

**Deutscher Bundestag**  
Innenausschuss

Ausschussdrucksache  
17(4)252 G

**DVD**

Deutsche Vereinigung  
für Datenschutz e. V.

Rheingasse 8 - 10  
53113 Bonn

Telefon: 0228/22 24 98  
Telefax: 0228/24 38 470

dvd@datenschutzverein.de  
www.datenschutzverein.de

Berlin/Bonn, den 17.05.2011

Verfasser : Sönke Hilbrans, Berlin  
Rechtsanwalt und Fachanwalt für Strafrecht

## **Öffentliche Anhörung im**

### **Innenausschuss des Deutschen Bundestages**

#### **zum Gesetzentwurf der Bundesregierung**

#### ***Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes***

**BT-Drucksache 17/4230 u. a.**

**am 23.05.2011**

### **Schriftliche Stellungnahme**

Die folgenden Ausführungen befassen sich im Wesentlichen mit dem Gesetzentwurf der Bundesregierung für ein Gesetz zur Regelung des Beschäftigtendatenschutzes (BT-Drs. 17/4230 vom 15.12.2010) und dem Arbeitspapier der Berichterstatter der Koalitionsfraktionen vom 10.05.2011. Diese Auswahl erfolgt allein im Hinblick auf den Verlauf des Gesetzgebungsverfahrens und möge nicht als Ablehnung der Gesetzentwürfe BT-Drs. 17/69 und BT-Drs. 17/4853 verstanden werden.

## I. Allgemeines

Der Gesetzentwurf der Bundesregierung verfolgt das Ziel, praxisgerechte Regelungen für die Verarbeitung von Beschäftigtendaten zu schaffen, die Datenverarbeitung auf das zu Zwecken des Beschäftigungsverhältnisses Erforderliche zu beschränken, Beschäftigte wirksam vor Bespitzelungen am Arbeitsplatz zu schützen und gleichzeitig Arbeitgebern verlässliche Grundlagen für die Erfüllung von Compliance-Anforderungen und den Kampf gegen Korruption an die Hand zu geben. Diese Ziele verfehlt der Gesetzentwurf, weil

- er keine klare gesetzliche Differenzierung zwischen den mit personenbezogenen Daten von Beschäftigten verfolgten Zwecken trifft,
- daher informationelle Gewaltenteilung in Betrieb und Unternehmen nicht geschaffen wird,
- schutzwürdige Interessen von Beschäftigten im Wesentlichen mittels allgemeiner Verhältnismäßigkeitsabwägungen oder in der Praxis nicht abgrenzungsscharfer Generalklauseln geschützt werden sollen,
- effektive Verfahrensregelungen und Sanktionen zum Schutz der Beschäftigten vor Datenschutzverstößen (etwa Zustimmungsvorbehalte für den betrieblichen Datenschutzbeauftragten, Verwertungsverbote) nicht geschaffen werden.

Dagegen zielt der vorgelegte Entwurf auf Vorschriften, welche eine Überwachung und Ausforschung von Beschäftigten rechtlich absichern würden, die nach geltendem Recht unzulässig wären. In der Sache würden damit Datenschutzverstöße, welche noch in jüngster Zeit als Skandale gewertet wurden, legalisiert. Demgegenüber werden fortschrittliche Initiativen, welche Beschäftigte vor sachlich nicht angezeigten Eingriffen in ihre Persönlichkeitsrechte wirksam schützen könnten, nicht aufgegriffen. Auch hätte sich eine Gestaltung des Beschäftigtendatenschutzes in einem besonderen, von dem Bundesdatenschutzgesetz geschiedenen Gesetz empfohlen.

## **II. Zu den Regelungen des Entwurfs der Bundesregierung (BT-Drs. 17/4230) im Einzelnen:**

### **1. § 32 BDSG-E: Datenerhebung von Bewerbern**

**a.) (§ 32 Abs. 2 BDSG-E):** Die Anpassung der Erhebung sensibler Daten von Bewerbern an die Voraussetzungen des § 8 Abs. 1 AGG ist – anders als im Arbeitspapier der Berichterstatter der Koalitionsfraktionen vom 10.05.2011 befürchtet – nicht mit einer Ausweitung des Anwendungsbereichs des Allgemeinen Gleichbehandlungsgesetzes verbunden und in der Sache zu begrüßen. Es empfiehlt sich allerdings, im Hinblick auf den bestehenden und auch von der EU- Datenschutzrichtlinie geforderten gesetzlichen Schutz besonderer Arten personenbezogener Daten (§ 3 Abs. 9, § 28 Abs. 6 – 9 BDSG u. a.), die verschiedenen Schutzsysteme für besonders zu schützende Daten aneinander anzupassen. Im Hinblick darauf und auf die etablierte Rechtsprechung deutscher und europäischer Gerichte sollte eine Erhebung von Bewerberdaten über eine Gewerkschaftszugehörigkeit und Schwangerschaft generell verboten werden.

**b.) (§ 32 Abs. 6 S. 2 und 3 BDSG-E):** Der Zugriff von Arbeitgebern auf veröffentlichte Informationen bedarf einer Regulierung. Veröffentlichungen können von den Betroffenen ebenso wenig effektiv kontrolliert werden wie Einträge in kommerziellen Datenbanken (etwa von Auskunftsteilen). Es liegt auch auf der Hand, dass von den Betroffenen in jüngerer Zeit selbst veröffentlichte Daten nicht den gleichen Schutzbedarf auslösen wie Daten, die schon lange zurückliegende Sachverhalte abbilden oder von Dritten in Unkenntnis oder gegen den Willen der Betroffenen erhoben und veröffentlicht werden. Das von Arbeitgeberseite regelmäßig wiederholten Bedürfnis nach der Erhebung und Verarbeitung veröffentlichter Daten wird von dem Gesetzentwurf nur unzureichend kanalisiert. Die in Abs. 6 S. 2 und 3 abgebildeten Arbeitgeberinteressen fallen in ihrer Wertigkeit erheblich hinter denen zurück, die § 4 Abs. 2 S. 2 BDSG für die Abweichung von dem Prinzip der offenen Direkterhebung im Allgemeinen voraussetzt. Für diese Privilegierung von Arbeitgebern gegenüber anderen Datenverarbeitern ist kein zwingender Grund ersichtlich. Auch sind sowohl die allgemeine Zugänglichkeit von Daten (Abs. 6 S. 2) als auch die Zweckbestimmung von sozialen

Netzwerken (Abs. 6 S. 3 2. Halbsatz) im Einzelfall nicht treffsicher zu bestimmen. So ist die Allgemeinzugänglichkeit von Daten bspw. in bestimmten Datenbanken in anderem datenschutzrechtlichen Kontext umstritten. Eine Hinweispflicht für den Arbeitgeber (Abs. 6 S. 2) zieht keinen effektiven verfahrensrechtlichen Schutz nach sich und wirft auch die Frage auf, ob die Informationspflicht nach Art. 11 EU-Datenschutzrichtlinie hinreichend umgesetzt wurde.

Der Entwurf ist daher zu überarbeiten mit dem Ziel, die Umgehung des gesetzlichen Primats der offenen Direkterhebung (§ 4 Abs. 2 S. 1 BDSG) auf Fälle zu beschränken, in denen Zweifel an der Vereinbarkeit der Erhebung mit dem allgemeinen Persönlichkeitsrecht der Bewerber nicht bestehen. Dies können Fälle nach Abs. 6 S. 3 1. Halbsatz sein.

**c.) (§ 32 Abs. 6 BDSG-E):** Der Gesetzentwurf untertrifft das erforderliche Schutzniveau auch, soweit Bewerberdaten bei sonstigen Dritten erhoben werden dürfen. Denn gerade bei sonstigen Dritten – etwa früheren Arbeitgebern, Auskunftsteilen usw. – gespeicherte personenbezogene Daten sind regelmäßig einer effektiven Kontrolle durch die Betroffenen entzogen. Auch wenn die besonderen Formbestimmungen für die datenschutzrechtliche Einwilligung (§ 4a Abs. 1 BDSG) eingehalten werden, ist eine freiwillige Einwilligung in die Erhebung von Bewerberdaten bei Dritten praktisch nicht vorstellbar. Der Streit um ein bestehendes Fragerecht wird auf diesem Wege von dem Gesetzgeber allenfalls auf den Streit um eine bestehende Freiwilligkeit verlagert, ohne dass Rechtssicherheit geschaffen würde. Da es Arbeitgebern in den Fällen, in denen ein dringendes Informationsbedürfnis besteht, regelmäßig frei steht, von den Betroffenen selbst die erforderlichen Daten zu erheben – und sich etwa Zeugnisse vorlegen zu lassen – bedarf es einer für die Persönlichkeitsrechte der Betroffenen höchst gefährlichen Regelungen wie § 32 Abs. 6 S. 4 BDSG-E nicht.

## 2. § 32a BDSG-E: Ärztliche Untersuchungen und Eignungstests

a.) (§ 32a Abs. 1 BDSG-E): Die verkürzende Anlehnung an § 8 Abs. 1 AGG bei der Regelung betriebsärztlicher Einstellungsuntersuchungen geht insoweit fehl, als auch die gesundheitlichen Voraussetzungen im Hinblick auf die Bedingungen der Ausübung einer Tätigkeit untersucht werden können sollen. Denn soweit arbeitsmedizinische Voraussetzungen am Arbeitsplatz eingehalten werden, bedarf es eines spezifischen Abstellens auf die Bedingungen der Ausübung einer Tätigkeit nicht und reicht es aus, die Tauglichkeit des Bewerbers im Hinblick auf die objektiven allgemeinen gesundheitlichen Voraussetzungen der Tätigkeit zu prüfen.

b.) (§ 32a Abs. 2 BDSG-E): Der Entwurfstext will die Prüfung der Eignung eines Bewerbers für eine auszuübende Tätigkeit in jedweder Hinsicht eröffnen. Um eingriffsintensive, im Ergebnis sachlich nicht mehr gerechtfertigte Eignungstests insbesondere jenseits bestehender anerkannter wissenschaftlicher Methoden zu unterbinden, ist die Durchführung solcher Tests auf die Ermittlung einer objektiven fachlichen Eignung zu beschränken. Eine Einwilligung nach § 32a Abs. 2 S. 4 BDSG-E kann, da der Bewerber faktisch jenseits des Abbruchs des Bewerbungsverfahrens keine Wahlfreiheit bei der Teilnahme an Eignungstests hat, die persönlichkeitsrechtlichen Mängel des Entwurfs nicht heilen.

## 3. § 32b BDSG-E: Verarbeitung und Nutzung von Bewerberdaten

Die Löschungspflicht nach § 32b Abs. 3 BDSG-E ist zu schärfen: Der nach der Gesetzesbegründung nur deklaratorisch verstandene Verweis auf § 35 Abs. 2 S. 2 BDSG in § 32b Abs. 3 BDSG-E kann entfallen. Auf diese Weise werden angesichts des differenzierten normativen Programms von § 35 Abs. 2 S. 2 BDSG Auslegungsschwierigkeiten vermieden.

Dagegen besteht Anlass, in § 32b Abs. 3 BDSG-E den Hinweis aufzunehmen, dass eine Einwilligung in die weitere Speicherung von Bewerberdaten nach Abschluss des Bewerbungsverfahrens lediglich für Zwecke nach § 32b Abs. 2 S. 1 Nr. 1 BDSG-E und nur für einen von dem Bewerber zu bestimmenden Zeitraum Geltung haben soll.

#### **4. § 32c BDSG-E: Datenerhebung im Beschäftigungsverhältnis**

**a.) Allgemeines:** Auch die dem Innenausschuss nunmehr vorliegende Entwurfsfassung lässt Zweifel an dem Zweckprogramm der Verarbeitung und Nutzung von Beschäftigtendaten aufkommen: Zwar beschreiben § 32c Abs. 1 S. 2 Nr. 1 und 2 BDSG-E noch definierte Zwecke, so dass eine Datenerhebungsbefugnis auf diese Zwecke bezogen und beschränkt verstanden werden kann. Demgegenüber ist jede generelle Erlaubnis zur Erhebung von Beschäftigtendaten zwecks Wahrnehmung allgemein bestehender Rechte des Arbeitgebers einschließlich der Verhaltens- oder Leistungskontrolle (§ 32 Abs. 1 S. 2 Nr. 3 BDSG-E) in sich nicht differenziert. Da auch auf der Verwendungsebene (§ 32d Abs. 1 Nr. 2 BDSG-E) keinerlei Differenzierung erfolgt, handelt es sich um eine Erhebungsgeneralklausel ohne normatives Eigengewicht. In der Sache dürften, soweit das Direktionsrecht des Arbeitgebers reicht, zu beliebigen Zwecken mit Bezug zur Beschäftigung Daten erhoben werden. Damit bekennt sich § 32c Abs. 1 S. 2 Nr. 3 BDSG-E zu einem gleichsam Globalzweck von Beschäftigtendaten im Arbeitsverhältnis. Diese Zweckbeschreibung untertrifft die verfassungsrechtlichen Anforderungen an eine an den Grundsätzen der Verhältnismäßigkeit, Datensparsamkeit und informationellen Gewaltenteilung orientierten Datenschutzgesetzgebung.

#### **b.) (§ 32c Abs. 1 S. 3 BDSG-E): Datenerhebung unter Umgehung des Betroffenen**

Die Ausführungen zu § 32 Abs. 6 S. 4 BDSG-E gelten entsprechend. Es sollte bei der allgemeinen Regel nach § 4 Abs. 2 BDSG bleiben.

**c.) (§ 32c Abs. 3 BDSG-E):** Ein Recht des Arbeitgebers, ärztliche Untersuchungen und Eignungstests im Hinblick auf eine (von dem Arbeitgeber) beabsichtigte Versetzung oder Umsetzung zu verlangen, geht zu weit. Ein praktisches Bedürfnis nach einer Erweiterung der bisherigen gesetzlichen Regeln des Arbeitsschutzes durch § 32c Abs. 3 Nr. 1 BDSG-E ist nicht ersichtlich. Die Möglichkeit, schon durch von dem Arbeitgeber bloß kund getane Absicht ein intrusives Datenerhebungsprogramm auszulösen (Abs. 3 Nr. 2), eröffnet erhebliche Missbrauchsmöglichkeiten. Eine Selektion von Beschäftigten nach Gesundheit oder – fachlichen wie unsachlichen - Eignungskriterien muss grundsätzlich unterbunden werden, zumal die arbeitsrechtliche Praxis ohne eine solche Regelung auskommt. Arbeitnehmern steht es ggf. frei, sich unternehmensintern auf eine andere Stellen zu bewerben und dadurch die Rechtsfolgen von § 32a ff BDSG-E auszulösen. § 32c Abs. 4 BDSG kompensiert diesen Mangel nicht, weil das Zweckprogramm von § 32c Abs. 3 BDSG-E keine Einschränkung erfährt.

## **5. Datenverarbeitung und –nutzung im Beschäftigungsverhältnis**

**a.) (§ 32d Abs. 1 und Abs. 2 BDSG-E):** Der Entwurf bekennt sich mit § 32d Abs. 1 Nr. 1 und 2 BDSG-E, wie bereits mit § 32c Abs. 1 S. 2 Nr. 3 BDSG-E, zu einem gleichsam Globalzweck von Beschäftigtendaten im Arbeitsverhältnis (vergl. auch die insoweit schonungslos offene Entwurfsbegründung zu § 32d Abs. 4 BDSG-E). Damit relativiert der Entwurf mit Wirkung für alle im Beschäftigungsverhältnis erhobenen Daten den Grundsatz der Zweckbindung und klaren Zweckbestimmung jeder Datenverarbeitung. Auch und gerade für die Verarbeitung von im Verlauf des Arbeitsprozesses, bei der Erbringung der Arbeitsleistung oder sonst im Betrieb angefallene Beschäftigtendaten (Abs. 2) ist eine Beschränkung der Datenverarbeitung auf den Zweck, zu dem die Daten generiert wurden, dringend angezeigt.

Da der Gesetzentwurf damit – auch entgegen Ansätzen in der arbeitsgerichtlichen Rechtsprechung zum allgemeinen Persönlichkeitsrecht – innerhalb einer verantwortlichen Stelle (§ 3 Abs. 7 BDSG) keine Nutzungsbeschränkungen vorsieht, fehlt es an tragfähigen Ansätzen für informationelle Gewaltenteilung im Unternehmen. Eine wesentliche

verfassungsrechtliche Forderung an jede verfassungskonforme Datenverarbeitung, nämlich die auch organisatorische Differenzierung der Zweckverfolgung, wird sehenden Auges verfehlt.

Die Erinnerung an den Grundsatz der Verhältnismäßigkeit (§ 32d Abs. 1 Nr. 3 BDSG-E) fügt dem normativen Programm des Entwurfs nichts hinzu, sondern wiederholt nur einen für alle Eingriffe in das allgemeine Persönlichkeitsrecht geltende Selbstverständlichkeit.

Da der Entwurf auf eine umfassende Regelung zielt, sollte in Absatz 1 klargestellt werden, dass die allgemeinen Regelungen des Bundesdatenschutzgesetzes (etwa nach § 28 Abs. 1 BDSG) keine Anwendung finden, mithin Beschäftigtendaten nur unter den Voraussetzungen von § 32d BDSG-E verarbeitet oder genutzt werden dürfen.

**b.) (§ 32d Abs. 3 BDSG-E):** Die Vorschrift legalisiert die unternehmensinterne Rasterfahndung, die in der Vergangenheit den Kern viel beachteter Datenschutzskandale ausgemacht hat und im öffentlichen Bereich bzw. zur Strafverfolgung nur unter qualifizierten Voraussetzungen und mit Zustimmung eines Richters zulässig wäre. Das gesetzliche Programm der Rasterfahndung legt mit der ausdrücklichen Erlaubnis einer Repersonalisierung (§ 32d Abs. 3 S. 2 BDSG-E) offen, dass allenfalls mit pseudonymisierten, weiterhin aber im Rechtssinne personenbezogenen Daten gearbeitet werden soll (vergl. nur § 3 Abs. 1 BDSG). Auch die Formel für die nachträgliche Unterrichtung der Beschäftigten (§ 32d Abs. 3 S. 4 BDSG-E) greift zu kurz. Zwar lehnt sie sich an das Recht der Strafverfolgung und Gefahrenabwehr an, jedoch hat gerade diese Form in der Vergangenheit eine verbreitete Auslegung dergestalt erfahren, dass bereits das Bekanntwerden der Anwendung einer bestimmten Methode den Zweck der Erhebung gefährden sollte. Da Maßnahmen nach § 32d Abs. 3 BDSG-E der Aufdeckung von zurückliegenden Pflichtverletzungen und nicht der Gefahrenabwehr dienen sollen, wäre im Falle ihrer gesetzlichen Legalisierung bereits eine Unterrichtung der Beschäftigten nach Ende der Maßnahme und/oder bei Repersonalisierung der verwendeten Daten möglich und auch angezeigt.

Auf dieses skandalumwitterte Instrument sollte der Gesetzgeber aber im Ergebnis verzichten. Diejenigen Unternehmen, welche von solchen Maßnahmen noch profitieren wollen, sollten das Verantwortungsbewusstsein aufbringen, im Wege der Betriebsvereinbarung die Rechtsgrundlagen für unabweisbare betriebliche Sicherheitsanwendungen zu schaffen.

**c.) (§ 32d Abs. 4 BDSG-E):** Datenübermittlung an Dritte, welche nach dem Zusammenhang der Vorschrift offenbar nach den schon für die Verarbeitung und Nutzung durch den Arbeitgeber zu weit geratenen § 32d Abs. 1 und 2 BDSG-E zulässig sein soll, sind von Gesetzes wegen an strengste Voraussetzungen zu binden. Die auch von der Entwurfsbegründung angenommene Freiheit des Arbeitgebers, zu jedem mit dem Beschäftigungsverhältnis verbundenen Zweck Beschäftigtendaten an Dritte übermitteln zu dürfen (vergl. Begründung zu Abs. 4 und oben zu a.)), verfehlt bei Weitem den gebotenen Schutz des Persönlichkeitsrechts der Betroffenen.

Der Entwurf verzichtet damit nicht nur auf ein Mindestmaß an Übermittlungsschutz für die Beschäftigten. Es fehlt auch an elementaren verfahrensrechtlichen Sicherungen: Lediglich die Mitteilung an dem Empfänger über den Zweck übermittelter Daten reicht dazu bei Weitem nicht aus, zumal ein trennscharfer legitimer Übermittlungszweck gerade in dem gesetzlichen Zweckprogramm nach § 32d Abs. 1 BDSG nicht identifiziert werden kann. Ferner fehlt es an der obligatorischen Kennzeichnung übermittelter Daten als Beschäftigtendaten, ohne welche der Übermittlungsempfänger die besondere Schutzwürdigkeit dieser Daten gar nicht verfahrenstechnisch absichern könnte. Weitere verfahrensrechtliche Sicherungen, wie etwa eine obligatorischen Benachrichtigung der Betroffenen, fehlen ebenfalls.

Der Entwurf ist daher durch ein enges, gesetzlich bestimmtes Zweckprogramm der Übermittlung von Beschäftigtendaten zu ergänzen.

## 6. § 32e BDSG-E: Heimliche Datenerhebung zur Bekämpfung von Straftaten u. a.

**a.) (§ 32 Abs. 1 S. 2 BDSG-E):** Mit § 32 Abs. 1 S. 2 BDSG in der geltenden Fassung hat der Gesetzgeber in Einklang mit der etablierten arbeitsrechtlichen Rechtsprechung eine eng gefasste Vorschrift geschaffen, welche heimliche Datenerhebungen in notwehrähnlicher Lage ausnahmsweise rechtfertigt. Dieser Regelungsgedanke wird nunmehr über den Verdacht von Straftaten hinaus erweitert auf sonstige arbeitsvertragsrechtliche Pflichtverletzungen, die zu einer Kündigung aus wichtigem Grund (§ 626 BGB) führen könnten. Damit bekennt sich der Gesetzentwurf ausdrücklich zur Anwendung heimlicher Mittel auch in denjenigen Fällen, in denen zwar kein nennenswerter Schaden für den Arbeitgeber oder Dritte eingetreten ist bzw. droht, gleichwohl aber eine Pflichtverletzung eine Kündigung rechtfertigt (sog. Maultaschenkündigung). Wenn sich aber die Bedeutung einer potentiellen Verfehlung aus arbeitsvertragsrechtlichen Wertungen ableitet, emanzipiert sich das Gesetz von dem Rechtsgüterschutz als Eingriffsrechtfertigung und geht die auch zusätzliche Verhältnismäßigkeitsschranke nach § 32e Abs. 3 S. 1 BDSG-E ins Leere. Der Gesetzgeber ist, wenn er nicht eine potentiell verfassungswidrige Blankettermächtigung für eingriffsintensive heimliche Datenerhebungen schaffen will, aufgefordert, das Zweckprogramm nach § 32e Abs. 2 Nr. 1 BDSG-E auf Straftaten oder sonstige Pflichtverletzungen zu beschränken, welche einen erheblichen Schaden für den Arbeitgeber oder Dritte nach sich ziehen (können). Arbeitsvertragsrechtlich zulässige Kündigungen werden dadurch nicht ausgeschlossen, können aber nicht ohne Weiteres mittels hochgradig eingriffsintensiver Ausnahmeinstrumente herbeigeführt werden.

Die Verfolgung von Zielen einer betrieblichen inneren Sicherheit durch die Arbeitgeber selbst bedarf im Übrigen nicht der umfangreiche Legalisierung, die ihr der Entwurf zubilligt: Es steht verantwortungsbewussten Arbeitgebern auch nach dem Entwurf frei, durch Betriebsvereinbarung zu einer auf die Spezifika des jeweiligen Unternehmens abgestimmten Feinabstimmung von unternehmerischen Bedürfnissen und den Persönlichkeitsrechten der Beschäftigten zu kommen. Die von der Gesetzesbegründung als Anwendungsbeispiel angesprochene Aufdeckung von Korruptionsnetzwerken unter maßgeblicher Beteiligung von Unternehmen außerhalb des Arbeitgebers ist nicht etwa ein plastisches Beispiel dafür, dass extensive Datenerhebungen unter Einschluss von Dritten zwingend erforderlich sind.

Vielmehr illustrieren derartige Fallkonstellationen, dass Arbeitgeber nur durch frühzeitiges Einschalten der Polizei in der Lage sind, forensisch verwertbare Beweise zu erheben und zu sichern. Es ist daran zu erinnern, dass es im Rechtsstaat die Justiz ist, welche zuständig ist für die Verfolgung von Straftaten und ihre Sanktionierung. Nur so, und nicht durch eine Legalisierung unternehmerischer Eigeninitiative, können die Voraussetzungen für ein rechtsstaatliches Verfahren zum Schutz der Belange der Unternehmen geschaffen und gesichert werden.

**b.) (§ 32e Abs. 4 BDSG-E):** Das Erhebungsmethodenarsenal bei heimlichen Ermittlungen nach § 32e Abs. 2 BDSG-E wird von § 32e Abs. 4 BDSG-E nur ansatzweise beschränkt. Offenbar sollen weiterhin Privatdetektive, Observationen innerhalb und außerhalb von Betriebsgeländen, beliebige Anfragen bei Dritten und die Nutzung aller im Unternehmen angefallenen personenbezogenen Daten zulässig sein. Nicht geregelt ist ferner die Folge von Übertretungen der in sich schon vagen Einschränkungen nach § 32e Abs. 4 S. 1 BDSG. Der Gesetzentwurf kann dies nur ausgleichen, indem er sich zu Verwendungs- und Verwertungsverboten für im Widerspruch zur gesetzlichen Regel erhobene Daten bekennt.

**c.) (Verfahrensrechtliche Absicherungen, § 32e Abs. 3 S. 2 – 4, Abs. 5 – 7 BDSG-E):** Die verfahrensrechtlichen und materiell-erhebungsrechtlichen Absicherungen nach § 32e Abs. 3 S. 2 – 4, Abs. 5 – 7 BDSG-E sind im Grundsatz zustimmungswürdig. Sie greifen aber angesichts der Eingriffstiefe, welche die geregelten Maßnahmen entfalten könnten, zu kurz: So fehlt es weiterhin an einer Vorschrift, welche ausdrücklich verbietet, heimliche Datenerhebung gegen andere als die verdächtigen Beschäftigten zu richten und mehr als unvermeidbar Daten über Dritte zu erheben, welche nicht Beschuldigte sind.

Während staatlicher Rechtsgüterschutz und Straftatenbekämpfung in ein dichtes Geflecht rechtsstaatlicher Kontrolle und Verwendungsregelungen eingebunden sind, verzichtet der Entwurf auf verfahrensrechtliche Sicherungen unter Einschaltung unabhängiger Kontrollorgane. Die nach der Entwurfsbegründung nur als deklaratorische Erinnerung gedachte Anspielung auf die Vorabkontrolle nach § 4d Abs. 5 BDSG (§ 32e Abs. 5 S. 4 BDSG-E) kompensiert diesen Mangel nicht. Denn sie schöpft das Potential der

Vorabkontrolle bei weitem nicht aus: Die Vorabkontrolle ist nach § 4d Abs. 5 BDSG an spezifische, auslegungsfähige Voraussetzungen gebunden. Die effektive Kompensation der Heimlichkeit von Ermittlungen nach § 32e Abs. 2 BDSG-E kann nur durch Vorabkontrolle und zusätzliche obligatorische Einbindung von Betriebsräten, bei Ermangelung solcher durch Einbindung der Aufsichtsbehörden sichergestellt werden.

Zu einer Überwachungsfreiheit der Kommunikation mit Betriebsrat, Personalrat, Jugend- und Auszubildendenvertretung, Schwerbehindertenvertretung, Gleichstellungsbeauftragten oder betriebsinternen theologischen oder medizinischen Beratungsstellen bekennt sich der Gesetzentwurf in der Gesetzesbegründung an anderer Stelle (BT-Drs. 17/4230, S. 20 zu § 32i Abs. 1 BDSG-E). Dieser Grundsatz ist allgemein für die betriebliche Datenerhebung – deklaratorisch – gesetzlich festzuschreiben.

Schließlich fehlt es sowohl in § 32e BDSG-E wie bei allen Datenerhebungsbefugnissen nach dem Entwurf an der effektiven Absicherung auf der Verwendungs- und Verwertungsebene (s. schon oben zu b.). Der Entwurf sollte zumindest Regelungen dergestalt aufnehmen, dass Kündigungen oder sonstige arbeitsvertragsrechtliche oder zivilrechtliche Folgen von dem Arbeitgeber nicht auf Daten gestützt werden können, welche unter Verstoß gegen § 32e Abs. 2 – 7 BDSG-E und andere wesentliche Schutzvorschriften erhoben wurden. Solange ein Sanktionsapparat für Datenschutzverstöße des Arbeitgebers lediglich theoretisch existiert, bleibt die Erkennung und Bestimmung schutzwürdiger Interessen der Beschäftigten ebenso allein Sache des Arbeitgebers wie etwa die Bestimmung von Anlass und Streubreite bzw. Stichprobengröße heimlicher Nutzungen zu Sicherheitszwecken (vergl. auch § 32i Abs. 1 BDSG-E, dazu sogleich). Mangels trennscharfer Verbote kann nach geltendem Verfahrensrecht die Auslegung der Generalklauseln und Ermessensvorschriften des Bundesdatenschutzgesetzes durch den Arbeitgeber nur in exzessiven Missbrauchsfällen sicher in eine Sanktion oder gar ein verfahrensrechtliches Verwertungsverbot münden. Die Risiken der Rechtsanwendung durch den Arbeitgeber verbleiben nach dem Entwurf einmal mehr bei den Arbeitnehmern.

d.) (§ 32e Abs. 5 S. 5 BDSG-E): Die Unterrichtung der Zielpersonen heimlicher Maßnahmen greift zu kurz. Vielmehr sind alle Betroffenen von heimlichen Erhebungen zu unterrichten. (Zum Wegfall der Zweckgefährdung als Unterrichtungsvoraussetzung siehe schon oben zu 5. b.)).

## 7. § 32f BDSG-E (Videoüberwachung)

a.) (§ 32f Abs. 1 S. 1 BDSG-E): Videoüberwachung steht, auch wenn sie offen erfolgt, nach der an den persönlichkeitsrechtlichen Grenzen der unternehmerischen Gestaltungsfreiheit und damit unmittelbar an Verfassungsrecht orientierten Rechtsprechung des Bundesarbeitsgerichts unter erheblichem Rechtfertigungsdruck. Das von dem Entwurf eröffnete gesetzliche Zweckprogramm der Videoüberwachung ist demgegenüber konturenschwach und kann sich nur bei oberflächlicher Betrachtung auf zwingende betriebliche Interessen und hochrangige Rechtsgüter stützen.

Besonders augenfällig wird diese Emanzipation vom bestehenden Recht an dem Erhebungszweck der Qualitätskontrolle: Dieser lässt sich schon nicht hinreichend von der Verhaltens- oder Leistungskontrolle unterscheiden. Eine Videoüberwachung zu diesem Zweck erweise sich auch gleichsam automatisch als schwerwiegender und unverhältnismäßiger Eingriff in das Persönlichkeitsrecht der Betroffenen. Da jede Videoüberwachung der Erbringung der Arbeitsleistung den Kern des menschlichen Verhaltens im Betrieb betrifft, sind Überwachungen von Arbeitsplätzen stattdessen von Verfassungs wegen möglichst auszuschließen.

Die zusätzlichen Voraussetzungen nach Abs. 1 S. 1 werden sich als wirkungslos erweisen: Da die Qualitätskontrolle immer ein „wichtiges betriebliches Interesse“ im Sinne der Vorschrift sein kann, läuft der Entwurf auch bei wortgetreuer Beachtung der Vorschrift Gefahr, sich an den verfassungsrechtlichen Grenzen zulässiger Persönlichkeitsrechtseinschränkungen in der Arbeitswelt zu vergehen. Dagegen spricht auch nicht die von dem Gesetzentwurf gewählte Einschränkungen, dass keine Anhaltspunkte

dafür bestehen dürfen, dass schützwürdige Interessen der Betroffene am Ausschluss der Datenerhebung überwiegen (Abs. 1 S. 1 a.E.). Zwar ist gegen eine Berücksichtigung schon von Anhaltspunkten für schützwürdige Interessen nichts zu erinnern. Die Orientierung am Ausschluss der Überwachung greift allerdings an dieser Stelle zu kurz. Denn angesichts des weiten Gestaltungsspielraums des Arbeitgebers bei der Gestaltung technischer Überwachung ist der Totalverzicht (Ausschluss der Datenerhebung) die falsche Referenzgröße. Tatsächlich wäre die Orientierung an der konkret von dem Arbeitgeber beabsichtigten Datenerhebung richtig. Auch ist ein Überwiegen schützwürdiger Interessen der Betroffenen angesichts des Zweckkatalogs von § 32f Abs. 1 S. 1 BDSG-E nicht angemessen. Eine Videoüberwachung hätte aus Gründen der Verhältnismäßigkeit bereits dann auszubleiben, wenn schützwürdige Interessen beeinträchtigt würden (vergl. auch das Regelungsmodell in § 32f Abs. 3 BDSG-E).

**b.) (§ 32f Abs. 2 S. 2 BDSG-E):** Die Freistellung von Überwachung müsste klarstellend auch auf sonstige Sozialräume erstreckt werden.

**c.) (§ 32f Abs. 3 BDSG-E):** Der Vorschrift fehlt bisher jede zeitliche Beschränkung der Videoüberwachung. Das Bundesarbeitsgericht hat auf die Gefahr permanenten Überwachungsdrucks durch auch nur zeitweilige Videoüberwachung eindrucksvoll hingewiesen und ihre persönlichkeitsrechtliche Unerträglichkeit verdeutlicht. Für jede, auch offene, Videoüberwachung ist daher von vorneherein festzuhalten und auch bekannt zu machen, in welchem zeitlichen Umfang sie erfolgt, wann und zu welchen konkreten Zwecken eine Speicherung erfolgen soll und aus welchem Anlass. Da § 32f Abs. 1 BDSG-E sich seinem Wortlaut nach nur als Erhebungsvorschrift versteht, fehlt es dem Entwurf dagegen sogar an einer gesetzlichen Legitimation für eine Speicherung. Aus welchen Gründen und zu welchen Zwecken eine Speicherung erforderlich ist, wäre konsequenterweise gesetzlich zu regeln. Dabei müsste, verbreiteter Regelungstechnik im öffentlichen Bereich folgend, eine nur durch überwiegende konkrete Verwendungsinteressen im Einzelfall durchbrochene kurze Speicherungshöchstdauer festgelegt werden.

## 8. § 32h BDSG-E (biometrische Verfahren)

Ungeachtet einer zunehmenden Verbreitung biometrischer Verfahren zu Identifikationszwecken ist die Erhebung und Verarbeitung biometrischer Daten weiterhin mit einem empfindlichen Eingriff in das Persönlichkeitsrecht der Betroffenen verbunden. Wie kein anderes Merkmal sind biometrische Daten unveränderlich mit dem Betroffenen verknüpft. Ihre Verwendung zu betrieblichen Identifikationszwecken ist daher, zumal für gewöhnliche betriebliche Nutzungen ausreichend technische Alternativen zur Verfügung stehen, auf das zwingend erforderliche Maß zu beschränken in Fällen, in denen gleichwirksame Methoden nicht zur Verfügung stehen.

Der Entwurf stellt demgegenüber den Einsatz biometrischer Verfahren in das Ermessen des Arbeitgebers, zumal die Formel nach § 32h Abs. 1 S. 1 a.E. BDSG-E keine effektive Schranke darstellt (s. oben 7. b.)).

## 9. § 32i BDSG-E (Nutzung von Telekommunikationsdiensten)

**a.) (Vorbemerkung):** Das gesetzliche Regelungsmodell, welches auf die ausschließlich zu beruflichen oder dienstlichen Zwecken erlaubte Nutzung von Telekommunikationsdiensten abstellt, erweist sich als nur eingeschränkt praxisrelevant. Aus guten Gründen vermeiden Arbeitgeber eine Beschränkung der Nutzung ihrer Telekommunikationstechnik auf ausschließlich berufliche oder dienstliche Zwecke, zumal dies mit dem unternehmerischen Bedürfnis nach einer kommunikativen, weltgewandten und informierten Belegschaft kollidieren müsste. In Zeiten, in denen gerade auch von Arbeitnehmerinnen und Arbeitnehmern erwartet wird, in weit höherem Maße als früher kommunizierend zur Verfügung zu stehen, erschiene ein Verbot von privater Mitbenutzung geschäftlicher Telekommunikationsanlagen als veraltet.

Gleichwohl erweist schon die Regelung des datenschutzrechtlich einfachen Falles der nur zu beruflichen oder dienstlichen Zwecken erlaubte Nutzung betrieblicher Telekommunikationsinfrastruktur als äußerst schwierig. Der Entwurf verfehlt eine konsistente und angemessene Lösung.

**b.) (Datenverarbeitung vor und nach Abschluss eines Telekommunikationsvorgangs):**

Der Gesetzentwurf verfehlt mit der Unterscheidung von Datenerhebung während und nach dem Telekommunikationsvorgang schon eine konsistente Regelung und ist neu zu fassen: Die Entwurfsfassung leidet an einem durch Auslegung nicht mehr zu behebbenden Formierungsmangel. Während § 32i Abs. 1 – 3 BDSG-E offenbar die Erhebung bzw. Speicherung von Daten aus Telekommunikationsvorgängen während laufender Telekommunikation betreffen sollen, sieht § 34i Abs. 4 BDSG-E für die Erhebung, Verarbeitung und Nutzung von Daten nach Abschluss eines Telekommunikationsvorgangs die Geltung der allgemeinen Regeln nach §§ 32c und 32d BDSG-E vor. Abgesehen von den Inhaltsdaten von Sprachtelefonie sind aber alle bei der Nutzung von Telekommunikationsanlagen anfallenden Daten – insbesondere Telekommunikationsverbindungsdaten und Inhaltsdaten von betrieblichen Emails - nach Abschluss der Telekommunikation noch vorhanden. Eine Beschränkung der Erhebung bzw. Speicherung, wie sie § 32i Abs. 1 und Abs. 3 BDSG-E vornehmen, wird nach dem Entwurf mithin mit dem Moment gegenstandslos, in dem die Telekommunikation beendet ist. § 32i Abs. 4 S. 1 BDSG-E erweist sich daher als sinnwidrig.

**c.) (§ 32i Abs. 1 BDSG-E):** Die stichprobenartige oder anlassbezogen gezielte Leistungs- oder Verhaltenskontrolle mittels Telekommunikationsverbindungsdaten (§ 32i Abs. 1 S. 1 Nr. 3 BDSG-E) kommt in ihrer Überwachungsintensität einer Videoüberwachung gleich und ist abzulehnen. Die Gesetzesbegründung legt dazu offen, dass das persönlichkeitsrechtlich kritische Potential der Auswertung von Verbindungsdaten – nämlich die Erstellung von Kommunikationsprofilen und deren Auswertung – Arbeitgebern zukünftig zugänglich sein soll. Während die Rechtsprechung die Speicherung und Verarbeitung von Telekommunikationsverbindungsdaten zu anderen als Abrechnungszwecken nur in eng begrenzten Ausnahmefällen hinnimmt, zielt der Gesetzentwurf mit der Erlaubnis zu stichprobenartige oder anlassbezogene Kontrollen darauf, allenfalls flächendeckende oder

jeden vernünftigen Anlasses entbehrende Kontrollen auszuschließen. Da es an einer begleitenden Kontrolle der Telekommunikationsüberwachung durch eine unabhängige Stelle und der ausdrücklichen Anordnung einer Vorabkontrolle für eine konkrete Auswertungsmaßnahme (wie etwa in § 32e Abs. 5 S. 4 BDSG-E) fehlt, bleibt es dem Zufall bzw. der Gefährdungseinschätzung des Arbeitgebers nach § 32i Abs. 1 S. 2 BDSG-E überlassen, ob den Betroffenen die Auswertung ihrer Telekommunikation bekannt wird oder nicht. Eine derart unregelte Arbeitnehmerüberwachung hätte in einer freiheitlichen Betriebsverfassung keinen Platz.

**d.) (§ 32i Abs. 2 BDSG-E):** Die Erhebung und Verwendung der flüchtigen Inhalte von Sprachtelefonie wird gemeinhin zu den sensibelsten Eingriffen in das Persönlichkeitsrecht und die Telekommunikationsfreiheit (Art. 10 Abs. 1 GG) der Betroffenen gerechnet. Nach geltendem Recht sind arbeitgeberseitige Inhaltskontrollen von Telefonaten grundsätzlich verboten und nur ausnahmsweise hinzunehmen, wenn sie offen erfolgen und qualifizierte Bedürfnisse des Arbeitgebers sie unentbehrlich machen. So hat die Rechtsprechung etwa das offene Mithören in Callcentern zu Ausbildungszwecken im Einzelfall hingegenommen. Daran will offenbar § 32i Abs. 2 S. 1 BDSG-E anschließen, welcher das heimliche Mithören von Telefonaten jenseits der Call-Center-Regelung (§ 32i Abs. 2 S. 2 BDSG-E, dazu sogleich) verbietet.

Nicht verständlich ist daher, dass ausgerechnet für diesen höchst eingriffsintensiven Überwachungseingriff nach dem Entwurf eine Einwilligung eingeholt werden soll. Von einer freiwilligen, ohne Zwang abgegebenen Einwilligung in das hohe Opfer des Verzichts auf die Telekommunikationsfreiheit kann unter diesen Umständen nicht ausgegangen werden, zumal der Arbeitnehmer keine angemessene Kompensation oder sonstigen Anreiz für eine Mitwirkung erhält und lediglich von der Vermeidung von Nachteilen motiviert sein kann. Unter diesen Umständen ist und bleibt die Freiheit der Einwilligung des Arbeitnehmers, was sie bisher schon in den allermeisten Fällen war: Wunschdenken. Kann der Arbeitnehmer daher, ungeachtet einer formellen Einwilligung, der Überwachung tatsächlich nicht ausweichen, ist die Berechtigung zur Inhaltskontrolle zwecks Wahrung von Arbeitgeberinteressen der Übergang in eine Totalüberwachung der Inhalte der Telekommunikation und verfassungswidrig.

e.) (§ 32i Abs. 2 S. 2 BDSG-E): Auch die Call-Center-Regelung übergeht, indem sie „im Einzelfall“ eine dem Beschäftigten nicht erkennbare Gesprächsüberwachung erlaubt, das persönlichkeitsrechtliche Verbot der heimlichen Telefonüberwachung im Arbeitsverhältnis. Dieser Eingriff kann auch nicht dadurch in seiner Eingriffsintensität abgefedert werden, dass die Beschäftigten vorab abstrakt über die Möglichkeit der Überwachung informiert werden. Denn auch insoweit entsteht durch die Möglichkeit jederzeitigen Mithörens ein Überwachungsdruck, der die Persönlichkeitsrechte der Betroffenen stranguliert. Dass die Anwendung technologisch anspruchsvoller und besonders eingriffsintensiver Auswertungsmethoden wie der automatisierten Worterkennung oder der automatisierten Analyse des emotionalen Gesprächsverlaufs den Betroffenen – und damit auch den Gesprächspartnern – mitgeteilt werden muss, sieht der Entwurf über dies nicht vor.

f.) (§ 32i Abs. 3 BDSG-E): Zur Nutzung von Inhalten sonstiger Telekommunikationsdienste – insbesondere Email, Videodienste – gilt das zu § 32i Abs. 1 BDSG-E Gesagte (s. oben c.).

## **10. Modifikationen des allgemeinen Teils des Bundesdatenschutzgesetzes (§ 32i BDSG-E)**

a.) (§ 32i Abs. 1 BDSG-E): Ein gesetzlicher Kanon einwilligungsfähiger Verarbeitungen ist ungeachtet überwiegend bedenklicher Vorschläge des Entwurfs die richtige Antwort für die strukturelle Unterlegenheit der Beschäftigten gegenüber dem Arbeitgeber. Wohl nur der Gesetzgeber kann auch eine den Vorgaben der EU-Datenschutzrichtlinie genügende Festlegung treffen. Für eine weitere Flexibilisierung des Gesetzesvorbehalts für Einwilligungen im Arbeitsleben, wie sie die Berichterstatter der Koalitionsfraktionen im Arbeitspapier vom 10.05.2011 anregen, besteht auch kein praktisches Bedürfnis. Detaillösungen lassen sich einerseits kollektiv-rechtlich erzielen. Andererseits kann der Arbeitgeber zur Datenerhebung auf die gesetzlichen Verarbeitungsgeneralklauseln zurück greifen, wenn schutzwürdige Belange der Beschäftigten im Einzelfall nicht gefährdet sein

sollen. Denn eine Datenerhebung ohne bestehendes unternehmerisches Bedürfnis kann unterbleiben und bedarf daher auch keiner Einwilligung.

**b.) (§ 32I Abs. 4 BDSG-E):** Der Entwurf will mit dieser Vorschrift offenbar eine vereinzelt gebliebene Rechtsprechung fortschreiben, nach welcher die Mitteilung von Verstößen des Arbeitgebers gegen Gesetz und Recht an Strafverfolgungs- oder Aufsichtsbehörden eine Pflichtverletzung im Arbeitsverhältnis darstellen soll. Ein solches Privileg für verantwortliche Stellen, welche als Arbeitgeber i. S. § 3 Abs. 13 S. 1 BDSG-E grundsätzlich besondere Schutzpflichten gegenüber den Beschäftigten haben, ist sachlich nicht gerechtfertigt. Wer selbst von Persönlichkeitsrechtsverletzungen betroffen ist oder von solchen Kenntnis hat, muss sich ohne Weiteres an die dafür gesetzlich zuständigen Stellen wenden können, anstatt von dem Gesetzgeber für die Mauer des Schweigens über Datenschutzverstöße von Arbeitgebern in die Pflicht genommen zu werden. Es kann das Recht, Aufsichtsbehörden einzuschalten, auch im Konfliktfall nicht davon abhängig gemacht werden, ob tatsächlich Anhaltspunkte für einen Verdacht i. S. § 32I Abs. 4 BDSG bestanden haben oder nicht. Dies gilt insbesondere auch für öffentliche Stellen, welche Arbeitgeber i. S. § 3 Abs. 13 BDSG-E sind. Ebenso wenig ist den Beschäftigten zuzumuten, ohne Beistand der Aufsichtsbehörde oder Dritter zu beurteilen, ob im Einzelfall eine Abhilfe tatsächlich geschaffen wurde und ob diese unverzüglich erfolgt ist. Die im Arbeitsverhältnis strukturell drohende Sanktionslosigkeit von Datenschutzverstößen wird durch die Entwurfsfassung damit weiter abgesichert. Dem sollen weit reichende Duldungspflichten der Beschäftigten bei heimlichen und/oder eingriffsintensiven Datenerhebungen gegenüberstehen.

Die Vorschrift, welche auch eine effektive behördliche Strafverfolgung behindert, ist daher ersatzlos zu streichen. Klarstellend sollte § 6 Abs. 1 BDSG um das Recht der jederzeitigen Anrufung von Aufsichtsbehörde und Datenschutzbeauftragten ergänzt werden. Eine verfahrensrechtliche Waffengleichheit zwischen Arbeitgeber und Beschäftigtem und unter den Betriebsparteien und die effektive Wahrnehmung nicht nur von datenschutzrechtlichen Ansprüchen würden sonst ernsthaft in Frage gestellt.

**b.) (§ 32I Abs. 5 BDSG-E):** Die in Zusammenhang mit § 32I Abs. 3 BDSG-E (Unberührtheit der Rechte der Interessenvertretung der Beschäftigten) und § 6 Abs. 1, Abs. 3 BDSG zu sehende Vorschrift ist als lange fällige Klarstellung in einem ausdauernd geführten Streit zu begrüßen.

Berlin, den 17.05.2011

Sönke Hilbrans