennungsparameter und Data Mining-Methoden vorgegeben. Sie bestimmen die Zielrichtung der Untersuchung und damit die Qualität des Untersuchungsergebnisses im Hinblick auf die aufzuspürenden Kriterien.[18] Verfolgt man den Zweck der Abweichungsentdeckung gehört dazu auch die Modellierung von Normverhalten.[19]

(2.) Transformation/Strukturierung: Sodann werden die Daten gesammelt und vorverarbeitet (2), das heißt in ein für Data Mining-Verfahren geeignetes Format transformiert und strukturiert.[20]

(3.) Analyse: Zum Aufspüren von Verstößen durch Beschäftigte wird insbesondere die Abweichungsentdeckung eingesetzt. Sie kann, anders als OLAP-basierte Verfahren, auch ohne Kenntnis von Missbrauchsschemata unerwünschte Handlungen aufspüren.[21]

(4.) Evaluation/Interpretation: Unabhängig von konkreten Suchzielen lassen sich Abweichungen vom Normverhalten aufspüren und ausgeben.[22] Diese Abweichungen können Indizien für verbotene Handlungen sein, treten aber auch in gewöhnlichen Geschäftsabläufen auf.[23] Sie können nur zur Verdachtsgenerierung dienen, nicht aber zum Nachweis von verbotenen Handlungen, die etwa strafrechtlich relevant sind. Deshalb muss im letzten Schritt eine Evaluation und Interpretation erfolgen und anschließend die Entscheidung getroffen werden, ob Anschlussermittlungen durchgeführt werden. Allein durch Data Mining ist eine Untersuchung mit Beweiswert für den Einzelfall nicht möglich.

3. Screening-Software und -Dienstleister

Zum Durchsuchen von Datenbeständen nach Verstößen durch Beschäftigte sind unterschiedliche, auf diesen Zweck abgestimmte Softwarelösungen erhältlich,[24] die von Unternehmen unmittelbar einsetzbar sind. OLAP und Data Mining sind auch als Dienstleistung in Form von Forensic Services, Forensic Accounting oder Fraud Detection erhältlich und werden vielfach von Wirtschaftsprüfungsunternehmen angeboten.[25] Am Markt sind alle beschriebenen OLAP- und Data Mining-Verfahren verfügbar, so dass es wesentlich von der Entscheidung der verantwortlichen Stelle abhängt, welches Verfahren im Einzelnen angewendet wird.

III. Rechtliche Rahmenbedingungen

Allen beschriebenen Verfahren ist gemein, dass sie Daten mit dem Zweck auswerten, darin Hinweise auf regelwidriges Verhalten von Unternehmensangehörigen und Dritten zu finden oder darüber hinausgehend Ergebnisse mit Beweiswert zu erhalten.[26] Als Datenquelle kommen alle Bereiche der Unternehmens-IT in Frage. Außerdem ist eine Anreicherung mit Kontextdaten zu außerhalb des Unternehmens zu findenden Informationen zur Erhöhung der Aussagekraft denkbar. Bei der Durchführung werden regelmäßig auch solche Daten verwendet, die einen Personenbezug i.S.d. § 3 BDSG aufweisen, so

12 *Frosch-Wilke*, DuD 2003, 597 (598 ff.); *Hahn*, DuD 2003, S. 605 (605 f.).
13 *Frosch-Wilke*, DuD 2003, 597 (601).
14 *Baeriswyl*, RDV 2000, 6 f.
15 *Heinson et al.* DuD 2010, 75 (78).
16 Beispiel in *Krahl/Windheuser/Zick*, Data Mining, 1998, S. 106 f.
17 Systematik nach *Piazza*, Data Mining im Personalmanagement, 2010, S. 36 f.
18 *Piazza*, Data Mining im Personalmanagement, 2010, S. 34 f.
19 *Piazza*, Data Mining im Personalmanagement, 2010, S. 51.
20 *Piazza*, Data Mining im Personalmanagement, 2010, S. 36 f.
21 *Frosch-Wilke*, DuD 2003, 597 (602).
22 *Wrobel*, KI 1998, 6 (7).
23 *Salvenmoser/Hauschka*, NJW 2010, 331 (332).
24 Einige Anbieter von Software zur Aufdeckung von Verstößen: Delta Miner der *Bissantz & Company GmbH (www.bissantz.de/deltamaster/)*, Gritbot von *Rulequest Research (www.rulequest.com/gritbot-info.html)* sowie verschiedene Software von *Wizsoft (www.wizsoft.com/)*.
25 der *PriceWaterhouseCoopers (www.pwc.de/redirect/Ihre_Branche/Finanzdienstleistung/Corporate_Governance_Services/Forensic_Services/)*; s. hierzu *Eisele/Uhlen*, ZCG 2009, 176.
26 *Heinson et al.*, DuD 2010, 75 (76).

dass für die rechtliche Bewertung die Vorgaben des Datenschutzrechts zu beachten sind.[27] Eine Ausnahme ergäbe sich nur, wenn die verarbeiteten Daten keinen Personenbezug aufweisen, also anonym sind. In diesem Fall ist das Datenschutzrecht nicht mehr anwendbar, so dass sich hieraus keine Verarbeitungsbeschränkungen ergeben können.[28] Für OLAP und Data Mining ergibt sich jedoch eine Reihe von Problemen. Zum einen sinken Aussagekraft und der Beweiswert von Untersuchungen, die mit anonymen Daten durchgeführt wurden. Zum anderen muss die Effektivität der Anonymisierung sichergestellt und insbesondere technisch ausgeschlossen sein, dass Rückschlüsse von Daten auf Einzelpersonen während und nach der Datenverarbeitung möglich sind. Nach § 3 Abs. 7 BDSG sind nämlich nur solche Daten anonym, die nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand einer Person zugeordnet werden können.

1. Anonymisierungstechnik

Allgemein geeignet zum Ausschluss des Personenbezugs sind Verfahren, bei denen während der Verarbeitung und nach dessen Abschluss Rückschlüsse auf Einzelpersonen technisch wirksam verhindert oder wesentlich erschwert werden. Der einfachste Ansatz zur Anonymisierung besteht darin, alle Daten zu *löschen*, die eine Zuordnung zu einer Person ermöglichen.[29] Der offensichtliche Nachteil ist die Verringerung der Datenbasis. Bei einer anderen Methode wird die Eindeutigkeit der Zuordnung von Daten zu einer Person beseitigt, indem Daten *generalisiert* werden (beispielsweise Zugehörigkeit zu einer Unternehmensabteilung anstelle namentlicher Identifikation).[30] Dies ist nur dann sinnvoll, wenn es auf ein einzelnes Datum nicht ankommt. Eine Dritte Methode ist die *Aggregierung*. Hier wird mit einem statistischen Durchschnitt einer Datenmenge gearbeitet und so versucht, eine Rückzuordnung auszuschließen.[31]

Diesen Anonymisierungstechniken stehen eine wachsenden Zahl von Re-Identifikationstechniken entgegen, die es ermöglichen den Personenbezug nachträglich wieder herzustellen.[32] Untersuchungen haben gezeigt, dass Rückschlüsse auch bei minimalem Datenbestand mit sehr hoher Wahrscheinlichkeit möglich sind. Beispielsweise genügten bei einer Online-Videothek mit fünfhunderttausend Nutzern sechs Nutzerbewertungen von Filmtiteln, um in ca. 84 % der Fälle den Bewerter eindeutig zu identifizieren.[33] Ähnliches gilt für eine Kombination aus Postleitzahl, Geburtsdatum und Geschlecht innerhalb der gesamten US-Bevölkerung.[34] Der Grund liegt darin, dass nur sehr wenige Personen genau dieselbe Kombination an Datensätzen aufweisen und sich so eindeutig bestimmen lassen. Diese Erkenntnis zieht die Wirksamkeit sämtlicher Anonymisierungstechniken in Zweifel und legt den Schluss nahe, dass personenbezogene Daten in der Regel technisch nicht sicher zu anonymisieren sind.[35] Ein anderer Schluss kann sich in einer rechtlichen Wertung allenfalls ergeben, wenn der Aufwand zur Wiederherstellung des Personenbezugs unverhältnismäßig hoch ist und die Daten deshalb anonym gem. § 3 Abs. 6 BDSG sind. Dies hängt u.a. von Zusatzwissen der datenverarbeitenden Stelle ab.[36] Zusatzwissen ist in Unternehmen oder anderen Organisationen typischerweise vorhanden, weil neben vermeintlich anonymen Daten auch der nicht-anonymisierte Datenstamm verfügbar ist.[37] Deshalb ist davon auszugehen, dass in einem IT-gestützten Compliance-System eine wirksame Anonymisierung nicht garantiert werden kann. Hinzu kommt, dass durch Anonymisierung die Ergebnisqualität der Datenauswertung ganz wesentlich gemindert werden kann.[38]

2. Pseudonymisierungstechnik

Ein weiteres technisches Verfahren für den datenschutzverträglichen Umgang mit personenbezogenen Daten ist die Pseudonymisierung, die auch in § 3 Abs. 6a und § 3a Satz 2 BDSG gesetzlich vorgesehen ist. Hierbei wird das identifizierende Merkmal einer Person (etwa der Name) durch einen Schlüssel (Zuordnungsregel) ersetzt. Da die die datenverarbeitenden Personen oder Stellen bei nicht über die Zuordnungsregeln verfügen, ist während einer Untersuchung keine Zuordnung von Daten zu Personen möglich. Die eingriffsintensive ‚Rasterung' findet mit anonymen Daten statt. Im Unterschied zur Anonymisierung lässt sich am Ende des Verfahrens bei Verdachtsfällen eine Re-Identifikation durch Nutzung der Zuordnungsregeln vorsehen. Da der Einzelne so keine Falschverdächtigung fürchten muss, die über das allgemeine Lebensrisiko hinausgeht,[39] ist die Zuordnung von Daten und Person bei Vorliegen eines konkreten Verdachts verhältnismäßig und zu rechtfertigen.[40]

Für eine effektive Senkung der Eingriffsintensität darf dabei für die datenverarbeitende Stelle nicht die Möglichkeit verbleiben, die Personenzuordnung wieder herzustellen.[41] Ist eine Aufdeckung „auf Zuruf" des Auftraggebers möglich, ist die Eingriffsintensität nur scheinbar gesenkt (unechte Pseudonymisierung).[42] Beim Einsatz für Ermittlungen wie OLAP und Data Mining müssen deshalb Schutzmechanismen geschaffen werden, die echte Pseudonymität herstellen. Dies kann etwa durch die Einbeziehung einer dritten Stelle als Treuhänder in

27 A.A. *Bierekoven*, CR 2010, 203, ohne Begründung von der Unanwendbarkeit des BDSG ausgehend; nach *Salvenmoser/Hauschka*, NJW 2010, 331 (332) soll das BDSG nur in Einzelfällen anwendbar sein.

28 Vgl. *Roßnagel/Scholz*, MMR 2000, 721 (722); *Gola* in Gola/Schomerus BDSG § 3 Rz. 43.

29 *Sweeney*, Achieving k-anonymity privacy protection using generalization and suppression, International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002, S. 571, 574.

30 *Sweeney*, Achieving k-anonymity privacy protection using generalization and suppression, International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002, S. 571, 574.

31 Siehe *Ohm*, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (13.8.2009), University of Colorado Law Legal Studies Research Paper Nr. 09-12, *http://ssrn.com/abstract=1450006*, S. 14 (Fn. 57) m.w.N.; *Dammann* in Simitis, BDSG, § 3 Rz. 207; *Weichert*, RDV 2003, 116 (119).

32 BVerfG v. 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, BVerfGE 65, 1 (45); *Dammann* in Simitis, BDSG, § 3 Rz. 26 ff.

33 *Narayanan/Shmatikov*, Robust De-anonymization of Large Sparse Datasets (How To Break Anonymity of the Netflix Prize Dataset), Proceedings of 29th IEEE Symposium on Security and Privacy, Oakland, CA, May 2008, S. 111 (S. 124, Grafik 11).

34 *Sweeney*, Uniqueness of Simple Demographics in the U.S. Population, Carnegie Mellon University, School of Computer Science, Data Privacy Laboratory, Technical Report LIDAP-WP4, 2000.

35 Siehe *Ohm*, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (13.8.2009), University of Colorado Law Legal Studies Research Paper Nr. 09-12, *http://ssrn.com/abstract=1450006*, S. 1.

36 *Roßnagel/Scholz*, MMR 2000, 722 (728); *Dammann* in Simitis, BDSG, § 3 Rz. 30 ff.

37 *Weichert*, RDV 2003, 113 (119).

38 *Piazza*, Data Mining im Personalmanagement, 2010, S. 139 f.

39 Siehe BVerfG v. 4.4.2006 – 1 BvR 518/02, BVerfGE 115, 320 (351) m.w.N. = CR 2006, 594 m. Anm. *Schmitz*.

40 *Bizer* in Simitis, BDSG, § 3 Rz. 221.

41 *Bizer* in Simitis, BDSG, § 3 Rz. 217.

42 Das Problem erkennt auch das BVerfG, s. BVerfG v. 4.4.2006 – 1 BvR 518/02, BVerfGE 115, 320 (354) = CR 2006, 594 m. Anm. *Schmitz*; dennoch vorgeschlagen bei *Kock/Francke*, NZA 2009, 646 (648).

das Verfahren erreicht werden.[43] Die Stelle, etwa der Betriebsrat, könnte mit der Verwahrung der Zuordnungsregeln betraut werden und sicherstellen, dass diese nur im Trefferfall herausgegeben werden. Pseudonymisierung leidet zudem an denselben Schwächen wie Anonymisierung: neben der Zuordnungsregel können auch Zusatzwissen und Re-Identifikationstechniken für eine Zuordnung von Datum und Person genutzt werden. Deshalb bleiben pseudonyme Daten zusätzlich zu dem Problem des Umgangs mit der Zuordnungsregel unter den gleichen Voraussetzungen personenbezogen, wie bei dem Einsatz von Anonymisierungstechnik.

Aus den genannten Gründen bleibt für OLAP und Data Mining deshalb regelmäßig Datenschutzrecht einschlägig. Aus § 4 Abs. 1 BDSG ergibt sich, dass eine Erlaubnisvorschrift oder eine schriftliche Einwilligung des Betroffenen für den Umgang mit Daten notwendig ist. OLAP und Data Mining benötigen technisch bedingt jedoch große Quelldatenbestände und damit auch Daten über viele Personen. Die Einholung einer schriftlichen Einwilligung jedes Betroffenen gem. § 4a Abs. 1 BDSG ist hierbei nicht mit vertretbarem Aufwand zu gewährleisten,[44] so dass eine alternative Rechtfertigung für die Datenverarbeitung zur Aufdeckung von Regelverstößen durch Beschäftigte notwendig ist. Dies können insbesondere Betriebsvereinbarungen (s. 2. unten), gesetzliche Erlaubnistatbestände zur Datenverarbeitung in Beschäftigungsverhältnissen gem. § 32 Abs. 1 BDSG (s. 3.a) unten) oder die zur Datenverarbeitung für eigene Geschäftszwecke gem. § 28 Abs. 1 BDSG (s. 3.b) unten) sein.

2. Betriebsvereinbarungen

Die Verarbeitung von Arbeitnehmerdaten kann aufgrund einer Betriebsvereinbarung nach § 77 BetrVG gerechtfertigt werden. Ihr Inhalt unterliegt bezüglich der Ermittlungen mit OLAP und Data Mining gem. § 87 Abs. 1 Nr. 6 BetrVG einem betrieblichen Mitbestimmungsrecht, da es sich hierbei um technische Methoden handelt, die dazu bestimmt und objektiv geeignet sind, das Verhalten und die Leistung der Arbeitnehmer zu überwachen.[45] Beim Abschluss von Betriebsvereinbarungen sind die Parteien gem. § 75 Abs. 2 BetrVG zur Beachtung der informationellen Selbstbestimmung verpflichtet.[46] Das hierdurch gewährte Schutzniveau steht nicht zur Disposition der Parteien,[47] sie können aber im Rahmen der gesetzlichen Vorgaben einzelfallbezogene Regelungen treffen, die Anwendungsvorrang gegenüber dem BDSG genießen.[48] Soweit die Regelungen der Betriebsvereinbarung personell oder sachlich nicht anwendbar sind oder nicht abschließend sind, bedarf es des Rückgriffs auf gesetzliche Regelungen.

3. Verarbeitung von Beschäftigtendaten nach BDSG

Die Verarbeitung von Daten zu eigenen Geschäftszwecken unter Einschluss der Verarbeitung von Arbeitnehmerdaten richtete sich ursprünglich nach § 28 Abs. 1 BDSG.[49] Mit der BDSG-Novelle 2 wurde mit § 32 Abs. 1 BDSG eine Norm für die Verarbeitung von Beschäftigtendaten zu beschäftigungsvertraglichen Zwecken geschaffen.[50]

a) Abgrenzung der Anwendungsbereiche

Trotz Schaffung einer spezialgesetzlichen Regelung für die Datenverarbeitung in Beschäftigungsverhältnissen durch § 32 BDSG verbleibt ein Anwendungsbereich für § 28 Abs. 1 BDSG in der Beziehung des Beschäftigungsgebers zu seinen Beschäftigten.[51] Der Schluss, dass § 32 BDSG nur § 28 Abs. 1 S. 1 Nr. 1 BDSG verdränge und § 28 Abs. 1 BDSG im Übrigen insgesamt anwendbar bleibe[52], oder dass § 28 Abs. 1 S. 1 (Nr. 2) BDSG weiterhin anzuwenden wäre, wenn Daten des Beschäftigten bei Dritten erhoben werden,[53] ist zu weitgehend. Die Abgrenzung der Anwendungsbereiche hat sich an dem diesbezüglich klaren Wortlaut von § 32 Abs. 1 BDSG zu orientieren. Erfasst sind hiervon Datenverarbeitungen durch den Beschäftigungsgeber zu Zwecken des Beschäftigungsverhältnisses.[54] Liegen diese Voraussetzungen nicht vor, bleibt § 28 Abs. 1 BDSG anwendbar und ist im Verhältnis zwischen Beschäftigtem und Beschäftigungsgeber nur teilweise verdrängt.[55] Ein beschäftigungsvertraglicher Zweck ist insbesondere dann nicht gegeben, wenn sich Beschäftigungsgeber und Beschäftigter nicht in ihrer Eigenschaft als solche, sondern wie Dritte im Rechtsverkehr gegenüber stehen. Dies ist der Fall bei der Weitergabe von Beschäftigtendaten bei Unternehmenstransaktionen[56] oder wenn Beschäftigtendaten zum Anbieten oder zur Erbringung vertraglicher Leistungen genutzt werden, die keine unmittelbare Verbindung zum Beschäftigungsverhältnis haben. Die Nichtbeachtung von Compliance-Anforderungen durch Beschäftigte bedeutet regelmäßig einen Verstoß gegen beschäftigungsvertragliche Pflichten zur Rücksichtnahme, Loyalität und Schadensabwehr[57] und haben einen unmittelbaren Bezug zum Beschäftigungsverhältnis, so dass sich die Rechtmäßigkeit der Verarbeitung von Beschäftigtendaten im Rahmen von OLAP und Data Mining regelmäßig nach § 32 Abs. 1 BDSG bestimmt.

b) Datenverarbeitung gem. § 32 Abs. 1 BDSG

Aus § 32 Abs. 1 Satz 1 BDSG ergeben sich die allgemeinen Voraussetzungen der Datenverarbeitung im Rahmen von Beschäftigungsverhältnissen. Eine Sonderregel für die Datenverarbeitung zur Aufdeckung von Straftaten findet sich in § 32 Abs. 1 Satz 2 BDSG. Aus dem Wortlaut folgt hier, dass Datenverarbeitung zur Aufdeckung von Straftaten nur zulässig ist, wenn ein konkreter Verdacht gegenüber den betroffenen Be-

43 Siehe *Bizer* in Simitis, BDSG, § 3 Rz. 221; *Weichert* RDV 2003, 113 (119).
44 Siehe *Heinson et al.*, DuD 2010, 75 (78).
45 Vgl. BAG v. 14.9.1984, AP Nr. 9 zu § 87 BetrVG1972; *Kania* in Erfurter Kommentar zum Arbeitsrecht, § 87 BetrVG Rz. 55 ff. m.w.N.
46 *Kania* in Erfurter Kommentar zum Arbeitsrecht, § 75 BetrVG Rz. 9 f.
47 Dazu *Latendorf/Rademacher*, CR 1989, 1105.
48 Ausführlich *Sassenberg/Bamberg* DuD 2006, 226.
49 Hierzu *Schmidt*, BB 2009, 1295.
50 BGBl. I 2009, Nr. 54 v. 19.8.2009, 2814.
51 Von einer vollständigen Verdrängung des § 28 Abs. 1 BDSG im Anwendungsbereich des § 32 Abs. 1 S. 2 BDSG ausgehend, die Frage nach der Vorrangstellung von § 32 Abs. 1 S. 1 BDSG nicht *aufgreifend Bierekoven*, CR 2010, 203 (204 f.).
52 *Grentzenberger/Schreibauer/Schuppert*, K&R 2009, 535 (540); *Rolf/Rötting*, RDV 2009, 263 (264); *Schmidl*, ZJS 2009, 453 (455 f.); *Thüsing*, NZA 2009, 865 (869).
53 *Vogel/Glas*, DB 2009, 1747 (1750 f.).
54 BT-Drucks. 16/13657, 35; so auch *Erfurth*, NJOZ 2009, 2914 (2922); *Gola/Jaspers*, RDV 2009, 212 (213 f.); *Schmidt*, DuD 2010, 207 (208); *Selk*, RDV 2009, 254 (261 f.); *Wybitul*, BB 2009, 1582.
55 *Grentzenberger/Schreibauer/Schuppert*, K&R 2009, 535 (540); *Vogel/Glas*, DB 2009, 1747 (1750 f.).
56 Hierzu *Selk*, RDV 2009, 254.
57 *Schmidt*, Compliance in Kapitalgesellschaften, 2010, S. 167 ff.; *Schmidt*, BB 2009, 1295 (1298).

schäftigten besteht,[58] der auf tatsächliche Anhaltspunkte gestützt ist.[59]

Soweit OLAP und Data Mining nicht der Aufdeckung von strafrechtlich relevanten Verstößen dienen, bestimmt sich ihre datenschutzrechtliche Zulässigkeit nach § 32 Abs. 1 Satz 1 BDSG. Dies trifft insbesondere für die Verletzung vertraglicher Pflichten, Ordnungswidrigkeiten und ‚einfache' Rechtsverstöße zu. Sie mit Mitteln der Datenverarbeitung aufzuklären, ist in Beschäftigungsverhältnissen folglich zulässig, wenn es für die Entscheidung über die Begründung oder danach die Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Diesbezüglich ist auf die nebenvertragliche Pflicht von Beschäftigten zur Beachtung von Compliance-Standards und der Mitwirkung hieran hinzuweisen.[60] An der Kontrolle dieser Beschäftigtenpflicht hat der Beschäftigungsgeber ein hohes Interesse. Welche Maßnahmen hierbei zulässig sind und wie der Beschäftigungsgeber diese auszugestalten hat, richtet sich nach ihrer Verhältnismäßigkeit.

Diese Abgrenzung eignet sich indes nicht für Verfahren, bei denen Ermittlungen regelmäßig nicht an bekannt gewordene Verdachtsfälle anknüpfen, sondern auch dazu dienen, Anhaltspunkte für Verstöße erstmals zu generieren (Vorfeldermittlungen).[61] Sowohl OLAP als auch Data Mining fielen damit dem Grundsatz nach unter Satz 1. Gleichzeitig können aber bereits bei Vorfeldermittlungen Beweise für strafrechtlich relevante Verstöße anfallen, die zur Überführung von Tätern dienen können. Sie dienen deshalb potentiell beiden Zwecken. Der Ansatz in der Gesetzesbegründung, die Trennlinie zwischen Satz 1 und Satz 2 bei Prävention und Repression zu ziehen,[62] ist für Maßnahmen ungeeignet, die gleichzeitig präventiv und repressiv wirken. Bei der Abgrenzung sind zunächst zwei Fragen entscheidend: Welche Verdachtshärte erfordert Satz 2, und wie ist das Merkmal „zur Aufdeckung von Straftaten" auszulegen?

Ein Ansatz geht davon aus, die Zulässigkeit einer Datenverarbeitung auch dann an Satz 1 zu messen, wenn eine Ermittlung theoretisch geeignet ist strafrechtlich relevante Sachverhalte, unter Umständen nur als unbeabsichtigte Nebenfolge, zu liefern.[63] Die Datenverarbeitung zur Weiterverfolgung ermittelter Verdachtsfälle richtet sich nach diesem Ansatz nach Satz 2 und erfordert das Vorliegen eines durch tatsächliche Anhaltspunkte begründeten Verdachts. Der rechtliche Anknüpfungspunkt dieser Theorie liegt in der restriktiven Konkretisierung des Begriffs ‚Aufdeckung von Straftaten' i.S.d. § 32 Abs. 1 Satz 2 BDSG. Hierunter wird nicht der gesamte Prozess der Aufklärung von Straftaten und jede hierzu theoretisch geeignete Maßnahme verstanden, sondern nur die Überprüfung von ermittelten red flags. OLAP und Data Mining, die sich zur Ermittlung von strafrechtlichen und anderen Rechtsverstößen eignen, wären daher gem. § 32 Abs. 1 Satz 1 BDSG zu beurteilen und vorbehaltlich ihrer Verhältnismäßigkeit zulässig, während Maßnahmen die der Erhärtung von Verdachtsfällen im Hinblick auf strafrechtlich relevantes Verhalten dienen, an den strengeren Voraussetzungen gem. § 32 Abs. 1 Satz 2 BDSG zu messen wären. Letztere wären nur zulässig, wenn ein konkreter Verdacht gegenüber jedem betroffenen Beschäftigten besteht.

Ein alternativer Ansatz zur Begründung interessengerechter Ergebnisse nimmt die Anwendbarkeit von § 32 Abs. 1 Satz 2 BDSG unabhängig vom Willen der datenverarbeitenden Stelle an, wenn die Datenverarbeitung – auch als unbeabsichtigte Nebenfolge – dazu geeignet ist, zur Aufdeckung von Straftaten beizutragen.[64] Ist dies nicht der Fall, müssen die Voraussetzungen aus Satz 2 erst recht bei der Anwendung von Satz 1 gelten. Dies ergibt sich aus dem Verhältnismäßigkeitsgrundsatz. Hierfür spricht insbesondere, dass ein Eingriff in die informationelle Selbstbestimmung der Betroffenen zur Bekämpfung von Straftaten grundrechtlich leichter zu rechtfertigen ist, als ein präventiver Eingriff ohne Anlass.[65] An einen grundrechtlich leichter zu rechtfertigenden Eingriff aufgrund eines Erlaubnistatbestands (hier Satz 2) können jedoch keine höheren Anforderungen gestellt werden, als an schwerere Eingriffe, die durch Anwendung von Satz 1 gerechtfertigt werden sollen. Das Kriterium des Vorliegens tatsächlicher Anhaltspunkte ist deshalb (auch wenn es nicht als ungeschriebenes Tatbestandsmerkmal zu verstehen ist) bei der grundrechtskonformen Auslegung von § 32 Abs. 1 Satz 1 BDSG im Rahmen der Verhältnismäßigkeitsprüfung zu berücksichtigen.

Für die Rechtfertigung von OLAP und Data Mining ist daher auf tatbestandlicher Ebene letztlich nicht entscheidend, ob sich diese nach § 32 Abs. 1 Satz 1 oder Satz 2 BDSG richten, zumal eine Abgrenzung der Anwendungsbereiche nur schwer möglich ist. Die Frage der datenschutzrechtlichen Rechtfertigung wird vielmehr von den Wertungen des Verhältnismäßigkeitsprinzips bestimmt. Ausgehend vom Zweck der Untersuchung und der eingesetzten Technik muss durch Gestaltung des Verfahrens sichergestellt werden, dass nicht unverhältnismäßig in die Rechte der Betroffenen eingegriffen wird.

c) Datenverarbeitung gem. § 28 Abs. 1 BDSG

Neben Beschäftigtendaten werden bei OLAP und Data Mining regelmäßig, teilweise unbeabsichtigt, Daten von Dritten verarbeitet. Dies sind etwa Vertragsdaten aus Rechtsbeziehungen mit Kunden und Lieferanten, aber auch Daten aus alltäglichen Vorgängen wie Zugangskontrollsystemen. Diese werden von Betriebsvereinbarungen nicht erfasst, so dass als Maßstab der Rechtmäßigkeit allein die §§ 28 Abs. 1 Satz 1 Nr. 1 und Nr. 2 BDSG heranzuziehen sind.

Die Datenverarbeitung ist gem. § 28 Abs. 1 Satz 1 Nr. 1 BDSG gerechtfertigt, soweit sie zur Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich ist. Hiervon erfasst sind die zur Vertragszweckerreichung erforderlichen Daten, aber auch solche, die zur Durchsetzung eigener Rechte erforderlich sind.[66] Die Regelung geht von einem Interessengleichlauf bei der datenverarbeitenden Stelle und der betroffenen Person aus, so dass keine Abwägung vorzunehmen, sondern vielmehr nach objektiven Kriterien festzustellen ist, ob die Daten für die Durchführung des Vertrages erforderlich sind.[67] Eine Rechtfertigung von Ermittlungen mit

58 Zu Massenscreenings *Bergmann/Möhrle/Herb*, BDSG, § 32 Rz. 168.
59 *Wedde* in Däubler/Klebe/Wedde/Weichert, BDSG, § 32 Rz. 126 ff.; *Zöll* in Taeger/Gabel, BDSG, § 32 Rz. 43.
60 Hierzu *Schmidt*, BB 2009, 1295 (1298).
61 *Heinson et al.*, DuD 2010, 75 (76).
62 BT-Drucks. 16/13657, 21.
63 *Schmidt*, DuD 2010, S. 207 (210 f.); *Schmidt*, RDV 2009, S. 193 (195 f.); *Zöll* in Taeger/Gabel, BDSG, § 32 Rz. 40 f.
64 *Heinson et. al.*, DuD 2010, 75 (78 f.); *Mähner*, MMR 2010, 379 (381); *Erfurth*, NJOZ 2009, 2914 (2921), nach dem Satz 2 sogar eine Sperrwirkung entfalte; wohl auch *Bierekoven*, CR 2010, 203 (207 f.).
65 BAG v. 26.8.2008 – 1 ABR 16/07, NZA 2008, 1187.
66 So im Ergebnis auch *Erfurth*, NJOZ 2009, 2914 (2921).
67 *Taeger* in Taeger/Gabel, BDSG, § 28 Rz. 50.

OLAP und Data Mining gem. § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist denkbar, wenn es um die Feststellung der Gefährdung des Vertragszwecks durch Nebenpflichtverletzungen geht. Dies ist z.B. bei der Aufklärung gegen das Unternehmen gerichteter rechtswidriger Verhaltensweisen durch den Vertragspartner der Fall. Der Tatbestand ist jedoch restriktiv auszulegen und setzt eine enge Bindung der Datenverarbeitung an den Vertragszweck voraus. Nicht erfasst werden Datenverarbeitungen, die die Pflichterfüllung oder Rechtdurchsetzung lediglich unterstützen oder fördern.[68] Die Rechtfertigung gem. § 28 Abs. 1 Satz 1 Nr. 1 BDSG erfordert daher einen unmittelbarer Bezug zur Durchführung eines konkreten Vertragsverhältnisses. Ermittlungen werden jedoch häufig ohne unmittelbaren Anlass durchgeführt, so dass regelmäßig die Rechtfertigung gem. § 28 Abs. 1 Satz 1 Nr. 1 BDSG nicht anwendbar ist. Ausnahmen von diesem Grundsatz sind denkbar, soweit eine Maßnahme der Aufklärung des konkreten Verdachts einer Vertragspflichtverletzung dient.

Im Übrigen ist auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG abzustellen. Die Datenverarbeitung ist hiernach zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass entgegenstehende schutzwürdige Interessen des Betroffenen überwiegen. Ein berechtigtes Interesse des Unternehmens besteht, da der Einsatz von Compliance-Systemen eine Rechtspflicht im Unternehmen darstellt. § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist jedoch kein datenschutzrechtlicher Auffangtatbestand und daher eng auszulegen.[69] Die Anforderung, dass kein Grund zur Annahme überwiegender schutzwürdiger Interessen der Betroffenen vorliegen darf, erfordert von der verarbeitenden Stelle eine besonders gründliche Prüfung der entgegenstehenden Interessen, die das Abwehr- und Aufklärungsinteresse der Organisation und das grundrechtlich geschützte Interesse der Betroffenen zum Ausgleich bringt.[70] Aufgrund des weit formulierten Tatbestandes kommt für die Rechtfertigung von Eingriffen daher der Verhältnismäßigkeitsprüfung entscheidende Bedeutung zu.

IV. Rechtskonformer Einsatz von OLAP und Data Mining

Bei allen beschriebenen Rechtfertigungsgründen erweist sich die Rechtmäßigkeit einer konkreten Anwendung von OLAP und Data Mining letztlich anhand ihrer Verhältnismäßigkeit. Dies ergibt sich für Betriebsvereinbarungen aus § 75 Abs. 2 BetrVG. Innerhalb des BDSG folgt es bei § 32 Abs. 1 Satz 2 BDSG und § 28 Abs. 1 Satz 1 Nr. 2 BDSG aus ihren Abwägungsklauseln. Für die Datenverarbeitung gem. § 32 Abs. 1 Satz 1 BDSG[71] und § 28 Abs. 1 Satz 1 Nr. 1 BDSG[72] ist wegen der Verwendung unbestimmter Rechtsbegriffe im Wege der Drittwirkung bei der Konkretisierung der jeweiligen Eingriffsermächtigungen die informationelle Selbstbestimmung zu berücksichtigen, was ebenfalls eine Verhältnismäßigkeitsprüfung auslöst[73]:

1. Verarbeitungszweck

Bezogen auf das mit der Ermittlung verfolgte Ziel (den Untersuchungszweck) muss die gewählte Untersuchungsmethode abstrakt in der Lage sein, die erstrebten Ergebnisse zu liefern. Unzulässig sind damit jede Datenverarbeitung die im Hinblick auf den angestrebten Zweck offensichtlich ungeeignet sind.

2. Erforderlichkeit

Die Datenverarbeitung muss auch erforderlich sein. Bezogen auf den Verarbeitungszweck darf kein gleich effektives, aber weniger eingreifendes Mittel zur Verfügung stehen. So wird sichergestellt, dass nur solche Daten verarbeitet werden, die zur Erfüllung des Zwecks notwendig sind.[74] Sofern Erforderlichkeit als ausdrückliches Tatbestandsmerkmal in der jeweiligen Erlaubnisnorm vorkommt, ist dies als Hinweis auf den entsprechenden Schritt in der Verhältnismäßigkeitsprüfung zu verstehen.[75] Die Überprüfung Unschuldiger[76] und die Nutzung nicht relevanter Datenbestände ist daher zur Senkung der Eingriffsintensität technisch-organisatorisch zu vermeiden. Dies kann praktisch umgesetzt werden, indem die Datenbasis schon vor der Untersuchung etwa auf Daten aus korruptionsanfälligen Geschäftsbereichen eingeschränkt wird.

3. Angemessenheit

Die Datenverarbeitung muss zudem angemessen sein. Es gilt daher die rechtlichen Interessen der Betroffenen mit denen der verarbeitenden Stelle abzuwägen. Dabei kommt es auf die Voraussetzungen für die Einleitung der Maßnahme, die Zahl der Betroffenen und die Intensität der Grundrechtsbeeinträchtigung an.[77] Datenverarbeitende Stellen müssen im Einzelfall das rechtliche Interesse an einer Ermittlung mit OLAP und Data Mining mit den entgegenstehenden Interessen der Betroffenen zu einem schonenden Ausgleich bringen. Vor der Datenverarbeitung ist zunächst zu prüfen, ob das gewünschte Ergebnis nicht auch mit anderen Mitteln zu erreichen ist. Gerade im Bereich Fraud Prevention und Korruptionsbekämpfung gibt es dafür eine Vielzahl an technisch-organisatorischen Maßnahmen, bei denen keine Datenverarbeitung notwendig ist. Dazu gehören etwa das Vier-Augen-Prinzip und Sicherheitsrichtlinien.[78] Zwar wird dies häufig nicht ausreichen, um Compliance-Risiken effektiv zu begegnen. Diese Mittel können aber immerhin dazu beitragen, dass OLAP und Data Mining weniger häufig und regelmäßig mit geringerer Eingriffstiefe notwendig werden. Bleibt eine Untersuchung notwendig, ist sie nach Art und Umfang so zu begrenzen, dass sie nur so tief wie nötig in die Rechte der Betroffenen eingreift. Als Mittel kommen hier trotz der beschriebenen Schwächen und Re-Identifikationstechniken zunächst Anonymisierung und Pseudonymisierung in Frage.

68 *Taeger* in Taeger/Gabel, BDSG, § 28 Rz. 47 f.; *Simitis* in Simitis, BDSG, § 28 Rz. 133.

69 *Taeger* in Taeger/Gabel, BDSG, § 28 Rz. 62; *Wedde* in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rz. 52.

70 *Simitis* in Simitis, BDSG, § 28 Rz. 161 ff.

71 *Gola/Jaspers*, RDV 2009, 212 (213); *Schmidt*, RDV 2009, 193 (198); *Thüsing*, NZA 2009, 865 (868); *Wybitul*, BB 2009, 1582.

72 *Albers*, ZRFC 2009, 150 (154); *Busse* in Besgen/Prinz, Neue Medien und Arbeitsrecht, 2006, § 10 Rz. 33; *Kock/Francke*, ArbRB 2009, 110 (111).

73 BVerfG v. 23.10.2006 – 1 BvR 2027/02, MMR 2007, 93; v. 19.10.1993 – 1 BvR 567/89, 1 BvR 1044/89, BVerfGE 89, 214 (234).

74 So auch *Mähner*, MMR 2010, 379 (380); hierzu auch *Deutsch/Diller*, DB 2009, 1462 (1463), wobei nicht eindeutig von der Frage nach dem legitimen Verarbeitungszweck abgegrenzt wird.

75 Anders *Wybitul*, BB 2010, 1085 (1086), nachdem das Merkmal Erforderlichkeit eine weitere, rekursive Verhältnismäßigkeitsprüfung auslösen solle, innerhalb derer erneut eine „Erforderlichkeit im engeren Sinne" zu prüfen sei.

76 BVerfG v. 4.4.2006 – 1 BvR 518/02, BVerfGE 115, 320 (347) m.w.N. = CR 2006, 594 m. Anm. *Schmitz*; BAG v. 26.8.2008 – 1 ABR 16/07, NZA 2008, 1187 (1192); *Kock/Francke*, NZA 2009, 646 (648).

77 Siehe BAG v. 29.6.2004 – 1 ABR 21/03, NZA 2004, S. 1278.

78 *Heinson et al.*, DuD 2010, 75 (79) m.w.N.

Auch echte Pseudonymisierung ist jedoch kein Allheilmittel zur Rechtfertigung von Ermittlungen mit OLAP und Data Mining, da trotz einer Verminderung des Personenbezugs während der Überprüfung eine generelle Verdächtigung einer großen Gruppe „pseudonym" Unschuldiger stattfindet, solange eine Rück-Zuordnung mit der Zuordnungsregel möglich ist. Dies gilt auch, wenn gewährleistet ist, dass diese nur im Trefferfall erfolgt. Eine Grundregel ist, dass kein permanenter Überwachungsdruck auf die Beschäftigten erzeugt werden darf.[79] Daher kann auch Pseudonymisierung nur ein Baustein zur Verminderung der Eingriffsintensität sein und muss stets mit der Beschränkung der Untersuchung auf potentiell verdächtige Personengruppen einhergehen. Nur so wird erreicht, dass die Zahl der Betroffenen möglichst gering ist. So wird es in vielen Fällen etwa genügen, Daten aus korruptionsanfälligen Unternehmensbereichen zu verarbeiten. Keinesfalls dürfen Daten mit Zusatzwissen aus umfangreichen Drittquellen angereichert werden. Zwar sind die besten Ergebnisse der Auswertung bei möglichst umfangreichem Datenbestand zu erwarten. Mit der Menge der Daten erhöht sich aber auch die Zahl der Betroffenen und damit die Streubreite des Eingriffs in die Informationelle Selbstbestimmung, dessen Einschränkung in diesen Fällen durch Arbeitgeberinteressen nicht mehr zu rechtfertigen ist.[80]

79 BAG v. 29.6.2004 – 1 ABR 21/03, NZA 2004, S. 1278 (1281); BVerfG v. 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, BVerfGE 65, 1 (42 f.); *Schmidt*, RDV 2009, 193 (199); *Kock/Francke*, NZA 2009, 646 (648); *Kratz/Gubbels*, NZA 2009, 652 (654).

80 Vgl. *Weichert*, RDV 2003, 113 (114).

V. Fazit

Gesellschaftsrechtliche Wertungen verpflichten die Geschäftsleitungsorgane von Kapitalgesellschaften zur Herstellung von Compliance. Besonders in großen Unternehmensstrukturen liegt es nahe, auf IT-gestützte Verfahren zurückzugreifen. Diese ermöglichen es, Unternehmensdaten effizient, effektiv und wirtschaftlich auf Verstöße gegen Compliance-Standards zu untersuchen. Damit diese Maßnahmen jedoch nicht selbst zum Compliance-Risiko werden, gilt es ihren Einsatz datenschutzkonform zu gestalten. Gelingt es dabei, Datenbestände zu anonymisieren, so ist das Datenschutzrecht nicht mehr anwendbar und es bestehen keine Beschränkungen der Verarbeitungsbefugnisse. Anonymisierung stehen hoher technischer Aufwand, leichte Re-Identifikation und geringerer Ergebniswert entgegen. Pseudonymisierung hat potentiell höheren Ergebniswert, leidet aber unter denselben sonstigen Schwächen wie Anonymisierung und hat zusätzlich das Problem des datenschutzkonformen Umgangs mit den Zuordnungsregeln. Es bleibt letztlich nur die Möglichkeit, Ermittlungen mit OLAP und Data Mining im Rahmen der datenschutzrechtlichen Zulässigkeit durchzuführen. Um Maßnahmen so wenig eingriffsintensiv wie möglich zu gestalten, gilt es insbesondere Alternativen zu OLAP und Data Mining zu erwägen und zudem trotz möglichst effektiver Pseudonymisierung oder Anonymisierung die Gruppe der betroffenen Personen im Vorfeld auf potentiell Verdächtige zu begrenzen. Diese Anforderungen ergeben sich aus dem Grundsatz der Verhältnismäßigkeit, dem aufgrund der tatbestandlich unklar gefassten Erlaubnistatbestände in § 28 Abs. 1 S. 1 BDSG und § 32 Abs. 1 BDSG weiterhin die entscheidende Bedeutung zukommt.