Deutscher Bundestag **Drucksache 16/10216**

16. Wahlperiode 12. 09. 2008

Antrag

der Abgeordneten Silke Stokar von Neuforn, Volker Beck (Köln), Birgitt Bender, Cornelia Behm, Alexander Bonde, Hans-Josef Fell, Britta Haßelmann, Ulrike Höfken, Renate Künast, Fritz Kuhn, Markus Kurth, Monika Lazar, Nicole Maisch, Jerzy Montag, Brigitte Pothmer, Christine Scheel, Dr. Gerhard Schick, Dr. Wolfgang Strengmann-Kuhn, Dr. Harald Terpe, Wolfgang Wieland, Josef Philip Winkler und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Datenschutz stärken – Bewusstsein schaffen – Datenmissbrauch vorbeugen

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag fordert die Bundesregierung auf, einen Gesetzentwurf vorzulegen, der folgende Regelungen umfasst:

1. Grundlegende Modernisierung des Bundesdatenschutzgesetzes

Im Datenschutz muss das Prinzip gelten „Meine Daten gehören mir“. Das Bundesdatenschutzgesetz (BDSG) muss künftig angemessen der Tatsache Rechnung tragen, dass die Privatwirtschaft mittlerweile der größte Datensammler ist und dass der Staat den Schutz des Einzelnen auch gegenüber privaten Unternehmen zu gewährleisten hat. Das Bundesdatenschutzgesetz ist grundlegend zu modernisieren und im Sinne der nachfolgenden Punkte neu auszurichten.

2. Stärkung des Grundrechts auf informationelle Selbstbestimmung im BDSG

Wer informationelle Selbstbestimmung stärken will, darf das Grundrecht nicht durch immer neue Ausnahmeregelungen aushöhlen. Künftig sollen daher weniger bereichspezifische Regelungen in Sondergesetzen außerhalb des BDSG geschaffen werden. Das BDSG selbst soll vielmehr zu einem allgemeinen Datenschutzgesetzbuch weiter entwickelt werden. Grundsätzlich gelten für alle die gleichen Rechte und Pflichten. Auch innerhalb des BDGS sollen nur dort Sondervorschriften geschaffen werden, wo sie zu Gunsten besonders schutzbedürftiger Gruppen erforderlich sind, beispielsweise im Arbeitnehmerdatenschutz oder im Verbraucherdatenschutz.

3. Sensible Daten besser schützen – Geo-Scoring verbieten

Sensible Daten sind im Interesse der betroffenen Menschen besonders zu schützen. Aber auch bei anderen Daten besteht durch ihre Kombination die Gefahr, dass Betroffene diskriminiert werden. Wenn beispielsweise bei der Überprüfung der Kreditwürdigkeit – wie im Regierungsentwurf zur Novellierung vorgesehen – an verhaltensunabhängige (Geo-)Daten wie die Adressdaten angeknüpft wird, hat dieses eine verheerende Wirkung für das soziale Zusammenleben. Die Nutzung dieser Geodaten beim sog. Kreditscoring führt zu Ausgrenzung und Sippenhaft – Geoscoring ist zu verbieten.

4. Einwilligung stärken – Kopplungsverbote einführen

Der Grundsatz „Meine Daten gehören mir“ wird dort eingehalten, wo der Betroffene wirksam eingewilligt hat. Dieser Grundsatz wurde in der Vergangenheit durch zahlreiche gesetzliche Erlaubnisse ausgehöhlt. Künftig muss die ausdrückliche Einwilligung wieder zur Regel, die gesetzliche Erlaubnis die Ausnahme werden. Den Betroffenen ist keine stillschweigende bzw. mutmaßliche Einwilligung zu unterstellen; es darf nicht zu sog. Scheineinwilligungen kommen. Firmen dürfen es nicht mehr zur Bedingung eines Vertragsschlusses machen, dass die Kunden der Nutzung ihrer Daten zustimmen, obwohl es für den Vertragsschluss gar nicht erforderlich ist. Hierzu sind sogenannte Kopplungsverbote einzuführen, wie es sie wenigstens im Ansatz bereits im Telemediengesetz oder im Telekommunikationsgesetz gibt. Wird der Betroffene über den Zweck der Datenerhebung getäuscht oder nicht aufgeklärt, wie etwa bei bestimmten Preisausschreiben oder Glücksspielen, so ist dies sittenwidrig und muss klar sanktioniert werden. Immer muss diese Einwilligung widerruflich bleiben.

5. Datenhandel grundsätzlich verbieten – „Opt-In“ einführen

Der Handel mit persönlichen Daten anderer ist grundsätzlich zu beschränken – und bei sensiblen Daten ganz zu verbieten. Daten Dritter sollen künftig nur noch dann gehandelt werden dürfen, wenn der Betroffene in diesen Handel ausdrücklich eingewilligt hat. Hier ist das derzeitige Regel-Ausnahme-Verhältnis zwischen Erlaubnis und Einwilligung ebenfalls auf den Prüfstand zu stellen. Künftig sollen Verbraucherinnen und Verbraucher nicht länger die Notbremse des „Opt-Out“ ziehen müssen, um Datenklau gerade noch zu verhindern. Stattdessen soll der Grundsatz der ausdrücklichen Einwilligung (Opt-In) auch im Datenschutzgesetz eingeführt werden. Dabei ist eine informierte Einwilligung zu fordern, d. h. der Erwerber muss vorher aufgeklärt haben, wofür er die Daten haben will.

6. Stärkung der Auskunfts- und Informationsrechte der Betroffenen

Bürgerinnen und Bürger sollen künftig wissen, wer über ihre Daten verfügt. Der Datenweg muss nachvollziehbar werden. Die Betroffenen sind grundsätzlich automatisch von einer Datenweitergabe zu benachrichtigen, und die Daten müssen mit einer Herkunftskennzeichnung versehen werden. Im Fokus stehen hier Auskunfteien, die anhand sog. Scoring-Verfahren die Kreditwürdigkeit von Verbraucherinnen und Verbraucher bewerten. Betroffene sollen in Zukunft automatisch informiert werden, wenn ihre Daten zu einem Datenprodukt mit Werturteil (z. B. Scorewert) verarbeitet werden sowie wenn dieser Scorewert weitergegeben wird. Verbraucherinnen und Verbraucher sollen nicht nur – wie im Regierungsentwurf zur Novellierung vorgesehen – einmal jährlich eine kostenlose Selbstauskunft über ihre Scorewerte erhalten können. Branchenübergreifende Auskunftssysteme sind zu begrenzen und die Auskunfteitätigkeit ist auf relevante Informationen zu Zahlungsverhalten, Einkommens- und Vermögensverhältnisse zu beschränken. Damit jeder selbst überprüfen kann, welche Unternehmen Daten über ihn zusammenstellen, ist ein Portal zu schaffen, das als Wegweiser zu allen Auskunfteien dient. Auf diesem Bürgerportal muss es allein den Betroffenen möglich sein, mit einem Mausklick alle Informationen darüber zu erhalten, was über sie gespeichert ist.

7. Datenschutzaudit - Gütesiegel im Datenschutz einführen

Wo Datenschutz draufsteht, muss künftig auch Datenschutz drin sein. Das „Datenschutzaudit“ soll mit einem Gütesiegel Verbraucherinnen und Verbraucher in die Lage versetzen, sich selbst ein besseres Bild über den Datenschutzstandard eines Unternehmens machen zu können. Und Unternehmen

können nach zahlreichen Datenschutzskandalen verlorenes Vertrauen zurückgewinnen. Datenschutzaudit ist ein Schlüssel für die positive Entwicklung des elektronischen Handels.

8. Sorgfaltspflichten und neue Verbraucherrechte

Sorgfaltspflichten der Unternehmen beim Umgang mit Kundendaten sind neu zu definieren. Unternehmen müssen Verstöße und Datenpannen melden. Banken müssen mehr kritisches Bewusstsein und stichprobenartige Plausibilitätsprüfungen beim Einzugsverfahren entwickeln. Kundinnen und Kunden sind bei Hinweisen auf illegale Abbuchungen umgehend zu informieren – insbesondere, wenn bereits Beschwerden über nicht genehmigte Bankeinzüge vorliegen. Bei Verdacht auf Straftaten ist auch die Staatsanwaltschaft zu informieren. Zumindest bei der ersten Abbuchung sollte sich das Kreditinstitut vergewissern, dass eine Einzugsermächtigung tatsächlich vorliegt. Werden Daten dennoch erschwindelt, sollen die Betroffenen künftig bei den betreffenden Unternehmen einen Auskunftsanspruch geltend machen können, damit die Datenweiterleitungskette komplett zurückverfolgt und die Daten überall gelöscht werden.

9. Gewinne abschöpfen, Sanktionen verschärfen

Unternehmen, die Verstöße gegen Datenschutzregelungen bewusst in Kauf nehmen, um Kasse zu machen, sollen diesen Gewinn nicht länger behalten dürfen. Ähnlich wie im Wettbewerbs- und Kartellrecht ist der Gewinn abzuschöpfen, und zwar auch bei Fahrlässigkeit. Bisher sind Verstöße gegen die §§ 28, 29 BDGS in der Regel allenfalls Ordnungswidrigkeiten. Nur wenige Verstöße können bisher mit dem maximalen Ordnungsgeld von bis zu 250 000 Euro geahndet werden – die besonders praxisrelevanten Verstöße des § 43 Abs. 1 BDSG haben nur ein maximales Bußgeld von 25 000 Euro. Das ist angesichts der wachsenden Bedeutung der Datenhighways und des Datenhandels nicht länger akzeptabel. Der Bußgeldkatalog ist insgesamt transparenter zu gestalten und der Bußgeldrahmen muss an der Leistungsfähigkeit des Unternehmens orientiert werden. Schwerste Verstöße müssen auch strafrechtlich sanktioniert werden.

10. Kontrollinstanzen stärken

Die Unabhängigkeit und Kompetenz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sind gesetzlich zu stärken.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,
weitere flankierende Maßnahmen zur Stärkung des Datenschutzes zu ergreifen:

1. Finanzielle Ausstattung verbessern

Neben der Änderung weiterer Bundesgesetze ist es erforderlich, den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit organisatorisch und personell besser auszustatten.

2. Illegale Praktiken aufdecken, Verbandsklage einführen

Heimlichem Datenklau unter Vorspiegelung falscher Tatsachen ist präventiv zu begegnen. Ein schriftliches Widerrufsrecht genügt dabei nicht. Vertragsabschlüsse, die durch unerlaubtes Telefonmarketing oder rechtswidrige Datennutzung angebahnt wurden, bedürfen einer nochmaligen Bestätigung. Unerwarteten Überrumpelungssituationen wird so entgegengewirkt. Anerkannte Verbraucherverbände sollten bei Datenschutzverstößen künftig das Recht der Verbandsklage erhalten, um illegale Praktiken frühzeitig aufzudecken.

3. Bund-Länder-Kooperation verbessern

Auf die Länder soll eingewirkt werden, die dortigen Datenschutzbeauftragten ebenfalls organisatorisch und personell besser auszustatten, genauso die Ermittlungsbehörden. Weiterer Missbrauch mit den bereits umlaufenden Datenmengen ist dadurch zu begrenzen, dass noch stärker als bisher ermittelt wird. Wir brauchen Schwerpunktstaatsanwaltschaften und wir brauchen eine regelmäßige Zusammenarbeit von Strafverfolgung und Datenschützern, ähnlich wie bei der institutionalisierten Vernetzung von Strafverfolgung und Gewerbeaufsicht. Nur so können bei der Strafverfolgung von Datenmissbrauch Schwachstellen bereits frühzeitig erkannt werden.

4. Staat als Vorbild – Mehr Datensparsamkeit

Wenn der IT-Sektor im Datenbereich staatlich reguliert wird, dann muss der Staat dabei mit gutem Beispiel vorangehen. Die Bundesregierung ist aufgefordert, den staatlichen Umgang mit Daten an folgenden Grundsätzen zu orientieren:

- Datensparsamkeit und Zweckbindung müssen nicht nur das Gebot der Stunde, sondern selbstverständlicher Standard sein, immer und überall.
- Das Gleiche gilt für die Verschlüsselung von Daten.
- Der Staat muss selbst grundsätzlich darauf verzichten, Daten auf Vorrat zu speichern und er darf erst recht nicht private Unternehmen dazu anhalten – wie zum Beispiel im Telekommunikationsbereich – auf Vorrat zu speichern, sonst wird der Anlass für künftige Begehrlichkeiten geschaffen.
- Sofern der Staat Daten speichern muss, sind die Informationsrechte Betroffener zu stärken und die Auskunftsrechte Dritter stärker einzuschränken. Auch hier muss der Grundsatz gelten keine Weitergabe ohne Einwilligung.
- Zentrale Datenbanken gehören auf den Prüfstand, erst recht neue Datenbanken wie das Bundesmelderegister. Bei der bevorstehenden Schaffung des Bundesmeldegesetzes sind die vorhandenen Auskunftsrechte Dritter weitestgehend zu beschränken. Betroffene sollen ein Widerspruchsrecht haben. Die Weitergabe von Meldedaten darf keine weitere Grundlage für illegalen Datenhandel legen.

Berlin, den 12. September 2008

Renate Künast, Fritz Kuhn und Fraktion

Begründung

Eine Kette von Datenschutzskandalen und Affären hat der Bevölkerung vor Augen geführt, wie schlecht es derzeit um den Schutz ihrer persönlichen Daten in Deutschland bestellt ist. Diese Daten künftig besser zu schützen, auch gegenüber privaten Unternehmen, ist die Aufgabe des Parlaments.

Die Ursprünge des jetzigen BDSG liegen im Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahre 1983. Damals waren in vielen Behörden und Unternehmen noch Karteikarten weiter verbreitet, die Informationstechnologie steckte in den Kinderschuhen. Die Geschäftswelt und der Alltag haben sich durch neue Technologien seitdem sprunghaft weiter entwickelt. Die Summe der verfügbaren Daten hat sich potenziert – und die Gefahr ihres Missbrauchs ebenfalls.

Der Gesetzgeber hat mit dieser technologischen Entwicklung bisher überhaupt nicht Schritt gehalten. Das BDSG ist nicht mehr auf der Höhe der Zeit. Die ohnehin anstehende Datenschutznovelle bietet nun die Chance, das BDSG nicht nur im Bereich der Auskunfteien zu ergänzen, sondern den Datenschutz insgesamt zu modernisieren – und den notwendigen Schutz der Bürgerinnen und Bürger endlich sicherzustellen.

Die Fraktion BÜNDNIS 90/DIE GRÜNEN hat bereits einen Gesetzentwurf zur Aufnahme des Datenschutzes in das Grundgesetz vorgelegt (vgl. Bundestagsdrucksache 16/9607). Durch das Grundgesetz sollen Behörden und Gerichte, aber auch das Parlament in Zukunft verpflichtet werden, die Grundsätze der Datensparsamkeit und Zweckbindung besser einzuhalten und Datenpannen vorzubeugen. Parallel dazu schlägt dieser Antrag umfangreiche Änderungen am BDSG vor, verbunden mit einem Maßnahmekatalog zur Stärkung des Datenschutzes.

Die technologische Entwicklung in der Informationsgesellschaft hat in den vergangenen Jahren die Arbeitsabläufe rasant verändert. Die Informationstechnologie wird nicht nur zur Kontrolle und Überwachung der Arbeitnehmerinnen und Arbeitnehmer eingesetzt, vielmehr werden auch die Kundendaten zur begehrten Handelsware. Die Skandale bei der Überwachung im Einzelhandel, die Bespitzelung von Aufsichtsräten und Gewerkschaftsmitgliedern, die Datenpannen bei Meldebehörden oder Datenklau und Datenmissbrauch beim Datenhandel – das ist bisher nur die Spitze des Eisberges.

Verbraucherinnen und Verbraucher, die ihre Einkäufe zunehmend online und mit bargeldlosen Zahlungsmitteln erledigen, werden zum Objekt der Marktforschung. Die verwendete Speicherungs- und Verarbeitungskapazität für die Kundendaten waren noch um die Jahrtausendwende kaum vorstellbar. Für viele Unternehmen, beispielsweise für Auskunfteien wie die Schufa, sind diese Kundendaten längst die eigentliche Geschäftsgrundlage. Um Auskünfte über die Kreditwürdigkeit anderer liefern zu können, werden sog. Scoring-Werte erstellt. Weitere Informationen werden den Verbraucherinnen und Verbrauchern durch Meinungsumfragen, Glücksspiele oder Kundenkartenprogramme wie Payback oder HappyDigits entlockt. In sog. sozialen Netzwerken wie StudiVZ oder Xing tauschen die Beteiligten auch in ihrer Freizeit private Daten ganz bewusst und öffentlich, gleichzeitig wird auch ihr individuelles Surfverhalten im Internet durch Softwareanbieter erfasst. Erfasst wird auch, wer wohin Flugzeuge, Schiffe oder Züge bucht und Auto fährt. Wer Mobiltelefone nutzt, der kann auch durch private Anbieter zielgenau und kostengünstig lokalisiert werden. Komplettiert werden diese Daten durch gezielte Telefonanrufe der Call-Center-Branche und die Erfassung und Kartierung ganzer Stadtteile durch Firmen wie Google. Die Kombination solcher Daten erlaubt längst die Erstellung von Persönlichkeitsprofilen, sie können zudem mit frei verfügbaren Daten aus öffentlichen Registern (Beispiel: Meldedaten) noch kombiniert werden. Die Gefahren des Missbrauchs dieser Daten sind heute größer als jemals zuvor – ohne dass ein ausreichender Schutz dagegen vorhanden wäre.

Die vorhandenen gesetzlichen Regelungen sind nicht mehr geeignet, die Persönlichkeitsrechte der Bürgerinnen und Bürger wirksam zu schützen. Sofern das BDSG bislang überhaupt geändert wurde, zielte es häufig nicht auf ein Mehr, sondern ein weniger an Datenschutz. So wurde der Datenschutz durch zahlreiche bereichsspezifische Regelungen in anderen Gesetzen verwässert, wurden weitere Erlaubnisse für die Datenerhebung geschaffen, oder der Grundsatz der Einwilligung in die Freigabe von Daten weiter ausgehöhlt. Die Unterstellung von „konkludenten“ oder „mutmaßlichen“ Einwilligungen geht dabei bedenklich weit (vgl. BGH, Urteile vom 17. Juli 2008, Az. I ZR 195/05 – FC Troschenreuth – und Az. I ZR 75/06 – Royal Cars –) und soll gesetzgeberisch unterbunden werden.

Datenschutzbeauftragte, Verbraucherschutzverbände, Bürgerrechtsorganisationen und die Gewerkschaften fordern seit langem klare gesetzliche Regelungen zum besseren Schutz der Persönlichkeitsrechte – und die Modernisierung des Datenschutzgesetzes. Auch das Parlament hat mehrfach anlässlich des Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit auf den Reformbedarf im Datenschutz hingewiesen (vgl. Bundestagsdrucksachen 13/11168, 14/5353, 15/4597 und 16/4882).

Die Fraktion BÜNDNIS 90/DIE GRÜNEN hat für viele Bereiche bereits detaillierte Vorschläge zur Verbesserung des Datenschutzes vorgelegt, sei es gegen Vorratsdatenspeicherung (vgl. Bundestagsdrucksache 16/1622), gegen uferlosen Datenaustausch (Bundestagsdrucksache 16/9360), zum Scoring (Bundestagsdrucksache 16/683) oder für mehr Arbeitnehmerdatenschutz (Bundestagsdrucksache 16/9311).

Hat die Bundesregierung immerhin anerkannt, dass hinsichtlich der Auskunfteien Reparaturbedarf beim BDSG besteht, so zeigen sich bereits jetzt neue Schutzlücken beim Datenhandel. Die deshalb ohnehin anstehende Datenschutznovelle bietet nun die Chance, das BDSG grundlegend zu modernisieren. Die auf dem Datenschutzgipfel am 4. September 2008 vereinbarten Änderungen des Bundesdatenschutzgesetzes gehen diesbezüglich nicht weit genug. Zu viele Fragen bleiben unbeantwortet oder wurden gar nicht angesprochen: Wie ist das Problem des bereits entstandenen und bestehenden Datenhandels, insbesondere beim Handel mit den Meldedaten, zu lösen? Welche Auswirkungen hat die staatliche Vorratsdatenspeicherung auf die Datenpannen in der Privatwirtschaft gehabt? Es sind daher weitere flankierende Maßnahmen zur Stärkung des Datenschutzes erforderlich.

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