**GESELLSCHAFT FÜR DATENSCHUTZ
UND DATENSICHERHEIT e.V.**

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)252 B

S t e l l u n g n a h m e

zum

a) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes
(BT-Drucksache 17/4230)
unter Berücksichtigung des
Arbeitspapiers der Berichterstatter der Koalitionsfraktionen
(Ausschussdrucksache 17(4)255)

b) Gesetzentwurf der Fraktion der SPD
Entwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis (Beschäftigtendatenschutzgesetz)
(BT-Drucksache 17/69)

c) Gesetzentwurf der Fraktion BÜNDNIS 90/DIE GRÜNEN
Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen
(BT-Drucksache 17/4853)

d) Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN
Persönlichkeitsrechte abhängig Beschäftigter sichern – Datenschutz am Arbeitsplatz stärken
(BT-Drucksache 17/121)

e) Antrag der Fraktion DIE LINKE
Datenschutz für Beschäftigte stärken
(BT-Drucksache 17/779)

erstellt von

Rechtsanwalt Andreas Jaspers,

Geschäftsführer der GDD e.V.

Gesellschaft für Datenschutz
und Datensicherheit e.V.
Pariser Str. 37 · 53117 Bonn
Tel.: 0228/69 43 13 · Fax: 0228/69 56 38
Internet: www.gdd.de · E-Mail: info@gdd.de

I. Vorbemerkung

Die Stellungnahme hat im Schwerpunkt den Gesetzentwurf der Bundesregierung zum Gegenstand (BT-Drucksache 17/4230). Zu den übrigen Gesetzentwürfen und Anträgen wird thematisch Bezug genommen.

Es ist zu begrüßen, dass die Bundesregierung ihrer Ankündigung gefolgt ist, in seinem Entwurf den Beschäftigtendatenschutz nicht in einem eigenständigen Gesetzeswerk, sondern als Abschnitt des Bundesdatenschutzgesetzes zu regeln. Positiv zu bewerten ist auch die Intention des Regierungsentwurfs, eine gesetzliche Konkretisierung des richterrechtlich geprägten Arbeitnehmerdatenschutzes herbeizuführen. Zugleich ist es für die Fortentwicklung des Beschäftigtendatenschutzes sinnvoll, den Einsatz der Informations- und Kommunikationstechnologien im Beschäftigungsverhältnis unter dem Gesichtspunkt des Persönlichkeitsrechtsschutzes zu konkretisieren.

Der Regierungsentwurf sieht keine Regelung der Datenschutzkontrolle beim Betriebsrat vor. Wie das Bundesarbeitsgericht in seiner Entscheidung vom 11.11.1997 angeregt hat, sollte in einem Arbeitnehmerdatenschutzgesetz die ungeklärte Rechtsfrage der Kontrolle des Betriebsrates durch den betrieblichen Datenschutzbeauftragten geregelt werden. Diese Rechtsfrage ist nach dem vorliegenden Entwurf weiterhin ungeklärt.

Der Referentenentwurf trägt auch nicht Datenverarbeitungen von Beschäftigten im Konzern und Unternehmensverbünden Rechnung. Zunehmend werden unternehmerische Ziele in nationalen und multinationalen Unternehmensverbünden verfolgt, wobei die Konzerne im wachsenden Maße darauf angewiesen sind, Mitarbeiterdaten im Rahmen ihrer Geschäftstätigkeit an konzernangehörige Unternehmen zu transferieren. Vielfach ist die Rechtsgrundlage für die notwendigen Datentransfers nicht ausreichend klar.

Generell ist im Hinblick auf die Gesetzestechnik anzumerken, dass entgegen der üblichen BDSG-Systematik getrennte Regelungen für die Datenerhebung bzw. die anschließende Datenverarbeitung und -nutzung geschaffen werden. Hier wäre es im Sinne der Verständlichkeit der gesetzlichen Regelungen ratsam, einheitliche Lebenssachverhalte jeweils in einer Vorschrift zusammenzuführen und z.B. eine Vorschrift über die Erhebung, Verarbeitung und Nutzung im Bewerbungsverfahren zu schaffen. Dadurch können auch gesetzliche Redundanzen und Verweisungen, die die Verständlichkeit und Lesbarkeit des Gesetzes erheblich erschweren, vermieden werden.

II. Zu den einzelnen Regelungen

Zu §§ 3 Nr. 12, 27 Abs. 3 BDSG-E (Definition Beschäftigtendaten)

Der Begriff der Beschäftigtendaten in § 3 Abs. 12 BDSG-E ist zu weit gefasst und entspricht daher nicht dem Anwendungsbereich der §§ 32 ff. BDSG-E. Hier bedarf es einer Trennung von Beschäftigten- und sonstigen personenbezogenen Mitarbeiterdaten. Auszunehmen aus den Beschäftigtendatenschutzregelungen der §§ 32 ff. BDSG-E sind Daten von Bewerbern und Mitarbeitern, deren Erhebung, Verarbeitung oder Nutzung nicht der Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses dienen sollen. Für diese personenbezogenen Daten gelten – je nach Art ihrer Verarbeitung – die allgemeinen Regelungen des BDSG bzw. das im Arbeitsrecht entwickelte Datenschutzrecht (vgl. Gola/Jaspers, RDV 2009, S. 212). Maßgebend für die Anwendung der §§ 32 ff. BDSG-E ist die beabsichtigte Zweckbestimmung der Daten (vgl. § 27 Abs. 3 BDSG-E).

Hier ist dem Vorschlag Nr. 1 der Berichterstatter der Koalitionsfraktionen zuzustimmen.

Zu §§ 4 Abs. 1, 32l Abs. 5 BDSG-E (Betriebsvereinbarungen)

Ein absolutes Verbot, durch Betriebsvereinbarungen zu Ungunsten der Beschäftigten vom Beschäftigtendatenschutzgesetz abzuweichen, hat nicht zu unterschätzende Konsequenzen in der Praxis. Der Vorteil von Betriebsvereinbarungen als Reglungsinstrument für den Umgang mit Beschäftigtendaten ist regelmäßig, verfahrens- oder anwendungsbezogen passgenaue betriebliche Regelung zu schaffen. Durch die geplante Neuregelung besteht die Gefahr, dass den Betriebspartnern die Motivation genommen werden wird, von dem flexiblen und bewährten Instrument der Betriebsvereinbarung Gebrauch zu machen. Die Betriebspartner hätten nach dem Gesetzentwurf jedenfalls nicht mehr wie bisher die Möglichkeit, die Unbestimmtheiten des BDSG zu beseitigen.

Bereits im Jahr 1986 hat das BAG (RDV 1986, S. 199 = DB 1986, S. 2080) entschieden, dass Betriebsvereinbarungen den Datenschutz der Arbeitnehmer auch abweichend vom Bundesdatenschutzgesetz regeln können. Nach der Entscheidung des BAG sind Betriebsvereinbarungen nicht darauf beschränkt, nur unbestimmte Rechtsbegriffe des BDSG unter Berücksichtigung der betrieblichen Besonderheiten näher zu konkretisieren oder den Arbeitnehmerdatenschutz zu verstärken. Danach stellt das BDSG keinen unabdingbaren Mindeststandard dar. Gleichzeitig hat das Gericht aber festgestellt, dass die Grundsätze über den Persönlichkeitsschutz im Arbeitsverhältnis zu beachten sind (vgl. zuletzt BAG, RDV 2008, S. 238, wonach der Grundsatz der Verhältnismäßigkeit als Prüfungsmaßstab heranzuziehen ist). Der Gestaltungsfreiraum der Parteien der Betriebs- oder Dienstvereinbarung ist nach dem BAG sofern begrenzt, als sie sich an „grundgesetzlichen Wertungen, zwingendem Gesetzesrecht und den sich aus allgemeinen Grundsätzen des Arbeitsrechts ergebenden Beschränkungen“ auszurichten haben. Hierauf aufsetzend sieht der aktuelle Gesetzentwurf nunmehr unabdingbare Vorschriften zum Beschäftigtendatenschutz als zwingendes Gesetzesrecht vor. Ein Abweichen von den neuen Vorschriften zum Beschäftigtendatenschutz zu Ungunsten der Beschäftigten wäre mithin generell ausgeschlossen.

Bedenkt man den sich aus § 75 Abs. 2 BetrVG für Arbeitgeber und Betriebsrat gleichermaßen ergebenden Schutzauftrag, so sind Beispiele, in denen eine an sich nach BDSG unzulässige Personaldatenverarbeitung durch Betriebsvereinbarung gleichwohl gestattet sein könnte, bereits nach bisheriger Rechtslage ohnehin eher selten (vgl. Gola/Schomerus, BDSG, § 4 Rdnr. 10 m.w.N.). Vor diesem Hintergrund könnte man es bei der bisherigen Rechtslage belassen und ergänzend unmittelbar im Gesetzestext darauf hinweisen, dass Betriebs- oder Dienstvereinbarungen die gesetzlichen Regelungen durchaus konkretisieren

oder Alternativen gestalten können, um den jeweiligen betrieblichen Besonderheiten Rechnung zu tragen.

Zumindest sollten jedoch bei bestimmten Datenverarbeitungsverboten Öffnungsklauseln vorgesehen werden. Sinnvoll wäre es z.B. die am Verhältnismäßigkeitsgrundsatz orientierte Rechtsprechung des BAG zur heimlichen Videoüberwachung per Betriebsvereinbarung fortzuführen (vgl. zuletzt BAG, RDV 2008, S. 238). Schließlich gibt es in bestimmten Fällen kein anderes Mittel zur Aufklärung von Straftaten und auch für die betreffenden Mitarbeiter kann die allein vom Arbeitgeber – ohne eine gesetzlich befohlene Involvierung staatlicher Stellen – als ultima ratio veranlasste verdeckte Überwachung ein milderes Mittel sein. Dieses Beispiel verdeutlicht, dass gerade Betriebsvereinbarungen den vom Gesetzgeber angestrebten Interessenausgleich unternehmensspezifisch möglich machen können, ohne die gesetzgeberische Wertung eins zu eins zu übernehmen.

Zu berücksichtigen ist ferner, dass ein absolutes Verbot von zu Ungunsten der Beschäftigten abweichenden Betriebsvereinbarungen nach dem Gesetzentwurf mit dem weitgehenden Wegfall der Einwilligung als Rechtsgrundlage kumuliert, was nicht unbedingt im Sinne von informationeller Selbstbestimmung und unternehmerischer Selbstregulierung wäre. Insbesondere dort, wo dem Beschäftigten insgesamt eine Erweiterung seiner Rechtsposition zugebilligt werden soll (vgl. hierzu auch Art. 29-Gruppe, WP 114, S. 13), muss Raum für Individualeinwilligungen und Kollektivvereinbarungen verbleiben, selbst wenn letztere nicht exakt dem Datenschutzstandard des geplanten BDSG-Unterabschnitts zum Beschäftigtendatenschutz entsprechen. Einer expliziten Klarstellung im Gesetzestext – und nicht nur in der Gesetzesbegründung – bedarf insofern auch die nach Maßgabe einer Betriebsvereinbarung zulässige Kontrolle der privaten Internet- und E-Mail-Nutzung am Arbeitsplatz. Ansonsten bestünde die Gefahr, dass Arbeitgeber vorsichtshalber die Privatnutzung des Internet- und E-Mail-Systems gänzlich untersagen. Eine solche Lösung wäre aber weder praxistauglich noch interessengerecht. Die Notwendigkeit von Rechtsklarheit in diesem äußerst praxisrelevanten Punkt hat auch bereits der Bundesrat in seiner Stellungnahme zu dem Regierungsentwurf betont.

Für eine erweiterten Regelungsrahmen von Betriebsvereinbarungen spricht ferner, dass abweichende Betriebsvereinbarungen - in dem von der Rechtsprechung erlaubten Rahmen - weiterhin bei Verarbeitungen erlaubt sind, die nicht der Zweckbestimmung der §§ 32 ff. BDSG-E dienen, da hier das Verbot des § 32l Abs. 5 BDSG-E nicht gilt.

Schließlich ist darauf hinzuweisen, dass die bisherigen Bemühungen zahlreicher Betriebspartner, über Betriebsvereinbarungen einen sachverhaltsbezogenen Interessenausgleich herzustellen, nachträglich in Frage gestellt würden. Zu prüfen wäre in diesem Zusammenhang auch, inwieweit bereits abgeschlossene Betriebsvereinbarungen Bestandsschutz genießen müssen.

Zu § 32 BDSG-E (Fragerecht des Arbeitgebers)

§ 32 BDSG-E enthält Regelungen für die Datenerhebung vor Begründung des Beschäftigungsverhältnisses. Der Datenumgang im Zusammenhang mit internen Stellenausschreibungen stellt in der Praxis allerdings eine vergleichbare Problemstellung dar. Insofern ist eine Ergänzung der geplanten Regelung zu erwägen.

Die Regelung in § 32 Abs. 2 BDSG-E erweitert mit Blick auf Fragen zu Vermögensverhältnissen, Vorstrafen und laufenden Ermittlungsverfahren den Anwendungsbereich des Allgemeinen Gleichbehandlungsgesetzes (AGG). Bislang richtet sich der Berechtigung der Kenntnis von Vorstrafen oder Angaben über die Vermögensverhältnisse danach, ob sie für die Entscheidung über die Geeignetheit des Bewerbers für den zu besetzenden Arbeitsplatz erforderlich ist (§ 32 Abs. 1 S. 1 BDSG). In Betrachtung des § 32 Abs. 2 E-BDSG-E und des

§ 8 Abs. 1 AGG stellt sich die Frage, ob demnächst noch nach den gleichen Kriterien entschieden werden kann. Abzustellen ist nicht mehr auf die Erforderlichkeit der Information, sondern darauf, dass das Nichtvorliegen der Vorstrafe wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung eine wesentliche und entscheidende berufliche Anforderung darstellt. Die spezielle Regelung in § 32 Abs. 2 E-BDSG macht nur Sinn, wenn die Anforderungen für die Erhebung dieser Daten über die in der Generalklausel des § 32 Abs. 1 E-BDSG vorausgesetzte Erforderlichkeit hinausgehen. Abzustellen wäre darauf, welcher Maßstab an die Begriffe „ wesentlich und entscheidend“ zu stellen ist bzw. wann das Merkmal „unverzichtbare Voraussetzung“ für die zu erbringende Tätigkeit ist. Entscheidend im genannten Sinne ist eine Anforderung erst dann, wenn der Umstand aus objektiver Sicht in einem laufenden Arbeitsverhältnis kündigungsrelevant wäre.
Für die nicht diskriminierungsrelevanten Merkmale der Vermögensverhältnissen, Vorstrafen und laufenden Ermittlungsverfahren ist diese Anforderung im Bewerbungsverfahren zu hoch und in der Regel nicht eindeutig zu beurteilen. Hier sollte die bestehende Rechtlage, die an das Vorliegen eines berechtigten Interesses anknüpft, beibehalten werden. Dem Vorschlag Nr. 3 der Berichterstatter der Koalitionsfraktionen ist insoweit zuzustimmen.

Die Regelung des § 32 Abs. 3 BDSG-E gibt die bestehende Rechtslage wieder, wonach im Bewerbungsverfahren keine Auskunftspflicht im Hinblick auf das Vorliegen einer Schwerbehinderung besteht. Aus Gründen der Rechtsklarheit sollte jedoch ergänzend darauf hingewiesen werden, dass freiwillige Angaben des Bewerbers zur Inanspruchnahme seiner in SGB IX genannten Rechte verwendet werden dürfen.

Problematisch sind auch die gesetzlichen Vorschläge zur Internetrecherche des Arbeitgebers in § 32 Abs. 6 BDSG-E. Hier hat der Regelungsvorschlag zur Recherche in sozialen Netzwerken, der danach differenziert, ob die Darstellung der beruflichen Qualifikation oder lediglich der Kommunikation des Bewerbers dient, erhebliche Abgrenzungsschwierigkeiten zur Folge. Fraglich ist, wie angesichts der Dynamik der technischen Entwicklung diese Widmung nachvollzogen werden kann. Hier ist – entsprechend der Überlegung Nr. 4 der Berichterstatter der Koalitionsfraktionen - eine Differenzierung nach öffentlich zugänglichen Informationen und solchen, die nur einem eingeschränkten Benutzerkreis zur Verfügung gestellt werden, zielführender.

§ 32 Abs. 7 BDSG-E regelt den Grundsatz der Verhältnismäßigkeit bei der Datenerhebung vor Begründung eines Beschäftigungsverhältnisses. Mit Blick auf die Bedeutung des Verhältnismäßigkeitsprinzips empfiehlt sich, diesen Grundsatz in Zusammenhang mit der Regelung zur Erforderlichkeit in § 32a Abs. 1 BDSG-E zu verankern.

Zu § 32a BDSG-E (Ärztliche Untersuchungen / Eignungstests)

Nach § 32l Abs. 1 BDSG-E ist die Einwilligung als Erlaubnistatbestand nur noch in den im Gesetz genannten Fällen zulässig. Ein Beispiel ist die vor einer ärztliche Untersuchung notwendige abzugebende Erklärung (§ 32a Abs. 3 BDSG-E). Regelmäßig fehlt es jedoch an der zur Wirksamkeit der Einwilligung gebotenen Freiwilligkeit des Bewerbers, da er ohne Untersuchung nicht eingestellt würde.

Für ein gesetzliches Einwilligungserfordernis bei gesundheitlichen Untersuchungen bleibt in der Regel auch wenig Raum. Auf Grund von Vorschriften zur Arbeitssicherheit ist der Arbeitgeber zum Teil verpflichtet, vor Einstellung eine Untersuchung zu fordern. Die Teilnahme an der Untersuchung ist insofern notwendige Voraussetzung für die Einstellung. Daneben kann es weitere Fälle geben, in denen die gesundheitliche Tauglichkeit zwingende Voraussetzung für die Erfüllung der vorgesehenen arbeitsvertraglichen Verpflichtungen ist.

Sinn macht das Gebot der Einwilligung nur insofern, dass der Bewerber in dem in § 4a BDSG vorgeschrieben Umfang über Art und Weise und Ziel der Untersuchung aufzuklären ist. Statt der Einwilligung sollte daher diese Informationspflicht vorgesehen werden. Dass im übrigen eine Teilnahme von der Zustimmung des Betroffenen abhängt, ist sachbedingt.

Eine ähnliche Problematik stellt sich bei § 32a Abs. 2 BDSG-E, der die Durchführung von Eignungstests ebenfalls von der Einwilligung des Betroffenen abhängig macht. Auf welche Weise der Arbeitgeber die fachliche und persönliche Eignung eines Bewerbers ermittelt, ist zunächst seinem Ermessen überlassen. Insofern kann er die Entscheidung über die Einstellung auch von der Mitwirkung des Bewerbers an einem Assessment-Center abhängig machen. Auf eine förmliche Einwilligung kommt es insoweit nicht an, da es dem Bewerber freisteht, an dem Assessment-Center teilzunehmen oder nicht. Insoweit bedarf es hinsichtlich der Eignungstests nur einer gesetzlichen Klarstellung, dass diese nach den Regeln der Fachkunde durchzuführen sind.

Bestehen bleiben kann auch die Regelung in § 32a Abs. 2 Satz 5 BDSG-E, wonach bei Vorliegen beruflicher Schweigepflichten nur das Ergebnis des Eignungstests mitzuteilen ist. Jedoch sollte auch hier (vgl. § 32 Abs. 1 S. 5 BDSG-E) gegenüber dem Betroffenen die Pflicht bestehen, dieses Ergebnis zu begründen

Zu § 32b BDSG-E (Datenverarbeitung vor Begründung des Beschäftigungsverhältnisses)

§ 32b Abs. 2 BDSG-E regelt die Datenverarbeitung und -nutzung ohne vorherige Datenerhebung nach § 32a BDSG-E. Systematisch ist aber schwer abzugrenzen, wann eine solche Datenverarbeitung bzw. -nutzung ohne vorausgehende Erhebung vorliegt. Deshalb sollte der Gesetzgeber zum besseren Verständnis die Formulierung aus der Gesetzesbegründung aufgreifen, wo daran angeknüpft wird, dass der Arbeitgeber Beschäftigtendaten ohne Nachfrage vom Beschäftigten erhält bzw. ihm die Daten auf andere Weise zugetragen werden.

Die Regelung des § 32b Abs. 2 S. 2 BDSG-E erlaubt dem Arbeitgeber Initiativbewerbungen zu berücksichtigen. Aber auch freiwillige Mitteilungen in einem laufenden Bewerbungsverfahren werden vom Wortlaut erfasst. Zutreffend steht es einer Einwilligung gleich, wenn der Bewerber bestimmte Information im Rahmen eines Bewerbungsverfahrens ungefragt mitteilt und damit seinen Wunsch zu deren Berücksichtigung bei der Einstellungsentscheidung zum Ausdruck bringt. § 32b Abs. 2 S. 2 E-BDSG erlaubt jedoch dem Arbeitgeber diese Daten auch dann für die Feststellung der Eignung oder zur Entscheidung über die Begründung des Arbeitsverhältnisses heranzuziehen, auch wenn er sie nicht nach §32 oder §32a E-BDSG hätte erheben dürfen. Diese Regelung bedarf einer Einschränkung. Keine Verwendung finden dürfen Daten, durch die Mitbewerber diskriminiert oder indirekt – um gleichzuziehen – gezwungen werden, auf ihre Persönlichkeitsrechte zu verzichten. So wird ein nicht vorbestrafter Bewerber ggf. ein Führungszeugnis bereits von sich aus vorlegen. Eine Frau mag ggf. zu Recht denken, dass ein Arbeitgeber zu ihrer Einstellung motiviert wird, wenn sie ihm ein ärztliches Attest darüber vorliegt, dass sie nicht mehr schwanger werden kann. Würde der Arbeitgeber diese Information verwenden, würde das eine unzulässige Diskriminierung der Bewerber bedeuten, die von ihrem Schweigerecht Gebrauch machen. Zudem darf sich die Verarbeitungsermächtigung nur auf zur Zweck der Einstellung mitgeteilte Daten erstrecken. Daten die der Bewerber z.B. im Zusammenhang mit einer parallel bestehenden Kundenbeziehung, mitgeteilt hat, sind nicht verwertbar.

§ 32b Abs. 3 BDSG-E regelt, dass Bewerberdaten nicht gelöscht werden müssen, wenn der Beschäftigte in ihre weitere Speicherung eingewilligt hat. In der Praxis hat sich als interessengerecht herausgestellt, dass bei einem weiteren Interesse an einem Bewerber dieser

über die weitere Speicherung seiner Daten informiert und ihm ggf. ein Widerspruchsrecht eingeräumt wird.

Die beabsichtigte Neuregelung fordert hingegen eine förmliche Einwilligung nach § 4a BDSG. Dies ist für die Unternehmen mit erheblichem Aufwand verbunden und wird auch vom Bewerber als bürokratischer Formalismus empfunden.

Überdies könnte die beabsichtigte Regelung dahingehend interpretiert werden, dass ohne Einwilligung Bewerberdaten nach Abschluss des Bewerbungsverfahrens unmittelbar zu löschen sind. Eine weitere Speicherung kann jedoch auch auf Grund unternehmenseigener Interessen gerechtfertigt sein (z.B. Speicherung von Bewerberdaten, so lange ggf. noch Ansprüche wegen AGG-Verstößen geltend gemacht werden können). Insoweit empfiehlt sich, die vorgesehene Regelung ersatzlos zu streichen.

Hier sollte an die Rechtsprechung des BAG (NJW 1984 S. 2910) angeknüpft werden, die generell die fortdauernde Speicherung bei Bestehen berechtigter Interessen erlaubt, wodurch auch die Frage einer durch das AGG bedingten dreimonatigen Aufbewahrungsfrist abgedeckt wäre.

Offen ist, ob das Löschungsgebot auch für die in § 32 Abs. 1 S. 1 BDSG-E genannten Daten gilt, so dass, wie es der Praxis entspricht, die Tatsache der Bewerbung auch nach Abschluss des Verfahrens weiter gespeichert werden kann.

Zu § 32d Abs. 3 BDSG-E (Automatisierter Datenabgleich)

Vor dem Hintergrund in der Vergangenheit bekannt gewordener und schon seinerzeit als rechtswidrig einzustufender umfassender Datenabgleiche erscheint diese Regelung sinnvoll, weil sie Ausmaß und Folgen von Datenabgleichen mit Bezug auf Beschäftigtendaten begrenzt.

Auch für den Datenabgleich gilt der allgemeine datenschutzrechtliche Grundsatz, dass Überwachungsmaßnahmen zur Erreichung eines Zwecks erforderlich sein müssen. Nach dem Entwurfstext darf der Arbeitgeber nur zum Zweck der Aufdeckung von Straftaten oder anderer schwerwiegender Pflichtverletzungen einen Datenabgleich durchführen. Auch wenn sich nicht immer bei einem Unternehmen bereits ein konkreter Anlass dafür ergeben hat, wäre es unter dem Gesichtspunkt der Compliance rechtswidrig, erst auf diesen zu warten anstatt auf Grund von Eintrittswahrscheinlichkeiten (z.B. der gesamten Branche) mit diesbezüglichen Risiken zu rechnen. Anlässe für Überwachungsmaßnahmen müssen also nicht konkret eingetreten sein, sondern ergeben sich aus Gefährdungsanalysen. Die näheren Umstände dazu hat der Arbeitgeber nach dem Gesetzentwurf zu dokumentieren. Aus der Gefährdungsanalyse wird sich in der Regel ergeben, dass nicht alle Beschäftigten, sondern nur eine Gruppe von Beschäftigten für das zu untersuchende Risiko in Betracht kommt (z.B. Miles & More nur bei Vielfliegern).

Diese Konkretisierung des Erforderlichkeitsgrundsatzes sollte auch im Gesetzestext des § 32d Abs. 3 Satz 1 BDSG-E aufgenommen werden.

Wäre allerdings nur das Vorliegen eines Anfangsverdachtes der Anlass einer Überwachungsmaßnahme, setzt das voraus, dass mit Bestimmtheit zeitlich vorgelagert etwas Ordnungs- oder Gesetzwidriges, zumindest aber Unplausibles eingetreten ist. Letzteres lässt sich in der Regel nur durch vorher durchgeführte Datenabgleiche feststellen (z.B. Inventurdifferenz), die u.U. nicht erlaubt gewesen wären.

Der weite Begriff der Beschäftigtendaten kann dazu führen, dass jeder Datensatz einer Datei einen Personenbezug zu einem oder mehreren Beschäftigten aufweisen kann, die bei Pflichtverletzungen ggf. zur Verantwortung gezogen werden können. Das darf aber nicht bedeuten, dass eine verantwortliche Stelle als Unternehmen nicht mehr ihre geschäftlich anfallenden Daten prüfen darf, weil sie gleichzeitig als Arbeitgeber „Beschäftigtendaten" abgleicht.

Eine Beschränkung des automatisierten Datenabgleichs erfolgt zudem über die Forderung des Gesetzentwurfs nach datensparsamer Vorgehensweise. Nach dem Abziehen von Datenbeständen ohne Identifikationsmerkmale der Beschäftigten können anonyme Auswertungen produziert werden, und zwar dergestalt, dass einzelne nicht plausible Datenkonstellationen erkannt und gruppiert (z.B. in Fehlerklassen) dargestellt werden, aber keine Zuordnung zu einem Beschäftigten vorgenommen werden kann, weil die Auswertenden keinen Zugriff auf die dazugehörigen Identifikationsmerkmale haben. Erst in einem zweiten Schritt ist zu entscheiden, ob die Auswertung so viele gewichtige unplausible Konstellationen enthält, die eine weitere Aufklärung erforderlich macht. Abhängig von Risikolage kann auch eine pseudonyme Auswertung angezeigt sein, bei der zumindest ein Merkmal (z.B. Satznummer) mitgeliefert wird, welches im Nachhinein die Re-Identifizierung eines Beschäftigten ermöglicht.

Zu § 32e BDSG-E (Datenerhebung ohne Kenntnis des Betroffenen)

§ 32e Abs. 2 Nr. 1 BDSG-E stellt darauf ab, dass ein Verdacht gegen einen Beschäftigten vorliegt, im Beschäftigungsverhältnis eine schwerwiegende Vertragsverletzung begangen zu haben. In der Praxis wird es aber vielfach so sein, dass sich der Verdacht der schwerwiegenden Vertragsverletzung nicht gegen einen einzelnen Beschäftigten, sondern gegen eine Gruppe von Beschäftigten richtet, von denen einzelne oder mehrere die Tat begangen haben können. Insoweit bedarf es einer entsprechenden Anpassung des Gesetzestextes, wonach der Verdachtsmoment auf Beschäftigte (Plural) abstellt. Eine entsprechende Vorbildregelung für den Verdacht hinsichtlich einer Beschäftigtengruppe enthält § 32f Abs. 2 BDSG-E.

Abzustellen ist nach § 32e Nr. 1 BDSG-E auf eine schwerwiegende Vertragsverletzung zu Lasten des Arbeitgebers, die diesen zu einer fristlosen Kündigung aus wichtigem Grund berechtigen würde. Als Voraussetzung für konkrete Maßnahmen zur Durchsetzung der Compliance birgt dies erhebliche Risiken. Die Hürden für eine fristlose Kündigung gem. § 626 BGB sind sehr hoch und in der Regel auch unwägbar. Im Vorfeld ist kaum sicher prognostizierbar, ob sich bestehende Verdachtsmomente bestätigen werden und die aufzudeckende Vertragsverletzung eine außerordentliche Kündigung rechtfertigen wird. Daher sollte allein auf den konkreten Verdacht einer schwerwiegenden Vertragsverletzung abgestellt werden.

Zu § 32f BDSG-E (Offene Videoüberwachung)

§ 32f BDSG-E regelt die Beobachtung nicht öffentlich zugänglicher Betriebsstätten durch Videoüberwachung. Sinnvoll wäre, den Beschäftigtendatenschutz in Zusammenhang mit der Videoüberwachung in § 32f BDSG-E abschließend zu regeln, also auch Arbeitsplätze in öffentlich zugängliche Bereiche einzubeziehen.

Die zugelassenen Kontrollzwecke dienen sekundär auch einer Verhalts- und Leistungskontrolle. Gefahren für das Eigentum oder die Sicherheit am Arbeitsplatz können auch von Beschäftigten ausgehen und können nach ihrer Feststellung zu arbeitsrechtlichen Konsequenzen führen. In einem Satz 2 des Abs. 1 sollte jedoch klargemacht werden, dass die Heranziehung der Überwachungsergebnisse zwecks einer von der Zweckbestimmung losgelösten allgemeinen Leistungskontrolle unzulässig ist.

Zu § 32g BDSG-E (Ortungssysteme)

Die in § 32g Abs. BDSG-E geforderte unverzügliche Löschung ist zu restriktiv, da die Ortungsdaten ggf. auch für Dokumentationen und Rechtsstreitigkeiten relevant sein können. Ein Verweis auf die entsprechende Erforderlichkeit wäre besser.

Zu § 32h BDSG-E (Biometrische Verfahren)

Lichtbilder sind nicht regelmäßig biometrische Verfahren im Sinne der Vorschrift. Insoweit macht es Sinn, die Verwendung von Lichtbildern von Beschäftigten aus der Vorschrift des § 32h BDSG-E herauszulösen und allgemein zu regeln.

Zu § 32i BDSG-E (Nutzung von Telekommunikationsdiensten)

Die Regelungen über die Nutzung von Telekommunikationsdiensten differenzieren zwischen der Erhebung von Inhalten und Verkehrsdaten während der Kommunikation und der in Absatz 4 geregelten nachgelagerten Kontrolle. Die Regelungen beziehen sich dabei nur auf die dienstliche Kommunikation. Lediglich in § 32i Abs. 4 Satz 2 wird der Zugriff auf Daten der privaten Kommunikation zum Zwecke des ordnungsgemäßen Dienst- und Geschäftsbetriebs geregelt. Hier sollte aus Gründen der Rechtssicherheit auf „erkennbar“ private Daten abgestellt werden.

Da in der Praxis sehr häufig auch eine zumindest geduldete Privatnutzung der Telekommunikationsanlagen des Arbeitgebers anzutreffen ist, sollte eine Öffnung für eingeschränkte Kontrollmöglichkeiten durch den Arbeitgeber auf Grundlage einer Einwilligung ggf. nach den Vorgaben einer Betriebsvereinbarung vorgesehen werden. Hierzu bedarf es einer Öffnungsklausel für Betriebsvereinbarungen in § 32l Abs. 5 (siehe vorstehend) und einer Erweiterung der Tatbestände für eine erlaubte Einwilligung im beschäftiungsverhältnis.

Zu § 32j BDSG-E (Unterrichtungspflichten bei Datenpannen)

§ 32j BDSG-E fordert bei Datenverlusten immer die Unterrichtung des Beschäftigten und zwar unabhängig davon, ob der Datenverlust zu einer Beeinträchtigung der Rechte oder schutzwürdigen Interessen führt. Ein Bedürfnis für eine solche Regelung ist nicht ersichtlich. Dem Schutzbedürfnis der Betroffenen wird durch § 42a BDSG hinreichend Rechnung getragen. § 32j BDSG-E sollte daher ersatzlos gestrichen werden.

Zu § 32l BDSG-E (Einwilligung als Erlaubnistatbestand)

§ 32l BDSG-E verbietet die Einwilligung als Erlaubnistatbestand für den Umgang mit Beschäftigtendaten, sofern dies nicht ausdrücklich vorgesehen ist.

Hier ist zunächst vom Grundsatz her darauf hinzuweisen, dass die Einwilligung in Art. 7 a) der EG-Datenschutzrichtlinie (RL95/46/EG) einen eigenständigen Erlaubnistatbestand darstellt, der zwar unter dem Vorbehalt der Freiwilligkeit steht, nicht jedoch für das Beschäftigungsverhältnis eingeschränkt ist.

Die Regelungsentwurf verkennt, dass auch im Arbeitsverhältnis Einwilligungen vielfach notwendige Rechtsgrundlage sind. Die im Gesetz in Bezug genommenen Erlaubnistatbestände fehlen für solche Beschäftigungsverhältnisse, die nur mit einer Einwilligung des Bewerbers bzw. Arbeitnehmers durchführbar sind (z.B. Einwilligung in ein Prüfrecht vor Ort bei Telearbeit; Einwilligung in die Sicherheitsüberprüfung, Einwilligung in eine eingeschränkte Kontrolle der Privatnutzung von Telekommunikationsdiensten).

Zudem kommt es insbesondere in Konzernen unternehmensübergreifend zur Arbeit in Matrixstrukturen. Weiterhin ist Bestandteil der Personalarbeit der Aufbau von konzernweit zugänglichen Datenbanken mit Kenntnissen und Fähigkeiten (Skills) von Mitarbeitern. In Ermangelung einer anderen Rechtsgrundlage erfolgt die hierfür notwendige Datenverarbeitung auf Grundlage einer Einwilligung, deren Freiwilligkeit unproblematisch ist. Deshalb sollte von einem generellen Verzicht auf die Einwilligung als Erlaubnistatbestand für die Arbeit mit Beschäftigtendaten abgesehen werden. Die Einholung einer Einwilligung könnte jedoch klarstellend an die Voraussetzung geknüpft werden, dass der Arbeitgeber an ihrer Abgabe ein berechtigtes Interesse hat.

III. Evidente Regelungslücken

Weitergabe von Mitarbeiterdaten im Unternehmensverbund

Regelungsbedürftig ist die Weitergabe von Mitarbeiterdaten im Unternehmensverbund. Angesichts der Tatsache, dass weder die EU-Datenschutzrichtlinie noch das Bundesdatenschutzgesetz ein „Konzernprivileg“ kennen, ist vielfach ein notwendiger Austausch von Mitarbeiterdaten zwischen verbundenen Unternehmen datenschutzrechtlich nicht unproblematisch. Hier sollten für Tatbestände, die betriebswirtschaftlich sinnvoll und für den Datenschutz der Mitarbeiter regelmäßig unschädlich sind, wie der Betrieb von Shared-Service-Centern, die zentrale Führungskräftebetreuung oder die konzernweite Steuerung der IT-Infrastruktur, gesetzliche Zulässigkeitstatbestände geschaffen werden.

Ein Beispiel für eine Konzernklausel bietet der Gesetzentwurf von BÜNDNIS90/DIE GRÜNEN (BT-Drucksache 17/4853) in § 7 Abs. 2, der einen Zulässigkeitstatbestand für die Übermittlung von Beschäftigtendaten innerhalb von Konzernverbünden und eine Öffnungsklausel für entsprechende Betriebsvereinbarungen schafft. Die Regelung eines Konzernprivilegs kann unter den in diesem Gesetzentwurf genannten Vorrausetzungen als Ausgestaltung der Datenverarbeitung auf Grundlage einer Interessenabwägung erfolgen, die Art. 7 f) der EG-Datenschutzrichtlinie (RL95/46/EG) als generellen Erlaubnistatbestand vorsieht.

Unbeschadet von einer Konzernklausel bleibt das Erfordernis des angemessenen Schutzniveaus bei den konzernangehörigen Unternehmen gemäß § 4b Abs. 2 S. 2 BDSG.

Datenschutzkontrolle beim Betriebsrat

Die Kontrolle der personenbezogenen Datenverarbeitung beim Betriebsrat ist seit einer Entscheidung des Bundesarbeitsgerichtes aus dem Jahre 1997 gesetzlich ungeregelt. Das Bundesarbeitsgericht hatte seinerzeit entschieden, dass die Datenverarbeitung des Betriebsrates nicht durch den betrieblichen Datenschutzbeauftragten kontrolliert werden dürfe. Seitdem besteht im Unternehmen ein quasi kontrollfreier Raum. Die Gesetzeslücke führt dazu, dass zwar das Unternehmen gegenüber dem Betroffenen als verantwortliche Stelle zur Gewährleistung des Datenschutzes verpflichtet ist, diesen jedoch gegenüber dem Betriebsrat nicht durchsetzen kann.

Die vom BAG für seine Entscheidung angeführte mangelnde Unabhängigkeit des betrieblichen Datenschutzbeauftragten hat der Gesetzgeber durch den besonderen Kündigungsschutz in § 4f Abs. 3 Satz 4 BDSG teilweise korrigiert. Einer Erweiterung bedarf die Verschwiegenheitsverpflichtung des Datenschutzbeauftragten nach § 4f Abs. 4 BDSG, die sich bisher nur auf die Identität des Betroffen bezieht. Diese müsste um die Beratung und Kontrolle des Betriebsrates erweitert werden.

Bonn, den 17. Mai 2011