Deggendorfer Forum zur
digitalen Datenanalyse e.V. (Hrsg.)

Compliance in digitaler Prüfung und Revision

Technische Möglichkeiten – rechtliche Grenzen

ESV
ERICH SCHMIDT VERLAG

Compliance in digitaler Prüfung und Revision

Technische Möglichkeiten – rechtliche Grenzen

Herausgegeben vom

Deggendorfer Forum zur
digitalen Datenanalyse e. V.

Mit Beiträgen von

Anke Giegandt
Prof. Dr. Georg Herde
Prof. Andreas Kohl
Prof. Dr. Norbert Nolte
Evelyn Schmidt
Ernst Rudolf Töller

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation
in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet über
http://dnb.d-nb.de abrufbar.

Weitere Informationen zu diesem Titel finden Sie im Internet unter
ESV.info/978 3 503 14137 1

Gedrucktes Werk: ISBN 978 3 503 14137 1
eBook: ISBN 978 3 503 14138 8

Dieses Papier erfüllt die Frankfurter Forderungen
der Deutschen Nationalbibliothek und der Gesellschaft
für das Buch bezüglich der Alterungsbeständigkeit und
entspricht sowohl den strengen Bestimmungen der US Norm
Ansi/Niso Z 39.48-1992 als auch der ISO-Norm 9706.

Druck und Bindung: Hubert & Co., Göttingen

Vorwort

Das Einhalten der rechtlichen Richtlinien und Ausnutzen der technischen Möglichkeiten der Compliance in Bezug auf Prüfung und Revision wird im heutigen, rasanten Zeitalter des technischen Fortschritts nicht nur für Großunternehmen immer wichtiger. Auch für kleine und mittelständische Unternehmen werden Investitionen hinsichtlich dieser Thematik erforderlich, um zukünftig in der Wirtschaft mithalten zu können.

Prof. Dr. Norbert Nolte, Rechtsanwalt und Partner in der Sozietät Freshfields Bruckhaus Deringer in Köln, stellt in seinem Beitrag die Leitlinien für die Interne Revision vor. Hierbei geht er auf die Schwierigkeiten ein, gute Arbeit abzuleisten und gleichzeitig die gesetzlichen Vorgaben erfüllen zu können. Als Grenzen der Revisionstätigkeit werden der Beschäftigtendatenschutz und das Fernmeldegeheimnis aufgezeigt.

In ihrem Beitrag „Datenschutz bei der Analyse von Massendaten in Revisionsprozessen" beschreibt Anke Giegandt von der Internen Revision der Bosch Siemens Hausgeräte GmbH zunächst die Ausgangslage. Im weiteren Verlauf ihres Beitrages geht sie auf die Rahmenbedingungen der Revision ein. Aufgabenbereiche der Internen Revision, die Unterscheidung von Standardrevision und Sonderuntersuchung und Gesetzesgrundlagen wie zum Beispiel das Bundesdatenschutzgesetz sind ihre Themen. Zusätzlich legt Frau Giegandt das Datenschutzkonzept bei Datenanalysen der Internen Revision dar und verdeutlicht dieses anhand von Fallbeispielen.

Über die Thematik der Korruptionsverhinderung und des Datenschutzes aus Sicht der Internen Revision berichtet Frau Evelyn Schmidt. Sie leitet beim Deutschen Institut für Interne Revision e.V. die Grundsatzabteilung und ist Geschäftsführerin der DIIR Dienstleistungen GmbH. Nicht nur die Kontrolle der Unternehmensprozesse und die Haftung der Unternehmungsleitung sind Bestandteile ihres Beitrages, auch auf den Problembereich der Datenanalysen geht Frau Schmidt ein und bietet Lösungsansätze an. Lösungsvorschläge und Forderungen des DIIR zum Beschäftigtendatenschutz runden ihren Beitrag zum 7. Tagungsband des DFDDA ab.

Die Ergebnisse einer umfangreichen Umfrage aus dem Jahre 2011 zur Akzeptanz der digitalen Prüfungsunterstützung werden von dem Kollegen Prof. Andreas Kohl und mir in einem Beitrag vorgestellt. An dieser Stelle noch einmal herzlichen Dank für die große Unterstützung der Teilnehmer im Bereich der prüfenden Berufe.

Im abschließenden Beitrag versuchen Ernst Rudolf Töller von der BDO AG und ich die Anforderungen und Parameter von zukunftsorientierter Analysesoftware

herauszuarbeiten. Hierbei werden die Verwendbarkeit von Analysesoftware, mathematische Modelle und die technischen Anforderungen an Analysesoftware auf den Prüfstand gestellt.

Die Erstellung eines Tagungsbandes ist wie im jedem Jahr ein Kraftakt, der ohne die Referenten und viele helfende Hände nicht möglich gewesen wäre. Allen Mitwirkenden möchte ich im Namen des Vereins und persönlich recht herzlich danken für ihr großartiges Engagement und die Mühe, mit der sie ihr Wissen und ihre Erfahrungen in diesen Tagungsband eingebracht haben.

Mein Dank richtet sich auch an die Kooperationspartner: ACL Ltd., AM:DataConsult GmbH, BDO AG, dab: GmbH, DATEV eG, IBS Schreiber GmbH und die HDU Deggendorf, die das Forum in Hamburg unterstützt haben.
Für die Anpassung der schriftlichen Beiträge an ein einheitliches Layout bedanke ich mich bei Herrn Beck von der Hochschule Deggendorf sowie bei beim Erich Schmidt Verlag.

Georg Herde Deggendorf, im Mai 2012

Inhaltsverzeichnis

Datenanalyse und Datenschutz – Leitlinien für die interne Revision

Prof. Dr. Norbert Nolte

Rechtsanwalt und Partner
in der Sozietät
Freshfields Bruckhaus Deringer

Im Zollhafen 24
50678 Köln

norbert.nolte@freshfields.com

www.freshfields.com

Aus: Deggendorfer Forum zur digitalen Datenanalyse e. V. (Hrsg.), Compliance in digitaler Prüfung und Revision

Inhaltsübersicht

1 Einführung

Die Interne Revision befindet sich im Konflikt, sie steht „mit einem Fuß im Strafrecht und mit dem anderen Fuß im Ordnungswidrigkeitenrecht des Beschäftigtendatenschutzes.“ [1]
Einerseits hat die Interne Revision die Aufgabe, die Unternehmenstätigkeit auf Übereinstimmung mit den gesetzlichen Vorgaben zu überprüfen. Hierzu ist sie im Rahmen ihrer Compliance-Verantwortung[2] verpflichtet. Im Einzelfall kann dies sogar zu einer strafrechtlichen (Mit-)verantwortung für Gesetzesverstöße führen[3]. Zudem kommt bei mangelhafter Organisation der Überprüfung eine Haftung des Unternehmens nach § 130 OWiG in Betracht[4]. Die in Frage stehenden Risiken sind keine Bagatellen: es geht um die Bekämpfung von Straftaten wie Korruption, Betrug, Untreue, Geldwäsche, von Insolvenz-, Urkunds- und Steuerdelikten, von bilanzrechtlichen Straftaten sowie von Kartellverstößen[5].
Andererseits ist die Revision in der Wahl ihrer Mittel erheblich eingeschränkt. Gegenüber Beschäftigten des Unternehmens ist sie an die Wahrung von Persönlichkeitsrechten, namentlich das Recht auf informationelle Selbstbestimmung, sowie an das Datenschutzrecht gebunden. Verletzt sie diesbezüglich ihre Pflichten, verursacht sie unter Umständen eine Schadensersatzhaftung des Unternehmens[6], handelt ordnungswidrig[7] oder setzt sich sogar strafrechtlichen Risiken[8] aus.

Nachdem jahrelang die Diskussion um Wirtschaftsstraftaten Öffentlichkeit und Justiz geprägt hatte[9], verlagerte sich die Aufmerksamkeit nach den sogenannten Datenschutzskandalen bei Lidl, Deutsche Telekom, Deutsche Bahn etc. auf die Frage nach der datenschutzkonformen Ausgestaltung der unternehmensinternen Präventions- und Verfolgungsmaßnahmen .
Die Diskussion findet vor dem Hintergrund einer äußerst unklaren Rechtslage statt. Datenschutzrecht ist vielfach kein tatbestandliches Subsumtionsrecht, sondern Ab-

1 So Schmitt-Rolfes, AuA 2010, 8, 10; s. auch Zöll, BB 2010, 2310 f.; Barton, jurisPR-StrafR 16/2010, Anm. 1: *„Kollisionslage“* und *„strafrechtliches Haftungsrisiko“*.

2 Zur Compliance-Pflicht: Schmidt, DuD 2010, 207, 210; zur Garantenstellung des Datenschutzbeauftragten: Barton, a.a.O.; zum Compliance Officer: Kamp/Körffer, RDV 2010, 72.

3 BGHSt 54, 44 (Garantenpflicht des Leiters der Innenrevision).

4 Schmidt, DuD 2010, 207, 210.

5 Lützeler/Bissels, AuA 2010, 14, 17; Straf- und Bußgeldnormen: §§ 331ff., 263, 266, 261, 267, 283 StGB; § 370 AO; § 331 HGB; § 81 GWB.

6 § 7 BDSG.

7 § 43 BDSG.

8 § 44 BDSG, §§ 202a, 206 StGB; ausführlich: Schuster, ZIS 2010, 68.

9 Süddeutsche.de vom 13.03.2007: http://www.sueddeutsche.de/wirtschaft/bestechungsskandal-bei-siemens-auftraege-brachten-millionen-euro-1.810732 und vom 20.11.2003: http://www.sueddeutsche.de/politik/muellprozess-auftakt-wirtschaftskrimi-aus-koeln-1.298850.

wägungsrecht[10]. Es kommt also nicht nur darauf an, bestimmte vom Gesetzgeber vorgegebene Voraussetzungen zu erfüllen. Vielmehr sind die Interessen der Beteiligten in Einklang zu bringen, eben gegeneinander abzuwägen. Für diese Abwägung im Rahmen der Erforderlichkeits- und Verhältnismäßigkeitsprüfung (i. e. S.) fehlt es dem Praktiker oft an klaren Vorgaben. Die Billigung der Abwägungsergebnisse durch Justiz und Verwaltungsbehörde scheint deshalb wenig berechenbar.

Die Verunsicherung ist nachvollziehbar, aber im Ergebnis unbegründet. Denn trotz der Schwierigkeiten und Unsicherheiten gibt es fast immer einen Weg, die Datenanalyse effizient und dennoch gesetzeskonform zu gestalten.

Der eigentliche Konflikt der Internen Revision wurzelt in §32 BDSG. Die Norm wurde nach den erwähnten sogenannten Datenschutzskandalen im Herbst 2009 in einer Eilaktion des Gesetzgebers in Kraft gesetzt[11]. Sie sollte Klarheit zum Beschäftigtendatenschutz bringen. Von vielen als Schnellschuss kritisiert[12], hat die Norm in der Tat aber eher zur Rechtsunsicherheit beigetragen und neue Fragen aufgeworfen.

Eine schnelle Lösung in Form eines systematisch geregelten Beschäftigtendatenschutzes ist derzeit wohl nicht in Sicht. Während der deutsche Gesetzgeber seit 2009 an einem weiteren Regelungskomplex zum Beschäftigtendatenschutz arbeitete, hat die Europäische Kommission im Januar 2012 den Entwurf einer Datenschutz-Grundverordnung[13] veröffentlicht. Dieser Entwurf würde mitgliedstaatliche Datenschutzgesetze auf die Vorgaben dieser Verordnung verhaften (Vollharmonisierung). Zudem hat der EuGH im November 2011 zur europäischen Datenschutzrichtlinie[14] entschieden[15], dass nationale Gesetze keine zusätzlichen Bedingungen für die Verarbeitung personenbezogener Arbeitnehmerdaten vorsehen dürfen. Der deutsche Gesetzgeber wird die europäische Entwicklung nun höchstwahrscheinlich abwarten. Mit einer schnellen Einführung neuer nationaler Regelungen ist daher nicht mehr zu rechnen[16].

---

10 Schneider, 2010, 1201, 1205.

11 Bundesgesetzblatt Teil I, 2009, Nr. 54, S. 2814-2820 vom 19.08.2009.

12 Schmitt-Rolfes, AuA 2010, 71, mit Nachweisen.

13 KOM(2012) 11 vom 25.01.2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF.

14 Richtlinie 95/46/EG vom 24.10.1995, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:DE:PDF.

15 EuGH, Urteil vom 24.11.2011 - C-468/10, C-469/10 (Tribunal Supremo) mit Anmerkung Fleddermann in ArbRAktuell 2011, 661.

16 Straube/Klagges in ArbRAktuell 2012, 81: *„Beschäftigtendatenschutzgesetz: Wiedervorlage in vier Jahren?“*

2 Der Beschäftigtendatenschutz als Grenze der Revisionstätigkeit (§ 32 BDSG)

Aktuell regelt also vornehmlich § 32 BDSG die Frage, welche Ermittlungsmaßnahmen der Internen Revision mit Bezug zum Beschäftigten zulässig sind.
Im Folgenden sollen hierzu Lösungsansätze vorgestellt werden.

2.1 Verfassungsrechtlicher Hintergrund

Das BDSG zieht seine Rechtfertigung aus dem Schutz des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1, 1 Abs. 1 GG), genauer dem vom BVerfG daraus abgeleiteten Recht auf informationelle Selbstbestimmung[17]. Danach hat jeder Bürger das Bestimmungsrecht über die ihn betreffenden Daten. In dieses Recht darf nur aufgrund eines Gesetzes eingegriffen werden und der Staat muss dieses Recht auch vor Eingriffen Privater schützen.
Mit dem BDSG kommt der Staat seinem Schutzauftrag nach, indem er die Verarbeitung personenbezogener Daten durch Private, die als grundsätzlich notwendig erkannt ist, besonderen gesetzlichen Vorgaben unterwirft. Damit trägt er sowohl dem informationellen Selbstbestimmungsrecht der Betroffenen (Art. 2 Abs. 1, 1 Abs. 1 GG) als auch der unternehmerischen Entscheidungsfreiheit der datenverarbeitenden Stellen (Art. 12 Abs. 1 GG)[18] Rechnung.
Vor diesem Hintergrund sind Eingriffe in das informationelle Selbstbestimmungsrecht durch datenverarbeitende Stellen, also auch solche durch die Tätigkeit der Internen Revision, zu beurteilen.

2.2 Datenschutzrechtlicher Hintergrund

Diese Abwägung zwischen informationeller Selbstbestimmung und unternehmerischer Entscheidungsfreiheit erfolgt im BDSG dergestalt, dass für jeden Eingriff entweder eine Einwilligung des Betroffenen bzw. Beschäftigten oder eine gesetzliche Erlaubnis gefordert wird (§ 4 BDSG). § 32 BDSG kann eine solche gesetzliche Erlaubnis für datenschutzrechtliche Eingriffe sein, soweit keine wirksame Einwilligung des Betroffenen vorliegt.

2.2.1 Einwilligung im Beschäftigtendatenschutz

Die herrschende Meinung in Rechtsprechung und Literatur geht davon aus, dass Arbeitnehmer aufgrund der Über-/Unterordnungssituation nicht wirksam in den

---

17 BVerfGE 65, 1 – „Volkszählungsurteil“ vom 15.12.1983, Gola/Schomerus, BDSG, 10. Aufl. 2010, § 1. Rn. 6; Simitis, BDSG, 7. Aufl. 2011, § 1, Rn. 23 ff., 26; siehe auch Art. 8 Europäische Grundrechte-Charta (GRCh).

18 Vgl. Art. 16, 17 GRCh (unternehmerische Freiheit).

datenschutzrechtlichen Eingriff einwilligen können, weil es an der erforderlichen Freiwilligkeit der Erklärung mangele.
Die Voraussetzungen einer Einwilligung regelt u.a. § 4a BDSG. Eine Einwilligung muss danach freiwillig erteilt werden. Aufgrund der „typischen Machtasymmetrie“[19] bzw. des „sozialen Machtgefälles“[20] in Beschäftigungsverhältnissen wird überwiegend angenommen, dass es bei der Einwilligung eines Arbeitnehmers in (erhebliche) Eingriffe des Arbeitgebers in seine Persönlichkeitsrechte regelmäßig an der Freiwilligkeit fehlen wird. Schon deshalb sei die Einwilligung des Arbeitnehmers nicht wirksam möglich[21]. Die zwei von *Brink/Schmidt*[22] exemplarisch aufgeworfenen Fragen verdeutlichen dies: Lässt der Arbeitgeber dem Arbeitnehmer wirklich die Wahl, ob dieser an Maßnahmen der Revision teilnehmen will? Und wie würde der Arbeitgeber auf eine Weigerung reagieren?
Dazu kommt, dass der Entwurf der europäischen Datenschutz-Grundverordnung[23] in Art. 7 Abs. 4 eine Einwilligung für nicht wirksam erklärt, wenn zwischen Verantwortlichem und Betroffenem ein „erhebliches Ungleichgewicht“ besteht. In Ziffer 34 der Gründe heißt es *„zum Beispiel dann, wenn personenbezogene Daten von Arbeitnehmern durch den Arbeitgeber im Rahmen von Beschäftigungsverhältnissen verarbeitet werden.“* Ähnliche Regelungen finden sich auch in den deutschen Entwürfen zu einem neuen Beschäftigtendatenschutz.

2.2.2 Betriebsvereinbarungen regelmäßig keine taugliche Alternative

Auch Betriebsvereinbarungen (§ 77 BetrVG) geben dem Unternehmen nicht die nötige Sicherheit. Sie gelten zwar unmittelbar und zwingend (§ 77 Abs. 4 BetrVG) und damit als andere Rechtsvorschrift im Sinne von § 4 BDSG[24]. Unternehmen können damit nach herrschender Meinung auch Fragen des Datenschutzes regeln und theoretisch sogar die Vorgaben des BDSG unterschreiten[25]. Allerdings schreibt § 75 Abs. 2 BetrVG vor, dass Arbeitgeber und Betriebsrat die freie Entfaltung der Persönlichkeit der Arbeitnehmer zu schützen und zu fördern haben. Damit darf zwar mit einer Betriebsvereinbarung auch zu Ungunsten der Arbeitnehmer vom BDSG abgewichen werden, den Grundsätzen des Persönlichkeitsschutzes ist aber Rechnung zu tragen[26].

---

19 Schneider, NZG 2010, 1201, 1204.
20 Brink/Schmidt, MMR 2010, 592, 593.
21 Schneider, a.a.O.; Brink/Schmidt, a.a.O.; beide mit Nachweisen.
22 Brink/Schmidt, a.a.O.
23 Siehe oben, Fußnote 13.
24 Gola/Schomerus, BDSG, 10. Aufl. 2010, § 4, Rn. 10; Sokol in Simitis, BDSG, 7. Aufl. 2011, § 4, Rn. 11, 14ff.
25 Sokol in Simitis, a.a.O., Rn. 16.
26 BAG Beschluss 1 ABR 48/84 vom 27.05.1986 = BAGE 52, 88.

Aus dieser Voraussetzung schließt ein Teil der Literatur, dass Betriebsvereinbarungen das Schutzniveau des BDSG schon jetzt nicht unterschreiten dürfen[27], weil die Persönlichkeitsrechte zu schützen und zu fördern sind. Mit dem Entwurf des neuen Beschäftigtendatenschutzes, träte er so in Kraft, würde dieser Streit obsolet[28]. Darin heißt es in § 32l Abs. 5 BDSG-E[29] *„Von den Vorschriften dieses Unterabschnitts darf nicht zu Ungunsten der Beschäftigten abgewichen werden."*
Abweichungen von den Vorgaben des BDSG in Betriebsvereinbarungen zu Lasten der Arbeitnehmer sind, wenn überhaupt, nur möglich, soweit sie mit der Schutzpflicht von Arbeitgeber und Betriebsrat vereinbar sind. Das bedeutet, soweit die Eingriffe aufgrund überwiegender Allgemeininteressen erforderlich sind und in der Betriebsvereinbarung die Einzelinteressen der Arbeitnehmer berücksichtigt werden, kann von den Vorgaben des BDSG abgewichen werden. Die Berücksichtigung der Einzelinteressen der Arbeitnehmer nehmen allerdings auch die Autoren, die ein Abweichen vom BDSG für zulässig halten, vor, indem sie auf die Abwägung aus § 32 BDSG zurückgreifen. § 32 dient also insoweit als Maßstab[30].
Schon diese kurze Darstellung zeigt, dass Betriebsvereinbarungen bei der derzeitigen Rechtslage regelmäßig nicht die nötige Sicherheit geben können, die für die gesetzeskonforme Tätigkeit der Internen Revision bei Datenanalysen nötig ist.

2.2.3 Anwendungsbereich des § 32 BDSG

Als Rechtsgrundlage für Datenanalysen der Internen Revision kommt in erster Linie die gesetzliche Erlaubnis aus § 32 BDSG in Betracht.
§ 32 Abs. 1 S. 1 BDSG bestimmt, dass personenbezogene Daten (§ 3 Abs. 1 BDSG) eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden dürfen, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.
§ 32 Abs. 1 S. 2 BDSG wiederum regelt, dass zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden dürfen, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

---

27 Heinson/Schmidt, CR 2010, 540, 544; Heinson, BB 2010, 3084, 3085; Brink/Schmidt, MMR 2010, 592, 593.

28 Heinson, BB, 2010, 3084, 3085.

29 Entwurf des BMI vom 25.08.2010.

30 Erfurth, DB 2011, 1275, 1277, der die gesamte Thematik anschaulich aufarbeitet und zum Ergebnis kommt, dass sich in einer BV kaum Regelungen werden treffen lassen können, die von § 32 abweichen.

§ 32 Abs. 2 BDSG erweitert den Anwendungsbereich des § 32 Abs. 1 BDSG auf nicht digitalisierte Daten.

Die Vorschrift erfasst alle Beschäftigten im Sinne von §3 Abs. 11 BDSG, also neben Arbeitnehmern unter anderem auch Auszubildende, Scheinselbständige, Beamte, Richter, Soldaten sowie Bewerber und Personen, deren Beschäftigungsverhältnis beendet ist.

Wie die Formulierung *„personenbezogene Daten eines Beschäftigten […] für Zwecke des Beschäftigungsverhältnisses“* verstanden werden muss, ist umstritten[31]. In das BDSG eingefügt am 14. August 2009, tritt § 32 BDSG auf dem Terrain des Beschäftigtendatenschutzes – jedenfalls zum Teil – an die Stelle des § 28 Abs. 1 S. 1 Nr. 1 BDSG. Für jeden Eingriff ist ein Zweck notwendig, für dessen Erreichung die Maßnahme erforderlich sein muss. Bevor § 32 in das BDSG eingefügt wurde, kamen als legitime Zwecke entweder ein Schuldverhältnis (sprich: Beschäftigungsverhältnis) oder berechtigte Interessen des Arbeitgebers, § 28 Abs. 1 S. 1 Nr. 1 oder Nr. 2 BDSG in Betracht. Unstreitig ist, dass der neue § 32 BDSG den Zweck des Schuldverhältnisses auf den des Beschäftigungsverhältnisses verdichtet und damit § 28 Abs. 1 S. 1 Nr. 1 BDSG insoweit nicht mehr anwendbar ist. Umstritten ist jedoch, ob noch Raum für andere Zwecke bleibt, also nach § 28 Abs. 1 S. 1 Nr. 2 BDSG auch weiterhin auf berechtigte Interessen des Arbeitgebers abgestellt werden kann, oder ob § 32 BDSG abschließend alles regelt, was im Zusammenhang mit dem Beschäftigungsverhältnis steht.

Die strengste Ansicht sieht von § 32 BDSG alle personenbezogenen Daten erfasst, die irgendeinen Bezug zum Arbeitnehmer haben. Danach wären nur personenbezogene Daten ausgenommen, die nicht im Zusammenhang mit der Beschäftigung stehen[32]. Weil auch aus reinen Buchungs-, Rechnungs- oder Lieferdaten schon mit einer User-ID ein Bezug zum Mitarbeiter hergestellt werden kann, würden nahezu sämtliche Geschäftsdaten (z.B. SAP-Daten) § 32 BDSG unterfallen. Selbst Massendatenanalysen, die schon vom Analysezweck her nicht auf einzelne Mitarbeiter abzielen, können Beschäftigtendaten enthalten[33]. Da solche Daten aber nicht zum Zweck des Beschäftigungsverhältnisses erhoben oder verarbeitet werden, könnten diese Maßnahmen nach dieser strengen Ansicht vom ausschließlich anzuwendenden § 32 BDSG nicht gerechtfertigt werden, sie wären unzulässig.

Dieses Beispiel zeigt schon, dass der Gesetzgeber nicht gewollt haben kann, alle Maßnahmen des Arbeitgebers an § 32 BDSG zu messen. Vorzugswürdig ist es, darauf abzustellen, wofür die personenbezogenen Daten des Beschäftigten genutzt werden sollen. Sollen sie für Zwecke des Beschäftigungsverhältnisses genutzt werden, so ist § 32 BDSG zu beachten. Für alle anderen Fälle kommt es auf § 28 Abs. 1 S. 1 Nr. 2 BDSG an, es muss also ein berechtigtes Interesse des Arbeitgebers vor-

---

31 Gola/Schomerus, BDSG, 10. Aufl. 2010, § 32, Rn. 31f.; Seifert in Simitis, BDSG, 7. Aufl. 2011, § 32, Rn. 16f.; Zöll in Taeger/Gabel, BDSG, 2010, § 32, Rn. 6.

32 Schneider, NZG 2010, 1201, 1205; Schmidt, DuD 2010, 207, 208f.

33 Bönner/Riedl/Wenig, Digitale SAP-Massendatenanalyse, 2011, S. 21.

liegen, wenn dieser personenbezogene Daten eines Arbeitnehmers für einen anderen Zweck als das Beschäftigungsverhältnis nutzen will.
Damit sind auch alle unternehmensinternen Datenanalysen ohne Bezug zum einzelnen Mitarbeiter sinnvoller Weise zulässig. SAP-Daten wären dann so zu analysieren, dass alle Bezüge zu Arbeitnehmern unkenntlich gemacht sind (Pseudonymisierung). Finden sich im Rahmen der Analyse dann Anhaltspunkte für einen Verdacht, könnte die Analyse auf die relevanten und erkannten Datensätze begrenzt werden, um dann mit § 32 Abs. 1 S. 2 BDSG als Rechtfertigung auch mit Bezug zu den dann verdächtigen Mitarbeitern entweder wiederholt zu werden oder es wäre die Pseudonymisierung in Bezug auf die relevanten Daten aufzulösen.

2.2.4 Rechtfertigung der Datenanalyse durch § 32 BDSG

§ 32 Abs. 1 S. 1 BDSG ist die allgemeine Erlaubnisnorm für die Erhebung, Verarbeitung und Nutzung (zusammengefasst die „Verwendung“) von Beschäftigtendaten. Die Norm beschränkt die Verwendung von Beschäftigtendaten auf solche Daten, die der Arbeitgeber zur Erfüllung seiner Pflichten und zur Wahrnehmung seiner Rechte aus dem Beschäftigungsverhältnis vernünftigerweise benötigt[34]. Zu den Pflichten des Arbeitgebers gehören beispielsweise Personalverwaltung und Entgeltzahlung, zu den Rechten die Erteilung von Weisungen und die Leistungs- und Verhaltenskontrolle[35].
§ 32 Abs. 1 S. 1 BDSG ist auch die einschlägige Rechtsgrundlage für Präventivmaßnahmen[36], die der Arbeitgeber ergreift, um Straftaten und sonstigen Rechtsverstößen in seinem Unternehmen vorzubeugen und Risikobereiche zu ermitteln. Die Norm ist also einschlägig, wenn die Interne Revision Datenabgleiche durchführt oder ein Meldesystem (Whistleblower-Hotline) einrichtet, das es Arbeitnehmern ermöglicht, unternehmensinterne Verstöße (anonym) zu melden[37].
Soweit es um die Aufklärung und Verfolgung von Straftaten bei konkretem Tatverdacht geht, greift § 32 Abs. 1 S. 2 BDSG[38]. § 32 Abs. 1 S. 2 BDSG normiert die speziellen Voraussetzungen für repressive Maßnahmen des Arbeitgebers. Voraussetzung ist der konkrete Verdacht einer Straftat, also konkrete tatsächliche Anhaltspunkte für ein strafbares Verhalten müssen vorliegen[39].
Dabei ist umstritten, ob § 32 Abs. 1 S. 2 BDSG auch bei der Verfolgung von Ordnungswidrigkeiten und sonstigen Rechtsverstößen, die keine Straftaten darstellen, oder bloßen Vertragsverstößen von Beschäftigten herangezogen werden muss. Die

---

34 Gola/Schomerus, BDSG, 10. Aufl. 2010, § 32, Rn. 11.

35 Schmidt, DuD 2010, 207, 209.

36 Gola/Schomerus, a.a.O., § 32, Rn. 24 f.; Seifert in: Simitis, a.a.O., § 32, Rn. 103; Heldmann, DB 2010, 1235, 1237; Koch, ITRB 2010, 164, 165; Schneider, NZG 2010, 1201, 1206; Wybitul, BB 2010, 1085.

37 Gola/Schomerus, BDSG, § 32, Rn. 24f., 16.

38 Gola/Schomerus, BDSG, § 32, Rn. 26.

39 Gola/Schomerus, BDSG, § 32, Rn. 26.

befürwortenden Stimmen verweisen auf die Gesetzesbegründung[40], die ablehnenden auf den Wortlaut[41]. Da nicht davon ausgegangen werden kann, dass der Gesetzgeber die repressive Verfolgung von Ordnungswidrigkeiten und Vertragsverstößen gänzlich ausschließen oder aber aus dem Beschäftigtendatenschutz ausnehmen wollte, ist wohl anzunehmen, dass diese grundsätzlich nach § 28 Abs. 1 S. 1 BDSG legitimiert werden kann[42]. Die diesbezüglichen Maßnahmen sollten aber sicherheitshalber nicht weiter gehen als von § 32 Abs. 1 S. 2 BDSG erlaubt[43].

2.2.4.1 Präventive Maßnahmen

Präventive Maßnahmen der Internen Revision richten sich zunächst nach § 32 Abs. 1 S. 1 BDSG. Die Datenverwendung muss danach der Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses (beschäftigungsvertraglicher Zweck[44]) dienen und zum Erreichen dieses Zwecks erforderlich sein.
Die Datennutzung dient insbesondere dann keinem beschäftigungsvertraglichen Zweck, wenn der Arbeitgeber dem Beschäftigten wie ein beliebiger Dritter gegenübersteht[45]. Dies ist etwa der Fall bei der Erteilung von Auskünften im Rahmen der Erfüllung hoheitlich auferlegter Pflichten (z.B. im Rahmen polizeilicher Ermittlungstätigkeit, wenn die Polizei das Unternehmen um Auskunft ersucht) oder beim Anbieten von Leistungen, die keine direkte Verbindung zum Beschäftigungsverhältnis haben[46]. Dient eine Maßnahme dazu, Straftaten durch Beschäftigte im Unternehmen zu verhindern, so verfolgt sie unproblematisch einen beschäftigungsvertraglichen Zweck[47].
Die Maßnahme ist erforderlich, wenn sie das mildeste aller gleich wirksamen Mittel ist, um ihrem Zweck Rechnung zu tragen[48]. Das bedeutet, dass unter allen Maßnahmen, die gleichermaßen geeignet sind, den angestrebten Zweck zu erreichen, insbesondere Rechtsverstößen präventiv entgegenzuwirken, diejenige auszuwählen ist, die die Beschäftigten am wenigsten belastet. Abzustellen ist dabei auf Dauer, Umfang und Intensität der Maßnahme, also über welchen Zeitraum sie sich erstreckt, wie breit die Datenbasis ist, auf die zurückgegriffen wird, wie sensibel die betroffenen Daten sind etc.

---

40 Schmitt-Rolfes, AuA 2010, 71 (Gesetzesentwurf spricht von „Straftaten und sonstigen Rechtsverstößen“).

41 Seifert in: Simitis, BDSG, § 32, Rdn. 102; Koch, ITRB 2010, 164, 166; Heldmann, DB 2010, 1235, 1237 ist für Anwendung von § 28 BDSG.

42 So auch: Gola/Schomerus, BDSG, § 32, Rdn. 29

43 Eine Übersicht über die aktuelle Meinungslage bietet Zöll in Taeger/Gable, BDSG, 2010, § 32, Rn. 39ff.

44 Schmidt, DuD 2010, 207, 209.

45 Schmidt, a.a.O.

46 Schmidt, DuD 2010, 207, 209.

47 Seifert in: Simitis, a.a.O., § 32, Rn. 77.

48 Gola/Schomerus, DBSG, § 32, Rn. 12; Seifert in: Simitis, BDSG, § 32, Rn. 11.

Im Rahmen der Erforderlichkeit ist auch das Gebot der Datensparsamkeit nach § 3a BDSG zu beachten, wonach bei Erhebung, Verarbeitung und Nutzung personenbezogener Daten so wenig Daten wie möglich zu verwenden und diese soweit es geht zu anonymisieren oder zu pseudonymisieren sind. Es soll also nur mit unabdingbar notwendigen und, soweit die Maßnahme es erlaubt, mit anonymisierten oder pseudonymisierten Daten gearbeitet werden.

„Anonymisieren" ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Lebensverhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (§ 3 Abs. 6 BDSG). „Pseudonymisieren" ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren (§ 3 Abs. 6a BDSG). Eine echte Anonymisierung ist nur gegeben, wenn eine Reanonymisierung (unter normalen Bedingungen) unmöglich, der Personenbezug also nicht mehr herstellbar ist[49]. Die Pseudonymisierung stellt dagegen nicht zwingend Anonymität der Betroffenen her, denn sie geht in der Regel mit der Verfügbarkeit einer Referenzdatei einher, mit deren Hilfe das Pseudonym wieder aufgelöst werden kann[50]. Bei der Pseudonymisierung geht es deshalb nicht darum, die Anonymität auf Dauer, sondern darum, sie während der Datenverarbeitung herzustellen, um dann gegebenenfalls nur die „Treffer" aufzulösen; d.h. für sie den Personenbezug wieder herzustellen.

Teilweise wird vertreten, „zur Aufdeckung einer Straftat" umfasse vom reinen Wortlaut her auch vorbeugende Maßnahmen zur Aufdeckung von potenziellen Straftaten. Folgt man dieser Meinung, wäre für alle vorbeugenden Analysen ein konkreter und dokumentierbarer Verdacht erforderlich. Dieser Widerspruch zwischen vorbeugender Compliance und erst verdachtsgetriebener Maßnahme kann mit dem Gesetz nicht zweifelsfrei aufgelöst werden[51]. Aufgrund der nicht eindeutigen Rechtslage kann hier nur empfohlen werden, bei präventiven Maßnahmen ohne konkreten Tatverdacht die Prüfung der Erforderlichkeit und Angemessenheit der Datenverwendung besonders sorgfältig vorzunehmen und die Prüfungsschritte sowie das Prüfungsergebnis zu dokumentieren.

Es ist also bei präventiven Maßnahmen besonders darauf zu achten, dass die am wenigsten eingriffsintensive Variante gewählt wird, dass z.B. nur stichprobenartige Überprüfungen anstelle von vollständigen Analysen durchgeführt oder verwendete Beschäftigtendaten weitgehend anonymisiert oder zumindest pseudonymisiert werden.

---

49 Gola/Schomerus, BDSG, § 3, Rdn. 44.

50 Gola/Schomerus, BDSG, § 3, Rdn. 46.

51 Zöll in Taeger/Gabel, a.a.O., § 32, Rn. 39 ff, der einen umfangreichen Überblick über die vertretenen Ansichten gibt.

Dass Datenschutz zunehmend als Schlüsselthema der digitalen Gesellschaft gelten kann, zeigen nicht nur aktuelle Debatten um Datenkraken und immer ausgefeiltere technische Spionagemethodik. Auch die Interne Revision muss zunehmend den Spagat meistern, technische Spielräume auszunutzen, ohne rechtliche Richtlinien und andere Compliance-Anforderungen zu verletzen.

Dieser Band betrachtet die fachlich hoch komplexe und mehrdimensionale Thematik aus ihren vielseitigen technischen, rechtlichen und ökonomischen Blickwinkeln. Schwerpunkte sind u.a.

- **Datenanalyse und Datenschutz** mit Leitlinien für die Interne Revision
- **Datenschutz bei der Analyse von Massendaten** in Revisionsprozessen
- **Korruptionsverhinderung und Datenschutz** aus Sicht der Internen Revision
- Empirische Befunde zur **Akzeptanz der digitalen Prüfungsunterstützung**
- Anforderungen und Parameter **zukunftsorientierter Analysesoftware**

Ein komprimierter Überblick, um compliance-relevante Fragestellungen und Risiken in der Internen Revision und anderen überwachenden Funktionsbereichen wirkungsvoll in Prüfungsprozesse einzubinden.

Leseprobe, mehr zum Buch unter ESV.info/978-3-503-14137-1

9 783503 141371

€ (D)
29,95

www.ESV.info