

Stellungnahme des Deutschen Anwaltvereins
durch den Arbeitsrechtsausschuss
in Abstimmung mit dem Informationsrechtsausschuss
zum
Arbeitnehmerdatenschutz

Mitglieder des Ausschusses:

Rechtsanwalt Prof. Dr. Heinz Josef Willemsen,
Düsseldorf (Vorsitzender)
Rechtsanwalt Dr. Jobst-Hubertus Bauer, Stuttgart
Rechtsanwalt und Notar Paul-Werner Beckmann,
Herford
Rechtsanwältin Dr. Susanne Clemenz, Gütersloh
Rechtsanwalt Prof. Dr. Björn Gaul, Köln (Berichterstatter)
Rechtsanwalt Roland Gross, Leipzig (Berichterstatter)
Rechtsanwältin Angela Leschnig, Würzburg
Rechtsanwalt Dr. Stefan Lunk, Hamburg
Rechtsanwalt Dr. Hans-Georg Meier, Berlin
Rechtsanwältin Dr. Ulrike Schweibert, Frankfurt
Rechtsanwalt Dr. Uwe Silberberger, Düsseldorf
Rechtsanwältin Regina Steiner, Frankfurt

weitere Berichterstatterin für den Arbeitsrechtsausschuss:

Rechtsanwältin Dr. Nathalie Oberthür, Köln

zuständige DAV-Geschäftsführerin:

Rechtsanwältin Dr. Katharina Freytag

Verteiler:

Bundesministerium für Arbeit und Soziales

An die Mitglieder des Ausschusses für Arbeit und Soziales des Deutschen Bundestages

An die Mitglieder des Rechtsausschusses des Deutschen Bundestages

Bundesministerium für Wirtschaft und Technologie

An die Mitglieder des Ausschusses für Wirtschaft und Technologie des Deutschen Bundestages

Bundesvereinigung der Deutschen Arbeitgeberverbände

Deutscher Gewerkschaftsbund

Deutscher Arbeitsgerichtsverband e.V.

Deutscher Steuerberaterverband

Bund der Richterinnen und Richter der Arbeitsgerichtsbarkeit

Bundesministerium der Justiz

Bundesrechtsanwaltskammer

An die Rechtsanwaltskammern in der Bundesrepublik Deutschland

An die Justizministerien und Justizverwaltungen der Bundesländer der Bundesrepublik Deutschland

An die Mitglieder des Ausschusses Arbeitsrecht des Deutschen Anwaltvereins

An die Mitglieder des Geschäftsführenden Ausschusses der Arbeitsgemeinschaft Arbeitsrecht des Deutschen Anwaltvereins

An die Ministerien für Arbeit der Länder

Bundesarbeitsgericht

An die Landesarbeitsgerichte in der Bundesrepublik Deutschland

An die Mitglieder des Vorstandes des Deutschen Anwaltvereins e.V.

An die Vorsitzenden der Landesverbände des Deutschen Anwaltvereins e.V.

An die Vorsitzenden der Fach- und Gesetzgebungsausschüsse des Deutschen Anwaltvereins e.V.

Forum Junge Anwaltschaft

Neue Zeitschrift für Arbeitsrecht (NZA)

Zeitschrift Recht der Arbeit

Zeitschrift Arbeitsrechtliche Entscheidungen (AE)

Frankfurter Allgemeine Zeitung (FAZ)

Handelsblatt

Süddeutsche Zeitung

Financial Times

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit 67.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

I. Einführung

Auch nach Einführung eines neuen § 32 BDSG besteht weiterhin erheblicher Diskussionsbedarf über den Schutz des Rechts auf informationelle Selbstbestimmung bei der Datenverarbeitung im Arbeitsverhältnis. Insbesondere im Hinblick auf den Umgang mit Daten, die während des Beschäftigungsverhältnisses erhoben und verarbeitet werden, stellt sich die Frage nach klaren Regelungen. Dies gilt vor allem im Bereich des Internet-, Telefon- und E-Mail-Verkehrs am Arbeitsplatz. Dabei gewährleisten zwar die bereits existierenden gesetzlichen Regelungen und Grundsätze der Rechtsprechung schon heute ein sehr weitreichendes Niveau des Datenschutzes. Die aktuelle Diskussion lässt allerdings erkennen, dass Rechtsunsicherheit in Bezug auf den Anwendungsbereich einzelner Vorschriften besteht. Dies gilt es, bei einer Neuregelung des Arbeitnehmerdatenschutzes zu berücksichtigen.

II. Entwicklungen im Arbeitnehmerdatenschutzrecht

Am 01.09.2009 sind mit dem „Gesetz zur Änderung datenschutzrechtlicher Vorschriften“ (BGBl. I 2009, 2814 ff.) weitreichende Änderungen im Datenschutzrecht in Kraft getreten. Der Gesetzgeber hat damit auf tatsächliche oder vermeintliche Datenschutzverstöße verschiedener Unternehmen reagiert, die in den vorangegangenen Monaten bekannt geworden waren. Mit der Neuregelung sollte ein allgemeiner gesetzlicher Rahmen für den Umgang mit Arbeitnehmerdaten in Unternehmen und damit einhergehend für den Schutz des Persönlichkeitsrechts des Arbeitnehmers bei der Datenverarbeitung geschaffen werden. Ausweislich der Begründung der Beschlussempfehlung des Innenausschusses vom 01.07.2009 (BT-Drucks.16/13657), die als Grundlage für die Beschlussfassung des Bundestags am 03.07.2009 herangezogen wurde, sollte die Neuregelung ein eigenständiges Arbeitnehmerdatenschutzgesetz allerdings nicht entbehrlich machen, sondern im Wesentlichen die bislang von der Rechtsprechung erarbeiteten Grundsätze des Datenschutzes in Beschäftigungsverhältnissen zusammenfassen. Ein Präjudiz für das in der nächsten Legislaturperiode beabsichtigte Arbeitnehmerdatenschutzgesetz sollte damit ausdrücklich nicht verbunden sein. Schon der Koalitionsvertrag vom 26.10.2009 sieht indes vor, dass wesentliche Fragen des Datenschutzes konkretisiert und der Arbeitnehmerdatenschutz künftig in einem eigenen Kapitel des BDSG geregelt werden soll. Ergänzend hierzu hat die SPD-Fraktion im November 2009 den Entwurf eines Beschäftigtendatenschutzgesetzes in das Gesetzgebungsverfahren eingebracht

(BT-Drucks. 17/76), der derzeit den Ausschüssen zur Beratung zugewiesen ist. Bei der weiteren Ausgestaltung gesetzlicher Regelungen zum Arbeitnehmerdatenschutz sollten insbesondere die nachfolgend angesprochenen Fragen Berücksichtigung finden.

III. Aktuell: Änderung des Bundesdatenschutzgesetzes mit § 32 BDSG

Mit der letzten Änderung des Bundesdatenschutzgesetzes ist ein neuer § 32 BDSG eingeführt worden, der die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses regelt. Die bislang auch in Beschäftigungsverhältnissen geltende allgemeine Regelung des § 28 Abs. 1 Satz 1 Nummer 1 und Satz 2 BDSG sollte durch diese Spezialregelung konkretisiert und insoweit verdrängt werden.

Gemäß § 32 Abs. 1 Satz 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses zulässig, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung eines Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Über diese Generalklausel hinaus ist gemäß § 32 Abs. 1 Satz 2 BDSG die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten eines Beschäftigten zulässig, wenn sie aufgrund zu dokumentierender tatsächlicher Anhaltspunkte zur Aufdeckung von im Beschäftigungsverhältnis begangener Straftaten erforderlich ist und das schutzwürdige Interesse des Arbeitnehmers an dem Ausschluss der Datennutzung nicht überwiegt, diese insbesondere nicht unverhältnismäßig ist.

Die Neuregelung ist bereits im Vorfeld kontrovers diskutiert worden. Sie wirft zahlreiche neue Fragen auf, die im Zusammenhang mit einer Neuregelung des Arbeitnehmerdatenschutzes geklärt werden sollten; sie lässt darüber hinaus die bislang diskutierten Fragestellungen im Wesentlichen offen.

1. Sachlicher Anwendungsbereich von § 32 Abs. 2 BDSG

Die Regelungen des § 32 BDSG sollen künftig ohne Rücksicht auf die Form der Erhebung, Verarbeitung oder Nutzung der Daten gelten. Die Neuregelung beschränkt sich damit nicht mehr auf die Datenverarbeitung in automatisierten Systemen bzw. in oder aus nicht-automatisierten Dateien, sondern stellt ausdrücklich klar, dass auch die nicht-automatisierte Erhebung, Verwendung und Nutzung von Daten unter den Geltungsbereich der Regelungen des § 32 BDSG fällt. Eine Anpassung des § 1 Abs. 2 Nr. 3 BDSG, der die automatisierte Datennutzung als Voraussetzung für die Anwendbarkeit des BDSG auf nicht-öffentliche Stellen normiert, ist demgegenüber ebenso wenig erfolgt wie eine Änderung des § 27 Abs. 2 BDSG, der nicht-automatisierte Daten den Regelungen der §§ 27 ff BDSG nur dann unterstellt, wenn diese offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind.

Inhaltlich sollten mit § 32 BDSG ausweislich der Beschlussempfehlung des Innenausschusses lediglich die Grundsätze umgesetzt werden, die die Rechtsprechung an den Datenschutz im Arbeitsverhältnis stellt und die gemäß § 12 Abs. 4 BDSG auch für die öffentlichen Stellen des Bundes gelten. Allerdings betrifft die insoweit zitierte Rechtsprechung des BAG (Urteil vom 15.07.1987 - 5 AZR 215/86; Urteil vom 12.09.2006 - 9 AZR 271/06) lediglich Daten, die in der Personalakte des Beschäftigten enthalten waren. Ob dementsprechend § 32 Abs. 2 BDSG ebenfalls nur Daten erfasst, die zumindest eine strukturierte Datensammlung darstellen, ist jedoch ausweislich des letztlich eindeutigen Gesetzeswortlauts wohl zu verneinen. Demnach würden beispielsweise auch einzelne handschriftliche Aufzeichnungen des Arbeitgebers den Bestimmungen des BDSG unterfallen, ebenso die Datenerhebung durch rein tatsächliches Handeln, etwa durch Taschen- und Torcontrollen, durch die Befragung des Arbeitnehmers oder eines früheren Arbeitgebers oder durch die Beobachtungen des Wach- und Sicherheitspersonals. Diese Maßnahmen wären künftig nicht mehr allein an dem allgemeinen Persönlichkeitsrecht zu messen, sondern unterlägen auch dem strengen Erlaubnisvorbehalt des § 32 BDSG.

Der Ausschuss ist der Auffassung, dass eine derart weitreichende Verrechtlichung der betriebsinternen Kommunikation nicht sachgerecht ist. Sie widerspricht auch § 27 Abs. 2 BDSG. Themenbereiche wie etwa das Fragerecht des Arbeitgebers unterliegen bereits jetzt umfassenden Restriktionen durch den Persönlichkeitsrechtsschutz und den Vorgaben des AGG, so dass eine zusätzliche Unterstellung unter das Datenschutzrecht zur Wahrung eines ausreichenden Schutzniveaus nicht erforderlich ist. Auch die Datenschutzrichtlinie 95/46/EG erfasst bei der nicht automatisierten Datenverarbeitung nur Dateien, deren Inhalt nach personenbezogenen Kriterien strukturiert ist, nicht aber unstrukturierte Akten. § 32 Abs. 2 BDSG sollte daher ersatzlos gestrichen und der Anwendungsbereich des BDSG im nichtautomatisierten Bereich auf Dateien i.S.d. § 3 Abs. 2 Satz 2 BDSG beschränkt bleiben. Andernfalls besteht die Gefahr, dass schon der zwischenmenschliche Umgang im Rahmen des Arbeitsverhältnisses an datenschutzrechtlichen Vorgaben zu messen ist. Dies gilt schon für die Begrüßung: „Guten Morgen, wie geht es Ihnen?“ Die Frage nach dem persönlichen Befinden wäre unzulässig, weil aus der Sicht des Juristen für die Durchführung des Arbeitsverhältnisses nicht erforderlich.

2. Verhältnis des § 32 BDSG zu anderen Erlaubnistatbeständen

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist gemäß § 4 Abs. 1 BDSG zulässig, wenn dies durch eine Rechtsvorschrift erlaubt oder angeordnet ist. § 32 BDSG ist dabei (wie z.B. auch § 28 Abs. 1 Nr. 1 BDSG) ein Erlaubnistatbestand in diesem Sinne. Das Verhältnis von § 32 BDSG zu anderen datenschutzrechtlichen Erlaubnistatbeständen bedarf allerdings der Klarstellung. Dies gilt umso mehr, als § 32 Abs. 1 S. 1 2. Satzteil BDSG den Eindruck erweckt, dass nur die dort genannte Voraussetzung einer „Erforderlichkeit“ erfüllt werden muss, um personenbezogene Daten bei Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses zu verarbeiten. Es fehlt eine Regelung, die zu erkennen gibt, dass die in anderen Rechtsvorschriften enthaltenen Regelungen weiterhin Grundlage und Schranke der Datenverarbeitung sind. Beispielfhaft sei hier nur auf die Weiterleitung personenbezogener Daten an Betriebsrat,

Schwerbehindertenvertretung oder Integrationsamt oder die Verarbeitung solcher Daten im Zusammenwirken mit Betriebs- oder Personalrat (z. B. Personalbeurteilungssystem, Sozialplan mit Zuschlagsregelungen für Abfindungen) hingewiesen.

Ausweislich der Beschlussempfehlung des Innenausschusses sollen durch § 32 BDSG maßgeblich die Regelungen des § 28 Abs. 1 Satz 1 Nummer 1 und 2 und Satz 2 BDSG verdrängt werden. Die Datennutzung für Zwecke des Beschäftigungsverhältnisses soll sich damit ausschließlich nach § 32 BDSG richten. Die übrigen allgemeinen und bereichsspezifischen Datenschutzvorschriften werden demgegenüber durch § 32 BDSG nicht verdrängt. Sie werden zunehmende Bedeutung erlangen, wenn die Datenverarbeitung keinen unmittelbaren Zusammenhang mit den Zwecken des Beschäftigungsverhältnisses aufweist. Hier ist etwa auf die Durchführung einer arbeitsrechtlichen Due Diligence hinzuweisen, die auch die Übermittlung personenbezogener Daten an den potentiellen Erwerber beinhaltet. Deren Zulässigkeit dürfte auch künftig vor allem an §§ 28 Abs. 1 Nr. 2, 28 Abs. 2 Nr. 2 BDSG zu messen sein.

Auch die Möglichkeit, die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten auf der Grundlage einer freiwillig erteilten, schriftlichen Einwilligung des Beschäftigten (§§ 4, 4 a BDSG) vorzunehmen, ist unverändert geblieben. Dies sollte im Interesse einer praktikablen Handhabung des Datenschutzes auch in Zukunft beibehalten werden. Dabei spielt es aus Sicht des Ausschusses keine Rolle, ob die Einwilligung im Arbeitsvertrag oder im Rahmen einer gesonderten Erklärung erfolgt.

Da § 4 Abs. 1 BDSG ausdrücklich von einer Rechtfertigung durch „dieses Gesetz oder eine andere Rechtsvorschrift“ spricht, schließt dies andere gesetzliche oder kollektivrechtliche Regelungen (z. B. BDSG, BetrVG, Tarifvertrag, Betriebsvereinbarung) als weitere Rechtfertigung zur Datenverarbeitung nicht aus. Allerdings entzieht sich auch § 32 BDSG der Lösung der bislang kontrovers diskutierten Frage, ob kollektive Regelungen wie Tarifverträge und Betriebsvereinbarungen, die als Rechtsvorschriften in diesem Sinne zu qualifizieren sind, von den Vorgaben des BDSG abweichen dürfen, oder ob das BDSG den datenschutzrechtlichen Mindeststandard vorgibt, an den auch die Sozial- und Betriebspartner gebunden sind. Ausgehend von der Rechtsprechung des BAG (Urteil vom 27.05.1986 - 1 ABR 48/84) ist bislang überwiegend angenommen worden, dass durch kollektive Regelungen von den gesetzlichen Bestimmungen auch zum Nachteil des Betroffenen abgewichen werden kann. Ob an dieser Auffassung festgehalten werden kann, ist insbesondere nach Einführung des § 32 BDSG streitig geworden. Das Verlangen, kollektiven Regelungen lediglich die Möglichkeit einer Auslegung und Konkretisierung des BDSG einzuräumen, nicht aber eine Absenkung des materiellen Schutzniveaus, wird unter anderem mit den Vorgaben der Datenschutzrichtlinie 95/46/EG begründet, die keine Ausnahmen zulasse. Das Schutzniveau des BDSG geht indes im Bereich des Arbeitsrechts über die Vorgaben der Datenschutzrichtlinie hinaus; außerdem können individuelle Regelungen die betrieblichen Bedürfnisse häufig besser erfassen als allgemeine Vorgaben, wobei sich ohnehin die Sozial- und Betriebspartner ebenfalls an den grundgesetzlichen Wertungen auszurichten haben, so dass ein erhebliches Absenken der Schutzstandards kaum

denkbar ist. Diese Frage sollte im Interesse der Rechtssicherheit im Rahmen des weiteren Gesetzgebungsverfahrens geklärt werden.

3. Das Merkmal der „Erforderlichkeit“ in § 32 BDSG

§ 32 Abs. 1 Nr. 1 und 2 BDSG erlaubt die Datenerhebung, -verarbeitung und -nutzung, wenn dies zur Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder für dessen Durchführung oder Beendigung „erforderlich“ ist. Demgegenüber war die Datennutzung gemäß § 28 Abs. 1 Nr. 1 BDSG zulässig, wenn sie der Zweckbestimmung des Beschäftigungsverhältnisses „dienlich“ war. Dies wirft die Frage auf, ob mit dem Begriff der „Erforderlichkeit“, der jetzt auch in § 28 Abs. 1 Nr. 1 BDSG genannt wird, eine Verschärfung oder – wovon der Ausschuss ausgeht – eine inhaltsgleiche Neubenennung des Prüfungsmaßstabs verbunden sein soll.

Bislang wurde angenommen, dass die Erhebung, Verarbeitung und Nutzung geschützter Daten zulässig und damit erforderlich ist, wenn ein unmittelbarer Zusammenhang zwischen der beabsichtigten Speicherung und dem konkreten Verwendungszweck besteht. Dabei musste die Datennutzung nicht „unabdingbar“ sein, war jedoch an dem Grundsatz der Verhältnismäßigkeit zu messen (BAG vom 22.10.1986 - 5 AZR 660/85). Es liegt nahe, dass § 32 BDSG diesen Maßstab übernehmen wollte. Dennoch bleibt im Detail etwa unklar, ob die Erforderlichkeit nur dann bejaht wird, wenn der vorgegebene Zweck durch die Datennutzung gerade noch erreicht wird, oder ob die Datennutzung auch zur bestmöglichen Zweckerfüllung zulässig ist. Bislang war die Erhebung, Verarbeitung und Nutzung zulässig, wenn berechnete Interessen des Unternehmens auf andere Weise nicht oder nicht angemessen gewährleistet wurden.

Darüber hinaus beinhaltet § 32 Abs. 1 BDSG in den Sätzen 1 und 2 einen Wertungswiderspruch, indem die Aufklärung von Straftaten an deutlich strengere tatbestandliche Voraussetzungen gebunden wird, als die allgemeine Datenerhebung und -nutzung im Rahmen der Durchführung des Arbeitsverhältnisses. Dies kann auch dann relevant werden, wenn die Beendigung eines Arbeitsverhältnisses in Rede steht. Denn hier würden dem Wortlaut des Gesetzes nach an eine Beendigung wegen des Verdachts einer Straftat strengere datenschutzrechtliche Anforderungen gestellt als an eine Beendigung wegen sonstiger Formen einer Vertragspflichtverletzung. Auch mit Blick auf europarechtliche Vorgaben regt der Ausschuss daher an, einen einheitlichen Prüfungsmaßstab der Verhältnismäßigkeit einzuführen, der in Anlehnung an die bisherige Rechtsprechung unter Berücksichtigung der Eignung, Erforderlichkeit und Angemessenheit der Datenverarbeitung eine Abwägung der wechselseitigen Interessen beinhaltet, deren Ausgangspunkt und Schranke die Festlegung eines legitimen Zwecks ist.

Änderungen im Hinblick auf den Umfang der Zweckbestimmung hat § 32 BDSG nicht mit sich gebracht. Auch weiterhin dürfte daher die Datenspeicherung und -nutzung für Zwecke zulässig sein, die noch nicht aktuell, wohl aber in Zukunft vorliegen könnten. Forderungen nach einer Zweckbestimmung ex ante, die dem Arbeitgeber die Nutzung der Daten zu einem anderen als dem ur-

sprünglichen Zweck untersagt, sind in § 32 BDSG zu Recht ebenso wenig umgesetzt worden wie die gesetzliche Festschreibung berücksichtigungsfähiger Zwecksetzungen.

4. Prävention und Aufdeckung von Straftaten

Im wesentlichen Fokus der öffentlichen Diskussion stand zuletzt die Frage, in welchem Umfang Arbeitgeber personenbezogene Daten zur Kriminalitätsbekämpfung oder –prävention nutzen dürfen. § 32 Abs. 1 Satz 2 BDSG sieht nunmehr vor, dass zur Aufdeckung von Straftaten personenbezogene Daten erhoben, verarbeitet oder genutzt werden dürfen, wenn zu dokumentierende tatsächliche Anhaltspunkte bestehen, dass die Datennutzung zur Aufdeckung von im Beschäftigungsverhältnis begangener Straftaten erforderlich ist und das schutzwürdige Interesse des Beschäftigten an der Datennutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

§ 32 Abs. 1 Satz 2 BDSG ist damit auf bereits begangene Straftaten fokussiert; Maßnahmen zum Zwecke der Prävention sollen wohl von dieser Vorschrift nicht erfasst werden, wenn auch der Begriff der Aufdeckung von Straftaten im weitesten Sinn Präventionsmaßnahmen erfasst. Ausweislich der Beschlussempfehlung des Innenausschusses sollen „Maßnahmen zur Verhinderung von Straftaten oder sonstigen Rechtsverstößen“ weiterhin nach der Generalklausel in § 32 Abs. 1 Satz 1 BDSG zu beurteilen sein, also dem Wortlaut des Gesetzes nach nicht notwendigerweise einen Anfangsverdacht voraussetzen. Hier wäre zur Begründung dieser Erfordernisse auf allgemeine datenschutzrechtliche Voraussetzungen zurückzugreifen, die § 32 Abs. 1 S. 1 BDSG selbst aber nicht nennt. Ausgehend davon, dass auch § 28 Abs. 1 S. 1 Nr. 1 BDSG Compliance-Maßnahmen gegen eine Rechtsverletzung durch Dritte erfasst und an die gleichen Voraussetzungen knüpft, wäre es sinnvoll, den Anwendungsbereich von §§ 28 Abs. 1 S. 1 Nr. 1, 32 Abs. 1 S. 1, 2 BDSG, die tatbestandlichen Voraussetzungen und das Verhältnis der Regelungen zueinander klarzustellen. Denn wenn § 32 BDSG vorbeugende Maßnahmen zur Kriminalitätsbekämpfung in Gänze ausschließen oder einschränken würde, wären auch die gesetzlich vorgegebenen Compliance-Maßnahmen, insbesondere eine wirksame Korruptionsbekämpfung (etwa durch Screening, Scoring, Whistle-blowing) in Unternehmen künftig weitgehend ausgeschlossen. Dies würde auch allgemeine Maßnahmen bis hin zur Einlasskontrolle und Trainingsmaßnahmen betreffen. Gesetzgeberisch gewollt ist dies trotz unklaren Wortlauts aber offenbar nicht. Denn der Gesetzgeber hat gerade klargestellt, dass § 32 Abs. 1 Satz 1 BDSG präventiven Maßnahmen nicht ausschließen soll, ohne jedoch für diese eine eindeutige rechtliche Grundlage zu schaffen. Der Ausschuss regt deshalb an, wegen der allgemeinen Bedeutung und der strafrechtlichen Konsequenzen solcher Verhaltensweisen eine ausdrückliche Regelung zur Zulässigkeit von Präventionsmaßnahmen zu treffen, insbesondere dann, wenn Maßnahmen sowohl Arbeitnehmer als auch Dritte betreffen (z. B. Schutzvorschriften gegen Werksspionage, die mit einer Kontrolle von personenbezogener Daten verbunden sind, Serverprotokollierung, Torkontrolle durch Videoaufnahme). Dies gilt gerade für die verdachtsunabhängige (präventive) Datenerhebung im Rahmen eines Compliance-Frühwarnsystems. Dabei ist zu berücksichtigen, dass der Schutz der Beschäftigten bereits durch §

87 Abs. 1 Nr. 6 BetrVG und das übergreifende Gebot der Datensparsamkeit (§ 3 a BDSG) in erheblichem Maße gewährleistet wird.

Problematisch ist weiterhin, dass der Anwendungsbereich des § 32 Abs. 1 Satz 2 BDSG auf Straftaten beschränkt ist und weder Ordnungswidrigkeiten noch Vertragspflichtverstöße einschließt. Auch hier dürfte die Generalklausel des § 32 Abs. 1 Satz 1 BDSG einschlägig sein, wobei dann allerdings nicht nachzuvollziehen ist, weshalb die Aufdeckung von Straftaten an strengere tatbestandliche Voraussetzungen gebunden werden soll, als dies bei der Aufdeckung weniger schwerwiegender Vertragspflichtenverstöße der Fall ist. Auch angesichts der Bedeutung, die Vertragspflichtenverstöße im Arbeitsverhältnis bereits unterhalb der Schwelle strafbaren Handelns haben können (z. B. Verstoß gegen Vertretungsregelungen, Ordnungswidrigkeiten im Bereich der Arbeitnehmerüberlassung oder des Umweltrechts), sollte daher eine weitergehende Klarstellung der Voraussetzungen und der zulässigen Intensität entsprechender Maßnahmen vorgenommen werden.

Unklar ist bislang schließlich Art und Umfang der Pflicht zur Dokumentation der Anhaltspunkte, aus denen der Anfangsverdacht hergeleitet wird. Fraglich ist auch, insbesondere im Hinblick auf die Löschungspflicht gemäß § 35 Abs. 2 BDSG, wie lange der Arbeitgeber diese Dokumentation vorhalten muss, selbst wenn sich der Anfangsverdacht nicht erhärtet.

5. Datenschutz nach Beendigung des Beschäftigungsverhältnisses

§ 32 BDSG enthält keine Regelung über die Behandlung von Daten aus beendeten Arbeitsverhältnissen. Allerdings unterfallen dem Begriff des Beschäftigten gemäß § 3 Abs. 11 BDSG n.F. auch Personen, deren Beschäftigungsverhältnis beendet ist. Dem entspricht die Beschlussempfehlung des Innenausschusses, nach der der Begriff der Beendigung auch die Abwicklung des Beschäftigungsverhältnisses nach seiner Beendigung umfassen soll. Dieses Verständnis ist auch sachgerecht, wäre doch anderenfalls ein Rückgriff auf § 28 BDSG erforderlich, was wiederum der Intention des § 32 BDSG als einheitliche Generalklausel für den Datenschutz in Beschäftigungsverhältnissen widerspräche. Unabhängig von dieser Frage sind auch zukünftig nach der Beendigung des Beschäftigungsverhältnisses Daten gemäß § 35 Abs. 2 Nr. 3 BDSG zu löschen, wenn und sobald sie zur Abwicklung des Beschäftigungsverhältnisses und zur Erfüllung gesetzlicher Vorschriften nicht mehr erforderlich sind.

6. Persönlicher Anwendungsbereich des Arbeitnehmerdatenschutzrechts

§ 32 BDSG gilt für Beschäftigte; dies erfasst nach der Legaldefinition des § 3 Abs. 11 BDSG n.F. unter anderem Arbeitnehmer, Auszubildende, arbeitnehmerähnliche Personen, Bewerber, ehemalige Beschäftigte und Beamte, Richter und Soldaten des Bundes. Für die Arbeitnehmer öffentlicher Stellen des Bundes verweist § 12 Abs. 4 BDSG n.F., für Arbeitnehmer der Länder § 12 Abs. 2 BDSG jedenfalls zum Teil auf die Geltung des § 32 BDSG. Für Beamte der Länder gelten demgegenüber eigenständige Regelungen. Hier dürfte sich eine Vereinheitlichung anbieten, wobei zu

prüfen wäre, ob und in welchem Umfang bestehende Unterschiede zwischen öffentlichen und privaten Arbeitgebern unterschiedliche Regelungen erfordern.

Im Hinblick auf die Einbeziehung der arbeitnehmerähnlichen Personen weist der Ausschuss darauf hin, dass Arbeitnehmerschutzvorschriften in der Vergangenheit zu Recht nur dann auf diese Personengruppe erstreckt wurden, wenn dies zur Gewährleistung eines angemessenen Schutzniveaus unabdingbar gewesen ist. Demgegenüber ist mittlerweile eine Tendenz festzustellen, arbeitnehmerähnliche Beschäftigte den Arbeitnehmern generell gleichzustellen (z. B. AGG, PflegezG). Der Ausschuss regt an, die Notwendigkeit einer Einbeziehung der arbeitnehmerähnlichen Personen in den Anwendungsbereich des Arbeitnehmerdatenschutzes kritisch zu überprüfen, da diese selbständig tätig und mangels Einbindung in den Betrieb nicht in vergleichbarer Weise schutzbedürftig sind. Durch die Erstreckung des Anwendungsbereichs des Arbeitnehmerdatenschutzes auf arbeitnehmerähnliche Selbständige entsteht demgegenüber die Gefahr, dass künftige Änderungen des Arbeitnehmerdatenschutzes ungeprüft auch auf arbeitnehmerähnliche Selbständige erstreckt werden. Ein Bedürfnis hierfür besteht nicht, da § 28 BDSG ein ausreichendes Schutzniveau für den Zivilrechtsverkehr gewährleistet, das sogar dem Wortlaut nach inhaltsgleich ist.

IV. Ausblick: Fragestellungen für ein künftiges Arbeitnehmerdatenschutzrecht

Mit § 32 BDSG ist der überwiegende Teil datenschutzrechtlicher Fragestellungen ganz bewusst offen gelassen worden, um die politische Diskussion nicht unter den Zeitdruck der ablaufenden Legislaturperiode zu stellen. Denn die Frage, wie ein neues Arbeitnehmerdatenschutzrecht aussehen soll, ist höchst umstritten.

Teilweise wird gefordert, zunächst einmal Vollzugsdefizite abzubauen. Die bereits bestehenden gesetzlichen Bestimmungen und die von der Rechtsprechung entwickelten Grundsätze reichen nach dieser Auffassung aus, um die kollidierenden Interessen von Arbeitgebern und Arbeitnehmern in einen angemessenen Ausgleich zu bringen. Durch die Anwendung der bestehenden Regelungen und eine konsequente Ahndung etwaiger Verstöße sei ein ausreichendes Schutzniveau gewährleistet. Auch führe eine kleinteilige Gesetzgebung angesichts der technischen Entwicklung schnell zu einer Überregulierung. Ein kodifiziertes Arbeitnehmerdatenschutzrecht dürfe schließlich angesichts des im internationalen Vergleich bereits hohen Datenschutzniveaus nicht dazu führen, dass Einstellungs-, Durchführungs- oder Beendigungsprozesse im Arbeitsleben erschwert und die Wettbewerbsbedingungen deutscher Unternehmen im europäischen und außereuropäischen Markt dadurch verschlechtert werden.

Demgegenüber wird eine zum Teil massive Begrenzung der Datennutzung gefordert, um Arbeitnehmer möglichst umfassend zu schützen. Ein breiter Konsens ist hier nicht erkennbar. Die offenen Fragen sollten deshalb in dem anstehenden Gesetzgebungsverfahren beantwortet und entsprechend umgesetzt werden. Vor dem Hintergrund der umfassenden inhaltlichen Kontroverse

sieht der DAV-Arbeitsrechtsausschuss zu diesem Zeitpunkt davon ab, konkrete Vorschläge für die beabsichtigte gesetzliche Neuregelung zu unterbreiten. Der Ausschuss weist jedoch darauf hin, dass im Rahmen des weiteren Gesetzgebungsverfahrens insbesondere die nachfolgend zusammengefassten Fragestellungen weiter intensiv diskutiert und gegebenenfalls zum Gegenstand einer datenschutzrechtlichen Neuregelung gemacht werden sollten. Zu einem Entwurf solcher Neuregelungen soll dann eine Stellungnahme des Ausschusses im Rahmen des Gesetzgebungsverfahrens erfolgen.

1. Regelung im BDSG oder Arbeitnehmerdatenschutzgesetz

Der Gesetzgeber wird zu entscheiden haben, ob inhaltliche Änderungen des Datenschutzrechts in das BDSG eingefügt oder in einem gesonderten Arbeitnehmerdatenschutzgesetz niederlegt werden. Hierzu sieht der Koalitionsvertrag der 17. Legislaturperiode vor, dass der Arbeitnehmerdatenschutz in einem eigenen Kapitel im BDSG geregelt werden soll. Dies wird begrüßt, da dadurch eine Zersplitterung des Datenschutzrechts vermieden wird und auch allgemeine Regelungen des Datenschutzes für das Arbeitsverhältnis nutzbar gemacht werden können.

2. Datenschutz im Bewerbungsverfahren

a) Allgemeine Grundsätze

Die Frage, welche Daten im Bewerbungsverfahren erhoben werden dürfen, ist mit Blick auf das allgemeine Persönlichkeitsrecht von der Rechtsprechung im Zusammenhang mit dem „Fragerecht“ des Arbeitgebers bereits in weitem Umfang geklärt. Weitere Einschränkungen ergeben sich aus dem AGG. Nach Auffassung des Ausschusses ist damit ein ausreichendes Schutzniveau gewährleistet, so dass eine weitergehende Bestimmung der zulässigerweise zu erfassenden Daten an sich nicht erforderlich ist.

Allerdings ist bislang ungeklärt, auf welche Weise die Daten erhoben werden dürfen, etwa im Hinblick auf die zunehmende Erhebung von Bewerberdaten aus dem Internet (insbesondere aus den sog. „sozialen Netzwerken“ StudiVZ, Facebook, Xing etc.). Grundsätzlich müssen Daten gemäß § 4 Abs. 2 BDSG bei dem Betroffenen selbst erhoben werden; eine Ausnahme von dem Gebot der Direkterhebung gilt jedoch, wenn dies für den Ablauf des Bewerbungsprozesses auch unter Abwägung mit den Interessen des Beschäftigten erforderlich ist, ebenso, gemäß § 28 Abs. 1 Nr. 3 BDSG, wenn die Daten allgemein zugänglich sind. Es sollte klargestellt werden, dass diese Ausnahme auch für das Beschäftigtenverhältnis weiterhin gilt. Denn die Besonderheit solcher Netzwerke liegt nicht nur darin, dass die Daten durch den Betroffenen frei veröffentlicht werden. Hinzu kommt, dass eine gesetzliche Regelung neben den datenschutzrechtlichen Überlegungen auch den Grundrechten der Meinungs- und Informationsfreiheit Rechnung tragen müsste. Die Erhebung und Nutzung von Daten entsprechender Netzwerke unter Missachtung bestehender Zugangsregelungen ist bereits heute unzulässig.

Ein weiterer Regelungskomplex betrifft die Frage mit dem Umgang der Bewerberdaten nach Abschluss des Bewerbungsverfahrens. Nach der Entscheidung über die Besetzung des Arbeitsplatzes ist die Grundlage für die Ermächtigung zur Datennutzung gemäß § 32 Abs. 1 Satz 1 BDSG entfallen, dennoch verbleibt im Hinblick auf etwaige Entschädigungsansprüche aus dem AGG ein erhebliches Interesse des Arbeitgebers an der weiteren Speicherung der Daten. Allgemein ist bislang umstritten, ob und für welche Dauer Bewerberdaten aufbewahrt werden dürfen und ob und unter welchen Voraussetzungen Bewerberpools gebildet werden dürfen.

Ergänzend ist zu prüfen, ob eine gesetzliche Klarstellung erfolgen soll, ob, unter welchen Voraussetzungen und in welchem Umfang Daten aus psychologischen und medizinischen Tests erhoben und genutzt werden dürfen, in welcher Form die Einwilligung des Betroffenen erteilt werden muss und ob und ggf. unter welchen Voraussetzungen dem Bewerber ein Auskunfts- oder Lösungsrecht zusteht.

b) Gendiagnostische Untersuchungen

Gendiagnostische Maßnahmen sind bereits Gegenstand der §§ 19 und 20 des Gendiagnostikgesetzes (GenDG) vom 31.07.2009 (BGBl. I 2009, 2529 ff.), das überwiegend am 01.02.2010 in Kraft treten wird. Gemäß § 19 GenDG kann der Arbeitgeber von Beschäftigten weder vor noch nach Begründung des Beschäftigungsverhältnisses die Vornahme genetischer Untersuchungen oder Analysen oder die Mitteilung von Ergebnissen bereits vorgenommener genetischer Untersuchungen oder Analysen verlangen, solche Ergebnisse entgegennehmen oder verwenden. Dasselbe gilt für arbeitsmedizinische Vorsorgeuntersuchungen; in diesem Rahmen sind jedoch gemäß § 20 Abs. 2 GenDG diagnostische genetische Untersuchungen durch Genproduktanalyse zulässig, soweit sie zur Feststellung genetischer Eigenschaften erforderlich sind, die für schwerwiegende Erkrankungen oder schwerwiegende gesundheitliche Störungen, die bei einer Beschäftigung an einem bestimmten Arbeitsplatz oder mit einer bestimmten Tätigkeit entstehen können, ursächlich oder mitursächlich sind. Gemäß § 20 Abs. 4 GenDG i.V.m. § 13 GenDG dürfen die dem Arbeitgeber zur Verfügung gestellten Ergebnisse einer etwaigen genetischen Untersuchung nur für die Zwecke verwendet werden, für die sie gewonnen wurden; sie sind zu vernichten, sobald sie für diese Zwecke nicht mehr benötigt werden oder die betroffene Person ihre Einwilligung widerrufen hat. Flankiert werden diese Regelungen von einem arbeitsrechtlichen Benachteiligungsverbot in § 21 GenDG.

c) Ärztliche (Einstellungs-) Untersuchungen

Ärztliche Untersuchungen vor oder nach der Begründung des Arbeitsverhältnisses sollen die Eignung des Beschäftigten für die von ihm angestrebte oder ausgeübte Beschäftigung feststellen. Das Untersuchungsergebnis kann über die Einstellung, Beförderung oder Kündigung des Beschäftigten entscheiden. Aus diesem Grund dürfen ärztliche Untersuchungen nur mit ausdrücklicher Einwilligung des Betroffenen durchgeführt werden, zumal diese regelmäßig mit einem Eingriff in die körperliche Unversehrtheit und das Recht auf informationelle Selbstbestimmung (Art. 1, 2 GG) ver-

bunden sind. Soweit demgegenüber lediglich die körperliche Geschicklichkeit geprüft werden soll, sind Einstellungsuntersuchungen arbeitsrechtlich bislang zulässig.

Hier wird zu diskutieren sein, ob ärztliche Einstellungsuntersuchungen zukünftig tatsächlich gemäß § 32 Abs. 2 BDSG dem Maßstab des § 32 BDSG unterstellt sein sollen, und ob weitergehende Regelungen über die grundsätzlichen Voraussetzungen und die zulässigen Inhalte der Untersuchung und über die Verwertung der gewonnenen Erkenntnisse getroffen werden sollen. Gleiches gilt für die Zulässigkeit von Drogen- und Alkoholtests. Für diese Fragen sollten nach Auffassung des Ausschusses weiter die spezialgesetzlichen Regelungen und allgemeine Vorgaben zum Schutz des Persönlichkeitsrechts maßgeblich sein.

d) Psychologische Eignungsuntersuchungen

Auch psychologische Eignungsuntersuchungen sind grundsätzlich nur mit Einwilligung des Betroffenen und mit einem konkreten Bezug zu dem jeweiligen Arbeitsplatz zulässig (hierzu BAG 13. 2. 1964 - 2 AZR 286/63) Weiterhin muss der Betroffene über die Funktionsweise und den Zweck der Untersuchung aufgeklärt werden. Ungeklärt ist bislang, ob der Arbeitgeber vorrangig alternative Erkenntnisquellen nutzen muss und ob die die Auswertung der Daten auf die Frage der allgemeinen Eignung beschränkt werden muss oder auch auf konkrete Bewertungen erstreckt werden darf. Hier wird zum Teil gefordert, psychologische Eignungsuntersuchungen auf einen bestimmten Personenkreis (Führungskräfte) und die Erhebung „weicher“ Qualifikationsmerkmale (zB. Sozialkompetenz, Leistungsfähigkeit) insgesamt oder auf bestimmte Arbeitnehmergruppen zu beschränken.

e) Graphologische Gutachten

Auch graphologische Gutachten dürfen nach derzeitiger Rechtslage nur mit Einwilligung des Bewerbers eingeholt werden. Allerdings wird überwiegend eine konkludente Einwilligung bereits dann angenommen, wenn der Bewerber einen handschriftlichen Lebenslauf vorlegt; in diesem Fall müsse er damit rechnen, dass ein graphologisches Gutachten eingeholt werde. Inhaltlich darf das graphologische Gutachten allerdings nicht weiter gehen, als die Erkenntnisse für die Durchführung des Arbeitsverhältnisses von Bedeutung sind; die Erstellung einer allgemeinen Charakterstudie ist unzulässig. In diesem Zusammenhang wird insbesondere zu klären sein, ob die Annahme einer konkludenten Einwilligung im Hinblick auf § 4 a BDSG datenschutzrechtlich ausreichend ist oder ob gesetzlich weitergehende Voraussetzungen an die Einwilligung, aber auch an die Ausführung der Untersuchung bestimmt werden müssen.

f) Biometrische Daten

Biometrische Daten dienen stets der Ermittlung der Identität einer Person. Biometrische Verfahren werden dadurch ermöglicht, dass verschiedene Körper- oder Verhaltensmerkmale einem bestimmten Menschen zuzuordnen sind. Erkannt - etwa im Rahmen besonderer Zugangssysteme - wird der Betroffene hier anhand seiner körperlichen Individualität. Biometrische Daten sind als beson-

dere Art personenbezogener Daten besonders geschützt und dürfen nur unter den engen Voraussetzungen des § 28 Abs. 6 BDSG erhoben, verarbeitet oder genutzt werden. Hier wird zu erwägen sein, ob dieses Schutzniveau ausreicht, oder ob, wie teilweise gefordert wird, die Nutzung biometrischer Daten im Arbeitsverhältnis gänzlich ausgeschlossen oder noch weiter begrenzt wird.

3. Datenschutz während des Beschäftigungsverhältnisses

Zahlreiche datenschutzrelevante Maßnahmen während der Durchführung des Arbeitsverhältnisses bleiben auch nach Inkrafttreten des § 32 BDSG ungelöst und sollten in dem bevorstehenden Gesetzgebungsverfahren behandelt werden.

a) Kontrolle des E-Mailverkehrs sowie der Telefon- und Internetnutzung

Erhebliche Bedeutung hat die Frage des Arbeitnehmerdatenschutzes im Zusammenhang mit der Überwachung von Telefon-, Internet- und E-Mail-Verkehr am Arbeitsplatz. Zulässigkeit und Grenzen eines Zugriffs des Arbeitgebers auf diese Daten sind zum Teil heftig umstritten und sollten im Interesse der Rechtssicherheit umfassend geregelt werden.

Für den E-Mail-Verkehr wird bislang angenommen, dass sich bei ausschließlich dienstlicher Nutzung der betrieblichen Kommunikationssysteme die Möglichkeiten der Datenerfassung und -kontrolle durch den Arbeitgeber nach den Bestimmungen des BDSG richten. Dabei wird die Erfassung von Verbindungsdaten überwiegend als zulässig angesehen, wobei dies im Hinblick auf die in Ziel- bzw. Senderadressen regelmäßig enthaltenen Namen streitig ist. Auch die Berechtigung des Arbeitgebers, die Inhalte dienstlicher E-Mails zur Kenntnis zu nehmen, ist umstritten. Überwiegend wird angenommen, der Arbeitgeber müsse das uneingeschränkte Recht haben, auf Arbeitsvorgänge und -ergebnisse der Mitarbeiter zuzugreifen, ein Recht der Arbeitnehmer, ihren Arbeitsbereich vor dem Arbeitgeber geheim zu halten, sei abzulehnen. Die geschäftliche E-Mail sei der schriftlichen Geschäftskorrespondenz gleichzustellen, die der Arbeitgeber ebenfalls uneingeschränkt einsehen dürfe. Demgegenüber wird teilweise eingewandt, die Kommunikation per E-Mail sei dem Telefonat angenähert, so dass eine inhaltliche Überwachung allenfalls bei dem begründeten Verdacht strafbarer Handlungen oder schwerer Vertragsverstöße zulässig sei.

Ist demgegenüber die private Nutzung der betrieblichen Kommunikationsmittel erlaubt oder zumindest geduldet, wird der Arbeitgeber nach überwiegender, wenn auch ebenfalls streitiger Auffassung zum Telekommunikationsdiensteanbieter. Er unterliegt damit - jedenfalls für die Dauer des Übermittlungsvorgangs (Hessischer VGH vom 19.05.2009 - 6 A 2672/08) - dem Fernmeldegeheimnis gemäß §§ 85 ff. TKG und hat zusätzlich die Vorschriften über die Datenerhebung, -verarbeitung und -nutzung nach § 3 TDSV und § 3 TDDSG zu beachten (ArbG Hannover 28.04.2005 - 10 Ca 791/04). Demnach dürfen allenfalls Verkehrsdaten kontrolliert werden, etwa zu Abrechnungszwecken gem. § 96 Abs. 1 TKG oder bei einem Verdacht auf Leistungserschleichung oder sonst rechtswidriger Inanspruchnahme der Telekommunikationsnetze gemäß § 100 Abs. 3 TKG. Eine weitergehende, insbesondere inhaltliche Datenkontrolle ist bei Anwendung der tele-

kommunikationsrechtlichen Vorschriften grundsätzlich ausgeschlossen, wobei in der arbeitsrechtlichen Literatur Ausnahmen, insbesondere bei dem begründeten Verdacht von Straftaten oder schweren Vertragsverletzungen, erwogen werden.

Auch die Kontrollmöglichkeiten des Arbeitgebers bei Call-Center-Arbeitsplätzen werden kontrovers beurteilt. Die dort üblichen Überwachungsmethoden des „Silent Monitoring“ (verdecktes Mithören) und des „Voice Recording“ (Aufzeichnen der Anrufe) werden zwar bei verhältnismäßiger Ausprägung - Einwilligung des Betroffenen, nur stichprobenartige Überwachung, angemessene Überwachungsintervalle, ausreichende Information des Betroffenen, begrenzte Verwertbarkeit der Ergebnisse - überwiegend als zulässig erachtet, doch fehlt auch hier ein hinreichend klar abgegrenztes Spektrum zulässigen Handelns.

Diese Spannungsfelder sollten durch eindeutige Regelungen bereinigt werden. Dem schutzwürdigen Interesse des Arbeitnehmers, private Daten, die keine Relevanz zum Arbeitsverhältnis besitzen, vor einer Erfassung und Verarbeitung durch den Arbeitgeber zu schützen, muss ebenso Geltung verschafft werden wie dem Interesse des Arbeitgebers, die geschäftliche Kommunikation auch ohne Einwilligung des Arbeitnehmers zu überblicken und die Arbeitsleistung zu kontrollieren. Dies gilt insbesondere wenn – wie bei Call Center-Mitarbeitern – die Tätigkeit des Arbeitnehmers ganz oder im wesentlichen in der Erbringung von Kommunikationsleistungen besteht.

Angesichts der notwendigen Differenzierung in Bezug auf die Zulässigkeit einer privaten Nutzung betrieblicher Einrichtungen regt der Ausschuss an, eine gesetzliche Vermutung zu normieren, nach der die Nutzung betrieblicher Kommunikationssysteme im Zweifel ausschließlich zu dienstlichen Zwecken gestattet ist. Ein schutzwertes Bedürfnis der Arbeitnehmer an einer Privatnutzung besteht nicht, so dass es angesichts der weitreichenden Folgen für den Arbeitgeber angemessen ist, die Berechtigung zur privaten Nutzung nur bei entsprechenden (ggf. schriftlichen) Vereinbarungen anzunehmen. Aus denselben Gründen sollte das Recht des Arbeitgebers normiert werden, ein eingeräumtes Recht zur Privatnutzung für die Zukunft jederzeit zu widerrufen. Umfang und Intensität des Zugriffsrechts des Arbeitgebers auf die Kommunikationsdaten sollten für betriebliche und private Nutzung eindeutig geregelt werden, wobei bei der Gestaltung entsprechender Regelungen die Wertungen des Bundesverfassungsgerichts (Urteil vom 27.02.2008 - 1 BvR 370/07) zu staatlichen Online-Durchsuchungen, das aus dem allgemeinen Persönlichkeitsrecht gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ein neues Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme abgeleitet hat, zu beachten sein werden. Dieses Grundrecht ist anzuwenden, wenn die Eingriffsermächtigung des Staates Systeme erfasst, die personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt erhalten können, dass durch einen Zugriff auf das System ein Einblick in wesentliche Teile der Lebensgestaltung einer Person gewonnen oder sogar ein aussagekräftiges Bild der Persönlichkeit erlangt werden kann. Insoweit wird zu prüfen sein, inwiefern diese Wertungen bei der Kontrolle betrieblicher Informationssysteme zu berücksichtigen sind. Und schließlich sollte die Reichweite des Geltungsbereichs des TKG im Rahmen der betrieblichen Kommunikationsmittel klargestellt werden.

b) Überwachungssysteme (Videoaufzeichnungen, GPS, RFID etc.)

Die Zulässigkeit der Arbeitnehmerüberwachung ist wesentlicher Bestandteil der aktuellen Diskussion. Ob für diesen Bereich weitergehende gesetzliche Regelungen erforderlich sind, ist dabei umstritten. So wird zum Teil das Erfordernis einer Kodifikation angesichts der bestehenden Gesetzeslage und der einschlägigen Rechtsprechung abgelehnt. Das BAG hat mit Beschluss vom 29.06.2004 (1 ABR 21/03) und vom 26.08.2008 (1 ABR 16/07) der Überwachung von Beschäftigten einerseits strenge Grenzen gesetzt, andererseits aber eine einzelfallbezogene Betrachtung verlangt. Bei der insoweit erforderlichen Interessenkollision muss eine Güterabwägung unter Berücksichtigung der Umstände des Einzelfalls durchgeführt werden. Für die Abwägung ist insbesondere die Anzahl der überwachten Personen, die Art, Dauer und Intensität der Überwachung, die Einbeziehung unbeteiligter Dritter und der Anlass der Überwachung von Bedeutung. Der heimlichen Überwachung werden noch engere Grenzen gezogen; sie soll nur dann zulässig sein, wenn eine notwehrähnliche Situation besteht. Diese Rechtsprechung wird von § 32 BDSG aufgegriffen, wobei die Regelung präventiver Maßnahmen unzureichend geblieben ist (Ziffer II.4). Erweiternd wird zum Teil verlangt, die Regelung des § 6b BDSG auch auf nicht-öffentliche Räume auszudehnen und heimliche Überwachungen gänzlich auszuschließen.

Entgegen vereinzelt vertretener Auffassung hat der Gesetzgeber bislang auch keinen eigenständigen Regelungsbedarf für den Einsatz der RFID-Technik gesehen. Diese Technik ermöglicht es, die mit Hilfe von Funketiketten (RFID-Chips) gespeicherten Daten berührungslos und ohne Sichtkontakt an ein Empfangsgerät (oft verbunden mit einem Computer) zu übermitteln. Werden Arbeitnehmer oder von ihnen mitzuführende Gegenstände (zB. Firmenausweis, Dienstbekleidung) mit RFID-Chips versehen, kann jederzeit festgestellt werden, zu welchem Zeitpunkt sich ein Arbeitnehmer an welchem Ort im Betrieb aufgehalten hat. Hier wird zu prüfen sein, ob die allgemeinen Bestimmungen des BDSG, verbunden mit den besonderen Informationspflichten bei mobilen Speichermedien gemäß § 6c BDSG, ausreichend sind.

c) Schutz von Kunden- und Arbeitnehmerdaten vor Zugriffen durch Mitarbeiter

Nicht abschließend geklärt ist bislang der Schutz von Kunden- und Mitarbeiterdaten gegen den unbefugten Zugriff anderer Mitarbeiter. Gegen die missbräuchliche Nutzung der vom Arbeitgeber zulässigerweise gespeicherten personenbezogenen Daten werden in der Praxis vorwiegend technische (Passwortgeschützter Zugang zu Datenbanken, verschließbare Aktenschränke) oder vertragliche (Daten- und Kundenschutzklauseln) Maßnahmen ergriffen. Rechtsgrundlage hierfür ist § 9 BDSG i.V.m. der Anlage zu § 9 BDSG, woraus sich die vom Arbeitgeber als verantwortlicher Stelle zu treffenden technischen und organisatorischen Maßnahmen (insbesondere zur Zutritts-, Zugangs- und Zugriffskontrolle) ergeben. Hier ist zu erwägen, ob die bestehenden gesetzlichen Rahmenbedingungen klarer gefasst werden müssen, um Kunden- und Arbeitnehmerdaten vor Zugriffen anderer Mitarbeitern zu schützen.

4. Besondere Arten personenbezogener Daten (Beispiel: Krankheit, Behinderung)

Nach der überwiegenden Auffassung war die Rechtsgrundlage für die Verarbeitung besonderer Daten im Arbeitsverhältnis in § 28 Abs. 6 BDSG zu sehen. Folgt man der Beschlussempfehlung des Innenausschusses, wird lediglich § 28 Abs. 1 Nr. 1 und 2 BDSG durch § 32 BDSG verdrängt. § 28 Abs. 6 BDSG findet damit weiterhin Anwendung. Darüber hinaus mag erwogen werden, den Umgang mit Gesundheitsdaten, etwa im Rahmen des betrieblichen Eingliederungsmanagements gemäß § 84 SGB IX, weitergehend zu konkretisieren. Dies gilt allerdings nicht nur für etwaige Einschränkungen. Vielmehr sollte angesichts der aktuellen Diskussion beispielsweise auch klargestellt werden, dass der Arbeitgeber krankheitsbedingte Daten speichern und verarbeiten darf, deren Kenntnis notwendig ist, um das Vorliegen der gesetzlichen Voraussetzungen für besondere Pflichten zu erkennen (z. B. Zahl der Krankheitstage) und diese Pflichten auch ausfüllen zu können (z. B. Art und Ursache einer Erkrankung). Die letztgenannte Kenntnis ist notwendig, um das Eingliederungsmanagement nach § 84 Abs. 2 SGB IX ordnungsgemäß umzusetzen. Entsprechendes gilt für die Art und die Folgen einer Behinderung, damit die aus § 81 Abs. 4 SGB IX folgenden Pflichten zur Ausgestaltung des Arbeitsplatzes und der Arbeitsabläufe erfüllt werden können.

5. Rechte der betrieblichen Arbeitnehmervertretung

Weiterhin wird zu klären sein, ob die bestehenden Regelungen zum Datenschutz einschließlich etwaiger Neuregelungen die Mitwirkungs- und Mitbestimmungsrechte der betrieblichen Arbeitnehmervertretung berühren. Problematisch ist daran, dass schon heute in der Praxis selten zwischen der bloßen Überwachung einer Einhaltung des BDSG und anderer Vorschriften zum Arbeitnehmerdatenschutz (§ 80 Abs. 1 Nr. 1 BetrVG) und der Mitbestimmung bei der Anwendung technischer Einrichtungen, die geeignet sind, Leistung oder Verhalten von Arbeitnehmern zu überwachen (§ 87 Abs. 1 Nr. 6 BetrVG), differenziert wird. Vielfach wird eine Mitbestimmung auch dort geltend gemacht, wo bloße Datenverarbeitung erfolgt, ohne dass die technischen Einrichtungen leistungs- oder verhaltensbezogene Daten erfassen können (z. B. Adressdaten).

Zum Teil wird verlangt, die Rechte der betrieblichen Arbeitnehmervertretung, bei der Planung und Durchführung der Erhebung, Verarbeitung und Nutzung von personenbezogenen und personenbeziehbaren Arbeitnehmerdaten mitzubestimmen, vor dem Hintergrund veränderter technischer Bedingungen auszubauen. Es sollen neue Mitbestimmungsrechte, insbesondere Veto-Rechte bei Maßnahmen des Arbeitgebers zur Realisierung des Arbeitnehmerdatenschutzrechts geschaffen werden. Dies gilt zum Beispiel für ein Mitbestimmungsrecht bei der Bestellung und Abberufung des Datenschutzbeauftragten, der anderenfalls keine Kompetenz besitzt, die Einhaltung des Datenschutzrechts durch die Arbeitnehmervertretung zu überprüfen (BAG vom 11.11.1997 - 1 ABR 21/97). Eine Ausweitung der betrieblichen Mitbestimmung wird von Vertretern der gegenteiligen Auffassung demgegenüber abgelehnt. Die Kernbereiche des kollektiven Arbeitsrechts dürften nicht unter dem Deckmantel des Datenschutzes ausgedehnt werden. Der Datenschutz solle das notwendige Maß an Persönlichkeitsrechtsschutz im Betrieb sicherstellen, nicht aber ein Einfallstor für unzulässige Koppelungsgeschäfte eröffnen. Einer Ausweitung der Mitbestimmungsrechte, die be-

reits heute eine umfassende Beteiligung gewährleisten, bedürfe es deshalb auch im Bereich des Arbeitnehmerdatenschutzes nicht. Die heutigen Bestimmungen seien ausreichend, man müsse sie nur gesetzeskonform umsetzen. Dies gelte schon wegen der umfassenden Berechtigung zur Überwachung einer Einhaltung von Arbeitnehmerschutzvorschriften, die auch das Recht zur Vorlage der erforderlichen Unterlagen beinhaltet.

6. Datenschutzbeauftragter

Gleichzeitig mit der Einführung des § 32 BDSG wurden auch die Rechte der betrieblichen Datenschutzbeauftragten gestärkt. Gemäß § 4f Abs. 3 BDSG genießt der Datenschutzbeauftragte künftig unabhängig davon, ob der Kündigungsgrund einen Bezug zu seiner Amtsausübung besitzt, für die Dauer seiner Amtszeit und für einen nachwirkenden Zeitraum von einem Jahr besonderen Kündigungsschutz dahingehend, dass eine Kündigung nur aus wichtigem Grund gemäß § 626 BGB zulässig ist. Zusätzlich hat er zur Gewährleistung hinreichender fachlicher Kompetenz Anspruch auf die Teilnahme an Fort- und Weiterbildungsmaßnahmen.

Umstritten und im weiteren Gesetzgebungsverfahren klärungsbedürftig ist, ob und inwiefern darüber hinausgehend Regelungen mit dem Ziel einer Stärkung des betrieblichen Datenschutzbeauftragten getroffen werden sollen. So wird teilweise gefordert, Betriebsrat und betrieblichen Datenschutzbeauftragten zur engen Zusammenarbeit zu verpflichten und den Datenschutzbeauftragten im Sinne einer Vorabkontrolle in datenschutzrelevante Entscheidungen des Arbeitgebers einzubeziehen. Auch wird eine Begrenzung der Gründe zur Abberufung des Datenschutzbeauftragten erwogen. Darüber hinaus wird zur Steigerung des Qualitätsniveaus die Festlegung einheitlicher Leitlinien für den Beruf des betrieblichen Datenschutzbeauftragten gefordert, wobei nach Auffassung des DGB zusätzlich geboten sei, den betriebsinternen Datenschutzbeauftragten generell von seiner Pflicht zur Arbeitsleistung freizustellen. Erwogen wird weiterhin, das Übergehen des Datenschutzbeauftragten zu sanktionieren.

7. Informationsrechte des Arbeitnehmers

Fraglich ist, ob die existierende Informationspflicht § 4 Abs. 3 BDSG und die Rechte auf Benachrichtigung, Auskunft und Berichtigung nach den §§ 33 ff. BDSG genügen, um den Arbeitnehmer darüber in Kenntnis zu setzen, welche Daten zu welcher Zeit und zu welchem Zweck über ihn erhoben worden sind und in welcher Art und Weise sie ausgewertet werden. Aus diesem Grund wird zum Teil gefordert, die Arbeitnehmer aus Gründen der Transparenz umfassend darüber zu informieren, welche Daten zu welcher Zeit auf welche Weise und zu welchem Zweck über sie erhoben und in welcher Art und Weise sie ausgewertet werden. Zusätzlich werden umfassende Auskunfts- und Einsichtsrechte gefordert. Hier wird eine Abwägung zwischen dem berechtigten Informationsbedarf des Arbeitnehmers und der praktikablen Durchführung der Informationspflichten getroffen werden müssen.

8. Einführung eines Konzernprivilegs

Der Datenaustausch innerhalb eines Konzernverbundes wird derzeit nicht anders behandelt als der Datenaustausch mit einem beliebigen Dritten. Er bereitet immer dann rechtliche Probleme, wenn nicht auf das Privileg der Auftragsdatenverarbeitung gemäß § 11 BDSG zurückgegriffen werden kann. Dieses erlaubt die Verarbeitung personenbezogener Daten durch andere (Konzern-) Unternehmen nur dann, wenn die beauftragte Stelle in Abhängigkeit des Arbeitgebers agiert und damit lediglich Hilfs- und Unterstützungsfunktionen ausübt. Dies kann bei einer konzern einheitlichen Personalabteilung der Fall sein. Sobald aber die beauftragte Stelle bei der Datenverarbeitung eigene Interessen verfolgt (z.B. Budgetplanung, Personalentwicklung, Compliance), liegt keine reine Auftragsverarbeitung mehr vor. Ähnliche Probleme ergeben sich bei der einheitlichen Führung eines Gemeinschaftsbetriebes durch mehrere Unternehmen. Hier ist streitig, ob die konzernweite Datenverwendung durch die Einführung eines Konzernprivilegs erleichtert werden, oder ob im Gegenteil die Möglichkeit der Auftragsdatenverarbeitung ausgeschlossen oder zumindest eingeschränkt werden soll.

Damit verbunden ist die Frage nach einer Überwachung der datenschutzrechtlichen Bestimmungen durch die Arbeitnehmervertretungen. Die Wahrung jedenfalls des europäischen Datenschutzniveaus muss auch bei grenzüberschreitenden Sachverhalten in Drittländer nicht nur gewährleistet, sondern auch von den Arbeitnehmern und Arbeitnehmervertretern überprüfbar bleiben. Bislang beschränkt sich das Recht des Betriebsrats, die Einhaltung der datenschutzrechtlichen Bestimmungen zu überwachen, auf den jeweiligen Betrieb im Inland. Sollte der unternehmensüberschreitende Datenverkehr erleichtert werden, wird zu erwägen sein, ob und ggf. in welcher Weise die Kontrollmöglichkeiten der Arbeitnehmervertreter entsprechend anzupassen sind.

9. Datenschutzrechtliches Territorialprinzip / Cloud Computing

Bislang wenig beleuchtet ist die Zulässigkeit der grenzüberschreitenden Datenverlagerung. Beim sogenannten „Cloud Computing“ wird das IT-System durch den Arbeitgeber nicht mehr selbst betrieben, sondern über einen oder mehrere externe Anbieter bezogen. Software und Daten befinden sich nicht mehr auf dem lokalen Rechner im Unternehmen, sondern bei dem externen Anbieter; der Zugriff auf diese entfernten Systeme erfolgt über ein [Netzwerk](#), in der Regel über das [Internet](#). Problematisch ist dabei, dass nicht mehr ohne weiteres festgestellt werden kann, wo sich die Daten tatsächlich physisch befinden. Dem deutschen Datenschutzrecht liegt aber das Territorialprinzip nach § 1 Abs. 5 BDSG zugrunde, so dass personenbezogene Daten nur dann geschützt werden, wenn die datenschutzrechtlich relevante Handlung im Inland vorgenommen wird. Beim Cloud Computing können sich die Daten aber nicht nur in verschiedenen Ländern befinden, sondern innerhalb kürzester Zeit auch an einen anderen Ort verlagert werden. Die Geltung des BDSG, aber auch die Zuständigkeit der deutschen Gerichtsbarkeit ist kaum festzustellen, wenn der Ort der Vornahme der datenschutzrechtlich relevanten Handlung unklar ist. Es besteht daher Diskussionsbedarf dahingehend, wie hinreichender Datenschutz auch im Bereich des Cloud Computing sichergestellt werden kann. Dabei wird erwogen, Abweichungen von dem Territorialprinzip zuzulas-

sen, so dass die betroffene Person unabhängig davon, wo sich die Daten befinden, datenschutzrechtlichen Schutz genießt; im Hinblick auf die Datenübertragung in außereuropäische Drittländer wird dies auch von der Datenschutzrichtlinie 95/46/EG gefordert, sofern das Drittland kein ausreichendes eigenes Datenschutzniveau aufweist..

10. Aufsichtsbehörden

Zu klären ist die Frage, ob und ggf. inwieweit die Möglichkeiten der Aufsichtsbehörde auszubauen sind, auf Verstöße gegen Datenschutzregeln zu reagieren. Erste Schritte schafft § 38 Abs. 5 Satz 1 BDSG. Danach sollen Aufsichtsbehörden nicht mehr nur Bußgeldverfahren einleiten, sondern auch anordnen können, dass der entsprechende Verstoß eingestellt wird. Die jüngsten BDSG-Novellen haben überdies zu einer Erhöhung des Bußgeldrahmens geführt und die Möglichkeit der Gewinnabschöpfung eröffnet.

11. Verwertungsverbote

Streitig ist bislang, ob und in welchem Umfang Daten, die unter Verstoß gegen datenschutz-, aber auch mitbestimmungsrechtliche Bestimmungen erworben worden sind, vor Gericht verwertet werden können. Die im US-amerikanischen Recht verankerte „fruit of the poisonous tree“ - Doktrin, nach der im Fall einer rechtsfehlerhaften Daten- bzw. Beweiserhebung die Verwertung der gewonnenen Informationen im Sinne eines umfassendes prozessuales Verwertungsverbot unzulässig wäre, ist dem deutschen Prozessrecht fremd (BVerfG vom 02.07.2009 - 2 BvR 2225/08). Rechtswidrig erlangte Daten unterliegen daher ohne ausdrückliche Rechtsgrundlage keinem prozessualen Verwertungsverbot. Ein Beweisverwertungsverbot kann sich allerdings ergeben, wenn der Schutzzweck der verletzten Norm eine solche Sanktion zwingend gebietet. Ob dies bei einem Verstoß gegen datenschutzrechtliche Bestimmungen der Fall ist, ist Streitig (bejahend ArbG Frankfurt vom 25.01.2006 - 7 Ca 3342/05); bei einem Eingriff in Persönlichkeitsrechte des Arbeitnehmers wird in der Regel durch eine Güterabwägung im Einzelfall ermittelt, ob das allgemeine Persönlichkeitsrecht den Vorrang verdient (BAG vom 13.12.2007 - 2 AZR 537/06). Es wäre deshalb zu diskutieren, ob ein allgemeines datenschutzrechtliches Beweisverwertungsverbot geschaffen oder ob an den bisherigen einzelfallabhängigen Grundsätzen festgehalten werden soll.

12. Sanktionen

Im Rahmen einer Überarbeitung des Arbeitnehmerdatenschutzrechts sollte geprüft werden, ob eine Erweiterung der Straftatbestände geboten ist, um einen wirksamen Arbeitnehmerdatenschutz zu gewährleisten. So wird beispielsweise gefordert, den rechtswidrigen Umgang mit besonders geschützten Daten als Straftatbestand in den § 44 BDSG aufzunehmen und Verstöße gegen das BDSG nicht mehr als Antrags-, sondern als Officialdelikte auszugestalten.