Deutscher Bundestag **Drucksache 16/12670**

16. Wahlperiode 22. 04. 2009

Antrag

der Abgeordneten Gisela Piltz, Dr. Heinrich L. Kolb, Jens Ackermann, Dr. Karl Addicks, Christian Ahrendt, Uwe Barth, Rainer Brüderle, Angelika Brunkhorst, Ernst Burgbacher, Patrick Döring, Mechthild Dyckmans, Jörg van Essen, Ulrike Flach, Horst Friedrich (Bayreuth), Hans-Michael Goldmann, Miriam Gruß, Joachim Günther (Plauen), Dr. Christel Happach-Kasan, Heinz-Peter Haustein, Elke Hoff, Birgit Homburger, Gudrun Kopp, Jürgen Koppelin, Heinz Lanfermann, Harald Leibrecht, Ina Lenke, Sabine Leutheusser-Schnarrenberger, Michael Link (Heilbronn), Dr. Erwin Lotter, Horst Meierhofer, Patrick Meinhardt, Jan Mücke, Burkhardt Müller-Sönksen, Dirk Niebel, Hans-Joachim Otto (Frankfurt), Detlef Parr, Cornelia Pieper, Frank Schäffler, Dr. Konrad Schily, Marina Schuster, Dr. Hermann Otto Solms, Dr. Max Stadler, Carl-Ludwig Thiele, Florian Toncar, Christoph Waitz, Dr. Claudia Winterstein, Dr. Volker Wissing, Hartfrid Wolff (Rems-Murr), Dr. Guido Westerwelle und der Fraktion der FDP

Schutz von Arbeitnehmerdaten durch transparente und praxisgerechte Regelungen gesetzlich absichern

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

1. Der Schutz von Arbeitnehmerdaten ist unzureichend gesetzlich geregelt. Während eines Beschäftigungsverhältnisses sammeln sich umfangreiche personenbezogene Daten der Mitarbeiterinnen und Mitarbeiter an, deren Verarbeitung in ganz überwiegendem Maße in automatisierter Form erfolgt. Die Bewertung dieser Sachverhalte anhand der geltenden landes- und bundesdatenschutzrechtlichen Vorschriften erweist sich dabei oftmals als schwierig und unübersichtlich. Sowohl Arbeitgeber als auch Arbeitnehmer werden auf eine Analyse der bestehenden Rechtsprechung verwiesen, die indes regelmäßig einzelfallbezogen ist und allenfalls von einem kleinen Expertenkreis überblickt wird.
2. Zwischen Arbeitnehmern und Arbeitgebern besteht oftmals kein gleichberechtigtes Verhältnis. Arbeitnehmer machen nicht selten wegen der mangelnden Kenntnis der Rechtslage von den ihnen bereits jetzt bei Verstößen gegen datenschutzrechtliche Bestimmungen zur Verfügung stehenden Möglichkeiten keinen Gebrauch. Darüber hinaus droht die Situation einzutreten, dass Arbeitnehmer aus Angst vor Nachteilen oder gar dem Verlust des Arbeitsplatzes auf die Geltendmachung eigener Rechte bewusst verzichten.
3. Nur ein umfassendes Arbeitnehmerdatenschutzrecht wird dem Schutz der Persönlichkeitsrechte der Arbeitnehmer gerecht. Die Ausgestaltung der Rahmenbedingungen gerade eines so vielgestaltigen Themenbereiches der Judikatur zu überlassen, ist als der falsche Weg. Ein gesetzgeberisches Handeln ist längst überfällig.

4. Die Daten müssen grundsätzlich beim Betroffenen erhoben werden. Hinsichtlich der zulässigen Fragen an Bewerber ist die geltende Rechtslage ausreichend. Unzulässige Fragen dürfen schon jetzt weder dokumentiert noch gegenüber den Betroffenen oder Dritten durch den potentiellen Arbeitgeber verwendet werden. Öffentlich zugängliche Daten über den Bewerber können zur Kenntnis genommen werden (Erlangung von Spezialkenntnissen auch durch Nutzung von Angeboten, die einer Registrierung bedürfen, wie z. B. XING). Das Verbot der automatisierten Einzelentscheidung (bisher § 6a des Bundesdatenschutzgesetzes – BDSG), das insbesondere bei psychologischen Auswahltests eine Rolle spielen kann, soll auch in Arbeitsverhältnissen und bei ihrer Begründung gelten.
5. Bei gefahrgeneigter Tätigkeit soll es zum Schutz Dritter, des Arbeitgebers und des Arbeitnehmers selbst möglich sein, regelmäßige Untersuchungen durchzuführen. Diese Untersuchungen sollen allerdings nur möglich sein, wenn sie für die Eignung, die Tätigkeit auszuüben, zwingend notwendig sind (z. B. Alkoholtest bei Lkw-Fahrern). Untersuchungen, die keine Aussage zur Leistungsfähigkeit des Arbeitnehmers bzgl. der konkreten Tätigkeit zulassen, dürfen nicht vorgenommen werden. Gentests oder Fragen zu genetischen Dispositionen sollen ausgeschlossen werden.
6. Bewerbungsunterlagen sind dem Bewerber zurückzusenden und die Bewerberdaten zu löschen. Im Falle einer erfolglosen Bewerbung dürfen Daten nur so lange aufbewahrt werden, wie dies rechtlich geboten ist, z. B. im Hinblick auf die Anforderungen des Allgemeinen Gleichbehandlungsgesetzes (AGG). Wird eine längere Aufbewahrung seitens des Arbeitgebers gewünscht, setzt dies das Einverständnis des Bewerbers voraus.
7. Zur Personalakte gehören alle Unterlagen und Vorgänge, die in einem unmittelbaren inneren Zusammenhang mit dem Beschäftigungsverhältnis des Mitarbeiters stehen. Zur Personalakte gehören daher auch alle schriftlichen Aufzeichnungen, die sich mit der Person des Arbeitnehmers und dem Inhalt und Verlauf seines Beschäftigungsverhältnisses befassen. Es ist dabei nicht entscheidend, wo, in welcher Form und unter welcher Bezeichnung die Daten gespeichert sind. Demjenigen, der Personalentscheidungen zu treffen hat, stehen die für eine sachgerechte Entscheidung erforderlichen Unterlagen zur Verfügung. Der Kreis der Zugriffsberechtigten ist so klein wie möglich zu halten. Bei elektronischer Aktenführung muss die Zugriffsberechtigung geregelt werden. Betriebsräte haben nur mit Zustimmung des Betroffenen Einsicht in die Personalakte. Auf Stammdaten können der Dienstvorgesetzte und der Betriebsrat zugreifen. In die Personalakte dürfen nur korrekte Informationen/Daten aufgenommen werden. Andernfalls stehen dem Betroffenen gegen die entsprechenden Inhalte/Daten unabhängig von der Art der Verarbeitung neben dem bestehenden arbeitsrechtrechtlichen Anspruch auf Gegendarstellung, Abwehrrechte nach dem BDSG (Löschung, Berichtigung, Auskunft, Sperrung) zur Verfügung. Dem Betroffenen ist Gelegenheit zur Stellungnahme zu geben.
8. Die Übermittlung von Arbeitnehmerdaten an Dritte ist ohne Einwilligung des betroffenen Mitarbeiters nur dann zulässig, wenn ein „gravierendes Interesse“ an der Durchbrechung des Grundsatzes der Vertraulichkeit besteht. Ein solches gravierendes Interesse kann z. B. bei Unternehmensverkäufen bestehen. Bei einem Unternehmensverkauf mit „Due Diligence Prüfungen“ dürfen Daten nur anonymisiert weitergegeben werden. Daten von Angestellten im Sinne des § 5 Absatz 2 bis 4 des Betriebsverfassungsgesetzes (BetrVG) dürfen jedoch weiter gegeben werden. Ein europaweites Konzernprivileg ist grundsätzlich möglich. Über Europa hinaus soll ein Konzernprivileg nur dann möglich sein, wenn ein vergleichbares Datenschutzniveau besteht und die Rechte des Betriebsrates, die Einhaltung der gesetzlichen Voraussetzungen zu prüfen, erhalten bleiben.

9. Biometrische Daten dürfen nur zu dem Zweck verwendet werden, für den sie ursprünglich erhoben wurden. Zweckänderungen sind unzulässig. Zugangskontrollen sollen grundsätzlich nur der Identitäts- und Anwesenheitskontrolle dienen. Die Arbeitnehmer müssen darüber informiert werden, welche Daten gespeichert werden. Lösungen, bei denen die gespeicherten Referenzdaten unter der alleinigen Kontrolle der Betroffenen stehen und ausschließlich zum Vergleich verarbeitet werden (datensparsame Templates), sind vorzuziehen. Nichtdiskriminierende Ausweichmöglichkeiten sind grundsätzlich vorzusehen, da ein ausnahmsloser Benutzerzwang gegen das Recht auf informationelle Selbstbestimmung verstoßen kann. Insbesondere lassen sich grundsätzlich biometrische Verfahren, die der Verifikation dienen, mit einer dezentralen Datenspeicherung betreiben (1:1 Abgleich). Es müssen detaillierte Zugriffskonzepte geschaffen werden, um eine zweckwidrige Nutzung zu vermeiden und die Daten vor unberechtigtem Zugriff und vor Diebstahl zu schützen. Eine Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten ist zu etablieren. Biometrische Daten sollen innerhalb festgesetzter Fristen gelöscht werden und deren Löschung muss überprüfbar sein.

10. Neben dem im Einzelfall berechtigten Einsatz spezieller Überwachungssystem dürfen Videoüberwachungssysteme oder andere permanente technische Systeme mit vergleichbarer Eingriffsintensität (RFID, GPS) nicht zu Zwecken der Leistungs- und Verhaltenskontrolle, zum Leistungsvergleich oder zur Leistungsbemessung eingesetzt werden. Dies gilt insbesondere für Verfahren des Data Minings oder Screenings. Die Überwachung von Produktionsabläufen zur Einhaltung gewerblicher Auflagen sowie von Kassen und sonstigen öffentlich zugänglichen Geschäftsbereichen soll möglich bleiben. Vor dem Einsatz von Videoüberwachung ist eine Vorabkontrolle des Systems durch den betrieblichen Datenschutzbeauftragten durchzuführen. Die Überwachung von einzelnen Beschäftigten mittels Videoüberwachung und Aufzeichnungssystemen ist grundsätzlich untersagt, ebenso wie eine Videoüberwachung, die die Intimsphäre der Arbeitnehmer verletzt (z. B. Toilette und Umkleidekabinen). Auswertungen von Videoaufzeichnungen dürfen bei konkretem Anlass zur Aufklärung oder Verhinderung von Straftaten genutzt werden und sind zu protokollieren. Heimliche Videoüberwachungen sind grundsätzlich nicht gestattet. Aufzeichnungen sind unverzüglich zu löschen, wenn sie nicht mehr erforderlich sind oder schutzwürdige Interessen der Beschäftigten entgegenstehen. Darüber hinaus dürfen unzulässige Videoaufzeichnungen nicht gegen den Betroffenen verwendet werden.

11. Der Arbeitgeber ist nicht verpflichtet, in die private Nutzung von E-Mails, Internet und Telefon einzuwilligen oder diese als sozialadäquates Verhalten zu dulden. Auch bei dienstlicher Nutzung von z. B. E-Mail, Internet oder Telefon ist eine Auswertung, die die systematische Kontrolle des Beschäftigten zum Ziel hat, unzulässig. Möglich sind lediglich stichprobenhafte und zeitnahe Auswertungen zu Protokolldaten. Dabei ist ein transparentes Verfahren sicherzustellen und die Straf- und Ordnungswidrigkeitsvorschriften sind entsprechend anzupassen. Die Arbeitnehmer sind über die Inhalte und Details von Protokolldaten zu informieren, Löschungsfristen sind vorzusehen. Eine technische Überwachung des digitalen Arbeitsplatzes ohne Kenntnis der Arbeitnehmer darf grundsätzlich nicht durchgeführt werden. Soweit der Arbeitgeber die private Nutzung von Informations- und Kommunikationstechnik gestattet, hat er für den Schutz der Privatsphäre des Arbeitnehmers Sorge zu tragen.

12. Der Betriebsrat muss datenschutzrechtliche Belange der Arbeitnehmerinnen und Arbeitnehmer wahrnehmen können. Dies gilt insbesondere vor dem Hintergrund des bestehenden Abhängigkeitsverhältnisses zwischen Arbeitnehmer und Arbeitgeber, das nicht zu einer „datenschutzrechtlichen Abhän-

gigkeit“ des Arbeitnehmers führen darf, z. B. diesen zur Zustimmung zu Erhebung, Nutzung und Verarbeitung von Daten zu bewegen. Die Mitbestimmungsregeln zugunsten des Betriebsrates dürfen nicht dazu führen, dass der einzelne Arbeitnehmer übergangen wird, z. B. wenn es um die Zustimmung zu Überwachungsmaßnahmen geht. Das Allgemeine Persönlichkeitsrecht ist ein höchstpersönliches Rechtsgut und darf nicht der alleinigen Disposition eines Kollektivorgans unterworfen werden. Eine formalisierte Informationspflicht des Arbeitgebers gegenüber den Betriebsräten im Hinblick auf Arbeitnehmerdatenverarbeitung außerhalb der Personalverwaltung ist zu etablieren. Die Beachtung datenschutzrechtlicher Bestimmungen und die Sanktionierung von etwaigen Verstößen muss auch in Betrieben sichergestellt werden, die nicht über einen Betriebsrat verfügen. An die Verletzung der Unterrichtungspflicht an den betrieblichen Datenschutzbeauftragten muss eine unmittelbare Rechtsfolge geknüpft sein. Transparenz im Mitbestimmungsrecht soll gefördert werden, wobei eine unnötige Behinderung des Produktivgeschäftes vermieden werden sollte. Eine Informationspflicht für den Fall der Datenverarbeitung im Auftrag, auch im Bereich der Personalverwaltung, ist zu etablieren.

13. Soweit Daten der Arbeitnehmer nicht mehr zur Sicherung von Rechtspositionen benötigt werden, sind diese umgehend und umfassend zu löschen. Dem ausgeschiedenen Arbeitnehmer muss die Möglichkeit eröffnet werden, den Löschvorgang einzusehen und nachzuvollziehen. Soweit gesetzliche oder vertragliche Vorgaben eine umgehende Löschung verbieten, sind die verbleibenden Daten nur für diese konkreten Vorgaben zu verwenden. Eine anderweitige Nutzung ist ausgeschlossen. Nach Ablauf der Aufbewahrungsfristen sind vorhandene Unterlagen einer ordnungsgemäßen Entsorgung (nach DIN 32757 Stufe 3) zuzuführen. Die Entsorgung ist zu dokumentieren. Die Verarbeitung gesperrter personenbezogener Daten ist grundsätzlich untersagt.

14. Soweit keine besonderen Bestimmungen für den Arbeitnehmerdatenschutz getroffen werden, gelten die Bestimmungen des BDSG und des BetrVG.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. unter Berücksichtigung der vorgenannten Erwägungen einen Gesetzentwurf für ein umfassendes und transparentes Arbeitnehmerdatenschutzrecht vorzulegen, der insbesondere der Zielsetzung einer einfachen und anwenderfreundlichen Handhabung für die Arbeitnehmerinnen und Arbeitnehmer gerecht wird;

2. das Datenschutzniveau im Geltungsbereich des öffentlichen Dienstrechts anhand der vorgenannten Grundsätze und unter Berücksichtigung der dort geltenden Besonderheiten zu überprüfen, und, sofern erforderlich, auch insoweit gesetzliche Regelungsvorschläge vorzulegen.

Berlin, den 21. April 2009

Dr. Guido Westerwelle und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333