

**65. Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
am 27./28. März 2003 in Dresden**

EntschlieÙung

**Forderungen der Konferenz der Datenschutzbeauftragten des Bundes
und der Länder an Bundesgesetzgeber und Bundesregierung**

Immer umfassendere Datenverarbeitungsbefugnisse, zunehmender Datenhunger, sowie immer weitergehende technische Möglichkeiten zur Beobachtung und Durchleuchtung der Bürgerinnen und Bürger zeichnen den Weg zu immer mehr Registrierung und Überwachung vor. Das Grundgesetz gebietet dem Staat, dem entgegenzutreten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, das Recht auf informationelle Selbstbestimmung der Bürger und Bürgerinnen, wie in den Verfassungen zahlreicher deutscher Länder und in den Vorschlägen des Europäischen Verfassungskonvents, als eigenständiges Grundrecht im Grundgesetz zu verankern.

Die Datenschutzbeauftragten werden Bundesgesetzgeber und Bundesregierung bei der Weiterentwicklung des Datenschutzes unterstützen. Sie erwarten, dass die in der Koalitionsvereinbarung enthaltenen Absichtserklärungen zur umfassenden Reform des Datenschutzrechtes in der laufenden Legislaturperiode zügig verwirklicht werden.

Sie sehen dabei folgende essentielle Punkte:

- ◆ Schwerpunkte für eine Modernisierung des Bundesdatenschutzgesetzes
 - Im Vordergrund muss die Stärkung der informationellen Selbstbestimmung und des Selbstdatenschutzes stehen: Jeder Mensch

muss tatsächlich selbst entscheiden können, welche Datenspuren er hinterlässt und wie diese Datenspuren verwertet werden. Ausnahmen müssen so gering wie möglich gehalten und stets in einer präzise formulierten gesetzlichen Regelung festgeschrieben werden.

- Es muss im Rahmen der gegebenen Strukturunterschiede ein weitgehend gleichmäßiges Schutzniveau für den öffentlichen und den nicht öffentlichen Bereich gelten. Die Einwilligung in die Datenverarbeitung darf nicht zur Umgehung gesetzlicher Aufgaben- und Befugnisgrenzen missbraucht werden.
 - Die Freiwilligkeit der Einwilligung muss gewährleistet sein.
 - Vor der Nutzung von Daten für Werbezwecke muss die informierte und freie Einwilligung der Betroffenen vorliegen („opt in“ statt „opt out“).
- ◆ Technischer Datenschutz

Wesentliche Ziele des technischen Datenschutzes müssen darin bestehen, ein hohes Maß an Transparenz bei der Datenverarbeitung zu erreichen und den System- und Selbstdatenschutz zu stärken. Hersteller und Anbieter müssen verpflichtet werden, den Nutzerinnen und Nutzern die geeigneten Mittel zur Geltendmachung ihrer Rechte auch auf technischem Wege zur Verfügung zu stellen.

- ◆ Realisierung von Audit und Gütesiegel als marktwirtschaftliche Elemente im Datenschutz

Bislang ist das Datenschutzrecht in Deutschland in erster Linie als Ordnungsrecht ausgestaltet. Seine Einhaltung soll durch Kontrolle, Kritik und Beanstandung durchgesetzt werden. Dagegen fehlen Anreize für Firmen und Behörden, vorbildliche Datenschutzkonzepte zu verwirklichen. Mit dem Datenschutzaudit könnte Firmen und Behörden ein gutes Datenschutzkonzept bestätigt werden und es würde ihnen die

Möglichkeit eröffnen, damit zu werben. Das Gütesiegel ist ein Anreiz, IT-Produkte von vornherein datenschutzgerecht zu gestalten und damit Marktvorteile zu erringen.

Eine datenschutzkonforme Technikgestaltung ist eine wichtige Voraussetzung für einen effizienten Datenschutz. Audit und Gütesiegel würden die Aufmerksamkeit auf das Thema Datenschutz lenken und so die stärkere Einbeziehung von Kundinnen und Kunden fördern. Deshalb müssen die noch ausstehenden gesetzlichen Regelungen zur Einführung des im Bundesdatenschutzgesetz vorgesehenen Datenschutzaudits umgehend geschaffen werden.

- ◆ Förderung von datenschutzgerechter Technik

Die Verwirklichung des Grundrechtsschutzes hängt nicht allein von Gesetzen ab. Auch die Gestaltung der Informationstechnik hat großen Einfluss auf die Möglichkeit für alle Menschen, ihr Recht auf informationelle Selbstbestimmung auszuüben. Bisher spielt das Thema Datenschutz bei den öffentlichen IT-Entwicklungsprogrammen allenfalls eine untergeordnete Rolle. Neue IT-Produkte werden nur selten unter dem Blickwinkel entwickelt, ob sie datenschutzgerecht, datenschutzfördernd oder wenigstens nicht datenschutzgefährdend sind.

Notwendig ist, dass Datenschutz zu einem Kernpunkt im Anforderungsprofil für öffentliche IT-Entwicklungsprogramme wird.

Datenschutzgerechte Technik stellt sich nicht von alleine ein, sondern bedarf auch der Förderung durch Anreize. Neben der Entwicklung von Schutzprofilen und dem Angebot von Gütesiegeln kommt vor allem die staatliche Forschungs- und Entwicklungsförderung in Betracht. Die Entwicklung datenschutzgerechter Informationstechnik muss zu einem Schwerpunkt staatlicher Forschungsförderung gemacht werden.

- ◆ Anonyme Internetnutzung

Das Surfen im World Wide Web mit seinen immensen Informationsmöglichkeiten und das Versenden von e-mails sind heute für viele selbstverständlich. Während aber in der realen Welt jeder Mensch zum Beispiel in einem Buchladen stöbern oder ein Einkaufszentrum durchstreifen kann, ohne dass sein Verhalten registriert wird, ist dies im Internet nicht von vornherein gewährleistet. Dort kann jeder Mausklick personenbezogene Datenspuren erzeugen, deren Summe zu einem aussagekräftigen Persönlichkeitsprofil und für vielfältige Zwecke (z. B. Marketing, Auswahl unter Stellenbewerbungen, Observation von Personen) genutzt werden kann. Das Recht auf Anonymität und der Schutz vor zwangsweiser Identifizierung sind in der realen Welt gewährleistet (in keiner Buchhandlung können Kundinnen und Kunden dazu gezwungen werden, einen Ausweis vorzulegen). Sie werden aber im Bereich des Internet durch Pläne für eine umfassende Vorratsspeicherung von Verbindungs- und Nutzungsdaten bedroht.

Das Recht jedes Menschen, das Internet grundsätzlich unbeobachtet zu nutzen, muss geschützt bleiben. Internet-Provider dürfen nicht dazu verpflichtet werden, auf Vorrat alle Verbindungs- und Nutzungsdaten über den betrieblichen Zweck hinaus für mögliche zukünftige Strafverfahren oder geheimdienstliche Observationen zu speichern.

- ◆ Unabhängige Evaluierung der Eingriffsbefugnisse der Sicherheitsbehörden

Schon vor den Terroranschlägen des 11. September 2001 standen den deutschen Sicherheitsbehörden nach einer Reihe von Antiterrorgesetzen und Gesetzen gegen die Organisierte Kriminalität weitreichende Eingriffsbefugnisse zur Verfügung, die Datenschutzbeauftragten und Bürgerrechtsorganisationen Sorgen bereiteten:

Dies zeigen Videoüberwachung, Lauschangriff, Rasterfahndung, langfristige Aufbewahrung der Daten bei der Nutzung des Internet und der Telekommunikation, Zugriff auf Kundendaten und Geldbewegungen bei den Banken.

Durch die jüngsten Gesetzesverschärfungen nach den Terroranschlägen des 11. September 2001 sind die Freiräume für unbeobachtete individuelle oder gesellschaftliche Aktivitäten und Kommunikation weiter eingeschränkt worden. Bürgerliche Freiheitsrechte und Datenschutz dürfen nicht immer weiter gefährdet werden.

Nach der Konkretisierung der Befugnisse der Sicherheitsbehörden und der Schaffung neuer Befugnisse im Terrorismusbekämpfungsgesetz sowie in anderen gegen Ende der 14. Legislaturperiode verabschiedeten Bundesgesetzen ist vermehrt eine offene Diskussion darüber notwendig, wie der gebotene Ausgleich zwischen kollektiver Sicherheit und individuellen Freiheitsrechten so gewährleistet werden kann, dass unser Rechtsstaat nicht zum Überwachungsstaat wird. Dazu ist eine umfassende und systematische Evaluierung der im Zusammenhang mit der Terrorismusbekämpfung eingefügten Eingriffsbefugnisse der Sicherheitsbehörden notwendig.

Die Datenschutzbeauftragten halten darüber hinaus eine Erweiterung der im Terrorismusbekämpfungsgesetz vorgesehenen Pflicht zur Evaluierung der neuen Befugnisse der Sicherheitsbehörden auf andere vergleichbar intensive Eingriffsmaßnahmen – wie Telefonüberwachung, großer Lauschangriff und Rasterfahndung - für geboten.

Die Evaluierung muss durch unabhängige Stellen und an Hand objektiver Kriterien erfolgen und aufzeigen, wo zurückgeschnitten werden muss, wo Instrumente untauglich sind oder wo die negativen Folgewirkungen überwiegen. Wissenschaftliche Untersuchungsergebnisse zur Evaluation des Richtervorbehalts z. B. bei Telefonüberwachungen machen deutlich, dass der Bundesgesetzgeber Maßnahmen zur Stärkung des

Richtervorbehalts – und zwar nicht nur im Bereich der Telefonüberwachung - als grundrechtssicherndes Verfahrenselement ergreifen muss.

- ◆ **Stärkung des Schutzes von Gesundheitsdaten**

Zwar schützt die Jahrtausende alte ärztliche Schweigepflicht Kranke davor, dass Informationen über ihren Gesundheitszustand von denjenigen unbefugt weitergegeben werden, die sie medizinisch betreuen. Medizinische Daten werden aber zunehmend außerhalb des besonderen ärztlichen Vertrauensverhältnisses zu Patienten und Patientinnen verarbeitet. Telemedizin und High-Tech-Medizin führen zu umfangreichen automatischen Datenspeicherungen. Hinzu kommt ein zunehmender Druck, Gesundheitsdaten z. B. zur Einsparung von Kosten, zur Verhinderung von Arzneimittelnebenfolgen oder „zur Qualitätssicherung“ einzusetzen. Die Informatisierung der Medizin durch elektronische Aktenführung, Einsatz von Chipkarten, Nutzung des Internets zur Konsultation bis hin zur ferngesteuerten Behandlung mit Robotern erfordern es deshalb, dass auch die Instrumente zum Schutz von Gesundheitsdaten weiterentwickelt werden.

Der Schutz des Patientengeheimnisses muss auch in einer computerisierten Medizin wirksam gewährleistet sein. Die Datenschutzbeauftragten begrüßen deshalb die Absichtserklärung in der Koalitionsvereinbarung, Patientenschutz und Patientenrechte auszubauen. Dabei ist insbesondere sicherzustellen, dass Gesundheitsdaten außerhalb der eigentlichen Behandlung soweit wie möglich und grundsätzlich nur anonymisiert oder pseudonymisiert verarbeitet werden dürfen, soweit die Verarbeitung im Einzelfall nicht durch ein informiertes Einverständnis gerechtfertigt ist. Das Prinzip des informierten und freiwilligen Einverständnisses ist insbesondere auch für eine Gesundheitskarte zu beachten und zwar auch für deren Verwendung im Einzelfall.

Der Bundesgesetzgeber wird auch aufgefordert gesetzlich zu regeln, dass Patientendaten, die in Datenverarbeitungsanlagen außerhalb von Arztpraxen und Krankenhäusern verarbeitet werden, genauso geschützt sind wie die Daten in der ärztlichen Praxis.

Geprüft werden sollte schließlich, ob und gegebenenfalls wie der Schutz von Gesundheitsdaten durch Geheimhaltungspflicht, Zeugnisverweigerungsrecht und Beschlagnahmeverbot auch dann gewährleistet werden kann, wenn diese, z. B. in der wissenschaftlichen Forschung, mit Einwilligung oder auf gesetzlicher Grundlage von anderen Einrichtungen außerhalb des Bereichs der behandelnden Ärztinnen und Ärzte verarbeitet werden.

- ◆ **Datenschutz und Gentechnik**

Die Entwicklung der Gentechnik ist atemberaubend. Schon ein ausgefallenes Haar, ein Speichelrest an Besteck oder Gläsern, abgeschürfte Hautpartikel oder ein Blutstropfen - dies alles eignet sich als Untersuchungsmaterial, um den genetischen Bauplan eines Menschen entschlüsseln zu können. Inzwischen werden Gentests frei verkäuflich angeboten. Je mehr Tests gemacht werden, desto größer wird das Risiko für jeden Menschen, dass seine genetischen Anlagen von anderen auch gegen seinen Willen analysiert werden. Versicherungen oder Arbeitgeber und Arbeitgeberinnen werden ebenfalls Testergebnisse erfahren wollen.

Niemand darf zur Untersuchung genetischer Anlagen gezwungen werden; die Durchführung eines gesetzlich nicht zugelassenen Tests ohne Wissen und Wollen der betroffenen Person und die Nutzung daraus gewonnener Ergebnisse muss unter Strafe gestellt werden.

In der Koalitionsvereinbarung ist der Erlass eines „Gen-Test-Gesetzes“ vorgesehen. Ein solches Gesetz ist dringend erforderlich, damit der datenschutzgerechte Umgang mit genetischen Daten gewährleistet wird.

Die Datenschutzbeauftragten haben dazu auf ihrer 62. Konferenz in Münster vom 24. bis 26. Oktober 2001 Vorschläge vorgelegt.

- ◆ **Datenschutz im Steuerrecht**

Im bisherigen Steuer- und Abgabenrecht finden sich äußerst lückenhafte datenschutzrechtliche Regelungen. Insbesondere fehlen grundlegende Rechte, wie ein Akteneinsichts- und Auskunftsrecht. Eine Pflicht zur Information der Steuerpflichtigen über Datenerhebungen bei Dritten fehlt ganz.

Die jüngsten Gesetzesnovellen und Gesetzesentwürfe, die fortschreitende Vernetzung und multinationale Vereinbarungen verschärfen den Mangel: Immer mehr Steuerdaten sollen zentral durch das Bundesamt für Finanzen erfasst werden. Mit einheitlichen Personenidentifikationsnummern sollen Zusammenführungen und umfassende Auswertungen der Verbunddaten möglich werden. Eine erhebliche Ausweitung der Kontrollmitteilungen von Finanzbehörden und Kreditinstituten, die ungeachtet der Einführung einer pauschalen Abgeltungssteuer geplant ist, würde zweckungebundene und unverhältnismäßige Datenübermittlungen gestatten. Die zunehmende Vorratserhebung und –speicherung von Steuerdaten entspricht nicht dem datenschutzrechtlichen Grundsatz der Erforderlichkeit.

Die Datenschutzbeauftragten fordern deshalb, die Aufnahme datenschutzrechtlicher Grundsätze in das Steuerrecht jetzt anzugehen und den Betroffenen die datenschutzrechtlichen Informations- und Auskunftsrechte zuzuerkennen.

- ◆ **Arbeitnehmerdatenschutz**

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, zum Beispiel durch

- die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,
- die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutzstandard der EG-Datenschutzrichtlinie gilt,
- die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,
- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die hierzu von den Arbeitsgerichten entwickelten Schranken wirken unmittelbar nur im jeweils entschiedenen Einzelfall und sind auch nicht allen Betroffenen hinreichend bekannt. Das seit vielen Jahren angekündigte Arbeitnehmerdatenschutzgesetz muss hier endlich klare gesetzliche Vorgaben schaffen.

Die Datenschutzbeauftragten fordern deshalb, dass für die in der Koalitionsvereinbarung enthaltene Festlegung zur Schaffung von gesetzlichen Regelungen zum Arbeitnehmerdatenschutz nunmehr rasch ein ausformulierter Gesetzentwurf vorgelegt und anschließend zügig das Gesetzgebungsverfahren eingeleitet wird.

- ◆ **Stärkung einer unabhängigen, effizienten Datenschutzkontrolle**

Die Datenschutzbeauftragten fordern gesetzliche Vorgaben, die die völlige Unabhängigkeit der Datenschutzkontrolle sichern und effektive Einwirkungsbefugnisse gewährleisten, wie dies der Art. 28 der EG-Datenschutzrichtlinie gebietet.

Die Datenschutzkontrollstellen im privaten Bereich haben bis heute nicht die völlige Unabhängigkeit, die die Europäische Datenschutzrichtlinie vorsieht. So ist in der Mehrzahl der deutschen Länder die Kontrolle über

den Datenschutz im privaten Bereich nach wie vor bei den Innenministerien und nachgeordneten Stellen angesiedelt und unterliegt damit einer Fachaufsicht. Selbst in den Ländern, in denen die Landesbeauftragten diese Aufgabe wahrnehmen, ist ihre Unabhängigkeit nicht überall richtlinienkonform ausgestaltet.

- ◆ Stellung des Bundesdatenschutzbeauftragten

Die rechtliche Stellung des Bundesdatenschutzbeauftragten als unabhängiges Kontrollorgan muss im Grundgesetz abgesichert werden.

- ◆ Verbesserung der Informationsrechte

Die im Bereich der Informationsfreiheit tätigen Datenschutzbeauftragten unterstützen die Absicht in der Koalitionsvereinbarung, auf Bundesebene ein Informationsfreiheitsgesetz zu schaffen. Nach ihren Erfahrungen hat sich die gemeinsame Wahrnehmung der Aufgaben zum Datenschutz und zur Informationsfreiheit bewährt, weshalb sie auch auf Bundesebene realisiert werden sollte. Zusätzlich muss ein Verbraucherinformationsgesetz alle Produkte und Dienstleistungen erfassen und einen Informationsanspruch auch gegenüber Unternehmen einführen.