

Gesetzentwurf

der Abgeordneten Dr. Konstantin von Notz, Beate Müller-Gemmeke, Volker Beck (Köln), Birgitt Bender, Katrin Goering-Eckardt, Memet Kilic, Sven-Christian Kindler, Maria Klein-Schmeink, Stephan Kühn, Jerzy Montag, Brigitte Pothmer, Elisabeth Scharfenberg, Christine Scheel, Dr. Harald Terpe, Wolfgang Wieland, Josef Philip Winkler und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen

A. Problem

Bislang fehlt es an einer übergreifenden, das verfassungsrechtliche Leitbild informationeller Selbstbestimmung verwirklichenden bereichsspezifischen Regelung für den Umgang mit Daten und Informationen der Beschäftigten im Arbeitsverhältnis.

Im Bundesdatenschutzgesetz (BDSG) wurde mit der letzten Novelle des Gesetzes im Jahre 2009 zwar die Generalklausel des § 32 BDSG eingeführt, ansonsten aber kommen dessen allgemeine Bestimmungen zur Anwendung. Das Akteneinsichtsrecht in § 83 des Betriebsverfassungsgesetzes wurde 1972 festgeschrieben. In § 106 Bundesbeamtengesetz (BBG) etwa wird der Umgang mit der Personalakte von Beamtinnen und Beamten geregelt. Das Betriebsverfassungsgesetz (BetrVG) schafft insbesondere mit den §§ 80, 87, 94 BetrVG eine Mitsprache für Betriebsräte. Geregelt wurden damit lediglich Einzelfragen. Eine Systematisierung der verstreuten Regelungen gibt es nicht. Weiterer Schutz der Beschäftigten erfolgt durch die Rechtsprechung. Die Urteile betreffen lediglich Teilaspekte der Sachprobleme, sind von der Einzelfallperspektive geprägt und gelegentlich nicht frei von Widersprüchen. Von führenden Arbeitsrechtlerinnen und Arbeitsrechtlern wird dieser Zustand schon lange beklagt, ebenso von Gewerkschaften und den Vertreterinnen und Vertretern des Datenschutzes. Die Forderung nach für alle Beteiligten klaren und transparenten gesetzlichen Regelungen zum Schutz der persönlichen Daten der Beschäftigten wurde auch im Deutschen Bundestag über die Parteigrenzen hinweg immer wieder erhoben. Der Beschäftigtendatenschutz ist aber einer der wenigen Bereiche, dem bis heute die nahezu einhellig geforderte bereichsspezifische Regelung wichtiger Fragen des Datenschutzes versagt geblieben ist. Dabei hat die weitgehende Durchdringung aller Abläufe und Funktionen mit Informationstechnologien die Arbeit selbst von kleineren Betrieben und Verwaltungen grundlegend verändert.

Die Beschäftigten sind in privaten Unternehmen und bei öffentlichen Stellen zahlreichen Kontrollen ausgesetzt. Der Einsatz komplexer und leistungsfähiger Informations- und Kommunikationstechniken macht eine immer engmaschigere Überwachung der Beschäftigten bis in den privaten Bereich möglich. Die neuen technischen Möglichkeiten haben dazu geführt, dass die Telekommunikation, der E-Mail-Verkehr und die Internetnutzung der Beschäftigten ohne konkreten Anlass bis ins Detail kontrolliert werden können.

Immer häufiger kommt es vor, dass Kunden und Beschäftigte gleichermaßen mit Kameras und Zugangskontrollsystemen bewacht und gespeichert werden. Fahrerinnen und Fahrer sowie Beschäftigte im Außendienst über das Handy zu orten ist keine Ausnahme mehr. Bei der Überwachung werden auch illegale Methoden eingesetzt. Es herrscht ein bürgerrechtlich zunehmend unhaltbarer Zustand.

B. Lösung

Die zahlreichen besonderen Regelungsprobleme erfordern eigene, sachgerechte Regelungen. Diese ergänzen, neben und mit anderen Spezialregelungen wie etwa dem Allgemeinen Gleichbehandlungsgesetz (AGG) und dem Gendiagnostikgesetz als bereichsspezifische Lösungen die allgemeinen Regelungen des BDSG, welches nur in ausdrücklich genannten Fällen zur Anwendung kommt.

Die Schaffung einer bereichsspezifischen Regelung folgt zugleich den grundrechtlichen Vorgaben. Der Schutz des Grundgesetzes gilt auch und insbesondere in der Arbeitswelt. Es ist dringend geboten, normenklare gesetzliche Regelungen zu schaffen, um die technische Entwicklung so zu steuern, dass „Gläserne Beschäftigte“ in Wirtschaft und Verwaltung verhindert werden. Gegenwärtig wissen weder die Beschäftigten noch die Betriebe, woran sie mit dem Datenschutz sind. Das zersplitterte Recht muss endlich zusammengefasst und an die Stelle der Kasuistik ein transparentes neues und in sich geschlossenes Gesetz treten.

Bei der Schaffung eines eigenen Gesetzes zum Schutz der persönlichen Daten der Beschäftigten in Privatunternehmen und in öffentlichen Stellen des Bundes und der Länder ist der Leitlinie zu folgen, dass in das allgemeine Persönlichkeitsrecht und in das Grundrecht der Beschäftigten auf informationelle Selbstbestimmung nicht tiefer eingegriffen werden darf, als es der Zweck des Arbeitsverhältnisses unbedingt erfordert. Das Bundesarbeitsgericht hat diesen Weg in seiner Rechtsprechung vielfach bereits vorgezeichnet. Urteile können aber Gesetze nicht ersetzen.

Die Neuregelungen dieses Gesetzentwurfs gelten für den gesamten Bereich der Nutzung von Telekommunikation im Betrieb, ebenso wie für die Telearbeit, die Personalbuchhaltung und die technische Überwachung. Die Bestimmungen des Gesetzes setzen gerade auch dort klare Grenzen, wo es keine gewerkschaftliche Vertretung, keine Personal- oder Betriebsräte und auch keine Tarifverträge sowie Betriebsvereinbarungen/Dienstvereinbarungen gibt.

Das Gesetz baut auf bereits bestehende Schutzbestimmungen insbesondere des Bundesdatenschutzgesetzes auf, konkretisiert und erweitert sie aber in Bezug auf die Besonderheiten eines Beschäftigungsverhältnisses. Das gilt für den strengen Zweckbindungsgrundsatz für die Verarbeitung von Beschäftigtendaten ebenso wie für ein striktes Verwertungsverbot für unrechtmäßig erlangte Informationen.

Im Einzelnen sieht der Gesetzentwurf eine Klagebefugnis für Gewerkschaften vor, um gerade dort den Schutz der Beschäftigten wirksam zu verbessern, wo die Beschäftigten aus Sorge um ihren Arbeitsplatz auf die Durchsetzung ihrer Rechte verzichten.

Gestärkt wird die Unabhängigkeit der betrieblichen Datenschutzbeauftragten, die auch für den Beschäftigtendatenschutz zuständig sein sollen. Ihre Rechte werden erweitert und ihre Bestellung wird mitbestimmungspflichtig. Die Beauftragten müssen bereits vor Einführung neuer technischer Systeme, Verfahren, Fragebogen oder medizinischer Tests umfassend mit eingebunden werden.

Geregelt wird ein ausdrücklich verbrieftes Maßregelungsverbot für die Arbeitgebenden. Beschäftigte, die ihre Rechte wahrnehmen, dürfen keinen Benachteiligungen unterliegen.

Besonders geschützt werden auch die Daten über die Gesundheit und die privaten Verhältnisse von Bewerberinnen und Bewerbern, ebenso wie der Beschäftigten. Heimliches Erheben von Daten ist in jedem Fall untersagt.

Streng begrenzt wird auch die Kontrolle und Überwachung der Beschäftigten. Auch hier gilt der Grundsatz, dass heimliche Überwachungen zur Leistungskontrolle nicht zulässig sind.

Zur Durchsetzung der Bestimmungen dieses Gesetzes zum Schutz der Beschäftigtendaten sollen die Aufsichtsbehörden empfindliche Geldbußen verhängen dürfen. In bestimmten Fällen können diese bis zu einer Million Euro betragen.

Die gesetzlichen Neuregelungen dürfen nicht allein auf große Betriebe und Konzerne zugeschnitten sein. Sie müssen auch in kleinen Betrieben handhabbar und praxistauglich sein.

C. Alternativen

Der von der Bundesregierung vorgelegte Entwurf eines Beschäftigtendatenschutzgesetzes (Bundestagsdrucksache 17/4230) stellt keine geeignete Alternative dar. Durch die Einfügung in das BDSG wird das Verständnis sowohl des BDSG insgesamt als auch der neuen Vorschriften erheblich erschwert. Bei Bestimmungen zum Beschäftigtendatenschutz handelt es sich ferner ganz überwiegend um bereichsspezifisches Recht, dessen Zusammenlegung mit den das gesamte Datenschutzrecht übergreifend betreffenden BDSG-Bestimmungen nicht sachgerecht erscheint. Der Entwurf der Bundesregierung trägt zudem der auf das Arbeitsverhältnis zu übertragenden verfassungsrechtlichen Verpflichtung des Gesetzgebers zur Schaffung von wirksamen Datenschutzregelungen nicht angemessene Rechnung: insbesondere fehlt es an hinreichenden Maßnahmen zum Schutz im Bewerbungsverhältnis, vor der Überwachung der am Arbeitsplatz genutzten Kommunikationsmittel sowie bei der Gewährleistung einer effektiven und breiter gefächerten Datenschutzaufsicht.

D. Finanzielle Auswirkungen auf öffentliche Haushalte

Die neuen Befugnisse der Datenschutzbeauftragten in den öffentlichen Stellen werden aller Voraussicht nach einen erhöhten Schulungsbedarf mit sich bringen. Dieser Mehraufwand ist aber gerechtfertigt. Beim Schutz der Beschäftigtenrechte geht es um eine substantielle Erweiterung des Tätigkeitsfeldes der Beauftragten. Wir haben es hier mit besonders sensiblen Daten zu tun, gerade im Bereich der Gesundheitsdaten. Der verstärkte Kontakt mit den Beschäftigten und deren Interessenvertretungen wird auch den Zeitaufwand für die Arbeit erhöhen. Gewisse Mehrkosten entstehen auch durch einen leicht erhöhten sächlichen Aufwand der Beauftragten und durch eine erweiterte Freistellung von den sonstigen Aufgaben.

E. Sonstige Kosten

Für Unternehmen werden durch die verbesserten Maßnahmen zum Schutz der personenbezogenen Beschäftigtendaten gewisse finanzielle Mehrbelastungen entstehen, beispielsweise durch Einsatz datenschutzfreundlicher Verfahren. Kosten entstehen auch durch die erweiterten Informationspflichten gegenüber den Beschäftigten und dem Datenschutzbeauftragten. Der Ausbau der Stellung der betrieblichen Datenschutzbeauftragten ist mit zusätzlichen finanziellen Aufwendungen verbunden. So sind weitere Schulungen nötig. Die zu erwartenden Mehrkosten halten sich aber in einem überschaubaren Rahmen. Sie werden zum Teil sogar kompensiert, weil auf die Bestellung zusätzlicher Beauftragter innerhalb des Betriebs oder der Behörde verzichtet wird.

F. Bürokratiekosten

Bei der Umsetzung des Beschäftigtendatenschutzes im öffentlichen Bereich können geringfügig höhere Verwaltungskosten und Kosten für eine verbesserte Software entstehen. Kosten entstehen auch durch die erweiterten Informationspflichten gegenüber den Beschäftigten und dem Datenschutzbeauftragten. Für Betriebe sind erhöhte Bürokratiekosten nicht oder nur in einem sehr geringen Umfang zu erwarten. Dem steht aber ein deutlich angehobener Standard von Datenschutz und Datensicherheit in den Behörden und Betrieben gegenüber.

elektronische Vorabfassung*

Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen

Vom.....

Der Bundestag hat das folgende Gesetz beschlossen:

Inhaltsübersicht:

Artikel 1 Beschäftigtendatenschutzgesetz (BDatG)

1. Abschnitt: Allgemeine Grundsätze

- § 1 Ziel des Gesetzes
- § 2 Anwendungsbereich
- § 3 Begriffsbestimmungen

2. Abschnitt: Datenverarbeitung von Beschäftigtendaten

- § 4 Zulässigkeit und Grundsätze der Datenverarbeitung
- § 5 Datengeheimnis, Datensparsamkeit, Datensicherheit
- § 6 Datenverarbeitung vor Begründung eines Beschäftigungsverhältnisses
- § 7 Übermittlung der Beschäftigtendaten an Dritte
- § 8 Datenerhebungen im Bewerbungsverhältnis
- § 9 Gesundheitsdaten und Testverfahren

3. Abschnitt: Besondere Kontrollen der Beschäftigten

- § 10 Videoüberwachung am Arbeitsplatz
- § 11 Raster-Abgleich von Beschäftigtendaten (Screening-Verfahren)
- § 12 Einsatz von Telekommunikationsdiensten
- § 13 Benachrichtigungspflicht

4. Abschnitt: Einsatz besonderer Verfahren

- § 14 Fernarbeit
- § 15 Einsatz von Ortungssystemen
- § 16 Einsatz biometrischer Verfahren
- § 17 Trennung der Daten aus Arbeits- und Schuldverhältnis

5. Abschnitt: Rechte und Pflichten

- § 18 Informationsrechte der Beschäftigten
- § 19 Benachrichtigung bei unrechtmäßiger Kenntniserlangung von Daten
- § 20 Führung und Einsicht der Personalunterlagen
- § 21 Korrekturen
- § 22 Ansprüche der Beschäftigten bei Verstoß gegen ihre Rechte
- § 23 Verbandsklagerecht für Betriebsräte und Gewerkschaften
- § 24 Grenzen der Verschwiegenheitspflicht für Beschäftigte
- § 25 Arbeitsrechtliches Benachteiligungsverbot

6. Abschnitt: Sonderbestimmungen

- § 26 Überwachung im Auftrag der Arbeitgebenden
- § 27 Datenübermittlung bei Betriebsübergang

7. Abschnitt: Organisatorischer Datenschutz

§ 28 Betriebliche Datenschutzbeauftragte

§ 29 Vorabkontrolle durch die Datenschutzbeauftragten

§ 30 Anrufung der Beauftragten für den Beschäftigtendatenschutz

§ 31 Aufsichtsbehörde

8. Abschnitt: Datenschutz in den Interessenvertretungen

§ 32 Rechte von Betriebs- und Personalräten

§ 33 Datenverarbeitung von Betriebs- und Personalräten

9. Abschnitt: Schlussbestimmungen

§ 34 Unabdingbare Rechte der Beschäftigten

§ 35 Bußgeldvorschriften

Artikel 2**Änderung des Bundesdatenschutzgesetzes****Artikel 3****Änderung des Betriebsverfassungsgesetzes****Artikel 4****Änderung des Bundespersonalvertretungsgesetzes****Artikel 5****Änderung des Gendiagnostikgesetzes****Artikel 6****Änderung des Sozialgesetzbuchs III****Artikel 7****Änderung des Arbeitsgerichtsgesetzes****Artikel 8****Inkrafttreten**

Artikel 1 **Beschäftigtendatenschutzgesetz (BDatG)**

1. Abschnitt: Allgemeine Grundsätze

§ 1

Ziel des Gesetzes

Ziel dieses Gesetzes ist die Stärkung der Persönlichkeitsrechte und des Grundrechts auf informationelle Selbstbestimmung der Beschäftigten bei der Verarbeitung ihrer personenbezogenen Daten und Informationen im Beschäftigtenverhältnis.

§ 2

Anwendungsbereich

(1) Dieses Gesetz gilt für die Verarbeitung von Beschäftigtendaten durch Arbeitgebende und die in ihrem Auftrag handelnden Personen handelnden Stellen.

(2) Dieses Gesetz gilt für alle Formen der Verarbeitung personenbezogener Daten Beschäftigter durch öffentliche und nicht-öffentliche Arbeitgebende selbst und in deren Auftrag durch Dritte im Zusammenhang mit der Anbahnung, Durchführung und Abwicklung von Beschäftigungsverhältnissen.

(3) Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(4) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(5) Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen. Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zweck des Transits durch das Inland eingesetzt werden. § 38 Abs. 1 Satz 1 BDSG bleibt unberührt.

§ 3

Begriffsbestimmungen

(1) Beschäftigte sind

1. Arbeitnehmerinnen und Arbeitnehmer,
2. zu ihrer Berufsausbildung Beschäftigte,
3. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,
4. Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

5. Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Leiharbeit, Heimarbeit, als Honorarkräfte und in Praktika Beschäftigten.

(2) Arbeitgebende ist jede natürliche oder juristische Person oder Personengesellschaft (nicht-öffentliche Stelle) sowie eine öffentliche Stelle, die andere Personen im Sinne von Nr. 1 beschäftigt, beschäftigt hat oder ein Beschäftigungsverhältnis anbahnt. Bei in Heimarbeit Beschäftigten und den ihnen Gleichgestellten sind Arbeitgebende die Auftraggebende oder Zwischenmeister im Sinne des Heimarbeitsgesetzes, bei Beschäftigten, die einem Dritten zur Arbeitsleistung überlassen werden, auch der Dritte.

(3) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person.

(4) Beschäftigtendaten sind personenbezogene oder personenbeziehbare Daten und Informationen über Angehörige der in Abs. 1 Nr. 1 bis 5 genannten Personengruppen, die in Zusammenhang mit der Anbahnung, Begründung, Durchführung, Beendigung oder Abwicklung eines Beschäftigungsverhältnisses oder für die in diesem Gesetz im Einzelnen aufgeführten zulässigen Zwecke verarbeitet werden.

(5) Personalakte im nicht-öffentlichen Bereich ist jede Sammlung von schriftlichen Unterlagen über bestimmte Beschäftigten, ohne Rücksicht auf die Form, in der sie geführt werden, sofern sie mit dem Beschäftigungsverhältnis in einem inneren Zusammenhang steht.

(6) Verarbeitung personenbezogener Daten von Beschäftigten ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten.

(7) Biometrische Daten sind Verkörperungen physiologischer Merkmale, die geeignet sind, einen Menschen eindeutig und zweifelsfrei zu kennzeichnen.

(8) Ein Raster-Abgleich von Daten (Screening-Verfahren) im Sinne dieses Gesetzes ist die Analyse von zu unterschiedlichen Zwecken vorliegenden Datenbeständen im Sinne eines systematischen Testverfahrens, das verwendet wird, um innerhalb einer bestimmten Gruppe von Beschäftigten Eigenschaften, Verhältnisse oder Verhaltensweisen zu identifizieren.

(9) Fernarbeit ist die Verarbeitung personenbezogener Daten im Rahmen der beruflichen Tätigkeit in den privaten Räumen der Beschäftigten, Telearbeitszentren, im Rahmen mobiler Telearbeit oder eines Zusammenschlusses rechtlich unabhängiger selbstständiger Unternehmen.

2. Abschnitt: Datenverarbeitung von Beschäftigtendaten

§ 4

Zulässigkeit und Grundsätze der Datenverarbeitung

(1) Die Verarbeitung von personenbezogenen Daten Beschäftigter ist außer in den Fällen des Absatz 4 nur zulässig, soweit dieses Gesetz, eine auf Grundlage dieses Gesetzes geschaffene Betriebs- oder Dienstvereinbarung sowie Tarifvertrag oder eine andere Rechtsvorschrift dies erlaubt, ausdrücklich anordnet oder in ausdrücklich in diesem Gesetz geregelten Fällen die Einwilligung der Beschäftigten

vorliegt. Die Rechte der Betroffenen nach diesem Gesetz sowie anderen Rechtsvorschriften zum Schutz ihrer personenbezogenen Daten können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Einwilligungen sind nur wirksam, wenn sie auf der freien Entscheidung der Beschäftigten beruhen. Es ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Vor Beginn der Datenverarbeitung sind die betroffenen Beschäftigten umfassend über den Zweck zu informieren.

(3) Neben diesem Gesetz kommen die weitergehenden spezialgesetzlichen Bestimmungen zur Anwendung. Das Bundesdatenschutzgesetz bleibt anwendbar, soweit dieses Gesetz kein höheres Schutzniveau einräumt. Insbesondere die Bestimmungen der §§ 4 Absatz 1, 12 Abs. 4, 16, sowie der 28-32 BDSG sind nicht anwendbar.

(4) Der Arbeitgebende darf personenbezogene Daten der Beschäftigten verarbeiten, wenn deren Kenntnis erforderlich ist, um während des Beschäftigungsverhältnisses oder nach dessen Beendigung die Verpflichtungen zu erfüllen, die sich

1. durch Gesetz oder auf Grund eines Gesetzes bestehende Offenlegungs-, Erhebungs-, Auskunfts-, Melde- oder Zahlungspflichten oder
2. durch vertragliche Verpflichtungen aus dem Beschäftigungsverhältnis gegenüber dem Beschäftigten ergeben

Gesetzliche Verpflichtungen sind den Beschäftigten mitzuteilen.

(5) Daten, deren Verarbeitung entgegen den Bestimmungen dieses Gesetzes oder anderer Vorschriften zum Schutz der personenbezogenen Daten der Beschäftigten, einer Betriebsvereinbarung, eines Tarifvertrages oder eines Mitbestimmungstatbestandes erfolgt, dürfen nicht zu weiteren Zwecken verwendet werden.

§ 5

Datengeheimnis, Datensparsamkeit, Datensicherheit

(1) Beschäftigtendaten dürfen nicht unbefugt verarbeitet werden. Die mit dieser Aufgabe betrauten Personen sind schriftlich auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

(2) Zum Schutz des Datengeheimnisses legt der Arbeitgebende den Kreis der Personen oder Stellen fest, die Beschäftigtendaten verarbeiten. Er hat die technischen und organisatorischen Maßnahmen nach § 9 des BDSG zu treffen.

(3) Die Verarbeitung und die Auswahl und Gestaltung von informationstechnischen Systemen zur Verarbeitung von Beschäftigtendaten sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. Insbesondere sind personenbezogene Daten zu anonymisieren oder anderenfalls zu pseudonymisieren, soweit es für den Verwendungszweck möglich ist und keinen im Verhältnis zum angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

(4) Beschäftigtendaten, die zur Datenschutzkontrolle und Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage in Dateien gespeichert oder in Unterlagen

aufgenommen wurden, dürfen nur für diese Zwecke verwendet werden. Zum Schutz der Vertraulichkeit von Beschäftigtendaten und zum Schutz vor unbefugten Veränderungen sollen diese verschlüsselt werden.

§ 6

Datenverarbeitung vor Begründung eines Beschäftigungsverhältnisses

(1) Personenbezogene Daten sind unmittelbar bei Bewerbenden und Beschäftigten zu erheben. Im Einzelfall ist die Einholung von Informationen bei Dritten oder durch Dritte zulässig, wenn diese für die Feststellung der Eignung für die vorgesehene Tätigkeit wesentlich und entscheidend sind und die Betroffenen dem Verfahren schriftlich zugestimmt haben. Bewerbenden und Beschäftigte sind über den Inhalt der Informationen zu unterrichten.

(2) Kommt ein neues Beschäftigungsverhältnis oder eine vergleichbare Veränderung bei dem gleichen Arbeitgebenden nicht zustande, sind die Unterlagen den Bewerbern oder den Beschäftigten binnen zwei Monaten nach Abschluss des Bewerbungsverfahrens zu übergeben. Gespeicherte personenbezogene Daten sind zu löschen und Aufzeichnungen zu vernichten. Satz 1 findet keine Anwendung, wenn die Bewerber oder die Beschäftigten in eine längere Aufbewahrung ausdrücklich einwilligt haben.

(3) Gibt der Arbeitgebende auf der eigenen Internetseite Gelegenheit, elektronische Bewerbungen durchzuführen, ist diese Internetverbindung zu verschlüsseln. Die gespeicherten Daten sind durch besondere technische Sicherungsmaßnahmen zu schützen. Die Nutzung der übermittelten Daten ist ausschließlich auf das Bewerbungsverfahren beschränkt.

(4) Der Arbeitgebende hat keinen Anspruch auf Auskunft über medizinische Diagnosen und Befunde der Bewerbenden bzw. Beschäftigten.

(5) Der Arbeitgebende hat bei sonstigen Tests, die Fähigkeiten und Kenntnisse der Bewerbernde bzw. Beschäftigten erfassen, über Methoden, Ergebnisse und weitere Auswirkungen dieser Verfahren die Beschäftigten bzw. Bewerbenden umfassend zu unterrichten. Die Erstellung von Profilen, die über die für die Eignungsfeststellung für konkrete Tätigkeiten unbedingt erforderlichen Informationen hinausgehen, ist unzulässig.

(6) Die Vorschriften des Zweiten Abschnitts über die Erhebung der Daten bei den Beschäftigten bzw. Bewerbenden nach § 4 Absatz 1 und 2 sowie die Vorschriften über die Datenerhebungen im Bewerbungsverhältnis nach § 8 und den Schutz der Gesundheitsdaten nach § 9 gelten auch zum Schutz der personenbezogenen Daten während des Beschäftigungsverhältnisses.

(7) Nach Abschluss des Beschäftigungsverhältnisses sind alle personenbezogenen Daten und Akten der ausgeschiedenen Beschäftigten zu löschen oder zu vernichten, soweit diese keinen gesetzlichen, satzungsmäßigen oder vertraglichen Aufbewahrungsfristen unterliegen. In diesen Fällen sind die Unterlagen ausschließlich für Zwecke der Aufbewahrung zu verarbeiten.

(8) Die Verfahren nach Absatz 2 und 3 unterliegen neben der Vorabkontrolle der betrieblichen Datenschutzbeauftragten auch der Kontrolle des Betriebsrats oder der Personalvertretung.

(9) Daten, deren Verarbeitung gegen Bestimmungen dieses Gesetzes oder anderer Vorschriften zum Schutz der personenbezogenen Daten der Bewerbenden bzw. Beschäftigten, einer Betriebsvereinbarung, eines Tarifvertrages oder eines Mitbestimmungstatbestands erhoben wurden, dürfen nicht verwendet werden.

§ 7

Übermittlung der Beschäftigtendaten an Dritte

(1) Die §§ 4a Absatz 1 und 2, 4b, 4c, 11, 16 und 39 BDSG bleiben unberührt.

(2) Die Übermittlung von Beschäftigtendaten zwischen rechtlich selbständigen Unternehmen innerhalb von Konzernverbänden ist nur zulässig, soweit sie zur Wahrung eines betrieblichen Interesses, das in

unmittelbarem Zusammenhang mit dem Beschäftigungsverhältnis steht, erforderlich ist und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Vor oder bei der Übermittlung muss das übermittelnde Unternehmen den Betroffenen Zweck, und Ausmaß mitteilen. Zweck, Ausmaß und andere Modalitäten der Übermittlung können auf Grundlage dieses Gesetzes auch durch Betriebsvereinbarung geregelt werden, soweit dadurch das Schutzniveau dieses Gesetzes nicht unterschritten wird.

(3) Die Übermittlung der Daten erfolgt in verschlüsselter Form.

(4) Dritte dürfen diese Daten nur für den Zweck verarbeiten, für den sie ihnen übermittelt wurden. Dies gilt im Fall des Absatzes 2 entsprechend.

§ 8

Datenerhebungen im Bewerbungsverhältnis

(1) Datenerhebungen zu besonderen Arten personenbezogener Daten nach § 3 Abs. 9 des Bundesdatenschutzgesetzes sind unzulässig, es sei denn ihre Kenntnis ist im Einzelfall erforderlich, um Beeinträchtigungen bei der Verwendung auf dem vorgesehenen Arbeitsplatz festzustellen, die sich wesentlich und entscheidend auf die Erbringung der geschuldeten Arbeitsleistung auswirken. Fragen nach dem Sexualleben oder der sexuellen Identität (Orientierung) sind unzulässig.

(2) Datenerhebungen zu den persönlichen Vermögensverhältnissen sind unzulässig, es sei denn, die Kenntnis ist erforderlich, weil die auszuübende Tätigkeit ausschließlich oder ganz überwiegend in der Betreuung fremden Vermögens besteht und ein besonderes Vertrauensverhältnis begründet. Fragen nach dem früheren Gehalt dürfen im Einzelfall gestellt werden, soweit sie Gegenstand der Verhandlung über die Einstellung sind oder für die Feststellung der Qualifikation der Bewerberin oder des Bewerbers erforderlich sind; diese Regelung gilt entsprechend für die Zulässigkeit von Selbstauskünften bei Auskunfteien.

(3) Datenerhebungen zu einer vorliegenden oder geplanten Schwangerschaft sowie Fragen zu den Familienverhältnissen sind unzulässig.

(4) Fragen nach einer Behinderung sind unzulässig, es sei denn eine bestimmte körperliche Funktion oder geistige Fähigkeit oder die seelische Gesundheit stellt eine wesentliche und unabdingbare berufliche Anforderung für die auszuübende Tätigkeit dar.

(5) Fragen nach geleistetem oder bevorstehenden Wehr- oder Zivildienst sind bei Begründung eines nicht befristeten Beschäftigungsverhältnisses unzulässig.

(6) Fragen nach laufenden Ermittlungsverfahren, anhängigen Strafverfahren oder Vorstrafen sind grundsätzlich unzulässig. Sie dürfen im Einzelfall nur dann gestellt werden, wenn sie in einem unmittelbaren Bezug zu der auszuübenden Tätigkeit stehen.

(7) Die Einholung und Verwendung graphologischer Gutachten durch die Arbeitgebenden ist unzulässig.

§ 9

Gesundheitsdaten und Testverfahren

(1) Der Abschluss des Arbeitsvertrages darf nicht von einer Gesundheitsprüfung abhängig gemacht werden, es sei denn, die medizinische oder psychologische Untersuchung ist erforderlich für die Feststellung, ob diese Daten der Bewerberin oder des Bewerbers zum Zeitpunkt der Arbeitsaufnahme

wegen der Art der auszuübenden Tätigkeit und der Bedingungen ihrer Ausübung wesentliche und entscheidende berufliche Anforderungen oder Hindernisse darstellen.

(2) Eine Gesundheitsprüfung ist nur zulässig, wenn die Bewerberin oder der Bewerber nach vorheriger Aufklärung über Art und Umfang der Gesundheitsprüfung schriftlich zugestimmt hat. Die Bewerberin oder der Bewerber hat einen Anspruch auf umfassende Information über die Untersuchung und den Zusammenhang mit der Entscheidung über die Begründung oder das Nichtzustandekommen des Arbeitsverhältnisses.

(3) Eine Gesundheitsuntersuchung der Beschäftigten bzw. Bewerbenden ist unzulässig, es sei denn, sie ist im Gesetz oder auf Grund eines Gesetzes angeordnet und für die jeweilige Aufgabenstellung insbesondere bei gefahrgeneigten Tätigkeiten unerlässlich. Der Umfang der Untersuchung ist auf die Informationen zu beschränken, die auch bei medizinischer Behandlung die Erfüllung der vertraglich geschuldeten Tätigkeiten der Beschäftigten gefährden würde.

(4) Medizinische und psychologische Tests dürfen nur durch Fachpersonal durchgeführt werden. Eine Entbindung von der Schweigepflicht ist unwirksam. Arbeitgebenden gegenüber darf ausschließlich der Grad der Eignung der Bewerberinnen und Bewerber mitgeteilt werden.

(5) Alkohol- oder Drogentests ohne Wissen der Beschäftigten und Bewerbenden sind unzulässig. Mit Zustimmung der Betroffenen sind Tests nur dann zulässig, wenn besondere Unfallrisiken oder Fremdgefährdungen bestehen oder der Arbeitsplatz mit einer Sicherheits- und Überwachungstätigkeit oder dem Gebrauch von Waffen verbunden ist.

(6) Tests ohne Wissen der Beschäftigten und Bewerbenden auf übertragbare vorhandene Erkrankungen, insbesondere Infektions- oder Immunschwächekrankheiten, sind unzulässig. Mit Zustimmung der Betroffenen sind Tests nur dann zulässig, wenn ansonsten ein unvertretbares Infektionsrisiko für Dritte bestünde.

(7) Für gendiagnostische Untersuchungen gelten die Vorschriften des Fünften Abschnitts des Gendiagnostikgesetzes über genetische Untersuchungen im Arbeitsleben.

3. Abschnitt: Besondere Kontrollen der Beschäftigten

§ 10

Videüberwachung am Arbeitsplatz

(1) Im Betrieb verwendete Überwachungssysteme, die geeignet sind, in das informationelle Selbstbestimmungsrecht der Beschäftigten einzugreifen, dürfen nicht zu deren Leistungskontrolle und zur Leistungsmessung eingesetzt werden. Ihr Einsatz in Bereichen, die auch als kollektive und kommunikative Rückzugsräume sowie der privaten Lebensgestaltung dienen, ist unzulässig.

(2) Daten von Beschäftigten, die bei der Überwachung des Betriebsgeländes, des Betriebsgebäudes, der Betriebsräume oder den Räumen der öffentlichen Stelle mit optisch-elektronischen Überwachungsgeräten anfallen, dürfen nur unter den Voraussetzungen und im Rahmen der Zweckbestimmung und der Lösungsfristen des § 6b des BDSG erhoben und verwendet werden. Die Beobachtung ist durch gut sichtbare Hinweisschilder erkennbar zu machen.

(3) Eine Beobachtung ohne Wissen der Beschäftigten mit optisch-elektronischen Einrichtungen ist unzulässig, es sei denn, in einem konkret bestimmten Einzelfall begründen bestimmte Tatsachen den Verdacht, dass

1. der oder die Beschäftigte im Beschäftigungsverhältnis Straftaten zum Nachteil des Betriebs oder des öffentlichen Arbeitgebenden begangen hat und die Tat schwer wiegt,
2. die Erhebung zur deren Aufklärung geeignet und erforderlich ist,
3. das Interesse des Arbeitgebenden an der Aufklärung das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Überwachung überwiegt, und

4. auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Daten der Beschäftigten erfasst werden, die für die Erforschung des Sachverhalts von Bedeutung sind, und

5. die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre.

Der Zeitraum für die Beobachtung ist insgesamt auf höchstens drei Wochen zu begrenzen.

(4) Die Verwendung von Überwachungssystemen, die ihrer äußeren Form als Nachbildungen von Überwachungssystemen den Anschein von Videoüberwachung hervorrufen (Attrappen) sind den Systemen nach Absatz 1 gleichgestellt.

(5) Die gespeicherten Bilddaten sind unverzüglich zu löschen, wenn sie zur Erreichung des Beobachtungszwecks nicht mehr erforderlich sind.

§ 11

Raster-Abgleich von Beschäftigtendaten (Screening-Verfahren)

(1) Ein Raster-Abgleich von Daten (Screening-Verfahren) von Beschäftigtendaten ist nur im Einzelfall zulässig, soweit und solange konkrete Anhaltspunkte den Verdacht begründen, dass Beschäftigte im Beschäftigungsverhältnis Straftaten gegen den Wettbewerb zum Nachteil der Arbeitgebenden nach dem Sechszwanzigsten Abschnitt des Strafgesetzbuchs oder nach §§ 333, 334, auch in Verbindung mit § 335 Absatz 1 Nr. 1 b des Strafgesetzbuches, begangen haben.

(2) Bei der Durchführung der Screening-Verfahren sind die Grundsätze der Verhältnismäßigkeit zu beachten. Die Verfahren sind, soweit möglich, anonymisiert, ansonsten pseudonymisiert durchzuführen. Die Daten sind nach Erreichung ihres Zwecks zu löschen.

§ 12

Einsatz von Telekommunikationsdiensten

(1) Die Nutzung von Telefon, E-Mail, Internet und anderen Telekommunikationsdiensten soll durch Tarifvertrag oder Betriebsvereinbarung geregelt werden. Ist der Abschluss durch Tarifvertrag oder Betriebsvereinbarung nicht möglich, sollen die Arbeitgebenden direkt mit den Beschäftigten eine Vereinbarung treffen, in der festgelegt wird, ob und in welchem Umfang und unter welchen Voraussetzungen die Nutzung der in Satz 1 genannten Einrichtungen auch zu privaten Zwecken erlaubt ist. Die Zustimmung zur angemessenen privaten Nutzung der Einrichtungen gilt als erteilt, wenn kein Tarifvertrag oder Betriebsvereinbarung geschlossen, noch eine individuelle Vereinbarung mit den Beschäftigten geschlossen wurde.

(2) Ist den Beschäftigten die private Nutzung der Telekommunikationseinrichtungen untersagt, sind die Arbeitgebenden nur berechtigt, Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (Verkehrsdaten) zu erheben. Die Verarbeitung der Verkehrsdaten ist nur zulässig, wenn dies erforderlich ist zur Gewährleistung der Datensicherheit, zur Gewährleistung des ordnungsgemäßen Betriebs der Telekommunikationsnetze- oder dienste oder zur Abrechnung. Die Verkehrsdaten dürfen nur anonymisiert verwendet werden. Eine Erhebung der Inhalte der Nutzung ist unzulässig.

(3) Das heimliche Mithören und Aufzeichnen von Telefongesprächen der Beschäftigten ist unzulässig. Ein Mithören oder Aufzeichnen dienstlicher Gespräche ist nur dann zulässig, wenn dies zur Sicherung der Qualität oder zu Schulungszwecken erforderlich ist, lediglich stichprobenartig erfolgt und alle betroffenen Kommunikationsteilnehmenden dieser Maßnahme ausdrücklich zugestimmt haben. Die Aufzeichnungen sind nach Erfüllung ihres Zwecks zu löschen.

(4) Der Inhalt dienstlicher E-Mails oder Internet-Nutzungen darf von Arbeitgebenden im Einzelfall erhoben werden

1. zur Gewährleistung der Datensicherheit,
2. bei unabweisbaren dienstlichen Belangen,
3. wenn bestimmte Anhaltspunkte den Verdacht begründen, dass eine Beschäftigte oder ein Beschäftigter im Beschäftigungsverhältnis eine Straftat begangen hat,
4. bei Vorliegen einer Betriebsvereinbarung auch bei Verdacht auf besonders schwerwiegende Verletzungen des Arbeitsvertrags

und wenn bei Abwägung der Interessen das berechnete und schutzwürdige Interesse der Arbeitgebenden das Interesse der Beschäftigten auf Schutz seiner Privatsphäre überwiegt.

(5) Soweit die private Nutzung von Telefon, E-Mail, Internet und IT-technischen Systemen erlaubt ist, dürfen die Arbeitgebenden die dazu vorliegenden Daten, insbesondere die Verkehrsdaten ausschließlich zur Gewährleistung der Datensicherheit, zur Sicherstellung des ordnungsgemäßen Betriebes von Telekommunikationsnetzen oder Telekommunikationsdiensten oder zur Abrechnung verarbeiten. Eine Inhalteauswertung ist unzulässig.

(6) Die Verkehrsdaten sind unverzüglich, spätestens nach sieben Kalendertagen, zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Beschäftigten einer weiteren Speicherung entgegenstehen.

§ 13

Benachrichtigungspflicht

Werden Daten von Beschäftigten im Rahmen von Maßnahmen nach diesem Abschnitt bei Verdacht auf eine Straftat verarbeitet, sind die Arbeitgebenden verpflichtet, den betroffenen Beschäftigten unmittelbar nach Abschluss dieser Maßnahmen über deren Grund, die angewandten Methoden und Verfahren sowie die erhobenen Daten schriftlich zu unterrichten. Die Verpflichtung entfällt, wenn ansonsten die Aufdeckung einer Straftat gefährdet wäre.

4. Abschnitt: Einsatz besonderer Verfahren

§ 14

Fernarbeit

(1) Findet die Datenverarbeitung im Rahmen von Fernarbeit statt, bleiben die Auftraggebenden als verantwortliche Stellen nach § 3 Absatz 7 des Bundesdatenschutzgesetzes für die Datenverarbeitung verantwortlich; für Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag gelten die Vorschriften des § 11 des Bundesdatenschutzgesetzes.

(2) Eine Fernüberwachung zur Leistungs- oder Verhaltenskontrolle von Personen, die in Fernarbeit nach § 3 Absatz 9 tätig sind, ist unzulässig. (3) Die Arbeitgebenden haben als verantwortliche Stellen für die in Fernarbeit geleistete Verarbeitung personenbezogener Daten die erforderlichen technischen und organisatorischen Maßnahmen nach § 9 des Bundesdatenschutzgesetzes zu treffen. Für die Fernarbeitsplätze in privaten Räumen ist ein Datenschutzkonzept festzulegen, das die Vertraulichkeit der verarbeiteten Daten gegenüber Dritten, die Sicherheit der Datenintegrität sowie eine ausreichende Revision der Verarbeitung gewährleistet.

§ 15

Einsatz von Ortungssystemen

(1) Der Einsatz von Ortungssystemen zur Erhebung von Beschäftigtendaten ist nur zulässig, wenn die Daten für die Sicherheit des Beschäftigten erforderlich sind

und

keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Beschäftigten überwiegen.

(2) Eine Verwendung der Daten für andere Zwecke, insbesondere für die Erstellung von Bewegungsprofilen der Beschäftigten und zur Verhaltens- und Leistungskontrolle, ist unzulässig.

(3) Die Daten sind nach Erreichen des Zwecks ihrer Erhebung unverzüglich zu löschen.

§ 16

Einsatz biometrischer Verfahren

(1) Die Erhebung biometrischer Daten einschließlich der Verwendung von Lichtbildern zur Erhebung von Beschäftigtendaten ist nur zulässig, wenn

1. dies zu Autorisierungs- und Authentifizierungszwecken in besonders sicherheitsrelevanten Bereichen erforderlich ist,

2. die Beschäftigten nach § 4a Absatz 1 des Bundesdatenschutzgesetzes eingewilligt haben und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Beschäftigten überwiegen.

(2) Die Erhebung biometrischer Daten zur Zeiterfassung ist unzulässig.

(3) Zugriffe auf biometrische Daten sind zu protokollieren.

§ 17

Trennung der Daten aus Arbeits- und Schuldverhältnis

(1) Arbeitgebende dürfen personenbezogene Daten aus einem anderen Rechtsgeschäft mit einem oder einer Beschäftigten nicht mit den jeweiligen Beschäftigtendaten zusammenführen. Die jeweils für die Verarbeitung der rechtsgeschäftlichen Daten und der Beschäftigtendaten zuständigen Personen sind auf die Einhaltung der unterschiedlichen Zweckbestimmung der Daten hinzuweisen.

(2) Die personalverantwortliche Stelle darf auf die Daten aus anderen Rechtsgeschäften keinen Zugriff haben; die Unterlagen sind grundsätzlich getrennt aufzubewahren. Für die technischen und organisatorischen Maßnahmen gilt § 9 des Bundesdatenschutzgesetzes entsprechend.

5. Abschnitt: Rechte und Pflichten

§ 18

Informationsrechte der Beschäftigten

(1) Die Beschäftigten können nach Maßgabe von § 34 des Bundesdatenschutzgesetzes Auskunft über ihre bei den Arbeitgebenden vorliegenden Daten verlangen.

(2) Sie sind vor der erstmaligen Erhebung sowie vor einer beabsichtigten Nutzung und Verarbeitung der sie betreffenden Daten und auf Wunsch jährlich zu unterrichten. Diese Auskunft ist unentgeltlich.

(3) Werden Daten von Beschäftigten im Rahmen von Maßnahmen nach dem Vierten Abschnitt verarbeitet, sind die Arbeitgebenden verpflichtet, die betroffenen Beschäftigten vor Beginn dieser Maßnahmen über deren Grund, die angewandten Methoden und Verfahren sowie die erhobenen Daten zu unterrichten.

(4) Die Arbeitgebenden sind verpflichtet, einen Abdruck dieses Gesetzes an geeigneter Stelle zur Einsichtnahme auszulegen oder auszuhändigen.

§ 19

Benachrichtigung bei unrechtmäßiger Kenntniserlangung von Daten

(1) Arbeitgebende haben über ihre Informationspflicht nach § 42a des Bundesdatenschutzgesetzes hinaus die betroffenen Beschäftigten von sich aus unverzüglich und unmittelbar nach Kenntnisnahme über alle Fälle zu unterrichten, in denen Beschäftigtendaten unrechtmäßig übermittelt wurden oder deren Daten auf sonstige Weise Unbefugten zugänglich gemacht oder auf andere Weise in deren Bereich gelangt sind, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen wurden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird.

(2) Arbeitgebende sind nach Maßgabe des § 42a des BDSG verpflichtet, auch die betrieblichen Datenschutzbeauftragten zu benachrichtigen.

(3) Bei erheblichen Eingriffen in den Schutzbereich von Beschäftigten ist zusätzlich die nach § 38 BDSG zuständige Aufsichtsbehörde zu benachrichtigen.

§ 20

Führung und Einsicht der Personalunterlagen

(1) In der Personalakte dürfen grundsätzlich nur Informationen aufgenommen werden, die einen unmittelbaren Bezug zum Arbeitsverhältnis haben und deren Korrektheit nachweisbar ist.

(2) Die Beschäftigten haben ein Recht auf Einsicht in alle über sie geführten Personalakten und Unterlagen. Dieses Recht bleibt auch nach Beendigung des Beschäftigungsverhältnisses bestehen.

(3) Stellungnahmen der Beschäftigten zum Inhalt der Personalakten und zum Arbeitsverhältnis sind den Personalakten beizufügen.

(4) Das Recht auf Einsicht in die Personalakte haben auch Hinterbliebene der Beschäftigten.

(5) Medizinische und psychologische Befunde, die mit Zustimmung der Beschäftigten in die Personalakten aufgenommen wurden, müssen von den übrigen Unterlagen getrennt aufbewahrt werden. In die Personalakten ist ein entsprechender Hinweis aufzunehmen. Auf diese Daten darf von den Arbeitgebenden nur zurückgegriffen werden, wenn bei anstehenden Personalentscheidungen der Gesundheitszustand eine erhebliche Rolle spielt.

(5) Für das Verfahren der Akteneinsicht im nicht-öffentlichen Bereich findet § 83 Absatz 1 des Betriebsverfassungsgesetzes Anwendung. Die Rechte der Beamtinnen und Beamten aus den §§ 106 bis 115 des Bundesbeamtengesetzes sowie den entsprechenden Vorschriften des Landesrechts bleiben von den Vorschriften dieses Gesetzes unberührt.

(6) Abmahnungen werden nach spätestens zwei Jahren wirkungslos und sind aus der Personalakte zu entfernen.

§ 21

Korrekturen

(1) Arbeitgebende dürfen Beschäftigtendaten, die unrichtig sind oder in unzulässiger Weise erhoben wurden, nicht verwenden. Der Vorgang ist zu protokollieren.

(2) Die Arbeitgebenden haben die in die Unterlagen aufgenommenen oder gespeicherten Beschäftigtendaten unverzüglich zu entfernen oder zu löschen, wenn deren Aufnahme unzulässig war oder zur Erfüllung einer gesetzlichen Vorschrift nicht mehr erforderlich ist.

(3) Im nicht-öffentlichen Bereich sind die in Unterlagen oder Dateien aufgenommenen Missbilligungen von Beschäftigten spätestens nach Ablauf von drei Jahren zu entfernen, sofern in dieser Zeit keine erneute Missbilligung für ein vergleichbares Verhalten der Beschäftigten vorliegt. Beschäftigte haben einen Anspruch, die Aufnahme einer Gegenerklärung in die Personalakte zu verlangen; § 83 Absatz 2 des Betriebsverfassungsgesetzes gilt entsprechend.

(4) Die Arbeitgebenden haben die Beschäftigtendaten zu kennzeichnen, deren Verwendung durch eine Sperrung eingeschränkt ist. § 35 Abs. 3 und 4 des Bundesdatenschutzgesetzes finden entsprechende Anwendung.

§ 22

Ansprüche der Beschäftigten bei Verstoß gegen ihre Rechte

(1) Wenn aufgrund konkreter Anhaltspunkte zu erwarten ist, dass Arbeitgebende gegen eine Vorschrift dieses Gesetzes verstoßen, sind sie den Beschäftigten gegenüber zur Beseitigung und zur Unterlassung verpflichtet.

(2) Fügen die Arbeitgebenden den Beschäftigten durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Verarbeitung seiner personenbezogenen Daten einen Schaden zu, sind sie den Beschäftigten unabhängig von einem Verschulden zum daraus entstandenen Schadensersatz verpflichtet. Bei einem Schaden, der nicht Vermögensschaden ist, ist der Schaden angemessen in Geld zu ersetzen.

(3) Ansprüche der Beschäftigten gegen die Arbeitgebenden aus anderen Rechtsvorschriften bleiben unberührt.

§ 23

Verbandsklagerecht für Betriebsräte und Gewerkschaften

Bei einem Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz von Beschäftigten kann der Betriebsrat bzw. Personalrat, eine im Betrieb vertretene oder zuständige Gewerkschaft oder ein anerkannter Verband von den Arbeitgebenden Unterlassung verlangen und diese Forderungen auch gerichtlich geltend machen.

§ 24

Grenzen der Verschwiegenheitspflicht für Beschäftigte

(1) Sind Beschäftigte auf Grund konkreter Anhaltspunkte der Auffassung, dass im Betrieb oder bei einer betrieblichen Tätigkeit gesetzliche Pflichten nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz verletzt werden, können sie von den Arbeitgebenden Abhilfe verlangen. Das Recht zur Anrufung der betrieblichen Interessenvertretung oder des betrieblichen Datenschutzbeauftragten bleibt unberührt. Kommen die Arbeitgebenden dem Verlangen nach Abhilfe nicht oder nicht ausreichend nach, haben die Beschäftigten bei Gefahr von Verstößen das Recht, sich unmittelbar an die für den Datenschutz zuständige Kontrollbehörde zu wenden. Ihre Eingaben haben die Aufsichtsbehörden vertraulich zu behandeln.

(2) Ein vorheriges Verlangen nach Abhilfe ist nicht erforderlich, wenn dies den Beschäftigten nicht zumutbar oder erkennbar aussichtslos ist. Unzumutbar ist ein solches Verlangen jedenfalls dann, wenn die Beschäftigten aufgrund konkreter Anhaltspunkte der Auffassung sind, dass

1. eine Straftat geplant ist, durch deren Nichtanzeige sie oder er sich selbst der Strafverfolgung aussetzen würde, und
2. eine innerbetriebliche Abhilfe nicht oder nicht ausreichend erfolgen wird.

(3) Von den Absätzen 1 und 2 kann nicht zuungunsten der Beschäftigten abgewichen werden.

(4) Beschwerderechte der Beschäftigten nach anderen Rechtsvorschriften und die Rechte ihrer Interessenvertretungen bleiben unberührt.

§ 25

Arbeitsrechtliches Benachteiligungsverbot

Die Arbeitgebenden dürfen Beschäftigte nicht benachteiligen, die

1. von ihren Rechten nach diesem Gesetz Gebrauch machen,
2. ein unzulässiges Auskunftersuchen nicht oder unrichtig beantwortet haben,
3. eine unzulässige gesundheitliche oder sonstige Untersuchung oder Prüfung abgelehnt haben oder
4. eine unzulässige Erhebung oder Verwendung von Beschäftigtendaten in Anspruch genommen haben.

6. Abschnitt: Sonderbestimmungen

§ 26

Überwachung im Auftrag des Arbeitgebenden

Eine verdeckte Erhebung von Daten über Bewerberinnen und Bewerber sowie über Beschäftigte im Auftrag der Arbeitgebenden, insbesondere durch Detekteien, ist unzulässig.

§27

Datenübermittlung bei Betriebsübergang

(1) Die Übermittlung von personenbezogenen Daten der Beschäftigten vor Betriebsübergang an mögliche Erwerbende ist grundsätzlich unzulässig. Besteht ein überwiegendes Interesse der Erwerbenden an der Übermittlung von Beschäftigtendaten, erfolgt die Übermittlung in anonymisierter Form, sofern die Zahl der Beschäftigten für ein solches Verfahren ausreicht. In einem solchen Fall ist mit schriftlicher Einwilligung der Beschäftigten die Personifizierung der Daten zulässig. Im Einzelfall können für innerbetriebliche Führungskräfte abweichende Regelungen vorgesehen werden.

(2) Für den in § 613 a Abs. 6 genannten Zeitraum kann der Beschäftigte der Übermittlung der Daten widersprechen.

7. Abschnitt: Organisatorischer Datenschutz

§ 28

Betriebliche Datenschutzbeauftragte

(1) Die Aufgabe der Beschäftigtendatenschutzbeauftragten wird von den betrieblichen Datenschutzbeauftragten wahrgenommen. Die Bestellung eigener Beauftragten für den Beschäftigtendatenschutz ist zulässig.

(2) Beauftragte für den Beschäftigtendatenschutz sind zuständig für die Überwachung der Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften zum Schutz der Daten von Beschäftigten. Sie arbeiten mit den Arbeitgebenden, dem Betriebs- oder Personalrat und unter den Voraussetzungen des Absatzes 1 Satz 2 mit dem betrieblichen Datenschutzbeauftragten zum Wohl der Beschäftigten und des Betriebs oder der öffentlichen Stelle zusammen. Sie unterrichten regelmäßig den Betriebsrat oder den Personalrat über die Angelegenheiten des Datenschutzes der Beschäftigten.

(3) Beauftragte für den Beschäftigtendatenschutz bemühen sich bei Verstößen gegen dieses Gesetz und andere Rechtsvorschriften zum Schutz der Beschäftigtendaten gegenüber den Arbeitgebenden um Abhilfe. Kommt eine Einigung nicht zustande, sind sie verpflichtet, den Betriebs- oder Personalrat zu unterrichten. Schwerwiegende Verstöße, insbesondere gegen die Regelungen der §§ 10 bis 15, sind der Aufsichtsbehörde nach § 38 Absatz 6 des Bundesdatenschutzgesetzes mitzuteilen.

(4) Zur Erfüllung seiner Aufgaben haben die Beauftragten für den Beschäftigtendatenschutz einen Anspruch auf Teilnahme an Fort- und Weiterbildungsveranstaltungen; die Kosten tragen die Arbeitgebenden.

(5) Für die Bestellung und Abberufung finden die Bestimmungen des § 4f des Bundesdatenschutzgesetzes entsprechende Anwendung. Für die Mitbestimmung von Betriebs- und Personalräten gelten § 87 Absatz 1 Nummer 14 des Betriebsverfassungsgesetzes und § 75 Absatz 1 Nummer 8 des Bundespersonalvertretungsgesetzes.

§ 29

Vorabkontrolle durch die Datenschutzbeauftragten

(1) Soweit die Verarbeitung der Beschäftigtendaten besondere Risiken für die Rechte und Freiheiten der Beschäftigten aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn

1. die Verarbeitung von personenbezogenen Daten vorgenommen wird, für die eine Einwilligung der Betroffenen nach diesem Gesetz erforderlich ist,
2. Daten nach § 8 (Gesundheitsdaten) verarbeitet werden,
3. statistische Auswertungen betriebsärztlicher Daten verarbeitet werden,
4. Verfahren nach dem dritten Abschnitt dieses Gesetzes (Video-Überwachung, Raster-Abgleich, Telefonüberwachung, E-Mailüberwachung, Internetnutzungskontrolle) eingesetzt werden,
5. mobile Datenträger, insbesondere Chipkarten und RFID-Chips, zum Einsatz kommen sollen, die in den Bereich der informationellen Selbstbestimmung der Beschäftigten eingreifen,
7. die Datenschutzkonzepte bei der Fernarbeit nach § 14 zum Einsatz kommen,
8. der Einsatz biometrischer Verfahren nach § 16 vorgesehen ist,
9. Beurteilungssysteme, die Persönlichkeitsprofile zur Bewertung von Leistungen, Fähigkeiten oder Verhalten ermöglichen, eingesetzt werden,
10. Verfahren elektronischer Zeit- und Leistungserfassung eingesetzt werden,
11. Fragebogen zur Erhebung personenbezogener Daten, insbesondere Kundenbefragungen mit Leistungsbezug, eingesetzt werden,
12. Einstellungs- und Eignungstests vorgenommen werden,
13. neue Verfahren der elektronischen Personalaktenführung eingeführt werden,
14. medizinische oder psychologische Tests durchgeführt werden,
15. ein Betriebsübergang ansteht.

(2) Zuständig für das Verfahren der Vorabkontrolle sind die Beauftragten für den Datenschutz. Sie haben sich in Zweifelsfällen an die Aufsichtsbehörde zu wenden.

§ 30

Anrufung der Beauftragten für den Beschäftigtendatenschutz

Die Beschäftigten haben das Recht, sich jederzeit mit Anliegen oder Beschwerden beim Umgang mit ihren personenbezogenen Daten an die Beauftragten für den Beschäftigtendatenschutz zu wenden.

§ 31

Aufsichtsbehörde

(1) Die Aufsichtsbehörde nach § 38 Absatz 6 des Bundesdatenschutzgesetzes überwacht die Ausführung dieses Gesetzes und der anderen Rechtsvorschriften zum Schutz von Beschäftigtendaten.

(2) Die Vorschriften des § 38 Absatz 1 bis 7 des Bundesdatenschutzgesetzes über die Aufsichtsbehörden finden entsprechende Anwendung.

8. Abschnitt: Datenschutz in den Interessenvertretungen

§ 32

Rechte von Betriebs- und Personalräten

Die bestehenden gesetzlichen Rechte der Betriebs- und Personalräte werden von den Vorschriften dieses Gesetzes nicht berührt.

§ 33

Datenverarbeitung von Betriebs- und Personalräten

(1) Die Verarbeitung von Beschäftigendaten durch Betriebs- und Personalräte ist im Rahmen ihrer Zuständigkeit zulässig. Die Vorschriften dieses Gesetzes und anderer Rechtsvorschriften zum Schutz der Beschäftigendaten finden entsprechende Anwendung.

(2) Betriebs- und Personalräte mit mehr als fünf Mitgliedern sollen Beauftragte für die Kontrolle der Datenverarbeitung in ihrem Bereich bestimmen. Die Beauftragten sind bei der Ausübung dieser Tätigkeit zur Verschwiegenheit gegenüber die Arbeitgebenden verpflichtet.

9. Abschnitt: Schlussbestimmungen

§ 34

Unabdingbare Rechte der Beschäftigten

(1) Die Rechte der Beschäftigten können von Erben, Bevollmächtigten oder gesetzlichen Vertretern der Betroffenen geltend gemacht werden.

(2) Tarifverträge und Betriebsvereinbarungen zum Schutz der Beschäftigendaten dürfen den Schutz der personenbezogenen Daten durch dieses Gesetz nicht einschränken.

(3) Die Verwirkung von Ansprüchen aus diesem Gesetz ist ausgeschlossen. Ausschlussfristen für die Geltendmachung von Ansprüchen nach diesem Gesetz sind unzulässig.

§ 35

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 6 Absatz 2 der Pflicht zur Rückgabe der Unterlagen der Bewerberinnen und Bewerber oder Löschung der Bewerberdaten trotz Aufforderung durch die Betroffenen nicht nachkommt,
2. entgegen § 6 Abs. 5 S. 2 dem Verbot der Erstellung weitergehender Profile zuwider handelt,
3. entgegen § 9 Absatz 1 mit Wissen oder gemäß 3, 4 Satz 1, Absatz 5 oder 6 ohne Wissen der Beschäftigten medizinisch- oder psychologische Tests über Gesundheit, Alkohol oder Drogen oder über übertragbare Infektionskrankheiten durchführt oder durchführen lässt,
4. entgegen § 10 Absatz 1 Daten aus betrieblichen Überwachungssystemen zur Leistungskontrolle oder Leistungsmessung verwendet,
5. entgegen § 10 Absatz 2 Daten aus Videoüberwachung außerhalb ihrer Zweckbestimmung verwendet,
6. entgegen § 10 Absatz 3 eine heimliche Beobachtung von Beschäftigten mit optisch-elektronischen Einrichtungen vornimmt oder vornehmen lässt,
7. entgegen den Vorschriften des § 11 einen Raster-Abgleich von Beschäftigungsdaten vornimmt oder vornehmen lässt,
8. entgegen den Vorschriften des § 12 Absatz 2 Verkehrsdaten verarbeitet oder diese nicht anonymisiert oder deren Inhalte erhebt,

9. entgegen § 12 Absatz 3 Satz 1 oder 2 Telefongespräche mithört oder aufzeichnet,
10. entgegen den Voraussetzungen des § 12 Absatz 4 den Inhalt dienstlicher E-Mails oder Internet-Nutzungen erhebt,
11. entgegen § 13 der Benachrichtigungspflicht nicht nachkommt,
12. entgegen § 14 Absatz 2 bei der Telearbeit eine Fernüberwachung zur Leistungs- oder Verhaltenskontrolle durchführt,
13. entgegen § 15 Absatz 1 Ortungssysteme einsetzt,
14. entgegen § 15 Absatz 2 Daten aus Ortungssystemen zur Erstellung von Bewegungsprofilen oder zur Leistungs- oder Verhaltenskontrolle verwendet,
15. entgegen § 16 Absatz 1 oder 2 biometrische Daten erhebt,
16. entgegen § 17 Absatz 1 Satz 1 die Beschäftigtendaten mit den Daten aus dem Rechtsgeschäft mit den Beschäftigten zusammenführt,
17. die Informationsrechte der Beschäftigten nach § 18 trotz Aufforderung durch die Beschäftigten oder die betrieblichen Datenschutzbeauftragten oder die Interessenvertretung der Beschäftigten nicht erfüllt,
18. entgegen § 19 der Verpflichtung zur Benachrichtigung bei unrechtmäßiger Kenntniserlangung gegenüber Beschäftigten, betrieblichen Datenschutzbeauftragten oder der zuständigen Aufsichtsbehörde nicht nachkommt,
19. entgegen § 21 Absatz 1 oder 2 unrichtige oder unzulässig erhobene Daten der Beschäftigten verarbeitet oder ihre Korrektur oder Entfernung aus den Unterlagen verweigert,
20. entgegen der Schutzvorschrift des § 25 Beschäftigte dadurch benachteiligt, dass damit erkennbar in Zusammenhang stehende erhebliche betriebliche bzw. dienstliche Zurücksetzungen erfolgen,
21. entgegen § 26 verdeckt Daten erhebt oder erheben lässt,
22. gegen das Verwertungsverbot nach § 4 Absatz 5 verstößt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,
2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,
3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abrufen oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,
4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,
5. entgegen den Vorschriften dieses Gesetzes die übermittelten Daten für andere Zwecke verwendet, indem er sie an Dritte weitergibt.

(3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden.

(4) Wird die Handlung nach Absatz 2 gegen Entgelt begangen, kann die Ordnungswidrigkeit mit einer Geldbuße bis zu einer Million Euro geahndet werden.

Artikel 2

Änderungen des Bundesdatenschutzgesetzes

Das Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66); neugefasst durch Bek. v. 14.1.2003, (BGBl. I S. 66); zuletzt geändert durch ...wird wie folgt geändert:

1. § 3 Absatz 11 wird aufgehoben.

2. § 4f

Absatz 3 Satz 2 wird wie folgt neu gefasst:

„Er ist in Ausübung seiner Fachkunde und der Erfüllung seiner gesetzlichen Aufgaben weisungsfrei.“

3. § 12 Abs. 4 wird aufgehoben.

4. § 32 wird aufgehoben.

Artikel 3**Änderung des Betriebsverfassungsgesetzes**

Das Betriebsverfassungsgesetz in der Fassung der Bekanntmachung vom 25. September 2001 (BGBl. I S. 2518); neugefasst durch...;

zuletzt geändert durch ..., wird wie folgt geändert:

1. § 87 Absatz 1 wird wie folgt geändert:

- a) In Nr. 13 wird der Punkt durch ein Komma ersetzt.
- b) Nach Nummer 13 werden folgende Wörter angefügt:

„14. Bei der Bestellung der betrieblichen Datenschutzbeauftragten nach § 4f des Bundesdatenschutzgesetzes;

15. „Das Verfahren nach den Absätzen § 9 Abs. 1 bis 5 BeschäftigungsdatenschutzG“

Artikel 4**Änderung des Bundespersonalvertretungsgesetzes**

Das Bundespersonalvertretungsgesetz vom 15. März 1974 (BGBl. I S. 693), zuletzt geändert durch ..., wird wie folgt geändert:

§ 75 Absatz 1 wird wie folgt geändert:

1. In Nummer 7 wird der Punkt durch ein Komma ersetzt.
2. Nach Nummer 7 werden folgende Wörter angefügt:
„8. der Bestellung der Datenschutzbeauftragten nach § 4f des Bundesdatenschutzgesetzes.

Artikel 5**Änderung des Gendiagnostikgesetzes**

Das Gesetz über genetische Untersuchungen bei Menschen (Gendiagnostikgesetz – GenDG) vom 31. Juli 2009 (BGBl. I S. 2529, 3672) wird wie folgt geändert:

1. § 20 wird wie folgt geändert:

a) In § 20 Absatz 2 GenDG wird nach Satz 2 folgender Satz angefügt: „Lehnen die Arbeitnehmenden die Durchführung einer Untersuchung nach Satz 1 ab, so begründet dies kein Beschäftigungsverbot.“

b) § 20 Absatz 3 Satz 2 GenDG wird wie folgt geändert:

- aa) Nach der Angabe „Satz 2“ wird die Angabe „und 3“ eingefügt.
- bb) Das Wort „gilt“ wird durch das Wort „gelten“ ersetzt.

2. § 22 wird wie folgt geändert:

a) in Nr. 1 werden die Wörter „des Bundes“ gestrichen, das Wort „sowie“ durch ein Komma ersetzt und nach dem Wort „Soldaten“ die Wörter „sowie Zivildienstleistende“ eingefügt.

b) in Nr. 3 werden nach dem Wort „Bund“ ein Komma sowie die Wörter „die Länder“ eingefügt und das Wort „bundesunmittelbare“ durch das Wort „bundes- oder landesunmittelbare“ ersetzt.

Artikel 6**Änderung des Sozialgesetzbuchs III**

Das Sozialgesetzbuch (SGB) Drittes Buch (III) – Arbeitsförderung – (SGB III) vom 24. März 1997 (BGBl. I S. 594); zuletzt geändert durch ... wird wie folgt geändert:

§ 394 wird wie folgt geändert:

1. Nach Absatz 1 wird folgender Absatz 2 eingefügt:

„Sind die personenbezogenen Daten der Arbeitssuchenden in jeweiligen Datenverarbeitungssystemen nicht anonymisiert, ist die Verarbeitung dieser Daten nur zulässig, wenn sie zu Bearbeitung von Anträgen auf Geldleistungen, zur Unterstützung der Planung von Hilfen sowie zu Eingliederung in den

Arbeitsmarkt erforderlich sind und die Verarbeitung ausschließlich von den zuständigen Mitarbeiterinnen und Mitarbeitern der örtlichen Behörden vorgenommen wird.“

2. Nach Absatz 2 wird folgender Absatz 3 eingefügt:

„Sind personenbezogene Daten von Arbeitssuchenden in Ausbildungs- und Arbeitsvermittlungsbörsen gespeichert, dürfen die Daten Dritten nur dann zugänglich gemacht werden, wenn diese als Arbeitgebende einen Bedarf an Arbeitskräften darlegen.“

3. Der bisherige Absatz 2 wird Absatz 4.

Artikel 7 Änderung des Arbeitsgerichtsgesetzes

Das Arbeitsgerichtsgesetz (ArbGG) vom 03.09.1953, zuletzt geändert am ..., wird wie folgt geändert:

In § 2 Abs. 1 Nr. 10 wird der Punkt durch ein Semikolon ersetzt und folgende Nr. 11 angefügt: „11. Rechtsstreitigkeiten nach § 23 Beschäftigtendatenschutzgesetz“

Artikel 8

Inkrafttreten

Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft.

Berlin, 22. Februar 2011

Renate Künast, Jürgen Trittin und Fraktion

Begründung

A. Allgemeiner Teil

I. Ziel des Entwurfs

Der Entwurf verfolgt das Ziel, das seit über 25 Jahren auch vom Deutschen Bundestag immer wieder geforderte Beschäftigtendatenschutzgesetz umzusetzen.

Ein verbesserter Schutz für die Beschäftigten ist dringender denn je: Kunden und Beschäftigte gleichermaßen werden mit Kameras und Zugangskontrollsystemen überwacht. Beschäftigte im Außendienst werden ohne ihr Wissen über das Handy geortet, private Detekteien zur Kontrolle eingeschaltet und das Telefon überwacht. Mögliche Bußgelder für diese Eingriffe sind so gering, dass sie nicht zur Gesetzestreue motivieren. Das Unrechtsbewusstsein in Wirtschaft und Verwaltung ist vielfach unterentwickelt oder gar nicht erst vorhanden. So hat die Deutsche Bahn massenhaft Datenabgleiche durchgeführt, ohne dass gegen die einzelnen Betroffenen ein Verdacht auf Begehen strafbarer Handlungen bestanden hat.

Durch immer weiter entwickelte Technologien erweitern sich auch die Kontrollmöglichkeiten von Beschäftigten ständig. Das gilt in hohem Maße auch für die Entwicklung im Gesundheitswesen, die zu neuen Diagnosemöglichkeiten und molekulargenetischen Untersuchungsmethoden führt. Dadurch gelangen die Unternehmen an Daten von Bewerberinnen und Bewerbern, die tief in deren Menschenwürde eingreifen. Gewerkschaften, Datenschützerinnen und Datenschützer, aber auch das Bundesarbeitsgericht fordern klare gesetzliche Regelungen zum besseren Schutz der Persönlichkeitsrechte von Arbeitnehmerinnen und Arbeitnehmern.

Es ist erforderlich, das Recht auf informationelle Selbstbestimmung für die Beschäftigten zu stärken, das vom Bundesverfassungsgericht in den Rang eines Grundrechts gestellt wurde. Dazu bedarf es normenklar gefasster gesetzlicher Regelungen für den Persönlichkeitsschutz im Arbeitsleben. Es zeigt sich, dass gerade Beschäftigte und noch mehr die Bewerberinnen und Bewerber sich häufig in einem Abhängigkeitsverhältnis gegenüber den Arbeitgebenden befinden. Sie haben Angst um ihren Arbeitsplatz oder sie hoffen, überhaupt einen zu bekommen. An dieser schwachen Position kann oftmals auch ein Betriebsrat nichts ändern. In vielen Fällen fehlt aber auch diese Interessenvertretung, so dass es um den Schutz der Betroffenen besonders schlecht bestellt ist. Unter dem Druck der Verhältnisse sind viele Betroffene bereit, Eingriffe in ihre Rechte hinzunehmen. Der Gesetzgeber ist von daher in der Verantwortung, dieser bürgerrechtlich negativen Entwicklung Einhalt zu gebieten. Es ist von daher unausweichlich, auf das Arbeitsleben zugeschnittene klare Ge- und Verbotregeln zu schaffen, die es bisher nicht gibt. Es muss Klarheit geschaffen werden, dass heimliche oder verdeckte Datenerhebungen generell verboten und nur in ganz bestimmten, gesetzlich genau beschriebenen Bereichen im Einzelfall zulässig sein können.

Das Gesetz soll die Betroffenen besser schützen, zugleich aber auch die legitimen Belange von Betrieben und Verwaltungen im Auge behalten. Die Neuregelungen müssen auch für kleine Betriebe umsetzbar und praktikabel sein. Für alle Beteiligten soll mehr Rechtsklarheit geschaffen werden, an der es zur Zeit mangelt.

II. Die wesentlichen Inhalte des Gesetzentwurfs

1. Schaffung einer eigenen gesetzlichen Spezialregelung

Der Gesetzentwurf verzichtet darauf, Regelungen des Bundesdatenschutzgesetzes zu wiederholen oder leicht modifiziert in das Gesetz aufzunehmen. Eine solche Übernahme wird dem Charakter des Bundesdatenschutzgesetzes als „Grundgesetz des Datenschutzes“ nicht gerecht. Formelhafte oder modifizierte Wiederholungen längst geltender Regelungen schaffen aber Unklarheiten bei der Auslegung des Gesetzes und tragen von daher nicht zur Rechtsklarheit bei. Der Gesetzentwurf schafft eine auf die Besonderheiten des Arbeitsverhältnisses zugeschnittene Spezialregelung. Weitere spezielle Regelungen bleiben daneben in ihrer Wirksamkeit erhalten, während das allgemeine Bundesdatenschutzgesetz nur in ausdrücklich genannten Fällen zum Tragen kommt.

2. Grundzüge der Novellierung

Dieses Gesetz schafft für alle Beteiligten die notwendige Klarheit. Sie setzt dem Umgang mit personenbezogenen Daten der Beschäftigten klare Grenzen.

Die Durchführung medizinischer oder psychologischer Untersuchungen ist künftig nur unter der Voraussetzung zulässig, dass sie für die Sicherheit der Berufsausübung erforderlich sind. Für Blutuntersuchungen gelten wegen der besonderen Missbrauchsgefahr gesetzlich besonders strenge Voraussetzungen.

Ein Überwachung durch optische und andere elektronische Einrichtungen zur Leistungs- und Verhaltenskontrolle ist nur in eng begrenzten Fällen zulässig.

Der Schutz vor Überwachung mit optischen und elektronischen Geräten wird deutlich erweitert. Das gilt für den Einsatz von Videokameras, das sog. Screening von Daten sowie den Einsatz der vielfältigen technischen Systeme zur Kontrolle am Arbeitsplatz. Eine optische und akustische Rundum-Überwachung der Beschäftigten durch die Arbeitgebenden oder im Auftrag der Arbeitgebenden ist in jedem Fall ein unzulässiger Eingriff in die Persönlichkeitsrechte.

Das heimliche Aufzeichnen oder das heimliche Mithören von Gesprächen ist als Verletzung der Persönlichkeitsrechte in jedem Fall unzulässig. Der Einsatz von Telekommunikation am Arbeitsplatz wird in diesem Gesetzentwurf insgesamt neu geregelt.

Regelungen zur Nutzung von Telefon, E-Mail und Internet am Arbeitsplatz werden in Zukunft dem Mitbestimmungsrecht des Betriebs- und Personalrates unterliegen. Sofern die Arbeitgebenden eine Privatnutzung digitaler Unternehmensnetze zulassen, unterliegt diese dem Fernmeldegeheimnis sowie den datenschutzrechtlichen Bestimmungen des Telekommunikationsgesetzes.

Die Stellung und Aufgaben der Datenschutzbeauftragten wird grundlegend weiter entwickelt. Diese Position ist künftig unabhängig von der Leitung des Betriebs. Diese Unabhängigkeit ist die Voraussetzung dafür, dass der oder die Beauftragte auch für die Kontrolle des Umgangs mit den Beschäftigtendaten zuständig werden kann. Das gilt auch für die Kontrolle der Tätigkeit des Betriebs- oder Personalrats beim Umgang mit den personenbezogenen Daten der Beschäftigten. Nur als unabhängige Stelle ist es dem oder der Beauftragten möglich, diese zusätzlichen Aufgabenbereiche wahrzunehmen. Bei ihrer Benennung und Abberufung müssen daher die betrieblichen Interessenvertretungen ein Mitbestimmungsrecht bekommen.

Bei einem groben Verstoß gegen den Beschäftigtendatenschutz können künftig der Betriebsrat oder eine im Betrieb vertretene oder zuständige Gewerkschaft von den Arbeitgebenden verlangen, diese Verstöße wirksam zu unterbinden. Sie erhalten auch das Recht, diese Forderungen zum Schutz der Beschäftigten im Rahmen eines eigenen Verbandsklagerechts gerichtlich geltend zu machen.

Erleiden die Beschäftigten durch unzulässige oder falsche Verarbeitung ihrer personenbezogenen Daten einen Schaden, sind die Arbeitgebenden zu Schadensersatz verpflichtet. Verstöße sind als Ordnungswidrigkeiten zu ahnden und der Rahmen für ein Bußgeld wird deutlich angehoben und ein Mindestbetrag festgelegt. Das gilt auch für den Fall der Nichtbestellung der betrieblichen Datenschutzbeauftragten. Betriebe und Behörden dürfen aus der Verletzung der Persönlichkeitsrechte keinen wirtschaftlichen Vorteil ziehen.

Die Daten der Beschäftigten dürfen künftig nur unter strenger Beachtung datenschutzrechtlicher Sicherungen verarbeitet werden. Die Beschäftigten erhalten das gesetzlich verbrieftete Recht, über die Speicherung informiert zu werden und in die Unterlagen Einblick zu nehmen. Die Beschäftigten erhalten einen gesetzlichen Unterlassungsanspruch und ein Verwertungsverbot bei unrechtmäßig erhobenen oder ausgewerteten Daten.

Das neue Gesetz verhilft dem Grundsatz zum Durchbruch, dass personenbezogene Daten der Beschäftigten eng begrenzt nur für den konkreten Zweck verwendet werden dürfen, für den sie erhoben wurden. Die Beschäftigten müssen ein umfassendes gesetzliches Einsichtsrecht in die von den Unternehmen bekommen. Aus der Wahrung der Rechte aus dem Beschäftigtendatenschutzgesetz dürfen ihnen keinerlei Nachteile erwachsen.

Das Gesetz verbessert den Schutz der persönlichen Daten von Arbeitssuchenden. Auch die staatlichen Jobbörsen müssen das Recht auf informationelle Selbstbestimmung anerkennen. Der Zugang zu Daten von hilfebedürftigen Personen ist auf die zuständigen Mitarbeiterinnen und Mitarbeiter der örtlichen Behörden zu beschränken. Bei Verstößen sollen auch Behörden Bußgelder bezahlen müssen. Zum Schutz von Bewerberinnen und Bewerbern dürfen nur solche Daten erhoben werden, die für die angestrebte Anstellung tatsächlich und nachweisbar erforderlich sind. Kommt das Beschäftigungsverhältnis nicht zustande, sind die Daten zu löschen.

III. Gesetzgebungskompetenz des Bundes

Die Gesetzgebungskompetenz des Bundes folgt aus 74 Nr. 12, Arbeitsrecht, und Art. 73 Nr. 8, Bundesbeamte.

IV. Vereinbarkeit mit dem Recht der Europäischen Union

Die vorgeschlagenen Änderungen betreffen Vorschriften, durch die Vorgaben der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (sog. EG-Datenschutzrichtlinie) umgesetzt wurden.

Die Vorschriften dieses Geszentwurfs sind mit den Vorschriften der EG-Datenschutzrichtlinie vereinbar, da sie deren allgemeine Vorgaben konkretisieren. Das gilt sowohl für die gestärkte Unabhängigkeit der Datenschutzbeauftragten wie auch für die Umsetzung der Vorgaben bei der Verarbeitung besonders schützenswerter Daten in Artikel 8 der Richtlinie.

B. Besonderer Teil

Zu Abschnitt 1: Allgemeine Grundsätze

Zu § 1 (Ziel des Gesetzes)

Zweck dieses Gesetzes ist die Stärkung des Persönlichkeitsrechts von abhängig Beschäftigten in der privaten Wirtschaft und in öffentlichen Stellen. Das in der Rechtsprechung des Bundesverfassungsgerichts entwickelte Recht der informationellen Selbstbestimmung wie auch das Recht auf Schutz und Integrität informationstechnischer System muss auch im Arbeitsleben gelten. Dieses Gesetz steht in enger Verbindung mit den Regelungen des Bundesdatenschutzgesetzes und ist als Schutzgesetz ausgestaltet. Es knüpft in seiner Zweckbestimmung daran an.

Mit den Regelungen zum Beschäftigtendatenschutz wird auch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1998 in nationales Recht umgesetzt.

Zu § 2 (Anwendungsbereich)

Zu Absatz 1

Das Gesetz hat Geltung für private Unternehmen ebenso wie für den öffentlichen Sektor. In den Schutzbereich des Gesetzes fallen auch die Beschäftigten im nicht-öffentlichen Bereich. Der Anwendungsbereich wird zur Erzielung einer einheitlichen gleichgerechten Praxis weit gezogen und umfasst auch öffentliche Stellen der Länder.

Zu Absatz 2

Die gesetzlichen Regelungen zum Beschäftigtendatenschutz gelten für sämtliche Formen der Verarbeitung personenbezogener Daten von Beschäftigten durch öffentliche und nicht-öffentliche Arbeitgebende selbst und in deren Auftrag durch Dritte im Zusammenhang mit dem Beschäftigungsverhältnis. Mit dieser Konkretisierung wird ein Bereich erfasst, der Eigenheiten aufweist (etwa die strukturelle Unterlegenheit der einzelnen Beschäftigten; Dauerverhältnis) und daher einer besonderen Regelung zugeführt wird. Das Beschäftigungsverhältnis kann nach den Phasen der Anbahnung, der Durchführung und der Beendigung unterschieden werden, die jeweils rechtliche Besonderheiten aufweisen.

Zu Absatz 3

Die Vorschrift verweist auf die Subsidiarität dieses Gesetzes gegenüber spezielleren Geheimnisverpflichtungen. Sie entspricht § 1 Abs. 3 S. 2 BDSG.

Zu Absatz 4

Die Bestimmung stellt eine Vorrangregelung gegenüber dem Verwaltungsverfahrensgesetz dar und bindet damit die sehr weiten Sachermittlungsbefugnisse von Bundesbehörden. Sie entspricht inhaltlich dem § 1 Abs. 4 des BDSG.

Zu Absatz 5

Die Regelung entspricht § 1 Abs. 5 des BDSG und setzt die Vorgaben von Artikel 4 der EG-Datenschutzrichtlinie um.

Zu § 3 (Begriffsbestimmungen)

Die Begriffsbestimmungen dieses Gesetzes knüpfen an die Definitionen des Bundesdatenschutzgesetzes an und präzisieren diese im Hinblick auf die besonderen Gegebenheiten in Betrieben und Verwaltungen. Im Gegensatz zum Bundesdatenschutzgesetz wird aber hier bei der Begriffsbestimmung „Verarbeiten“, an die Begrifflichkeit der EU-Datenschutzrichtlinie anknüpft. Nach dieser Definition umfasst das „Verarbeiten“ immer auch die Erhebung und die Weitergabe der Daten.

Zu Absatz 1

Die Definition der Beschäftigten umfasst die einem Dritten zur Arbeitsleistung überlassenen Beschäftigten, Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden), in anerkannten Werkstätten für behinderte Menschen; Beschäftigte, nach dem Jugendfreiwilligendienstegesetz; Beschäftigte, Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten.

Zu Absatz 2

Unter „Arbeitgebenden“ versteht dieses Gesetz die Führung von Wirtschaftsunternehmen wie auch die Leitung öffentlicher Stellen. Gemeint ist jede natürliche oder juristische Person oder Personengesellschaft (nicht-öffentliche Stelle) sowie eine öffentliche Stelle, die andere Personen beschäftigen. Hierzu zählen auch die sog. Tendenzbetriebe und Kirchen, soweit diese als Arbeitgebende tätig werden.

Zu Absatz 3

Die Definition folgt der Legaldefinition des § 3 Abs. 1 Bundesdatenschutzgesetz.

Zu Absatz 4

Die Definition zielt auf die sachgerechte Eingrenzung der erfassten Sachverhalte. Maßgeblich ist demnach der Zweck der Verarbeitung der erfassten Daten.

Zu Absatz 5

Für den Begriff der Personalakte spielt es keine Rolle, ob die Daten in elektronischer oder anderer Form vorliegen. Die Definition in diesem Gesetz bedeutet auch künftig keine Verpflichtung, Personalakten anzulegen. Während für gewerblich Beschäftigte bislang keine gesetzlichen Regelungen gelten, finden für Beamtinnen und Beamte die Vorschriften der §§ 90 bis 90g des Bundesbeamtengesetzes Anwendung. Hier ist die Führung einer Personalakte für die Beamtinnen und Beamten des Bundes verbindlich festgeschrieben.

Es ist aber auch im nicht-öffentlichen Bereich gängige Praxis bei den Arbeitgebenden, eine Akte pro Mitarbeiterin oder Mitarbeiter anzulegen. In dieser Akte befinden sich die Unterlagen, die in Zusammenhang mit dem Arbeitsverhältnis stehen. Dabei handelt es sich üblicherweise um Bewerbungsunterlagen, Zeugnisse, Beurteilungen und Bewertungen, Beförderungen oder Maßregelungen, Krankenversicherungen, Rentenversicherung etc. Mehr und mehr gehen die Betriebe und Verwaltungen dazu über, eine elektronische oder digitale Personalakte anzulegen. Wegen dieser Vielfalt ist es geboten, die gesetzliche Regelung „technikneutral“ zu formulieren.

Zu Absatz 6

Die Begriffsbestimmung für die „Verarbeitung personenbezogener Daten von Beschäftigten“ knüpft an die Begriffsbestimmung in Artikel 2 Buchstabe b der EU-Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 an. Danach ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten.

Zu Absatz 7

Biometrische Daten im Sinne dieses Gesetzes sind physiologische Merkmale, die einen Menschen eindeutig und zweifelsfrei kennzeichnen. Sie erfahren eine dem besonderen Risikogehalt für das Persönlichkeitsrecht Rechnung tragende Regelung unter § 16 dieses Gesetzes.

Zu Absatz 8

Raster Abgleich (Screening-Verfahren) im Sinne dieses Gesetzes ist die Anwendung eines systematischen Testverfahrens, das verwendet wird, um innerhalb einer bestimmten Gruppe von Beschäftigten Eigenschaften oder Verhaltensweisen zu identifizieren (dazu im Einzelnen: § 11).

Diese in der Praxis auch digitale Massendatenanalyse geriet in die Kritik, als Anfang 2009 bekannt wurde, dass die Bahn AG seit 1998 mehrfach nahezu sämtliche Mitarbeiterinnen und Mitarbeiter sogenannten Massen-Screenings unterzogen hat. Auf diese Weise sollten nach Angaben des Unternehmens im Rahmen interner Korruptionsbekämpfungsmaßnahmen Fälle aufgedeckt werden, in denen sich Mitarbeiterinnen und Mitarbeiter über Scheinfirmen selbst Aufträge verschaffen.

Zu Absatz 9

Fernarbeit ist die Verarbeitung personenbezogener Daten im Rahmen der beruflichen Tätigkeit in den privaten Räumen der Beschäftigten. Dieser immer wichtiger werdende Bereich wird in § 14 dieses Gesetzes geregelt. Eine gesetzliche Regelung ist dringend erforderlich, weil die neue Informations- und Kommunikationstechnologien eine immer größere Bedeutung erlangen. So ist es technisch möglich, dass die Beschäftigten nicht mehr ganz oder teilweise im Betrieb tätig sind. Von daher wird vielfach der Arbeitsplatz verlagert, gerade auch in die Wohnung der Beschäftigten. Telearbeit stützt sich auf Informationstechniken. Die Tätigkeit wird ganz oder teilweise außerhalb der Betriebsstätte ausgeübt. Der Telearbeitsplatz ist aber mit dem Betrieb durch elektronische Kommunikationsmittel verbunden.

Zu Abschnitt 2: (Datenverarbeitung von Beschäftigendaten)

Zu § 4 (Zulässigkeit und Grundsätze der Datenverarbeitung)

Zu Absatz 1

Die Vorschrift des Satz 1 konkretisiert den verfassungsrechtlichen Gesetzesvorbehalt für die Verarbeitung von Beschäftigendaten. Hinsichtlich der Betriebs- und Tarifvereinbarungen sind die Normen des BetrVG sowie des TVG einschlägig. Allerdings gilt für die Tarifparteien eine Bindung an die Grundrechte, so dass eine Unterschreitung des Schutzniveaus dieses speziell die informationelle Selbstbestimmung der Beschäftigten ausgestaltenden Gesetzes ausgeschlossen ist.

Zu Absatz 2

Die Einwilligung ist grundsätzlich auch im Arbeitsverhältnis als Rechtsgrundlage für Datenverarbeitungen möglich. Allerdings gilt dies ausschließlich in den in diesem Gesetz ausdrücklich benannten Fällen. Damit wird dem besonderen Machtungleichgewicht zwischen Beschäftigten und Arbeitgebenden Rechnung getragen, welches Vereinbarungen auf Augenhöhe oftmals verunmöglicht. Einwilligungen dürfen deshalb nicht de facto erzwungen werden können. Die Vorschrift knüpft an die Regelung für die Einwilligung in § 4a BDSG an, wird allerdings den Besonderheiten des Arbeitsverhältnisses gerecht. So kann eine Ausnahmeregelung für eine wissenschaftliche Forschung nach § 4 a Absatz 2 BDSG nicht in Betracht gezogen werden. Die Regelung in § 4a BDSG fordert eine vorherige Einverständniserklärung der Betroffenen in Anlehnung an die Begrifflichkeit es § 183 BGB. Das allein reicht aber nicht aus, wenn die Einwilligung nicht mit einer Verpflichtung der Arbeitgebenden zur umfassenden Information der Beschäftigten verknüpft ist.

Zu Absatz 3

Dieses Gesetz soll speziellere und damit sachgerechtere Bestimmungen nicht verdrängen. Bedeutsam ist die Einschränkung der Anwendbarkeit des Bundesdatenschutzgesetzes, da ansonsten dessen weit gehaltene Zulässigkeitsbestimmungen keine wirksame Eingrenzung der bestehenden Verarbeitungspraxis bewirken können.

Zu Absatz 4

Die Bestimmung enthält die Verarbeitungserlaubnis für diejenigen Verarbeitungen, die nicht unmittelbar mit der Erfüllung der arbeitsvertraglichen Bindung zu tun haben, darunter die zahlreichen gesetzlichen Meldepflichten der Arbeitgebenden, aber auch die im Rahmen eines Arbeitsverhältnisses häufig anfallenden sonstigen Datenverarbeitungen z.B. im Zusammenhang mit Werkortkontrollen, Bereitstellung von Daten für die Durchführung von Zusatzleistungen (Kantinenkarten etc.). Abs. 4 Nr. 4 ist eng auszulegen: es handelt sich um eine Auffangbestimmung, mit der die spezielleren Regelungen dieses Gesetzes nicht umgangen werden dürfen. Zudem sind bei diesen Verarbeitungen die Betriebsdatenschutzbeauftragten einzubeziehen. Auch bei der Verarbeitung von Daten der Beschäftigten während des Arbeitsverhältnisses hat der Grundsatz zu gelten, dass der Arbeitgebende nur so weit in das informationelle Selbstbestimmungsrecht seiner Mitarbeiterinnen und Mitarbeiter eingreifen darf, wie dies für das Vertragsverhältnis tatsächlich und auch nachvollziehbar begründet erforderlich ist. Eine stereotype Behauptung, die bisherige Praxis habe sich bewährt und solle so fortgeführt werden, genügt den Anforderungen des verfassungsrechtlich geschützten Rechts auf informationelle Selbstbestimmung nicht.

Die Arbeitgebenden dürfen von daher die rechtmäßig erhobenen personenbezogenen Daten der Beschäftigten nur in dem Umfang und in der Zeit verarbeiten, die erforderlich sind, um seine vertraglichen Verpflichtungen gegenüber den Beschäftigten zu erfüllen. Der Erfüllung der Vertragspflichten gleichgestellt ist die Erfüllung gesetzlicher Pflichten der Arbeitgebenden. Diese beiden Ausnahmen dienen auch dem Schutz der Beschäftigten, weil hier Offenlegungs- und Zahlungspflichten zu erfüllen sind, die im Rahmen des Beschäftigungsverhältnisses entstanden sind. Es ist notwendig, diese

Verpflichtungen den Beschäftigten mitzuteilen. Die Vorschriften der §§ 6 und 7 finden entsprechende Anwendung.

Zu Absatz 5

Die Tragweite dieser Vorschrift ist erheblich. Sie betrifft alle Arten der Erhebung, Nutzung und Verarbeitung personenbezogener Beschäftigendaten, die nach der Systematik dieses Gesetzes unter dem Begriff der Verarbeitung gefasst werden. Das gilt sowohl für die heimliche Aufzeichnung von Telefongesprächen, die heimliche Speicherung des E-Mail-Verkehrs wie auch die Videoüberwachung.

Das Bundesarbeitsgericht hat hier in seiner Rechtsprechung bereits den Grundsatz entwickelt, dass beispielsweise die heimliche Aufzeichnung von Telefongesprächen nicht zulässig ist. Aus der Unzulässigkeit dieser Erhebung wurde regelmäßig auch ein Beweisverwertungsverbot abgeleitet. Den Arbeitgebenden war damit untersagt, diese so erhobenen Daten beispielsweise für Kündigungen zu verwenden.

Es herrscht aber Unklarheit über die Grenzen des Beweisverwertungsverbots. So hat der 2. Senat des Bundesarbeitsgerichts in seiner Entscheidung vom 13.12. 2007 durchaus offen gelassen, inwieweit nicht doch die heimliche Nutzung zulässig ist (BAG, Urteil vom 13.12.2007 – 2 AZR 537/06). In dem Urteil wurde den Arbeitgebenden zugestanden, bei der Begründung einer Kündigung auf Informationen zurückzugreifen, die unter Verstoß gegen eine Betriebsvereinbarung gewonnen wurden. Es muss befürchtet werden, dass gerade Beschäftigte in Betrieben ohne Betriebsrat dem erhöhten Risiko einer unzulässigen Überwachung ausgesetzt sind. Der Gesetzgeber ist daher gehalten, eine klare Regelung zum Schutz der Beschäftigten gegen die Verwertung illegal erworbener Informationen zu treffen.

Zu § 5 (Datengeheimnis, Datensparsamkeit, Datensicherheit)

Zu Absatz 1

Die Vorschrift beinhaltet eine allgemeine Regelung zur Wahrung des Datengeheimnisses bei der Verarbeitung der personenbezogenen Daten der Beschäftigten durch die Arbeitgebenden. Datensicherheitsgrundsätze gelten in Anlehnung an das Bundesdatenschutzgesetz. Dazu zählt auch das Gebot der Anonymisierung bzw. der Pseudonymisierung sowie der allgemeine Grundsatz der Datensparsamkeit, soweit dieser mit dem Gebot der Erforderlichkeit in Verbindung mit dem Zweckfestlegungsgrundsatz vereinbar erscheint. Die Vorschrift knüpft an eine Entscheidung des Bundesverwaltungsgerichts aus dem Jahre 1986 an (BVerwG 2 C 51.84). Die Fürsorgepflicht des Dienstherrn gebietet es nach der Rechtsprechung des BAG, den Kreis der mit Personalakten befassten Beschäftigten möglichst eng zu halten. Die gesetzliche Festschreibung dieser Vorsichtsmaßnahme zum Schutz aller Beschäftigten, auch in der Privatwirtschaft, schützt in der Praxis auch Datengeheimnis des § 5 BDSG. Diese Regelung muss aber auch in der Praxis Wirkung entfalten. Daher wird der Arbeitgebende verpflichtet, die Personen oder Stellen zu benennen, die für die Verarbeitung der Beschäftigendaten zuständig sind. Diese Personen müssen der Verpflichtung auf das Datengeheimnis vor Beginn ihrer Tätigkeit zugestimmt haben.

Zu Absatz 2

Die Bestimmung stellt klar, dass es eines abgegrenzten und vorab benannten Personenkreises bedarf, welche überhaupt nur mit Personaldaten umgehen dürfen. Die entsprechende Abteilung ist zu benennen. Zudem sind weitere Maßnahmen nach § 9 BDSG zu treffen, die den besonderen Vorgaben und Risiken bei der Personaldatenverarbeitung Rechnung tragen.

Zu Absatz 3

Die Vorschrift enthält eine Klarstellung der Geltung des Datenvermeidungs- bzw. Datensparsamkeitsgebots auf die Personaldatenverarbeitung. Eben so gilt dies für den Anonymisierungs- bzw. Pseudonymisierungsgrundsatz. Beide Vorgehensweisen sollen präventiv wirken und die Risiken des Missbrauchs personenbezogener Daten mindern.

Zu Absatz 4

Absatz 4 der Regelung verdeutlicht, dass die Verwendung der Beschäftigtendaten einer strengen Zweckbindung unterworfen ist. Die Erforderlichkeit dieser Regelung ergibt sich aus der automatisierten Verwaltung der Personaldaten. Sie sind technisch in der Lage, das Verhalten der Beschäftigten immer lückenloser zu erfassen, ohne dass die Betroffenen davon wissen. Moderne „Skill-Datenbanken“ speichern Kompetenzen, Kenntnisse und auch Erfahrungen von Beschäftigten. Diese Daten stehen dann innerhalb von Konzernen zur Verfügung, oft weltweit. Mit Recht befürchtet hier der Deutsche Gewerkschaftsbund die Schaffung von „Gläsernen Mitarbeitern“, die heimlichen externen Leistungsbewertungen unterworfen werden (Profil Arbeitnehmerdatenschutz, Hrsg. DGB-Bundesvorstand, August 2009, S. 9). Die besondere Festschreibung einer strengen Zweckbindung ist daher erforderlich. Die Daten dürfen nur zur Datenschutzkontrolle und Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage in Dateien gespeichert oder in Unterlagen aufgenommen wurden.

Zu § 6 (Datenverarbeitung vor Begründung eines Beschäftigungsverhältnisses)

Zu Absatz 1

An dieser Stelle wird der datenschutzrechtliche Grundsatz der Direkterhebung bei den Betroffenen selbst festgeschrieben. Die Arbeitgebenden haben Auskünfte unmittelbar bei den Beschäftigten einzuholen, es sei denn, die Betroffenen haben ausdrücklich in das Auskunftersuchen gegenüber Dritten eingewilligt. Diese Vorschrift steht in direkter Linie zu den Bestimmungen im fünften Abschnitt der EU-Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 und § 4 Absatz 2 des Bundesdatenschutzgesetzes über die Erhebung personenbezogener Daten bei den Betroffenen selbst. Die Bestimmung erfährt Anwendung auch auf interne Bewerbungsverfahren einer bereits im Betrieb oder in der Verwaltung tätigen Person.

Gerade im Bewerbungsverfahren sind die Betroffenen notgedrungen bereit, viele Informationen über sich zu offenbaren. Menschen, die dringend auf eine Beschäftigung angewiesen sind, kann nicht zugemutet werden, ihre Einstellung durch die Verweigerung einer „freiwilligen“ Auskunft zu verhindern. Hier ist der Gesetzgeber gefordert, klare Grenzen zu setzen und das Sammeln der Daten auf den Zweck der Anbahnung des Arbeitsverhältnisses zu beschränken. Von dieser Regel kann nur im Einzelfall abgewichen werden, wenn mit ausdrücklicher schriftlicher Einwilligung der Beschäftigten Informationen von anderer Stelle herbeigezogen werden müssen, weil diese Information von ausschlaggebender Bedeutung sind. Hier würde ein weitergehendes Erhebungsverbot den Beschäftigten zum Nachteil gereichen.

Der Recherche über die Person der Bewerberinnen und Bewerber oder der Beschäftigten, die sich innerhalb des Betriebs oder der Verwaltung um eine andere Tätigkeit bemühen, sind klare Grenzen gesetzt. So ist es unzulässig, ohne Wissen und Einwilligung der Betroffenen das Internet zu nutzen, um an Informationen über die Betroffenen zu gelangen. Denn die dort erhältlichen Informationen entstammen den unterschiedlichsten, mit den angestrebten Beschäftigungsverhältnissen in keiner Weise zusammenhängenden Lebensbereichen und entziehen sich damit der berechtigten Erwartung der Betroffenen, ihre Persönlichkeit nur im Hinblick auf das für die konkrete Stelle Erforderliche offenlegen zu müssen. Trotz der Ubiquität der Zugänglichkeit solcher Informationen etwa über Suchmaschinen ist der Gesetzgeber gehalten, aus Gründen des Persönlichkeitsschutzes das zulässige Verfahren entsprechend festzulegen.

Nach Absatz 1 S. 2 gilt eine Ausnahme für die Einholung von Auskünften z.B. beim vorherigen Arbeitgebenden.

Zu Absatz 2

Die Daten von Bewerberinnen und Bewerbern sollen im Regelfall binnen zwei Monaten zurückgegeben werden, wenn das Beschäftigungsverhältnis nicht zustande kommt. Alternativ dazu können die Daten auch gelöscht werden. Die Regelung ist angesichts der in der Praxis üblichen langen Wartezeiten notwendig. Die Frist orientiert sich am Ablauf der nach AGG eingeräumten Frist, so dass Arbeitgebende für etwaige Beschwerden keine Beweisverschlechterung erfahren. Die Regel darf aber im Interesse der Bewerberinnen und Bewerber nicht ohne Ausnahme gelten. In vielen Fällen liegt es sogar in deren Interesse, dass die Personalabteilung bei einer anderen freien Stelle auf die Bewerbung zurückgreift. Von daher sind die Bewerbenden im eigenen Interesse frei, über den Umgang mit diesen Unterlagen zu entscheiden.

Zu Absatz 3

Die besonderen Sicherheitsstandards im Umgang mit den Daten der Bewerbenden tragen dem erhöhten Schutzbedarf der Beteiligten Rechnung.

Zu Absatz 4

Die erst kürzlich bekanntgewordene Praxis weitgehender Gesundheitsuntersuchungen in bundesdeutschen Betrieben gibt Anlass, die ausufernde Praxis der Untersuchung von Beschäftigten auf das notwendige Maß zu beschränken. Satz 1 schreibt den Grundsatz fest, dass die Arbeitgebenden keinen Anspruch auf Auskunft über medizinische Diagnosen und Befunde der Beschäftigten haben. Insoweit bekräftigt der Satz die Rechtsprechung. Eine Gesundheitsuntersuchung oder Prüfung der Beschäftigten kann nicht von vornherein gänzlich ausgeschlossen werden, vgl. dazu § 9 dieses Entwurfes. Es ist aber sicher zu stellen, dass die Arbeitgebenden nur über das Ergebnis informiert wird. Die zu beantwortende Frage reduziert sich auf die Einschätzung, ob die Beschäftigten gesundheitlich in der Lage sind, auch mit medizinischer Hilfe, eine bestimmte Tätigkeit zu verrichten oder nicht. Sie ist aber nur dann zulässig, wenn sie angeordnet ist und in direktem Bezug zu der jeweiligen beruflichen Aufgabenstellung tatsächlich und nachweisbar unerlässlich ist.

Zu Absatz 5

Die Beschäftigten dürfen nicht im Unklaren gelassen werden, warum Tests erforderlich sind und was mit den Unterlagen geschieht. Die Betroffenen haben einen Anspruch auf umfassende Transparenz.

Zu Absatz 6

Die Regelung stellt klar, dass die Vorschriften des Zweiten Abschnitts über die Erhebung der Daten bei den Beschäftigten nach § 4 Absatz 1 und 2 sowie die Vorschriften über die Begrenzung des Auskunftsverlangens nach § 8 und den Schutz der Gesundheitsdaten nach § 9 nicht nur für Bewerberinnen und Bewerber, sondern auch für die bestehende Belegschaft gelten. Da Bewerbungsverfahren auch innerbetrieblich eine wichtige Rolle spielen, dürfen die Beschäftigten hier nicht schlechter gestellt werden als externe Bewerberinnen und Bewerber.

Zu Absatz 7

Klarstellungsbedürftig sind die Rechte von ehemaligen Beschäftigten. Ist das Beschäftigungsverhältnis beendet, sind grundsätzlich die Informationen zu löschen. Allerdings kann dieser Grundsatz auch im Interesse der Beschäftigten nicht schrankenlos gelten. Es können Aufbewahrungsfristen vorliegen, die zu beachten sind. So gibt es beispielsweise Vereinbarungen, die im Zusammenhang mit der Zahlung einer Abfindung ein zeitlich begrenztes Verbot für einen Wechsel von Beschäftigten zu Konkurrenten vorsehen. Hier wäre es unbillig, vom Betrieb die unverzügliche Löschung der Daten dieser früheren Beschäftigten zu verlangen. Es soll auch möglich sein zu vereinbaren, eine spätere Rückkehr von Beschäftigten in den früheren Betrieb zu erleichtern. Es muss aber sicher gestellt sein, dass in diesen Fällen die Unterlagen ausschließlich für Zwecke der Aufbewahrung zu verarbeiten sind.

Zu Absatz 8

Neben der Vorabkontrolle des betrieblichen Datenschutzbeauftragten nach § 29 Nr. 6 unterliegen die Verfahren zur Gesundheitskontrolle zusätzlich dem Mitbestimmungsrecht der Interessenvertretungen der Beschäftigten.

Zu Absatz 9

Die Vorschrift enthält ein Verwertungsverbot für Daten, denen es an einer wirksamen Rechtsgrundlage fehlt.

Zu § 7 (Übermittlung der Beschäftigtendaten an Dritte)**Zu Absatz 1**

Das Bundesdatenschutzgesetz enthält bereits eine Reihe von Vorschriften über die Weitergabe von Daten an Dritte. Das gilt insbesondere für die ergänzend zu diesem Gesetz anwendbaren Vorschriften der §§ 4a, 4b, 4c, 16, 39 des Bundesdatenschutzgesetzes. Dies wird durch Absatz 1 Satz 2 klargestellt.

Die Übermittlung von Beschäftigtendaten an Dritte unterliegt zusätzlich den engen Voraussetzungen des Absatz 1 Satz 1.

Die Beschäftigtendaten sind über die bestehenden Vorschriften des Bundesdatenschutzgesetzes hinaus geschützt. So findet die Vorschrift des § 4a Absatz 3 über den Schutz besonderer Arten persönlicher Daten auf alle Beschäftigtendaten Anwendung. Diese Daten können grundsätzlich nur dann weitergegeben werden, wenn sich die Einwilligung der Beschäftigten zur Weitergabe der Daten an Dritte konkret auf die weiterzugebenden Daten bezieht. Dieses strikte Zustimmungserfordernis kann indes nicht schrankenlos gelten. In Anlehnung an die Ausnahmeregelungen bei der Datenspeicherung,-veränderung und -nutzung in § 14 Abs. 2 BDSG muss unter bestimmten streng geregelten Voraussetzungen auch ohne Zustimmung der Betroffenen eine Weitergabe möglich sein, wenn beispielsweise eine gesetzliche Bestimmung dies ausdrücklich vorsieht, oder Straftaten zu verfolgen sind, oder überwiegende Rechte Dritter betroffen sind.

Zu Absatz 2

Die Regelung privilegiert die Weitergabe von Beschäftigtendaten innerhalb von Konzernverbänden. Sie trägt damit der verbreiteten Praxis der Konzerndatenverarbeitung von Beschäftigtendaten Rechnung, die in Absprache mit den Aufsichtsbehörden der Länder bislang zumeist als Auftragsdatenverarbeitung eingestuft wurde. Zusätzliche Anforderungen, etwa an die laufend zu gewährleistende Transparenz gegenüber Beschäftigten (z.B. bei Veränderungen hinsichtlich der konzernbeteiligten Unternehmen) und die Vorabkontrolle durch die betrieblichen Datenschutzbeauftragten der beteiligten Konzernteile, bleiben späterer Regelung vorbehalten.

Zu Absatz 3

Zum Schutz der Persönlichkeitsrechte der Betroffenen muss die Übermittlung der Daten in verschlüsselter Form erfolgen.

Zu Absatz 4

Die Bestimmung zielt auf eine weitere Eingrenzung der zulässigen Verwendung von an Dritte weitergegebenen Daten, um die Transparenz der Weitergabe und damit auch die Kontrollierbarkeit zu erhalten.

Zu § 8 (Datenerhebungen im Bewerbungsverhältnis)**Zu Absatz 1**

Die Regelung schützt die Bewerberinnen und Bewerber davor, mehr personenbezogene Daten zu übermitteln als erforderlich. Nicht erforderlich ist im Regelfall die Kenntnis über die besonders schutzwürdigen persönlichen Daten nach § 3 Absatz 9 BDSG. Hier bedarf es einer gesetzlichen Beschränkung. Die Arbeitgebenden dürfen Auskunft über fachliche und persönliche Kenntnisse und Erfahrungen nur soweit verlangen, wie dieses Wissen tatsächlich erforderlich ist, um über die Einstellung der Betroffenen entscheiden zu können. Maßstab ist immer die persönliche Eignung. An dieser Stelle ist eine Abwägung vorzunehmen. Die Arbeitgebenden müssen die persönlichen und fachlichen Fähigkeiten der Bewerberinnen und Bewerber sachgerecht einschätzen können, was auch in deren Interesse ist. Das Auskunftsverlangen kann aber auf der anderen Seite auch nur dann zulässig sein, wenn das berechnete und schutzwürdige Interesse der Arbeitgebenden das Interesse der Bewerberin oder des Bewerbers auf Schutz seiner Privatsphäre überwiegt. So kann es in einem besonders begründeten Einzelfall erforderlich sein, für die Begründung eines Arbeitsverhältnisses bestimmte sensible Informationen zu bekommen.

Gerade Tendenzbetrieben kann nicht das Recht abgesprochen werden zu erfahren, ob die Bewerberinnen und Bewerber das verlangte Stellenprofil beispielsweise für die Redaktion eines Verbandsmagazins zu erfüllen. Die Erforderlichkeit des Tendenzschutzes kann jedoch nur anhand der konkret zu besetzenden Stelle anerkannt werden. So wäre es beispielsweise unzulässig, eine Reinigungskraft in einer Beratungsstelle danach zu fragen, ob sie mit den Zielen des Verbandes übereinstimmt oder nicht. Hinsichtlich der Kirchen kann nach dem in der Rechtsprechung entwickelten Kriterium der verkündungsnahen und verkündungsfernen Tätigkeiten unterschieden werden, wobei hier zusätzlich die Privilegierung des AGG zum Tragen kommen kann.

Die Fragen dürfen aber nicht ins Blaue hinein, sondern nur in Bezug auf die konkrete Eignung für den vorgesehenen Arbeitsplatz gestellt werden. Die Arbeitgebenden haben zu begründen, ob die besondere Kenntnis im Einzelfall tatsächlich erforderlich ist, um beispielsweise bestimmte Beeinträchtigungen bei der Verwendung auf dem vorgesehenen Arbeitsplatz festzustellen. Diese Beeinträchtigungen müssen sich aber direkt auf die Erbringung der geschuldeten Arbeitsleistung auswirken.

Zu Absatz 2

Das Bundesarbeitsgericht hat bereits 1983 entschieden, dass die Frage nach den früheren Bezügen jedenfalls dann unzulässig ist, wenn sie von den Bewerbenden nicht von sich aus als Mindestvergütung für die neue Stelle eingefordert wurden (BAG 2 AZR171/81). Ein generelles Verbot der Frage ist nicht geboten, da erfahrungsgemäß Gehaltsverhandlungen ein wichtiger Teil des Bewerbungsverfahrens sind. Die bisherige Einstufung der Bewerbenden kann daher nicht gesetzlich aus dem Verfahren ausgeklammert werden. Letztlich liegt es an den Bewerbenden selbst, inwieweit diese Frage eine Rolle spielt.

Nur in sehr eingegrenzten Ausnahmefällen zulässig sind Fragen nach den persönlichen Vermögensverhältnissen. Hier muss es für die Arbeitgebenden schlechthin unzumutbar sein, auf die Kenntnis der Vermögenslage der Bewerberin oder des Bewerbers verzichten zu müssen. Aufgrund ihres Ausnahmecharakters muss diese Frage allerdings auf die wenigen Fälle begrenzt bleiben, in denen die berufliche Tätigkeit der Betroffenen gerade in einem selbstständigen und eigenverantwortlichen Umgang mit dem Vermögen anderer besteht. Das betrifft beispielsweise eine verantwortliche Tätigkeit in Vermögensverwaltungen. Ein bloßer Umgang mit dem Geld der Arbeitgebenden oder dem Geld Dritter reicht dazu nicht aus. Ansonsten bestünde die Gefahr, dass beispielsweise Kassiererinnen und Kassierer verpflichtet wären, ihre Vermögensverhältnisse offen zu legen. Eine derartige Frage ist nach diesem Gesetz in jedem Fall unzulässig.

Unzulässig ist auch die Beauftragung Dritter mit der Beschaffung entsprechender Informationen. Eine derartige heimliche Beschaffung von Informationen etwa bei Kreditauskunfteien ist unter keinen Umständen erlaubt.

Zu Absatz 3

Fragen nach einer vorliegenden oder geplanten Schwangerschaft oder andere Fragen zur Familienplanung sind ohne jede Ausnahme unzulässig.

Zu Absatz 4

Fragen nach Behinderungen sind grundsätzlich unzulässig. Damit wird der Verhinderung von Diskriminierung und dem Bedürfnis nach weiterer Gleichstellung Rechnung getragen. Tätigkeitsneutrale Fragen etwa nach Schwerbehinderungen sind damit generell ausgeschlossen. Insbesondere das allgemeine Gleichstellungsgesetz und die neuere arbeitsgerichtliche Rechtsprechung haben den Weg vorgezeichnet, so dass nur unter den engen Voraussetzungen dieser Vorschrift in bestimmten Einzelfällen entsprechende Fragen ausnahmsweise zulässig bleiben.

Zu Absatz 5

Wehr- und Zivildienstleistende dürfen wegen der Erfüllung ihrer gesetzlichen Frist nicht noch weitere Nachteile erleiden. Daher sind Fragen nach geleistetem oder bevorstehenden Wehr- oder Zivildienst bei der Begründung eines unbefristeten Beschäftigungsverhältnisses unzulässig.

Zu Absatz 6

Nach Verbüßung einer Kriminalstrafe sollen den Betroffenen ihre Vergangenheit nicht wie ein Mühlstein um den Hals hängen bleiben. Das stünde dem auch verfassungsrechtlich anerkannten Gedanken der Resozialisierung fundamental entgegen. Fragen nach Vorstrafen sind daher auch bei der Begründung eines Arbeitsverhältnisses grundsätzlich nicht zulässig. Dieser Grundsatz kann indes nicht uneingeschränkt gelten. Steht die begangene Straftat in einem unmittelbaren Bezug zu der Tätigkeit, die an dem zu besetzenden Arbeitsplatz zu leisten ist, kann die Frage nach einer Vorstrafe im Einzelfall erlaubt sein. Das gilt auch für Ermittlungsverfahren und laufende Strafverfahren. Fragen nach Vorstrafen und Ermittlungsverfahren sind in diesem Fall wahrheitsgemäß zu beantworten, wenn sich beispielsweise ein wegen Betrug oder Unterschlagung vorbestrafter Bankangestellter sich um eine neue Anstellung bewirbt. In bestimmten Fällen kann es sogar dienstrechtlich oder auch gesetzlich geboten sein, bestimmte vorbestrafte Personen auszuschließen. So wäre es sogar schlechterdings unverantwortlich, sich bei der Einstellung einer Person für die Betreuung von Kindern nicht zu erkundigen, ob eine Vorstrafe wegen Kindesmissbrauchs vorliegt. In derartigen Fällen wäre vom Bewerber nach der Rechtsprechung des Bundesarbeitsgerichts ohnehin zu verlangen, die Vorstrafe von sich aus offen zu legen. Ansonsten hätte der Arbeitgebende ein Anfechtungsrecht. Im Allgemeinen kann aber davon ausgegangen werden, dass bei besonders sensiblen Tätigkeiten der Arbeitgebende standardmäßig ein polizeiliches Führungszeugnis anfordert.

Von sich aus anzugeben hat die Bewerberin oder der Bewerber für ein unbefristetes Arbeitsverhältnis ohnehin eine zu verbüßende Haftstrafe. Hier käme es nicht auf die Frage an, ob eine Bestrafung in einem Zusammenhang mit der angestrebten beruflichen Tätigkeit steht. Entscheidend ist hier, dass es dem Betroffenen nicht möglich ist, die vertragmäßige Leistungspflicht aufgrund der anstehenden Haftstrafe zu erfüllen.

Zu Absatz 7

Die Einholung graphologischer Gutachten ist auch in den Fällen unzulässig, in denen die Bewerberin oder der Bewerber zugestimmt haben. Die heimliche Einholung ist nach der Rechtsprechung eine schuldhaft Verletzung des Persönlichkeitsrechts und begründet einen Schadensersatzanspruch nach § 847 des Bürgerlichen Gesetzbuchs (LAG Tübingen, AZ 8 Sa 109/71). Es kann auch kein stillschweigendes Einverständnis in die Einholung unterstellt werden, wenn sich handschriftliche Unterlagen der Beschäftigten im Besitz des Betriebs befinden.

Unter dem Druck einer Bewerbungssituation werden die Betroffenen aber vielfach ihr Einverständnis erklären, auch wenn das ihrem Rechtsverständnis zutiefst widerstrebt. Von daher genügt es nicht, nur den heimlichen Einsatz dieser äußerst fragwürdigen Untersuchungsmethode zu verbieten, die Methode bei Zustimmung aber zu erlauben (BAG 2 AZR 228/80).

Zu § 9 (Gesundheitsdaten und Testverfahren)

Zu Absatz 1

Die Regelung unterbindet die immer weiter um sich greifende Praxis, Bewerberinnen und Bewerber im Hinblick auf ihre gesundheitliche Leistungsfähigkeit zu durchleuchten. An dieser Stelle wird eine Grundsatzentscheidung getroffen, dass es mit dem Recht der Betroffenen unvereinbar ist, eine Untersuchung mit einer allgemeinen Prognose über die gesundheitliche Entwicklung zu begründen. Medizinische oder psychologische Tests haben sich ausschließlich darauf zu beschränken, die Fähigkeit der Bewerberinnen und Bewerber zu ermitteln, die geschuldete Arbeitsleistung, auch mit medizinischer Hilfe, tatsächlich erbringen zu können.

Zu Absatz 2

Untersuchungen, auch wenn sie zulässig sind, dürfen niemals heimlich stattfinden oder die betreffenden Personen im Unklaren lassen, welchem Zweck die Untersuchung dient und was mit den Daten geschehen soll. Diese Regelung ist eine zusätzliche Sicherheit zu dem Schutz nach Absatz 1, der medizinische Untersuchungen streng reglementiert.

Die Bewerberinnen oder der Bewerber müssen in jedem Fall vorab über Art und Umfang der Untersuchung aufgeklärt werden. Nur wenn sie danach dem gewählten Verfahren schriftlich zustimmen, ist dieses zulässig. Sie haben einen Anspruch auf Information über das Ergebnis der Untersuchung und dem Zusammenhang mit der Entscheidung über die Begründung oder das Nichtzustandekommen des Arbeitsverhältnisses. Bewerberinnen und Bewerber werden zwar unter dem Druck, die Stelle bekommen zu müssen geneigt sein, diese Unterschrift zu leisten. Sie haben aber ein Beweismittel in der Hand, um sich beispielsweise an die Aufsichtsbehörden zu wenden. Insofern ist die verbindliche Schriftform in jedem Fall zweckmäßig.

Zu Absatz 3

Es gilt der bereits in Absatz 1 festgeschriebene Grundsatz, dass Gesundheitsprüfungen bei Beschäftigte nur dann zulässig sind, wenn dies unbedingt im Einzelfall für die jeweilige Stellenbesetzung erforderlich ist. Nicht zulässig ist eine Gesundheitsüberprüfung mit dem Ziel, eine allgemeine Prognose darüber zu erstellen, ob die Betroffenen möglichst wenige Fehlzeiten wegen Krankheit haben. Das gilt auch für psychologische Begutachtungen.

Angesichts der weit fortgeschrittenen Diagnosemethoden besteht die große Gefahr, dass serienmäßig Gesundheitsdaten erhoben und dann gegenüber den Personen als „Herrschaftswissen“ missbraucht werden. Die gesetzliche Regelung muss diesen Gefahren vorbeugen.

Die Regelung sieht davon ab, Gesundheitstests generell zu verbieten. Es ist vielmehr notwendig, das Interesse der Bewerberinnen und Bewerber auf Schutz ihrer Persönlichkeitsrechte mit dem legitimen Interesse der Arbeitgebenden abzuwägen, bestimmte Stellen mit Personen zu besetzen, die den Anforderungen auch tatsächlich gewachsen sind. Das gilt beispielsweise bei gefahrgeneigten Tätigkeiten, bei deren Verrichtung den Arbeitgebenden eine besondere Fürsorge und Verantwortung für den Einsatz seiner Mitarbeiterinnen und Mitarbeitern zukommt. Das setzt aber eine Kenntnis der Gefahren des Arbeitsplatzes voraus ebenso wie die Kenntnis bestimmter gesundheitlicher Einschränkungen der Beschäftigten.

Es gilt der Grundsatz, dass der Abschluss des Arbeitsvertrages nicht von einer Gesundheitsprüfung abhängig gemacht werden darf, es sei denn, die medizinische oder psychologische Untersuchung ist im Einzelfall tatsächlich und begründbar erforderlich für die Feststellung, ob die Bewerberin oder der Bewerber zum Zeitpunkt der Arbeitsaufnahme den Anforderungen seiner neuen Tätigkeit gewachsen ist.

Zu Absatz 4

Es muss sicher gestellt werden, dass unabdingbar notwendige medizinische Tests nur von entsprechend ausgebildetem Fachpersonal durchgeführt werden darf. Für die Ärztinnen und Ärzte gilt zum Schutz der Betroffenen die ärztliche Schweigepflicht auch gegenüber den Arbeitgebenden; hier gilt § 203 StGB. Da die Bewerberinnen und Bewerber im Bewerbungsverfahren in einer besonders schwachen Position sind, wäre ihnen nicht geholfen, den gesetzlichen Schutz durch ihre Zustimmung außer Kraft zu setzen. Von daher ist eine Entbindung von der Schweigepflicht unwirksam. Den Arbeitgebenden darf von Seiten der untersuchenden Ärztinnen und Ärzte ausschließlich der Grad der Eignung der Bewerberin oder des Bewerbers mitgeteilt werden. Zum Schutz der Betroffenen unterliegen statistische Auswertungen betriebsärztlicher Daten zudem der Vorabkontrolle des oder der Datenschutzbeauftragten.

Zu Absatz 5

Die Regelung ist angelehnt an die Erhebung von Gesundheitsdaten. Auch hier sind heimliche Tests ausnahmslos unzulässig. Angeordnete Alkohol- oder Drogentests sind ebenfalls grundsätzlich unzulässig, es sei denn, es bestehen besondere Unfallrisiken oder der Arbeitsplatz birgt die Möglichkeit erheblicher Fremdgefährdungen. Beim Umgang mit Waffen im Rahmen einer Sicherheits- und Überwachungstätigkeit ist es jedoch angezeigt, einen Alkohol- oder Drogentest zuzulassen, weil der Gebrauch von Waffen mit ganz besonderen Gefahren verbunden ist, die jederzeit ein hohes Maß an psychischer Belastbarkeit erforderlich macht. An dieser Stelle hat die öffentliche Sicherheit einen besonders hohen Rang.

Zu Absatz 6

Diese Regelung konkretisiert die Vorschrift des Absatzes 5 insbesondere für HIV-Tests. Ein Test, auch auf andere, übertragbare vorhandene Infektions- oder Immunschwächekrankheiten ist grundsätzlich unzulässig. Das Verbot kann aber nicht uneingeschränkt gelten. Bestünde ansonsten ein unvertretbares Infektionsrisiko für Dritte, muss an dieser Stelle der Schutz des Betroffenen zurücktreten.

Zu Absatz 7

Für genetische Untersuchungen im Arbeitsleben gelten die Vorschriften der §§ 19-22 des Gendiagnostikgesetzes. In den §§ 19 und 20 Abs. 1 des Gesetzes ist das Verbot genetischer Untersuchungen verankert. Es ist mit Ausnahme der Regelung in § 20 Abs. 2 Satz 2 GenDG unzulässig, vor oder nach der Begründung eines Beschäftigungsverhältnisses oder aus anderen Gründen Gendiagnostik durchzuführen. Auch eine Verwendung von Informationen aus vorgenommenen Untersuchungen ist unzulässig. Dieser Schutz der Persönlichkeitsrechte der Beschäftigten umfasst auch das Recht auf Nichtwissen. Es soll aber auch vermieden werden, dass Beschäftigte durch „freiwillige“ Tests einen Vorteil gegenüber anderen erlangen können. Die Regelungen dienen aber auch der Vermeidung von Diskriminierungen derer, die ansonsten aufgrund bestimmter genetischer Dispositionen möglicherweise nicht eingestellt oder beruflich benachteiligt wären.

Zu Abschnitt 3: (Besondere Kontrollen der Beschäftigten)

Zu § 10 (Videoüberwachung am Arbeitsplatz)

Zu Absatz 1

Diese Bestimmung stellt ausdrücklich klar, dass Überwachungskameras, die nur der Wahrung des Hausrechts oder der Ausübung der Zutrittskontrolle dienen, nicht zur Leistungs- oder Verhaltenskontrolle

eingesetzt werden darf. Überwachungssysteme zur Überwachung von Arbeitnehmerinnen und Arbeitnehmern sind vielfach üblich geworden. Oft fehlt in den Betrieben aber das Bewusstsein dafür, dass Video- und Filmkameras bereits nach der Rechtsprechung des Bundesarbeitsgerichts nur im Rahmen einer Interessenabwägung eingesetzt werden dürfen (BAG, RDV 1992, 179). Sind die Beschäftigten einem dauernden Druck durch derartige Überwachungsmaßnahmen ausgesetzt, liegt ein Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen vor (Roßnagel/Büllesbach, Handbuch Datenschutzrecht, Kap. 6.1. Rn. 57). Ausdrücklich stellt der Gesetzentwurf klar, dass der Einsatz in Bereichen, die nicht ausschließlich der beruflichen Nutzung dienen, unzulässig ist. Dies gilt beispielsweise für Dusch- oder Ruheräume, aber auch für Aufenthaltsräume, Küchen oder Betriebsgelände, die der Pausengestaltung dienen.

Zu Absatz 2

§ 6b BDSG erfasst grundsätzlich nicht die Beobachtung am Arbeitsplatz. Die Bestimmung greift nur am Rande, wenn die Beschäftigten in öffentlich zugänglichen Räumen tätig sind, beispielsweise das Sicherungspersonal in Museen. Dies ist aber nicht die Regel. Selbst bei Fehlen einer Eingangskontrolle ist beispielsweise ein Firmengelände kein öffentlich zugänglicher Raum (dazu Gola/Schomerus, Datenschutzgesetz. 9. Aufl., zu § 6b Rn 9). Sinn und Zweck der Neuregelung ist es, die gesetzliche Schutzlücke für die Beschäftigten zu schließen. Die Beschäftigtendaten, die bei der Überwachung des Betriebsgeländes, des Betriebsgebäudes, der Betriebsräume oder den Räumen der öffentlichen Stelle mit optisch-elektronischen Überwachungsgeräten anfallen, dürfen nur unter den Voraussetzungen des § 6b BDSG erhoben und verwendet werden. Das Gleiche gilt auch für die Zweckbestimmung.

Wichtig ist, dass die Beschäftigten in jedem Fall darüber informiert werden, dass die Kameras eingesetzt werden. Die Beobachtung durch optisch-elektronische Medien ist analog § 6b Abs. 2 BDSG durch entsprechende gute sichtbare Hinweisschilder kenntlich zu machen.

Zu Absatz 3

Eine heimliche Beobachtung und Aufzeichnung der mit Kameras aufgenommenen Daten ohne Kenntnis der Betroffenen ist nicht zulässig. Diese Grundsatzregelung ist erforderlich, um den hohen Rang dieser Transparenzbestimmung zum Schutz der Beschäftigten unmissverständlich zum Ausdruck zu bringen.

Die Ausnahmen von der Beobachtung ohne Kenntnis der Betroffenen müssen auf sehr eng begrenzte Bereiche beschränkt bleiben, wo im konkreten Einzelfall eine solche Maßnahme erforderlich und auch strikt verhältnismäßig ist. Aus rechtsstaatlichen Gründen bedarf es zudem einer zeitlichen Befristung von Überwachungsmaßnahmen, die sich gegen Beschäftigte richten. Die Maßnahmen sind auf höchstens drei Wochen befristet.

Eine Beobachtung bestimmter Beschäftigter kann nur dann und im Einzelfall gerechtfertigt sein, wenn ganz bestimmte gesetzlich genau festgelegte Voraussetzungen tatsächlich erfüllt sind. So müssen tatsächliche Anhaltspunkte für den Verdacht vorliegen, dass der oder die Beschäftigte im Beschäftigungsverhältnis eine Straftat zu Lasten des Arbeitgebenden begangen hat und die Erhebung zur deren Aufklärung erforderlich ist. Zusätzlich muss auch ein darstellbares überwiegendes Interesse der Arbeitgebenden an der Aufklärung gegenüber dem schutzwürdigen Interesse der Betroffenen vorliegen, um diese Kontrollmaßnahme zu rechtfertigen. Dem besonderen Schutzbedürfnis des betroffenen Beschäftigten trägt auch die Regelung des § 87 Abs. 1 Nr. 6 BetrVG Rechnung, wonach neben der Vorabkontrolle des betrieblichen Datenschutzbeauftragten (§ 29 Abs. 1 Nr. 5) auch die Interessenvertretung der Beschäftigten dieser Maßnahme zustimmen muss.

Zu Absatz 4

Die Regelung stellt die vielfach verwendeten Attrappen von Kameras den echten gleich. Sie üben bei Unkenntnis ihrer fehlenden Funktionstüchtigkeit auf die Beschäftigten eine das persönliche Verhalten steuernde Wirkung aus, die geeignet ist, in ihre Rechte einzugreifen.

Zu Absatz 5

Aus rechtsstaatlichen Gründen bedarf es einer strengen Löschungsvorschrift. Die durch die Beobachtung gespeicherten Daten der oder des Beschäftigten müssen unverzüglich gelöscht werden, sobald der Zweck der Beobachtung erreicht und eine weitere Beobachtung nicht mehr erforderlich ist. Der Zeitraum für die Beobachtung ist auf höchstens drei Wochen begrenzt.

Angesichts der besonderen Brisanz der Überwachung durch derartige technische Systeme und zum Schutz der Betroffenen und zur Vorbeugung vor Willkür ist in dieser Vorschrift ausdrücklich klargestellt, dass die Verfahren nach dieser Vorschrift von Anfang an der Vorabkontrolle des betrieblichen Datenschutzbeauftragten und der Mitbestimmung der Interessenvertretungen der Beschäftigten unterliegen, vgl. § 29.

Zu § 11 (Raster-Abgleich von Beschäftigtendaten (Screening-Verfahren))

Zu Absatz 1

Screening-Verfahren haben durch zahlreiche bekannt bewordene Skandale eine große öffentliche Verunsicherung hervorgerufen. Mit Recht wird hier von Seiten des Datenschutzes, aber auch der Öffentlichkeit verlangt, strenge Maßstäbe für derartige Verfahren anzulegen, oder sie sogar ganz zu verbieten.

Dem gegenüber kann jedoch nicht verkannt werden, dass die Korruptionsproblematik auch in der Privatwirtschaft ein ernsthaftes Problem darstellt. Ein völliges Verbot jedes Screening-Verfahrens könnte hier möglicherweise die Korruptionsbekämpfung über Gebühr erschweren. Von daher bedarf es einer strengen Begrenzung der Verfahren auf die Fälle, in denen konkrete Anhaltspunkte dafür vorliegen, dass entsprechende Straftaten von einzelnen Beschäftigten begangen worden sein könnten. Diese sind auf Straftaten zu beschränken, die im Zusammenhang mit Korruption oder bei Straftaten gegen den Wettbewerb einschlägig werden.

Die Definition des Screening-Verfahrens findet sich in § 3 Absatz 8. Das Compliance-Screening von Beschäftigten ist nur unter strengen Voraussetzungen zulässig. Das Verfahren ist in der Vergangenheit, insbesondere bei der Deutschen Bahn, massiv zur Kontrolle der Beschäftigten bis in den Privatbereich hinein missbraucht worden. Das Verfahren unterliegt wegen seiner besonderen Brisanz künftig der Vorabkontrolle des betrieblichen Datenschutzbeauftragten.

Zu Absatz 2

Das Verfahren unterliegt dem strengen rechtsstaatlichen Gebot der Verhältnismäßigkeit. Bei der Durchführung der Screening-Verfahren sind zudem auch die Grundsätze der Anonymisierung bzw. Pseudonymisierung als auch der Datensparsamkeit zu beachten. Die im Zuge des Verfahrens gewonnenen Daten sind zu pseudonymisieren.

Zu § 12 (Einsatz von Telekommunikationsdiensten)

Zu Absatz 1

Die Nutzung der betrieblichen Telekommunikationsmittel ist ein häufiger Streitpunkt in den Betrieben. Erlauben die Arbeitgebenden den Beschäftigten eine private Nutzung von E-Mails, sind sie an das Fernmeldegeheimnis gebunden. Nach der Rechtsprechung des Bundesarbeitsgerichts haben die Arbeitgebenden die arbeitsvertragliche Nebenpflicht, die Persönlichkeitssphäre der Arbeitnehmenden zu

achten (BAG NZA 1988, 53). Auch bei dienstlichen Telefonaten haben die Beschäftigten das "Recht am eigenen Wort". Das heimliche Mithören durch Dritte ist wie die heimliche Tonbandaufnahme ein Eingriff in die Persönlichkeitssphäre. Allerdings ist es dem Betrieb grundsätzlich erlaubt, sich vom Versendungszeitpunkt einer E-Mail und von der Person des Adressaten Kenntnis zu verschaffen.

Die Kontrolle des Inhalts des E-Mail-Verkehrs unterliegt wiederum der Voraussetzung des Fernmeldegeheimnisses. Hinsichtlich des E-Mail-Inhaltes gilt indes, dass die Arbeitgebenden nur dann zulässig darauf zugreifen können, wenn beispielsweise ein auf Tatsachen gestützter Verdacht für eine strafbare Handlung besteht. Der neue § 32 Absatz 1 Satz 2 BDSG benennt hier das Verraten von Betriebs- und Geschäftsgeheimnissen. Den Beschäftigten ist zwar erlaubt, betrieblich veranlasste E-Mails zu verschlüsseln. Bei begründetem Verdacht auf strafbare Handlungen sind sie jedoch zu Entschlüsselung verpflichtet. Viele Einzelheiten sind jedoch umstritten und bedürften einer gesetzlichen Klarstellung.

Die Regelung in Absatz 1 trägt dem Umstand Rechnung, dass immer mehr Beschäftigte in Betrieben tätig sind, die über keinen Betriebsrat verfügen. Von daher ist der Gesetzgeber gehalten, auch für den Fall Vorsorge zu treffen, wo kein Betriebsrat die Interessen der Beschäftigten vertreten kann.

Betriebsrat und Geschäftsleitung sollen die Nutzung von Telefon, E-Mail, Internet und anderen Telekommunikationsdiensten durch Betriebsvereinbarung regeln. Eine derartige Vereinbarung ist dann eine „andere Rechtsvorschrift“ in Sinne des § 4 Abs. 1 BDSG. Nur wenn kein Betriebsrat existiert, sind die Arbeitgebenden aufgefordert, direkt mit den Beschäftigten einzeln eine Vereinbarung zu treffen. Dort soll insbesondere die private Nutzung geregelt werden. Die Beschäftigten sollen wissen, ob und in welchem Umfang und unter welchen Voraussetzungen die Nutzung der in Satz 1 genannten Einrichtungen auch zu privaten Zwecken zulässig ist oder nicht.

Das Gesetz geht hier davon aus, dass private Nutzung erlaubt ist, wenn nichts Gegenteiliges festgelegt ist. Gibt es weder eine Betriebsvereinbarung noch eine Vereinbarung mit den Beschäftigten, gilt die Nutzung der Einrichtungen als erlaubt. Eine solche Erlaubnis mit Verbotsvorbehalt schafft Klarheit. Eine Einschränkung des Verbotsrechts der Arbeitgebenden wäre hingegen verfassungsrechtlich im Hinblick auf die Eigentumsgarantie des Grundgesetzes und das Recht am eingerichteten und ausgeübten Gewerbebetrieb problematisch. Greift die Vermutung der privaten Nutzung, sind die Bestimmungen der §§ 7-10 TMG hinsichtlich der Einschränkungen der Haftbarkeit anwendbar.

Zu Absatz 2

Trotz der Regelvermutung einer Zulässigkeit privater Nutzung in Absatz 1 werden die Arbeitgebenden aus verfassungsrechtlichen Gründen auch in Zukunft berechtigt sein, die Nutzung der von ihnen zur Verfügung gestellten Arbeitsmittel im Rahmen bestimmter Voraussetzungen zu kontrollieren. Diese Kontrolle der Nutzungen eigener Telekommunikationsanlagen ist kein Eingriff in das Fernmeldegeheimnis, findet aber seine Begrenzung im informationellen Selbstbestimmungsrecht der Beschäftigten (dazu: Roßnagel/Rieß, Handbuch Datenschutzrecht, Kap. 6.4. Rn. 31). Eine vollständige anlasslose Überwachung und Aufzeichnung der Telekommunikationsinhalte verstößt hingegen gegen das Recht auf informationelle Selbstbestimmung in ähnlicher Weise wie heimliches Mithören oder eine flächendeckende Videoüberwachung (Roßnagel/Rieß ebd., mit weiteren Verweisen).

Die Verweigerung der privaten Nutzung von Telekommunikationsanlagen durch die Arbeitgebenden darf indes nicht dazu führen, eine überbordende Kontrolle zu legitimieren. In diesem Fall ist es den Arbeitgebenden nur erlaubt, die Verkehrsdaten im Sinne der Definition des § 96 Absatz 1 TKG zu verarbeiten. Diese Verarbeitung ist aber nur zulässig, soweit und solange dies erforderlich ist zur Gewährleistung der Datensicherheit, zur Gewährleistung des ordnungsgemäßen Betriebs der Telekommunikationsnetze- oder dienste oder zur Abrechnung. Zum Schutz der Beschäftigten dürfen die Verkehrsdaten nur in anonymisierter Form verwendet werden. Eine Erhebung der Inhalte der Nutzung ist ausdrücklich untersagt.

Zu Absatz 3

Das heimliche Mithören und Aufzeichnen von Telefongesprächen von Beschäftigten ist grundsätzlich unzulässig. Dieses Verbot betrifft sowohl private wie auch dienstliche Gespräche der Beschäftigten. Das Abhören privater Gespräche ist ohnehin schon nach der geltenden Rechtsprechung des Bundesarbeitsgerichts als Eingriff in das Fernmeldegeheimnis verboten.

Anders als bei der privaten Kommunikation vom Arbeitsplatz ist die Rechtslage bei dienstlichen Gesprächen gelagert. Die Überwachung der eigenen Kommunikationsanlagen durch die Arbeitgebenden ist kein Eingriff in das Fernmeldegeheimnis, wohl aber in das Recht auf informationelle Selbstbestimmung angesehen (Roßnagel/Rieß, Handbuch Datenschutzrecht, Kap. 6.4 Rn. 31 mit zahlreichen weiteren Verweisen).

Ein Mithören oder Aufzeichnen von Gesprächen der Mitarbeiterinnen und Mitarbeiter kann im Ausnahmefall nur dann zulässig sein, wenn es sich um dienstliche Gespräche handelt. Die Überwachung darf auch nur der Sicherung der Qualität gelten oder zu Schulungszwecken erforderlich sein. Alle Kommunikationsteilnehmende müssen ihr auch ausdrücklich zugestimmt haben. Das gilt gerade auch für Dritte, die einen Anspruch auf Information darüber haben müssen, dass dieses Gespräch aufgezeichnet wird.

Die Zustimmung der Beschäftigten mit der Aufzeichnung bzw. Überwachung setzt voraus, dass zuvor eine ausdrückliche Information der Beschäftigten durch die Betriebsleitung ausdrücklich erfolgt ist. Eine pauschale Vorab-Zustimmung der Beschäftigten ist unzulässig. Die Aufzeichnungen sind zum Schutz der Beschäftigten, aber auch von Dritten, nach Erfüllung ihres Zwecks zu löschen.

Zu Absatz 4

Das Verbot der Kontrolle privater Kommunikation gilt ohne Ausnahme. Erlaubt der Betrieb beispielsweise die Versendung privater E-Mails, ist deren Auswertung unzulässig, sobald deren privater Inhalt erkennbar ist.

Der Inhalt dienstlicher E-Mails oder Internet-Nutzungen darf im Einzelfall erhoben werden, wenn dies erforderlich ist, um die Datensicherheit im Betrieb zu gewährleisten.

Eine Kontrolle der Arbeitgebenden oder auf deren Veranlassung hin ist auch in bestimmten Fällen notwendig, beispielsweise im Fall einer dienstlichen oder gesundheitlich bedingten Abwesenheit der Beschäftigten. In diesen Fällen muss es zulässig sein, auch ohne ausdrückliche Einwilligung der Betroffenen deren E-Mails dienstlichen Inhalts auszuwerten, wenn dies tatsächlich zur Erfüllung dringender dienstlicher Belange notwendig ist.

Die Auswertung von Kommunikationsinhalten dienstlichen Charakters ist auch dann zulässig, wenn bestimmte Anhaltspunkte den Verdacht begründen, dass Beschäftigte im Beschäftigungsverhältnis eine Straftat begangen haben. Dieser Eingriff setzt aber ebenso wie bei den anderen Fällen des Absatzes 4 eine Abwägung der dienstlichen Interessen mit dem Interesse der Beschäftigten auf Schutz seiner Privatsphäre voraus.

Existiert eine Betriebsvereinbarung, so kann dort auch geregelt werden, dass eine Beobachtung ohne Kenntnis der Betroffenen dann zulässig ist, wenn der Verdacht einer besonders schwerwiegenden Verletzung des Arbeitsvertrags besteht. Gibt es hingegen keine betriebliche Interessenvertretung der Beschäftigten und dementsprechend keine Betriebsvereinbarung, ist dem Arbeitgebenden die Überwachung aus diesem Grund nicht gestattet.

Zu Absatz 5

Der Absatz regelt die Befugnis der Arbeitgebenden, wenn diese die private Nutzung erlaubt haben. Verkehrsdaten dürfen allein zu Abrechnungszwecken, zur Gewährleistung der Datensicherheit oder zur

Sicherstellung des ordnungsgemäßen Betriebes von TK-Netzen oder TK-Diensten verarbeitet werden. Inthalttauswertungen sind ausdrücklich verboten.

Zu Absatz 6

Die Verkehrsdaten aus der dienstlichen Kommunikation sind unverzüglich, spätestens nach sieben Kalendertagen, zu löschen. Eine längere Speicherfrist ist nur dann zulässig, wenn beispielsweise bei der Aufklärung einer Straftat eine längere Aufbewahrung der Daten erforderlich ist. Umgekehrt gilt, dass bei Erreichen des Ziels der Speicherung auch einer frühere Löschung geboten ist.

Zu § 13 (Benachrichtigungspflicht)

Der von einer Überwachung betroffene Beschäftigte muss nach Abschluss der Maßnahme unverzüglich unterrichtet werden. Ihm ist so die Möglichkeit zu geben, sich, auch mit Hilfe von Gerichten zur Wehr zu setzen und die Rechtmäßigkeit der Maßnahmen überprüfen zu lassen.

Zu Abschnitt 4: (Einsatz besonderer Verfahren)

Zu § 14 (Fernarbeit)

Der Datenschutz für Arbeitsplätze in den Privatwohnungen der Beschäftigten oder auch auf deren Laptop stellt eine große Herausforderung dar. Die Fern- oder Telearbeit mit ihren spezifischen datenschutzrechtlichen Problemstellungen gewinnt in der Praxis eine immer größere Bedeutung. Mittlerweile sind ca. 10 Prozent aller Beschäftigten in Deutschland überwiegend in ihrer Wohnung tätig. Die Entwicklung der Informations- und Kommunikationstechnik erweitert die Möglichkeiten zur Auslagerung von Arbeitsplätzen. Das trägt dem Bedürfnis nach familiengerechter Flexibilität ebenso Rechnung wie dem Wunsch der Wirtschaft, die Kosten für die Anmietung von Büros zu senken (dazu im Einzelnen: Roßnagel/Hartig/Eiermann, Handbuch Datenschutzrecht, 2004, Rn. 6.5.3). Telearbeit findet in unterschiedlichen Formen statt. Vielfach findet sie als Heimarbeit in der Wohnung der Beschäftigten statt, oft auch in einer Mischform von Heimarbeit und Tätigkeit am betrieblichen Arbeitsplatz. Gestiegen ist auch die Zahl der Fernarbeitszentren, in denen zahlreiche Fernarbeitsplätze zusammengefasst sind. Telearbeit findet aber auch mobil statt, so bei Mitarbeiterinnen und Mitarbeitern im Außendienst. So unterschiedlich wie die räumliche Ausgestaltung sind auch die Rechtsformen der Telearbeit. Die Beschäftigten können als Angestellte, freiberuflich Tätige oder auch als (formal) Selbstständige arbeiten. Es kann davon ausgegangen werden, dass die Zahl derartiger Arbeitsplätze in Zukunft steigen wird.

Zu Absatz 1

Die rechtlichen Voraussetzungen für den Datenschutz hängen gegenwärtig noch von der Rechtsform des Beschäftigungsverhältnisses ab. Findet die Fernarbeit im Rahmen der Selbstständigkeit statt, findet für die Auftragsverarbeitung nach § 11 des Bundesdatenschutzgesetzes die Regelung des § 28 BDSG für die Datenverarbeitung für eigene Zwecke Anwendung. Bei einer Funktionsübertragung wiederum bleiben die Auftraggebenden nach § 11 Absatz 1 BDSG für die Einhaltung der datenschutzrechtlichen Regelungen zuständig (Roßnagel/Hartig/Eiermann, Datenschutzrecht, Rn. 6.5.6).

Die bestehende rechtliche Zersplitterung behindert die Entwicklung eines wirksamen Datenschutzrechts bei der Telearbeit. Dabei besteht gerade in der Fernarbeit die Gefahr der Verletzung der Privatsphäre der Beschäftigten, weil die Grenze zwischen Privatleben und Erwerbsarbeit verschwimmt und sie die Möglichkeiten der Fernüberwachung bis in den Privatbereich hinein verstärken. Zur Regelung dieser Fragen kommt Betriebsvereinbarungen eine wichtige Rolle zu. Viele Betriebe haben aber keine betrieblichen Interessenvertretungen, so dass hier der Gesetzgeber klare und verbindliche Vorgaben machen muss. Die Vorschriften des Gesetzes gelten auch für alle in der Telearbeit beschäftigten Personen.

Zu Absatz 2

Eine Fernüberwachung zur Leistungs- oder Verhaltenskontrolle ist im Rahmen der Fernarbeit nicht zulässig.

Zu Absatz 3

Für die Telearbeitsplätze in privaten Räumen hat der Arbeitgebende ein Datenschutzkonzept zu entwickeln und verbindlich festzuschreiben, das die Vertraulichkeit der verarbeiteten Daten gegenüber Dritten, die Sicherheit der Datenintegrität sowie eine ausreichende Revision der Verarbeitung gewährleistet. Für die Kontrolle dieses Konzepts ist sowohl der Betriebsrat und Personalrat wie auch die oder der betriebliche Datenschutzbeauftragte zuständig.

Für die Arbeitgebenden als verantwortliche Stellen im Sinne des BDSG gelten die Vorschriften des § 9 BDSG. Sie haben die technischen und organisatorischen Maßnahmen zu treffen, die in der Anlage zu § 9 Satz 1 BDSG vorgeschrieben sind.

Zu § 15 (Einsatz von Ortungssystemen)**Zu Absatz 1**

Der Einsatz von Ortungssystemen ist heute technisch kein Problem mehr. Diese einfache Handhabung verführt jedoch auch zum Missbrauch. Hier hat das Gesetz Grenzen zu setzen. Ortungssysteme dürfen nicht dazu verwendet werden, ohne Wissen der Beschäftigten Bewegungsprofile zu erstellen und sie so versteckt zu kontrollieren. Das Gesetz knüpft die Zulässigkeit des Einsatzes an bestimmte Bedingungen.

Der Einsatz ist nur dann zulässig, wenn die gewonnenen Daten für die Sicherheit des Beschäftigten erforderlich sind.

Erforderlich für die Zulässigkeit der Anwendung von Ortungssystemen ist die Prüfung, ob Anhaltspunkte für das Vorliegen schutzwürdiger Interessen der Beschäftigten vorliegen, die den Einsatz der Systeme ausschließen.

Zu Absatz 2

Der Einsatz von Ortungssystemen ist stets mit der Gefahr einer Kontrolle der Beschäftigten verbunden. Das Gesetz legt daher eine strenge Zweckbindung fest um zu vermeiden, dass die erhobenen Daten auch für andere Zwecke, wie beispielsweise für die Erstellung von Bewegungsprofilen der Beschäftigten, verwendet werden.

Zu Absatz 3

Die Löschungsvorschrift hat einen klarstellenden Charakter. Die Daten sind unverzüglich zu löschen.

Zu § 16 (Einsatz biometrischer Verfahren)**Zu Absatz 1**

Biometrische Verfahren werden nicht nur bei Pässen und Personalausweisen eingesetzt. Auch in den Betrieben spielen diese Verfahren eine zunehmende Rolle, ohne dass es hier gesetzliche Regelungen gibt. Es muss daher gesetzlich klargestellt werden, dass der Einsatz biometrischer Verfahren ausschließlich zur Feststellung der Identität der Beschäftigten in besonders sicherheitsrelevanten Bereichen zulässig ist. Diese Begrenzung auf die Identitätskontrolle beruht auf dem datenschutzrechtlichen Grundsatz der Datenvermeidung und der Datensparsamkeit. Biometrische Daten müssen unter Kontrolle der Betroffenen selbst bleiben. Sie dürfen ausschließlich zum Vergleich mit den jeweils eingespeicherten Vorlagen

verarbeitet werden. Das Verfahren unterliegt zum Schutz der Beschäftigten der Vorabkontrolle der betrieblichen Datenschutzbeauftragten.

Zu Absatz 2

Die Bestimmung trägt den zahlreichen Alternativen Rechnung, die anstelle der zumeist eingriffsintensiveren biometrischen Erfassung für eine Zeiterfassung herangezogen werden können.

Zu Absatz 3

Die jeweiligen Zugriffe auf biometrische Daten müssen nach Maßgabe der technischen Voraussetzungen protokolliert werden. Diese Verpflichtung dient dem Schutz der Beschäftigten insbesondere vor heimlicher Überwachung.

Zu § 17 (Trennung der Daten aus Arbeits- und Schuldverhältnis)

Zu Absatz 1

In vielen Fällen ist es üblich, dass Beschäftigte auch Kunden in ihrem Unternehmen sind. So kaufen Beschäftigte im Einzelhandel – bisweilen gefördert durch Sonderrabatte – ein. Beschäftigte von Versicherungen vereinbaren mit ihrem Unternehmen begünstigte Vertragsbedingungen.

In diesen Fällen tritt aber das Problem auf, dass es zu einer Vermischung der Daten aus dem Arbeits- und Beschäftigungsverhältnis kommt. Besonders misslich ist, wenn durch diese Vermischung ein Persönlichkeitsprofil der Betroffenen entwickelt werden kann, das sich bei einer ausschließlichen Nutzung der Daten aus dem Arbeits- oder Schuldverhältnis nicht entwickeln ließe. Es muss daher Sorge getragen werden, ein Zusammenführen dieser unterschiedlichen Informationen zu unterbinden.

Zu Absatz 2

Die Bestimmung enthält Klarstellungen im Hinblick auf die Trennung und den Umgang mit von zu unterschiedlichen Zwecken erhobenen und verarbeiteten Daten.

Zu Abschnitt 5: (Rechte und Pflichten)

Zu § 18 (Informationsrechte der Beschäftigten)

Zu Absatz 1

Die Regelung über die Auskunft an Betroffene in § 34 BDSG findet hier, allerdings modifiziert, Anwendung. So können Ausnahmen von der Auskunftspflicht in § 34 Absatz 1 Satz 3 für geschäftsmäßig zum Zweck der Übermittlung gespeicherte Daten im Beschäftigungsverhältnis keine Anwendung finden. Das gilt auch für den Schutz von Geschäftsgeheimnissen in Absatz 3, der im Rahmen des Beschäftigungsverhältnisses nicht zum Tragen kommen kann. Es kann auch keine Ausnahme von der Informationspflicht im Rahmen wissenschaftlicher Erhebungen i.S. des § 34 Absatz 4 i. V. mit § 33 Absatz 2 Satz 1 Nummer 5 BDSG geben.

Zu Absatz 2

Es wird hier klargestellt, dass es keine Ausnahme von der Unentgeltlichkeit der Auskunft geben kann, § 34 Absatz 5 Satz 2 BDSG.

Zu Absatz 3

Die Regelung verpflichtet den Arbeitgebenden zu einer umfassenden Transparenz gegenüber den Beschäftigten, die sich auf die Zielsetzung der Datenverarbeitung ebenso erstreckt wie auf die angewandten Verfahren und Methoden.

Zu Absatz 4

Die Bestimmung stellt die innerbetriebliche Kenntnisnahme sicher.

Zu § 19 (Benachrichtigung bei unrechtmäßiger Kenntniserlangung von Daten)

Zu Absatz 1

Die Bestimmung konkretisiert die Regelung des mit dem Gesetz vom 14.08.2009 neu geschaffenen § 42a BDSG. Die hier vorgeschriebene Benachrichtigungspflicht bei unrechtmäßiger Kenntniserlangung gilt in jedem Fall. Sie hängt nicht davon ab, ob den betroffenen Beschäftigten schwerwiegende Nachteile drohen oder nicht. Der Arbeitgebende hat sie in jedem Fall von sich aus unverzüglich nach Kenntnisnahme zu unterrichten, wenn die entsprechenden Daten der Beschäftigten unrechtmäßig übermittelt wurden oder auf sonstige Weise Unbefugten zugänglich gemacht oder auf andere Weise in den Bereich Dritter gelangt sind.

Zu Absatz 2

Die Regelung des Absatzes 2 stellt klar, dass der Arbeitgebende im Rahmen seiner Verpflichtung aus diesem Gesetz und aus § 42a BDSG verpflichtet ist, in jedem Fall des Absatzes 1 neben den betroffenen Beschäftigten auch die oder den betriebliche/n Datenschutzbeauftragte/n zu benachrichtigen. Die Regelung des Satzes 2 hat klarstellenden Charakter. Bei erheblichen Eingriffen in den Schutzbereich einer oder mehrerer Beschäftigter im Sinne des § 42 a Satz 1 BDSG ist zusätzlich die nach § 38 BDSG zuständige Aufsichtsbehörde zu benachrichtigen.

Zu Absatz 3

Die Verpflichtung zur gleichzeitigen Mitteilung an die Aufsichtsbehörden ergibt sich aus § 42 Satz 1 BDSG. In diesem Fall beschränkt sich die Mitteilungspflicht auf die in dieser Vorschrift genannten Fälle einer schwerwiegenden Beeinträchtigung der Interessen der Betroffenen. Die Mitteilungspflicht an die Beschäftigten geht insofern weiter als die Mitteilungspflicht an die Aufsichtsbehörden; diese Differenzierung wird in Absatz 2 ausgestaltet. Ansonsten wäre zu besorgen, dass die ohnehin stark belasteten Aufsichtsbehörden mit einer Vielzahl von Informationen überzogen würden, denen sie kaum nachgehen könnten. Sollten die Beschäftigten der Auffassung sein, dass die nur ihnen vom Arbeitgebenden übermittelten Daten besonders schwerwiegender Natur sind, steht ihnen der Weg zu den Datenschutz-Aufsichtsbehörden, insbesondere aber zu den betrieblichen Datenschutzbeauftragten, frei.

Zu § 20 (Führung und Einsicht der Personalunterlagen)

Zu Absatz 1

Die Vorschrift stellt die Verpflichtung des Arbeitgebenden klar, bei der Aufnahme von Informationen für die Personalunterlagen das rechtsstaatliche Gebot der Datensparsamkeit zu beachten und gewissenhaft auf die Richtigkeit der Informationen zu achten. In der Personalakte im Sinne des § 3 Nummer 4 dieses Gesetzes dürfen daher grundsätzlich nur Informationen aufgenommen werden, die einen unmittelbaren Bezug zum Arbeitsverhältnis haben und deren Korrektheit nachweisbar ist. Die Regelung verzichtet allerdings darauf, analog zur Regelung des § 1 Absatz 1 BBG eine ausdrückliche Pflicht zur Führung von Personalakten vorzuschreiben und auch die Einzelheiten des Verfahrens gesetzlich zu regeln. Die Gegebenheiten einer öffentlichen Stelle lassen sich nicht automatisch auf den höchst differenzierten nicht-

öffentlichen Bereich übertragen. Eine Regelung zur Führung der Personalakten muss auch den Belangen kleiner Betriebe mit nur wenigen Beschäftigten Rechnung tragen.

Zu Absatz 2

Der grundsätzliche Anspruch der Betroffenen auf Auskunft findet sich bereits in § 34 BDSG. Mit dieser neuen Bestimmung wird das Recht der Beschäftigten auf eine umfassende Einsicht in ihre Personalakten aber auf das Arbeitsverhältnis zugeschnitten und der Regelung für Beamtinnen und Beamte aus § 110 Absatz 1 des Bundesbeamtengesetzes angepasst. Das Recht auf Akteneinsicht ist über die Regelung des § 83 Absatz 1 des Betriebsverfassungsgesetzes hinaus auch noch nach der Beendigung des Beschäftigungsverhältnisses möglich.

Es wird gesetzlich klargestellt, dass die Beschäftigten einen Anspruch haben, dass ihnen die vollständige Personalakte zugänglich gemacht wird. Die Beschäftigten haben auch weiterhin das Recht, ein Mitglied des Betriebsrats bzw. des Personalrats bei der Akteneinsicht hinzuzuziehen. Die Regelung des § 83 Absatz 1 Satz BetrVG bleibt unverändert. Das gilt auch für die Verschwiegenheitspflicht des Betriebsrats bzw. des Personalrats nach Absatz 1 Satz 3. Auf die unveränderte Gültigkeit der Regelungen des Betriebsverfassungsgesetzes weist Absatz 4 dieses Gesetzes ausdrücklich hin.

Zu Absatz 3

Die Bestimmung stellt das Recht klar, den Aussagegehalt der eigenen Akte durch entsprechende schriftliche Stellungnahmen/ Gegendarstellungnahmen beeinflussen zu können.

Zu Absatz 4

Zur Klarstellung der Rechte von Hinterbliebenen der Beschäftigten wird auch für die Hinterbliebenen das Recht auf Einsicht in die Personalunterlagen ihrer Angehörigen festgeschrieben.

Zu Absatz 5

Das Trennungsprinzip hinsichtlich der genannten Unterlagen verwirklicht einen praktischen Schutz vor undifferenzierter Kenntnisnahme besonders schutzwürdiger Informationen durch möglicherweise unbefugte Dritte.

Die Bestimmungen des Bundesbeamtengesetzes zur Führung und dem Zugang zu den Personalakten im Unterabschnitt 4 des Bundesbeamtengesetzes (der §§ 106 bis 115 BBG) sowie die entsprechenden landesrechtlichen Regelungen bleiben unberührt. Damit soll vermieden werden, dass der bestehende beamtenrechtliche Schutz durch die Regelungen des Beschäftigtendatenschutzgesetzes unterschritten wird. Der Gesetzentwurf greift eine entsprechende Anregung des Sachverständigen Petri in der Anhörung des Ausschusses für Arbeit und Soziales vom 7 Mai 2009 auf (Ausschussdrucksache 16 (1) 138 S. 1).

Zu Absatz 6

Die Vorschrift beschränkt die Zulässigkeit der Aufbewahrung von Abmahnungen in der Akte, um eine dauerhafte Belastung der Beschäftigten zu verhindern.

Zu § 21 (Korrekturen)

Zu Absatz 1

Der Arbeitgebende darf Beschäftigtendaten, die unrichtig sind oder unzulässig erhoben wurden, nicht verwenden. Die entsprechenden Regelungen des Zweiten Abschnitts des Bundesdatenschutzgesetzes über die Datenverarbeitung öffentlicher Stellen zur Berichtigung, Löschung und Sperrung der Daten des Bundesdatenschutzgesetzes in § 20 BDSG finden entsprechende Anwendung. Im Hinblick auf die besondere Schutzwürdigkeit der Personalunterlagen kann das Absehen von der Lösungsverpflichtung in 35 Absatz 3 Nummer 3 des Bundesdatenschutzgesetzes keine Anwendung finden. Der Vorgang ist zu protokollieren.

Zu Absatz 2

Die Regelung verpflichtet die Arbeitgebenden, die in die Unterlagen aufgenommenen oder gespeicherten Beschäftigtendaten unverzüglich zu entfernen oder zu löschen, sobald erkennbar ist, dass die Aufnahme dieser Daten nicht zulässig war oder nicht mehr länger zulässig ist. Die unverzügliche Löschungspflicht tritt auch dann ein, wenn die weitere Speicherung der Daten aus sachlichen Gründen oder zur Erfüllung einer gesetzlichen Vorschrift nicht mehr länger erforderlich ist.

Zu Absatz 3

Die gesetzliche Begrenzung der Speicherung unliebsamer Eintragungen in die Personalunterlagen geht über den Schutz der personenbezogenen Daten hinaus. Er stärkt insgesamt die Rechtsposition der Beschäftigten, weil hier klar geregelt wird, dass derartige Missbilligungen nach einer bestimmten Zeit regelmäßig aus den Unterlagen zu entfernen sind. Die Lösungsfrist beläuft sich hier auf drei Jahre. Eine Ausnahme von der Lösungsfrist ist dann gegeben, wenn eine erneute Missbilligung für ein vergleichbares Verhalten des Beschäftigten vorliegt. Die Beschränkung auf ein „vergleichbares“ Verhalten soll vermeiden, dass einzelne Vorgänge aufgrund von Problemen in anderen Bereichen über Gebühr lange in den Unterlagen verbleiben und so die Position der Beschäftigten unverhältnismäßig beeinträchtigen.

Zu Absatz 4

Der Arbeitgebende hat die Beschäftigtendaten zu kennzeichnen, deren Verwendung durch eine Sperrung eingeschränkt ist. Hier finden die Regelungen in § 20 Abs. 3 und 4 BDSG entsprechende Anwendung.

Zu § 22 (Ansprüche der Beschäftigten bei Verstoß gegen ihre Rechte)**Zu Absatz 1**

Aufgrund der besonderen Nähe im Rahmen eines Beschäftigungsverhältnisses muss das Gesetz auch eine Regelung für die Fälle schaffen, in denen die Beschäftigten von geplanten oder heimlichen Verstößen der Arbeitgebenden gegen Vorschriften dieses Gesetzes erfahren. Wenn aufgrund konkreter Anhaltspunkte zu erwarten ist, ein solcher Verstoß ansteht, haben die Beschäftigten einen Anspruch auf Beseitigung und Unterlassung dieser für sie nachteiligen Maßnahmen.

Zu Absatz 2

Diese Vorschrift schafft auch für abhängig Beschäftigte im nicht-öffentlichen Bereich die verschuldensunabhängige Haftung. Der im Bundesdatenschutzgesetz verankerte Verzicht auf eine solche Haftung in § 7 wird für den Bereich des Arbeitsrecht aufgegeben und stattdessen der Regelungsansatz des § 8 für den Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen übernommen. Eine Übernahme der Vorschrift des § 8 BDSG wird nicht vorgenommen, weil sie beispielsweise durch die Beschränkung der Geldentschädigung auf schwere Verletzungen des Persönlichkeitsrechts nachteilig ist. Auch die in § 8 Absatz 3 BDSG vorgesehene Begrenzung des Schadensersatzes auf höchstens 130.000 Euro wird durch den Verzicht auf eine Verweisung ausdrücklich nicht übernommen.

Bei immateriellen Schäden ist der Schaden finanziell auszugleichen. Der Arbeitgebende ist nur dann nicht zum Ersatz des immateriellen Schadens verpflichtet, wenn er im Rahmen einer Umkehr der Beweislast nachweisen kann, dass er die Pflichtverletzung nicht zu vertreten hat. Das kann beispielsweise dann der Fall sein, wenn ihm ein technischer Fehler nachweisbar nicht zuzurechnen ist.

Zu Absatz 3

Ansprüche der Beschäftigten gegen die Arbeitgebenden aus anderen Rechtsvorschriften bleiben von den Vorschriften dieses Gesetzes unberührt.

Zu § 23(Verbandsklagerecht für Personalräte, Betriebsräte und Gewerkschaften)

Die Stellung der Beschäftigten in vielen Betrieben ist vielfach aufgrund der wirtschaftlichen Gegebenheiten geschwächt. Viele Betriebe haben nicht einmal einen Betriebsrat. Deren Bildung wird oftmals sogar massiv behindert. Von daher genügt es nicht, gesetzliche Vorschriften zum Schutz der Beschäftigten in Kraft zu setzen. Es ist auch erforderlich, wirksame Instrumente zu schaffen, diese Rechte in der betrieblichen und behördlichen Praxis auch durchzusetzen.

In Anlehnung an andere Regelungen, beispielsweise beim Allgemeinen Gleichbehandlungsgesetz, sollen die Interessenvertretungen der Beschäftigten die Möglichkeit bekommen, von sich aus aktiv zu werden und auch zu klagen. Allerdings ist in vielen Betrieben kein Betriebsrat vorhanden. Dieser Fallkonstellation muss das Gesetz Rechnung tragen. Bei einem groben Verstoß gegen dieses Gesetz oder andere Vorschriften zum Schutz der Daten von Beschäftigten bekommen daher sowohl der Betriebsrat wie auch die im Betrieb vertretene oder zuständige Gewerkschaft das Recht, gegenüber den Arbeitgebenden gegen diese Verstöße vorzugehen. Betriebsrat und Gewerkschaft können diese Forderungen auch gerichtlich geltend machen.

Zu § 24 (Grenzen der Verschwiegenheitspflicht für Beschäftigte)

Zu Absatz 1

Den Beschäftigten steht der gesetzlich verbrieft Anspruch zu, von den Arbeitgebenden die Einstellung von Verstößen gegen Datenschutzvorschriften zu verlangen. Bestehen Anhaltspunkte für einen solchen Verstoß, müssen die Beschäftigten ihre Rechte wahrnehmen können, ohne dafür Sanktionen befürchten zu müssen.

Die Regelung gilt auch für datenschutzrechtliche Vorschriften zum Schutz der Beschäftigten in anderen Gesetzen. Zur Klarstellung sieht dieses Gesetz in § 25 ausdrücklich vor, dass niemand bei Wahrnehmung der gesetzlichen Rechte benachteiligt werden darf.

Die Einschaltung der betrieblichen Datenschutzbeauftragten in dem Verfahren ist zu jeder Zeit möglich, ja sogar sinnvoll. Dieser kann sogar jederzeit auch ohne konkreten Anlass zu Rate gezogen werden, § 31.

Fruchtet die Intervention bei den Arbeitgebenden nicht und besteht der mögliche Verstoß gegen gesetzliche Vorschriften fort, haben die Beschäftigten das Recht, sich in einem solchen Fall an die für den Datenschutz zuständige Kontrollbehörde zu wenden. Auch diese Beschwerde darf keine Sanktion nach sich ziehen, auch dann nicht, wenn die Behörde keinen Verstoß gegen geltendes Recht vorsieht.

Zu Absatz 2

Die in Absatz 1 vorgesehene Regelung, wonach vor Einschaltung der Aufsichtsbehörden der Konflikt zunächst innerbetrieblich bereinigt werden soll, stößt aber in bestimmten Fallkonstellationen an die Grenzen der Zumutbarkeit für die Beschäftigten.

Der Gesetzentwurf nimmt hier für bestimmte Fälle eine Regelvermutung für ein solches Überschreiten der Zumutbarkeitsgrenze vor. Das ist dann der Fall, wenn es sich bei dem rechtswidrigen Handeln, das vom Arbeitgebenden selbst oder von Dritten in dessen Namen oder in dessen Geschäftsbereich vorgenommen wird um eine Straftat handelt und der oder die Beschäftigte sich womöglich selbst der Gefahr aussetzt, sich einer Strafverfolgung auszusetzen. Unzumutbarkeit kann auch dann vorliegen, wenn nach Lage der Dinge die innerbetriebliche Abhilfe nach Absatz 1 dieses Gesetzes kein Erfolg versprechende Abhilfe verspricht.

Zu Absatz 3

Die Vorschrift stellt klar, dass von den gesetzlichen Vorschriften der Absätze 1 und 2 weder durch innerbetriebliche Vereinbarungen noch durch Arbeitsvertrag abgewichen werden darf.

Zu Absatz 4

Die Regelungen der Absätze 1 bis 3 lassen die Rechte der Interessenvertretungen der Beschäftigten aus anderen Gesetzen unberührt. Das gilt sowohl für den öffentlichen- wie den nicht-öffentlichen Bereich.

Zu § 25 (Arbeitsrechtliches Benachteiligungsverbot)

In Zeiten hoher Arbeitslosigkeit und einer verbreiteten Angst vor dem Verlust des Arbeitsplatzes reichen gesetzliche Rechte zum Schutz der Beschäftigten allein nicht aus. Sie müssen durch wirksame Verfahrensregelungen ergänzt werden, damit die Betroffenen aufgrund von Existenzangst nicht auf ihre Rechte verzichten.

Es gilt der Grundsatz, dass die diejenigen vor Maßregelungen zu schützen sind, die unter Berufung auf dieses Gesetz ihre Rechte wahrnehmen.

Beschäftigte können auch nicht gezwungen werden, Anweisungen auszuführen oder Ansinnen nachzukommen, die rechtswidrig sind. Sie müssen auch keine Fragen beantworten, wenn diese Fragen ein unzulässiges Auskunftsersuchen darstellen. Das schließt ein, für eine falsche Beantwortung nicht zur Rechenschaft gezogen zu werden.

Beschäftigte, Bewerberinnen und Bewerber eingeschlossen, müssen auch keine unzulässige gesundheitliche oder sonstige Untersuchung oder Prüfung über sich ergehen lassen oder es hinnehmen, für eine unzulässige Erhebung oder Verwendung von Beschäftigtendaten in Anspruch genommen zu werden.

Zu Abschnitt 6: (Sonderbestimmungen)

Zu § 26 (Überwachung im Auftrag der Arbeitgebenden)

Der Einsatz externer Kräfte, insbesondere von Detekteien, hat in der Privatwirtschaft nach allen zur Verfügung stehenden Informationen zugenommen. Das hat zu massiven Eingriffen in die Sphäre der Beschäftigten geführt. Der Gesetzgeber muss zum Schutz der Beschäftigten dieser Entwicklung Einhalt gebieten und diese Form der heimlichen Überwachung untersagen.

Zu § 27 (Datenübermittlung bei Betriebsübergang)

Zu Absatz 1

Der Betriebsübergang nach § 613a BGB darf nicht zu einem „Verfügungsrecht“ über die Personaldaten führen. Erforderlich sind vielmehr die Voraussetzungen des § 28 Absatz 1 Nummer 2 BDSG (Däubler, RDV 2004, 55). So muss es ausgeschlossen bleiben, dass vor einem Verkauf des Betriebes potenzielle Erwerbende Einblick in die Personalunterlagen gewährt wird. Ansonsten bestünde die Gefahr, dass Unterlagen über Krankenstände oder Mitgliedschaft in Gewerkschaften oder Betriebsräten weitergegeben würden (Gola, BDSG, § 28 Rn. 42). Die Übermittlung von personenbezogenen Daten vor Betriebsübergang ist von daher grundsätzlich unzulässig.

Für den Fall, dass die alten Betriebsinhabende im Zuge der Verhandlungen über einen Verkauf gar keine andere Möglichkeit haben, den Verkauf ohne Kenntnisnahme von Beschäftigtendaten zu realisieren, besteht aber die Gefahr, dass die Gespräche scheitern und somit Arbeitsplätze gefährdet werden. Das kann nicht im Interesse der Beschäftigten sein. Daher sieht der Gesetzentwurf für einen solchen Fall vor, dass bei einem überwiegenden Interesse der Erwerbenden an der Übermittlung von Beschäftigtendaten eine solche Übermittlung erfolgen kann. Dies hat jedoch in anonymisierter Form zu geschehen. Diese Anonymisierung macht allerdings nur Sinn, wenn die Zahl der Beschäftigten für ein solches Verfahren

überhaupt ausreicht. In einem solchen Fall genügt es für die Zulässigkeit der Übermittlung der Daten, wenn die betroffenen Beschäftigten schriftlich ihre Zustimmung erteilen.

Zu Absatz 2

Ist der Betriebsübergang nach § 613a BGB erfolgt, muss den Beschäftigten analog zu den Rechten beim Widerspruch gegen den Betriebsübergang auch für die Weitergabe der persönlichen Daten an den neuen Arbeitgebenden ein solches Widerspruchsrecht zugestanden werden. Die §§ 613a Abs. 5 und 6 BGB finden für die Unterrichtungspflicht und das Widerspruchsverfahren selbst entsprechende Anwendung. Der Widerspruch muss gemäß § 613 a Abs. 6 BGB innerhalb eines Monats schriftlich erklärt werden, nachdem der Betroffene über den Betriebsübergang informiert worden ist. Der Widerspruch kann dann sowohl gegenüber den bisherigen Arbeitgebenden als auch gegenüber den neuen Inhabenden erklärt werden.

Zu Abschnitt 7: (Organisatorischer Datenschutz)

Zu § 28 (Betriebliche Datenschutzbeauftragte)

Zu Absatz 1

Alle Behörden, die personenbezogene Daten automatisiert verarbeiten und Betriebe ab einer bestimmten Mindestgröße sind verpflichtet, einen Datenschutzbeauftragten zu bestellen. Die Beauftragten erfüllen eine unverzichtbare Rolle im Rahmen der innerbetrieblichen bzw. innerbehördlichen Selbstkontrolle. Dazu ist ein Höchstmaß an Unabhängigkeit erforderlich, um diese Aufgabe erfüllen zu können. Die Bestellung interner Datenschutzbeauftragten ist zwar nach der EU-Datenschutzrichtlinie zwar nicht zwingend vorgeschrieben. Die Alternative wäre eine Meldepflicht bei einer staatlichen Kontrollbehörde nach Artikel 18 Absatz 2 der Richtlinie. Aus gutem Grund hat sich der Gesetzgeber gegen diese Alternative ausgesprochen und sich für betriebliche Datenschutzbeauftragten entschieden. Unabhängig von der Frage der Organisationsform müssen nach Artikel 20 der Richtlinie besonders sensible Daten durch eine Vorabprüfung bei der Kontrollstelle oder dem Datenschutzbeauftragten geschützt werden. Die Richtlinie betont ausdrücklich, dass Kontrollbehörden und betriebliche Datenschutzbeauftragten zur „unabhängigen“ Überwachung in der Lage sein müssen.

In seiner Entscheidung vom 9. März 2010 hat der Europäische Gerichtshof entschieden, dass die Bundesrepublik Deutschland gegen ihre Verpflichtungen aus Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46/EG verstoßen hat, indem sie die für die Überwachung der Verarbeitung personenbezogener Daten durch nichtöffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen zuständigen Kontrollstellen in den Bundesländern staatlicher Aufsicht unterstellt und damit das Erfordernis, dass diese Stellen ihre Aufgaben „in völliger Unabhängigkeit“ wahrnehmen, falsch umgesetzt hat.“ Das Gericht führt aus, „Nach alledem ist Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 dahin auszulegen, dass die für die Überwachung der Verarbeitung personenbezogener Daten im nichtöffentlichen Bereich zuständigen Kontrollstellen mit einer Unabhängigkeit ausgestattet sein müssen, die es ihnen ermöglicht, ihre Aufgaben ohne äußere Einflussnahme wahrzunehmen. Diese Unabhängigkeit schließt nicht nur jegliche Einflussnahme seitens der kontrollierten Stellen aus, sondern auch jede Anordnung und jede sonstige äußere Einflussnahme, sei sie unmittelbar oder mittelbar, durch die in Frage gestellt werden könnte, dass die genannten Kontrollstellen ihre Aufgabe, den Schutz des Rechts auf Privatsphäre und den freien Verkehr personenbezogener Daten ins Gleichgewicht zu bringen, erfüllen.“

Die Entscheidung betrifft unmittelbar die Stellung der staatlichen Kontrollbehörden. Sie zeigt aber auch, dass Unabhängigkeit eine wesentliche Voraussetzung für jede Kontrolle ist. Insofern ist die Entscheidung auch für die Regelung der Stellung der betrieblichen Datenschutzbeauftragten von großer Bedeutung. Die Gefahr, dass gerade im Bereich der Privatwirtschaft auf deren Arbeit möglicherweise stärker Einfluss genommen wird als auf die für den öffentlichen Bereich zuständigen Kontrollbehörden, liegt auf der Hand. Die vom Gesetzgeber in der letzten Novelle des BDSG vom 14. 08.2009 (BGBl. 1 Seite 2814)

vorgenommene Verbesserung des Kündigungsschutzes in § 4 f Absatz 3 ist ein wichtiger erster Schritt für mehr Unabhängigkeit. Das reicht aber noch nicht aus.

Die fehlende Unabhängigkeit der internen Beauftragten versperrt ihnen den Zugang zu den Betriebs- und Personalräten (Simitis, Arbeitnehmerdatenschutz, RdA 2003, Sonderbeilage, S. 43). Es ist daher erforderlich, deren Stellung auszubauen und vor allem die Unabhängigkeit von der Betriebsleitung zu stärken. Die Unabhängigkeit des betrieblichen Datenschutzbeauftragten ist auch eine Voraussetzung dafür, dass er befugt ist, künftig auch den Beschäftigtendatenschutz in Verwaltungen und Betrieben zu kontrollieren. Das Bundesarbeitsgericht hat dazu in seinem viel diskutierten Beschluss vom 11.11.1997 (Az.: 1 ABR 21/97) den betrieblichen Datenschutzbeauftragten untersagt, die Datenverarbeitung des Betriebsrats zu kontrollieren. Er hat diese Entscheidung gerade mit der fehlenden Unabhängigkeit der betrieblichen Datenschutzbeauftragten begründet, die von den Arbeitgebenden ausgewählt werden (Absatz 30). Der Beschluss drückt die Besorgnis aus, dass die Datenschutzbeauftragten zum „verlängerten Arm“ der Arbeitgebenden werden können (Absatz 38). Das Gericht arbeitet die Bedeutung der Unabhängigkeit aus Funktionsvoraussetzung für eine Arbeit im Sinne der Beschäftigten heraus. Diese Überlegungen lassen sich auch auf die Frage der Kontrollbefugnis für Mitarbeiterdaten übertragen. Das Gericht weist aber in seiner Entscheidungsbegründung auch den Weg, dass eine Veränderung der Stellung der Beauftragten sogar dazu führen kann, ihm die Befugnis der Kontrolle der Datenverarbeitung des Betriebsrats zu ermöglichen (Artikel 53). Voraussetzung dafür ist die Mitbestimmung des Betriebsrats bei der Berufung und der Abberufung. Die Beauftragten bedürfen des Vertrauens von Arbeitgebenden und Betriebsrat. Diese Voraussetzungen werden in diesem Gesetz geschaffen.

Für die Erweiterung der Aufgabenstellung der betrieblichen Datenschutzbeauftragten um die Kontrolle des Schutzes der Beschäftigtendaten sprechen auch gewichtige praktische Überlegungen. Es wäre mit nicht unerheblichen Kosten und einer Steigerung der Unübersichtlichkeit im Betrieb verbunden, würde nicht nur eine Person, sondern zwei für den Datenschutz zuständig sein. Würde dann noch der Betriebsrat selbst von der Kontrollbehörde kontrolliert und auch der Betriebsrat selbst in diesem Feld tätig sein, entstünde eine unübersichtliche Situation mit erheblichem Zeitaufwand und einem beachtlichen Koordinierungsbedarf. Es erscheint mehr als zweifelhaft, ob diese bürokratische Gemengelage den Datenschutz im Betrieb tatsächlich verbessern würde.

Die Aufgabe der Beschäftigtendatenschutzbeauftragten wird daher von den betrieblichen Datenschutzbeauftragten wahrgenommen. Es sollte aber auch möglich sein, diese Aufgabe zu trennen, was insbesondere bei großen Betrieben sinnvoll sein kann. Die Bestellung eines oder einer eigenen Beauftragten für den Beschäftigtendatenschutz wird ausdrücklich zugelassen.

Zur Rechtsklarheit wird das Verfahren nach § 4f BDSG über den Beauftragten für den Datenschutz übertragen. Das gilt auch in den Fällen, in denen eigene Beauftragte für den Beschäftigtendatenschutz bestellt wird.

Zu Absatz 2

Die Regelung des Absatzes 2 hebt hervor, dass die Beauftragten für den Beschäftigtendatenschutz nicht nur mit den Arbeitgebenden, sondern auch mit dem Betriebs- oder Personalrat vertrauensvoll zusammenarbeiten. Zur Stärkung der Kooperation sind die die Beauftragten verpflichtet, regelmäßig den Betriebsrat oder den Personalrat über die Angelegenheiten des Datenschutzes der Beschäftigten zu unterrichten.

Zu Absatz 3

Die Beauftragten für den Beschäftigtendatenschutz nehmen eine herausgehobene Verantwortung für die innerbetriebliche Selbstkontrolle wahr. Ihr Aufgabe ist es, festgestellte Verstößen gegen dieses Gesetz und andere Rechtsvorschriften zum Schutz der Beschäftigtendaten so schnell und so wirkungsvoll wie möglich abzuwenden. Gelingt eine Verständigung mit dem Arbeitgebenden nicht, hat er den Betriebs- oder Personalrat über diesen Konflikt zu unterrichten.

Die Datenschutzskandale der vergangenen Monate haben jedoch gezeigt, dass Verstöße ab einer bestimmten Erheblichkeitsschwelle nicht mehr betriebsintern gelöst werden können. Wenn etwas die Deutsche Bahn Teile ihre Belegschaft einem heimlichen Scanning-Verfahren unterzieht, werden grundlegende öffentliche Belange berührt. Anhaltspunkt für eine Meldepflicht der betrieblichen Datenschutzbeauftragten sind die Ordnungswidrigkeiten nach diesem Gesetz und dem Bundesdatenschutzgesetz. Derart schwerwiegende Verstöße, insbesondere gegen die Regelungen der §§ 10 bis 13, sind der Aufsichtsbehörde nach § 38 Absatz 6 BDSG mitzuteilen.

Zu Absatz 4

Diese Regelung ergänzt die Vorschriften für die Arbeitsmöglichkeiten der Datenschutzbeauftragten in öffentlichen- und nicht-öffentlichen Stelle. Um die verantwortungsvolle Tätigkeit beim Schutz der personenbezogenen Personaldaten erfüllen zu können, steht den Beauftragten für den Beschäftigtendatenschutz der gesetzliche Anspruch auf Teilnahme an Fort- und Weiterbildungsveranstaltungen zu. Die Kosten für diese Maßnahmen tragen die Arbeitgebenden.

Zu Absatz 5

Absatz 5 trifft die erforderlichen Regelungen für die Bestellung und Abberufung sowie für die Mitbestimmung.

Zu § 29 (Vorabkontrolle durch die Datenschutzbeauftragten)

Zu Absatz 1

Die Regelung dieses Gesetzes knüpft an die „datenschutzrechtliche Vorabkontrolle“ in § 4d Abs. 5 BDSG an. Die Vorschrift setzt damit die EG-Datenschutzrichtlinie um, die 2001 ins Bundesdatenschutzgesetz aufgenommen wurde. Zuständig für die Vorabkontrolle sind die betrieblichen Datenschutzbeauftragten nach § 4d Abs. 6 Satz 1 BDSG. Diese nehmen nach diesem Gesetz auch die Aufgabe des Beauftragten für den Schutz der Beschäftigtendaten wahr.

Die Beauftragten können jedoch erst dann ihre Aufgabe erfüllen, wenn ihnen die gesetzlich vorgesehene Übersicht mit den nötigen Angaben zum Verfahren vorgelegt wird, (§ 4d Abs. 6 Satz 2 unter Verweis auf § 4g Abs. 2 Satz 1 BDSG). Die Übersicht muss aber alle gesetzlich vorgesehenen Angaben enthalten, um die gesetzlich vorgesehene Handlungspflicht auszulösen (§ 4g Abs. 2 Satz 1 BDSG unter Verweis auf § 4e Satz 1 BDSG).

Anders als bei der Vorabkontrolle nach BDSG reicht es für die Kontrolle des Schutzes sensibler Personaldaten nicht aus, wenn die betrieblichen Datenschutzbeauftragten von der Geschäftsleitung nur informiert werden, wenn beispielsweise neue Verfahren im Bereich der für die Beschäftigten relevanten Datenverarbeitung eingeführt werden sollen. Die Vorabkontrolle ist verbindliche Voraussetzung für die Zulässigkeit der Verfahren. Der Einsatz eines Verfahrens ist nicht rechtmäßig, wenn diese gesetzlich notwendige Vorabkontrolle unterbleibt. Findet sie nicht statt, sieht das Gesetz ein Bußgeld vor. Das Unternehmen kann sich dann nicht auf fehlende Absicht oder Fahrlässigkeit berufen. Wer heikle Daten verarbeitet, muss für die gesetzlich vorgesehene Kontrolle sorgen, die in diesem Gesetz einzeln festgeschrieben ist.

Die Vorabkontrolle ist in Abweichung von den Regelungen des BDSG ohne Ausnahme auch dann vorgeschrieben, wenn der Betrieb keine automatisierten Verfahren verwendet. Es wird hier davon ausgegangen, dass wie in den vom BDSG vorgesehenen Fällen des § 4d Absatz 5 stets davon auszugehen ist, dass besondere Risiken für die Rechte und Freiheiten der Betroffenen vorliegen. Ein Verfahren muss vor seiner erstmaligen Verwendung darauf überprüft werden, ob es die gesetzlich vorgeschriebenen datenschutzrechtlichen Vorgaben erfüllt.

Die Kontrolle vor Beginn der Verarbeitung (Vorabkontrolle) findet für folgende Verfahren Anwendung:

- die Verarbeitung von personenbezogenen Daten, für die eine Einwilligung der Betroffenen nach diesem Gesetz erforderlich ist,
- den Einsatz von Verfahren nach dem vierten Abschnitt dieses Gesetzes,
- den Einsatz von Geräten zur Videoüberwachung nach § 10 und von Netzwerk-Kameras, beispielsweise den WEB-Kameras,
- den Einsatz von mobilen Datenträgern, insbesondere Chipkarten und RFID-Chips,
- Die Kontrolle der Screening-Verfahren nach § 10 Absatz 5,
- die Datenschutzkonzepte bei der Fernarbeit nach § 14 Absatz 2,
- den Einsatz biometrischer Verfahren nach § 16,
- den Einsatz von Beurteilungssystemen, die die Möglichkeit haben, Persönlichkeitsprofile der Beschäftigten zu entwickeln, deren Leistungen, Fähigkeiten oder Verhalten zu bewerten,
- Verfahren der elektronischen Zeit- und Leistungserfassung,
- den Einsatz von Fragebogen zur Erhebung personenbezogener Daten, insbesondere Kundenbefragungen mit Leistungsbezug,
- Einstellungs- und Eignungstests,
- die Verfahren der elektronischen Personaktenführung,
- die Durchführung medizinischer oder psychologischer Tests,
- das Verfahren beim Betriebsübergang nach § 27,
- Datenverarbeitung in Auftrag im Inland,
- die Übermittlung von Beschäftigtendaten ins Ausland.

Zu Absatz 2

Das Verfahren der Vorabkontrolle weicht von den wenig übersichtlichen und teilweise auch widersprüchlichen Regelungen des Bundesdatenschutzgesetzes ab. Während § 4d Absatz 5 BDSG nur Verfahren mit besonderen Risiken als Grund für eine Vorabkontrolle vorsieht und viele Abgrenzungsfragen ungeklärt lässt, führt das Beschäftigtendatenschutzgesetz alle einzelnen Tatbestände auf, für die ein solches Verfahren vorgesehen ist. Es verstärkt dieses Instrument, weil gerade in Betrieben, die einen großen Druck auf ihre Belegschaft ausüben und wo auch kein Betriebsrat die Interessen der Beschäftigten wahrnimmt, den betrieblichen Datenschutzbeauftragten eine besondere Verantwortung zum Schutz der Rechte der Betroffenen zuwächst. Hier ist deren verbindlich vorgeschriebene möglichst frühe Einbindung unabdingbar.

Zuständig für die Vorabkontrolle sind die betrieblichen Datenschutzbeauftragten. Analog zur Regelung des § 4d Absatz 6 Satz 3 BDSG ist er in den Fällen des Absatzes 1 verpflichtet, sich in Zweifelsfällen an die Aufsichtsbehörden zu wenden. Diese Verpflichtung wird für die Vorabkontrolle der Beschäftigtendaten ausdrücklich übernommen, um die Kontrolle der Persönlichkeitsrechte in dem sensiblen Bereich des Umgangs mit diesen Daten sicher zu stellen.

Zu § 30 (Anrufung der Beauftragten für den Beschäftigtendatenschutz)

Die Regelung steht in einem engen Zusammenhang mit der des § 24 zum Whistleblowing. Die Beschäftigten haben mit diesem Gesetz das Recht, sich jederzeit und ohne weitere Voraussetzungen mit Anliegen und Beschwerden an die für ihren Betrieb zuständigen Beauftragten für den Beschäftigtendatenschutz zu wenden. Das Recht der Anrufung des Betriebsrats bleibt selbstverständlich davon unberührt. Das Recht, sich nicht nur mit Beschwerden, sondern auch mit Anregungen an den Beauftragten zu wenden, geht insofern über das reine Beschwerderecht in § 84 BetrVG hinaus. Die gesetzliche Schwelle ist niedrig angesetzt, damit die Betroffenen nicht nur reagieren können, sondern auch Fragen und Anregungen einbringen können.

Zu § 31 (Aufsichtsbehörde)

Zu Absatz 1

Der Aufsichtsbehörde nach § 38 Absatz BDSG kommt eine besondere Verantwortung bei der Kontrolle des betrieblichen und behördlichen Datenschutzes zu. Sie hat sogar nach Absatz 5 Satz 3 und § 4 Absatz 3 Satz 4 das Recht, unter bestimmten Voraussetzungen die Abberufung des betrieblichen Datenschutzbeauftragten zu verlangen.

Die Aufsichtsbehörde überwacht die Ausführung dieses Gesetzes ebenso wie der anderen Rechtsvorschriften zum Schutz von Beschäftigtendaten. Die Regelungen des § 38 BDSG finden hier entsprechende Anwendung.

Zu Absatz 2

Die Vorschrift stellt klar, dass die Aufsichtsbehörde im Bereich des Beschäftigtendatenschutzes die gleichen Befugnisse hat wie bei der Wahrnehmung ihrer Aufgaben nach dem Bundesdatenschutzgesetz. Das gilt auch für die Stellung der Landesregierungen und die von ihnen ermächtigten Stellen nach § 38 Abs. 7 BDSG.

Zu Abschnitt 8: (Datenschutz in den Interessenvertretungen)

Zu § 32 (Rechte von Betriebs- und Personalräten)

Diese Vorschrift dient der Klarstellung. Die Stärkung der Rechte der betrieblichen Datenschutzbeauftragten darf nicht zu Lasten der Betriebs- und Personalräte gehen. Deren Rechte bleiben unangetastet; sie werden von den Vorschriften dieses Gesetzes nicht berührt.

Zu § 33 (Datenverarbeitung von Betriebs- und Personalräten)

Die Interessenvertretungen der Beschäftigten, die nach den Vorschriften des Betriebsverfassungsgesetzes, des Bundespersonalvertretungsgesetzes oder des Landespersonalvertretungsgesetzes gebildet werden, sind bei der Verarbeitung der Daten keine eigenständigen nicht-öffentlichen Stellen (Roßnagel/Wedde, Handbuch Datenschutzrecht, Kap. 4.3. Rn. 56). Sie handeln im Rahmen ihrer Kollektivrechte und nicht als Dritte im Sinne des § 3 Absatz 8 BDSG. Anders ist die Rechtslage bei Konzernbetriebsräten oder Gesamtpersonalräten, die nicht direkt der verantwortlichen Stelle zuzurechnen sind. Das gilt ebenso für Gewerkschaften (Roßnagel/Wedde, Rn. 58).

Zu Absatz 1

Die Verarbeitung von Beschäftigtendaten durch Betriebs- und Personalräte ist im Rahmen ihrer Zuständigkeit zulässig und auch praktisch unerlässlich. Das heißt aber auch, dass sich Betriebs- und Personalräte an datenschutzrechtliche Regeln zu halten haben, obwohl das BDSG selbst nur beschränkt Anwendung findet. Betriebsverfassungsrechtliche Regelungen verdrängen das Bundesdatenschutzgesetz (Roßnagel/Büllesbach, Kap. 6.1, Rn.77). Die Vorschriften dieses Gesetzes und anderer Rechtsvorschriften zum Schutz der Beschäftigtendaten finden von daher sinngemäß Anwendung.

Betriebliche Interessenvertretungen sind selbst in hohem Maße an der Verarbeitung von Beschäftigtendaten beteiligt. So werden beispielsweise im Fall von Sozialplanverhandlungen dem

Betriebsrat von der Geschäftsleitung personenbezogene Daten der Beschäftigten in einem erheblichen Umfang zur Verfügung gestellt. Das ist auch in anderen Fällen bei der Übermittlung von Lohn- und Gehaltslisten der Fall. Es ist selbstverständlich, dass auch Betriebs- und Personalräte an die gesetzlichen Datenschutzvorschriften gebunden sind. Die Zweckbindung der Beschäftigtendaten bleibt nach diesem Gesetz auch dann erhalten, wenn der Betrieb im Rahmen seiner Datenverarbeitung Beschäftigtendaten aus dem Bereich der Interessenvertretungen verwaltet. Die Nutzung dieser Daten für Zwecke der Tätigkeit als Interessenvertretung ist unzulässig. Für die Verarbeitung von Verkehrsdaten findet § 12 Abs. 2 und 5 entsprechende Anwendung.

Ob sie dabei als „Dritte“ tätig werden oder nicht, ist in der Literatur heftig umstritten. Ein besonderes Problem ist dabei die datenschutzrechtliche Kontrolle der Interessenvertretungen. Nach dem Beschluss des Bundesarbeitsgerichts vom 11.11. 1997 (Az.: 1 ABR 21/97) ist nach geltendem Recht dem betrieblichen Datenschutzbeauftragten untersagt, die Datenverarbeitung des Betriebsrats zu kontrollieren (dazu die Ausführungen zu § 29 Absatz 1). Begründet hat das Gericht seine Entscheidung mit der fehlenden Unabhängigkeit des betrieblichen Datenschutzbeauftragten. Es lässt jedoch Raum für eine andere Entscheidung, sofern die gesetzliche Unabhängigkeit der Beauftragten von der Betriebsleitung gewährleistet wird.

Zu Absatz 2

Angesichts der Erforderlichkeit einer Kontrolle der Datenverarbeitung der betrieblichen Interessenvertretung sind Betriebs- und Personalvertretungen gehalten, einen oder eine Beauftragte/n zu benennen. § 9 des Betriebsverfassungsgesetzes verknüpft die Zahl der Betriebsratsmitglieder mit der Zahl der wahlberechtigten Beschäftigten. Die Soll-Vorschrift greift daher bei Betrieben und Verwaltungen ab einer Größe von 151 Beschäftigten.

Zu Abschnitt 9: (Schlussvorschriften)

Zu § 34 (Unabdingbare Rechte der Beschäftigten)

Zu Absatz 1

Die Regelung knüpft an die Bestimmung des § 6 BDSG an. Die Rechte der Beschäftigten nach diesem Gesetz sowie anderen Rechtsvorschriften zum Schutz ihrer personenbezogenen Daten sind unabdingbar. Das heißt, sie können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden. Die Unabdingbarkeit schützt davor, dass die Betroffenen unter Druck gegenüber dem Betrieb auf ihre Rechte verzichten. Klargestellt wird aber, dass unabdingbar hier nicht mit höchstpersönlich gleichgesetzt wird. So können beispielsweise auch Erben, Bevollmächtigte oder gesetzliche Vertreter der Betroffenen einen Auskunftsanspruch wahrnehmen.

Zu Absatz 2

In der Praxis spielen Betriebsvereinbarungen im Bereich datenschutzrechtlicher Regelungen eine große Rolle. Diese Betriebsvereinbarungen zum Schutz der Beschäftigtendaten dürfen aber den Schutz ihrer personenbezogenen Daten, wie er durch dieses Gesetz vorgenommen wird, nicht vermindern. Sonst bestünde die Gefahr, dass die Rechte von Beschäftigten an dieser Stelle unterlaufen werden könnten.

Zu Absatz 3

Diese Regelung ergänzt die Bestimmungen zur Unabdingbarkeit der gesetzlichen Rechte. Deren Verwirkung ist gesetzlich ausgeschlossen. Ausschlussfristen für die Geltendmachung von Ansprüchen nach diesem Gesetz sind unzulässig.

Zu § 35 (Bußgeldvorschriften)

Zu Absatz 1

Der Katalog der Bußgeldvorschriften muss dem Umstand gerecht werden, dass wir es ähnlich wie im BDSG auch im Bereich des Beschäftigtendatenschutzes mit einer Vielzahl von Vorgängen zu tun haben, die unter bestimmten Voraussetzungen die Rechte der Beschäftigten in erheblichem Umfang verletzen können. Nicht jede Unrichtigkeit darf eine Sanktion nach sich ziehen. Eine Sanktion ist jedoch dann erforderlich, wenn die Verletzung der Betroffenenrechte erheblich ist. Aber auch Verletzungen von Verfahrensvorschriften müssen geahndet werden, um auch den Aufsichtsbehörden Maßstäbe für ihr Handeln zu vermitteln.

Zur Vermeidung von Wertungswidersprüchen entspricht die Höhe der Bußgelder denen für Ordnungswidrigkeiten in § 43 Absatz 3 Altern. 1 BDSG in Höhe von bis zu 50.000 Euro (Abs. 3).

Zu Nr. 1

Mit einem Bußgeld von bis zu 50.000 Euro kann belegt werden, wer entgegen § 6 Abs. 2 die Pflicht zur Rückgabe der Unterlagen der Bewerberinnen und Bewerber oder Löschung der Bewerberdaten trotz Aufforderung durch die Betroffenen nicht nachkommt. Diese Regelung stärkt die Rechte von Bewerberinnen und Bewerbern gegenüber Betrieben und Behörden. In der Praxis wird die Rückgabe eingereicherter Dokumente oftmals sehr nachlässig gehandhabt.

Zu Nr. 2

Das Profiling mit Hilfe von Beschäftigtendaten ist als erheblicher Eingriff bußgeldbewehrt.

Zu Nr. 3

Eine Ordnungswidrigkeit begeht ebenfalls, wer unter Verstoß gegen die Vorschrift des § 9 heimlich Gesundheitstests bzw. Tests über Alkohol oder Infektionskrankheiten selbst durchführt oder von Dritten durchführen lässt.

Zu Nr. 4

Wer entgegen § 10 Absatz 1 die Daten aus betrieblichen Überwachungssystemen für Zwecke der Leistungskontrolle oder Leistungsmessung verwendet, begeht eine Ordnungswidrigkeit nach Nr. 3. Die Vorschrift betrifft insbesondere den Einsatz von Videoüberwachung. Sie stellt bereits den Einsatz als solchen unter Bußgeldandrohung, wenn er mit der Zielrichtung einer Leistungskontrolle oder – messung erfolgt. Die spätere Verwendung von Daten aus betrieblichen Überwachungssystemen ist durch Nr. 4 gesondert bußgeldbewehrt, sofern sie zu unzulässigen Zwecken erfolgt. Nr. 3 stellt auch den Einsatz betrieblicher Überwachungssysteme in nicht ausschließlich der beruflichen Nutzung dienenden Räumen wie Duschräume (siehe Begründung zu § 10 Absatz 1) unter Bußgeldandrohung.

Zu Nr. 5

Eine Ordnungswidrigkeit begeht, wer entgegen § 10 Absatz 2 Daten zweckwidrig verwendet. Die Vorschrift ergänzt Nr. 3. Sie betrifft insbesondere die zweckwidrige Verwendung von Daten aus der Videoüberwachung. Diese Vorschrift stärkt den verfassungsrechtlichen Grundsatz der strengen Zweckbindung bei der Nutzung und Weitergabe personenbezogener Daten.

Zu Nr. 6

Ordnungswidrig handelt auch, wer entgegen § 10 Absatz 3 die Beschäftigten eine Beobachtung ohne Kenntnis der Betroffenen vornimmt oder von Dritten vornehmen lässt. Die Vorschrift betrifft – unabhängig von Nr. 3 – den heimlichen Einsatz von Videoüberwachung und anderen optisch-elektronischen Einrichtungen. Während Nr. 3 den offenen Einsatz von Überwachungssystemen betrifft, erfasst Nr. 5 das Überschreiten der – inhaltlichen wie zeitlichen – Grenzen des heimlichen Einsatzes.

Zu Nr. 7

Wer gegen die gesetzlichen Schutzvorschriften bei der Durchführung von Screening-Verfahren nach § 10 verstößt, begeht eine Ordnungswidrigkeit nach Nr. 6.

Zu Nr. 8

Wer entgegen der Voraussetzungen des § 12 Absatz 2 Verkehrsdaten verarbeitet oder diese Daten vorschriftswidrig nicht anonymisiert oder Inhalte erhebt.

Zu Nr. 9

Ordnungswidrig handelt, wer gegen die Schutzvorschrift des § 12 Absatz 3 verstößt, indem er ohne Wissen der Betroffenen deren Telefon abhört oder aufzeichnet oder dienstliche Gespräche mithört oder aufzeichnet, ohne dass die Grenzen des § 12 Absatz 3 Satz 2 eingehalten werden.

Zu Nr. 10

Eine Ordnungswidrigkeit nach Nr. 9 ist erfüllt, wenn jemand entgegen den Voraussetzungen des § 12 Absatz 4 dienstliche E-Mails liest oder die Nutzung der Internetnutzung ausforscht.

Zu Nr. 11

Ordnungswidrig nach Nr. 10 handelt, wer die Beschäftigten unter Verletzung der Vorschrift des § 13 die Beschäftigten nicht nachträglich über die Datenerhebung unterrichtet.

Zu Nr. 12

Wenn Arbeitgebende bei der Telearbeit (Fernarbeit) entgegen § 14 Absatz 2 bei in der Telearbeit Beschäftigten eine Leistungs- oder Verhaltenskontrollen durchführt, muss mit einem Bußgeld nach Nr. 11 rechnen. Hier werden grundlegende Rechte der Persönlichkeit der Beschäftigten vor unzulässigen Grenzüberschreitungen der Arbeitgebenden geschützt. Beschäftigte, die außerhalb des Betriebes, meist zu Hause, tätig sind, bedürfen eines Schutzes vor heimlicher Überwachung zum Zweck der Kontrolle ihrer Leistungen.

Zu Nr. 13

Wer entgegen der Zulässigkeitsgrenze nach § 15 Absatz 1 ein Ortungssystem einsetzt, kann mit einer Geldbuße belegt werden.

Zu Nr. 14

In dem Einsatz von Daten aus Ortungssystemen zur Erstellung von Bewegungsprofilen oder zur Leistungs- oder Verhaltenskontrolle liegt ebenfalls eine Ordnungswidrigkeit.

Zu Nr. 15

Bußgeldbewehrt ist auch die Erhebung biometrischer Daten, sofern sie nicht nach § 16 Absatz 1 zulässig sind. Bußgeldbewehrt ist auch der gegen § 16 Absatz 2 verstoßende Missbrauch biometrischer Verfahren zur Zeiterfassung der Beschäftigten.

Zu Nr. 16

Unzulässig und mit einem Bußgeld bewährt ist die Zusammenführung von Daten aus einem Rechtsgeschäft mit den Beschäftigten. Das betrifft die Fälle, in denen Beschäftigte zugleich auch Kunden in ihrem Betrieb sind. Diese Daten aus dem Arbeitsverhältnis sind zweckgebunden. Sie dürfen weder im eigenen Betrieb noch durch Weitergabe zu anderen Zwecken wie Werbung etc. verwendet werden.

Zu Nr. 17

Bußgeldbewehrt ist die Verletzung der Informationspflicht gegenüber den Beschäftigten nach § 1.

Zu Nr. 18

Wer entgegen § 19 seine gesetzliche Verpflichtung zur Benachrichtigung bei unrechtmäßiger Datenübermittlung gegenüber den Beschäftigten, den betrieblichen Datenschutzbeauftragten oder der Aufsichtsbehörde verletzt, begeht eine Ordnungswidrigkeit. Diese Vorschrift dient auch dem Schutz der Arbeit der Aufsichtsbehörden. Diese müssen wissen, wenn es zu nicht unerheblichen „Pannen“ bei der Datenverarbeitung im Betrieb gekommen ist.

Zu Nr. 19

Wer trotz der Vorschrift des § 21 Absatz 1 und 2 unrichtige oder unzulässig erhobene Daten verarbeitet, verletzt die Rechte der Beschäftigten. Er muss im Fall der wiederholten Weigerung trotz Aufforderung, die Daten zu korrigieren, mit einem Bußgeld rechnen.

Zu Nr. 20

Die Vorschrift des § 25 schützt Beschäftigte vor Benachteiligungen, wenn sie auf der Wahrung ihrer gesetzlich verbrieften Persönlichkeitsrechte bestehen. Die Skandale der letzten Monate und Jahre haben gezeigt, dass viele Betroffene aus Sorge um ihren Arbeitsplatz von ihren Rechten keinen Gebrauch machen. Das Gesetz sieht zum Schutz der Beschäftigten ein ausdrückliches Benachteiligungsverbot vor. Voraussetzung sind erhebliche Zurücksetzungen, bei denen ein Zusammenhang mit der Ausübung der Rechte nach § 25 besteht. Beispielfhaft genannt seien Umsetzungen, Gehaltsverschlechterungen, wiederholte Zurücksetzungen bei Arbeitszeitfragen. Damit dies effektiv durchgesetzt werden kann, sieht Nr. 19 bei Verstoß eine Ordnungswidrigkeit vor.

Zu Nr. 21

Mit einer Sanktion muss auch derjenige rechnen, der entgegen § 26 die Beschäftigten im Auftrag durch Detektive überwachen lässt. Diese Bußgeldvorschrift gibt den Aufsichtsbehörden Gelegenheit, gegen das Ausspähen von Beschäftigten mit der Verhängung von Bußgeldern vorzugehen.

Zu Nr. 22

Unzulässig und Bußgeld bewährt ist der Verstoß gegen das Verwertungsverbot in § 4 Absatz 5.

Zu Absatz 2

Die Abstufung zwischen „einfachen“ und „schweren“ Ordnungswidrigkeiten, die sich in der unterschiedlichen Höhe der Bußgelder ausdrücken, folgt der Regelungssystematik des BDSG.

Zu Nr. 1

Mit einem Bußgeld von bis zu 300.000 Euro müssen Betriebe rechnen, die unbefugt personenbezogene Daten von Beschäftigten verarbeiten, sofern sie nicht allgemein zugänglich sind. Die Vorschrift übernimmt die Regelung des § 43 Absatz 2 Nummer 1 BDSG. Im Unterschied zum BDSG umfasst in diesem Gesetzentwurf gemäß § 3 Absatz 6 der Begriff der „Verarbeitung“ die Verarbeitung von der Erhebung bis zu Verwendung der gewonnenen Daten, einschließlich der Löschung und der Nutzung.

Zu Nr. 2

Das erhöhte Bußgeld muss entrichten, wer unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält. Die Regelung übernimmt die des § 43 Absatz 2 Nummer 2 BDSG. Sinn und Zweck dieser Regelung ist es, auch im Arbeitsverhältnis zu verhindern, dass mit der Entscheidung der Abrufmöglichkeit die Daten offen gelegt werden können. Diese abstrakte Gefährdungsmöglichkeit soll ausgeschlossen werden (dazu: Gola, Bundesdatenschutzgesetz, zu § 43 Rn. 21).

Zu Nr. 3

Mit dem erhöhten Bußgeld muss auch rechnen, wer unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abrufen oder sich oder einem anderen aus automatisierten Verarbeitungen oder

nicht automatisierten Dateien verschafft. Diese Regelung übernimmt die Bestimmung des § 43 Absatz 2 Nummer 3 BDSG.

Zu Nr. 4

Die Bestimmung die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht, soll die illegale Datenbeschaffung, insbesondere durch Hacker, verhindern. Illegale Datenbeschaffung kann aber auch durch Firmen oder Personen erfolgen, die als Dritte die Informationssysteme in einem Betrieb neu einrichten oder warten. „Erschleichen“ meint auch, sich in den Besitz eines gültigen Passworts zu bringen. Die Vorschrift übernimmt den Wortlaut des § 43 Absatz 2 Nummer 4 BDSG.

Zu Nr. 5

Ordnungswidrig handelt auch, wer entgegen den Vorschriften dieses Gesetzes die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt. Die Regelung übernimmt die Schutzvorschrift für die strenge Zweckbindung der Daten in § 43 Absatz 2 Nummer 5 BDSG.

Zu Absatz 3

Die Vorschrift übernimmt die Höhe der Bußgelder in § 43 Absatz 3 BDSG. Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden. In den schwereren Fällen des Absatzes 2 beträgt die Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Bußgeldvorschriften wurden in der letzten Datenschutznovelle 2009 erhöht.

Zu Absatz 4

Die Strafvorschrift des § 44 BDSG entfaltet in der Praxis keine Wirkung. Dies beklagt mit Recht auch der DGB (Profil Arbeitnehmerdatenschutz, S. 18). Gerade in großen Betrieben ist es ohnehin schwierig, die für die Verhängung einer Kriminalstrafe erforderliche Zuordnung der persönlichen Verantwortung festzustellen. Andererseits ist es notwendig, den Aufsichtsbehörden wirksame Instrumente zu geben, die Vorschriften zum Schutz der Beschäftigtendaten durchzusetzen. Dazu gehören auch scharfe Sanktionen. Auf das Tatbestandsmerkmal der Schädigungsabsicht in § 44 BDSG wird hier in der als Ordnungswidrigkeit ausgestalteten Vorschrift ausdrücklich verzichtet, da sich in der Praxis die Absicht der Schädigung kaum nachweisen lässt.

In Anknüpfung an die Tatbestandsvoraussetzungen des § 44 BDSG werden für Handlungen nach Absatz 2 dieses Gesetzes Geldbußen von bis zu einer Million Euro zu bezahlen sein, wenn die Handlung gegen Entgelt begangen wurde.

Zu Artikel 2 (Änderung des Bundesdatenschutzgesetzes)

Zu Nummer 1 (§ 3 Absatz 11)

Die Definition der „Beschäftigten“ wird nicht mehr im Bundesdatenschutzgesetz, sondern in § 3 Absatz 1 des Beschäftigtendatenschutzgesetzes vorgenommen. Die Definition wird erweitert um die sog. Leiharbeiterinnen und Leiharbeiter.

Zu Nummer 2 (§ 4f Absatz 3 Satz 2)

Die Stellung der betrieblichen Datenschutzbeauftragten wird durch die Erwähnung der gesetzlichen Pflichten mit der Novellierung der Vorschrift im Bundesdatenschutzgesetz gestärkt. Die gesetzliche Stärkung der besonderen Rolle ist die Voraussetzung dafür, dass sie die zusätzlichen Aufgaben im Bereich des Schutzes der Beschäftigtendaten erfüllen können. Ohne diese Unabhängigkeit wäre es rechtlich nicht zu verantworten, die Prüfung sowohl der Beschäftigtendaten wie auch der Datenverarbeitung der Interessenvertretungen der Beschäftigten in die Hand der Beauftragten zu legen.

Zu Nummer 3 (§ 12 Absatz 4)

§ 12 Abs. 4 enthält die bisherige Regelung zum Beschäftigtendatenschutz gemäß der BDSG-Reform von 2009, welche durch den vorliegenden Vorschlag ersetzt wird.

Zu Nummer 4 (§ 32)

Die Aufhebung der Generalklausel des § 32 BDSG über „Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses“ ist die logische Konsequenz aus dem Inkrafttreten des neuen und eigenständigen Beschäftigtendatenschutzgesetzes.

Zu Artikel 3 (Änderung des Betriebsverfassungsgesetzes)

Datenschutzfragen unterliegen nach geltendem Recht bereits dem Mitbestimmungsrecht im Sinne des Betriebsverfassungsgesetzes und des Personalvertretungsrechts. Betriebs- und Personalräte müssen am Entscheidungsprozess in Form von Vereinbarungen beteiligt werden. Das Mitbestimmungsrecht des Betriebsrates besteht nach § 87 Abs. 1 Nr. 1 und 6 BetrVG für die Bereiche Ordnung des Betriebes, Arbeitnehmerverhalten und Technische Kontrolleinrichtungen. Ein Mitbestimmungsrecht bei der Bestellung der betrieblichen Datenschutzbeauftragten besteht indes nicht.

Die Erweiterung der Mitbestimmungsrechte des Betriebsrats dient der Stärkung der Stellung der betrieblichen Datenschutzbeauftragten. Die vorgesehene Ergänzung des § 87 BetrVG räumt dem Betriebsrat ein Mitbestimmungsrecht bei der Bestellung der betrieblichen Datenschutzbeauftragten ein. Erreicht werden soll die verstärkte Unabhängigkeit von der Geschäfts- oder Behördenleitung.

Ohne ein solches Mitbestimmungsrecht bei der Bestellung der Beauftragten wäre es unmöglich, den Beauftragten die Kontrolle der Datenverarbeitung des Betriebsrats zu übertragen. Mit dieser Bestimmung wird eine Voraussetzung für die Erweiterung der Zuständigkeiten der betrieblichen Datenschutzbeauftragten für die Kontrolle der Datenverarbeitung der Betriebs- und Personalräte erfüllt. Das Gericht hatte in seinem Beschluss vom 11.11. 1997 (Az.: 1 ABR 21/97) von den – noch ausstehenden – Sondervorschriften für Arbeitnehmerdatenschutz eine Regelung des Verhältnisses von Interessenvertretung und Beauftragten angemahnt (Artikel 49). Als eine der Voraussetzungen für die Kontrolle der Datenverarbeitung des Betriebsrats durch die betrieblichen Beauftragten nennt das Gericht die Erweiterung der Mitbestimmungsrechte des Betriebsrats bei Bestellung und Abberufung der Beauftragten (Artikel 53). Das BAG verlangt, dass die Beauftragten das Vertrauen beider Seiten genießen müssen. Diese Voraussetzung wird hier durch die Erweiterung der Mitbestimmungsrechte erfüllt.

Hier ist ein besonderes Vertrauensverhältnis zwischen der Interessenvertretung der Beschäftigten und den betrieblichen Datenschutzbeauftragten nicht nur rechtlich geboten, sondern auch in der Praxis praktisch unverzichtbar.

Zu Artikel 4 (Änderung des Bundespersonalvertretungsgesetzes)

Die Mitbestimmungsrechte der Personalvertretungen in Personalangelegenheiten sind nach geltendem Recht bereits umfänglich geregelt. In § 90g des Bundesbeamtengesetzes und in § 56 des Beamtenrechtsrahmengesetzes finden sich detaillierte Vorschriften zur automatisierten Personaldatenverarbeitung.

Dennoch ist die hier vorgenommene Ergänzung der Mitbestimmungsrechte im Katalog des § 75 Absatz 1 des Bundespersonalvertretungsgesetzes als Klarstellung sinnvoll, um auch im Bereich des öffentlichen Dienstrechts ausdrücklich die besondere Rolle der Datenschutzbeauftragten herauszustellen. Da auch die Datenverarbeitung der Personalvertretungen von den Beauftragten geprüft werden soll, bedarf es eines besonderen Vertrauensverhältnisses zwischen den Beauftragten und der Personalvertretung. Es darf auch bei den öffentlichen Stellen nicht dazu kommen, dass die betrieblichen Datenschutzbeauftragten in die Gefahr kommen, als Instrumente der Behördenleitung zu agieren. Die Personalvertretung soll daher wie

der Betriebsrat im Rahmen der Wahrnehmung seiner Rechte aus dem Betriebsverfassungsgesetz die Zustimmung zur Bestellung verweigern und die Abberufung verlangen können.

Zu Artikel 5 (Änderung des Gendiagnostikgesetzes)

Zu § 20 Absatz 2

Der Vorschlag sichert das Recht der Arbeitnehmenden auf Nicht-Wissen für den Bereich der Arbeitsschutzuntersuchungen ab. Nummer 1 regelt dies für Genproduktanalysen und die Nummer 2 durch Verweis für molekulargenetische und zytogenetische Untersuchungen.

Bereits nach den allgemeinen Prinzipien des Arbeitsschutzrechtes gilt grundsätzlich, dass arbeitsmedizinische Untersuchungen ein Angebot an die Beschäftigten sind (vgl. etwa § 11 ArbSchG) und also kein Zwang zur Durchführung solcher Untersuchungen besteht. Hauptzweck ist die Aufklärung und Beratung der Beschäftigten hinsichtlich der mit ihrer Arbeit verbundenen individuellen Gesundheitsrisiken. In einigen Spezialbereichen – etwa des Gefahrstoffrechtes – ist aber vorgesehen, dass das Ergebnis spezifischer Untersuchung das Urteil „nicht geeignet“ sein kann, welches ein Beschäftigungsverbot begründen kann. Gleiches gilt, wenn die Arbeitnehmenden eine solche Untersuchung ablehnen. Ein solches Beschäftigungsverbot kann dann Anlass sein, die Beschäftigten nicht einzustellen oder – wenn sie schon eingestellt sind – zu kündigen. Diese schwerwiegende Rechtsfolge ist für den vorliegenden Bereich nicht akzeptabel, da sie einen faktischen Zwang begründen würde, eine genetische Untersuchung vornehmen zu lassen, und damit tief in das Recht auf Nichtwissen eingriffe. Dem beugt der vorliegende Gesetzentwurf vor. Für diese Klarstellung besteht dabei Anlass, da aus der Zulassung genetischer Untersuchungen in diesem Bereich in der Praxis geschlossen werden könnte, nunmehr könnten genetische Untersuchungen – abweichend von der bisherigen Rechtslage – auch verpflichtender Bestandteil von spezialgesetzlich angeordneten arbeitsmedizinischen Untersuchungen sein. Insbesondere ließe sich vertreten, dass auch das Benachteiligungsverbot (§ 21 GenDG) in diesem Fall nicht eingreift, weil § 20 GenDG in Verbindung mit der jeweiligen spezialgesetzlichen Regelung insoweit etwas anderes vorsieht. Diesem Missverständnis muss vorgebeugt werden. Diese Regelung entspricht der Position des Bundesrates (BR-Drs. 633/1/08, Nr. 31, § 20 Abs. 2 S. 3).

Zu § 22

Art. 74 Abs. 1 Nr. 26 GG in Verbindung mit Art. 72 Abs. 2 GG überträgt dem Bund die Gesetzgebungskompetenz für die genetische Diagnostik, „wenn und soweit die Herstellung gleichwertiger Lebensverhältnisse im Bundesgebiet oder die Wahrung der Rechts- oder Wirtschaftseinheit im gesamtstaatlichen Interesse eine bundesgesetzliche Regelung erforderlich macht“. Im Gesetzentwurf selbst wird unter A. II. die bundesgesetzliche Regelung des GenDG mit der Notwendigkeit eines einheitlichen Schutzes des Rechts auf informationelle Selbstbestimmung und der Vermeidung von genetischer Diskriminierung begründet. Zur Wahrung der Rechtseinheit sollte bei der Umsetzung dieser grundlegenden Wertentscheidungen nicht differenziert werden zwischen privatwirtschaftlichen Rechtsverhältnissen und öffentlich-rechtlichen Verhältnissen und nicht danach, ob es sich um Beamtinnen oder Beamte des Bundes oder der Länder handelt. Auch aus Gründen der Gleichbehandlung und der Rechtssicherheit ist eine bundesgesetzliche Regelung auch für Beamtinnen und Beamte in den Ländern erforderlich, wie sie in diesem Änderungsantrag vorgeschlagen wird. Ebenfalls sollten die entsprechenden Schutzvorschriften Zivildienstleistende nicht ausnehmen.

Zu Artikel 6 (Änderung des Sozialgesetzbuchs III)

Der Schutz personenbezogener Daten ist nicht nur für Beschäftigte wichtig. Auch Arbeitssuchende haben einen Anspruch auf eine den Grundrechten gemäße Behandlung.

Zu Nummer 1

Die Bestimmung legt die zulässigen Zwecke der Verarbeitung klarstellend fest und soll damit die missbräuchliche Nutzung der betreffenden Daten insbesondere durch zugriffsberechtigte Dritte eingrenzen helfen.

Zu Nummer 2

Durch Einfügung eines neuen Absatzes 3 wird sicher gestellt, dass mit den Daten der Betroffenen sorgsam umzugehen ist und das Gebot der Zweckbindung zu beachten ist. Sind personenbezogene Daten von Arbeitssuchenden in Ausbildungs- und Arbeitsvermittlungsbörsen gespeichert, dürfen diese Daten anfragenden Dritten gegenüber nur unter der Voraussetzung zugänglich gemacht werden, wenn diese Dritten als Arbeitgebende einen Bedarf an Arbeitskräften darlegen.

Zu Nummer 3

Die Verschiebung der Ziffernfolge bei den Absätzen ist eine Folgeänderung zu Nummern 1 und 2.

Zu Artikel 7

Die Einfügung dient der Festlegung des Gerichtsstandes für die eröffnete Klagemöglichkeit nach diesem Gesetz.

Zu Artikel 8

Der Artikel regelt das Inkrafttreten.