



# **FDP-Bundestagsfraktion**

## **Positionspapier**

### **Datenschutz im öffentlichen und nicht- öffentlichen Bereich**

Beschluss der FDP-Bundestagsfraktion vom 14. Oktober 2008

## Inhalt

<b>I. Ausgangslage</b> .....	3
<b>II. Datenschutz ins Grundgesetz</b> .....	3
<b>III. Datenschutzrecht modernisieren</b> .....	4
Datenschutzrecht für die Informationsgesellschaft rüsten .....	4
Rechtszersplitterung beenden .....	4
<b>IV. Potenziale des Marktes und der Technik für den Datenschutz nutzen</b> .....	5
Marktwirtschaftliche Anreize setzen .....	5
„Stiftung Datenschutz“ ins Leben rufen .....	5
Datenschutz-Gütesiegel jetzt einführen .....	5
Technik datenschutzgerecht gestalten .....	6
Stand der Technik verbindlich festschreiben .....	6
<b>V. Datenschutzaufsicht effektiver ausgestalten</b> .....	6
Zersplitterung der Aufsichtslandschaft beenden .....	6
Unabhängigkeit der Kontrollstellen stärken .....	6
Eingriffsbefugnisse und Sanktionsmöglichkeiten überprüfen .....	7
<b>VI. Datenschutz im nicht-öffentlichen Bereich verbessern</b> .....	7
Daten sparsam verwenden .....	7
Weitergabe der Daten nur mit Zustimmung der Verbraucher .....	7
Rückverfolgbarkeit von Daten sicherstellen .....	8
Scoring transparent und diskriminierungsfrei gestalten .....	8
Stellung des betrieblichen Datenschutzbeauftragten absichern .....	8
Wettbewerbsrecht in den Dienst des Datenschutzes stellen .....	9
Haftungsrecht für Datenschutz nutzen .....	9
Lastschriftverfahren überprüfen .....	9
Datenschutzkultur verbessern .....	10
<b>VII. Datenschutzkompetenz in der Bevölkerung stärken</b> .....	10
<b>VIII. Datenschutz im virtuellen Leben</b> .....	10
<b>IX. Arbeitnehmerdatenschutz verbessern</b> .....	12
Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Arbeitsverhältnis regeln .....	12
Überwachung am Arbeitsplatz minimieren .....	12
Lückenlose Kontrolle personenbezogener Daten auch beim Betriebsrat .....	13
<b>X. Datenschutz im öffentlichen Bereich verbessern</b> .....	13
Melddaten besser schützen .....	13
Datenschutz bei der GEZ einfordern .....	13
Gesetzentwürfe auf bürgerrechtliche Relevanz prüfen .....	14
Sicherheitsgesetze evaluieren .....	14
Bankgeheimnis wiederherstellen – Vorratsdatenspeicherung aussetzen .....	14
Datenschutz internationalisieren .....	14

## **I. Ausgangslage**

Privatheit ist der Kern persönlicher Freiheit. Diese Freiheit ist gefährdet. Staatliche Überwachung, wirtschaftliche Interessen, wuchernde Bürokratien, Sorglosigkeit von Verbrauchern, aber auch gut Gemeintes, wie das Streben nach Gleichheit und sozialer Gerechtigkeit, bedrohen die Privatsphäre und damit die Freiheit. Sie zu verteidigen ist Aufgabe liberaler Politik.

Das geltende Datenschutzrecht in Deutschland wird dieser Aufgabe immer weniger gerecht. Der heutige Datenschutz konzentriert sich einseitig auf das Verhältnis Staat und Bürger. Im nicht-öffentlichen Bereich ist der Datenschutz nur schwach ausgebildet. Hinzu kommt, dass er den Chancen und Risiken der neuen Technologien nur unzureichend Rechnung trägt.

Bislang sind alle Versuche, das Datenschutzrecht zu modernisieren, stecken geblieben. Zeitweise geriet der Datenschutz gänzlich aus dem Blick. Insbesondere nach den Anschlägen vom 11. September 2001 musste der Datenschutz weitreichende Einschränkungen hinnehmen. Er wurde als Täterschutz diskreditiert. Er musste als Ausrede herhalten, wenn es Fahndungsspannen oder Bürokratismus zu beklagen galt.

Das scheint sich nun zu ändern. Eine ganze Serie von Datenschutzskandalen in der Wirtschaft und die Freiheitsverluste durch die drastische Zunahme der Überwachung nach den Anschlägen vom 11. September 2001 beginnen Bürgern und Politik die Augen zu öffnen, dass es so nicht weiter gehen kann.

Nunmehr gilt es, aus den Fehlentwicklungen und Skandalen, aber auch der wachsenden Sensibilität des Einzelnen für die Bedeutung und den Wert des Datenschutzes die richtigen politischen Schlussfolgerungen zu ziehen, um Überwachung, Kontrolle und Datenmissbrauch vorzubeugen. Im nicht öffentlichen Bereich muss Datenschutz zu einem zentralen Anliegen moderner Verbraucherpolitik werden. Die Souveränität der Verbraucher und Verbraucherinnen im Umgang mit ihren persönlichen Daten zu erhalten und zu schützen ist unser Ziel.

## **II. Datenschutz ins Grundgesetz**

Der Datenschutz gehört ins Grundgesetz. 60 Jahre nach Inkrafttreten des Grundgesetzes, 25 Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts und mit Blick auf das Urteil Karlsruhe zur Online-Durchsuchung vom 27. Februar 2008 ist es an der Zeit, das Grundrecht auf informationelle Selbstbestimmung sowie auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme - kurz Computer-Grundrecht – ausdrücklich im Grundgesetz zu verankern.

Hierdurch würde die ständige Rechtsprechung des Bundesverfassungsgerichts auch durch den Verfassungsgesetzgeber ausdrücklich anerkannt. Die Bürgerinnen und Bürger würden in die Lage versetzt, ihre grundlegenden Rechte unmittelbar aus der Verfassung zu entnehmen. Der Verfassungsgesetzgeber würde zudem den landespolitischen und europarechtlichen Entwicklungen Rechnung tragen. So haben bereits zehn

Landesverfassungen ein Datenschutzgrundrecht explizit in ihren Grundrechtskatalog aufgenommen. Gleiches gilt für die Europäische Grundrechtscharta. Hinzu kommt, dass es der Verfassungsgesetzgeber auf diese Weise in der Hand hätte, die grundrechtlichen Gewährleistungen im Bereich des Datenschutzes gegen allfällige Änderungen im Bereich der Rechtsprechung abzusichern. Anknüpfungspunkt für die Gesetzgebungsarbeit können Vorschläge des Bundestages und des Bundesrates im Rahmen der Verfassungskommission Anfang der neunziger Jahre sein.

Die grundrechtliche Gewährleistung ist dabei so auszugestalten, dass ihr nicht nur ein abwehrrechtlicher, sondern auch ein objektivrechtlicher Gehalt zukommt, der die Bedeutung der informationellen Selbstbestimmung für Freiheit, Demokratie und Rechtsstaat zum Ausdruck bringt. Dieser Aspekt ist insbesondere für die Datenverarbeitung im nicht-öffentlichen Bereich unter dem Gesichtspunkt der Drittwirkung des Grundrechts bedeutsam. Des Weiteren sollte eine institutionelle Absicherung der Datenschutzkontrolle erfolgen, um deren Unabhängigkeit und Arbeitsfähigkeit zu gewährleisten. Unverzichtbar ist darüber hinaus, dass dieses Grundrecht nur durch ein qualifiziertes Gesetz im überwiegenden öffentlichen oder privaten Interesse eingeschränkt werden kann. Mindestens muss das Schutzniveau auf der Grundlage der bisherigen Rechtsprechung abgesichert werden, anderenfalls wäre mit der Verankerung des Datenschutzes im Grundgesetz nichts gewonnen. Gesetzgeberische Schnellschüsse, die einseitig der parteipolitischen Profilierung dienen und einer reinen Symbolpolitik verpflichtet sind, sind abzulehnen. Dies wäre das falsche rechtspolitische Signal.

### **III. Datenschutzrecht modernisieren**

#### **Datenschutzrecht für die Informationsgesellschaft rüsten**

Die Anerkennung der informationellen Selbstbestimmung als Grundrecht könnte ein wichtiger Schritt auch für die Modernisierung des Datenschutzrechts insgesamt sein. Die Notwendigkeit, das einfach-gesetzliche Datenschutzrecht zu modernisieren, besteht unverändert fort. Das Bundesdatenschutzgesetz stammt aus dem Jahre 1977, als Computer noch groß waren wie Garagen und Rabattmarken noch von Hand in bunte Heftchen geklebt wurden.

Trotz mehrfacher Mahnung des Deutschen Bundestages in seinen Entschlüssen zu den Tätigkeitsberichten des Bundesbeauftragten für den Datenschutz ist die Modernisierung und Weiterentwicklung des Datenschutzrechts bislang nicht vorangekommen. Ein im Jahre 2000 vom Bundesministerium des Innern in Auftrag gegebenes Gutachten zur Modernisierung des Datenschutzrechts blieb folgenlos, obwohl es eine Reihe konkreter Lösungsvorschläge enthielt. Der Abstand zwischen den geltenden datenschutzrechtlichen Bestimmungen und der rasanten technologischen Entwicklung mit ihren Folgen in allen Lebensbereichen ist seitdem immer größer geworden. Der Datenschutz liefert kaum mehr Antworten auf die Probleme, aber auch Chancen moderner Informationstechnik.

#### **Rechtszersplitterung beenden**

Unverändert aktuell ist deshalb die Forderung nach einem modernen, leicht verständlichen und übersichtlichen Datenschutzrecht. Anzustreben ist die Verankerung allgemeiner

Datenschutzgrundsätze in einem allgemeinen Gesetz, das für den öffentlichen und für den nicht-öffentlichen Bereich gleichermaßen gilt. In beiden Bereichen ist das gleiche Datenschutzniveau zu gewährleisten. Die bisherige Regelungstechnik ist aufzugeben. An die Stelle von hunderten von speziellen Gesetzen, die unübersichtlich und schwer zu handhaben sind, soll ein Bundesdatenschutzgesetzbuch treten, das bereichsspezifischen Regelungen vorgeht. Auf diese Weise können die bisherige Normenflut und Rechtszersplitterung verringert und Widersprüche vermieden werden. Das wäre nicht nur ein Gewinn für den Datenschutz, das wäre auch ein wirtschaftlicher Standortvorteil. Hinzu kommen positive Effekte in Sachen Bürokratieabbau.

## **IV. Potenziale des Marktes und der Technik für den Datenschutz nutzen**

### **Marktwirtschaftliche Anreize setzen**

Moderner Datenschutz muss datenschutzgerechte Technik fordern und fördern. Moderner Datenschutz sollte zu einem integrierten Element bei der Produktgestaltung und zu einem Produktargument werden. Um dieses Ziel zu erreichen, muss Datenschutz künftig durch, nicht gegen Technik verwirklicht werden. Es müssen Instrumente und Anreizmechanismen vorgesehen werden, die die Marktkräfte für den Datenschutz aktivieren und dem Grundsatz „privacy sells“ verpflichtet sind.

### **„Stiftung Datenschutz“ ins Leben rufen**

Es ist eine „Stiftung Datenschutz“ zu errichten, die nach dem Vorbild der Stiftung Warentest Produkte und Dienstleistungen privater und öffentlicher Anbieter unter Datenschutzgesichtspunkten vergleicht und bewertet.

### **Datenschutz-Gütesiegel jetzt einführen**

Seit dem Jahr 2001 enthält das Bundesdatenschutzgesetz in § 9a einen Verweis auf das Datenschutzaudit, mit dem Unternehmen die Einhaltung des Datenschutzes zertifizieren können – ein entsprechendes Durchführungsgesetz fehlt jedoch noch immer. Hersteller datenschutzgerechter Produkte und Anbieter datenschutzgerechter Dienstleistungen müssen endlich die Möglichkeit erhalten, diese zertifizieren zu lassen und mit dem Zertifikat werben zu können. Es ist an der Zeit, dass die Bundesregierung die Forderung des Deutschen Bundestages aus den Entschlüssen zum 19. und 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Vorlage eines Datenschutzauditgesetzes gem. § 9a BDSG aufgreift, damit ein Datenschutzauditgesetz noch in dieser Legislaturperiode verabschiedet werden kann. Anzustreben ist eine privatrechtliche Ausgestaltung des Zertifizierungsverfahrens, ggf. unter staatlicher Aufsicht. Darüber hinaus sollten staatliche Stellen verpflichtet werden, datenschutzgerechte Produkte zu verwenden, wo solche zur Verfügung stehen.

## **Technik datenschutzgerecht gestalten**

Um den Datenschutz soweit wie möglich in Produkte, Dienstleistungen und Verfahren zu integrieren, ist eine Regelung zu erwägen, derzufolge verkaufte Hard- und Software so voreinzustellen ist, dass ihre Benutzung nicht gegen das Datenschutzrecht verstößt. Computerprodukte sollten mit einer sicheren und datensparsamen Grundeinstellung ausgeliefert werden. Eine europaweit einheitliche Regelung ist anzustreben.

## **Stand der Technik verbindlich festschreiben**

§ 9 BDSG ist dahin zu konkretisieren, dass die technischen und organisatorischen Maßnahmen, die öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, zu treffen haben, dem jeweiligen Stand der Technik entsprechen müssen. Auf diese Weise ließe sich das Datenschutzrecht dynamisieren und der Abstand zwischen dem geschriebenen Recht und dem technologischen Fortschritt verkleinern.

## **V. Datenschutzaufsicht effektiver ausgestalten**

### **Zersplitterung der Aufsichtslandschaft beenden**

Die Datenschutzkontrolle für den öffentlichen und nicht-öffentlichen Bereich ist zusammenzuführen, die Zersplitterung der Kontrolllandschaft ist zu beenden. Das ist auch europarechtlich geboten. Die Aufspaltung der Datenschutzkontrolle in einen öffentlichen und einen nicht-öffentlichen Sektor ist der Europäischen Datenschutzrichtlinie fremd. Das Nebeneinander von Zuständigkeiten führt zur Verschwendung von Ressourcen, zu unterschiedlichen Auslegungs- und Verwaltungspraktiken und mithin zu einem unterschiedlichen Datenschutzniveau. Die Datenschutzkontrolle sollte deshalb einheitlich beim Bundes- und den Landesbeauftragten für den Datenschutz und die Informationsfreiheit angesiedelt werden. Hieraus ergeben sich nicht nur Synergieeffekte. Für die Betroffenen wird es auch leichter, ihre Rechte wahrzunehmen.

### **Unabhängigkeit der Kontrollstellen stärken**

Darüber hinaus ist die Unabhängigkeit der Kontrollstellen zu stärken. Die in vielen Bundesländern praktizierte Einbindung der Aufsichtsbehörden in die Innenverwaltung und die daraus folgende Weisungsgebundenheit ist mit der von der Europäischen Datenschutzrichtlinie geforderten völligen Unabhängigkeit der Kontrollstellen nicht vereinbar. Es ist daher zu überlegen, auf die Rechtsaufsicht über die öffentlichen Datenschutzbeauftragten zu verzichten, um so bereits den Anschein einer Einflussnahme zu vermeiden. In Betracht zu ziehen ist weiterhin, den Datenschutzbeauftragten das Recht zu geben, im Parlament (Haushaltsausschuss) ihre Interessen selbst vortragen und vertreten zu können. Eine solche Regelung entspricht der Struktur, dass es sich bei den Datenschutzbeauftragten um Stellen handelt, die vom Parlament eingerichtet werden und ihm in der Sache unmittelbar berichten können. Darüber hinaus ist die Einrichtung des

Bundesbeauftragten als oberste Bundesbehörde wünschenswert. Damit würde auch dem Umstand Rechnung getragen, dass der Bundesbeauftragte dem Bundesminister des Innern zu- aber nicht untergeordnet ist.

## **Eingriffsbefugnisse und Sanktionsmöglichkeiten überprüfen**

Nach geltendem Recht stehen bei den staatlichen Datenschutzkontrollstellen Beratungs- und Serviceaufgaben im Vordergrund. Es ist zu prüfen, inwieweit die Entwicklung der Datenverarbeitung, aber auch die aktuellen Vorfälle weiterreichende exekutive Befugnisse erforderlich machen, wie etwa die Möglichkeit, die Löschung von Daten, die widerrechtlich verarbeitet oder weitergegeben wurden, anzuordnen.

Das Sanktionssystem ist darauf hin zu überprüfen, inwieweit es noch abschreckende Wirkung hat, damit sich Verstöße gegen den Datenschutz nicht lohnen. Ggf. ist eine Erhöhung des Bußgeldrahmens vorzunehmen.

Soweit die unzulässige Datenverarbeitung eine Straftat darstellt, wird diese bislang nur auf Antrag verfolgt. Vor dem Hintergrund der jetzt bekannt gewordenen Datenschutzdelikte, die offensichtlich über individuelle Verstöße hinausgehen und dem Bereich der Wirtschaftskriminalität zuzuordnen sind, ist zu prüfen, ob auf das Antragserfordernis zu verzichten ist und Straftaten nach dem Bundesdatenschutzgesetz als Officialdelikte auszugestalten sind. In jedem Fall zu verbessern ist die personelle und finanzielle Ausstattung der Aufsichtsbehörden. Nur so lassen sich die bestehenden Vollzugsdefizite beseitigen.

## **VI. Datenschutz im nicht-öffentlichen Bereich verbessern**

### **Daten sparsam verwenden**

Der beste Weg, um Datenskandale effektiv zu verhindern, ist die strikte Beachtung des Grundsatzes der Datenvermeidung und Datensparsamkeit. Soweit möglich, muss ein Personenbezug von Anfang an vermieden oder nachträglich durch Löschung der Daten, Verschlüsselung, Anonymisierung oder Pseudonymisierung beseitigt werden, um dem Grundsatz der Souveränität des Verbrauchers über seine Daten angemessen Rechnung zu tragen. In den neuen Techniken liegen große Chancen und Potenziale für den Datenschutz, die es zu nutzen gilt. In Unternehmen sollten dezentrale Datenspeicherungen zentralen Lösungen vorgezogen werden.

### **Weitergabe der Daten nur mit Zustimmung der Verbraucher**

Sollen Verbraucher über die Verwendung ihrer Daten eigenverantwortlich bestimmen, müssen sie zum einen über Informationsrechte verfügen, welche Daten zu welchem Zweck erhoben, gespeichert und verwendet werden. Zum anderen muss Datenverarbeitung dem Grundsatz der Zweckbindung entsprechen. Eine Verarbeitung personenbezogener Daten darf danach nur zu bestimmten, ausdrücklich festgelegten Zwecken erfolgen. Um dies sicherzustellen, ist die sog. Opt-in-Lösung einzuführen. Danach setzt die Datenverarbeitung

und Datenweitergabe im nicht-öffentlichen Bereich grundsätzlich die vorherige Einwilligung der betroffenen Person voraus. Insbesondere die Weitergabe von neu erhobenen personenbezogenen Daten für Werbezwecke sollte unter Einwilligungsvorbehalt gestellt werden. Dieser ist so auszugestalten, dass er die Reichweite der geplanten Verarbeitung und Nutzung hinreichend erläutert und den Verbrauchern die Tragweite ihrer Erklärung verdeutlicht. Eine solche Lösung stellt den schonendsten Ausgleich zwischen Unternehmen, die Arbeitsplätze zur Verfügung stellen und auf persönliche Daten von Kunden angewiesen sind, und Verbrauchern dar.

## **Rückverfolgbarkeit von Daten sicherstellen**

Um Verbrauchern die Durchsetzung ihrer Datenschutzrechte zu erleichtern, sind in den Datensätzen der Wirtschaft sog. Marker zu setzen, die Auskunft über den Datenfluss und darüber geben, woher die Daten ursprünglich stammen. Damit wird Transparenz für den Bürger hergestellt und eine lückenlose Rückverfolgbarkeit von personenbezogenen Daten garantiert. Zur weiteren Absicherung des Grundsatzes der Datensparsamkeit ist ein Kopplungsverbot vorzusehen. Das Verbot soll Unternehmen daran hindern, den Vertragsschluss von der Angabe personenbezogener Daten abhängig zu machen, die dazu nicht erforderlich sind. Die Weitergabe von überflüssigen Daten an Dritte kann so wirksam unterbunden werden.

## **Scoring transparent und diskriminierungsfrei gestalten**

Vertragsabschlüsse, Konditionen und Zahlungsmodalitäten werden im Handel und bei Dienstleistungen immer stärker von Bonitätsprüfungen abhängig gemacht, für die Kundendaten unter Einschaltung von Auskunftsteilen mit statistischen Verfahren miteinander verknüpft werden. Für den Einsatz und die Ausgestaltung von sog. Scoreverfahren, die die Bürgerinnen und Bürger hinsichtlich ihrer wirtschaftlichen Leistungsfähigkeit beurteilen, sind rechtliche Regelungen zu treffen. Je intensiver Scoring von der Wirtschaft genutzt wird, desto mehr Gewicht kommt dem Anspruch des Verbrauchers auf Transparenz hinsichtlich der angewendeten Verfahren, der Datenbasis und etwaiger Korrekturmöglichkeiten zu. Zudem sind Bürgerinnen und Bürger vor diskriminierender Verwendung ihrer Daten zu schützen. Die Nutzung von so genannten Geodaten beim Scoring, z.B. zum Zwecke der Einstufung in soziale, finanzielle oder andere Kategorien anhand von Wohnadressen in bestimmten Gegenden, ist auszuschließen.

## **Stellung des betrieblichen Datenschutzbeauftragten absichern**

Um das Datenschutzniveau und das Datenschutzbewusstsein in der Wirtschaft zu stärken und Betriebsabläufe datenschutzfreundlich zu gestalten, ist die Stellung der betrieblichen Datenschutzbeauftragten besser institutionell abzusichern.

Die Anforderungen, die an betriebliche Datenschutzbeauftragte zu stellen sind, sind zu konkretisieren. Zukünftig ist ein einheitliches Berufsbild „betrieblicher Datenschutzbeauftragter“ zu schaffen. Das geltende Recht begnügt sich mit unbestimmten Begriffen wie „erforderliche Fachkunde und Zuverlässigkeit“. Mindeststandard müssen dem

Stand der Technik entsprechende Kenntnisse in der Informationstechnik sowie entsprechende datenschutzrechtliche Kenntnisse sein. Es bietet sich an, die Einzelheiten in einer Rechtsverordnung zu regeln.

Zu prüfen ist eine Regelung, wonach Wirtschaftsprüfer in das Testat bzw. den Prüfbericht Feststellungen zur Beachtung des Datenschutzes aufnehmen.

## **Wettbewerbsrecht in den Dienst des Datenschutzes stellen**

Verstöße gegen den Datenschutz dürfen sich nicht lohnen. Um dies sicherzustellen, sind Maßnahmen vorzusehen, die über die interne und externe staatliche Kontrolle hinausgehen und bei den Marktteilnehmern selbst ansetzen. In diesem Zusammenhang sind erforderlichenfalls auf europäischer Ebene die Voraussetzungen für eine Ergänzung des Gesetzes gegen den unlauteren Wettbewerb (UWG) dergestalt zu schaffen, dass Wettbewerber beim Verstoß gegen Datenschutzpflichten im Rahmen einer privatrechtlichen Konkurrentenklage als unlauteren Wettbewerbsvorteil geltend machen können. Bislang ist die Rechtsprechung der Auffassung, dass Datenschutzvorschriften nicht wettbewerbsschützend seien. Dabei ist gerade das Wettbewerbsrecht ein effizientes, unbürokratisches und bewährtes Instrument, dessen Erstreckung auf dem Bereich des Datenschutzes sich geradezu anbietet. Hierzu ist klarzustellen, dass die Verletzung von gesetzlichen Datenschutzerfordernungen einen Verstoß gegen die guten Sitten im Sinne des § 1 UWG und unzutreffende Datenschutzerklärungen eine irreführende Angabe im Sinne von § 3 UWG sein können. Dann kann jeder Wettbewerber den Wettbewerbsverstoß im Rahmen einer Unterlassungsklage geltend machen.

## **Haftungsrecht für Datenschutz nutzen**

Vorrang vor gesetzgeberischen Eingriffen zur Verbesserung des Datenschutzniveaus in der Wirtschaft haben aus Sicht der FDP-Bundestagsfraktion Selbstverpflichtungen der Marktteilnehmer, z.B. auch durch Aufnahme des Datenschutzes in den Corporate Governance Kodex.

Darüber hinaus sollte auch das Haftungsrecht als effizientes Rechtsdurchsetzungsinstrument für den Datenschutz nutzbar gemacht werden. Bislang ist für die Geschädigten der Nachweis der Ursächlichkeit und des Verschuldens nahezu unmöglich. Das Haftungssystem des Datenschutzrechts ist daraufhin zu überprüfen, inwieweit es einen spürbaren Anreiz für die konkrete Einhaltung der Datenschutzregelungen gibt und dazu anhält, durch ein effizientes Datenschutzmanagementsystem Haftungsrisiken zu vermindern.

## **Lastschriftverfahren überprüfen**

Das Lastschriftverfahren hat sich grundsätzlich bewährt und ist für die Abwicklung des Zahlungsverkehrs in Deutschland unverzichtbar. Die Kreditwirtschaft ist zur Vermeidung gesetzgeberischer Maßnahmen aufgefordert, an einer weiteren Verbesserung des Systems zu arbeiten. Im Interesse der Sicherheit des Zahlungsverkehrs ist eine anlassbezogene und risikoadäquate Prüfung vorzusehen. Namentlich sind Unternehmen, die in der Vergangenheit

missbräuchlich Abbuchungen haben vornehmen lassen, von der Teilnahme am Zahlungsverkehr auszuschließen. Dies ist auch im Interesse der einziehenden Bank, die ansonsten Gefahr läuft, den finanziellen Schaden selbst tragen zu müssen. Bei Unternehmen, die erstmals am Lastschriftverfahren teilnehmen oder die wiederholt Anlass zu Beschwerden gegeben haben, sind die Kontrollpflichten zu verschärfen. Insbesondere ist hier vor Ausführung der Transaktion die Vorlage der schriftlichen Einzugsermächtigung zu verlangen.

## **Datenschutzkultur verbessern**

Zur Verbesserung der Datenschutzkultur in der Wirtschaft müssen Unternehmen verpflichtet werden, Datenschutzverstöße den Datenschutzaufsichtsbehörden mitzuteilen. Im Falle von Datenschutzverstößen, bei denen eine Gefahr für personenbezogene Daten besteht, müssen darüber hinaus auch die Betroffenen informiert werden. Nur so werden Betroffene in die Lage versetzt, ihre Rechte durchzusetzen und nur dann ist sichergestellt, dass mit der Benachrichtigung nicht genau das Gegenteil bewirkt wird, nämlich die weitere Ausnutzung von Sicherheitslücken.

Soweit ein betrieblicher Datenschutzbeauftragter bestellt ist, sollten Angaben, die eine schnelle Kontaktaufnahme mit diesem ermöglichen, auf der Internetseite des Unternehmens verfügbar gemacht werden.

## **VII. Datenschutzkompetenz in der Bevölkerung stärken**

Datenschutz ist nicht nur Aufgabe des Staates, sondern auch Verantwortung eines jeden Einzelnen. Immer mehr Menschen stellen höchstpersönliche Daten ins Internet, insbesondere bei sozialen Netzwerken, ohne an die möglichen Konsequenzen zu denken. Sie machen es dabei Datendieben und Betrügern besonders einfach. Projekte, die das Datenschutzbewusstsein fördern, müssen daher fester Bestandteil der schulischen, aber auch der beruflichen Ausbildung werden, so dass vor allem jüngere Menschen den verantwortungsvollen Umgang mit persönlichen Daten erlernen. Der Datenschutz muss auch bei der Förderung der Medienkompetenz eine größere Rolle spielen.

## **VIII. Datenschutz im virtuellen Leben**

Informations- und Kommunikationsnetze sind ein fester Bestandteil bei beruflichen und privaten Aktivitäten und im täglichen Leben nicht mehr wegzudenken. Auch bei Nutzung der neuen Medien muss ein anonymes und überwachungsfreies Handeln möglich sein und die Privatsphäre im virtuellen Leben gewahrt bleiben, so wie auch im tatsächlichen Leben. Dies ist derzeit nicht der Fall, weil das Verhalten von Nutzern im Internet bis ins kleinste aufgezeichnet wird. Die Gefahr, dass Nutzungsprofile erstellt werden, ist im Internet besonders hoch, da schon wenige Eingaben reichen, um ein aussagekräftiges Interessen- und Verhaltensprofil zu erhalten. Personenbezogene Nutzerprofile sollten nur mit Einwilligung des Nutzers erstellt werden. Anonymität im Internet muss der Regelfall sein und

darf nicht die Ausnahme darstellen. Nur so wird Datenmissbrauch effektiv verhindert und das Nutzervertrauen gestärkt. Dazu ist eine Umkehrung der bisherigen Darlegungs- und Beweislast bei § 13 Abs. 6 TMG hinsichtlich der Zumutbarkeit, anonyme Nutzungsmöglichkeiten bei Dienste- und Kommunikationsdiensten anzubieten, notwendig.

Korrekturansprüche im Internet müssen verbessert werden. Unrichtig gewordene Daten oder rechtswidrig erhobene Daten lassen sich nur schwer wieder entfernen, weil unklar ist, wie oft diese Daten zwischenzeitlich vervielfältigt worden sind. Wenn die tatsächlichen Möglichkeiten begrenzt sind, zu verhindern, dass unzulässige oder falsche Inhalte verbreitet werden, muss es zumindest ein Recht auf Gegendarstellung geben; nur so lassen sich Verleumdung und Denunziation im Internet verhindern. Das Internet darf nicht zum Pranger werden. Ebenso muss ein sicherer gesetzlicher Rahmen vorgesehen werden, wie, in welcher Art und in welchem Umfang Geodaten – wie z.B. die Nutzung vorhandener Satelliten- bzw. anderer Luftbildaufnahmen oder die eigene Erhebung solcher Daten durch das Abfotografieren bzw. Abfilmen ganzer Straßenzüge – erhoben, gespeichert und genutzt werden dürfen.

Darüber hinaus sind klare Regelungen für Lösungsfristen auch im Internet eine unabdingbare Voraussetzung, um das Vertrauen der Bürger in die neuen Medien zu stärken. Verfallsdaten bei digitalen Daten sollten als technische Lösungen bevorzugt werden.

## **IX. Arbeitnehmerdatenschutz verbessern**

### **Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Arbeitsverhältnis regeln**

Das Arbeitsverhältnis als Grundlage der wirtschaftlichen Existenz der Menschen erfordert ein besonderes Augenmerk dahin, dass Arbeitnehmerinnen und Arbeitnehmer nicht zur Aufgabe oder Einschränkung ihrer Grundrechte gezwungen werden. Vielmehr müssen Regelungen gefunden werden, die im Verhältnis zwischen Arbeitnehmern und Arbeitgebern einen schonenden Interessenausgleich sicherstellen. Dabei muss das vom Bundesverfassungsgericht neu entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme besondere Berücksichtigung finden.

Der allgemeine Grundsatz der Datensparsamkeit hat besonders im Arbeitsverhältnis eine herausragende Bedeutung. Hinsichtlich der Zulässigkeit der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist im Arbeitsverhältnis sowohl nach den Datenarten als auch nach dem Zeitpunkt zu unterscheiden. Im Falle einer erfolglosen Bewerbung besteht ein berechtigtes Interesse des Bewerbers, dass Daten nur so lange aufbewahrt werden, wie dies rechtlich geboten ist, z.B. im Hinblick auf das Allgemeine Gleichbehandlungsgesetz (AGG). Wird eine längere Aufbewahrung seitens des Arbeitsgebers gewünscht, um z.B. zu einem späteren Zeitpunkt auf die Bewerbung zurückkommen zu können, setzt dies das Einverständnis des Bewerbers voraus. Während des Arbeitsverhältnisses darf sich die Datenverarbeitung nur auf solche Daten beziehen, die für das Arbeitsverhältnis erforderlich sind. Eine Datenverarbeitung, die sich auf außerdienstliches Verhalten, wie z.B. Äußerungen zu politischen Sachverhalten in Blogs oder im Freundeskreis bei Facebook, bezieht, muss grundsätzlich ausgeschlossen sein. Nach Beendigung des Arbeitsverhältnisses müssen Daten umfassend gelöscht werden, soweit sie nicht mehr zur Sicherung von Rechtspositionen erforderlich sind. Vor, während und nach dem Arbeitsverhältnis müssen den Betroffenen Auskunfts-, Einsichts- und Berichtigungsrechte zustehen, damit sie Herr ihrer Daten bleiben. Gesundheitsbezogene Daten dürfen im Arbeitsverhältnis nur erhoben werden, wenn sie für den jeweiligen konkreten Arbeitsplatz relevant sind. Arbeitgeber dürfen die Erstellung und Vorlage eines Gentests von den Arbeitnehmerinnen und Arbeitnehmern nicht verlangen.

Weder das Bundesdatenschutzgesetz noch die EG-Datenschutzrichtlinie kennen ein „Konzernprivileg“. Der vielfach notwendige Austausch von Mitarbeiterdaten in verbundenen Unternehmen, z.B. bei der zentralen Führungskräftebetreuung, beim Betrieb von Shared-Service-Centern oder der konzernweiten Steuerung von IT-Systemen, sollte gesetzlich geregelt werden.

### **Überwachung am Arbeitsplatz minimieren**

Die Überwachung der Nutzung technischer Systeme am Arbeitsplatz durch Aufzeichnung und Speicherung von Zugriffen auf bestimmte Dateien, das Mitlesen von E-Mails oder die Protokollierung der aufgerufenen Internetseiten muss sich daran messen lassen, ob dies im Einzelfall verhältnismäßig ist. Eine generelle Rundum-Protokollierung des digitalen Arbeitsumfeldes muss unzulässig sein. Auf Inhalte elektronischer Kommunikation darf nur in

besonderen Fällen zugegriffen werden. Das gilt insbesondere, wenn auch eine private Nutzung dienstlicher informationstechnischer Systeme zulässig ist. Für Zugangssysteme, die mit Biometrie oder Betriebs- und Chipausweise funktionieren, sind klare Regelungen zur dezentralen Speicherung und Zugriffsberechtigung zu schaffen, um eine zweckfremde Nutzung auszuschließen. In jedem Fall sind Mitarbeiter über die Kontrollsysteme und die Art der Datenspeicherung und Verarbeitung zu informieren.

## **Lückenlose Kontrolle personenbezogener Daten auch beim Betriebsrat**

Seitdem das Bundesarbeitsgericht 1997 entschieden hatte, dass die Datenverarbeitung des Betriebsrates nicht durch den betrieblichen Datenschutzbeauftragten kontrolliert werden dürfe, besteht in den Unternehmen quasi ein kontrollfreier Raum: Die Unternehmen sind den Betroffenen als verantwortliche Stellen zur Gewährleistung des Datenschutzes verpflichtet, können dies jedoch gegenüber dem Betriebsrat nicht durchsetzen. Diese Gesetzeslücke muss geschlossen werden.

## **X. Datenschutz im öffentlichen Bereich verbessern**

### **Meldedaten besser schützen**

Im Rahmen der Föderalismusreform ist die ausschließliche Gesetzgebung für das Melderecht auf den Bundesgesetzgeber übergegangen. Deshalb ist es jetzt auch Aufgabe des Bundes, für einen besseren Schutz der Meldedaten der Bürger zu sorgen. Nach geltendem Recht erhält jeder, der bestimmte Mindestangaben zu einer Person machen kann, eine so genannte einfache Melderegisterauskunft. Der Bürger hat keine Möglichkeit, dem zu widersprechen. Einzig bei Auskünften über das Internet ist ein solcher Widerspruch möglich. Um Adresshandel in großem Stil und damit eine Kommerzialisierung der Meldedaten zu verhindern, ist eine Regelung dergestalt vorzusehen, dass Auskünfte nur noch bei Vorliegen eines berechtigten Interesses erteilt werden, z.B. um Rechtsansprüche durchzusetzen, oder soweit der Bürger ausdrücklich sein Einverständnis erklärt hat. Auf diese Weise wird es gelingen, Melderegisterauskünfte zu vermeiden, die einzig und alleine für Reklamezwecke genutzt werden sollen. Eine Übergangsfrist ist vorzusehen.

### **Datenschutz bei der GEZ einfordern**

Dringender Handlungsbedarf besteht auch bei der Weitergabe von Meldedaten an die GEZ. Bei jedem Umzug eines Einwohners erhält die GEZ vom Einwohnermeldeamt Daten aus dem Melderegister. Im Melderecht aller Bundesländer sind entsprechende Befugnisse geschaffen worden. Das Einwohnermeldeamt übermittelt u. a. Familiennamen, Vornamen, Geburtsdatum, Familienstand, bisherige und neue Anschrift sowie Tag des Ein- und Auszugs. Die GEZ gleicht diese Daten mit ihrem Datenbestand ab, korrigiert auf dieser Basis die Daten bei angemeldeten Personen und schreibt die Personen an, die bisher nicht angemeldet waren. Schließlich beschafft sich die GEZ bei privaten Adresshändlern jährlich mehrere Millionen Adressen. Dabei handelt es sich um gezielt aufbereitete Datenbestände von solchen Personengruppen, bei denen das Vorhandensein von Fernsehern oder Radios vermutet werden kann. Darunter sind z. B. Abonnenten von Fernsehzeitschriften oder des

Bezahlfernsehens (PayTV) sowie Teilnehmer an Gewinnspielen von Rundfunksendern. Hier ist eine Überprüfung der bisherigen Praxis der Datenweitergabe unter dem Gesichtspunkt der Verhältnismäßigkeit dringend geboten.

Die FDP-Bundestagsfraktion setzt sich darüber hinaus dafür ein, die Rundfunkgebühr durch eine allgemeine Medienabgabe zu ersetzen. Die Ministerpräsidenten der Länder, die Landesparlamente und die öffentlich-rechtlichen Rundfunkanstalten werden aufgefordert, zur dauerhaften Sicherung und zukunftsfähigen Gestaltung des Bestandes und der Finanzierung des dualen Rundfunksystems in Deutschland entsprechende Änderungen am Rundfunkstaatsvertrag unter stärkerer Beachtung der Grundsätze des Datenschutzes vorzunehmen.

## **Gesetzentwürfe auf bürgerrechtliche Relevanz prüfen**

Die Vielzahl verfassungswidriger Sicherheitsgesetze nach den Anschlägen vom 11. September 2001 und die damit einhergehende Beschneidung des Datenschutzes erfordern ein Umdenken. Zentrale Datenspeicherungen sollten auch im staatlichen Bereich vermieden werden. Gesetzentwürfe müssen künftig nicht nur auf ihre finanziellen Auswirkungen hin überprüft werden, sondern auch auf ihre bürgerrechtliche Relevanz.

## **Sicherheitsgesetze evaluieren**

Erforderlich ist eine Evaluierung sämtlicher seit 1998 beschlossenen Überwachungsgesetze unter den Gesichtspunkten der Wirksamkeit, der Verfassungsmäßigkeit und der dadurch gebundenen Mittel.

## **Bankgeheimnis wiederherstellen – Vorratsdatenspeicherung aussetzen**

Als Sofortmaßnahmen im Bereich der Sicherheitsgesetzgebung sollten das Bankgeheimnis wieder hergestellt sowie die Vorratsdatenspeicherung ausgesetzt werden.

## **Datenschutz internationalisieren**

Bei europäischen oder internationalen Verhandlungen muss das Parlament stärker eingebunden werden und frühzeitig informiert werden. Die Verhandlungsführer müssen darüber hinaus auch an die Vorgaben des Parlaments gebunden sein.

Auf europäischer Ebene ist unverzüglich ein Rahmenbeschluss für den Datenschutz im Bereich der so genannten 3. Säule herbeizuführen, um ein datenschutzrechtliches Gegengewicht zum zunehmenden Austausch von Daten zwischen Polizei- und Strafverfolgungsbehörden in Europa zu schaffen. Dabei muss ein Datenschutzniveau erreicht werden, wie es sich für den Bereich des Binnenmarktes aus der europäischen Datenschutzrichtlinie ergibt.