



Datenschutz und Datensicherheit

“Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. [...] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art 2 Abs. 1 in Verbindung mit Art 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

Auszug aus der Urteilsbegründung des Bundesverfassungsgerichts zum sog. Volkszählungsurteil vom 15. Dezember 1983.

Zu Zeiten von Kunden- Treue- und Bonuskarten, von Videoüberwachung, RFID Chips, elektronischer Gesundheitskarte und Web 2.0 erscheint der Inhalt dieses Urteils von 1983 schon beinahe anachronistisch. Trotzdem und gerade deshalb sieht UnternehmensGrün es als sozial und ökologisch orientierter Verband als besonders wichtig an, zum Thema Datenschutz deutlich Stellung zu beziehen.

UnternehmensGrün setzt sich ausdrücklich für das Recht auf informationelle Selbstbestimmung ein! Jeder Bürger und jede Bürgerin hat das Recht zu wissen, welche Daten wo, wie und warum über sie und ihn gespeichert sind.

I. Das Recht auf informationelle Selbstbestimmung

1. Wie verletzbar ist unsere informationelle Selbstbestimmung?

Neue Technologien und eine veränderte Gesellschaftsform ermöglichen heute vielfältigen Missbrauch von gesammelten und gespeicherten Daten. Die Industriegesellschaft hat sich durch die Entwicklung neuer Technologien und veränderter Arbeitsprozesse zusehends in eine Informationsgesellschaft gewandelt.

Informationen und Daten über Menschen wer-

den gesammelt, gespeichert, verarbeitet und gehandelt, oftmals ohne das Wissen der betroffenen Personen.

"Jeder hat das Recht, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen. Dazu gehört das Recht auf Auskunft und Einsicht in amtliche Unterlagen. Dieses Recht darf nur durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden, soweit überwiegende Interessen der Allgemeinheit es erfordern."

So lautete ein konkreter Vorschlag des Bundestages und des Bundesrates Anfang der neunziger Jahre im Rahmen der Verfassungskommission. Bislang existiert jedoch keine befriedigende Vorgabe, die das Sammeln und Speichern von personenbezogenen Daten regelt. Im Grundgesetz fehlt diese Regelung gänzlich. Doch genau hierher gehört eine Datenschutzkontrolle, denn der Umgang mit personenbezogenen Daten greift tief in die Privatsphäre jeder Bürgerin und jedes Bürgers ein.

2. Der Begriff des „gläsernen Menschen“ ist aktueller denn je

• RFID-Technik und Scoring – Einsatz nur mit Zustimmung:

Die RFID-Chips (RFID = Radio Frequency Identifikation) hält mehr und mehr Einzug in unseren Alltag. Sie werden unsichtbar eingesetzt an Gegenständen, wie z.B. Waren, Eintrittskarten, Autoschlüsseln oder Handys. Sie dienen u.a. zum Zweck der Ortung, um Werbung an nah befindliche potenzielle Kunden zu senden. Persönliche Daten werden mit Wareninformationen verknüpft, Konsumprofile werden erstellt. Gespeicherte Informationen können kontaktlos über größere Entfernungen gesendet werden. Die *Möglichkeiten* von RFID-Chips gehen aber noch weit darüber hinaus.

Dieses darf nur mit ausdrücklicher Einwilligung der Verbraucherinnen und Verbraucher geschehen.

Waren, die mit RFID-Chips bestückt sind, müssen als solche markiert werden und die Chips müssen bei Bedarf ohne komplizierte Anleitung deaktiviert werden können.

Kreditscoring wird als ein statistisches Verfahren von Kreditinstituten angewendet, um eine Risikoklassifizierung für private standardisierte Ratenkredite und Kleinkredite durchzuführen. Es werden persönliche Eigenschaften wie etwa der Beruf, Arbeitgeber, Familienstand, Kontoführung im eigenen Haus, positive und negative Merkmale der SCHUFA-Auskunft und wirtschaftliche Verhältnisse (verfügbares Einkommen sowie Vermögensverhältnisse, erwartete Ausgaben) herangezogen und dies ohne das Wissen der Betroffenen. Die erfassten Merkmale werden durch eine Punktbewertung von 0 bis 1000 Punkte standardisiert. Fakt ist, dass nicht persönliches Verhalten des Einzelnen etwas über seine Kreditwürdigkeit aussagt, sondern bloße statistische Daten.

Die Offenlegung von Scoring-Verfahren ist unumgänglich.

Die Gefahr von sozialer Ausgrenzung und Diskriminierung besteht, denn Statistiken und Zahlen können fehlerhaft sein, Lebensumstände können sich ändern.

• Ausschluss von Datenmissbrauch

Da die Datenerhebung mittlerweile viele persönliche Bereiche betreffen, muss einem Missbrauch mit diesen Daten vorgebeugt werden. Auf der geplanten elektronischen Gesundheitskarte werden etwa nicht nur Daten wie Namen, Geburtsdatum etc. abgespeichert, sondern auch differenzierte Informationen über Krankheiten, Lebensweise etc. Ebenso sensibel sind Sozialdaten, die vielfach im Rahmen der Gewährung des ALG II erhoben werden. Auch mit diesen Daten kann ein detailliertes Profil über die betroffene Person erstellt werden.

Banken können im Rahmen der Kreditvergabe automatisierte Kontenabrufe tätigen, wodurch gläserne Konten geschaffen werden. Die Kundinnen und Kunden bekommen hier von nichts mit. Hier sind unbedingt Regelungen erforderlich, die diese Praxis eingrenzen.

Bei Datenpannen, also dem unsachgemäßen Umgang mit ihren Daten, müssen die Betroffenen unverzüglich informiert werden. Alle Stellen, die Daten verarbeiten, müssen verpflichtet werden, die Betroffenen in Kenntnis zu setzen, wenn die vertrauliche Behandlung ihrer personenbezogenen Daten nicht mehr gewährleistet ist. Gegenüber Unternehmen müssen zivilrechtliche Schadensersatzansprüche bestehen, wenn vertrauliche Daten in unbefugte Hände gelangt sind.

Für all diese Bereiche gilt: Persönliche Daten müssen geschützt werden, es muss klar sein, wer für die Daten verantwortlich ist und wie sie behandelt werden.

- **Arbeitnehmerdatenschutzgesetz:**

Unter dem Deckmantel der Produktionsüberwachung werden vielerorts Arbeitsplätze bzw. Arbeitnehmerinnen und Arbeitnehmer überwacht. Per Handyortung werden Bewegungsprofile für Kuriere und Fahrer erstellt, Videokameras zeichnen die Arbeit des Personals und deren Verhalten auf. Betriebliche Vereinbarungen gibt es nur selten und diese bieten auch nur ungenügenden Schutz. In den bestehenden Datenschutzgesetzen fehlen präzise Zweckbindungs- und Löschungsregelungen, Bestimmungen über die elektronische Kommunikation und Überwachung und der besondere Schutz sensibler Gesundheits- und Gen-daten.

Die Arbeit der Datenschutzbeauftragten zu stärken.

Es bedarf einer besseren Vorbereitung der betrieblichen Datenschutzbeauftragten auf ihre Tätigkeit, größerer Unabhängigkeit der Datenschutzbeauftragten von der Geschäftsleitung und die Möglichkeit für KMUs die gesetzlich geforderten Aufgaben der betriebli-

chen Datenschutzbeauftragten auf Berufsverbände oder Kammern zu übertragen.

- **Behörden und der Datenschutzbeauftragte:**

Damit auch in Behörden die Datenschutzbeauftragten eine effektive Arbeit leisten können, gelten auch hier die Forderungen nach Unabhängigkeit. Dies bedarf einer Stärkung der Datenschutzbeauftragten in den obersten Bundesbehörden zum Zweck der Koordinierung des Datenschutzes in den nachgeordneten Behörden.

3. Die europäische und internationale Ebene

Auf EU-Ebene – auch im Programm für die deutsche EU-Präsidentschaft – sieht es ebenfalls kläglich aus mit dem Datenschutz für deutsche Bürgerinnen und Bürger: Allen Mitgliedsstaaten sowie Europol und der Europäischen Staatsanwaltschaft Eurojust sollen die nationale Datenbanken zur Verfügung gestellt werden. Ohne die dringend notwendigen, einheitlichen EU-Standards zum Datenschutz sollen DNA-Daten oder Fingerabdrücke für den internationalen Zugriff freigegeben werden. Hierdurch wird ein unumkehrbarer Prozess mit unkalkulierbaren Folgen in Gang gesetzt.

Der EU-Vertrags sieht die „Unabhängigkeit der Datenschutzbeauftragten“ vor. Da diese Unabhängigkeit bisher nicht erfüllt ist, läuft gegen Deutschland, welches die derzeitige EU-Präsidentschaft innehat, ein Vertragsverletzungsverfahren!

Über EU-Grenzen hinaus, in der Zusammenarbeit mit den Sicherheitsbehörden der USA, klafft eine noch größere Datenschutzlücke. Am 31.7.2007 läuft das Interimsabkommen, das sowohl gegen europäisches wie gegen nationales Datenschutzrecht verstößt, mit den USA über die Weitergabe von Fluggastdaten aus.

Im internationalen Datenaustausch gilt es zu erreichen, dass in allen Ländern Mindeststan-

dards im Datenschutz eingehalten werden und Daten auch hier zukünftig ausschließlich zweckgebunden behandelt werden.

4. Die (internationale) Wirtschaft und der Datenschutz

Auf allen Ebenen wird deutlich: neue Formen der Wirtschaft und des Marketings, sei es Internet-Handel, internationaler Zahlungsverkehr oder generelle Kommunikation über die neuen Medien, werden auf Dauer nur dann angenommen, wenn ein ausreichender Schutz der persönlichen Daten gewährleistet ist. Durch die konstruktive Zusammenarbeit mit ExpertInnen des Daten- und Verbraucherschutzes können folgenschwere Verletzungen der Persönlichkeitsrechte mit Auswirkungen sowohl für die betroffenen Personen als auch für die Wirtschaft verhindert werden.

Datenschutz darf nicht länger als lästiges Anhängsel gesehen werden, sondern muss eine reelle Chance bekommen: als Instrument zur Bildung von Vertrauen und Akzeptanz.

5. Ohne Datenschutz kann Demokratie nicht funktionieren

Auch wenn es Menschen gibt, die bereitwillig ihre Daten hergeben (siehe z.B. Web 2.0) – oft ohne sich über die Folgen, wie Verkauf der Daten an Dritte etc. im Klaren zu sein – muss denjenigen, die sich dafür entscheiden, ihre Daten selbstbestimmt und bewusst zu behandeln, durch einen verlässlichen Datenschutz diese Selbstbestimmung garantiert werden.

Verbraucherinnen und Verbraucher ernst nehmen

Zur Informationstechnologie gehören auch Entwicklungen, die darauf zielen, immer mehr, immer lückenlosere, immer genauere Informationen über Verbraucherinnen und Verbraucher unwiderruflich zu sammeln.

Die meisten Prozesse der Datensammlung,

des Datenhandels oder sonstiger Datenverwertung bleiben im Dunkeln, so dass für betroffene Bürgerinnen und Bürger keine Möglichkeit des Überblicks über die eigenen im Umlauf befindlichen Daten besteht.

Bürgerinnen und Bürger dürfen nicht unter Generalverdacht gestellt werden; niemand darf ungefragt auf Schritt und Tritt beobachtet werden. Es muss möglich sein, sich zu bewegen, ohne ständig digitale Spuren oder sonstige persönliche Daten zu hinterlassen. Das gilt auch für die Überwachung öffentlicher Räume und der digitalen Welt:

Eigenverantwortung kann nur entstehen, wo Selbstbestimmung möglich ist! Hierfür gilt es, das Vertrauen zwischen Bürgerinnen und Bürgern einerseits und dem Staat und der Wirtschaft andererseits herzustellen und zu bewahren.

Nur mit Aufklärung und Transparenz – auch im öffentlichen Dialog – kann selbstbestimmtes Handeln entstehen und damit ein einvernehmlicher, vertrauensvoller Umgang von Wirtschaft und Staat einerseits und Verbraucherinnen und Verbrauchern andererseits erfolgreich funktionieren.

Selbstbestimmung setzt die ausdrückliche Einwilligung der Betroffenen bei jeglicher Handhabung der eigenen Daten voraus, die Auskunftspflicht der Datensammler und nicht zuletzt den Einsatz von unabhängigen Aufsichtsbehörden. Hierfür müssen Verbraucherinnen und Verbraucher wissen, welche Daten von ihnen gespeichert sind. Es muss möglich sein, Datenbestände bei Bedarf zu widerrufen oder zu löschen, Daten einzusehen, Datensammlungen ausdrücklich zu verhindern, wenn sie nicht gewünscht sind, sowie die Datenweitergabe zu untersagen.

Die Einführung von verlässlichen und vereinheitlichten Gütesiegeln ist dabei ein sinnvoller Kontrollmechanismus, für den klare Richtlinien zu erstellen sind.

Wir brauchen Standards für Gütesiegel, die den Verbraucherinnen und Verbrauchern zeigen, dass von zertifizierten Anbietern kein Missbrauch mit ihren Daten getrieben wird.

6. Fazit - Anpassung des Bundesdatenschutzgesetzes an aktuelle Rahmenbedingungen

Das Bundesdatenschutzgesetz ist veraltet – die grundlegenden Vorgaben stammen aus dem Jahr 1977 – und lässt sich nur schwer auf die neuen technischen Möglichkeiten der Informationsgesellschaft anwenden.

Deshalb muss ein modernes Bundesdatenschutzgesetz geschaffen werden, worin bestehende Lücken sinnvoll ergänzt werden, welches für Bürgerinnen und Bürger Transparenz garantiert und klare Auskunftsrechte definiert. Dies bezieht ebenso das Fernmeldegeheimnis ein, das bedingt durch mannigfaltige neue Kommunikationsformen zu einem umfassenden Mediennutzungsgeheimnis weiterentwickelt werden muss. Da die Entwicklung der neuen Technologien ständig fortschreitet, ist eine kontinuierliche Überprüfung und Anpassung an neue Möglichkeiten im Umgang mit personenbezogenen Daten unverzichtbar.

II. Datenschutz und Sicherheitspolitik

1. Terrorismus

Terroristische Bedrohungen dürfen nicht als Rechtfertigung dienen, um das informationelle Selbstbestimmungsrecht zu untergraben, nach dem Motto „viel hilft viel“. Die gesammelten Daten müssen durch die Sicherheitsbehörden verantwortlich und zweckgebunden verwaltet werden.

Transparenz und Zweckbindung als Schlüssel für das Vertrauen zwischen Staat und BürgerInnen.

Nur wenn der Einzelne weiß, welche Daten zu welchem Zweck über ihn angefordert und

gesammelt werden und die Daten zu diesem ausschließlichen Zweck verwendet werden, kann eine Vertrauensbasis geschaffen werden. Diese war im Vorfeld von Heiligendamm - um nur ein Beispiel aus jüngster Vergangenheit zu nennen - verspielt worden.

Werden Daten aber entgegen vorheriger Ankündigung für andere Zwecke ausgewertet oder gehandelt, so entsteht Misstrauen. So geschehen im Fall der Maut-Erfassung, bei der die Datensammlung in eine Sicherheitsdatei umgewandelt wurde.

Das Gleiche betrifft die verdachtsunabhängige Vorratsdatenspeicherung, wie Telekommunikationsüberwachung und die Überwachung der Internet-Nutzung.

Die geplante europaweite verdachtlose Totalüberwachung der elektronischen Kommunikation ist mit keinem Strafverfolgungszweck zu begründen und steht damit in keinem rechtsstaatlichen Verhältnis zu einer dadurch angeblich höheren Sicherheit der Bürgerinnen und Bürger.

Der Bundesinnenminister fordert zudem die heimliche Online-Fahndung. Das muss unterbunden werden. Die Polizei darf nur im Internet fahnden, wenn der konkrete Verdacht auf Straftaten oder Gefährdungen vorliegt.

Ein Großteil des Privatlebens ist mittlerweile in PCs im privaten Umfeld gespeichert. Wird dem Staat der heimliche Zugang zum heimischen PC erlaubt, ist einem - mit rechtsstaatlichen Prinzipien unvereinbaren - Aushorchen per Trojaner Tür und Tor geöffnet.

Durch RFID-Chips, Fingerabdrücke und Gesichtsbild in Personalausweisen, wie es der derzeitige Bundesinnenminister sie fordert, entstehen völlig neue Sicherheitsrisiken: der Identitätsdiebstahl als neue Form von Kriminalität. Hieraus folgt:

Keine biometrischen Daten in Ausweisen.

In den USA beispielsweise warnt die Smart Card Alliance davor, RFID-Chips, die über mehrere Meter kontaktlos ausgelesen werden können, für ID-Karten zu verwenden. Dies sei zu unsicher. Sollten die Forderungen des Bun-

desinnenministers umgesetzt werden, sehen wir den

Identitätsdiebstahl als eine neue Form der Kriminalität.

2. Der unbemerkte "gläserne Mensch"

Unter dem Deckmantel der Verwaltungsmodernisierung sollen - ebenfalls nach dem Vorhaben des Bundesinnenministers - verbotene Personenkenneichen eingeführt werden. Damit wird die Zweckbindung der Meldedaten in Einwohnermeldeämtern aufgehoben, die Daten können zwischen den Behörden ausgetauscht werden. Jede Bürgerin und jeder Bürger enthält eine eigene Nummer, unter der die Daten jedes Einzelnen umfassend erfasst, registriert und jederzeit abgerufen werden können.

Personenkenneichen müssen verboten bleiben

Daten von Einwohnermeldeämtern dürfen nicht zweckentfremdet – zu wirtschaftlichen oder parteipolitischen Zwecken – weitergegeben werden.

3. Gezielte Medienpädagogik

Uns ist klar, dass viele Menschen, gerade Jugendliche, sich über die Gefahren und Konsequenzen des sorglosen Umgangs mit ihren Daten, sei es im Internet oder anderswo, überhaupt nicht bewusst sind.

Umso dringlicher ist es eine konsequente Aufklärung bereits in der Grundschule zu vermitteln. Nur bestens informierte Jugendliche werden zu verantwortungsvoll handelnden Erwachsenen. Der Erstkontakt mit den so genannten „Neuen Medien“ erfolgt heute, statistisch betrachtet, bereits in den ersten sechs Lebensjahren. Die Berücksichtigung des Datenschutzes verlangt verpflichtend nach einer aufklärenden Lehre bereits in der Grundschule.

4. Datenschutz – eine Frage der Ethik

Datenschutz ist eine Frage der Ethik und damit auch als Bestandteil der unantastbaren Menschenwürde, wie sie nach Art. 1 GG verfassungsmäßig garantiert ist, zu sehen. Hieraus folgt, dass jede Bürgerin und jeder Bürger das das Recht hat,

- die über sie und ihn gespeicherten Daten einzusehen und auf Wunsch zu korrigieren
- bei jeglicher Datenweitergabe an andere Stellen um Einwilligung befragt zu werden
- bei unsachgemäßem Gebrauch darüber informiert zu werden und
- keiner heimlichen Überwachung auf Grund eines Generalverdachts unterstellt zu werden

UnternehmensGrün fordert im Einzelnen:

- **Das Recht der Bürger und Bürgerinnen auf informationelle Selbstbestimmung**
- **Die Einführung des Datenschutzes in das Grundgesetz**
- **Die sofortige gesetzliche Umsetzung des EU-Vertrages zur „Unabhängigkeit des Datenschutzbeauftragten“**
- **Kein gesetzwidriges Sonderabkommen mit den USA zur Weitergabe von Flugpassdaten**
- **Die Schaffung eines neuen, modernen Bundesdatenschutzgesetzes, welches ausdrücklich eine ständige Überprüfung und Anpassung an die neuen Technologien vorsieht**
- **Die Aufnahme von präzisen Zweckbindungs- und Lösungsregelungen, Bestimmungen über die elektronische Kommunikation und Überwachung und den besonderen Schutz sensibler**

Gesundheits- und Gendaten in das Datenschutzgesetz

- **Die Einführung eines verlässlichen, vereinheitlichten Gütesiegels für Unternehmen, Produkte und Institutionen die entsprechenden Zertifizierungen erwerben**
- **Waren, die mit RFID-Chips bestückt sind, müssen als solche markiert werden und die Chips müssen bei Bedarf ohne komplizierte Anleitung deaktiviert werden können**
- **Eine Transparenz und Offenlegung von Scoring Verfahren**
- **Eine bessere Vorbereitung der Datenschutzbeauftragten in den Betrieben sowie eine größere Unabhängigkeit von der Geschäftsleitung**
- **Die Möglichkeit für KMU`s die gesetzlich geforderten Aufgaben der betrieblichen Datenschutzbeauftragten auf Verbände und Kammern zu übertragen**
- **Keine verdachtsunabhängige Vorratsdatenspeicherung**
- **Keine heimliche Online Fahndung**
- **Keine biometrischen Daten in Ausweispapieren**
- **Keine Einführung von Personenkennzeichen in den Einwohnermeldeämtern**
- **Aufklärung über den Datenschutz im Rahmen einer verbindlichen Medienpädagogik bereits ab der Grundschule**

Wolfgang Otto

Vorstand Unternehmensgrün