ARGE DATEN - Österreichische Gesellschaft für Datenschutz
Dr. Hans G. Zeger, 1170 Wien, Sautergasse 20, Tel: +43/1/31 077 40 - Fax.: +43/1/31 031 02 - PSK-Konto: 7214.741 - DVR: 0530794

Wien, 24.03.1994 | Ihr Zeichen: | Unser Zeichen: ARGPRÄ07.DOC

An das
Präsidium des Nationalrates

Parlament
1010 WIEN

GESETZENTWURF
Zl. 26 -GE/19 94
Datum: 28. MRZ. 1994
Verteilt 30. März 1994

Betreff: Entwurf Novelle des Datenschutzgesetzes GZ 810.026/0-V/3/94

Sehr geehrtes Präsidium!

In der Anlage übermitteln wir Ihnen die Stellungnahme der ARGE DATEN - Österreichische Gesellschaft für Datenschutz zum oben genannten Entwurf..

Mit freundlichen Grüßen

Dr. Hans G. Zeger, Präsident

Anlage: 25fach

Ab 1. April 94 neue Adresse: 1170 Wien, Sautergasse 20

Stellungnahme der ARGE DATEN zur

Novelle des Datenschutzgesetzes

(Entwurf des Bundeskanzleramtes)

Die ARGE DATEN begrüßt, daß mit dem vorliegenden Entwurf die Aufhebung des § 14 DSG durch den Verfassungsgerichtshof saniert werden soll. Wir sind jedoch der Ansicht, daß diese Novelle zum Anlaß genommen werden sollte, eine grundlegende Reform des Datenschutzgesetzes vorzunehmen. Das Gesetz ist nun über fünfzehn Jahre alt. Die Praxis hat - nicht zuletzt aufgrund des enorm angestiegenen EDV-Einsatzes - zahlreiche Probleme aufgezeigt. Wir wollen daher einige grundlegende Verbesserungen des österreichischen Datenschutzrechts anregen.

Übersicht

- Die Unterscheidung zwischen öffentlichem und privatem Bereich sollte aus dem Gesetz gestrichen werden. Die DSK sollte auch für den privaten Bereich zuständig sein.
- Die Schaffung einer Verbandsklage soll es ermöglichen, daß über Einzelfälle hinaus Datenschutzrechte durchgesetzt werden.
- Eine neu zu schaffende Zulassungs- und Prüfbehörde sollte bei Datenverarbeitern Systemprüfungen durchführen und Systeme approbieren. Damit soll die Einhaltung von Datensicherheits- und Datenschutzstandards sichergestellt werden. Dazu soll ein Katalog von entsprechenden Qualitätsstandards geschaffen werden.
- Ähnlich wie im Medienrecht soll auch bei Datenschutzverletzungen eine Entschädigung für erlittene ideelle Schäden gewährt werden.
- Vom rechtlichen Schutz sollen auch nicht automationsunterstützt verarbeitete Daten umfaßt sein.
- Juristische Personen sollen datenschutzrechtlich nicht geschützt sein, da die Informationsrechte natürlicher Personen meist überwiegen und die für Unternehmen wichtigen Daten ohnehin durch das Betriebs- und Geschäftsgeheimnis geschützt sind.
- Der Katalog der Datenschutzrechte soll erweitert werden, etwa um das Widerspruchsrecht oder um das Verbot der rein automationsunterstützten Personenbeurteilung.

1. Rechtsschutzsystem des DSG

1.1. Zuständigkeit der DSK auch im privaten Bereich

Im privatrechtlichen Bereich hat der Betroffene, der sich in seinen Datenschutzrechten verletzt fühlt, nur die Möglichkeit der Klage bei Gericht. Einem großen Prozeßrisiko und hohen Kosten steht dabei eine zweifelhafte Aussicht auf Erfolg gegenüber: Man kann nämlich nur auf Unterlassung, nicht auch auf Ersatz der (ideellen) Schäden klagen. Daher verzichteten in der Vergangenheit die Betroffenen in den meisten Fällen auf eine Klage.

Auf die Unterscheidung in einen "öffentlichen" und einen "privaten" Bereich sollte daher verzichtet werden. Die Datenschutzkommission sollte einzige Beschwerdestelle für den gesamten Bereich des Datenschutzes sein.

Damit wäre auch das äußerst schwierige Problem der Abgrenzung zwischen öffentlichem und privatem Bereich gelöst. Die mißglückte Regelung der Abgrenzung dieser beiden Bereiche in den §§ 4 und 5 DSG war in der Begründung des Verfassungsgerichtshofes zur Aufhebung des § 14 DSG wesentlich und hat schon einmal (bei der Aufhebung des § 5 Abs. 2 DSG im Jahr 1989) für verfassungsrechtliche Probleme gesorgt.

1.2. Verbandsklage

Ein weiteres Rechtsschutzproblem besteht darin, daß nur Betroffene berechtigt sind, eine Beschwerde bei der DSK oder eine Klage bei Gericht einzubringen. Die Betroffenen wissen aber oft gar nicht, daß ihre Datenschutzrechte verletzt wurden und sind daher nicht motiviert, für die Durchsetzung ihrer Rechte zu sorgen. In vielen Fällen (etwa bei den "freiwilligen Verzichtserklärungen", die zu unterschreiben potentielle Versicherungs- und Bankkunden genötigt werden) schrecken Betroffene vor rechtlichen Schritten zurück, weil sie persönliche Nachteile befürchten (etwa die Ablehnung des Versicherungsantrags oder die Kündigung des Bankkontos).

Als problematisch hat sich auch herausgestellt, daß Entscheidungen nur im Einzelfall gelten. Stellt die DSK etwa aufgrund einer Beschwerde fest, daß die Verarbeitung der Daten einer bestimmten Person rechtswidrig war, so muß der Auftraggeber die Daten nur in diesem Einzelfall löschen - auch wenn viele andere in gleicher Weise betroffen sind. Die DSK hätte zwar (§ 15 DSG) die Befugnis, in solchen Fällen ein amtswegiges Verfahren einzuleiten und einen für alle Betroffenen gültigen Bescheid zu erlassen, der ARGE DATEN ist ein solcher Bescheid der DSK bis jetzt allerdings nicht bekannt.

Es wäre daher die Einrichtung der Möglichkeit einer Verbandsklage sinnvoll. Wie etwa im Bereich des unlauteren Wettbewerbs sollte es die Möglichkeit geben, daß Vereine zur Förderung des

Datenschutzes ein Klagerecht in solchen Fällen haben, die einen größeren Personenkreis betreffen. Als Vorbild für die Formulierung könnte § 14 UWG herangezogen werden.

1.3. Schlichtungsstellen und Datenschutzanwalt

Weitere Möglichkeiten zur Verbesserung des Rechtsschutzes sind die Einführung von Schlichtungsstellen (wie im Mietrecht) oder eines Datenschutzanwalt (vergleichbar dem Patientenanwalt). Solche Stellen sind aber nur sinnvoll, wenn sie eine erste Instanz mit Entscheidungsbefugnis sind. Die derzeit im Bundeskanzleramt eingerichtete Schlichtungsstelle hat keine durch Gesetz eingeräumte Kompetenz und kann daher wenig ausrichten. Eine im DSG verankerte Schlichtungsstelle hingegen könnte innerhalb weniger Wochen eine erste bindende Entscheidung fällen.

Einem Datenschutzanwalt könnte die Kompetenz übertragen werden, in Fällen, die an ihn herangetragen werden, oder die ihm aus den Medien bekanntwerden, Rechtsschutz zu gewähren, indem er die Betroffenen vor den zuständigen Behörden vertritt und - wenn die Anrufung eines Gerichts oder ein anderes kostenaufwendiges Verfahren nötig ist - die Prozeßkosten übernimmt. Der Datenschutzanwalt könnte gezielt aktuelle Fälle aufgreifen und daher sehr schnell auf neue technische Entwicklungen reagieren.

1.4. Schadenersatzrecht

Schon beim Beschluß des DSG im Jahr 1978 forderte der Verfassungsausschuß im Nationalrat die Bundesregierung auf, einen Entwurf für die zur Ergänzung des DSG notwendigen schadenersatzrechtlichen Regelungen vorzulegen. Seither sind über 15 Jahre vergangen und es gibt noch immer keine Regelung. Nur zum Teil kann Schadenersatz geltend gemacht werden, etwa bei Ehrenbeleidigung oder Kreditschädigung. In allen Fällen muß derzeit aber ein Vermögensschaden (etwa Verdienstentgang) nachgewiesen werden. Ungedeckt sind alle ideellen Schäden, also solche, die die Gefühlssphäre betreffen.

Es sollte (vergleichbar dem Schmerzengeld bei Körperverletzung) auch der Schaden aufgrund einer Verletzung der Privatsphäre abgedeckt werden. - Das Medienrecht ging in einer vergleichbaren Problematik neue Wege und hat für verschiedene Fälle einen Schadenersatz "für die erlittene Kränkung" (in den meisten Fällen bis zu 200.000 S) vorgesehen. Einen ähnlichen Anspruch sollte man auch im Datenschutzrecht schaffen. Der Entschädigungsanspruch sollte dabei (wie im Medienrecht) schon mit der Verletzung des Gesetzes entstehen und nicht davon abhängen, daß der Betroffene die konkrete Höhe seines Schaden (z. B. Kränkung) ziffernmäßig nachweist.

2. Zulassung und Qualitätsprüfung von Datenverarbeitungen

2.1. Zulassungs- und Prüfbehörde

Die Registrierung von Datenverarbeitern im Datenverarbeitungsregister (DVR) erfolgt derzeit nach einem rein formalen Konzept. Die Sicherheit und Qualität der zu verarbeitenden Daten wird nicht geprüft. Daher sollte eine Zulassungsbehörde geschaffen werden, die nach einem standardisierten Bewertungskatalog (z. B. den derzeit europaweit ausgearbeiteten "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)") prüft, ob die geplante Verarbeitung gewissen datenschutzrechtlichen Mindestanforderungen entspricht. Zu vergleichen wäre eine solche Behörde z. B. mit der KFZ-Zulassungsbehörde oder dem TÜV.

Es ist nicht unbedingt nötig, daß alle Datenverarbeiter dazu verpflichtet werden, eine derartige Zulassung zu beantragen. Es wäre auch möglich, Anreize zu schaffen, damit Datenverarbeiter und Anbieter von Software von sich aus beantragen, die verwendete Software approbieren zu lassen. Ein solcher Anreiz könnte etwa eine Beweislastumkehr sein: Beim approbierten Produkt wird gesetzlich vermutet, daß es die geprüften Eigenschaften besitzt. Man könnte auch vorsehen, daß sich der Betreiber einer nicht approbierten Datenverarbeitung eher eine behördliche Systemprüfung (siehe gleich unten) gefallen lassen muß.

Zu schaffen wäre auch eine Prüfbehörde, die bei bestehenden Datenverarbeitungen Systemprüfungen durchführt. Derzeit werden solche Systemprüfungen nur in sehr geringer Zahl und nur im öffentlichen Bereich von der DSK durchgeführt. Eine Behörde, die etwa einen Adreßverlag systematisch auf die Einhaltung des DSG prüft, gibt es nicht. Daher kommt es z. B. immer wieder vor, daß ein Datenverarbeiter nicht mehr weiß, woher bestimmte von ihm verarbeitete Daten stammen oder an wen er sie übermittelt hat.

2.2. Qualitätskriterien

Als Minimalanforderung für die Qualität von Daten können die folgenden Qualitätsprinzipien der Art. 5 und 6 des von Österreich ratifizierten Europarats-Abkommens zum Datenschutz angesehen werden. In Österreich ist nur ein Teil dieser Prinzipien verwirklicht (obwohl Österreich durch die Ratifizierung des Abkommens dazu verpflichtet wäre, alles umzusetzen).

- Personenbezogene Daten müssen nach Treu und Glauben und auf rechtmäßige Weise beschafft sein und verarbeitet werden (Prinzip der Rechtmäßigkeit der Datenverarbeitung)
- Sie dürfen nur für festgelegte und rechtmäßige Zwecke verwendet werden (Prinzip der Zweckbindung von Datenverarbeitungen)
- Die Daten müssen für diese Zwecke erheblich sein und dürfen nicht darüber hinausgehen (Prinzip der minimalen Datenmenge)

- Sie müssen sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht worden sein.
- Sie dürfen nicht länger als nötig aufbewahrt werden (Prinzip der minimalen Speicherdauer).
- Besonders sensible Daten (etwa rassische oder ethnische Zugehörigkeit, Religionsbekenntnis, politische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheitsdaten, Sexualleben) müssen auch besonders geschützt werden.

Ein Problem dieser und anderer Prinzipien ist, daß sie nur über Aufsichtsbehörden oder Verbandsklagen effektiv durchsetzbar sind. Natürlich müssen auch nach geltendem Recht rechtswidrig ermittelte Daten gelöscht werden. Sie werden aber nur im Einzelfall gelöscht - oft erst nach langwierigen Verfahren. Daß der Datenverarbeiter auch die Daten Tausender anderer, in ähnlichem Maße betroffener, löscht, wird ihm von niemandem vorgeschrieben.

3. Umfang des Rechts auf Datenschutz

3.1. Nicht automationsunterstützt verarbeitete Daten

Derzeit sind von wichtigen Teilen des Datenschutzrechts (Rechte auf Auskunft, Richtigstellung, Löschung) nur die automationsunterstützt verarbeiteten Daten umfaßt. Wichtige Datensammlungen liegen aber in Form von Karteien vor. Manchmal sind im Computer nur Verweise auf die (viel wichtigeren) Akten gespeichert. Außerhalb eines Verwaltungsverfahrens hat aber niemand das Recht, in seine eigenen Akten Einsicht nehmen zu können.

Auch im DSG sollten die Rechte auf Auskunft, Richtigstellung und Löschung (so wie derzeit schon der Anspruch auf Geheimhaltung nach § 1 Abs. 1 DSG) unabhängig davon geltend gemacht werden können, ob Daten automationsunterstützt verarbeitet werden oder nicht. Die Datenschutzrechte sollen für alle Datensammlungen gelten, die in irgendeiner Form organisiert oder strukturiert sind.

3.2. Juristische Personen

Die Erfahrung hat gezeigt, daß der Datenschutz auch juristischer Personen von diesen eher mißbraucht als benötigt wird. Probleme gibt es vor allem im Bereich des Umweltschutzes und des Konsumentenschutzes. Hier haben die Bürger z. B. einen legitimen Anspruch darauf, zu erfahren, wer die Umwelt wie stark verschmutzt oder aus welchen Substanzen ein im Handel erhältliches Produkt besteht. In vielen Fällen verfügen die zuständigen Behörden über die gewünschten Informationen, können diese aber nicht an ratsuchende Bürger weitergeben, weil dem die "Datenschutzinteressen" des Unternehmens entgegenstehen.

Die Mehrzahl der Datenschutzgesetze anderer europäischer Staaten sehen nur einen Schutz natürlicher Personen vor. Auch das

österreichische DSG sollte bloß natürliche Personen schützen. Die für die Unternehmen wirklich wichtigen Daten werden ohnehin durch das Betriebs- und Geschäftsgeheimnis geschützt.

4. Neue Grundrechte

4.1. Zustimmungserklärungen

Ein großes Problem (vor allem im Bereich der Banken und Versicherungen) ist, daß Kunden oder möglichen Kunden eine allgemeine Verzichtserklärung zur Unterschrift vorgelegt wird. Versicherungen lassen sich damit etwa einen Freibrief zur Beschaffung von Gesundheitsdaten ausstellen.

Daher sollte ein Kernbereich besonders sensibler Daten definiert werden, bei dem man nicht auf das Grundrecht auf Datenschutz verzichten kann (vgl. den unverzichtbaren Anspruch auf Gewährleistung im Konsumentenschutzrecht). In diesen Kernbereich sollten etwa Daten zu Gesundheit oder Sexualleben fallen. Außerdem sollte in der Verfassung als Grundsatz festgeschrieben werden, daß Daten prinzipiell beim Betroffenen selbst ermittelt werden sollen.

Durch aufsichtsbehördliche Kontrolle und mit Verbandsklagen soll sichergestellt werden, daß die schon jetzt bestehenden Mindestanforderungen für derartige Zustimmungserklärungen eingehalten werden - etwa, daß diese nicht in allgemeinen Geschäftsbedingungen versteckt werden.

4.2. Informationspflichten

Datenverarbeiter sollten verpflichtet sein, Betroffene bei der Erhebung von Daten darüber zu informieren,

- wer für die Datenverarbeitung verantwortlich ist,
- für welchen Zweck die Daten erhoben werden,
- ob die Beantwortung der gestellten Fragen verpflichtend ist bzw. welche Konsequenzen eine unterlassene Beantwortung hat,
- an wen die Daten in der Folge voraussichtlich übermittelt werden und
- daß es die Rechte auf Auskunft, Richtigstellung und Löschung gibt.

Wird die Erhebung direkt beim Betroffenen durchgeführt, so ist diese Information (z. B. auf den zur Erhebung verwendeten Formularen) leicht möglich. Werden Daten von einem Dritten ermittelt, so soll der Betroffene verständigt werden müssen, daß seine Daten weitergegeben wurden. Eine solche Verständigungspflicht ist notwendig, damit der Betroffene überhaupt weiß, wem gegenüber er seine Rechte geltend machen kann.

4.3. Widerspruchsrecht

Derzeit gibt es das Problem, daß der Betroffene die Löschung einmal rechtmäßig ermittelter Daten nicht durchsetzen kann - obwohl der Datenverarbeiter die Daten nicht mehr benötigt oder sein Interesse an der weiteren Speicherung das Interesse des Betroffenen nicht mehr überwiegt. Daher sollte es für den Betroffenen das Recht geben, jederzeit Widerspruch dagegen einlegen zu können, daß seine Daten Gegenstand einer Verarbeitung sind. Wichtig ist dieses Recht vor allem bei Kunden- und Interessentendateien. Hier hat der Unternehmer meist nur ein geringes Interesse daran, daß der Kunde X oder die Kundin Y weiterhin gespeichert ist - diese aber wollen die Löschung, da sie dann sicher sein können, daß ihre Daten nicht an Adreßverlage übermittelt werden.

4.4. Verbot rein automationsunterstützter Personenbeurteilung

Es sollte verboten sein, jemanden ausschließlich aufgrund eines automationsunterstützt erstellten Personenprofils zu beurteilen und einer benachteiligenden oder beschwerenden Maßnahme zu unterwerfen.

Dieses Verbot umfaßt die rein automationsunterstützte Entscheidung, ob Personen von bestimmten Einrichtungen (etwa Bildungseinrichtungen, Universitäten, usw.) ausgeschlossen werden, ob ihnen als Stellenbewerber aufgrund automationsunterstützter Tests ein bestimmter Arbeitsplatz verwehrt wird oder ob sie aufgrund automatisierter Selektionskriterien keinen Zugnag zu bestimmten Förderungen, Subventionen oder Karrieremaßnahmen erhalten.

Ein weiteres Problem in diesem Zusammenhang sind die sogenannten "Verknüpfungsabfragen": Der wachsende Einsatz großer Datensammlungen macht es immer leichter, innerhalb kurzer Zeit eine Gruppe von "Verdächtigen" einzugrenzen. Es gibt eine wachsende Tendenz zu Fragestellungen wie den folgenden: "Wer bekommt mehr als eine bestimmte Anzahl von Medikamenten verschrieben?" (vielleicht verkauft er sie an Drogensüchtige), "Wer hat seine Versicherung oft gewechselt?" (vielleicht ein Risikofall), "Wer ist öfter als zehnmal monatlich in Ungarn?" (vielleicht ein Schlepper oder Schmuggler) Eine völlig unbeteiligte Person muß sich dann eine lästige Überprüfung oder eine echte Benachteiligung (etwa die Ablehnung eines Versicherungsantrags) gefallen lassen - nicht, weil man ihr etwas vorwerfen könnte oder weil ein konkreter Verdacht besteht, sondern weil sie im Computer irgendwie aufgefallen ist.

5. Sonderregelungen für Spezialgebiete

Zuletzt möchten wir darauf hinweisen, daß eine Reihe von Spezialgebieten besondere Problemstellungen aufweisen, die auch eine gesonderte gesetzliche Regelung erfordern würden. Auch im Hinblick auf diese Gebiete ist eine grundlegende Diskussion des

österreichischen Datenschutzrechts dringend notwendig. Hier seien nur die wichtigsten Probleme stichwortartig dargestellt:

- Banken und Versicherungen: Zu den formularmäßigen "freiwilligen Zustimmungserklärungen" siehe oben. Ein weiteres Problem sind die zentralen Datensammlungen (etwa der Kreditschutzverbände), deren Datenqualität oft zweifelhaft ist. Eine gesetzliche Regelung sollte Mindeststandards für die Qualität der Daten vorsehen.

- Datensammlungen in Archiven und Bibliotheken, bei Medien und in öffentlichen Volltextdatenbanken ermöglichen in zunehmendem Ausmaß die automationsunterstützte Beantwortung von Fragen wie "Was ist in den letzten Jahren alles über Frau X in der Zeitung gestanden?". Diese Problemstellung (Informationsfreiheit vs. Datenschutz) entzieht sich weitgehend den Kategorien klassischer Datenschutzregelungen.

- Telekommunikation, insbesondere ISDN: In der EU wird parallel zur Datenschutzrichtlinie eine ISDN-Richtlinie diskutiert, in Deutschland gibt es schon seit Jahren detaillierte Sonderregelungen. Auch in Österreich müssen die technischen Möglichkeiten von ISDN gesetzlich kontrolliert werden. Das neue Fernmeldegesetz reicht dazu nicht aus.

- Weitere Rechtsgebiete sind etwa Statistik und Wissenschaft oder soziale Sicherheit und Gesundheit.