DEUTSCHER BUNDESTAG Ausschussdrucksache 16(11)**1374**
Ausschuss für
Arbeit und Soziales 8. Mai 2009
16. Wahlperiode

Materialien

zur öffentlichen Anhörung von Sachverständigen am 11. Mai 2009 in Berlin zum

a) Antrag der Abgeordneten Brigitte Pothmer, Dr. Thea Dückert, Kerstin Andreae, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Rechte der Beschäftigten von Discountern verbessern - Drucksache 16/9101 -

b) Antrag der Abgeordneten Silke Stokar von Neuforn, Kerstin Andreae, Volker Beck (Köln), weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Persönlichkeitsrechte abhängig Beschäftigter sichern - Datenschutz am Arbeitsplatz stärken - Drucksache 16/9311 -

c) Antrag der Abgeordneten Jan Korte, Wolfgang Neskovic, Sevim Dagdelen, weiterer Abgeordneter und der Fraktion DIE LINKE.

Datenschutz für Beschäftigte stärken - Drucksache 16/11376 -

d) Antrag der Abgeordneten Gisela Piltz, Dr. Heinrich L. Kolb, Jens Ackermann, weiterer Abgeordneter und der Fraktion der FDP

Schutz von Arbeitnehmerdaten durch transparente und praxisgerechte Regelungen gesetzlich absichern - Drucksache 16/12670 -

Zusammenstellung der schriftlichen Stellungnahmen

7. Mai 2009

Deutscher Bundestag
16. Wahlperiode
Ausschuss für Arbeit und Soziales
(11. Ausschuss)

Sekretariat des Ausschusses: ☎32487
Fax: 36030
Sitzungssaal: ☎30269
Fax: 36295

Mitteilung

Tagesordnung

124. Sitzung des
Ausschusses für Arbeit und Soziales
am Montag, den 11. Mai 2009, 12.30 bis 13.30 Uhr
10557 Berlin, Paul-Löbe-Haus, Sitzungssaal 4.900
Vorsitz: Abg. Gerald Weiß (Groß-Gerau)

Einziger Tagesordnungspunkt

Öffentliche Anhörung von Sachverständigen

a) Antrag der Abgeordneten Brigitte Pothmer, Dr. Thea Dückert, Kerstin Andreae, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Rechte der Beschäftigten von Discountern verbessern

(BT-Drucksache 16/9101)

Hierzu Ausschussdrucksachen/BT-Drucksachen: 16(11)1337

Ausschuss für Arbeit und Soziales *(federführend)*
Rechtsausschuss
Ausschuss für Wirtschaft und Technologie
Ausschuss für Ernährung, Landwirtschaft und Verbraucherschutz

b) Antrag der Abgeordneten Silke Stokar von Neuforn, Kerstin Andreae, Volker Beck (Köln), weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Persönlichkeitsrechte abhängig Beschäftigter sichern - Datenschutz am Arbeitsplatz stärken

(BT-Drucksache 16/9311)

Hierzu Ausschussdrucksachen/BT-Drucksachen: 16(11)1337

Ausschuss für Arbeit und Soziales *(federführend)*
Innenausschuss
Rechtsausschuss
Ausschuss für Wirtschaft und Technologie

c) Antrag der Abgeordneten Jan Korte, Wolfgang Neskovic, Sevim Dagdelen, weiterer Abgeordneter und der Fraktion DIE LINKE.

Datenschutz für Beschäftigte stärken

(BT-Drucksache 16/11376)

Hierzu Ausschussdrucksachen/BT-Drucksachen: 16(11)1337

Ausschuss für Arbeit und Soziales *(federführend)*
Innenausschuss
Ausschuss für Wirtschaft und Technologie
Ausschuss für Ernährung, Landwirtschaft und Verbraucherschutz
Ausschuss für die Angelegenheiten der Europäischen Union

d) Antrag der Abgeordneten Gisela Piltz, Dr. Heinrich L. Kolb, Jens Ackermann, weiterer Abgeordneter und der Fraktion der FDP

Schutz von Arbeitnehmerdaten durch transparente und praxisgerechte Regelungen gesetzlich absichern

(BT-Drucksache 16/12670)

Ausschuss für Arbeit und Soziales *(federführend)*
Innenausschuss
Rechtsausschuss
Ausschuss für Wirtschaft und Technologie

Gerald Weiß (Groß-Gerau)
Vorsitzender

Anlage

Sachverständigenliste

- Deutscher Gewerkschaftsbund DGB
- Bundesvereinigung Deutscher Arbeitgeberverbände e.V. BDA
- Berufsverband der Datenschutzbeauftragten e. V. BvD
- Der Bundesbeauftragte für den Datenschutz und
- die Informationsfreiheit BfDI
- Dr. Martin Diller, Stuttgart
- Hans Gliss, Hamburg
- Dr. Ulrike Fleck, Ludwigshafen
- Dr. Thomas Petri, Berlin
- Andreas Jaspers, Bonn
- Karin Schuler, Bonn
- Dr. Gerhard Schäfer, Bonn

DEUTSCHER BUNDESTAG
Ausschuss für
Arbeit und Soziales
16. Wahlperiode

Ausschussdrucksache 16(11)**1365**

6. Mai 2009

Stellungnahme

zur öffentlichen Anhörung von Sachverständigen am 11. Mai 2009 in Berlin zum

a) Antrag der Abgeordneten Brigitte Pothmer, Dr. Thea Dückert, Kerstin Andreae, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Rechte der Beschäftigten von Discountern verbessern - Drucksache 16/9101 -

b) Antrag der Abgeordneten Silke Stokar von Neuforn, Kerstin Andreae, Volker Beck (Köln), weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Persönlichkeitsrechte abhängig Beschäftigter sichern - Datenschutz am Arbeitsplatz stärken - Drucksache 16/9311 -

c) Antrag der Abgeordneten Jan Korte, Wolfgang Neskovic, Sevim Dagdelen, weiterer Abgeordneter und der Fraktion DIE LINKE.

Datenschutz für Beschäftigte stärken - Drucksache 16/11376 -

d) Antrag der Abgeordneten Gisela Piltz, Dr. Heinrich L. Kolb, Jens Ackermann, weiterer Abgeordneter und der Fraktion der FDP

Schutz von Arbeitnehmerdaten durch transparente und praxisgerechte Regelungen gesetzlich absichern - Drucksache 16/12670 -

Deutscher Gewerkschaftsbund DGB

Aktuelle Situation

Der Umgang mit Internet, E-Mail und Mobiltelefonen, Online-Banking, Kreditkarten und Bonuskartensystemen ist in den letzten Jahren für die meisten zur Selbstverständlichkeit geworden. Bequem und schnell wird kommuniziert und gehandelt. Dabei fallen persönliche Daten an, die oft nur unzureichend gegen unrechtmäßige Nutzung und Weitergabe an Dritte gesichert sind.

Im Arbeitsverhältnis werden Chipkarten eingesetzt, die den Zugang der Beschäftigten aufzeichnen, bei der Verwendung von RFID (radio frequency identification) können Tätigkeitsprofile erstellt werden und Handys ermöglichen über GPS (global positioning system) jederzeit die Feststellung, wo sich Beschäftigte befinden. Leistungskontrollen sind über die Benutzerprofile am Computer auch ohne besondere Software möglich. Und nicht zuletzt werden unter dem Stichwort Terrorbekämpfung von staatlichen Stellen über den Arbeitgeber im Rahmen der Sicherheitsüberprüfung Daten z.B. über religiöse Präferenzen oder ethnische Herkunft ermittelt und weitergegeben - sogar an ausländische Stellen und für Daten, die eigentlich dem Persönlichkeitsschutz unterliegen. Zusätzlich entstehen mit Vorhaben wie der elektronischen Gesundheitskarte und dem Verfahren des elektronischen Einkommensnachweises (ELENA) riesige Datensätze, deren Verwendung zwar gesetzlich geregelt ist, die aber durchaus neue Begehrlichkeiten wecken können.

Besondere Gefahren für Beschäftigte

Durch all dies entstehen erhebliche Gefahren. So wurden vonseiten der Landesbeauftragten für den Datenschutz erhebliche verfassungsrechtliche Bedenken gegen den ELENA geäußert. Denn unter staatlicher Verantwortung und Verfügungsmacht werde eine riesige Datensammlung entstehen. Die betroffenen ArbeitnehmerInnen hätten keine Einflussmöglichkeiten. Diese riesige Datensammlung verstieße gegen das verfassungsrechtliche Verbot einer Datenspeicherung auf Vorrat. Es wäre ein unverhältnismäßiger Eingriff in das Grundrecht auf informationelle Selbstbestimmung.

Im Übrigen hat sich gezeigt, dass die persönlichen Daten insbesondere von Beschäftigten, aber auch im allgemeinen Geschäftsverkehr außerordentlich mißbrauchsanfällig sind. Die Vorfälle bei Lidl und anderen Discountern, die die Überwachung von Mitarbeitern bis hin zur Videobeobachtung in Umkleideräumen angeordnet haben, die Telefonbespitzelung bei der Telekom und die Wei-

tergabe der Gewerkschaftsmitgliedschaft im Rahmen des Abkommens zur Datenübermittlung zwischen Deutschland und den USA haben gezeigt, dass die Hemmschwelle, das Persönlichkeitsrecht von Beschäftigten und Bürgern zu verletzen, soweit überhaupt noch vorhanden, zumindest außerordentlich niedrig ist.

Der DGB und seine Mitgliedsgewerkschaften fordern seit Jahren wirksame gesetzliche Regelungen in einem eigenständigen Arbeitnehmerdatenschutzgesetz, die sicherstellen, dass dem Persönlichkeitsrecht der Beschäftigten im Arbeitsverhältnis endlich Rechnung getragen wird. Dabei bedeutet Datenschutz den Schutz personenbezogener und -beziehbarer Daten von Beschäftigten vor Missbrauch.

Notwendigkeit klarer gesetzlicher Regelungen

Zweck des Datenschutzes muss es sein, den Einzelnen davor zu schützen, dass durch Missbrauch seiner Daten eine Beeinträchtigung seines grundrechtlich geschützten Persönlichkeitsrechts erfolgt. Obwohl der Koalitionsvertrag der ersten rot-grünen Regierung ein solches gesetzgeberisches Vorhaben vorsah, ist dieses Vorhaben weder auf nationaler Ebene noch auf europäischer Ebene bislang auch nur ansatzweise verwirklicht worden. Gerade auf Grund der aktuellen Vorfälle ist es deshalb notwendig, die bisherigen Forderungen zu bekräftigen und die Politik aufzufordern, ihrer Verpflichtung, die Grundrechte zu schützen, durch wirksame Gesetze nachzukommen und deren Einhaltung durch wirksame Sanktionen zu gewährleisten.

Die Regelung dieses wichtigen Bereiches darf nicht der Rechtsprechung allein überlassen werden, die nur in der Lage ist, in Einzelfällen zu entscheiden. Zudem kann die Rechtsprechung keine unmittelbare Bindungswirkung im Allgemeinen entfalten. Das informationelle Selbstbestimmungsrecht und das allgemeine Persönlichkeitsrecht müssen im Arbeitsverhältnis geschützt werden.

Insgesamt ist die Forderung nach einem Arbeitnehmerdatenschutzgesetz nach wie vor dringlich. Zurzeit stellt sich die Rechtslage unübersichtlich und unklar dar. Ziel einer eigenständigen gesetzlichen Regelung muss daher auch sein, für Arbeitgeber und Arbeitnehmer klare und möglichst verständliche Regelungen zu schaffen. Die Vorschriften müssen klar strukturiert sein. Der Schutz der Beschäftigten vor unzulässiger Datenerhebung, -verarbeitung und -nutzung könnte so besser in der Praxis durchgesetzt werden, und die Arbeitgeber bekämen den Rahmen aufgezeigt, in dem sie sich legal bewegen können.

Dabei muss ebenfalls klargestellt werden, dass das Datenschutzgesetz einen Minimalstandard regelt, der auch durch Betriebsvereinbarungen nicht unterschritten werden darf.

Forderungen des DGB

1. Die gezielte Beobachtung und Überwachung von Beschäftigten am Arbeitsplatz, aber auch im privaten Umfeld muss ausdrücklich verboten werden. Es muss klargestellt werden, dass weder eine direkte Überwachung durch Beauftragte, Externe noch durch Mitarbeiter oder eine indirekte Überwachung durch Video- oder Tonaufnahmen gerechtfertigt ist. Auch screenings oder scorings müssen grundsätzlich ausgeschlossen sein. Soweit der Schutz von Anlagen eine Überwachung notwendig macht, ist dies durch Betriebsvereinbarung zu regeln. Ebenso wenig kann die Kontrolle der Beschäftigten durch Auswertung oder mit Hilfe computergesteuerter oder biometrischer Systeme erlaubt sein. Nur für den Fall, dass der begründete Verdacht einer strafbaren Handlung, eines Missbrauchs oder einer schwerwiegenden Schädigung des Arbeitgebers besteht, kann auf gesetzlicher Grundlage eine Überwachung im Einzelfall zulässig sein. Die Anordnung einer solchen Überwachung bedarf jedoch immer der Zustimmung der betrieblichen Interessenvertretung. Ebenso kann ausnahmsweise die Überwachung aufgrund höherrangiger Interessen wie der Sicherheit und der Gesundheit der Bevölkerung (z. B. bei der Überwachung von Atomkraftwerken) gerechtfertigt sein. Dann muss der Eingriff in das Persönlichkeits-recht der Beschäftigten so gering wie möglich gehalten werden.
2. Bei elektronischer Datenverarbeitung ist eine besondere Schutzbedürftigkeit in Bezug auf das allgemeine Persönlichkeitsrecht gegeben, da im Hinblick auf die Vielzahl und die Qualität der verwendeten Daten, die Kombinations- und Auswertungsmöglichkeiten, den Kontextverlust und die zeitlich unbegrenzte Verfügbarkeit besondere Risiken bestehen. Um der strukturellen Unterlegenheit von Beschäftigten Rechnung zu tragen, kann deshalb das grundsätzliche Verbot des Zugriffs auf personenbezogene oder beziehbare Nutzerdaten bei der Verwendung moderner Kommunikationsmittel durch den Arbeitgeber auch nicht durch eine generelle Einwilligung des Arbeitnehmers ausgeschlossen werden. Durch gesetzliche Regelungen kann die Datenerfassung durch Arbeitgeber aus dringenden betrieblichen Gründen für bestimmte Fälle vorgesehen werden.
3. Das Fragerecht des Arbeitgebers bei der Einstellung und die Möglichkeit der Anordnung von ärztlichen Untersuchungen muss gesetzlich auf die Fälle beschränkt werden, die die Rechtsprechung bislang vorsieht. Das bedeutet, dass nur die Fragen bei der Einstellung zulässig sind, die für die konkrete Tätigkeit von entscheidender Bedeutung sind. Ebenso darf nur dann eine ärztliche Untersuchung angeordnet werden, wenn dies ausdrücklich gesetzlich geregelt ist (z. B. im Jugendarbeitsschutzgesetz). Verboten werden muss, dass der Arbeitgeber die Ergebnisse ärztlicher Untersuchungen entgegennimmt oder verwendet, insbesondere im Zusammenhang mit Pflichtverletzungen aus dem Arbeitsvertrag. Dies muss im besonderen Maße für Genomanalysen gelten.

   Für Drogen- und Alkoholtests muss gelten, dass ihre Durchführung weder angeordnet, noch die Ergebnisse entgegengenommen werden dürfen, es sei denn, es liegt ein begründeter Verdacht des Drogen- und Alkoholmissbrauchs vor und der Beschäftigte hat in den Test eingewilligt. Außerdem muss vor Anordnung aller Untersuchungen die Zustimmung des Betriebsrates vorliegen.
4. Sofern Beschäftigte gleichzeitig auch Kunden ihres Arbeitgebers sind, wie dies z.B. bei Banken, Versicherungen oder auch in Krankenhäusern häufig der Fall ist, muss sicher gestellt werden, dass die den Kundenbereich betreffenden Daten gesondert geführt und geschützt werden. Insbesondere muss gewährleistet sein, dass die personalverantwortliche Stelle auf die Daten nicht zugreifen kann.

5. Sofern Arbeitnehmer interne Daten über schwerwiegende Rechtsverstöße des Arbeitgebers, die geeignet sind, Gesundheit oder Leben der Beschäftigten oder der Allgemeinheit zu gefährden, wie zum Beispiel bei den Fleisch- oder Schwarzgeldskandalen der jüngsten Vergangenheit an staatliche Stellen weiterleiten müssen sie vor Repressalien durch den Arbeitgeber geschützt werden. Dies kann dadurch erfolgen, dass das Recht zur Weitergabe ausdrücklich geregelt wird, mit der Folge, dass dieses Recht dann dem Maßregelungsverbot unterliegt.
6. Erlaubte Datenerhebung muss diskriminierungsfrei erfolgen, unrechtmäßig erworbene Daten müssen einem Beweisverwertungsverbot unterliegen.
7. Die Rechtsposition des betrieblichen Datenschutzbeauftragten muss verbessert werden. Dazu kommt in Betracht, dass er, wie Betriebsräte auch, vor Kündigungen geschützt wird. Zudem müssen die Mitbestimmungsrechte der Betriebsräte beim Datenschutz gestärkt werden.
8. Die Einhaltung der gesetzlichen Bestimmungen kann nur dann gewährleistet werden, wenn die alleinige Last der Durchsetzung ihrer Rechte durch Klage von den betroffenen Beschäftigten genommen wird. Die Erfahrung zeigt, dass Arbeitnehmer im bestehenden Beschäftigungsverhältnis in der Regel nicht gegen den Arbeitgeber klagen können. Zu groß ist die Gefahr von Repressalien bis hin zur Kündigung.

   Deshalb reicht es nicht aus, dass gesetzlich ein so genanntes Maßregelungsverbot vorgesehen wird, d. h., dass dem Arbeitgeber verboten wird, Beschäftigte wegen der Wahrnehmung ihrer Ansprüche aus einem Arbeitnehmerdatenschutzgesetz zu benachteiligen. Vielmehr muss ein Verbandsklagerecht vorgesehen werden.
9. Um den gesetzlichen Regelungen auch tatsächlich Wirkung zu verleihen, sind angemessene und abschreckende Sanktionen vorzusehen. Zum einem muss demjenigen, dessen Persönlichkeitsrecht verletzt worden ist, ausdrücklich ein konkreter Anspruch auf Schmerzensgeld in Form einer Entschädigung, entsprechend der Entschädigungsregelung in § 15 AGG bei Verstoß gegen das Diskriminierungsverbot, zugebilligt werden. Dieser Entschädigungsanspruch kann entweder direkt für bestimmte Verstöße die Höhe der Entschädigung regeln oder die gesetzliche Regelung muss den abschreckenden Charakter einer solchen Entschädigungszahlung ausdrücklich hervorheben. Darüber hinaus muss die Verletzung des allgemeinen Persönlichkeitsrechts strafbewehrt werden. Die bloße Ordnungswidrigkeit reicht angesichts der rechtsverneinenden Praxis der Arbeitgeberseite nicht aus.
10. Bei Verfahren wie der elektronischen Gesundheitskarte und ELENA muss zwingend sichergestellt werden, dass die persönlichen Daten der Betroffenen vor unbefugtem Zugriff geschützt sind und nur in Kenntnis und mit Zustimmung der Betroffenen verwendet werden können. Solange daran Zweifel bestehen, muss die Verwendung ausgeschlossen sein.
11. Das Bundesdatenschutzgesetz muss den heutigen technischen Gegebenheiten des Internets angepasst werden. Im Falle einer Datenverarbeitung im Auftrag müsste im § 11 BDSG dahingehend präzisiert werden, dass für die in Auftrag gegebene Datenverarbeitung und die zu treffenden technisch-organisatorischen Maßnahmen ein Vertrag abzuschließen ist und welchen Mindestanforderungen er entsprechen sollte. Die Nutzung muss dokumentiert werden. Außerdem wird der Sanktionsrahmen weder im Bereich des Ordnungswidrigkeitenrechts noch im Strafrecht vollständig ausgeschöpft. Deshalb sollten Verstöße gegen das Bundesdatenschutzgesetz Offizialdelikte statt Antragsdelikte sein.
12. Beim europäischen Datenfluss im Zusammenhang mit Migration ist unbeschadet der Einführung angemessener Instrumente des Datenschutzes auf Behördenebene darauf zu achten, dass die dort gewonnenen Daten möglichst vor dem Zugriff durch Arbeitgeber geschützt sind.

DEUTSCHER BUNDESTAG
Ausschuss für
Arbeit und Soziales
16. Wahlperiode

Ausschussdrucksache 16(11)**1373**

8. Mai 2009

Stellungnahme

zur öffentlichen Anhörung von Sachverständigen am 11. Mai 2009 in Berlin zum

a) Antrag der Abgeordneten Brigitte Pothmer, Dr. Thea Dückert, Kerstin Andreae, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Rechte der Beschäftigten von Discountern verbessern - Drucksache 16/9101 -

b) Antrag der Abgeordneten Silke Stokar von Neuforn, Kerstin Andreae, Volker Beck (Köln), weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Persönlichkeitsrechte abhängig Beschäftigter sichern - Datenschutz am Arbeitsplatz stärken - Drucksache 16/9311 -

c) Antrag der Abgeordneten Jan Korte, Wolfgang Neskovic, Sevim Dagdelen, weiterer Abgeordneter und der Fraktion DIE LINKE.

Datenschutz für Beschäftigte stärken - Drucksache 16/11376 -

d) Antrag der Abgeordneten Gisela Piltz, Dr. Heinrich L. Kolb, Jens Ackermann, weiterer Abgeordneter und der Fraktion der FDP

Schutz von Arbeitnehmerdaten durch transparente und praxisgerechte Regelungen gesetzlich absichern - Drucksache 16/12670 -

Bundesvereinigung der Deutschen Arbeitgeberverbände e.V. BDA

A) Zusammenfassung

Der Datenschutz ist in Deutschland hoch entwickelt. Deutschland verfügt über ein auch im internationalen Vergleich hohes Datenschutzniveau. Dies gilt im Verhältnis des Bürgers zum Staat, es gilt ebenso für das Verhältnis der Bürger untereinander, insbesondere auch für das Arbeitsverhältnis. Vor dem Hintergrund dieses auch im europäischen Umfeld hohen Niveaus des Datenschutzes haben auch Kommission und Rat der Europäischen Union ihr Vorhaben aufgegeben, eine eigenständige Richtlinie für den Arbeitnehmerdatenschutz zu entwickeln.

Allerdings ist auch im Datenschutz nicht alles klar und eindeutig geregelt. Die Vorschriften für den Datenschutz finden sich außerhalb des Bundesdatenschutzgesetzes wie auch innerhalb des Bundesdatenschutzgesetzes an verschiedenen Stellen und könnten im Einzelfall klarer und besser aufeinander abgestimmt sein. Hier könnte durch eine Novellierung des Datenschutzrechts mehr Klarheit geschaffen werden. Insbesondere aktuelle Rechtsfragen, die Arbeitgeber und Arbeitnehmer betreffen wie der Datenaustausch im Konzern oder mit dem nicht europäischen Ausland, könnten so einer Klärung zugeführt werden.

Ein ausgewogener Datenschutz im Arbeitsverhältnis ist sinnvoll. Ein solcher Datenschutz muss die Vertraulichkeit der Daten und Geschäftsgeheimnisse von Arbeitgeber und Arbeitnehmer wahren. Ein ausgewogener Datenschutz muss gleichzeitig sicherstellen, dass es möglich bleibt Korruptionen und Kriminalität in den Betrieben wirkungsvoll zu bekämpfen.

B) Im Einzelnen

I. Datenschutz im Arbeitsverhältnis

Die datenschutzrechtlichen Fragestellungen innerhalb des Arbeitsverhältnisses sind vielfach gleich gelagert, wie innerhalb anderer Rechtsbeziehungen. Wo die Notwendigkeit besteht, die komplexen Vorschriften des Datenschutzes im Arbeitsverhältnis handhabbar zu machen, werden die unterschiedlichsten freiwilligen Regelungen und Leitlinien, z. B. für die Nutzung von Internet und E-Mail am Arbeitsplatz getroffen. Solche betriebsnahen Lösungen sind besser geeignet, komplexe Datenschutzaspekte verständlich zu kommunizieren, als bürokratische Überregulierungen.

Kollektivrechtlich wird dies durch die Vorschriften des Betriebsverfassungsrechts flankiert. So existiert beispielsweise ein Mitbestimmungsrecht des Betriebsrates

bei der Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Dieses Mitbestimmungsrecht wird von der Rechtsprechung bereits exzessiv ausgelegt und angewendet.

II. Datenschutz überschaubar machen

Insbesondere für kleine und mittlere Unternehmen ist das Datenschutzrecht unnötig kompliziert und aufgrund der Tatsache, dass es auf zahlreiche unterschiedliche Gesetze verteilt ist, schlecht überschaubar.

Inhaltliche Verbesserungen hinsichtlich Rechtsklarheit und -sicherheit sind zum Beispiel hinsichtlich folgender Themenbereiche denkbar:

- Die effektive Kriminalitätsbekämpfung und die Bekämpfung von Korruption sind von herausragender Bedeutung für die Unternehmen. In einer Novellierung des Bundesdatenschutzgesetzes sollte daher klargestellt werden, dass zum Beispiel gegenüber einer konkreten Gruppe von Arbeitnehmern, unter denen es Verdachtsfälle gibt, ein so genanntes Screening, also ein Abgleich vorhandener Daten, möglich ist.
- Die Vertraulichkeit von Unternehmensdaten muss gewährleistet werden. Diese müssen wirkungsvoll vor dem Zugriff Unbefugter geschützt werden.
- Vertragsverletzungen und strafrechtlich relevantes Verhalten im Zusammenhang mit der Nutzung von Informations- und Kommunikationstechnologien am Arbeitsplatz müssen ausgeschlossen und ein effizientes Risikomanagement betrieben werden können. Dazu gehört, wie das Beispiel Finnland zeigt, auch die Möglichkeit eine Emails zu überprüfen.
- Das Mitbestimmungsrecht des Betriebsrates kann diesen in eine kritische Lage bringen, wenn er bei der Überwachung durch moderne Informations- und Kommunikationseinrichtungen einbezogen werden muss. Es ist daher zu überlegen, die Zustimmungsnotwendigkeit partiell durch eine nachträgliche Informationspflicht zu ersetzen.
- Der Datenaustausch im Konzern muss – auch über nationale Grenzen hinweg – erleichtert werden. Diese Forderung betrifft auch das europäische Recht. Bereits auf nationaler Ebene kann aber klargestellt werden, dass die Funktionsübertragung im Konzernverbund ebenso wie die Auftragsdatenverarbeitung möglich ist, ohne die Einzeleinwilligung der betroffenen Arbeitnehmer einholen zu müssen.
- Auch die Frage der Geltung des Fernmeldegeheimnisses bei der Nutzung betrieblicher Kommunikationsmittel durch die Arbeitnehmer ist mit großen Unsicherheiten behaftet. Diese Unsicherheiten führen dazu, dass sich Arbeitgeber bei der Kontrolle - selbst bei offensichtlichen Missbrauchsfällen - in einer rechtlichen Grauzone befinden. Hier sind Regelungen notwendig, die dem Arbeitgeber ausreichende Kontrollmöglichkeiten einräumen. Es muss klargestellt werden, dass das Fernmeldegeheimnis nur auf den Übermittlungsvorgang ausschließlich privater elektronischer Post Anwendung findet.

III. Datenschutz, Korruptionsbekämpfung und Compliance

Der verantwortungsvolle Umgang mit persönlichen Daten im Rahmen des Arbeitsverhältnisses ist für die Arbeitgeber eine Selbstverständlichkeit. Gleichzeitig tragen die Unternehmen die Verantwortung für eine zuverlässige Anwendung der Gesetze (Compliance). So sind sie beispielsweise zu einer effizienten Korruptionsbekämpfung verpflichtet.

Um sicherzustellen, dass die Gesetze und interne Regelungen des Unternehmens eingehalten werden, ist Kontrolle notwendig. – auch die des einzelnen Arbeitnehmers. Die Möglichkeit des Einsatzes moderner Informations- und Kommunikationstechnik in diesem Bereich darf nicht zu Lasten einer wirksamen Compliance eingeschränkt werden.

C) Zu den Anträgen

Zu Recht hat die Bundesregierung am 18. Februar dieses Jahres beschlossen, in der kurzen Zeitspanne, die bis zum Ablauf der 16. Wahlperiode bleibt, keine neuen das Datenschutzrecht ändernden Regelungen für das Arbeitsverhältnis mehr zu schaffen. Auf Grund der Kürze der Zeit müsste ein solches Gesetz oder entsprechende gesetzliche Einzelregelungen im Hau-Ruck-Verfahren verabschiedet werden. Dies ist für die komplexe Materie des Datenschutzes und des Arbeitnehmerdatenschutzes unangemessen. Insoweit können auch die vorliegenden Anträge der Fraktion Bündnis ’90/Die Grünen (Rechte der Beschäftigten von Discountern verbessern und Persönlichkeitsrechte abhängig Beschäftigter sichern), der Linken (Datenschutz für Beschäftigte stärken) und der FDP (Schutz von Arbeitnehmern durch transparente und praxisgerechte Regelungen gesetzlich absichern) allenfalls Anregungen für eine Diskussion in der nächsten Legislaturperiode sein.

Auch solche Anregungen für eine gesetzliche Änderung des Arbeitnehmerdatenschutzrechts dürfen jedoch nicht als Vehikel genutzt werden, unter dem Deckmantel des Datenschutzes Kernmaterien des Arbeitsrechts zu ändern - z. B. die betriebliche Mitbestimmung auszuweiten - und neue Bürokratie im Arbeitsrecht zu schaffen.

Eine solche unzulässige Vermischung von nicht unmittelbar zusammenhängenden Regelungsmaterien findet sich insbesondere im Antrag der Linken und den beiden Anträge der Fraktionen Bündnis ’90/Die Grünen. In ihnen geht es nicht um die Stärkung des individuellen Datenschutzes des einzelnen Arbeitnehmers. Vielmehr wird eine Ausdehnung der Rechtsstellung des Betriebsrats und der Gewerkschaften vorgesehen.

Der Datenschutz ist kein Mittel zur Ausdehnung von Betriebsratsrechten. Er soll ein notwendiges Maß an Persönlichkeitsschutz im Betrieb sicherstellen und nicht dem Betriebsrat ein Einfallstor für unzulässige Koppelungsgeschäfte öffnen. Die Vorschläge in den genannten Anträgen gehen damit schon in der Tendenz in eine Richtung, die vom Ansatz her nicht gedeckt ist, ein praktikables Datenschutzrecht zu schaffen.

I. Antrag Bündnis 90/Die Grünen: Rechte der Beschäftigten von Discountern verbessern (BT-Drucksache 16/9101)

1. Allgemeine Anmerkungen:

Das deutsche Datenschutzrecht gewährt einen hohen Schutzstandard in allen Bereichen, auch im Arbeitsrecht. Dieser gilt für jeden in Deutschland ansässigen Betrieb. Eine besondere Regelung für bestimmte Branchen ist deshalb unnötig.

2. Betriebsverfassungsgesetz

Der Antrag sieht eine Ausdehnung der Mitbestimmung vor, insbesondere zielen die geforderten Änderungen auf eine massive Erweiterung der Rolle der Gewerkschaften. Dies hat mit Datenschutzrecht nichts zu tun.

3. Persönlichkeitsrecht

Durch die Rechtsprechung des Bundesverfassungsgerichts ist ein Recht auf informationelle Selbstbestimmung anerkannt, das eine Ausformung des allgemeinen Persönlichkeitsrechts ist. Dies ist Maßstab bei der Prüfung der Rechtsprechung, ob bestimmte Maßnahmen zulässig sind. Es folgt somit immer eine Prüfung, ob ein Eingriff in das Persönlichkeitsrecht der Beschäftigten zulässig ist oder nicht. Je tiefer der Eingriff in das Recht der Beschäftigten, desto höher sind die Anforderungen, die die Rechtsprechung an die vom Arbeitgeber intendierten Maßnahmen stellt. Dies gilt für den Einsatz von Videokameras (Ziffer II.3.a) sowie Zugangskontrollen u. ä. Bereits heute ist somit das Persönlichkeitsrecht mithin Maßstab der Zulässigkeit. Eine weitere Verschärfung ist nicht notwendig. Dies wird bei der Videoüberwachung besonders deutlich. Videokontrollen sind vielfach unumgänglich. Dies gilt zum einen für öffentliche Verkaufsräume, in denen durch die Videoüberwachung die Sicherheit vor Straftaten gewährleistet wird, wie beispielsweise für die Überwachung von Maschinen während eines Produktionsvorganges. Hier unterliegt der Einsatz den strengen Kriterien der Rechtsprechung.

4. Datenschutzbeauftragter

Soweit zusätzlich die Stärkung des betrieblichen Datenschutzbeauftragten und die Erweiterung seiner Aufgaben gefordert werden, ist dies vor dem Hintergrund des geltenden Rechts nicht nachvollziehbar. Die Unternehmen sind verpflichtet, ein funktionierendes Compliance-System vorzuhalten. Hierzu gehört auch die Einhaltung datenschutzrechtlicher Regelungen. Der betriebliche Datenschutzbeauftragte ist bereits heute gegen eine Abberufung geschützt. Einer darüber hinausgehenden Veränderung seiner Stellung bedarf es nicht.

II. Antrag Bündnis 90/Die Grünen - Persönlichkeitsrechte abhängig Beschäftigter sichern - Datenschutz am Arbeitsplatz stärken (BT-Drucksache 16/9311)

Im Antrag werden Regeln zum Arbeitnehmerdatenschutz gefordert, die die gesamte Durchführung des Arbeitsverhältnisses betreffen, von der Bewerbung bis zur Beendigung und dabei die Voraussetzungen für Datenerhebung und Datenverarbeitung teilweise deutlich verengen. Dies schränkt die Unternehmen in für sie wichtigen Bereichen erheblich ein, beispielsweise im Bereich der Korruptionsbekämpfung.

Im Einzelnen:

1. Schutz von Bewerbern

- Fragerecht des Arbeitgebers

  Nach geltendem Recht ist der Arbeitgeber grundsätzlich berechtigt, für ihn maßgebliche Informationen durch Fragen an den Bewerber einzuholen. Dem Frage- und Informationsrecht des Arbeitgebers werden enge Grenzen durch das Persönlichkeitsrecht der Bewerber gesetzt. Insofern dürfen nur Fragen gestellt werden, an deren wahrheitsgemäße Beantwortung der Arbeitgeber ein berechtigtes, billigenswertes und schutzwürdiges Interesse hat, auf Grund dessen die Belange der Bewerber zurücktreten müssen. Dies ist nach der ausdifferenzierten Rechtsprechung nur der Fall, wenn die Beantwortung der Frage für den angestrebten Arbeitsplatz und die zu verrichtende Tätigkeit selbst von Bedeutung ist.

- Übertragung bei Online-Fragebögen

  Soweit für das Bewerbungsverfahren gefordert wird, dass bei der Verwendung von Online-Fragebögen ein sicherer Übertragungsweg zu verwenden ist, ist auch dies schon durch das geltende Recht ausreichend gewährleistet. Dies ist in der Anlage zu § 9 BDSG (Nr. 3 und 4 der Anlage) geregelt. Danach muss durch die speichernde Stelle sichergestellt werden, dass bei einer Übertragung von Daten diese vor oder während ihres Transports nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

2. Schutz der Arbeitnehmerdaten während des Beschäftigungsverhältnisses.

- Personalaktenführung

  Soweit unter Ziffer II.2.b. gefordert wird, dass die Daten in der Personalakte von den übrigen personenbezogenen Daten des Beschäftigten technisch und organisatorisch getrennt verarbeitet werden sollen, entspricht dies der ganz überwiegenden betrieblichen Praxis. In der Führung der Personalakte gab und gibt es zwischen Arbeitnehmern und Arbeitgebern kaum Streit. Wertet man die Rechtsprechung aus, so zeigt sich, dass die Grundsätze der Personalaktenführung klar sind und von den Unternehmen auch beachtet werden. Eine gesetzliche Regulierung ist nicht notwendig.

- Informationsrechte der Arbeitnehmer

  Soweit unter Ziffer II.2.c. gefordert wird, dass Arbeitnehmer regelmäßig über ihre Rechte zu informieren sind, führt dies eher zur Verunsicherung als dass es für die Information der Betroffenen dienlich ist. Den Betroffenen stehen Auskunftsrechte zu (§ 34 BDSG). Wenn die Beschäftigten über ihre Rechte im Unklaren sind, so stehen ihnen eine Vielzahl von Möglichkeiten zur Seite, sich entsprechenden Rat einzuholen. Zu weit gehende und zu häufige Informationspflichten sind bürokratisch und führen nicht zum besseren Schutz von Beschäftigten. Erfahrungsgemäß werden viele Informationen, wenn eine bestimmte Anzahl überschritten ist oder die Informationen zu detailliert sind, nicht mehr zur Kenntnis genommen.

- Übermittlung von Arbeitnehmerdaten

  Ähnliche personalpolitische Bedenken bestehen auch gegen Ziffer II.2.d. Danach sollen Arbeitnehmerdaten nur mit ausdrücklicher Zustimmung der Arbeitnehmer und nur auf vertraglicher Grundlage an Dritte, sei es eine Übermittlung an andere Arbeitgeber oder sei es eine Übermittlung ins Ausland im Rahmen einer Auftragsdatenverarbeitung, möglich sein. Dies ist abzulehnen.

  Wie bisher muss die Übermittlung bei Vorliegen eines der bestehenden Erlaubnistatbestände möglich sein. Wäre für jede Übermittlung eine Zustimmung nötig, wäre dies für die Unternehmen kaum zu leisten. Allein der Wechsel des IT-Anbieters auf dessen Server Be-

schäftigtendaten gespeichert sind, würde zu einer Zustimmungspflicht der Arbeitnehmer führen, genauso wie der Wechsel von einem Lohnbüro zu einem anderen Lohnbüro. Dies würde dazu führen, dass die Arbeitnehmer durch das Erteilen von unzähligen Einwilligungen verunsichert wären, ohne dass dies tatsächlich einen Mehrwert an Schutz bedeutet. Der Schutz der Arbeitnehmerdaten bei einer Übermittlung ist bereits durch die Notwendigkeit des Vorliegens der entsprechenden Erlaubnistatbestände gewährleistet.

Unabhängig davon würde ein Zustimmungserfordernis für faktisch jede Übermittlung bedeuten, dass Prozesse nicht mehr aufrechterhalten werden können, wenn einzelne Arbeitnehmer nicht zustimmen. Eine einheitliche Lohnabrechnung wäre zum Beispiel nicht mehr gewährleistet, wenn ein Teil der Arbeitnehmer einer Weitergabe ihrer Daten an ein Lohnabrechnungsbüro widersprechen würden. Dies überfordert nicht nur kleine, sondern auch große und mittlere Arbeitgeber Die Forderung ist deshalb vollständig abzulehnen.

- Beweisverwertungsverbot

  Ein Verwertungsverbot, wie unter Ziffer II.2.e., gefordert, darf nicht eingeführt werden. Rein formale Fehler dürfen beispielsweise nicht dazu führen, dass ein Mitarbeiter der zu Lasten des Arbeitgebers einen Betrug begeht, entlassen werden kann. Insoweit ist der Ansatz der Rechtsprechung, ein Verwertungsverbot nur bei tief greifenden Verletzungen des Persönlichkeitsrechtes anzuerkennen, angemessen.

- Unterlassungsanspruch

  Das Risiko besteht auch bei der Forderung unter Ziffer II.2.g. Danach soll dem Betriebsrat und dem betrieblichen Datenschutzbeauftragten ein Widerspruchsrecht bei Nichteinhaltung von Arbeitnehmerdatenschutzregelungen im Personalbereich zustehen. Die damit beabsichtigte Erweiterung der Rechte des Betriebsrates ist abzulehnen. Da der Einsatz von technischen Einrichtungen, die zur Überwachung und Kontrolle des Verhaltens und der Leistung von Arbeitnehmern geeignet sind, mitbestimmungspflichtig ist, bestehen hier üblicherweise Betriebsvereinbarungen. Werden diese nicht eingehalten, steht dem Betriebsrat bereits heute ein Unterlassungsanspruch gegenüber dem Arbeitgeber zu. Flankierend besteht die Regelung des § 80 Abs. 1 BetrVG, nach dem der Betriebsrat darüber zu wachen hat, dass zu Gunsten der Arbeitnehmer geltende Gesetze beachtet werden. Dies gilt auch für das Bundesdatenschutzgesetz. Dieser Schutz ist ausreichend.

3. Schutz von Gesundheitsdaten

- Gesundheitsdaten

  Soweit unter Ziffer II.3. die Verbesserung des Schutzes von Gesundheitsdaten gefordert wird, muss zunächst betont werden, dass Gesundheitsdaten als sensible Daten i. S. § 3 Abs. 1 Ziffer 9 BDSG bereits heute besonders geschützt werden. Der Aspekt der Sicherheit und des Schutzes von Dritten darf aber nicht hinter dem Persönlichkeitsrecht des Arbeitnehmers zurücktreten. Medizinische Tests sind notwendig zum Schutz des Beschäftigten, zum Schutz anderer Beschäftigter und zum Schutz Dritter, wie beispielsweise bei Piloten, LKW-Fahrern etc. Es ist auch wenig überzeugend hierfür eine Zustimmungsverpflichtung eines Betriebsrates beziehungsweise des betrieblichen Datenschutzbeauftragten einzuführen. Entweder solche Tests sind auf Grund einer gesetzlichen Regelung zulässig, dann bedarf es nicht eines zusätzlichen Schutzes eines Zustimmungserfordernisses des Datenschutzbeauftragten oder der Arbeitnehmervertretung. Dies gilt beispielsweise für die verpflichtenden Untersuchungen, wie sie im Infektionsschutzgesetz vorgeschrieben sind. Ist dies nicht der Fall, handelt es sich im Regelfall um Einzelfälle. Eine solche Rechtswahrnehmung in Einzelfällen steht systematisch weder dem Datenschutzbeauftragten noch der Arbeitnehmervertretung zu.

- Messung von Sozialverhalten und Leistungsfähigkeit

  Soweit unter Ziffer II.3.d. die Messung des Sozialverhaltens und die Messung der Leistungsfähigkeit eingeschränkt werden soll, ist dies abzulehnen. Gefordert wird, dass eine Messung des Sozialverhaltens, soweit es für die Arbeitsanforderung auf der Stelle nicht unmittelbar und nachweislich ausschlaggebend ist, unzulässig sein soll. Unabhängig von der Frage, inwieweit Sozialverhalten überhaupt gemessen werden kann, ist zumindest die Beurteilung des Sozialverhaltens bei den meisten Arbeitsplätzen von erheblicher Bedeutung. Heutzutage finden viele Arbeiten in Arbeitsgruppen bzw. im Team statt. Damit eine Arbeitsgruppe reibungslos funktioniert, kommt es auf das Sozialverhalten Einzelner an. Dies gilt ebenso für sämtliche Berufe, in denen Kundenkontakt besteht. Auch hier ist das Sozialverhalten von großer Bedeutung und dessen Beurteilung muss nach wie vor zulässig sein.

  Das Gleiche gilt für die Messung der Leistungsfähigkeit. Zwar wird im Antrag anerkannt, dass die Messung der Leistungsfähigkeit unter bestimmten Voraussetzungen und im Rahmen der Erforderlichkeit zulässig sein kann, dies verkennt jedoch die grundlegenden arbeitsrechtlichen Prinzipien. Das Arbeitsverhältnis ist ein auf Austausch von Leistung und Gegenleistung gerichtetes Rechtsverhältnis und der Arbeitnehmer bietet seine Tätigkeit als Leistung an und erhält hierfür eine Vergütung. Dem Arbeitgeber muss es immer - unter Beachtung des Persönlichkeitsrechts des Arbeitnehmers - möglich sein, die Leistung und damit auch die Leistungsfähigkeit des Arbeitsnehmers zu bewerten. Nur so kann der Arbeitgeber sicherstellen, dass das ursprüngliche vereinbarte Verhältnis zwischen Leistung und Gegenleistung tatsächlich funktioniert. Insoweit stellt die Kontrolle der Leistung und mithin der Leistungsfähigkeit einen Kernbereich arbeitsrechtlicher Kontrolle dar, die zulässig sein muss.

4. Überwachung mit optischen und elektronischen Geräten

   Unter Ziffer II.4. beschäftigt sich der Antrag mit dem Schutz von Überwachung mit optischen und elektronischen Geräten. Richtig ist, dass mit optischen und elektronischen Geräten eine weitergehende Überwachung möglich geworden ist als dies in der Vergangenheit möglich war.

- Einsatz von Videokameras

  Aus diesem Grund wird der Einsatz von Videokameras und anderen technischen Systemen zur Kontrolle

am Arbeitsplatz durch die Rechtsprechung bereits heute eng begrenzt. Eine Rundumüberwachung von Beschäftigten ist bereits heute unzulässig. Auch in Zukunft muss aber die Kontrolle, insbesondere von öffentlich zugänglichen Räumen, wie Verkaufsräumen möglich sein. Ebenso muss eine Leistungskontrolle durch elektronische Überwachungseinrichtungen gegebenenfalls zulässig sein.

- Telekommunikation am Arbeitsplatz

  Soweit unter Ziffer II.5. der Einsatz der Telekommunikation am Arbeitsplatz behandelt wird, geht insbesondere die Forderung unter Ziffer II.5.a. hinsichtlich der Leistungskontrolle zu weit. Danach wäre eine personenbezogene Überwachung der Arbeitnehmer mit Hilfe von Logdateien oder einer entsprechenden Software zur Leistungskontrolle unzulässig. Wie bereits erläutert, ist die Leistungskontrolle wesentlicher Teil des Arbeitsverhältnisses. Eine Leistungskontrolle per Software muss möglich bleiben.

5. Betrieblicher Datenschutzbeauftragter

   Die Forderungen nach einer Ausweitung der Stellung des Datenschutzbeauftragten unter Ziffer II.6. gehen an der betrieblichen Realität vorbei. Ein Mitbestimmungsrecht bei Benennung und Abberufung des betrieblichen Datenschutzbeauftragten ist fehl am Platz (Ziffer II.6.g.). Ebenso ist der Mehrwert der Verpflichtung, die Beschäftigten über den betrieblichen Datenschutzbeauftragten zu informieren (Ziffer II.6.e.) zweifelhaft, da die Proliferation der Informationspflichten im Regelfall nicht zu einer Verbesserung des Schutzes führt, sondern eher zu Verunsicherung und Desinteresse bei den Beschäftigten.

   Soweit verlangt wird, dass der Datenschutzbeauftragte zur Vermeidung von Interessenkonflikten möglichst keine weiteren Aufgaben im Bereich der betrieblichen Datenverarbeitung oder der Personalverwaltung wahrnehmen soll (Ziffer II.6.b.), ist dies vor dem Hintergrund der notwendigen Sachkunde problematisch. Häufig haben nur Mitarbeiter, die sich tatsächlich mit der betrieblichen Datenverarbeitung und deren technischen Voraussetzungen beschäftigen, die Fachkunde, um im Bereich der elektronischen Datenverarbeitung überhaupt erst tätig zu werden und beurteilen zu können, ob die Maßnahme zulässig und sinnvoll ist.

III. Antrag der Fraktion Die Linke – Datenschutz für Beschäftigte stärken (BT Drucksache 16/11376)

Die generelle Forderung nach einem Arbeitnehmerdatenschutzgesetz, bzw. die Verschärfung der bestehenden Rechtslage ist abzulehnen. Die geltenden Regelungen bieten ausreichend Schutz.

Im Einzelnen:

1. Erhebung, Speicherung, Veränderung, Übermittlung und Nutzung personenbezogener oder personenbeziehbarer Daten von Beschäftigten

- Anwendungsbereich

  Soweit unter Ziffer I.a. gefordert wird, dass ein Arbeitnehmerdatenschutzgesetz auf alle Daten, unabhängig von der Form der Speicherung, Anwendung finden soll, ist dies zu weitgehend. Voraussetzung für die Anwendung sollte entweder die elektronische Datenverarbeitung oder das Vorliegen einer Datei, wie im Bundesdatenschutzgesetz derzeit geregelt, notwendig sein. Die Notwendigkeit eines höheren Schutzniveaus in der modernen Arbeitswelt lässt sich nur durch die moderne Datenverarbeitung und den Einsatz elektronischer Überwachungseinrichtungen rechtfertigen. Es besteht kein Anlass und keine Notwendigkeit diesen erhöhten Schutzstandard auf Situationen zu übertragen, in denen diese potentielle Gefährdung überhaupt nicht besteht.

  Abzulehnen ist auch die unter Ziffer I.c. geforderte Ausdehnung des Anwendungsbereiches eines Arbeitnehmerdatenschutzgesetzes auf „freelancer“. Ist jemand nicht als Arbeitnehmer tätig, wie dies bei einem „freelancer“ der Fall ist, so ist dieser kein Arbeitnehmer, sondern ein selbständiger Auftragnehmer. Insoweit finden dann die allgemeinen datenschutzrechtlichen Regelungen aus dem Bundesdatenschutzgesetz Anwendung. Alles Andere wäre ein nicht zu rechtfertigender Systembruch.

  Unklar ist die Forderung, dass mit Personen, die nicht auf dem Betriebsgelände beschäftigt werden, unter Hinzuziehung der Interessenvertretung und des betrieblichen Datenschutzbeauftragten eine konkrete Vereinbarung zur Einhaltung der Regelung des Arbeitnehmerdatenschutzgesetzes abzuschließen ist. Auch Mitarbeiter, die nicht auf dem Betriebsgelände eingesetzt werden, wie beispielsweise Außendienstmitarbeiter können sich auf das Bundesdatenschutzgesetz berufen, da sie unabhängig von ihrem Arbeitsort Arbeitnehmer sind. Einer zusätzlichen Regelung bedarf es deshalb nicht.

- Begrenzung der Erlaubnistatbestände

  Soweit unter Ziffer I.d gefordert wird, dass diei Erhebung, Speicherung, Veränderung oder Übermittlung sowie Nutzung der Daten von Beschäftigten nur zulässig sein sollen, wenn sie durch Gesetz oder sonstige Rechtsvorschrift erlaubt sind oder ein mit den Betroffenen geschlossener Vertrag erfordert, ist dies zu eng. Entsprechend dem derzeitigen Recht muss eine Datenverarbeitung auch dann zulässig sein, wenn dies zur Wahrung berechtigte Interessen des Arbeitgebers erforderlich ist und schutzwürdige Belange des Arbeitnehmers nicht entgegenstehen entsprechend ist derzeit geltende § 28 Abs. 1 Nr. 2 BDSG. Die Interessenabwägung spielt heute bei der Nutzung von Daten im Arbeitsverhältnis in der Rechtsprechung die entscheidende Rolle. Die Zulässigkeit der Erhebung, Nutzung und Verarbeitung von Arbeitnehmerdaten wird im Regelfall daran gemessen, ob die Interessen des Arbeitgebers hieran die Interessen des Arbeitnehmers überwiegen.

  So schlussfolgert zum Beispiel das Bundesarbeitsgericht aus § 87 Absatz 1 Nr. 6 Betriebsverfassungsgesetz, dass ein Mitbestimmungsrecht des Betriebsrats schon dann besteht, wenn eine technische Einrichtung zur Verhaltens- oder Leistungsüberwachung geeignet ist. Die gesetzliche Vorschrift statuiert demgegenüber ein Mitbestimmungsrecht für den Fall, dass die technische Einrichtung hierzu bestimmt ist.

  Es ist daher wahrscheinlich, dass es mit der Aufgabe der Interessenabwägung als Rechtfertigungsgrund für die Nutzung von Arbeitnehmerdaten zu einer Beschränkung der Datennutzung auf das für die Durchführung des Arbeitsverhältnisses unmittelbar Erfor-

derliche käme. Als unmittelbar erforderlich wird bisher nur die Datennutzung angesehen, die in einem unmittelbaren sachlichen Zusammenhang zwischen der beabsichtigten Datennutzung und dem konkreten Vertragszweck – also dem arbeitsrechtlichen Austauschverhältnis – steht.

Dies würde zwangsläufig eine betrieblich veranlasste notwendige Nutzung von Daten in Situationen einschränken, wo eine solche zurzeit durch die mögliche Interessenabwägung erlaubt ist.

- Verhältnis Betriebsvereinbarung - Bundesdatenschutzgesetz

  Auch die Forderung in I.e. geht weit über die geltende Rechtslage hinaus. Derzeit kann nach der Rechtsprechung des BAG (BAG vom 27. Mai 1986 – 1 ABR 48/84) auch zu Ungunsten der Arbeitnehmer von den Vorschriften des Bundesdatenschutzgesetzes abgewichen werden. Diese Rechtsprechung ist aufrecht zu erhalten.

- Datenschutzkonzept

  Soweit in I.f. gefordert wird, dass personenbezogen oder personenbeziehbare Daten nur erhoben, gespeichert, verändert, übermittelt oder genutzt werden dürfen, wenn ein Datenschutzkonzept mit Festlegung der Zugriffsberechtigung und der erforderlichen Sicherheitsmaßnahmen vorliegt, das mit dem betrieblichen Datenschutzbeauftragten und dem Betriebs-/Personalrat abgestimmt ist, ist die damit einhergehende Erweiterung der Rechte des Betriebsrates über § 87 BetrVG hinaus, abzulehnen. Diese Erweiterung ist auch nicht zum Schutz der Arbeitnehmer notwendig. Es besteht mit der Anlage zu § 9 BDSG eine gesetzliche Regelung und diese ist vom Arbeitgeber umzusetzen. Ein Mitbestimmungsrecht des Betriebsrates bei sämtlichen Details der Zugriffskontrolle wäre zu weitgehend. Es muss dem Arbeitgeber überlassen sein, welche Leitungsebene, und welche Teile in der Personalabteilung zugreifen dürfen und wie dies in der entsprechenden IT-Landschaft ausgestaltet wird.

- Personalaktenführung

  Zu der Forderung unter I.h. nach der Personalaktendaten und sonstige Daten des Beschäftigten getrennt zu speichern und zu verarbeiten sind, ist auf das oben Gesagte zu verweisen.

- Direkte Erhebung beim Beschäftigten

  Die Forderung unter Ziffer I.k., dass Daten bei den Beschäftigten direkt zu erheben sind, ist abzulehnen. In der Rechtsprechung ist anerkannt, dass auch eine Datenerhebung bei Dritten, wie beim ehemaligen Arbeitgeber möglich ist. Gleichzeitig ist auch der Zugriff auf allgemein zugänglich Daten nach § 28 Abs. 1 Nr. 3 BDSG erlaubt. Es muss auch in Zukunft möglich sein, eine Recherche im Internet durchzuführen. Bei Bewerbungsverfahren ist es üblich, auf das Internet zurückzugreifen. Dies gilt für Bewerber wie für Arbeitgeber. Bewerber stellen sich in sozialen Netzwerken vor und nutzen diese Plattformen gezielt, um neue Möglichkeiten zu erkunden und berufliche Netzwerke zu knüpfen. Arbeitgeber nutzen diese Möglichkeit und suchen gezielt neue Mitarbeiter. Gleichzeitig kann der Arbeitgeber öffentlich gemachte Informationen einsehen, die für ihn von Interesse sind, beispielsweise im Wissenschaftsbereich über Publikationen und Vorträge. Diese Daten sind allgemein zugänglich und es muss deshalb auch dem Arbeitgeber weiter möglich sein, auf diese Daten zuzugreifen. Ein Verbot wäre bei der zu erwartenden noch zunehmenden Nutzung solcher Netzwerke lebensfremd.

- Konkrete Zwecke für die Verarbeitung

  Die Forderung unter Ziffer I.l. ist zu weitgehend, wenn gefordert wird, dass die Erhebung, Speicherung, Veränderung, Übermittlung oder Nutzung nur zulässig sein soll, wenn und solange sie zur Erreichung eines vorher konkret festgelegten Zwecks erforderlich sind. Zudem steht die Forderung im Widerspruch zur Forderung unter Ziffer I.j. Nach Ziffer I.j. soll eine Datenverarbeitung zulässig sein, wenn sie dem Zweck des Arbeitsverhältnisses dient. Insoweit würde Ziffer I.l. eine Einschränkung darstellen, wenn noch ein weiterer Zweck innerhalb des Arbeitsverhältnisses vorliegen muss.

- Festlegung im Voraus

  Letztlich nicht leistbar ist auch die weitere in Ziffer I.l. enthaltene Forderung, nach der die technischen Mittel einer Erhebung, Speicherung, Veränderung, Übermittlung und Nutzung im Voraus festzulegen sind. Dies ist in der täglichen Unternehmenspraxis nicht durchführbar. Die technischen Mittel könnten lediglich ganz allgemein angegeben werden. Bei einer zu spezifischen Angabe, kann im Voraus nicht abgeschätzt werden, ob und wann sich dies ändert. Es wäre unnötiger und bürokratischer Aufwand, wenn die technischen Mittel bei jeder Datenverarbeitung im Voraus festzulegen wären.

- Mitteilungspflicht

  Eine ähnlich belastende Regelung findet sich in Ziffer I.m. Wenn den Betroffenen über die Erhebung, Speicherung, Veränderung, Übermittlung oder Nutzung ihrer Daten Mitteilung zu machen ist, sollen auch die zugrunde liegenden Grundsätze, der Verwendungszusammenhang, die verwendeten technischen Mittel und Methoden, Empfänger, Herkunft, Beginn und Dauer der Speicherung sowie die Art derjenigen Daten, die zusätzlich in die Erhebung, Speicherung, Veränderung, Übermittlung oder Nutzung eingehen, mitgeteilt werden. Zusätzlich sind neben der verantwortlichen Stelle auch die verantwortlichen Personen und deren Erreichbarkeit mitzuteilen. Eine solche Auskunftsverpflichtung ist zu weitgehend und belastet die Unternehmen mit einer ausufernden Bürokratie. Selbst wenn man eine solche Mitteilungspflicht nur auf besonderen Antrag des Arbeitnehmers statuieren würde, wäre die bürokratische Belastung der Unternehmen immens. Die gesamten geforderten Informationen müssten ständig für jeden Mitarbeiter bereitgehalten werden, um sicherzustellen, dass ein entsprechendes Auskunftsverlangen zeitnah und ordnungsgemäß bearbeitet werden kann. Dieser Aufwand ist für die Unternehmen, insbesondere auch für kleine und mittlere Unternehmen nicht tragbar.

2. Schutz besonderer Arten von Daten

   Soweit in Ziffer II.a. gefordert wird, dass eine Datenverarbeitung von besonderen Daten gem. § 3 Abs. 9 BDSG nur möglich sein soll, wenn dies für einen konkreten Zweck zwingend erforderlich ist und der

Betriebsrat und der betriebliche Datenschutzbeauftragte beteiligt sind, ist diese Ausweitung des Mitbestimmungsrechtes über § 87 Abs. 1 Nr. 6 BetrVG abzulehnen. Wenn diese Daten in technischen Einrichtungen gespeichert werden, besteht ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG.

3. Schutz von Bewerberinnen und Bewerbern

Im Hinblick auf das Fragerecht des Arbeitgebers und psychologische Tests, übernimmt der Antrag die bestehende Rechtslage. Eine Verschärfung der aktuell geltenden Rechtslage wird zu folgenden Punkten verlangt:

- Die unter Ziffer III.d. verlangte Löschung der Bewerberdaten, falls die Bewerbung erfolglos bleibt, ist zu weitgehend. Dem Arbeitgeber muss zumindest die Möglichkeit erhalten bleiben, die Daten sechs Monate zu speichern, um sicher zu gehen, dass er gegebenenfalls auf eine Klage nach dem AGG reagieren kann.
- Soweit unter Ziffer III.f. verlangt wird, dass dem Bewerber ein Schadensersatzanspruch zusteht, wenn eine unzulässige Frage gestellt wird, ist der Schadensersatzanspruch auf den materiellen Schaden zu begrenzen, bzw. im Hinblick auf die ausufernden Summen, die im Rahmen der Anwendung des AGG gefordert werden, ist der Schadensersatzanspruch von vornherein zu beschränken.
- Auch die unter Ziffer III.g. vorgesehene Verpflichtung, dass Bewerber Anspruch auf kostenlose Auskunft und fortlaufende Unterrichtung über die zu ihrer Person gespeicherten Daten haben, ist zu weitgehend. Der derzeit normierte Auskunftsanspruch des § 34 BDSG ist ausreichend.

4. Schutz während und nach der Beendigung des Beschäftigungsverhältnisses

Die unter IV.1 geforderten Grundsätze zum Umgang mit Daten während des Beschäftigungsverhältnisses würden die Personalverwaltung im Unternehmen bürokratisieren und sind in der Praxis nicht zu erfüllen.

- Grundsätze der Datenvermeidung und Datensparsamkeit

  Soweit zunächst gefordert wird, dass in der betrieblichen Personalarbeit datenvermeidende und datensparsame Instrumente eingesetzt werden, so entspricht dies bereits der heutigen Rechtslage. Auch derzeit gelten die Grundsätze der Datenvermeidung und Datensparsamkeit. Umso problematischer ist jedoch die Forderung, dass Daten nur erhoben, gespeichert, verändert, übermittelt oder genutzt werden dürfen, wenn zuvor die technisch-organisatorischen Voraussetzungen und die ausschließlich verwendeten Datenfelder, die zulässigen Auswertungen und Zweckbestimmungen, die Speicherdauer, die verwendeten Programme, die zugriffsberechtigten Stellen und die verfügbaren Schnittstellen nach den Kriterien der Erforderlichkeit und Zweckbindung abschließend definiert wurden. Es mag bei einigen Prozessen möglich sein, dies alles vorab zu bestimmen, allerdings führt die heutige Entwicklung im IuK-Bereich dazu, dass das geforderte nicht geleistet werden kann. Es kann nicht sein, dass alleine eine veränderte Auswertungsmöglichkeit nach einem Softwareupdate dazu führt, dass die Datenverarbeitung unzulässig wird, da diese Auswertungsmöglichkeit nicht vorab abschließend definiert wurde.

  Die Frage, ob eine Auswertungsmöglichkeit möglich ist oder nicht, darf nicht daran festgemacht werden, ob diese vorab vorgesehen wurde oder ob der Zweck geändert wurde. Dies kann an einem Beispiel deutlich gemacht werden. Die Fehlzeiten von Arbeitnehmern wurden immer erfasst, allein um überprüfen zu können, wann die Lohnfortzahlungspflicht der Arbeitgeber endet. Durch die Einführung des betrieblichen Eingliederungsmanagements müssen die Fehlzeiten nun auch wegen der Pflicht des Arbeitgebers, ein betriebliches Eingliederungsmanagement durchzuführen, ausgewertet werden. Es kann nicht sein, dass eine solche - neue - Auswertung nicht möglich ist, da diese nicht bereits von Anfang an vorgesehen war. Es darf deshalb nur darauf ankommen, ob eine Auswertung als solche zulässig ist, da sie unter einen bestehenden Erlaubnistatbestand fällt und nicht darauf, ob diese bereits von Anfang an vorgesehen war oder nicht.

- Unterrichtung des Arbeitnehmers

  Der unter IV.1.b. vorgesehene Anspruch auf kostenlose und fortlaufende Unterrichtung ist zu weitgehend und unnötig. Der bestehende Auskunftsanspruch des § 34 BDSG ist ausreichend und gewährleistet, dass die Betroffenen, also im Arbeitsverhältnis die Beschäftigten, ihre Rechte wahrnehmen können.

- Löschung nach Beendigung

  Soweit unter IV.1.c gefordert wird, dass die Daten nach Beendigung des Arbeitsverhältnisses zu löschen sind, ist sicherzustellen, dass der Arbeitgeber, die Daten ausreichend lang speichern zu können, um sich ggf. gegen Klagen, die sich auf eine Verletzung des AGG stützen, verteidigen zu können. Richtig ist in diesem Zusammenhang, dass eine Einwilligung in eine zeitlich darüber hinaus gehende Speicherung möglich sein muss.

- Leistungs- und Verhaltenskontrollen

  Unter Ziffer IV.2. wird die Zulässigkeit von Leistungs-, Verhaltens- und Bewegungsprofilen von Beschäftigten behandelt.

  Bereits die Vereinheitlichung der Anforderungen an die Zulässigkeit von Leistungs- und Verhaltensprofilen geht am Kern des Arbeitsverhältnisses vorbei. Das Verhalten des Arbeitnehmers muss kontrollierbar sein, soweit es das Verhalten am Arbeitsplatz betrifft.

  Abzulehnen ist jede Form der Einschränkung von Leistungskontrollen. Die Einschränkung der Leistungskontrolle muss die Ausnahme bilden. Die Kontrolle der Leistung des Arbeitnehmers ist dem Arbeitsverhältnis inhärent. Das Arbeitsverhältnis ist ein Austauschverhältnis. Der Arbeitgeber muss daher berechtigt sein, die Leistung jederzeit zu kontrollieren und zu messen. Er darf dabei nur Einschränkungen unterliegen, die sich nach Abwägung der Interessen des Arbeitgebers und des Arbeitnehmers unter Beachtung des allgemeinen Persönlichkeitsrechts des Arbeitnehmers ergeben, wie beispielsweise das Verbot einer Rundumüberwachung.

  Wenn, wie in IV.2.a. gefordert, Datenerhebung und -verarbeitung von Daten, die einer Verhaltenskontrolle- und/oder Leistungskontrolle dienen, nur noch dann möglich sein soll, wenn es um die Arbeitsvertragser-

füllung geht, Einsatzplanungen und Einsatzsteuern vorzunehmen oder Qualifizierungsmaßnahmen daraus abzuleiten, ist dies zu weitgehend. Leistungskontrollen müssen, wie dargelegt, zulässig sein.

Die im Antrag vorgeschlagenen Ausnahmen, Kontrolle der Arbeitsvertragserfüllung, Einsatzplanung und Einsatzsteuerung sind deutlich zu eng. Allein die Engführung auf die Einsatzplanung zeigt, dass eine extreme Begrenzung der Datenverwendung gewünscht ist. Personalplanung ist weitaus mehr als lediglich Einsatzplanung. Es kann nicht in Frage stehen, dass der Arbeitgeber Leistungs- und Verhaltensdaten für eine umfassende Personalplanung oder andere betriebs- oder unternehmensbedingte Planungserfordernisse erheben darf.

5. Nutzung von Telekommunikationsanlagen

- Barrierefreie Nutzung

  Im Hinblick auf die Nutzung von Telekommunikations- und Telemedieneinrichtungen (Ziffer IV.3) werden Ansprüche der Arbeitnehmer eingefordert, die eher an eine allumfassende Fürsorgepflicht des Arbeitgebers denken lassen, als ein Austauschverhältnis zwischen zwei Parteien. So wird unter Ziffer IV.3.a. ein barrierefreier Zugang zu den digitalen Netzwerken des Arbeitgebers gefordert und der Ausbau der Präsenz der Gewerkschaften in elektronischen Netzwerken. Der Aufbau eines barrierefreien Netzwerkes ist mit erheblichen Kosten verbunden. Ob ein solches Netzwerk notwendig ist, muss allein dem Arbeitgeber überlassen werden. Eine generelle Verpflichtung, die sogar dann Anwendung findet, wenn kein Beschäftigter auf ein solches barrierefreies Netz angewiesen ist, ist abzulehnen und zeigt erneut die geringe Praxisnähe des Antrags.

- Überwachung Kommunikationsverhalten

  Die zur Überwachung des Kommunikationsverhaltens der Beschäftigen unter Ziffer IV.4 aufgelisteten Forderungen sind unterschiedlich zu beurteilen.

  Richtig ist, dass Eingriffe in das Telekommunikationsgeheimnis für einen bestimmten Zeitraum, durch Stichproben und nach vorheriger Ankündigung, die einer angemessenen Form bedarf, zulässig sein sollen (Ziffer IV.4.b.) – es wird dabei davon ausgegangen, dass mit Telekommunikationsgeheimnis das Fernmeldegeheimnis gemeint ist.

  Soweit allerdings Ansprüche des Arbeitgebers auf Herausgabe beruflicher Kommunikationsvorgänge eingeschränkt werden soll (Ziffer IV.4.c.), ist dies nicht tragbar. Sämtliches Handeln, und mithin auch sämtlich beruflich veranlasste Kommunikation muss durch den Arbeitgeber kontrollierbar sein. Die im Antrag vorgenommen Einschränkungen hierzu sind abzulehnen. Der Arbeitnehmer ist Erfüllungsgehilfe des Arbeitgebers, und vertritt den Arbeitgeber nach außen. Insoweit muss der Arbeitgeber auf diese Kommunikation vollständigen Zugriff haben, dies ergibt sich bereits aus haftungsrechtlichen Gründen.

  Wenn unter Ziffer IV.4.d für den Fall einer zugelassenen Privatnutzung gefordert wird, dass die Nutzung dem Fernmeldegeheimnis unterfällt, wird die in der Rechtsprechung vorgenommene Differenzierung nicht aufgenommen. Danach gilt das Fernmeldegeheimnis nur für den reinen Übertragungszeitraum. Eine weitergehende Geltung des Fernmeldegeheimnisses ist abzulehnen.

  Die Forderung der Ziffer IV.4.e, dass die Kommunikation von Beschäftigten mit dem betrieblichen Datenschutzbeauftragten sowie den Organen der betrieblichen Mitbestimmung überwachungsfrei zu gewährleisten ist, ist bereits heute erfüllt.

  Die Forderungen unter Ziffer IV.5 zur Überwachung mit optoelektronischen Geräten gehen zu weit. Vorab ist festzustellen, dass eine heimliche Videoüberwachung einzelner Beschäftigter innerhalb der engen Voraussetzungen, die die Rechtsprechung aufgestellt hat, möglich bleiben muss – nämlich immer dann, wenn eine Straftat aufgeklärt werden muss, die nicht durch andere mildere Mittel aufgeklärt werden kann.

  Die Forderungen zum betrieblichen Datenschutzbeauftragten unter Ziffer V. sind zu weitgehend. Wenn aber einer Beschäftigtenzahl von 5 Mitarbeitern ein Datenschutzbeauftragter bestellt werden soll, ist dies im Hinblick auf die in kleinen Betrieben vorgenommene Datenverarbeitung unverhältnismäßig.

IV. Antrag FDP-Fraktion: Schutz von Arbeitnehmerdaten durch transparente und praxisgerechte Regelungen gesetzlich absichern (BT-Drucksache 16/12670).

Zu den spezifischen Forderungen im Einzelnen:

- Zu Ziffer 5 – Gesundheitstests und regelmäßige Untersuchungen

  Zu begrüßen ist, dass anerkannt wird, dass regelmäßige Untersuchungen zum Schutz Dritter, des Arbeitgebers und des Arbeitnehmers notwendig sein können. Die unter Ziffer 5 vorgenommene Einschränkung auf gefahrgeneigte Tätigkeiten ist allerdings wenig überzeugend. Der Begriff der gefahrgeneigten Arbeit wird heute nicht mehr in der Rechtsprechung verwendet. Die Frage, ob medizinische Untersuchungen notwendig sind, muss sich allein danach richten, ob diese zum Schutz Dritter, des Arbeitnehmers selbst oder des Arbeitgebers notwendig sind und nicht danach, ob eine gefahrgeneigte Arbeit vorliegt.

- Ziffer 6 – Bewerbungsunterlagen

  Eine gesetzliche Verpflichtung, Bewerbungsunterlagen zwingend an den Bewerber zurückzusenden, belastet die Unternehmen mit einem hohen bürokratischen Aufwand. Dies gilt insbesondere dann, wenn nicht zwischen gezielten Bewerbungen auf ausgeschriebene Stellen und Blindbewerbungen unterschieden wird. Zumindest für Blindbewerbungen muss eine verpflichtende Rücksendung ausgeschlossen sein.

  Zu begrüßen ist, dass Daten ausreichend lange nach einer erfolglosen Bewerbung gespeichert werden können, um auf Klagen auf Grund des Allgemeinen Gleichbehandlungsgesetzes zu reagieren.

- Zu Ziffer 7 – Personalaktenführung

  Die Anforderungen an die elektronische Aktenführung ergeben sich auch für Arbeitnehmerdaten aus der Anlage zu § 9 BDSG. Danach ist entsprechend der Ziffer 3 die Zugriffsberechtigung zu regeln.

Auch der Grundsatz der Richtigkeit der Personalakte ist von jeher Grundsatz des Personalaktenrechts. Durch die bestehenden arbeitsrechtlichen Ansprüche auf Gegendarstellung, ggf. Entfernung und die Abwehrrechte nach dem BDSG, wird diesem tragenden Grundsatz des Personaktenrechts ausreichend Rechnung getragen.

- Ziffer 8 – Übermittlung von Arbeitnehmerdaten an Dritte

  Zu begrüßen ist, dass anerkannt wird, dass neben den Erlaubnistatbeständen Zweck des Arbeitsverhältnisses und Einwilligung auch der derzeit bestehende Erlaubnistatbestand der berechtigten Interessen des Arbeitgebers unabdingbar ist. Dass es dieses Erlaubnistatbestandes weiter bedarf, zeigt die in Ziffer 8 erwähnte Due Diligence Prüfung im Rahmen eines Unternehmensverkaufs.

  Soweit detaillierte Regelungen zum Unternehmensverkauf vorgeschlagen werden, bedürfen diese noch weiterer Ergänzung. Richtig ist, dass im Grundsatz bei einem Unternehmenskauf Daten nur anonymisiert weitergegeben werden sollten. Für bestimmte Mitarbeiter muss es hiervon jedoch Ausnahmen geben. Der insoweit unter Ziffer 8 vorgeschlagene Kreis der leitenden Angestellten im Sinne des § 5 Abs. 2 des Betriebsverfassungsgesetzes ist allerdings zu eng. Es kann auch im Bereich der Forschung und Entwicklung für den Erwerber wichtig sein zu wissen, welche Arbeitnehmer in der entsprechenden Abteilung tätig sind. Hier sollte der Kreis nicht auf leitende Angestellte beschränkt werden, sondern die namentliche Übermittlung im Rahmen einer Due Diligence Prüfung sollte möglich sein, wenn es im Rahmen eines Unternehmenskaufs wesentlich auf die entsprechenden Mitarbeiter ankommt.

- Zu Ziffer 9 – Verwendung von biometrischen Datensystemen.

  Die Einführung solcher Systeme ist teuer und ein Arbeitgeber wird sich genau überlegen, ob er ein solches System einführt. In bestimmten Bereichen, beispielsweise in Bereichen, in denen das SÜG Anwendung findet, kann der Einsatz solcher biometrischer Erkennungsverfahren allerdings sinnvoll sein, beispielsweise die Fingerprinterkennung in Kernkraftwerksbereichen und ähnliches. Ob die im Antrag geforderten engen Voraussetzungen im Rahmen der Durchführung notwendig sind, mag bezweifelt werden. Es fehlen insoweit noch belastbare Informationen aus der Praxis.

- Ziffer 10 – Einsatz von Videoüberwachungssystemen und andere permanente technische Systeme mit vergleichbarer Eingriffsintensität.

  Klarzustellen ist, dass die Überwachung von Produktionsabläufen, die Einhaltung gewerblicher Auflagen und die Videoüberwachung von Kassen und sonstigen öffentlich zugänglichen Geschäftsbereichen möglich bleiben muss – wie dies auch in der Ziffer 10 klargestellt wird.

  Die Überwachung von einzelnen Beschäftigten mittels Videoüberwachung und elektronischen Systemen darf nicht gänzlich untersagt sein. Eine Überwachung muss entsprechend der bisherigen Rechtsprechung des Bundesarbeitsgerichtes möglich sein, wenn eine Straftat aufzuklären ist, die anderweitig nicht aufgeklärt werden konnte und keine anderen milderen Mittel zu Verfügung stehen.

- Ziffer 11 – Kontrolle der Nutzung von E-Mails, Internet und Telefon

  Richtig ist die Klarstellung, dass der Arbeitgeber nicht verpflichtet ist, in die private Nutzung von E-Mail, Internet und Telefon einzuwilligen.

  Im Hinblick auf die Kontrolle ist auch richtig, dass dem Arbeitgeber eine stichprobenhafte und zeitnahe Auswertung von Protokolldaten zustehen soll.

- Ziffer 12 – Rolle des Betriebsrates

  Bereits heute besteht ein umfassendes Mitbestimmungsrecht des Betriebsrates nach § 87 Abs. 1 Nr. BetrVG. Soweit gefordert wird, eine formalisierte Informationspflicht des Arbeitgebers gegenüber den Betriebsräten im Hinblick auf Arbeitnehmerdatenverarbeitung außerhalb der Personalverwaltung ist zu etablieren, ist dies nicht notwendig. Der Arbeitgeber ist verpflichtet den Betriebsrat über sämtliche in seinen Aufgabenbereich fallende Angelegenheiten zu unterrichten. Im Hinblick auf das Mitbestimmungsrecht des § 87 Abs. 1 Nr. 6 BetrVG besteht bereits eine entsprechende Unterrichtungspflicht. Diese zu formalisieren würde den Arbeitgeber mit weiterer Bürokratie belasten.

DEUTSCHER BUNDESTAG
Ausschuss für
Arbeit und Soziales
16. Wahlperiode

Ausschussdrucksache 16(11)**1370**

7. Mai 2009

Stellungnahme

zur öffentlichen Anhörung von Sachverständigen am 11. Mai 2009 in Berlin zum

a) Antrag der Abgeordneten Brigitte Pothmer, Dr. Thea Dückert, Kerstin Andreae, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Rechte der Beschäftigten von Discountern verbessern - Drucksache 16/9101 -

b) Antrag der Abgeordneten Silke Stokar von Neuforn, Kerstin Andreae, Volker Beck (Köln), weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Persönlichkeitsrechte abhängig Beschäftigter sichern - Datenschutz am Arbeitsplatz stärken - Drucksache 16/9311 -

c) Antrag der Abgeordneten Jan Korte, Wolfgang Neskovic, Sevim Dagdelen, weiterer Abgeordneter und der Fraktion DIE LINKE.

Datenschutz für Beschäftigte stärken - Drucksache 16/11376 -

d) Antrag der Abgeordneten Gisela Piltz, Dr. Heinrich L. Kolb, Jens Ackermann, weiterer Abgeordneter und der Fraktion der FDP

Schutz von Arbeitnehmerdaten durch transparente und praxisgerechte Regelungen gesetzlich absichern - Drucksache 16/12670 -

Berufsverband der Datenschutzbeauftragten e.V.

Allgemeines

Der BvD e.V. bestätigt den in allen Drucksachen zum Ausdruck gekommenen Handlungsbedarf. Der BvD e.V. ist erstaunt darüber, wie groß anlässlich der jüngsten Datenschutzpannen die Un-sicherheit im Umgang mit datenschutzrechtlichen Vorschriften selbst bei Konzernen wie der Telekom oder der Bahn AG zwischenzeitlich geworden zu sein scheint. Der BvD e.V. stellt in Deutschland insgesamt ein sich kontinuierlich verschlechterndes Datenschutzniveau im Verhältnis zwischen Arbeitgeber/Arbeitnehmer fest, welches im Wesentlichen auf Unkenntnis der bestehenden Regelungen und der vielfältigen verschiedeninstanzlichen Rechtsprechung im Arbeitnehmerdatenschutzrecht bei den Parteien zurückzuführen ist. Der BvD e.V. betrachtet sich nicht als politische Instanz zur Vertretung von Arbeitnehmer- oder Arbeitgeberinteressen. Er nimmt hierzu, soweit die Bundestagsdrucksachen hierauf eingehen, keine Stellung.

Arbeitnehmerdatenschutz

Der BvD e.V. empfiehlt zur Erlangung von Rechtssicherheit und Rechtsklarheit in Bezug auf den Umgang mit Personendaten im Arbeitsverhältnis die Schaffung eines verbindlichen gesetzgeberischen Regelwerks wie es als Konzept von Mitgliedern des BvD entwickelt wurde und in der Anlage beigefügt ist. An der Entwicklung waren Juristen, Betriebswirte und EDV-Experten beteiligt. Bei den Beteiligten handelte es sich vorwiegend um interne oder externe Datenschutzbeauftragte - auch solchen von Großunternehmen wie ABB oder Metro AG.

Die Situation zum Arbeitnehmerdatenschutz lässt sich wie folgt zusammenfassen:

1. Die vorhandene Fülle von Urteilen und Literatur zu einzelnen Aspekten des Arbeit-nehmerdatenschutzes aber auch die zum großen Teil unspezifischen gesetzlichen Regelungen führen bis heute zu erheblicher Unsicherheit in Fragen des Datenschutzes im Arbeitsverhältnis, da mit ihnen praktikable allgemeinverbindliche Lösungen für den Einzelfall nicht einhergehen.

2. Die Rechtsunklarheit wird auch nicht durch das Bundesdatenschutzgesetz gelöst, da dieses keine spezifischen Regelungen enthält, die das Arbeitsverhältnis abbilden.

3. Das Arbeitsverhältnis ist eine der existenziell wichtigsten gesellschaftlichen Beziehung von Bürgern und Institutionen untereinander. Es erfordert entsprechend seiner Bedeutung klare Regelungen in Form

von Erlaubnis- und Verbotstatbeständen, in Bezug auf die darin anfallenden personenbezogenen Daten. Es muss klar erkennbar sein, welche Daten welchen Schutz erfahren müssen und welche Arbeitnehmerdaten wie, wo und in welcher Weise genutzt werden können bzw. dürfen.

4. Schon jetzt fällt im Arbeitsverhältnis eine fast unüberschaubare Menge von Daten an. Eine sich immer weiter entwickelnde Technik stellt immer höhere Anforderungen an den Datenschutz gerade im Verhältnis Arbeitgeber-/Arbeitnehmer, da auch in den Unternehmen immer größere verkettbare Datenmengen entstehen, die bei unkritischer Nutzung das Risi-ko von Datenschutzverletzungen vergrößern. Der BvD e.V. geht davon aus, dass prinzipiell kein Arbeitgeber an einer rechtswidrigen Nutzung vorhandener Daten interessiert ist bzw. diese in Kauf nehmen würde.
5. Detailregelungen deren Notwendigkeit sich aus den oben angesprochenen Punkten ergeben, enthält das bereits erwähnte anliegende Regelungskonzept, dessen maßgeblicher Inhalt aus dem Inhaltsverzeichnis erkennbar ist.

Berufsstandards als Qualitätsvoraussetzung einer erfolgreichen Beauftragtenstellung

Zwischenzeitlich vom BvD e.V. entwickelte Berufsstandards (Anlage) werden ein Qualitätsniveau für die Ausübung des Berufs gewährleisten, das geeignet ist, den intern oder extern bestellter Datenschutzbeauftragten fachlich kompetent aufzutreten zu lassen. Hieran mangelt es in den meisten Fällen. Ein nur schwach oder gar nicht qualifizierter Datenschutzbeauftragter stellt nach Erkenntnissen des BvD e.V. regelmäßig ein erhebliches datenschutzrechtliches Risiko für die Betroffenen und auch das Unternehmen dar. Dieses scheint sich vor dem Hintergrund wachsender Datenmengen und deren Verknüpfungsmöglichkeit permanent zu bestätigen. Mangels einer Berufsordung bzw. anerkannten allg. Berufs - und Ausbildungsstandards ist es den Unternehmen derzeit nicht möglich, die vorhandene Qualifikation der bestellten Datenschutzbeauftragten zu überprüfen.

Der BvD e.V. empfiehlt daher dringend die Einführung von allgemeinverbindlichen Berufsstandards für den Datenschutzbeauftragten.

Anlage

BvD Leitlinien zum Beruf des Datenschutzbeauftragten

1. Die Tätigkeit des Datenschutzbeauftragten ist darauf gerichtet, die Grundrechte, insbesondere in Form des Rechts auf informationelle Selbstbestimmung, zu sichern. Er gewährleistet den grundrechtssicheren Umgang mit persönlichen Daten in Unternehmen und Behörden.
2. Der Datenschutzbeauftragte arbeitet darauf hin, das Vertrauen von Bürgern, Kunden und Beschäftigten in die Datenverarbeitung des jeweiligen Unternehmens bzw. der Behörde zu stärken. Er bewirkt außerdem, Risiken von Datenmissbrauch in Unternehmen und Behörden zu minimieren.
3. Der Datenschutzbeauftragte verfügt ungeachtet von Branche und Größe des Unternehmens bzw. der Behörde über umfassendes Fachwissen sowie Fertigkeiten und Fähigkeiten.
4. Der Datenschutzbeauftragte übernimmt nur dann eine Bestellung, wenn er fachlich und organisatorisch dazu in der Lage ist, alle damit verbundenen Aufgaben zu erfüllen.
5. Zu den Kernaufgaben des Datenschutzbeauftragten gehören das Prüfen von Verfahren der Geschäftsprozesse, der internen Regelungen und Verträge sowie der IT-Systeme. Außerdem gestaltet er die Datenschutzorganisation mit, schult und sensibilisiert die Beschäftigten, wirkt bei der datenschutzgerechten Gestaltung von Betriebs- bzw. Behördenprozessen mit, initiiert Prozesse zur Umsetzung des Datenschutzes und informiert und berichtet regelmäßig.
6. Der Datenschutzbeauftragte übt seinen Beruf unabhängig aus. Sein Fachwissen ist die wichtigste Grundlage für die unabhängige Berufsausübung. Er ist fachlich weisungsfrei tätig. Er hat eine beratende, keine umsetzende Funktion.
7. Der Datenschutzbeauftragte ist verantwortlich für seine Tätigkeit und haftet für die Qualität und die Richtigkeit seiner Beratung. Er ist verschwiegen. Er ist loyal gegenüber den Interessen der Betroffenen. Er vermeidet Interessenkollisionen. Er fordert aktiv alle notwendigen Informationen zu seiner Aufgabenerfüllung ein.
8. Die Anforderungen des Bundesverfassungsgerichtes, der EU-Datenschutzrichtlinie und der Bundes- und Landesdatenschutzgesetze an den Beruf werden durch die Berufsgrundsätze konkretisiert.
9. Die Berufsgrundsätze beschreiben die Tätigkeiten und Fähigkeiten des Datenschutzbeauftragten und grenzen von untypischen oder unseriösen Berufsausübungen ab.

DEUTSCHER BUNDESTAG
Ausschuss für
Arbeit und Soziales
16. Wahlperiode

Ausschussdrucksache 16(11)**1371**

7. Mai 2009

Stellungnahme

zur öffentlichen Anhörung von Sachverständigen am 11. Mai 2009 in Berlin zum

a) Antrag der Abgeordneten Brigitte Pothmer, Dr. Thea Dückert, Kerstin Andreae, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Rechte der Beschäftigten von Discountern verbessern - Drucksache 16/9101 -

b) Antrag der Abgeordneten Silke Stokar von Neuforn, Kerstin Andreae, Volker Beck (Köln), weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Persönlichkeitsrechte abhängig Beschäftigter sichern - Datenschutz am Arbeitsplatz stärken - Drucksache 16/9311 -

c) Antrag der Abgeordneten Jan Korte, Wolfgang Neskovic, Sevim Dagdelen, weiterer Abgeordneter und der Fraktion DIE LINKE.

Datenschutz für Beschäftigte stärken - Drucksache 16/11376 -

d) Antrag der Abgeordneten Gisela Piltz, Dr. Heinrich L. Kolb, Jens Ackermann, weiterer Abgeordneter und der Fraktion der FDP

Schutz von Arbeitnehmerdaten durch transparente und praxisgerechte Regelungen gesetzlich absichern - Drucksache 16/12670 -

der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Gesetzlich geregelter Arbeitnehmerdatenschutz - dringender denn je

I. Ausgangssituation

Das in Art. 2 i.V.m. Art. 1 GG verankerte allgemeine Persönlichkeitsrecht ist Grundlage des Grundrechts auf informationelle Selbstbestimmung) Grundrecht auf Datenschutz). Als Menschenrecht gewährleistet es die Würde, Privatsphäre und Handlungsfreiheit der von jedermann. Die Arbeitswelt ist hiervon nicht ausgenommen.

Persönlichkeitsrechte, insbesondere das Recht auf Datenschutz, sind im Arbeitsverhältnis in vielfältiger Weise betroffen:

Während eines Berufslebens sammelt sich über jeden Beschäftigten umfangreiches Datenmaterial bei Arbeitgebern an. Sie erhalten im Rahmen von Bewerbung Angaben über Schulbildung, berufliche Ausbildung, bisherige Tätigkeiten etc.. In der Regel finden sich diese Angaben in den Personalakten der Mitarbeiterinnen und Mitarbeiter. Diese Angaben werden mit der Zeit immer weiter ergänzt, z. B. durch Leistungsbewertungen und Beurteilungen, Gehaltsdaten, Fehlzeiten, Krankmeldungen und Urlaubdaten. Zudem werden in anderen Bereichen des Betriebes oder der Behörde Mitarbeiterdaten erfasst:

- in Arbeitszeiterfassungssystemen Daten über die An- bzw. Abwesenheit erhoben und in Arbeitszeitkonten übermittelt.
- digitale Telefonanlagen registrieren die Verbindungsdaten der Telekommunikation der Mitarbeiterinnen und Mitartbeiter.
- bei der Nutzung des Internets fallen Daten über E-Mails und das Surfverhalten an.
- Computer- und Kassensysteme ermöglichen die direkte Erfassung von Leistungsparametern – z.B. zu den von einer Schreibkraft eingegebenen Zeichen und zur Fehlerhäufigkeit. Immer mehr Arbeitsplätze werden durch Videokameras überwacht.
- über Controllingverfahren werden Leistung und das Verhalten von Beschäftigten überwacht.

Die ließe ließ sich fortsetzen.

Informationstechnische Systeme, die eine immer größere Überwachungsdichte ermöglichen, haben schleichend

Besitz vom beruflichen Alltag ergriffen. Unternehmen und ihre Beschäftigten laufen dabei Gefahr, sich an immer umfassendere Kontrollen und an permanente Überwachung zu gewöhnen.

Bislang zielgerichtete Überwachung von Beschäftigten wird zunehmend ausgeweitet und durch sog. Screening-Verfahren werden rasterfahndungsähnlich alle Arbeitnehmerinnen und Arbeitnehmer eines Unternehmens in Überwachungsmaßnahmen einbezogen. Hinter derartigen Überwachungsmaßnahmen steckt nicht immer böser Wille des Arbeitgebers, sondern in aller Regel vielfältige andere Zwecke (z.B. Korruptionsbekämpfung im Unternehmen etc.) und – ganz banal – die sich immer rascher entwickelnden technischen Möglichkeiten Der Einsatz von Informationstechnik für Kontrollzwecke wird immer billiger, einfacher in der Anwendung, komplexer, intelligenter und immer stärker vernetzt. Das technologisch bedingt immer umfangreichere Datenaufkommen trifft auf die Begehrlichkeit nach immer umfassenderer Überwachung.

II. Fehlende Regelungen zum Arbeitnehmerdatenschutz

1. Rechtsprechung ist lückenhaft und Einzelfallbezogen

Es gibt bis heute bedauerlicherweise keine speziellen gesetzlichen Regelungen zum Arbeitnehmerdatenschutz. Arbeitnehmer und Arbeitgeber sind daher im Wesentlichen darauf angewiesen, sich an der lückenhaften und im Einzelfall für die Betroffenen nur schwer zu erschließenden einschlägigen Rechtsprechung zu orientieren.

2. Einwilligung der Beschäftigten nur eingeschränkt sinnvoll

Einwilligung – ein ansonsten durchaus sinnvoller Ansatz, der die Datenverarbeitung außerhalb gesetzlicher Regelungen nur zulässt, wenn der Betroffene eingewilligt hat – ist im Arbeitsverhältnis nur sehr eingeschränkt sinnvoll. Die Einwilligung des BDSG setzt die Möglichkeit *freier* Entscheidung voraus. Arbeitnehmer können im Regelfall nicht wirklich frei von Zwang entscheiden. Welcher Arbeitnehmer kann sich in der heutigen Zeit der hohen Arbeitslosenzahlen schon seinem Arbeitgeber entgegenstellen, um seine Privatsphäre zu schützen. Im Regelfall ist die Furcht vor Repressalien bis hin zum Verlust des Arbeitsplatzes größer sein.

3. Tragweite der Einwilligung nicht absehbar

Ein weiterer Aspekt ist, dass die Arbeitnehmerin/der Arbeitnehmer die Tragweite der Einwilligung zur Nutzung eines neuen informationstechnischen Systems, einer Software oder eines neuen Verfahrens oftmals nicht erkennen kann. Häufig ist ihr/ihm gar nicht bewusst, dass hier ihr/sein informationelles Selbstbestimmungsrecht tangiert wird. Welche/r Beschäftigte weiß schon Bescheid über die genauen Datenflüsse bei Einführung und Betrieb von Personalverwaltungs- oder Personalinformationssystemen oder beim Einsatz von Videotechnik am Arbeitsplatz und die damit verbundenen Risiken für die Persönlichkeitsrechte.

4. Beteiligung der Interessenvertretungen

Die Einführung automatisierter Systeme unterliegt in weiten Bereichen der Mitbestimmung des Betriebs- oder Personalrats. Das Betriebsverfassungsgesetz wie die Personalvertretungsgesetze des Bundes und der Länder verpflichten Arbeitgeber/Dienstherr und Betriebs- bzw. Personalrat, „die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern“. Hierzu gehört auch das Recht auf informationelle Selbstbestimmung.

Mitbestimmungsrechte bestehen etwa, wenn technische Einrichtungen eingeführt werden, mit der sich das Verhalten oder die Leistung der Mitarbeiterinnen und Mitarbeiter kontrollieren oder messen lässt. Dabei muss die Möglichkeit der Verhaltens- oder Leistungskontrolle noch nicht einmal der eigentliche Sinn und Zweck der Einführung derartiger Verfahren sein; es reicht aus, dass – sozusagen als Nebenprodukt – eine solche Verhaltens- oder Leistungskontrolle ermöglicht wird. So müssen Betriebs- oder Personalräte zustimmen, wenn Mitarbeiterinnen und Mitarbeiter Internetdienste (www, E-Mail) nutzen dürfen oder sollen oder ein Controllingsystem (z.B. Gleitzeituhren) eingeführt werden soll. Für die Einführung solcher Systeme sind Regelwerke (insbesondere in der Form von Betriebs- bzw. Dienstvereinbarungen) zu erstellen, die detailliert beschreiben, wie die Systeme zu nutzen sind und welche Konsequenzen Missbrauch zur Folge hat.

In vielen Unternehmen und Behörden achten die Arbeitnehmervertretungen mit Argusaugen auf die Gewährleistung des Arbeitnehmerdatenschutzes. Diese Kontrolle entfällt aber regelmäßig, wenn ein Betrieb wegen seiner geringen Größe oder aus anderen Gründen keinen Betriebsrat hat. Auch betriebliche Datenschutzbeauftragte leisten wertvolle Hilfestellung. In manchen Unternehmen fehlt allerdings auch diese unternehmensinterne Kontrollinstanz, weil die Voraussetzungen für die Bestellung eines Datenschutzbeauftragten nicht gegeben sind (§ 4f BDSG) oder weil ein solcher entgegen den gesetzlichen Vorgaben nicht ernannt wurde. In diesen Fällen sind die Beschäftigten darauf angewiesen, den Beteuerungen der Unternehmensleitung zu glauben. Zwar kann sich jedermann an die zuständige Datenschutzaufsichtsbehörde wenden, falls er vermutet, dass gegen Datenschutzbestimmungen verstoßen wird. Im betrieb-behördlichen Alltag sind allerdings – wohl aus der verständlichen Angst vor Repressalien – nur wenige Beschäftigte zu diesem Schritt bereit.

5. Arbeitnehmerdatenschutzgesetz dringend erforderlich

Um den Schutz der informationellen Selbstbestimmung und damit der Persönlichkeit der Beschäftigten nicht von all diesen Unwägbarkeiten abhängig zu machen, fordern die Datenschutzbeauftragten des Bundes und der Länder seit vielen Jahren gesetzliche Regelungen zum Arbeitnehmerdatenschutz (vgl. zuletzt meinen 22. Tätigkeitsbericht Nr. 1.1 sowie die Entschließung der 77. Konferenz der Datenschutzbeauftragten von Bund und Ländern - Anlage -).

Obwohl der Deutsche Bundestag entsprechende Forderungen wiederholt mit großen, fraktionsübergreifenden Mehrheiten unterstützt hat, hatten die verschiedenen Bundesregierungen bislang keine konkreten Aktivitäten auf diesem Gebiet entwickelt. In ihrer Stellungnahme zum 21. Tätigkeitsbericht hat sich die Bundesregierung dahingehend geäußert, dass sie die Auffassung des BfDI teile, dass ein Gesetz zum Schutze der Arbeitnehmerdaten notwendig sei. Das vom Bundesminister des Innern im Februar 2009 initiierte Spitzengespräch mit dem Bundesministern für Arbeit und Wirtschaft, den Arbeitgeberverbänden, den Gewerkschaften und dem Bundes-

beauftragten für den Datenschutz und die Informationsfreiheit ist ein hoffnungsvoller Schritt auf dem Weg zu den dringend benötigten gesetzlichen Regelungen zum Schutze der Daten von Arbeitnehmern. Diesem ersten Schritt müssen allerdings auch weitere Schritte folgen.

Angesichts stetig wachsender technischer Möglichkeiten muss klar geregelt werden, welche Daten Unternehmen über ihre Beschäftigten erheben und verwenden dürfen. Die Achtung des Grundrechts auf Datenschutz der Arbeitnehmer zählt ebenso zu guten und fairen Arbeitsbedingungen wie Chancengleichheit oder gerechte Bezahlung. Beschäftigtendatenschutz erhöht zudem die Motivation, trägt und fördert die Arbeitszufriedenheit und bedeutet damit auch für die Unternehmen einen nicht zu unterschätzenden Standortvorteil.

Darüber hinaus muss eine Stärkung des betrieblichen Datenschutzbeauftragten erfolgen. Dazu gehört, dass er vor der Umsetzung betrieblicher Maßnahmen umfassend beteiligt wird und einen wirksamen Kündigungsschutz genießt. Nachgedacht werden sollte auch darüber, ob künftig dem Betriebs-/Personalrat ein Mitwirkungsrecht bei der Bestellung des betrieb-/behördlichen Datenschutzbeauftragten zugestanden wird. Schon heute sollte der Betriebs-/Personalrat eine enge Zusammenarbeit mit dem betrieb-/behördlichen Datenschutzbeauftragten einfordern. Auch dies sollte auf eine gesetzliche Grundlage gestellt werden.

Aus diesen Überlegungen resultieren die folgenden

III. Forderungen an ein Arbeitnehmerdatenschutzgesetz

- Personenbezogene Daten des Arbeitnehmers dürfen nur erhoben, verarbeitet und genutzt werden, wenn dies zur Begründung, Durchführung, Beendigung oder Abwicklung eines Arbeitsverhältnisses erforderlich oder sonst gesetzlich vorgeschrieben ist.
- Personenbezogene Arbeitnehmerdaten dürfen nur für den Zweck, für den sie erhoben worden sind, verwendet werden. Daten, die für diesen Zweck nicht mehr erforderlich sind, sind zu löschen.
- Die Datenerhebung hat grundsätzlich beim Arbeitnehmer selbst zu erfolgen.
- Arbeitnehmer sind umfassend darüber zu informieren, welche Daten zu welcher Zeit, auf welche Weise und zu welchem Zweck über sie erhoben und in welcher Art und Weise sie ausgewertet werden. Dies schließt umfassende Auskunfts- und Einsichtsrechte des Arbeitnehmers ein.
- Der Umfang des Fragerechts bei Einstellungen ist klar zu regeln
- Einstellungstests haben sich auf das unbedingt notwendige Maß bezogen auf den konkreten Arbeitsplatz zu beschränken.
- Graphologische Gutachten und Gentests sind grundsätzlich zu verbieten.
- Die Erhebung, Verarbeitung und die Pflicht zur Löschung von Daten im Rahmen von Bewerbungen und Einstellungen muss klar geregelt werden.
- Die Voraussetzungen zur Überwachung des Telefon-, Internet- und E-Mail Verkehrs am Arbeitsplatz sind eindeutig festzulegen
- Heimliche Kontrollen und Überwachungen sind grundsätzlich unzulässig.
- Leistungs- und Verhaltenskontrollen sind nur unter streng geregelten Umständen erlaubt.
- Kontrollen durch optisch-elektronische Einrichtungen, ortungs- oder biometriegestützter Systeme sind nur nach klar erkennbaren Regeln zulässig.
- Der Schutz der Beschäftigtendaten bei Übermittlungen zur Weiterverarbeitung im In- und Ausland ist sicherzustellen.
- Für unrechtmäßig erhobene Daten ist ein Beweisverwertungsverbot festzulegen. Bei Verletzung des Persönlichkeitsrechts steht dem Beschäftigten ein Schadensersatzanspruch zu.
- Verstöße gegen das Arbeitnehmerdatenschutzgesetz sind mit wirksamen Sanktionen zu belegen.
- Verpflichtung zur Bestellung einen unabhängigen betrieblichen Datenschutzbeauftragten mit umfassenden Kontrollbefugnissen.
- Die Interessenvertretungen sind bei der Bestellung des betrieblichen Datenschutzbeauftragten und bei allen datenschutzrelevanten Entscheidungen zu beteiligen zu beteiligen.

Anlage

11 Mitarbeiterdatenschutz

11.1 Dringender Handlungsbedarf beim

Arbeitnehmerdatenschutz

Eine Reihe von Vorfällen zeigt, dass die Datenschutzkultur in manchen Unternehmen zu wünschen übrig lässt. Insbesondere der Schutz der Arbeitnehmer bedarf größerer Aufmerksamkeit. Deshalb muss das seit langem geforderte Arbeitnehmerdatenschutzgesetz endlich realisiert werden.

Nahezu jeder Arbeitsplatz ist heute mit einem Internet-Zugang ausgestattet, an dem man surfen und auch E-Mail verschicken kann. Wird die Nutzung des Computers protokolliert, sagt das viel über den Arbeitnehmer aus. Mit geringem Aufwand kann heutzutage nahezu der gesamte Büroalltag lückenlos überwacht werden. Texte lassen sich auf Schlagworte hin absuchen, die Zahl der Tastenanschläge und die Fehleingaben geben Auskunft über das Tempo und die Qualität der Arbeit. Mit Netzwerkanalysen können Chefs herausfinden, wer wen im Unternehmen um Rat fragt. Beschäftigtendaten werden nicht mehr nur in Akten, sondern auch in leistungsfähigen Personalinformationssystemen gesammelt, die sich zur Erstellung von Persönlichkeitsprofilen eignen. Immer häufiger kommen offen oder heimlich installierte Videokameras zum Einsatz, die die Überwachung des Arbeits- und Pausenverhaltens ermöglichen.

Das rasante Anwachsen von Datenbeständen, deren fortschreitende Vernetzung und der hohe ökonomische Wert von personenbezogenen Daten multiplizieren das Gefahren- und Missbrauchspotential. Oft werden technische Systeme nicht in erster Linie zur Überwachung der Mitarbeiter eingeführt, sondern zur Kontrolle von Betriebsabläufen, zur Verhinderung von Kundendiebstählen oder zur Sicherung gefährdeter Räume, wie z. B. Kassenbereichen. So nützlich solche Systeme erscheinen, darf es bei ihrem Einsatz keine heimliche Überwachung

der Arbeitnehmer geben. Ausnahmen müssen sich auf klar definierte Fälle beschränken, z. B. bei Vorliegen konkreter Verdachtsmomente.

Von besonderer Bedeutung ist eine strikte Zweckbindung bei der Verarbeitung und Nutzung von Arbeitnehmerdaten. Betriebs- und Dienstvereinbarungen, die genau festschreiben, welche Arten der Registrierung und Auswertung von Daten über Beschäftigte erlaubt sind, können zur Rechtsklarheit für alle Beteiligten beitragen. Auch wenn so . bezogen auf das einzelne Unternehmen . ein verbesserter Schutz von Beschäftigtendaten erreicht werden kann, können betriebliche Regelungen klare gesetzliche Vorgaben zum Arbeitnehmerdatenschutz nicht ersetzen.

Es gibt keine speziellen gesetzlichen Regelungen für die Datenerhebung, -verarbeitung und -nutzung in einem Arbeitsverhältnis. Arbeitgeber und Arbeitnehmer müssen mit einer erheblichen Rechtsunsicherheit leben. Das Bundesdatenschutzgesetz mit seinen allgemeinen Regelungen sowie arbeitsrechtliche Vorschriften bieten nur unzureichenden Schutz. Arbeitnehmer und Arbeitgeber müssen sich im Wesentlichen an der zwar umfangreichen, aber lückenhaften und nur schwer erschließbaren Rechtsprechung orientieren.

Kasten zu Nr. 11.1

Forderungen an ein Arbeitnehmerdatenschutzgesetz

- Personenbezogene Daten des Arbeitnehmers dürfen nur erhoben, verarbeitet und genutzt werden, wenn dies zur Begründung, Durchführung, Beendigung oder Abwicklung eines Arbeitsverhältnisses erforderlich oder sonst gesetzlich vorgeschrieben ist.
- Die Datenerhebung erfolgt grundsätzlich beim Arbeitnehmer selbst.
- Personenbezogene Arbeitnehmerdaten dürfen nur für den Zweck, für den sie erhoben worden sind, verwendet werden. Daten, die für diesen Zweck nicht mehr erforderlich sind, sind zu löschen.
- Aus Gründen der Transparenz sind Arbeitnehmer umfassend darüber zu informieren, welche Daten zu welcher Zeit, auf welche Weise und zu welchem Zweck über sie erhoben und in welcher Art und Weise sie ausgewertet werden. Dies muss umfassende Auskunfts- und Einsichtsrechte des Arbeitnehmers einschließen.
- Die Rolle des betrieblichen Datenschutzbeauftragten ist zu stärken; seine umfassende Beteiligung vor der Umsetzung betrieblicher Maßnahmen ist sicher zu stellen.
- Dem Betriebsrat ist bei der Bestellung des betrieblichen Datenschutzbeauftragten ein Mitwirkungsrecht einzuräumen.
- Betriebsrat und betrieblicher Datenschutzbeauftragten sind zur engen Zusammenarbeit verpflichtet.

Auch Einwilligungen der Arbeitnehmer können Datenspeicherungen rechtfertigen, wenn sie auf einer freien Entscheidung des Betroffenen beruhen (§ 4a BDSG). Ob die Arbeitnehmer sich im Arbeitsleben aber frei entscheiden können, darf bezweifelt werden. Oftmals erkennen die Betroffenen auch die Tragweite der Einwilligung nicht. Betriebs- und Personalräte können zwar im Rahmen von Mitbestimmungsrechten einen gewissen Einfluss auf die Gewährleistung des Arbeitnehmerdatenschutzes nehmen. Es gibt allerdings nicht überall Arbeitnehmervertretungen und deren Handlungsmöglichkeiten sind begrenzt. Deshalb fordern die Datenschutzbeauftragten des Bundes und der Länder bereits seit Jahren bereichsspezifische Regelungen zum Arbeitnehmerdatenschutz. Der Bundesrat hat am 7. November 2008 (Bundesratsdrucksache 665/08) die Bundesregierung aufgefordert, angesichts der Vorfälle von Arbeitnehmerüberwachung in Unternehmen (Lidl, Telekom) und angesichts der für Arbeitgeber und Arbeitnehmer unübersichtlichen Rechtslage gesetzliche Regelungen zum Arbeitnehmerdatenschutz vorzulegen. Wiederholt hatte auch der Deutsche Bundestag mit großen fraktionsübergreifenden Mehrheiten die Bundesregierung aufgefordert, schnellstmöglich einen Gesetzentwurf zum Arbeitnehmerdatenschutz vorzulegen. Bleibt zu hoffen, dass die Bundesregierung endlich einen entsprechenden Gesetzentwurf vorlegt.

BfDI 22. Tätigkeitsbericht 2007-2008

Entschließung

der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. März 2009 in Berlin

Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz

Datenskandale der letzten Zeit haben deutlich gemacht, dass bei der Verarbeitung von Beschäftigtendaten weder Transparenz noch Rechtssicherheit besteht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, nach jahrelanger Untätigkeit jetzt unverzüglich einen entsprechenden Gesetzentwurf vorzulegen.

Ziel des neuen Beschäftigtendatenschutzgesetzes muss sein, Rechtssicherheit herzustellen, Regelungslücken zu schließen und bereits vorhandene Regelungsaspekte sowie Vorgaben der Rechtsprechung in einem Spezialgesetz zusammenzufassen. Die Konferenz der Datenschutzbeauftragten hält deshalb vor allem folgende Eckpunkte für unverzichtbar:

- Die Regelungen des Beschäftigtendatenschutzgesetzes müssen sowohl für die Beschäftigten der Privatwirtschaft als auch für die Beschäftigten im öffentlichen Dienst gelten.
- Es muss klar geregelt werden, welche Daten Unternehmen und öffentliche Stellen im Rahmen des Einstellungsverfahrens und im weiteren Verlauf des Arbeitslebens über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Es bedarf besonderer Festlegungen im Hinblick auf Gesundheitsdaten (u. a. zur Frage der Zulässigkeit von Drogen-Screening, psychologischen Testverfahren, ärztlichen Untersuchungen, etc.)
- Einen umfassenden anlass- und verdachtslosen Datenabgleich darf es nicht geben. Der Zugriff von Kontrollinstanzen wie z. B. der Innenrevision auf er-

hobene Personaldaten bedarf enger gesetzlicher Vorgaben.

- Moderne Informations- und Kommunikationstechnologien dürfen nicht zu lückenlosen Verhaltens- und Leistungskontrollen eingesetzt werden. Da die Nutzung von Telefon, Internet und E-Mail-Diensten nicht mehr aus dem Arbeitsleben wegzudenken ist, sind auch die Voraussetzungen für eine beschäftigtenbezogene Auswertung dieser Kommunikationsmittel eindeutig und restriktiv festzulegen. Dabei ist auch zu regeln, welcher Personenkreis solche Auswertungen durchführen darf und ab welchem Verfahrensstand ggf. Dritte (z. B. Mitarbeitervertretungen oder Datenschutzbeauftragte) hinzugezogen werden müssen. Auswertungen von Datenbeständen der Zugangs- und Personalinformationssysteme sind strikt zu begrenzen.
- Der Einsatz von Überwachungssystemen, wie z. B. Videokameras und Ortungssystemen, ist auf das unbedingt notwendige Maß zu beschränken und unter Wahrung der Beteiligungsrechte der Mitarbeitervertretungen zulässig. Die Verwendung biometrischer Verfahren bedarf besonders enger Vorgaben.
- Es bedarf der Festlegung der Rechte der Beschäftigten, z. B. im Hinblick auf Auskunfts-, Einsichts-, Widerrufs-, Berichtigungs-, Löschungs- und Schadensersatzansprüche.
- Der Schutz von Persönlichkeitsrechten der in Deutschland tätigen Beschäftigten weltweit agierender Unternehmen oder Konzerne ist sicherzustellen.
- Eine effektive Kontrolle durch die zuständigen Datenschutzbehörden muß gewährleistet werden. Die betrieblichen und behördlichen Datenschutzbeauftragten sind bei allen personaldatenschutzrechtlich relevanten Verfahren und Entscheidungen frühzeitig einzubinden und umfassend zu beteiligen. Ihre Rechte und Befugnisse gegenüber den Mitarbeitervertretungen sind gesetzlich festzulegen.
- Verstöße gegen die Bestimmungen des Beschäftigtendatenschutzgesetzes müssen ein gesetzliches Verwertungsverbot der dadurch gewonnenen Daten nach sich ziehen. Zur Abschreckung bedarf es wirksamer Sanktionen.

DEUTSCHER BUNDESTAG
Ausschuss für
Arbeit und Soziales
16. Wahlperiode

Ausschussdrucksache 16(11)**1372**

8. Mai 2009

Stellungnahme

zur öffentlichen Anhörung von Sachverständigen am 11. Mai 2009 in Berlin zum

a) Antrag der Abgeordneten Brigitte Pothmer, Dr. Thea Dückert, Kerstin Andreae, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Rechte der Beschäftigten von Discountern verbessern - Drucksache 16/9101 -

b) Antrag der Abgeordneten Silke Stokar von Neuforn, Kerstin Andreae, Volker Beck (Köln), weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Persönlichkeitsrechte abhängig Beschäftigter sichern - Datenschutz am Arbeitsplatz stärken - Drucksache 16/9311 -

c) Antrag der Abgeordneten Jan Korte, Wolfgang Neskovic, Sevim Dagdelen, weiterer Abgeordneter und der Fraktion DIE LINKE.

Datenschutz für Beschäftigte stärken - Drucksache 16/11376 -

d) Antrag der Abgeordneten Gisela Piltz, Dr. Heinrich L. Kolb, Jens Ackermann, weiterer Abgeordneter und der Fraktion der FDP

Schutz von Arbeitnehmerdaten durch transparente und praxisgerechte Regelungen gesetzlich absichern - Drucksache 16/12670 -

Dr. Martin Diller, Stuttgart

14 Thesen für ein modernes Arbeitnehmer-Datenschutzrecht

1. **Das Datenschutzrecht im Arbeitsverhältnis ist dringend reformbedürftig, insbesondere wegen der ungeklärten Überlagerung des Datenschutzrechts durch das Telekommunikationsrecht, die technische Entwicklung, die modernen arbeitsteiligen Konzernstrukturen sowie das ungeklärte Nebeneinander von Mitarbeitervertretungen und betrieblichen Datenschutzbeauftragten.**
2. **Ziel des Arbeitsnehmerdatenschutzrechts darf nicht sein, die Speicherung und Nutzung von Daten durch den Arbeitgeber auf das zur Vertragsdurchführung erforderliche Mindestmaß zu reduzieren. In einer sich immer schneller wandelnden Arbeitswelt kommt dem Arbeitgeber auch die Aufgabe zu, den Arbeitnehmer zu fördern, ihm neue Kenntnisse und Fertigkeiten zu vermitteln und ihm beruflichen Aufstieg und Weiterentwicklung zu ermöglichen. Das setzt voraus, dass der Arbeitgeber ausreichend über den Arbeitnehmer informiert ist.**
3. **Der besondere Schutz von Gesundheitsdaten ist wichtig. Zugleich sind die Arbeitgeber aber auch in der Pflicht, auf gesundheitliche Einschränkungen der Arbeitnehmer zu reagieren, z.B. durch betriebliche Umorganisation oder Versetzungen (vgl. das erst vor wenigen Jahren eingeführte betriebliche Eingliederungsmanagement in §§ 83, 84 SGB IX). Die Integration von Mitarbeitern mit körperlichen oder psychischen Einschränkungen darf nicht an überzogenem Datenschutzrecht scheitern.**
4. **Das Recht des Arbeitgebers, auf die Arbeitsvorgänge und -ergebnisse der Mitarbeiter jederzeit zuzugreifen, muss unangetastet bleiben. Ein Recht der Arbeitnehmer, ihre Arbeitsergebnisse und ihren Arbeitsplatz vor dem Arbeitgeber geheim zu halten, kann es nicht geben. Deshalb muss es ein uneingeschränktes Zugriffsrecht des Arbeitgebers auf alle geschäftlichen Vorgänge und insbesondere auch auf geschäftliche E-Mails geben.**
5. **Compliance ist, wie Fälle aus der jüngsten Zeit gezeigt haben, auch zukünftig ein wichtiges Thema. Unternehmen müssen sicherstellen, dass Mitarbeiter ihre Arbeit korrekt und im Einklang mit allen geltenden Gesetzen erledigen. Schlagkräftige interne Revisionsabteilungen werden künftig eher**

noch wichtiger werden als sie heute sind. Solche internen Revisionen dürfen nicht an überzogenen Datenschutzgrundsätzen scheitern.

6. **Flächendeckende Leistungs- und Verhaltenskontrollen durch elektronische Systeme tangieren das Persönlichkeitsrecht der Arbeitnehmer. In der Praxis hat sich das insoweit bestehende Mitbestimmungsrecht der Mitarbeitervertretungen (§ 87 Abs. 1 Nr. 6 BetrVG) als ausreichendes Instrument erwiesen, um angemessene Beschränkungen herbeizuführen. Weitergehender gesetzlicher Verbote bedarf es deshalb nicht.**

7. **Eine flächendeckende Videoüberwachung ist ein schwerwiegender Eingriff in das Persönlichkeitsrecht der Arbeitnehmer und kommt - entsprechend der vom Bundesarbeitsgericht aufgestellten Grundsätze - nur im Einzelfall und nur aufgrund besonderer Umstände in Betracht.**

8. **Angesichts der Schnelllebigkeit der Arbeitsabläufe und der Möglichkeiten der modernen Informationsgesellschaft ist eine Ex-ante-Zweckbindung jeder Datenspeicherung abzulehnen. Dürfte der Arbeitgeber Daten stets nur zu denjenigen Zwecken nutzen, die er bei der Datenerhebung definiert hat, müssten ständig Daten neu erhoben bzw. die Zustimmung der Arbeitnehmer eingeholt werden, was die betrieblichen Abläufe lahmlegen würde.**

9. **Eine Weiterleitung von Mitarbeiterdaten an Dritte im Wege der Auftragsdatenverarbeitung (§ 11 BDSG) muss zulässig bleiben, insbesondere damit kleine und mittlere Betriebe die immer komplizierter werdende Lohn- und Gehaltsbuchhaltung auch künftig auslagern können. Die Datenweitergabe in Konzernen ist, jedenfalls innerhalb Deutschlands und der EU, durch ein Konzernprivileg zu erleichtern. Die Weitergabe von Mitarbeiterdaten an Dritte zu vertragsfremden Zwecken (Werbung, Adresshandel) muss dagegen weiterhin untersagt sein.**

10. **Die derzeit bestehenden Sanktionen bei Verletzungen des Datenschutzgesetzes reichen aus. Verschärfte Strafen oder Bußgelder sind ebenso wenig erforderlich wie ein - dem deutschen Prozessrecht fremdes - prozessuales Verwertungsverbot.**

11. **Der Datenschutzbeauftragte sollte entsprechend der aktuellen Konzeption des BDSG eine auf die Rechtmäßigkeitsprüfung beschränkte Institution bleiben. Eine Einbeziehung des Datenschutzbeauftragten bei Ermessensentscheidungen ist systemfremd und abzulehnen.**

12. **Ein Mitbestimmungsrecht der Mitarbeitervertretungen beim Datenschutz wäre systematisch verfehlt. Nach der Konzeption von BetrVG und den PersVG sind die Mitarbeitervertretungen für die Vertretung der Mitarbeiterinteressen bei Ermessensentscheidungen zuständig. Eine Einbindung in die Beurteilung reiner Rechtsfragen sehen BetrVG und PersVG nicht vor. Daran sollte nicht gerüttelt werden, zumal Arbeitnehmerdaten in den meisten Unternehmen (z.B. Banken, Versicherungen) nur einen Bruchteil der insgesamt anfallenden personenbezogenen Daten ausmachen. Der Betriebsrat ist nicht der bessere Datenschutzbeauftragte.**

13. **Datenschutzrecht wird immer ein Abwägungsrecht bleiben. Es ist nicht möglich, alle denkbaren Fragen präzise zu regeln. Deshalb sollte sich auch das neu zu schaffende Arbeitnehmerdatenschutzrecht auf Abwägungsgrundsätze beschränken und keine Überregulierung versuchen, die aufgrund der technischen Entwicklung und der Veränderung der betrieblichen Verhältnisse rasch überholt wäre.**

14. **Eine Überinformation der Belegschaften, insbesondere durch laufende schriftliche Informationspflichten des Arbeitgebers, verbessert nichts und sollte vermieden werden. Auskunftsrechte sind genauso effektiv wie Informationspflichten, reduzieren aber die betriebliche Bürokratie erheblich.**

A. Vorbemerkungen zu den Anträgen der BT-Drucksache 16/9101, 9311 und 11376

I. Die Anträge erwecken den Eindruck, dass es bei sogenannten „Discountern“ besonders gravierende Schutzlücken beim Arbeitsrecht, insbesondere beim Arbeitnehmerdatenschutz sowie bei Betriebsratsgründungen gibt. Für diese These gibt es keinen Beleg. Tatsächlich spricht alles dafür, dass die arbeitsrechtlichen und datenschutzrechtlichen Verhältnisse in den Filialen von **Discountern** sich nicht wesentlich von den arbeitsrechtlichen und datenschutzrechtlichen Bedingungen in vergleichbar großen anderen Unternehmen und Betrieben unterscheiden. So zeigt das verfügbare statistische Material beispielsweise, dass das Nichtbestehen von Betriebsräten in Betrieben bis 50 Mitarbeiter geradezu die Regel ist; Discounter-Filialen haben häufig nur zwischen fünf und zehn Mitarbeiter. Es spricht viel dafür, dass Discounter nur deshalb im Brennpunkt der aktuellen arbeitsrechtlichen und datenschutzrechtlichen Diskussion stehen, weil von Gewerkschaftsseite wegen der größeren Öffentlichkeitswirkung vermeintliche Missstände immer dann besonders vehement angeprangert werden, wenn es sich um Unternehmen handelt, deren Namen jeder kennt.

II. Dass das **Datenschutzrecht**, bezogen auf das Arbeitsverhältnis, **dringend reformbedürftig** ist, wird von niemandem bestritten. Die datenschutzrechtlichen Regeln des Betriebsverfassungsgesetzes sind völlig veraltet, das Gesetz stammt von 1972 und ist nie grundlegend an die elektronische Revolution angepasst worden. Das Bundesdatenschutzgesetz behandelt den Datenschutz im nicht-öffentlichen Bereich nur sehr rudimentär (§§ 27 und 28 BDSG) und diese Normen stellen auch nur allgemeine Regeln für den Datenschutz in „Vertragsverhältnissen“ auf, ohne zwischen Mietverträgen, Zeitungsabonnementsverträgen oder Arbeitsverträgen zu differenzieren. Zudem hat der Zugriff der Arbeitnehmer auf E-Mail und Internet dazu geführt, dass die vorhandenen betriebsverfassungsrechtlichen und datenschutzrechtlichen Regeln zusätzlich überlagert werden durch telekommunikationsrechtliche Normen. Das Zusammenspiel dieser Normenkomplexe bewirkt Unklarheit und Rechtsunsicherheit. Nach den bestehenden Normen sind einerseits harmlose und im Betriebsinteresse dringend erforderliche Verfahren verboten oder wer-

den gar kriminalisiert, während andererseits Schutzlücken bestehen. Die unzweifelhaft bestehende dringliche gesetzgeberische Aufgabe, ein einheitliches, in sich geschlossenes „Datenschutzrecht des Arbeitsplatzes“ zu schaffen, darf also nicht dahingehend missverstanden werden, dass es nur darum ginge, das bestehende Datenschutzniveau zugunsten der Arbeitnehmer zu verbessern. Genauso wichtig ist es, an anderer Stelle widersinnige und dem wohlverstandenen Unternehmenswohl und damit auch der Arbeitsplatzsicherung zuwiderlaufende datenschutzrechtliche Hürden behutsam zurückzuschneiden (z.B. künftig erleichterte Datenweitergabe im Konzern bei zentralisierter Personalverwaltung und Lohnbuchhaltung).

Im Einzelnen ist zu den Drucksachen Folgendes zu sagen:

B. Drucksache 16/9101 Rechte der Beschäftigten von Discountern verbessern

I. Feststellungen

S. oben A.I., II.

II. Vorschläge

1. a. Erleichterung von Betriebsratswahlen

Bedarf für die Erleichterung der Einleitung von Betriebsratswahlen ist nicht ersichtlich. Bereits nach der aktuellen Rechtslage kann eine im Betrieb vertretene Gewerkschaft (im Einzelhandel durchweg ver.di) die Errichtung eines Betriebsrats herbeiführen, wenn auch nur ein einziger Arbeitnehmer des jeweiligen Betriebs mitmacht. Die Gewerkschaft kann zu einer Versammlung der Mitarbeiter einladen, auf der ein Wahlvorstand bestellt wird. Kommt die Bestellung des Wahlvorstands nicht zustande (z.B. weil sich die Mehrheit der anwesenden Mitarbeiter gegen die Durchführung einer Betriebsratswahl ausspricht), kann die Gewerkschaft durch das Arbeitsgericht einen Wahlvorstand bestellen lassen. Es ist nicht ersichtlich, wie das Verfahren noch weiter zugunsten einer gewerkschaftlichen Initiative vereinfacht werden sollte.

Überdies ist es nach der Konzeption des deutschen Betriebsverfassungsrechts ganz bewusst den Mitarbeitern selbst überlassen, ob sie einen Betriebsrat errichten wollen oder nicht. Der Gesetzgeber hat bewusst davon Abstand genommen, in Betrieben oberhalb einer bestimmten Größenordnung die Belegschaften oder den Arbeitgeber zu zwingen, für die Errichtung eines Betriebsrats zu sorgen.

Kein Bedarf ist dafür ersichtlich, als Mitglieder des Wahlvorstands auch nicht im Betrieb beschäftigte Gewerkschaftsvertreter zuzulassen. Betriebsratswahlen scheitern erfahrungsgemäß nicht daran, dass sich niemand finden würde, der in den Wahlvorstand geht. Ganz im Gegenteil streben die Initiatoren einer Betriebsratswahl immer an, auch im Wahlvorstand vertreten zu sein, schon wegen des verbesserten Kündigungsschutzes nach § 15 KSchG. Überdies ist Aufgabe des Wahlvorstands insbesondere die sachgerechte Ermittlung der für die Wahl wesentlichen Fakten (z.B. Beschäftigtenzahl, Anzahl der zu wählenden Betriebsratsmitglieder, Festlegung der Betriebsgrenzen in filialisierten Unternehmen etc.). Dabei kann sich der Wahlvorstand der Hilfe der Gewerkschaften bedienen. Es ist aber nicht notwendig und entspricht auch nicht der gesetzgeberischen Intention, die Durchführung der Wahl in die Hand der Gewerkschaft zu legen.

Überdies ist der Gesetzgeber dort, wo er Gewerkschaftsrechte in der Betriebsverfassung vorgesehen hat, bei der Schaffung des BetrVG im Jahr 1972 stillschweigend vom Gewerkschaftsmonopol der DGB-Gewerkschaften ausgegangen (was damals den faktischen Umständen durchaus entsprach). Derzeit erleben wir aber eine Aufsplitterung der Gewerkschaftslandschaft, nicht nur durch christliche Gewerkschaften (die es seit dem Kaiserreich gibt), sondern auch durch Berufs- und Spartengewerkschaften. Überall dort, wo der Gesetzgeber der Gewerkschaft Rechte in der Betriebsverfassung einräumt, wird deshalb über kurz oder lang die Frage auftauchen, welche von mehreren konkurrierenden Gewerkschaften denn die Rechte wahrnehmen soll. Die Gewerkschaftsrechte im Betrieb zu stärken, kann deshalb langfristig Streitereien eher vermehren als vermindern.

1. b. Verschärfung der Straf- und Bußgeldvorschriften bei Behinderung der Betriebsratswahl oder der Betriebsratstätigkeit

Die Forderung ist populistisch. Die Höhe der bestehenden Sanktionen (insbesondere für Ordnungswidrigkeiten nach § 119 BetrVG) ist mit EUR 250.000 absolut ausreichend.

In der Praxis ist die Verhängung von Geldbußen wegen der genannten Ordnungswidrigkeiten fast immer ein Beweisproblem (Beispiel: Ist die fristlose Kündigung eines Mitarbeiters wegen einer Unterschlagung, der kurz zuvor Unterschriften für eine Betriebsratswahl gesammelt hat, gezielt auf Behinderung der Betriebsratswahl ausgerichtet oder nicht?). Höhere Geldbußen erleichtern die Wahrheitsfindung nicht.

Allerdings hat der Fall Volkerts/VW gezeigt, dass die §§ 119 ff. BetrVG einen gravierenden Webfehler insofern haben, als **nur der Arbeitgeber** bestraft wird, der Betriebsräte um ihrer Arbeit willen begünstigt, **nicht** aber **das Betriebsratsmitglied**, welches die Vergünstigung annimmt oder gar fordert. Wenn die Straf- und Bußgeldvorschrift überarbeitet werden sollen, wäre diese Lücke zu schließen.

1. c. Bekanntmachung/Aushändigung des Sonderkündigungsschutzes für die Initiatoren von Betriebsversammlungen sowie für Wahlvorstände, Wahlbewerber und Betriebsratsmitglieder

Eine Pflicht des Arbeitgebers, diese Normen im Betrieb ausdrücklich bekannt zu machen oder gar zusammen mit dem Arbeitsvertrag auszuhändigen, erscheint nicht erforderlich. Wenn es irgendeine Norm gibt, die fast allen, auch juristisch ungebildeten Arbeitnehmern bekannt ist, dann ist dies der besondere Kündigungsschutz für Betriebsräte, Wahlbewerber und Initiatoren von Betriebsratswahlen. Dies gilt umso mehr, als häufig im Zuge der Initiierung von Betriebsratswahlen die Gewerkschaft um Hilfe gebeten wird, die selbstverständlich die entsprechenden Normen kennt und die Mitarbeiter darüber auch noch einmal unterrichtet.

1. d. Anspruch befristet beschäftigter Betriebsratsmitglieder auf Entfristung ihrer Arbeitsverträge bei Wahl in den Betriebsrat

Dieser Vorschlag ist nicht vereinbar mit der Grundaussage des BetrVG, wonach die Betriebsratstätigkeit grundsätzlich ein „Ehrenamt“ ist (§ 37 BetrVG). Würde an die Betriebsratstätigkeit ein erheblicher materieller Vorteil (hier: die Verlängerung des befristeten Arbeitsvertrages) geknüpft, wäre dies ein Anreiz dafür, die Betriebsratstätigkeit aus materiellen Erwägungen heraus anzustreben. Überdies ist es nicht so, dass die Errichtung von Betriebsräten überproportional häufig in Betrieben mit vielen befristet Beschäftigten scheitert. Gerade bei Discountern setzen sich die Filialbelegschaften häufig aus Mitarbeitern mit sehr langen Dienstzeiten zusammen. Überdies sind Mitarbeiter mit weniger als sechs Monaten Betriebszugehörigkeit ohnehin nicht passiv wahlberechtigt (§ 8 BetrVG).

1. e. Erleichterung der Betriebsratsbildung in Konzernunternehmen mit vielen kleinen Filialen

Der Vorschlag ist nicht verständlich. Schon nach der jetzigen Fassung des BetrVG ist gewährleistet, dass auch in Filialunternehmen lückenlos Betriebsräte errichtet werden können. Betriebsratsfähig sind grundsätzlich alle Filialen, sofern dort nicht weniger als fünf Mitarbeiter beschäftigt sind. Dabei zählt das BetrVG nur nach Köpfen, so dass auch fünf Teilzeitmitarbeiter für die Errichtung eines Betriebsrats ausreichen. In Mini-Filialen mit vier oder weniger Mitarbeitern fehlt es regelmäßig an einem eigenständigen Leitungsapparat, so dass überhaupt kein Betrieb vorliegt, sondern auf die nächst größere Einheit abzustellen ist; dann ist ein regionaler Betriebsrat unter Zusammenfassung aller kleineren Filialen zu wählen.

2. Transparenz/Offenlegung von Konzernstrukturen

Der Vorschlag ist nicht verständlich. Eine mögliche Verschleierung von Konzern- und Unternehmensstrukturen hat mit der Bildung von Betriebsräten nichts zu tun. Betriebsräte werden grundsätzlich unabhängig von Unternehmens- und Konzernzugehörigkeit in den jeweiligen Betrieben (Betriebsstätten) gebildet. Dementsprechend wären Versuche, Betriebsratsgründungen durch intransparente Konzernstrukturen zu vereiteln, von vornherein unsinnig. Soweit in der Begründung des Antrags darauf abgestellt wird, bei undurchsichtigen Konzernstrukturen sei der „verantwortliche Ansprechpartner auf Arbeitgeberseite“ oft unklar, ist dies nicht nachvollziehbar. Es ist Sache des Arbeitgebers, wen er als Ansprechpartner für den Betriebsrat benennt, und das ist von Konzernstrukturen unabhängig. Werden Rechte des Betriebsrats verletzt, weil sich niemand um dessen Anliegen kümmert, steht dem Betriebsrat genauso der Weg zu den Arbeitsgerichten offen, wie wenn der Ansprechpartner feststünde, aber die Anliegen des Betriebsrats einfach ignoriert.

3. Schaffung eines Arbeitnehmer-Datenschutzgesetzes

(1) Wie oben bereits ausgeführt, ist in der Tat das Arbeitnehmerdatenschutzrecht dringend kodifizierungsbedürftig. Allerdings wird auch eine Kodifizierung nichts daran ändern, dass das Datenschutzrecht - im Arbeitsverhältnis wie auch sonst - immer ein **Abwägungsrecht** bleiben wird. Per Gesetz das Erlaubte vom Unerlaubten **trennscharf** abzugrenzen, ist eine nicht umsetzbare **Utopie**. Auch ein Arbeitnehmerdatenschutzgesetz kann - gerade angesichts des rasanten Wandels der Informationstechnologie - nie alle aktuell denkbaren Fallgestaltungen erfassen, und noch weniger zukünftige Konstellationen regeln.

(2) Nach der derzeitigen Konzeption des BDSG besteht bei der Speicherung und Nutzung von Daten im Rahmen eines Vertragsverhältnisses eine Zweckbindung nur insoweit, als die Daten nur zum Zwecke der Durchführung des Vertrages verwendet werden dürfen. Für Arbeitsverhältnisse bedeutet dies, dass die Arbeitnehmerdaten vom Arbeitgeber grundsätzlich für alles genutzt werden dürfen, was die **Durchführung und Abwicklung des Arbeitsverhältnisses** mit sich bringt. Der Arbeitgeber darf die Daten der Arbeitnehmer beispielsweise verwenden für die korrekte Lohnabrechnung, die Abführung von Abgaben, Wählerlisten für den Betriebsrat, Beförderungsentscheidungen, Schulungsangebote, Erfassung von Arbeitszeiten und Überstunden, Sozialauswahl bei betriebsbedingten Kündigungen etc. Würde man nun die Konzeption des Arbeitnehmerdatenschutzes ändern und verlangen, dass für jedes einzelne persönliche Datum von **vornherein festgelegt** werden muss, zu **welchem Zweck** es gespeichert und genutzt werden darf, so stünden angesichts der Weiterentwicklung von Unternehmen, aber auch der Weiterentwicklung der Informationstechnologie, die Arbeitgeber ständig vor dem Problem, dass sie Daten für dringend benötigte legitime betriebliche Zwecke nicht nutzen dürfen. Um an einem Beispiel zu verdeutlichen, wohin die geforderte Neuregelung führen würde: *Der Arbeitgeber hat ein System eingeführt, wonach die Mitarbeiter einmal jährlich von ihren Vorgesetzten beurteilt werden. Die Beurteilung dient zum einen dazu, Beförderungsentscheidungen vorzubereiten, zum anderen wird anhand der Beurteilungen über freiwillige außerplanmäßige Gehaltserhöhungen und Jahresgratifikationen entschieden. Dementsprechend würde der Arbeitgeber nun festlegen müssen, dass die in den Beurteilungen enthaltenen personenbezogenen Daten zum Zwecke der Entscheidung über Beförderungen und Sondervergütungen gespeichert und genutzt werden können. Ein Jahr später beschließt der Arbeitgeber, ein Förderprogramm für Nachwuchsführungskräfte aufzulegen: Er möchte besonders engagierte und qualifizierte Mitarbeiter langfristig für Führungsaufgaben vorbereiten und diese entsprechend schulen, z.B. durch Teilnahme an externen Fortbildungskursen. Um zu entscheiden, welcher Mitarbeiter in das Programm aufgenommen und auf Fortbildung geschickt werden soll, wäre der Zugriff auf die Beurteilungen wichtig. Der Arbeitgeber müsste nun aber die Daten zu einem anderen Zweck nutzen als zu dem, zu dem sie ursprünglich erhoben wurden, und das dürfte er nicht.*

Das Beispiel zeigt, dass es kontraproduktiv wäre, bei der Datenerhebung und -speicherung diese mit einer bestimmten Zweckbindung zu verknüpfen und dann eine Nutzung der Daten zu anderen Zwecken auszuschließen (oder von der Zustimmung der Arbeitnehmer, des Datenschutzbeauftragten oder des Betriebs-

rats abhängig zu machen). Sachgerechter ist deshalb die derzeitige Struktur des BDSG, die Datenerhebung und -speicherung für alle mit dem Vertragsverhältnis zusammenhängenden Zwecke zulässt.

(3) Auch eine **gesetzliche Festschreibung**, **welche Zwecke** der Arbeitgeber innerhalb des Arbeitsverhältnisses legitimerweise verfolgen darf und welche nicht, erscheint nicht sinnvoll. Eine präzise Abgrenzung wird kaum möglich sein. Auch hier wieder ein Beispiel zur Verdeutlichung: *Im Regelfall geht es den Arbeitgeber nichts an, was der Arbeitnehmer in seiner Freizeit treibt. Deshalb darf er grundsätzlich Daten über die Freizeitaktivitäten des Arbeitnehmers weder erheben noch speichern. Anerkanntermaßen gibt es jedoch Sonderfälle, in denen das private Verhalten des Arbeitnehmers erhebliche Auswirkungen auf das Arbeitsverhältnis hat, und in diesen Fällen muss selbstverständlich der Arbeitgeber berechtigt sein, die Erkenntnisse aus dem Privatleben des Mitarbeiters zu speichern. Man denke beispielsweise an den Erzieher eines Kindergartens, gegen den ein Ermittlungsverfahren wegen Besitzes von kinderpornografischem Material läuft. Dafür muss sich der Arbeitgeber schon aufgrund seiner Schutzpflichten interessieren. Auch muss der Arbeitgeber nicht tatenlos zuschauen, wenn der Arbeitnehmer in seiner Freizeit verbotenerweise ein Konkurrenzunternehmen betreibt (vgl. § 60 HGB) oder in Öffentlichkeit und Presse unsachlich gegen den Arbeitgeber agitiert (Beispiel: Der Arbeitnehmer ist Mitglied einer rechtsextremen Partei und beschimpft im Internet seinen Arbeitgeber, weil dieser „viel zu viele Türken und Neger beschäftigt“).*

(4) Ebenso wenig überzeugend ist es, von vornherein einen **zulässigen Zeitraum** für Datenspeicherung festzulegen. Welche personenbezogenen Daten der Arbeitgeber zur sachgerechten Durchführung des Arbeitsverhältnisses wann benötigt, ist nie vorhersehbar. So kann z.B. die Information über Familienstand und Unterhaltspflichten jahrelang irrelevant seien, dann aber bei der Beendigung des Arbeitsverhältnisses (z.B. im Rahmen der Sozialauswahl bei einer betriebsbedingten Kündigung) oder gar erst nach Beendigung des Arbeitsverhältnisses (z.B. bei der Berechnung einer Betriebsrente) relevant werden.

(5) Nicht nachvollziehbar ist der Vorschlag, ein **umfassendes Einsichtsrecht** des Arbeitnehmers in seine gespeicherten personenbezogenen Daten vorzusehen. Schon nach geltendem Recht (§ 83 BetrVG) besteht ein umfassendes Einsichtsrecht in die Personalakte (die vollständig sein muss) sowie ein umfassender Auskunftsanspruch über die gespeicherten Daten nach § 34 BDSG.

3.a Einsatz von Videokameras, Privatdetektiven und Zugangskontrollen

(1) Wie der Vorschlag selbst erwähnt, ist **nach geltendem Recht** eine **flächendeckende Videoüberwachung** von Arbeitnehmern **unzulässig**, während nach der Rechtsprechung des Bundesarbeitsgerichts im Einzelfall bei Vorliegen bestimmter Gründe (z.B. konkreter Verdacht von Unterschlagungen) eine zeitlich und örtlich eingeschränkte Videoüberwachung zulässig sein kann. Das Recht der Arbeitnehmer auf informationelle Selbstbestimmung ist durch die – sehr restriktive - Rechtsprechung des Bundesarbeitsgerichts ausreichend geschützt. Eine gesetzliche Regelung, die notwendigerweise unspezifisch bleiben und sich in allgemeinen Abwägungsfloskeln erschöpfen müsste, brächte keinen Rechtsfortschritt.

(2) Die Forderung nach einer **uneingeschränkten Hinweispflicht** des Arbeitgebers auf eine ausnahmsweise stattfindende Videoüberwachung ist nicht nachvollziehbar. Sie würde sich bei einer Überwachung zum Zwecke der Erhärtung von Verdachtsmomenten betreffend Unterschlagungen oder ähnlicher Straftaten selbst ad absurdum führen. Soweit dagegen die Überwachung des Arbeitnehmers nur ungewollte Folge der Überwachung öffentlich zugänglicher Räume aus anderen Gründen ist (z.B. Videoüberwachung von Bankschaltern zur Prävention gegen Bankraub), ist die Überwachung für die Arbeitnehmer zum einen offensichtlich, zum anderen greift insoweit bereits eine Unterrichtungspflicht nach geltendem Recht (§ 6b BDSG).

3.b Stellung des Datenschutzbeauftragten

Über eine **Stärkung** der Stellung des **betrieblichen Datenschutzbeauftragten** mag man nachdenken, hier käme auf die Details an. Eine Pflicht des Arbeitgebers, die **Beschäftigten** über die **Person des betrieblichen Datenschutzbeauftragten** und über ihre Rechte und Pflichten nach den Datenschutzgesetzen zu **informieren**, erscheint nicht erforderlich. Normalerweise bereitet es den Beschäftigten keinerlei Problem, den für sie zuständigen Datenschutzbeauftragten zu identifizieren (Telefonbuch, Intranet etc.). Eine Aufklärung über die Rechte und Pflichten nach den Datenschutzgesetzen wäre keine messbare Verbesserung, da sich diese Aufklärung notwendigerweise in der Wiedergabe von Gesetzeswortlaut erschöpfen würde, der notwendigerweise außerordentlich abstrakt ist und einem nichtjuristisch geschulten Leser kaum Aufschluss über die Rechtslage gibt.

Ein **Mitbestimmungsrecht des Betriebsrats** bei der **Benennung und Abberufung des Datenschutzbeauftragten** erscheint nicht sachdienlich. Denn Aufgabe des Datenschutzbeauftragten ist auch die Prüfung, ob der Betriebsrat korrekt mit den ihm zugänglich gemachten personenbezogenen Daten umgeht. Im Übrigen beschränkt sich die Aufgabe des Datenschutzbeauftragten ja nicht auf den korrekten Umgang mit Arbeitnehmerdaten, sondern in den meisten Unternehmen fallen auch eine Vielzahl anderer personenbezogener Daten an (Patientendaten im Krankenhaus, Kundendaten einer Versicherung etc.).

C. Drucksache 16/9311 Persönlichkeitsrechte abhängig Beschäftigter sichern – Datenschutz am Arbeitsplatz stärken

I. Feststellungen

(1) Die Darstellungen im zweiten Absatz entsprechen nicht der betrieblichen Realität. **Kontrollen von E-Mail-Verkehr und Internetnutzung** sind keineswegs betrieblicher Alltag, sondern – schon wegen der Masse der anfallenden Daten – **absolute Ausnahmen**. Das Gleiche gilt für Überwachung von Beschäftigten mit Kameras: Diese kommt im betrieblichen Alltag fast immer nur als Nebenfolge einer aus anderen Zwecken erforderlichen Videoüberwachung

vor (Beispiel: Überwachung von Schalterräumen in Banken zur Abschreckung von Bankräubern). Auch die Ortung von Fahrern und Außendienstmitarbeitern über Mobiltelefon oder andere Ortungssysteme ist nach wie vor die große Ausnahme. Und die Überwachung von Arbeitnehmern durch private Detekteien ist – schon wegen der extrem hohen Kosten – ein absoluter Einzelfall und kommt praktisch nur bei konkretem Verdacht erheblicher Straftaten vor. Richtig ist allein die Feststellung, dass **Zugangskontrollen** inzwischen zum betrieblichen Alltag gehören. Diese sind aber seit Jahrzehnten gebräuchlich (Stechuhren) und zur korrekten Erfassung und Abrechnung der Arbeitszeit unverzichtbar, mit Überwachung haben sie nichts zu tun. Von einem *„skandalösen Ausmaß der Überwachung"* (Abs. 5) kann deshalb **nicht die Rede** sein.

(2) Zur Forderung, dass Daten nur für den Zweck gespeichert werden dürfen, für den sie erhoben wurden, siehe oben unter B.II.3.(2).

(3) Die Forderung, dass die Erhebung, Verarbeitung oder Nutzung von Daten nur dann zulässig sein soll, wenn sie **„unerlässlich"** ist, würde dem stetigen Wandel der Arbeitswelt und des einzelnen Arbeitsverhältnisses sowie der notwendigen Fortentwicklung betrieblicher Strukturen entscheidend entgegenstehen. Während sich allgemein die Erkenntnis durchsetzt, dass das Arbeitsleben einem ständigen Wandel unterliegt und ständige Weiterqualifikation der Arbeitnehmer der Schlüssel zu Vollbeschäftigung ist, würde ein **„Einzementieren"** des über den einzelnen Arbeitnehmer verfügbaren Datenbestands unüberwindliche Hürden für die Weiterentwicklung von Arbeitsplatzanforderungen, Qualifizierungsmaßnahmen und sonstigen betrieblichen Verbesserungen sein.

Zu den **Vorschlägen unter II.** ist wie folgt Stellung zu nehmen:

1. Schutz von Bewerbern

1.a (1) Die Begrenzung der zu erhebenden Daten von Bewerberinnen und Bewerbern auf solche Daten, die für die angestrebte Anstellung **erforderlich** sind, entspricht der geltenden Rechtslage.

(2) Eine unbedingte Pflicht zur **Löschung von Daten nach Abschluss eines Bewerberverfahrens** ist nicht zweckmäßig. Zum einen kommt es häufig vor, dass der eingestellte Bewerber die Stelle doch nicht antritt oder das Arbeitsverhältnis sehr kurzfristig bereits in der Probezeit wieder endet. Dann ist es im Interesse sowohl des Arbeitgebers als auch der übrigen Bewerber, wenn der Arbeitgeber noch über die Daten der nächstbestqualifizierten Bewerber verfügt. Auch die Anlage von **Bewerberpools** erscheint sinnvoll, gerade auch im Interesse der Bewerber selbst; deshalb sollte sie nicht von deren Zustimmung abhängig gemacht werden. Eine längere Aufbewahrung von Bewerberdaten ist auch deshalb sinnvoll, damit Unternehmen bei **Zweitbewerbungen** der gleichen Person auf die Erkenntnisse des ersten Bewerbungsverfahrens (z.B. Ergebnisse eines Vorstellungsgesprächs) zurückgreifen können.

1.b. Die **Beschränkung des Fragerechts** auf diejenigen Fragen, die für das betreffende Arbeitsverhältnis **relevant sind**, entspricht der **geltenden Rechtslage**.

1.c. Die **Beschränkung des Fragerechts** nach **Gesundheitszustand**, Erkrankungen und Behinderungen auf unmittelbar stellenrelevante Fragen entspricht der geltenden Rechtslage.

1.d. Die Beschränkung des Fragerechts nach (vorhandener oder geplanter) **Schwangerschaft** entspricht der geltenden Rechtslage.

1.e. Die Forderung ist nicht verständlich. Es sind bislang noch keine Fälle bekannt geworden, in denen **Online-Bewerbungsunterlagen** unautorisiert Dritten zur Kenntnis gebracht oder gar manipuliert worden wären.

2. Schutz der Arbeitnehmerdaten während des Beschäftigungsverhältnisses

2.a. Dass eine **Ex-ante-Begrenzung der Speicherdauer**, der **Nutzungszwecke** und der **zugriffsberechtigten Stellen** unmöglich ist und den stetigen Wandlungen des Arbeitsverhältnisses entgegenstehen würden, habe ich oben bereits ausgeführt (B.II.3.(2) und (3)). Unklar ist die Forderung, die entsprechende Dokumentation habe **„revisionssicher"** zu erfolgen; der Begriff „Revisionssicherheit" ist mir unbekannt.

Eine **Anwendung von § 7 BDSG** auf den Arbeitnehmerdatenschutz erscheint nicht geboten, zumal bislang noch keine Fälle bekannt geworden sind, in denen Arbeitnehmer durch unzulässige oder unrichtige Datenerhebung oder -verarbeitung materielle Schäden erlitten hätten. Im Übrigen sieht § 7 BDSG keineswegs eine verschuldensunabhängige Haftung vor, sondern weist lediglich der verantwortlichen Stelle die Beweislast für fehlendes Verschulden zu.

2.b. Es ist nicht erkennbar, welchen Schutzzweck die **Aufspaltung der Arbeitnehmerdaten** in solche, die zur Begründung und Aufrechterhaltung des Beschäftigungsverhältnisses benötigt werden (?) und allen übrigen Daten haben soll. Gerade bei Versetzungs- oder sonstigen Auswahlentscheidungen lässt sich das eine vom anderen schlechterdings nicht trennen.

2.c. Eine **regelmäßige Information der Arbeitnehmer** über ihr Recht auf Auskunft bezüglich der über sie gespeicherten persönlichen Daten mag man einführen. Eine signifikante Verbesserung des Datenschutzes wird dadurch aber nicht erreicht.

2.d. Die Unsinnigkeit des Vorschlages in Satz 1 wird in Satz 2 selbst erkannt: Der Arbeitgeber muss selbstverständlich die Möglichkeit haben, auch ohne Zustimmung der Arbeitnehmer deren Daten im Wege der **Auftragsdatenverarbeitung (§ 11 BDSG)** verarbeiten zu lassen. Nicht nur kleine Unternehmen sind darauf angewiesen, die Lohn- und Gehaltsbuchhaltung extern (über Steuerberater oder spezialisierte pay-roll services) durchführen zu lassen. Auch in mittelständischen und großen Unternehmen besteht

ein entsprechendes Bedürfnis. Die Auftragsdatenverarbeitung scheitern zu lassen, wenn auch nur ein einziger Arbeitnehmer nicht zustimmt, würde zum Erliegen vieler Unternehmen führen. Nicht nur das Arbeitsrecht, sondern vor allem das Sozialversicherungs- und Steuerrecht sind mittlerweile so kompliziert, dass kaum ein kleines und mittleres Unternehmen eine korrekte Lohnabrechnung noch selbst durchführen kann.

2.e. Ein **Unterlassungsanspruch** hinsichtlich der Verwendung unrechtmäßig erhobener oder ausgewerteter Daten entspricht bereits der **geltenden Rechtslage**. Auch das **Benachteiligungsverbot** bei Wahrnehmung der Rechte aus den Datenschutzgesetzen entspricht geltender Rechtslage (§ 612a BGB).

2.f. Der Vorschlag ist sprachlich wohl verunglückt und nicht verständlich.

2.g. Der Vorschlag, sowohl den Betriebsrat als auch den Datenschutzbeauftragten ein **Widerspruchsrecht mit aufschiebender Wirkung** einzuräumen, bedeutet de facto, dass sowohl Betriebsrat als auch Datenschutzbeauftragter in der Hand hätten, **nach Belieben jedes Unternehmen auf unabsehbare Zeit lahm zu legen** (*Beispiel: Plant der Arbeitgeber eine Umstrukturierung und würde der Betriebsrat einen fehlerhaften Umgang mit Arbeitnehmerdaten reklamieren, müsste der Arbeitgeber die Umstrukturierung solange auf Eis legen, bis Gerichte über die Zulässigkeit der Datenverwendung entschieden hätten.*). Dem Betriebsrat (und auch den Datenschutzbeauftragten) wäre damit ein schärferes Schwert in die Hand gegeben, als er es nach irgendeiner vergleichbaren Norm derzeit hat. Die Lahmlegung jedes Unternehmens wäre auf diese Weise einfacher zu bewerkstelligen als durch einen Arbeitskampf, noch dazu ohne finanzielles Risiko. Die Drohung mit einem Widerspruch würde de facto dem Betriebsrat eine Blankovollmacht für die Durchsetzung jedweden anderen Anspruchs geben.

2.h. Die Anregung, dass der Arbeitnehmer bei **Verstößen des Arbeitgebers** gegen Informations- oder Auskunftspflichten die **Löschung seiner Daten** verlangen kann, ist widersinnig. Denn der Arbeitgeber speichert die Daten ja deshalb, weil er sie zur Durchführung des Arbeitsverhältnisses braucht. Werden die Daten als Sanktion für Verstöße gegen Informations- oder Auskunftspflichten gelöscht, würde dies nur dazu führen, dass der Arbeitgeber die Daten neu erheben muss. Die Sanktionsebene ist also falsch gewählt.

3. Schutz von Gesundheitsdaten

3.a. Der Vorschlag ist durch die neuen gesetzlichen Regelungen zur **Gendiagnostik** überholt.

3.b. Es ist kein Bedürfnis dafür ersichtlich, dem Arbeitgeber bei der Einstellung **psychologische Untersuchungen der Bewerber** hinsichtlich Sozialverhalten und sozialer Kompetenz zu untersagen. Solche Untersuchungen sollten auch nicht auf Führungspositionen oder die Einstellung von Pädagogen etc. beschränkt sein. In der heutigen Arbeitswelt sind Sozialverhalten bzw. soziale Kompetenz mindestens ebenso wichtig wie Ausbildung, Kenntnisse und Erfahrungen. Wesentliches Element eines jeden Vorstellungsgesprächs ist es, das Sozialverhalten des Bewerbers einzuschätzen, er muss in den Betrieb „passen“. Es ist niemandem gedient, wenn man die Arbeitgeber darauf verweist, nicht in den Betrieb „passende“ Bewerber während der Probezeit wieder auszusieben. Man mag die Tauglichkeit mancher in der Praxis verbreiteter psychologischer Einstellungstests (z.B. Assessment-Center) bezweifeln. Einen Bedarf für ihre gesetzliche Untersagung besteht aber nicht. Es ist grundsätzlich Sache des Arbeitgebers, auf welche Weise er sich ein möglichst umfassendes Bild der Bewerber verschaffen will.

3.c. Dass die Durchführung **medizinischer oder psychologischer Tests** von der Zustimmung der Betroffenen abhängig ist, ist **geltendes Recht**. Unabhängig davon müssen medizinische Tests der Sicherheit der Berufsausübung (Piloten etc.) dienen. Die gleiche Anforderung für psychologische Tests aufzustellen, erscheint nicht erforderlich.

Systemwidrig ist die Forderung, dass solche Tests nur mit **Zustimmung des Datenschutzbeauftragten** zulässig sein sollen. Nach der gesetzgeberischen Konzeption hat der **Datenschutzbeauftragte** die Einhaltung **rechtlicher Rahmenbedingungen** zu gewährleisten, ist jedoch **keine Entscheidungsinstanz bei Ermessensentscheidungen**. Mitbestimmungsrechte des **Betriebsrats** bestehen bereits nach geltendem Recht (§ 94 BetrVG).

3.d. Der Vorschlag ist **nicht verständlich**. Bislang ist nicht bekannt geworden, dass Arbeitgeber **Sozialverhalten „messen“**, d.h. mit objektiven Bewertungsverfahren evaluieren. Die Einschätzung des Sozialverhaltens geschieht in der Praxis vielmehr formlos, insbesondere durch persönlichen Eindruck.

4. Schutz vor Überwachung mit optischen und elektronischen Geräten

4.a. Siehe die Ausführungen oben unter B.II.1.f.

4.b. Siehe oben B.II.1.f.

4.c. Der Vorschlag ist **nicht nachvollziehbar**. Er wird darauf hinauslaufen, dass der Arbeitgeber jedwedes elektronische System **nicht zur Leistungs- und Verhaltenskontrolle** nutzen dürfte. Es kann aber nicht sein, dass der Arbeitgeber beispielsweise nicht mehr prüfen dürfte, ob der in der Buchhaltung beschäftigte Arbeitnehmer Buchungsvorgänge korrekt abwickelt, ob der in einem Call-Center beschäftigte Mitarbeiter Anrufe tatsächlich bearbeitet, ob der Mitarbeiter tatsächlich zur Arbeit erscheint oder ob er per E-Mail Geschäftsgeheimnisse an die Konkurrenz weiterleitet. Dass der Arbeitgeber jedenfalls stichprobenartig die Korrektheit aller Arbeitsabläufe und auch das korrekte Verhalten

der Mitarbeiter prüft, ist ein seit Urzeiten anerkannter Grundsatz. Jedes Unternehmen ab einer bestimmten Größenordnung hat eine **interne Revisionsabteilung**, die in regelmäßigen Abständen Geschäftsvorfälle auf Ordnungsgemäßheit prüft. Das Unterhalten einer internen Revisionsabteilung ist nicht nur zulässig, sondern auch rechtlich geboten. Unter Compliance-Gesichtspunkten, aber auch zur Vermeidung ihrer persönlichen Haftung müssen die Geschäftsführer/Vorstände sicherstellen, dass rechtliche Standards im Unternehmen von den Mitarbeitern eingehalten werden.

Richtigerweise ist deshalb nach der aktuellen gesetzlichen Konzeption die Leistungs- und Verhaltenskontrolle **nicht schlechterdings** unzulässig, sondern ihr Umfang ist dem **Mitbestimmungsrecht des Betriebsrats unterworfen** (§ 87 Abs. 1 Nr. 6 BetrVG). Dabei sollte es bleiben.

4.d. Der Vorschlag entspricht der **geltenden Rechtslage** nach der Rechtsprechung des Bundesarbeitsgerichts.

5. Einsatz von Telekommunikation am Arbeitsplatz

5.a. Siehe die Ausführungen zu 4.c.

5.b. Der Vorschlag entspricht der **geltenden Rechtslage**, d as **Aufzeichnen oder Mithören von Gesprächen** ist ohne Zustimmung des Arbeitnehmers strafbar.

5.c. Die vorgeschlagenen Einschränkungen sind zu weitgehend. Es kann nicht darauf ankommen, ob ein **Verdacht „begründet"** ist, sondern die Begründetheit eines Verdachts soll ja gerade durch die Datenauswertung festgestellt werden. Ob beispielsweise der Arbeitnehmer anwesend ist oder „blau macht" muss der Arbeitgeber auch ohne konkreten Verdacht überprüfen können. Die Forderung, dass in jedem Fall Datenschutzbeauftragter und Arbeitnehmervertretung „beteiligt" (?) werden sollen, schießt über das Ziel hinaus. Es ist Sache der Betriebspartner, in Regelungen nach § 87 Abs. 1 Nr. 6 BetrVG die Beteiligung der Mitarbeitervertretung so zu regeln, wie sie dies für sinnvoll halten. Die **Hinzuziehung des Datenschutzbeauftragten** ist **systemwidrig**. Aufgabe des Datenschutzbeauftragten ist, die Einhaltung allgemeiner Datenschutzstandards zu gewährleisten, nicht aber die Hinzuziehung zu einzelnen Datenverarbeitungs- oder Erhebungsvorgängen.

6. Datenschutzbeauftragter und Aufsichtsbehörde

6.a. Der Vorschlag entspricht der **geltenden Rechtslage**. Nach § 4f Abs. 2 BDSG muss der **Datenschutzbeauftragte** die **erforderliche Sachkunde und Zuverlässigkeit** besitzen. Es macht keinen Sinn, den Nachweis der Sachkunde demjenigen aufzubürden, der bestellt werden soll. Vielmehr ist es Aufgabe des Unternehmens, die Sachkunde zu prüfen.

6.b. Der Vorschlag, wonach der Datenschutzbeauftragte möglichst **keine weiteren Aufgaben im Bereich der betrieblichen Datenverarbeitung und der Personalverwaltung** wahrnehmen soll, **überlastet** kleine und mittlere Betriebe, da die Grenze für die Bestellung gem. § 4f Abs. 1 BDSG bereits bei 20 Arbeitnehmern verläuft. Der Vorschlag würde darauf hinauslaufen, dass in einem Betrieb mit 21 Mitarbeitern 5 % der Belegschaft für Datenschutzzwecke „reserviert" sein müssten (andere Mitarbeiter als solche aus der Personal- oder IT-Abteilung kommen in den meisten Betrieben als Datenschutzbeauftragte mangels entsprechender Kenntnisse nicht in Betracht).

6.c. Entspricht der **geltenden Rechtslage**.

6.d. Die **Auskunftspflicht des Arbeitgebers** entspricht der **geltenden Rechtslage**, da nach § 80 Abs. 1 Be trVG der Betriebsrat auch über die Einhaltung des Datenschutzgesetzes zu wachen hat und ihm dazu der Arbeitgeber nach § 80 Abs. 2 BetrVG die erforderlichen Auskünfte zu erteilen hat.

6.e. Siehe die Ausführungen unter B.II.3.b.

6.f. Entspricht der **geltenden Rechtslage**.

6.g. Siehe die Ausführungen unter B.II.3.b.

6.h. Entspricht der **geltenden Rechtslage**.

7. Schadensersatz und Ordnungswidrigkeiten

7.a. Die **Schadensersatzpflicht** des Arbeitgebers entspricht der geltenden Rechtslage, setzt allerdings Verschulden voraus. Eine Garantiehaftung des Arbeitgebers ohne Verschulden erscheint angesichts der vielfältigen Fehlerquellen der elektronischen Datenverarbeitung als überzogen (s. auch C.II.2.a.).

7.b. Dass Verstöße gegen das BDSG **Ordnungswidrigkeiten** sind, entspricht der geltenden Rechtslage. Die Höchstgrenze für Geldbußen von EUR 2 50.000 ist die allgemeine Grenze für Sanktionen bei Ordnungswidrigkeitenverstößen. Es ist nicht ersichtlich, warum Verstöße gegen Datenschutzrecht stärker geahndet werden sollten als andere Ordnungswidrigkeiten.

7.c. Keine Anmerkungen.

7.d. Der Antrag betrifft die **Praxis der Bußgeldbemessung** durch die Ordnungsbehörden, nicht die Änderung gesetzlicher Vorschriften.

D. Drucksache 16/11376 Datenschutz für Beschäftigte stärken

I. Feststellungen

S. die Ausführungen unter A. sowie B.I. und C.I.

II. Vorschläge

I. Grundsätze der Erhebung, Speicherung, Veränderung, Übermittlung und Nutzung personenbezogener oder personenbeziehbarer Daten von Beschäftigten

I.a. Der Vorschlag würde dem **Datenschutzrecht** eine **völlig neue Dimension** verleihen. Bislang ist das Eingreifen datenschutzrechtlicher Regelungen von der **Form** abhängig, in der die Daten gespeichert sind (**elektronisch** oder in **systematisierten Dateien**). Der

Vorschlag würde das Datenschutzrecht ausweiten auf persönliche Daten, die im **Gespräch** ausgetauscht, gemerkt, **handschriftlich** niederlegt oder in jeder anderen Form verkörpert sind. Das würde das Datenschutzrecht von seiner ursprünglichen Stoßrichtung (Schutz des Individuums vor den besonderen Gefahren der Technologiegesellschaft) vollständig lösen. Schon der **„Tratsch in der Kantine" würde gesetzlich reglementiert**. Das kann man nicht ernsthaft wollen.

I.b. Entspricht der **derzeitigen Rechtslage**.

I.c. Der anzustrebende **Anwendungsbereich** eines zu schaffenden Arbeitnehmerdatenschutzgesetzes erscheint **zutreffend**. Die Abgrenzung zwischen „Freelancern/Outgesourcten und anderen Auftragnehmern des Unternehmen wäre allerdings noch klarzustellen.

I.d. Die Bindung der Zulässigkeit von Datenverarbeitung an die **„Erforderlichkeit" schießt über das Ziel hinaus**. Beispiel: Der Arbeitgeber will nach bestimmten Kriterien Mitarbeiter auswählen, die er auf eine Fortbildung schicken will. Die Fortbildung ist im Interesse der Arbeitnehmer sinnvoll, aber sicherlich nicht „erforderlich". Nach der vorgeschlagenen Neufassung dürfte der Arbeitgeber nicht auf die gespeicherten Personaldaten zugreifen, um zu entscheiden, welchen Arbeitnehmer die Fortbildung voranbringt und für wen sie am besten passt. Überdies muss der Arbeitgeber auch **zugunsten der Mitarbeiter** auf die Daten zurückgreifen können. Muss er beispielsweise einen Mitarbeiter aus einer Abteilung heraus wegen Arbeitsmangels versetzen, so muss er auf die Daten der Arbeitnehmer zurückgreifen können, um zu entscheiden, wen die Maßnahme am wenigsten hart trifft.

I.e. Es ist unklar, ob das **Verbot rechtsgeschäftlicher Einschränkungen** der datenschutzrechtlichen Bestimmungen bedeuten soll, dass dem Arbeitnehmer die bislang bestehende Möglichkeit (§ 4a BDSG), in eine bestimmte Datenverarbeitung **einzuwilligen**, nicht mehr offenstehen soll. Das wäre **fatal**, da ein Gesetz niemals lückenlos alle Erlaubnistatbestände aufzuzählen kann. Es wäre **absurd**, wenn bei Auftreten einer neuen Konstellation Arbeitgeber und Arbeitnehmer nicht einvernehmlich regeln könnten, dass bestimmte Daten verarbeitet werden können.

Nach zutreffender Rechtsprechung des Bundesarbeitsgerichts sind **Betriebsvereinbarungen** i.S.d. § 77 BetrVG „Rechtsnormen" i.S.d. BDSG, die eine Datenverarbeitung erlauben können. Das darf nach richtiger Auffassung selbstverständlich nicht soweit gehen, dass der Betriebsrat auf Datenschutz insgesamt oder in substantiellem Umfang verzichtet. Möglich sein muss aber eine gewisse **Anpassung der datenschutzrechtlichen Gesetzeslage auf die betrieblichen Bedürfnisse**. So ist es beispielsweise sinnvoll, in Konzernen die Datenweiterleitung innerhalb des Konzerns durch Betriebsvereinbarung zu regeln. Nach dem Vorschlag, wonach die gesetzlichen Regelungen durch Kollektivvereinbarungen nur „ergänzt und verbessert" werden dürfen, wäre dies nicht mehr möglich. Das ist nicht sachgerecht

I.f. Zu den massiven **Bedenken** gegen **fixierte Datenschutzkonzepte** ohne Flexibilität für zukünftige Veränderungen siehe oben B.II.3.(2). Noch weniger überzeugend ist das Erfordernis, diese Konzepte **vorab mit Datenschutzbeauftragten und Mitarbeitervertretung „abzustimmen"** (womit wohl ein echtes Mitbestimmungsrecht gemeint sein soll). Angesichts der komplexen Materie und der Vielzahl der zu klärenden Fragen macht die Pflicht zur Vorab-Zustimmung von Betriebsrat und Datenschutzbeauftragtem keinen Sinn und würde diesen ein Instrument in die Hand geben, **nach Belieben den Betrieb lahmzulegen** (oder ggf. auf diese Weise sachfremde Forderungen durchzusetzen). Sachgerechter erscheint der gegenwärtige gesetzgeberische Ansatz, Datenschutzbeauftragtem und Mitarbeitervertretung lediglich ein **Überwachungsrecht** nebst Möglichkeit zur Einschaltung der Aufsichtsbehörden vorzusehen.

Im Übrigen erscheint es **nicht sinnvoll**, dem Arbeitgeber gleich **zwei mit gleichen Rechten ausgestattete Überwachungsorgane** überzuordnen, nämlich einerseits den Datenschutzbeauftragten und andererseits den Betriebsrat. Eine solche Verdoppelung der Aufsicht ist überbordende Bürokratie und lähmt das Unternehmen, insbesondere weil nicht ersichtlich ist, wie eine Einigung herbeigeführt werden soll, wenn das eine Aufsichtsorgan zustimmt und das andere nicht.

I.g. Keine Anmerkungen.

I.h. Siehe oben.

I.i. Unverständlich.

I.j. Satz 1 entspricht der **derzeitigen Rechtslage** (§ 28 BDSG). Der Vorschlag, der Arbeitgeber müsse jeweils gegenüber dem betroffenen Arbeitnehmer und dem Datenschutzbeauftragten **schriftlich begründen**, warum er bestimmte Daten erhebt oder speichert oder verarbeitet, wäre angesichts der Vielzahl der Datenverarbeitungsvorgänge in modernen Unternehmen ein bürokratischer „Overkill".

Die Forderung, dass **ausschließlich aktuelle und nachprüfbare Daten** verwendet werden, ist **undurchführbar**. Sie würde den Arbeitgeber zwingen, ständig ohne Not auf Aktualisierung von Daten (z.B. zum Familienstand) zu drängen, obwohl diese Information möglicherweise jahrelang keine Rolle spielt. Eine Nachprüfbarkeit wird in vielen Fällen ohnehin fehlen (bei persönlichen Beurteilungen, Beobachtungen, Einschätzungen etc.).

I.k. Die Forderung, dass Daten **bei den Beschäftigten direkt erhoben** werden sollen, ist unerfüllbar. Selbstverständlich kann es den Arbeitgebern nicht verwehrt sein, die Leistungen und das Verhalten des Arbeitnehmers auch auf andere Weise zu bewerten (z.B. durch Befragung von Mitarbeitern, Kunden etc.).

I.l. Zum Vorschlag, die Datenverarbeitung an **vorher konkret festgelegte Zwecke** zu binden, siehe B.II.3.(2).

Die **Beschränkung des Zugriffs** auf mit der konkreten Datenverarbeitung befasste Personen entspricht der **geltenden Rechtslage** (Gebot der Datenvermeidung bzw. der Datensparsamkeit), das Gleiche gilt für die **Pflicht zur Löschung** von nicht mehr benötigten Daten nach angemessener Frist.

I.m. Die hier aufgestellten umfassenden Anforderungen an die **Information der Betroffenen** kann nur als **„bürokratischer Super-Gau“** bezeichnet werden. Die Erfüllung all dieser Informationsauflagen würde die Einstellung von Heerscharen neuer Mitarbeiter erfordern, die nichts anderes zu tun hätten, als die erforderlichen Papierberge zu erstellen, zumal sich die verwendeten technischen Mittel und Methoden und der Verwendungszusammenhang ständig ändern, so dass ständig neu zu informieren wäre. Am Ende würden die Mitarbeiter in Papierbergen ertrinken, die keiner mehr liest und die auch niemandem einen Vorteil bringen. Wer sich wirklich für die über ihn gespeicherten Daten interessiert, ist ausreichend durch seine Auskunftsansprüche geschützt.

I.n. Einen Anlass für die vorgeschlagene Regelung gibt es nicht. In der Praxis kommen **automatisierte Personalentscheidungen** im Bereich der §§ 99, 102 BetrVG **nicht vor**, schon weil sie den Interessen des Arbeitgebers an sachgerechter Entscheidung zuwiderlaufen würden.

I.o. Entspricht der **geltenden Rechtslage**. Zur erforderlichen Sonderregelung für die Datenweiterleitung im **Konzern** siehe oben I.e. und A.II.

II. Schutz besonderer Arten von Daten

II.a. Entspricht der **aktuellen Rechtslage**. Zu den Bedenken gegen Mitbestimmungsrechte des Betriebsrats sowie des Datenschutzbeauftragten bei der datenschutzrechtlichen Ermessensentscheidungen siehe I.f. und C.II.3.c.

II.b. Die Ausweitung des besonderen Datenschutzes nach § 3 Abs. 9 BDSG für **Daten über die physische und psychische Konstitution** ist überzogen. Viele Arbeitgeber sind darauf angewiesen, Daten über die Leistungsfähigkeit der Arbeitnehmer zu speichern (Beispiel: Leiharbeitsunternehmen müssen wissen, ob ihre Arbeitnehmer den Anforderungen des Entleihers in physischer und psychischer Hinsicht gerecht werden können. Und in Betrieben mit körperlich besonders anstrengender Arbeit muss der Arbeitgeber Informationen darüber haben, welchen Arbeitnehmern er aufgrund physischer oder psychischer Einschränkungen Schonarbeitsplätze zuweisen muss. Überdies will der Gesetzgeber an anderer Stelle (**betriebliches Eingliederungs-Management** nach § 84 SGB IX) gerade, dass der Arbeitgeber Gesundheitsdaten zur Kenntnis nimmt, um Arbeitsausfall und Verschlimmerung von Leiden vorbeugen zu können.

Die Forderung, die Nutzung von Gesundheitsdaten auf Personen zu beschränken, die der **ärztlichen Schweigepflicht** unterliegen ist wohl so zu verstehen, dass die Datenverarbeitung nicht auf Ärzte beschränkt sein soll, sondern dass diese Daten einer besonderen strafbewehrten Vertraulichkeitspflicht unterliegen sollen; dagegen ist nichts einzuwenden.

II.c. Keine Anmerkungen, **entspricht der Praxis**.

II.d. Durch die aktuellen **Gentechnik-Gesetze** überholt.

II.e. Ob das **Gebot der Verschlüsselung** sinnvoll ist, hängt vom Grad der verlangten Verschlüsselung ab. Verschlüsselung kommt ohnehin nur bei elektronischer Speicherung in Betracht, macht aber bei in Papierform aufbewahrten Daten keinen Sinn.

III. Schutz von Bewerberinnen und Bewerbern

III.a. Das **Direkterhebungsgebot** würde es dem Arbeitgeber verwehren, bei Dritten (z.B. früheren Arbeitgebern) Auskünfte einzuholen. Im Interesse einer sachgerechten Personalauswahl erscheint dies nicht geboten.

Generell macht es **keinen Sinn**, die **Erkenntnismöglichkeiten des Arbeitgebers** im Bewerbungsverfahren immer weiter zu beschränken. Die eigentliche Bewerberauswahl wird dadurch letztlich nur **in die Probezeit verlagert**, d.h. es kommt zu einer Vielzahl von Fällen, in denen Fehlgriffe durch rasche Trennung korrigiert werden. Damit ist niemandem gedient. Ganz im Gegenteil ist es für einen Bewerber erheblich besser, eine Stelle nicht zu bekommen, als nach wenigen Wochen die Stelle wieder zu verlieren. Es ist auch nicht im Interesse gut qualifizierter Arbeitssuchender, wenn der Arbeitgeber weniger qualifizierte Bewerber einstellt, nur weil man ihm Erkenntnisquellen versperrt.

Die Forderung, dass Bewerber über die Tatsache einer **maschinellen Auswertung von Bewerbungsunterlagen** informiert werden, ist unpraktikabel. Ob es zu einer maschinellen Auswertung kommt (meistens zur Herbeiführung einer sinnvoll reduzierten Zahl der in die engere Wahl kommenden Bewerbungen) hängt von der Zahl der eingehenden Bewerbungen ab, und die weiß man nicht vorher. Deshalb ist es nicht möglich, schon in der Stellenanzeige darauf hinzuweisen (zumal Stellenanzeigen oft sehr kurz sind und durch solche Hinweise unnötig aufgebläht würden). Es auch nicht ersichtlich, welche Interessen der Bewerber dadurch verletzt werden, dass der Arbeitgeber durch ein maschinelles Verfahren eine gewisse Vorauswahl trifft.

III.b. Zur **Sinnhaftigkeit psychologischer Tests** siehe oben C.II.3.c. Zur **Systemwidrigkeit der Beteiligung des Datenschutzbeauftragten bei Ermessensentscheidungen** siehe oben C.II.3.c.

III.c. Die Regelung ist überflüssig, da **grafologische Tests** in der betrieblichen Praxis der **Vergangenheit** angehören.

III.d. siehe oben C.II.1.a.

III.e. Die vorgeschlagene Regelung entspricht der **geltenden Rechtslage**.

III.f. Der Vorschlag entspricht der **geltenden Rechtslage**, das zentrale Problem ist allerdings die Beweislast.

III.g. Es ist **kein Grund ersichtlich**, warum man die Auskunftsansprüche von Bewerbern **weiter fassen** sollte als die allgemeinen Auskunftsansprüche nach den Datenschutzgesetzen.

IV. Schutz von Beschäftigten während und nach Beendigung des Beschäftigungsverhältnisses

1. Grundsätze

1.a. Siehe die Ausführungen unter B.II.3.

1.b. Siehe oben III.g. und I.m.

1.c. Entspricht der **geltenden Rechtslage**.

2. Leistungs-, Verhaltens- und Regelungsprofile von Beschäftigten

2.a. Die **Zwecklosigkeit** des Unterfangens, die Datenverarbeitung durch den Arbeitgeber von der Verfolgung **enumerativ aufgezählter Zwecke** abhängig zu machen (s. oben B.II.3.), wird hier besonders deutlich. Nach dem Vorschlag wäre es dem Arbeitgeber beispielsweise verwehrt, zur Vorbereitung von Beförderungsentscheidungen, für Versetzungsentscheidungen oder für individuelle Boni auf die Verhaltens- oder Leistungsdaten zuzugreifen.

Zur Unsinnigkeit einer Vorab-Zustimmungspflicht von Betriebsrat und Datenschutzbeauftragten siehe I.f.

2.b. Entspricht der **geltenden Rechtslage**.

2.c. Entspricht der **geltenden Rechtslage**.

3. Nutzung von Telekommunikations- und Telemedieneinrichtungen

3.a. Wenn man einen Anspruch auf Zugang zu den digitalen Netzwerken des Unternehmens gewährleistet, muss man dem **Arbeitgeber die Möglichkeit einräumen**, die **Grenzen dieses Rechts festzulegen**. Es kann nicht sein, dass beispielsweise uneingeschränkt während der Arbeitszeit privat im Internet gesurft oder E-Mails geschrieben werden dürfen. Der Arbeitgeber muss beispielsweise die Möglichkeit haben, die Nutzung ausschließlich in den Pausen zuzulassen.

Die Nutzung von Internet und E-Mail **durch Betriebsräte** entspricht der **geltenden Rechtslage und der Praxis**. Eine Nutzung durch **Gewerkschaften** (z.B. zum Zwecke der Mitgliederwerbung) würde Datenschutzrecht verletzt, wenn die Gewerkschaft Zugang zu personenbezogenen Daten der Mitarbeiter hätte, was z.B. den Zugriff auf E-Mail-Verteiler ausschließt.

4. Überwachung des Kommunikationsverhaltens der Beschäftigten

4.a. Räumt man den Arbeitnehmern Anspruch auf Nutzung der betrieblichen Kommunikationseinrichtungen (Telefon, E-Mail, Internet) auch für private Zwecke ein, muss nach dem oben Gesagten der **Arbeitgeber dies durch Regeln begrenzen können**. Es kann nicht sein, dass die Arbeitnehmer ihre privaten Haus- und Mobil-Telefonanschlüsse auflösen und künftig auf Kosten des Arbeitgebers telefonieren; das gleiche gilt für E-Mail-Verkehr. Dann muss aber der Arbeitgeber auch die Möglichkeit haben, die Einhaltung der Regelungen in angemessenem Umfang zu **kontrollieren**.

Es gibt **keinen Anlass**, den **Zugriff des Arbeitgebers auf geschäftliche Kommunikation** in irgendeiner Weise zu **begrenzen**. So wie der Arbeitgeber – schon nach § 670 BGB – jederzeit Zugriff auf die Arbeitsunterlagen und Arbeitsergebnisse des Mitarbeiters haben muss, wenn diese in Papier vorliegen, muss es auch bei geschäftlicher elektronischer Kommunikation der Fall sein. Es ist kein schutzwürdiges Interesse der Arbeitnehmer daran erkennbar, dass der Arbeitgeber zwar schriftliche Arbeitsergebnisse jederzeit zur Kenntnis nehmen darf, dies jedoch nicht gelten soll, wenn diese in elektronischer Form vorliegen.

4.b. Die vorgeschlagene Regelung ist **zu weitgehend**, soweit sie eine **Vorab-Ankündigung** verlangt. Insbesondere bei Verdacht erheblicher Straftaten oder erheblicher Verletzungen des Arbeitsvertrages müssen Zugriffe auch ohne Vorab-Information möglich sein. Zur Forderung der Vorab-Zustimmung von Datenschutzbeauftragtem und Mitarbeitervertretung siehe oben C.II.2.g.

4.c. Die Regelung ist **unverständlich**. Selbstverständlich muss der Arbeitgeber jederzeit uneingeschränkten Zugriff auf die Arbeitsunterlagen und Arbeitsergebnisse eines Mitarbeiters haben, dies ergibt sich schon aus § 670 BGB. Eine Beschränkung der jederzeitigen Einsichtnahme auf **Einzelfälle** wird den betrieblichen Gegebenheiten **nicht gerecht** (man denke z.B. an das Erfordernis der jederzeitigen gegenseitigen Vertretung bei Krankheit, der Übertragung von Aufgaben auf andere Mitarbeiter etc.).

4.d. Hier gilt das oben zu 4.a. Gesagte. Die **Einhaltung der Grenzen** der Privatnutzung **muss der Arbeitgeber kontrollieren** können.

4.e. Entspricht der **geltenden Rechtslage**.

5. Überwachung mittels optoelektronischer Geräte in Unternehmen

5.a. Ich gehe davon aus, dass mit „optoelektronischen Geräten“ Überwachungskameras gemeint sind. Unter dieser Prämisse entsprechen die Vorschläge lit. a bis d weitgehend der **geltenden Rechtslage** (zum Zustimmungsvorbehalt von Mitarbeitervertretung und Datenschutzbeauftragten siehe oben C.II.2.g.).

5.d. Zu eng ist allerdings die Eingrenzung nach 5.d.: Im Einklang mit der derzeitigen Rechtsprechung müssen Überwachungsmaßnahmen auch bei konkreten Verdachtsmomenten hinsichtlich **anderer Delikte** als Eigentumsdelikte möglich sein, desgleichen bei schwerwiegender Vertragsverletzung (Beispiel: Stempelkartenbetrug).

V. Betriebliche Datenschutzbeauftragte

a. Die **Untergrenze von fünf Mitarbeitern** ist **zu niedrig**. In kleinen Handwerksbetrieben beispielsweise wird sich niemand finden, der ausreichende Kenntnisse hat, auch würden solche Betriebe durch die Bestellung eines Datenschutzbeauftragten übergebühr belastet.

b. Die Ausweitung des **Kündigungsschutzes** für **Datenschutzbeauftragte** analog § 103 BetrVG ist überzogen. In der Praxis sind Versuche, missliebig gewordene Datenschutzbeauftragte unter einem Vorwand fristlos zu kündigen, bislang nicht bekannt geworden.

Die Forderung nach einer § 78 BetrVG (**Benachteiligungsverbot**) nachgebildeten Schutzvorschrift ist

nicht nachvollziehbar, da § 4f Abs. 3 BDSG eine solche Regelung bereits enthält.

c. Zur Forderung, die Bestellung des Datenschutzbeauftragten von der **Zustimmung der Arbeitnehmervertretung** abhängig zu machen, siehe oben B.II.3.b.

VI. Betriebs- und Personalräte

Der Vorschlag geht dahin, in jedem Betrieb **parallel zwei mit gleichen Rechten ausgestattete Aufsichtsbehörden** für den Datenschutz zu errichten, nämlich einerseits den Datenschutzbeauftragten, andererseits den Betriebsrat. Eine Verdoppelung von Aufsicht ist per se **systemwidrig**. Der **richtige Ansatz** kann nur sein, eine **einheitliche Aufsichtsinstanz** mit ausreichenden Rechten zu schaffen. Das Nebeneinander zweier Instanzen hilft nicht weiter, wenn beide Instanzen unzureichende Rechte haben. Haben beide dagegen ausreichende Rechte, führt die Verdoppelung nur zu unnötiger Bürokratie, von den Abstimmungsschwierigkeiten bei Meinungsverschiedenheiten abgesehen.

Unabhängig davon **überfordert** man auch die meisten **Betriebsräte** (insbesondere in kleineren gewerblichen Betrieben) wenn man sie zum Aufsichtsorgan in datenschutzrechtlichen Fragen macht. Datenschutzrecht wird – auch nach der Schaffung eines Arbeitnehmerdatenschutzgesetzes – eine hoch komplizierte juristische Materie bleiben, die sich dem juristischen Laien nur schwer erschließt.

Abzulehnen ist die Forderung, der Arbeitgeber müsse der Mitarbeitervertretung stets **sämtliche Daten vom Beschäftigten herausgeben**. Es gibt gute Gründe für vertrauliche Gespräche zwischen Arbeitgeber und Arbeitnehmer, die den Betriebsrat nichts angehen (z.B. über private Probleme, Alkoholprobleme, Unzufriedenheit mit dem Betriebsrat etc.).

VII. Aufsichtsbehörden

Keine Anmerkungen

VIII. Schiedsstellen für den Schutz der Daten von Beschäftigten

Der Vorschlag ist nicht verständlich. Es bleibt unklar, welche Kompetenzen die Schiedsstelle haben sollte. Im Übrigen würde es auch hier wieder nur zu einer **unnötigen Verdoppelung von Verfahren und Instanzen** (s. VI.) kommen. Im Übrigen verstehen sich schon nach der derzeitigen Praxis die Aufsichtsbehörden als Instanzen, die in Streitfällen zwischen den Beteiligten zu vermitteln versuchen und konsensuale Lösungen herbeiführen.

Abzulehnen ist das Ansinnen, datenschutzrechtliche Fragen weitgehend in die Hände der **Sozialpartner** zu legen. Dort gehören sie nicht hin, jedenfalls so lange es ein gesetzliches Datenschutzrecht mit zwingender Wirkung und Aufsichtsbehörden gibt. Das Datenschutzrecht in die Hände der Sozialpartner zu legen würde nur dann Sinn machen, wenn man parallel dazu auf ein geschriebenes Datenschutzrecht verzichtet und es den Sozialpartnern überlässt, Regeln über die Zulässigkeit oder Unzulässigkeit von Datenerhebung und -nutzung am Arbeitsplatz aufzustellen. Belässt man es dagegen bei dem traditionell in Deutschland verfolgten Ansatz, das Datenschutzrecht öffentlich-rechtlich durch Verbote und Gebote zu regeln, ist für erweiterte Beteiligung der Sozialpartner kein sinnvoller Raum.

IX. Schadensersatz und Sanktionen

a. Entspricht der **geltenden Rechtslage**. Für eine Beweislastumkehr zu Lasten des Arbeitgebers besteht kein Anlass.

d. Der Rahmen für Geldbußen ist mit einer Obergrenze von EUR 2 Mio. erheblich überzogen und steht insbesondere nicht in Relation zu den Strafrahmen anderer Gesetze (s. B.II.1.b.).

f. Hier gilt das zu lit. d. Gesagte.

DEUTSCHER BUNDESTAG
Ausschuss für
Arbeit und Soziales
16. Wahlperiode

Ausschussdrucksache 16(11)**1337**

22. April 2009

Stellungnahme

zur öffentlichen Anhörung von Sachverständigen am 11. Mai 2009 in Berlin zum

a) Antrag der Abgeordneten Brigitte Pothmer, Dr. Thea Dückert, Kerstin Andreae, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Rechte der Beschäftigten von Discountern verbessern - Drucksache 16/9101 -

b) Antrag der Abgeordneten Silke Stokar von Neuforn, Kerstin Andreae, Volker Beck (Köln), weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Persönlichkeitsrechte abhängig Beschäftigter sichern - Datenschutz am Arbeitsplatz stärken - Drucksache 16/9311 -

c) Antrag der Abgeordneten Jan Korte, Wolfgang Neskovic, Sevim Dagdelen, weiterer Abgeordneter und der Fraktion DIE LINKE.

Datenschutz für Beschäftigte stärken - Drucksache 16/11376 -

Hans Gliss, Hamburg

Datenverarbeitung im Personalwesen und Arbeitnehmerdatenschutz

I. Begriffsbestimmungen

1. Unter „Personalwesen“ werden folgende Arbeitsbereiche verstanden:

   Arbeitsvertragswesen, Personalakten, Nebenaufzeichnungen

   Zeit- und Leistungserfassung, Abwesenheiten, Entgeltabrechnung, Lohnkonto

   Melde- und Bescheinigungswesen zu Personaldaten

   Aus- und Weiterbildungspläne und -maßnahmen

   Statistiken

   Personalplanung: Bestand, Entlohnung, Fähigkeiten

   „Skill-Datenbank“: Eignungsprofile von Spezialisten

   Sozialwesen, freiwillige Leistungen des Arbeitgebers, Unterstützungskasse

   Interne Dienste, dazu zählen auch Berechtigungsprofile (Anmelden/Abmelden am Netzwerk)

   Betriebliche Altersversorgung

2. Daten des Personalwesens werden auch genutzt von den Bereichen:

   Betriebsrat, Personalrat

   Schwerbehinderten-Obmann

   Werksarzt

   Rechnungswesen

   Sucht- und Gleichstellungsbeauftragte

   Werkschutz, Interne Sicherheit

   Kommunikation (Werkszeitschrift, Schwarzes Brett, Presse- und Öffentlichkeitsarbeit)

II. Personaldaten und Datenschutz

Das BDSG untersagt die Verarbeitung personenbezogener Daten und definiert Erlaubnisse, die hier in einer Reihenfolge gelistet sind, die von „einfacher“ bis zu „schwieriger“ Handhabung von oben nach unten geordnet sind:

a) Sind alle verarbeiteten Daten aus allgemein zugänglicher Quelle? Dann ist keine weitere Prüfung nötig, die Verarbeitung ist zulässig. Der Fall dürfte im Personalwesen allerdings die Ausnahme sein; z.B. Stellenanzeigen in Zeitungen.

b) Rechtsvorschriften erlauben oder ordnen die Verarbeitung an; Zweckbestimmung und Erfordernis sind zu beachten

c) Anbahnung und Durchführung eines Vertragsverhältnisses (auch „vertragsähnliches Vertrauensverhältnis“); Zweckbestimmung und Erfordernis sind zu beachten

d) „Güterabwägung“: Das berechtigte Interesse des Verarbeiters oder eines Dritten begründet die Rechtmäßigkeit, sofern nicht überwiegende Interessen des Betroffenen am Ausschluss der Verarbeitung zu erkennen sind. → Wichtig: Diese Rechtfertigung der Datenverarbeitung gilt nicht für „sensitive Daten“ (§ 3 Abs. 9 BDSG).

e) Einwilligung des Betroffenen → Hier sind besondere Formvorschriften einzuhalten, damit die Einwilligung rechtlich wirksam zustande kommt. Im Personalwesen kann die Einwilligung nicht als Rechtsgrundlage zur Datenverarbeitung dienen, weil die herrschende Meinung davon ausgeht, dass im Arbeitsleben eine wesentliche Voraussetzung, die der Freiwilligkeit, nicht gegeben ist.

NB: Obiger Text verwendet um der leichteren Lesbarkeit halber nicht den Wortlaut des BDSG, sondern stellt die Regeln in einer umgangssprachlichen Diktion dar.

Diese Erlaubnistatbestände muss man sich vor Augen halten, wenn man die Verfahren beurteilen will, die im Personalwesen üblich sind.

III. Arbeitsbereiche des Personalwesens

1. Arbeitsvertragswesen, Personalakten, Nebenaufzeichnungen

   Suche nach geeigneten Arbeitskräften und Einstellungsverfahren liegen im Vorfeld eines vielleicht zustande kommenden Arbeitsvertrags. Datenquellen sind: Stellengesuche aus Zeitungen, Vorschläge der Bundesagentur für Arbeit, Spontanbewerbungen, Vorschläge von Head Huntern.

   → Rechtsgrundlage der Datenverarbeitung ist zunächst die Güterabwägung, bei weiteren Kontakten mit Bewerbern das „vertragsähnliche Vertrauensverhältnis“, erst beim Abschluss des Arbeitsvertrags kommt der Vertragsverhältnis für die Rechtfertigung der Datenverarbeitung infrage.

   Kommt der Arbeitsvertrag zustande, wird eine Personalakte angelegt. Hierzu gibt es keine gesetzlichen Vorgaben, aber Rechtsprechung des BAG, vor allem zur Vertraulichkeit von Personalakten.

   → Rechtsgrundlage für die Aufzeichnung: Arbeitsvertrag. Da der Arbeitsvertrag finanzwirksame Daten enthält, sind die Rechtsgrundlagen für diese Daten HGB und AO, dazu Lohnsteuerrichtlinien und einschlägige Erlasse der Finanzverwaltung (z.B.: GoBS).

   Nicht alle Personaldaten gehören zur Personalakte: Amtliche Dokumente (z.B. Lohnsteuerkarte und Schwerbehindertennachweis) sowie die Aufzeichnungen des Werksarztes. Aber auch Werkschutz und Sozialwesen haben eigene Datenbestände, die sich aus dem Arbeitsverhältnis ableiten.

   → als Rechtfertigung der Datenverarbeitung: Rechtliche Vorgaben, Güterabwägung, besondere Vertragsverhältnisse mit den Beschäftigten

2. Zeit- und Leistungserfassung, Abwesenheiten, Entgeltabrechnung, Lohnkonto

   Je nach Art der Bezahlung sind zu erfassen: Gearbeitete Zeiten (Zeitlohn), Leistungsmerkmale (Leistungslohn), bezahlte und unbezahlte Abwesenheiten; die Einsatzzeiten werden auf die Minute genau erfasst, wenn steuer- und beitragsfreie Zuschläge gezahlt werden.

   → Rechtsgrundlagen: Arbeitsvertrag und steuer- und sozialversicherungsrechtliche Vorschriften

   Die Entgeltabrechnung beziffert für jeden Beschäftigten das Bruttoentgelt des Abrechnungszeitraums und die gesetzlichen und persönlichen Abzüge, darüber hinaus üblicherweise auch die im Jahr aufgelaufenen Summen, damit die Abrechnung als Verdienstbescheinigung verwendet werden kann.

   → Rechtsgrundlagen: Arbeitsvertrag und steuer- und sozialversicherungsrechtliche Vorschriften, soweit es sich um den Abrechnungszeitraum handelt. Die Darstellung der im Jahr aufgelaufenen Summen ist ein zusätzlicher Service des Arbeitgebers, zu dem weder Rechtsvorschriften oder der Arbeitsvertrag verpflichten.

   Lohnkonto: Das Lohnkonto ist je Abrechnungszeitraum und in jährlicher Zusammenfassung zu führen und entsprechend den Vorschriften der AO und des Sozialversicherungsrechts aufzubewahren. Es steht zu Prüfzwecken (Lohnsteueraußenprüfung, Beitragsprüfung) zur Verfügung, aber auch zur Beantwortung amtlicher Anfragen nach Verdienstbescheinigungen. Wenn ein Mitarbeiter für seine eigenen Zwecke eine Bescheinigung für zurückliegende Zeiträume braucht, wird in der Regel ebenfalls aufs Lohnkonto zurückgegriffen.

   → Rechtsgrundlagen: Steuer- und sozialversicherungsrechtliche Vorschriften; aktueller oder ehemaliger Arbeitsvertrag

3. Melde- und Bescheinigungswesen zu Personaldaten

   Behörden und Gerichte haben diverse Ansprüche auf Auskunft zum Beschäftigungsverhältnis, Verdiensten und Ansprüchen des Arbeitnehmers.

   → Rechtsgrundlagen: Rechtsvorschriften

   Bescheinigungen werden aber auch ohne Rechtsgrundlage angefordert, eher im Privatbereich, teils aber auch durch Behörden (z.B. ausländische Gerichte). Bevor eine Bescheinigung ausgestellt wird, muss geprüft werden, ob eine Bescheinigungspflicht besteht. Wenn nicht, muss nach Lage der Dinge entschieden werden, ob bescheinigt werden darf oder nicht. Ziel ist dabei, dass dem (ggf. ehemaligen) Arbeitnehmer kein Schaden entsteht (weder durch Verweigerung noch durch Ausstellen einer Bescheinigung.

   → Rechtsgrundlagen: Güterabwägung

4. Aus- und Weiterbildungspläne und -maßnahmen

   Unternehmen verfolgen unterschiedlich ehrgeizige Personalentwicklungspläne – von Auszubildenden bis hin zu Spezialisten. Zweck ist, künftigen Herausforderungen des Marktes mit gut ausgebildeten Mitarbeitern rasch begegnen zu können. Dabei spielen auch Interessen der Mitarbeiter eine wichtige Rolle: Zufriedenheit, Karriere, Aneignung von Fach- und Allgemeinwissen werden gefördert. Beide Seiten profitieren davon.

   → Rechtsgrundlagen: Güterabwägung

5. Statistiken

   Regelmäßige statistische Auswertungen der Personaldaten sind einerseits aufgrund gesetzlicher Meldepflichten, andererseits für interne Steuerungsmechanismen erforderlich. Neben den regelmäßig erzeugten Auswertungen sind hin und wieder Ad-hoc-Statistiken erforderlich, beispielsweise im Vorfeld von Tarifverhandlungen oder zur Vorbereitung von Verhandlungen mit dem Betriebsrat bei beabsichtigten Betriebsänderungen (§§ 111 ff BetrVG).

   → Rechtgrundlagen: Rechtsvorschriften, Güterabwägung

6. Personalplanung: Bestand, Entlohnung, Fähigkeiten

   Als Ergebnis statistischer Auswertungen des Personalbestands, seiner Veränderungen und Prognosen hinsichtlich der Geschäftsentwicklung werden Personalstände, Entlohnungsstrukturen und Fähigkeitsprofile herangezogen, um künftige Personalbesetzungen realistisch einschätzen zu können (Fehlbedarf, Überkapazitäten, Wissensdefizite sollen rechtzeitig erkannt werden).

   → Rechtsgrundlage: Güterabwägung

7. „Skill-Datenbank“: Eignungsprofile von Spezialisten

   Global operierende Unternehmen, die wesentliche Teile ihrer Wertschöpfung durch Spezialwissen der Mitarbeiter generieren, legen Eignungsprofile an, damit die einzelnen Stellen – weltweit – nach Spezialisten suchen können, wenn plötzlich Bedarf entsteht. Datenschutzrechtlich unbednkliche Verfahren sind bekannt: Jedes Profil wird unter einem „nicht sprechenden Code“ abgelegt; nur die Personalabteilung kann nachvollziehen, welche Person sich hinter dem abgespeicherten Profil verbirgt. Damit ist rasche Personalentsendung möglich, wenn Bedarf entsteht. Sofern das Unternehmen die Skill-Datenbank verschlüsselt speichert, schützt sie sich außerdem gegen Attaken von Head Huntern.

   → Rechtsgrundlage: Güterabwägung

8. Sozialwesen, freiwillige Leistungen des Arbeitgebers (Bonusausschüttungen, Betriebskindergarten, Unterstützungskasse)

   Es gibt bei zahlreichen Unternehmen soziale Einrichtungen, die den Beschäftigten zur Verfügung stehen, ohne dass ein Rechtsanspruch besteht.

   → Rechtsgrundlage: Güterabwägung

9. Interne Dienste (Dienstwagen, Firmenkreditkarten, Parkplätze, Kantine, Werkswohnungen, Firmenausweise, Berechtigungsverwaltung für Zugang zu oder Zugriff auf geschützte Objekte)

   Interne Dienste regeln die alltäglichen Dinge, die für einen funktionierenden Betrieb nötig sind. Wer welche Berechtigungen bekommt, wer welche Einschränkungen – z.B. bei Hotelbuchungen – hinnehmen muss, das ist von Daten der Personaldatenbank abhängig.

   → Rechtsgrundlage: Güterabwägung

10. Betriebliche Altersversorgung

    Kommt vor als

    (1) Freiwillige Leistung des Arbeitgebers (ohne Rechtsanspruch)

    (2) Verbindliche Zusage (unverfallbare Anwartschaft) des Arbeitgebers; entweder im Arbeitsvertrag oder als eigener Vertrag regelt.

    → Rechtgrundlagen: Güterabwägung (Fall 1), sonst Vertragsverhältnis i.V.m. dem Gesetz zur Verbesserung der betrieblichen Altersversorgung

IV. Schnittstellen des Personalwesens zu anderen Bereichen im Unternehmen

1. Betriebsrat, Personalrat

   Der Arbeitnehmervertretung stehen gesetzliche definierte Informationsrechte an Personaldaten zu, um die Mitbestimmung wahrnehmen zu können.

   → Rechtsgrundlagen: BetrVG in der Wirtschaft und Personalvertretungsgesetze (Bund, Länder) bei Behörden.

   Darüber hinaus kommt es zu in Einzelfragen zur Offenlegung von Daten, wenn die Arbeitnehmervertreter Fälle und Anliegen vortragen, die einzelne Beschäftigte betreffen. Hier greift die vom BetrVG postulierte „vertrauensvolle Zusammenarbeit“. Der Arbeitgeber muss prüfen, inwieweit er Daten gegenüber der Arbeitnehmervertretung offenbaren kann, um Problemfälle gütlich zu klären.

   → Rechtsgrundlage: Güterabwägung.

2. Schwerbehinderten-Obmann

   Führt Karteien und Aufzeichnungen

   → Rechtsgrundlage: Rechtsvorschriften zur Beschäftigung von Behinderten

3. Werksarzt

   Der werksärztliche Dienst hat Anamnesen und Diagnosen für sich aufzuzeichnen und nicht dem Arbeitgeber zu offenbaren (§ 203 StGB). Er berichtet dem Arbeitgeber über Eignung/Nichteignung für einen definierten Arbeitsplatz. Darüber hinaus sind Reihenuntersuchungen und Gesundheitstests in bestimmten Arbeitsbereichen routinemäßig vorgesehen (z.B. Kantinenpersonal).

   → Rechtsgrundlagen: Gesetzliche Vorschriften

4. Rechnungswesen

   Das Rechnungswesen verarbeitet die finanzwirksamen Daten, die zum einzelnen Beschäftigten anfallen: Lohn/Entgelt, Ausfallvergütungen (Urlaub, Krankheit, Kurzarbeit), Lohnabzüge (unentschuldigtes Fehlen, unbezahlter Urlaub), Erstattung von Aufwand, z.B. Reisekosten, zweiter Wohnsitz, Heimfahrten.

   → Rechtsgrundlagen: AO, HGB, Lohnsteuerrichtlinien

5. Sucht- und Gleichstellungsbeauftragte

   Besondere Vertrauenspersonen mit heiklen Aufgaben

   → Rechtsgrundlage: Rechtsvorschriften

6. Werkschutz, Interne Sicherheit

(1) Der Werkschutz ist für den Zugang zum Unternehmen zuständig, aber auch zur Kontrolle von Personen, die das Werksgelände verlassen (Erkennung von Diebstählen).

→ Rechtsgrundlagen: Güterabwägung, Arbeitsvertrag (falls dort ausdrücklich geregelt)

(2) Interne Sicherheit wird für finanzwirksame Daten durch GoBS und Aktiengesetz als „Internes Kontrollsystem" vorgeschrieben. Hierunter fallen Themen wie Korruptionsbekämpfung, Datenabfluss, Insidergeschäfte etc. Die GoBS sind zwar „nur" ein ministerieller Erlass, erfüllen aber damit eine wesentliche Anforderung an die Ordnungsmäßigkeit der Verarbeitung finanzwirksamer Daten. Kontrollmechanismen, die Leistung oder Verhalten von Arbeitnehmern nachzeichnen, unterliegen der erzwingbaren Mitbestimmung (§ 87 Abs. 1 Nr. 6 BDSG); hierzu abgeschlossene Betriebsvereinbarungen sind damit zusätzlich Rechtsgrundlage der Verarbeitung.

→ Rechtsgrundlagen: Aktiengesetz, HGB, AO, GoBS, Betriebsvereinbarungen nach § 87 Abs. 1 Nr. 6 BetrVG).

7. Interne und externe Kommunikation (Werkszeitschrift, Schwarzes Brett, Presse- und Öffentlichkeitsarbeit)

   Jubiläen, wichtige Stellenbesetzungen, Informationen zur innerbetrieblichen Kommunikation, der Versand von Werks- oder allgemein wirtschaftsbezogen informierenden Zeitschriften (z.B. „aktiv"), Warnung vor Gefahren am Arbeitsplatz oder beim Erreichen des Werksgeländes

   → Rechtsgrundlage: Güterabwägung

V. Kontrollen

Kontrollmaßnahmen bei Lidl, Telekom und Bahn haben jüngst für öffentliche Empörung gesorgt. Das Thema ist aber wesentlich älter: Am 6.12.1983 hat das Bundesarbeitsgericht in einem Grundsatzurteil (PAN-AM-Entscheidung) festgestellt, dass Computersysteme „technische Einrichtungen" im Sinne des § 87 Abs. 1 Nr. 6 BetrVG sind. Seither unterliegen alle computergestützten Aufzeichnungen und Auswertungen, wenn sie Mitarbeiterdaten betreffen, der „erzwingbaren Mitbestimmung".

Kontrollen sind im Arbeitsleben eine Selbstverständlichkeit und gehören zu den Pflichten von Vorgesetzten. Das Betriebsverfassungsgesetz (BetrVG) regelt vor allem diejenigen Kontrollen, die mittels technischer Einrichtungen, also automatisiert, erfolgen (§ 87 Abs. 1 Nr. 6 BetrVG). Hier hat der Betriebsrat ein Mitbestimmungsrecht, das im Streitfall arbeitsgerichtlich durchgesetzt werden kann. Das Besondere daran ist dies: Nur wenn gesetzliche oder tarifvertragliche Vorschriften Kontrollmechanismen im Detail regeln (z.B. Fahrtenschreiber im LKW) ist die Mitbestimmung erledigt; fordern aber andere Vorschriften (Gesetz, Tarif, Satzung) Kontrollen, ohne sie näher zu spezifizieren, ist die Ausgestaltung der Kontrollmaßnahmen Gegenstand der Mitbestimmung (hier geht es also nicht um das „ob" von Kontrollen, sondern um das „wie"). Diese Konstellation ist häufig Anlass für Unstimmigkeiten zwischen Arbeitgeber und Betriebsrat, weil das Mitbestimmungsrecht des Betriebsrats von den Verantwortlichen im Unternehmen nicht erkannt wird, weil sie davon ausgehen, eine gesetzliche Anforderung umsetzen zu müssen.

Beispiele hierzu:

Die handelsrechtlichen Vorschriften (HGB, AO, GoBS, Lohnsteuerrichtlinien) zwingen zu genauer Aufzeichnung von Arbeitsleistungen, wenn steuer- und beitragsfreie Zuschläge gezahlt werden; außerdem sind die Aufzeichnungen fürs Lohnkonto rechtlich verbindlich vorgegeben. Reisekosten dürfen nur dann steuerfrei erstattet werden, wenn der Kostennachweis plausibel ist.

Das Bundesdatenschutzgesetz verpflichtet die verantwortliche Stelle (hier: den Arbeitgeber), Nachweise über Eingaben in Computersysteme zu führen (§ 9 BDSG nebst Anlage).

GoBS und Aktiengesetz verpflichten Unternehmen, ein Internes Kontrollsystem (IKS) einzurichten, das es erlaubt, finanzielle Schieflagen rechtzeitig zu erkennen. Dergleichen geht nicht ohne Kontrollmaßnahmen wie Datenabgleiche zur Korruptionsbekämpfung oder Auswertung von finanzwirksamen Transaktionen hinsichtlich unlogischer Sachverhalte.

Der Mitarbeiter des Werkschutzes, der seine Rundgänge macht, meldet sich an Kontrollstellen mit einem Schlüssel oder maschinenlesbaren Ausweis, um nachzuweisen, dass er aktiv war.

Wer sein Netzwerk sicher halten will, kommt um Filter- und Auswertungsfunktionen an der Schnittstelle zum Internet nicht herum. Dergleichen Kontrollen sind dem Betreiber aber nur gestattet, solange er kein „Diensteanbieter" im Sinne des TGK ist; die Bewegungen im Internet dürfen nur ausgewertet werden (dazu gehört auch die Erkenntnis auf Attacken von außen), wenn den Mitarbeitern die private Nutzung von E-Mail und Internet untersagt ist. Wir haben es mit einer für viele Internetbenutzer absurd wirkenden Gesetzgebung zu tun: Mitarbeitern muss jegliche private Internetnutzung am Arbeitsplatz untersagt werden, damit das Unternehmen wirksame Schutzmechanismen einrichten kann. Ist die private Nutzung erlaubt, begeht jeder Netzadministrator eine strafbare Handlung, wenn er dringend gebotene Kontroll- und Filtermechanismen einrichtet und nutzt.

NB: Unter Juristen ist umstritten, ob die Befugnis zu Kontrollmaßnahmen auch bei privater Nutzung kann sich aus § 9 BDSG i.V.m. § 96 Abs. 2 TKG in neuer Fassung ergeben kann. Gerichtsentscheidungen zu dieser Frage gibt es bisher nicht.

Die Liste ließe sich beliebig verlängern. Fazit: Kontrollen sind vielfältig nötig, die rechtlichen Grundlagen sind oft nicht einleuchtend für den gebildeten Laien.

Hierzu noch eine Anmerkung: 1986 wurde das Gesetz zur Bekämpfung der Wirtschaftskriminalität novelliert. Der damalige Justizminister Engelhard führte einen prominenten Fall an, um die Notwendigkeit der Novelle zu begründen: Einem Beschäftigten eines bayerischen Arbeitsamts war es geglückt, 176.000 DM durch fiktive Kinder in knapp zwei Jahren abzuzweigen. Die Bundesanstalt für Arbeit hatte wenige Jahre zuvor eine Vereinbarung mit dem Personalrat als beispielhaft gefeiert, wonach die Auswertung von Arbeiten von Beschäftigen der BA am Terminal untersagt wurde. Damit war dann

der „aggressiven Vermögensbildung“ Tür und Tor geöffnet.

VI. Meine Einschätzung:

Was bei Lidl, Bahn, Drogeriekette Müller und Telekom – für die Öffentlichkeit bisher bekannt – gelaufen ist, war ohne jeden Zweifel illegal. Es konnte passieren, weil interne Kontrollmechanismen nicht installiert waren oder nicht gegriffen haben. Diese Dinge darf aber man nicht der in gutem Glauben arbeitenden Wirtschaft als Generalverdacht überstülpen. Mittelständische Unternehmen haben wegen der Nähe zu den Beschäftigten mehr Augenmaß als Großkonzerne (die Vermutung, dass die Staatsnähe - Bahn – Post – Telekom besonders verführerisch wirkte, Gesetzesvorgaben zu ignorieren, liegt vielleicht nahe). Es geht darum, vorsichtig zu unterscheiden:

- Bedarf nach gesetzlicher Präzisierung
- Beseitigung von Vollzugsdefiziten bei der Datenschutzaufsicht
- Vermeidung einer Überregulierung

Dazu im Einzelnen:

Bedarf nach gesetzlicher Präzisierung:

Hier sind drei Regelungen zum Arbeitnehmerdatenschutz denkbar und sinnvoll:

1. Der betriebliche Datenschutzbeauftragte wird verpflichtet, bei **allen Verfahren des Personalwesens** eine Vorabkontrolle, bestehend aus Sachverhaltsbeschreibung, Bewertung und Empfehlungen, durchzuführen und seine Einschätzung der Geschäftsführung und der Arbeitnehmervertretung zur Kenntnis zu bringen.
2. Besteht im Unternehmen keine Arbeitnehmervertretung, so hat der Datenschutzbeauftragte gleichwohl die für die IT anzuwendenden Bestimmungen des BetrVG (§ 94, § 87 Abs. 1 Nr. 1 und Nr. 6) bei seiner Vorabkontrolle zu berücksichtigen.
3. Die von § 3 Abs. 9 BDSG besonders geschützten Daten enthalten u.a. Angaben über Gesundheit. Der unerlaubte Umgang mit solchen Daten sollte als Straftatbestand in den § 44 BDSG aufgenommen werden. Dann wird zahlreichen Befürchtungen über leichtfertigen Umgang mit Gesundheitsdaten von Mitarbeitern und Bewerbern begegnet.

Beseitigung von Vollzugsdefiziten bei der Datenschutzaufsicht:

Wenn eine Aufsichtsbehörde, namentlich die von Baden-Württemberg, in ihrem Tätigkeitsbericht die Meinung äußert (von anderen Aufsichtsbehörden bestritten – durch Dr. Thilo Weichert voran), Datenverarbeitung im Personalwesen sei nur zulässig aufgrund von Rechtsvorschriften oder in der Durchführung des Arbeitsvertrags, dann kann das wohl nur jemand geschrieben haben, der vom Personalwesen nicht mehr versteht, als seinen eigenen Arbeitsvertrag und den monatlichen Entgeltnachweis zu lesen.

Vermeidung einer Überregulierung:

Wenn der Gesetzgeber den Verfahren des Personalwesens mit einem Arbeitnehmerdatenschutz gerecht werden wollte, fördert das die Bürokratisierung. Punktuelle Verbesserung der bestehenden Gesetzeslage (siehe oben) und Abbau von Vollzugsdefiziten beim geltenden Recht halte ich für den besseren Ansatz.

21. April 2009

DEUTSCHER BUNDESTAG
Ausschuss für
Arbeit und Soziales
16. Wahlperiode

Ausschussdrucksache 16(11)**1367**

7. Mai 2009

Stellungnahme

zur öffentlichen Anhörung von Sachverständigen am 11. Mai 2009 in Berlin zum

a) Antrag der Abgeordneten Brigitte Pothmer, Dr. Thea Dückert, Kerstin Andreae, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Rechte der Beschäftigten von Discountern verbessern - Drucksache 16/9101 -

b) Antrag der Abgeordneten Silke Stokar von Neuforn, Kerstin Andreae, Volker Beck (Köln), weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Persönlichkeitsrechte abhängig Beschäftigter sichern - Datenschutz am Arbeitsplatz stärken - Drucksache 16/9311 -

c) Antrag der Abgeordneten Jan Korte, Wolfgang Neskovic, Sevim Dagdelen, weiterer Abgeordneter und der Fraktion DIE LINKE.

Datenschutz für Beschäftigte stärken - Drucksache 16/11376 -

d) Antrag der Abgeordneten Gisela Piltz, Dr. Heinrich L. Kolb, Jens Ackermann, weiterer Abgeordneter und der Fraktion der FDP

Schutz von Arbeitnehmerdaten durch transparente und praxisgerechte Regelungen gesetzlich absichern - Drucksache 16/12670 -

Dr. Ulrike Fleck, Ludwigshafen

Ein ausgewogener Datenschutz im Arbeitsverhältnis ist ein wichtiges Element in der Zusammenarbeit zwischen Arbeitgeber und Arbeitnehmern, denn hier geht es um eine interessengerechte Balance zwischen erfolgreichem unternehmerischen Handeln - nicht zuletzt zum Zwecke des Erhalts der Wettbewerbsfähigkeit und der Arbeitsplätze – und Eingriffen in die Persönlichkeitssphäre des Mitarbeiters. Datenschutz ist somit ein Thema, das in den Unternehmen ebenso ernst genommen werden muss wie beispielsweise die betriebliche Mitbestimmung oder das Thema Compliance.

Vor dem Hintergrund der jüngsten Ereignisse in einigen Unternehmen ist es daher nachvollziehbar, dass der Gesetzgeber sich veranlasst sieht, Klarstellungen im Datenschutzrecht vorzunehmen, die zu einer Verbesserung der Transparenz der bestehenden Regelungen und damit zu mehr Rechtssicherheit bei Fragen des Datenschutzes im Arbeitsverhältnis führen sollen. Dies kann grundsätzlich auch durchaus sinnvoll sein, denn datenschutzrechtliche Regelungen sind über das BDSG hinaus auch an zahlreichen anderen Stellen zu finden, was den Unternehmen eine besonders hohe Sorgfalt abfordert. Dass es beispielsweise naheliegend sei, bei Veröffentlichung eines bebilderten Berichts über eine betriebliche Veranstaltung für Mitarbeiter und ihre Familien in den werksinternen Medien auch die Voraussetzungen des § 23 KunstUrhG zu beachten, wird niemand behaupten wollen.

Dennoch darf nun von gesetzgeberischer Seite der Bogen nicht überspannt werden. Es wäre falsch, entlang der Einzelthemen, die in den letzten Monaten als kritisch identifiziert wurden, Regelungen zu treffen und dabei das Gesamtbild der Wirkungsweise des Datenschutzrechts im Arbeitsverhältnis außen vor zu lassen.

Es wäre auch verfehlt, über die Schiene des Datenschutzes bewährte arbeitsrechtliche Rechtsprechung, die die Interessen von Arbeitgeber und Arbeitnehmern sorgsam gegeneinander abwägt, eingrenzen und Themen, die in ihrem Schwerpunkt das Arbeitsrecht und nicht das Datenschutzrecht betreffen, die aber in einem anderen Kontext wegen der unterschiedlichen Positionen verschiedener Interessenvertreter schwer regelbar sind, nun aus Anlass datenschutzrechtlicher Verfehlungen oder Fehleinschätzungen einzelner Arbeitgeber über die Schiene des Datenschutzes regeln zu wollen.

Es ist auch widersprüchlich, den Unternehmen auf der einen Seite national und europarechtlich gesetzliche Pflichten zur Kontrolle von Mitarbeitern aufzuerlegen, für deren Umsetzung ein großer Aufwand in den Unternehmen anfällt, wie es z. B. durch das SÜG oder durch

die europäische Antiterrorgesetzgebung geschehen ist, und andererseits die einfache Leistungskontrolle oder gar die Prävention gegen ungesetzliches Handeln gesetzlich nur deshalb verbieten oder erheblich einschränken zu wollen, weil heute Prozesse in den Unternehmen IT-gestützt ablaufen und moderne Informations- und Kommunikationstechnik zum Einsatz kommt. Selbstverständlich darf diese Technik nicht dazu führen, dass ungerechtfertigte Eingriffe in die Persönlichkeitsrechte der Arbeitnehmer erfolgen; die datenschutzrechtlichen Nutzungsregelungen sind aber mit Augenmaß vorzunehmen.

Das heutige BDSG trifft sehr ausgewogene Regelungen, die es dem Arbeitgeber bei jeder Datennutzung und -verarbeitung im Arbeitsverhältnis erneut zur Pflicht machen, eine Interessenabwägung zwischen den Unternehmens- und Mitarbeiterinteressen zu treffen. Auf dieser Grundlage ist der verantwortungsbewusste Umgang mit Mitarbeiterdaten für vernünftig agierende Unternehmen eine Selbstverständlichkeit. Unbestritten können die heutigen Regelungen, wie im Übrigen ebenfalls jede neu geschaffene Spezialnorm, auch verletzt werden. Aber auch unter heute geltender Rechtslage kann - und wie man in den Fällen der letzten Monate gesehen hat, wird davon auch Gebrauch gemacht - gegen die Verantwortlichen vorgegangen werden.

Daher sollte von Seiten des Gesetzgebers sehr sorgsam abgewogen werden, an welchen Stellen das national ohnehin schon sehr hohe Datenschutzniveau noch angehoben werden soll. Ein kodifiziertes Arbeitnehmerdatenschutzrecht darf in keinem Fall dazu führen, dass Einstellungs-, Durchführungs- und Beendigungsprozesse von Arbeitsverhältnissen in den Unternehmen erschwert, das nationale Arbeitsrecht noch verschärft und damit die Wettbewerbsbedingungen der deutschen Unternehmen im europäischen Markt und auf dem Weltmarkt verschlechtert werden. Die Einführung des AGG hat gezeigt, dass die Unternehmen, die schon vor Inkrafttreten dieses Gesetzes keine Auseinandersetzungen um Diskriminierungen hatten, auch unter neuer Rechtslage keine solchen Auseinandersetzungen führen. Dennoch sind in allen Unternehmen ein erheblicher Umsetzungsaufwand und überflüssige bürokratische Hindernisse entstanden. Ähnlich würde es sich auch hinsichtlich der Umsetzung der in den oben genannten Anträgen enthaltenen Regelungsvorschläge entwickeln.

Dies vorausgeschickt, ergeben sich folgende Kernpunkte:

1. Mehr Transparenz in der Systematik der datenschutzrechtlichen Bestimmungen ist wünschenswert.
2. Eine Regelung des Arbeitnehmerdatenschutzes darf - insbesondere vor dem Hintergrund des im europäischen Vergleich ohnehin hohen Datenschutzniveaus - nicht zu erhöhter Bürokratie oder sonstigen Wettbewerbsnachteilen führen. Dies gilt zum einen hinsichtlich der Einschränkung von Erlaubnistatbeständen zur Datenverarbeitung, der Reglementierung bestimmter Sachverhalte, aber auch hinsichtlich etwaiger Informationspflichten gegenüber Arbeitnehmern.
3. Daten müssen sicher aufbewahrt, verwaltet, einem strengen Zugriffssystem unterworfen sein und der innerbetrieblichen Datenschutzkontrolle unterliegen.
4. Die Rechtsprechung hat ausgewogene Interessenabwägungen von Arbeitgeber- und Arbeitnehmerinteressen insbesondere bei der Einstellung von Bewerbern entwickelt. Diese müssen aufrecht erhalten werden.
5. Die Beteiligungsrechte der Arbeitnehmervertretungen nach dem BetrVG/BPersVG sind bei der Datenverarbeitung zu beachten. Einer Ausweitung dieser Regelungen bedarf es nicht, auch die heutigen Bestimmungen bieten ausreichend Schutz für die Arbeitnehmer, sie brauchen nur gesetzeskonform umgesetzt zu werden. Ein Mehr an Regelungen gewährleistet aber bekanntlich nicht die bessere Umsetzung.
6. Datenverarbeitung im Arbeitsverhältnis geht weit über die in den Anträgen beschriebenen Regelungsbereiche hinaus. Hier sei beispielweise angemerkt, dass im Rahmen von börsenaufsichtsrechtlichen Verpflichtungen insbesondere in den USA und bei Unternehmenskäufen zum Zwecke der Fusions- und sonstigen Wettbewerbskontrolle durch ausländische Behörden gesetzliche Pflichten anderer Staaten zu erfüllen sind. Auch arbeitssicherheitsrechtliche Aspekte, die Umsetzung bestimmter Unternehmensentscheidungen oder die Bewertung von Informationen zum Zwecke bestimmter unternehmerischer Ziele (z. B. Diversity oder Maßnahmen, mit denen demografischen Aspekten Rechnung getragen werden soll), Angebote von Unternehmen an ihre Mitarbeiter und Pensionäre (z. B. Einkauf in betriebseigenen Shops etc.) erfordern die Verarbeitung von Daten. Es gilt, auch hierfür verlässliche Rechtsgrundlagen zu gewährleisten und nicht durch Beschränkung der heutigen Erlaubnistatbestände Rechtsunsicherheiten zu schaffen.
7. Zum Schutze aller Mitarbeiter und Dritter, die sich auf einem Werksgelände bewegen, muss es möglich sein, sowohl präventiv als auch aufklärend bei allen Arten von Verstößen gegen Arbeitsvertrag, betriebliche Ordnung oder sonstige Rechtsvorschriften vorzugehen. Erst Recht gilt das, wenn es um die Aufklärung von Straftaten, Korruption und sonstigen Compliance-Verstößen geht. Eine Überprüfung dahingehend, ob ein Mitarbeiter mittels moderner Medien Betriebs- und Geschäftsgeheimnisse an Dritte, möglicherweise sogar an Konkurrenzunternehmen verbreitet, darf ebenfalls nicht eingeschränkt werden. Zu diesen Zwecken muss auch die Durchführung von Stichprobenkontrollen zulässig sein, sofern diese vorher transparent in Art und Umfang beschrieben werden, ihre Verhältnismäßigkeit sichergestellt ist und die Mitarbeiter in nachvollziehbarer Art und Weise darüber unterrichtet wurden.
8. Datenschutzrechtliche Nutzungsregelungen für betrieblich zur Verfügung gestellte Internet- und E-Mail-Systeme sind mit Augenmaß vorzunehmen. Auch hier gilt wieder, dass sich Anforderungen an Inhalt, Umfang, Häufigkeit, Regeln zur Verhältnismäßigkeit im Übrigen und zur Sicherstellung der Information der Mitarbeiter über Stichprobenkontrollen normativ beschreiben lassen.
9. Der Datenaustausch im Konzern muss erleichtert werden. Die heute erforderlichen umfangreichen - zudem in der Regel genehmigungspflichtigen - Vertragswerke zwischen den Konzerngesellschaften insbesondere beim Datentransfer in das außereuropäische Ausland stellen hohe bürokratische Hürden dar.

Im Einzelnen:

I. Stellungnahme zum ersten Diskussionsvorschlag der Bundesregierung zur geplanten Grundsatzregelung des § 32 BDSG

Die im ersten Diskussionsvorschlag formulierte Neufassung des § 32 BDSG beinhaltet zwei zentrale, für die Unternehmen unverhältnismäßig einschränkende Neuregelungen:

1. Die Erlaubnistatbestände der Datenverarbeitung im Arbeitsverhältnis sollen zum einen um folgenden Tatbestand eingeschränkt werden: ..... soweit die Datenverarbeitung zur Wahrung berechtigter Interessen des Arbeitgebers erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Arbeitnehmers an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. ....

   Zum anderen wird auch der Erlaubnistatbestand der Zweckbestimmung, der sich bisher allgemein auf den Zweck des Arbeitsverhältnisses bezogen hat, im geplanten Diskussionsvorschlag zu § 32 BDSG eingeschränkt.

   Somit verbleiben nur noch die Erlaubnistatbestände der Einwilligung des Arbeitnehmers und der Erlaubnistatbestand der Datenverarbeitung auf Grundlage einer ermächtigenden Rechtsvorschrift.

   Mit der erlaubenden oder anordnenden Rechtsvorschrift und der Einwilligung alleine ist es aber für einen Arbeitgeber nicht möglich, Datenverarbeitung im Arbeitsverhältnis und damit im Zusammenhang stehender Fragen in der durch moderne Technologie geprägten Arbeitswelt durchzuführen. Eine einmal erteilte Einwilligung kann schon nach heute geltender Rechtsprechung nicht als Erlaubnistatbestand für zukünftige Datenverarbeitungsvarianten herangezogen werden. Betrachtet man sich die Entwicklung der IT-gestützten Personalprozesse allein in den letzten 15 Jahren, so hätten die Unternehmen ohne die übrigen Erlaubnistatbestände jährlich mehrfach Einwilligungen zur Datenverarbeitung einholen müssen. Dies ist insbesondere in größeren Unternehmen völlig unpraktikabel und führt zudem nach langjährigen betriebspraktischen Erfahrungen zu immer wiederkehrender Verunsicherung der Mitarbeiter. Mitarbeiter erwarten, dass ihre im Zusammenhang mit dem Arbeitsverhältnis stehenden Angelegenheiten durch den Arbeitgeber ordnungsgemäß erledigt werden und sie vertrauen in aller Regel auch den handelnden Personen ihrer Personalabteilungen und erst recht bei mitbestimmten Vorgängen ihrer Arbeitnehmervertretung. Jede unternehmensweite Unterschriftsaktion wird von den Mitarbeitern daher häufig als ungewöhnlich und beängstigend empfunden. Schon aus diesem Grunde können die Einwilligung und die ermächtigende Rechtsvorschrift allein keine probaten Mittel sein, Datenverarbeitungsvorgänge in Personalprozessen zu legitimieren.

   Die bisherige weit gehaltene Erlaubnisnorm der Zweckbestimmung eines Vertragsverhältnisses in § 28 Abs. 1 Nr. 1 BDSG würde durch die im Diskussionsvorschlag enthaltene Änderung des § 32 BDSG ebenfalls eingeschränkt. Zwar dürften personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses weiterhin verarbeitet werden, aber nur dann, wenn dies entweder für die **Entscheidung** über die Begründung eines Beschäftigungsverhältnisses erforderlich oder **nach Begründung** für dessen Durchführung oder Beendigung erforderlich oder durch eine Rechtsvorschrift erlaubt oder angeordnet wäre.

   Hier ist zum einen unverständlich, weshalb die Datenverarbeitung zwar für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses zulässig sein soll, nicht aber die Begründung selbst. Zum anderen reichen diese Erlaubnistatbestände bei weitem nicht aus: Der Diskussionsvorschlag zur Neuregelung des §32 BDSG zentriert die Datenverarbeitung auf den Kern des eigentlichen Arbeitsverhältnisses. Würde man also ein Lehrbuch zum Arbeitsrecht aufschlagen, könnten die sich dort wiederfindenden Inhalte, z. B. Datenerhebung im Rahmen von Einstellungsbefragungen, Datenerfassung in einer elektronischen Personalakte, Datenverarbeitung zum Zwecke der korrekten Entgeltauszahlung etc. problemlos über den neu zugeschnittenen Erlaubnistatbestand der Zweckbestimmung gerechtfertigt werden. Ein Arbeitsverhältnis hat aber viele Facetten, die außerhalb dieses eigentlichen Kernbereichs liegen. Es ist jetzt schon vorherzusehen, dass der veränderte Zweckbestimmungserlaubnistatbestand und der wegfallende Erlaubnistatbestand der Datenverarbeitung im berechtigten Interesse des Unternehmens zu zahlreichen Rechtsstreitigkeiten um die Frage führen würde, ob denn die im Einzelfall vorliegende Datenverarbeitung noch zum Kern des Arbeitsverhältnisses zählt und damit legitimiert ist oder nicht.

   Ist beispielsweise ein deutsches Unternehmen an der amerikanischen Börse gelistet, unterliegt es den börsenaufsichtsrechtlichen Bestimmungen des Sarbanes-Oxley-Acts. Danach sind auch deutsche Unternehmen verpflichtet, bestimmte Prüfmechanismen individuell beim einzelnen Mitarbeiter zu etablieren. Hier wird man trefflich darüber streiten können, ob dies der Durchführung des Arbeitsverhältnisses dient. Im Gegenteil, betriebspraktische Erfahrungen zeigen, dass zum Schutz der Mitarbeiter vor diesen Kontrollmechanismen, die in einer IT-gestützten Arbeitswelt selbstverständlich nicht ohne Datenverarbeitung ablaufen können, häufig kollektive Regelungen mit den Arbeitnehmervertretungen über die Auswirkungen dieser Kontrollpflichten im einzelnen Arbeitsverhältnis geschlossen wurden. Gleiche Problematik stellt sich bei Unternehmenskäufen, bei denen ausländische Wettbewerbsbehörden beteiligt sind und ihre aufsichtsrechtlichen Pflichten wahrnehmen. Auch in diesem Rahmen gibt es Auskunftspflichten der deutschen Unternehmen, die, wenn es sich beispielsweise um ein Spezialgebiet handelt, durchaus einzelne Mitarbeiter betreffen können.

   Auch die Arbeitssicherheit in einem Unternehmen erfordert unter Umständen Maßnahmen, die ohne den Erlaubnistatbestand der Zweckbestimmung in bisheriger Ausprägung und insbesondere ohne den Erlaubnistatbestand des berechtigten Interesses nicht durchführbar wären. Sind beispielsweise bestimmte Abfüllvorgänge chemischer Substanzen in dafür vorgesehene Kesselwagen zu tätigen, ist es aus Arbeitssicherheitsgesichtspunkten geboten, den Abfüllvorgang (und damit auch den abfüllenden Mitarbeiter) mit ei-

ner Videokamera zu überwachen, um sofort eingreifen zu können, wenn dieser bei der Durchführung des Vorgangs verletzt würde oder vom Kesselwagen oder gar in den Kesselwagen stürzen würde. Auch die Auswertung bestimmter personenbezogener Medien (z. B. Fahrtenschreiber) zur Aufklärung von Unfällen ist unerlässlich, wäre aber möglicherweise nach dem Vorschlag zu § 32 BDSG problematisch.

Zweifelhaft wäre auch, ob ein Unternehmen auf Basis einer Betriebsvereinbarung als rechtfertigende Rechtsvorschrift weiterhin entscheiden könnte, eine Verpflichtung der Mitarbeiter zur offenen Ausweistragepflicht zu etablieren.

Auch im Servicebereich, in dem es heute schon ein Gebot der Höflichkeit ist, dass Namensschilder an der Kleidung getragen werden, würde sich das Problem in gleicher Weise stellen.

Ferner gibt es auch insbesondere in den größeren Unternehmen Vorgänge, zu denen die Mitarbeiter oder Pensionäre allein aufgrund ihrer Betriebszugehörigkeit berechtigt sind, z. B. in werkseigenen Shops einkaufen oder in eigenen Weiterbildungszentren Medien zum Selbststudium ausleihen. Der Zusammenhang zur Durchführung des Arbeitsverhältnisses ist hier schwer zu begründen. Dennoch wird niemand ernsthaft behaupten wollen, dass eine entsprechende Abrechnung über das Gehalt künftig wegen nicht mehr erlaubter Datenspeicherung entfallen muss und das für den Mitarbeiter einen größeren Schutz und damit Vorteil darstellen würde. Gleiches gilt für die Zusendung von betrieblichem Infomaterial an Privatadressen von Mitarbeitern und Pensionären. Letztere Gruppe wäre ja nach dem jetzigen Stand des Diskussionsvorschlags gänzlich von derartigen Vergünstigungen abgeschnitten.

Neben diesen Beispielen, die die Thematik sehr deutlich machen, gibt es aber auch andere Felder, auf denen Unsicherheit über die Zulässigkeit der Datenverarbeitung entstehen würde:

Dies betrifft zunächst einmal die Umsetzung bestimmter Unternehmensziele: Will ein Unternehmens beispielsweise Diversity fördern und damit die Chancen von einzelnen Mitarbeitergruppen verbessern, oder will es angesichts der demografischen Entwicklung zielgerichtet für ältere Mitarbeiter bestimmte Angebote eröffnen, muss es zunächst einmal eine tragfähige Faktenbasis als Grundlage schaffen. Hierzu ist es notwendig, bestimmte Auswertungen personenbezogener Daten zu erstellen. Auch hier wird man trefflich darüber streiten können, ob dies vom geplanten § 32 BDSG noch erfasst wäre.

Auch Alltäglichkeiten könnten in die Kritik geraten: Soll beispielsweise ein neues Abrechnungssystem eingeführt werden und besteht in dem Unternehmen kein Betriebsrat, so dass keine Betriebsvereinbarung als Erlaubnisnorm geschlossen werden kann, sind dennoch Testläufe mit Echtdaten der Mitarbeiter erforderlich. Diese wären aber kaum zu rechtfertigen. Oder soll schlicht eine Statistik erstellt werden, wie viele Auszubildende im Rahmen einer Verbundausbildung mit vielen Verbundpartnern in welchem Ausbildungsberuf ausgebildet werden, dann muss zum einen eine Datenübermittlung zulässig und zum anderen die Auswertung erlaubt sein.

Und schließlich: Auch Leistungsbeurteilungen stützen sich in einer Arbeitswelt, in der die allermeisten Arbeitspflichten IT-gestützt verrichtet werden, auf personenbezogene Daten. Es wäre fernliegend, wenn hier eine Diskussion darüber entstehen würde, ob dies noch im Rahmen der Erforderlichkeit der Durchführung des Beschäftigungsverhältnisses liegt, allerdings ist auch eine solche Diskussion im Hinblick auf die die Arbeitgeber gelegentlich überraschende Rechtsprechung zu bestimmten Themen nicht völlig ausgeschlossen.

2. Die Beschränkung der im Diskussionsvorschlag zu § 32 Abs. 1 Ziffer 3 BDSG vorgesehenen Erlaubnisnorm hinsichtlich **begangener Straftaten** ist für die Unternehmenspraxis vollkommen untauglich. Sie steht auch in nicht zu erklärendem Widerspruch zu den Verpflichtungen, denen Unternehmen im Hinblick auf die Umsetzung des Sicherheitsüberprüfungsgesetzes und der europäischen Verordnungen zur Terrorismusbekämpfung unterworfen sind. Zum Schutze aller Mitarbeiter und Dritter, die sich auf einem Werksgelände bewegen, muss es möglich sein, sowohl präventiv als auch aufklärend bei allen Arten von Verstößen gegen Arbeitsvertrag, betriebliche Ordnung oder sonstige Rechtsvorschriften vorzugehen. Beispielsweise können Verstöße gegen Sicherheitsbestimmungen in einem chemischen Unternehmen gravierende Auswirkungen haben, die personenbezogen aufgeklärt und arbeitsrechtlich gemaßregelt werden müssen, um weiteren Verstößen vorzubeugen. Ferner sind Unternehmen heute in hohem Maße verpflichtet, umfassende Maßnahmen zu ergreifen, um die Einhaltung ihrer Compliance-Regeln sicherzustellen. Hierzu muss es dem Unternehmen auch möglich sein, Stichprobenkontrollen durchzuführen. Berücksichtigt man den Diskussionsvorschlag zu § 32 Abs. 2 BDSG, dann wäre es nicht einmal mehr möglich, Torkontrollen durchzuführen und damit vorzubeugen, dass Unternehmenseigentum nicht illegal aus dem Werk verbracht wird.

II. Stellungnahme zum oben genannten Antrag der LINKEN

Der einleitenden Bemerkung der LINKEN, dass das Fehlen gesetzlicher Vorgaben zum Schutz der Daten von Beschäftigten offensichtlich bei vielen Unternehmen die Ansicht entstehen ließ, alles zu dürfen, um ihre Beschäftigten zu überwachen, muss aus der praktischen Erfahrung in einem Großunternehmen, in dem jährlich über 500 Schulungsmaßnahmen zum Datenschutz durchgeführt werden, ca. 50 Vorabkontrollen von IT-Systemen stattfinden und in einem zentral geführten Verfahrensverzeichnis mehrere tausend Einträge vorhanden sind, widersprochen werden.

1. Zu den im Antrag enthaltenen Grundsätzen der Datenverarbeitung lässt sich folgendes anmerken:

   Eine Ausdehnung des Datenschutzgesetzes auf den nicht öffentlichen Bereich ist nicht erforderlich, denn das Datenschutzgesetz gilt auch in seiner heutigen Fassung für private Unternehmen.

   Damit gilt es bereits heute für alle Arten der Erbringung von Arbeitsleistung, nicht hingegen für alle Arten von Vertragsgestaltungen. Lässt ein Unternehmen Leistungen im Wege des Werkvertrages erbringen, müssen - auch zur Verhinderung von Schwarzarbeit

und illegaler Ausländerbeschäftigung - Daten auch von Fremdfirmenmitarbeitern erhoben und verarbeitet werden. Diese Art der Datenverarbeitung lässt sich aber mit den genannten Erlaubnistatbeständen nicht rechtfertigen. Das BDSG heutiger Fassung gilt auch nicht, und dies mit gutem Grund, für die in I. c) genannten Outgesourcten, denn diese haben in der Regel ein Arbeitsverhältnis mit einem neuen Arbeitgeber begründet, der für den Schutz ihrer Daten zuständig ist und auch künftig bleiben sollte.

Zuzustimmen ist der Forderung in Ziffer I. g), dass Personaldatenverarbeitung nur durch solche Beschäftigte erfolgen sollte, die vorher gemäß § 5 BDSG auf das Datengeheimnis verpflichtet wurden und eine angemessene Schulung erhalten haben.

Sinnvoll ist auch der in Ziffer I. f) vorgesehene Schutzmechanismus der klaren Festlegung eines Zugriffberechtigungskonzeptes. Eine Abstimmung mit dem Betriebsrat geht aber insoweit über § 87 Abs. 1 Nr. 6 BetrVG hinaus.

Hinsichtlich der im Antrag enthaltenen Erlaubnistatbestände in Ziffer I. d), e), j), k), l) und o) wird auf die Ausführungen zu § 32 BDSG verwiesen. Der Antrag sieht eine noch weitere Einschränkung vor, diese ist jedoch schon vor der dargelegten Begründung zu § 32 BDSG in der Praxis nicht umsetzbar.

An den Erfordernissen und tatsächlichen Gegebenheiten der Praxis vorbei geht auch die in Ziffer I. h) enthaltene Forderung, die in elektronischen Personalakten gespeicherten Daten von Mitarbeitern von den übrigen Daten getrennt zu verarbeiten. IT-Systeme sind heute so konzipiert, dass für bestimmte Personalprozesse immer wieder auf einen Grunddatenbestand zurückgegriffen wird, der auch Bestandteil von Personalakten ist. Nutzen die Unternehmen also die auf dem Markt gängigen Personaldatenverarbeitungssysteme, könnten sie die in Ziffer I. f) enthaltene Forderung ohne zusätzliche Programmierung und entsprechende IT-Kosten gar nicht umsetzen.

Ziffer I. i) betrifft die Datenverarbeitung auf Serviceplattformen. Hat sich ein Unternehmen dazu entschlossen, Servicedienstleistungen einzelner Konzerngesellschaften aus dem Personal- (z. B. auch die Entgeltabrechnung) und Finanzbereich auf zentrale Serviceplattformen zu übertragen, wäre diese für den Konzern kostensparende Standardisierung nach dem Antrag der LINKEN nicht mehr zulässig. In diesem Zusammenhang stellt sich für die Unternehmen aber eine andere zentrale Frage des Datenschutzes, die weder im Diskussionsvorschlag zu § 32 BDSG noch in einem der vorliegenden Anträge Berücksichtigung gefunden hat, nämlich die Frage des Datenaustausches im Konzern. Dieser ist heute nur auf Basis umfangreicher, zumeist genehmigungsbedürftiger vertraglicher Verpflichtungen zwischen den Konzernunternehmen zulässig, soweit es um den Datenaustausch im außereuropäischen Rechtsraum geht. Dies ist mit hohem bürokratischem Aufwand und mit Rechtsunsicherheiten verbunden. In diesem Zusammenhang noch ein weiteres Beispiel: soll eine Position im Ausland mit einem deutschen Mitarbeiter besetzt werden und stehen mehrere Kandidaten zur Auswahl, ist es unerlässlich, dass die lokalen Führungskräfte Daten über alle Kandidaten erhalten können, um ihre Entscheidung sachgemäß zu treffen.

Die Pflicht zur Information der Mitarbeiter über die Nutzung ihrer personenbezogenen Daten ist sinnvoll und schafft Rechtsklarheit, darf in der Ausgestaltung jedoch nicht zu übermäßigem bürokratischem Aufwand führen. Gleiches gilt für die Verschlüsselung zum Schutz besonderer Arten von Daten.

Datenerhebungen gerade bei besonderen Arten von Daten, z. B. solcher Daten, die von Betriebsärzten erhoben und genutzt werden, die einer gesetzlichen Schweigepflicht unterliegen, der Beteiligung des Betriebsrates zu unterwerfen, wäre nur im Hinblick auf die Frage, welche Arten von Daten erhoben und in welchen Systemen sie gespeichert werden und wer Zugriff auf diese Systeme hat, in der Praxis ohne Verwerfungen mit einzelnen Mitarbeitern möglich. Würde man den Betriebsrat individualisiert beteiligen wollen, wäre dies angesichts der Interessenlage problematisch: Mitarbeiter wollen diese besonderen Arten von Daten oftmals nicht preisgeben, auch nicht den Arbeitnehmervertretungen, was sich auch in der Rechtsprechung des BAG zur Frage der Mitteilung einer Schwangerschaft an den Betriebsrat zeigt.

Hinsichtlich des Umgangs mit Bewerberdaten geht der Antrag der LINKEN in folgenden Punkten über die heute den Interessen von Bewerbern und potenziellen Arbeitgebern ausgewogen Rechnung tragenden Rechtsprechungskasuistik hinaus: Zunächst einmal wird es für bestimmte Berufsgruppen immer ein berechtigtes Interesse eines Unternehmens geben, über die Informationen hinaus, die aus dem Bewerbungsbogen entnommen werden können, Daten zu erheben, insbesondere dann, wenn es sich um Berufsgruppen handelt, bei denen im öffentlichen Dienst die Vorlage eines Führungszeugnisses verlangt wird. Soll beispielsweise ein Feuerwehrmann in die Werksfeuerwehr eingestellt werden, dann darf dieser Bewerbungsvorgang nicht anders behandelt werden als der einer städtischen Feuerwehr. Auch können besondere Vertrauensstellungen die Erhebung zusätzlicher Informationen erforderlich machen, beispielsweise bei der geplanten Einstellung eines Personenschützers für die Geschäftsleitung des Unternehmens.

Die Forderung, Bewerbungsdaten unverzüglich nach Abschluss des Bewerbungsvorgangs zu löschen, steht im Widerspruch zur in einem Rechtsstreit erforderlichen Dokumentation nach dem AGG. Ferner sind nach der Rechtsprechung des Bundesarbeitsgerichts Fragen (und demgemäß die entsprechende Datenspeicherung) nach Straftaten und Ordnungswidrigkeiten, die nicht mehr in ein Führungszeugnis aufgenommen werden dürfen, zulässig, wenn sie für die Art des zu besetzenden Arbeitsplatzes von Bedeutung sind. Auch Fragen nach Vermögensverhältnissen sind für bestimmte Positionen im Unternehmen erlaubt. Die Frage nach dem Wehrdienst, der Schwangerschaft, der Partei- oder Religionszugehörigkeit sowie nach der Gewerkschaftszugehörigkeit sind auch jetzt schon nach der Rechtsprechung des Bundesarbeitsgerichts bei Bewerbern unzulässig, wobei letztere im laufenden Arbeitsverhältnis zulässig wäre, um eine korrekte Gehaltsabrechnung für den Fall unterschiedlicher Gehaltsbestandteile von Gewerkschaftsmitgliedern und Nichtmitgliedern sicherzustellen. Die

Frage nach Gesundheitsdaten ist in eingeschränktem Umfang zulässig, wobei das Bundesarbeitsgericht hier eine sehr ausgewogene Interessenabwägung vornimmt. Bei der seit vielen Jahren bewährten Rechtsprechung des Bundesarbeitsgerichts sollte es verbleiben. Auch ein zusätzlicher Schadensersatzanspruch über die im AGG enthaltenden Ansprüche hinaus würde keinen Mehrwert im Hinblick auf die Verbesserung des Datenschutzes bei Bewerbungen bringen.

Die in Ziffer IV. 1. enthaltenen Forderungen entsprechen im Wesentlichen bereits heute guter Unternehmenspraxis in Unternehmen, die den Datenschutz im Arbeitsverhältnis gesetzeskonform durchführen. Zuzustimmen ist insbesondere der in Ziffer IV. 2. b) enthaltenen Forderung, wonach die Erstellung von Leistungs- oder Verhaltensprofilen zur ständigen oder uneingeschränkten Überwachung der Beschäftigten unzulässig ist.

Bei der Nutzung von Telekommunikations- und Telemedieneinrichtungen ist der Antrag der LINKEN auf die Stärkung von Gewerkschafts- und Arbeitnehmervertretungsrechten gerichtet, nicht jedoch auf die Verbesserung des Datenschutzes. Die Regelungsmaterien sollten aber nicht vermischt werden. Auch hier hat die Rechtsprechung des Bundesarbeitsgerichts eine ausgewogene Interessenabwägung insbesondere hinsichtlich des Zugangs zu E-Mail- und Internet-Systemen von Unternehmen entwickelt. Zur Klarheit der Rechtslage würde allerdings tatsächlich beitragen, eine gesetzliche Regelung über Privatnutzung von dienstlichen Telemedieneinrichtungen zu treffen. Diese müsste dann aber mit der Möglichkeit entsprechender Kontrollmechanismen ausgestattet sein, um missbräuchliche Nutzung zu verhindern. Es kann nicht im Interesse der Beschäftigten sein, dass ihr diesbezügliches Nutzungsverhalten nur noch in dem in Ziffer IV. d) des Antrags vorgesehenen Umfang kontrolliert werden darf, denn in Zeiten des harten Wettbewerbs der Unternehmen und der Regionen wäre es fatal, wenn Internet und E-Mail-Systeme beispielsweise zur Weitergabe von Betriebs- und Geschäftsgeheimnissen, zur Begehung von Straftaten (z. B. Betrug oder auch Internet-Kinderpornografie) oder auch nur zu arbeitsvertragswidrigen Handlungen genutzt werden könnten. Dies muss, anders als in Ziffer IV. e) vorgesehen, mit Blick auf § 75 BetrVG auch für den Betriebsrat gelten. Selbstverständlich muss eine solche Kontrolle bestimmten Regeln unterliegen, die auch für den Mitarbeiter transparent sind und sie darf nicht unverhältnismäßig sein. Wenn also die Inhalte einer Stichprobenauswertung in einer Betriebsvereinbarung genau geregelt wären, ferner dort die Häufigkeit der Stichprobe beschrieben wäre und gleichzeitig, um die Verhältnismäßigkeit sicherzustellen, immer nur ein geringer im Voraus definierter Prozentsatz der Belegschaft einer solchen Kontrolle unterworfen würde und ggfls. zusätzlich die Mitarbeiter durch Unterschrift bestätigten, dass sie über die Art der Stichprobe und der sich daraus ergebenden Rechtsfolgen im Falle eines sich daraus ergebenden Verdachtes aufgeklärt wurden, dann dürfte den Interessen der Mitarbeiter schon damit ausreichend Rechnung getragen sein. Wenn zudem noch die Frage, ob einem sich aus einer Stichprobe ergebenden Verdacht nachgegangen wird oder nicht, in einer Kommission mit den Arbeitnehmervertretungen entschieden würde, dann ist kein Grund mehr ersichtlich, der aus Arbeitnehmerdatenschutzsicht gegen eine solche Stichprobe sprechen würde. Es wäre durchaus möglich, eine derartige gesetzliche Regelung zu schaffen, sie würde Rechtssicherheit für alle Beteiligten bringen.

Einem Arbeitgeber muss es ferner– unter Wahrung der Beteiligungsrechte des Betriebsrats - möglich bleiben, die überdurchschnittliche Leistung oder die Minderleistung eines Mitarbeiters auch dann noch zu beurteilen, wenn dieser seine Arbeit elektronisch verrichtet, zumal moderne Entgeltsysteme in der Regel leistungsorientiert ausgestaltet sind. Surft beispielsweise ein Mitarbeiter regelmäßig einen Großteil seiner Arbeitszeit im Internet, dann muss dieser Nachweis auch bei in angemessenem Umfang erlaubter Privatnutzung möglich sein.

Die Überwachung mittels optoelektronischer Geräte in Unternehmen kann, wie bereits in den Ausführungen zu § 32 BDSG deutlich gemacht, insbesondre im Sinne von Arbeitssicherheit sinnvoll sein und dem hohen Gut des Gesundheitsschutzes der Mitarbeiter dienen. Eine zu starke Einschränkung trägt hier der Interessen der Beschäftigten nicht Rechnung, vielmehr ist eine genauere Interessenabwägung erforderlich.

Die in den Abschnitten V. und VI. enthaltenen Regelungsvorschläge zum betrieblichen Datenschutzbeauftragten und zu Betriebs- und Personalräten sind wieder gekennzeichnet von der Ausweitung von Rechten, die insbesondere bei Ziffern VI. b) und c) jedoch weiterhin den bereits genannten Einschränkungen des Betriebsverfassungsgesetzes und der entsprechenden Rechtsprechung unterliegen sollten, um den Mitarbeitern nicht die Entscheidung darüber zu entziehen, welche Daten sie einer Arbeitnehmervertretung preisgeben wollen und welche nicht.

Die in Ziffer VIII. vorgeschlagene Regelung zur Einrichtung einer Schiedsstelle schafft derzeit noch nicht absehbare Folgen und wird auch nicht im Sinne der Aufsichtsbehörden sein.

Angesichts der jüngsten Datenschutzverstöße in verschiedenen Unternehmen ist es durchaus verständlich, die Rechtsfolgenseite solcher Verstöße abweichend von §§ 7, 43, 44 BDSG heutiger Fassung regeln zu wollen, weil diese – von § 7 BDSG abgesehen - aus der hoheitlichen Sicht des Datenschutzes herrühren. Eine dem AGG nachgebildete Schadensersatz- und Entschädigungspflicht verbunden mit der Umkehr der Beweislast ist jedoch nicht das probate Mittel: Würde der Antrag der LINKEN in der vorgeschlagenen Form Gesetz, würde dieser wie aufgezeigt zu erheblichen, jetzt schon zum Teil konkret vorherzusagenden Rechtsunsicherheiten führen und somit ein unverhältnismäßiges Risiko für alle Beteiligten begründen.

III. Stellungnahme zum Antrag der GRÜNEN

Die Stellungnahme bezieht sich im Folgenden nur noch auf die vom Antrag der LINKEN abweichenden wesentlichen Regelungsvorschläge.

Hinsichtlich der in Ziffer I. vorgeschlagenen Regelung der Erlaubnistatbestände für die Datenverarbeitung wird auf die Ausführungen zu § 32 BDSG verwiesen. Ohne

die heute geltenden Erlaubnistatbestände wird der Datenschutz im Arbeitsverhältnis mit Unsicherheiten versehen, die kein Arbeitgeber mehr beherrschen kann.

Die Berücksichtigung des AGG in Ziffer II 1. a) des Antrags ist positiv. Ebenso bringt der Regelungsvorschlag Klarheit, Bewerberpools nur auf der Grundlage freiwilliger schriftlicher Einwilligungserklärungen zu bilden. Ebenso zu befürworten ist, dass die Unternehmen im Falle der Verwendung von Online-Bewerbungsverfahren für einen sicheren Datentransport sorgen müssen.

Positiv hervorzuheben ist auch, dass der Antrag der GRÜNEN berücksichtigt, dass es auch einen Datenaustausch zwischen Arbeitgebern und auch mit datenverarbeitenden Stellen im Ausland geben kann. Allerdings ist, wie in den Ausführungen zu § 32 BDSG dargelegt, die Einholung einer individuellen Einwilligung für jeden datenverarbeitenden Vorgang unpraktikabel und auch im Interesse der Mitarbeiter nicht wünschenswert.

Mit den Ziffern 2 e) und g) werden zahlreiche Rechtsstreitigkeiten darüber erwachsen, ob eine Datenverarbeitung unrechtmäßig erfolgt ist oder nicht. Insbesondere das Widerspruchsrecht des Betriebsrats, das weit über seine sonstigen Regelungskompetenzen des Betriebsverfassungsgesetzes hinausgeht und dessen Systematik zuwiderläuft, würde, wenn es von den Betriebsräten missbräuchlich eingesetzt würde, zur kompletten Blokkade von personalwirtschaftlichen Vorgängen führen können. Richtig ist hingegen, dass den Mitarbeitern aus der Geltendmachung von Rechten aus dem BDSG keine Nachteile erwachsen dürfen. Etwas problematisch erscheint hingegen wieder die Regelung in Ziffer 2 h), wonach der Arbeitnehmer bei Verstößen gegen Informations- und Auskunftspflichten die Löschung seiner Daten verlangen können soll. Zum einen wird das Interesse des Mitarbeiters nicht in der Löschung, sondern an der Berichtigung von gespeicherten Daten bestehen, zum anderen ist ein unmittelbarer Zusammenhang zwischen Verletzung von Auskunftspflichten und Datenlöschung nicht zu erkennen.

Warum gemäß Ziffer 3 b) des Antrags die Sozialkompetenz eines Bewerbers nicht gemessen werden soll, ist völlig unverständlich. Gerade diese Kompetenzen sind es doch, die die Zusammenarbeit im Betrieb prägen. Hat jemand hervorragende Fachkenntnisse, ist aber beispielsweise nicht geeignet, in einem Team zu arbeiten, dann werden sich für seine Kollegen und Mitarbeiter während des gesamten Arbeitslebens Schwierigkeiten ergeben. Erkennt man das - noch dazu anhand standardisierter, nachvollziehbarer Kriterien - schon bei der Bewerbung, sollte man die Möglichkeit haben, dies bei der Einstellungsentscheidung zu berücksichtigen. Gleiches gilt auch für regelmäßige Beurteilungen im laufenden Arbeitsverhältnis, wie sie in Ziffer 3 d) angesprochen sind, insbesondere wenn es um die Beurteilung von Mitarbeitern mit Führungsaufgaben geht.

Nach Ziffer 4 des Antrags soll die Überwachung mit optischen und elektronischen Geräten geregelt werden. Dies würde Rechtssicherheit im Verhältnis zum heutigen Zustand bringen, allerdings sind, wie oben bei § 32 BDSG ausgeführt, die beschriebenen Zweckbestimmungen zu kurz gegriffen - Eigentumsschutz und Hausrecht reichen an dieser Stelle nicht aus. Über eines dürfte aber Einigkeit zwischen allen Parteien und Fachexperten bestehen: diese Geräte dürfen, so wie es der Antrag auch formuliert, nicht für eine allgemeine Kontrolle der Beschäftigten missbraucht werden.

Ziffer 5 des Antrags schränkt die Kontrollmöglichkeiten bei der Nutzung von Internet und E-Mail-Systemen in einer Art und Weise ein, die, wie ausgeführt, eine echte Gefahr für jedes Unternehmen und damit auch für seine Mitarbeiter darstellen kann. Über die genannten Medien lassen sich viele Arten von Vertragsverletzungen und auch Straftaten begehen, da muss es dem Arbeitgeber möglich sein, auch ohne konkreten Verdacht eine Nutzungskontrolle vorzunehmen. Diese muss, wie ausgeführt, bestimmten Regeln unterliegen, die auch für den Mitarbeiter transparent sind und sie darf nicht unverhältnismäßig sein.

In den Ziffern 6 d) und g) werden die Beteiligungsrechte der Arbeitnehmervertretungen ausgeweitet. Hierzu sei auf die Ausführungen zum Antrag der LINKEN verwiesen. Im Übrigen werden die vorgeschlagenen Regelungen in Ziffer 6 heute schon in vielen Unternehmen so gelebt.

IV. Stellungnahme zum Antrag der GRÜNEN - Rechte der Beschäftigten bei Discountern verbessern

Vorab sei bemerkt, dass die im Antrag enthaltenen Regelungsvorschläge anders als der Titel des Antrags es erwarten lässt, nicht auf die Rechte von Mitarbeitern bei Discountern zielen, sondern es im Kern schlicht um eine Neuregelung der gesetzlichen Bestimmungen über Betriebsratswahlen geht.

Die gesonderte Bekanntmachung des Sonderkündigungsschutzes für Wahlvorstände etc. ist überflüssig, denn neben den klassisch aushangpflichtigen Arbeitsschutzgesetzen werden die Mitarbeiter häufig auch in mitbestimmungsrechtlich relevanten Fragen geschult.

Eine Entfristung von befristeten Verträgen zum Zwecke der Begleitung und Durchführung einer Betriebsratswahl ist mit Blick auf das TzBfG schlicht systemwidrig.

Die in Ziffer 3 beschriebenen datenschutzbezogenen Bestimmungen sind nicht spezifiziert genug. Insoweit wird auf die Ausführungen oben verwiesen.

06.05.2009

DEUTSCHER BUNDESTAG
Ausschuss für
Arbeit und Soziales
16. Wahlperiode

Ausschussdrucksache 16(11)**1364**

6. Mai 2009

Stellungnahme

zur öffentlichen Anhörung von Sachverständigen am 11. Mai 2009 in Berlin zum

a) Antrag der Abgeordneten Brigitte Pothmer, Dr. Thea Dückert, Kerstin Andreae, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Rechte der Beschäftigten von Discountern verbessern - Drucksache 16/9101 -

b) Antrag der Abgeordneten Silke Stokar von Neuforn, Kerstin Andreae, Volker Beck (Köln), weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Persönlichkeitsrechte abhängig Beschäftigter sichern - Datenschutz am Arbeitsplatz stärken - Drucksache 16/9311 -

c) Antrag der Abgeordneten Jan Korte, Wolfgang Neskovic, Sevim Dagdelen, weiterer Abgeordneter und der Fraktion DIE LINKE.

Datenschutz für Beschäftigte stärken - Drucksache 16/11376 -

d) Antrag der Abgeordneten Gisela Piltz, Dr. Heinrich L. Kolb, Jens Ackermann, weiterer Abgeordneter und der Fraktion der FDP

Schutz von Arbeitnehmerdaten durch transparente und praxisgerechte Regelungen gesetzlich absichern - Drucksache 16/12670 -

Andreas Jaspers, Bonn

I. Ausgangssituation

Der Schutz von Arbeitnehmerdaten ist in Deutschland nicht ungeregelt. Neben den bereichsspezifischen gesetzlichen Regelungen findet das Bundesdatenschutzgesetz auch auf die Verwendung von Arbeitnehmerdaten Anwendung. Zudem ist der Arbeitnehmerdatenschutz auch durch betriebliche Regelungen, insbesondere durch Betriebsvereinbarungen, geregelt. Weiterhin hat die Rechtsprechung das Persönlichkeitsrecht im Arbeitsverhältnis konkretisiert.

Gegenstand einer Kodifizierung des Arbeitnehmerdatenschutzes sind zunächst die bestehenden materiellen Regelungslücken. Weiterhin ist der Einsatz der modernen Informations- und Kommunikationstechnik im Arbeitsverhältnis mit Blick auf die Gewährleistung des Persönlichkeitsrechts von Arbeitnehmern zukunftsweisend datenschutzkonform auszugestalten.

II. Evidente Regelungslücken

1. Weitergabe von Mitarbeiterdaten im Unternehmensverbund

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

2. Datenschutzkontrolle beim Betriebsrat

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

3. Stärkung der Rechtsstellung des betrieblichen Datenschutzbeauftragten

Der unzulässigen Verwendung von Mitarbeiterdaten kann dadurch wirksam begegnet werden, dass die interne Kontrollinstanz der Unternehmen eine rechtliche und unternehmenspolitische Stärkung erhält. Die innerbetriebliche Selbstkontrolle in den Unternehmen wird vom betrieblichen Datenschutzbeauftragten wahrgenommen, den bereits Unternehmen zu bestellen haben, die zehn oder mehr Mitarbeiter mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Insbesondere bedarf es einer Effektivierung der präventiven Arbeit des Datenschutzbeauftragten.

Naturgemäß können die Datenschutzbeauftragten ihrem gesetzlichen Auftrag zur Hinwirkung auf die Einhaltung der Datenschutzvorschriften nicht gerecht werden, wenn sie über die Datenverarbeitungen nicht rechtzeitig informiert werden. Insofern ist auf die bestehende Gesetzeslage hinzuweisen, wonach der Datenschutzbeauftragte über Vorhaben der automatisierten Verarbeitung rechtzeitig zu unterrichten ist, damit er die ordnungsgemäße Anwendung von Datenverarbeitungsprogrammen überwachen kann. In Ergänzung zur Überwachung der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen zählt die gesetzlich vorgeschriebene Vorabkontrolle im Fall von besonders risikobehafteten Datenverarbeitungen zu den Aufgaben des Datenschutzbeauftragten. Eine Pflicht zur Vorabkontrolle besteht derzeit insbesondere in Fällen der Verarbeitung sensitiver Daten bzw. im Rahmen der Erstellung von Persönlichkeitsbewertungen. Die aktuellen Datenschutzskandale geben Anlass dazu, explizit alle Überwachungssysteme und -maßnahmen generell der Vorabkontrolle mit entsprechender schriftlicher Freigabeerklärung durch die Datenschutzbeauftragten zu unterziehen.

Umstritten ist, ob eine gesetzeswidrig unterbliebene Vorabkontrolle überhaupt spürbare Rechtsfolgen nach sich zieht. Es sollte gesetzlich klargestellt werden, dass ein Übergehen des Datenschutzbeauftragten sanktioniert wird. Dies hätte zur Folge, dass Verarbeitungen, die ohne das notwendige Vorabkontrollverfahren durchgeführt werden, als Ordnungswidrigkeiten oder Straftaten verfolgt werden könnten. Durch eine solche Aufwertung der Kompetenzen des Datenschutzbeauftragten würde auch dessen Verantwortung im Unternehmen steigen. Deshalb ist im Interesse der Gewährleistung einer unabhängigen Überprüfung der Zulässigkeit der Verarbeitung und Weitergabe personenbezogener Daten auch die Rechtsstellung des Datenschutzbeauftragten im Unternehmen zu stärken.

Seiner unabhängigen Kontrollaufgabe kann der Datenschutzbeauftragte nur dann nachkommen, wenn der Bestand seines Arbeits- oder Dienstverhältnisses vom Ergebnis der Überprüfung nicht berührt wird. Insoweit ist ein Sonderkündigungsschutz für den betrieblichen Datenschutzbeauftragten notwendig. Hierzu gibt es bereits einen Gesetzentwurf der Bundesregierung (BT-Drucks. 16/12011). Zugleich erfordert eine Erweiterung des Aufgaben- und Kompetenzbereichs des Datenschutzbeauftragten eine Ausweitung seiner zeitlichen und wirtschaftlichen Ressourcen für diese Tätigkeit. Es ist davon auszugehen, dass durch eine entsprechende Stärkung des Datenschutzbeauftragten Skandale, sofern diese nicht einen kriminellen Hintergrund haben, vermieden werden können und damit das Grundrecht auf informationelle Selbstbestimmung der Mitarbeiter erheblich gestärkt werden kann.

III. Gesetzliche Konkretisierungen

Das bestehende Datenschutzrecht ist weitgehend technikneutral. Der Einsatz moderner Informations- und Kommunikationstechniken im Arbeitsverhältnis ist bisher auf Grundlage unbestimmter Rechtsbegriffe und Interessenabwägungen zu entscheiden. Angesichts der rasanten Technikentwicklung ist dieser gesetzgeberische Ansatz auch weiterhin zu verfolgen.

Unabhängig hiervon kann es in einzelnen Zweifelsfällen angezeigt sein, gesetzgeberische Zielvorgaben für die Beurteilung der Zulässigkeit des Einsatzes der modernen Techniken im Arbeitsverhältnis aufzustellen.

1. Medizinische Untersuchungen

Medizinische Untersuchungen sollten nur zulässig sein, wenn sie mit Blick auf die auszuübende Tätigkeit zwingend notwendig sind. Dies ist insbesondere bei gefahrgeneigter Arbeit der Fall. Gentests sind mit Ausnahme der im Gendiagnostikgesetz geregelten Ausnahmetatbestände im Arbeitsverhältnis regelmäßig unzulässig.

2. Nutzung biometrischer Daten

Biometrische Daten im Arbeitsverhältnis dürfen grundsätzlich nur der Identitätskontrolle dienen. Der allgemeine datenschutzrechtliche Grundsatz der Datenvermeidung und der Datensparsamkeit gebietet es, dass biometrische Daten unter der alleinigen Kontrolle des Betroffenen stehen und ausschließlich zum Vergleich verarbeitet werden dürfen. Die Nutzung bedarf der Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten, deren gesetzlicher Anwendungsbereich insoweit auszuweiten ist.

3. Überwachungssysteme

Überwachungssysteme wie der Einsatz der Videotechnik oder andere Systeme mit vergleichbarer Eingriffsmöglichkeit in die informationelle Selbstbestimmung wie RFID oder GPS dürfen grundsätzlich nicht zu Zwecken Leistungskontrolle und Leistungsbemessung eingesetzt werden. Dies gilt insbesondere für Verfahren des Data Mining zum Zwecke der Mitarbeiterkontrolle und der Erstellung von Persönlichkeitsprofilen. Der gesetzliche Anwendungsbereich der Regelung zur Videoüberwachung in § 6b BDSG sollte nicht wie bisher auf „öffentlich zugängliche Räume“ beschränkt bleiben. Vielmehr ist die Vorschrift mit ihren Zulässigkeits- und Transparenzregeln auf den Einsatz der Videotechnik insgesamt zu erstrecken. Der Einsatz von Systemen, die eine Mitarbeiterüberwachung ermöglichen, sind generell der gesetzlichen Vorabkontrolle durch den Datenschutzbeauftragten zu unterwerfen.

4. Screening von Mitarbeitern

Das Screening von Mitarbeitern zum Zwecke der Prüfung von Compliance-Anforderungen darf nur unter Beachtung der Grundsätze der Verhältnismäßigkeit und der Datensparsamkeit durchgeführt werden. Für legitime Kontrollzwecke ist insbesondere vom Einsatz von Verfahren der Pseudonymisierung Gebrauch zu machen. Die Kontrollfrequenz und der betroffene Personenkreis bedarf der Begrenzung nach Erforderlichkeitsgesichtspunk-

ten. Auch hier empfiehlt sich eine generelle Vorabkontrollpflicht.

5. Nutzung der Informations- und Kommunikationstechnik am Arbeitsplatz

Der Einsatz und die Kontrolle der Informations- und Kommunikationstechnik am Arbeitsplatz, insbesondere die Nutzung von Telefon, E-Mail und Internet, ist im Wege der Selbstregulierung, ggf. durch Betriebsvereinbarungen, gestaltbar. Dabei muss es dem Arbeitgeber möglich bleiben, wahlweise die Privatnutzung der IuK-Technik zu verbieten oder eine eingeschränkte Nutzung für private Zwecke durch den Arbeitnehmer zu erlauben. Hier haben sich bereits verschiedene Vorgehensweisen etabliert, die den jeweiligen betrieblichen Bedürfnissen Rechnung tragen. Nur für den ungeregelten Zustand verbleibt hinsichtlich der Reichweite des Fernmeldegeheimnisses mit Blick auf die Privatnutzung eine Rechtsunsicherheit bezüglich der Kontrollmöglichkeiten für legitime Zwecke durch den Arbeitgeber. Hier kann durch den Gesetzgeber klargestellt werden, dass auch bei Zulassung der Privatnutzung der Informations- und Kommunikationstechnik am Arbeitsplatz eine Kontrolle zur Aufdeckung von Straftaten und Missbrauch zulässig ist.

IV. Regelung des Arbeitnehmerdatenschutzes

Dass es wegen vorbezeichneter Gesetzeslücken und Empfehlungen für eine gesetzliche Konkretisierung des Arbeitnehmerdatenschutzes zwangsläufig eines eigenständigen Arbeitnehmerdatenschutzgesetzes bedarf, ist nicht zwingend. Hier kämen alternativ auch Regelungen im Bundesdatenschutzgesetz oder im Betriebsverfassungsgesetz in Betracht. Der Gesetzgeber sollte darauf achten, das Datenschutzrecht nicht durch neue bereichsspezifische Gesetze weiter zu zersplittern. Vielmehr sollte das Bundesdatenschutzgesetz als zentrales Gesetz, das die wesentlichen Datenschutzthemen regelt, auch die Grundlagen des Arbeitnehmerdatenschutz beinhalten. Die umfassende Geltung des Gesetzes bei der Verarbeitung von Personaldaten kann dadurch erreicht werden dass sein Anwendungsbereich sich hier nicht auf automatisierte oder dateigebundene Verarbeitungen beschränkt. Dadurch würden eine Reihe von ansonsten in einem Arbeitnehmerdatenschutzgesetz erforderliche Doppelregelungen vermieden.

Bonn, den 4. Mai 2009

DEUTSCHER BUNDESTAG
Ausschuss für
Arbeit und Soziales
16. Wahlperiode

Ausschussdrucksache 16(11)**1368**

7. Mai 2009

Stellungnahme

zur öffentlichen Anhörung von Sachverständigen am 11. Mai 2009 in Berlin zum

a) Antrag der Abgeordneten Brigitte Pothmer, Dr. Thea Dückert, Kerstin Andreae, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Rechte der Beschäftigten von Discountern verbessern - Drucksache 16/9101 -

b) Antrag der Abgeordneten Silke Stokar von Neuforn, Kerstin Andreae, Volker Beck (Köln), weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Persönlichkeitsrechte abhängig Beschäftigter sichern - Datenschutz am Arbeitsplatz stärken - Drucksache 16/9311 -

c) Antrag der Abgeordneten Jan Korte, Wolfgang Neskovic, Sevim Dagdelen, weiterer Abgeordneter und der Fraktion DIE LINKE.

Datenschutz für Beschäftigte stärken - Drucksache 16/11376 -

d) Antrag der Abgeordneten Gisela Piltz, Dr. Heinrich L. Kolb, Jens Ackermann, weiterer Abgeordneter und der Fraktion der FDP

Schutz von Arbeitnehmerdaten durch transparente und praxisgerechte Regelungen gesetzlich absichern - Drucksache 16/12670 -

Dr. Thomas Petri, Berlin

Vorbemerkung

Die Notwendigkeit eines speziellen Bundesgesetzes für den Datenschutz von Beschäftigten ist offenkundiger denn je. Dies haben nicht erst die skandalösen Vorkommnisse beim Discounter Lidl und anderen Unternehmen deutlich gemacht. Das Bundesdatenschutzgesetz mit seinen generalklauselartigen Befugnisnormen und der alternativen Rechtfertigung einer Verarbeitung personenbezogener Daten durch die Einwilligung Betroffener ist kein ausreichender Rechtsrahmen für die Verarbeitung der Daten abhängig Beschäftigter. Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb seit Jahrzehnten wiederholt, zuletzt bei ihrer 77. Konferenz am 26./27. März 2009, ein Gesetz zum Beschäftigtendatenschutz gefordert. Die in dieser jüngsten Entschließung enthaltenen unverzichtbaren Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz (im Folgenden fett) bilden die Grundlage dieser Stellungnahme.

Alle drei Anträge, die Gegenstand der Anhörung sind, enthalten zahlreiche positive und begrüßenswerte Ansätze für ein umfassendes Beschäftigtendatenschutzgesetz. In einzelnen Punkten empfiehlt sich allerdings eine stärkere Differenzierung. Teilweise entsprechen die Anträge auch bereits dem geltenden Recht.

1. **Die Regelungen des Beschäftigtendatenschutzgesetzes müssen sowohl für die Beschäftigten der Privatwirtschaft als auch für Beschäftigten im öffentlichen Dienst gelten** (vgl. auch Ziff. I b des Antrags DIE LINKE). Es müsste die für das Beamtenrecht des Bundes und der Länder bereits geltenden Regeln zum Umgang mit Personalaktendaten aufgreifen und dürfte den dort erreichten Schutzstandard nicht unterschreiten.

2. **Es muss klar geregelt werden, welche Daten Unternehmen und öffentliche Stellen im Rahmen des Einstellungsverfahrens und im weiteren Verlauf des Arbeitslebens über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Es bedarf besonderer Festlegungen im Hinblick auf Gesundheitsdaten (u.a. zur Frage der Zulässigkeit von Drogen-Screening, psychologischen Testverfahren, ärztlichen Untersuchungen, etc.).**

   Dabei schließt der Begriff des personenbezogenen Datums schon nach dem Bundesdatenschutzgesetz personenbeziehbare Daten (also Daten über eine bestimmbare natürliche Person) mit ein (§ 3 Abs. 1 BDSG). Einer ausdrücklichen Erweiterung dieses

Begriffs auf personenbeziehbare Daten für Zwecke des Arbeitnehmerdatenschutzes, wie sie der Antrag der LINKEN vorsieht (Ziff. I a), bedarf es deshalb nicht. Erwägenswert ist allerdings eine Erstreckung des gesetzlichen Schutzes auf Daten, die sich auf Gruppen von Beschäftigten beziehen. Vergleichbare Vorschläge zum Schutz vor informationeller Diskriminierung ganzer Personengruppen werden auch außerhalb des Beschäftigtendatenschutzes im Rahmen der Modernisierung des allgemeinen Datenschutzrechts diskutiert. Im Bereich des Beschäftigtendatenschutzes ist insbesondere an den Schutz von Gewerkschaftsmitgliedern oder Angehörigen bestimmter ethnischer Gruppierungen zu denken. Teilweise wird dieser Schutzbedarf auf verfassungsrechtlicher Ebene durch die Grundrechte nach Art. 3 Abs.3 und 9 Grundgesetz gedeckt, was allerdings der einfachgesetzlichen Konkretisierung bedürfte.

Bereits vor Abschluss eines Arbeitsvertrages muss der Schutz der Daten von Bewerberinnen und Bewerbern sichergestellt werden. Das Fragerecht des Arbeitgebers ist auf die Fragen zu beschränken, die für das jeweilige Beschäftigungsverhältnis unabdingbar sind. Das gilt auch für Fragen nach dem Gesundheitszustand bzw. nach Behinderungen (vgl. Ziff. II 1 a-c Antrag Bündnis 90/DIE GRÜNEN, 16/9311). Über diesen Antrag hinaus sollten allerdings Fragen nach einer vorhandenen oder geplanten Schwangerschaft stets unzulässig sein und den Bewerberinnen auch gesetzlich das in der Rechtsprechung des Bundesarbeitsgerichts anerkannte Recht zugestanden werden, solche Fragen wahrheitswidrig zu verneinen (Recht zur Lüge). Denn die Ablehnung der Beantwortung solcher Fragen führt in aller Regel dazu, dass die Bewerbung erfolglos bleibt.

Die von der Fraktion Bündnis 90/DIE GRÜNEN erhobene Forderung, dass Daten aus psychologischen Untersuchungen im Einstellungsverfahren nur unter engen Voraussetzungen erhoben und verwertet werden dürfen (16/9311, Ziff. II 3 b), ist zu unterstützen. Das gilt auch für Begrenzung der Messung des Sozialverhaltens auf Führungspositionen. Die in diesem Antrag zusätzlich genannte Einschränkung, dass medizinische oder psychologische Tests ohne Zustimmung des Betroffenen unzulässig sind, ist insofern sinnvoll, als derartige Tests nur offen und nach entsprechender Information des Betroffenen durchgeführt werden dürfen. Wenn dieser seine Zustimmung verweigert, müsste geregelt werden, welche Konsequenzen dies für ihn hat. Nur wenn der Test für die jeweilige Tätigkeit erforderlich ist, würde der Betroffene aus dem Bewerberkreis ausscheiden (und dies müsste ihm auch vorab verdeutlicht werden).

Die von der Fraktion DIE LINKE vorgeschlagene Ergänzung des Bundesdatenschutzgesetzes, wonach Daten über die physische oder psychische Konstitution von Bewerberinnen, Bewerbern und Beschäftigten den besonderen Datenarten nach § 3 Abs. 9 gleichgestellt werden sollten (Ziff. II b, 16/11376), ist zu begrüßen, weil dadurch der Begriff der Gesundheitsdaten präzisiert würde. Allerdings würde die ersatzlose Streichung des Merkmals „rassische Herkunft“ gegen die EG-Datenschutzrichtlinie verstoßen, die in Art. 8 Abs. 1 dieses Merkmal ausdrücklich als besonders schutzwürdig bezeichnet. Deshalb ist eine Regelung im Bundesdatenschutzgesetz vorzuziehen, die entsprechend dem § 6a Abs. 1 des Berliner Datenschutzgesetzes auf Art. 8 Abs. 1 der EG-Datenschutzrichtlinie verweist.

Auch erscheint die Forderung der Fraktion DIE LINKE, dass die Erhebung und Verarbeitung von Nutzungsdaten nur durch Personen erfolgen darf, die der ärztlichen Schweigepflicht unterliegen (Ziff. II b), als zu weitgehend, weil darüber hinaus Beschäftigte von Personalstellen oder Personalakten führenden Stellen mit zulässigerweise erhobenen Gesundheitsdaten umgehen müssen.

Zu unterstützen ist dagegen das von der Fraktion DIE LINKE vorgeschlagene Verbot der Durchführung von graphologischen Tests (Ziff. III c), weil die Aussagefähigkeit dieser Methode wissenschaftlich nicht gesichert ist.

Ein regelungsbedürftiger Bereich ist auch die Schnittstelle zwischen dem Beschäftigtendatenschutz und dem Allgemeinen Gleichbehandlungsgesetz (AGG). Zu Recht wird im Antrag der Fraktion Bündnis 90/DIE GRÜNEN insoweit gefordert, dass Daten von Bewerberinnen und Bewerbern nach Abschluss des Auswahlverfahrens erst nach Ablauf der Fristen unverzüglich zu löschen sind, innerhalb derer Klagen gegen die Auswahlentscheidung nach dem AGG zulässig sind (Ziff. II 1 a, 16/9311). Demgegenüber geht der Antrag der Fraktion DIE LINKE zu weit, wenn in ihm die unverzügliche Löschung und Rückgabe von Bewerbungsdaten einschließlich der Tatsache der Bewerbung gefordert wird, wenn die Bewerbung erfolglos war (Ziff. III d, 16/11376). In jedem Fall wird man dem Arbeitgeber bzw. der Arbeitgeberin die Speicherung der Tatsache einer (gescheiterten) Bewerbung zu Dokumentationszwecken für eine klar bestimmte Frist gestatten müssen. Die Bewerbungsunterlagen sind in jedem Fall zurückzugeben, es sei denn der Bewerber oder die Bewerberin ist damit einverstanden, dass sie bei dem Unternehmen oder der Verwaltungsbehörde weiter (für künftige Stellenbesetzungen) vorgehalten werden.

3. **Einen umfassenden anlass- und verdachtslosen Datenabgleich darf es nicht geben. Der Zugriff von Kontrollinstanzen wie z.B. der Innenrevision auf erhobene Personaldaten bedarf enger gesetzlicher Vorgaben.**

   Zunehmend überprüfen große Unternehmen, aber auch Behörden ihre Beschäftigten pauschal und ohne konkrete Verdachtsmomente, um Anhaltspunkte für Straftaten wie Korruption oder Geheimnisverrat zu erhalten. Derartige Rasterungen zur Verdachtsgewinnung sind bereits nach geltendem Recht unzulässig. Ein Beschäftigtendatenschutzgesetz sollte dies aber eindeutig klarstellen und zugleich den Zugriff von Kontrollinstanzen wie z.B. der Innenrevision begrenzen. Bei konkreten Verdachtsmomenten für Straftaten sind die Strafverfolgungsbehörden einzuschalten.

4. **Moderne Informations- und Kommunikationstechnologien dürfen nicht zu lückenlosen Verhaltens- und Leistungskontrollen eingesetzt werden. Da die Nutzung von Telefon, Internet und E-Mail-Diensten nicht mehr aus dem Arbeitsleben wegzudenken ist, sind auch die Voraussetzungen für eine beschäftigtenbezogene Auswertung dieser Kom-**

munikationsmittel eindeutig und restriktiv festzulegen. Dabei ist auch zu regeln, welcher Personenkreis solche Auswertungen durchführen darf und ab welchem Verfahrensstand Dritte (z.B. Mitarbeitervertretungen und Datenschutzbeauftragte) hinzugezogen werden müssen. Auswertungen von Datenbeständen der Zugangs- und Personalinformationssysteme sind strikt zu begrenzen.

Auch wenn in den meisten jüngst bekannt gewordenen Fällen, in denen die Kommunikation der Beschäftigten heimlich überwacht worden ist (z.B. bei der Deutschen Telekom), zweifelsfrei gegen geltendes Recht verstoßen wurde und möglicherweise auch Straftatbestände verwirklicht worden sind, herrscht in diesem Bereich noch immer eine erhebliche Rechtsunsicherheit, die gerade im Interesse der Beschäftigten, aber auch der Unternehmen und Verwaltungsbehörden durch den Gesetzgeber beendet werden muss. Dabei ist der Schutz des Fernmeldegeheimnisses stets dann zu gewährleisten, wenn der Arbeitgeber die private Nutzung von dienstlich überlassenen Kommunikationsmitteln ausdrücklich zulässt oder duldet. In diesen Fällen dürfen Eingriffe in das Telekommunikationsgeheimnis nur in eng begrenzten Ausnahmefällen (insofern etwas zu unbestimmt der Antrag der Fraktion DIE LINKE, Ziff. IV 4 b, 16/11376) und nur mit Zustimmung des betrieblichen oder behördlichen Datenschutzbeauftragten sowie des Betriebs- bzw. Personalrats vorgenommen werden. Der Gesetzgeber sollte in Fällen, in denen der Verdacht einer strafbaren Handlung besteht, die zeitnahe Einschaltung der Strafverfolgungsbehörden vorschreiben.

Selbst wenn die private Nutzung ausdrücklich untersagt ist, muss eine Nutzung und Auswertung von Protokolldateien oder anderen Metainformationen, die bei der Nutzung solcher Kommunikationsmittel entstehen, zur Leistungs- und Verhaltenskontrolle der Beschäftigten gesetzlich untersagt werden. Die entsprechenden Vorschläge der Fraktion Bündnis 90/DIE GRÜNEN (Ziff. II 5, 16/9311) und DIE LINKE (Ziff. IV 4 d, 16/11376) sind deshalb zu unterstützen. Der Arbeitgeber kann allerdings Daten über berufliche bzw. dienstliche Kommunikationsvorgänge herausverlangen oder die Beschäftigten dazu auffordern, sie im gebotenen Umfang aktenkundig zu machen (vgl. Ziff. IV 4 c, 16/11376). Auch ist der Vorschlag zu unterstützen, dass die Kommunikation mit den betrieblichen oder behördlichen Datenschutzbeauftragten und den Betriebs- und Personalräten überwachungsfrei möglich sein müssen (Ziff. IV 4 e, ebda.).

Ergänzend sei auf die Orientierungshilfe des Arbeitskreises Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz verwiesen:

http://www.datenschutz.mvnet.de/dschutz/informat/nutzuint/nutzuint.pdf

5. **Der Einsatz von Überwachungssystemen, wie z.B. Videokameras und Ortungssystemen, ist auf das unbedingt notwendige Maß zu beschränken und nur unter Wahrung der Beteiligungsrechte der Mitarbeitervertretungen zulässig. Die Verwendung biometrischer Verfahren bedarf besonders enger Vorgaben.**

Den Fraktionen Bündnis 90/DIE GRÜNEN und DIE LINKE ist zuzustimmen, wenn sie einen umfassenden gesetzlichen Schutz der Beschäftigten vor der Überwachung durch optische und elektronische Geräte fordern (Ziff. II 4, 16/9311, und Ziff. IV 5, 16/11376). Die Rechtsprechung des Bundesarbeitsgerichts ist insoweit uneinheitlich (Ziff. I, 16/9311). Angesichts der bekannt gewordenen Fälle, in denen – offenkundig rechtswidrig – Beschäftigte auch in Umkleide- oder Pausenräumen mit Videotechnik überwacht worden sind, muss der Gesetzgeber klare Grenzen ziehen und deren Überschreitung auch mit empfindlichen Sanktionen belegen.

Allerdings ist eine heimliche Videoüberwachung einzelner Beschäftigter in eng begrenzten Ausnahmefällen dann zuzulassen, wenn der konkrete Verdacht einer strafbaren Handlung besteht (Ziff. II 4 d, 16/9311). Auch die Fraktion DIE LINKE will die Übermittlung von Daten aus einer optischen oder elektronischen Überwachung an die Strafverfolgungsbehörden zulassen, wenn dies der Aufklärung von Straftaten dient (Ziff. IV 5 e; insoweit besteht ein gewisser Gegensatz zu Ziff. IV 5 a).

Die im Antrag der Fraktion DIE LINKE vorgesehene Einschränkung für die Erhebung und Verarbeitung von biometrischen Daten (Ziff. II c) geht zwar in die richtige Richtung, ist aber nicht präzise genug. Denn nicht überall dort, wo Autorisierungs- und Authentifizierungszwecke vorliegen, sollten auch biometrische Daten erhoben und verarbeitet werden dürfen. Das sollte nur in solchen Bereichen zugelassen werden, in denen eine derart zuverlässige Form der Autorisierung oder Authentifizierung auch verhältnismäßig und geboten erscheint.

6. **Es bedarf der Festlegung der Rechte der Beschäftigten, z.B. im Hinblick auf Auskunfts-, Einsichts-, Widerrufs-, Berichtigungs-, Löschungs- und Schadensersatzansprüche.**

Die Beschäftigtenrechte sind angesichts der besonderen Abhängigkeit vom Arbeitsplatz weiter zu fassen als im allgemeinen Datenschutzrecht. Das gilt insbesondere für die der Transparenz dienenden Individualrechte. So reicht es nicht aus, wenn die Fraktion Bündnis 90/DIE GRÜNEN fordert, dass die Beschäftigten regelmäßig über ihr Recht zu informieren sind, Art und Umfang der gespeicherten personenbezogenen Daten umfassend einzusehen und zu den Daten Stellung zu nehmen (Ziff. II 2 c, 16/9311). Darüber hinaus sollten die Beschäftigten in geeigneter Weise vorab über die Nutzung und Verarbeitung der sie betreffenden Daten informiert werden.

Andererseits erscheint es als zu weitgehend, den Beschäftigten Löschungsanprüche stets dann einzuräumen, wenn der Arbeitgeber gegen Informations- und Auskunftsrechte verstoßen hat (so der Vorschlag Bündnis 90/DIE GRÜNEN, Ziff. II 2 h, 16/9311). Denn Daten über ein bestehendes Arbeits- oder Dienstverhältnis sollten nur gelöscht werden, wenn sie (inzwischen) unrichtig sind bzw. rechtswidrig erhoben wurden. Allerdings sollte die Verletzung von Informations- und Auskunftspflichten stärker als bis-

her als Ordnungswidrigkeit geahndet werden können (dazu s. noch unten 9.).

7. **Der Schutz von Persönlichkeitsrechten der in Deutschland tätigen Beschäftigten weltweit agierender Unternehmen oder Konzerne ist sicherzustellen.**

   Angesichts der zunehmenden Internationalisierung gerade auch der Personaldatenverarbeitung müssen zusätzliche Anstrengungen unternommen werden, um das Schutzniveau von Beschäftigten in Deutschland - und darüber hinaus in der Europäischen Union – zu sichern. Bereits jetzt greifen Konzernmütter mit Sitz in Drittländern (z.B. in den USA) auf Personaldatenbestände der Tochterunternehmen in Deutschland zu oder verlangen die Verlagerung der Personaldatenverarbeitung ins Drittland. Die Datenexportklauseln der Europäischen Datenschutz-Richtlinie und die hierzu von der Europäischen Kommission beschlossenen Standardvertragsklauseln stellen einen angemessenen grenzüberschreitenden Beschäftigtendatenschutz nicht hinreichend sicher. Letztlich wird hier die Bundesregierung auf eine Änderung der Europäischen Datenschutzrichtlinie oder die Verabschiedung einer besonderen Richtlinie zum Beschäftigtendatenschutz dringen müssen.

   Es erscheint allerdings nicht zielführend, die Weitergabe von Daten der Beschäftigten an Auftragnehmer auch im Ausland von der Zustimmung der Beschäftigten abhängig zu machen (vgl. Ziff. II 2 d, 16/9311). Die Zustimmung ist im Arbeitsverhältnis grundsätzlich keine tragfähige Legitimation der Datenverarbeitung, da sie nicht realistisch verweigert werden kann. Allerdings müssen die Verantwortung des inländischen Auftraggebers präzisiert und die grenzüberschreitende Kontrolle der Datenverarbeitung effektiviert werden. Auch dies erfordert möglicherweise Rechtsänderungen auf europäischer Ebene.

8. **Eine effektive Kontrolle durch die zuständigen Datenschutzbehörden muss gewährleistet werden. Die betrieblichen und behördlichen Datenschutzbehörden sind bei allen personaldatenschutzrechtlich relevanten Verfahren und Entscheidungen frühzeitig einzubinden und umfassend zu beteiligen. Ihre Rechte und Befugnisse gegenüber den Mitarbeitervertretungen sind gesetzlich festzulegen.**

   Sowohl die Fraktion Bündnis 90/DIE GRÜNEN als auch DIE LINKE fordern mit Recht die Einführung der Mitbestimmung der Arbeitnehmervertretungen bei der Bestellung des betrieblichen Datenschutzbeauftragten, wie dies einzelne Bundesländer in ihren Landesdatenschutzgesetzen für die Bestellung der behördlichen Datenschutzbeauftragten bereits vorsehen (Ziff. II 6 g, 16/9311; Ziff. V c 16/11376). Dies ist die entscheidende Voraussetzung dafür, dass betriebliche und behördliche Datenschutzbeauftragte auch die Datenverarbeitung der Arbeitnehmervertretungen kontrollieren können. Bisher ist dies ausgeschlossen, weil der Datenschutzbeauftragte vom Arbeitgeber einseitig bestimmt und deshalb von den Interessenvertretungen nicht als unabhängiges Kontrollorgan akzeptiert werden kann.

   Zugleich haben die Vorkommnisse bei der Deutschen Telekom und in anderen Unternehmen gezeigt, dass die unabhängige Stellung des betrieblichen Datenschutzbeauftragten vom Gesetzgeber (nicht nur aus Gründen des Beschäftigtendatenschutzes) deutlich gestärkt werden muss. Dazu haben beide Fraktionen sinnvolle Vorschläge gemacht.

   Bedenken bestehen allerdings gegenüber dem Vorschlag der Fraktion Bündnis 90/DIE GRÜNEN, dem betrieblichen Datenschutzbeauftragten ein Widerspruchsrecht als suspensives Veto gegen Maßnahmen im Personalbereich einzuräumen, die gegen Arbeitnehmerdatenschutzregelungen verstoßen. Nach geltendem Recht ist die verantwortliche Stelle (das Unternehmen, die Verwaltungsbehörde) für die Datenverarbeitung allein verantwortlich. Ein Widerspruchsrecht des betrieblichen oder behördlichen Datenschutzbeauftragten würde diesen in die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung in systemwidriger Weise einbeziehen. Wenn der betriebliche oder behördliche Datenschutzbeauftragte nicht widersprochen hat, bestünde nach der vorgeschlagenen Regelung die Gefahr, dass die Unternehmens- oder Behördenleitung ihm die Verantwortung zuschiebt. Tendenzen dazu sind bereits jetzt (wenngleich im Widerspruch zum geltenden Datenschutzrecht) zu beobachten.

   Problematisch erscheint auch der Vorschlag der Fraktion DIE LINKE, eine Schiedsstelle für den Schutz der Daten von Beschäftigten analog zur Einigungsstelle einzurichten (Ziff. VIII, 16/11376). Zwar soll das Recht der Betroffenen, sich direkt an die Aufsichtsbehörde zu wenden, unberührt bleiben. Unklar ist aber, was bei widersprechenden Entscheidungen der Schiedsstelle und der Aufsichtsbehörde gelten soll, wer also das Letztentscheidungsrecht haben soll. Falls dies bei der Schiedsstelle läge, bestünde keine Konformität mit dem Erfordernis der völligen Unabhängigkeit nach Art. 28 der Europäischen Datenschutzrichtlinie.

   Zweifelhaft erscheint auch, ob es sinnvoll ist, den Schwellenwert für die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten auf 5 Beschäftigte (unabhängig davon, ob sie bei der Verarbeitung personenbezogener Daten beschäftigt sind) abzusenken (so der Vorschlag der Fraktion DIE LINKE, Ziff. V a, 16/11376). Damit würden auch kleine Unternehmen (z.B. Handwerksbetriebe) dieser Pflicht unterworfen, ohne dass damit spezifische datenschutzrechtliche Risiken aufgefangen würden.

9. **Verstöße gegen die Bestimmungen des Beschäftigtendatenschutzgesetzes müssen ein gesetzliches Verwertungsverbot der dadurch gewonnenen Daten nach sich ziehen. Zur Abschreckung bedarf es wirksamer Sanktionen.**

   Es ist zu begrüßen, dass die Fraktion Bündnis 90/DIE GRÜNEN – wie die Konferenz der Datenschutzbeauftragten – ein gesetzliches Verwertungsverbot für rechtswidrig erhobene Daten von Beschäftigten fordert (Ziff. II 2 e, 16/9311). Die Fraktion DIE LINKE sieht eine Löschungspflicht bei rechtswidrig erlangten oder erfassten Daten vor (Ziff. I n, 16/11376), wobei unklar ist, ob sich diese Löschungspflicht nur auf Verstöße gegen das Verbot automatisierter Einzelentscheidungen bezieht.

Insgesamt ist der Bußgeldkatalog des § 43 BDSG deutlich auszuweiten. Hierzu enthält der Antrag der Fraktion DIE LINKE eine Reihe sinnvoller Vorschläge (Ziff. IX, 16/11376). Insbesondere muss auch die rechtswidrige Nutzung von Beschäftigtendaten als Ordnungswidrigkeit geahndet werden können. Darüber hinaus sind Verstöße gegen Informations- und Transparenzpflichten, die über das geltende Recht hinausgehen, als Bußgeldtatbestände auszugestalten. Auch die Pflicht zum Ersatz von immateriellen Schäden von Beschäftigten ist zu unterstützen.

Abschließend sei – unabhängig von den vorliegenden Anträgen - darauf verwiesen, dass der Bundesgesetzgeber den **Schutz von Whistleblowern** dringend gesetzlich verankern muss. Der von der Bundesregierung eingebrachte Entwurf für einen neuen § 612a BGB war ohnehin nur ein unzureichender erster Schritt, der noch dazu nicht über die Ausschussberatungen hinausgekommen ist. Stattdessen muss ein umfassendes Gesetz zum Schutz von Beschäftigten verabschiedet werden, die auf Rechtsverstöße in Unternehmen und Behörden hinweisen. Vorbild kann insofern Großbritannien sein, das bereits seit 1998 den Public Interest Disclosure Act hat. Zugleich wäre in einem solchen Gesetz nicht nur der Datenschutz der meldenden, sondern auch der belasteten Personen zu regeln. Es ist daran zu erinnern, dass zahlreiche Skandale der letzten Zeit nicht öffentlich geworden wären, wenn nicht aus den Unternehmen unter hohem Risiko entsprechende Hinweise an die Medien oder die Aufsichtsbehörden gegeben worden wären. Zugleich darf die belastete Person auch in informationeller Hinsicht nicht völlig schutzlos gestellt werden. Unter diesen Voraussetzungen ist der Schutz von Whistleblowern zugleich ein wichtiger Baustein für eine verbesserte Datenschutzkontrolle.

DEUTSCHER BUNDESTAG
Ausschuss für
Arbeit und Soziales
16. Wahlperiode

Ausschussdrucksache 16(11)**1369**

7. Mai 2009

Stellungnahme

zur öffentlichen Anhörung von Sachverständigen am 11. Mai 2009 in Berlin zum

a) Antrag der Abgeordneten Brigitte Pothmer, Dr. Thea Dückert, Kerstin Andreae, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Rechte der Beschäftigten von Discountern verbessern - Drucksache 16/9101 -

b) Antrag der Abgeordneten Silke Stokar von Neuforn, Kerstin Andreae, Volker Beck (Köln), weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Persönlichkeitsrechte abhängig Beschäftigter sichern - Datenschutz am Arbeitsplatz stärken - Drucksache 16/9311 -

c) Antrag der Abgeordneten Jan Korte, Wolfgang Neskovic, Sevim Dagdelen, weiterer Abgeordneter und der Fraktion DIE LINKE.

Datenschutz für Beschäftigte stärken - Drucksache 16/11376 -

d) Antrag der Abgeordneten Gisela Piltz, Dr. Heinrich L. Kolb, Jens Ackermann, weiterer Abgeordneter und der Fraktion der FDP

Schutz von Arbeitnehmerdaten durch transparente und praxisgerechte Regelungen gesetzlich absichern - Drucksache 16/12670 -

Dr. Gerhard Schäfer, Bonn

1. Grundproblem des (Arbeitnehmer-)Datenschutzes

Bei der Frage der Zulässigkeit der Erhebung und Nutzung von im Zusammenhang mit einem Arbeitsverhältnis erhobenen und angefallenen Daten des Arbeitnehmers durch den Arbeitgeber geht es im Grunde immer um den interessengerechten Ausgleich von allgemeinem Persönlichkeitsrecht bzw. informationellem Selbstbestimmungsrecht des Arbeitnehmers sowie ggf. Schutz des Fernmeldegeheimnisses einerseits und der Eigentumsgarantie, der Berufsfreiheit und dem sog. Recht am eingerichteten und ausgeübten Gewerbebetrieb des Arbeitgebers andererseits. Das Kernproblem einer jeden Erhebung und Nutzung von Arbeitnehmerdaten ist, eine im Einzelfall interessengerechte und auch rechtssichere Abwägung widerstreitender Interessen zu finden. Jedem Abwägungsergebnis droht dabei interessenbedingt das Schicksal, als zu weitgehend oder eben als unzureichend eingestuft zu werden.

2. Bewährte Grundsätze des deutschen Datenschutzes

Die dem Ausschuss vorgelegten Anträge verfolgen alle das legitime Ziel, das aus dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs 1 i.V.m. Art. 1 GG abgeleitete informationelle Selbstbestimmungsrecht zu stärken, wonach jeder einzelnen die Befugnis haben soll, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen er persönliche Lebenssachverhalte offenbart und in welcher Weise seine „Lebensdaten“ verwendet werden sollen/dürfen.

Letzten Endes kombinieren alle Anträge die im deutschen Datenschutz geltenden Grundsätze der *Datenvermeidung* und *Datensparsamkeit*, wonach sich die Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten hat, keine (= Datenvermeidung) oder so wenig personenbezogene Daten wie möglich (= Datensparsamkeit) zu erheben, zu verarbeiten und zu nutzen. Datensparsamkeit und Datenvermeidung sind grundlegende Konzepte im Bereich Datenschutz und bspw. in § 3a BDSG niedergelegt. Die Anträge nehmen richtigerweise den weiteren traditionellen datenschutzrechtlichen Grundsatz auf, wonach nur diejenigen personenbezogenen Daten verarbeitet werden dürfen, die für die Erfüllung der jeweiligen Aufgabe benötigt werden (*Erforderlichkeit*). Allen Anträgen ist auch das Anliegen gemein, den das deutschen Datenschutz durchziehenden Grundsatz der *Transparenz* weiter Geltung zu verschaffen.

Wie im Bundesdatenschutzgesetz geregelt wird auch in den Anträgen die Zulässigkeit des Umgangs mit perso-

nenbezogenen Daten des Arbeitnehmers dem *Verbotsprinzip* unterstellt. Den Anträgen liegt das gemeinsame Verständnis zugrunde, dass der Umgang mit personenbezogenen Daten im Arbeitsverhältnis grundsätzlich verboten und nur dann erlaubt sein soll, wenn sich eine Befugnis hierzu ergibt.

3. Zulässigkeitserwägungen des Bundesarbeitsgerichts

Die Anträge kombinieren die allgemeinen und bewährten Grundsätze des deutschen Datenschutzes konsequenter Weise um die vom Bundesarbeitsgericht in Einzelfallentscheidungen herausgearbeiteten Zulässigkeitserwägungen. Nach den Grundsätzen der Rechtsprechung orientiert sich der Datenschutz im Arbeitsverhältnis an einer Abwägung der berechtigten, billigenswerten und schutzwürdigen (Informations-) Interessen des Arbeitgebers einerseits und dem Persönlichkeitsschutz („informationelle Selbstbestimmung“) des Arbeitnehmers andererseits. Letztlich maßgebend bei dieser Abwägung ist die Verhältnismäßigkeit. Nach den allgemeinen Grundsätzen muss die zu begutachtende Maßnahme zur Erreichung eines legitimen Ziels geeignet, erforderlich und angemessen sein.[1]

Im Einzelnen:

3.1. Geeignetheit

Geeignet ist eine Maßnahme, wenn mit ihrer Hilfe der erstrebte Zweck gefördert werden kann.

3.2. Erforderlichkeit

Erforderlich ist eine Maßnahme, wenn kein anderes, gleich wirksames und das Persönlichkeitsrecht weniger einschränkendes Mittel zur Verfügung steht.

3.3. Angemessenheit

Dreh- und Angelpunkt ist die Angemessenheit der Maßnahme. Es bedarf einer Gesamtabwägung der Intensität des Eingriffs und des Gewichts der ihn rechtfertigenden Gründe. Die Prüfung an diesem Maßstab kann dazu führen, dass ein an sich geeignetes und erforderliches Mittel zur Erreichung des legitimen Ziels nicht angewandt werden darf, weil die davon ausgehenden Grundrechtsbeeinträchtigungen die rechtfertigenden Eingriffsgründe überwiegen. Ein Ausgleich der widerstreitenden Interessen kann dazu führen, dass bspw. bestimmte (intensive) Grundrechtseingriffe erst von bestimmten Verdachts- oder Gefahrenstufen an vorgesehen werden dürfen.

Das Bundesarbeitsgericht hat für Überwachungsmaßnahmen eine Reihe von Kriterien herausgearbeitet, zu denen etwa zählen:

Für die Schwere des Eingriffs sind u.a. die Anzahl der betroffenen Personen, das Gewicht der Beeinträchtigungen und die Ausgestaltung der Eingriffsvoraussetzungen von Relevanz. Das Gewicht der Beeinträchtigung hängt wiederum u.a. davon ab, ob die Betroffenen als Personen anonym bleiben, welche Aspekte des informationellen Selbstbestimmungsrechts wie intensiv betroffen sind oder welche Nachteile den Grundrechtsträgern aus der Kontroll– und Überwachungsmaßnahme drohen oder von ihnen nicht ohne Grund befürchtet werden. So ist die Eingriffsintensität hoch, wenn Informationen betroffen sind, bei deren Erlangung Vertraulichkeitserwartungen verletzt werden, vor allem solche, die unter besonderem Grundrechtsschutz stehen.[2] Maßgeblich ist zudem Art und Dauer der Maßnahme, ob der Betroffene einen ihm zurechenbaren Anlass für die Datenerhebung und –nutzung geschaffen hat -- etwa durch eine Rechtsverletzung- oder, ob diese anlasslos erfolgt und eine große Zahl unverdächtiger Dritter betrifft, ob die Maßnahme zeitlich und örtlich beschränkt ist. Eine zeitlich unbeschränkte Maßnahme einer Überwachung kann bei den betroffenen Personen einen psychischen Anpassungsdruck erzeugen, durch den sie in ihrer Freiheit, aus eigener Selbstbestimmung zu planen und zu entscheiden, wesentlich gehemmt werden. Diesen Anpassungsdruck erzeugt dabei nicht erst eine ständige, anlassunabhängige Überwachung, sondern schon die objektive Möglichkeit zur Durchführung der Maßnahme.[3] Schon mit dem “Gefühl des Überwachtwerdens” können Einschüchterungseffekte verbunden sein, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen.[4] Abzustellen ist auch auf die “Persönlichkeitsrelevanz” der erfassten Informationen. Grundsätzlich gilt, dass die Heimlichkeit einer in Grundrechte eingreifenden Ermittlungsmaßnahme das Gewicht der Freiheitsbeeinträchtigung erhöht. Den Betroffenen kann hierdurch vorheriger Rechtsschutz faktisch verwehrt und nachträglicher Rechtsschutz erschwert werden.

4. Gedanken zur Reform des Arbeitnehmerdatenschutzes

Eine gesetzliche Regelung des Arbeitnehmerdatenschutzes kann nur dann Sinn haben, wenn sie gegenüber den allgemeinen Abwägungsgrundsätzen des Bundesarbeitsgerichts konkreter ist. Da am Grundsatz des Erlaubnisvorbehalts nicht gerüttelt werden soll und darf, wird eine gesetzliche Regelung die Eingriffstatbestände differenziert zu regeln haben. Dabei wird es freilich wenige Konstellationen geben, bei denen etwas generell erlaubt oder generell verboten ist.

Selbst bei heiklen persönlichen Umständen wie

1. Alkohol- und Drogenkonsum oder -abhängigkeit
2. Aufenthalts- und Arbeitserlaubnis
3. Berufliche Fähigkeiten/Werdegang/bisherige Beschäftigungsverhältnisse
4. Berufliche Verfügbarkeit
5. Krankheiten
6. Geschlecht
7. Gewerkschaftszugehörigkeit
9. Lebensalter
10. Nebentätigkeit
11. Nichtrauchereigenschaft
12. Parteizugehörigkeit

---

1 Aus jüngster Zeit etwa zur Videoüberwachung, Bundesarbeitsgericht, Beschluss vom 26.08.2008, Az 1 ABR 16/07, NZA 2008, 1187, 1190.

2 Wie etwa bei Eingriffen in das Grundrecht auf Unverletzlichkeit der Wohnung nach Art. 13 GG oder das Fernmeldegeheimnis nach Art. 10 GG. Siehe auch die besonderen Arten von personenbezogenen Daten des § 3 Abs. 9 BDSG.

3 Bundesarbeitsgericht, Beschluss vom 14.12.2004, 1 ABR 34/03, RDV 2005, 216ff..

4 Vgl. BVerfG vom 11.03.2008, Az.: 1 BvR 2074/05 und 1 BvR 1254/07, NJW 2008, 1505.

13. Persönliche Lebensverhältnisse
14. Religionszugehörigkeit
15. Scientology
17. Schwerbehinderteneigenschaft/Behinderung
18. Tätigkeiten im Ministerium für Staatssicherheit
19. Vermögen und Pfändung von Lohnansprüchen
20. Vorheriges Arbeitseinkommen
21. Vorstrafen/Strafverfahren
22. Wehr- bzw. Zivildienst
23. Wettbewerbsverbote

u.v.a.

können beispielsweise Fragen je nach den Besonderheiten des jeweiligen Arbeitsverhältnisses zulässig sein. Das Bundesarbeitsgericht erkennt grundsätzlich ein Recht des Arbeitgebers zur Frage an, wenn er ein berechtigtes Interesse an deren Beantwortung hat. Betrifft eine Frage lediglich die Privatsphäre eines Bewerbers und liefert ihre Beantwortung keine Informationen, die für die Eingehung des Arbeitverhältnisses von Bedeutung sind, ist sie i.d.R. unzulässig. Gefordert wird ein unmittelbarer Zusammenhang zwischen der beabsichtigten Nutzung und dem konkreten Verwendungszweck, was bedeutet, dass die Daten zur Erfüllung des konkret vorgesehenen Arbeitsverhältnisses erforderlich sein müssen.[5] Eine pauschalierende Lösung verbietet sich in der Regel.

So können bspw. strafrechtliche Verurteilungen – je nach Vertragsverhältnis – gar nicht, unter Umständen (Straßenverkehrsdelikte bei einem Kraftfahrer, Vermögensdelikte bei einem Bankmitarbeiter) oder aufgrund einer erforderlichen besonderen Vertrauensstellung (Mitarbeiter eines Sicherheitsdienstes) generell für den Arbeitgeber relevant sein. Entsprechend sind auch Fragen des Arbeitsgebers hierzu zulässig.[6]

Auch die aktuellsten Diskussionen um das Gendiagnostikgesetz zeigen, dass selbst Fragen nach dem Genom jedenfalls bei bestimmten Versicherungen nicht gänzlich unzulässig sind.

5. Zu den vorliegenden Reformüberlegungen und Anträgen der Fraktionen

Soweit in den Anträgen einzelne Regelungspunkte herausgearbeitet sind, kann diesen und den Detailausführungen dazu dem Grunde nach zugestimmt werden. Die Anträge entsprechen auch weitgehend bereits geltenden Grundsätzen des deutschen Datenschutzes und der Rechtsprechung des Bundesarbeitsgerichts. Ob es daher eines eigenen Arbeitnehmerdatenschutzgesetzes bedarf, kann zur Diskussion gestellt werden. Bis zur Verabschiedung einer umfassenden Regelung wäre aber an eine Ergänzung des Bundesdatenschutzgesetzes zu denken.

Bei den Reformüberlegungen wird dem in der seitherigen Rechtssprechung zutreffend heraus gearbeiteten Umstand Rechnung getragen werden müssen, dass es letzten Endes immer auf die Verhältnismäßigkeit ankommt. Ein für jeden Einzelfall ausdifferenziertes Regelwerk droht – wie etwa gegenwärtig im Steuerrecht zu beobachten - unübersichtlich und damit unpraktikabel zu werden. Eine gesetzliche Regelung würde den angestrebten Sinn einer normenklaren Regelung nur dann erfüllen können, wenn sie sich nicht in Einzelheiten verliert und diese vielmehr der Gesetzesbegründung überlässt.

Eine gesetzliche Regelung muss auch laufenden Veränderungen der Arbeitsverhältnisse gerecht werden. Solche Veränderungen sind denkbar etwa im Bereich der Anti-Diskriminierung auf der einen, aber auch etwa im Rahmen fortschreitender Korruptionsbekämpfung in Unternehmen auf der anderen Seite. § 130 OWiG[7] begründet bspw. unter näher bezeichneten Voraussetzungen eine bußgeldrechtliche Verantwortlichkeit des Inhabers von Betrieben und Unternehmen für Zuwiderhandlungen gegen betriebsbezogene Pflichten. Danach sind Aufsichtsmaßnahmen durchzuführen, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist. Zu diesen Pflichten gehören auch Aufsichtsmaßnahmen zur Prävention von betriebs- und unternehmensschädigenden Handlungen, wie Korruption, Untreue oder Betrug. Auf weitergehende Verpflichtungen aus dem Sarbanes-Oxley Act oder den EG-Verordnungen zur Bekämpfung des Terrorismus Nr. 881/2002 und Nr. 2580/2001 (verbotene Geldzuwendungen an gelistete Personen und Vereinigungen) sei nur am Rande hingewiesen. So wären bspw. nach der von der Bundesregierung mit Beschluss vom 18.02.2009 angekündigten Grundsatzregelung zum Arbeitnehmerdatenschutz im Bundesdatenschutzgesetz[8], bei der es sich ersichtlich um eine auf Arbeitnehmerdaten im Rahmen eines Beschäftigungsverhältnisses bezogene Spezialvorschrift handelt, Präventivmaßnahmen zur Korruptionsbekämpfung nicht zulässig, da die Nutzung der Arbeitnehmerdaten nach § 32-E Abs. 1 Nr. 3 BDSG nur „bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte zur Aufdekkung von im Beschäftigungsverhältnis begangenen Straftaten“ legitimiert sein soll. Ob dies gewollt ist, ist nicht ersichtlich.

Eine Generalklausel, die auf „berechtigte Interessen“ abstellt, könnte gesellschaftlichen Veränderungen, die zu einer verändernden Betrachtung der Antidiskriminierung

---

5 Gola/Wronka, Arbeitnehmerdatenschutz, 4. Auflage 2007, Rz 124; Simitis, BDSG, 6. Auflage 2006, § 28, Rz 91.

6 Däubler, Gläserne Belegschaften?, 4. Auflage 2002, Rz 217ff..

7 § 130 Abs. 1 Satz 1 OWiG lautet: Wer als Inhaber eines Betriebes oder Unternehmens vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, handelt ordnungswidrig, wenn eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre.

8 § 32 Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses
(1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies
1. für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist,
2. nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich oder durch eine Rechtsvorschrift erlaubt oder angeordnet ist oder
3. bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte zur Aufdeckung von im Beschäftigungsverhältnis begangenen Straftaten erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.

(3) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt."

von Korruptionsbekämpfung führen, besser gerecht werden, als jede kasuistische Lösung, wäre aber nicht mehr als die Umsetzung der Grundsätze der Rechtsprechung in das Gesetz.

Für den sehr sensiblen und auch derzeit viel diskutierten Bereich der Überwachung – Kontrollen am Arbeitsplatz (u.a. Videoüberwachung und Datenscreening) könnte eine ausdrückliche gesetzliche Regelung angezeigt sein, die etwa zwischen präventiven und repressiven Maßnahmen unterscheidet und dementsprechend Art, Umfang und Dauer denkbarer Maßnahmen umschreibt. Aber auch dazu gibt es detaillierte Rechtsprechung des Bundesarbeitsgerichts.

Zweckmäßig erscheint auch eine verstärkte Regelung der Verfahrensvorschriften. So ist an eine verfahrensrechtliche Absicherung von Kontroll- und Überwachungsmaßnahmen zu denken. „Verfahrensfehler“ in diesem Bereich würden nicht nur das individuelle Vertrauen eines Betroffenen, sondern die Vertrauensgrundlage eines Unternehmens (zu seinen Mitarbeitern und Kunden) insgesamt gefährden. Dies wäre dann genau das Gegenteil dessen, was durch die Vorhaben bewirkt werden soll: Integrität und Vertrauen zu stärken.

DEUTSCHER BUNDESTAG
Ausschuss für
Arbeit und Soziales
16. Wahlperiode

Ausschussdrucksache 16(11)**1366**

7. Mai 2009

Stellungnahme

zur öffentlichen Anhörung von Sachverständigen am 11. Mai 2009 in Berlin zum

a) Antrag der Abgeordneten Brigitte Pothmer, Dr. Thea Dückert, Kerstin Andreae, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Rechte der Beschäftigten von Discountern verbessern - Drucksache 16/9101 -

b) Antrag der Abgeordneten Silke Stokar von Neuforn, Kerstin Andreae, Volker Beck (Köln), weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Persönlichkeitsrechte abhängig Beschäftigter sichern - Datenschutz am Arbeitsplatz stärken - Drucksache 16/9311 -

c) Antrag der Abgeordneten Jan Korte, Wolfgang Neskovic, Sevim Dagdelen, weiterer Abgeordneter und der Fraktion DIE LINKE.

Datenschutz für Beschäftigte stärken - Drucksache 16/11376 -

d) Antrag der Abgeordneten Gisela Piltz, Dr. Heinrich L. Kolb, Jens Ackermann, weiterer Abgeordneter und der Fraktion der FDP

Schutz von Arbeitnehmerdaten durch transparente und praxisgerechte Regelungen gesetzlich absichern - Drucksache 16/12670 -

Karin Schuler, Bonn

1. Allgemeine Bewertung

Angesichts langjähriger Erfahrung bei der Datenschutzberatung von Arbeitnehmervertretungen und betrieblichen Datenschutzbeauftragten unterstütze ich, auch im Namen der Deutschen Vereinigung für Datenschutz e.V., das grundsätzliche Anliegen, ein Arbeitnehmerdatenschutzgesetz zu verabschieden.

In der Praxis zeigt sich seit langem, dass das Bundesdatenschutzgesetz zwar theoretisch auch für den betrieblichen Bereich eine solide Grundlage bietet, aber dennoch dem besonderen Abhängigkeitsverhältnis zwischen Arbeitgeber und Arbeitnehmer nicht gerecht wird. Die Unbestimmtheit mancher Begriffe, wie zum Beispiel der Zweckbestimmung, um nur ein Beispiel zu nennen, führt in der betrieblichen Praxis häufig zu unakzeptabler, aber phantasievoller Definitionsjonglage des Arbeitgebers. Wird erst einmal so etwas Schwammiges wie „Optimierung von Abläufen“ als Zweckbestimmung akzeptiert, so lassen sich hernach alle auf dieser Grundlage gesammelten Beschäftigtendaten (Tastenanschläge, minutiöse Überwachung von Außendienstmitarbeitern, sogar die Zahl der Toilettengänge) für fast alle denkbaren Auswertungen einsetzen, ohne, formal gesehen, den ursprünglichen Zweck zu ändern. Dass einigen Arbeitgebern sowohl bei der Sammlung als auch bei der Auswertung die Erfordernis der Abwägung mit den Persönlichkeitsrechten der Beschäftigten abhanden gekommen scheint, kann nun seit einigen Monaten auch öffentlich in den Medien verfolgt werden. Gerade diese Fähigkeit zur Abwägung ist zur Anwendung des BDSG jedoch unerlässlich. Da Unternehmen aus unterschiedlichsten Gründen diese Abwägung seit langen Jahren nicht vornehmen oder vornehmen können, scheint die Konkretisierung der Datenschutzprinzipien für den Arbeitsbereich der einzig erfolgversprechende Weg.

Soll ein Arbeitnehmerdatenschutzgesetz erfolgreich anwendbar sein, so muss es auf den Grundlagen des BDSG aufbauen und durch konkrete betriebliche Regelungen einen Mehrwert für den Datenschutz erzielen. Es muss sich an der betrieblichen Praxis orientieren und festlegen, wie die Prinzipien „Verbot mit Erlaubnisvorbehalt“, „Erforderlichkeit“, „Zweckbindung“ und „Transparenz“ in Bezug auf den Umgang mit Arbeitnehmerdaten umzusetzen sind. Ein zweites BDSG, bei dem nur die Worte „Betroffener“ durch „Beschäftigte“ und „verantwortliche Stelle“ durch „Arbeitgeber“ ersetzt würden, wäre nicht wünschenswert.

Da ein Arbeitnehmerdatenschutzgesetz in diesem Sinne eine bereichsspezifische Ergänzung des BDSG darstellt und nicht das BDSG ersetzen soll, erscheint es nicht sinnvoll, bereits im BDSG geregelte Sachverhalte nochmals ohne weitere Konkretisierung „abzuschreiben". Dies ist nicht nur unnötig, es stiftet auch insofern Verwirrung als der fälschliche Eindruck entstehen könnte, mit Verabschiedung eines Arbeitnehmer-Datenschutzgesetzes sei das BDSG für den Umgang mit Beschäftigtendaten nicht mehr einschlägig.

Als unbedingte Nebenpflicht zur Verabschiedung eines Arbeitnehmerdatenschutzgesetzes erscheint die Ausstattungsverbesserung der Aufsichtsbehörden und aktives Sanktionieren von Verstößen gegen Grundpflichten (Bestellung bDSB, Meldepflicht, Schulungspflicht, Erstellung Verfahrensverzeichnis,...)

2. Überflüssiges

Beispielhaft, jedoch in Bezug auf die vorgelegten Anträge nicht abschließend, im Folgenden Regelungsvorschläge, die entweder konkretisiert oder aufgrund ihrer Verankerung im BDSG nicht im AN-DSG Eingang finden sollten, da sie bereits eindeutig heutiger Rechtslage entsprechen:

- Mit personenbezogene Daten darf auch heute schon nur nach Verpflichtung auf § 5 BDSG und Datenschutz-Unterweisung umgegangen werden [11376]
- Die Gleichstellung personenbeziehbarer Daten mit personenbezogenen Daten [11376] ist auch heute schon unstrittig. Strittig ist allerdings, wann ein Datum (Beispiel IP-Adresse) personenbeziehbar ist. Gerade hierzu wäre eine Klarstellung im betrieblichen Umfeld wünschenswert, die auf die Zugriffsmöglichkeiten des Arbeitgebers Bezug nimmt.
- Das Fragerecht im Bewerbungsverfahren verbietet auch heute schon viele Fragen, z. B. nach einer Schwangerschaft [9311].
- Die Rechte der Arbeitnehmervertretungen auf Information und Mitbestimmung sind bereits heute in BetrVG, PersVG und weiteren ausführlich geregelt [9311]

3. Schädliches

Folgende Regelungsvorschläge stellten sogar eine Verschlechterung der heutigen Rechtlage dar und sollten so keinesfalls umgesetzt werden:

- Die Beschränkung des Geltungsbereichs auf Regelungen zur Erhebung, Speicherung, Veränderung, Übermittlung und Nutzung personenbezogener Daten [11376] nimmt aus nicht offensichtlichen Gründen die Löschung und Sperrung als Verarbeitungsphasen aus. Gerade zur Löschung (Fristen, Löschkonzepte, Löschansprüche) sollte ein gutes Arbeitnehmerdatenschutzgesetz aber konkrete Aussagen treffen.
- Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist auch heute schon nur nach Identifizierung einer Zulässigkeitsgrundlage (Arbeitsvertrag, sonstiger Vertrag, Einwilligung) zulässig [11376]. Zur Problematik des Ausklammern von Löschung und Sperrung siehe oben. Das „Interesse des Betroffenen" als zusätzliche Zulässigkeitsgrundlage einzuführen, würde den bekannten, problematischen Interpretationskunststücken Tür und Tor öffnen.
- Die Verknüpfung der Zulässigkeit der Verarbeitung mit dem Vorliegen eines nicht näher spezifizierten Datenschutzkonzepts [11376] ist wenig hilfreich. Es gibt keine allgemein akzeptierte Definition, welchen Inhalt und Umfang ein Datenschutzkonzept haben muss und die geforderte Dokumentation der Zugriffrechte und Sicherheitsmaßnahmen ist weit weniger als nach heutiger Rechtslage im Verfahrensverzeichnis gemäß § 4g (2) BDSG vor Aufnahme einer Verarbeitung zu dokumentieren ist.
- Solange Betriebsräte kein Mitbestimmungsrecht bei der Bestellung des/der Datenschutzbeauftragten haben, ist es nicht akzeptabel, den Betriebsrat der Aufsicht des betrieblichen Datenschutzbeauftragten zu unterwerfen [11376], da dies die gesetzlich garantierte Unabhängigkeit des Betriebsrats gefährdet (siehe hierzu auch BAG-Urteil 1 ABR 21/97).
- Ein Konzernprivileg zu konstatieren, gar ein europäisches [12670], geht hinter die Schutzregelungen des BDSG zurück, das aus gutem Grund ein solches Privileg ausdrücklich nicht vorsieht, da in heutigen Konzern- und Unternehmensstrukturen die Verflechtungen eine Grenzziehung (als Übermittlungsschranken) nicht mehr ermöglichen. Die Einführung eines Konzernprivilegs käme einem Dammbruch gleich, der die unkontrollierbare Verteilung von Beschäftigtendaten zur Folge hätte.

Aus praktischer Sicht erscheinen einige der vorgeschlagenen Regelungen aufgrund der Gestaltung heutiger IT-Systeme weder umsetzbar noch hilfreich:

- Die Definition der Personalakteninhalte als „in unmittelbarem inneren Zusammenhang mit dem Beschäftigungsverhältnis stehend" [12670] ist nebulös und wenig hilfreich. Auch Änderungsbelege in SAP (z. B. an der Hotline: wer hat wann welche Störungsmeldungen aufgenommen) erfüllen je nach Arbeitsaufgabe diese Definition – und sind doch alles andere als klassische Personalakteninhalte. Die geforderte technische und organisatorische Trennung bestimmter, besonders sensibler Beschäftigtendaten („Personalaktenqualität") von weiteren Beschäftigtendaten [11376, 9311] erscheint realitätsfremd. Damit wäre kein SAP-System mehr legal zu betreiben, da derartige Systeme gerade so aufgebaut sind, dass zu einer Person unterschiedliche Datenklassen existieren, die jedoch immer an zentralen Stammdaten festgemacht werden. Aus Datenschutzsicht ist aber auch gar nicht entscheidend, dass die Datenklassen getrennt geführt werden (mit heutiger IT stellt eine Zusammenführung aus getrennten Systemen ohnehin kein Problem dar), sondern dass die Berechtigungssysteme feingranulare Einstellungen erlauben – und entsprechend dem „need-to-know"-Prinzip genutzt werden.
- Gesundheitsdaten unterfallen bereits heute den besonderen Daten gem. § 3 (9) BDSG. Eine Klarstellung erscheint insofern nicht erforderlich. Die Beschränkung der Verarbeitung von Gesundheitsdaten auf Personen, die der ärztlichen Schweigepflicht unterliegen [11376], würde es jedem Meister verunmöglichen, die Krankmeldungen seiner Schichtarbeiter zur Kenntnis zu nehmen.
- So sehr die Begrenzung des Einsatzes opto-elektronischer Geräte wünschenswert ist, so wenig kann

man das Verbot der Verhaltensüberwachung generell durchhalten. Leitstände, sicherheitsrelevante Meldezentralen, Rechenzentren und anderer sind auf den Einsatz angewiesen – und zwar gerade zur Überwachung des Verhaltens. Eine fallunterscheidende Nutzungsbegrenzung ist daher zum Schutz der Betroffenen unbedingt erforderlich.

- Bei Zulässigkeit privater Nutzung die (nicht abdingbare!) Geltung des Fernmeldegeheimnisses und der entsprechenden TKG-Bestimmungen zu verlangen, würde bei jedem sicherheitsbewussten Unternehmen zu sofortigem Verbot privater Nutzung führen. Denn der sichere Betrieb einer IT-Infrastruktur in einem Unternehmen erfordert Schutzmechanismen, Protokollierungen und Sicherungskopien, die mit dem Fernmeldegeheimnis nicht vereinbar sind. Da andererseits auf der technischen Ebene private nicht von dienstlicher Nutzung zu unterscheiden ist, könnte eine private Nutzung nicht mehr toleriert werden. Unabhängig davon, dass dies auch mit Revisions- und Überprüfungspflichten eines Unternehmens kollidiert, scheint dieser Vorschlag realitätsfern. Sinnvoller wäre stattdessen eine Klarstellung, dass ein Unternehmen gerade nicht als Telekommunikationsdiensteanbieter im Sinne des TKG gilt, dass aber für die transparente Gestaltung der Netzüberwachung und die betriebsöffentliche Dokumentation der Überwachungsmaßnahmen strenge, willkürverhindernde Vorschriften gelten.

Erforderliches

Die folgenden Regelungsvorschläge sind, soweit sie aus den Anträgen stammen, im Sinne einer Konkretisierung des Arbeitnehmerdatenschutzes ausdrücklich zu begrüßen oder wären aus praktischer Sicht dringend erforderlich:

- Die Abkoppelung des Schutzes betroffener Beschäftigter von formalen Anstellungsverhältnissen und die Einbeziehung von Bewerber/innen, Leiharbeitnehmern, Freiberuflern etc. [9311, 11376] Zusätzlich sollten Beschäftigte von Fremdfirmen (z. B. Subunternehmer) für die Dauer ihres Arbeitseinsatzes bei einem Auftraggeber geschützt sein (z. B. bei der Fragestellung, ob man Beschäftigte von Fremdfirmen stärker durch Videoüberwachung kontrollieren darf als die eigenen Mitarbeiter/innen). Außerdem sind Auftragnehmer davor zu schützen, dem Auftraggeber eine direkte Kontrolle ihrer Beschäftigten zu gestatten (was z. B. in vielen Branchen von Automobilzulieferern bis zu Sachbearbeitungsbüros üblich ist).
- Das Verbot, alle gesetzlich garantierten Rechte Beschäftigter durch Rechtsgeschäft, also auch durch Betriebsvereinbarungen einzuschränken [11376]. Allerdings ist eindeutig zu spezifizieren, was eine zulässige „Verbesserung“ sein kann. Es sollte eindeutig geklärt werden, unter welchen Voraussetzungen eine Betriebsvereinbarung Zulässigkeitsgrundlage für eine automatisierte Verarbeitung sein kann (enger Bezug zur Erbringung der Arbeitsleistung, kein konkurrierendes Individualrecht etc.)
- Die Festschreibung von Mitbestimmungsrechten der Arbeitnehmervertretung für alle vom Arbeitnehmerdatenschutzgesetz erfassten Verarbeitungen. Die Festlegungen sollten sich an der Begrifflichkeit des BetrVG (mitbestimmen, beraten, vorschlagen) orientieren und keine neuen, unkonkreten Begriffe (z. B. abstimmen) einführen.
- Eine Konkretisierung und Ausgestaltung des Verfahrensverzeichnisses gemäß $ 4 d (2) BDSG derart, dass der Detaillierungsgrad für Arbeitnehmerdaten im Verzeichnis erhöht wird und das Verzeichnis mitbestimmungspflichtig wird.
- Die Verarbeitung und Nutzung von Beschäftigtendaten aus Protokolldateien (Serversysteme, Arbeitsplatzrechner) sollte der besonderen Zweckbindung gemäß § 31 BDSG unterfallen, nur dem ordnungsgemäßen Betrieb der Systeme dienen und ausschließlich den mit dem Betrieb direkt betrauten Personen zugänglich sein.
- Die Einrichtung einer paritätisch besetzten Schiedsstelle analog zur Einigungsstelle gem. BetrVG erscheint sinnvoll. Besetzung und Kostenträgerschaft sollten konkretisiert werden.
- Die Stärkung der Position betrieblicher Datenschutzbeauftragter ist zu begrüßen [11376]. Gleiches gilt für die Sanktionierung bei Nichtbestellung [9311] und bei fehlender Unterrichtung [12670]. Zusätzlich zu dem vorgeschlagenen Kündigungsschutz sollten verbindliche Mengengerüste bzgl. personeller und kapazitativer Unterstützung vorgesehen werden.
- Dem Betriebsrat sollte ein Mitbestimmungsrecht bei der Bestellung des betrieblichen Datenschutzbeauftragten eingeräumt werden [9311]. Die Voraussetzungen für eine Abberufung des Datenschutzbeauftragten sollten klar geregelt und in Fällen möglich sein, in denen der Datenschutzbeauftragte seine Aufgaben nicht ordnungsgemäß versieht.
- Konkrete Schutzvorschriften, insbesondere Verschlüsselungserfordernisse für bestimmte Arten von Daten (Online-Bewerbungen, Personalakten etc., Versand per E-Mail) [9311, 11376] sind erforderlich, da die Bereitschaft von Unternehmen, personenbezogene Daten in öffentlichen Netzen durch angemessene, sichere Verfahren vor unberechtigter Einsichtnahme zu schützen, generell zu schwach ausgeprägt ist.
- Eine Klarstellung, dass BDSG und BetrVG subsidiär neben einem Arbeitnehmerdatenschutzgesetz bestehen [12670], erscheint zur Klarstellung hilfreich. Es sollte außerdem klargestellt werden, wie das Verhältnis zu gesetzlichen oder sonstigen Normen zur IT-Sicherheit zu gestalten ist, die die Verarbeitung von Beschäftigtendaten verlangen (z. B. Forensische Analysen, Whistleblowing, EU-Sanktionslistenscanning, Sarbanes-Oxley Act u.s.w.
- Die Einsatzmöglichkeiten von Videokameras im nicht-öffentlichen Betriebsbereich sollte, unabhängig von allen anderen sinnvollen Einschränkungen, nur zulässig sein, wenn im Herrschaftsbereich des AG (kein „Vermietervideo“).
- Die Rahmenbedingungen für Taschenkontrollen, Röntgenkontrollen sollten so konkretisiert werden, dass strenge Bedingungen formuliert und eine Aufzeichnung elektronischer Daten untersagt sind.
- Dem Arbeitgeber muss verboten sein, in den privaten Bereich der Beschäftigten einzudringen (z. B. durch Privatdetektive).

- Bewegungsdaten sollten einer strengen Zweckbindung und einer kurzen Löschfrist unterworfen werden (Location Based Services, GPRS, GSM u.ä. die für Flottenverwaltung, Dispositionssteuerung u.ä. verwendet werden.)
- Dem Betriebsrat sollte eine Mitbestimmung bei allen Löschfristen eingeräumt werden, die nicht gesetzlich geregelt sind.
- Die Gestaltungsanforderungen an Auftrags-DV-Verträge innerhalb von Konzernen (z. B. zur Erbringung von Personalbüro-Dienstleistungen) müssen konkretisiert werden, so dass notwendige Regelungsinhalte (Auftragsbeschreibung, Weisungsdurchsetzung, Kontrollrecht, Beschreibung der Schutzmaßnahmen etc.) ablesbar sind. Es sollte konkret geregelt werden, welche Verarbeitungen innerhalb eines Konzerns überhaupt als Auftrags-Datenverarbeitung gem. § 11 BDSG organisiert werden dürfen.
- Daten, die ein Betriebsarzt im Rahmen seiner rechtmäßigen Tätigkeit im Unternehmen über Beschäftigte erhebt (die also bis auf die Pflicht zur Mitteilung von arbeitsverhindernden Sachverhalten der Schweigepflciht unterliegen) dürfen nicht in Systemen des Arbeitgebers abgelegt werden, es sei denn, durch Verschlüsselung ist der alleinige Zugriff des Betriebsarztes sicher gestellt.
- Erlaubter Umfang und Zweck von Aufzeichnungen bei Rückkehrergesprächen gem. § 84 SGB IX sollten konkretisiert werden.
- Betriebsrat und Datenschutzbeauftragter sollten das ausdrückliche Recht erhalten, sich jederzeit, ohne dem Vorwurf der Illoyalität ausgesetzt zu sein, an die Aufsichtsbehörde zu wenden.