Arbeitnehmerdatenschutz rechtssicher gestalten

Gesetzes- und Pflichtverstöße wirksam verhindern

Stellungnahme zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes und anderen Entwürfen

18. Mai 2011

Aktenzeichen
02.02.02.04./Bal

Arbeitsrecht

arbeitsrecht@arbeitgeber.de

T +49 30 2033-1200
F +49 30 2033-1205

BDA Bundesvereinigung der
Deutschen Arbeitgeberverbände

EU-Register der Interessenvertreter
Nr. 7749519702-29

BDI Bundesverband der
Deutschen Industrie e.V.

EU-Register der Interessenvertreter
Nr. 1771817758-48

Mitglieder von
BUSINESSEUROPE

Haus der
Deutschen Wirtschaft
Breite Straße 29
10178 Berlin

Zusammenfassung

Die Einhaltung von Gesetzen, Verträgen und betrieblichen Regelungen ist für die Unternehmen ein wichtiges Anliegen. Hierzu gehört auch der Arbeitnehmerdatenschutz. Daher begrüßen BDA und BDI das Anliegen, die Rechtsfragen des Arbeitnehmerdatenschutzes im Rahmen des Bundesdatenschutzgesetzes klarzustellen. Das Ziel muss sein, hierdurch rechtssichere Regelungen für Korruptions- und Kriminalitätsbekämpfung in den Unternehmen zu gewährleisten und gleichzeitig das in Deutschland hohe Niveau des Datenschutzes auch weiterhin im Betrieb sicherzustellen.

Ein eigenständiges Arbeitnehmerdatenschutzgesetz ist hierfür nicht notwendig. Die Gesetzentwürfe, die ein solch eigenständiges Gesetz vorsehen, kommen nicht umhin, auf das Bundesdatenschutzgesetz Bezug zu nehmen (vgl. § 4 der BT-Drs. 17/69 und § 4 Abs. 3 der BT-Drs. 17/4853). Auch soweit – zu Recht – der Arbeitnehmerdatenschutz weiterhin im Bundesdatenschutzgesetz verortet bleiben soll (Drs. 17/4230) bedarf der Gesetzentwurf erheblicher Änderungen, um die Compliance-Anforderungen der Unternehmen – zu denen auch der Datenschutz gehört – zu gewährleisten.

1. Gesetzentwurf der Bundesregierung (BT-Drs. 17/4230)

Der Gesetzentwurf zur Regelung des Beschäftigtendatenschutzes erfüllt diese Zielsetzung noch nicht. In der vorliegenden Form ist er nicht geeignet, Rechtssicherheit für Arbeitgeber und Arbeitnehmer bei der Verwendung personenbezogener Daten im Arbeitsverhältnis und die Einhaltung der Compliance im Unternehmen zu gewährleisten.

Der Entwurf sieht achtzehn neue Informationspflichten vor und geht von einer zusätzlichen Kostenbelastung der Wirtschaft mit Informationspflichten von 9,49 Mio. Euro jährlich und einmaligen Umstellungskosten von 10,3 Mio. Euro aus. Insbesondere vor dem Hintergrund der begrüßenswerten Bemühungen der Bundesregierung, Bürokratie flächendeckend abzubauen, ist dieser Aufbau neuer Bürokratie bedenklich und besonders problematisch für kleine und mittlere Unternehmen.

Der Gesetzentwurf bedarf vielfältiger Korrekturen. In diesem Rahmen ist insbesondere erforderlich:

- Der Abschluss von Betriebsvereinbarungen zum Arbeitnehmerdatenschutz muss weiterhin eine rechtssichere Grundlage für die Erhebung, Nutzung und Verarbeitung von Daten sein. Betriebsnahe Lösungen sind wichtig, um die gesetzlichen Vorgaben in den Betrieben anzuwenden und mit Leben zu erfüllen. Dem Ziel eines praxisnahen Arbeitnehmerdatenschutzes genügen solche Regelungen vielfach besser und nachhaltiger als gesetzliche Regelungen.
- Nach dem Gesetzentwurf ist die Einwilligung des Arbeitnehmers in eine Datenerhebung, -verarbeitung und -nutzung grundsätzlich nicht mehr möglich. Dieser Ausschluss der Einwilligungsmöglichkeit wird den Interessen der Arbeitnehmer und der Arbeitgeber nicht gerecht. Die Möglichkeit der Einwilligung muss daher als Grundlage für eine Datenerhebung, -verarbeitung und -nutzung erhalten bleiben.
- Korruptions- und Kriminalitätsbekämpfung ist für Arbeitgeber und Arbeitnehmer ein wichtiges Anliegen. Arbeitnehmerdatenschutz muss die Bekämpfung von Korruption und Kriminalität unterstützen. Dazu sind präventive Kontrollen und Datenanalysen unabdingbar.

- Zur Unterstützung von Korruptions- und Kriminalitätsbekämpfung kann auch eine gezielte Videoüberwachung erforderlich sein. Deren absolutes Verbot ist nicht akzeptabel.
- Es muss klargestellt werden, dass die Regelungen des Gesetzesentwurfs ausschließlich auf Beschäftigtendaten und nicht auf Daten des Tagesgeschäfts (Geschäftsdaten aus Buchhaltungssystemen mit einer Verknüpfung zum Anwender oder Benutzer wie bspw. Personenkürzel o.ä.) bezogen sind. Hierzu ist eine Definition von Geschäftsdaten in Abgrenzung zu Beschäftigtendaten festzulegen.
- Die Nutzung elektronischer Kommunikation muss grundlegend geregelt werden. Hierzu ist insbesondere eine klare Regelung zum Verhältnis der datenschutzrechtlichen Vorschriften zum TMG und TKG zu treffen.
- Eine gesetzliche Regelung muss den Datenaustausch zwischen Konzernunternehmen sicherstellen. Bisher ist ein solcher auf die Konzernstruktur zugeschnittener Datenschutz nicht vorgesehen. Schon lange notwendig ist eine rechtssichere Möglichkeit, um zum Beispiel Beschäftigtendaten von Konzerntöchtern an die Konzernmütter weitergeben zu können.

2. Gesetzentwürfe von SPD (BT-Drs. 17/69)und BÜNDIS 90/DIE GRÜNEN (BT-Drs. 17/4853)

Die vorgelegten Gesetzentwürfe der Oppositionsfraktionen von SPD und BÜNDNIS 90/DIE GRÜNEN weisen ebenfalls inhaltliche Mängel auf. Insbesondere ist es nicht akzeptabel, Beschäftigtendatenschutz zu einer Ausweitung von Mitbestimmungsrechten zu nutzen, z.B. indem die Berufung eines erstmals vorgesehenen Beschäftigtendatenschutzbeauftragten nur mit Zustimmung des Betriebsrats zulässig sein soll.

Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes (BT-Drs. 17/4230)

(Gesetzentwurf der Bundesregierung)

Im Einzelnen

1. § 3 – Definition von Beschäftigtendaten und Arbeitgeber

Regelungsgehalt: Beschäftigtendaten werden als personenbezogene Daten von Beschäftigten definiert. Arbeitgeber sind u. a. auch Dritte, denen Beschäftigte zur Arbeitsleistung überlassen werden.

Die Definition von „Beschäftigtendaten“ lässt die Auslegung zu, dass auch Daten den besonderen Bestimmungen zur Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten unterliegen sollen, die nicht unmittelbar mit einer Beschäftigung verbunden sind (wie zum Beispiel Kantinenabrechnungen, Arbeitgeberdarlehen). Die neuen Regelungen beschränken sich hingegen auf die „Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses“. Aus Gründen der Rechtsklarheit sollte sich der Zweckbezug zum Beschäftigungsverhältnis auch in der Definition der Beschäftigtendaten wie folgt wieder finden: „Beschäftigtendaten sind personenbezogene Daten von Beschäftigten, die im unmittelbaren Zusammenhang zur Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses stehen“.

Zur Abgrenzung des jeweiligen gesetzlichen Regelungsbereichs sollte klargestellt werden, dass Daten, die überwiegend dem Geschäftsbetrieb des Arbeitgebers zuzurechnen sind, nicht als Beschäftigtendaten gelten. Daten eines solchen Geschäftsbetriebs sind insbesondere Daten, die bei der Erfüllung der arbeitsvertraglichen Pflichten anfallen und keine Rückschlüsse auf besonders schützenswerte personenbezogene Daten des Arbeitnehmers im Sinne des § 3 Absatz 9 BDSG zulassen, wie beispielsweise der Benutzername in einem Buchhaltungssystem. Im Hinblick auf die Arbeitgeberdefinition sollte in der Gesetzesbegründung klargestellt werden, dass hiermit ausschließlich Fälle der Arbeitnehmerüberlassung im Sinne des AÜG gemeint sind.

2. § 4 Absatz 1 i.V.m. § 32l Absatz 5 – Betriebsvereinbarungen als andere Rechtsvorschriften

Regelungsgehalt: Der Gesetzentwurf sieht vor, dass andere Rechtsvorschriften im Sinne dieses Gesetzes auch Betriebs- und Dienstvereinbarungen sind. Diese Regelung wird durch § 32l Absatz 5 des Entwurfs eingeschränkt, der vorgibt, dass von den Vorschriften zum Arbeitnehmerdatenschutz nicht zu Ungunsten der Beschäftigten abgewichen werden kann.

Die Klarstellung, dass die Datenerhebung, -verarbeitung und -nutzung auch durch Betriebsvereinbarungen ausgestaltet werden kann, läuft durch die Einschränkung des § 32l Absatz 5 leer. Faktisch wird die Betriebsvereinbarung ausgeschlossen. der Gesetzgeber muss sich entscheiden, ob die Betriebsvereinbarung eine Abweichung ermöglichen soll. Um die Autonomie der Betriebsparteien zu erhalten, sollte § 35 Absatz 5 gestrichen werden.

Der Abschluss von Betriebsvereinbarungen zum Arbeitnehmerdatenschutz muss weiterhin eine Grundlage für die Erhebung, Nutzung und Verarbeitung von Daten sein können. Betriebsnahe Lösungen sind wichtig, um die gesetzlichen Vorgaben in den Betrieben anzuwenden und mit Leben zu erfüllen. Dem Ziel eines praxisnahen Arbeitnehmerdatenschutzes genügen solche Regelungen vielfach besser und nachhaltiger als gesetzliche Regelungen.

Darüber hinaus ist eine Klarstellung dahingehend erforderlich, dass andere Rechtsvorschriften im Sinne von § 4 Absatz 1 auch Tarifverträge sein können. Tarifverträge werden nicht als sonstige Regelung erwähnt. Lediglich in der Gesetzesbegründung zu § 32l wird ausgeführt, dass nicht ausgeschlossen sei, dass Tarifverträge, Betriebs- oder Dienstvereinbarungen die gesetzlichen Regelungen konkretisieren oder Alternativen gestalten. Diese Wertung muss in den Gesetzestext einfließen. Es muss klar sein, dass die Datenerhebung, -verarbeitung und -nutzung wie bisher auch auf der Grundlage einer sonstigen Regelung wie in Tarifverträgen, Betriebs- und Dienstvereinbarungen erfolgen kann.

3. § 27 Absatz 3 – Anwendungsbereich der Vorschriften des BDSG für das Arbeitsverhältnis

Regelungsgehalt: § 27 Absatz 3 sieht vor, dass die Vorschriften des Beschäftigtendatenschutzes auch dann gelten, wenn Daten nicht automatisiert verarbeitet werden.

Es ist ein Systembruch, die nicht automatisierte Datenverarbeitung den Vorschriften des Beschäftigtendatenschutzes zu unterstellen. Dieser Systembruch muss beseitigt werden. Das Bundesdatenschutzgesetz dient dem Schutz vor den Gefahren, die sie sich aus der automatisierten Datenverarbeitung ergeben, beispielsweise aufgrund eines Kontextverlusts oder den Verknüpfungsmöglichkeiten.

Um diese Unklarheiten zu vermeiden, sollte deshalb zu der Rechtslage vor dem 1. September 2009 zurückgekehrt werden, nach der die entsprechenden datenschutzrechtlichen Regelungen nur bei automatisierter Verarbeitung von Dateien Anwendung finden. Es ist also ein einheitlicher Datenbegriff erforderlich.

4. § 32 - Datenerhebung vor Begründung eines Beschäftigungsverhältnisses

a) Absatz 1

Regelungsgehalt: Absatz 1 regelt die Zulässigkeit der Erhebung von Beschäftigtendaten vor Begründung eines Arbeitsverhältnisses. Abgesehen vom Namen, der Anschrift, Telefonnummer und E-Mail-Adresse darf alles erhoben werden, dessen Kenntnis erforderlich ist, um die Eignung des Beschäftigten für eine vorgesehene Tätigkeit festzustellen.

Der Arbeitgeber hat ein berechtigtes Interesse, im Rahmen der Bewerbung Erkenntnisse über sog. „soft skills“ wie Sozialkompetenz, Teamfähigkeit oder Zuverlässigkeit für jede in Betracht kommende Tätigkeit zu erlangen. Der Wortlaut des § 32 Abs. 1 des Entwurfs macht nicht deutlich, ob der Erwerb von Kenntnissen über solche „soft skills“ zulässig ist, weil der Arbeitgeber nur noch für die konkrete Tätigkeit erforderliche Kenntnisse und nicht auch allgemeine Fähigkeiten erfragen können soll, obwohl diese sogar als Ziel der Berufsausbildung ausdrücklich vom Gesetzgeber verlangt werden (Fähigkeiten iSd. BBiG).

Die Formulierung „Kenntnis (…) erforderlich (...), um die Eignung des Beschäftigten für die vorgesehenen Tätigkeiten festzustellen“ ist zu eng, falls z.B. noch nicht endgültig feststeht, auf welcher offenen Stelle der Arbeitnehmer eingesetzt werden soll. Besser wäre deshalb folgende Formulierung: „…für sämtliche in Betracht kommende Tätigkeiten festzustellen“. Gleichzeitig muss der Begriff der Erforderlichkeit ersetzt werden durch folgende Formulierung: „dem Zweck dient, die Eignung (…) festzustellen“.

b) Absatz 2

Regelungsgehalt: Absatz 2 des Entwurfs sieht vor, dass der Arbeitgeber außerhalb besonderer Erlaubnistatbestände gem. § 8 Absatz 1 AGG Auskunft über besondere Arten personenbezogener Daten nur verlangen kann, wenn und soweit sie „wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung wesentliche und entscheidende berufliche Anforderungen darstellen“.

Die vorgesehene Beschränkung auf Daten, „soweit sie wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung wesentliche und entscheidende berufliche Anforderungen darstellen“, schafft neue Rechtsunsicherheit aufgrund einer Vielzahl von Auslegungsmöglichkeiten. In der Praxis ist es schwierig zu entscheiden, ob die gewonnenen Erkenntnisse eine „wesentliche und entscheidende berufliche Anforderung“ für die auszuübende Tätigkeit darstellen. Da ein Verstoß gegen das Datenerhebungsrecht mit einem Bußgeld von bis zu 300.000 € bedroht ist, gilt es, solche Rechtsunsicherheiten unbedingt zu vermeiden.

Die strengen Anforderungen des § 8 Absatz 1 AGG sollen auch für die Frage nach Vorstrafen oder Ermittlungsverfahren gelten. Dies ist nicht gerechtfertigt. Nach der Rechtsprechung des BAG konnte nach Vorstrafen und nach den Vermögensverhältnissen gefragt werden, „wenn und soweit die Art des zu besetzenden Arbeitsplatzes dies erfordert“ (BAG vom 25.4.1980 – 7 AZR 322/78). Dies muss ausreichend sein. Die Einführung des Begriffs „wesentliche und entscheidende berufliche Anforderungen“ ist eine Verschärfung, die vor dem Hintergrund der ausdifferenzierten Rechtsprechung nicht notwendig ist.

c) Absatz 3

Regelungsgehalt: Es ist ein generelles Verbot der Auskunftsbitte im Hinblick auf eine Schwerbehinderung vorgesehen.

Das ist überflüssig. Absatz 3 sollte gestrichen werden. Einzelfälle sollten im Gesetzentwurf nicht explizit aufgegriffen werden. Zudem unterliegen Gesundheitsdaten ohnehin dem besonderen Schutz des § 3 Abs. 9 BDSG und der Sondervorschriften des § 1 AGG und des § 81 Abs. 2 SGB IX.

d) Absatz 6

Regelungsgehalt: Dieser gibt vor, dass Beschäftigtendaten unmittelbar beim Beschäftigten zu erheben sind. Allgemein zugängliche Daten dürfen nur dann ohne Mitwirkung des Beschäftigten erhoben werden, wenn er hierauf vor der Erhebung hingewiesen wurde und sein schutzwürdiges Interesse nicht überwiegt. Eine Datenerhebung aus sozialen Netzwerken ist nicht möglich. Hiervon sind solche sozialen Netzwerke ausgenommen, die zur Darstellung der beruflichen Qualifikation bestimmt sind.

Diese Regelung wird der täglichen Praxis beim Umgang mit allgemein zugänglichen Daten nicht gerecht. Es ist nicht ersichtlich, warum im Bewerbungsverfahren nur unter erschwerten Voraussetzungen auf Zeitungsartikel, Interneteinträge etc. zurückgegriffen werden können soll. Insbesondere in Bezug auf das Internet ist zu berücksichtigen, dass jeder für das Einstellen von Beiträgen in der Regel selbst verantwortlich ist.

Nach diesen Vorgaben wäre ein Arbeitgeber quasi gezwungen, nach Eingang einer Bewerbung dem Bewerber individuell einen Hinweis zukommen zu lassen, sofern er allgemein zugängliche Informationen nutzen möchte. Andernfalls bliebe ihm nur, in der Stellenausschreibung einen entsprechenden Hinweis aufzunehmen, was in der Praxis für potentielle Bewerber aber eher abschreckend wirken könnte.

Durch die Vorschrift wird die Bereitschaft, Mitarbeiter einzustellen und Arbeitsplätze zu schaffen, neuen überflüssigen Belastungen ausgesetzt. Das Ziel des Arbeitsrechts, Beschäftigung zu fördern, wird hierdurch nicht unterstützt.

Weder der Gesetzestext noch die Begründung sehen eine klare Abgrenzung von sozialen Netzwerken und sozialen Netzwerken zur Darstellung der beruflichen Qualifikation vor. Es ist sehr wahrscheinlich, dass sich in Zukunft Netzwerke bilden, die sowohl die berufliche als auch die soziale Komponente gleich stark gewichten. Rechtsunsicherheit ist hier vorprogrammiert.

5. § 32a – ärztliche Untersuchungen und Eignungstests

a) Absatz 1

Regelungsgehalt: Absatz 1 regelt die Zulässigkeit von Gesundheitsuntersuchungen im Anbahnungsverhältnis. Die Erfüllung bestimmter gesundheitlicher Voraussetzungen muss wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung eine wesentliche und entscheidende berufliche Anforderung zum Zeitpunkt der Arbeitsaufnahme darstellen. Die Einwilligung des Beschäftigten ist erforderlich.

Die gesetzlichen Voraussetzungen, unter denen Gesundheitsuntersuchungen zulässig sein sollen, sind zu eng. So werden zum Beispiel in der chemischen Industrie vielfach bei Einstellungen Alkohol- und Drogenuntersuchungen unabhängig davon vorgenommen, wo der konkrete Einsatz später erfolgen soll. Dies ist notwendig, da der Konsum von Alkohol und Drogen nicht mehr dem privaten Bereich zugeordnet werden kann, wenn dadurch die sicherheitsempfindlichen Verfahrensabläufe in den Unternehmen gefährdet würden. Die Regelung sollte deshalb Gesundheitsuntersuchungen zulassen, um die Eignung des Bewerbers unabhängig von der auszuübenden Tätigkeit zu prüfen. Der Begriff der „Zweckdienlichkeit“ sollte in diesem Zusammenhang eingeführt werden. Unklar bleibt zudem, welche Tätigkeiten ihrer Art nach erfasst werden sollen. So kann ein gesunder Rücken für eine überwiegend sitzende Tätigkeit eine wesentliche und entscheidende berufliche Anforderung sein. Zudem muss ausreichend sein, den Beschäftigten über die Art der Untersuchung (Blut- und Urinuntersuchung) zu informieren, bevor eine Einwilligung erteilt wird.

Insgesamt muss das Verhältnis von Arbeitnehmerdatenschutz und Arbeitsschutz klargestellt werden. So muss sichergestellt werden, dass die Pflichtuntersuchungen, die die Verordnung zur arbeitsmedizinischen Vorsorge vorsieht, nicht den Voraussetzungen des § 32a Absatz 1 unterliegen.

b) Absatz 2

Regelungsgehalt: Absatz 2 regelt die Zulässigkeit von Eignungstests vor Begründung des Beschäftigungsverhältnisses. Die Untersuchung oder Prüfung muss wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung erforderlich sein, um die Eignung des Beschäftigten für die vorgesehene Tätigkeit festzustellen. Der Beschäftigte muss in den Eignungstest und in die Weitergabe der Ergebnisse des Tests an den Arbeitgeber einwilligen.

Die Restriktionen bei den grundsätzlich zulässigen Eignungstests sind zu weitgehend. Dies gilt insbesondere für die Erforderlichkeit der Untersuchung/Prüfung in Bezug auf die Art der auszuübenden Tätigkeit oder die Bedingungen ihrer Ausübung, aber auch für die notwendige Einwilligung. Die Teilnahme an Auswahl-/Testverfahren ist prinzipiell freiwillig. Eine explizite Einwilligung zu fordern, ist praxisfern.

Welches Ergebnis der Arbeitgeber erfahren darf, ist nicht hinreichend geklärt: Inhaltliche Untersuchungsergebnisse dürfen dem Arbeitgeber nicht zur Kenntnis gegeben werden, wenn die Tests durch Personen, die einer Schweigepflicht unterliegen, durchgeführt werden. Dann darf dem Arbeitgeber nur das „Ob“ zur Kenntnis gegeben werden. Dies ist praxisfern. So werden die meisten Assessment-Center unter der Beteiligung von Psychologen durchgeführt. Es wäre unpraktikabel, wenn der Arbeitgeber nur über das „Ob“ einer Eignung informiert wird. Nach der vorgeschlagenen Regelung wäre sogar eine Rangliste unter mehreren geeigneten Bewerbern unzulässig.

6. § 32b – Datenverarbeitung und -nutzung vor Begründung eines Beschäftigungsverhältnisses

Regelungsgehalt: Die weitere Nutzung von Bewerberdaten wird von der Erforderlichkeit für die Feststellung der Eignung des Beschäftigten für die vorgesehene Tätigkeit abhängig gemacht. Unverlangt eingesandte Daten dürfen nur soweit genutzt werden, wie dies für die vorgesehene Tätigkeit erforderlich ist. Beschäftigtendaten müssen entsprechend § 35 Absatz 2 Satz 2 gelöscht werden.

Auch hier ist die Voraussetzung der Erforderlichkeit wiederum zu eng, um bei der Entscheidung über die Nutzung von Daten eine rechtssichere Grundlage zu liefern. Das zeigt sich insbesondere dann, wenn der Arbeitgeber bei unverlangt durch den Bewerber überlassenen Daten zwischen erforderlichen und nicht erforderlichen Daten selektieren muss. So müsste der Arbeitgeber sich zum Beispiel fragen, ob er Bewerbungsunterlagen, in denen ein unter AGG-Aspekten kritisches und vom Arbeitgeber nicht verlangtes Bewerberfoto enthalten ist, weiter komplett einscannen kann oder hier – kaum praktikabel – eine Selektion in „erforderliche“ und „nicht erforderliche“ Daten vornehmen muss. Darüber hinaus muss berücksichtigt werden, dass der Bewerber mit der Zusendung seiner Daten diese freiwillig dem Arbeitgeber überlässt und sich hieraus für den Arbeitgeber zum Beispiel im Hinblick auf eine Angabe zur Schwerbehinderung gesetzliche Verpflichtungen ergeben.

Zur Vermeidung einer Überbürokratisierung des Bewerbungsverfahrens sollte daher auch hier der Begriff „erforderlich“ durch „dienlich“ ersetzt werden.

Zudem sollte die Formulierung „ohne dass der Arbeitgeber hierzu Veranlassung gegeben hat“ in „ohne dass der Arbeitgeber den Arbeitnehmer aufgefordert hat“ präzisiert werden. Andernfalls könnte man argumentieren, dass jede Überlassung von Informationen durch den Bewerber im Rahmen einer ausgeschriebenen Stelle letztlich durch den Arbeitgeber veranlasst ist.

Im Hinblick auf die Löschungsvorgaben sollte klargestellt werden, dass eine Speicherung nach § 35 Abs. 2 BDSG so lange zulässig ist, bis der Arbeitgeber mit Sicherheit davon ausgehen kann, dass keine Ansprüche zum Beispiel nach dem AGG gegen ihn geltend gemacht werden oder nach Ablauf der Probezeit feststeht, dass er auf keine anderweitigen Bewerber zurückgreifen muss. Im Hinblick auf die Einwilligung des Bewerbers in die weitere Speicherung sollte zudem sichergestellt bleiben, dass auch eine konkludente Einwilligung in die Aufbewahrung von Bewerberdaten möglich ist.

7. § 32c – Datenerhebung im Beschäftigungsverhältnis

Regelungsgehalt: § 32c regelt die Datenerhebung im Beschäftigungsverhältnis. Die Datenerhebung ist zulässig, wenn dies zu dessen Durchführung, Beendigung und Abwicklung erforderlich ist. Dazu gibt § 32c Regelbeispiele, in denen Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses erhoben werden dürfen. Hinsichtlich der Zulässigkeit von gesundheitlichen Untersuchungen und Eignungstests wird auf § 32a Absatz 1 und 2 verwiesen.

Gemäß § 32c Absatz 1 Satz 3 gilt § 32 Absatz 6 entsprechend. Damit wäre eine Erhebung allgemein zugänglicher Daten und von Daten aus sozialen Netzwerken im laufenden Beschäftigungsverhältnis eingeschränkt bzw. unzulässig. Dies widerspricht arbeitsrechtlichen Grundsätzen. Dem Arbeitnehmer obliegen Loyalitäts- und Rücksichtspflichten. Würde ein Arbeitnehmer zum Beispiel ehrverletzende Äußerungen über den Arbeitgeber in soziale Netzwerke einstellen, wäre die arbeitsrechtliche Sanktionierung de facto ausgeschlossen, da eine entsprechende Datenerhebung unzulässig wäre. Dies darf nicht sein. Der Arbeitgeber muss ein solches Verhalten sanktionieren können und zwar auch dann, wenn er zufällig hierauf stößt.

Klargestellt werden muss auch, dass die Erhebung, Nutzung und Verarbeitung von Gesundheitsdaten außerhalb von Gesundheitsuntersuchungen nach § 32c und d

zulässig ist. Dies gilt sowohl für Informationen zu Fehlzeiten als auch für eventuell bekannte Diagnosen, die für den Arbeitgeber für die Frage der Zulässigkeit einer personenbedingten Kündigung oder für andere Einsatzmöglichkeiten von erheblicher Bedeutung sein können. Zudem müssen die für die Praxis besonders wichtigen datenschutzrechtlichen Fragen bei der Durchführung des gesetzlich zwingenden Gesundheitsmanagements geklärt werden. Hier ist vor dem Hintergrund dieser Regelung sowie von § 32d Absatz 5 für die Betriebe nicht klar, welche Daten bei der Durchführung eines betrieblichen Eingliederungsmanagements erhoben und genutzt werden dürfen.

§ 32c Absatz 2 kann gestrichen werden, da die Veränderung der Tätigkeit unter die Durchführung des Beschäftigungsverhältnisses in Absatz 1 fällt. Die Regelung ist daher überflüssig.

Die in § 32c Absatz 3 vorgesehene Regelung, wonach ärztliche Untersuchungen gem. § 32a Absatz 1 und Eignungstests gem. § 32a Absatz 2 ohne konkreten Anlass unzulässig sein sollen, hat erhebliche Auswirkungen. In bestimmten Industriezweigen mit besonderem Gefahrenpotential, wie der chemischen Industrie, muss die Gewähr geboten werden, dass die erforderlichen Sicherheitsstandards eingehalten werden. Dies kann auch die Durchführung routinemäßiger Alkohol- und Drogenkontrollen erforderlich machen. Absatz 3 sollte deshalb ergänzt werden durch die Formulierung: „oder dies zur Arbeitssicherheit oder aus Gründen des Gesundheitsschutzes erforderlich ist“.

8. § 32d Datenverarbeitung und -nutzung im Beschäftigungsverhältnis

a) Absatz 3

Regelungsgehalt: Die Regelung sieht u. a. vor, dass zur Aufdeckung von Straftaten oder schwerwiegenden Pflichtverletzungen durch Beschäftigte im Beschäftigungsverhältnis ein automatisierter Abgleich von Beschäftigtendaten in anonymisierter oder pseudonymisierter Form durchgeführt werden kann.

Unternehmen sind kontinuierlich gestiegenen aktien- und gesellschaftsrechtlichen sowie aufsichtsbehördlichen Anforderungen in Bezug auf Organisations- und Sorgfaltspflichten ausgesetzt. Automatisierte Abgleiche von Beschäftigtendaten sind für die Erfüllung dieser Verpflichtungen wesentlich. Sie müssen sowohl präventiv als auch repressiv erfolgen können. Der Wortlaut des Gesetzentwurfs sowie die Gesetzesbegründung sprechen dafür, dass kein konkretisierter Verdacht vorliegen muss, bevor ein Abgleich durchgeführt werden kann. Um hier endgültige Klarheit zu schaffen, sollte der in vorherigen Referentenentwürfen genutzte Begriff „verhindern“ in Bezug auf Straftaten und Pflichtverletzungen wieder aufgenommen werden.

Darüber hinaus ist die Beschränkung der Überprüfungsmöglichkeiten insbesondere auf schwerwiegende Pflichtverletzungen zu eng. Der Arbeitgeber muss vielmehr in der Lage sein, Pflichtverletzungen, Ordnungswidrigkeiten oder Straftaten aufzudecken und zu verhindern, ohne zuvor zu einer rechtsunsicheren Prüfung gezwungen zu werden, ob der Sachverhalt tatsächlich eine „schwerwiegende Pflichtverletzung“ darstellt oder nicht.

Die Regelung, dass die Beschäftigten über Inhalt, Umfang und Zweck des automatisierten Abgleichs zu unterrichten sind, sollte klargestellt werden. Allenfalls kann gewollt sein, dass Personen, deren Daten personalisiert wurden, im Sinne des Transparenzgebots unterrichtet werden. Daher muss die Unterrichtungspflicht auf diesen Personenkreis beschränkt werden.

b) Absatz 5

Regelungsgehalt: Weiterhin wird geregelt, dass die automatisierte Zusammenführung einzelner Lebens- und Personaldaten kein Gesamtbild der wesentlichen geis-

tigen und charakterlichen Eigenschaften oder des Gesundheitszustandes des Beschäftigten ergeben darf.

Dieser Absatz sollte entfallen. Es ist völlig unklar, wann ein „Gesamtbild“ in diesem Sinne vorliegt. Zielt diese Regelung auf ein die gesamte Person im beruflichen wie persönlichen Umfeld umfassendes Bild oder genügt der Bezug zu bestimmten Lebensbereichen? Eine Eingrenzung auf den beruflichen Kontext könnte in der Konsequenz dazu führen, dass Arbeitnehmer nicht mehr von Unterstützungsleistungen des Arbeitgebers profitieren könnten. Dies gilt zum Beispiel im Hinblick auf Führungskräftepools. Gerade für Führungskräfte spielen neben den fachlichen auch die charakterlichen Eigenschaften eine wesentliche Rolle. Es ist deshalb für ein Unternehmen unvermeidbar, sich auch von den charakterlichen Eigenschaften eines Arbeitnehmers zu überzeugen, bevor diese Person in den Führungskräftepool aufgenommen wird. Würde sich hierdurch bereits ein Gesamtbild der wesentlichen geistigen und charakterlichen Eigenschaften ergeben, müssten entscheidende Kriterien bei der Auswahl von Führungskräften in Zukunft unberücksichtigt bleiben.

Unklarheit besteht auch in Bezug auf das „Gesamtbild des Gesundheitszustandes des Beschäftigten“. So muss es im Interesse beider Arbeitsvertragsparteien auch in Zukunft möglich sein, Fehlzeiten- und Krankengespräche zu führen. Das wird insbesondere im Hinblick auf das sog. betriebliche Eingliederungsmanagement deutlich. Um nach einer Erkrankung dem Arbeitnehmer eine sinnvolle und vernünftige Wiedereingliederung in den Betrieb zu ermöglichen, ist der Arbeitgeber darauf angewiesen, Informationen zum Gesundheitszustand des Betroffenen zu erhalten. Je weitergehender der Gesundheitszustand bekannt ist, desto besser kann der Arbeitnehmer bei der Rückkehr in den Betrieb unterstützt werden. Sollten in Zukunft aus datenschutzrechtlichen Gründen nur noch Teilbereiche des Gesundheitszustandes offengelegt werden dürfen, würde das betriebliche Eingliederungsmanagement sinnentleert.

9. § 32e – Datenerhebung zur Aufdeckung und Verhinderung von Straftaten und schwerwiegenden Pflichtverletzungen

Regelungsgehalt: Die Regelung sieht enge Voraussetzungen für die Erhebung von Arbeitnehmerdaten ohne Kenntnis des Arbeitnehmers vor. So soll dies u. a. nur möglich sein, wenn den Verdacht begründende Tatsachen auf eine Straftat bzw. schwerwiegende Pflichtverletzung vorliegen, die den Arbeitgeber zu einer Kündigung aus wichtigem Grund berechtigen würden. Zudem darf die Erhebung zur Verhinderung von Straftaten bzw. schwerwiegenden Pflichtverletzungen nur unter bestimmten Voraussetzungen erfolgen. Die Erforschung des Sachverhalts auf andere Weise müsste erschwert oder weniger erfolgversprechend sein. Die Datenerhebung wird sowohl zeitlich als auch im Hinblick auf die eingesetzten Mittel erheblich eingeschränkt. Der Kernbereich privater Lebensführung darf nicht angetastet werden.

Arbeitnehmerdatenschutz muss die Bekämpfung von Korruption und Kriminalität unterstützen. Die scharfen Voraussetzungen des § 32e sind vor dem Hintergrund der Haftungsrisiken der Unternehmensleitung im Hinblick auf die Einhaltung von Complianceregelungen bedenklich.

Der Anwendungsbereich des § 87 Abs. 1 Nr. 6 bei einer Datennutzung nach § 32e muss klargestellt werden. Es kann den Betriebsrat in eine kritische Lage bringen, wenn er vorab von bestimmten – heimlich vorzunehmenden – Datenerhebungen informiert ist. Soweit Maßnahmen nach § 32e als kollektive Maßnahmen mitbestimmungspflichtig sein sollten, sollte das Mitbestimmungsrecht für die konkrete Kontrolle/Ermittlung in eine nachträgliche Informationspflicht umgewandelt werden.

a) Absatz 2

Die Einschränkung in § 32e Absatz 2, dass eine Datenerhebung nur zulässig ist, wenn die Straftat bzw. Pflichtverletzung so schwerwiegend ist, dass sie den Arbeit-

geber zu einer Kündigung aus wichtigem Grund berechtigen würde, ist zu eng. Wann eine Kündigung aus wichtigem Grund heute – insbesondere nach der sogenannten Emmely-Entscheidung – noch möglich ist, lässt sich von niemandem sicher vorhersagen. Man kann dem Arbeitgeber schwerlich eine Verhältnismäßigkeitsprüfung auferlegen, die er nicht rechtssicher durchführen kann.

Darüber hinaus muss der Arbeitgeber berechtigt sein, Straftaten oder schwerwiegende Pflichtverletzungen von Anfang an zu unterbinden. Dies muss auch dann gelten, wenn er zufällig auf sie stößt. Sollte er erst einmal abwarten müssen, bis ein Verdacht durch Tatsachen begründet wird, würde dies dem Präventionsgedanken nicht gerecht.

Ist beispielsweise ein Mitarbeiter aus der Versicherungsbranche berechtigt, Ersatzleistungen bis zu einem bestimmten Betrag anzuweisen, so muss eine Überprüfung möglich sein, ob ein höherer Schadenbetrag zeitnah in mehrere Teilbeträge aufgeteilt wird, die auf demselben Konto gutgeschrieben werden. Nur so können rechtzeitig Hinweise auf einen Missbrauch der Befugnisse entdeckt werden. Gleiches gilt im Hinblick auf eine Überprüfung, ob Schadenzahlungen ständig knapp unter der Grenze der Regulierungsbefugnis liegen. Auch hier muss die Möglichkeit bestehen, Hinweise auf ein mögliches kollusives Zusammenwirken zwischen einem Mitarbeiter und einem Dritten aufdecken zu können. Derartige präventiv angelegte Prüfroutinen zur Verhinderung von Straftaten müssen auch im Rahmen von § 32e BDSG-E zulässig sein.

Es muss zudem ausreichend sein, dass ein Verdacht gegen eine konkrete Beschäftigtengruppe besteht, wie dies auch aus der Gesetzesbegründung hervorgeht. Dies sollte im Gesetzestext klargestellt werden.

Präventive Datenerhebung erhöht das Risiko entdeckt zu werden und reduziert damit die Wahrscheinlichkeit, dass kriminelle Handlungen begangen werden. Die Möglichkeiten, präventiv Daten zu erheben, sind im Gesetzentwurf jedoch zu eng gefasst. Eine Verknüpfung zwischen einer ursprünglichen Straftat bzw. schwerwiegenden Pflichtverletzung und im Zusammenhang damit stehenden weiteren Straftaten bzw. schwerwiegenden Pflichtverletzungen, um präventiv vorgehen zu können, wird den Erfordernissen der Praxis nicht gerecht. So muss z.B. eine Umfrage bei Lieferanten zur Abwicklung von Ausschreibungen bzw. zur Gewährung von Geschenken und Belohnungen weiterhin möglich sein.

b) Absatz 3

Wann die Erforschung des Sachverhalts auf andere Weise erschwert oder weniger erfolgversprechend wäre, ist völlig unklar und stellt die Arbeitgeber vor erhebliche Rechtsunsicherheiten. Diese der StPO entnommene Formulierung mag für staatliche Stellen angemessen sein. Ansonsten muss die Datenerhebung aber zulässig sein, wenn sie geeignet ist.

c) Absatz 4

Der Erhebungszeitraum sowie die für die Datenerhebung eingesetzten Mittel werden erheblich eingeschränkt. Auch hierdurch ergibt sich Rechtsunsicherheit. So stellt sich die Frage, was eine „planmäßig angelegte Beobachtung“ in diesem Sinne ist und unter welchen Voraussetzungen von getrennten Beobachtungen gesprochen werden kann.

Der Beobachtungszeitraum von 24 Stunden ohne Unterbrechung oder an mehr als vier Tagen ist zu kurz. Soll zum Beispiel durch einen Detektiv geklärt werden, welche Person von einem Telefon in einem ansonsten ungenutzten Gebäudeteil des Betriebs unerlaubter Weise Telefonate führt, kann hierfür eine Beobachtung erforderlich sein, die über den genannten Zeitraum hinausgeht.

d) Absatz 5

Entgegen dem Wortlaut des § 32e Absatz 5 soll nach der Gesetzesbegründung eine Pflicht zur schriftlichen Dokumentation bestehen. Eine schriftliche Dokumentation wäre jedoch unnötig bürokratisch. Es ist ausreichend, wenn der Arbeitgeber eine elektronische Dokumentation im Sinne von § 126b BGB vornimmt.

Die ebenfalls in Absatz 5 vorgesehene Unterrichtungspflicht kann in der Praxis zu Problemen führen, wenn zum Beispiel der Nachweis einer Pflichtverletzung (die aber tatsächlich begangen wurde) nicht erbracht werden kann. Es besteht die Gefahr, dass der Betroffene sogar zusätzlich motiviert wird, wenn zwar z. B. eine Straftat vorliegt, diese jedoch durch die Datenerhebung nicht nachgewiesen werden konnte.

Die Durchführung einer Vorabkontrolle vor Beginn der Datenerhebung steht der Notwendigkeit entgegen, kurzfristige Erhebungen durchzuführen und schafft hierdurch die Gefahr, dass der Zweck der Untersuchung nicht erreicht werden kann.

e) Absatz 7

Die Regelung zu Daten, die den Kernbereich privater Lebensgestaltung betreffen, wird in der Praxis zu Rechtsunsicherheit führen. Das gilt umso mehr, als auch in der Gesetzesbegründung offen gelassen wird, was unter dem Kernbereich privater Lebensgestaltung verstanden wird. So stellt sich z. B. die Frage, inwieweit ein Arbeitgeber bei einem Verdacht auf Vortäuschung einer Arbeitsunfähigkeit Nachforschungen anstellen kann, ohne hierdurch in den Kernbereich privater Lebensgestaltung einzugreifen. Um solche Rechtsunsicherheiten auszuräumen, sollte der Ausdruck entsprechend § 32f Absatz 2 Satz 2 des Gesetzentwurfs konkretisiert werden.

10. § 32f – Beobachtung nicht öffentlicher Betriebsstätten mit optisch-elektronischen Einrichtungen

Regelungsgehalt: § 32f regelt, dass eine offene Videoüberwachung in öffentlich nicht zugänglichen Betriebsstätten aus bestimmten Gründen zulässig ist. Schutzwürdige Interessen der Betroffenen am Ausschluss der Datenerhebung dürfen nicht überwiegen. Die in den Referentenentwürfen noch geregelte Möglichkeit der gezielten Videoüberwachung ist nun nicht mehr vorgesehen.

Es ist nicht nachvollziehbar, warum die nach der bisherigen Rechtslage als ultima ratio zulässige Videoüberwachung nun nicht mehr möglich sein soll. Der Gesetzentwurf bleibt hiermit weit hinter dem zurück, was sowohl vom Bundesarbeitsgericht als auch den Landesbeauftragten für den Datenschutz unter bestimmten Voraussetzungen als zulässig angesehen wird.

Das ist für die Praxis nicht hinnehmbar. So belaufen sich zum Beispiel im deutschen Einzelhandel die jährlichen Inventurverluste auf etwa 4 Milliarden Euro. Nach vorsichtigen Schätzungen ist davon auszugehen, dass gut ein Viertel hiervon, also etwa eine Milliarde Euro, auf Diebstähle durch eigene Mitarbeiter oder Lieferanten zurückzuführen ist. Vor diesem Hintergrund ist eine hohe Aufklärungsquote wesentlich. Die gezielte Videoüberwachung trägt erheblich dazu bei, die Aufklärung solcher Fälle voranzutreiben. Als konkretes Bespiel mag der Fall dienen, in dem aus einem Lager größere Mengen an Tabakwaren gestohlen worden waren. Nachdem weder der Einsatz von Detektiven während der Ladenöffnungszeiten noch sonstige Maßnahmen Aufklärung brachten, musste der Tabak außerhalb der Ladenöffnungszeiten entwendet worden sein. Nachdem der Einsatz eines Detektivs zu dieser Zeit zu auffällig gewesen wäre, wurde eine gezielte Videoüberwachung durchgeführt und eine Reinigungskraft als Täter überführt. Eine solche Überwachung würde bei der im Gesetzentwurf vorgesehenen Regelung entfallen, die Aufklärung wäre nicht mehr möglich.

Hinzu kommt, dass die gezielte Videoüberwachung bislang stets mit dem Einverständnis der Betriebsräte und der betrieblichen Datenschutzbeauftragten erfolgte. Vor diesem Hintergrund sollte die gezielte Videoüberwachung sowohl bei öffentlich zugänglichen als auch bei nicht öffentlich zugänglichen Betriebsstätten möglich sein.

Kritik ist auch an der jetzt vorgesehenen Ausgestaltung der offenen Videoüberwachung in § 32f zu üben.

So ist zwar die Regelung von konkreten Fällen, in denen generell die offene Videoüberwachung zulässig ist, sinnvoll. Diese Liste sollte jedoch Regelbeispiele enthalten und gleichzeitig noch ergänzt werden um den allgemeinen Punkt „Aufklärung von Straftaten".

Problematisch ist zudem der Verweis auf § 6b Abs. 3 BDSG. Danach dürfen die durch die Videoüberwachung gewonnen Daten nur für einen anderen Zweck verarbeitet werden, wenn dies zur Verfolgung von Straftaten erforderlich ist. Dies ist für das Arbeitsverhältnis nicht ausreichend. Die so gewonnenen Daten sollten auch dann für den Arbeitgeber verwertbar sein, wenn es sich um eine schwerwiegende Vertragsverletzung des Arbeitnehmers handelt. Bei der offenen Überwachung einer Maschine kann beispielsweise eine solche schwerwiegende Vertragsverletzung bemerkt werden. Wegen § 6b Abs. 3 BDSG kann der Arbeitgeber diese Zufallsfunde nicht als Beweismittel für die begangene arbeitsvertragliche Pflichtverletzung im Kündigungsschutzprozess verwerten. Dies ist mit dem Arbeitsverhältnis als Dauerschuldverhältnis nicht vereinbar, da das Arbeitsverhältnis ein Vertrauensverhältnis voraussetzt. Es ist deshalb klarzustellen, dass auch eine Verwertungsmöglichkeit für Zufallsfunde besteht, wenn eine schwerwiegende Vertragspflichtverletzung vorliegt.

Darüber hinaus muss weiterhin sichergestellt werden, dass bei Proben und Aufführungen von Theatern und Orchestern eine Übertragung des Geschehens auf der Bühne z.B. in die Räumlichkeiten des Leitungspersonals und die Aufenthaltsräume der Mitwirkenden möglich ist. Das ist notwendig, um die Leitung über den künstlerischen Proben- und Aufführungsverlauf zu informieren, bzw. die Mitwirkenden über den Stand der Probe/Aufführung, damit sie wissen, wann sie sich wieder zur Bühne begeben müssen. Um diese gängige Praxis auch in Zukunft beibehalten zu können, sollten Aufführungs- und Proberäume von Gebäuden, die der Durchführung öffentlicher Veranstaltungen dienen, von der Regelung des § 32f ausgenommen werden.

11. § 32g - Ortungssysteme

Regelungsgehalt: Ortungssysteme zur Bestimmung eines geographischen Standortes dürfen zur Sicherheit des Beschäftigten oder zur Koordinierung des Einsatzes des Beschäftigten eingesetzt werden. Sie dürfen unter bestimmten Voraussetzungen auch zum Schutz beweglicher Sachen eingesetzt werden.

Die Klarstellung der Zulässigkeit des Einsatzes von geographischen Ortungssystemen ist sinnvoll. Die in der Vorschrift vorgesehenen Einschränkungen sind allerdings zu restriktiv.

Die dort vorgesehene Verhältnismäßigkeitsprüfung ist zu eng, da verlangt wird, dass keine Anhaltspunkte bestehen dürfen, dass schutzwürdige Interessen des Beschäftigten am Ausschluss der Datenerhebung überwiegen. Der Einsatz von Ortungssystemen ist beispielsweise in Logistikunternehmen ein kaum mehr verzichtbares Werkzeug zum wirtschaftlichen Flotteneinsatz. Allein das Bestehen von Anhaltspunkten, dass schutzwürdige Interessen des Arbeitnehmers überwiegen, kann deshalb nicht ausreichend sein, um den Einsatz zu untersagen.

Die Beschränkung der Überwachungszeit auf die Arbeitszeit des Beschäftigten ist abzulehnen. Gerade bei Tätigkeiten, die außerhalb des Betriebs z.B. auf Baustellen ausgeführt werden, besteht oftmals auch außerhalb der regulären Arbeitszeit die

Gefahr, dass Dienstfahrzeuge durch Arbeitnehmer absprachewidrig für eigene Zwecke genutzt werden. Denkbar ist dies insbesondere in den Fällen, in denen dem Arbeitnehmer das Firmenfahrzeug zu dem Zweck überlassen wurde, Baustellen bzw. Kunden direkt von seiner Wohnung aus anzufahren. Hier muss es für den Arbeitgeber kontrollierbar sein, ob der Arbeitnehmer das Fahrzeug nach Feierabend oder vor Arbeitsbeginn nicht unrechtmäßig für private Zwecke einsetzt. Gleiches gilt z.B., wenn der Fahrer in der Fahrerkabine eines Nutzfahrzeugs übernachtet. Der Arbeitgeber könnte nach dem Gesetzestext nicht die Einhaltung der Ruhezeiten überwachen und das Fahrzeug durch das Ortungssystem sichern.

Unklar ist, für welche Zwecke Beschäftigtendaten, die beim Einsatz von Ortungssystemen erhoben werden, genutzt und verarbeitet werden dürfen. Wir gehen davon aus, dass die Koordinierung des Einsatzes von Beschäftigten auch die Kontrolle des Einsatzes erfasst. Dies sollte klargestellt werden. Ansonsten könnte aus der Beschränkung des § 32g Abs. 1 S. 4 geschlossen werden, dass die Nutzung der Daten zur Kontrolle der Vertragserfüllung unzulässig ist. Dies wäre wenig überzeugend. Ortungssysteme müssen auch zur Kontrolle der Vertragserfüllung durch den Arbeitnehmer (z.B. Außendienstmitarbeiter) zulässig sein – zumindest in den Fällen, in denen Ortungssysteme die einzige Kontrollmöglichkeit darstellen und dies ausdrücklich klargestellt wird.

Zudem entsteht durch Absatz 1 weitere Rechtsunsicherheit, da in Satz 4 im Hinblick auf die erlaubte Verarbeitung und Nutzung nur auf Absatz 1 Satz 1, nicht aber auf Absatz 2 verwiesen wird. Ortungssysteme dürfen nach Abs. 2 auch zum Schutz beweglicher Sachen eingesetzt werden, d.h. dass auch insofern die Verarbeitung und Nutzung von Daten zulässig sein müsste. Deshalb muss dies als zulässiger Zweck in Abs. 1 Satz 4 aufgenommen werden.

Unklar ist das Verhältnis zu § 32e. Durch die Pflicht zur Kenntlichmachung von Ortungssystemen gem. § 32g Absatz 1 S. 3 könnte eine Nutzung nach § 32e zur Aufdeckung von Straftaten oder schwerwiegenden Pflichtverletzungen ausgeschlossen sein. Dies wäre nicht akzeptabel. Es ist anerkannt, dass die Ortung weniger eingriffsintensiv ist als andere Grundrechtseingriffe, wie beispielsweise das heimliche Abhören eines Telefonates. Es ist deshalb durchaus berechtigt, die Ortung im Bereich der Arbeitnehmerüberwachung für die Aufklärung von Straftaten und schwerwiegenden Pflichtverletzungen zu verwenden. Im Hinblick auf § 32g Absatz 1 S. 3 ist deshalb klarzustellen, dass § 32e nicht eingeschränkt wird.

Nach Absatz 2 darf der Arbeitgeber Ortungssysteme auch zum Schutz beweglicher Sachen einsetzen, die vom Beschäftigten genutzt werden oder sich in seiner Obhut befinden. Die Ortung darf jedoch nicht erfolgen während der erlaubten Nutzung und der erlaubten Inobhutnahme der Sache. Dies ist mit dem Eigentumsrecht nicht vereinbar und bedarf daher einer Regelung dahingehend, dass es dem Arbeitgeber erlaubt sein muss, ein Ortungssystem einzusetzen, wenn der begründete Verdacht besteht, dass der Arbeitnehmer Eigentum des Arbeitgebers vertragswidrig oder gar zu Straftaten missbraucht.

Weiterhin scheint die geforderte unverzügliche Löschung nach Absatz 3 als zu eng, da die Ortungsdaten ggf. auch für Dokumentationen und Rechtsstreitigkeiten relevant sein können.

12. § 32h – Biometrische Verfahren

Regelungsgehalt: Biometrische Daten dürfen grundsätzlich nur zu Autorisierungs- und Authentifikationszwecken genutzt werden.

Es muss klargestellt werden, dass bei einer Nutzung der biometrischen Daten zu Autorisierungs- oder Authentifikationszwecken bei Zugangsberechtigungssystemen die üblicherweise mit Zugangserfassungssystemen verbundenen Daten erhoben und im Rahmen des § 32d genutzt werden können. So werden Zugangskontrollsys-

teme zu Räumen oder Daten und Diensten auch häufig als Zeiterfassung genutzt. Es muss sichergestellt sein, dass die so erhobenen Zeiterfassungsdaten nicht unter § 32h fallen, sondern entsprechend § 32d genutzt und verarbeitet werden können.

Auch hier muss der Begriff der „Erforderlichkeit“ überdacht werden. So könnte dieser Begriff hier dazu führen, dass eine biometrische Erhebung des Fingerabdrucks für das Einloggen auf einem Laptop nicht möglich ist, wenn gleichzeitig die Möglichkeit besteht, sich über ein Passwort einzuloggen. Das wäre vor dem Hintergrund des häufigen Missbrauchs von Passwörtern sehr bedenklich.

13. § 32i – Nutzung von Telekommunikationsdiensten

Die BDA begrüßt, dass der Gesetzgeber die Nutzung der betrieblichen Telekommunikationsdienste im Arbeitsverhältnis regelt. Derzeit sind bei Nutzung der betrieblichen Telekommunikationsdienste durch die Arbeitnehmer noch viele Fragen nicht abschließend geklärt, so dass eine gesetzliche Regelung, die in der Praxis zu mehr Rechtssicherheit führt, ein Gewinn für die Unternehmen wäre.

Die vorgeschlagene Regelung orientiert sich am Telekommunikationsrecht. Problematisch ist grundsätzlich, dass der Arbeitgeber bei zugelassener Privatnutzung nach wie vor als Diensteanbieter im Sinne des Telekommunikationsrechts angesehen werden kann, da dies im Gesetzestext nicht ausdrücklich ausgeschlossen ist. Hier muss die Chance genutzt werden, sich vom Telekommunikationsrecht – das auch in Terminologie und Systematik nicht auf die Rechtsbeziehung von Arbeitgeber und Arbeitnehmer passt – zu lösen und eine vollständig eigenständige Regelung zu finden.

So wurde bei der Vorratsdatenspeicherung, wie sie in den §§ 113 a TKG geregelt ist, in der Literatur die Frage erörtert, ob auch der Arbeitgeber zur Vorratsdatenspeicherung verpflichtet ist. Dies macht deutlich, dass die Anwendung der Telekommunikationsvorschriften auf das Verhältnis Arbeitgeber – Arbeitnehmer zu Rechtsunsicherheit führt. Auch fehlt es an einer überzeugenden Begründung, warum die Telekommunikationsvorschriften auf den Arbeitgeber Anwendung finden sollen. In der Gesetzesbegründung zum Telekommunikationsgesetz wurde klargestellt, dass beispielsweise Hotels, die eine entsprechende Nebenstellenanlage vorhalten, Diensteanbieter sind (BT-Drs. 13/3609). Dies ist nachvollziehbar, da diese ihren Gästen die Möglichkeit einräumen wollen, das Telefon oder den Zugang zum Internet ohne weitere Einschränkungen zu nutzen. Auch wenn der Arbeitgeber die private Nutzung zulässt, ist die Situation nicht mit dem des Hoteliers, der eine Nebenstellenanlage für seine Gäste vorhält, zu vergleichen.

Zu der Regelung im Einzelnen:

a) Absätze 1 und 3 - ausschließlich dienstliche Nutzung von Telekommunikationsdiensten

Regelungsgehalt: Ist die private Nutzung untersagt, so kann der Arbeitgeber die Verkehrsdaten erheben, verarbeiten und nutzen, wenn dies zur Gewährleistung des ordnungsgemäßen Betriebs des Telekommunikationsdienstes, zu Abrechnungszwecken oder zu stichproben- oder anlassbezogenen Leistungs- oder Verhaltenskontrollen erforderlich ist.

Auf die Inhaltsdaten von E-Mails kann der Arbeitgeber nur zugreifen, wenn dies zur Gewährleistung des ordnungsgemäßen Betriebes des Telekommunikationsdienstes oder zu einer stichprobenartigen oder anlassbezogenen Leistungs- und Verhaltenskontrolle erforderlich ist.

Dies ist zu eng. Für den Zugriff auf dienstliche E-Mails kann es keine Beschränkung geben. Dienstliche E-Mails sind Teil der Arbeitsleistung, als solche auch ggf. nach § 257 HGB zu archivieren. Rein dienstliche E-Mail-Korrespondenz ist auch immer

Korrespondenz des Arbeitgebers. Eine Einschränkung ist deshalb nicht akzeptabel und auch nicht wegen des Fernmeldegeheimnisses geboten. Ist die private Nutzung ausgeschlossen, so ist der Arbeitgeber kein Diensteanbieter i.S.d. Telekommunikationsrechts.

Ebenso ist im Hinblick auf die Erhebung von Verkehrsdaten eine nur auf bestimmte Fallgruppen beschränkte Gestattung nicht akzeptabel. Gerade im Bereich der rein dienstlichen Nutzung muss es dem Arbeitgeber unter anderem möglich sein, Leistungs- und Verhaltenskontrollen durchzuführen; dies schon im Hinblick auch auf die Einhaltung der rein dienstlichen Nutzung. Die anfallenden Daten sind hier alleine Teil der Arbeitsleistung.

Verkehrsdaten müssen auch erhoben werden können, um die wirtschaftliche Nutzung der telefonischen Kommunikationsmittel im Betrieb zu gewährleisten. Unternehmen müssen beispielsweise in der Lage sein, anhand der Verkehrsdaten die telefonische Auslastung von Arbeitnehmern ermitteln zu können, um die Abteilungen entsprechend zu besetzen und ein Kostencontrolling durchzuführen. Auch ist die dauerhafte Erhebung und Auswertung von Verkehrsdaten unverzichtbar, um einer Vereinbarung über variable Vergütung auf Basis von Erreichbarkeitsquoten oder der Anzahl der entgegengenommenen Anrufe durch Ermittlung des Anteils nachkommen zu können. Der Gesetzestext ist auch hier zu eng und muss entsprechend angepasst werden: Hier ist ergänzend klarzustellen, dass die bei der Nutzung von Telekommunikationsdiensten anfallende personenbezogene Daten vom Arbeitgeber erhoben, verarbeitet und genutzt werden dürfen, soweit dies zur Durchführung des ordnungsgemäßen Dienst- und Geschäftsbetriebs und für die Umsetzung von Vergütungsmodellen erforderlich ist

b) Absatz 2 - dienstliche Nutzung von Telefondiensten

Regelungsgehalt: Die Nutzung von Inhaltsdaten ist bei einer rein dienstlichen Nutzung nur zulässig, wenn dies zur Wahrung der berechtigten Interessen des Arbeitgebers erforderlich ist und beide Gesprächspartner im konkreten Einzelfall vorher informiert wurden und eingewilligt haben.

Die Regelung ist im Grundsatz gelungen und entspricht überwiegend der geltenden Rechtslage. Problematisch ist allerdings, dass – entgegen der Rechtsprechung – keinerlei Ausnahmen zulässig sind. Aus den Entscheidungen des BAG und des BVerfG lässt sich entnehmen, dass das heimliche Mithören von Telefonaten zwar grundsätzlich unzulässig ist. Das BAG erkennt jedoch im Grundsatz an, dass Rechtfertigungsgründe vorliegen könnten. In einer notstandsähnlichen Situation ist deshalb ein heimliches Mithören nach geltender Rechtslage zulässig (BAG, 29.06.2004 – 1 ABR 21/03). Bei Anwendung des § 32i nach dem Gesetzentwurf wäre dies nicht mehr zulässig. Entsprechend der geltenden Rechtsprechung muss in Ausnahmefällen auch ein heimliches Mithören von Telefonaten möglich sein.

Eine andere praktische Notwendigkeit ist eine Ausnahmeregelung für innerbetriebliche Notrufnummern, wie beispielsweise bei Werksfeuerwehren. In Notrufzentralen von Werksfeuerwehren werden alle eingehenden Notrufe aus Sicherheitsgründen aufgezeichnet ohne dass zuvor eine gesonderte Einwilligung eingeholt wird. Dies wäre für eine Notfallsituation völlig praxisfern und auch häufig kaum möglich. Insgesamt muss dies für alle sicherheitskritischen Leitstellen und Stellen zur Störungskoordination (z.B. Gasversorgung, Kraftwerke) gelten. Für diese Sonderfälle muss klargestellt werden, dass in diesen Fällen von den Voraussetzungen des § 32i Abs. 2 abgewichen werden kann.

c) Absatz 4 – erlaubte private Nutzung

Regelungsgehalt: Ist die private Nutzung von Telekommunikationsdiensten zugelassen, so kann der Arbeitgeber nach Abschluss der Telekommunikation sowohl die Verkehrsdaten als auch die Inhaltsdaten nur erheben, verarbeiten und nutzen,

wenn dies zur Gewährleistung des ordnungsgemäßen Dienst- und Geschäftsbetriebs unerlässlich ist und er den Beschäftigten hierauf schriftlich hingewiesen hat.

Diese so genannte Mischnutzung ist in der Praxis gängig. Sie ist wegen der zu engen Rechtsprechung z.B. bei Krankheitsfall, Ausscheiden des Mitarbeiters, Zugriffsrecht für andere Arbeitnehmer, aber auch bei der Kontrolle kaum zu handhaben. Vorangestellt werden muss, dass die Unternehmen ihren Mitarbeiter die private Nutzung – im sozialadäquaten Maß – durchaus einräumen wollen. Führt dies allerdings dazu, dass der Zugriff auf geschäftliche E-Mails wegen der verfehlten Anwendung der telekommunikationsrechtlichen Vorschriften gesperrt ist oder ansonsten bestehende Kontrollmöglichkeiten entfallen, muss der Arbeitgeber hier zum Schutz seiner berechtigten Interessen die private Nutzung untersagen. Eine Regelung der „Mischnutzung" muss deshalb sicherstellen, dass der Zugriff auf geschäftliche Korrespondenz und die Kontrollmöglichkeiten nicht eingeschränkt wird. Zudem sollte klargestellt werden, dass der Arbeitgeber befugt ist, zu Abrechnungszwecken Daten zu erheben, zu nutzen und zu verarbeiten.

Darüber hinaus muss geklärt werden, ob und in welchem Ausmaß noch eine Missbrauchskontrolle bei übermäßiger privater Nutzung oder Versendung strafrechtlich relevanten Materials möglich ist. Dies ist vor dem Hintergrund, dass der Arbeitgeber bei erlaubter privater Nutzung als Diensteanbieter im Sinne des Telekommunikationsrechts angesehen werden muss, fraglich. Auch wenn man davon ausgeht, dass in den vorliegenden Fällen § 100 Abs. 3 TKG einschlägig ist, ist dies wenig überzeugend. Eine Missbrauchkontrolle nach § 100 Abs. 3 TKG muss der Bundesnetzagentur angezeigt werden. Dies ist völlig ungeeignet für die Situation im Arbeitsverhältnis, da es um Vertragsverletzungen in einem Vertrauensverhältnis geht. Zudem wäre dies in der Praxis insbesondere für kleinere und mittlere Unternehmen kaum handhabbar. Dies ist ein Bespiel dafür, dass die Diensteanbieterschaft des Arbeitgebers nicht praktikabel ist.

Nach § 32l ist eine Einwilligung nur noch in gesetzlich vorgesehenen Fällen möglich, wurde aber für die Mischnutzung nicht eingeräumt. Dies ist kontraproduktiv. Für den Fall der Mischnutzung muss eine Einwilligung des Arbeitnehmers in die Datenverarbeitung nach wie vor möglich sein. Die Einwilligung in die private Nutzung war bisher immer anerkannt, da keine Zwangssituation besteht, da der Arbeitnehmer auch auf die private Nutzung verzichten kann.

14. § 32j – Unterrichtungspflichten

Regelungsgehalt: Stellt ein Arbeitgeber Verletzungen der aufgeführten Regelungen fest, so muss er dies unverzüglich den Betroffenen mitteilen, bei schwerwiegenden Verstößen auch der Aufsichtsbehörde.

Die Vorschrift trifft eine schärfere Sonderregelung gegenüber dem im letzten Jahr eingefügten neuen § 42a BDSG und verweist zudem auf dessen Sätze 3 bis 4 und 6.

Die Verschärfung ist abzulehnen. Eine Unterrichtungspflicht sollte gegenüber dem Arbeitnehmer nur bestehen, wenn ihm Nachteile drohen. Da ein Verstoß gegen § 32j auch durch eine Ergänzung des § 43 als Ordnungswidrigkeit sanktioniert wird, kann in Fällen, in denen ein Verstoß gegen eine materielle Vorschrift vorliegt, die der Arbeitgeber nicht gemäß § 32j meldet, eine doppelte Sanktion greifen. Vor diesem Hintergrund und angesichts des § 42a, der diesen Bereich bereits regelt, sollte § 32j gestrichen werden.

15. § 32l – Einwilligung, Beschwerderecht, Unabdingbarkeit

a) Absatz 1

Regelungsgehalt: Nach § 32l Absatz 1 ist die Erhebung, Verarbeitung und Nutzung von Arbeitnehmerdaten durch den Arbeitgeber auf Grund einer individuellen Einwil-

ligung des Arbeitnehmers abweichend von § 4 Absatz 1 BDSG nur zulässig, soweit dies in den Vorschriften des neuen Unterabschnitts ausdrücklich vorgesehen ist.

Die Einschränkung der Einwilligung ist nicht akzeptabel. Die Einwilligung ist wegen der Möglichkeit des Widerrufs bereits heute nicht die wichtigste Rechtsgrundlage für die im Beschäftigungsverhältnis erforderliche Datenverarbeitung. Sie ist aber unersetzlich für Datenverarbeitungen, die auf freiwilligen Leistungen im engen und weiteren Sinne des Arbeitgebers beruhen. Solche Leistungen für die Arbeitnehmer anzubieten, kann für Arbeitgeber gerade vor dem Hintergrund der demographischen Entwicklung zur Rekrutierung, Motivation und Bindung der Arbeitnehmer ein wesentlicher Aspekt sein. In einem Unternehmen beispielsweise, das vielfältige Möglichkeiten der Inanspruchnahme von Leistungen bietet (z.B. in Vereinen, Restaurantbetrieben, Sozialeinrichtungen wie Kindergärten, die jeweils eigene Rechtspersönlichkeiten darstellen können), kann es zudem im Interesse der jeweiligen Mitarbeiter liegen, durch Einwilligung die Verarbeitung und Nutzung ihrer personenbezogenen Daten freizugeben. Diese Interessen dürfen nicht unnötig beschränkt werden.

Darüber hinaus muss bedacht werden, dass bisher die Einwilligung des Arbeitnehmers die rechtssichere Möglichkeit war, mit Gesundheitsdaten im Rahmen des betrieblichen Eingliederungsmanagements nach § 84 Absatz 2 SGB IX umzugehen. Die Einwilligung des Arbeitnehmers muss auch in Zukunft möglich sein. Ein Wertungswiderspruch zwischen dem SGB IX und dem BDSG darf den Arbeitgeber nicht der Gefahr aussetzen, sich ordnungswidrig zu verhalten.

Die jetzt vorgesehene Regelung, dass die Einwilligungsmöglichkeit nur ausnahmsweise besteht, muss umgekehrt werden in ein Regel-Ausnahme-Verhältnis, nach dem die Einwilligung immer möglich ist, es sei denn, sie wird im Einzelfall ausdrücklich ausgeschlossen. Es muss zudem klargestellt werden, dass Einwilligungsmöglichkeiten aufgrund anderer Gesetze (z.B. zum betrieblichen Eingliederungsmanagement) bestehen bleiben.

In jedem Fall muss klargestellt werden, dass zumindest eine Betriebsvereinbarung die Einwilligung als Rechtsgrundlage festschreiben kann. Zumindest sollte zwischen „normalen“ Mitarbeitern und dem Management differenziert werden, wie dies auch im Arbeitsrecht geschieht und das Management, wie leitende Angestellte, vom Anwendungsbereich des § 4 Absatz 1 ausgenommen werden.

b) Absatz 4

Regelungsgehalt: Der Arbeitnehmer erhält ein Beschwerderecht bei der Aufsichtsbehörde.

Bereits heute kann der Betroffene sich jederzeit mit einer Eingabe an die Aufsichtsbehörde wenden. Deshalb ist die o.g. Regelung nicht erforderlich und sollte gestrichen werden.

c) Absatz 5

Regelungsgehalt: Die Möglichkeit zum Abschluss von Kollektivvereinbarungen wie u. a. Betriebs- und Dienstvereinbarungen wird durch § 32l Absatz 5 des Entwurfs faktisch ausgeschlossen, da von den Vorschriften zum Arbeitnehmerdatenschutz nicht zu Ungunsten der Arbeitnehmer abgewichen werden kann.

Der Abschluss von Betriebsvereinbarungen zum Arbeitnehmerdatenschutz muss weiterhin eine Grundlage für die Erhebung, Nutzung und Verarbeitung von Daten sein können, auch wenn in einer solchen Betriebsvereinbarung teilweise von gesetzlichen Vorgaben abgewichen wird. Bislang wurden Betriebsvereinbarungen von Arbeitgebern und Arbeitnehmervertretern auch genutzt, um Rechtsunsicherheiten zu begegnen. Nachdem der Gesetzentwurf viele unbestimmte Rechtsbegriffe und andere Regelungen enthält, die zu Rechtsunsicherheit führen können, muss auch

weiterhin durch Betriebsvereinbarungen diese Unsicherheit unbeschränkt ausgeräumt werden können. Das gilt umso mehr, als auch der Begriff „zu Ungunsten“ ein unbestimmter Rechtsbegriff ist, der viele Fragen aufwirft. So müssten Arbeitgeber und Betriebsrat im konkreten Fall beurteilen, ob zum Beispiel eine zur gesetzlichen Regelung alternative Vorgabe eine Regelung zu Ungunsten des Arbeitnehmers ist. Das ist in der Praxis nicht zu leisten. Gleiches gilt für den Abschluss von Tarifverträgen. § 32l Abs. 5 sollte gestrichen werden.

16. Weiterer Klarstellungs- und Regelungsbedarf

a) Datenaustausch im Konzern

Der Gesetzentwurf sieht keine Regelung der Erleichterung des Datenverkehrs im Konzern vor.

Die nunmehr angestrebte bereichsspezifische Regelung zum Datenschutz bietet die Möglichkeit, eine auf Beschäftigtendaten beschränkte Regelung aufzunehmen. Diese sollte die Rechtsunsicherheit bei der Abgrenzung der Auftragsdatenverarbeitung von der Funktionsübertragung beseitigen und auch für Konzerne ohne Betriebsrat sowie für die leitenden Angestellten eine sinnvolle Möglichkeit schaffen, bei einer konzerninternen Bündelung von Aufgaben die Voraussetzung für eine Übermittlung zu schaffen. Dies muss auch für Konzernunternehmen mit Sitz der Konzernmutter im Ausland gelten. Bei der Überarbeitung der entsprechenden europarechtlichen Vorgaben sollte dieser Aspekt berücksichtigt werden.

Eine Regelung könnte wie folgt aussehen: Zumindest im Unterordnungskonzern muss eine Möglichkeit für die Weitergabe der Beschäftigtendaten der Tochter an die Mutter geschaffen werden. Dies entspricht der häufigen Praxiskonstellation, dass die Personalverwaltung einheitlich bei der Muttergesellschaft stattfindet. Verantwortlich für die Einhaltung der Vorschriften des Bundesdatenschutzgesetzes wäre die Konzernmutter. Der Arbeitnehmer wäre über die Weitergabe zu informieren. Zusätzlich müsste die Möglichkeit der Datenweitergabe zwischen Töchtern oder von der Muttergesellschaft an eine andere Tochtergesellschaft geregelt werden. Für Konzerne nach § 18 AktG muss die Möglichkeit eröffnet werden, die Daten von Tochter zu Tochter oder auch von der Muttergesellschaft an eine andere Tochter weiterzugeben. Der so entstehende weitergehende Datenfluss muss, um die datenschutzrechtlich notwendige Transparenz zu gewährleisten, verfahrensrechtlich anders abgesichert sein. Hier ist eine an § 11 BDSG angelehnte Gestaltung denkbar. Danach wäre der Vertragsarbeitgeber bei einer Verarbeitung von Daten durch ein anderes Konzernunternehmen für die Einhaltung der Vorschriften dieses Gesetzes verantwortlich – ähnlich wie bisher bei der Auftragsdatenverarbeitung. Hier kann, ähnlich wie in § 11 BDSG, verlangt werden, dass eine Vereinbarung zwischen den Unternehmen abgeschlossen wird, die sicherstellt, dass die entsprechenden Verfahrensanforderungen eingehalten werden, wobei jedoch nicht dieselben Kontrollpflichten ausgelöst werden dürfen.

b) Verhältnis zu Vorschriften aus anderen Gebieten des Arbeitsrechts

In den Unternehmen treten immer wieder Fälle auf, in denen arbeitsrechtliche und datenschutzrechtliche Pflichten kollidieren. Das daraus für die Unternehmen entstehende Dilemma ist nicht tragbar und bedarf vor dem Hintergrund der Einheit der Rechtsordnung einer dringenden Klärung. Eine solche Kollision ist zum Beispiel gegeben, wenn im Rahmen eines betrieblichen Eingliederungsmanagements der Betriebsrat vor der Einwilligung des Arbeitnehmers auf die Arbeitnehmerdaten zugreifen will und die Einigungsstelle dem Arbeitgeber eine entsprechende Verpflichtung auferlegt hat, während der Datenschutzbeauftragte die Weitergabe von Daten ohne Einwilligung als rechtswidrig ansieht. Problematisch ist zum Beispiel auch der Fall, in dem einem Arbeitnehmer wegen einer negativen Gesundheitsprognose gekündigt wurde und im anschließenden Kündigungsschutzprozess das Arbeitsgericht die Kündigung für rechtswidrig erklärt, weil der Arbeitgeber nicht nach evtl. geplan-

ten Rehamaßnahmen des Arbeitnehmers gefragt hat, obwohl dies datenschutzrechtlich nicht erlaubt ist.

c) Auftragsdatenverarbeitung

Die Auftragsdatenverarbeitung ist für viele kleine und mittlere Unternehmen eine rechtssichere Lösung, um den zahlreichen bürokratischen Pflichten, z.B. im Bereich der Entgeltabrechnung, nachzukommen. Die Anforderungen an die Auftragsdatenverarbeitung wurden mit der am 1. September 2009 in Kraft getretenen Änderung des § 11 BDSG bereits erheblich verschärft. Im Rahmen einer Neuregelung müssen deshalb mögliche Vereinfachungen geprüft werden. Bereits das Schriftformerfordernis stellt für die Praxis ein erhebliches Problem dar. Hier sollte als erster Entlastungsschritt zumindest die Möglichkeit der Textform nach § 126b BGB vorgesehen werden.

d) Sanktionslisten

Es fehlt bislang eine Aussage im Hinblick auf den Abgleich von Arbeitnehmerdaten mit den Sanktionslisten der so genannten Terrorismus-Verordnungen. Im Einführungserlass der Dienstanweisung „Zugelassener Wirtschaftsbeteiligter – AEO“ stellt das Bundesfinanzministerium klar, dass nach Auffassung der Bundesregierung ein Abgleich von Mitarbeiterdaten mit diesen Sanktionslisten datenschutzrechtlich zulässig ist. Diese Feststellung sollte klarstellend in die Regelungen zum Arbeitnehmerdatenschutz aufgenommen werden.

Entwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis (Beschäftigtendatenschutzgesetz – BDatG) (BT-Drs. 17/69)

(Fraktion der SPD)

Allgemein

Der Gesetzentwurf verfehlt die dringend notwendige Förderung der Rechtssicherheit und trägt zudem zu mehr Bürokratie im Arbeitsrecht bei. Nicht akzeptabel ist die Ausweitung der Mitbestimmungsrechte des Betriebsrats. Der Datenschutz soll das Persönlichkeitsrecht des Arbeitnehmers stützen. Er dient nicht dazu, Mitbestimmungsrechte auszuweiten.

Die wichtigsten Kritikpunkte

1. § 4 – Zulässigkeit der Datenerhebung und Datenverwendung

Regelungsgehalt: Der Gesetzentwurf soll als Spezialgesetz nur das Erheben und Verwenden von Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses regeln.

Selbst wenn man ein Arbeitnehmerdatenschutzgesetz befürworten würde, wäre dies nur sinnvoll, wenn sämtliche für das Arbeitsverhältnis geltenden datenschutzrechtlichen Vorschriften zusammengefasst würden. Mehr Rechtssicherheit und Rechtsklarheit würde nur dann erreicht, wenn das BDSG und andere datenschutzrechtlichen Vorschriften, z.B. im TKG, im Zusammenhang mit dem Arbeitsverhältnis durch das Beschäftigtendatenschutzgesetz vollständig ersetzt würden.

2. § 6 – Datenerhebung im Einstellungsverfahren

Regelungsgehalt: Festgelegt wird, dass Beschäftigtendaten unmittelbar beim Bewerber, bei Dritten nur mit Einwilligung des Bewerbers eingeholt werden dürfen und diese auch nur im Rahmen der Erforderlichkeit für die Eignung des Bewerbers erhoben werden dürfen, verbunden mit einer zusätzlichen Einschränkung des Fragerechts des (potentiellen) Arbeitgebers. Auch wird in Absatz 6 eine Kostenerstattungspflicht für den Arbeitgeber gegenüber dem Bewerber für das Vorstellungsgespräch begründet.

In erster Linie betreffen diese Regelungen arbeitsrechtliche und nicht originär datenschutzrechtliche Regelungen. Gerade das mit dem Gebot der unmittelbaren Datenerhebung einhergehende Verbot von Internetrecherchen, in denen der Arbeitnehmer seine Daten freiwillig und eigenverantwortlich preisgibt, wird die eigentliche Auswahl des Bewerbers immer mehr in die Probezeit verlagert. Es liegt nicht im Interesse gut qualifizierter Bewerber, wenn der Arbeitgeber weniger qualifizierte Bewerber einstellt, weil ihm gängige Erkenntnisquellen versperrt sind.

BDA BDI

3. § 8 – Datenerhebung nach Begründung des Beschäftigungsverhältnisses

Regelungsgehalt: Festgelegt wird, dass die Datenerhebung durch den Arbeitgeber zulässig ist, wenn dies zu dessen Durchführung, Beendigung und Abwicklung erforderlich ist. Dazu werden Regelbeispiele gegeben, in denen Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses erhoben werden dürfen.

Diese Regelung führt zu Rechtsunsicherheiten, die über die Rechtsunsicherheiten auf Grund des bestehenden § 32 BDSG noch hinausgehen. Hierzu trägt beispielsweise die Vorschrift des Abs. 6 bei, wonach bei Datenerhebung die Zwecke, für die die Beschäftigtendaten erhoben werden, konkret festzulegen sind und die Datenerhebung einer Verhältnismäßigkeitskontrolle zu unterziehen ist. Aus der Begründung wird nicht deutlich, wie diese Zweckbestimmung vorgenommen werden muss und was daraus bei berechtigten Zweckänderungen folgt. Die Zulässigkeit der Datenerhebung setzt nach § 8 voraus, dass der Arbeitgeber eine gesetzliche oder sonstige Pflicht damit erfüllt. Es bleibt offen, ob auch die Erfüllung von Obliegenheiten durch den Arbeitgeber hiervon umfasst ist, beispielsweise bei der Durchführung eines betrieblichen Eingliederungsmanagements.

4. § 11 Opto-elektronische Einrichtungen (Videoüberwachung)

Regelungsgehalt: Die offene Videoüberwachung auf dem Betriebsgelände wird dergestalt eingeschränkt, dass sie nur zu ganz bestimmten Zwecken zulässig sein soll. Auch die zielgerichtete Videoüberwachung wird an sehr enge Voraussetzungen, wie das Vorliegen tatsächlicher Anhaltspunkte für den Verdacht einer Straftat geknüpft.

Die an § 6b BDSG angelehnte Regelung zur Videoüberwachung stellt ähnlich wie § 32 Abs. 1 Satz 2 BDSG zu hohe Anforderungen an deren Zulässigkeit. Die offene Videoüberwachung darf nicht an konkrete Vorgaben gekoppelt werden, sondern muss den betriebsspezifischen Gegebenheiten und Erfordernissen angepasst werden können. Auch vor dem Hintergrund, dass die Anforderungen an die Unternehmen Korruptionsbekämpfung sicherzustellen, ständig zunehmen und auf der anderen Seite die Anforderungen der Rechtsprechung an den Arbeitgeber bei verhaltensbedingter Kündigung und Verdachtskündigung gestiegen sind, muss eine Überwachung weiterhin möglich bleiben. Bei einer Verdachtskündigung muss der Arbeitgeber beispielsweise nachweisen, dass er alles ihm Mögliche unternommen hat, um die Angelegenheit aufzuklären. Diese hohen Anforderungen müssen ihre Entsprechung in den Möglichkeiten der Kontrolle finden.

5. § 12 Ortungssysteme

Regelungsgehalt: Die Möglichkeit des Einsatzes von Ortungssystemen (GPS) wird durch die Regelung des § 12 erheblich eingeschränkt, indem deren Einsatz auf die Erforderlichkeit für die Sicherheit der Beschäftigten und der Koordinierung der Einsätze beschränkt wird.

Die Möglichkeit des Einsatzes von Ortungssystemen, soweit dies erforderlich zur Sicherheit der Beschäftigten oder zur Koordinierung eines wechselnden Einsatzes der Beschäftigten ist, reicht nicht aus. In Tätigkeitsbereichen, in denen die Überwachung durch Ortungssysteme die einzige Möglichkeit ist, die Einhaltung von gesetzlichen und arbeitsvertraglichen Pflichten zu überprüfen, muss diese Überwachungsmöglichkeit genutzt werden können. Andernfalls würde auch hier die notwendige Gewährleistung von Compliance und Kriminalitätsbekämpfung behindert.

6. § 14 – Telekommunikationsdienste

Regelungsgehalt: Hiernach soll die Nutzung von Telefon, E-Mail, Internet oder anderen Telekommunikationsdiensten durch Vereinbarung mit dem Arbeitgeber geregelt werden können. Wird keine Vereinbarung getroffen, so soll die private Nutzung als erlaubt gelten. Daneben werden die Erhebungsrechte des Arbeitgebers von

Verkehrsdaten auch bei rein dienstlicher Nutzung nur für bestimmte Zwecke erlaubt, bei privater Nutzungserlaubnis noch weiter beschränkt.

Die Regelung des Abs. 1, wonach die Nutzung von Telefon, E-Mail, Internet oder anderen Telekommunikationsdiensten durch Vereinbarung mit dem Arbeitgeber geregelt werden kann und in dieser Vereinbarung festgelegt werden soll, ob und inwieweit die Nutzung der Telekommunikationsdienste auch zu privaten Zwecken erlaubt ist, beschreibt eine Selbstverständlichkeit, die sich aus allgemeinen Rechtsgrundsätzen ergibt. Der dritte Satz dieses ersten Absatzes bedeutet allerdings eine Abkehr von der bisherigen – von der Rechtsprechung geprägten – Rechtslage. Die Nutzung von Telefon, E-Mail, Internet und anderen Telekommunikationsdiensten zu privaten Zwecken soll als erlaubt gelten, wenn keine Vereinbarung getroffen wird und betriebliche Belange nicht beeinträchtigt werden. Es ist nicht nachvollziehbar, dass die private Nutzung von Betriebsmitteln des Arbeitgebers bei fehlender ausdrücklicher Regelung erlaubt sein soll. Den Eigentumsverhältnissen an diesen Arbeitsmitteln entsprechend müsste die Regelung umgekehrt lauten. Die Einschränkung, dass betriebliche Belange nicht beeinträchtigt werden dürfen, ist wiederum eine Selbstverständlichkeit, die sich aus den arbeitsvertraglichen Pflichten ergibt. Die Vorschrift greift in den grundgesetzlichen Eigentumsschutz des Arbeitgebers ein. Eine generelle Erlaubnis der privaten Nutzung von Informations- und Kommunikationseinrichtungen würde nicht nur das Eigentumsrecht des Arbeitgebers an diesen Einrichtungen empfindliche beeinträchtigen, sondern auch die im Synallagma stehenden arbeitsvertraglichen Pflichten des Arbeitnehmers in Frage stellen. Nutzt der Arbeitnehmer die Informations- und Kommunikationseinrichtungen für private Zwecke, so kann er währenddessen keine Arbeitsleistung erbringen und verstößt damit gegen seine arbeitsvertraglichen Pflichten. Wird eine gesetzliche Regelung zu dem Themenkomplex angestrebt, kann diese nur ein Verbot der privaten Nutzung von Informations- und Kommunikationseinrichtungen des Arbeitgebers mit Erlaubnisvorbehalt vorsehen.

7. § 20 – Einsichtsrecht

Regelungsgehalt: § 20 gibt dem Arbeitnehmer ein umfangreiches Recht zur Einsicht in seine Personalakte sowie zur Abgabe von hierin aufzunehmenden Erklärungen.

Hiermit wird wiederum eine rein arbeitsrechtliche, keine originär datenschutzrechtliche Regelung getroffen. Die Regelung überschneidet sich mit der Regelung des § 83 BetrVG und geht noch über diese hinaus. Ohne eine Klärung des Verhältnisses der Vorschrift des § 20 zu § 83 BetrVG sollte eine solche Doppelregelung nicht vorgenommen werden, weil sie zu zusätzlicher Rechtsunsicherheit und Unübersichtlichkeit führt. Stattdessen sollte allein der bisherige § 83 BetrVG beibehalten werden.

8. § 22 – Korrekturen

Regelungsgehalt: § 22 trifft Regelungen zu Ansprüchen des Arbeitnehmers auf Berichtigung, Entfernung und Sperrung seiner Daten.

Neben einer Anlehnung an § 20 BDSG wird hier auch eine arbeitsrechtliche Regelung zur Entfernung von „in Dateien gespeicherten Missbilligungen“ von Beschäftigten nach Ablauf von drei Jahren geregelt. Aus der Gesetzesbegründung ergibt sich, dass hiermit in erster Linie Abmahnungen gemeint sind. Bisher besteht nach der Rechtsprechung ein solches Recht auf Entfernung einer Abmahnung nur dann, wenn der abgemahnte Pflichtverstoß für das Arbeitsverhältnis bedeutungslos geworden ist. Deshalb ist die Einführung einer fixen Frist für den Entfernungsanspruch

problematisch. Zumindest muss die Frist mit der Bedingung verknüpft werden, dass das missbilligte Verhalten für das Arbeitsverhältnis nicht mehr von Bedeutung ist.

9. § 28 – Bestellung von Beauftragten für den Beschäftigtendatenschutz

Regelungsgehalt: § 28 legt fest, dass neben dem betrieblichen Datenschutzbeauftragten auch ein Beauftragter für den Beschäftigtendatenschutz zu bestellen sein soll.

Die Vorschrift des § 28 macht wiederum deutlich, dass eine Systematik, die ein Beschäftigtendatenschutzgesetz neben das Bundesdatenschutzgesetz stellt, für die Praxis untauglich ist. Sie hat zur Folge, dass zusätzlich zu dem Betrieblichen Datenschutzbeauftragten nach dem BDSG auch noch ein Beschäftigtendatenschutzbeauftragter vom Arbeitgeber zu bestellen ist, sofern er mindestens 5 Beschäftigte hat. Der Betriebliche Datenschutzbeauftragte nach dem Bundesdatenschutzgesetz hat selbstverständlich bereits heute die Aufgabe, über die Rechtmäßigkeit der Verwendung der Daten der Beschäftigten zu wachen. Eine zusätzliche Position ist aufgrund der Aufgaben des Betrieblichen Datenschutzbeauftragten nach dem BDSG überflüssig.

10. § 34 – Unabdingbarkeit, Verzicht, Verwirkung
Regelungsgehalt: Allgemein wird hier festgelegt, dass von den Vorschriften dieses Gesetzes nicht zu Ungunsten der Beschäftigten abgewichen werden kann.

Betriebsvereinbarung und Einwilligung sind zentrale Elemente des Datenschutzes, die durch die Norm ausgehebelt werden. Betriebs- und Privatautonomie werden eingeschränkt. Das ist kontraproduktiv und nicht nachvollziehbar.

Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen (BT-Drs. 17/4853)

(Fraktion BÜNDNIS 90/DIE GRÜNEN)

Allgemein

Der Gesetzentwurf vom 22.02.2011 gewährleistet insbesondere nicht die Rahmenbedingungen für eine gerade auch im Interesse der Belegschaft liegende effektive Kriminalitäts- und Korruptionsbekämpfung. In dem Regelwerk sind zwar teilweise auch praxisorientierte Ansätze enthalten, wie beispielsweise im Hinblick auf die gezielte Videoüberwachung. Der vorgelegte Gesetzentwurf erfüllt insgesamt die Anforderungen an eine sinnvolle und praxisnahe Regelung des Beschäftigtendatenschutzes aber nicht. Im Einzelnen sind nachstehend die wichtigsten Kritikpunkte des Entwurfs dargestellt.

Die wichtigsten Kritikpunkte

1. § 3 – Begriffsbestimmungen

Regelungsgehalt: In § 3 Absatz 4 definiert Beschäftigtendaten als personenbezogene oder personenbeziehbare Daten und Informationen über Angehörige der in § 1 Absatz 1 benannten Beschäftigtengruppen, die in Zusammenhang mit der Anbahnung, Begründung, Durchführung, Beendigung oder Abwicklung eines Beschäftigungsverhältnisses oder für die in diese Gesetz im Einzelnen aufgeführten zulässigen Zwecke verarbeitet werden.

Enthalten ist hier lediglich eine weite Definition des Begriffs des Beschäftigtendatums, nicht allerdings eine Abgrenzung zum Begriff des Geschäftsdatums. Eine Abgrenzung des jeweiligen gesetzlichen Regelungsbereichs ist notwendig, um Geschäftsdaten weiterhin sinnvoll bearbeiten zu können. Daten, die überwiegend dem Geschäftsbetrieb des Arbeitgebers zuzurechnen sind, müssen aus dem regelungsbereich ausgenommen werden.

2. § 4 – Zulässigkeit und Grundsätze der Datenverarbeitung

Regelungsgehalt: Nach Absatz 1 wird die Möglichkeit der Einwilligung auf ausdrücklich im Gesetz geregelte Fälle beschränkt.

Die Möglichkeit der Einwilligung des Beschäftigten in die Erhebung, Verarbeitung und Nutzung seiner Daten muss gewährleistet werden. Schon heute werden strenge Anforderungen an die Freiwilligkeit einer solchen Einwilligung gestellt. Unter diesen Voraussetzungen muss es auch weiterhin möglich sein, mit dem Beschäftigten als „Herr über seine Daten“ einzelfallbezogene und damit praxisgerechte Vereinbarungen zu treffen.

3. § 11 – „Raster-Abgleich“ von Beschäftigtendaten (Screening-Verfahren)

Regelungsgehalt: Die Vornahme eines Abgleichs von Beschäftigtendaten wird auf den Einzelfall beschränkt, soweit und solange konkrete Anhaltspunkte den Verdacht begründen, dass Beschäftigte im Beschäftigungsverhältnis bestimmte Straftaten.

Unternehmen sind gesetzlichen und aufsichtsbehördlichen Anforderungen in Bezug auf Kriminalitäts- und Korruptionsbekämpfung ausgesetzt. Abgleiche von Beschäftigtendaten sind für die Erfüllung dieser Verpflichtungen unverzichtbar.

4. § 12 – Einsatz von Telekommunikationsdiensten

Regelungsgehalt: Im Fall einer privaten Nutzung von Telekommunikationsdiensten dürfen Verkehrsdaten nach § 12 nur unter engen Voraussetzungen und Inhaltdaten gar nicht verarbeitet bzw. ausgewertet werden. Zudem legt § 12 Absatz 1 Satz 3 fest, dass die angemessene private Nutzung von Telekommunikationsdiensten generell erlaubt sein soll, soweit keine anderweitige Vereinbarung vorliegt. Untersagt werden kann die private Nutzung hiernach nur im Rahmen einer individuellen oder Betriebsvereinbarung.

Den Eigentumsverhältnissen an diesen Arbeitsmitteln entsprechend müsste die Regelung genau umgekehrt lauten. Für den Fall, dass keine Regelung getroffen wurde, müsste sie automatisch verboten sein. Die Einschränkung, dass betriebliche Belange nicht beeinträchtigt werden dürfen, ist eine Selbstverständlichkeit, die sich aus den arbeitsvertraglichen Pflichten ergibt. Eine generelle Erlaubnis der privaten Nutzung von Informations- und Kommunikationseinrichtungen würde nicht nur das Eigentumsrecht des Arbeitgebers an diesen Einrichtungen beeinträchtigen, sondern auch die im Synallagma stehenden arbeitsvertraglichen Pflichten des Arbeitnehmers in Frage stellen. Nutzt der Arbeitnehmer die Informations- und Kommunikationseinrichtungen für private Zwecke, so kann er währenddessen keine Arbeitsleistung erbringen und verstößt damit gegen seine arbeitsvertraglichen Pflichten. Wird eine gesetzliche Regelung zu dem Themenkomplex angestrebt, kann diese nur ein Verbot der privaten Nutzung von Informations- und Kommunikationseinrichtungen des Arbeitgebers mit Erlaubnisvorbehalt vorsehen.

Eine Regelung der „Mischnutzung“ muss sicherstellen, dass der Zugriff auf geschäftliche Korrespondenz und die Kontrollmöglichkeiten nicht eingeschränkt wird. Darüber hinaus muss geklärt werden, ob und in welchem Ausmaß eine Missbrauchskontrolle bei übermäßiger privater Nutzung oder Versendung strafrechtlich relevanten Materials möglich ist.

5. § 15 – Einsatz von Ortungssystemen

Regelungsgehalt: Die Möglichkeit des Einsatzes von Ortungssystemen wird durch die Regelung erheblich eingeschränkt, indem deren Einsatz auf die Erforderlichkeit für die Sicherheit des Beschäftigten beschränkt wird.

Gerade im Außendienstbereich muss schon die Koordinierung von Einsätzen anhand der Übermittlung von Daten durch Ortungssysteme möglich sein. Zudem existieren Tätigkeitsbereiche, in denen die Überwachung durch Ortungssysteme die einzige Möglichkeit ist, die Einhaltung von gesetzlichen und arbeitsvertraglichen Pflichten zu überprüfen.

6. § 21 – Korrekturen

Regelungsgehalt: § 21 trifft Regelungen zu Ansprüchen des Arbeitnehmers auf Berichtigung und Löschung seiner Daten. Zudem sollen nach Ablauf von spätestens drei Jahren im nicht-öffentlichen Bereich die in Unterlagen oder Dateien aufgenommene Missbilligungen von Beschäftigten entfernt werden.

Gerade im Hinblick auf die Drei-Jahres-Frist wird hier eine arbeitsrechtliche Regelung getroffen. Aus der Gesetzesbegründung kann geschlossen werden, dass in erster Linie Abmahnungen gemeint sind. Bisher besteht nach der Rechtsprechung ein solches Recht auf Entfernung einer Abmahnung nur dann, wenn der abgemahnte Pflichtverstoß für das Arbeitsverhältnis bedeutungslos geworden ist. Deshalb ist die Einführung einer fixen Frist für den Entfernungsanspruch problematisch. Zumindest muss die Frist mit der Bedingung verknüpft werden, dass das missbilligte Verhalten für das Arbeitsverhältnis nicht mehr von Bedeutung ist.

7. § 28 – Betriebliche Datenschutzbeauftragte

Regelungsgehalt: § 28 beinhaltet eine Erweiterung der Befugnisse der betrieblichen Datenschutzbeauftragten und legt zudem fest, dass die Bestellung des betrieblichen Datenschutzbeauftragten nach § 4 f BDSG der Mitbestimmung des Betriebsrats unterliegen soll.

Diese Regelung bedeutet eine Ausdehnung der Mitbestimmung, die nicht Aufgabe des Datenschutzes ist.

8. § 34 – Unabdingbare Rechte der Beschäftigten

Regelungsgehalt: Der Abschluss von Betriebsvereinbarungen soll zur Regelung der Verarbeitung personenbezogener Daten ausdrücklich erlaubt sein., allerdings nur soweit sie den Schutz der personenbezogenen Daten durch dieses Gesetz nicht einschränken. Gleiches soll für Tarifverträge gelten.

Der Abschluss von Betriebsvereinbarungen zum Arbeitnehmerdatenschutz muss weiterhin eine Grundlage für die Erhebung, Nutzung und Verarbeitung von Daten sein. Wann eine Abweichung „zu Ungunsten“ vorliegt, wirft darüber hinaus weitere Fragen und Rechtsunsicherheiten auf. Ausschlaggebend ist jedoch das Gesamtbild der Betriebsvereinbarung. Die Betriebsparteien müssen in der Lage sein, betriebsspezifische und damit praxisgerechte Vereinbarungen auch und gerade im Bereich des Beschäftigtendatenschutzes zu treffen, um betriebliche rechtssicherheit zu schaffen.