Bernd Schmidt, Christian Jakob

Die Zulässigkeit IT-gestützter Compliance- und Risikomanagementsysteme nach der BDSG-Novelle

EDV durchdringt in zunehmendem Maße die Unternehmen. Sie ist das Werkzeug des Managements für die Steuerung und Überwachung sämtlicher Prozesse. Sie kann unter anderem zur Unterstützung bei der Erfüllung von Risikomanagement- und Compliance-Pflichten eingesetzt werden und muss es abhängig von der Durchdringung des Unternehmens mit IT gesteuerten Prozessen auch. Mit dem IT-Einsatz verbinden sich neben einem möglichen Nutzen aber auch Risiken, die es zu beachten gilt. Es ist sicherzustellen, dass rechtliche, insbesondere datenschutzrechtliche, Anforderungen an den IT-Einsatz beachtet werden. So gilt es das Interesse der Unternehmen an einer möglichst umfassenden und effizienten Kontrolle von Unternehmensprozessen mit dem Interesse der Beschäftigten an ihrer informationellen Selbstbestimmung in Einklang zu bringen. IT-gestützte Compliance- und Risikomanagementsysteme bewegen sich daher in einem Spannungsfeld zwischen Nutzen, Risiken und rechtlichen Anforderungen. Die geplante Novelle des BDSG nimmt sich dieses Spannungsfeldes an und soll bisher fehlende klare gesetzliche Regelungen schaffen, um Beschäftigte zu schützen und Arbeitgebern eine verlässliche Grundlage für die Datenverarbeitung an die Hand zu geben.

Dr. jur. Bernd Schmidt LL.M.

ist Rechtsreferendar in Bremen. Er promovierte am Lehrstuhl von Prof. Dr. Taeger an der Universität Oldenburg zum Thema „Compliance in Kapitalgesellschaften".
E-Mail: mail@berndschmidt.eu

Dipl. Jur. Christian Jakob LL.M.

ist Rechtsreferendar in Oldenburg und Doktorand am Lehrstuhl von Prof. Dr. Taeger an der Universität Oldenburg.
E-Mail: mail@christian-jakob.eu

1 Compliance und Risikomanagement

Hinter Compliance steht das Interesse von Unternehmen, Schäden durch illegale Aktivität aus dem Unternehmen heraus zu vermeiden. Zur Herstellung von Compliance sind die Geschäftsführungsorgane von Kapitalgesellschaften verpflichtet, für die sich ihre Compliance-Pflicht aus der intern erforderlichen Sorgfalt ergibt.[1] Diese beinhaltet die Verantwortung für die Abwehr von Schäden, die Wahrung von Vorteilen[2] und die Pflicht zur Legalität.[3] Der Regierungsentwurf enthält eine Compliance-Definition, die hieran anknüpft und sie als Einhaltung relevanter Gesetze, Verordnungen, Richtlinien und Selbstverpflichtungen durch ein Unternehmen als Ganzes versteht.[4]

Das Management hat aufgrund seiner Compliance-Pflicht die Voraussetzungen für rechtskonformes Verhalten der Unternehmensangehörigen und der Unternehmensorganisation zu schaffen. Darüber hinaus erfordert die Herstellung von Compliance auch ein Element der Überwachung. Hierbei können IT-gestützte Systeme von großem Nutzen sein. So können mittels OLAP-basierter Verfahren selbst große Datensammlungen durchsucht werden und „fraud-patterns" mittels definierter Kriterien gefunden werden.[5] Hierunter fallen auch als Screening bezeichnete Datenabgleiche, wie sie von

1 Vgl. für die AG §§ 76 Abs. 1, 93 Abs. 1 S. 1 AktG, für die GmbH § 43 Abs. 1 S. 1 GmbHG und für die Genossenschaft §§ 27 Abs. 1 S. 1, 34 Abs. 1 S. 1 GenG.

2 Hierzu BGHZ 21, 354 (357); Fleischer, in: Spindler/Stilz, AktG, § 93, Rn. 11; Hopt, in: GK, AktG, § 93, Rn. 72.

3 Reichert/Ott, ZIP 2009, S. 2173; Thole, ZHR 2009, S. 504 (509 f.).

4 BR-Drs. 535/10, S. 35; zum Compliance-Begriff im Allgemeinen vgl. Schmidt, Compliance in Kapitalgesellschaften, S. 18 ff.

5 Hierzu ausführlich Heinson/Schmidt, CR 2010, S. 540 (542).

der Deutschen Bahn im sog. Datenskandal durchgeführt wurden.[6] Data Mining Anwendungen gehen hierüber hinaus. Sie sind nicht darauf angewiesen, nach definierten Mustern zu suchen, sondern können diese eigenständig erzeugen.[7]

In einem inhaltlichen Zusammenhang zur Compliance steht die Verpflichtung zum Risikomanagement. Dieses kann als bewusster und organisierter Umgang mit Risiken im Unternehmen beschrieben werden.[8] Dahinter steht das Interesse des Unternehmens an der Beherrschung wirtschaftlicher Risiken, die den Fortbestand des Unternehmens gefährden können. Zur Erfüllung von Risikomanagementanforderungen sind, wie bei der Compliance-Pflicht, die Geschäftsleitungsorgane von Kapitalgesellschaften aufgrund ihrer Sorgfaltspflicht intern verpflichtet. Die Regelung in § 91 Abs. 2 AktG dient nur deren Hervorhebung für die Aktiengesellschaft.[9] Für das Management ergibt sich aus der Risikomanagementpflicht die Verantwortung, die Lage der Gesellschaft im Hinblick auf Risiken für ihren Fortbestand zu analysieren. Hierfür ist die Überwachung von definierten Kenngrößen und die Bewertung von Entwicklungen innerhalb und außerhalb des Unternehmens notwendig. Dies setzt wiederum den Umgang mit großen Datenmengen voraus.[10]

Für die Erfüllung von Compliance-Pflichten und für den Betrieb von Risikomanagementfunktionen gilt daher, dass sie ohne IT-Unterstützung praktisch nicht mehr erfüllbar sind. Soweit hierbei personenbezogene Daten erfasst und verarbeitet werden, hängt es von den Wertungen des BDSG ab, ob die konkrete Maßnahme zulässig ist. Nur wenn Daten keinen Personenbezug aufweisen, ist ihre Verarbeitung nicht an den Voraussetzungen des BDSG zu messen. Für Compliance-Anwendungen ist hiervon nur in Ausnahmefällen auszugehen, da es im Rahmen der Compliance-Überwachung um das Aufdecken von Rechtsverstößen und die Täterermittlung geht. Der Ausschluss der Anwendbarkeit des BDSG für Compliance-Anwendungen würde voraussetzen, dass nur anonymisierte Daten verwendet werden. Hierbei stellen sich hohe Anforderungen an eine technisch wirksame Anonymisierung, die regelmäßig nicht zu realisieren sind.[11] Zudem wird die Nutzbarkeit der Ergebnisse hierdurch gemindert oder aufgehoben.

Für IT-gestützte Risikomanagementsysteme ist es nicht im gleichen Umfang wie für Maßnahmen der Compliance-Überwachung essentiell, auf personenbezogene Daten zurückzugreifen. Es ergeben sich nennenswerte Bereiche, in denen Daten keinen Personenbezug aufweisen oder dieser ohne Beeinträchtigung der Ergebnisqualität dauerhaft entfernt werden kann. Dies gilt etwa für die Verarbeitung wirtschaftlicher Kennzahlen. Die Anwendbarkeit des BDSG lässt sich aber auch für das Risikomanagement nicht vollständig ausschließen. Dies gilt insbesondere, wenn die Lokalisierung eines Risikos im Unternehmen gewünscht oder erforderlich ist und ein Zusammenhang mit einer Person oder Personengruppe besteht. Auch für den Betrieb von Risikomanagementfunktionen sind damit datenschutzrechtliche Vorgaben im Allgemeinen und solche des Beschäftigtendatenschutzes zu beachten.

2 Datenschutzrechtliche Wertungen

Die Zulässigkeit der Nutzung personenbezogener Daten ergibt sich aus den Wertungen des BDSG. Hierbei gilt der Grundsatz, dass eine Datenverarbeitung nur zulässig ist, wenn sie durch Gesetz oder Rechtsvorschrift zugelassen ist oder der Betroffene einwilligt.[12]

Für die Verarbeitung von Beschäftigtendaten allgemein und zur Erfüllung von Compliance- und Risikomanagementpflichten kommt einer Einwilligungslösung bereits nach derzeitiger Rechtslage nur nachrangige Bedeutung zu. So ergeben sich in Beschäftigungsverhältnissen aufgrund bestehender wirtschaftlicher Abhängigkeit des Beschäftigten vom Arbeitgeber hohe Anforderungen an die gem. § 4a Abs. 1 BDSG erforderliche Freiwilligkeit der Einwilligung.[13] Zudem ist eine Einwilligungslösung für IT-gestützte Compliance- und Risikomanagementmaßnahmen wenig praktikabel, da typischerweise eine große Personengruppe betroffen ist und die Einholung individueller Einwilligungen mit erheblichem Organisationsaufwand verbunden ist. Zudem ist eine erteilte Einwilligung jederzeit frei widerruflich, so dass ein einheitlicher Standard im Unternehmen nicht dauerhaft garantiert werden kann.

Die hohen rechtlichen Anforderungen an die Einwilligung im Beschäftigtendatenschutz werden durch den Gesetzentwurf der Bundesregierung noch weiter verschärft. So sieht § 32l BDSG-E vor, dass abweichend von § 4 Abs. 1 BDSG eine Einwilligung von Beschäftigten in eine Datenerhebung, -verarbeitung oder -nutzung durch den Arbeitgeber nur noch zulässig ist, wenn dies ausdrücklich im Gesetz vorgesehen ist. Die für Datenverarbeitungen zu Compliance- und Risikomanagementzwecken relevanten Vorschriften der §§ 32c, 32d und 32e BDSG-E sehen die Möglichkeit einer Einwilligung nicht vor.[14]

Die Zurückdrängung der Möglichkeit zur Rechtfertigung der Datenverarbeitung in Beschäftigtenverhältnissen wird im Schrifttum kritisch gesehen. So wird hierin ein Verstoß gegen Vorgaben der EG-Datenschutzrichtlinie gesehen[15] und zu Recht vorgetragen, dass die Einwilligung auch in arbeitsrechtlichen Beziehungen ein angemessenes Mittel zur Rechtfertigung der Datenverarbeitung sein kann, soweit die Freiwilligkeit der Entscheidung gesichert ist.[16]

Für die hier relevanten Bereiche IT-gestützter Compliance- und Risikomanagementsysteme ist das Entfallen der Möglichkeit der Rechtfertigung im Wege der Einwilligungslösung von nachgeordneter Bedeutung, da hierdurch eine bisher allenfalls theoretisch mögliche Rechtfertigung der Datenverarbeitung entfällt. Soweit die Verfahren Daten von Nichtbeschäftigten verarbeiten bleibt diese (theoretische) Möglichkeit der Rechtfertigung bestehen.

6 Hierzu Barton, RDV 2009, 200 ff.; Heinson, BB 2010, S. 3084; Schmidt, Compliance in Kapitalgesellschaften, S. 193.

7 Heinson/Schmidt, CR 2010, S. 540 (542).

8 So auch Meyer, in: Kalwait/Meyer/Romeike/Schellenberger/Erben, Risikomanagement in der Unternehmensführung, S. 48.

9 BT-Drs. 13/9712, S. 15.

10 Gleißner/Romeike, in: Kalweit/Meyer/Romeike/Schellenberger/Erben, Risikomanagement in der Unternehmensführung, S. 309.

11 Heinson/Schmidt, CR 2010, S. 540 (543).

12 Taeger, in: Taeger/Gabel, BDSG, § 4, Rn. 14.

13 Ausführlich hierzu Taeger, in: Taeger/Gabel, BDSG, § 4a, Rn. 58 ff.; zur Einwilligung nach dem BDSG-E Tinnefeld/Petri/Brink, MMR 2010, S. 727 (729).

14 Vgl. Heinson, BB 2010, S. 3080 (3085).

15 Thüsing, RDV 2010, S. 147 (148).

16 Gola, RDV 2010, S. 97 f.; Thüsing, RDV 2010, S. 147 (148); Tinnefeld/Petri/Brink, MMR 2010, S. 727 (729).

2.1 Erhebung und Verwendung von Bewerberdaten vor Begründung des Beschäftigtenverhältnisses gem. §§ 32-32b BDSG-E

Aus den §§ 32-32b BDSG-E ergibt sich die Zulässigkeit der Datenerhebung und -nutzung vor Begründung des Beschäftigungsverhältnisses.[17] In dieser Anbahnungsphase dürfen die in § 32 BDSG-E spezifizierten Daten erhoben und unter den Voraussetzungen gem. § 32b Abs. 1 BDSG-E verarbeiten werden, um die Eignung des Bewerbers festzustellen und über die Begründung eines Beschäftigungsverhältnisses zu entscheiden. Die Regelungen sind auf einen Interessenausgleich vor dem Bestehen eines Beschäftigungsvertrages ausgerichtet. Der Bewerber ist noch nicht Teil der Unternehmensorganisation und sein Verhalten allenfalls in Ausnahmen von Relevanz für die Datenverarbeitung zu Compliance- oder Risikomanagementzwecken. Denkbar wäre in diesem Zusammenhang bereits im Vorfeld die Einstellung von solchen Mitarbeitern zu verhindern, die bereits im Rahmen von Compliance relevanten Straftaten wie Untreue, Diebstahl oder Korruptionsdelikten in Erscheinung getreten sind. Relevant werden die Daten von Bewerbern im Wesentlichen erst dann, wenn sie in die Unternehmensorganisation eingegliedert und Beschäftigte geworden sind. Die Zulässigkeit der Erhebung von Beschäftigtendaten ergibt sich nach Maßgabe des § 32c Abs. 1 BDSG-E. Allerdings ist für die Verwendung von Beschäftigtendaten nicht entscheidend, ob diese vor oder nach der Begründung eines Beschäftigungsverhältnisses erhoben wurden. Aus § 32 Abs. 1 Nr. 1 BDSG-E folgt, dass auch Daten aus der Anbahnungsphase des Beschäftigungsverhältnisses im Rahmen der Durchführung des Beschäftigungsverhältnisses verwendet werden dürfen. Damit wird der Formalismus vermieden, dass diese nach Abschluss eines Beschäftigungsvertrages neu zu erheben sind.

2.2 Erhebung von Beschäftigtendaten gem. § 32c BDSG-E

Die §§ 32c, 32d BDSG-E regeln die Datenerhebung, -verarbeitung und -nutzung im Beschäftigungsverhältnis.[18] Sie widmen sich damit dem für den Betrieb von Compliance- und Risikomanagementfunktionen primär relevanten Zeitabschnitt von Beschäftigungsverhältnissen. Wie für die Datenverarbeitung vor Begründung eines Beschäftigungsverhältnisses wird auch im Beschäftigungsverhältnis nach der Erhebung von Beschäftigtendaten und deren Verwendung differenziert. Die Erhebung von Daten ist in § 32c BDSG-E geregelt und gem. dem aus § 32c Abs. 1 S. 1 BDSG-E folgenden Grundsatz zulässig, wenn sie für die Durchführung, Beendigung oder Abwicklung eines Beschäftigungsverhältnisses erforderlich ist. § 32c Abs. 1 S. 2 BDSG-E enthält einen nicht abschließenden Katalog von Beispielen, in denen die Datenerhebung erforderlich ist. Für die Erhebung von Beschäftigtendaten zu Compliance- und Risikomanagementzwecken relevant ist insbesondere § 32c Abs. 1 S. 2 Nr. 3 BDSG-E, wonach die Datenerhebung zulässig ist, soweit sie zur Wahrnehmung von Rechten des Arbeitgebers gegenüber dem Beschäftigten, einschließlich der Leistungs- und Verhaltenskontrolle, erforderlich ist.

Einschränkungen seiner Befugnisse ergeben sich aus dem Grundsatz der Verhältnismäßigkeit, wie sich auch aus § 32c Abs. 4 BDSG-E klarstellend ergibt.[19] Der Arbeitgeber hat daher die Datenerhebung auf das erforderliche Maß einzuschränken. Soweit hierdurch der Zweck der Datenerhebung nicht gefährdet wird, ergibt sich daher stets eine Pflicht zur Entfernung des Personenbezuges verwendeter Daten. Soweit dies im Hinblick auf den Erhebungszweck nicht möglich erscheint, sind erhobene Daten jedenfalls zu pseudonymisieren. Nur wenn beide Maßnahmen des technischen Datenschutzes im Hinblick auf den Datenerhebungszweck nicht möglich erscheinen, kann von ihnen abgesehen werden.

2.3 Erhebung von Beschäftigtendaten gem. § 32e BDSG-E

§ 32e Abs. 1 BDSG-E enthält den Grundsatz, dass Beschäftigtendaten nur mit Kenntnis des Beschäftigten erhoben werden dürfen. Auch wenn für Beschäftigtendaten eine § 32 Abs. 6 BDSG-E entsprechende Regelung fehlt, so gilt hier der Grundsatz der Direkterhebung mit Kenntnis des Beschäftigten. § 32e Abs. 2 BDSG-E enthält hiervon eine Ausnahme.[20] Dabei geht es nicht um die Umnutzung im Unternehmen vorliegender Daten, sondern um die anlassbezogene Erweiterung des Datenbestandes. Diese bildet nach dem gesetzlichen Leitbild die Ausnahme, die nur unter weiteren Voraussetzungen zulässig sein soll.[21] Anknüpfungspunkt zur Rechtfertigung sind Tatsachen, die den Verdacht begründen, dass der Beschäftigte eine Straftat oder eine andere schwerwiegende Pflichtverletzungen im Beschäftigungsverhältnis begangen hat (Nr. 2) und die Datenerhebung erforderlich ist, um die Straftat, die Pflichtverletzung oder weitere Straftaten oder schwere Pflichtverletzungen des Beschäftigten zu verhindern (Nr. 2). Der Verdacht muss sich, anders als eine isolierte Betrachtung des Wortlauts ergeben würde, nicht gegen einen bestimmten Beschäftigten richten, sondern kann sich auch auf eine Gruppe von Beschäftigten beziehen.[22] Dennoch kann die Datenerhebung nach § 32e Abs. 2 BDSG-E nicht wahllos auf die gesamte Belegschaft oder große Teile hiervon ausgedehnt werden. Der Grundsatz der Datensparsamkeit und des Verhältnismäßigkeitsgrundsatzes erfordern die Begrenzung des Umfangs der Datenverarbeitung auf eine möglichst kleine Gruppe.[23]

Der Verdacht muss sich zudem auf eine schwerwiegende Pflichtverletzung beziehen. Schwerwiegend i.S.d. Norm ist eine Pflichtverletzung, wenn sie eine Kündigung aus wichtigem Grund rechtfertigen würde. Damit wird an die Wertung in § 626 BGB angeknüpft.[24]

Eine Präzisierung des Verhältnismäßigkeitsgrundsatzes findet sich in Abs. 3. Die Vorschrift normiert, dass eine Erhebung nur zulässig ist, wenn eine anderweitige Erforschung des Sachverhalts erschwert oder weniger Erfolg versprechend wäre (Erforderlichkeit). Die Maßnahmen sind abzubrechen bzw. zu unterbrechen, wenn das beabsichtigte Ziel nicht bzw. zeitwei-

17 Vgl. BR-Drs. 535/10, S. 27; siehe auch Tinnefeld/Petri/Brink, MMR 2010, S. 727 (729 f.).

18 Heinson/Sörup/Wybitul, CR 2010, S. 751 (753); Tinnefeld/Petri/Brink, MMR 2010, S. 727 (731).

19 Kritisch zur Einführung des Verhältnismäßigkeitsgrundsatzes in die gesetzliche Terminologie Tinnefeld/Petri/Brink, MMR 2010, S. 727 (731).

20 Vgl. Tinnefeld/Petri/Brink, MMR 2010, S. 727 (731 f.).

21 BR-Drs. 535/10, S. 36.

22 BR-Drs. 535/10, S. 36; siehe auch Heinson, BB 2010, S. 3084 (3087).

23 Im Ergebnis zustimmend Heinson, BB 2010, S. 3084 (3086 f.); Heinson/Sörup/Wybitul, CR 2010, S. 751 (755).

24 BR-Drs. 535/10, S. 36.

se nicht erreichbar ist (Geeignetheit) und müssen zeitlich auf das notwendige Maß beschränkt werden. Soweit der Zweck der Datenerhebung vorübergehend nicht erreichbar ist, muss sie zudem solange unterbrochen werden.

Aus § 32e Abs. 4 BDSG-E ergeben sich Verbote der Datenerhebung und damit eine Einschränkung der Erlaubnis des § 32e Abs. 2 BDSG-E. So ist eine Datenerhebung gem. § 32e Abs. 4 Nr. 1 BDSG-E unzulässig, wenn sie planmäßig angelegt und für mehr als 24 Std. ununterbrochen oder an mehr als vier Tagen stattfinden soll. § 32e Abs. 4 Nr. 2 BDSG-E verbietet die Datenerhebung mittels technischer Mittel zur Abhörung oder Aufzeichnung des nicht öffentlich gesprochenen Wortes. § 32e Abs. 4 Nr. 3 BDSG-E verbietet die Datenerhebung mittels besonderer technischer Mittel für Beobachtungszwecke, macht jedoch eine Rückausnahme für den Einsatz von Ferngläsern und Fotoapparaten. Ausgeschlossen ist damit gem. § 32e Abs. 4 BDSG-E eine systematische Dauerüberwachung, die heimliche Aufzeichnung des nicht öffentlich gesprochenen Wortes sowie die versteckte Überwachungen mit Videokameras.[25] § 32e Abs. 7 BDSG-E enthält ein Verbot der Erhebung, Verarbeitung und Nutzung für Daten aus dem Kernbereich privater Lebensgestaltung und ordnet an, dass diese unverzüglich zu löschen sind, sollten sie dennoch erhoben worden sein.

In § 32e Abs. 5 BDSG-E wird eine Zweckbindung der nach der Vorschrift erhobenen Daten und Dokumentations- sowie Unterrichtungspflichten konstituiert. Es ist vor der Datenerhebung schriftlich niederzulegen, welche Tatsachen den Verdacht auf ein nach Abs. 2 Nr. 1 tatbestandliches Verhalten zulassen. Nach Abschluss der Datenerhebung sind die näheren Umstände der Datenerhebung zu dokumentieren. Hierdurch werden die Voraussetzungen für eine nachträgliche Rechtmäßigkeitskontrolle geschaffen und Konsequenzen aus den Datenskandalen gezogen.[26]

Nach § 32e Abs. 6 BDSG-E sind Daten unverzüglich zu löschen, wenn sie nicht länger zur Zweckerreichung erforderlich sind oder schutzwürdige Belange des Beschäftigten der weiteren Speicherung entgegenstehen. Ferner sind der Grund der Speicherung und die Löschung zu dokumentieren.

2.4 Verarbeitung von Beschäftigtendaten gem. § 32d BDSG-E

Soweit Beschäftigtendaten zulässig erhoben worden sind, können diese unter den Voraussetzungen des § 32d BDSG-E verwendet werden. § 32d Abs. 1 BDSG-E enthält den allgemeinen Grundsatz für die Zulässigkeit der Beschäftigtendatenverarbeitung und knüpft diese neben der Rechtmäßigkeit ihrer Erhebung nach §§ 32, 32a und 32c BDSG-E an zwei weitere Voraussetzungen. So muss die Datenverarbeitung dem Zweck ihrer Erhebung oder einem Zweck dienen, für den die Datenerhebung zulässig ist. Zudem muss die Datenerhebung verhältnismäßig sein.[27] Daten, die den Arbeitgeber auf anderem Wege, als dem gem. §§ 32, 32a und 32c BDSG-E erhoben hat, darf er gem. § 32d Abs. 2 BDSG-E verarbeiten, wenn es für die Durchführung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses erforderlich und verhältnismäßig ist und die Erhebung zu diesem Zweck gerechtfertigt gewesen wäre.

Die Datenverarbeitung im Rahmen des Risikomanagements ist mangels einer spezielleren Norm an den Voraussetzungen gem. § 32d Abs. 1 und 2 BDSG-E zu messen. Voraussetzung ihrer Rechtfertigung ist damit, dass die Datenerhebung zur Erfüllung von Pflichten des Arbeitgebers (§ 32c Abs. 1 Nr. 1-2 BDSG-E) oder zur Wahrnehmung von Rechten gegenüber den Beschäftigten erforderlich ist und die Voraussetzungen der Verhältnismäßigkeit gewahrt sind. Im Zusammenhang mit dem IT-gestützten Risikomanagement ist die Rechtfertigung gem. § 32c Abs. 1 Nr. 1 BDSG-E eröffnet, da sie der Erfüllung gesetzlicher Risikomanagementpflichten dient. Soweit Gegenstand der Datenverarbeitung die Kontrolle der Mitwirkung von Beschäftigten an Maßnahmen des Risikomanagements ist, kommt auch die Rechtfertigung gem. § 32c Abs. 1 Nr. 3 BDSG-E in Betracht. Diese Hürde ist für Arbeitgeber leicht zu überwinden, da sich aus gesetzlichen Risikomanagementpflichten regelmäßig keine Einschränkung der hierzu erforderlichen Datenverarbeitung ergibt. Zentral für die Rechtfertigung der Datenverarbeitung ist damit auch nach neuer Rechtslage die Beachtung der Verhältnismäßigkeit der Maßnahmen mit den bekannten Problemen in der Praxis.

Auch für die Datenverarbeitung zu Compliance-Zwecken ist der Anwendungsbereich von § 32d Abs. 1 und 2 BDSG-E eröffnet. In seinem Anwendungsbereich ist § 32d Abs. 3 BDSG-E jedoch spezieller und geht der Regelung in § 32d Abs. 1 und 2 BDSG-E vor. Es handelt sich dabei um eine gesetzliche Erlaubnis, die dem Arbeitgeber die Nutzung von Beschäftigtendaten und deren automatisierten Abgleich erlaubt, um Straftaten oder Pflichtverletzungen von Beschäftigten aufzudecken. Angesprochen sind damit Verfahren des Massenscreenings, wie sie im sog. Bahndatenskandal angewendet wurden. Die Rechtfertigung der Datenverarbeitung in Massenscreenings setzt voraus, dass es sich um eine schwerwiegende Pflichtverletzung oder Straftat handelt, die in ihrer Intensität den Regelbeispielen des § 32d Abs. 3 BDSG-E nahe kommt und die im Zusammenhang mit dem Beschäftigungsverhältnis begangen wurde.[28] Hierbei muss die Datenverarbeitung nicht auf die Kontrolle eines einzelnen Mitarbeiters gerichtet sein, sondern kann eine größere Gruppe, theoretisch auch die gesamte Belegschaft, erfassen. Hiermit wird die Wertung des § 32e Abs. 2 BDSG-E aufgegriffen, nach der ein Verdacht gegen eine größere Gruppe hinreichend für die geheime Datenerhebung sein kann. Die Datennutzung steht hierbei unter der Voraussetzung, dass es sich um besonders qualifizierte Pflichtverletzungen handelt. Hierbei kann es sich sowohl um eine Straftat, als auch um eine schwerwiegende Pflichtverletzung handeln, worunter auch die Begehung einer hinreichend erheblichen Ordnungswidrigkeit fallen kann.[29] Ausgangspunkt für die Bemessung der erforderlichen Schwere bilden die im Normentwurf beispielhaft aufgenommenen Straftatbestände. Erforderlich ist darüber hinaus, dass die Pflichtverletzung im Zusammenhang mit dem Beschäftigungsverhältnis begangen wurde. Die ausdrücklich genannten Strafvorschriften §§ 266, 299, 331 bis 334 StGB weisen darauf hin, dass es sich bei der Pflichtverletzung insbesondere um ein korruptives Verhalten handeln kann, bei dem die durch die Einbettung in die Unterneh-

25 BR-Drs. 535/10, S. 37; vgl. § 32f BDSG-E; diese Wertung begrüßend Tinnefeld/Petri/Brink, MMR 2010, S. 727 (735).

26 Tinnefeld/Petri/Brink, MMR 2010, S. 727 (731 f.).

27 Vgl. BR-Drs. 353/10, S. 34.

28 BR-Drs. 535/10, S. 35; hierzu Heinson/Sörup/Wybitul, CR 2010, S. 751 (754 f.).

29 BR-Drs. 353/10, S. 35.

mensorganisation zugewiesene Stellung ausgenutzt wird, um sich einen Vorteil zu verschaffen oder einen Vorteil für das Unternehmen im Wettbewerb zu erlangen. Der Bundesrat kritisiert, in dieser Konsequenz nicht unbedingt nachvollziehbar, den Ansatz des Regierungsentwurfs und fordert Screenings nur noch zur Ermittlung strafrechtlich relevanter Vorgänge zuzulassen, da andere Pflichtverletzungen datenschutzrechtlicher Gewährleistungen nicht einschränken könnten.

§ 32d Abs. 3 BDSG-E schränkt die Zulässigkeit von Datenabgleichen dahingehend ein, dass sie anonym oder pseudonym durchzuführen sind. Erst mit Bejahung eines Verdachtsfalls ist die Zusammenführung der Klardaten der Beschäftigten mit den auffälligen Datensätzen und damit eine Personalisierung zulässig.[30] Die Möglichkeit der Personalisierung kann sich hier nur auf die pseudonyme Datenverarbeitung beziehen, da eine anonyme Datenverarbeitung voraussetzt, dass eine Repersonalisierung technisch nicht mehr möglich ist.[31] Das Konzept des Schutzes von Beschäftigten durch Anonymisierung und Pseudonymisierung wird vom Bundesrat kritisiert. So sei insbesondere in kleinen Betrieben die Wirksamkeit solcher Maßnahmen gering.[32]

Zur Wahrung der Transparenz der ergriffenen Maßnahmen müssen schließlich eine Dokumentation und eine Unterrichtung der Beschäftigten erfolgen. Nicht von der Hand zu weisen ist diesbezügliche Kritik, dass hier erhebliche Vollzugsdefizite zu erwarten sind, da die Erfüllung von Informationspflichten des Arbeitgebers durch die Beschäftigten praktisch nicht kontrollierbar ist.[33]

Soweit IT-gestützte Compliance-Systeme andere Verfahren als Massenscreenings nutzen, ist der Anwendungsbereich gem. § 32d Abs. 1-2 BDSG eröffnet und unter vergleichbaren Anforderungen, wie für das IT-gestützte Risikomanagement zulässig. So ist die Voraussetzung, dass eine Pflicht des Arbeitgebers i.S.d. § 32c Abs. 1 Nr. 1 BDSG-E oder ein Recht gegenüber dem Beschäftigten besteht. Als gesetzliche Pflicht ist in diesem Zusammenhang die Compliance-Pflicht geeignet, die Datenverarbeitung zu rechtfertigen. Zusätzlich kann sich der Arbeitgeber auf sein Recht und die korrespondierende Pflicht der Beschäftigten zur Mitwirkung an der Compliance-Organisation berufen. Beschäftigte sind nämlich aus dem Grundsatz von Treu und Glauben sowie aus arbeitsvertraglicher Treuepflicht zur Rücksichtnahme auf Unternehmensinteressen verpflichtet. Hieraus ergibt sich auch, dass sie Rechtsverstöße zu unterlassen und an der Sicherung eines hinreichenden Compliance-Standards und dem Betrieb der Compliance-Organisation mitzuwirken haben.[34] Wie für die Rechtfertigung von Maßnahmen des IT-gestützten Risikomanagements, kommt der Verhältnismäßigkeit der konkreten Maßnahme die zentrale Rolle auch bei der Rechtfertigung von Maßnahmen der IT-gestützten Compliance-Organisation zu. Für den Bereich IT-gestützter Maßnahmen der Compliance-Organisation stellt sich zudem das Problem der Abgrenzung der Anwendungsbereiche der §§ 32d Abs. 1-2 BDSG-E einerseits und § 32d Abs. 3 BDSG-E andererseits. Der Regierungsentwurf lässt hier offen, ob nur „klassische Massenscreenings", also die Überprüfung von zwei oder mehr Datenbanken auf Übereinstimmungen in festgelegten Merkmalen erfasst sein sollen oder ob auch komplexere Verfahren des Dataminings nur unter den Voraussetzungen gem. § 32d Abs. 3 BDSG-E zulässig sein sollen. Für einen weiten Anwendungsbereich des § 32d Abs. 3 BDSG-E spricht das Anliegen, einen umfassenden Schutz der Beschäftigten zu gewährleisten sowie der Umstand, dass die Schutzwürdigkeit der Beschäftigten auch bei komplexeren Verfahren der Ermittlung von Verdachtsfällen hoch einzuschätzen ist. Eine Klarstellung wäre zu begrüßen.

3 Verarbeitung von Nichtarbeitnehmerdaten gem. § 28 Abs. 1 BDSG

Für die Datenverarbeitung im Rahmen des Compliance- und Risikomanagementsystems sind natürlich nicht nur Beschäftigtendaten, sondern auch Daten von unternehmensexternen Personen relevant. Dieser Bereich wird von der BDSG-Novelle nicht erfasst, so dass für die Rechtfertigung wie nach alter Rechtslage auf § 28 BDSG als Erlaubnisnorm zurück zu greifen ist.[35] § 28 BDSG regelt die Zulässigkeit der Datenverarbeitung im Rahmen vertraglicher Beziehungen und ist im Hinblick auf die Rechtfertigung der Datennutzung zu Compliance- und Risikomanagement-Zwecken insbesondere für die Nutzung von Kunden- und Lieferantendaten relevant. Die Datenverarbeitung ist hiernach zulässig, wenn sie der Zweckbestimmung des zugrunde liegenden Vertrages dient, es zur Wahrung berechtigter Interessen erforderlich ist oder die Daten allgemein zugänglich sind. Zweckdienlich i.S.v. § 28 Abs. 1 Nr. 1 BDSG ist eine Datenverarbeitung, wenn sie der Vertragserfüllung oder der Durchsetzung von Rechten aus dem Vertragsverhältnis dient.[36] In Betracht kommt diese Rechtfertigung der Datenverarbeitung insbesondere, wenn es um die Feststellung der Gefährdung des Vertragszwecks durch Nebenpflichtverletzungen geht. Denkbar ist dies etwa im Fall des kollusiven Zusammenwirkens eines Lieferanten oder Kunden mit einem Angestellten zu Lasten des Unternehmens. Der Betrieb von Compliance- und Risikomanagementsystemen stellt in Unternehmen zudem eine Rechtspflicht dar, an der ein berechtigtes Interesse i.S.d. § 28 Abs. 1 Nr. 2 BDSG besteht, so dass die Verarbeitung unternehmensfremder Daten für Compliance-Zwecke bei einem überwiegenden Interesse auch hiernach gerechtfertigt werden kann.

4 Verhältnismäßigkeit

Ergänzend zum Vorliegen eines datenschutzrechtlichen Erlaubnistatbestands war es bereits nach alter Rechtslage erforderlich, dass die Datenverarbeitung verhältnismäßig ist. Dieser datenschutzrechtliche Grundsatz wird von der BDSG-Novelle an verschiedenen Stellen aufgegriffen und klarstellend tatbestandlich normiert.[37] Verhältnismäßigkeit setzt voraus, dass jede Verarbeitung personenbezogener Daten für die Herstellung von Compliance bzw. zum Betrieb von Risikomanagementsystemen geeignet, erforderlich und angemessen ist. Dass IT-gestützte Systeme zur Unterstützung von Compliance und Risikomanagementfunktionen geeignet sind, dürfte unbestritten sein. Erforderlich ist eine Datenverarbeitung, wenn keine gleich geeigneten und weniger eingriffs-

30 Vgl. BR-Drs. 535/10, S. 35.
31 Heinson/Sörup/Wybitul, CR 2010, S. 751 (755).
32 BR-Drs. 535/10 S. 18.
33 Tinnefeld/Petri/Brink, MMR 2010, S. 727 (732).
34 Zimmer/Stetter, BB 2006, S. 1445 (1449) (Pflichtverletzung durch Korruption).
35 So auch Heinson, BB 2010, S. 3084 (3085).
36 Gola/Schomerus, BDSG, § 28, Rn. 13; Spindler/Nick, in: Spindler/Schuster, Recht der elektronischen Medien, BDSG, § 28, Rn. 4.
37 Vgl. Heinson, BB 2010, S. 3084 (3086).

intensiven Maßnahmen zur Wahl stehen. Daten, die keinen oder nur geringen Aufschluss über Compliance und Risikomanagement relevante Umstände geben, sind daher von der Datenverarbeitung auszuschließen. Ferner kann die anonymisierte oder pseudonymisierte Verarbeitung als weniger eingriffsintensive Maßnahme zu wählen sein. Im Rahmen der Angemessenheitsprüfung sind die entgegenstehenden Interessen festzustellen und zu einem schonenden Ausgleich zu bringen. Maßnahmen der IT-Compliance und des IT-Risikomanagements können damit intensivere Eingriffe rechtfertigen, wenn sie der Abwehr größerer Schädigungspotentiale für das Unternehmen dienen. Mit zunehmender Intensität und Dauer solcher Maßnahmen ergibt sich aber auch eine erhöhte Rechtfertigungslast. Unzulässig ist die Nutzung personenbezogener Daten jedenfalls, wenn ein ständiger Überwachungsdruck erzeugt wird[38] oder Daten vieler unbeteiligter Personen betroffen sind.[39]

38 BVerfG NJW 1984, 419; BAG NZA 2004, 1278 (1281); Kock/Francke, NZA 2009, S. 646 (648); Kratz/Gubbels, NZA 2009, S. 652 (654).

5 Fazit

Die Neuregelung des Arbeitnehmerdatenschutzes in §§ 32-32l BDSG-E hat den Anspruch, seit langer Zeit geforderte Regelungen zum Arbeitnehmerdatenschutz zu schaffen, die bisher allgemeinen und im Einzelfall unklaren oder schwer verständlichen und wenig spezifischen Regelungen abzulösen und klare Regelungen und damit Rechtssicherheit für die Beschäftigten, aber auch die Arbeitgeber zu schaffen.[40] Damit hat sich der Gesetzgeber, wie es lange von der Literatur gefordert wurde, eines hoch komplexen Regelungsbereiches angenommen. Belegt wird dies nicht zuletzt durch den Umfang der Neuregelung. Dreizehn neue und umfangreiche Paragraphen werden mit der Novelle in das BDSG eingefügt und viele tatbestandliche Voraussetzungen der Datenerhebung und -verarbeitung explizit normiert, die sich zuvor nur aus den Generalklauseln der §§ 28 und 32 BDSG ableiten ließen. Zu fragen ist, ob hiermit tatsächlich ein mehr an Rechtsklarheit für die Betroffenen geschaffen wird oder nur eine komplexe Konkretisierung außerhalb der gesetzlichen Regelung zulasten der Normenverständlichkeit in das Gesetz übernommen wird. Trotz ihres Umfangs stoßen aber auch diese umfassenden Neuregelungen auf das Problem jeder gesetzlichen Regelung. Sie können nicht jeden Einzelfall abschließend regeln. Die Rechtfertigung der Datenverarbeitung in Beschäftigungsverhältnissen allgemein und zur Erfüllung von Compliance- und Risikomanagementpflichten mittels IT-gestützter Verfahren wird daher auch künftig zu wesentlichen Teilen von ihrer Verhältnismäßigkeit im Einzelfall abhängen.

39 BVerfG NJW 2004, 999; Brandt, CuA 3/2009, S. 25 (26); Brandt, CuA 11/2009, S. 6 (8); Forst, RDV 2009, S. 204 (210); Kock/Francke, NZA 2009, S. 646 (648); Taeger/Schmidt, in: Taeger/Gabel, BDSG, Einl., Rn. 27; Schmidt, RDV 2009, S. 193 (198); Steinkühler, BB 2009, S. 1294 f.; a.A. offenbar Diller, BB 2009, S. 438 (439 f.).

40 BR-Drs. 535/10, S. 1f.