Eidgenössischer Datenschutzbeauftragter

Préposé fédéral à la protection des données

4. Tätigkeitsbericht 1996/97

4ème Rapport d'activités 1996/97

Eidgenössischer Datenschutzbeauftragter

Tätigkeitsbericht 1996/97

Der Eidgenössische Datenschutzbeauftragte hat dem Bundesrat periodisch einen Bericht über seine Tätigkeit vorzulegen (Art. 30 Datenschutzgesetz). Der vorliegende Bericht deckt den Zeitraum zwischen 1. April 1996 und 31. März 1997 ab.

INHALTSVERZEICHNIS

*: Originaltext auf Französisch

*: Originaltext auf Französisch

*: Originaltext auf Französisch

ABKÜRZUNGSVERZEICHNIS

AHVG	Bundesgesetz über die Alters- und Hinterlassenenversicherung
AHVV	Verordnung über die Alters- und Hinterlassenenversicherung
AUPER	Automatisiertes Personenregistratursystem
BAP	Bundesamt für Polizeiwesen
BSV	Bundesamt für Sozialversicherung
BUWAL	Bundesamt für Umwelt, Wald und Landschaft
DOSIS VO	Verordnung über das Datenverarbeitungssystem zur Bekämpfung des illegalen Betäubungsmittelhandels
DSG	Bundesgesetz über den Datenschutz
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDSK	Eidgenössische Datenschutzkommission
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EMRK	Europäische Menschenrechtskonvention
EPA	Eidgenössisches Personalamt
ETV	Die Elektronischen Telefonverzeichnisse
EVD	Eidgenössisches Volkswirtschaftsdepartement
FMH	Verbindung der Schweizer Ärzte (Foederatio Medicorum Helveticorum)
GPK	Geschäftsprüfungskommission des Nationalrates
GVG	Bundesgesetz über den Geschäftsverkehr der Bundesversammlung (Geschäftsverkehrsgesetz)
HMV	Schweizerischen Vereinigung der Haftpflicht- und Motorfahrzeug-Versicherer
IDK	Identitätskarte
ISDN	Dienstintegrierendes digitales Netz
ISIS	Staatsschutz-Informations-System
ISIS-VO	Verordnung über das provisorische Staatsschutz-Informations-System
IV	Invalidenversicherung
KVG	Bundesgesetz über die Krankenversicherung
KVV	Verordnung über die Krankenversicherung
PKU	Schweizerische Vereinigung privater Kranken- und Unfallversicherer
RIPOL	Automatisiertes Fahndungssystem
StGB	Schweizerisches Strafgesetzbuch
URG	Urheberrechtsgesetz
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
VPB	Verwaltungspraxis der Bundesbehörden
ZAR	Zentrales Ausländerregister
ZEK	Zentralstelle für Kreditinformation
ZS BM	Zentralstelle für die Bekämpfung des unerlaubten Betäubungsmittel-handels
ZSG	Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes

I. AUSGEWÄHLTE THEMEN

1. Polizeiwesen

1.1. Spielbankengesetz

Im Rahmen der Ämterkonsultation hatten wir die Möglichkeit, zum Entwurf des Bundesgesetzes über das Glücksspiel und über die Spielbanken (Spielbankengesetz) sowie der dazugehörigen Botschaft Stellung zu nehmen.

Uns wurde vom Bundesamt für Polizeiwesen (BAP) die Möglichkeit gegeben, zum Entwurf des vorgenannten Bundesgesetzes sowie der dazugehörigen Botschaft im Rahmen der Ämterkonsultation Stellung zu nehmen. Das Spielbankengesetz regelt die Bedingungen im Zusammenhang mit der Führung von Spielbanken. Aus sozialen Gründen sowie aus Eigeninteressen der Spielbanken dürfen diese die Identität der Spieler prüfen sowie unter bestimmten Bedingungen Spielsperren verhängen und Darlehen gewähren. Die Spielbanken haben die verhängten Spielsperren an andere Spielbanken weiterzuleiten. Bei Verdacht von Geldwäscherei ist dies der Meldestelle für Geldwäscherei zu melden. Die Spielbanken sollen dem Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor unterstellt werden. Nach diesem Gesetz führt die Zentralstelle für organisierte Kriminalität des Bundesamtes für Polizeiwesen die Meldestelle für Geldwäscherei. Bestehende Differenzen bezüglich Art und Umfang der Informationsbeschaffung seitens der Spielbanken im Zusammenhang mit der Verhängung von Spielsperren und der Gewährung von Darlehen sowie der Speicherung und Löschung von Daten konnten ausgeräumt werden. Zu beobachten bleibt jedoch von unserer Seite die Entwicklung der vorgesehenen Unterstellung der Spielbanken unter das Geldwäschereigesetz und die damit verbundene Datenweitergabe an die Meldestelle für Geldwäscherei. Auch hoffen wir, frühzeitig in die Ausarbeitung der zum Spielbankengesetz gehörenden Verordnung einbezogen zu werden.

1.2. Anschluss der Kantone an ISIS

Die Schweizerische Bundespolizei führt zur Erfüllung ihrer Aufgaben das Staatsschutz-Informations-System ISIS. Hierbei handelte es sich ursprünglich um ein Inselsystem. An dieses sind durch Revision der ISIS-Verordnung Stellen von neun Kantonen angeschlossen worden.

Gemäss der Verordnung über das provisorische Staatsschutz-Informations-System (ISIS-Verordnung) betreibt die Schweizerische Bundespolizei zur Erfüllung ihrer gesetzlichen Aufgaben ein provisorisches informatisiertes Staatsschutz-Informations-System (ISIS). ISIS war ursprünglich als Inselsystem angelegt. Es entstand jedoch seitens der Staatsschutzbehörden bald das Bedürfnis, dass auch Staatsschutzorgane von Kantonen einen Direktanschluss an ISIS erhielten. Dementsprechend hat bereits 1994 die Schweizerische Bundesanwaltschaft den revidierten Entwurf der ISIS-Verordnung in die Ämterkonsultation geschickt, der den Direktanschluss von mit eidgenössischem Staatsschutzaufgaben betrauten kantonalen Organen an ISIS vorsah. Bereits damals haben wir die Gelegenheit zur Stellungnahme wahrgenommen und konkrete Änderungsvorschläge unterbreitet. Im Jahre 1996 verwiesen wir in ei-

ner weiteren Ämterkonsultation im wesentlichen auf unsere frühere Stellungnahme. Inhaltlich wurde unseren Forderungen

- nach Beschränkung der Zugriffsberechtigungen auf einige wenige Kantone,
- nach Beschränkung der Zugriffsberechtigungen auf Kurzpersonalien (Name, Vorname, Organisation/Firma, Aliasname, phonetisierte Schreibweise aller Namen und Vornamen, Geburtsjahr, Geburtsdatum, Staatsangehörigkeit, Heimatort),
- nach Beschränkung der Zugriffsberechtigungen auf Vorgangsdaten sowie die dazugehörigen vollständigen Stammdaten, zu welchen die Informationen vom betreffenden Organ stammen oder diesem von der Bundespolizei mitgeteilt wurden,
- sowie nach Verzicht auf einen Anschluss an die Datenbank «Dokumentation» entsprochen.

In der Zwischenzeit wurde das Geschäft wegen Kompetenzproblemen zwischen der Schweizerischen Bundespolizei und dem Bundesamt für Polizeiwesen sistiert. Unklar ist, welche dieser beiden Behörden für den Bereich der organisierten Kriminalität verantwortlich ist.

1.3. Das Datenverarbeitungssystem DOSIS

Online-Zugriff auf DOSIS-Daten

Die Zentralstelle für die Bekämpfung des unerlaubten Betäubungsmittelverkehrs (ZS BM) des Bundesamtes für Polizeiwesen (BAP) verfügt zur Bekämpfung des illegalen Drogenhandels über das Datenverabeitungssystem DOSIS. Es haben zu viele Personen Online-Zugriff auf die in DOSIS gespeicherten Personendaten.

Gemäss dem Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes (ZSG) führt das Bundesamt für Polizeiwesen (BAP) die Zentralstelle für die Bekämpfung des unerlaubten Betäubungsmittelhandels (ZS BM). Die ZS BM verfügt gemäss Verordnung über das Datenverarbeitungssystem zur Bekämpfung des illegalen Drogenhandels (VO DOSIS) über das Datenverarbeitungssystem DOSIS. In der VO DOSIS ist ausdrücklich festgelegt, dass nur die ZS BM und die Betäubungsmitteldienste der kantonalen Polizeikorps durch Abrufverfahren an DOSIS angeschlossen werden dürfen. Anhang 2 zur VO DOSIS dehnt jedoch die Zugriffsberechtigungen contra legem auf Mitarbeiter des BAP aus, die nicht Mitarbeiter der ZS BM sind. Wir haben das BAP mit einem Schreiben auf diesen Umstand aufmerksam gemacht und es aufgefordert, bei der Datenbearbeitung in DOSIS unseren Ausführungen Rechnung zu tragen.
In diesem Zusammenhang ist zu prüfen, ob eine Revision von ZSG und VO DOSIS an die Hand zu nehmen ist, um den vor allen Dingen im Spannungsfeld organisierte Kriminalität/Drogenhandel auftretenden Problemen gerecht zu werden.

DOSIS-Bearbeitungsreglement

Gemäss Verordnung zum Bundesgesetz über den Datenschutz (VDSG) sind die Bundesorgane, die automatisierte Datensammlungen betreiben, unter bestimmten Bedingungen zur Erstellung eines Bearbeitungsreglementes verpflichtet. Das Bundesamt für Polizeiwesen (BAP) hat das Bearbeitungsreglement für das Datenbearbeitungssystem DOSIS erstellt.

Gemäss VDSG müssen Bundesorgane, die automatisierte Datensammlungen führen, ein Bearbeitungsreglement erstellen, wenn die Datensammlung besonders schützenswerte Personendaten oder Persönlichkeitsprofile enthält, die Datensammlung durch mehrere Bundesorgane benutzt, Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen zugänglich gemacht wird oder mit anderen Datensammlungen verknüpft ist. Mit 1. August 1996 wurde der Betrieb des Datenverarbeitungssystems DOSIS endgültig aufgenommen. Dies benötigte vom BAP ein Bearbeitungsreglement für DOSIS. Uns wurde während der Ausarbeitung des Bearbeitungsreglementes die Möglichkeit zur Mitarbeit geboten. Auf diese Weise konnten wir auf verschiedene Aspekte hinweisen, die aus Sicht des Datenschutzes problematisch oder gar unzulässig waren. Leider konnten in einem wesentlichen Punkt die Differenzen nicht bereinigt werden. Gemäss der VO DOSIS sind an DOSIS neben der ZS BM auch die Betäubungsmitteldienste der kantonalen Polizeikorps im Abrufverfahren angeschlossen. In dem vom BAP ausgearbeiteten Bearbeitungsreglement wird unseres Erachtens dieser Kreis der Zugriffsberechtigten unzulässigerweise ausgeweitet. Das Bearbeitungsreglement sieht vor, dass auch Mitarbeiter der Polizeikorps, die nicht einem Betäubungsmitteldienst angehören, zur Erfüllung rechtlicher Aufgaben an DOSIS angeschlossen werden können. Wir sind der Auffassung, dass für diese Ausweitung der Zugriffsberechtigungen keine rechtliche Grundlage in der VO DOSIS besteht. Die Umsetzung des Bearbeitungsreglementes in die Praxis wäre somit rechtswidrig.
Im übrigen müssen wir feststellen, dass es sich bei dem Bearbeitungsreglement mit seinen integrierten Anhängen um ein umfangreiches Werk handelt, bei dessen Ausarbeitung sich das BAP sehr viel Mühe gegeben hat.

Trennung der vor einem gerichtspolizeilichen Ermittlungsverfahren beschafften Daten von Daten der gerichtlichen Polizei des Bundes und der Kantone in DOSIS

Im Datenverarbeitungssystem DOSIS zur Bekämpfung des illegalen Betäubungsmittelhandels werden sowohl Daten bearbeitet, die in einem gerichtspolizeilichen Ermittlungsverfahren, als auch Daten, die vor Einleitung eines gerichtspolizeilichen Ermittlungsverfahren erhoben wurden. Diese Daten sind laut Bundesgesetz über die Zentralstellen des Bundes getrennt zu führen.

Die Zentralstelle für die Bekämpfung des unerlaubten Betäubungsmittelhandels (ZS BM) des Bundesamtes für Polizeiwesen (BAP) führt das Datenverarbeitungssystem DOSIS zur Bekämpfung des illegalen Betäubungsmittelhandels. In diesem System werden zum einen Daten über Personen gespeichert und bearbeitet, die im Rahmen eines gerichtspolizeilichen Ermittlungsverfahren beschafft wurden, zum anderen Daten der gerichtlichen Polizei des Bundes und der Kantone.
Das Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes (ZSG) schreibt vor, dass diese Daten in DOSIS getrennt zu führen sind. Eine Trennung in einem Datenverarbeitungssystem kann grundsätzlich physisch oder logisch erfolgen. Auf eine physische Trennung, d.h. das Führen zweier Datenbanken, wurde vorliegend verzichtet. In DOSIS erfolgt jedoch keine obligatorische, logische Trennung der Daten. Vielmehr werden die Daten lediglich auf einer Einheitsmaske mit «GerPol Ja/Nein» gekennzeichnet. Wir haben das BAP in einem Schreiben darauf hingewiesen, dass der bestehende Zustand unseres Erachtens gegen das Gesetz verstösst, und haben gefordert, die Datenbearbeitung in DOSIS unseren Ausführungen entsprechend anzupassen.

Die Beurteilung, ob es sich um Daten, die vor Einleitung eines gerichtspolizeilichen Ermittlungsverfahrens beschafft wurden, oder um Daten der gerichtlichen Polizei der Kantone handelt, richtet sich nach den zum Teil sehr unterschiedlichen kantonalen Strafprozessordnungen. Dies kann je nach Kanton zu einer Ungleichbehandlung ein und derselben Information und damit zu Praktikabilitätsproblemen führen.

Indirektes Auskunftsrecht in DOSIS

Das Auskunftsrecht des Bürgers in bezug auf eine mögliche Speicherung in dem Datenverarbeitungssystem DOSIS unterscheidet sich von dem durch das DSG vorgesehene Auskunftsrecht in erheblicher Weise: Es ist ein indirektes Auskunftsrecht, das über den Eidgenössischen Datenschutzbeauftragten ausgeübt werden muss.

Das DSG sieht ein Auskunftsrecht vor, das jeder Person das Recht gibt, vom Inhaber einer Datensammlung Auskunft darüber zu verlangen, ob Daten über sie bearbeitet werden. Die betroffene Person gelangt mit ihrem Auskunftsbegehren direkt an den Inhaber der Datensammlung.
Gemäss der VO DOSIS kann die betroffene Person lediglich in den Fällen, in denen der Bund die gerichtspolizeilichen Ermittlungsverfahren geführt hat, direkt beim Inhaber der Datensammlung Auskunft verlangen. Bezüglich der Daten, die vor Einleitung eines gerichtspolizeilichen Ermittlungsverfahrens beschafft wurden, und der Daten der gerichtlichen Polizei der Kantone gilt - wie bereits in unserem 2. Tätigkeitsbericht S. 10 ff. - ausgeführt, das sogenannte indirekte Auskunftsrecht. Dieses richtet sich nach den Bestimmungen des Bundesgesetzes über kriminalpolizeiliche Zentralstellen des Bundes, die wesentlich von den Bestimmungen des DSG abweichen. Demzufolge muss die betroffene Person bei uns nachfragen, ob in DOSIS Daten rechtmässig bearbeitet werden. Wir haben der gesuchstellenden Person in einer stets gleichlautenden Antwort mitzuteilen, dass über sie entweder keine Daten unrechtmässig bearbeitet werden oder dass wir bei Vorhandensein allfälliger Fehler in der Bearbeitung eine Empfehlung zu deren Behebung an die ZS BM gerichtet haben. Dieses indirekte Auskunftsrecht ist sowohl für die betroffene Person unbefriedigend als auch für uns untragbar. Die betroffene Person erhält keine klare Antwort, ob und wenn ja welche Daten über sie bearbeitet werden. Für uns bedingt das indirekte Auskunftsrecht, dass wir einerseits im Datenverarbeitungssystem DOSIS kontrollieren müssen, ob und welche Daten über die betreffende Person bearbeitet werden. Andererseits müssen wir die zum Teil sehr umfangreichen, auf Papier geführten Dossiers, die nicht immer nur eine bestimmte Person, sondern auch ganze Operationen betreffen können, durcharbeiten, um beurteilen zu können, ob die Erfassung und Bearbeitung der Daten in DOSIS rechtmässig erfolgt ist. Um tatsächlich Richtigkeit und/oder Rechtmässigkeit der Datenbearbeitung feststellen zu können, müssten auch wir Daten über die anfragende Person sammeln und bearbeiten. Dadurch würden wir selber zu Dateninhabern. Dies wäre jedoch mit der uns vom Gesetz übertragenen Aufgabe der Kontrollstelle nicht vereinbar und nicht akzeptabel. Im Jahr 1996 wurde an uns erst ein Gesuch um Auskunft gerichtet.

1.4. Vertrieb einer CD-ROM mit Fahrzeughalterdaten

Eine CD-ROM mit Daten über Fahrzeughalter wurde in der gesamten Schweiz (mit Ausnahme des Kantons Jura) vertrieben. Dies verstösst jedoch gegen die Bestimmungen des Datenschutzgesetzes und der Strassenverkehrsgesetzgebung. In einer

Empfehlung verlangten wir schliesslich die Einstellung der Produktion und des Vertriebs der CD-ROM.

Wir wurden von verschiedenen kantonalen Datenschutzstellen und Strassenverkehrsbehörden auf den Vertrieb eines Verzeichnisses der schweizerischen Fahrzeughalterdaten auf CD-ROM aufmerksam gemacht. Die entsprechende Firma wurde vom uns aufgefordert, die Produktion und den Vertrieb der CD-ROM bis zur Klärung des Sachverhaltes einzustellen. Sie bestätigte die provisorische Einstellung der Produktion und des Vertriebs der CD-ROM und nahm zu unseren Fragen schriftlich Stellung. Nach Klärung des Sachverhaltes stellte sich heraus, dass die Richtigkeit der Daten nicht gewährleistet ist und die Suchoptionen weitergehende Abfragemöglichkeiten erlauben. Ausserdem wurde festgestellt, dass die Daten von den offiziellen kantonalen Fahrzeughalterverzeichnissen übernommen und auf CD-ROM veröffentlicht wurden.
Gemäss der Strassenverkehrsgesetzgebung dürfen Name und Vorname eines Fahrzeughalters nur aufgrund des Fahrzeugschildes gesucht und bekanntgegeben werden. Damit hat der Gesetzgeber die Möglichkeiten der Bearbeitung von Fahrzeughalterdaten auf ein Minimum beschränken wollen, um schwerwiegende Eingriffe in die Persönlichkeit eines Fahrzeughalters zu vermeiden. Die vorgenannte CD-Rom erlaubt hingegen umfassende Suchkriterien (nach Name, Gemeinde, Postleitzahl, Kontrollschild) und somit praktisch unbeschränkte Suchmöglichkeiten. Dadurch wird nicht nur die Strassenverkehrsgesetzgebung, sondern auch das datenschutzrechtliche Verhältnismässigkeitsprinzip tangiert. Nach den einschlägigen Bestimmungen des Strassenverkehrsgesetzes ist die Bearbeitung von Fahrzeughalterdaten dem Bund vorbehalten. Dabei werden die Fahrzeughalterdaten zu Zwecken bearbeitet und veröffentlicht, die in einem direkten Zusammenhang mit der Erfüllung der strassenverkehrsrechtlichen Aufgaben, insbesondere mit der Erfüllung polizeilicher Aufgaben, stehen. Der Vertrieb der Fahrzeughalterdaten stellt jedoch eine kommerzielle Tätigkeit dar, die mit den Zielen der Strassenverkehrsgesetzgebung in keinem Zusammenhang steht.
Dadurch wird neben der Zuständigkeitsregelung auch das Prinzip des Zweckbindungsgebotes verletzt. Durch das Vertreiben falsch eingescannter und teilweise nicht aktualisierter Daten wird im übrigen das Gebot der Richtigkeit missachtet. Wir haben schliesslich empfohlen, die Produktion und den Vertrieb der CD-ROM definitiv einzustellen.

1.5. Vollautomatisiertes Strafregister VOSTRA

Das bis heute auf Papier geführte Strafregister soll automatisiert werden (Projekt VOSTRA). Im Strafregister werden unter anderem besonders schützenswerte Personendaten bearbeitet. Es ist deshalb notwendig, das neue System in einem formellen Gesetz zu verankern. Zur Zeit wird ein Pilotversuch mit einigen Kantonen durchgeführt, der bis Ende 1998 befristet ist.

Die Sektion Strafregister des Bundesamtes für Polizeiwesen führt ein Register über alle Personen, die auf dem Gebiet der Eidgenossenschaft verurteilt worden sind, sowie über alle im Ausland verurteilte Schweizer. Durch die Automatisierung des Registers soll die Verwaltung der Urteils- bzw. Strafregisterauszüge effizienter gestaltet werden. Das dafür geplante Projekt VOSTRA als Online-Applikation mit besonders schützenswerten Personendaten benötigt in Anlehnung an das Datenschutzgesetz ein formelles Gesetz.

Ein Augenschein beim Bundesamt für Polizeiwesen ergab, dass das Strafregister in seiner heutigen Form die ihm auferlegten gesetzlichen Aufgaben nur noch in ungenügender Weise wahrnehmen kann. Wir haben uns deshalb mit der Änderung der Strafregisterverordnung zur Schaffung der Grundlage für den Pilotversuch mit neun Kantonen sowie dem Oberauditorat einverstanden erklärt. Die Verordnung ist bis Ende 1998 befristet. Das Bundesamt für Polizeiwesen hat sich zudem verpflichtet, bis spätestens 31. Dezember 1998 die formellgesetzliche Grundlage für den Vollbetrieb des Systems VOSTRA zu schaffen. Die Strafregisterverordnung muss dannzumal total revidiert werden.

2. Ausländer- und Asylrecht

2.1. Polizeizugriffe auf die Asylbewerber- und Ausländerdatensammlungen des EJPD - Entscheid der EDSK

Auf unsere Beschwerden hin hat die EDSK die Verfügungen des EJPD aufgehoben und die Sache zur Neuentscheidung an die Vorinstanz zurückgewiesen. In ihrem Urteil hat die EDSK wichtige Datenschutzfragen klargestellt und sich auch zu unserer Beschwerdebefugnis geäussert. Das EJPD hat gegen diesen Entscheid beim Bundesgericht Verwaltungsgerichtsbeschwerde eingelegt. Damit tritt diese rechtliche Auseinandersetzung nun in ihr fünftes Jahr.

In einem Sicherheitsbericht von 1992 und in zwei Empfehlungen von 1994 haben wir uns dagegen ausgesprochen, dass die Asylbewerber- und Ausländerdaten zusammen mit Kriminaldaten gespeichert und bearbeitet werden. Zudem haben wir verlangt, dass den verschiedenen Polizeibehörden des Bundes ohne ausreichende Rechtsgrundlagen und ohne ausreichende Sicherheitsabklärungen und -massnahmen an den verwendeten Informatikmitteln keine Online-Zugriffe auf die sensiblen Asylbewerber- und Ausländerdaten gewährt werden. Die bestehenden Zugriffsmöglichkeiten nach dem Selbstbedienungsprinzip und mit der Gefahr unkontrollierter Datenabflüsse sollten vielmehr gestoppt bzw. auf das absolut erforderliche Mindestmass reduziert werden.
Die betroffenen Ämter und das EJPD lehnten unsere Empfehlungen bzw. Weiterziehungen ab, so dass wir mit Beschwerde an die Eidgenössische Datenschutzkommission (EDSK) gelangen mussten. Die EDSK hiess unsere Beschwerden in wichtigen Teilen gut, hob die angefochtenen Verfügungen des EJPD auf und wies die Sache zur Neuentscheidung an das EJPD zurück.
In ihrem Entscheid anerkannte die EDSK die Beschwerdebefugnis des EDSB gegen Entscheide der Departemente und der Bundeskanzlei, wenn der EDSB durch Entscheide dieser Behörden in der Ausübung seiner Tätigkeit erheblich beeinträchtigt wird. Wir selber hatten die Auffassung vertreten, unsere Beschwerdebefugnis gegenüber diesen Bundesorganen ergebe sich aus unserer unabhängigen Stellung innerhalb der Bundesverwaltung und stütze sich direkt auf das Verwaltungsverfahrensgesetz. Deshalb sei sie im Datenschutzgesetz nicht ausdrücklich erwähnt. Weiter erachtete die EDSK die gesetzlichen Grundlagen für die umstrittenen Online-Zugriffe jedenfalls im Zeitpunkt der Beschwerdeeinreichung als klar ungenügend. Zudem hielt die EDSK fest, dass für diese Online-Zugriffe Zugriffsprotokollierungen mit wirkungsvollen Protokollauswertungen hätten eingerichtet werden müssen. Namentlich die Asylbewerberdaten und in diesem Zusammenhang auch die Nationalität

seien besonders schützenswerte Angaben. Ferner seien die Daten von Personen, die nicht an einem Verfahren beteiligt sind, bei der Online-Abfrage nicht zugänglich zu machen. Überhaupt seien die Asylbewerber- und Ausländerdaten von den Strafdaten getrennt aufzubewahren und zu bearbeiten. In formeller Hinsicht verlangte die EDSK, dass die neu zu fällenden Entscheide des EJPD vollständig im Bundesblatt zu publizieren seien. Die angefochtenen Entscheide waren nur stark gekürzt im Bundesblatt publiziert worden, und auch das erst nach unserer Intervention.
Das EJPD hat gegen den Entscheid der EDSK beim Bundesgericht Verwaltungsgerichtsbeschwerde ergriffen.

2.2. Projekt EVA (elektronische Visum-Ausstellung)

Die schweizerischen Geschäftsstellen im Ausland und die grösseren Grenzkontrollposten der Schweiz stellen seit jeher auch Visa aus. Dabei obliegt es ihnen unter anderem, die Angaben der Gesuchsteller auf ihre Richtigkeit hin zu überprüfen. Mit dem Projekt EVA sollen elektronische Abfragen bestehender und neu zu schaffender Datensammlungen vor der Visaerteilung sowie der automatisierte Ausdruck der Visa ermöglicht werden. Es stellen sich vorab die Fragen, wie die Datenbearbeitungen und namentlich diejenigen im Ausland hinreichend gesichert werden können und ob die gesetzlichen Grundlagen für die insgesamt umfangreichen, neuen Datenbearbeitungen genügen.

Anlässlich zweier Kontrollen im Jahr 1996 (vgl. hierzu nachfolgend S. 54) erhielten wir einen guten Einblick in die Datenbearbeitungen bei der Visaerteilung in schweizerischen Geschäftsstellen im Ausland und an schweizerischen Grenzkontrollposten. Diese Behörden stellen die Visa bzw. Sichtvermerke manuell aus. Zuvor konsultieren sie den Schweizerischen Fahndungsanzeiger und in Zweifelsfällen das Bundesamt für Ausländerfragen in Bern, welches bei Bedarf weitere Abklärungen trifft. Die Grenzkontrollstellen verfügen seit kurzem über (beschränkte) Zugriffe auf das Fahndungssystem RIPOL, das Zentrale Ausländerregister ZAR und nunmehr auch auf die Asylbewerberdaten des AUPER. Die schweizerischen Geschäftsstellen im Ausland verfügen hingegen über keine solchen Zugriffe (mit Ausnahme von einigen grossen Botschaften, welche direkt auf das RIPOL greifen können). Missbräuchliches Verhalten von Gesuchstellern (z.B. mehrfache Gesuchseinreichung an verschiedenen Schaltern oder Grenzposten), Wartezeiten bei Abklärungen in Bern sowie der Wunsch nach einem benutzerfreundlichen Arbeitsinstrument am Schalter führten zur Projektidee der elektronischen Visa-Ausstellung. Das Projekt hat die Phase der Voranalyse durchlaufen und befindet sich zur Zeit in der Konzeptphase. Seitens des Datenschutzes haben wir die Prüfung der Frage angeregt, ob die schweizerischen Botschaften und Konsulate wirklich in jedem Fall auf die Abfragen der heiklen Datensammlungen RIPOL, ZAR und AUPER angewiesen sind und ob die Visaerteilung durch ortsansässiges ausländisches Personal nicht mit Risiken verbunden ist. Generell haben wir eine Risikobeurteilung nach den einschlägigen Vorschriften und die Erarbeitung eines Sicherheitskonzepts vorgeschlagen. Als besonderer Risikofaktor könnten sich die lokalen Netze der schweizerischen Geschäftsstellen im Ausland erweisen, über welche die Online-Abfragen abgehört oder von kriminellen Elementen gar für Angriffe auf die heiklen Datensammlungen in der Schweiz genutzt werden könnten. Unsere Anregungen wurden positiv aufgenommen. Eine Überprüfung hat ergeben, dass nur bei etwa 5% der Visa-Gesuche eingehendere Abklärungen nötig sind. Daher genügt es bei 95% der Gesuche, wenn nicht der Schalterbeamte, sondern das System (freilich in einem gesicherten Umfeld) eine Suchanfrage in den inte-

ressierenden Datensammlungen startet und hernach der schweizerischen Geschäftsstelle im Ausland lediglich die O.K.-Meldung erstattet. In den verbleibenden 5% der Fälle ist das Gesuch wie bisher nach Bern zu schicken. Die problematischen Online-Abfragen erübrigen sich.
Weiter haben wir uns in einem umfangreichen Gutachten zur Frage der gesetzlichen Grundlage geäussert. Dabei sind wir zum Schluss gekommen, dass für einzelne Aspekte der vorgesehenen neuen Datenbearbeitungen ausreichende Gesetzesgrundlagen bestehen oder dem Parlament bereits vorgeschlagen wurden (vgl. auch S. 17). Für die heute vorliegende Projektidee wäre indessen darüber hinaus eine klare Grundsatzbestimmung im Ausländergesetz erforderlich, welche zur Zeit fehlt und auch nicht vorgesehen ist. Dabei gilt es zu bedenken, dass eine umfangreiche, neue Datensammlung vorgesehen ist, welche sämtliche visarelevanten Personenbewegungen mit den dazugehörenden Attributen aufzeichnet und während längerer Zeit speichert. Diese Daten werden bei der Visaausstellung zusammen mit den Daten anderer grosser Datensammlungen bearbeitet, wobei viele Behörden regelmässig auf diese Daten - darunter auch besonders schützenswerte - greifen werden.

2.3. Übergreifendes Sicherheitskonzept für kantonale Anschlüsse an das ZAR

Die Frage der übergreifenden Sicherheit im Verhältnis zwischen Bund und Kantonen stellt sich natürlich auch bei der elektronischen Bearbeitung von Ausländerdaten. Viele Kantone haben sich mit der Übernahme der Sicherheitsanforderungen des Bundes einverstanden erklärt. Mit einem weiteren Kanton stehen wir zusammen mit den Sicherheitsspezialisten des Bundes in Verhandlung.

In einem, in VPB 60.10 publizierten Gutachten, haben wir uns bereits Ende 1994 zu den bundesrechtlichen Vorgaben bei der Bearbeitung von Ausländerdaten in Bund und Kantonen geäussert. Das Zentrale Ausländerregister ZAR steht auch den kantonalen Behörden zur Verfügung, soweit dies für die Aufgabenerfüllung erforderlich und mit dem ursprünglichen Datenerhebungszweck vereinbar ist. Darüber hinaus sind keine Datenbearbeitungen erlaubt. Alle Benützer des ZAR müssen dafür Gewähr bieten, dass die Daten des ZAR nicht zu anderen Zwecken bearbeitet werden oder dass Dritte unerlaubt in die Sammlung des ZAR eindringen und Daten entwenden oder beschädigen. Dabei leuchtet es ein, dass ein gemeinsamer, hoher Sicherheitsstandard gewählt werden muss. Für die Sicherheit im ZAR ist jeder einzelne Benutzer voll und ganz mitverantwortlich. Kantone, welche die Zugriffsberechtigung auf das ZAR an eine Vielzahl von eigenen Behörden delegieren wollen, müssen dafür sorgen, dass alle Benutzer den geforderten hohen Sicherheitsstandard aufweisen. Weil mit der Sicherheit auch Kosten verbunden sind, empfiehlt es sich, die Organisationsstrukturen kostenbewusst zu gestalten und allenfalls etwas zu straffen. Dies liegt auf der Linie des New Public Management und wird von vielen Kantonen praktiziert. Mit einem weiteren Kanton haben wir die Situation zusammen mit den Sicherheitsspezialisten des Bundes analysiert, so dass vor neuen Anschlüssen an das ZAR die erforderlichen Schutz- und Sicherheitsvorkehrungen getroffen werden können.

2.4. Vermerk «auf Stellensuche» und weitere Vermerke auf den Ausländerausweisen

Weil der Ausländerausweis heute zugleich als Verfügung dient, finden sich eine Vielzahl von Angaben darauf, die nichts mit der Identität einer Person zu tun haben. Eine gesetzliche Grundlage für derartige «Ausweise» fehlt, was aus datenschutzrechtlicher Sicht unbefriedigend ist.

Ein ausländischer Staatsangehöriger hat sich bei uns beklagt, weil auf seinem Ausländerausweis unter anderem die Vermerke «auf Stellensuche» und «abwartend Rentenentscheid» zu lesen waren. Aufgrund der Angaben der Ausländerbehörden würden solche Vermerke der Praxis entsprechen. Die zuständige Behörde hat indessen von sich aus den Vermerk «abwartend Rentenentscheid» aus dem Ausweis entfernt. Auf den Vermerk «auf Stellensuche» hat sie indessen nicht verzichten wollen. Sie begründete im wesentlichen, der Ausländerausweis stelle nicht nur eine Legitimationskarte, sondern zugleich eine Verfügung über die Anwesenheitsberechtigung dar. Auf dieser Verfügung müssten die nach Gesetz erforderlichen Gründe und Voraussetzungen für den Verbleib in der Schweiz ersichtlich sein. Es würde einen erheblichen Mehraufwand verursachen, neben diesem Ausweis zusätzlich eine separate Verfügung zuzustellen. Diese Begründung überzeugte uns nicht. Der Verwaltungs-Mehraufwand liesse sich durch Gebühren abgelten, und er wird heute in den meisten Amtsstellen durch die ohnehin schon vorhandenen Schreib- und Versandautomaten aufgefangen. Soweit die «Verfügungen» anfechtbar sind, fehlt zudem die Rubrik Rechtsmittelbelehrung. Es wurde auch nicht der Versuch unternommen, den «Verfügungsteil» privat bzw. abgedeckt auszugestalten. So muss bei jeder Präsentation dieses Dokuments zugleich ein mitunter doch recht weitgehender Einblick in die persönlichen Verhältnisse gegeben werden. Hierfür fehlt eine gesetzliche Grundlage, und auch das Datenschutzrecht steht einer solchen Praxis entgegen. Wir haben dies den zuständigen Behörden mitgeteilt. Im Sinne einer Sofortmassnahme hat sich das Bundesamt für Ausländerfragen bereit erklärt, die Liste der Vermerke auf den Ausländerausweisen zu straffen. Das Problem wird aber im Rahmen der Arbeiten an einer neuen Migrationsgesetzgebung in grundsätzlicher Weise angegangen werden müssen.

2.5. Bekanntgabe von Asylbewerberdaten an ausländische Staaten

Die Fingerabdrücke von Asylbewerbern dürfen nicht ins Ausland bekanntgegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde. Bei der Datenbekanntgabe an die Asylbehörden der EU mit gleichwertigem Datenschutz haben wir keine solche Gefährdung erkannt. Hingegen mussten wir zwei andere Datenbekanntgaben ins Ausland aufgrund der konkreten Umstände ablehnen.

In einem, in VPB 60.89 publizierten Gutachten, haben wir uns zur Bekanntgabe von Asylbewerberdaten an ausländische Staaten geäussert. Konkret ging es um die folgenden drei Fälle:

- die Bekanntgabe der Fingerabdrücke an den Heimatstaat zum Vollzug einer Wegweisungsverfügung;
- die Bekanntgabe an die Asylbehörden europäischer Staaten zur Ermittlung des Erstasyllandes;
- die Bekanntgabe an ausländische Interpol-Stellen zu polizeilichen Zwecken.

Gemäss dem aus der EMRK fliessenden Grundsatz des «Non-Refoulement» darf niemand der Folter bzw. unmenschlicher oder erniedrigender Strafe oder Behandlung unterworfen werden. Nach der EMRK-Rechtsprechung verbietet diese Bestimmung auch die Auslieferung oder Ausweisung in ein Land, in welchem mit Folter oder unmenschlicher oder erniedrigender Behandlung zu rechnen ist. Sie gilt nicht nur für Flüchtlinge, sondern auch für Straftäter, welche ausgeliefert werden sollen. Dieser Grundsatz wurde in verschiedenen landesrechtlichen Bestimmungen übernommen und näher ausgeführt, so im Asylgesetz, im Rechtshilfegesetz und nunmehr auch - zusammen mit dem Verfassungsgrundsatz der persönlichen Freiheit bzw. des Persönlichkeitsschutzes - im Datenschutzgesetz. Nach dessen Artikel 6 dürfen Personendaten nicht ins Ausland bekanntgegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil ein Datenschutz fehlt, der dem schweizerischen gleichwertig ist.
Unter Berücksichtigung all dieser Rechtsgrundlagen führte uns dies in den drei genannten Fällen zu folgendem Ergebnis: Die Bekanntgabe von Fingerabdrücken in ein Land mit schweren Menschenrechtsverletzungen, welches zudem über alle seine Bürger Fingerabdrücke besitzt und auch nur vermutete Regimegegner massiv verfolgt, erachten wir als geeignet, die Persönlichkeit der betroffenen Person schwerwiegend zu verletzen. Dies namentlich dann, wenn zu vermuten ist, dass bereits die Bekanntgabe der Fingerabdruckdaten zu einer politischen «Verdächtigung» und zu verunglimpfenden und diskriminierenden Datenbearbeitungen führen kann. Es müsste im konkreten Fall eine ausreichende Gewähr für einen guten Schutz der Menschenrechte (inkl. Persönlichkeitsschutz) nachgewiesen werden. Von vergleichbaren Überlegungen liess sich, soweit ersichtlich, auch das Schweizerische Bundesgericht in einem kürzlich beurteilten Auslieferungsfall leiten (vgl. BGE 122 II 373). Sie gelten auch für den Datenaustausch unter internationalen Fahndungs- und Strafbehörden. Demgegenüber sahen wir im Austausch von Asylbewerberdaten unter europäischen Asylbehörden mit gleichwertigem Datenschutz keine schwerwiegende Gefährdung der Persönlichkeit der betroffenen Personen.

2.6. Vertrag des Bundesarchivs mit Yad Vashem über die Bekanntgabe von Daten jüdischer Flüchtlinge

Yad Vashem, eine öffentlich-rechtliche Körperschaft Israels, welche die Interessen der Überlebenden des Holocaust und der Hinterbliebenen der Opfer vertritt, hat das Schweizerische Bundesarchiv um Übermittlung der Daten jüdischer Flüchtlinge von 1933-1945 gebeten.

Das Schweizerische Bundesarchiv stimmte dieser Übermittlung zu. Es unterbreitete uns einen Vertragsentwurf und zeigte uns die interessierenden Datenbestände. Wir regten an, die nach schweizerischem Recht nötigen Datenschutz- und Datensicherheitsklauseln darin festzuhalten. Danach sind die Nachforschungen im Interesse der jüdischen Flüchtlinge und ihrer Angehörigen oder Nachkommen auch in Israel möglich. Gleichzeitig werden ihre Personendaten vor unbefugtem Bearbeiten geschützt.

2.7. Anhörung des EDSB zur hängigen Revision des Asylgesetzes und Ausländergesetzes

Die vorberatende Kommission des Nationalrats lud uns zu einer Stellungnahme zu den Datenschutzbestimmungen der beiden Revisionsentwürfe ein.

Dabei wurden wir gebeten, unsere in den früheren Tätigkeitsberichten dargelegte Auffassung (vgl. zuletzt: 3. Tätigkeitsbericht 1995/96 S. 23.f) näher zu erläutern. Wir führten erneut aus, dass die Bekanntgabe von Personendaten ins Ausland auch nach Art. 6 DSG nicht zu einer schwerwiegenden Gefährdung der Betroffenen oder ihrer Angehörigen führen darf. Fehlt im Empfängerstaat ein dem schweizerischen gleichwertiges Datenschutzgesetz, sind durch bereichsspezifische Abkommen und weitere Massnahmen hinreichende Garantien für den Daten- und Persönlichkeitsschutz der betroffenen Personen und ihrer Angehörigen zu schaffen. Solche Abkommen erachten wir nicht als «Bagatellabkommen». Generell regten wir in diesem Zusammenhang auch an, die Frage näher zu prüfen, in welchen Fällen das Parlament internationale Abkommen im Migrationsbereich abschliessen bzw. genehmigen soll. Als problematisch erachten wir auch die heute geübte flächendeckende Erhebung von Fingerabdrücken bei Asylbewerbern und die Bekanntgabe dieser Daten in den Heimatstaat. Wir regten an, weniger weit gehende Lösungen zu prüfen. Neue Untersuchungen haben ergeben, dass nur ein ganz geringer Anteil der Asylbewerber missbräuchliche Doppelgesuche stellen (vgl. nachfolgend S. 51), und dass sich hierüber relativ leicht Prognosen machen lassen.
Gemäss unserer internen Umfrage bei verschiedenen Datenschutzbeauftragten anderer Staaten entspricht eine flächendeckende Erhebung der Fingerabdrücke von Asylbewerbern keineswegs einer allgemeinen europäischen Praxis. In verschiedenen europäischen Staaten werden die Fingerabdrücke von Asylbewerbern nur dann erhoben, wenn im Einzelfall Anhaltspunkte für ein missbräuchliches Verhalten bestehen. Es ist nicht einzusehen, weshalb nicht auch unser Land eine solche Lösung wählen soll. Für den Fall, dass sich in Europa aufgrund neuer multinationaler Abkommen wider Erwarten in näherer Zukunft Änderungen ergeben sollten, müsste dem Bundesrat freilich ein gewisser Handlungsspielraum eingeräumt werden, womit wir einverstanden wären. Erneut wiesen wir darauf hin, dass die Bekanntgabe von Daten aus den heiklen Asyl- und Ausländersammlungen nur dann im Abrufverfahren erfolgen darf, wenn dies zur Erfüllung der gesetzlichen Aufgabe wirklich *unerlässlich* ist.

2.8. Verlängerung des Bundesbeschlusses über das Asylverfahren

Weil der Bundesbeschluss über das Asylverfahren vor Abschluss der Totalrevision des Asylgesetzes ausläuft, muss er von den Eidg. Räten verlängert werden. Diesen bietet sich damit die elegante Möglichkeit, die an sich «fertigen», im Grundsatz unbestrittenen neuen Datenschutzbestimmungen des revidierten Asylgesetzes sogleich in Kraft zu setzen. Ein Zuwarten bis ins Jahr 2000 schiene uns demgegenüber verfehlt, zumal das DSG die Frist zum Erlass solcher Datenschutzbestimmungen auf den 1. Juli 1998 anberaumt hat.

Aus Anlass der Verlängerung des Asylverfahrensbeschlusses haben wir im Ämterkonsultationsverfahren angeregt, die an sich «fertigen» und im Grundsatz unbestrittenen Datenschutzbestimmungen des revidierten Asylgesetzes zugleich mit der Verlängerung des Beschlusses in Kraft zu setzen. Ein Zuwarten bis zur Inkraftsetzung des revidierten Asylgesetzes im Jahr 1999 oder noch später schien uns unangebracht. Denn Art. 38 Abs. 3 des Datenschutzgesetzes (DSG) verlangt, dass fehlende Datenschutzbestimmungen in formellen Gesetzen bis spätestens zum 1. Juli 1998 zu erlassen sind.
Der Bundesrat hat dem Parlament nun aber - ohne uns im Vernehmlassungsverfahren nochmals angehört zu haben - eine andere Lösung unterbreitet. Danach soll

in einem neuen Absatz 4 zu Artikel 38 DSG die besagte Anpassungsfrist für den Asylbereich bis zum 31. Dezember 1999 verlängert werden.
Wir sind jedoch der Meinung, dass bereits heute eine Reihe von heiklen Datenbearbeitungen im Asylbereich gesetzlich ungenügend abgestützt und auch durch das Übergangsrecht von Art. 38 DSG nicht gedeckt sind. Auch die Eidg. Datenschutzkommission scheint diese Auffassung in ihrem Entscheid vom 29. November 1996 zu teilen (vgl. vorne S. 13). In einem viel beachteten Urteil hat das schweizerische Bundesgericht zudem kürzlich eine kantonale Behörde dazu verpflichtet, ohne eine genügende gesetzliche Grundlage beschaffte heikle Daten zu vernichten. Damit besteht für die Asylbehörden ein erhebliches Risiko, wenn die fehlenden gesetzlichen Grundlagen nicht rasch erlassen werden. Aus allen diesen Gründen sind wir daher an den Bundesrat herangetreten und haben ihn gebeten zu prüfen, ob dem Parlament nicht doch noch die von uns vorgeschlagene Lösung unterbreitet werden könne.

3. Telekommunikation

3.1. Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs sowie den Einsatz technischer Überwachungsgeräte

Das Eidgenössische Justiz- und Polizeidepartement beauftragte eine Studiengruppe mit der Ausarbeitung eines Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs sowie den Einsatz technischer Überwachungsgeräte. Im Rahmen der Ämterkonsultation hatten wir Gelegenheit, zu dem Entwurf Stellung zu nehmen.

Wie schon im 1. Tätigkeitsbericht ausgeführt, forderte die Geschäftsprüfungsdelegation des Nationalrates (GPK) die Schaffung von strikteren Regelungen für die Überwachung des Post- und Fernmeldeverkehrs zu Zwecken der Strafverfolgung. Daraufhin wurde am 15. Oktober 1993 vom Vorsteher des Eidgenössischen Justiz- und Polizeidepartementes (EJPD) eine Studiengruppe mit dem Auftrag eingesetzt, entsprechende Regelungen auszuarbeiten. Im Januar 1995 wurden die Revisionsarbeiten der Studiengruppe bezüglich der Überwachung des Post- und Fernmeldeverkehrs sistiert. Anfang 1996 beauftragte das EJPD die Studiengruppe unter gleicher Zusammensetzung mit der Ausarbeitung eines Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs. Dabei waren die bisherigen Vorarbeiten zu integrieren, die Schaffung einer Zentralstelle zur technischen Durchführung von Überwachungen des Fernmeldeverkehrs zu prüfen und insbesondere deren Kosten abzuschätzen. Wir verzichteten aus personellen wie zeitlichen Gründen auf die weitere Teilnahme an dieser Studiengruppe. Jedoch konnten wir im Oktober 1996 zu dem uns vorgelegten Entwurf eines Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs sowie den Einsatz technischer Überwachungsgeräte Stellung nehmen. Im Rahmen dieser Ämterkonsultation konnten die bestehenden sowie die durch die Ausarbeitung des Gesetzes entstandenen Differenzen bereinigt werden.

3.2. Telecom PTT

ISDN-Rufnummeranzeige/-unterdrückung

Unsere Forderungen im Bereich ISDN-Rufnummerübermittlung stiessen bei der TELECOM PTT grösstenteils auf offene Ohren. Abgesehen von einem Punkt, der die Gebührenerhebung betrifft, konnte Einigkeit erzielt werden.
Die Rufnummeranzeige, die das dienstintegrierende digitale Netz (ISDN) ermöglicht, ist eine äusserst praktische und sinnvolle Einrichtung, stärkt sie doch die Position des Angerufenen indem er feststellen kann, von welchem Anschluss er angewählt wird. Auch der Anrufer geniesst Vorteile: Er kann direkt zur richtigen Person durchgestellt bzw. zurückgerufen werden.
In einzelnen Fällen kann jedoch die Rufnummerübermittlung für die anrufende Person zu einer gravierenden Persönlichkeitsverletzung führen. Beispielsweise will ein Anwalt nicht, dass seine Klienten, die von seiner Kanzlei aus Telefonate tätigen, als solche sofort erkannt werden. Ruft eine Patientin von ihrem Spezialarzt ihren Arbeitgeber an, können gar hochsensible Gesundheitsdaten bekannt werden. Weiter existiert das Bedürfnis, diejenigen Rufnummern geheimzuhalten, die unbedingt für abgehende Telefonate freigehalten werden müssen.
Im März 1996 haben wir eine Empfehlung (siehe Seite 115) an die TELECOM PTT gerichtet, deren Hauptpunkte von der TELECOM akzeptiert wurden:
Die fallweise Rufnummerunterdrückung wird im Laufe des Jahres 1998 auch für analoge Telefonanschlüsse angeboten werden. Weiter ist unserer Forderung nach Orientierung der Kundinnen und Kunden über die Anzeige und Unterdrückungsmöglichkeit entsprochen worden. Der einzige Punkt, über den keine vollständige Einigung erzielt werden konnte, betrifft die Kostenlosigkeit der Rufnummerunterdrückung. Die TELECOM hat zwar auf die monatliche Gebühr verzichtet, nicht aber auf eine einmalige Einschaltgebühr.
Wir haben festgestellt, dass diese Gebühr von 15 Franken, auch wenn sie als gering erscheinen mag, einen entscheidungsbeeinflussenden Charakter besitzt. Die Kunden sehen sich gezwungen, für die Wahrung ihrer Rechte Kosten zu übernehmen, bedingt durch eine technische Neuerung, auf die sie keinen Einfluss hatten. Wir sind daher der Meinung, dass die Einschaltgebühr entfallen muss und haben diese Punkt dem Eidg. Verkehrs- und Energiewirtschaftsdepartement vorgelegt, das im März 1997 entschieden hat, dass die einmalige Gebühr erhoben werden darf. Der EDSB hat keine Möglichkeit mehr, diesen Entscheid weiterzuziehen. Allerdings können die TELECOM-Kundinnen und Kunden als Betroffene diesen EVED-Entscheid bei der Eidg. Datenschutzkommission anfechten.

- Erzwingung der Anzeige

ISDN sieht die Funktion «Identifikation erzwingen» vor. Teilnehmer, die über diese Funktion verfügen, können eine aktivierte Rufnummerunterdrückung des Anrufers rückgängig machen. Diese Funktion muss auf einige wenige Institutionen wie Notrufdienste (Polizei, Feuerwehr, Sanität), die klare Sicherheitsgründe nachweisen können, beschränkt bleiben. Zudem müssen diese Institutionen bekannt sein.
Es sind Fälle bekanntgeworden, bei denen auch weitere Anschlüsse über diese Funktion verfügten. Dies kann nicht akzeptiert werden. Die TELECOM hat uns versichert, der Sache nachzugehen. Falls aus nicht sogleich behebbaren Gründen die Rufnummerunterdrückung nicht zuverlässig funktioniert, sind die Kunden darüber zu informieren.

Telefonohrbild

- Anrufe ins Ausland

Ein TELECOM Kunde teilte uns mit, dass es in bestimmten Fällen trotz einer in der Schweiz aktivierten Unterdrückung zu einer Rufnummeranzeige im Ausland kam. Die TELECOM gab uns bekannt, dass sie letztlich nicht garantieren könne, dass ihre ausländischen Partner das Unterdrückungssignal korrekt interpretieren. Auch hier ist, solange die technischen Gegebenheiten international nicht genügend abgestimmt sind, eine klare Information der Kunden erforderlich (Transparenzprinzip).

Elektronische Teilnehmerverzeichnisse

Die umfassenden Suchmöglichkeiten in elektronischen Verzeichnissen können zu unerwarteten und unerwünschten Offenlegungen von Informationen über die Betroffenen führen.

Das elektronische Telefonverzeichnis ETV der TELECOM, aber auch Produkte (v.a. CD-ROM) privater Anbieter bieten sehr umfassende und nützliche Suchmöglichkeiten. Für die Betroffenen können sie jedoch auch zu unerwünschten Datenbekanntgaben führen. So sind etwa alle Anschlüsse einer bestimmten Strasse, eines bestimmten Hauses oder alle auf einen Anschluss eingetragenen Personen (im selben Haushalt lebende Personen) eruierbar.
Auch der Umstand, dass frühere Einträge einige Monate im ETV verbleiben, können zu einer heiklen und ungewollten Offenlegung familiärer Verhältnisse führen, wie uns ein Kunde anhand seines Beispiels gezeigt hat.
Wir sind momentan daran zu prüfen, wie der Datenschutz in diesem Bereich verbessert werden kann. Dabei werden wir auch die vorgesehene Lockerung der heutigen Eintragungspflicht im revidierten Fernmeldegesetz in unsere Überlegungen einbeziehen.

Das «TELECOM-Leck»

Durch einen im August 1996 erschienenen Pressebericht wurde bekannt, dass auf einem allgemein zugreifbaren Internet-Server der TELECOM nicht für die Öffentlichkeit bestimmte Daten zugänglich waren.
Nach der Durchsicht der auf unser Verlangen von der TELECOM unterbreiteten detaillierten Unterlagen, stellten wir fest, dass neben einer Menge Sachdaten auch einige Personendaten (Adresslisten, Lebensläufe) zugänglich waren.
Der Vorfall zeigt, dass die Datensicherheitsmassnahmen noch ungenügend sind. Als unerlässlich halten wir eine stärkere Sensibilisierung der Mitarbeiter für Datenschutzanliegen. Die TELECOM hat Massnahmen zur Verbesserung des Datenschutzes und der Datensicherheit eingeleitet.

3.3. Post PTT

Postkonto

Im Rahmen der Automatisierung des Postzahlungsverkehrs wurden die Unterschriften der Kontoinhaber, die bisher auf Papierkarten abgelegt waren, «eingescannt», um sie in elektronischer Form zu verwenden (Verifikation der berechtigten Teilnehmer an

Zahlungsverkehrdienstleistungen). Ein Postkontoinhaber vermutete darin eine Persönlichkeitsverletzung.

Der erwähnte Postkontoinhaber war nicht bereit, dem «Einscannen» und der damit verbundenen elektronischen Weiterbearbeitung seiner Unterschrift zuzustimmen. Er machte sinngemäss geltend, dass er sich dadurch in seiner Persönlichkeit verletzt fühle.
Unsere Abklärungen ergaben, dass - auch wenn ein Missbrauch nie ganz auszuschliessen ist - die von der Post ergriffenen technischen und organisatorischen Massnahmen gegen ein unbefugtes Bearbeiten der elektronisch vorliegenden Unterschriften angemessen sind.
Wir stellten weiter fest, dass die Gesamtheit der pro Postkontoinhaber bearbeiteten Daten eine hohe Sensibilität aufweist. Bearbeitet werden neben den Personalien und dem Kontostand z. B. auch die Ein- und Auszahlungen der letzten 15 Monate, die Postomatbezüge, die Einkäufe mit Postcard etc. Hier können ohne weiteres Persönlichkeitsprofile entstehen.
Daher prüften wir insbesondere, ob der Zugriff, auf die - für die Abwicklung des Zahlungsverkehrs notwendigen - Daten postintern weiter eingeschränkt werden kann und auch die übrigen Datensicherheitsmassnahmen genügend sind. Untersucht wurden von uns auch die Postkontoeröffnungsformulare. Es geht hier vor allem um die Frage, welche Daten durch den Erhebungszweck legitimiert sind und die Transparenz für den Kunden. Diese Abklärungen sind noch nicht abgeschlossen.

3.4. Aufzeichnung von Mitarbeiterdaten bei der Nutzung von Internet-Diensten

Das Internet (bzw. Intranet) hält auch am Arbeitsplatz immer mehr Einzug. Das reichhaltige Angebot kann schon mal zu ausgedehnten und vom Arbeitgeber unerwünschten «Surftouren» verleiten. Die Kontrolle über das Verhalten der Mitarbeiter ist diesbezüglich nicht gestattet. Weiteren Kontrollen durch den Arbeitgeber sind jedoch klare Grenzen gesetzt.

Mehrere Leute wollten wissen, unter welchen Bedingungen und in welchem Mass Daten über die Nutzung von Internet-Diensten (bzw. vergleichbaren Diensten) bearbeitet werden dürfen.
Grundsätzlich gehört es zur Aufgabe der Linienvorgesetzten, die Einhaltung der Anordnungen an ihre Mitarbeiter zu überprüfen. Arbeitszeit und betriebliche Ressourcen z. B. dürfen nicht für private Zwecke benutzt werden. Dies ist in der Regel ohne detaillierte technische Überwachungsmassnahmen möglich.
Eine umfassende Aufzeichnung und Auswertung von Benutzeraktivitäten bei der Internetnutzung kann hingegen zu einem schweren Eingriff in die Persönlichkeit der Betroffenen führen. Denn die Entstehung von Persönlichkeitsprofilen ist ohne weiteres möglich.
Die Informatikdienste sind daher nicht befugt, die Benutzung der Internet-Dienste durch die Mitarbeiter zu analysieren. Erst bei konkreten Anhaltspunkten von Unregelmässigkeiten kann eine Aufzeichnung auf Anordnung der vorgesetzten Stelle verhältnismässig erscheinen.
Jedoch sind die Mitarbeiter vorgängig zu informieren, welche Daten über ihre Internet-Nutzung erfasst werden, wie sie bearbeitet werden und wer sie unter welchen Bedingungen auswertet.
Die Datenbearbeitung ist auf das Mass zu beschränken, das für den Zweck (Missbrauchsbekämpfung) absolut nötig ist. Nur Personen, die speziell damit beauftragt

Gläserner Mensch

worden sind, dürfen auf personenbezogene «Log-Dateien» zugreifen. Anschliessend sind die nicht mehr benötigten Daten sogleich zu vernichten.

4. Personalwesen

Bundesverwaltung

4.1. Inhalt des Personaldossiers und Auskunftsrecht

Der Arbeitgeber darf Notizen und Berichte über das Verhalten eines Arbeitnehmers nur dann im Personaldossier aufbewahren, soweit sie für das Arbeitsverhältnis relevant sind. Qualifikationen und Beurteilungen gehören zu den wichtigsten Daten im Personaldossier und können erst dann entfernt werden, wenn sie zur Durchführung des Arbeitsvertrages nicht mehr benötigt werden. Dem Arbeitnehmer steht grundsätzlich ein uneingeschränktes Auskunftsrecht zu.

Die Frage nach dem zulässigen Inhalt des Personaldossiers wurde von einem PTT-Angestellten aufgeworfen, nachdem er in seinem Personaldossier Berichte über sein Verhalten vorfand. Sie hatten hauptsächlich die Beschädigung von kleineren Gegenständen im Betrieb zum Inhalt. Die Berichte wurden schliesslich eingestellt, da sie keinen Anlass für disziplinarische Massnahmen gaben.
Wir machten die PTT darauf aufmerksam, dass Akten und Berichte über besondere Vorkommnisse im Betrieb nur dann im Personaldossier aufzunehmen sind, wenn sie für das Arbeitsverhältnis objektiv tatsächlich benötigt werden. Dokumente der oben beschriebenen Art hätten demzufolge nicht im Personaldossier aufbewahrt werden dürfen. Finden sich bedeutungslose Dokumente doch im Personaldossier, so müssten sie durch eine regelmässige Triage des Dossiers entfernt werden. Dies gilt auch für Dokumente, die erst nach einer bestimmten Zeit ihre Bedeutung für die weitere Durchführung des Arbeitsvertrages verloren haben. Andererseits sind Informationen im Personaldossier solange aufzubewahren, als sie tatsächlich benötigt werden. Die vorzeitige, endgültige Entfernung von Qualifikationsbögen aus dem Personaldossier während eines hängigen Auskunftsverfahrens kommt einer unverhältnismässig kurzen Aufbewahrungsdauer gleich. Diese Verletzung des Verhältnismässigkeitsprinzipes kann unter Umständen zusätzlich eine Missachtung von Treu und Glauben darstellen.
Dem PTT-Angestellten wurde zu Beginn das Auskunftsrecht wiederholt verweigert. Erst unter Einbezug der Kreispostdirektion wurde Einsicht ins Personaldossier gewährt. Das Fotokopieren des Inhaltes des Personaldossiers wurde erst später ermöglicht. Wir machten die PTT darauf aufmerksam, dass jede Person vom Inhaber einer Datensammlung Auskunft darüber verlangen kann, ob Daten über sie bearbeitet werden.
Im übrigen haben wir festgehalten, dass der Dateninhaber eine vollständige und wahrheitsgemässe Auskunft über den Inhalt des Personaldossiers geben muss. Dabei schliesst die Einsichtnahme des Personaldossiers durch die betroffene Person an Ort und Stelle das Fotokopieren des Inhaltes nicht aus. Der Inhaber der Datensammlung kann die Auskunft nur dann verweigern, einschränken oder aufschieben, soweit ein formelles Gesetz es vorsieht oder es wegen überwiegender Interessen eines Dritten erforderlich ist. Ein Bundesorgan kann zudem die Auskunft verweigern, einschränken oder aufschieben, soweit es wegen überwiegender öffentlicher Interessen, insbesondere der inneren und äusseren Sicherheit der Eidgenossenschaft,

erforderlich ist oder die Auskunft den Zweck einer Strafuntersuchung oder eines anderen Untersuchungsverfahrens in Frage stellt. Der Arbeitgeber ist zudem verpflichtet, die Arbeitnehmer über das Auskunftsrecht zu informieren. Wir haben dann die Bedeutung von Art. 328*b* des Schweizerischen Obligationenrechts (OR) unterstrichen. Diese Bestimmung gilt als ergänzendes Verwaltungsrecht und ist somit für Datenbearbeitungen durch den Bund analog anwendbar. Sie besagt, dass der Inhaber einer Datensammlung nur diejenigen Daten bearbeiten darf, die er für einen bestimmten Zweck objektiv tatsächlich benötigt. Der Personaldienst der in Frage stehenden Kreispostdirektion hat sich bereit erklärt, die Personaldossiers nach den einschlägigen datenschutzrechtlichen Grundsätzen zu führen und die Angestellten über das Auskunftsrecht - gegebenenfalls im Anstellungsschreiben - zu informieren.

4.2. Videoüberwachung am Arbeitsplatz

Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, dürfen nicht eingesetzt werden. Sind solche Systeme aus anderen Gründen erforderlich, sind sie insbesondere so zu gestalten und anzuordnen, dass Gesundheit, Persönlichkeit und Bewegungsfreiheit der Arbeitnehmer dadurch nicht beeinträchtigt werden.

Ein Angestellter der PTT-Betriebe hat sich bei uns über die Zulässigkeit der Videoüberwachung am Arbeitsplatz erkundigt. Wir teilten ihm mit, dass Arbeitnehmer Anspruch auf eine angemessene Privatsphäre am Arbeitsplatz haben. Sie müssen über die verwendeten Überwachungsmethoden informiert werden. Eine dauernde elektronische Überwachung ist nicht gestattet. Vorgesetzte, welche diese Grundsätze verletzen, müssen mit Disziplinarmassnahmen oder Entlassung rechnen (vgl. Richtlinien der Internationalen Arbeitsorganisation IAO). Bei Systemen, mit denen eine Überwachung aus Sicherheitsgründen (bspw. Kontrolle des Betriebsablaufes) durchgeführt wird, ist darauf zu achten, dass eine für die Persönlichkeit der Angestellten schonende Vorgehensweise gewählt wird. Das gilt auch für Anlagen, welche der Produktionssteuerung dienen. Wir schlugen deshalb der PTT vor, die Überwachung am Arbeitsplatz in internen Weisungen festzuhalten.

4.3. Telefonüberwachung am Arbeitsplatz

Telefonzentralen können unter bestimmten Voraussetzungen Überwachungs- und Kontrollsysteme darstellen. Dies ist z. B. dann der Fall, wenn die Telefonnummern aller ein- und ausgehenden Anrufe angezeigt und registriert oder die Dauer bzw. die Kosten der einzelnen Gespräche festgehalten werden. Insbesondere gehören auch Telefonsysteme dazu, die das Abhören von Gesprächen ohne Wissen der Betroffenen zulassen. Das Verhalten der Arbeitnehmer darf jedoch durch solche Überwachungs- und Kontrollsysteme nicht kontrolliert werden. Zulässig ist ihr Einsatz nur aus Sicherheitsgründen oder zur Produktionssteuerung (vgl. unseren 2. Tätigkeitsbericht, S. 44ff).

Ein Vertreter eines privaten Unternehmens hat sich bei uns über die Zulässigkeit des Einsatzes von Telefonzentralen erkundigt. Wir teilten ihm diesbezüglich mit, dass Arbeitgeber Telefonzentralen nur einsetzen dürfen, wenn die betroffenen Arbeitnehmer vorgängig informiert worden sind. Die Aufzeichnung der Teilnehmernummer der aus beruflichen Gründen angewählten Anschlüsse ist zulässig, sofern sie nicht zur

Kontrolle des Verhaltens der Arbeitnehmer vorgenommen wird (sondern z. B. für die Rechnungsstellung an Kunden). Die Teilnehmernummern der von den Arbeitnehmern angewählten privaten Anschlüsse dürfen unter keinen Umständen in vollständig identifizierbarer Form aufgezeichnet werden, wenn das Führen privater Telefongespräche nicht generell untersagt wird. Diese Aufzeichnung soll lediglich den betroffenen Personen dienen (z. B. für die Kontrolle der wegen privaten Gesprächen getätigten Lohnabzüge). Bei Vorliegen von offensichtlichen Unregelmässigkeiten bei den ausgewiesenen Kosten für einzelne Anschlüsse kann bspw. der Personalleiter des Unternehmens nach vorgängiger Information des Personals eine Detailauswertung zum entsprechenden Anschluss verlangen. Dabei sollen die Teilnehmernummern der angewählten privaten Anschlüsse in nicht identifizierbarer Form aufgezeichnet werden. Offensichtliche Unregelmässigkeiten werden dann vermutet, wenn bspw. bei einem Anschluss mehr als die doppelten Kosten des Durchschnitts der betreffenden Einheit innerhalb des Unternehmens ausgewiesen werden, ohne dass dies mit betrieblichen Erfordernissen erklärbar ist. Der Inhalt von Telefongesprächen darf nur aus Gründen der Leistungskontrolle (z. B. bei Telefonverkäufen oder zu Schulungszwecken) oder aus Sicherheitsgründen aufgezeichnet werden. Diese sehr einschneidende Kontrollmassnahme ist nur zulässig, wenn die Person, deren Gespräch aufgezeichnet oder mitgehört wird, damit einverstanden ist und jeweils darüber eindeutig und rechtzeitig in Kenntnis gesetzt wird (z. B. durch ein optisches oder akustisches Signal).

fax

4.4. Das Projekt BV-PLUS

Das System BV-PLUS sieht die Bearbeitung von besonders schützenswerten Personendaten vor (vgl. unseren 1. und 3. Tätigkeitsbericht, S. 57ff. bzw. 34). Deshalb verlangten wir vom Eidg. Personalamt die Verankerung des Systems in einem Gesetz im formellen Sinne. Wir verlangten auch, dass das System BV-PLUS lediglich für die Lohnbewirtschaftung zentral eingesetzt werde. Schliesslich erliessen wir eine Empfehlung, die an das Eidgenössische Finanzdepartement weitergezogen wurde.

Anfangs 1996 haben wir von der baldigen Inbetriebnahme des zentralen Datenbearbeitungssystems der Bundesverwaltung BV-PLUS erfahren. Bereits früher hatten wir dem Eidgenössischen Personalamt (EPA) auf die Tendenz zur dezentralen Datenbearbeitung in der Bundesverwaltung aufmerksam gemacht (vgl. unseren ersten Tätigkeitsbericht, S. 58ff). Wir begrüssten die Tendenz zur Dezentralisierung aus datenschutzrechtlichen, aber auch aus Wirtschaftlichkeits- und Effizienzgründen. Wir forderten deren Verankerung im damaligen Entwurf einer Verordnung zum Schutze der Daten von Bundesbediensteten. Das System hätte nur für die Lohnbewirtschaftung zentral geführt werden sollen.
Wegen der vorgesehenen Bearbeitung von besonders schützenswerten Personendaten durch das System BV-PLUS betonten wir die Notwendigkeit der Verankerung des Systems in einer gesetzlichen Grundlage im formellen Sinne. Das EPA hat aber diese Forderungen abgewiesen. Das EPA vertrat die Meinung, dass für BV-PLUS - mangels Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen - reduzierte Anforderungen an die gesetzliche Grundlage bestehen. Im Zusammenhang mit der Dezentralisierung der Datenbearbeitungen in der Bundesverwaltung weicht das System BV-PLUS nach Meinung des EPA vom bestehenden Personalinformationssystem PERIBU nicht ab. Wir empfahlen dem EPA, BV-PLUS lediglich für die Lohnbewirtschaftung und nur nach Schaffung der formell- und materiellgesetzlichen Grundlagen einzusetzen. Das EPA lehnte die Empfehlung ab. In der Folge legten wir die Angelegenheit dem Eidgenössischen Finanzdepartement zum Entscheid vor. Dieses teilte uns mit, dass für BV-PLUS eine Rechtsgrundlage auf Verwaltungsstufe geschaffen werde.
Ausserdem informierte uns das Finanzdepartement, dass BV-PLUS nicht mehr mit der ursprünglich vorgesehenen Software, sondern mit der Standardsoftware SAP R3 HR realisiert werde.
Wir wiesen zudem das Finanzdepartement noch auf die Notwendigkeit einer gesetzlichen Grundlage im formellen Sinne für das Personalbewirtschaftungssystem der Bundesverwaltung hin.
Unseres Erachtens ist vorliegend ein Gesetz im formellen Sinne nicht nur wegen der Bearbeitung von besonders schützenswerten Personendaten notwendig, sondern auch deshalb, weil die heutige Beamtengesetzgebung die Zuständigkeit des EPA zur Bearbeitung dieser Daten nicht vorsieht. Ausserdem würde die Schaffung einer solchen gesetzlichen Grundlage Gelegenheit zur Regelung der Aufgabenverteilung zwischen dem EPA und den einzelnen Personaldiensten geben.

4.5. INSIGHTS - Personalevaluations-System

Seit einigen Jahren steht die «Management-Mitarbeiter»-Version dieses Produktes den Verwaltungseinheiten des Bundes auf Diskette zur Verfügung. In unserem zweiten Tätigkeitsbericht (S. 47 ff.) haben wir verschiedene Aspekte angesprochen und geraten, solche Tests nicht bei der Einstellung zu verwenden, sondern allenfalls als

Instrument zur Teamführung ins Auge zu fassen. Da die Disketten mehrheitlich nicht durch ein Passwort geschützt sind, haben wir die Notwendigkeit betont, die Daten von Anfang an zu anonymisieren. Schliesslich haben wir angesichts der zeitlich begrenzten Aussagekraft der Testresultate davon abgeraten, die Analysen systematisch zu archivieren und aufzubewahren (vgl. auch Anhang S. 91 des vorliegenden Berichts).

Für die Tests werden keine Softwareprodukte verkauft, sondern eine bestimmte Anzahl Analysen, die der Bundesverwaltung in Diskettenform zur Verfügung gestellt werden.
Der Verkäufer empfiehlt, bestimmte Benutzungskriterien einzuhalten: Freiwilligkeit der Teilnahme am Testverfahren, Anspruch der betroffenen Person auf Herausgabe der Testresultate, Verfall der Analyseresultate nach zwei Jahren. Diese Empfehlungen bilden indessen nicht Teil des Vertrags. Ebensowenig werden die Käufer auf einen Ethikkodex verpflichtet, sondern können Analysen ohne Vorschulung erwerben und verwenden.
Die Diskette kann durch zwei verschiedene Passwörter geschützt werden: Das erste erlaubt die Eingabe der zu analysierenden Daten, das zweite ermöglicht das Ausdrucken der Resultate. Man hat uns ferner zugesichert, dass ein hohes Sicherheitsniveau eingehalten würde (Selbstvernichtung des Programms bei Versuchen, die Daten zu ändern; Piraterie ausgeschlossen).
Nach der Eingabe können die Daten - mit Ausnahme der Identitätsangaben, bei denen eine einmalige Änderung möglich ist - nicht mehr abgeändert werden.
Einige Mitarbeiter des Datenschutzbeauftragten haben sich dem Test unterzogen und die Resultate evaluiert bzw. von einer nahestehenden Person evaluieren lassen. Die Richtigkeit der Resultate wurde auf durchschnittlich 70 bis 80 % geschätzt.
Für den Fall, dass - wie in unserem Sekretariat - eine Diskette ohne Passwort in Umlauf gelangt, haben wir als erstes darauf hingewiesen, dass die Analysen von Anfang an anonymisiert werden müssen und der Schlüssel zur Identifizierung nur der betroffenen Person bekannt sein darf.
Wenn das Produkt systematisch als Instrument zur Personalführung eingesetzt wird, werden die Disketten mit mindestens einem Passwort (zwei, wenn die Abläufe Eingabe und Drucken getrennt werden sollen) geschützt. Maximal zwei Mitarbeiter des Personaldienstes haben Zugang zu den Daten, wobei auch da eine Anonymisierung zu erwägen ist, sobald der Bearbeitungsstand der Daten es erlaubt.
Im übrigen haben wir angesichts der zeitlich begrenzten Aussagekraft der Analyse von einer systematischen Archivierung und Aufbewahrung der Resultate abgeraten.
Da es sich um sehr allgemeine Analysen handelt, haben wir ferner hervorgehoben, dass das Produkt nicht als Instrument bei der Einstellung von Personal, sondern vielmehr zur Teamführung dienen kann.
Schliesslich müssen solche Tests im Einklang mit den Richtlinien des Eidgenössischen Personalamtes zur Anwendung von Einzel- und Gruppentestverfahren stehen (vgl. Anhang S. 91 des vorliegenden Berichts).

4.6. Einholen von Referenzen gegen den Willen der betroffenen Person

Im Rahmen einer Stellenbesetzung in der Bundesverwaltung wurden Informationen bei Dritten eingeholt. Das Einholen von Referenzen ist jedoch - ohne die vorherige Zustimmung des Stellenbewerbers - aus Sicht des Datenschutzes grundsätzlich nicht zulässig.

Ein Angestellter der Bundesverwaltung beschwerte sich bei uns darüber, dass anlässlich seiner Anstellung bei der Bundesverwaltung ohne seine Zustimmung Referenzen bei Dritten eingeholt wurden. Diese Dritten wurden im Bewerbungsschreiben nicht als Referenzquellen angegeben. Diesbezüglich teilten wir ihm folgende Grundsätze mit: Die Voraussetzungen von Datenbearbeitungen bei Stellenbesetzungen sind weder im Beamtenrecht, noch im Datenschutzgesetz oder in dessen Vollzugsverordnung geregelt. Die grundsätzliche Zulässigkeit von Datenbearbeitungen im Zusammenhang mit Stellenbewerbungen ergibt sich jedoch aus den allgemeinen Aufgaben der Departemente der Bundesverwaltung.
Der einzige Hinweis auf den Umfang der zulässigen Datenbearbeitungen im Zusammenhang mit Stellenbesetzungen innerhalb der Bundesverwaltung ist im Rundschreiben des Eidg. Personalamtes (EPA) über die Bearbeitung von Personendaten in der Bundesverwaltung vom 26. Januar 1984. Dieses Schreiben ist trotz Aufhebung der zugrundeliegenden Richtlinien bis heute in Kraft. Ziffer 2.4.1. dieses Rundschreibens lautet: «Genügen die von einem Stellenbewerber eingereichten Unterlagen und angegebenen Referenzen für die Beurteilung nicht, so ist das weitere Vorgehen mit dem Kandidaten abzusprechen». Daraus geht hervor, dass für die Einholung von Referenzen die Zustimmung der betroffenen Person erforderlich ist. Im übrigen sprechen wir uns auch in unserem «Leitfaden für die Bearbeitung von Personendaten im Arbeitsbereich durch private Personen» (S. 6/7) für diese Lösung aus. Die dort aufgeführten Grundsätze betreffen die Datenbearbeitung im privatrechtlichen Bereich, sind aber auf die Bundesverwaltung analog anwendbar.

5. Versicherungswesen

Sozialversicherungen

5.1. Invalidenversicherung und Datenschutz

Wir wurden vom Bundesamt für Sozialversicherung (BSV) aufgefordert, uns zum «Zusammenleben» zwischen der Invalidenversicherungs- und der Datenschutzgesetzgebung zu äussern. Unten folgen einige ausgewählte Fragen, die sich vor allem auf die Problematik der Bekanntgabe von Daten an Dritte beziehen, sowie unsere Antworten vom vergangenen Jahr.

Im Bereich der Invalidenversicherung (IV) wie auch bei den übrigen Sozialversicherungen ist das Verhältnis zwischen der einschlägigen Gesetzgebung und den Datenschutzbestimmungen besonders problematisch. Insbesondere haben wir zu den folgenden Fragen Stellung genommen:

- Ist es möglich, sich zur Bekanntgabe von - sogar schützenswerten - Daten an Drittpersonen auf Artikel 19 Absatz 1 Buchstabe d DSG zu stützen?

Grundsätzlich können sogar schützenswerte Personendaten - unter bestimmten Voraussetzungen - an Drittpersonen bekanntgegeben werden. Allerdings ist im IV-Bereich Artikel 19 Absatz 4 Buchstabe b DSG zu berücksichtigen, welcher «gesetzliche Geheimhaltungspflichten» vorbehält. Artikel 50 Absatz 1 des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG), der ebenfalls auf die IV anwendbar ist, sieht solche Pflichten vor. Vorbehalten bleiben die vom Bundesrat

vorgesehenen Ausnahmen, die in Artikel 209 bis der Verordnung über die Alters- und Hinterlassenenversicherung (AHVV) verankert werden. Die IV-Organe müssen sich also auf diese Bestimmung, nicht auf Artikel 19 DSG, stützen, wenn sie die Bekanntgabe von Daten ins Auge fassen.

- Kann das Bundesamt für Sozialversicherung (BSV) sich auf Artikel 19 Absatz 2 DSG berufen, um Drittpersonen mitzuteilen, ob eine bestimmte Person bei der IV angemeldet ist?

Wir haben diese Frage verneint. Bundesorgane sind zwar berechtigt (aber nicht verpflichtet), auf Anfrage Namen, Vornamen, Adresse und Geburtsdatum einer Person bekanntzugeben. Allerdings dürfen aus diesen Informationen keine weiteren Angaben und insbesondere keine schützenswerten Daten über den Beteiligten ersichtlich sein.
Genau dies wäre jedoch der Fall, wenn die IV-Abteilung des BSV die Identität eines Beteiligten bekanntgeben würde, weil daraus gleichzeitig dessen Anmeldung bei der IV zu ersehen wäre.

- Stimmt es, dass das BSV die Bekanntgabe von Personendaten sperren muss, wenn die betroffene Person dies gemäss Artikel 20 DSG verlangt?

In der Tat muss der Wunsch einer Person nach Sperrung der Bekanntgabe ihrer Personendaten selbst dann respektiert werden, wenn die vorgesehene Bekanntgabe an sich rechtmässig wäre.
Allerdings darf die verlangte Sperrung durch keinen der in Artikel 20 Absatz 2 DSG aufgezählten Gründe aufgehoben werden. Gemäss diesem Absatz können Bundesorgane die Sperrung verweigern oder aufheben, wenn eine Rechtspflicht zur Bekanntgabe besteht oder die Erfüllung ihrer Aufgabe sonst gefährdet wäre.
Eine Sperrung muss sich schliesslich auf genaue Daten beziehen und auf einem aktuellen und schutzwürdigen, von der betroffenen Person glaubhaft gemachten Interesse beruhen.

- Kann sich das BSV auf Artikel 22 DSG berufen, um die Bekanntgabe von Personendaten Forschungszwecken ohne Zustimmung der betroffenen Person zu rechtfertigen?

Wir haben darauf hingewiesen, dass Artikel 22 DSG aufgrund der gesetzlichen Geheimhaltungspflichten nicht anwendbar ist (vgl. Artikel 19 Abs. 4 DSG).
Im IV-Bereich stehen laut Artikel 50 AHVG beziehungsweise Artikel 209bis AHVV zwei Möglichkeiten für die Bekanntgabe von Daten an Drittpersonen offen: die Einwilligung des BSV oder die schriftliche Einwilligung der betroffenen Person.
Das BSV kann demnach darauf verzichten, die beteiligte Person um ihre Zustimmung zu ersuchen, indem es in die Bekanntgabe von Daten z.B. in Form von Einsicht in IV-Dossiers einwilligt. Das Bundesamt hat seine Einwilligung in Form einer Verfügung abzugeben, über welche die betroffenen Personen informiert werden müssen. Diese können die Verfügung mit Beschwerde anfechten (Artikel 209bis Absatz 3 AHVV).

Schliesslich haben wir daran erinnert, dass das BSV in erster Linie für die Einhaltung der im DSG verankerten Grundsätze verantwortlich ist. Daher muss das BSV insbe-

sondere bei der Datenbekanntgabe darauf achten, dass die seiner Aufsicht unterstellten Organe, wie die IV-Stellen, einheitliche Regeln anwenden.

5.2. Systematische Bekanntgabe der Diagnose an die Krankenkassen

Die Ausführungen unter dem Titel «5.1. Systematische Bekanntgabe der Diagnose an die Krankenkassen» (vgl. 3. Tätigkeitsbericht Seiten 39 ff.) zur Auslegung der Absätze 3 und 4 von Art. 42 KVG sind aus unserer Sicht nach wie vor gültig. Sie gaben jedoch teilweise zu Missverständnissen Anlass, welche hier kurz geklärt werden sollen. Aus dem Gesetzestext ergibt sich, dass genaue Diagnosen nur auf Anfrage, nicht jedoch systematisch (in jedem Fall) bekanntzugeben sind. Regelmässig dem Versicherer bekanntzugeben sind «diejenigen Angaben, die er benötigt, um die Berechnung der Vergütung und die Wirtschaftlichkeit der Leistung überprüfen zu können» (Art. 42 Abs. 4 KVG). Welches nun diese Daten sind, ergibt sich aus dem Verhältnismässigkeitsgrundsatz: Es sind nur solche Informationen, welche diese Prüfung erlauben (Kriterium der Geeignetheit), und darunter bloss diejenigen, welche dazu auch unabdingbar sind (Kriterium der Notwendigkeit).

5.3. Verzicht auf die Entbindung vom Arztgeheimnis beim Militärpflichtersatz

Das Bundesamt für Sanität und das Bundesamt für Militärversicherung müssen regelmässig Gesundheitsdaten an die kantonalen Militärpflichtersatzbehörden bekanntgeben. Aus Gründen der Verwaltungsökonomie soll bei erstmaligen Routineabklärungen inskünftig auf eine Einwilligung der Betroffenen verzichtet werden.

Im Bundesgesetz über den Militärpflichtersatz fehlt eine ausdrückliche Regelung über die Weitergabe der besonders schützenswerten Gesundheitsdaten. Daher stellte sich die Frage, ob bei einer Weitergabe dieser Daten ohne vorherige Einwilligung der Betroffenen nicht das Arztgeheimnis gemäss Strafgesetzbuch oder das Datenschutzgesetz verletzt würde. In einem Gutachten zur ersten Frage erachtete das Bundesamt für Justiz aufgrund der besonderen Umstände eine Verletzung des Arztgeheimnisses gemäss Strafgesetzbuch als nicht gegeben.
Setzt man die *stillschweigende Einwilligung* der Betroffenen jedenfalls für die Bekanntgabe *nicht* besonders schützenswerter Daten voraus, wäre die Weitergabe solcher Daten *im Einzelfall* gemäss Datenschutzgesetz zulässig. Bei den zunehmenden Datenvernetzungen erscheint es indessen als fraglich, ob die Betroffenen (selbst in Erwartung eines sie begünstigenden Behördenentscheids) alle möglichen Datenbearbeitungen gutzuheissen bereit sind, wenn nach ihrer Meinung weniger weitgehende Bearbeitungen ausreichen würden. Sind jedoch auch *besonders schützenswerte Daten über die Gesundheit* von den beabsichtigten Datenbekanntgaben betroffen, *kann nach unserer Auffassung jedoch nicht mehr auf eine stillschweigende Einwilligung geschlossen werden*. Die bestehende Lücke beim Militärpflichtersatz sollte bis zum 1. Juli 1998 geschlossen werden (vgl. hierzu auch S. 103).
Bis zum 1. Juli 1998 haben wir zu der beabsichtigten Praxis unser Einverständnis erklärt. Unsere Nachforschung hat ergeben, dass bei den ersten Routineabklärungen nur ganz wenige Daten übermittelt werden.

Privatversicherungen

5.4. Merkblatt und Einwilligungsklauseln

Die Konzeption der Merkblätter und der Einwilligungsklauseln im Privatversicherungsbereich scheint sich in der Praxis durchzusetzen und wurde in Zusammenarbeit mit den einzelnen Versicherungen weiterentwickelt. Einerseits verbesserte sich die Transparenz hinsichtlich der Merkblätter und der Einwilligungsklauseln erheblich. Andererseits erklärte sich erstmals eine Versicherungsgesellschaft bereit, die (von uns geforderte) Einwilligung für jedes spezifische Ereignis (Antrag, Anmeldung, Unfall, Leistung, Schaden etc.) von den Versicherten einzuholen.

Vorab sei - insbesondere was die Einwilligungsklauseln betrifft - auf die sehr umfassenden Ausführungen des dritten Tätigkeitsberichts verwiesen (vgl. S. 42 ff).
Das Merkblatt zum Datenschutz muss so ausgestaltet sein, dass der Versicherte so weit als möglich über die Bearbeitung seiner Daten informiert wird. (Transparenzprinzip). Es muss für ihn erkennbar sein, wer welche Daten zu welchem Zweck wem bekanntgibt. Zudem ist die Kenntnis der betroffenen Person über die Bearbeitung ihrer Daten Voraussetzung dafür, dass die einzelnen Versicherungsgesellschaften (juristische Personen) zahlreiche Datensammlungen nicht beim EDSB anmelden müssen.
Der Inhalt der durch uns überprüften Merkblätter ist im Vergleich zu früher genauer und umfassender. Insbesondere wird der Kunde ausführlich in Kenntnis gesetzt, worüber er Auskunft verlangen kann (vorhandene Daten, Zweck, Kategorien der bearbeiteten Personendaten, die an der Sammlung Beteiligten, Datenempfänger). Dem Auskunftsrecht ist in der Praxis die nötige Aufmerksamkeit zu schenken, gilt es allgemein als das zentrale Element des Datenschutzrechts.
Ebenso wurden die uns vorgelegten Einwilligungsklauseln durch die Versicherungen konkretisiert. Der Zweck der Datenbearbeitung sowie diejenigen Personen bzw. Stellen, mit denen die Versicherung Daten austauscht, sind anschaulicher und abschliessend formuliert.
Im weiteren verlangen wir schon seit jeher, dass die betroffene Person eine Einwilligungsklausel von Gesetzes wegen jederzeit widerrufen kann. Die Möglichkeit des jederzeitigen Widerrufs muss daher in jeder Einwilligungsklausel enthalten sein.
Zudem hat die Versicherung die Einwilligung immer im Zusammenhang mit einem spezifischen Ereignis einzuholen. Wir stehen in Kontakt mit einer Versicherung, die nach dem «Baukastenprinzip» für jede Versicherungsbranche und für jedes Ereignis spezifische Einwilligungsklauseln ausgearbeitet hat. Dies soll am Beispiel der Kollektiv-Krankenversicherung näher erläutert werden: Sowohl im Stadium des Antrags bzw. der Anmeldung als auch im Krankheitsfall sind - je nach Situation - spezifische Einwilligungen von der betroffenen Person einzuholen. Zudem legen wir Wert darauf, dass die Einwilligungsklauseln unmittelbar neben der Unterschrift auf den entsprechenden Versicherungsformularen fettgedruckt hervorgehoben werden.
Schliesslich ist im Anfangsstadium eines Versicherungsvertrages noch die Einwilligung des zu Versichernden für die Verwendung seiner Personalien für Marketingzwecke einzuholen. Auch hier ist auf das jederzeitige Widerrufsrecht hinzuweisen sowie auf den Umstand, dass ein Sperren der Daten für Marketingzwecke keine sonstigen negativen Auswirkungen auf den Vertragsabschluss haben darf. Der Vertragsabschluss darf also nicht davon abhängig gemacht werden, ob jemand seine Zustimmung dazu gibt oder nicht.

5.5. Mangelnde Vertraulichkeit von medizinischen Angaben in Versicherungsformularen

Ein Arbeitgeber bekam - im Rahmen einer Anmeldung für eine kollektive Krankentaggeldversicherung - unfreiwillig Einblick in die Gesundheitsdaten der Arbeitnehmerin. Aus datenschutzrechtlicher Sicht stellt dies jedoch eine Persönlichkeitsverletzung der betroffenen Arbeitnehmerin dar, sofern keine Rechtfertigungsgründe vorliegen.

Eine Arbeitnehmerin trat eine neue Stelle an und hatte die Absicht, sich bei der kollektiven Krankentaggeldversicherung ihres neuen Arbeitgebers versichern zu lassen. Sie füllte jedoch den im Anmeldeformular aufgeführten medizinischen Fragebogen nicht vollständig aus. Versicherungsnehmer und somit Vertragspartner der Versicherung war jedoch nicht die zu versichernde Arbeitnehmerin, sondern eine dafür geschaffene Stiftung, deren Adresse mit derjenigen des Arbeitgebers identisch war. Die Versicherung schickte in der Folge das unvollständig ausgefüllte Formular an den Arbeitgeber bzw. die Stiftung zurück mit der Bitte, dieses vollständig ausfüllen zu lassen. Sowohl die Arbeitnehmerin als auch der Arbeitgeber beschwerten sich daraufhin bei der Versicherung und machten sinngemäss geltend, dass dies datenschutzrechtlich nicht erlaubt sei.
Wir hielten fest, dass es aus datenschutzrechtlicher Sicht grundsätzlich nicht zulässig ist, besonders schützenswerte Personendaten - wie Angaben über den Gesundheitszustand - Dritten bekanntzugeben. Es ist vorliegend mehr als fraglich, ob die Stiftung (und zugleich der Arbeitgeber) Einblick in die Gesundheitsdaten der Arbeitnehmerin haben soll. Rein theoretisch wäre es ja denkbar, dass der Arbeitgeber aufgrund dessen das Arbeitsverhältnis kündigt, weil die Arbeitnehmerin z. B. an einer bestimmten Krankheit leidet. Es macht sowieso keinen Sinn, dass - mit Ausnahme der zu versichernden Person selbst - sonst jemand Einblick in deren Gesundheitsdaten erhält. Denn nur diese allein kann die Richtigkeit ihrer Gesundheitsangaben garantieren. Die Zusendung des medizinischen Fragebogens an den Arbeitgeber erfolgte somit widerrechtlich. Rechtfertigungsgründe lagen keine vor.
Die zuständige Versicherungsgesellschaft teilte schliesslich unsere Ansicht, wonach Gesundheitsdaten nicht an den Arbeitgeber weitergeleitet werden dürfen. Im weiteren überarbeitet sie die entsprechenden Anmeldeformulare in unserem Sinne.

5.6. Automatisches «Zusammenfügen» diverser Versicherungsdossiers im Rahmen eines Versicherungsabschlusses

Eine Anwältin beabsichtigte, bei einer Versicherung eine Berufshaftpflichtversicherung abzuschliessen. Dabei wollte der Versicherungsberater zwei bereits über sie existierende Dossiers - wovon eines einen Autounfall aus dem Jahre 1986 betraf - mit dem neuen Dossier zusammenfügen. Werden jedoch sämtliche bisherigen Versicherungsdossiers im Rahmen eines Versicherungsabschlusses automatisch zusammengelegt, kann dies leicht zu Verletzungen des Datenschutzgesetzes führen.

Eine Versicherungsgesellschaft beabsichtigte, eine seit kurzem als selbständig tätige Anwältin über die Möglichkeiten einer Berufshaftpflichtversicherung zu informieren. Anlässlich des ersten Beratungsgesprächs legte ihr der Versicherungsberater zwei Computerausdrücke vor, die sich auf zwei frühere Dossiers bezogen. Das eine Dossier betraf einen Autounfall aus dem Jahre 1986, bei welchem die Versicherung gegenüber ihr als Versicherer des schuldhaften Autofahrers auftrat. Das andere Dossier hingegen hatte die Berufshaftpflichtversicherung ihres ehemaligen Arbeitgebers

zum Inhalt, bei welchem sie ihr Anwaltspraktikum absolvierte. Beiläufig wurde die Anwältin noch in Kenntnis gesetzt, dass die Versicherungssumme ihres ehemaligen Arbeitgebers «nur» eine Million Franken betrage. Der Versicherungsberater beabsichtigte schliesslich, die beiden vorgenannten Dossiers mit dem neuen Dossier betreffend die Berufshaftpflichtversicherung zusammenzufügen.
Das automatische «Zusammenfügen» verschiedener Dossiers kann sehr schnell zu Verletzungen der datenschutzrechtlichen Grundsätze führen. So verstösst z. B. das Zusammenlegen des «Autounfalldossiers» mit dem neu zu eröffnenden «Berufshaftpflichtdossier» gegen das Verhältnismässigkeitsprinzip. Denn es ist für den Abschluss einer Berufshaftpflichtversicherung nicht erforderlich, dass die dort benötigten Angaben mit Daten - insbesondere Gesundheitsdaten - eines über 10 Jahre zurückliegenden Autounfalls in Verbindung gesetzt werden. Im übrigen ist es auch widerrechtlich, wenn die Versicherungssumme des ehemaligen Arbeitgebers - ohne dessen Einwilligung - an Dritte, sei es auch nur an eine frühere Arbeitnehmerin, bekanntgegeben wird. Immerhin kann es geschäftsschädigend sein, wenn Aussenstehende wie z. B. Klienten davon erfahren würden.
Zudem verlangten wir, die zu versichernde Person vorgängig und umfassend über den Inhalt der Datenbearbeitung zu informieren. Schliesslich ist eine möglichst klar umschriebene Einwilligung des zu Versichernden für das Zusammenlegen interner Versicherungsdossiers mit den Antragsunterlagen einzuholen (vgl. S. 34 Kapitel Merkblatt und Einwilligungsklausel).

5.7. ZIS (Zentrales Informationssystem)

ZIS ist eine Datensammlung der Versicherungswirtschaft über hängige und bereits abgeschlossene Straf- und Zivilverfahren. Hauptzweck von ZIS ist es, die Versicherungsgesellschaften vor betrügerischen Machenschaften zu schützen.

Die Datensammlung ZIS wurde beim EDSB angemeldet. Da sie besonders schützenswerte Personendaten enthält und wir von privater Seite darauf aufmerksam gemacht wurden, überprüften wir insbesondere die Legitimität von ZIS.
Die einzelnen Versicherungsgesellschaften melden dem Sekretariat des ZIS Versicherungsnehmer, Versicherte, Geschädigte, Lenker, Anspruchsteller, deren Hilfspersonen und andere Beteiligte, welche direkt oder indirekt an einem Versicherungsvertrag oder Schadenfall in Verbindung mit einem Delikt beteiligt waren. In Frage kommen u.a. die folgenden Straftatbestände: Veruntreuung, Hehlerei, Betrug, ungetreue Geschäftsführung sowie Urkundendelikte. Neben den vollendeten Delikten führen auch der Versuch, die Anstiftung sowie die Gehilfenschaft zum Eintrag. Sobald eine Versicherungsgesellschaft Kenntnis polizeilicher oder gerichtlicher Ermittlungsverfahren hat und ein dringender Tatverdacht besteht erstattet sie dem Sekretariat unverzüglich Meldung. Änderungen oder der Ausgang eines Straf- und/oder Zivilverfahrens werden dem Sekretariat ebenfalls unverzüglich angezeigt. Die Daten werden nicht EDV-mässig, bearbeitet, sondern auf Papierkarten erfasst. Das Sekretariat leitet periodisch aktualisierte Daten an die Versicherungsgesellschaften weiter.
Bei der Bearbeitung von Angaben über hängige oder abgeschlossene Straf- oder Zivilverfahren handelt es sich um besonders schützenswerte Personendaten. Für deren Bearbeitung und insbesondere deren Bekanntgabe an andere Gesellschaften (Dritte) ist ein Rechtfertigungsgrund erforderlich. Der Zweck von ZIS besteht darin, betrügerische Versicherungsansprüche zu erkennen und den Abschluss von Versicherungsverträgen mit betrügerischem Hintergrund zu verhindern. Im Interesse der

Versicherten sollen damit die Prämienrechnungen entlastet werden. Vor diesem Hintergrund muss eine Interessenabwägung zwischen der Bearbeitung der besonders schützenswerten Personendaten und den überwiegenden privaten Interessen der Gesellschaft beziehungsweise den überwiegenden öffentlichen Interessen vorgenommen werden.
Der Rechtfertigungsgrund des Bearbeitens von Personendaten in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags über den Vertragspartner kann vorliegend nicht herangezogen werden, da die Bekanntgabe an andere Gesellschaften durch das ZIS nicht mehr in einem unmittelbaren Zusammenhang steht. Ein überwiegendes privates Interesse ist somit zu verneinen.
Aufgrund der herrschenden Konjunkturlage ist die Tendenz, Versicherungsbetrug zu begehen steigend, was auch durch die Anzahl der im ZIS gemeldeten Fälle belegt wird (79 Meldungen 1992, 466 Meldungen 1996). In diesem Licht betrachtet, besteht ein ausgewiesenes Interesse der ehrlichen Versicherten, dass von den Versicherungen nicht unrechtmässige Beträge ausbezahlt werden müssen, welche eine Erhöhung der Prämien zur Folge hätten. Wir sind vorliegend zum Schluss gekommen, dass ein überwiegendes öffentliches Interesse der Versicherten die Bearbeitung dieser Personendaten rechtfertigt.
Ferner stellten wir fest, dass die Bearbeitung der Personendaten sich auf ein Reglement abstützt, dessen Anwendung von einer unabhängigen Aufsichtsstelle kontrolliert wird. Die monatliche Mitteilung der neuesten Änderungen (Gerichtsurteile) auf Papier gewährleistet ferner die Richtigkeit und Aktualität der Daten. Durch diese Vorkehrungen wird verhindert, dass der missbräuchlichen Verwendung besonders schützenswerter Daten Tür und Tor geöffnet wird (z.B. unkontrollierter Austausch unter den Gesellschaften). Der Entscheid, ob ein meldepflichtiger Fall vorliegt, liegt indes im Ermessen und der Verantwortung der einzelnen Gesellschaft.

6. Gesundheitswesen

6.1. Überprüfung der obligatorischen Krankenversicherung nach KVG

Die Kantone müssen nach dem neuen Krankenversicherungsgesetz für die Einhaltung der obligatorischen Versicherungspflicht sorgen. Soweit die Kantone von den Versicherten dafür eine Kopie des Versicherungsausweises verlangen, verstösst dies jedoch gegen die allgemeinen Datenschutzbestimmungen. In einem anderen Fall sollten die Krankenkassen mittels einer Informatikanwendung die entsprechenden Versicherungsangaben an die Kantone weiterleiten. Diese Vorgehensweise wurde ebenfalls als unrechtmässig eingestuft.

Kontrolle mittels eines Versicherungsausweises

Wir wurden mehrmals angefragt, ob die Kantone zur Überprüfung der Versicherungspflicht tatsächlich berechtigt seien, eine Kopie des Versicherungsausweises zu verlangen. Die Frage, inwiefern dies datenschutzrechtlich zulässig sei, fällt grundsätzlich in den Zuständigkeitsbereich der kantonalen Datenschutzbehörden. Dies soll uns jedoch nicht daran hindern, unsere Stellungnahme dazu abzugeben.
Aufgrund des neuen KVG müssen die Kantone für die Einhaltung der Versicherungspflicht sorgen. Nach welchem Verfahren dies konkret zu geschehen hat, wird den Kantonen bzw. den Gemeinden überlassen. Einige Gemeinden fordern deshalb

eine Kopie des Versicherungsausweises, der in der Regel nicht nur Angaben über die obligatorische Grundversicherung, sondern auch über Zusatzversicherungen, Vorbehalte etc. enthält. Dies ist unverhältnismässig und somit ein Verstoss gegen die allgemeinen datenschutzrechtlichen Grundsätze.
Unseres Erachtens genügt es, wenn die Kantone (oder die Gemeinden) ihre Einwohner mit einem Merkblatt über die Versicherungspflicht umfassend informieren. Zusätzlich kann noch der Hinweis angeführt werden, dass diejenigen Personen, die ihrer Versicherungspflicht nicht nachkommen, durch die zuständige kantonale Behörde automatisch einem Versicherer zugewiesen werden. Schliesslich kann noch auf die möglichen Straffolgen bei Zuwiderhandlungen aufmerksam gemacht werden. Eine mögliche Lösung wäre auch, dass die Kantone eine schriftliche Bestätigung der Versicherten verlangen würden.

Kontrolle über Datenbekanntgaben der Krankenkassen

Wir wurden von einer privaten Unternehmung angegangen, die kantonalen Behörden EDV-Dienstleistungen anbietet, welche die Überprüfung des Versicherungsobligatoriums nach KVG ermöglichen sollen. Gemäss dem uns vorgelegten Konzept sollten die Krankenkassen den kantonalen Behörden Daten über ihre im Kanton wohnhaften Versicherten liefern. In der Anfrage wurde uns mitgeteilt, dass für einen Kanton schon ein Dienstleistungsvertrag bestehe. Für diesen Kanton habe man sich «vertraglich dem Datenschutz unterstellt». Man fasse auch ins Auge, die Dienstleistung landesweit anzubieten.
Da die Krankenkassen im Bereich des Obligatoriums als Bundesorgane gelten, benötigen sie für jede Bekanntgabe von Personendaten eine Rechtsgrundlage. Ausnahmen von dieser Regel sind nur für Bekanntgaben im Einzelfall vorgesehen. Eine *gesetzliche Grundlage* für die fragliche Datenbekanntgabe ist weder im KVG noch in der Verordnung zum KVG zu finden, weshalb die Bekanntgabe in unrechtmässiger Art und Weise erfolgt.
Ein weiteres Problem ist in der mangelnden *Verhältnismässigkeit* der Datenbearbeitung zu erblicken. Schon vor Bestehen des KVG-Obligatoriums waren nämlich über 99% der Bevölkerung versichert. Es scheint daher *nicht angemessen*, eine derart grosse Menge von Daten betreffend die gesamte Bevölkerung bekanntzugeben, damit ein sehr kleiner Anteil dieser Bevölkerung seinem Obligatorium ebenfalls nachkommt. Sodann ist sowohl eine einmalige als auch eine periodische Bekanntgabe an die kantonalen Behörden *nicht geeignet*, das Obligatorium tatsächlich zu überprüfen. Denn solche Bekanntgaben erfolgen stets auf einen Stichtag, nach welchem neue Einwohner ins kontrollierte Gebiet zuziehen oder alte Einwohner wegziehen können. Der EDSB ist denn auch schon in Fällen angerufen worden, bei denen Personen von der Einwohnerkontrolle gemahnt wurden, obwohl sie schon weggezogen waren.
Eine vernünftiges Vorgehen bei der Obligatoriumskontrolle betrifft nur einmal die gesamte Bevölkerung des Kantons und beschränkt sich im folgenden auf die Kontrolle der Migrationen, welche direkt durch die Einwohnerkontrolle durchgeführt werden kann. In einem ersten Schritt können auf einen Stichtag die Bewohner eines Kantons - wie bereits oben schon erwähnt - mit einem Merkblatt auf ihre Versicherungspflicht und die Strafdrohung bei Missachtung hingewiesen werden. Ebenfalls denkbar ist es, von den Versicherten eine schriftliche Bestätigung für die Tatsache einzuholen, dass sie versichert sind. Nachdem die Verhältnisse für diesen Stichtag geklärt sind, genügt es schliesslich, von den Neuzuzügern einen Versicherungsnachweis zu verlangen. Das KVG verlangt nämlich, dass eine Person, die einmal versichert ist, auch

immer versichert bleibt. Denn gemäss Art. 7 Abs. 5 KVG endet das Versicherungsverhältnis zum alten Versicherer erst dann, wenn ein neuer Versicherer diesem mitteilt, «dass die betreffende Person bei ihm ohne Unterbrechung des Versicherungsschutzes versichert ist».
Diese Art der Obligatoriumskontrolle entspricht dem Verhältnismässigkeitsgrundsatz und ist wegen des geringeren Aufwandes auch kostengünstiger.

6.2. Medizinische Statistik der Krankenhäuser

Dieses Thema hat seit einigen Monaten zu Recht eine starke Medienpräsenz, weil die Zentralisierung auf diesem sensiblen Gebiet mit den geplanten Erhebungen neue Dimensionen annimmt. Es stellen sich insbesondere die Fragen der Verhältnismässigkeit und der Anonymisierung. Auf letzterem Gebiet sind in jüngster Zeit Fortschritte zu beobachten. Dennoch ist eine abschliessende Beurteilung im Moment nicht möglich.

Erst Ende 1996 wurde aufgrund von Beiträgen in den Medien der breiten Öffentlichkeit bewusst, welches Ausmass an Konzentration sensibler Daten die geplante medizinische Statistik der Krankenhäuser anstrebt. Die Medienberichte gehen wohl teilweise auch auf Resolutionen zurück, welche dieses Jahr von der Verbindung der Schweizer Ärzte (FMH) zu den medizinischen Statistiken des Bundes und von der nationalen Datenschutzkonferenz zu Datenbearbeitungen im Gesundheitswesen im allgemeinen verabschiedet wurden. Ebenfalls Ende 1996 wurde der EDSB von kantonalen Datenschutzaufsichtsstellen angefragt, zu den Fragen der gesetzlichen Grundlage und der Anonymisierung Stellung zu nehmen.
Die Frage der gesetzlichen Grundlage stellt sich im Bereich der Statistik auf besondere Weise. Erfolgt nämlich eine Datenbearbeitung zu rein statistischen Zwecken, so sind die Anforderungen an die gesetzlichen Grundlagen gelockert. Dies hat seine Berechtigung darin, dass diese Datenbearbeitungen ausschliesslich zu nicht personenbezogenen Zwecken erfolgen. Bei der Bearbeitung von sensiblen Daten ist jedoch dem *Grundsatz der Verhältnismässigkeit* bei der Datenbearbeitung besondere Beachtung zu schenken. Dieser Grundsatz stellt gewisse Anforderungen an das Verhältnis zwischen staatlichem Handeln und den durch dieses Handeln verfolgten Zielen. Bevor geprüft werden kann, ob diese Anforderungen erfüllt sind, müssen daher die Ziele des staatlichen Handelns möglichst genau definiert werden. Dabei ist auch zu prüfen, ob die gesetzten Ziele nicht schon auf anderem Weg verfolgt werden oder besser auf anderem Wege verfolgt würden. Insbesondere das Verhältnis zu Bewilligungen nach
Art. 321bis StGB für Forschung im Bereich der Medizin oder des Gesundheitswesens ist hierbei von Interesse.
Erst in zweiter Linie stellt sich das Problem der *Anonymisierung*. Dieses wird dann aktuell, wenn sich aus den zu verfolgenden Zielen ergibt, dass Merkmale erhoben werden müssen, woraus Rückschlüsse auf die Identität betroffener Personen möglich sind. Sodann ist das Problem der Anonymisierung in zwei Teilaspekte aufzuspalten. Zunächst geht es um den «Verbindungscode», welcher erlauben soll, sog. Mehrfachhospitalisationen zu erfassen. Dieser Code soll zwar aus identifizierenden Merkmalen eines jeden Patienten hergestellt werden. Der Code selbst darf jedoch keine Rückschlüsse auf den Patienten erlauben. In bezug auf die Herstellung dieses Codes sind gegenüber dem provisorischen Detailkonzept vom April 1997 Verbesserungen zu verzeichnen. Eine Beurteilung des betreffenden Verfahrens ist im Moment nicht möglich, da wir über wesentliche Details noch zuwenig Informationen besitzen.

Insbesondere ist uns noch unbekannt, welche Verfahren (sc.l. welche Hashfunktion) und welche Informationen zur Herstellung des Codes verwendet werden. Der zweite Teilaspekt der Anonymisierung betrifft die Gesamtheit aller erhobenen Merkmale, weil durch Kombination mehrerer Merkmale (beispielsweise genaues Geburtsdatum und Postleitzahl des Wohnortes) betroffene Personen identifiziert werden können, auch wenn jedes dieser Merkmale für sich allein dazu nicht genügend wäre. Solche Möglichkeiten müssen durch sog. Generalisierung (z.B. Geburtsjahr statt Geburtsdatum, Wohnregion statt Wohnort) vermieden werden, wo immer dies machbar ist, ohne die Ziele der Statistik zu vereiteln. Auch hierin ist ein Verweis auf den Grundsatz der Verhältnismässigkeit zu erblicken.

6.3. Ausserkantonale Hospitalisation - Bekanntgabe von medizinischen Daten an kantonale Kostengutsprachestellen

Der EDSB ist zur Beurteilung der Frage nach der Zulässigkeit dieser Datenbekanntgaben nicht zuständig. Weil die Angelegenheit die gesamte Schweiz betrifft, hat er sich nach Diskussionen mit der Arbeitsgruppe kantonaler Datenschutzaufsichtsstellen dennoch dazu geäussert. Wenn auch das Interesse der kantonalen Kostengutsprachestellen an der Datenbekanntgaben gegeben ist, so fehlt dazu dennoch die gesetzliche Grundlage.

Die vorliegende Problematik entspringt der Regelung, wonach ein kantonales Spital für ausserhalb des Kantons wohnhafte Patienten einen höheren Tarif in Rechnung stellen darf als für Kantonseinwohner. Nach Art. 41 Abs. 3 KVG hat in solchen Fällen der Wohnsitzkanton dieser Patienten die Differenz zwischen den in Rechnung gestellten Kosten und den Tarifen des Spitals für Einwohner des Kantons zu übernehmen, wenn die Behandlung *aus medizinischen Gründen* im anderen Kanton geschah. Medizinische Gründe liegen dabei vor in Notfällen, sowie bei denjenigen Behandlungen, welche weder im Kanton selbst noch in einem Spital der Spitalliste dieses Kantons angeboten werden. Entsprechend dem Wunsch des Wohnsitzkantons, diese Differenz nicht zu bezahlen, besteht dessen Interesse, das Vorliegen medizinischer Gründe zu verneinen. Dies wiederum veranlasst den Kanton, sich entsprechenden Informationen zu beschaffen.
Da die fraglichen Datenbekanntgaben von kantonalen Institutionen (Spitäler) an kantonale Kostengutsprachestellen erfolgen, konnte sich der EDSB zur Beurteilung der Frage nicht zuständigerweise äussern. Immerhin betrifft die Angelegenheit die gesamte Schweiz und der EDSB wurde von der Sanitätsdirektorenkonferenz sowie von verschiedenen Spitälern dazu angefragt. Nachdem mit der Arbeitsgruppe kantonaler Datenschutzaufsichtsstellen über die Angelegenheit diskutiert wurde, haben wir uns zur Frage geäussert, ob die Datenbekanntgaben gemäss KVG erlaubt seien.
Im KVG selbst findet sich keine ausdrückliche Ermächtigung an die Kantone, sich solche Informationen zu beschaffen. Auch eine entsprechende Verpflichtung der Spitäler ist weder im KVG noch in der dazugehörigen Verordnung enthalten. Es stellte sich daher die Frage, ob ein Kanton selbst solche Bestimmungen erlassen dürfe. Der tiefere Sinn der Regelung im KVG besteht darin, die Kantone zu koordinierter Planung und Nutzung von Spitalressourcen zu bewegen statt beim komplizierten Gutspracheverfahren Energien zu verwenden. Daraus wird klar, dass das KVG keine Grundlage für die Datenbekanntgaben an kantonale Kostengutsprachestellen liefern will. In zeitlicher Hinsicht verhält es sich aber so, dass gesamtschweizerisch flächendeckende Spitalabkommen, welche die Kostengutspracheverfahren überflüssig ma-

chen würden, nicht in einer kurzen Frist machbar sind. Den beteiligten Stellen wurden denn auch keine direkten Empfehlungen abgeben. Wir haben uns auf praktische Hinweise zur Verbesserung des Datenschutzes trotz Datenbekanntgaben beschränkt. Dabei wurde insbesondere betont, dass medizinische Informationen nicht einfach an Mitarbeiter einer Verwaltungsstelle gehen sollten. Vielmehr soll der Umgang mit diesen Daten denjenigen Personen vorbehalten bleiben, welche selbst Mediziner oder deren Hilfspersonen sind und daher den Umgang mit derartigen Informationen gewohnt sind.

6.4. Auskunftsberechtigung des Bundesamtes für Sozialversicherung gegenüber kantonalen Behörden (Kassenaufsicht)

Einige Kantone haben Zweifel, ob die durch das Bundesamt für Sozialversicherung (BSV) genehmigte Erhöhung der Krankenkassenprämien in ihren Gebieten berechtigt sei. Sie wollen deshalb im Genehmigungsverfahren des BSV mitwirken und verlangen vom BSV Einsicht in die entsprechenden Geschäftsunterlagen der Krankenkassen (Jahresbudgets betreffend die jeweiligen Kantonsgebiete). Für die Weitergabe dieser Daten durch das BSV an die Kantone fehlt jedoch - unseres Erachtens - die notwendige gesetzliche Grundlage im Krankenversicherungsgesetz (KVG).

Das Bundesamt für Sozialversicherung bat das Bundesamt für Justiz (BJ) abzuklären, ob und unter welchen Voraussetzungen die Weitergabe der erwähnten Geschäftsunterlagen durch das BSV an die Kantone in datenschutzrechtlicher Sicht zulässig sei. Das BJ kam zum Schluss, dass dafür eine gesetzliche Grundlage erforderlich sei. Das geltende Krankenversicherungsgesetz (KVG) biete jedoch eine hinreichende Grundlage, damit die Datenweitergabe sogar auf Verordnungsstufe geregelt werden könne. Schliesslich ersuchte uns das BJ noch um unsere Meinung.
Für die Weitergabe von Jahresbudgets durch das BSV an die Kantone ist gemäss Datenschutzgesetz grundsätzlich eine gesetzliche Grundlage erforderlich. Im Gegensatz zum BJ sind wir jedoch der Ansicht, dass das KVG keine Bestimmung enthält, welche die Datenweitergabe durch das BSV auf Verordnungsstufe erlauben würde. Wir verlangen, dass im KVG mindestens eine Norm darauf hinweist, die den Zweck, den Gegenstand sowie den Umfang der Delegation an das BSV möglichst klar umschreibt (Delegationsnorm). Eine solche Delegationsnorm fehlt unserer Meinung nach im KVG.
Es stellt sich zudem die Frage, ob nicht sogar eine abschliessende und umfassende Regelung im KVG zu fordern sei. Das Zusammenspiel zwischen dem BSV und den Kantonen kann einen starken Eingriff in die Rechtssphäre der Krankenkassen bedeuten. Denn die an die Kantone weitergeleiteten Daten werden von diesen mit den jeweiligen kantonalen Gesundheitskosten verglichen. Die Kantone geben ihre Beobachtungen dem BSV weiter, welches - u. a. gestützt darauf - dann die Prämientarife genehmigt oder nicht. Es besteht jedoch die Gefahr, dass die Kantone die Höhe der jährlichen Gesundheitskosten nicht korrekt wiedergeben bzw. wiedergeben können und somit die falschen Schlüsse ziehen. Die Krankenkassen würden dann fälschlicherweise der unerlaubten Quersubventionen bezichtigt. Zudem ist davon auszugehen, dass es den Kantonen im Rahmen des Genehmigungsverfahrens an der nötigen Objektivität und Neutralität mangeln könnte. Viele Kantone weisen z. B. sehr hohe Kosten bei der Spitalversorgung auf und sind deshalb zu einem gewissen Grad auch verantwortlich für die sehr hohen Prämienaufschläge. Eine Mitwirkung bzw. «Mitaufsicht» der Kantone bei der Prämiengestaltung bedarf somit mindestens einer klaren Delegationsnorm im KVG. Die Aufsicht über die Krankenkassen - dazu gehört

auch die Genehmigung der Prämientarife - obliegt sowieso dem Bundesrat bzw. dem BSV und nicht den Kantonen.
Ob und inwiefern die Weitergabe der Versicherungsdaten durch das BSV an die Kantone datenschutzrechtlich zulässig sei, ist eine Frage, welche nicht nur auf juristischer Ebene entschieden wird, sondern auch auf der politischen.
Mitte Februar 1997 fand schliesslich ein «Krankenversicherungs-Gipfel» mit allen Beteiligten statt. Es wurde dort beschlossen, die Kantone in die Prämienkontrolle einzubeziehen. Tatsächlich soll dies mit einer Verordnungsänderung geschehen, die bereits für die Prämienrunde 1998 Gültigkeit haben soll.

6.5. Verkauf einer Zahnarztpraxis (Goodwill)

Der Übernehmer einer Zahnarztpraxis darf nicht in die medizinischen Unterlagen eines Patienten Einsicht nehmen, solange der betreffende Patient dies nicht erlaubt. Auch kann der Übergeber der Praxis im Kaufvertrag keine solche Einsichtnahme versprechen.

Im Rahmen der Abwicklung eines Kaufvertrages wurde der EDSB angefragt, inwieweit der Käufer einer Zahnarztpraxis Einblick in die Patientenunterlagen nehmen dürfe. Grundsätzlich ist davon auszugehen, dass nur der Patient über die ihn betreffenden Informationen zu bestimmen hat. Dementsprechend liegt es auch an ihm, darüber zu verfügen. Die Einsicht in die blosse Adresskartei ist aber Voraussetzung dafür, dass der Käufer den Patientenstamm über seine Praxiseröffnung informieren kann, wenn dies nicht schon durch den Verkäufer geschehen ist. Die Einsicht in die Adresskartei einer Zahnarztpraxis wurde als unter dem Gesichtspunkt des Arztgeheimnisses unbedenklich bezeichnet. (In heikleren Bereichen, wie z.B. Psychiatrie, Onkologie oder Urologie wäre dies allenfalls anders zu beurteilen.) Eine Einsicht in die medizinischen Unterlagen kann der Verkäufer im Kaufvertrag nicht gültig versprechen. Denn er ist als Geheimnis*träger* jedem Patienten gegenüber verpflichtet, diese Informationen für sich zu behalten. Nur der einzelne Patient kann als Geheimnis*herr* die Weitergabe an Dritte erlauben. Er kann dies sowohl ausdrücklich als auch durch konkludentes Handeln tun, indem er zu erkennen gibt, dass er sich durch den Übernehmer der Praxis behandeln lassen will.

6.6. Medizinischer Fragebogen und die Einwilligung des Patienten für das Inkasso

Wenn ein Arzt von seinen Patienten eine Einwilligung für die Bekanntgabe ihrer Daten zu Inkasso- oder Buchhaltungszwecken einholt, muss dies auf einem separaten Blatt, getrennt von medizinischen Fragen, erfolgen. Aus der Einwilligungserklärung für Buchhaltungszwecke sollte ersichtlich sein, welche Daten zu welchen Zwecken an wen weitergegeben werden.

Eine Privatperson wurde gebeten, bei ihrem Arzt auf dem gleichen Blatt neben medizinischen Fragen eine Patientenerklärung zu unterschreiben. Mit der Patientenerklärung wurde u.a. die Einwilligung in die Weitergabe ihrer Daten für die Rechnungsstellung, Inkasso und Buchführung eingeholt. Die betroffene Person störte sich daran, dass sie nicht nur die Einwilligung zur Weitergabe ihrer allgemeinen Rechnungsdaten, sondern auch ihrer Gesundheitsdaten geben musste.
Es ist vorliegend grundsätzlich eine Unterscheidung zwischen den verschiedenen Personendaten (Rechnungstellung und Gesundheitsdaten) vorzunehmen. Es dürfen

nur diejenigen Personendaten beschafft werden, die sowohl nötig als auch geeignet sind, um einen bestimmten Zweck zu erreichen (Verhältnismässigkeitsprinzip). Die erhobenen medizinischen Fragen dringen weit in den persönlichen Bereich des Patienten ein, scheinen uns jedoch geeignet, die Qualität der ärztlichen Behandlung zu fördern. Der Patient hat in jedem Fall jedoch das Recht, bestimmte Fragen nicht zu beantworten.
Die Einwilligungsklausel muss eindeutig und klar sein. Wer in die Datenbearbeitung einwilligt, muss dies nicht bloss freiwillig, sondern auch und in Kenntnis aller Umstände über die ganze Bearbeitung tun. Vorliegend müssten dem Patient die Empfänger seiner Daten (Inkassobüros, Buchhaltungsfirma, weitere hierfür beauftragte Personen und Institutionen) namentlich bekannt sein. Die Nennung dieser Angaben sollte keine Probleme bieten, da der Arzt die Datenempfänger kennt.
Schliesslich präzisierte der Arzt in diesem Sinne die Patientenerklärung. Aufgrund der pauschalen Formulierung und somit mangelhaften Transparenz hätte ansonsten die Patientenerklärung als ungültig betrachtet werden müssen.

7. Kreditwesen

7.1. Die Führung von Kreditprüfsystemen

Informationen über die Kreditwürdigkeit dürfen nicht mit einem Branchen-Indexverzeichnis verknüpft werden, damit sämtliche Personen on-line abgefragt werden können. Ein Kreditprüfsystem ist technisch so zu gestalten, dass Abfragen nur einzelfallweise möglich sind. Die Eingabe des Namens und/oder der Adresse sollten genügen, um die gewünschten Angaben zu erhalten. Ein Versand von Grobübersichten schlechter Zahler ist ebenfalls nicht erlaubt.

Aufgrund der Empfehlung des EDSB vom 24. Oktober 1994 dürfen Kreditauskünfte nur auf Anfrage und einzelfallweise erfolgen. Pauschale, listenmässige Übermittlungen von Kreditwürdigkeitsinformationen oder Beantwortungen von allgemeinen, nicht anlassgebundenen Anfragen werden damit ausgeschlossen (BBl 1988 II 461).
Im Anschluss an die Empfehlung des Eidgenössischen Datenschutzbeauftragten richtete ein Verband ein EDV-Debitoren-System mit einem Reglement für interessierte Verbandsmitglieder ein. Damit sollte den Mitgliedern die einzelfallweise Abfrage von Kreditwürdigkeitsinformationen über ihre Kunden ermöglicht werden. Die Suchkriterien wurden EDV-mässig nicht optimal ausgestaltet. Wegen der schwerfällig gestalteten EDV-Abfrage konnten sich die Mitglieder nicht einwandfrei über allenfalls nicht solvente oder säumige Kunden informieren. Daher beabsichtigte der Verband, seine Mitglieder durch den Versand einer Grobübersicht von schlechten Zahlern und die Abfrage via Indexverzeichnis zu informieren.
Wir sprachen uns jedoch bereits in der erwähnten Empfehlung gegen das Versenden von Kreditwarnlisten aus. Wenn sämtliche Verbandsmitglieder Listen über Kunden in schwierigen finanziellen Verhältnissen erhalten, die zum Teil gar nicht benötigt werden, wird der Grundsatz der Verhältnismässigkeit verletzt. Ein Rechtfertigungsgrund, der diese Bearbeitung legitimieren würde, kann nicht geltend gemacht werden. Eine derartige Bearbeitung von Personendaten ist somit als ungerechtfertigt zu qualifizieren.
Ferner wurde vorgeschlagen, den Mitgliedern ein Branchenverzeichnis auf CD-Rom zur Verfügung zu stellen, womit sämtliche Kunden (ca. 2'300 Personen) mit Namen

und Adresse abgerufen werden könnten. Das Branchenverzeichnis wäre mit Angaben, welche die Mitglieder einer Zentrale liefern würden, verknüpft worden (reglementarische Verpflichtung der Mitglieder). Nur Mitglieder könnten einen Anschluss an das System erwerben, um gegen Entgelt die Zahlungsfähigkeit potentieller Kunden zu prüfen. Die Mitglieder hätten sich vertraglich dazu verpflichten müssen, ausschliesslich diejenigen Kunden abzurufen, die für einen allfälligen Vertragsabschluss in Frage gekommen wären.
Wir sind der Ansicht, dass beim Zugänglichmachen von Kreditinformationen nicht jedes Verbandsmitglied mit allen im Indexverzeichnis aufgeführten Personen einen Vertrag abschliessen will und deshalb nicht auf den Zugang (insbesondere Online) der Kreditinformationen sämtlicher möglicher Kunden angewiesen ist. Das Risiko, dass Unbefugte in Kreditinformationen des Indexverzeichnisses Einsicht nehmen, ist unseres Erachtens sehr hoch und kann vertraglich nicht hinreichend geregelt werden (Beweisfragen bei Missbrauch). Aufgrund dessen haben wir verlangt, die einzelfallweise Einsichtnahme der Kreditwürdigkeitsinformationen müsse mittels geeigneter, technischer Massnahmen bewerkstelligt werden. Jedes Mitglied sollte die Möglichkeit haben, mittels Eingabe des Kundennamens und/oder der Adresse und/oder Mehrwertsteuer-Nummer die gewünschte Information im Einzelfall abrufen zu können. Bei verschiedenen Firmennamen sowie bei grösseren Unternehmungen sollte eine einmalige Anfrage genügen, um sämtliche Informationen über eine Unternehmung mit verschiedenen Firmennamen oder Niederlassungen abfragen zu können.
Im heutigen Zeitpunkt wurde sowohl auf die Realisierung eines revidierten EDV-Systems als auch auf das Versenden einer Grobübersicht der schlechten Zahler verzichtet.

7.2. Neuausstellung der Kreditkarte und digitalisierte Unterschrift

Die Digitalisierung von Unterschriften soll einerseits die Authentizität der betreffenden Personen sicherstellen. Andererseits dient sie dem Schutz vor Fälschungen. Wer bestehende Unterschriften digitalisieren will, muss zuvor jedoch die Kunden informieren und deren Einwilligung einholen. Sofern weitere Änderungen damit verbunden sind, wie die Aufbewahrung der Daten oder Änderungen der Allgemeinen Geschäftsbedingungen, müssen die Kunden ebenfalls vorher darüber orientiert werden.

Eine private Person erkundigte sich, ob ihre Bank die Kreditkarte erneuern und die Unterschrift digitalisieren dürfe, ohne sie vorher darüber zu informieren oder ihre Einwilligung einzuholen.
Die Unterschrift ist eine Angabe, die sich auf eine bestimmte Person bezieht, weshalb deren Bearbeitung vom DSG erfasst wird. Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Die Digitalisierung der Unterschrift des Kunden stellte vorliegend eine weitergehende Datenbearbeitung dar, als im Kartenantrag und den Allgemeinen Geschäftsbedingungen vereinbart worden war. Die betroffenen Personen hätten deshalb vorher über allfällige Änderungen informiert werden müssen, um in die Digitalisierung der Unterschrift einzuwilligen. Das Vorgehen der Bank hatte daher nicht den allgemeinen Grundsätzen des DSG entsprochen. Ferner bleibt zu untersuchen, ob diese Massnahmen vom technischen Standpunkt aus für die angestrebten Sicherheitsvorkehrungen notwendig und geeignet sind.
Unabhängig von der Notwendigkeit und Zweckmässigkeit der Vorkehrung zur Sicherstellung der Authentizität der Unterschrift eines Kunden ist die Art und Weise

des Vorgehens nicht datenschutzkonform, weil sie ohne jegliche Information an die Kunden erfolgte. Die Betroffenen müssen auch über die Art und Weise der Aufbewahrung informiert werden.

7.3. Breite Bekanntgabe von ZEK-Daten an die Fremdenpolizei

Die Zentralstelle für Kreditinformation (ZEK) wurde wiederholt um Auskunfterteilung an die Fremdenpolizeibehörden ersucht. Es stellte sich die Frage, unter welchen Voraussetzungen die ZEK Auskunft erteilen darf.

Bei der Regelung der Anwesenheit von Ausländern sind die Fremdenpolizeibehörden gehalten, auch die finanziellen Verhältnisse eines Gesuchstellers angemessen zu berücksichtigen. Weil sich viele Ausländer mit vorgedruckten Formularen an die ZEK wandten, stellte sich u.a. die Frage, ob eine breite Erhebung bei der als privater Verein konstituierten ZEK kraft Ausländer- und Datenschutzrecht zulässig sei. In einem Gutachten kamen wir zum Schluss, dass breite Erhebungen unter Mitwirkung der ZEK unzulässig sind. Die Frage, ob die ZEK in begründeten Einzelfällen den Behörden Auskünfte erteilen darf, wurde uns nicht unterbreitet. Nach unserer Auffassung sollte dies möglich sein, wenn die Daten für den Empfänger im Einzelfall zur Erfüllung seiner gesetzlichen Aufgabe unentbehrlich sind und er glaubhaft macht, dass ihm die betroffene Person die Angaben rechtsmissbräuchlich verweigert. Vorbehalten bleiben überwiegende schutzwürdige Interessen und gesetzliche Geheimhaltungspflichten.

8. Direktmarketing

8.1. Datenbearbeitung zu Werbezwecken: Nichtbeachtung der Adress-Sperre

Siehe dazu Kontrollbericht auf Seite 45

Der EDSB hat ein Merkblatt für die Adress-Sperrungen erarbeitet, welches im Anhang auf S. 90 zu finden ist.

9. Statistik

9.1. Volkszählung 2000- Die Revision des Volkszählungsgesetzes

Die Geschäftsprüfungskommission des Nationalrates (vgl. unseren 3. Tätigkeitsbericht S. 57) beauftragte den Bundesrat, neue Lösungen für die künftige Ausgestaltung der Volkszählung zu suchen. Das Bundesamt für Statistik hat Vorschläge für die Neuausrichtung und Vereinfachung der Volkszählung vorbereitet. Im Rahmen der durchgeführten Ämterkonsultation nahmen wir zu den vorgeschlagenen Änderungen Stellung und haben uns zur beabsichtigten Verwendung der Volkszählungsdaten für die Nachführung von Verwaltungsregistern kritisch geäussert.

Damit die zukünftigen Volkszählungen mittels Registern durchgeführt werden können, müssen die Grundlagen für die Harmonisierung der Gemeinderegister geschaf-

fen werden. In diesem Sinne schlägt das BFS vor, die Personendaten, die bei der Volkszählung erhoben werden, für die Nachführung und Korrektur die Verwaltungsregister der Kantone und Gemeinden zu verwenden. Dies bedeutet, dass die Personendaten, die im Rahmen der Volkszählung erhoben und bis anhin nur für statistische Zwecke verwendet werden durften, in Zukunft auch für Verwaltungszwecke genutzt werden dürfen.

Mit der beabsichtigten Revision des Bundesgesetzes über die Volkszählung (VZG) würde das erst seit 1990 eingeführte Verbot der Verwendung von Volkszählungsdaten für personenbezogene Zwecke aufgehoben. Schon im Vorfeld der Volkszählung 1990 gab es Widerstände bei der Einführung der Datenschutzbestimmungen. Der Bundesrat sah damals jedoch die strenge Zweckbindung der erhobenen Daten als einzige Möglichkeit, um die Verwendung der Volkszählungsdaten wirksam begrenzen und kontrollieren zu können. Denn das zentrale Merkmal der statistischen Erhebungen ist die strikte Trennung zwischen statistischen Zwecken und administrativen Zielen. Das bedeutet, dass der Bürger von den Angaben, die er im Rahmen einer statistischen Erhebung macht, keinerlei Konsequenzen zu befürchten hat.

Mit der beabsichtigten Revision wird jedoch mit dem fundamentalen Prinzip der Statistik (Zweckbindungsgebot) gebrochen. Von der grundsätzlichen Trennung zwischen statistischen Aufgaben und administrativen Zielen wird definitiv Abschied genommen, und das vielgepriesene Statistikgeheimnis wird relativiert.

Wenn das Statistikgeheimnis aufgehoben wird und die Volkszählungsdaten für Verwaltungszwecke verwendet werden, besteht die Gefahr, dass der Bürger sein Vertrauen in die Statistik verliert und möglicherweise unvollständige oder falsche Angaben macht. Somit werden einerseits Qualität und Zuverlässigkeit der Volkszählungsdaten leiden und die Aufgaben der amtlichen Statistik erschwert, durch die Volkszählung möglichst präzise Personendaten zu erhalten. Andererseits besteht durch der Relativierung des Persönlichkeitsschutzes die Gefahr, dass die aus der Volkszählung gewonnenen Daten zum Nachteil der betroffenen Personen verwendet werden. Durch die Nachführung der Gemeinderegister könnten beispielsweise Anmeldeversäumnisse geahndet werden. Viel grösser ist jedoch die Bedrohung, dass die mit Volkszählungsdaten nachgeführten Einwohnerregister als Hilfsinstrument für viele andere Verwaltungsregister dienen. Die betroffenen Personen sind somit nicht in der Lage herauszufinden, welche Dienststelle die Daten weitergegeben hat beziehungsweise durch welche Daten oder durch welche Quelle ihnen der Nachteil erwachsen ist.

Wir haben die kostengünstige registergestützte Erhebung sowie auch die Harmonisierung der Gemeinderegister begrüsst. Letztere ist Voraussetzung, damit überhaupt eine Registerzählung stattfinden kann. Dies soll jedoch nicht zum Nachteil der betroffenen Personen geschehen, beziehungsweise sollen Verwaltungsregister nicht mit statistischen Daten nachgeführt werden.

Langfristig müssen die Volkszählungen registergestützt durchgeführt werden. Und wie die GPK in ihrem Bericht an den Bundesrat erwähnte, muss die Erstellung und Harmonisierung der kantonalen und kommunalen Register unterstützt werden. Dafür müssen zunächst die notwendigen Rechtsgrundlagen geschaffen werden. Die Kantone können anschliessend die Harmonisierung oder Erstellung von Verwaltungsregistern vorantreiben, welche auch für die Statistik notwendige Merkmale einbeziehen sollen. Diese administrativen Register würden in der Zukunft auch für die indirekte Erhebung der Volkszählungsdaten beigezogen werden, ohne dass es einen Rück-

VZ-Personencode

fluss von statistischen Daten beim «Abgleichprozess» in die Verwaltungsregister gibt (Rückflussverbot). Denn bei der Volkszählung liegt die Gefahr weniger in der Erhebung der Daten als in ihrer Nachführung und Kombination.
Auch andere europäische Länder, welche Registervolkszählungen durchführen, lassen aus unterschiedlichen Registern Daten zusammenfliessen. Der Rückfluss der Ergebnisse (Korrektur und Nachführung) der Zählung ist jedoch nicht erlaubt. Somit wird die Volkszählung durchgeführt, ohne dass das Statistikgeheimnis oder der Schutz der Persönlichkeit tangiert wird.

Ob bei der vorgesehenen Revision des Volkszählungsgesetzes die Übernahme von Volkszählungsdaten in die Einwohnerregister oder der effektive Schutz des Einzelnen gegenüber Verwaltungshandeln vorgeht, stellt einen politischen Entscheid dar und muss anhand einer Interessenabwägung beurteilt werden. Ein solcher Entscheid darf sich jedoch nicht nur von Überlegungen der Wirtschaftlichkeit und Effizienz leiten lassen. Deshalb muss bei der Änderung des Verwendungszweckes - nebst Kosten und Effizienz - auch der Schutz der Persönlichkeit berücksichtigt werden.
Einer Revision des Volkszählunggesetzes, welche das Statistikgeheimnis und den Persönlichkeitsschutz relativiert, können wir nicht zustimmen. Falls jedoch eine solche Änderung des VZG beschlossen wird, müssen die Rechte der Betroffenen und die Anforderungen des Persönlichkeitsschutzes gewährleistet werden.
Deshalb müssen mindestens folgende Voraussetzungen erfüllt werden:

- Unmissverständliche Information der Öffentlichkeit, dass die erhobenen Daten nebst der Volkszählung auch für die Nachführung von Verwaltungsregistern verwendet werden.
- Die Änderung des Verwendungszwecks muss im Volkszählungsgesetz klar und deutlich formuliert werden. Es muss klar definiert werden, welche Daten für die Nachführung der Register verwendet werden und in welchen Registern diese nachgeführt werden.
- Der Zeitraum, innerhalb dessen die Nachführung der Register erfolgt, muss zeitlich beschränkt werden (max. 6 Monate).
- Auf dem Erhebungsformular muss klar erkennbar sein, welche Personendaten auch für Verwaltungszwecke verwendet werden.
- Den Betroffenen dürfen keine Nachteile aufgrund von Angaben auf den Fragebögen erwachsen (Statuierung eines Nachteilsverbots). Wenn die Beantwortung des Fragebogens unter Androhung einer Strafe obligatorisch ist, dann soll der Betroffene keine Nachteile erfahren, nur weil er den Fragebogen korrekt ausgefüllt hat.

9.2. Unterschiede zwischen Datenbearbeitungen zu Statistik- und zu Verwaltungszwecken

Für die betroffene Person ist es ein wesentlicher Unterschied, ob ihre Daten zu rein statistischen Zwecken bearbeitet werden, oder ob sie aufgrund einer Datenbearbeitung mit konkreten Massnahmen rechnen muss. Daher sind für den letzteren Fall insbesondere die Anforderungen an gesetzliche Grundlagen strenger. Es ist zulässig, Verwaltungsdaten zu statistischen Zwecken auszuwerten, nicht aber umgekehrt.

Die in Art. 22 DSG aufgestellten Regeln beziehen sich auf alle Datenbearbeitungen *für nicht personenbezogene Zwecke*, wozu als Beispiele Forschung, Planung und Statistik genannt werden. Das Wesen statistischer Datenbearbeitungen liegt aus da-

tenschutzrechtlicher Sicht eben im Fehlen ihres Bezuges zu bestimmten Personen. Das Gegenstück dazu sind sog. personenbezogene Zwecke der Datenbearbeitungen, welche immer dann vorliegen, wenn die Datenbearbeitung in individuelle Massnahmen oder Entscheide gegenüber den Betroffenen münden kann. Aufgrund von Bearbeitungen zu nicht personenbezogenen Zwecken brauchen die Betroffenen jedoch keine konkreten Eingriffe in ihre Privatsphäre zu befürchten. Aus diesem Grund wird für nicht personenbezogene Bearbeitungen besonders schützenswerter Personendaten vom Erfordernis der ausdrücklichen Grundlage in einem formellen Gesetz abgesehen. Demselben Grundgedanken entspricht, dass Verwaltungsdaten zu statistischen Zwecken ausgewertet werden dürfen, die personenbezogene Verwendung von zu statistischen Zwecken erhobenen Daten jedoch grundsätzlich untersagt ist.
Dagegen sind im Rahmen statistischer Datenbearbeitungen bestimmte Regeln einzuhalten. Erstens dürfen die Bearbeitungen zu keinen anderen als statistischen Zwecken erfolgen, insbesondere natürlich nicht zu personenbezogenen Zwecken. Zweitens müssen die Daten anonymisiert werden, sobald es der Zweck des Bearbeitens erlaubt. Dies wiederum erfordert eine möglichst genaue Formulierung des statistischen Zwecks. Und drittens hat die Publikation von Ergebnissen in einer Form zu erfolgen, welche keinen Rückschluss auf die betroffenen Personen erlaubt.
Als konkretes Beispiel zu den unterschiedlichen Bearbeitungszwecken weisen wir auf die sog. Administrativdatenstatistik der Krankenversicherung hin. In diesem Bereich ist aufgrund der bestehenden gesetzlichen Regelung die Abgrenzung zwischen Bearbeitungen zu statistischen und zu personenbezogenen Zwecken kaum möglich. Auch aus der Dokumentation zu den geplanten Datenbearbeitungen lässt sich diesbezüglich wenig schliessen. Die unter dem Titel «Aufsicht und Statistik» stehenden Art. 21 - 23 KVG enthalten Regelungen zu beiden Arten von Datenbearbeitungen. Unter datenschutzrechtlichen Gesichtspunkten ist dies aufgrund der unterschiedlichen Anforderungen an Regelungsstufe und Detailliertheit problematisch. Die in Art. 28 - 32 der KVV formulierten Konkretisierungen der Datenbearbeitungen haben eine ausdrückliche Grundlage im KVG selbst nur insoweit, als sie effektiv statistische Datenbearbeitungen betreffen (Art. 23 KVG). Sollen sie auch darüber hinaus gültig sein, so besteht die datenschutzrechtlich saubere Lösung darin, die Ermächtigungsnorm im KVG zu erweitern. Angesichts des Kostendrucks im Gesundheitswesen sowie der Tatsache, dass eine Gesetzesrevision lange dauern kann, mag als Alternative vorläufig eine möglichst klare Formulierung der verschiedenen Verwendungszwecke genügen. Dadurch kann ein Mass an Transparenz und Klarheit erreicht werden, welches die Versicherer zur Überzeugung kommen lässt, dass dem Bundesamt für Sozialversicherung bestimmte Daten geliefert werden können.

10. Mietrecht

10.1. Anmeldeformulare für Mietwohnungen - Der Entscheid der EDSK

Inzwischen liegt uns der Entscheid der Eidgenössischen Datenschutzkommission (EDSK) betreffend unsere Empfehlung zur Frage vor, ob und inwieweit Vermieter Daten von Mietinteressenten erheben dürfen. Die EDSK teilt mit uns die Ansicht, dass im Hinblick auf den Abschluss eines Mietvertrages nicht uneingeschränkt Informationen zur Person der Mietinteressenten verlangt werden dürfen. Bei der datenschutzrechtlichen Beurteilung der Zulässigkeit einzelner Fragen ist jedoch nicht in allen Punkten Übereinstimmung erzielt worden.

Zusammenfassend äussert sich die EDSK wie folgt:
Die Frage nach der Anzahl, dem Alter und Geschlecht der Kinder gilt in Abänderung der Empfehlung als generell zulässig, weil diese Angaben sowohl die Vorselektion einer geeigneten Wohnung für den betreffenden Mietinteressenten als auch umgekehrt eine Vorselektion von Interessenten für eine bestimmte Wohnung erleichtern kann. Soweit es jedoch um die Erhebung der Daten von erwachsenen Personen geht, die im selben Haushalt leben, jedoch ohne Vertragspartei zu sein, ist dies - wie in unserer Empfehlung festgehalten - nur bei Vorliegen besonderer Voraussetzungen möglich (Bestehen einer gesetzlichen Pflicht, statutarische Zielsetzung der Liegenschaftsverwaltung, Vorliegen anderer wichtiger Gründe).
Die EDSK bestätigt in ihrer Beurteilung, dass die aufgrund der Empfehlung zulässige Frage nach dem Jahreseinkommen in abgestuften 10'000 Fr.-Schritten bis Fr. 100'000.- ausreicht, um die finanzielle Situation der Mietinteressenten abzuschätzen. Punktuelle Angaben zur finanziellen Situation, die nicht geeignet sind, ein vollständiges Bild der wirtschaftlichen Lage der Interessenten aufzuzeigen, dürfen jedoch nicht verlangt werden (z.B. Fragen nach Abzahlungsverträgen und Lohnzessionen). Hingegen erachtet die Kommission die Frage nach der Anzahl von Autos aus der Sicht des Persönlichkeitsschutzes als unproblematisch. Denn diese Angaben können für beide Vertragsparteien von Interesse sein (Verfügbarkeit von Autoeinstellplätzen).
Die Kommission bestätigt schliesslich, dass die Kenntnis des Zivilstandes nur bei Vorliegen besonderer Voraussetzungen erforderlich ist.
Hingegen wird die Frage nach der Nationalität (Schweizer/Ausländer) als generell zulässig erachtet, weil sich dies auf die Beziehung mit den anderen Mietern auswirken kann. Eine erweiterte Fragestellung, wie z.B. hinsichtlich der Kategorie der Ausländerbewilligung, ist aber im Rahmen einer Vorselektion nicht erlaubt.
Unsere Empfehlung, wonach das Einholen von Referenzen durch den Vermieter der Zustimmung des Mietinteressenten bedarf, wird als angemessen beurteilt. Jedoch hat sich das Informationsrecht auf die Bestätigung der im Formular gemachten Angaben zu beschränken. Die Kommission empfiehlt daher ihrerseits, dieser Rubrik den Vermerk «fakultativ» beizufügen. Dasselbe gilt im Ergebnis auch für die Frage nach dem Arbeitsort, dem Namen und der Adresse des gegenwärtigen Vermieters. Hingegen dürfen Adresse und Telefonnummer des Arbeitgebers erst im Hinblick auf den Vertragsabschluss verlangt werden.
Die Datenerhebung im Zusammenhang mit Wartelisten, die sich nicht auf ein konkretes Wohnobjekt beziehen, soll nach Ansicht der EDSK in gleichem Umfang wie bei Anmeldungen für eine bestimmte Wohnung möglich sein. Eine Beschränkung auf die Angabe von Name und Adresse, wie wir sie in diesem Fall empfohlen haben, rechtfertigt sich nicht. Dies deshalb, weil die Führung von Wartelisten nur sinnvoll ist, wenn der Vermieter dadurch diejenigen Daten erhält, die für die Auswahl des Mieters für das in Betracht fallende Wohnobjekt erforderlich sind. Es ist davon auszugehen, dass das Ausfüllen einer Warteliste in der Regel durch eine gültige Einwilligung gerechtfertigt ist.
Über die Beurteilung der oben abgehandelten Einzelfragen hinaus, werden einige Kernfragen des Datenschutzgesetzes durch die EDSK näher abgehandelt und präzisiert. Demnach ist der EDSB befugt, auch über den konkreten Einzelfall hinausgehende, generell-abstrakte Empfehlungen zu erlassen. Eine allfällige Weiterziehung an die EDSK hat sich jedoch gegen einen konkreten Adressaten zu richten.
Der EDSB kann grundsätzlich zwei Arten von Empfehlungen abgeben: Solche, die im Rahmen seiner Beratungstätigkeit abgegeben werden (Zweckmässigkeitsempfehlungen) und solche, die im Kontrollbereich erfolgen und welche letztere (bei Feststellung einer Rechtsverletzung) der EDSK vorgelegt werden können.

Die Empfehlungsbefugnis des EDSB ist nach Art. 29 Abs. 1 lit. a DSG weit zu interpretieren und nicht bloss auf Fehler von EDV-Informationssystemen zu beschränken. Von einem «Systemfehler» im Sinne der genannten Bestimmung ist auch dann zu sprechen, wenn das System der Bearbeitung rechtswidrig ist. Dies ist dann der Fall, wenn die Bearbeitung geeignet ist, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen.
Schliesslich wurden noch die Anforderungen an eine Einwilligungserklärung präzisiert. Demnach muss der Einwilligende die Möglichkeit haben, sich frei und in Kenntnis der sich aus der Einwilligung ergebenden Konsequenzen entscheiden zu können. Mit anderen Worten: Die Vertragsfreiheit sowie die freie Willensentscheidung bezüglich der im Rahmen des Vertragsabschlusses verlangten Datenbekanntgabe darf nicht eingeschränkt werden. Es kann daher nicht generell davon ausgegangen werden, dass die Bekanntgabe von Daten aufgrund einer rechtswirksamen Erklärung erfolgte.
Ob eine gültige Einwilligung vorliegt, ist jedoch aufgrund der tatsächlichen Situation im Einzelfall zu entscheiden. Generell gilt: Je heikler die Daten, desto höher sind die Anforderungen an die Einwilligung zu stellen.

II. DIE KONTROLLEN DES EDSB

1. Einmaliger Abgleich von 9000 Fingerabdruckdaten der Schweiz und Deutschlands zu statistischen Zwecken

Der Abgleich führte zum Ergebnis, dass 3,3% der Asylbewerber in der Schweiz und in Deutschland ein Asylgesuch gestellt haben. Ein Viertel dieser Zweifach-Gesuchsteller (d.h. weniger als 1% aller Gesuchsteller) sind in Deutschland unter einem anderen Namen als in der Schweiz verzeichnet. Wir haben uns den Abgleich technisch vorführen lassen und waren im grossen und ganzen mit Organisation und Sicherheit zufrieden.

Heute werden in der Schweiz praktisch bei allen Asylbewerbern die Fingerabdruckdaten erfasst und gespeichert. Wir haben diese Lösung wiederholt als unverhältnismässig bezeichnet und ein differenzierteres Vorgehen gefordert, wie es auch in anderen europäischen Ländern praktiziert wird. In diesem Zusammenhang haben wir auch vorgeschlagen, in Artikel 96 des revidierten Asylgesetzes eine «kann»-Vorschrift zu wählen und die «muss»-Vorschrift zu streichen. Das Ergebnis dieses statistischen Fingerabdruck-Abgleichs spricht nun für unseren Vorschlag. Es ist keineswegs so, dass die Mehrzahl der Asylbewerber den Rechtsstaat mit Doppelgesuchen «aushebelt», wie bisweilen argumentiert wird. Vielmehr entschliesst sich nur ein kleiner Teil zum Schritt eines Doppelgesuchs. Die statistische Auswertung gibt zu den jeweiligen Motiven keine nähere Auskunft. Zieht man weiter in Betracht, dass nur ein Viertel dieser 3,3% Zweifach-Gesuchsteller unter verschiedenen Namen verzeichnet sind, wird man jedenfalls bei den übrigen drei Vierteln achtbare Beweggründe vermuten dürfen. Aus der Statistik geht auch nicht hervor, in welchem Ausmass die unterschiedlichen Verzeichnungen in den beiden Antragsländern auf die hinlänglich *bekannten Probleme bei der Namensschreibweise* zurückzuführen sind. Insgesamt muss das immer wieder ins Feld geführte Argument des Miss-

brauchs doch erheblich relativiert werden. Wir hoffen, dass sich dies auf die gesetzgeberische Arbeit im Sinne unserer Vorschläge auswirkt.
Bei der Vorführung des Datenabgleichs im Bundesamt für Flüchtlinge erhielten wir im grossen und ganzen einen guten Eindruck über den Datenschutz und die Datensicherheit. Indessen waren wir erstaunt, dass man uns den Systembefehl «Ausdrucken der Konfiguration der verwendeten Informatikmittel» verweigern wollte. Der EDSB kann seine gesetzlichen Kontrollfunktionen nicht wahrnehmen, wenn er nicht unabhängig Einblick in die zu kontrollierenden Datenbearbeitungen und Bearbeitungsdokumentationen erhält. Ebenso waren wir über die räumliche und organisatorische Nähe erstaunt, in welcher die Polizeidaten und die Asylbewerberdaten bearbeitet werden. Unser vor Ort und im Rahmen einer Empfehlung geäusserter organisatorischer Vorschlag nach einer deutlicheren Abgrenzung zwischen asylbezogenen und polizeibezogenen Kompetenzen bei der Bearbeitung von Fingerabdruckdaten beim Schlüsselmanagement wurde indessen abgelehnt.

2. Überwachung der Angestellten durch Videokameras

Überwachungssysteme am Arbeitsplatz (insbesondere Videokameras) dürfen nur aus Sicherheitsgründen oder zur Kontrolle der Arbeitsleistung eingesetzt werden (vgl. 2. Tätigkeitsbericht, S. 44 ff.). In diesem Zusammenhang untersuchten wir ein Überwachungssystem einer im Papierhandel tätigen Unternehmung. Verstösse gegen das Datenschutzgesetz waren jedoch dort nicht festzustellen.

Nach Anregung eines Angestellten führten wir bei einer im Papiergrosshandel tätigen Basler Firma eine Kontrolle hinsichtlich der dort installierten Videokameras durch. Das Überwachungssystem besteht aus sieben Videokameras. Diese überwachen die im Betrieb strategisch wichtigen Punkte (Standort der Warenanlieferung, Haupteingang und Liftausgang zum Lagerraum). Arbeitsplätze werden nicht direkt erfasst. Zweck der Überwachung ist hauptsächlich die Verhinderung von Diebstählen, die Feststellung der unbefugten Anwesenheit von Fremdpersonen sowie eine verbesserte Organisation des Betriebsablaufes. Eine Überwachung des Verhaltens der Arbeitnehmer wird nicht bezweckt. Denn das Überwachungssystem eignet sich aufgrund seiner einfachen Beschaffenheit nicht dazu. Wir stellten des weiteren fest, dass das System nicht dauernd in Betrieb ist. Zudem erlaubt es nicht, die erfassten Bilder zu speichern und weiterzuverarbeiten. Im übrigen wird nicht davon Gebrauch gemacht, die kontrollierten Räume - obwohl ohne weiteres möglich - abzuhören. Das Personal wurde über die Installation der Kameras und der damit verfolgten Ziele informiert, und es wurde ihm die Möglichkeit gegeben, sich am Monitor selbst von den erfassten Bildausschnitten eine Vorstellung zu machen. Wir sind deshalb zum Schluss gekommen, dass die Überwachung der Räumlichkeiten aus datenschutzrechtlicher Sicht weder unrechtmässig noch unverhältnismässig ist.

3. Datenbearbeitung zu Werbezwecken: Nichtbeachtung der Adress-Sperre

Seitens einer kantonalen Datenschutzbehörde wurden wir erstmals auf die fragwürdigen Werbepraktiken einer Versandhandelsfirma aufmerksam gemacht, die im Bereich Astrologie und Wahrsagerei tätig ist. Unabhängig davon erhielten wir bisher weit über hundert Zuschriften von vielfach sehr verärgerten Personen, die trotz z.T. mehrfacher Abmahnung der besagten Versandhandelsfirma weiterhin von ihr Werbematerial er-

hielten. Wir sahen uns daher dringend veranlasst, die Adressbearbeitungen dieser Firma zu untersuchen.

Die betreffende Firma betreibt sehr intensiv Direktwerbung, um Produkte aus dem Bereich Wahrsagerei und Astrologie zu verkaufen. Die Adressen stammen einerseits aus Zeitungs-Inseraten oder werden in grossem Umfang bei verschiedenen Versandhäusern, v.a. in der Westschweiz zugemietet. Da in den diversen Adressdateien oftmals dieselben Namen figurieren, werden viele Leute immer wieder mit der gleichen Werbung belästigt. In Folge der fragwürdigen Prophezeiungen der verschiedenen Wahrsager, die für diese Firma tätig sind - in Wirklichkeit handelt es sich um standardisierte Computerhoroskope - hat sich in der Westschweiz Widerstand gegen die Werbeschreiben geregt.
Bei unserer Besichtigung der Firma zeigte sich, dass nur eine Kundendatei existierte, während refusierte Sendungen oder Adress-Sperrungen nicht erfasst wurden. Wir forderten daher die Firma auf, diesen Mangel innerhalb der ihr gesetzten Frist zu beheben. Sie sicherte uns zu, in Zukunft jeden Werbeversand zunächst mit einer Liste der gesperrten Adressen abzugleichen. Trotzdem erhielten wir weiterhin Reklamationen von Personen, die trotz Sperrungsanzeige weiterhin Werbesendungen zugeschickt bekamen. Wir sahen uns deshalb dazu verpflichtet, eine zusätzliche und noch eingehendere Kontrolle durchzuführen. Für den Fall, dass das System der Adress-Sperrliste unzureichend funktionieren sollte, stellten wir der Firma ein vorübergehendes Datenbearbeitungsverbot bis zur Behebung des Mangels in Aussicht.
Anlässlich der zweiten Kontrolle erhielten wir genauere Informationen über die Organisation und die Arbeitsweise der Firma. Insbesondere überprüften wir die neuangelegte Adress-Sperrdatei auf deren Vollständigkeit hin. Wir mussten zu unserem Bedauern feststellen, dass einige der uns als gesperrt gemeldeten Adressen in der entsprechenden Datei fehlten. Wie uns der zuständige Geschäftsführer erklärte, sei dies darauf zurückzuführen, dass die Bearbeitung der Sperrungsanzeigen, von deren Eingang an gerechnet, rund einen Monat in Anspruch nehmen würde. Er versicherte uns jedoch, für die sofortige Nachführung der Adress-Sperrdatei besorgt zu sein. Bei der Erwägung des weiteren Vorgehens wurde berücksichtigt, dass die fragliche Firma ordnungsgemäss im Register der Datensammlungen angemeldet ist und mit der Inbetriebnahme einer Adress-Sperrdatei Kooperationsbereitschaft gezeigt hat. Wir setzten der Firma daher eine letzte Frist zur Vervollständigung ihrer Adress-Sperrdatei sowie zur schriftlichen Orientierung der betroffenen Personen. Der zuständige Geschäftsführer hat uns inzwischen bestätigt, dass unserem Ersuchen Folge geleistet wurde.
Dieser Fall zeigt anschaulich, wie unerwünschte Werbesendungen zu einer Plage für die Betroffenen werden können. Insbesondere ältere und leichtgläubige Personen sind gegenüber unerbetenen Glücks- und Unglücksprophezeiungen und den hartnäckigen Mahnungen gleichermassen hilflos. Adressierte Werbung ist eine Erscheinung unserer Zeit. Sie stellt grundsätzlich eine erlaubte Form zur Erschliessung neuer Kundenkreise dar. Für den Fall jedoch, dass jemand solcherlei Werbung nicht wünscht, müssen im Interesse aller Beteiligten Mittel und Wege gefunden werden, dass der Wille der potentiellen Kundschaft respektiert wird. An dieser Stelle möchten wir betonen, dass die bestehenden Möglichkeiten der Adress-Sperrung (PTT und Robinsonliste) offenbar nicht ausreichen. Die einschlägigen Firmen selbst müssen daher unbedingt über ihre Pflicht, Adress-Sperrungen zu berücksichtigen, informiert werden.

4. Bearbeitung von Ausländerdaten in schweizer Geschäftsstellen im Ausland und an der Grenze

Auch die schweizerischen Geschäftsstellen im Ausland und die schweizerischen Grenzkontrollposten bearbeiten eine Vielzahl von Personendaten. Bei zwei Kontrollen in Freiburg i. Br. und im Grenzraum Basel erhielten wir einen positiven Eindruck über den dort praktizierten Datenschutz.

Anlässlich zweier Kontrollen im Jahr 1996 erhielten wir einen guten Einblick in die Datenbearbeitungen bei der Visaerteilung in einer schweizerischen Geschäftsstelle im Ausland (inzwischen geschlossenes Konsulat Freiburg i.Br.) und an verschiedenen schweizerischen Grenzkontrollposten im Raum Basel. Diese Behörden stellen die Visa bzw. Sichtvermerke manuell aus. Zuvor konsultieren sie den Schweizerischen Fahndungsanzeiger und in Zweifelsfällen das Bundesamt für Ausländerfragen in Bern, welches bei Bedarf weitere Abklärungen trifft. Die Grenzkontrollstellen verfügen seit kurzem über (beschränkte) Zugriffe auf das Fahndungssystem RIPOL, das Zentrale Ausländerregister ZAR und nunmehr auch auf die Asylbewerberdaten des AUPER. Die schweizerischen Geschäftsstellen im Ausland verfügen hingegen über keine solchen Zugriffe (mit Ausnahme von einigen grossen Botschaften, welche direkt auf das RIPOL greifen können).
Unsere Kontrolle der Datenbearbeitungen beim schweizerischen Konsulat in Freiburg i.Br. verlief positiv und gab zu keinen Beanstandungen Anlass.
Unsere Kontrolle an den verschiedenen Grenzposten im Raum Basel verlief ebenfalls positiv. Die kontrollierten Abfragen des RIPOL standen in Einklang mit der RIPOL-Verordnung. Bei den kontrollierten Abfragen des ZAR regten wir an, die auf dem Bildschirm angezeigten Rückweisungsgründe zu codieren. (Das AUPER war im Zeitpunkt der Kontrolle noch nicht eingerichtet.) Ebenso regten wir an, die zum Zeitpunkt der Kontrolle ausstehende Risikobeurteilung gemäss den Sicherheitsweisungen des Bundesamtes für Informatik möglichst umgehend durchzuführen und eine Chiffrierung der besonders schützenswerten Daten auf den elektronischen Geräten einzurichten, soweit dies nicht schon geschehen war. Die kontrollierten Bearbeitungen der Visadaten und Grenzkontrollrapporte (beide in Papierform) erachteten wir ebenfalls als datenschutzkonform.

5. Die neue Identitätskarte ID 95

Seit dem 1. Juli 1994 ist die neue schweizerische Identitätskarte (IDK) erhältlich. Die Ausstellung der Identitätskarte sowie die Bedingungen an die Bearbeitung von Personendaten sind in der Verordnung des Bundesrates über die Identitätskarte geregelt. In der Zeit von Oktober 1995 bis März 1996 kontrollierten wir die Einhaltung dieser Anforderungen im Bereich des Datenschutzes.

Die Bedingungen für die Ausstellung der IDK sowie die damit zusammenhängende Bearbeitung von Personendaten ist in der Verordnung über die schweizerische Identitätskarte vom 18. Mai 1994 geregelt. In der Zeit von Oktober 1995 bis März 1996 kontrollierten wir die Einhaltung dieser Anforderungen im Bereich des Datenschutzes. Wesentliche Gesichtspunkte der Kontrolle waren der Inhalt und der isolierte Charakter der vom Bundesamt für Polizeiwesen (BAP) verwalteten Datenbank, die Zugriffsberechtigungen, die Datenerfassung, die Weitergabe der Daten an den Kartenhersteller und das BAP, die Datenbearbeitung, insbesondere die Löschung der

Daten nach Ablauf der Aufbewahrungsdauer, die Verwendung des maschinenlesbaren Codes sowie die Informationen, die auf der Identitätskarte selbst enthalten sind.
Allgemein konnten wir feststellen, dass die vom BAP und vom Kartenhersteller durchgeführten Datenbearbeitungen der Verordnung genügen.
Das Eidgenössische Justiz- und Polizeidepartement ist jedoch seiner Pflicht, Weisungen über die Anforderungen an die Datensicherheit zu erlassen, nicht nachgekommen. Desweiteren mussten wir feststellen, dass die vorgeschriebene Frist von zehn Tagen, innerhalb derer der Kartenhersteller alle gespeicherten Daten zu löschen hat, nicht eingehalten wird.
In der Zwischenzeit ist gewährleistet, dass die Daten beim Kartenhersteller innerhalb von 10 Tagen elektronisch gelöscht werden. Demgegenüber ist die Ausarbeitung von Weisungen über die Anforderungen an die Datensicherheit bis anhin nicht an die Hand genommen worden.
Abschliessend möchten wir betonen, dass die Kontrolle in einem sehr guten Klima der Zusammenarbeit stattgefunden hat.

III. WEITERE THEMEN

1. Veröffentlichung von Personendaten

1.1. Veröffentlichung von Angaben über Hooligans in der Zeitung «Sport»

In der Zeitung «Sport» wurden Name, Adresse sowie Geburtsdatum von Personen veröffentlicht, die von der Disziplinar- und Sicherheitskommission der Nationalliga des Schweizerischen Fussballverbandes mit Stadionverboten belegt wurden.

In der Zeitung «Sport» wurden Name, Adresse und Geburtsdatum von Personen veröffentlicht, die von der Disziplinar- und Sicherheitskommission der Nationalliga des Schweizerischen Fussballverbandes mit Stadionverboten belegt wurden. Name, Adresse und Geburtsdatum sind Personendaten im Sinne des DSG. Die Verurteilung durch ein staatliches Gericht ist ein besonders schützenswertes Personendatum im Sinne des DSG. Wir haben vertreten, dass ein von der Disziplinar- und Sicherheitskommission verhängtes Stadionverbot eine mit den Urteilen staatlicher Gerichte vergleichbare Wirkung auf das gesellschaftliche Ansehen der betreffenden Person hat. Aus diesem Grund ist auch das von der Disziplinar- und Sicherhheitskommission gegen eine bestimmte Person verhängte Stadionverbot als besonders schützenswertes Personendatum anzusehen und geniesst deshalb einen hohen Schutz.
Die Veröffentlichung von Name, Adresse und Geburtsdatum von Personen, über die Stadionverbote verhängt wurden, darf nur erfolgen, wenn sie durch Einwilligung der betreffenden Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist. Eine Veröffentlichung, dass heisst die Bekanntgabe dieser Personendaten an die Leser der Zeitung «Sport» und damit an die Öffentlichkeit ist durch kein Gesetz gerechtfertigt, noch lässt sie sich durch ein privates oder öffentliches Interesse rechtfertigen. Dagegen lässt sich die Bekanntgabe der Personendaten an die Organe rechtfertigen, die für die Gewährleistung von Sicherheit und Ordnung bei den und im Umfeld von den stattfindenden Spielen zuständig sind. Es dürfen jedoch aus Gründen der Verhältnismässigkeit nicht vollständige Listen sämtlicher mit Stadionverboten belegten Personen an die Sicherheitsorgane

sämtlicher Stadien verteilt werden. Vielmehr sind die Personendaten nur den Sicherheitsorganen der Stadien mitzuteilen, für die das Stadionverbot ausgesprochen wurde.

1.2. Veröffentlichung eines Berichts über die Vermögen der Opfer des Nationalsozialismus

Die Information der Öffentlichkeit und das historische Interesse können die Veröffentlichung eines Berichtes über die Vermögen der Naziopfer und die Abkommen mit den osteuropäischen Ländern unter Nennung der Namen aller betroffenen Personen nicht rechtfertigen. Der Persönlichkeitsschutz und die Grundrechte erfordern eine weitgehende Anonymisierung des Berichts vor der Veröffentlichung. Einzig die Namen von natürlichen und juristischen Personen, die eine entscheidende öffentliche Rolle gespielt haben, dürfen veröffentlicht werden.

Der EDSB wurde im Zusammenhang mit der Veröffentlichung des Berichts zweier Historiker, die im Auftrag des EDA Licht in die Angelegenheit der Vermögen der Naziopfer und der Entschädigungsabkommen mit Osteuropa bringen sollten, um eine Stellungnahme gebeten. Der Bericht soll vor allem das Verhalten der schweizerischen politischen Behörden und der Verwaltung im Zusammenhang mit den von den Naziopfern in der Schweiz hinterlegten Vermögenswerten und mit der Entschädigung für - aufgrund der Abkommen zwischen der Schweiz und osteuropäischen Ländern - verstaatlichte Güter beleuchten. Der Bericht führt die Namen zahlreicher bereits verstorbener oder noch lebender Personen auf (Bundesräte, Minister, Botschafter, Direktoren, Beamte, Bankiers, Personen, die mit den nachrichtenlosen Vermögen zu tun hatten, Anwälte, usw.) sowie Informationen zu diesen Personen (vor allem Erklärungen oder Stellungnahmen). Sofern die Informationen sich auf noch lebende Personen beziehen, kommt das Bundesgesetz über den Datenschutz zur Anwendung. Der Persönlichkeitschutz verstorbener Personen jedoch endet grundsätzlich mit ihrem Ableben. Vorbehalten bleibt allerdings der Persönlichkeitsschutz der Angehörigen.

Weiter ist zu erwähnen, dass der Grossteil der fraglichen Forschungsarbeit sich nicht auf betroffene Personen bezieht und dass die Resultate in einer Form veröffentlicht werden sollten, die keine Identifizierung der betroffenen Personen zulässt. Allerdings wird in einem Teil der Forschungsarbeit doch auf diese Bezug genommen, zumal dort das Verhalten bestimmter öffentlicher Persönlichkeiten geprüft wird, die während der untersuchten Zeitperiode die Verantwortung in den erwähnten Bereichen übernommen hatten. Mithin untersteht die Veröffentlichung der diesbezüglichen Personendaten Artikel 19 DSG. Danach ist die Veröffentlichung nur zulässig, wenn

- sie auf einer Rechtsgrundlage beruht;
- die Daten für den Empfänger im Einzelfall für die Erfüllung seiner gesetzlichen Aufgabe unentbehrlich sind;
- die betroffene Person im Einzelfall eingewilligt hat oder die Einwilligung nach den Umständen vorausgesetzt werden darf;
- die betroffene Person ihre Angaben allgemein zugänglich gemacht hat.

Es ist davon auszugehen, dass zumindest implizit eine Rechtsgrundlage für ein überwiegendes öffentliches Interesse besteht. In Zukunft wird sich die Frage nicht mehr stellen: Mit dem Bundesbeschluss vom 14. Dezember 1996 betreffend die historische und rechtliche Untersuchung des Schicksals der infolge der nationalsozialistischen Herrschaft in die Schweiz gelangten Vermögenswerte wurde eine klare Ge-

setzesgrundlage für die Veröffentlichung der Forschungsresultate der Bergier-Kommission geschaffen.

Bei der Bekanntgabe bzw. der Veröffentlichung müssen zudem die allgemeinen Bearbeitungsgrundsätze für Daten und insbesondere der Grundsatz der Verhältnismässigkeit beachtet werden. Es ist darauf zu achten, dass die Bekanntgabe die Grundrechte und die Persönlichkeit der betroffenen Personen möglichst wenig beeinträchtigt. Vor allem aber ist die Tatsache zu berücksichtigen, dass ein solcher Bericht wegen seiner Bedeutung für Politik und Medien für eine breite Öffentlichkeit bestimmt ist. Höchstwahrscheinlich wird er auch bald auf einer Internet-Seite in der Schweiz oder im Ausland verfügbar sein. Aus diesem Grund ist vor der Veröffentlichung der Namen der betroffenen Personen grösste Vorsicht geboten. Die Veröffentlichung der Namen von Personen die im Zusammenhang mit subjektiven, nicht absolut fundierten oder sogar umstrittenen Beurteilungen muss somit vermieden werden, ausser wenn das öffentliche Interesse die Wahrung der Anonymität überwiegt (was jedoch im vorliegenden Fall nicht nachgewiesen wurde). Deshalb dürfen Namen von Personen nur veröffentlicht werden, wenn sie für das Verständnis der Geschehnisse unentbehrlich sind. Dabei handelt es sich insbesondere um die Namen von öffentlich bekannten, natürlichen und juristischen Personen (vor allem Persönlichkeiten des öffentlichen Lebens), die politische, wirtschaftliche und moralische Verantwortung trugen und Entscheidungen zu treffen hatten.

Der EDSB ist daher zum Schluss gelangt, dass die meisten der im Bericht genannten Personen anonymisiert werden können. So ist es nicht erforderlich, zusätzlich zu den jeweiligen Verwaltungsstellen die Namen der mit dem Dossier beauftragten Beamten zu nennen, sofern diese keine Führungspositionen inne hatten und in dieser Eigenschaft öffentlich bekannt waren. Gleiches gilt für die Namen der Naziopfer und ihrer Familien, welche Schritte eingeleitet hatten, um die Vermögenswerte zurückzuerlangen. Die noch lebenden Personen sind nicht unbedingt daran interessiert, dass ihr Name veröffentlicht und weit verbreitet wird. Schliesslich sollten auch die Namen der von den Opfern und ihren Familien beauftragten Anwälte nicht veröffentlicht werden. Prinzipiell spricht jedoch nichts dagegen, die Namen der involvierten Banken, der damaligen Bundesräte, der ausländischen Minister und der unmittelbar beteiligten Direktoren von Bundesämtern zu veröffentlichen. Gleiches gilt für die Botschafter und ranghohen Beamten, die an bestimmten Verhandlungen teilnahmen, sofern deren Namen für das Verständnis der Geschehnisse bekannt sein müssen.

1.3. Veröffentlichung von nicht anonymisierten Bundesgerichtsentscheiden im Internet

Das Bundesgericht stellt einen Teil der Bundesgerichtsentscheide der Öffentlichkeit in nicht anonymisierter Form über das Internet zur Verfügung. Im Bundesgesetz über den Datenschutz ist festgehalten, dass für eine solche Datenbekanntgabe eine rechtliche Grundlage notwendig ist.

Wir haben das Bundesgericht darauf aufmerksam gemacht, dass ein einfacherer Zugriff auf die Bundesgerichtsentscheide durchaus begrüssenswert sei. Dabei sind allerdings die rechtlichen Rahmenbedingungen für das Zugänglichmachen von Informationen zu berücksichtigen.

Das Bundesgesetz über den Datenschutz (DSG) hält in Art. 17 Absatz 2 fest, dass besonders schützenswerte Personendaten, wie z. B. strafrechtliche Verfolgungen oder Sanktionen (Art. 3 Bst. c DSG) nur bearbeitet werden dürfen, wenn dies in einem formellen Gesetz ausdrücklich vorgesehen ist. Im weiteren wird in Art. 19. Abs. 3 DSG aufgeführt, dass Bundesorgane Personendaten durch Abrufverfahren (z. B. Online-Verfahren via Internet) zugänglich machen dürfen, wenn dies ausdrücklich vorgesehen ist. Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile dürfen nur durch ein Abrufverfahren zugänglich gemacht werden, wenn ein formelles Gesetz dies ausdrücklich vorsieht. Dem Zweck der Informationsvermittlung über das Internet wäre Genüge getan, wenn die Daten in anonymisierter Form zur Verfügung gestellt würden. Dann würde aus der Sicht des Datenschutzes auch die Forderung nach einer rechtlichen Grundlage entfallen.

2. Zivildienst

2.1. Das Datenbearbeitungssystem über den Zivildienst ZIVI

Die Inbetriebsetzung des Systems ZIVI führt zu einer vereinfachten und effizienten Gestaltung des Vollzuges des Zivildienstes. Der dazugehörigen Verordnung über das Informationssystem des Zivildienstes stimmten wir unter dem Vorbehalt zu, dass diese bis Ende 1998 revidiert wird.

Mit dem Informationssystem ZIVI wird eine grössere Anzahl besonders schützenswerte Personendaten bearbeitet. Darunter finden sich Daten wie Religion, Weltanschauung, Zugehörigkeit zu Gruppierungen und Sekten, Arbeitslosigkeit, Disziplinarverfahren, Massnahmen der sozialen Hilfe und Gesundheit der zivildienstpflichtigen Personen. Am System ZIVI sind mehrere Stellen (zentrale und dezentrale Vollzugsstellen des Bundesamtes für Industrie, Gewerbe und Arbeit sowie die Militärversicherung) beteiligt. Auch Dritte, die mit dem Vollzug von Aufgaben in Zusammenhang mit dem Zivildienst betraut wurden, sind am System angeschlossen. Einige der beteiligten Stellen sind am System online verbunden. Das Bundesgesetz über den Datenschutz sieht für solche Systeme die Schaffung einer gesetzlichen Grundlage im formellen Sinne vor. Eine formelle gesetzliche Grundlage wurde im Bundesgesetz über den zivilen Ersatzdienst geschaffen. Dabei wurde jedoch die Bearbeitung von besonders schützenswerten Personendaten nicht vorgesehen. Die formellgesetzliche Grundlage des Systems ZIVI ist somit bei der nächsten Revision des Gesetzes an die datenschutzrechtlichen Anforderungen anzupassen. Wir haben weiter verlangt, dass die Verordnung über das Informationssystem ZIVI die Details der Bearbeitung von besonders schützenswerten Personendaten ausdrücklich regeln soll. Insbesondere soll die Verordnung die Zugriffsberechtigungen, die beteiligten Stellen und Dritte, den Zugriffszweck und -umfang sowie die davon betroffenen Daten normieren. Zum Zeitpunkt der Inkraftsetzung des Zivildienstgesetzes (1. Oktober 1996) erfüllte die entsprechende Verordnung die datenschutzrechtlichen Anforderungen noch nicht. Wir waren uns jedoch bewusst, dass das System ohne Verzug in Betrieb gesetzt werden musste. In diesem Sinne erklärten wir uns mit der Verordnung unter der Bedingung einverstanden, dass diese bis Ende 1998 zu revidieren ist.

3. Archivwesen

3.1. Schutzfrist für besonders schützenswerte Personendaten und Persönlichkeitsprofile im neuen Archivgesetz

Der Bundesrat hat die Schutzfrist für besonders schützenswerte Personendaten sowie für Persönlichkeitsprofile im neuen Archivgesetz auf 50 Jahre festgelegt.

Der Bundesrat hat nach Ämterkonsultation und grossem Mitberichtsverfahren Botschaft und Entwurf des neuen Archivgesetzes (vgl. dazu 1. Tätigkeitsbericht S. 50ff.) gutgeheissen und die Schutzfrist für besonders schützenswerte Personendaten und Persönlichkeitsprofile auf 50 Jahre seit dem jüngsten Dokument festgelegt.
Ursprünglich hatten wir für besonders schützenswerte Personendaten und Persönlichkeitsprofile eine Schutzfrist von mindestens bis zum Tod der betroffenen Person gefordert. Diese Forderung beruhte auf der Kenntnis, dass zum einen in anderen Ländern wie Deutschland Schutzfristen für alle Personendaten und nicht nur für besonders schützenswerte Personendaten und Persönlichkeitsprofile von bis zu 10 Jahren nach dem Tod bestehen, zum anderen auch in der Schweiz zum Beispiel der Kanton Zürich eine Schutzfrist für besonders schützenswerte Personendaten bis zum Tod der betroffenen Person vorsieht. Wir waren der Forderung einer Reduzierung nachgekommen und hatten uns mit dem Bundesarchiv auf eine Schutzfrist von 70 Jahren einigen können. Um so erstaunter waren wir, als wir aus den Medien erfahren mussten, dass zum einen das grosse Mitberichtsverfahren abgeschlossen wurde, ohne dass wir begrüsst wurden, zum anderen die Schutzfrist von 70 Jahren auf 50 Jahre reduziert wurde.

4. Bekanntgabe von Personendaten

4.1. Das Bereitstellen von Mitarbeiterdaten durch die Bundesverwaltung im Abrufverfahren

Am Anfang stand der Wunsch, den Inhalt des Eidgenössischen Staatskalenders und des Telefonverzeichnisses der Allgemeinen Bundesverwaltung in einem durch Abrufverfahren zugänglichem Verzeichnis zur Verfügung zu stellen. Der von der Arbeitsgruppe verabschiedete Vorschlag für eine Verordnung soll den Einsatz von Adressverzeichnissen in der Bundesverwaltung regeln.

Wie im 3. Tätigkeitsbericht (S. 27) erwähnt, wurde vom Bundesamt für Informatik eine Arbeitsgruppe mit Vertretern der Bundeskanzlei und uns ins Leben gerufen mit dem Ziel, für die Zurverfügungstellung von Angaben über Mitarbeiter in Verzeichnissen (z. B.: X.500) eine genügende Rechtsgrundlage auszuarbeiten. Mit der Erarbeitung eines Verordnungsentwurfs für die Bundeskanzlei wurde die Arbeitsgruppe aufgelöst, da die definitive Fassung der Verordnung im Rahmen der Ämterkonsultation festgelegt wird.
Dieser Entwurf beinhaltet Bestimmungen zu Adressverzeichnissen in der Bundesverwaltung. So werden Zweck, Inhalt, der Zugriff auf die Informationen, die Rechte der Betroffenen, die Pflicht zur Information über Risiken und Verantwortlichkeiten geregelt. Ebenso wurde festgelegt, dass der Zugang mittels Abrufverfahren verwal-

tungsextern auf Ansprechpartner (Mitarbeiter der Bundesverwaltung, die der Öffentlichkeit gegenüber als Ansprechpartner dienen) gegenüber Dritten beschränkt ist.

4.2. Weitergabe von Daten aus der Sonderabfall-Datensammlung des BUWAL

Fehlt eine ausreichende gesetzliche Ermächtigung, dürfen die Daten von Sonderabfall-Betrieben nur mit dem jeweiligen Einverständnis des betroffenen Betriebes weitergegeben werden. Wird die Datensammlung zu einem Dritten ausgelagert, gelten für diesen die gleichen Anforderungen, wie für das Bundesamt für Umwelt, Wald und Landschaft (BUWAL).

Das BUWAL unterbreitete uns die Frage, ob und unter welchen Voraussetzungen es seine Sonderabfall-Datensammlung auf elektronischem Datenträger einer privaten Firma übergeben dürfe und ob diese Daten an weitere Adressaten in der Schweiz und im Ausland bekanntgegeben werden dürften. In unserer Antwort teilten wir dem BUWAL mit, dass die fragliche Datensammlung nur aufgrund einer ausdrücklichen gesetzlichen Erlaubnis oder aber mit dem Einverständnis der betroffenen Betriebe an Firmen in der Schweiz oder im Ausland bekanntgegeben werden dürften. Die Adressaten hätten zudem hinreichende Gewähr für die sichere und zweckkonforme Bearbeitung der Daten zu bieten. Weil weder eine gesetzliche Ermächtigung noch die Einwilligung der Betroffenen vorlag, erachteten wir die Datenbearbeitungen als unzulässig und beantworteten die gestellte Frage negativ.

4.3. Weiterleitung von ausführlichen ärztlichen Berichten direkt an die Fremdenpolizeibehörden

Von ärztlicher Seite wurden wir darauf aufmerksam gemacht, dass Ärzte verschiedentlich angehalten werden, Berichte über ausländisch Patienten inklusive Diagnose und Krankengeschichte direkt den Fremdenpolizeibehörden zur Verfügung zu stellen. Eine vertrauensärztliche Instanz fehle.

Nach Ausländergesetz dürfen sich Ausländer zum Zweck der ärztlichen Behandlung in der Schweiz aufhalten. Soweit hierfür eine Bewilligung erforderlich ist, müssen sie der Bewilligungsbehörde die nötigen Angaben machen. Handelt es sich dabei um detaillierte Angaben über die Gesundheit, dürfen unseres Erachtens solche Angaben nur Personen zugänglich gemacht werden, welche dem Arztgeheimnis unterstehen (Medizinalpersonen). Diese sollen der zuständigen Behörde den entscheidwesentlichen Befund in knapper Form mitteilen. Auf diese Weise werden die Gesundheitsdaten grundsätzlich nur von Ärzten bearbeitet. Das Ausländergesetz kann so gleichwohl umgesetzt werden.
Wir stehen weiterhin mit den zuständigen Behörden in Kontakt, um auf eine datenschutzkonforme Praxis hinzuwirken.

4.4. Bekanntgabe eines administrativen Untersuchungsberichts an die Geschäftsprüfungskommissionen

Gemäss dem Bundesgesetz über den Geschäftsverkehr der Bundesversammlung (GVG) können die Geschäftsprüfungskommissionen der eidgenössischen Räte die Übermittlung eines Untersuchungsberichts verlangen. Sofern der Bericht Personen-

daten enthält, untersteht die Bekanntgabe grundsätzlich den Bestimmungen des Bundesgesetzes über den Datenschutz (DSG). Insbesondere ist der Grundsatz der Verhältnismässigkeit zu wahren. So sollten den Geschäftsprüfungskommissionen nur die zur Erfüllung ihrer gesetzlichen Aufsichtstätigkeiten notwendigen Daten bekanntgegeben werden. Wenn offensichtlich die Schlussfolgerungen und Empfehlungen des Berichts allein ausreichen bzw. die Namen der im Bericht erwähnten Personen nicht nötig sind, ist deren Bekanntgabe entweder einzuschränken oder der Bericht vor der Übermittlung teilweise oder vollständig zu anonymisieren.

Das EVD hat den EDSB um eine Stellungnahme zur Bekanntgabe eines administrativen Untersuchungsberichts an die Geschäftsprüfungskommissionen der eidgenössischen Räte gebeten. Im Bericht werden bestimmte Fehler und Nachlässigkeiten von Seiten der Beamten sowie bestimmte rechtswidrige Handlungen, die eine Strafverfolgung nach sich ziehen könnten, festgestellt. Der Bericht führt die Namen der in der fraglichen Angelegenheit involvierten Personen sowie deren Handlungen und Erklärungen auf. Sofern diese Informationen sich auf bestimmte und bestimmbare Personen beziehen, handelt es sich um Personendaten. Einige dieser Informationen gehören zu den besonders schützenswerten Daten, zumal sie auf gesetzwidrige Handlungen mit strafrechtlichen oder disziplinarischen Folgen verweisen. Die Bearbeitung und insbesondere die Bekanntgabe der Personendaten unterstehen dem DSG. Im vorliegenden Fall ist die Bekanntgabe nur möglich, wenn sie in einer Gesetzesbestimmung vorgesehen ist oder wenn die Informationen für den Empfänger zur Erfüllung seiner gesetzlichen Aufgaben unentbehrlich sind.

Die Bestimmungen des GVG bilden eine ausreichende gesetzliche Grundlage, um die Bekanntgabe des Untersuchungsberichts an die Geschäftsprüfungskommissionen zu rechtfertigen. Dem Antrag ist daher grundsätzlich stattzugeben, ausser wenn die Wahrung eines Amtsgeheimnisses, die Wahrung schutzwürdiger persönlicher Interessen oder ein noch nicht abgeschlossenes, laufendes Verfahren die Einreichung eines Sonderberichts rechtfertigen, worin einzig die Schlussfolgerungen und Empfehlungen des Untersuchungsberichts bekanntgegeben werden. Falls der Inhalt des Untersuchungsberichts bekanntgegeben wird, sind die Bestimmungen des DSG und namentlich die allgemeinen Bearbeitungsgrundsätze zu beachten. Dabei muss sich die Bekanntgabe auf jene Informationen beschränken, welche die Geschäftsprüfungskommissionen zur Erfüllung ihrer gesetzlichen Aufsichtsfunktionen benötigen; die Personendaten sind nach Möglichkeit zu anonymisieren. Kann der Bericht nicht anonymisiert werden, so sollten im übrigen die betroffenen Personen über die Bekanntgabe unterrichtet werden (Grundsatz von Treu und Glauben). Die letzte Anforderung konnte im vorliegenden Fall aus praktischen Gründen nicht erfüllt werden.

5. Datenschutz und rechtliche Rahmenbedingungen

5.1. Gesetzlich vorgeschriebene Datenbearbeitung und Information der Betroffenen

Wer Personendaten bearbeitet kann den Umgang mit dem Publikum erleichtern, wenn die betroffenen Personen vorher darüber informiert werden. Es ist jedoch darauf zu achten, dass ausschliesslich Daten verwendet werden, die aktuell und richtig sind. Falsche Daten müssen berichtigt werden können.

Mit der Revision des Urheberrechtsgesetzes (URG, SR 231.1) wurde einer privaten Person (Verwertungsgesellschaft) die Kompetenz zum Einfordern von Reprographie-Entschädigungen übertragen. Damit diese Bundesaufgabe erfüllt werden kann, mussten die erforderlichen Daten beschafft, bearbeitet und den betroffenen Personen in Rechnung gestellt werden. Wir wiesen die Verwaltungsgesellschaft darauf hin, dass die Betroffenen über die Bearbeitung ihrer Personendaten informiert werden sollten (Wahrnehmung einer Bundesaufgabe durch eine private Person, rechtliche Grundlagen, Kostenberechnung und ähnliches). Die betroffenen Personen wurden jedoch nicht darauf aufmerksam gemacht. Insbesondere wurden sie nicht über die Möglichkeit des Auskunfts- und Berichtigungsrechts gemäss DSG informiert.
Verschiedene Rechnungsempfänger ärgerten sich über die teilweise falschen Rechnungsangaben und wollten wissen, wer die falschen Daten über sie erhoben habe. Obwohl die Herkunft der Daten im Gesetz nicht ausdrücklich erwähnt wird, heisst dies nicht, dass Dritte, die im Auftrag Daten beschaffen, den betroffenen Personen auf Anfrage nicht gleichwohl bekanntgegeben werden müssen. Der Anspruch auf Kenntnis der Herkunft der Daten ergibt sich auch aus der persönlichkeitsschützenden sowie rechtsstaatlich-demokratischen Funktion des Auskunftsrechts. Die Bekanntgabe der Quelle an den Betroffenen darf erst dann unterbleiben, wenn dem überwiegende Geheimhaltungsinteressen gemäss Art. 9 DSG entgegenstehen. Eine Einschränkung der Auskunftspflicht müsste entsprechend begründet werden.
Eine private Person, die mit öffentlichen Aufgaben des Bundes betraut ist, wird im datenschutzrechtlichen Bereich als Bundesorgan betrachtet. Sie hat einem Gesuchsteller alle über ihn in der Datensammlung vorhandenen Daten mitzuteilen. Wenn zusätzlich auch die Herkunft der Daten und damit die Adresse von Auftragnehmern verlangt wird, sind diese wenn möglich bekanntzugeben. Die betroffene Person hat nämlich ein berechtigtes Interesse, ihre unrichtigen Daten auch bei Dritten berichtigen zu können. Aus diesen Gründen haben wir der Inhaberin der Datensammlung empfohlen, jenen Personen, über die unrichtige Daten bearbeitet wurden und welche die Herkunft der Daten verlangten, die Adresse (allenfalls nach vorgängiger Orientierung) der Firma bekanntzugeben, damit eine notwendige Berichtigung der Daten an den entsprechenden Stellen verlangt werden konnte. Falls die Herkunft der Daten nicht bekanntgegeben werden kann (z.B. unbekannte Quelle), muss die private Person selbst den betroffenen Personen zusichern, für die Berichtigung der unrichtigen Daten zu sorgen.
Mit den beiden obgenannten Varianten über die Berichtigung von falschen Daten (durch die betroffene Person selbst oder durch die Inhaberin der Datensammlung) kann die aus mangelhafter Information erzeugte Verunsicherung über die Herkunft und Richtigkeit der Daten beseitigt werden.

5.2. Das Recht auf Auskunft und das Register der Datensammlungen

Wer über die Bearbeitung seiner Daten Auskunft geltend machen will, muss dies vom Inhaber der Datensammlung verlangen. Hingegen erstellt und führt der EDSB ein öffentliches Register von Datensammlungen, die von Bundesorganen oder privaten Personen bearbeitet werden. Daraus ersichtlich sind jedoch nur Kategorien von Personendaten und keine persönlichen Angaben.

Der Eidgenössische Datenschutzbeauftragte erhält immer wieder Anfragen von privaten Personen, die Auskunft über ihre persönlichen Daten geltend machen. Diese

Anfragen können von uns nicht beantwortet werden, da der EDSB nur ein Register mit Kategorien von Datensammlungen ohne persönlichen Daten führt und deshalb keine Auskunft über den Inhalt geben kann.
Die ersten vier Bände des Registers des EDSB wurden 1996 publiziert und beinhalten Datensammlungen:

- des Eidgenössischen Departementes des Innern (A1);
- des Eidgenössischen Finanzdepartements und der Schweizerischen Nationalbank (A2);
- von Sozialversicherungen (A3);
- sowie Privatpersonen (B1).

Im 1997 wurden zwei weitere Bände publiziert (siehe dazu Seite 78).

Den anfragenden Personen wird regelmässig geraten, sich direkt an den Inhaber der sie interessierenden Datensammlung zu wenden. Sofern dies ein Bundesorgan oder eine private Person ist, kann diesfalls das Auskunftsrecht gemäss Art. 8 DSG geltend gemacht werden. Dazu hat die betroffene Person ein Gesuch um Auskunftserteilung einzureichen und sich dabei über ihre Identität (zum Beispiel Kopie von ID oder Pass) auszuweisen. In der Folge muss ihr der Inhaber der Datensammlung alle über sie vorhandenen Daten, gegebenenfalls die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger mitteilen. Die Auskunft oder der begründete Entscheid über die Beschränkung des Auskunftsrechts hat innert 30 Tagen grundsätzlich kostenlos zu erfolgen. Kann die Frist nicht eingehalten werden, hat der Inhaber der Datensammlung die anfragende Person zu benachrichtigen und ihr die Frist mitzuteilen, in der die Auskunft erfolgen wird. Normalerweise erfolgt die Mitteilung in Form eines Ausdrucks oder einer Fotokopie der betreffenden Dokumente.
Das Register dient auch als Kontrollinstrument und kann von jeder Person konsultiert werden, um erhaltene Auskünfte der Inhaber von Datensammlungen zu überprüfen.
Falls jemand sein Auskunftsrecht bei einer kantonalen Behörde geltend machen möchte, hat er sich direkt an die zuständige kantonale Stelle zu wenden.

5.3. Juristische Personen und das DSG

Private Personen, die Personendaten bearbeiten werden vom Geltungsbereich des DSG erfasst. Unter privaten Personen werden sowohl natürliche als auch juristische Personen verstanden. Zu den juristischen Personen gehören z.B. Aktiengesellschaften, Gesellschaften mit beschränkter Haftung, Genossenschaften, Stiftungen, Anstalten sowie Körperschaften.

Eine private Person reichte bei einer Stiftung ein Gesuch um Auskunftserteilung gemäss Art. 8 DSG ein. Das Gesuch wurde nicht beantwortet, weil davon ausgegangen wurde, dass die Stiftung vom DSG nicht erfasst werde.
Private Personen, die Personendaten bearbeiten, werden grundsätzlich vom DSG erfasst. Es ist jedoch nicht immer einfach, zu entscheiden, ob die datenbearbeitende Person als private Person oder als Bundesorgan einzustufen ist. Der Gesetzgeber hat als entscheidendes Kriterium die rechtliche Natur der Tätigkeit, welche der Datenbearbeitung zugrunde liegt, herangezogen. Von Fall zu Fall muss abgeklärt werden, ob eine Tätigkeit auf privatem oder öffentlichem Recht beruht. Eine Stiftung, welche die laufenden Geschäfte tätigt und dabei Miet- Arbeits- und Kaufverträge abschliesst, ist unseres Erachtens eine privatrechtliche Stiftung im Sinne des Zivilge-

setzbuches und damit eine juristische Person, die vom Geltungsbereich des DSG erfasst wird. Daher muss sie gewährleisten, dass sie ihre Auskunftspflicht erfüllt.
Wenn die Auskunft verweigert wird, besteht die Möglichkeit gegen die juristische Person eine Klage zur Durchsetzung des Auskunftsrechts einzureichen (Art. 15 DSG).

5.4. Umsetzung der Anforderungen des DSG bei der Gesetzgebung

Gemäss DSG müssen für bestehende Datensammlungen mit besonders schützenswerten Personendaten oder Persönlichkeitsprofilen bis zum 1. Juli 1998 formellgesetzliche Grundlagen geschaffen oder angepasst werden. In einem Rundschreiben haben wir die Departemente und Bundesämter nochmals an diese Pendenz erinnert.

Ergänzend haben wir sie auch auf unser in VPB 60.77 publiziertes Gutachten hingewiesen (vgl. auch unseren 3. Tätigkeitsbericht 1995/96 S. 64 f.) und ihnen die dort abgedruckte Checkliste beigelegt. Diese findet sich überdies im Anhang zu diesem Bericht (S. 103).

Logarithmus

5.5. Outsourcing als Beispiel eines Konfliktes zwischen Datenschutzrecht und vertraglichen Bestimmungen

Bei Unternehmen der EDV-Branche ist uns aufgefallen, dass in Verträgen oft die zwingenden Vorgaben des Datenschutzes nicht berücksichtigt oder sogar wegbedungen wurden.

Auch Privatfirmen müssen gemäss den Vorgaben des Bundesgesetzes über den Datenschutz (DSG) die notwendigen Datensicherheitsmassnahmen umsetzen. In Outsourcing-Verträgen soll z. B. nicht nur festgehalten werden, dass ein Zugriff auf die Daten der ausgegliederten Mitarbeiter für die Outsourcingfirma untersagt ist. Es ist auch Vorschrift, dass man die notwendigen technischen Vorkehrungen trifft, damit z. B. ein Zugriff auf die Daten gar nicht möglich ist. Sollte es aufgrund der Aufgabenerfüllung notwendig sein, auf die Daten zuzugreifen, so ist z. B. dafür zu sorgen, dass die Daten durch die Mitarbeiter der Outsourcingfirma nicht interpretiert werden können. Auch die Nachvollziehbarkeit der Datenbearbeitung durch die Outsourcingfirma wird für den Auftraggeber von Interesse sein. Er ist es, der gemäss den Vorschriften des Datenschutzgesetzes für die Datenbearbeitung verantwortlich ist. Gemäss Art. 14 DSG darf das Bearbeiten von Personendaten einem Dritten übertragen werden, wenn der Auftraggeber dafür sorgt, dass er die Daten nur so bearbeitet, wie er es selbst tun dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.
Kann bei einem Produkt durch technische Massnahmen ein Zugreifen auf die Kundendaten oder die Interpretierbarkeit der Daten (für Unberechtigte) verunmöglicht werden, so steigt die Qualität des Produkts erheblich. Damit erfüllt man die Forderungen des Datenschutzes und stellt den Kunden erst noch ein besseres und zweckmässigeres Produkt zur Verfügung.

6. Datenschutz und Datensicherheit

6.1. Datensicherheit in der Bundesverwaltung

In der Folge wird beschrieben, wie in der Bundesverwaltung die Datensicherheitsmassnahmen, die sich aus dem Datenschutz ableiten, umgesetzt werden und in welchen Bereichen nach wie vor Differenzen bestehen.

In der Bundesverwaltung geht man heute bei der Datensicherung von drei Schutzstufen aus. Bei der Schutzstufe 1 sind die Datensicherheitsmassnahmen minimal, bei der Stufe 3 maximal zu gestalten. Aus der Sicht des Datenschutzes sind die Schutzstufen wie folgt festgehalten:
Stufe 1: Personenbezogene Daten, deren Missbrauch keine besondere Beeinträchtigung erwarten lässt, sowie Personendaten, welche der Öffentlichkeit frei zugänglich sind; z. B. Adressangaben (Name, Vorname, Anschrift, Geburtsdatum), sofern sie neutral sind und nicht in einem sensiblen Zusammenhang stehen.
Stufe 2: Personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann; z. B. Daten über Mietverhältnisse, Daten über Geschäftsbeziehungen.
Stufe 3: Personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen kann, bzw. die einem besonderen Amtsgeheimnis unterliegen, z. B.

Patientenkarteien, Personaldaten sowie besonders schützenswerte Personendaten oder Persönlichkeitsprofile;
bzw. Personenbezogene Daten, deren Missbrauch für den Betroffenen Gefahren für Leib und Leben bedeuten, z. B. Adressen von Zeugen in bestimmten Strafverfahren.
Die Stufe 1 wird durch den Grundschutz aus der Sicht des Datenschutzes zum grössten Teil abgedeckt. Es ist die Aufgabe der jeweiligen Organisationseinheit, die Grundschutzmassnahmen selbständig umzusetzen. Bei den Schutzstufen zwei und drei sind die Schutzobjekte durch den Sicherheitsbeauftragten der Departemente oder Ämter bei der Sektion Informatiksicherheit des Bundesamtes für Informatik zur begleiteten Risikobeurteilung anzumelden. Im Handbuch Nr. 1 zur Weisung Informatiksicherheit Nr. S02 ist ein Gesamtmassnahmenkatalog aufgeführt, der es erlaubt, aufgrund der jeweiligen Schutzstufen, die notwendigen Massnahmen zu erkennen und umzusetzen. Zusätzlich werden dem Eidg. Datenschutzbeauftragten die Projektanträge der EDV-Projekte zugestellt, die innerhalb der Bundesverwaltung realisiert werden sollen. Je nach Sensitivität der jeweiligen Projekte, werden diese von Mitarbeitern des Eidg. Datenschutzbeauftragten mehr oder weniger stark in der Planungs-, Entwicklungs- und Betriebsphase begleitet bzw. aus der Sicht des Datenschutzes analysiert. Die oben aufgeführten Aspekte haben uns im Umfeld des Datenschutzes und der Datensicherheit schon ein rechtes Stück weiter gebracht. Allerdings müssen wir auch immer wieder feststellen, dass es in der Bundesverwaltung kaum möglich ist, auf eine angemessene Umsetzung der Datensicherheit hinzuarbeiten, wenn man nicht die notwendigen Mittel und/oder ausreichende rechtliche Grundlagen hat, um die Datensicherheit und damit auch einen Teil des Datenschutzes durchsetzen zu können.
Nach wie vor müssen wir in den Planungsphasen von Projekten feststellen, dass insbesondere die Abläufe (Ist/Soll) nicht oder nur ungenügend dokumentiert werden. In der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) wird in Art. 21 festgehalten, dass die Organisation der jeweiligen Bundesorgane dokumentiert werden muss. Im Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes wird zusätzlich konkretisiert, dass die Dokumentation der Organisation (Aufbau- und Ablauforganisation) um so detaillierter festgehalten werden muss, je sensitiver das jeweilige System aus Sicht des Datenschutzes ist. Bereits im 1. Tätigkeitsbericht von 1993/94 (S. 67) haben wir dies festgehalten. Bei ungenügender Systemdokumentation kann man nicht von einem transparenten System sprechen. Denn ein solches System ist weder datenschutzkonform, noch überschaubar und mit grosser Wahrscheinlichkeit auch nur durch langjährige Angestellte durchschaubar.
Aufgrund der obigen Überlegungen sowie aus der Sicht des Datenschutzes ist die nötige Transparenz zu fordern.

6.2. Schlüsselhinterlegung

Immer häufiger werden Daten verschlüsselt, so dass sie durch Dritte nicht mehr interpretiert werden können. Mit dem z. T. von Kontrollorganen geforderten Chiffrierverbot oder der Schlüsselhinterlegung lassen sich die für Ermittlungsbehörden auftauchenden Probleme jedoch nicht abschliessend lösen.

Privatpersonen, Betriebe und die öffentliche Verwaltung streben an, dass ihre Daten vertraulich, integer und verbindlich bearbeitet werden. Deshalb werden immer häufiger gute Chiffrierverfahren bei der automatisierten Bearbeitung von Informationen eingesetzt. Ein gewisser Nachteil bei der Chiffrierung besteht heute noch darin, dass

nicht für alle plattformübergreifenden EDV-Systeme Verschlüsselungsverfahren eingesetzt werden können und dass dazu zusätzliche Ressourcen (Kosten, Rechnerleistung) benötigt werden. Bedenkt man allerdings, wie hoch normalerweise die Wertschöpfung aus den bearbeiteten (sensitiven) Daten ist, so sind die zusätzlichen Aufwendungen der Organisationseinheiten für die Datensicherung eine lohnende Investition.

Aus Sicht von Ermittlungsbehörden wird z. T. argumentiert, dass die Datenchiffrierung ein Hindernis bei den Ermittlungen darstelle, weil die Informationen, welche von den Behörden allenfalls abgehört bzw. aufgezeichnet werden dürfen, von diesen nicht mehr oder nur mit sehr hohem Aufwand interpretiert werden können. Ein möglicher Lösungsansatz wäre die Schlüsselhinterlegung bei Kontrollorganen, so dass man die übertragenen Daten bei der Abhörung interpretieren könnte. Einerseits wird argumentiert, dass ein solches Vorgehen die Verbrechensbekämpfung verbessert. Andererseits wird dadurch das Grundrecht auf informationelle Selbstbestimmung jedes einzelnen beeinträchtigt. Wir bezweifeln, ob der Zugang zu verschlüsselten Daten die Effizienz der Verbrechensbekämpfung verbessern wird. Bestehen Dechiffrierungsmöglichkeiten für Kontrollinstanzen, so muss man davon ausgehen, dass kriminelle Organisationen ihre Informationen nicht mehr über diese unsicheren Kanäle bekanntgeben oder wie heute Begriffe verwenden, die für sie eine andere, als die herkömmliche Bedeutung haben. Dies würde solche Organisationen zwingen, neben den bereits bekannten Möglichkeiten andere Verfahren oder Sachmittel einzusetzen, um die Informationen schnell und sicher auszutauschen. Solche Möglichkeiten bestehen schon heute, indem man z. B. Bits von einem Bitmap (grafischer Aufbau eines Dokuments am Bildschirm) oder einer Audiodatei durch Informationen in Textform ersetzt, welche die Darstellung am Bildschirm nicht oder nur in dem Umfang verändert, dass diese Abweichungen für Dritte nicht erkennbar sind. Diese Technik wird als Steganographie bezeichnet. Das Wort stammt aus dem Griechischen und bedeutet nichts anderes als verstecktes Zeichnen oder Schreiben. Eine andere Möglichkeit der Dateneinsichtnahme für Ermittlungsbehörden würde darin bestehen, dass die Informationen durch diese bei der speichernden bzw. empfangenden Stelle eingesehen werden. Die Schlüsselverwaltung sollte dann allerdings so gestaltet werden, dass die Prozedur der Datenentschlüsselung transparent gestaltet wird.

Unseres Erachtens ist es äusserst zweifelhaft, ob ein Chiffrierverbot oder die Schlüssel-hinterlegung bei Kontrollinstanzen die notwendige Effektivität bei der Verbrechensbekämpfung gewährleisten würde.

Verschlüsselungsbild

6.3. Online-Registrierung von Software

Am Beispiel eines Softwareproduktes haben wir die mit der Online-Registrierung verbundene Datenbearbeitung vertieft untersucht und sind zum Schluss gekommen, dass die dafür nötige Einwilligung durch den Kunden ungenügend ist.

Eine Anzahl Softwareprodukte bietet die Möglichkeit der Online-Registrierung anstelle der Registrierung auf dem Postweg. Wir wurden von Dritten darauf aufmerksam gemacht, dass bei der Online-Registrierung ohne bzw. ohne genügende Kenntnisnahme Daten vom PC des Kunden zur Herstellerfirma übertragen würden.
Neben der Seriennummer des Produktes, Name und Adresse des Kunden können auch automatisch ermittelte Angaben über die Hardware- und Softwareausstattung des Rechners übertragen werden. Letztere Daten sind für die Registrierung der Software nicht notwendig; sie dienen dem Hersteller dazu, das Marketing gezielter auf die Kunden auszurichten.
Für teilweise geäusserte Vermutungen, es würden im Zusammenhang mit der Online-Registrierung weitere Daten vom Rechner des Kunden erfasst als angegeben, haben wir keinerlei Anhaltspunkte. Dies ist jedoch nicht völlig auszuschliessen.
Die Einwilligung des Kunden setzt voraus, dass er in einer *für ihn verständlichen Art und Weise* darüber informiert wird, welche Daten zu welchen Zwecken auf welche Weise bearbeitet werden. Beim untersuchten Produkt stellten wir eine ungenügende Einwilligung fest. Bereits *vor der ersten Maske zur Dateneingabe* sind insbesondere folgende Informationen unübersehbar zu erteilen: Zweck der Datenbearbeitung; Daten, die erfasst bzw. von der Übermittlung ausgeschlossen werden können; Ort der Speicherung und Weiterleitung ins Ausland; Information über das Auskunftsrecht.
Die Herstellerfirma hat sich bereit erklärt, unseren Forderungen bezüglich verbesserter Kenntnisnahme in naher Zukunft zu entsprechen.

7. Verschiedenes

7.1. Handel mit Daten aus dem Handelsregister

Daten aus dem Handelsregister sind grundsätzlich öffentliche Personendaten, die nicht beliebig zu privaten Zwecken verwendet werden dürfen. Durch die elektronische Datenverarbeitung werden innert Kürze verschiedene Informationen miteinander verknüpfbar, die nicht mit dem ursprünglichen Erhebungszweck übereinstimmen.

Eine private Person wollte die Handelsregisterdaten des Schweizerischen Handelsamtsblatt «einscannen» und auf Anfrage Informationen bekanntgeben. Durch die private Bearbeitung von Personendaten aus dem Handelsregister würden sogenannte öffentliche Daten aus dem spezifischen Sachzusammenhang des öffentlichen Registers genommen und entsprechend aufbereitet. Dabei könnten Kundenwünsche berücksichtigt werden, womit aus ursprünglich relativ einfachen Handelsregisterdaten aufschlussreichere Informationen gewonnen werden könnten. Dank den vielfältigen und sehr weitgehenden Such- und Selektionsmöglichkeiten der elektronischen Datenbearbeitung wären somit Zusatzangaben möglich, welche aus dem öffentlichen Register indes nicht ohne weiteres ersichtlich sind. Dadurch steigt das Risiko einer Persönlichkeitsverletzung der Betroffenen erheblich.
Ob Zusammenstellungen von Personendaten (z.B. neu gegründete Firmen, Firmeninhaber oder Statutenänderungen) durch Private zulässig sind, ist vom Zweck

des Handelsregisters abhängig. Die Tatsache, dass das Register öffentlichen Charakter hat, bedeutet nicht, dass die Daten unbeschränkt zu privaten Zwecken verwendet werden dürfen. Das Zweckbindungsgebot ist auch auf öffentlich zugängliche Daten anwendbar. Diese dürfen deshalb nicht zu Zwecken, die unvereinbar sind mit denjenigen, für die sie erhoben wurden, an Dritte übermittelt werden. (Grundsatz 2.2 der Empfehlung Nr. R (91)10 des Ministerkomitees des Europarates an die Mitgliedstaaten für die Übermittlung der von öffentlichen Stellen gespeicherten personenbezogenen Daten an Dritte). Bei der Bearbeitung von Personendaten darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzt werden. Falls beim Aufbereiten von Handelsregisterdaten der Grundsatz des Zweckbindungsgebotes verletzt wird, müsste ein Rechtfertigungsgrund vorliegen, damit sie nicht widerrechtlich ist.
Betroffene Personen müssen die Möglichkeit haben, ihr Auskunftsrecht gemäss Art. 8 DSG beim Inhaber der Datensammlung geltend zu machen. Wenn eine betroffene Person die Löschung ihrer Daten verlangt, muss sie ihr gewährt werden.

Ferner besteht beim Eidgenössischen Amt für das Handelsregister ein Projekt, welches die Handelsregisterdaten langfristig dem Publikum auch mittels elektronischer Datenbank zur Verfügung stellen will. Kriterien für das Abrufen werden vom Amt für das Handelsregister ausgearbeitet werden.

7.2. Anforderungen an die Briefcouverts im Postversand (Honorarrechnungen, Zahlungsverkehr)

Wer Briefe verschickt, muss dafür sorgen, dass der Inhalt vertraulich bleibt. Die Qualität der Briefumschläge sowie das Format des Fensters müssen so ausgestaltet sein, dass der Inhalt nicht durch das Fenster oder den Umschlag gelesen werden kann.

Eine private Person hatte von einer mit dem Inkasso beauftragten Stelle eine Kopie einer Honorarrechnung in einem Briefumschlag mit Fenster erhalten. Obwohl das Couvert verschlossen war, konnten diverse Angaben der Rechnung aufgrund der Grösse des Fensters gelesen werden. Insbesondere war ersichtlich wie lange ein Patient beim betreffenden Arzt in Behandlung war, ob eine Überweisung oder Stellvertretung erfolgte, ob Arbeitsunfähigkeit vorlag und die Behandlung weiter geführt oder abgeschlossen wurde. Bei diesen Angaben handelt es sich um Personendaten und teilweise um Gesundheitsdaten welche gemäss dem Datenschutzgesetz als besonders schützenstwert gelten.
Wer Personendaten bearbeitet, muss zudem für die Vertraulichkeit der Daten sorgen und bei der Bekanntgabe sowie beim Transport von Datenträgern verhindern, dass die Daten unbefugt gelesen werden. Damit die Vertraulichkeit der Patientendaten im Zahlungsverkehr gewährleistet werden kann, sind beim Versenden von Honorarrechnungen Couverts ohne Fenster zu verwenden, die keine Informationen über das Behandlungsverhältnis der Patienten offenbaren und das Arztgeheimnis entsprechend sicherstellen.
Die betreffende Inkasso Stelle hat nun angeordnet, Kopien von Honorarrechnungen müssten ausschliesslich in geschlossenen Couverts mit angeschriebener Adresse verschickt werden.
In einen anderen Fall beschwerte sich eine private Person über die mangelhafte Qualität der Briefumschläge von Banken. Unbefugte Dritte konnten aufgrund der durchsichtigen Couverts erkennen, was in ihren Gutschrifts- oder Bela-

stungsanzeigen stand. Nachdem die betroffenen Banken darauf aufmerksam gemacht wurden, werden Couverts verwendet die keine Informationen über den Zahlungsverkehr ihrer Kunden offenbaren und zudem das Bankgeheimnis entsprechend sicherstellen.

IV. INTERNATIONALES

1. Beitritt zur Europaratskonvention über den Datenschutz

Am 13. November 1996 hat der Bundesrat eine Botschaft an das Parlament betreffend den Beitritt der Schweiz zur Konvention des Europarates zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten verabschiedet (siehe BBl 1997 I 717; siehe auch 3. Tätigkeitsbericht, S. 85). Die Konvention war am 1. Oktober 1985 in Kraft getreten und ist bis heute von 17 Mitgliedstaaten des Europarates ratifiziert worden. Der schweizerische Beitritt könnte im Jahr 1997, nach der Annahme des diesbezüglichen Bundesbeschlusses durch das Parlament, erfolgen. In diesem Fall würde die Konvention Anfang 1998 in Kraft treten.

2. Europarat

Die Projektgruppe für Datenschutz ist - zuerst unter schweizerischem, anschliessend unter maltesischem Vorsitz - zweimal zusammengetreten und hat ihre Arbeiten im Zusammenhang mit der Verabschiedung der Empfehlung zum Schutz medizinischer Daten abgeschlossen. Das Ministerkomitee hat die Empfehlung an seiner 584. Sitzung vom 13. Februar 1997 verabschiedet. Die Empfehlung ist auf die Erhebung und automatisierte Bearbeitung medizinischer, einschliesslich genetischer Daten für jegliche Benutzung im öffentlichen und privaten Sektor anwendbar. Die Anforderungen an die Vertraulichkeit wurden durch die folgende Auflage verstärkt: Jede Bearbeitung medizinischer Daten muss grundsätzlich entweder von Berufsleuten aus dem Gesundheitsbereich oder von Personen und Organisationen, die im Auftrag dieser Berufsleute handeln, vorgenommen werden - soweit diese den identischen oder vergleichbaren Regeln der Vertraulichkeit unterstehen. Die Empfehlung regelt insbesondere die Voraussetzungen für die Rechtmässigkeit der Erhebung und Bearbeitung von Daten (einschliesslich der Beachtung der Grundsätze Zweckmässigkeit und Verhältnismässigkeit) und schränkt die Fälle der möglichen Bekanntgabe medizinischer Daten ein. Ferner gewährleistet sie die Rechte der betroffenen Person, insbesondere das Recht auf Information sowie das Auskunftsrecht. Die Empfehlung regelt die Aufbewahrung und Verwendung medizinischer Daten zum Zwecke der wissenschaftlichen Forschung und sieht die Verpflichtung vor, gegen jede unbefugte Bearbeitungsform die geeigneten technischen und organisatorischen Massnahmen zu ergreifen. Im Bereich der genetischen Daten orientiert sich die Empfehlung an die «Bioethik-Konvention», die den Schutz der Menschenrechte und der menschlichen Würde im Bereich der Biologie und der Medizin zum Inhalt hat. Abgesehen von Zwecken der Prävention, Diagnose, Therapie und wissenschaftlichen Forschung sowie von den Bedürfnissen eines Gerichtsverfahrens oder einer strafrechtlichen Untersuchung, die gesetzlich verankert und mit angemessenen Garantien verbunden ist, ist

die Bearbeitung genetischer Daten einzig aus gesundheitlichen Gründen zulässig. Dies schliesst insbesondere die Erhebung und Bearbeitung genetischer Daten zu rein prognostischen, nicht gesundheitlichen Zwecken aus. (Ausnahme: übergeordnete Interessen).
Daneben stehen die Arbeiten der Projektgruppe für Datenschutz für die Verabschiedung einer Empfehlung über den Schutz von Personendaten, die zu statistischen Zwecken erhoben und bearbeitet werden, kurz vor dem Abschluss. Der Textentwurf verstärkt den Schutz und die Vertraulichkeit der zu statistischen Zwecken erhobenen und bearbeiteten Daten und anerkennt gleichzeitig die Bedürfnisse der Statistiker nach einem relativ leichten Rückgriff auf Erhebung und Bearbeitung von Personendaten. Das Dokument ist das Ergebnis einer offenen und konstruktiven Zusammenarbeit zwischen Datenschutzexperten und Statistikern, besonders zwischen dem EDSB und dem Bundesamt für Statistik. Die Empfehlung dürfte noch in diesem Jahr vom Ministerkomitee verabschiedet werden; sie regelt die Erhebung und Bearbeitung von Daten zu statistischen Zwecken und schreibt vor allem strikte Anforderungen an die Grundsätze der Vertraulichkeit, Verhältnismässigkeit und Zweckmässigkeit fest. Zu statistischen Zwecken erhobene und bearbeitete Daten dürfen ausschliesslich für diese Zwecke benutzt werden. Sie dürfen nicht dazu dienen, eine Entscheidung oder Massnahme in bezug auf die betroffene Person zu treffen. Zudem misst die Empfehlung der Transparenz in der Bearbeitung sowie der Information der betroffenen Personen ein grosses Gewicht bei.
Im übrigen hat die Projektgruppe die Prüfung eines Empfehlungsentwurfs im Versicherungswesen aufgenommen. Der Entwurf stammt von der Arbeitsgruppe 14, an der wir uns ebenfalls beteiligt haben.
Schliesslich hat die Arbeitsgruppe 15 über die neuen Informationstechnologien ihre Arbeiten fortgesetzt. Sie soll sich in erster Linie mit den folgenden Aspekten befassen: Datenautobahnen, Chip-Karten, elektronische Überwachung (vor allem Videoüberwachung) und Umgang mit Informationsressourcen.
Der durch die Konvention 108 ins Leben gerufene beratende Ausschuss, der vor allem die Aufgabe hat, Stellungnahmen zur Anwendung der besagten Konvention abzugeben, hielt seine 12. Sitzung ab. Dabei setzte er sich vor dem Hintergrund der aktuellen technologischen Entwicklung insbesondere mit der Relevanz der Definitionen und Grundsätze der Konvention auseinander.

3. Internationale Konferenz der Beauftragten für den Datenschutz

Die XVIII. Internationale Konferenz der Datenschutzbeauftragten fand vom 18. bis am 20. September 1996 auf Einladung des kanadischen Datenschutzbeauftragten in Ottawa, Kanada, statt. An dieser Konferenz trafen die Datenschutzbeauftragten von 23 Staaten mit Regierungsexperten und Vertretern der Europäischen Union, der Informationsindustrie, Wirtschaft, Wissenschaft und des Dienstleistungssektors zusammen. Die Schweiz war durch den Eidgenössischen Datenschutzbeauftragten und den Datenschutzbeauftragten des Kantons Zürich vertreten. Die Konferenz bot Gelegenheit für einen Informationsaustausch über die jüngsten Entwicklungen im Datenschutz, vor allem über Probleme im Zusammenhang mit der EU-Richtlinie, die den Austausch von personenbezogenen Informationen zwischen den Ländern der Europäischen Union und Drittstaaten zum Inhalt hat. Unter dem Motto «grenzüberschreitender Persönlichkeitsschutz» befassten sich die Konferenzteilnehmer mit den Folgen des sich ausweitenden internationalen Informations- und Datenverkehrs. Auch in diesen Bereichen gilt es, den Schutz der Persönlichkeit und der Grundrechte

von Personen, über die Daten bearbeitet werden, zu garantieren. Der unaufhaltsame Einzug elektronischer Dienste und Informationsnetze (Datenautobahnen) in öffentliche Verwaltungen, private Unternehmen und Privathaushalte machen die Datenschutz-Prinzipien wichtiger denn je. Angesichts der Entwicklung hin zum «global village» müssen die Information der Bürger bzw. Verbraucher verstärkt, datenschutzrechtliche Verhaltenskodizes entwickelt und neue rechtliche wie technische Lösungen gefunden werden. Solche Instrumente sollten vor allem erarbeitet werden, um das Datenschutzdefizit beim Informationsaustausch zwischen Staaten mit Datenschutzgesetzen und solchen ohne angemessenen Schutz (z.B. die USA) auszugleichen. Ohne echtes Problembewusstsein auf allen Ebenen könnte die gegenwärtige Entwicklung das Ende der Privatsphäre bedeuten. Dies wurde an der Konferenz mit zahlreichen Beispielen veranschaulicht: Verwendung von Kreditkarten, Schaffung von Mega-Datenbanken dank Zugriff auf das Internet, grenzüberschreitende Informationsflüsse zwischen Europa und den Vereinigten Staaten, Reservierungssysteme wie Galileo oder Amadeus, Multimedia wie interaktives Fernsehen oder E-Mail (Problem der Anonymität und der Vertraulichkeit). Ferner wurden die Themen Personenidentifizierung (z.B. bei der Verwendung von Kreditkarten), Bearbeitung von Gesundheitsdaten, Expansion der Gesundheitskarten, genetische Daten und Überwachung von Drogenabhängigen angesprochen. Schliesslich wurde die Notwendigkeit betont, die Bearbeitung von Personendaten einzuschränken und die Massnahmen hinsichtlich Ethik und Vertraulichkeit medizinischer Daten zu verstärken.

4. Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation

Ziel der oben erwähnten Gruppe ist es, den Datenschutz im Bereich der Telekommunikation und der Medien zu verbessern. Die 20. Sitzung der Arbeitsgruppe fand am 18. und 19. November 1996 unter dem Vorsitz des Berliner Datenschutzbeauftragten in Berlin statt.
Das bereits in früheren Tagungen diskutierte Memorandum zum Datenschutz und der Privatsphäre im Internet wurde bereinigt und verabschiedet. Der Text ist auf Seite 93 dieses Berichtes zu finden. Weiter wurden unter anderem folgende Themen in Referaten behandelt und diskutiert: Systeme zur Bewertung und Ausfilterung bestimmter Internetangebote, Zugriff auf medizinische Daten via Internet, die Frage der Verschlüsselung, Electronic Cash, internationale Transport und Reservationssysteme sowie die künftige Kooperation der Arbeitsgruppe mit anderen Gremien.
Im Bereich der Telekommunikation sind nur grenzüberschreitende Lösungen sinnvoll. Die internationale Zusammenarbeit der Datenschutzstellen ist daher besonders wichtig.

5. Bilaterale und multilaterale Abkommen über die Rückübernahme und Durchbeförderung von ehemaligen Kriegsflüchtlingen

Mit der erhofften Rückkehr zur Normalität stellt sich auch die Frage der Rück- und Durchführung über fremdes Territorium der ehemaligen Kriegsflüchtlinge in ihre Heimat. In den entsprechenden Abkommen der Schweiz und anderer Staaten mit Kroatien und mit Jugoslawien wird auch der Datenschutz geregelt. Es stellt sich die Frage, ob diese Bestimmungen von den ehemaligen Kriegsparteien richtig umgesetzt werden und ob die Umsetzung kontrolliert wird.

PC-Einbrecher

Betreffend Kroatien wurden uns gleich drei Abkommen zur Stellungnahme unterbreitet, nämlich ein (bilaterales) Abkommen über die *Rückführung* sowie ein bilaterales und ein multilaterales Abkommen über die *Durchführung* von Personen durch Kroatien. Das Rückführungsabkommen stellt eine Ergänzung (Protokoll) zu einem Abkommen vom 8./9. Februar 1993 (SR 0.142.112.912) dar und regelt den Datenschutz nicht bzw. ungenügend. Wir haben eine Nachbesserung gemäss dem schweizerischen und europäischen Standard verlangt, welche uns auf einen späteren Termin, spätestens aber bis in zwei Jahren zugesichert wurde. Die beiden Durchbeförderungsabkommen regeln den Datenschutz gemäss schweizerischem und europäischem Standard. Mit Blick auf die konkreten Verhältnisse haben wir die Frage aufgeworfen, ob diese Datenschutzbestimmungen auch wirklich umgesetzt werden und ob (etwa im Rahmen der Umsetzung des sog. Dayton-Abkommens) gewisse minimale Kontrollmechanismen vorgesehen sind. Hier besteht bis zu einer vollständigen Normalisierung der Verhältnisse Handlungsbedarf. Unseres Erachtens müssen die auf den vorzuweisenden Sichtvermerken aufgeführten Personendaten beschränkt werden (z.B. strikte Entfernung von Angaben, welche auf die Ethnie hinweisen etc.).
Als ermutigend darf der Umstand bezeichnet werden, dass sich Kroatien nun ebenfalls ein Datenschutzgesetz gegeben hat. Über kein Datenschutzgesetz verfügt derzeit indessen die Bundesrepublik Jugoslawien. Auch wenn das uns ebenfalls zur Stellungnahme unterbreitete Rückführungs- und Rückübernahmeabkommen dem schweizerischen und europäischen Standard entspricht, stellen sich daher in verstärktem Mass die Fragen nach der Umsetzung des vereinbarten Datenschutz-Standards und nach der Kontrolle.

6. Die Aufnahme einer Datenschutzklausel in das Vierseitige Übereinkommen (A, CH, D, FL) im Bereich der Sozialen Sicherheit

Deutschland stellte den Antrag, neu eine Datenschutzklausel in das Zweite Zusatzabkommen zum Vierseitigen Übereinkommen im Bereich der Sozialen Sicherheit aufzunehmen. Wir begrüssten diesen Vorschlag, entspricht doch dessen Inhalt im wesentlichen dem DSG sowie den international gültigen datenschutzrechtlichen Mindeststandards.

Im Dezember 1996 fanden in Bern Besprechungen zwischen Vertretern Deutschlands, Liechtensteins, Österreichs und der Schweiz betreffend die Aufnahme einer Datenschutzklausel in das erwähnte Übereinkommen statt. Im Rahmen dieser Besprechungen wurden wir von der schweizerischen Delegation (Bundesamt für Sozialversicherung) eingeladen, dazu Stellung zu nehmen.
Wir bewerteten die von Deutschland vorgeschlagene Datenschutzklausel positiv. Dies vor allem deshalb, damit die in der Klausel aufgeführten datenschutzrechtlichen Grundsätze (Zweckbindungsgebot, Verhältnismässigkeit, Auskunftsrecht etc.) für die Behörden sowie für die betroffenen Personen transparent gemacht werden. Einerseits soll die Klausel den Behörden als Leitlinie dienen und andererseits sollen die Bürger, die unter das Übereinkommen fallen, über die Bearbeitung ihrer Daten hinreichend informiert werden.
Zudem enthält die Datenschutzklausel im wesentlichen die international gültigen datenschutzrechtlichen Mindeststandards und bedeutet auch für die Schweiz nichts Neues bzw. ist mit dem Inhalt des schweizerischen Datenschutzgesetzes praktisch identisch. Sie stellt also für die schweizer Behörden hinsichtlich der Datenbearbei-

tung grundsätzlich keine materiellen Änderungen dar, zumal sie nur dann zur Anwendung kommt, wenn das innerstaatliche Recht keine Regelung vorsieht (subsidiärer Charakter der Klausel).
Die Delegationen Liechtensteins, Österreichs und der Schweiz sind zur Zeit daran, den deutschen Vorschlag nochmals zu überprüfen. Wann und inwiefern die Datenschutzklausel in das Übereinkommen aufgenommen wird, ist noch offen.

V. REGISTER DER DATENSAMMLUNGEN (DATAREG)

1. Verwaltungssystem des Registers der Datensammlungen

Nachdem das Verwaltungssystem des Registers der Datensammlungen gut zwei Jahre in Betrieb ist, können anhand der aufgenommenen Registereinträge Aussagen zu Ausprägungen und Eigenschaften der Einträge gemacht werden.

Während 1994 im Zeichen der offiziellen Inbetriebnahme von DATAREG stand, wurden im 1995 Optimierungen am System vorgenommen. Im Jahre 1996 schliesslich lief das System mit voller Verfügbarkeit.
Um auch dieses Jahr einen Eindruck über die Eigenschaften und Ausprägungen der registrierten Datensammlungen geben zu können, wurden hier einige Zahlen zu DATAREG zusammengestellt. Die nachfolgenden Ausführungen und Kennzahlen beziehen sich auf den Stand Januar 1997 des Registers.
Es sind insgesamt 1480 Datensammlungen registriert. 33 Einträge zu Datensammlungen wurden bereits auf Antrag der anmeldenden Stelle gelöscht. 1143 Einträge sind von Bundesorganen, 337 von Privaten. Von den 1480 Registereinträgen sollen bis auf 38 alle publiziert werden.
Als Kategorien der bearbeiteten Personendaten sind bis jetzt 1209 Kategorien für die verschiedenen Registereinträge als bearbeitete Personendaten aufgenommen. Diese Kategorien werden von den Einträgen 9128 mal verwendet. Es werden also pro Datensammlung durchschnittlich 6 Kategorien von Personendaten gemeldet. Die Hitliste der Kategorien von bearbeiteten Personendaten wird angeführt von Adresse, Beruf, Identität, Nationalität/Heimatort, Arbeitsort, Sprachen vor AHV-Nummer, Ausbildung, Familie, Gesundheit und Einkommen.
Als Kategorien der Datenempfänger und der an der Datensammlung Beteiligten sind 862 aufgenommen, welche 2616 mal als Empfänger sowie 636 mal als Beteiligte aufgeführt werden.
Bei den Einträgen für Bundesorgane werden bis jetzt 504 verschiedene Rechtsgrundlagen genannt. Diese werden 1330 mal verwendet.
Bisher wurden 1227 Adressen der anmeldenden Stellen in das System aufgenommen. Für die Einträge von Privaten wurden bis jetzt 55 Branchenkategorien vergeben.

2. Publikation des Registers der Datensammlungen

1996 wurde das Register der Datensammlungen erstmals seit dem Inkrafttreten des Datenschutzgesetzes veröffentlicht. Dies erfolgte in einem Band für Datensammlungen von Privatpersonen, aufgeteilt in 33 Branchen. Die Publikation für Bundesorgane wurde in drei Bände aufgeteilt. Die Register sind bei der Eidgenössischen Drucksachen- und Materialzentrale erhältlich.

1996 wurde das Register der Datensammlungen zum ersten Mal veröffentlicht. Das Register wurde mit Stand März 96 publiziert und anlässlich der Pressekonferenz des EDSB vorgestellt.
Als Vorarbeit zur Veröffentlichung galt es, die Form, den Inhalt und die Aufteilung des Registers festzulegen. Schon bald war man sich einig, dass es eine getrennte Publikation für Bundesorgane und Privatpersonen geben soll.
Der Inhalt des Registers umfasst für Bundesorgane: die Bezeichnung und Registernummer der Datensammlung, den Kreis der betroffenen Personen, die ungefähre Anzahl der betroffenen Personen, den Zweck der Datensammlung, die Rechtsgrundlage, den Inhaber der Datensammlung, die Auskunftserteilung, die Kategorien der bearbeiteten Personendaten, die Kategorien der Datenempfänger und die Kategorien der Beteiligten.
Der Inhalt des Registers umfasst für Privatpersonen: die Bezeichnung und Registernummer der Datensammlung, den Zweck der Datensammlung, den Inhaber der Datensammlung, die Auskunftserteilung, die Kategorien der bearbeiteten Personendaten, die Kategorien der Datenempfänger und die Kategorien der Beteiligten.
Ein Band umfasst alle Einträge von Privatpersonen (Band B1). Dieses Register beinhaltet 337 Einträge zu Datensammlungen auf 33 Branchen verteilt. Die Branchen sind alphabetisch geordnet, und innerhalb der Branchen sind die Einträge nach den Inhabern der Datensammlungen ebenfalls alphabetisch gegliedert.
Für die Bundesorgane wurden bisher drei Bände veröffentlicht. Der Band A1 enthält die Angaben zu den Datensammlungen des Eidgenössischen Departements des Innern, A2 zu den Datensammlungen des Eidgenössischen Finanzdepartements und der Schweizerischen Nationalbank, A3 zu den Datensammlungen der Sozialversicherungen.
Diese Register beinhalten rund 600 ordentliche Einträge und rund 150 vereinfachte Einträge. Die Einträge sind nach Departementen und innerhalb der Departemente nach ordentlichen und vereinfachten Anmeldungen sowie nach Ämtern gegliedert. Gleichzeitig mit der Veröffentlichung des vorliegenden Berichtes sind die Bände A4 und A5 erschienen welche Datensammlungen von Bundesbehörden beinhalten (Stand 28. Februar 1997).
Band A4 beinhaltet Datensammlungen der Bundeskanzlei, der Bundesversammlung, des Eidg. Departementes für auswärtige Angelegenheiten und des Eidg. Justiz- und Polizeidepartementes (ausgenommen Bundesamt für Polizeiwesen).
Band A5 beinhaltet Datensammlungen des Eidg. Volkswirtschaftsdepartements, des Eidg. Verkehrs- und Energiedepartements (ausgenommen PTT und Bundesamt für Kommunikation), des Bundesamtes für Informatik, des Bundesgerichtes und des Eidg. Versicherungsgerichts.

VI. DER EIDGENÖSSISCHE DATENSCHUTZBEAUFTRAGTE

1. Ausstattung des Sekretariats

Dieses Berichtsjahr war für uns ein aussergewöhnliches Jahr. Der rapide Zuwachs der elektronischen Datenbearbeitungen in privaten und öffentlichen Stellen einschliesslich deren Vernetzung machte neue Überlegungen darüber erforderlich, wie unsere Aufgabe in der Zukunft sichergestellt werden kann. Zudem wurden unserem Sekretariat neue Räumlichkeiten ausserhalb der Stadt Bern zugewiesen. Angesichts unserer Aufgaben, welche eine erhöhte Mobilität der Sekretariatsmitarbeiter erfordern (Beratungs- und Kontrollfunktion), hat die Auslagerung nach Zollikofen einen erheblichen Verlust an Arbeitszeit und damit an Arbeitsqualität verursacht. Somit wurde unsere Aufgabenerfüllung zusätzlich erschwert. Viele Gesellschaften oder Privatpersonen, die bei uns um eine Besprechung baten, haben sich anschliessend über die Abgelegenheit der Örtlichkeiten und der schlechten Verbindungen der öffentlichen Verkehrsmittel beschwert.
Drei Mitarbeiter haben im Laufe des Geschäftjahres das Sekretariat verlassen und wurden durch neue Mitarbeiter ersetzt. Zudem wurde eine weitere Stelle für die Bewältigung der Aufgaben des Sekretariats insbesondere für den Bereich der Sozialversicherungen bewilligt.

2. Aufgabenentwicklung

Die Zahl der Anfragen sind in diesem Berichtsjahr erheblich angestiegen. Bei den Rechtsfragen stehen weiterhin die Bereiche Polizei-, Ausländer-, Vesicherungs-, und Gesundheitswesen im Vordergrund. Die Bundesverwaltung stellte vermehrt Anfragen über die Vernetzung von Datenbearbeitungssystemen und über die Weitergabe von Personendaten an Drittstellen. Privatpersonen haben insgesamt mehr von der Möglichkeit Gebrauch gemacht, sich beraten zu lassen. Anfragen über die Geltendmachung des Auskunftsrechts, die Möglichkeiten der Berichtigung und Löschung der Daten bei privat geführten Datensammlungen bildeten die Schwerpunkte.

3. Information der Öffentlichkeit

Vordergründig versuchten wir, den Bürger mit den datenschutzrechtlichen Bestimmungen vertraut zu machen. So haben wir an verschiedenen Informationsveranstaltungen und Konferenzen teilgenommen und unsere Broschüren versendet. Letztere haben eine breite Resonanz in der Bevölkerung gefunden. Aus Spargründen verfügen wir nicht über grössere Auflagen. Da wir nicht über ein eigenes Budget verfügen, sind wir nicht in der Lage, genügend Broschüren nachdrucken zu lassen. Deshalb waren wir oft gezwungen, nur Kopien der Broschüren zu versenden.
In der Zwischenzeit ist auch die Broschüre über die Bearbeitung von Personendaten im medizinischen Bereich erschienen.
Zudem sind wir mit einem eigenen Angebot im INTERNET präsent, welches ermöglicht, Informationen über den Datenschutz auch über das Netz abzurufen.

Eine Auswahl der verschiedenen telefonischen Anfragen, die bei uns eingegangen sind, finden sie in den nachfolgenden Tabellen (vgl. S. 82ff) grafisch dargestellt.

Der EDSB im Internet

Das Internet gibt aus Sicht des Datenschutzes zu manchen kritischen Stellungnahmen Anlass (Siehe Budapest-Berlin Memorandum, Seite 93). Für die aktuelle und günstige Verbreitung unserer Veröffentlichungen ist das Internet jedoch ein ausgezeichnetes Medium.

Um unsere Informationen dem interessierten Publikum rasch und effizient zugänglich zu machen, haben wir uns entschlossen, das Internet als zusätzliches Informationsmedium zu nutzen. Die meisten unserer Publikationen (Leitfäden, Berichte, Empfehlungen, Pressemitteilungen etc.), auch das Datenschutzgesetz mit seinen Verordnungen sowie internationale Datenschutzbestimmungen sind abrufbar. Zusätzlich bieten wir Links auf andere Internetseiten an, die sich mit Datenschutz und Datensicherheit befassen. Es besteht eine Suchmöglichkeit nach Stichworten über alle von uns bereitgestellten Dokumente.

4. Dritte schweizerische Konferenz der Datenschutzbeauftragten (1996)

Nachdem die beiden ersten schweizerischen Datenschutzkonferenzen 1993 und 1995 durch den Eidg. Datenschutzbeauftragten organisiert wurden, fungierte 1996 mit dem Datenschutzbeauftragten des Kantons Zürich erstmals ein Kanton als Gastgeber der Konferenz.
Unter anderen wurden folgende Themen behandelt: Verwendung der Volkszählungsdaten für Verwaltungszwecke, Datenschutz bei erkennungsdienstlichen Unterlagen der Polizei sowie bei der Archivierung.
Schliesslich verabschiedete die von zahlreichen kantonalen Vertretern besuchte Konferenz eine Resolution, in der alle Akteure des Gesundheitswesens aufgefordert werden, dem Persönlichkeitsschutz vermehrt Rechnung zu tragen.
Am 3. Oktober 1996 veranstaltete der Zürcher Datenschutzbeauftragte zusammen mit der ETH Zürich überdies ein vielbeachtetes *Symposium für Datenschutz und Datensicherheit* zum Thema «Vernetzte Informationstechnologie kontra Persönlichkeitsschutz ?»

internet bild

5. Statistik über die Tätigkeit des EDSB

Anzahl der Stellungnahmen

Anzahl der Stellungnahmen

Telefonauskunft

Telefonauskunft nach Anfragenden

Telefonauskunft nach Sachgebieten

6. Das Sekretariat des Eidgenössischen Datenschutzbeauftragten

Eidgenössischer Datenschutzbeauftragter:	**Guntern Odilo, Dr. iur.**
Stellvertreter:	Walter Jean-Philippe, Dr. iur.

Sekretariat:

Leiter:	Walter Jean-Philippe, Dr. iur.
Stellvertreterin:	Grand Carmen, lic. iur.
Delegierter für Information und Presse	Tsiraktsopulos Kosmas, lic. iur.
Rechtsdienst:	9 Personen
Informatikdienst:	4 Personen
Kanzlei:	4 Personen

VII. ANHANG

1. Merkblatt: Sperrung der Verwendung der Adresse zu Werbezwecken

Sperrung der Verwendung der Adresse zu Werbezwecken

Nach dem Bundesgesetz über den Datenschutz ist die Verwendung der Adresse zu Werbezwecken grundsätzlich zulässig, wenn die betroffene Person :
1. ihre Adresse der Öffentlichkeit zugänglich gemacht hat, und
2. die Verwendung für Werbezwecke nicht untersagt hat.

1. **Öffentlich zugänglich** ist die Adresse zum Beispiel,
- wenn sie im Telefonbuch eingetragen ist,
- wenn sie in einem anderem Verzeichnis eingetragen ist (Branchenverzeichnis, von einer privaten Firma oder Vereinigung herausgegebenes Adressbuch usw.)

2. Die **Verwendung der Adresse zu Werbezwecken** kann

*generell **verboten** werden :*	*im Einzelfall **verboten** werden :*
• durch Sperrung der Adresse bei der Telecom (PTT). Dann wird sie im Telefonbuch mit einem * markiert. Entsprechende Formulare finden sich in jedem Telefonbuch. • durch Sperrung der Adresse beim Schweizerischen Verband für Direktmarketing, dem eine Mehrzahl der schweizerischen Direktmarketingfirmen angeschlossen sind. Adresse : SVD, Postfach, 8708 Männedorf	• indem unerwünschte Werbeschriften mit dem Vermerk "Ich untersage die Verwendung meiner Adresse zu Werbezwecken" an den Absender retourniert werden (aus Beweisgründen ist es besser, wenn die Mitteilung der Firma eingeschrieben geschickt wird). • indem jedesmal, wenn die Adresse bekanntgegeben wird (bei Wettbewerben, Bestellungen von Informationsmaterial, Vereinsbeitritten, Spenden, Bestellungen bei Versandhäusern; wenn Kundenkarten, Ra-battkarten usw. ausgefüllt werden), dieser Vermerk angebracht wird.

Da mit Adressen für Werbezwecke in der Schweiz wie auch in anderen Ländern ein schwungvoller Handel getrieben wird, ist es schwierig, jegliche Zustellung von adressierter Werbung zu unterbinden. Eine konsequente Anwendung der aufgelisteten Sperrmöglichkeiten führt aber auf jeden Fall zu einer starken Reduktion der Werbezuschriften.

Gemäss Datenschutzgesetz hat jede Person das Recht, vom Inhaber einer Datensammlung **Auskunft** darüber zu verlangen, ob und welche Daten über sie bearbeitet werden. Einzelheiten zum Auskunftsrecht finden sich im *Leitfaden des Eidgenössischen Datenschutzbeauftragten über die Rechte der betroffenen Personen.*

Um den Leitfaden zu bestellen und weitere Auskünfte zu erhalten, wenden Sie sich an den *Eidgenössischen Datenschutzbeauftragten, 3003 Bern, Tel.: 031/322 43 95*.

2. Richtlinien des Eidg. Personalamtes zur Anwendung von Einzel- und Gruppentestverfahren in der allg. Bundesverwaltung

(vom 6. November 1996)

1. Zweck von Einzel- oder Gruppentestverfahren

Psychometrische Einzel- oder Gruppentestverfahren (wie Leistungs-, Intelligenz- oder Persönlichkeitstest) und andere Persönlichkeits- resp. Leistungsbeurteilungssysteme (wie graphologisches Gutachten, biographischer Fragebogen, Assessment, Assessment-Center) sind Hilfsmittel zur systematischen Einschätzung des aktuellen Potentials von gegenwärtigen oder künftigen Mitarbeiter/innen und/oder der künftigen beruflichen oder persönlichen Entwicklungsmöglichkeiten.

2. Grundsätzliches zum Einsatz von Einzel- oder Gruppentestverfahren in der allgemeinen Bundesverwaltung

2.1 Einzel- oder Gruppentestverfahren sind sehr selektiv anzuwenden.

Das heisst, wenn
- die bereits vorhandenen Daten für die Beurteilung nicht ausreichen,
- die Testpersonen dem oberen Kader angehören,
- es sich um eine Schlüsselstelle handelt oder
- dieselben Verfahren bei wiederkehrend gleichen Beförderungs-, resp. Selektionssituationen für grössere Personengruppen eingesetzt werden können,und sich Aufwand und Ertrag rechtfertigen lassen.

2.2 Die Verwendung psychometrischer und anderer Testverfahren zur Personalförderung und Personalselektion in der allgemeinen Bundesverwaltung liegt in der Kompetenz der Departemente/Bundesämter. Sie tragen die volle Verantwortung für Auswahl, Finanzierung und Einsatz der Testverfahren. Unter Einbezug der vorliegenden Richtlinien haben die Departemente mittels interner Weisung festzulegen, in welchen amtsspezifischen Situationen welche Testverfahren zur Anwendung kommen. Diejenigen Personen, die mit der Testdurchführung betraut werden, sind durch die Amtsdirektion zu bezeichnen. Es ist sicherzustellen, dass sie in der Testanwendung geschult und in der Anwendung professionell begleitet werden durch Psychologen/Psychologinnen (mit FSP[1)] -anerkannter Ausbildung oder IAP[2)] -Diplom), die in der Testanwendung,
-auswertung und -interpretation geschult und erfahren sind (entsprechend qualifizierte Fachpersonen können auch durch den Anbieter gestellt werden).

2.3 Die Beachtung der vorliegenden Richtlinien sichert ein faires und ethisch korrektes Verhalten gegenüber den Testpersonen und die Einhaltung der Datenschutzgesetzgebung.

2.4 Das Eidg. Departement für auswärtige Angelegenheiten erlässt in Anlehnung an die vorliegenden Richtlinien und im Einvernehmen mit dem Eidg. Personalamt interne Richtlinien für das Zulassungsverfahren zum diplomatischen und konsularischen Dienst.

3. Umgang mit Testverfahren

3.1 Es dürfen nur Testverfahren verwendet werden, die **wissenschaftlich geprüft** sind und **professionell durchgeführt** werden.

3.2 Den Anwendungen von Testverfahren müssen eine genaue Analyse des Anforderungsprofils und die Gewichtung dieser Anforderungen vorausgehen. Daraus müssen notwendigerweise die Selektions- resp. Förderkriterien für die derzeitigen und die künftigen Funktionen abgeleitet werden können. Die Testergebnisse wiederum müssen in direktem Bezug stehen zu den Kriterien und aussagekräftig sein.

3.3 Anzahl und Umfang der eingesetzten Testverfahren (inkl. Beurteilung bereits vorhandener Daten) und die zu erwartende Qualität der Ergebnisse müssen der Bedeutung der Stelle resp. der Fördermassnahme angepasst sein. Personeller, finanzieller und zeitlicher Aufwand sind kritisch zu prüfen.

3.4 **Psychometrische oder andere Testverfahren dürfen nie als einziges oder wichtigstes Instrument eingesetzt werden.** Die Durchführung von Einzel- oder Gruppentestverfahren erspart in keinem Fall weder die Auswertung der vorhandenen Bewerbungsunterlagen resp. der bereits bekannten Leistungen noch das persönliche Auswertungs-, Selektions- resp. Fördergespräch oder den zu treffenden Selektions- resp. Förderentscheid.

3.5 Die Testverfahren müssen in den drei Amtssprachen (deutsch, französisch, italienisch) angeboten werden können.

4. Persönlichkeitsschutz

4.1 Die Testperson muss im voraus um ihr **Einverständnis zur Teilnahme am Testverfahren** ersucht werden.

4.2 Die Diskretion muss gewahrt bleiben. Nehmen zwei oder mehrere Personen desselben Bundesamtes/-betriebes an einem Testverfahren teil, und kann die Anonymität nicht mehr gewährleistet werden (z.B. durch die Testanlage in einem Assessment-Center), sind die Testpersonen im voraus über diesen Umstand zu informieren.

4.3 Die getestete Person hat auf ihr Verlangen hin **jederzeit Anspruch auf uneingeschränkte Einsicht** in das gesamte verwendete Testmaterial (wie Fragebogen, Auswertungsskalen, Computeranalysen) und die gesamten Testdaten (wie Testantworten, Testergebnisse, Gesamtbewertungen).

4.4 Die Testverfahren erbringen **keine objektiven Daten**. Die Datenerhebung und -auswertung erfolgt immer aufgrund eines bestimmten Menschen- oder Persönlichkeitsbildes, das dem Testverfahren zugrunde liegt. Die getestete Person muss deshalb **in jedem Fall die Möglichkeit der persönlichen Stellungnahme** zu den Testdaten und deren Interpretation erhalten.

5. Umgang mit Testdaten

5.1 Die Testperson muss im voraus über den Zweck des Testverfahrens und über die Verwendung der Testdaten informiert sein. Das Testverfahren und Testdaten dürfen **zu keinem anderen als dem mit der Testperson vereinbarten Zweck verwendet** werden.

5.2 Sämtliche Testdaten sind durch angemessene technische und organisatorische Massnahmen **gegen unbefugte Einsicht und unbefugtes Bearbeiten zu schützen**. Grundsätzlich dürfen nur die Testperson und die testdurchführende Person Zugang zu den Testanworten und Testergebnissen haben. Entscheidungsbefugten Personen darf nur im konkreten Fall eine aus den Ergebnissen resultierende **Gesamtbewertung** zugänglich gemacht werden.

5.3 Die Testdaten aus Selektionsverfahren sind **nur bis zum Abschluss des Verfahrens aufzubewahren** und der Testperson nach Abschluss des Verfahrens vollständig und im Original auszuhändigen.

Testunterlagen, Testergebnisse oder Gesamtbeurteilungen, die einer internen Potentialerhebung dienen und über das Verfahren hinaus benötigt werden, können im Personaldossier unter Verschluss aufbewahrt werden. Die Testdaten lassen jedoch nur während einer begrenzten Zeit verlässliche Aussagen über das Potential der betroffenen Personen zu. Die Gültigkeit der Testdaten muss deshalb nach längstens zwei Jahren im Gespräch mit der getesteten Person (z.B. im Rahmen der Beurteilungsgespräche) überprüft und das Resultat festgehalten werden (z.B. mit einer Notiz im Beurteilungsblatt).

Von Personen, die nicht eingestellt werden, dürfen keine Testdaten aufbewahrt werden.

5.4 Die Verwendung von Testdaten zu **statistischen Zwecken**, auch durch den Testhersteller oder -vertreiber, darf nur mit Einverständnis der Testperson und in anonymisierter Form stattfinden.

5.5 Im übrigen gilt auch das Rundschreiben des EPA vom 26.01.1984 über den Schutz von Personaldaten in der allgemeinen Bundesverwaltung (C.3028). Zu beachten sind Art. 8 ff. Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (VDSG) und die Publikationen des Eidgenössischen Datenschutzbeauftragten zu diesem Thema, insbesondere der 'Leitfaden für die Bearbeitung von Personendaten in der Bundesverwaltung 1994.

3. Datenschutz im Internet - «Budapest - Berlin Memorandum»

Beim nachfolgenden Text handelt es sich um die Übersetzung des englischen Originaltextes «Data Protection and Privacy on the Internet, Report and Guidance» durch den Berliner Datenschutzbeauftragten.

Datenschutz und Privatsphäre im Internet

Bericht und Empfehlungen

(verabschiedet bei der 20. Sitzung der Internationalen Arbeitsgruppe für Datenschutz in der Telekommunikation in Berlin am 19. November 1996 auf der Basis der Diskussionen der Arbeitsgruppe in Budapest am 15. und 16. April 1996)

"Budapest-Berlin Memorandum"

Zusammenfassung

Es steht außer Zweifel, daß der gesetzliche und technische Datenschutz von Benutzern des Internet gegenwärtig unzureichend ist.

In diesem Dokument werden zehn Prinzipien zur Verbesserung des Datenschutzes im Internet beschrieben:

1. Die Diensteanbieter sollten jeden Benutzer des Internet unaufgefordert über die Risiken für seine Privatsphäre informieren. Der Benutzer wird dann diese Risiken gegen die erwarteten Vorteile abwägen müssen.

2. In vielen Fällen ist die Entscheidung, am Internet teilzunehmen und wie es zu benutzen ist, durch nationales Datenschutzrecht geregelt. Dies bedeutet z.B. daß personenbezogene Daten nur auf eine nachvollziehbare Art und Weise gespeichert werden dürfen. Medizinische und andere besonders sensible personenbezogene Daten sollten nur in verschlüsselter Form über das Internet übertragen oder auf den an das Internet angeschlossenen Computern gespeichert werden. Polizeiliche Steckbriefe und Fahndungsaufrufe sollten nicht im Internet veröffentlicht werden.

3. Initiativen für eine engere internationale Zusammenarbeit, ja sogar für eine internationale Konvention, die den Datenschutz im Zusammenhang mit grenzüberschreitenden Computernetzen und Diensten regelt, sollten unterstützt werden.

4. Es sollte ein internationaler Kontrollmechanismus geschaffen werden, der auf bereits existierenden Strukturen wie der Internet Society und anderer Einrichtungen aufbauen könnte. Die Verantwortung für den Schutz personenbezogener Daten muß in einem gewissen Ausmaß institutionalisiert werden.

5. Nationale und internationale Gesetze sollten unmißverständlich regeln, daß auch der Vorgang der Übermittlung (z. B. durch elektronische Post) vom Post- und Fernmeldegeheimnis geschützt wird.

6. Darüber hinaus ist es notwendig, technische Mittel zur Verbesserung des Datenschutzes der Benutzer auf dem Netz zu entwickeln. Es ist zwingend, Entwurfskriterien für Informations- und Kommunikationstechnologie und Multimedia-Hard- und Software zu entwickeln, die den Benutzer befähigen, die Verwendung seiner personenbezogenen Daten selbst zu kontrollieren. Generell sollten die Benutzer jedenfalls in den Fällen die Möglichkeit haben, auf das Internet ohne Offenlegung ihrer Identität zuzugreifen, in denen personenbezogene Daten nicht erforderlich sind, um eine bestimmte Dienstleistung zu erbringen,.

7. Auch für den Schutz der Vertraulichkeit sollten technische Mittel entwickelt werden. Insbesondere die Nutzung sicherer Verschlüsselungsmethoden muß eine rechtmäßige Möglichkeit für jeden Benutzer des Internet werden und bleiben.

8. Die Arbeitsgruppe würde eine Studie über die Machbarkeit eines neuen Zertifizierungsverfahrens durch die Ausgabe von "Qualitätsstempeln" für Diensteanbieter und Produkte im Hinblick auf ihre Datenschutzfreundlichkeit unterstützen. Diese könnten zu einer verbesserten Transparenz für die Benutzer der Datenautobahn führen.

9. Anonymität ist ein wichtiges zusätzliches Gut für den Datenschutz im Internet. Einschränkungen des Prinzips der Anonymität sollten strikt auf das begrenzt werden, was in einer demokratischen Gesellschaft notwendig ist, ohne jedoch das Prinzip als solches in Frage zu stellen.

10. Schließlich wird es entscheidend sein, herauszufinden, wie Selbstregulierung im Wege einer erweiterten "Netiquette" und datenschutzfreundliche Technologie die Implementierung nationaler und internationaler Regelung über den Datenschutz ergänzen und verbessern können. Es wird nicht ausreichen, sich auf eine dieser Handlungsmöglichkeiten zu beschränken: Sie müssen effektiv kombiniert werden, um zu einer globalen Informations-Infrastruktur zu gelangen, die das Menschenrecht auf Datenschutz und unbeobachtete Kommunikation respektiert.

Bericht

Das Internet ist gegenwärtig das größte internationale Computernetz der Welt. In mehr als 140 Ländern gibt es "Auffahrten" zu dieser "Datenautobahn". Das Internet besteht aus mehr als vier Millionen angeschlossenen Rechnern ("hosts"); mehr als 40 Millionen Benutzer aus aller Welt können wenigstens einen der verschiedenen Internet-Dienste nutzen und haben die Möglichkeit, miteinander durch elektronische Post zu kommunizieren. Die Benutzer haben Zugriff auf einen immensen Informationsbestand, der an verschiedenen Orten in aller Welt gespeichert wird. Das Internet kann als erste Stufe der sich entwickelnden Globalen Informationsinfrastruktur (GII) bezeichnet werden. Das World Wide Web bildet als die modernste Benutzeroberfläche im Internet eine Basis für neue interaktive Multimedia-Dienste. Die Internet-Protokolle werden zunehmend auch für die Kommunikation innerhalb großer Unternehmen genutzt ("Intranet").

Die Teilnehmer am Internet haben unterschiedliche Aufgaben, Interessen und Möglichkeiten:

Die Software-, Computer- und Telekommunikationsindustrien erstellen die Kommunikationsnetze und die angebotenen Dienste.

- Telekommunikationsorganisationen wie die nationalen Telekommunikationsunternehmen stellen die Basisnetze für die Datenübertragung zur Verfügung (Punkt-zu-Punkt- oder Punkt-zu-Mehrpunkt-Verbindungen).
- Dienstleistungsunternehmen stellen Basisdienste für die Speicherung, Übertragung und Darstellung von Daten zur Verfügung. Sie sind für den Datentransport im Internet verantwortlich (routing, delivery) und verarbeiten Verbindungsdaten.

- Informationsanbieter stellen den Benutzern in Dateien und Datenbanken gespeicherte Informationen zur Verfügung.

- Die Benutzer greifen auf die verschiedenen Internet-Dienste (elektronische Post, news, Informationsdienste) zu und nutzen das Netz sowohl zur Unterhaltung als auch für Teleshopping, Telearbeit, Fernunterricht und Telemedizin.

I. Probleme und Risiken

Anders als bei der traditionellen Verarbeitung personenbezogener Daten, bei der normalerweise eine einzelne Behörde oder ein Unternehmen für den Schutz der personenbezogenen Daten ihrer Kunden verantwortlich ist, ist im Internet eine solche Gesamtverantwortung keiner bestimmten Einrichtung zugewiesen. Darüber hinaus gibt es keinen internationalen Kontrollmechanismus zur Erzwingung der Einhaltung gesetzlicher Verpflichtungen, soweit diese existieren. Der Benutzer muß daher Vertrauen in die Sicherheit des gesamten Netzes setzen, das bedeutet in jeden einzelnen Bestandteil des Netzes, unabhängig davon, wo dieser angesiedelt ist oder von wem er verwaltet wird. Die Vertrauenswürdigkeit des Netzes wird durch die Einfüh-

rung neuer Software, bei deren Nutzung Programme aus dem Netz geladen werden und die mit einer Verschlechterung der Kontrolle der auf dem Rechner des Benutzers gespeicherten personenbezogenen Daten verbunden ist, sogar noch wichtiger werden.
Die schnelle Ausbreitung des Internet und seine zunehmende Nutzung für kommerzielle und private Zwecke führen zur Entstehung schwerwiegender Datenschutzprobleme:

- Das Internet ermöglicht die schnelle Übertragung großer Informationsmengen auf beliebige andere an das Netzwerk angeschlossene Computersysteme. Sensible personenbezogene Daten können in Länder übertragen werden, die nicht über ein angemessenes Datenschutzniveau verfügen. Informationsanbieter könnten personenbezogene Daten auf Rechnern in Ländern ohne jegliche Datenschutzgesetzgebung anbieten, auf die aus aller Welt durch einen einfachen Mausklick zugegriffen werden kann.

- Personenbezogene Daten können über Länder ohne jegliche oder ohne hinreichende Datenschutzgesetzgebung geleitet werden. Im Internet, das ursprünglich für akademische Zwecke eingerichtet wurde, ist die Vertraulichkeit der Kommunikation nicht sichergestellt.

  Es gibt keine zentrale Vermittlungsstelle oder sonstige verantwortliche Einrichtung, die das gesamte Netz kontrolliert. Damit ist die Verantwortung für Datenschutz und Datensicherheit auf Millionen von Anbietern verteilt. Eine übertragene Nachricht könnte an jedem Computersystem, das sie passiert, abgehört und zurückverfolgt, verändert, gefälscht, unterdrückt oder verzögert werden. Trotzdem nimmt die Nutzung des Internet für Geschäftszwecke exponentiell zu, und personenbezogene und andere sensible Daten (Kreditkarten-Informationen und Gesundheitsdaten) werden über das Internet übertragen.

- Bei der Nutzung von Internet-Diensten wird weder eine angemessene Anonymität noch eine angemessene Authentifizierung sichergestellt. Computernetzwerk-Protokolle und viele Internet-Dienste arbeiten in der Regel mit dedizierten (Punkt-zu-Punkt-) Verbindungen. Zusätzlich zu den Inhaltsdaten wird dabei die Identität (ID) von Sender und Empfänger übertragen. Jeder elektronische Brief enthält einen "header" mit Informationen über Sender und Empfänger (Name und IP-Nummer, Name des Rechners, Zeitpunkt der Übertragung). Der "header" enthält weitere Informationen über den Übertragungsweg und den Inhalt der Nachricht. Er kann auch Hinweise auf Publikationen anderer Autoren enthalten. Die Benutzer sind gezwungen, eine elektronische Spur zu hinterlassen, die zur Erstellung eines Benutzerprofils über persönliche Interessen und Vorlieben verwendet werden kann. Obwohl es keinen zentralen Abrechnungsmechanismus für Zugriffe auf news oder das World Wide Web gibt, kann das Informationsgebaren von Sendern und Empfängern zumindest von dem Dienstleistungsunternehmen, an das der Benutzer angeschlossen ist, verfolgt und überwacht werden.

- Andererseits sind die unzureichenden Identifizierungs- und Authentifizierungsprozeduren im Internet bereits dazu benutzt worden, in unzureichend geschützte Computersysteme einzudringen, auf dort gespeicherte Informationen zuzugreifen und diese zu verändern oder zu löschen. Das Fehlen einer

sicheren Authentifikation könnte auch genutzt werden, um auf kommerzielle Dienste auf Kosten eines anderen Benutzers zuzugreifen.

- Es gibt im Internet Tausende von speziellen news-groups, von denen die meisten jedem Nutzer offenstehen. Die Artikel können personenbezogene Daten von Dritten enthalten, die gleichzeitig auf vielen tausend Computersystemen gespeichert werden, ohne daß der Einzelne eine Möglichkeit hat, dagegen vorzugehen.

Die Teilnehmer am Internet haben ein gemeinsames Interesse an der Integrität und Vertraulichkeit der übertragenen Information: Die Benutzer sind an verläßlichen Diensten interessiert und erwarten, daß ihre personenbezogenen Daten geschützt werden. In bestimmten Fällen können sie ein Interesse daran haben, Dienste ohne Identifizierung benutzen zu können. Den Benutzern ist es normalerweise nicht bewußt, daß sie beim "Surfen" im Netz einen globalen Marktplatz betreten und daß jeder einzelne Schritt dort überwacht werden kann.
Andererseits sind viele Diensteanbieter an der Identifizierung und Authentifizierung von Benutzern interessiert: Sie benötigen personenbezogene Daten für die Abrechnung, könnten diese Daten aber auch für andere Zwecke nutzen. Je mehr das Internet für kommerzielle Zwecke genutzt wird, desto interessanter wird es für Diensteanbieter und andere Einrichtungen sein, so viele Verbindungsdaten über das Nutzerverhalten im Netz wie möglich zu speichern und damit das Risiko für den Datenschutz der Kunden zu verstärken. Unternehmen bieten in zunehmendem Maße freien Zugang zum Internet an, um sicherzustellen, daß die Kunden ihre Werbeanzeigen lesen, die zu einer der hauptsächlichen Finanzierungsquellen des gesamten Internets werden. Die Unternehmen wollen nachvollziehen können, in welchem Ausmaß, von wem und wie oft ihre Werbeanzeigen gelesen werden.
Im Hinblick auf die erwähnten Risiken kommt den Einrichtungen, die das Netz auf internationaler, regionaler und nationaler Ebene verwalten, insbesondere bei der Entwicklung der Protokolle und Standards für das Internet, bei der Festlegung der Regeln für die Identifikation der angeschlossenen Server und schließlich bei der Identifikation der Benutzer eine wichtige Funktion zu.

II. Vorhandene Regelungen und Empfehlungen

Obwohl verschiedene nationale Regierungen und internationale Organisationen (z. B. die Europäische Union) Programme gestartet haben, um die Entwicklung von Computernetzen und -diensten zu erleichtern und zu intensivieren, sind dabei nur sehr geringe Anstrengungen unternommen worden, um für ausreichende Datenschutz- und Datensicherheitsregelungen zu sorgen. Einige nationale Datenschutzbehörden haben bereits Empfehlungen für die technische Sicherheit von an das Internet angeschlossenen Computernetzen und über Datenschutzrisiken für die einzelnen Benutzer von Internet-Diensten herausgegeben. Solche Empfehlungen sind z. B. in Frankreich, Großbritannien (vgl. den 11. Jahresbericht des Data Protection Registrar, Anhang 6) und in Deutschland erarbeitet worden. Die wesentlichen Punkte können wie folgt zusammengefaßt werden:

- Das Anbieten von Informationen auf dem Internet fällt in den Regelungsbereich der nationalen Datenschutzgesetze und -regelungen. In dieser Hinsicht ist das Internet nicht so ungeregelt, wie oft behauptet wird. Es ist, um nur ein Beispiel zu nennen, einem deutschen Anbieter eines WorldWideWebServers verboten, ohne Wissen des Benutzers die vollständigen Angaben über den

auf ihr Angebot zugreifenden Rechner, die abgerufenen Seiten und heruntergeladene Dateien zu speichern (wie es im Netz allgemein praktiziert wird). Nationale Regelungen können eine Verpflichtung für Informationsanbieter enthalten, sich bei einer nationalen Datenschutzbehörde anzumelden. Nationale Gesetze enthalten darüber hinaus spezielle Regelungen im Hinblick auf internationales Straf-, Privat- und Verwaltungsrecht (Kollisionsrecht), die unter bestimmten Umständen Lösungen bereitstellen können.

- Bevor ein lokales Computernetz - z. B. das einer Behörde - an das Internet angeschlossen wird, müssen die Risiken für das lokale Netzwerk und die darauf gespeicherten Daten im Einklang mit dem nationalen Recht abgeschätzt werden. Dazu kann die Erarbeitung eines Sicherheitskonzepts und einer Abschätzung, ob es erforderlich ist, das gesamte Netz oder nur Teile davon an das Internet anzuschließen, gehören. Abhängig von dem verfolgten Zweck kann es sogar ausreichend sein, nur ein Einzelplatzsystem an das Netz anzuschließen. Es sollten technische Maßnahmen getroffen werden, um sicherzustellen, daß auf dem Internet nur auf Daten, die veröffentlicht werden könnten, zugegriffen werden kann, z. B. durch Einrichtung eines Firewall-Systems, das das lokale Netzwerk vom Internet trennt. Es muß jedoch festgestellt werden, daß der Anschluß eines Computernetzwerks an das Internet eine Erhöhung des Sicherheitsrisikos auch dann bedeutet, wenn solche technischen Maßnahmen getroffen worden sind.

- Falls personenbezogene Daten von Nutzern eines bestimmten Dienstes gespeichert werden, muß für die Benutzer klar sein, wer diese Daten nutzen wird und zu welchen Zwecken die Daten genutzt oder übermittelt werden sollen. Dies bedeutet eine Information am Bildschirm vor der Übermittlung und die Schaffung einer Möglichkeit, die Übermittlung zu unterbinden. Der Benutzer sollte in der Lage sein, diese Unterrichtung und aller übrigen Bedingungen, die durch den Diensteanbieter gestellt werden, auszudrucken.

- Wenn der Zugang zu personenbezogenen Daten auf einem Computersystem bereitgestellt wird - z. B. durch die Veröffentlichung biographischer Angaben über Mitarbeiter in einem Verzeichnis - muß der Informationsanbieter sicherstellen, daß diese Personen sich der globalen Natur des Zugriffs bewußt sind. Am sichersten ist es, die Daten nur mit der informierten Einwilligung der betroffenen Person zu veröffentlichen.

Darüber hinaus gibt es eine Reihe von internationalen gesetzlichen Bestimmungen und Konventionen, die u. a. auch auf das Internet anwendbar sind:

- Empfehlung des Rates über Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten,verabschiedet vom Rat der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) am 23. September 1980

- Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981

- Richtlinien betreffend personenbezogene Daten in automatisierten Dateien, von der Generalversammlung der Vereinten Nationen verabschiedet am 4. Dezember 1990

- Richtlinie des Rates der Europäischen Gemeinschaften 90/387/EWG vom 28. Juni 1990 zur Verwirklichung des Binnenmarktes für Telekommunikationsdienste durch Einführung eines offenen Netzzugangs (Open Network Provision - ONP) (in der Datenschutz als "grundlegende Anforderung" definiert wird)

- Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EU-Datenschutzrichtlinie)

- Allgemeines Abkommen über Handel und Dienstleistungen (GATS) (das in Artikel XIV regelt, daß die Mitgliedstaaten durch das weltweite Abkommen nicht daran gehindert werden, Regelungen über den Datenschutz von Einzelpersonen im Zusammenhang mit der Verarbeitung und Verbreitung von personenbezogenen Daten und dem Schutz der Vertraulichkeit von Akten und Aufzeichnungen über Einzelpersonen zu erlassen oder durchzusetzen).

Die Richtlinie der Europäischen Union enthält als erstes supra-nationales Gesetzeswerk eine wichtige Neudefinition des Begriffs "für die Verarbeitung Verantwortlicher", die im Zusammenhang mit dem Internet von Bedeutung ist. Artikel 2 Buchstabe c) definiert den "für die Verarbeitung Verantwortlichen" als die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Wenn man diese Definition auf die Nutzung des Internet für die Zwecke der Übermittlung elektronischer Post anwendet, muß der Absender einer elektronischen Nachricht als "für die Verarbeitung Verantwortlicher" dieser Nachricht angesehen werden, wenn er eine Datei mit personenbezogenen Daten absendet, da er die Zwecke und Mittel der Verarbeitung und Übermittlung dieser Daten bestimmt. Andererseits bestimmt der Anbieter eines Mailbox-Dienstes selbst die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten im Zusammenhang mit dem Betrieb des Mailbox-Dienstes und hat damit wenigstens eine Mitverantwortung für die Einhaltung der anwendbaren Regelungen über den Datenschutz.
Kürzlich hat die Europäische Kommission zwei Dokumente veröffentlicht, die zu einer europäischen Gesetzgebung führen könnten und in diesem Fall beträchtliche Auswirkungen auf den Datenschutz im Internet haben werden:
Mitteilung an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen über illegale und schädigende Inhalte im Internet (KOM(96) 487)
und
Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in den audiovisuellen und Informationsdiensten (KOM(96) 483).
Obwohl auch diese nicht rechtlich bindend und eher auf einer nationalen denn auf einer internationalen Ebene verabschiedet worden sind, sollten die

- Grundsätze für die Bereitstellung und Nutzung personenbezogener Daten "Privacy und die nationale Informations-Infrastruktur" verabschiedet von der Privacy Working Group des Information Policy Committee innerhalb der Information Infrastructure Task Force (IITF) am 6. Juni 1995

genannt werden, da sie einen Einfluß auf die internationalen Datenflüsse haben werden. Sie sind intensiv und fruchtbar mit der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation bei einem gemeinsamen Treffen in Washington D. C. am 28. April 1995 diskutiert worden.
In der Praxis werden einige wichtige und effektive Regeln zur Selbstregulierung von der Netzgemeinde selbst aufgestellt (z. B. "Netiquette"). Solche Maßnahmen dürfen im Hinblick auf die Rolle, die sie gegenwärtig und zukünftig für den Datenschutz des einzelnen Benutzers spielen können, nicht unterschätzt werden. Sie tragen mindestens dazu bei, die nötige Aufmerksamkeit unter den Benutzern dafür zu schaffen, daß Vertraulichkeit als eine Grundanforderung auf dem Netz nicht existiert ("Sende oder speichere niemals etwas in Deiner Mailbox, das Du nicht in den Abendnachrichten sehen möchtest"). Die EU-Datenschutzrichtlinie wiederum fordert Verhaltensregeln (Artikel 27), die von den Mitgliedstaaten und der Kommission gefördert werden sollen.

III. Empfehlungen

Es steht außer Zweifel, daß der gesetzliche und technische Datenschutz im Internet im Augenblick unzureichend ist.
Das Recht jedes Einzelnen, die Datenautobahn zu benutzen, ohne überwacht und identifiziert zu werden, sollte garantiert werden. Andererseits muß es im Hinblick auf die Nutzung personenbezogener Daten auf der Datenautobahn (z. B. von Dritten) Grenzen geben ("Leitplanken").
Eine Lösung für dieses Grunddilemma muß auf folgenden Ebenen gefunden werden:
1. Die Diensteanbieter sollten jeden potentiellen Nutzer des Internet unaufgefordert über die Risiken für seine Privatsphäre informieren. Der Benutzer wird dann diese Risiken gegen die erwarteten Vorteile abwägen müssen.
2. Da "sowohl die einzelnen Teile der Netzwerk-Infrastruktur als auch die Benutzer jeder einen physikalischen Standort haben, können Staaten einen bestimmten Grad von Verläßlichkeit in bezug auf die Netze und ihre Teilnehmer verhängen und durchsetzen" (Joel Reidenberg). In vielen Fällen ist die Entscheidung, am Internet teilzunehmen und wie es zu benutzen ist, durch nationale Datenschutzgesetze geregelt.
Personenbezogene Daten dürfen nur in einer nachvollziehbaren Art und Weise gespeichert werden. Medizinische und andere sensible personenbezogene Daten sollten nur in verschlüsselter Form über das Internet übertragen oder auf den am Internet angeschlossenen Computern gespeichert werden.
Es spricht viel dafür, die Nutzung des Internet für die Veröffentlichung von Steckbriefen und Fahndungsaufrufen durch die Polizei zu verbieten (das amerikanische Federal Bureau of Investigations veröffentlicht seit einiger Zeit eine Liste von gesuchten Verdächtigen im Internet). Die beschriebenen Defizite der Authentifizierungsprozeduren und die leichte Manipulierbarkeit von Bildern im Cyberspace scheinen die Nutzung des Internet für diesen Zweck auszuschließen.
3. Verschiedene nationale Regierungen haben internationale Übereinkommen über die globale Informations-Infrastruktur angeregt. Initiativen für eine engere internationale Zusammenarbeit, ja sogar eine internationale Konvention, die den Datenschutz im Hinblick auf grenzüberschreitende Netze und Dienste regelt, sollten unterstützt werden.
4. Es sollte ein internationaler Kontrollmechanismus geschaffen werden, der auf bereits existierenden Strukturen wie der Internet Society und anderer Einrichtungen aufbauen könnte. Die Verantwortung für den Schutz personenbezogener Daten muß in einem gewissen Ausmaß institutionalisiert werden.

5. Nationale und internationale Gesetze sollten unmißverständlich regeln, daß auch der Vorgang der Übermittlung (z. B. durch elektronische Post) vom Post- und Fernmeldegeheimnis geschützt wird.
6. Darüber hinaus ist es notwendig, technische Mittel zur Verbesserung des Datenschutzes der Benutzer auf dem Netz zu entwickeln. Es ist zwingend, Entwurfskriterien für Informations- und Kommunikationstechnologie und Multimedia-Hard- und Software zu entwickeln, die den Benutzer befähigen, die Verwendung seiner personenbezogenen Daten selbst zu kontrollieren. Generell sollten die Benutzer jedenfalls in den Fällen die Möglichkeit haben, auf das Internet ohne Offenlegung ihrer Identität zuzugreifen, in denen personenbezogene Daten nicht erforderlich sind, um eine bestimmte Dienstleistung zu erbringen. Konzepte für solche Maßnahmen sind bereits entwickelt und veröffentlicht worden. Beispiele sind das "Identity-Protector"-Konzept, das in "Privacy-enhancing technologies: The path to anonymity" von der niederländischen Registratiekamer und dem Datenschutzbeauftragten von Ontario/Kanada enthalten ist (vorgestellt auf der 17. Internationalen Konferenz der Datenschutzbeauftragten in Kopenhagen (1995)) und das "User Agent-Konzept", das auf der gemeinsamen Sitzung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation und der Privacy Working Group der Information Infrastructure Task Force vorgestellt wurde (April 1995).
7. Auch für den Schutz der Vertraulichkeit sollten technische Mittel entwickelt werden.
Die Nutzung sicherer Verschlüsselungsmethoden muß eine rechtmäßige Möglichkeit für jeden Benutzer des Internet werden und bleiben.
Die Arbeitsgruppe unterstützt neue Entwicklungen im Internet-Protokoll (z. B. IP v6), die die Vertraulichkeit durch Verschlüsselung, Klassifizierung von Nachrichten und bessere Authentifizierungsprozeduren verbessern. Die Hersteller von Software sollten den Sicherheitsstandard des neuen Internet-Protokolls in ihre Produkte aufnehmen und Diensteanbieter sollten die Nutzung dieser Produkte so schnell wie möglich unterstützen.
8. Die Arbeitsgruppe würde eine Studie über die Machbarkeit eines neuen Zertifizierungsverfahrens durch die Ausgabe von "Qualitätsstempeln" für Diensteanbieter und Produkte im Hinblick auf ihre Datenschutzfreundlichkeit unterstützen. Diese könnten zu einer verbesserten Transparenz für die Benutzer der Datenautobahn führen.
9. Anonymität ist ein wichtiges zusätzliches Gut für den Datenschutz im Internet. Einschränkungen des Prinzips der Anonymität sollten strikt auf das begrenzt werden, was in einer demokratischen Gesellschaft notwendig ist, ohne jedoch das Prinzip als solches in Frage zu stellen.
10. Schließlich wird es entscheidend sein, herauszufinden, wie Selbstregulierung im Wege einer erweiterten "Netiquette" und datenschutzfreundliche Technologie die Implementierung nationaler und internationaler Regelung über den Datenschutz ergänzen und verbessern können. Es wird nicht ausreichen, sich auf eine dieser Handlungsmöglichkeiten zu beschränken: Sie müssen effektiv kombiniert werden, um zu einer globalen Informations-Infrastruktur zu gelangen, die das Menschenrecht auf Datenschutz und unbeobachtete Kommunikation respektiert.
Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die weitere Entwicklung in diesem Bereich genau beobachten, Anregungen aus der Netzgemeinde berücksichtigen und weitere, detailliertere Vorschläge entwickeln.

4. Empfehlung des Europarats über die Bearbeitung von Personendaten im medizinischen Bereich

vgl. S. 223ff.

5. Datenschutzbestimmungen in formellen Gesetzen

- ***Rechtsquellen***: Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG; SR 235.1) Art. 4 Abs. 2 und 3, Art 6 Abs. 1, Art. 17 Abs. 2, Art. 19 Abs. 1, 3 und 4 sowie Art. 38 Abs. 3.

- ***Allgemein gilt***: Werden besonders schützenswerte Personendaten oder Persönlichkeitsprofile regelmässig bearbeitet, muss dies in einem formellen Gesetz gesagt werden. Dabei müssen ***Zweck und Umfang*** der Datenbearbeitung, allenfalls die dabei verwendeten ***Mittel*** sowie die zur Bearbeitung ***befugte(n) Behörde(n)*** hinreichend bestimmt sein. Mit Blick auf die anstehende Verwaltungsreorganisation erscheint es als ratsam, nach Möglichkeit aufgabenspezifische Behördenbezeichnungen zu wählen, soweit dadurch das Gebot der hinreichenden Bestimmtheit von Erlassen nicht verletzt wird.

- Sollen ***unter verschiedenen Behörden*** und zu verschiedenen Bearbeitungszwecken regelmässig Personendaten, namentlich besonders schützenswerte Personendaten oder Persönlichkeitsprofile, ***ausgetauscht*** werden, muss dies im formellen Gesetz ausdrücklich gesagt sein. Erhalten einzelne Behörden im ***Abrufverfahren*** Zugriff auf diese Daten, muss auch dieser Umstand ausdrücklich erwähnt und die ermächtigte Behörde genannt werden. Erfolgt der Austausch regelmässig mit ***Behörden des Auslandes***, muss dies ebenfalls ausdrücklich geregelt werden.

- Wird in diesem Zusammenhang ein grosses und verzweigtes ***EDV-System*** („verwendete Mittel“) bei der Datenbearbeitung eingesetzt, in welchem in erheblichem Umfang und von verschiedenen Behörden Personendaten, namentlich besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet werden, muss dies - wie dargelegt - ebenfalls im formellen Gesetz ausdrücklich gesagt sein.

- Erweisen sich gewisse Grundrechtseingriffe nur zusammen mit konkreten, bereichsspezifischen ***Schutzauflagen*** als grundrechtskonform, sind auch diese Schutzauflagen bzw. die Grenzen der vorgesehenen Eingriffe formellgesetzlich zu regeln. Beispiele solcher Vorschriften stellen die Bestimmungen über die ***Massnahmen der Personenüberwachung mit technischen Mitteln und deren Begrenzung bzw. Kontrolle*** im BStP dar (vgl. Art. 65 ff. BStP) oder die Bestimmungen über den ***Schutz der Daten unbeteiligter Dritter bei Personenabfragen*** aus dem Zentralen Ausländerregister zu Identifikationszwecken bei der Strafverfolgung (vgl. heute: Art. 7 Abs. 3 ZAR-Verordnung, SR 142.215, sowie Art. 22e Abs. 2 des Entwurfs gemäss bundesrätlicher Botschaft vom 4. Dezember 1995 zum revidierten Ausländergesetz, BBl 1996 II 179).

- ***Diese Aufzählung ist nicht abschliessend***. Ob und in welchem Umfang bspw. ***Delegationen*** angezeigt sind, hängt stark von den Besonderheiten des jeweiligen Regelungsgegenstandes ab. Ebensowenig soll mit den vorliegenden Ausführungen eine bestimmte zu wählende Systematik oder Gesetzessprache als „verbindlich“ erklärt werden.

- ***Literatur***: Kommentar zum Schweizerischen Datenschutzgesetz (Hsg. Urs Maurer/Nedim Peter Vogt), Basel/Frankfurt a.M. 1995; ferner: Gutachten vom 9.8.95 des EDSB, abgedruckt in VPB 60.77 mit weiterführenden Zitierungen; EDSB, Leitfaden für die Bearbeitung von Personendaten in der Bundesverwaltung, Bern 1994.

6. EMPFEHLUNGEN DES EDSB

6.1. Empfehlung über die Einführung des Datenbearbeitungssystems bezüglich des Personals der Bundesverwaltung BV-PLUS

Bern, den 4. Juli 1996

EMPFEHLUNG

gemäß

Art. 27 Abs. 4 des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (DSG)

in Sachen

Einführung des Datenbearbeitungssystems bezüglich des Personals der Bundesverwaltung BV-PLUS

I. Der Eidgenössische Datenschutzbeauftragte stellt fest:

1. Das Eidgenössische Personalamt hat 1992/1993 eine strategische Informationsplanung (SIP) zur Erhebung der Informationsbedürfnisse in der Bundesverwaltung durchgeführt. Nach Feststellung der eingetretenen Veränderungen wurde 1993 ein Projekt für ein neues Datenbearbeitungssystem bezüglich des Personals der Bundesverwaltung initialisiert und in den darauffolgenden Jahren nach dem HERMES-Verfahren entwickelt. Das Projekt, welches BV-PLUS (Bundesverwaltung, Personal-, Lohn- und Stellenbewirtschaftungssystem) genannt wurde, soll das bestehende Datenbearbeitungssystem PERIBU ablösen.

2. Am 25. Juni 1993 wurde das Eidgenössische Personalamt durch den Eidgenössischen Datenschutzbeauftragten auf die Tendenz einer dezentralisierten Datenbearbeitung in der Bundesverwaltung aufmerksam gemacht. Wegen der Bearbeitung von besonders schützenswerten Personendaten betonte der Eidgenössische Datenschutzbeauftragte im gleichen Schreiben die Notwendigkeit einer gesetzlichen Grundlage im formellen Sinne. Die Details der Datenbearbeitungen und der entsprechenden Systeme - mithin auch des BV-PLUS - hätten dann im damaligen Entwurf einer *Ordonnance concernant la protection des données relatives aux agents de la Confédération* (Verordnung über den Schutz der Daten von Bediensteten der Bundesverwaltung) geregelt sein müssen. Auch im Tätigkeitsbericht 1993/1994 des Eidgenössischen Datenschutzbeauftragten wurde, neben der Feststellung der Tendenz zur Dezentralisierung der Datenbearbeitung bezüglich des Personals in der Bundesverwal-

tung, auch die Notwendigkeit von gesetzlichen Grundlagen für die entsprechenden Datenbearbeitungssysteme festgehalten.

3. Zur Zeit befindet sich das Projekt BV-PLUS in der Phase der Realisierung und soll im Verlaufe von 1996/1997 im Rahmen eines Pilotversuches mit drei Bundesämtern getestet werden und schrittweise in den produktiven Betrieb übergehen. 1998 soll das System die ganze Bundesverwaltung bedienen. Vom Stand der Projektentwicklung hat der Eidgenössische Datenschutzbeauftragte erst anfangs 1996 Kenntnis erhalten.

4. Mit Schreiben vom 24. Januar 1996 verlangte der Eidgenössische Datenschutzbeauftragte vom Eidgenössischen Personalamt die Herausgabe sämtlicher Dokumentation in Zusammenhang mit der Entwicklung des Systems BV-PLUS zur Abklärung des Sachverhaltes.

5. Gleichzeitig wurde das System BV-PLUS durch das Eidgenössische Personalamt beim Eidgenössischen Datenschutzbeauftragten zur Registrierung angemeldet. Es wurde jedoch vorläufig nicht im Register der Datensammlungen aufgenommen und publiziert.

6. Eine anfangs April 1996 stattgefundene Sitzung zwischen dem Eidgenössischen Personalamt und dem Eidgenössischen Datenschutzbeauftragten ergab, daß das System BV-PLUS, welches die Bearbeitung von besonders schützenswerten Personendaten vorsieht, keine gesetzliche Grundlage aufweist. Insbesondere wurde die *Ordonnance concernant la protection des données relatives aux agents de la Confédération* nicht realisiert. Ein Bearbeitungsreglement - wie seitens des Eidgenössischen Personalamtes als gesetzliche Grundlage für BV-PLUS vorgeschlagen - genügt den datenschutzrechtlichen Anforderungen an die gesetzliche Grundlage nicht. Der Eidgenössische Datenschutzbeauftragte hält weiterhin fest, daß auch ein Pilotversuch mit BV-PLUS ohne geeignete gesetzlichen Grundlagen nicht gestartet werden kann. Das Eidgenössische Personalamt wird darauf aufmerksam gemacht, daß der Eidgenössische Datenschutzbeauftragte in die Projektentwicklung und in die Realisierung der gesetzlichen Grundlagen von Anfang an hätte einbezogen werden müssen.

7. Mit Schreiben vom 7. Mai 1996 äußert sich das Eidgenössische Personalamt zu den vom Eidgenössischen Datenschutzbeauftragten gestellten datenschutzrechtlichen Anforderungen an das System BV-PLUS. Nach Meinung des Eidgenössischen Personalamtes sollten für BV-PLUS mangels Bearbeitung von besonders schützenswerten Personendaten sowie Persönlichkeitsprofilen reduzierte Anforderungen an die gesetzliche Grundlage bestehen. Die Verankerung des Systems in einer höheren gesetzlichen Grundlage könnte allenfalls erst mittelfristig im Rahmen des neuen Bundespersonalgesetzes erfolgen.

II. Der Eidgenössische Datenschutzbeauftragte zieht in Erwägung:

1. BV-PLUS stellt ein Datenbearbeitungssystem im Sinne des Bundesgesetzes über den Datenschutz (DSG, SR 235.1) dar, weshalb dieses zur Anwendung

gelangt. Art. 27 DSG ermächtigt und verpflichtet den Eidgenössischen Datenschutzbeauftragten, die Einhaltung des Datenschutzgesetzes durch die Bundesorgane zu überwachen und bei der Feststellung einer Verletzung von Datenschutzvorschriften dem verantwortlichen Bundesorgan zu empfehlen, das Bearbeiten zu ändern oder zu unterlassen.

2. Nach dem Datenschutzgesetz untersteht die Datenbearbeitung durch ein Organ des Bundes dem Legalitätsprinzip (Art. 17 DSG). Dieses Prinzip soll einerseits den Rechtsschutz der Individuen, andererseits Transparenz und Vorhersehbarkeit der Aktivitäten von öffentlichen Organen gewährleisten. Die gesetzliche Grundlage muß allgemeiner und abstrakter Natur sein.

   Unter einer gesetzlichen Grundlage versteht man nicht nur ein Gesetz im formellen Sinne, sondern jegliche Rechtsnorm, die sich auf ein Gesetz im formellen Sinne stützt (Gesetz im materiellen Sinn). Der erforderliche Bestimmtheitsgrad der Norm hängt von der Wichtigkeit der Bearbeitung, den Kategorien der bearbeiteten Daten (Schwere der Persönlichkeitsverletzung), dem Kreis der betroffenen Personen und der Erheblichkeit des Informationssystems ab. So erfordert ein offenes Informationssystem, das verschiedenen Organen einen Zugriff auf die Daten erlaubt, eine detailliertere Reglementierung, die den Zweck der Datenbearbeitung, die Systemorganisation, den oder die Verantwortlichen des Informationssystems sowie die beteiligten Organe festlegt. Zudem muß die Rechtsgrundlage enthalten: die gespeicherten Daten, die Herkunft der Daten, die zugriffsberechtigten Personen und Organe, den Zugriffsumfang, die Aufbewahrungsdauer, die Datenbearbeitung, -benutzung und -weitergabe, eventuelle Abrufverfahren sowie die besonderen Sicherheitsmaßnahmen.

   Das DSG verlangt grundsätzlich eine gesetzliche Grundlage im formellen Sinne, wenn die Bearbeitung zu einem schweren Eingriff in die Freiheiten und Grundrechte der betroffenen Personen führen kann (Art. 17 Abs. 2 DSG). Je größer der Kreis der betroffenen Personen, je umfangreicher der Katalog der bearbeiteten Personendaten, je heikler die Daten oder das Bearbeitungsfeld und je offener das Informationssystem, desto schwerer ist der Eingriff in die Persönlichkeit und desto höhere Anforderungen sind an die Gesetzesstufe zu stellen. Die formellgesetzliche Norm muß zumindest den Zweck und den Umfang der Bearbeitung präzisieren. Eine systemspezifische Verordnung soll dann die Details regeln.

3. Art. 19 DSG sieht die Notwendigkeit von gesetzlichen Grundlagen für die Bekanntgabe von Personendaten durch Bundesorgane vor. Gemäß Absatz 3 dieser Bestimmung bedarf die Datenbekanntgabe einer gesetzlichen Grundlage im formellen Sinne, wenn besonders schützenswerte Personendaten und/oder Persönlichkeitsprofile durch ein Abrufverfahren bekanntgegeben werden.

4. Die vom Eidgenössischen Datenschutzbeauftragten aufgrund von Art. 27 DSG vorgenommenen Abklärungen haben ergeben, daß mit dem System BV-PLUS z. T. besonders schützenswerte Personendaten und/oder Persönlichkeitsprofile bearbeitet werden; dies ergibt sich insbesondere aus der Anmel-

dung der Datensammlung vom 23. Januar 1996. Die Daten werden an die Departemente und Ämter durch Abrufverfahren bekanntgegeben.

Die in der Anmeldung der Datensammlung angegebene Rechtsgrundlage für BV-PLUS (Beamtengesetz vom 30. Juni 1927, SR 172.221.10) vermag den gewünschten datenschutzrechtlichen Anforderungen an die gesetzliche Grundlage (Art. 17 Abs. 2 und 19 DSG) nicht zu genügen. Insbesondere erteilt Art. 64 Abs. 1 lit. d des Beamtengesetzes dem Eidgenössischen Personalamt lediglich die Aufgabe, organisatorische Maßnahmen vorzusehen, ohne daß dabei ein entsprechendes Datenbearbeitungssystem namentlich bezeichnet und zumindest dessen Zweck sowie Bearbeitungsumfang festgelegt wird. Eine systemspezifische Verordnung für BV-PLUS besteht auch nicht. Auch ein Bearbeitungsreglement genügt weder als formell- noch als materiellgesetzliche Grundlage für BV-PLUS.

5. Eine vorläufige Inbetriebsetzung von BV-PLUS ohne gesetzliche Grundlage käme einer Umgehung von Art. 17 DSG gleich, weshalb auch der vorgesehene Pilotversuch nicht durchgeführt werden kann. Pilotversuche werden grundsätzlich nur dann zugelassen, wenn kumulativ folgende Voraussetzungen erfüllt sind:

   - die Inbetriebsetzung des Systems dringlich ist,
   - keine Ersatzlösung besteht und
   - das neue System auf die konkreten Erkenntnisse des Pilotversuches angewiesen ist.

Keine dieser Voraussetzungen ist erfüllt.

6. Gemäß Art. 17 Abs. 2 lit. a DSG dürfen Bundesorgane besonders schützenswerte Personendaten und Persönlichkeitsprofile ausnahmsweise ohne Verankerung der Bearbeitung im formellen Gesetz bearbeiten, wenn es für eine in einem formellen Gesetz - vorliegend das Beamtengesetz vom 30. Juni 1927 - klar umschriebene Aufgabe unentbehrlich ist. Auf diese Ausnahmebestimmung kann sich jedoch das Eidgenössische Personalamt im vorliegenden Fall nicht berufen. Die Bestimmung wird namentlich nur dann Anwendung finden, wenn eine klar definierte Aufgabe, die normalerweise nicht die Bearbeitung von besonders schützenswerten Personendaten verlangt, im Einzelfall eine solche Bearbeitung erforderlich macht. Die Bestimmung ist jedoch nicht anwendbar, wenn die Aufgaben des Bundesorgans regelmäßig und dauerhaft - wie das beim BV-PLUS der Fall ist - die Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen verlangen.

   Auch Art. 17 Abs. 2 lit. b und c DSG findet keine Anwendung. Einerseits befindet man sich in einem die Persönlichkeit gefährdenden Bereich und der Bundesrat hat keine entsprechende Bewilligung erteilt (lit. b), andererseits müßten alle durch die Datenbearbeitung betroffenen Angestellten der Bundesverwaltung ihre Daten allgemein zugänglich gemacht haben oder zur Bearbeitung mit BV-PLUS eingewilligt haben (lit. c).

7. Gemäß Art. 38 Abs. 3 DSG dürfen Bundesorgane eine bestehende Datensammlung mit besonders schützenswerten Personendaten und/oder mit Per-

sönlichkeitsprofilen noch während fünf Jahren nach Inkrafttreten des Gesetzes benützen, ohne daß die Voraussetzungen von Artikel 17 Abs. 2 DSG erfüllt sind. Diese Bestimmung ist im vorliegendem Fall nicht anwendbar, da BV-PLUS ein neues und kein bestehendes Datenbearbeitungssystem darstellt.

8. Dem Eidgenössischen Personalamt obliegen u. a. Beratungs- und Unterstützungsfunktionen in Organisations- und Führungsfragen (Art. 11 Ziff. 3 lit. c der Verordnung über die Aufgaben der Departemente, Gruppen und Ämter, SR 172.010.15). Die Verordnung über die Führungs- und Organisationsberatung in der allgemeinen Bundesverwaltung (SR 172.010.61) regelt die Details der Aufgabenerfüllung. Keiner dieser Gesetzestexte ermächtigt das Eidgenössische Personalamt, ein zentralisiertes Datenbearbeitungssystem bezüglich des Personals der Bundesverwaltung zu entwickeln und zu betreiben. Vielmehr sind die einzelnen Ämter für die Organisation verantwortlich (Art. 47 Abs. 1 lit. b des Bundesgesetzes über die Organisation und Geschäftsführung des Bundesrates und der Bundesverwaltung, VwOG, SR 172.010). In Wahrnehmung dieser gesetzlichen Aufgabe haben verschiedene Bundesämter dezentralisierte Inselsysteme für die Datenbearbeitung entwickelt. Das zentralisierte Datenbearbeitungssystem BV-PLUS sprengt den zitierten gesetzlichen Rahmen. Insbesondere ist es unverhältnismäßig, das ein einziges Amt über die Gesamtheit der das Personal der Bundesverwaltung betreffenden Daten verfügt. Auch aus Datensicherheitsgründen erscheint ein einheitliches Bearbeitungssystem nicht als unproblematisch. So ist der Eidgenössische Datenschutzbeauftragte der Überzeugung, daß eine dezentralisierte Lösung den unterschiedlichen Bedürfnissen der Bundesämtern besser gerecht wird und höchstens die Lohnbewirtschaftung sich für eine zentralisierte Datenbearbeitung eignet. BV-PLUS soll demzufolge nur über die für die Erfüllung dieser Aufgabe unentbehrlichen Daten verfügen.
9. Der Eidgenössische Datenschutzbeauftragte behält sich vor, das Projekt BV-PLUS nach Prüfung der Unterlagen gegebenenfalls auch aus technischen und organisatorischen Gründen sistieren zu lassen (Art. 20 Abs. 3 VDSG, SR 235.11).

III. Aufgrund dieser Erwägungen empfiehlt der Eidgenössische Datenschutzbeauftragte:

1. Das Eidgenössische Personalamt soll das zentralisierte System BV-PLUS lediglich für die Lohnbewirtschaftung des Personals der Bundesverwaltung einsetzen. Die Datenmenge soll dabei auf die für die Erfüllung dieser Aufgabe unentbehrlichen Daten reduziert werden.

2. Das Eidgenössische Personalamt schafft vor Pilotversuch und definitive Inbetriebsetzung des Systems BV-PLUS die nötigen formell- und materiellgesetzlichen Grundlagen. Der Eidgenössische Datenschutzbeauftragte ist in der Ausarbeitung der gesetzlichen Grundlagen für BV-PLUS rechtzeitig einzubeziehen.

3. Das Eidgenössische Personalamt benachrichtigt den Eidgenössischen Datenschutzbeauftragten innerhalb von dreissig Tagen, ob es die Empfehlung ab-

lehnt oder nicht. Wird die Empfehlung abgelehnt oder stellt der Eidg. Datenschutzbeauftragte nach Ablauf der Frist fest, daß sie nicht eingehalten wird, so kann er die Angelegenheit gemäß Art. 27 Abs. 5 DSG dem Eidgenössischen Finanzdepartement zum Entscheid vorlegen.

EIDGENÖSSISCHER DATENSCHUTZBEAUFTRAGTER

O. Guntern

6.2. Empfehlung über die Produktion und Vertrieb des Verzeichnisses der schweizerischen Fahrzeughalter auf CD-ROM

Bern, den 17. Januar 1997

EMPFEHLUNG

gemäss

Art. 29 Abs. 3 des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (DSG)

in Sachen

Produktion und Vertrieb des Verzeichnisses der schweizerischen Fahrzeughalter auf CD-ROM *durch* die Firma x

I. Der Eidgenössische Datenschutzbeauftragte stellt fest:

1. Der Eidgenössische Datenschutzbeauftragte wurde von der Datenschutzaufsichtsstelle des Kantons Bern vom 26. November 1996, vom Strassenverkehrsamt des Kantons Zürich vom 27. November 1996, von der Aufsichtsbehörde für Datenschutz des Kantons Freiburg vom 28. November 1996 sowie von der Aufsichtsstelle Datenschutz Basellandschaft vom 2. Dezember 1996 auf die Produktion und den Vertrieb eines Verzeichnisses der schweizerischen Fahrzeughalter auf CD-ROM durch die Firma x, aufmerksam gemacht.

2. Mit Schreiben vom 6. Dezember 1996 wurde die Firma x durch den Eidgenössischen Datenschutzbeauftragten aufgefordert, die Produktion und den Vertrieb der fraglichen CD-ROM bis zur Klärung des Sachverhaltes einzustellen. Zu diesem Zweck wurde die Dex Handels GmbH durch den Eidgenössischen Datenschutzbeauftragten über die durch die CD-ROM bearbeiteten Personendaten, deren Herkunft und Richtigkeit sowie über die gebotenen Suchkriterien befragt.

3. Mit Schreiben vom 19. Dezember 1996 bestätigte die Firma x, vertreten durch Rechtsanwalt x, die Einstellung der Produktion und des Vertriebes der fraglichen CD-ROM und nahm zu den Fragen des Eidgenössischen Datenschutzbeauftragten Stellung.
   Die Dex Handels GmbH führte insbesondere aus, dass die CD-ROM-Daten aus den offiziellen kantonalen Verzeichnissen der Motorfahrzeughalter stammen und dass für die Produktion und den Vertrieb der CD-ROM kein offizielles Mandat besteht. Ferner erklärte sie, ein elektronisches Motorfahrzeugverzeichnis werde bereits von verschiedenen Firmen über Videotex angeboten.
4. Gemäss Produktebeschreibung der Firma enthält die CD-ROM die Daten von über 3 Mio. Schweizer Fahrzeughalter(inne)n. Der Eidgenössische Datenschutzbeauftragte stellte anhand der von der Winterthurer Firma zur Verfü-

gung gestellten CD-ROM weiter fest, dass die Richtigkeit und Aktualität der Daten nicht gewährleistet sei. Die Untersuchung der CD-ROM ergab ausserdem, dass mehrere Suchoptionen weitergehende Abfragemöglichkeiten erlauben. Die Suchoption *„nach Leihwagen"* kann zudem zu Missverständnissen führen, da nicht in jedem Fall feststeht, ob Verleiher oder Entlehner von Fahrzeugen betroffen sind.

II. Der Eidgenössische Datenschutzbeauftragte zieht in Erwägung:

1. Durch die Anwendung der CD-ROM AUTO*dex* findet eine Datenbearbeitung von Personendaten im Sinne des Bundesgesetzes über den Datenschutz (DSG, SR 235.1) statt, weshalb dieses zur Anwendung gelangt. Daran vermag die Tatsache, dass die durch die Firma x bearbeiteten Personendaten vorgängig schon veröffentlicht worden sind nichts zu ändern. Dabei handelt es sich insbesondere nicht um einen Anwendungsfall von Art. 12 Abs. 3 DSG (in der Regel keine Persönlichkeitsverletzung, wenn die betroffene Person die Daten allgemein zugänglich gemacht hat und ihre Bearbeitung nicht ausdrücklich untersagt hat), da die betroffenen Personen die Daten nicht selbst der Öffentlichkeit zugänglich gemacht haben.

   Grundlage für die rechtliche Beurteilung der Angelegenheit bilden neben dem Datenschutzgesetz auch das Strassenverkehrsgesetz (SVG, SR 741.01) und die dazugehörende Verordnung über die Zulassung von Personen und Fahrzeugen zum Strassenverkehr (VZV, SR 741.51).

2. Art. 29 Abs. 1 lit. a DSG ermächtigt und verpflichtet den Eidgenössischen Datenschutzbeauftragten, den Sachverhalt von sich aus oder auf Meldung Dritter näher abzuklären, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler). Ein Systemfehler liegt dann vor, wenn Fehler von Informationssystemen der EDV bestehen, oder aber wenn ein Datenbearbeitungssystem *inhaltlich* rechtswidrig, d. h. die Bearbeitung als solche so angelegt ist, dass sie geeignet ist, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Entscheid der Eidgenössischen Datenschutzkommission Nr. 1/95 vom 21. November 1996). Das Vorliegen eines Systemfehlers ist Voraussetzung für die Abgabe einer Empfehlung im Sinne von Art. 29 Abs. 3 DSG. Es ist demnach zu prüfen, ob die CD-ROM geeignet ist, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen. Zur Prüfung dieser Frage ist als erstes von Art. 126 Abs. 1 VZV auszugehen.
   Gemäss dieser Bestimmung dürfen Name und Vorname eines Fahrzeughalters nur aufgrund des Kontrollschildes gesucht und bekanntgegeben werden. Damit hat der Gesetzgeber die Bearbeitungsmöglichkeiten auf ein Minimum beschränken wollen, um schwerwiegende Eingriffe in die Persönlichkeit der Fahrzeughalter (etwa durch Ausspionieren der Privatsphäre, Belästigungen unbescholtener Personen, Erleichterungen krimineller Handlungen, usw.) möglichst zu vermeiden. Obwohl die gedruckten Verzeichnisse entgegen dem Wortlaut von Art. 126 VZV in gewissen Fällen auch Beruf und Titel der Fahrzeughalter bekanntgeben (diese Daten wurden auch in die CD-ROM aufgenommen), lassen sie entsprechend der VZV keine weiteren Suchkriterien zu. Die durch die CD-ROM vorgesehenen, zahlreichen Suchkriterien und -

optionen - nach Name, Gemeinde, Postleitzahl, Kontrollschild - stehen somit in Widerspruch zu Art. 126 VZV. Die fragliche CD-ROM, die Daten von über 3 Mio. Fahrzeughaltern beinhaltet, stellt zusammen mit den unzulässigen Suchoptionen eine Verletzung der Persönlichkeit einer grösseren Anzahl von Personen dar. Die angebotenen Suchmöglichkeiten kollidieren aus dem genannten Grund auch mit dem datenschutzrechtlichen Verhältnismässigkeitsprinzip von Art. 4 Abs. 2 DSG, wonach Bearbeitungsmethoden, die mangels eines öffentlichen Interesses nicht nötig sind, auch nicht vorzusehen sind. Die Unverhältnismässigkeit der fraglichen Bearbeitung lässt sich insbesondere durch Vergleich mit dem Auskunftsdienst 111 der Telecom PTT veranschaulichen. Dieser Dienst erteilt nur aufgrund der Schildnummer Auskunft über einen einzigen Fahrzeughalter pro Anfrage. Die CD-ROM erlaubt durch die zahlreichen, umfassenden Suchkriterien praktisch unbeschränkte Suche. Genau diese Gefahr hat der Gesetzgeber mit Art. 126 VZV vermeiden wollen.

Ferner kann die durch die CD-ROM vorgesehene Suchoption *„nur Leihwagen“* dadurch zu Missverständnissen führen, dass nicht in jedem Falle klar steht, ob die gefundenen Daten Verleiher oder Entlehner von Wagen betreffen. Dies stellt eine Missachtung des Transparenzprinzipes dar.

3. Art. 4 Abs. 3 DSG besagt, dass Personendaten nur zu dem Zweck bearbeitet werden dürfen, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Dieser Grundsatz findet sich auch in Ziff. 2.2 der Empfehlung Nr. R (91) 10 des Ministerkomitees des Europarates an die Mitgliedstaaten für die Übermittlung der von öffentlichen Stellen gespeicherten personenbezogenen Daten an Dritte. Fahrzeughalterdaten werden zu Zwecken bearbeitet und veröffentlicht, die in einem direkten Zusammenhang mit der Erfüllung der strassenverkehrsrechtlichen Aufgaben, insbesondere mit der Erfüllung polizeilicher Aufgaben (vgl. v. a. Art. 125 Abs. 2 VZV) stehen. Eine Weiterbearbeitung dieser Daten durch Private zu anderen Zwecken ist somit ausgeschlossen. Der Vertrieb der Fahrzeughalterdaten durch die Firma x stellt eine kommerzielle Tätigkeit dar, die mit den von der Strassenverkehrsgesetzgebung gestellten Ziele in Widerspruch steht. Dadurch wird das Zweckbindungsgebot von Art. 4 Abs. 3 DSG verletzt.

4. Die Überprüfung der CD-ROM hat dann weiter ergeben, dass die Richtigkeit der Daten gemäss Art. 5 Abs. 1 DSG und deren Aktualität z. T. nicht gewährleistet sind. So wird bspw. der Buchstabe A durch das Einscannen oft als Ziffer 4 wiedergegeben (vgl. bspw. die zur Schildnummer GR 25611 gehörenden Daten).

   Weitere, oft auftretende Einscannfehler werden bspw. bei den zur Schildnummer SG 18435 gehörenden Daten veranschaulicht. Andere Mängel treten bei der Wiedergabe der Ortschaft auf: so heisst bspw. die Ortschaft, welche die Postleitzahl 7745 hat, nicht CURT, sondern LI CURT.

5. Gemäss Art. 104 Abs. 5 SVG *haben die Kantone, wenn ein zureichendes Interesse glaubhaft gemacht wird, die Namen von Fahrzeughaltern und ihren Versicherern bekanntzugeben. Das Verzeichnis der Namen der Fahrzeughalter kann veröffentlicht werden.* Diese Norm legt eine klare und ausschliessliche Kompetenz der Kantone fest, Fahrzeughalterdaten zu veröffentlichen und

bekanntzugeben. Letztere können Dritte mit der Produktion und Vertrieb der Register der Fahrzeughalter beauftragen.

Wie die Firma x schriftlich bestätigt hat, wurde sie von den kantonalen Strassenverkehrsbehörden mit der Veröffentlichung der Fahrzeughalterdaten auf CD-ROM nicht beauftragt, sondern übernahm die Fahrzeughalterdaten direkt und ohne Einholung der Einwilligung durch die zuständigen kantonalen Behörden aus den kantonalen Strassenverkehrsverzeichnissen. Ein solches Einverständnis für die Verfolgung kommerzieller Zwecke wäre jedoch aufgrund der klaren Zielsetzungen der Strassenverkehrsgesetzgebung kaum denkbar gewesen. Es steht demnach fest, Firma x mit der Produktion und Vertrieb der fraglichen CD-ROM die in Art. 104 Abs. 5 SVG statuierte Kompetenznorm zugunsten der Kantone missachtet hat. Aus diesem Grunde erscheint die Aneignung und die Veröffentlichung der Fahrzeughalterdaten auf CD-ROM durch Firma x auch als eine Verletzung von Art. 4 Abs. 1 DSG, wonach Personendaten nur rechtmässig beschafft werden dürfen.

6. Die Bearbeitung von Personendaten durch private Personen stellt einen Verstoss gegen die Grundsätze von Art. 4 und 5 DSG dar (Art. 12 Abs. 2 lit. a DSG). Die Datenbearbeitung ist widerrechtlich, wenn sie nicht durch Einwilligung der Verletzten, durch Gesetz (Art. 13 Abs. 1 DSG) oder durch die in Art. 13 Abs. 2 DSG aufgezählten einzelnen Rechtfertigungsgründe gerechtfertigt ist.

   Wie bereits festgestellt, werden die Fahrzeughalterdaten nicht erst nach Einholung der Einwilligung der betroffenen Personen der Öffentlichkeit zugänglich gemacht, sondern die Publikation erfolgt von Gesetzes wegen (Art. 104 Abs. 5 SVG). Das SVG sieht dann auch nicht vor, dass die Fahrzeughalterdaten zu kommerziellen Zwecken bearbeitet werden dürfen. Schliesslich lässt sich ein überwiegendes privates oder öffentliches Interesse der Firma x im Sinne von Art. 13 Abs. 2 DSG nicht feststellen. Die durch die CD-ROM ermöglichte Datenbearbeitung ist demzufolge rechtswidrig.

7. Zusammenfassend ist davon auszugehen, dass die durch die Firma x auf dem Markt angebotene Bearbeitungsmethode durch die einschlägigen gesetzlichen Bestimmungen nicht abgedeckt ist. Einerseits ist die fragliche Datenbearbeitung dem Bund vorbehalten, womit die Datenbeschaffung durch die Winterthurer Firma unrechtmässig im Sinne von Art. 4 Abs. 1 DSG ist. Andererseits stellt sie eine Zweckentfremdung dar, verstösst gegen Transparenz- und Richtigkeitsprinzipien, ist unverhältnismässig und durch keinen Rechtfertigungsgrund abgedeckt. Dabei vermag die Tatsache, dass andere Firmen - bedenklicherweise - die gleichen Dienste auf Videotex anbieten, nichts zu ändern.

III. Aufgrund dieser Erwägungen empfiehlt der Eidgenössische Datenschutzbeauftragte:

1. Die Firma x hat die Produktion und den Vertrieb der CD-ROM definitiv einzustellen.

2. Die Firma x benachrichtigt den Eidgenössischen Datenschutzbeauftragten innerhalb von 30 Tagen, ob sie die Empfehlung ablehnt oder nicht. Wird die Empfehlung abgelehnt oder stellt der Eidgenössische Datenschutzbeauftragte nach Ablauf der Frist fest, dass sie nicht eingehalten wird, so kann er die Angelegenheit gemäss Art. 29 Abs. 4 DSG der Eidgenössischen Datenschutzkommission zum Entscheid vorlegen.

EIDGENÖSSISCHER
DATENSCHUTZBEAUFTRAGTER

O. Guntern

6.3. Empfehlung über die Rufnummernanzeige im Dienstintegrierenden Digitalen Netz (ISDN)

Bern, 13. März 1996

EMPFEHLUNG

gemäss

Art. 27 Abs. 4 Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG)

in Sachen

Rufnummernanzeige im Diensteintegrierenden Digitalen Netz (ISDN)

I. Der Eidgenössische Datenschutzbeauftragte stellt fest:

1. Im Diensteintegrierenden Digitalen Netz (ISDN) wird die Rufnummer des Anrufenden auf dem Display des über ein ISDN-Abonnement verfügenden Angerufenen noch vor Entgegennahme des Anrufs angezeigt.

2. Die einzelfallweise, d. h. pro Anruf per Knopfdruck vornehmbare Unterdrückung der Rufnummernanzeige durch den Anrufenden ist in der Ausbauphase SwissNet3 möglich, sofern der Anrufende über ein ISDN-Abonnement verfügt; für diese einzelfallweise Unterdrückung der Rufnummernanzeige hat der Anrufende jedoch eine einmalige Gebühr zu entrichten.

3. Die Anzeige der Rufnummer des von einem analogen Apparat ausgehenden Anrufs, der über eine digitale Telefonzentrale vermittelt wird, kann permanent, das heisst auf Dauer, gegen Entrichtung einer einmaligen Einrichtungsgebühr und einer monatlichen Abonnementsgebühr unterdrückt werden.

4. Über die Möglichkeit der Rufnummernübertragung im SwissNet/ISDN und der Rufnummernunterdrückung informiert die PTT Telecom lediglich im PTT-Amtsblatt sowie teilweise regional.

5. Mit Schreiben vom 17. Februar 1995 ist die PTT Telecom aufgefordert worden,

   - die Unterdrückung der Rufnummernanzeige kostenlos anzubieten,

   - in den Verzeichnissen die ISDN-Anschlüsse zu kennzeichnen, damit der Anrufende weiss, dass eine Rufnummern-Übertragung in Betracht kommt,

   - sowie alle Telefonabonnenten schriftlich zu informieren, dass ihre Rufnummer bei ISDN-Teilnehmern angezeigt werden kann und dass die Möglichkeit zur Unterdrückung der Rufnummernanzeige besteht.

6. Diese Forderungen wurden erneut im 2. Tätigkeitsbereicht 1994/1995 des Eidgenössischen Datenschutzbeauftragten Seite 27 f. vertreten.

7. Seitens der PTT Telecom wurde kein Kontakt mit dem Eidgenössischen Datenschutzbauftragten gesucht.

8. Die PTT Telecom hat unseren Forderungen bis jetzt nicht entsprochen und will ihnen gemäss Schreiben vom 23. Februar 1996 auch nicht entsprechen.

II. Der Eidgenössische Datenschutzbeauftragte zieht in Erwägung:

1. Die Rufnummernanzeige stellt ein Bearbeiten von Personendaten im Sinne des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1) dar, woraus sich die Legitimation des Eidgenössischen Datenschutzbeauftragten zum Erlass einer Empfehlung gemäss Art. 27 Abs. 4 DSG ergibt.

2. Jede Person muss, ausgehend von der Achtung der Persönlichkeits- und Grundrechte, insbesondere der persönlichen Freiheit, die Herrschaft über die sie betreffenden Informationen ausüben und eine Bearbeitung dieser Daten durch Dritte einschränken können (BUNTSCHU, Kommentar zum Schweizerischen Datenschutzgesetz (Hrsg. Maurer/Vogt), Basel/Frankfurt a. M. 1994, Art. 1 Rdn. 14).

3. Jeder einzelne sollte nicht nur in der Lage sein, einen Überblick über die Bearbeitung seiner Personendaten zu behalten, sondern auch als Ausfluss aus seinem Recht auf persönliche Freiheit das Recht auf informationelle Selbstbestimmung auszuüben, das durch das Bundesgesetz über den Datenschutz vom 19. Juni 1992 seine positivrechtliche Anerkennung erfahren hat (BUNTSCHU a.a.O. Rdn. 14, 17).

4. Aus dem Recht auf informationelle Selbstbestimmung sowie dem mit diesem in engem Zusammenhang stehende, durch Art. 36 Bundesverfassung garantierte Fernmeldegeheimnis folgt das Recht jedes einzelnen auf unbeobachtete Kommunikation.

5. Diese Rechte werden grundsätzlich durch die Rufnummernanzeige verletzt, weil

   - der Angerufene (beispielsweise Behörde) bei missliebigen, etwa zu Recht reklamierenden Personen die Entgegennahme des Anrufes unzulässigerweise verweigern kann,

   - durch den Einsatz entsprechender Software der Angerufene innerhalb von Bruchteilen von Sekunden noch vor Entgegennahme des Anrufes ohne Kenntnis und Einwilligung des Anrufenden dessen Name und Adresse herausfinden und speichern kann,

   - bereits durch die Rufnummernanzeige, erst recht aber bei Verwendung entsprechender Software auch Drittpersonen ohne Kenntnis und Einwilligung des Anrufenden erfahren können, wer angerufen hat;

- bei Inanspruchnahme von gewissen Hilfsorganisationen wie Anonyme Alkoholiker, AIDS-Hilfe, Kinder-Sorgentelefon, Seelsorge die Anonymität des Anrufenden nicht gewährleistet wäre.

6. Diese Rechte können nur ausgeübt und wahrgenommen werden, wenn

   - für alle Telekommunikationsabonnenten die Möglichkeit besteht, die Rufnummernanzeige zu unterdrücken,

   - jeder Telekommunikationsabonnent auf die Rufnummernübertragung und auf die Möglichkeit zur Unterdrückung in einer für ihn wahrnehmbaren und verständlichen Art und Weise hingewiesen wird,

   - den Abonnenten keine Gebühren als Hemmschwelle von der Wahrung seiner Rechte, die bis zur Einführung von ISDN selbstverständlich und kostenlos war, abhalten.

7. Ein Eingriff in diese Rechte wäre nur aufgrund einer ausdrücklichen hinreichenden gesetzlichen Grundlage zulässig, da es sich um Grundrechte handelt, die bis anhin gewährleistet waren.

8. Die PTT Telecom informieren ihre Kunden, die nicht über ein SwissNet/ISDN-Abonnement verfügen, nicht in einer einheitlichen, für alle Telekommunikationsteilnehmer gleich verständlichen und einfachen Form über die Folgen von SwissNet/ISDN sowie die Möglichkeit der Unterdrückung der Rufnummernanzeige, so dass die für die Wahrung der Rechte erforderliche allgemeine Information und Transparenz nicht gewährleistet ist.

9. Die gebührenfreie Unterdrückung, d.h. die Unterdrückung ohne "Hemmschwelle" (vgl. Schreiben PTT Telecom vom 23. Februar 1996) wird seitens der PTT Telecom abgelehnt, um auf dem Markt unter Missachtung der Rechte eines Grossteils ihrer Kunden SwissNet/ISDN zu lancieren.

10. Die Tatsache, dass bis Ende Dezember 1995 nur gerade

    - 633 von 69' 500 SwissNet-Kunden, also < 1%, und

    - 1650 von 4,3 Mio analogen Teilnehmern

    den Dienst "Identifikation unterdrücken" abonniert haben, spricht dafür, dass durch die Möglichkeit der gebührenfreien Unterdrückung weder den PTT Telecom ein grosser finanzieller Verlust beschieden wäre, noch das Produkt SwissNet/ISDN auf dem Markt bedroht wäre.

11. Da die PTT Telecom durch Einführung von SwissNet/ISDN die Rufnummernanzeige und damit den Eingriff in die Persönlichkeitsrechte von Kunden verursacht hat, ist es verursachergerecht und verhältnismässig, wenn die PTT Telecom die aus der Möglichkeit der Unterdrückung der Rufnummernanzeige entstehenden Kosten trägt und diese nicht auf die Kunden abwälzt.

12. Auch ist die Unterdrückung der Rufnummernanzeige bei Anrufen, die von analogen Apparaten ausgehen, nicht absolut unmöglich.

13. Die Empfehlung Nr. R (95)4 des Ministerkommitees des Europarates regelt

- unter Punkt. 7.16. Abs. 1, dass die Einführung der Rufnummernanzeige von Informationen an alle Abonnenten mit der Angabe begleitet sein sollte, dass verschiedene Abonnenten über die Rufnummernanzeige verfügen können und es deshalb möglich ist, dass die Telefonnummer dem Angerufenen enthüllt wird.
- unter Punkt 7.16. Abs. 2, dass die Einführung der Rufnummernanzeige für den anrufenden Abonnenten von der Möglichkeit begleitet sein muss, durch ein einfaches Mittel die Anzeige seiner Telefonnummer auf dem Endgerät des angerufenen Abonnenten zu unterdrücken.

14. In der geplanten "Richtlinie für den Datenschutz in öffentlichen Telekommunikationssystemen, insbesondere im Diensteintegrierenden Digitalen Netz, ISDN, und in digitalen Mobilfunknetzen" der Kommission der Europäischen Gemeinschaften ist

- unter Art. 8 Punkt 1 vorgesehen, dass im Falle der Rufnummernanzeige der anrufende Teilnehmer die Möglichkeit haben muss, auf einfache Weise die Übertragung seiner Teilnehmernummer von Fall zu Fall auszuschliessen;

- unter Art. 8 Punkt 2 vorgesehen, dass der Anrufende die Möglichkeit haben muss, auf Antrag die Rufnummernanzeige permanent zu unterdrücken;

- unter Artikel 8 Punkt 5 vorgesehen, dass die Option der Unterdrückung der Rufnummernanzeige kostenfrei angeboten werden muss.

III. Aufgrund dieser Erwägungen empfiehlt der Eidgenössische Daten-schutzbeauf-tragte:

1. PTT Telecom bietet die fallweise Unterdrückung der Rufnummernanzeige auch von analogen Apparaten aus an.

2. Die PTT Telecom bietet die Unterdrückung der Rufnummernanzeige kostenlos an.

3. Die PTT Telecom weist jeden Telekommunikationsabonnenten in einem Schreiben auf die Rufnummernanzeige im SwissNet/ISDN sowie auf die Möglichkeit der Rufnummernunterdrückung hin.

4. In den Telekommunikationsverzeichnissen werden bei jedem ISDN-Anschluss ein für die Verzeichnis-Benutzer verständlicher Hinweis angebracht, dass eine Rufnummernanzeige in Betracht kommt.

5. Die PTT Telecom teilt bis zum 15. April 1996 dem Eidgenössischen Datenschutzbeauftragten mit, ob sie diese Empfehlung annimmt oder ablehnt.

6. Diese Empfehlung wird der PTT Telecom sowie dem Generalsekretariat des EVED mitgeteilt.

EIDGENÖSSISCHER DATENSCHUTZBEAUFTRAGTER

O. Guntern