

Antrag

der Abgeordneten Jan Korte, Klaus Ernst, Dr. Petra Sitte, Matthias W. Birkwald, Ulla Jelpke, Jutta Krellmann, Wolfgang Neskovic, Petra Pau, Jens Petermann, Ingrid Remmers, Raju Sharma, Kersten Steinke, Frank Tempel, Halina Wawzyniak, Sabine Zimmermann und der Fraktion DIE LINKE.

Datenschutz für Beschäftigte stärken

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Moderne Informations- und Kommunikationstechniken werden nicht nur zunehmend in Unternehmen und im öffentlichen Leben eingesetzt, sondern prägen bereits die gesamte Arbeitswelt. Die internationale Vernetzung und Globalisierung der Wirtschaft bedingt, dass Daten von Beschäftigten nicht nur innerbetrieblich, sondern auch über den Betrieb hinaus erhoben, verarbeitet und genutzt werden.

Nicht erst die Bespitzelungsaffäre beim Discounter Lidl oder die Datenmissbräuche bei der Deutschen Bahn AG zeigen, dass Beschäftigte an ihrem Arbeitsplatz deutlich besser gegen die Verletzung ihres informationellen Selbstbestimmungsrechts geschützt werden müssen. Das Fehlen besonderer gesetzlicher Vorgaben zum Schutz der Daten von Beschäftigten und die Missachtung der Bestimmungen des Bundesdatenschutzgesetzes (BDSG) haben in vielen Unternehmen eine rechtswidrige Praxis befördert, die bis zu umfassender Überwachung und zum Einsatz modernster Technik wie biometrischen Erkennungsverfahren und Blut- bzw. Gentests gehen kann. In besonderer Weise trifft dies auf Unternehmen zu, in denen keine Arbeitnehmervertretungen bestehen, die durch Mitbestimmungsverfahren die Persönlichkeitsrechte der abhängig Beschäftigten schützen und fördern und an die sich Betroffene wenden können. Aber auch in Unternehmen mit existierenden Arbeitnehmervertretungen haben diese oft Schwierigkeiten, die Interessen der Beschäftigten durchzusetzen, da die Mitbestimmungsrechte in Bezug auf den Datenschutz im Betriebsverfassungsgesetz nur ungenügend geregelt sind.

Eine Erweiterung der bestehenden Regelungen ist deshalb im Sinne der Rechtsklarheit und Rechtsdurchsetzung dringend erforderlich. Darüber hinaus zeigen die Ereignisse bei der Deutschen Telekom AG und ihren Tochtergesellschaften mit immer neuen Fällen von massiver Überwachung von Arbeitnehmerinnen- und Arbeitnehmervertretungen, dass auch die betriebliche Interessenvertretung eines besseren Schutzes bedarf.

Der Deutsche Bundestag hat gegenüber der Bundesregierung bereits mehrfach, zuletzt in der Beschlussempfehlung zum Tätigkeitsbericht des Bundesbeauftragten für Datenschutz und Informationsfreiheit 2003/2004, die Forderung erhoben, den Schutz der Daten von Beschäftigten in einem gesonderten Arbeit-

nehmerdatenschutzgesetz zu regeln und eine entsprechende parlamentarische Initiative unverzüglich vorzulegen. Die Bundesregierung ist dieser Forderung bisher nicht nachgekommen.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

bis zum Beginn der parlamentarischen Sommerpause 2010 einen Gesetzentwurf zum Schutz der Daten von Beschäftigten im öffentlichen und nichtöffentlichen Bereich vorzulegen. Ziel ist es, diese vor einer unangemessenen Beeinträchtigung ihres informationellen Selbstbestimmungsrechts durch die Erhebung, Speicherung, Veränderung oder Übermittlung, Sperrung, Löschung sowie Nutzung ihrer personenbezogenen Daten vor, während und nach Bestehen eines Arbeitsverhältnisses zu schützen. Der Gesetzentwurf soll folgende Regelungen umfassen:

1. Grundsätze der Erhebung, Speicherung, Veränderung, Übermittlung und Nutzung, Sperrung und Löschung personenbezogener Daten (im Folgenden als Datenverarbeitung bezeichnet) von Beschäftigten

a) Das Gesetz zum Schutz der Daten von Beschäftigten umfasst Regelungen zur Verarbeitung personenbezogener Daten von Beschäftigten unabhängig von den dafür genutzten Medien, Methoden und Formen und unabhängig davon, ob die Daten in elektronischer oder anderer Form vorliegen. Zu den personenbezogenen Daten gehören auch Fotos der Beschäftigten.

Personenbeziehbare Daten (Daten, die unter Verwendung zusätzlicher Angaben auf eine Person bezogen werden können) sind personenbezogenen Daten gleichgestellt.

b) Das Gesetz zum Schutz der Daten von Beschäftigten gilt für öffentliche und nichtöffentliche Stellen.

c) Das Gesetz zum Schutz der Daten von Beschäftigten gilt für alle Personen, die in einem Arbeits- oder Dienstleistungsverhältnis beschäftigt sind (nachfolgend Beschäftigte) und für jede Art der Erbringung einer Arbeits- bzw. Dienstleistung oder der Vertragsgestaltung (auch Telearbeiterinnen und -arbeiter, mobile Außendienstlerinnen und Außendienstler, Freelancerinnen und Freelancer sowie ausgelagerte Beschäftigte, die in einem neuen Unternehmen arbeiten). Das Gesetz gilt auch für Bewerberinnen und Bewerber um ein Beschäftigungsverhältnis sowie für Auszubildende und Praktikantinnen und Praktikanten.

Mit Personen, die nicht auf dem Betriebsgelände beschäftigt werden, sind unter Hinzuziehung der Interessenvertretung und des betrieblichen Datenschutzbeauftragten konkrete Vereinbarungen zur Einhaltung der Regelungen des Gesetzes zum Schutz der Daten von Beschäftigten abzuschließen.

d) Die Verarbeitung der Daten von Beschäftigten ist nur zulässig, wenn sie durch Gesetz oder eine sonstige Rechtsvorschrift erlaubt ist oder ein mit den Betroffenen geschlossener Vertrag dies erfordert.

e) Die Rechte Beschäftigter nach diesem Gesetz können nicht durch Rechtsgeschäfte eingeschränkt oder ausgeschlossen werden. Durch Kollektivvereinbarungen kann das Gesetz zum Schutz der Daten von Beschäftigten ergänzt und verbessert, aber nicht eingeschränkt werden. Die Einschränkung von Rechten aus diesem Gesetz durch Einwilligung der betroffenen Beschäftigten, Bewerberinnen und Bewerber ist unzulässig.

f) Personenbezogene Daten dürfen nur erhoben, gespeichert, verändert, übermittelt oder genutzt werden, wenn Verzeichnisse gemäß § 4g Absatz 2 BDSG vorliegen, das mit dem betrieblichen Datenschutzbeauftragten und dem Betriebs- bzw. Personalrat abgestimmt ist.

- g) Personenbezogene Daten sind ausschließlich durch Personen zu erheben, zu speichern, zu verändern, zu übermitteln oder zu nutzen, die vorher gemäß § 5 BDSG schriftlich auf das Datengeheimnis verpflichtet wurden und eine angemessene Schulung erhalten haben.
- h) Daten in Personalaktenqualität, die zur Begründung und Aufrechterhaltung des Beschäftigungsverhältnisses benötigt werden, sind technisch und organisatorisch von den übrigen Daten der Beschäftigten getrennt zu speichern und zu verarbeiten, ohne dass hiervon die Auskunftsrechte der Betroffenen berührt werden. Alternativ dazu müssen die Zugangsberechtigungssysteme feingranulare Einstellungen erlauben, die die jeweiligen Berechtigungen eindeutig regeln und nach dem Need-to-know-Prinzip geführt werden.

Das gilt auch für Auftragsdatenverarbeitung.

- i) Daten einer speichernden Stelle dürfen nicht mit Daten einer anderen speichernden Stelle gemeinsam gespeichert werden, unabhängig davon, ob es sich bei beiden Datenmengen um Daten von Beschäftigten handelt.
- j) Werden personenbezogene Daten für ein künftiges oder im Rahmen eines bestehenden Arbeitsverhältnisses erhoben, gespeichert, verändert, übermittelt oder genutzt, ist dies nur zur Erfüllung des Zwecks des Arbeitsverhältnisses zulässig.
- k) Daten sind bei den Beschäftigten direkt zu erheben und diese müssen die Erhebung erkennen können. Sie sind auch über die technischen Mittel und Methoden der Verwendung sowie die zusätzlich verarbeiteten Daten zu informieren. Ohne Mitwirkung der Betroffenen dürfen Daten von Beschäftigten nur erhoben werden, wenn eine Rechtsvorschrift dies vorsieht.
- l) Die Verarbeitung der Daten von Beschäftigten sind nur zulässig, wenn und solange sie zur Erreichung eines vorher konkret festgelegten Zwecks erforderlich sind (Zweckbindung) und die Verwendung datenvermeidender Anwendungen diesen Zweck nicht oder nicht ohne unzumutbaren Aufwand erfüllen kann. Im Voraus festzulegen sind die technischen Mittel der Datenverarbeitung, die diesbezüglichen Grundsätze sowie diejenigen Daten, die zusätzlich in die Verarbeitung eingehen. Durch geeignete technische und organisatorische Maßnahmen ist sicherzustellen, dass nur Personen Zugriff auf personenbezogene Daten haben, zu deren Aufgaben dieser Zugriff gehört. Daten von Beschäftigten, deren Verarbeitung ihrem Zweck nach nur vorübergehend erforderlich ist, sind binnen angemessener Frist zu löschen.
- m) Soweit den Betroffenen über die Verarbeitung ihrer personenbezogenen Daten Mitteilung zu machen ist, sind 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 Verarbeitung eingehen, mitzuteilen. Neben der verantwortlichen Stelle sind auch die verantwortlichen Personen und deren Erreichbarkeit mitzuteilen. Durch Vereinbarung kann festgelegt werden, welche Mitteilungen ohne Personenbezug durch Offenkundigmachen oder auf andere Weise erfolgen können.
- n) Das Verbot automatisierter Einzelentscheidungen (§ 6a BDSG) ist in der Arbeitswelt zwingend zu befolgen. Personelle Einzelentscheidungen (§§ 99, 102 des Betriebsverfassungsgesetzes – BetrVG) dürfen nicht automatisch erfolgen. Rechtswidrig erlangte oder erfasste Daten sind unverzüglich zu löschen.
- o) Die Übermittlung der Daten von Beschäftigten an Dritte ist nur zur Erfüllung von gesetzlichen Pflichten oder arbeitsvertraglichen bzw. tariflichen Regelungen zulässig. Die Empfänger dieser Daten sind nachweislich auf die Grundsätze des Datenschutzes, insbesondere die Zweckbindung und das

Übermittlungsverbot gemäß § 28 Absatz 3 BDSG, hinzuweisen. Der Handel mit Daten von Beschäftigten ist verboten.

2. Schutz besonderer Arten von Daten

- a) Besondere Arten von Daten gemäß § 3 Absatz 9 BDSG bzw. Artikel 8 Absatz 1 der EG-Datenschutzrichtlinie von Beschäftigten dürfen nur verarbeitet werden, wenn und soweit es für einen konkreten Zweck zwingend erforderlich ist. Die Verarbeitung derartiger Daten unterliegt der Mitbestimmung des Betriebs- bzw. Personalrates sowie der Beteiligung des betrieblichen Datenschutzbeauftragten.
- b) Daten über die physische und psychische Konstitution von Bewerberinnen und Bewerbern oder Beschäftigten (Gesundheitsdaten) sind besondere Arten von Daten gemäß § 3 Absatz 9 BDSG. Das Merkmal „rassische Herkunft“ ist ersatzlos zu streichen.
- c) Biometrische Daten dürfen ausschließlich zu Autorisierungs- und Authentifizierungszwecken verarbeitet werden.
- d) Genetische Untersuchungen und Analysen bzw. die Entgegennahme, Verwendung oder das Verlangen von Mitteilung von Ergebnissen bereits erfolgter genetischer Untersuchungen und Analysen sind unzulässig. Ausnahmen sind nur gemäß den Regelungen des Gendiagnostikgesetzes erlaubt.
- e) Die Speicherung und Übermittlung besonderer Arten von Daten hat verschlüsselt zu erfolgen.

3. Schutz von Bewerberinnen und Bewerbern

- a) Daten in Bewerbungsvorgängen sind bei den Betroffenen direkt zu erheben. Sie dürfen nur bezogen auf die Art der angestrebten Tätigkeit verarbeitet werden. Die Bewerberinnen und Bewerber sind über die Tatsache einer maschinellen Auswertung der Bewerbungsunterlagen zu informieren.
- b) Daten aus psychologischen Tests dürfen in Einstellungsverfahren nur für die Prüfung der Eignung für rechtlich eng zu begrenzende Aufgaben verarbeitet werden. Die Erhebung, Speicherung, Veränderung, Übermittlung und Nutzung derartiger Daten setzen die Vorabkontrolle und Zustimmung des betrieblichen Datenschutzbeauftragten voraus.
- c) Graphologische Tests sind unzulässig.
- d) Führt eine Bewerbung nicht zur Begründung eines Arbeitsverhältnisses, sind die Bewerbungsdaten einschließlich der Tatsache einer Bewerbung unverzüglich zu löschen oder zurückzugeben. Die Löschung ist auf Verlangen schriftlich zu bestätigen.
- e) Fragen und Nachweisverlangen dürfen sich, soweit Besonderheiten des konkreten Arbeitsplatzes dies nicht zwingend erfordern, nicht beziehen auf:
 - straf- oder ordnungswidrigkeitsrechtliche Verfahren, die nicht oder nicht mehr in ein Führungszeugnis aufgenommen werden dürfen oder mit dem Arbeitsplatz in keinem sachlichen Zusammenhang stehen,
 - die Vermögensverhältnisse oder eventuelle Lohnpfändungen,
 - die Ableistung des Wehr- oder Zivildienstes,
 - die Mitgliedschaft in Parteien, Religionsgemeinschaften oder Gewerkschaften,
 - Schwangerschaften oder das Einsetzen des Klimakteriums,
 - Gesundheitsdaten, sofern diese keine Auswirkung auf die Erfüllung arbeitsvertraglicher Pflichten haben, und biometrische Daten,
 - sonstige besondere Arten von Daten i. S. d. § 3 Absatz 9 BDSG.

- f) Verweigert eine Bewerberin oder ein Bewerber die Auskunft auf eine unzulässige Frage und kommt das Arbeitsverhältnis aus diesem Grunde nicht zustande, ist ein Schadenersatzanspruch vorzusehen.
- g) Bewerberinnen und Bewerber haben Anspruch auf kostenlose Auskunft und fortlaufende Unterrichtung über die zu ihrer Person gespeicherten Daten, auch wenn ein Arbeitsverhältnis nicht begründet wird. Der Auskunftsanspruch umfasst auch den Zeitpunkt der Erhebung, die vorgesehene Speicherdauer, den Umfang und Zeitpunkt vorgenommener Veränderungen, die eventuelle Übermittlung sowie die Mitteilung über eine Auftragsdatenerhebung, Verarbeitung und Nutzung (§ 11 BDSG). Auf Verlangen ist die Auskunft schriftlich oder in anderer dauerhafter Form zu erteilen. An ein Auskunftsverlangen dürfen keine nachteiligen Folgen geknüpft werden.
4. Schutz von Beschäftigten während und nach Beendigung des Beschäftigungsverhältnisses
- a) Grundsätze
- aa) Arbeitgeberinnen und Arbeitgeber sind verpflichtet, in der betrieblichen Personalarbeit datenvermeidende und datensparsame Instrumente und Mittel einzusetzen. Personenbezogene Daten der Beschäftigten sind vertraulich zu behandeln und dürfen nur verarbeitet werden, 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.
- bb) Beschäftigte haben Anspruch auf kostenlose Auskunft und fortlaufende Unterrichtung über die zu ihrer Person gespeicherten Daten, auch wenn ein Arbeitsverhältnis nicht mehr besteht. Umfang und Rechtsfolgen des Auskunftsanspruchs entsprechen denen gemäß Abschnitt 3 Buchstabe g dieses Antrags. Auskunft darf den Betroffenen nur verweigert werden, wenn die Verarbeitung der Daten ausschließlich der Bekämpfung konkreter Straftaten gegen die betrieblichen Interessen oder die Interessen anderer Beschäftigter dient oder einen Vorgang zum Gegenstand hat, der eine Kündigung oder Abmahnung rechtfertigen würde.
- cc) Nach Beendigung eines Beschäftigungsverhältnisses sind Daten von Beschäftigten zu löschen, wenn und solange sie nicht zur Abwicklung des Beschäftigungsverhältnisses und zur Erfüllung gesetzlicher Vorschriften erforderlich sind. Die Höchstdauer der Speicherung ist gesetzlich festzulegen. Abweichungen sind für konkrete Zwecke und für einen vorher bestimmten Zeitraum zulässig, wenn die Betroffenen einwilligen.
- b) Leistungs-, Verhaltens- und Bewegungsprofile von Beschäftigten
- aa) Daten, die einer Verhaltens- und/oder Leistungskontrolle dienen, dürfen ausschließlich dazu verwendet werden, die Arbeitsvertragserfüllung zu sichern, Einsatzplanungen oder Einsatzsteuerungen vorzunehmen oder Qualifizierungsmaßnahmen daraus abzuleiten. Sie sind im Einzelfall und zur Erreichung des jeweiligen konkret bestimmten Zwecks zu verarbeiten. Über die besondere Zweckbestimmung sind die Betroffenen vorab zu informieren. Die Verarbeitung derartiger Daten ist einer Vorabkontrolle und Zustimmung durch den Betriebs-/Personalrat sowie den betrieblichen Datenschutzbeauftragten zu unterziehen. Änderungen bei der Verarbeitung von Kommunikationsdaten müssen allen Beschäftigten schriftlich mitgeteilt werden.

- bb) Die Erstellung von Leistungs- oder Verhaltensprofilen zur ständigen oder uneingeschränkten Überwachung der Beschäftigten ist unzulässig.
- cc) Die Erstellung von Bewegungsprofilen der Beschäftigten ist unzulässig.
- c) Nutzung von Telekommunikations- und Telemedieneinrichtungen
 - aa) Arbeitgeberinnen und Arbeitgeber sind verpflichtet, den Beschäftigten einen barrierefreien Zugang zu den digitalen Netzwerken des Unternehmens zu gewährleisten und Möglichkeiten der gewerkschaftlichen Präsenz sowie der Präsenz des betrieblichen Datenschutzbeauftragten in elektronischen Netzwerken auszubauen.

Beschäftigten, Personal- bzw. Betriebsräten und im Betrieb vertretenen Gewerkschaften sowie betrieblichen Datenschutzbeauftragten ist ein freier Zugang zu E-Mail-Systemen und Intranet der Unternehmen zu garantieren.
 - bb) E-Mails zwischen den Beschäftigten, auch solche mit nicht strikt geschäftlichem Inhalt, elektronische Rundschreiben des Betriebsrates und gewerkschaftliche Informationsbretter in Unternehmensnetzen sind zulässig.
- d) Überwachung des Kommunikationsverhaltens der Beschäftigten
 - aa) Die Erhebung, Speicherung, Veränderung, Übermittlung und Nutzung von Kommunikationsdaten sind an einen konkreten, im Voraus festgelegten Zweck zu binden und müssen zu den schutzwürdigen Interessen der Betroffenen in einem angemessenen Verhältnis stehen. Bezieht sich die Auswertung des Kommunikationsverhaltens auf bestimmte Arbeitnehmer, bedarf es eines besonderen Grundes, der den Betroffenen im Voraus schriftlich mitzuteilen ist. § 3a BDSG (Datenvermeidung und Datensparsamkeit) ist anzuwenden, soweit der Zweck der Verarbeitung von Kommunikationsdaten im Einzelfall eine Abweichung rechtfertigt.
 - bb) Die kurzfristige und angemessene Nutzung von Telekommunikations- und Telemedieneinrichtungen des Arbeitgebers durch Beschäftigte zu privaten Zwecken während der Arbeitszeit ist grundsätzlich zulässig. Das Nähere in Bezug auf zeitliche, örtliche und inhaltliche Nutzungsvorgaben ist in Betriebs- bzw. Personalvereinbarungen zu regeln.
 - cc) Der Einsatz von Software zur Aufzeichnung von Tastatureingaben (sogenannte Keylogger) oder Bildschirmaktivitäten (Screenshots und Ähnliches) zur automatisierten Kontrolle von Nutzungsverhalten und Leistung der Beschäftigten ist unzulässig.
 - dd) Daten über berufliche Kommunikationsvorgänge können Arbeitgeberinnen und Arbeitgeber von den Beschäftigten im Einzelfall oder in vorausbestimmten Fällen verlangen oder diese sind auf Aufforderung aktenkundig zu machen, soweit dies zur Dokumentation der Erbringung der vertraglichen Arbeitsleistung erforderlich ist.
 - ee) Die Kommunikation von Beschäftigten mit den betrieblichen Datenschutzbeauftragten sowie den Organen der betrieblichen Mitbestimmung ist überwachungsfrei zu garantieren.
- e) Überwachung mittels optoelektronischer Geräte in Unternehmen
 - aa) Die Überwachung einzelner Beschäftigter, ihrer Leistung oder ihres Verhaltens mittels optoelektronischer Geräte ist unzulässig. Sie kann auch nicht durch Vereinbarung mit Betriebs- oder Personalräten erlaubt werden.
 - bb) Erlaubt ist der Einsatz optoelektronischer Geräte einschließlich Videokameras, Webcams, Chipkarten, RFID-Chips und weiterer technischer

Systeme im Rahmen der Objektsicherung bestimmter Gebäude, Gebäudeteile oder vom Firmengelände. Die Zweckbestimmung des Einsatzes dieser Geräte ist schriftlich festzulegen und unterliegt der Mitbestimmung des Personal- bzw. Betriebsrates sowie der Zustimmung des betrieblichen Datenschutzbeauftragten.

- cc) Auf den Einsatz optoelektronischer Geräte ist durch entsprechende Hinweisschilder aufmerksam zu machen.
- dd) Die Verarbeitung von Daten aus einer Überwachung mittels optoelektronischer Geräte unterliegen einer strengen Zweckbindung. Der Zugriff auf diese Daten darf nur zur Aufklärung von Verstößen gegen die betriebliche Sicherheit oder von Eigentumsdelikten erfolgen. Die Daten sind spätestens nach sieben Tagen automatisiert zu löschen oder zu überschreiben. Dies ist zu protokollieren.
- ee) Zur Aufklärung von Straftaten ist die Übermittlung aufgezeichneter Daten aus der Überwachung mittels optoelektronischer Geräte an die Strafverfolgungsbehörden gestattet.

5. Betriebliche Datenschutzbeauftragte

- a) Betriebliche Datenschutzbeauftragte sind in öffentlichen und nichtöffentlichen Stellen zu bestellen, wenn eine gesetzlich festgelegte Mindestzahl von in der Regel fünf Beschäftigten erreicht wird.
- b) Die persönliche und sachliche Unabhängigkeit der betrieblichen Datenschutzbeauftragten ist besonders zu garantieren. Die Regelungen des § 4f BDSG sind dahingehend zu erweitern, dass der Datenschutzbeauftragte einem besonderen Kündigungsschutz gemäß § 103 BetrVG unterfällt. Für angestellte betriebliche Datenschutzbeauftragte und ihre Mitarbeiterinnen und Mitarbeiter ist außerdem eine Schutzvorschrift gemäß § 78 BetrVG vorzusehen. Wesentliche Störungen und Einflussnahmen auf die Tätigkeit des betrieblichen Datenschutzbeauftragten sind unter Strafe zu stellen.
- c) Bei der Bestellung und der Abberufung des betrieblichen Datenschutzbeauftragten hat der Betriebsrat ein Mitbestimmungsrecht. Der betriebliche Datenschutzbeauftragte hat einen Nachweis seiner Fachkunde zu erbringen. Betriebliche Datenschutzbeauftragte und Betriebs- bzw. Personalräte konsultieren und informieren sich im Rahmen ihrer Aufgaben gegenseitig.
- d) Betriebliche Datenschutzbeauftragte erstellen jährlich einen Bericht über den Schutz der Daten von Beschäftigten in ihrem Zuständigkeitsbereich und veröffentlichen diesen betriebsintern.

6. Betriebs- und Personalräte

- a) Betriebs- und Personalräte sind Teil der datenverarbeitenden Stelle und haben die gleichen Mitbestimmungs-, Auskunfts- und Informationsansprüche wie die betrieblichen Datenschutzbeauftragten.
- b) Betriebs- und Personalräte dürfen im Rahmen ihrer Aufgaben personenbezogene Daten von Beschäftigten verarbeiten. Sie unterliegen dabei der Aufsicht der entsprechenden Aufsichtsbehörde (in der Regel dem Landesdatenschutzbeauftragten).
- c) Arbeitgeberinnen und Arbeitgeber sind gegenüber Betriebs- und Personalräten zur Herausgabe der Daten von Beschäftigten verpflichtet.

7. Aufsichtsbehörden

Die für die Kontrolle des Datenschutzes zuständigen Aufsichtsbehörden der Länder sind unabhängige Institutionen. Sie kontrollieren die Ausführung und

Einhaltung des Gesetzes zum Schutz der Daten von Beschäftigten. Sie beraten die betrieblichen Datenschutzbeauftragten und die verantwortlichen Stellen bei der Anwendung des Gesetzes.

8. Schiedsstellen für den Schutz der Daten von Beschäftigten

- a) Zur Klärung von Streitfragen in Bezug auf den Schutz von Daten von Arbeitnehmerinnen und Arbeitnehmern kann eine paritätisch von Arbeitgeberinnen und Arbeitgebern sowie Gewerkschaften mit Beisitzerinnen und Beisetzern bestellte Schiedsstelle analog zur Einigungsstelle gemäß dem Betriebsverfassungsgesetz eingerichtet werden. Das Schiedsstellenverfahren ist analog dem im BetrVG festgelegten Einigungsstellenverfahren zu regeln.
- b) Die Schiedsstelle kann angerufen werden, wenn zu Fragen des Persönlichkeitsrechtsschutzes zwischen Arbeitgeberinnen und Arbeitgebern sowie betrieblicher Interessenvertretung unter Einbeziehung der oder des betrieblichen Datenschutzbeauftragten keine Einigung erzielt werden kann. Das Recht der Betroffenen, sich unmittelbar an die Aufsichtsbehörde für den Datenschutz zu wenden, bleibt davon unberührt.

9. Schadenersatz und Sanktionen

- a) Erleiden Beschäftigte durch eine nach dem Gesetz zum Schutz der Daten von Beschäftigten unzulässige oder unrichtige Datenverarbeitung ihrer personenbezogenen Daten einen materiellen oder immateriellen Schaden, ist die verantwortliche Stelle zum Schadenersatz verpflichtet. Es obliegt der verantwortlichen Stelle oder der in ihrem Auftrag handelnden Person, nachzuweisen, dass sie die gebotene Sorgfalt bei der Datenverarbeitung eingehalten hat.

Die Geltendmachung von Ersatzansprüchen nach anderen Rechtsgrundlagen wie beispielsweise nach § 823 des Bürgerlichen Gesetzbuchs sowie den §§ 7 und 8 BDSG und § 15 des Allgemeinen Gleichbehandlungsgesetzes (AGG) bleibt davon unberührt.

- b) Verstöße gegen die Bestimmungen dieses Gesetzes sind – soweit sie nicht vorsätzlich, in schädigender Absicht oder gegen Entgelt begangen werden – als Ordnungswidrigkeiten zu ahnden. Ordnungswidrig handelt insbesondere, wer fahrlässig
 1. ohne gesetzliche Grundlage Daten von Beschäftigten erhebt, speichert, verändert, übermittelt oder nutzt,
 2. Daten zusammenführt, die zu unterschiedlichen Zwecken erhoben wurden,
 3. dem berechtigten Verlangen der Beschäftigten nach Auskunft, Berichtigung, Sperrung oder Löschung nicht unverzüglich nachkommt,
 4. Beschäftigtendaten ins Ausland übermittelt ohne die EU-Standardvertragsklauseln zu verwenden oder die Regelungen des § 4c Absatz 2 BDSG einzuhalten,
 5. Fotos von Beschäftigten verwendet ohne dass eine gesetzliche Grundlage für die Verwendung existiert,
 6. Verfahren, die der Vorabkontrolle gemäß dem Gesetz zum Schutz der Daten von Beschäftigten unterliegen, ohne diese Vorabkontrolle anwendet.

- c) Das Handeln des Leiters der verantwortlichen Stelle ist ebenfalls als Ordnungswidrigkeit zu verfolgen, wenn er eine Handlung nach Buchstabe b zwar nicht selbsttätig ausführt, jedoch sorgfaltspflichtwidrig deren Ausführung durch andere Personen veranlasst oder duldet.
- d) Ordnungswidrigkeiten können mit einer Geldbuße von bis zu zwei Mio. Euro geahndet werden.
- e) Die Regelungen der §§ 43 und 44 BDSG bleiben unberührt.
- f) Wer vorsätzlich, in schädigender Absicht oder gegen Entgelt gegen die Bestimmungen des Gesetzes zum Schutz der Daten von Beschäftigten verstößt, wird mit Freiheitsstrafe von bis zu zwei Jahren oder mit Geldstrafe bestraft.

Berlin, den 23. Februar 2010

Dr. Gregor Gysi und Fraktion

