Eidgenössischer Datenschutzbeauftragter

Préposé fédéral à la protection des données

2. Tätigkeitsbericht 1994/95

2ème Rapport d'activités 1994/95

Vertrieb: Eidg. Drucksachen- und Materialzentrale, 3003 Bern

Eidgenössischer Datenschutzbeauftragter

Tätigkeitsbericht 1994/95

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 1994 und 31. März 1995 ab.

INHALTSVERZEICHNIS

*: Originaltext auf Französisch

*: Originaltext auf Französisch

*: Originaltext auf Französisch

ABKÜRZUNGSVERZEICHNIS

AHV	Alters- und Hinterlassenenversicherung
AUPER	Automatisiertes Personenregistratursystem
BA	Bundesanwaltschaft
BD	Beschwerdedienst
BUPO	Bundespolizei
BVG	Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge
CJ-PD	Projektgruppe für den Datenschutz im Europarat
DOSIS	Provisorisches Datenverarbeitungssystem zur Bekämpfung des illegalen Drogenhandels (Pilot)
DSG	Datenschutzgesetz
EDSB	Eidgenössischer Datenschutzbeauftragter
EDV	Elektronische Datenverarbeitung
EJPD	Eidg. Justiz- und Polizeidepartement
ISDN	Dienstintegrierendes digitales Fernmeldenetz (Integrated Digital Network)
ISIS	Provisorische Staatsschutz-Informations-System
OECD	Organisation für Zusammenarbeit und Entwicklung
OR	Obligationenrecht
REGI	Papierlose Personen- und Dossierverwaltung
RIPOL	Automatisiertes Fahndungssystem
RZ	Rechenzentrum
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
ZAR	Zentrales Ausländerregister

VORWORT

Seit bald zwei Jahren ist das Bundesgesetz über den Datenschutz in Kraft. Nun liegt der zweite Tätigkeitsbericht des Eidgenössischen Datenschutzbeauftragten (EDSB) vor. Das Berichtsjahr war von strukturellen Entwicklungen im Sekretariat des EDSB geprägt. Zeit beansprucht haben insbesondere das Anmeldeverfahren für Datensammlungen, die Erstellung des Registers der Datensammlungen sowie seine informatisierte Führung und die Vorkehrungen der Publikation. Daneben hatte das Sekretariat eine Fülle von Anfragen über aktuelle datenschutzrechtliche Belange der Bundesorgane und von Privatpersonen zu bewältigen.

Es hat sich wiederum bestätigt, dass Datenschutzfragen nicht allein durch materielle Grundsätze zu beantworten sind, sondern vielmehr eine dauernde Kommunikation sowohl mit den Betroffenen als auch mit den Datenbearbeitern erfordern. Dabei hat die Überzeugungsarbeit einen immer höheren Stellenwert. Wird die Persönlichkeit durch die Bearbeitung von Personendaten verletzt, so ist dies nämlich zumeist auf die fehlende Sensibilität für solche Verletzungen zurückzuführen und nicht auf eine bewusste Missachtung von Grundsätzen der Datenbearbeitung.

Wir haben festgestellt, dass zahlreiche Bundesbehörden und auch viele private Inhaber von Datensammlungen die Notwendigkeit des Schutzes von Personendaten erkannt haben und durchaus bereit sind, den Datenschutz zu fördern. Im Rahmen der Diskussion über die Bekämpfung der organisierten Kriminalität ist aber das Recht des einzelnen, selbst über den Umgang mit seinen Daten zu entscheiden, stark in den Hintergrund getreten. Deshalb hat auch dieses Jahr die Überzeugungsarbeit nebst den Bemühungen, die Einhaltung der Anforderungen des DSG durchzusetzen, grosses Gewicht.

Die verschiedenen Methoden der Bearbeitung von Personendaten und die dabei bestehenden Möglichkeiten entwickeln sich sehr unterschiedlich. In der Schweiz werden - dasselbe geschieht übrigens auf weltweiter Ebene - immer neue Systeme entwickelt, die immer mehr Personendaten erfassen und die sogenannte "informationelle Selbstbestimmung" weiter beschränken. Zu denken ist nicht nur an die neuen Polizei- und Sicherheitssysteme. Die Gefahr kommt auch aus anderen Bereichen wie beispielweise der Überwachung des Telefons am Arbeitsplatz oder den unerschöpflichen Abwicklungsmöglichkeiten des bargeldlosen Zahlungsverkehrs (Chip-Karten oder Telebanking). Der elektronische Zahlungsverkehr lässt - zumindest bei häufiger Benutzung - die Erstellung von Datenbanken zu, die über die Einsicht in die Zahlungsvorgänge ein umfassendes Bild der "Gewohnheiten" des Karteninhabers vermitteln. Daraus können Persönlichkeitsprofile entstehen.

Es steht ausser Zweifel, dass unsere Gesellschaft aufgrund ihrer technologischen Infrastruktur immer mehr auf die Bearbeitung von Personendaten angewiesen ist. Erstrebenswert ist nicht, diesen Informationsfluss einzuschränken oder zu verhindern. Vielmehr ist es notwendig, die Verwendung der Personendaten an eine strikte Zweckbindung zu knüpfen. Das ist auch der Kerngedanke des Datenschutzes: Er will Datenbearbeitungen nicht verbieten, sondern sie nur unter der Voraussetzung einer strikten Zweckgebundenheit ermöglichen.

I. AUSGEWÄHLTE THEMEN

1. Polizeiwesen

1.1. Organisiertes Verbrechen - Das neue indirekte Auskunftsrecht

Am 7. Oktober 1994 hat das Parlament das neue Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes verabschiedet. Dieses Gesetz ist das Ergebnis eines Gesetzgebungsprozesses, in dem sich die Debatten hauptsächlich auf das Problem der Ausübung des Auskunftsrechts konzentrierten. Infolge unserer Vorbehalte hinsichtlich der in der Botschaft des Bundesrates über die Schaffung einer Zentralstelle zur Bekämpfung des organisierten Verbrechens enthaltenen Beschränkungen des Auskunftsrecht, hat sich auch das Parlament dieser Problematik angenommen und lange darüber debattiert. Es hat sich schliesslich für die Ausarbeitung eines spezifischen Gesetzes zur Bekämpfung des organisierten Verbrechens entschieden und zum Auskunftsrecht eine besondere Bestimmung erlassen, die von den Vorschriften des Bundesgesetzes über den Datenschutz abweicht. Durch diese Bestimmung wird ein indirektes Auskunftsrecht eingeführt, indem vorgesehen wird, dass wir nachprüfen, ob die Datenbearbeitungen durch die Zentralstellen rechtmässig erfolgt sind. Die Bestimmung findet auch auf Auskunftsgesuche im Zusammenhang mit dem System DOSIS Anwendung.

Das politische Engagement für eine Verstärkung der Gesetzgebung im Hinblick auf eine wirksamere Bekämpfung neuer Verbrechensformen, insbesondere der Wirtschaftskriminalität und des organisierten Verbrechens, hat am 7. Oktober 1994 zur Verabschiedung des Bundesgesetzes über kriminalpolizeiliche Zentralstellen des Bundes geführt. Das am 15. März 1995 in Kraft getretene Gesetz, stützt sich auf die Botschaft über die Schaffung einer Zentralstelle zur Bekämpfung des organisierten Verbrechens, die am 12. Januar 1994 vom Bundesrat verabschiedet worden war. Es stellt eine Ergänzung zum "ersten Massnahmenpaket" gegen das organisierte Verbrechen dar, welches sich aus Strafnormen zur Geldwäscherei und zur mangelnden Sorgfalt bei Finanzgeschäften zusammensetzt. Es ergänzt aber auch das "zweite Massnahmenpaket", das vor allem das Melderecht des Financiers und den Begriff der kriminellen Organisation betrifft.

Das Gesetz über kriminalpolizeiliche Zentralstellen des Bundes soll in erster Linie die Aufgaben der Zentralstellen des Bundesamtes für Polizeiwesen bei der Bekämpfung des internationalen organisierten Verbrechens festlegen. Es regelt den Einsatz von Polizeiverbindungsleuten im Ausland, die Zusammenarbeit mit den Strafverfolgungsbehörden und den kantonalen und ausländischen Polizeidienststellen sowie die Datenbearbeitung und den nationalen und internationalen Austausch kriminalpolizeilicher Informationen. Das Gesetz umschreibt ausserdem die Aufgaben der Zentralstelle für die Bekämpfung des organisierten Verbrechens und der Zentralstelle für die Bekämpfung des unerlaubten Betäubungsmittelverkehrs. Innerhalb des Abschnitts über die Bearbeitung von Personendaten enthält das Gesetz über kriminalpolizeiliche Zentralstellen des Bundes - neben Bestimmungen über Datenbearbeitungssysteme, die Beteiligung der Kantone und die Weitergabe von Personendaten - einen Artikel 14 über die "Information der Betroffenen und Auskünfte".

Diese Sonderregelung ist das Ergebnis sehr langer Debatten im Parlament. Ursprünglich sah die Botschaft des Bundesrates über die Schaffung einer Zentralstelle zur Bekämpfung des

organisierten Verbrechens eine besondere Bestimmung vor, die sich an die deutsche Gesetzgebung anlehnte: gemäss dieser Bestimmung hätte die betroffene Person zur Ausübung ihres Auskunftsrechts einen konkreten Tatbestand vorweisen und ein besonderes Interesse an der Erteilung der Auskunft geltend machen müssen. Da wir derartige Bedingungen nicht gutheissen konnten, haben wir darauf hingewiesen, dass die Geltendmachung eines besonderen Interesses allenfalls im Rahmen der Bekämpfung des organisierten Verbrechens verlangt werden könnte, obwohl dies nicht der Rechtsprechung des Bundesgerichts entspricht. Dieser zufolge muss jede Person, ohne ein anderes schützenswertes Interesse nachweisen zu müssen, Einsicht in die über sie bearbeiteten Daten erhalten können, wenn sie mit einiger Wahrscheinlichkeit darlegen kann, dass die über sie bearbeiteten Daten geeignet sind, ihre persönliche Freiheit zu beeinträchtigen. Inakzeptabel war vor allem die Bedingung, dass sich die betroffene Person auf einen konkreten Tatbestand berufen müsste. Diese Bedingung käme nämlich einem Verstoss gegen die menschlichen Würde gleich. Sie würde dazu führen, dass die betroffene Person gezwungen wäre, sich selbst bestimmter Tatsachen zu bezichtigen. Ausserdem wäre die Erfüllung dieser Bedingung in der Praxis in all den Fällen unmöglich, in denen die betroffene Person sich nichts vorzuwerfen hat, sondern nur sicherstellen will, dass sie nicht Opfer einer missbräuchlichen oder unbegründeten polizeilichen Überwachung ist. Wir haben schliesslich daran erinnert, dass diese in Deutschland im Dezember 1990 in Kraft getretene Lösung bei ihrer Verabschiedung auf starke Opposition stiess und dass sie auch nach mehrjähriger Erfahrung, immer noch im Kreuzfeuer der Kritik steht, insbesondere von seiten des deutschen Bundesdatenschutzbeauftragten.

Unsere im Rahmen verschiedener Stellungnahmen angemeldeten Vorbehalte wurden im Zuge der Prüfung des Gesetzesentwurfs durch die eidgenössischen Räte von diesen diskutiert. Zudem wurden wir aufgefordert, unseren Standpunkt zu dieser Problematik vor der parlamentarischen Kommission darzulegen. Dies gab uns Gelegenheit, den Parlamentariern die verschiedenen in den anderen nationalen Gesetzgebungen vorgesehenen Verfahren vor Augen zu führen und uns zu deren Funktionsweise zu äussern. Nebst dem vom Bundesrat vorgeschlagenen Modell, das sich am deutschen Recht orientiert, wurden die Lösungen des englischen und französischen Rechts geprüft. Das französische Recht sieht namentlich ein indirektes Auskunftsrecht vor, das über die Nationale Kommission für Informatik und Freiheitsrechte (CNIL) ausgeübt wird. Diese eröffnet der gesuchstellenden Person, dass sie die gewünschte Überprüfung durchgeführt hat. Das Dekret berechtigt die CNIL, der betroffenen Person mit Einverständnis des Innenministers bestimmte Informationen, die vom Nachrichtendienst gesammelt wurden, bekanntzugeben. Dem Betroffenen stehen im Falle einer Auskunftsverweigerung ausserdem verschiedene Rechtswege offen. Im Zuge der Parlamentsdebatten wurde auch regelmässig auf das britische Modell hingewiesen. Dieses sieht die Ernennung eines speziellen Gerichts (security service Tribunal) vor, das Beschwerden über die Aktivitäten der Sicherheitsdienste behandelt. Ferner ist im britischen Modell die Ernennung eines speziellen Beauftragten (security service Commissioner) vorgesehen, der über ein Recht zur Einsichtnahme verfügt und die Aufgabe hat, das Gericht zu unterstützen.

Das Parlament hat schliesslich beschlossen, sich am britischen und am französischen Modell zu orientieren und den Artikel 14 des Bundesgesetzes über kriminalpolizeiliche Zentralstellen des Bundes verabschiedet. Mit dieser speziellen Bestimmung, die von den Regelungen des Bundesgesetzes über den Datenschutz abweicht, wird ein Verfahren mit einem *indirekten Auskunftsrecht*, das über unsere Stelle geltend gemacht werden kann, geschaffen. Dieses Verfahren ist nur in den Fällen anwendbar, die dem Gesetz über kriminalpolizeiliche Zentralstellen des Bundes unterstehen, wozu auch der Zugang zum

System DOSIS gehört. Die Verordnung, welche dieses provisorische System zur Bearbeitung von Daten im Zusammenhang mit der Bekämpfung des unerlaubten Betäubungsmittelhandels regelt, wird entsprechend angepasst werden müssen. Hingegen unterstehen andere Auskunftsgesuche, die nicht in den Anwendungsbereich des obenerwähnten Gesetzes fallen nach wie vor dem klassischen Verfahren des *direkten Auskunftsrechts*. Dazu gehören auch Gesuche die sich auf das Provisorische Staatsschutz-Informationssystem ISIS beziehen. Die diesbezüglichen Gesuche müssen gemäss den Bestimmungen des Bundesgesetzes über den Datenschutz direkt an die im jeweiligen Fall zuständige Behörde gerichtet werden !
Das neue indirekte Auskunftsrecht wird wie folgt ausgeübt: ❶ Jede Person kann vom Eidgenössischen Datenschutzbeauftragten verlangen, dass er prüft, ob bei einer Zentralstelle Daten über sie rechtmässig bearbeitet werden. ❷ Der Datenschutzbeauftragte teilt der gesuchstellenden Person in einer stets gleichlautenden Antwort mit, dass in bezug auf sie entweder keine Daten unrechtmässig bearbeitet werden oder dass er bei Vorhandensein allfälliger Fehler in der Datenbearbeitung eine Empfehlung zu deren Behebung an die Zentralstelle gerichtet hat. Ein Rechtsmittel gegen diese Mitteilung ist ausgeschlossen. ❸ Die betroffene Person kann jedoch von der Eidgenössischen Datenschutzkommission verlangen, dass diese die Mitteilung des Eidgenössischen Datenschutzbeauftragten oder den Vollzug der allenfalls von ihm abgegebenen Empfehlung überprüft. ❹ Die Eidgenössische Datenschutzkommission teilt der betroffenen Person in einer stets gleichlautenden Antwort mit, dass die Prüfung gemäss ihrem Gesuch durchgeführt worden ist. ❺ Schliesslich wird den registrierten Personen, die ein Auskunftsgesuch gestellt haben, beim Dahinfallen der Interessen der Strafverfolgung an der Geheimhaltung, spätestens aber bei Ablauf der Aufbewahrungsdauer, nach Massgabe des Datenschutzgesetzes Auskunft erteilt, sofern dies nicht mit unverhältnismässigem Aufwand verbunden ist. Das folgende Schema legt die Schritte dieses komplexen Verfahrens in vereinfachter Weise dar:

1.2. RIPOL-4 - Die Entwicklung des Systems

Das Bundesamt für Polizeiwesen führt in Zusammenarbeit mit den Kantonen das automatisierte Fahndungssystem RIPOL. Eine spezielle Bestimmung im Schweizerischen Strafgesetzbuch bildet die formelle gesetzliche Grundlage für dieses zur Personen- und Sachfahndung geschaffene System. Als Informatikinstrument zur Verbreitung von Personenbeschreibungen konzipiert, hat das System RIPOL seit seiner Einführung verschiedene Entwicklungen durchlaufen. Im Mittelpunkt der letzten - noch andauernden - Entwicklungsphase steht insbesondere die Schaffung einer neuen Datenbank für sämtliche noch ungeklärten Straftaten sowie für die Sachfahndung. Nachdem das Bundesamt für Polizeiwesen uns dieses Entwicklungsprojekt im Rahmen des Informatikkonzepts RIPOL-4 vorgelegt hatte, liess es uns im Vernehmlassungsverfahren ein Projekt zur Abänderung der jetzigen RIPOL-Verordnung zur Stellungnahme zukommen. Unsere Prüfung des Entwurfs hat sich auf die Einhaltung des durch das Strafgesetzbuch abgesteckten rechtlichen Rahmens und die Umsetzung der datenschutzrechtlichen Anforderungen konzentriert, die wir bei der Prüfung des Konzepts geltend gemacht hatten.

Das Informatiksystem RIPOL ist ein automatisiertes Personen- und Sachfahndungssystem, das die Unterstützung von Behörden des Bundes und der Kantone bei der Erfüllung bestimmter, klar festgelegter gesetzlicher Aufgaben zum Zweck hat. Die gesetzlichen Aufgaben werden in Artikel 351bis des Strafgesetzbuchs, der die formelle gesetzliche Grundlage des Systems RIPOL darstellt, abschliessend aufgezählt. Zu diesen Aufgaben gehören namentlich: Verhaftung von Personen oder Ermittlung ihres Aufenthaltsortes zu Zwecken der Strafuntersuchung oder des Straf- und Massnahmenvollzugs, Anhaltung bei vormundschaftlichen Massnahmen oder fürsorgerischer Freiheitsentziehung, Ermittlung des Aufenthaltes vermisster Personen, Kontrolle von Fernhaltemassnahmen gegenüber Ausländern oder aber die Fahndung nach abhandengekommenen oder gestohlenen Fahrzeugen und Gegenständen. Verschiedene Behörden können über das RIPOL Personenbeschreibungen verbreiten. Das Gesetz legt ausserdem fest, welchen Behörden Daten aus dem System RIPOL bekanntgegeben werden dürfen.

Nebst dem umschriebenen rechtlichen Rahmen ist zu erwähnen, dass das RIPOL seit seiner Einführung in technischer Hinsicht mehrfach ausgebaut und weiterentwickelt wurde. Ziel der letzten, noch laufenden Ausbauetappe ist insbesondere die Schaffung einer neuen Datenbank für alle ungeklärten Straftaten und für die Sachfahndung innerhalb des Systems RIPOL. Das diesbezügliche, als RIPOL-4 bezeichnete Konzept wurde uns zur Stellungnahme unterbreitet. Es ist das Ergebnis der vom Bundesamt für Polizeiwesen unternommenen Arbeiten zur Weiterentwicklung des Informatiksystems RIPOL. Dieses Bundesamt hat schon anlässlich eines vom Eidgenössischen Justiz- und Polizeidepartement organisierten Informationstages zu Handen der Presse sein Bestreben, das RIPOL ständig zu perfektionieren, zum Ausdruck gebracht und seine Vorhaben in einer erläuternden Broschüre mit dem Titel "Ausblick" veröffentlicht, die bei diesem Anlass verteilt wurde.

Wir verfolgen die Entwicklungen des RIPOL mit umso grösserer Aufmerksamkeit als sie bestimmte gesetzgeberische Anpassungen erforderlich machen. So hat das Bundesamt für Polizeiwesen bei den Arbeiten zur Anpassung der RIPOL-Verordnung, die mit Verabschiedung des Artikels 351bis des Strafgesetzbuchs als formeller gesetzlicher Grundlage des Systems nötig wurde, in seinem Verordnungsentwurf auch bestimmte, für das Konzept RIPOL-4 vorgesehene technische Entwicklungen berücksichtigt.

Gemäss den Informationen, die wir im Zuge der Prüfung dieses Konzepts erhalten haben, besteht bislang auf nationaler Ebene keine einheitliche Datenbank für ungeklärte Straftaten und für die Sachfahndung. Bis heute werden solche Sachverhalte in den Kantonen teils mittels elektronischer Datenverarbeitung, teils mittels Handkartotheken bearbeitet. Nur die wichtigsten Straftaten und die Sachfahndungen werden im "RIPOL-Fahndungsblatt" veröffentlicht, um sicherzugehen, dass wenigstens die schwerwiegendsten Fälle in allen Kantonen bekannt sind. Eine der Zielsetzungen, die mit dem RIPOL-4-Konzept verfolgt werden, besteht darin, das gegenwärtig vorhandene System auszubauen, indem man eine Datenbank und die entsprechenden Anwendungen für die Gesamtheit der ungeklärten Straftaten, die nach schweizerischem Recht strafbar sind, schafft und mit der Sachfahndung kombiniert. Diese Ausweitung von RIPOL ermöglicht den Abbau der kantonalen Systeme und garantiert eine aktualisierte Erfassung der Daten sowie eine nationale Verbreitung dieser Informationen.

Das Anliegen, die polizeiliche Tätigkeit effizienter zu gestalten, rechtfertigt diesen Entwicklungsschritt, der unserer Ansicht nach mit der neuen gesetzlichen Grundlage von RIPOL vereinbar ist. Artikel 351bis des Strafgesetzbuchs sieht nämlich vor, dass der Bund in Zusammenarbeit mit den Kantonen ein automatisiertes Personen- und Sachfahndungssystem führt, das der Unterstützung der Behörden des Bundes und der Kantone bei der Erfüllung ihrer gesetzlichen Aufgaben - wie etwa der Verhaftung von Personen oder der Ermittlung ihres Aufenthaltes im Rahmen eines gerichtlichen Verfahrens sowie der Fahndung nach abhandengekommenen oder gestohlenen Fahrzeugen und Gegenständen - dienen soll. Bei der Prüfung des Entwurfs der neuen RIPOL-Verordnung haben wir uns bemüht, darauf zu achten, dass die vorgeschlagenen Bestimmungen mit dem gesetzlichen Rahmen von Artikel 351bis des Strafgesetzbuchs vereinbar sind. Dasselbe haben wir bei der Prüfung der rechtlichen Umsetzung der technischen Entwicklungen getan, welche unsere Zustimmung erhielten.

So haben wir hervorgehoben, dass die im Gesetz aufgestellte Liste der Zwecke von Personenbeschreibungen, die ins RIPOL eingegeben werden können, abschliessend ist. Insbesondere haben wir daran erinnert, dass gerade dieser abschliessende Charakter während der Parlamentsdebatten bezüglich der Verabschiedung der formellen gesetzlichen Grundlage von RIPOL immer wieder betont wurde. Im Verlauf verschiedener Bemerkungen in bezug auf die Einhaltung des rechtlichen Rahmens, der durch das Strafgesetzbuch vorgegeben wird, haben wir die Abänderung einiger Bestimmungen des Verordnungsentwurfs vorgeschlagen. Wir haben ausserdem empfohlen, bestimmte technische und organisatorische Massnahmen zu präzisieren, die insbesondere die Protokollierung, die Datenchiffrierung, den Gebrauch der Freifelder und die Zugriffsbewilligungen betreffen.

Schliesslich haben wir festgestellt, dass eventuelle Veränderungen der "Philosophie" des Systems keinesfalls unsere Zustimmung erhielten. Hierunter fiele etwa die Umfunktionierung dieser auf Ausschreibungen ausgerichteten Datenbank zu einem System, das den Vergleich aller in den verschiedenen Datenbanken des Systems enthaltenen Informationen und damit die Rasterfahndung ermöglichen würde. Derartige Veränderungen der Grundlagen von RIPOL wären in der Tat mit Artikel 351bis des Strafgesetzbuchs nicht zu vereinbaren. Diese Bestimmung wurde geschaffen, um dem RIPOL als System zur Verbreitung von Fahndungsdaten eine formelle gesetzliche Grundlage zu geben. Dies wurde auch im Laufe der Parlamentsdebatten bestätigt. Zudem hat der Bundesrat im Rahmen der Botschaft über die Datenbearbeitung auf dem Gebiet der Strafverfolgung deutlich zum Ausdruck gebracht, dass die Bearbeitung polizeilicher Informationen auch eine gesetzliche Regelung

voraussetzt, wenn sehr leistungsstarke Informatikmittel eingesetzt werden, was bei der Rasterfahndung der Fall ist.

Gestützt auf diese Überlegungen haben wir den Entwurf für eine Weiterentwicklung des RIPOL-Systems geprüft, der vorsieht, eine Datenbank für unaufgeklärte Straftaten, kombiniert mit der Sachfahndung, zu schaffen. Wie bereits erwähnt, haben wir dieser Entwicklung grundsätzlich zugestimmt, da sie durch Artikel 351bis des Strafgesetzbuchs abgedeckt ist. Wir haben allerdings den Standpunkt vertreten, dass die diesbezügliche Bestimmung im Verordnungsentwurf aufgrund ihrer Formulierung Verwirrung stiften könnte. Es besteht die Gefahr, dass aufgrund der Formulierung Rasterfahndung und Datenabgleich vorgenommen werden. Angesichts der Tatsache, dass es sich hierbei um einen äusserst heiklen Bereich handelt, ist es wichtig, darauf zu achten, dass die Verordnung zum RIPOL keinerlei zweideutige oder unklare Stellen enthält. Wir haben empfohlen, in der Verordnung ausdrücklich festzulegen, dass keine Verbindung zwischen den Datenbanken des Systems und keine Rasterfahndung zulässig sind. Eine solche Lösung, welche die technische Entwicklung des RIPOL auf transparente Weise rechtlich festschreiben würde, hätte eine verbesserte Rechtssicherheit zur Folge.

1.3. Geldwäscherei - Vorentwurf zum Bundesgesetz

Das Eidgenössische Finanzdepartement hat einen Vorentwurf des Bundesgesetzes zur Bekämpfung der Geldwäscherei im Finanzsektor in die Vernehmlassung geschickt. In unserer Stellungnahme haben wir hauptsächlich darauf hingewiesen, dass trotz der zahlreichen Datenbearbeitungen, welche die Anwendung dieses Gesetzes mit sich bringen wird, der Datenschutz in keiner Weise in die Überlegungen miteinbezogen und keine einzige datenschutzspezifische Bestimmung in den Vorentwurf aufgenommen wurde.

Am 12. Januar 1994 hat der Bundesrat das Eidgenössische Finanzdepartement ermächtigt, einen Vorentwurf zu einem Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (nachfolgend: "Vorentwurf") in die Vernehmlassung zu schicken. Die im Januar 1995 veröffentlichten Ergebnisse des Vernehmlassungsverfahrens haben das Interesse der betroffenen Kreise an der Einführung der Identifizierungs- und Meldepflicht des Financiers, aber auch ihre Vorbehalte in bezug auf die konkrete Ausgestaltung dieser beiden Verpflichtungen aufgezeigt. Aufgrund der Ergebnisse des Vernehmlassungsverfahrens hat der Bundesrat beschlossen, den Vorentwurf vollständig zu überarbeiten. Wir haben diesen Beschluss mit grosser Befriedigung zur Kenntnis genommen, da nun bei der Ausführung dieses neuen Auftrags unsere im Rahmen des Vernehmlassungsverfahrens vorgebrachten Bemerkungen berücksichtigt werden können.

In der Tat haben wir die Eidgenössische Finanzverwaltung darauf aufmerksam gemacht, dass der Vorentwurf des Gesetzes zur Bekämpfung der Geldwäscherei für die verschiedenen betroffenen Stellen einen beachtlichen Datenbearbeitungsaufwand mit sich bringen wird. Dies gilt vor allem für die Erhebung von personenbezogenen Informationen, die beispielsweise für den Identitätsnachweis der Beteiligten nötig sind, aber auch für die Aufbewahrung von Daten, wie Dokumente und Belege einschliesslich Identitätsdokumenten und ebenso für organisatorische Massnahmen, wie etwa die Einrichtung eines Zentralregisters oder anderer Massnahmen, die die Erteilung der gewünschten Informationen ermöglichen. Schliesslich werden auch Datenbekanntgaben und -austausche erfolgen, da der Gesetzesvorentwurf eine Meldepflicht gegenüber den Strafverfolgungsbe-

hörden, dem Bundesamt für Polizeiwesen oder der Eidgenössischen Finanzverwaltung vorsieht. Letzteren muss auch durch die kantonalen Strafverfolgungsbehörden Meldung über die direkt bei ihnen eingegangenen Informationen erstattet werden.

Dennoch findet sich in den Erläuterungen zum Vorentwurf vom Januar 1994 keine Erwägung zu den datenschutzrechlichen Aspekten und es wurde keine spezifische Bestimmung zum Datenschutz in den Vorentwurf eingefügt. Unsere Nachforschungen haben ergeben, dass der Datenschutz von der interdepartementalen Arbeitsgruppe bei der Ausarbeitung des Vorentwurfs angesichts der verschiedenen noch bestehenden Unsicherheiten und der noch offenstehenden Optionen (z. B. Wahl der Koordinationsstelle und der Übermittlungsinstanz) überhaupt nicht angesprochen wurde. Da sich die datenschutzrechtlichen Gegebenheiten je nach letztlich getroffener Wahl möglicherweise noch beträchtlich verändern werden, haben wir im Einverständnis mit der Eidgenössischen Finanzverwaltung beschlossen, unsere Intervention auf eine provisorische Auflistung der "heiklen" Punkte, welche eine besondere Aufmerksamkeit erfordern, zu beschränken.

Wir haben darauf hingewiesen, dass im Zusammenhang mit der Bekämpfung der Geldwäscherei im Finanzsektor das Datenschutzgesetz sowohl hinsichtlich seiner allgemeinen Grundsätze als auch in seinen öffentlichrechtlichen (für das Bundesamt für Polizeiwesen und die Eidgenössische Finanzverwaltung) und privatrechtlichen Teilen (für die Banken, Treuhandgesellschaften, Vermögensverwalter, freien Anwälte usw.) anwendbar ist. Hingegen findet es keine Anwendung auf Datenbearbeitungen, die im Rahmen von Strafverfahren stattfinden, welche von den zuständigen Strafverfolgungsbehörden eröffnet werden. Unabhängig von der Anwendbarkeit des Bundesgesetzes über den Datenschutz haben wir angesichts der vielen im Gesetzesvorentwurf vorgesehenen Bearbeitungen von Personendaten die Aufnahme spezifischer Datenschutzbestimmungen in den Vorentwurf verlangt.

Was die Dauer der Datenaufbewahrung durch den Financier anbelangt haben wir hingewiesen, dass der Vorentwurf - unter Vorbehalt besonderer Vorschriften für die Aufbewahrung von Büchern - für Belege und Dokumente eine Aufbewahrung während mindestens fünf Jahren vorschreibt. Da diese Bestimmung auch Identitätsdokumente einschliesst, für die eine minimale Aufbewahrungsdauer von fünf Jahren ab Beendigung der Geschäftsbeziehungen vorgesehen ist, haben wir verlangt, dass für die Aufbewahrung dieser Angaben durch den Financier auch eine Maximaldauer vorgesehen wird. Ausserdem setzt diese Aufbewahrungspflicht ein Zentralregister oder andere Massnahmen voraus, die es ermöglichen, die verlangten Angaben zu liefern. Solche Register mit Angaben über die Kunden, ihre Konten, Sparbücher und Einlagen werden bereits von den Banken und anderen Finanzinstituten geführt. Jedoch wird durch die im Vorentwurf vorgesehene Meldepflicht gegenüber den zuständigen Behörden ein umfangreiches Verfahren für den Informationsaustausch zwischen dem Financier, dem Bundesamt für Polizeiwesen, der Eidgenössischen Finanzverwaltung und den Strafverfolgungsbehörden in Gang gesetzt. Es ist anzunehmen, dass die auf diese Weise bearbeiteten Informationen, namentlich die Ermittlungsergebnisse und die Entscheide seitens der anvisierten Behörden, vom Financier aufbewahrt werden, was die gesetzliche Festschreibung einer Maximaldauer für die Aufbewahrung dieser Daten umso dringlicher werden lässt.

Um die grösstmögliche Wirksamkeit der Bestimmungen über die Meldepflicht zu gewährleisten, sieht der Vorentwurf ein höchstens fünf Tage geltendes Verbot vor, die betroffenen Personen oder Dritte über die Meldung oder laufende Ermittlungen in Kenntnis zu setzen. Diese restriktive Vorschrift auf der Stufe eines formellen Gesetzes gab zu keinen

besonderen Bemerkungen von unserer Seite Anlass. Hingegen haben wir empfohlen, die Möglichkeit einer Verlängerung dieser Frist zu präzisieren und diese auf eine bestimmte Höchstdauer festzulegen.

Bezüglich der Bearbeitung von Daten durch das Bundesamt für Polizeiwesen im Zusammenhang mit dem organisierten Verbrechen und der Geldwäscherei haben wir die Finanzverwaltung auf mehrere, in datenschutzrechtlicher Hinsicht problematische Aspekte hingewiesen. So legt der Vorentwurf die Kompetenzen der zuständigen Behörden fest, insbesondere die Aufgaben der Koordinationsstelle und das Vorgehen bei der Weitergabe von eingegangenen Meldungen. Um die ihm in seiner Funktion als Koordinationsstelle anvertrauten Aufgaben erfüllen zu können, wird das Bundesamt für Polizeiwesen im Prinzip die verschiedenen bei ihm eingehenden Meldungen, die Ermittlungsergebnisse und die ihm von den kantonalen Strafverfolgungsbehörden übermittelten Informationen erheben und aufbewahren müssen. Da dieser Gesetzesentwurf in dieselbe Richtung geht, wie das Gesetz über kriminalpolizeiliche Zentralstellen des Bundes, muss entschieden werden, ob die Zentralstellen des Bundesamtes für Polizeiwesen diese Informationen in demselben Rahmen bearbeiten sollen, den auch das Bundesgesetz über kriminalpolizeiliche Zentralstellen für seine Datenbearbeitungen vorsieht, oder ob die Daten im Gegenteil völlig getrennt bearbeitet werden sollen. Von dieser Entscheidung wird abhängen, ob es erforderlich ist, im Vorentwurf einen Verweis auf das Gesetz über die kriminalpolizeilichen Zentralstellen anzubringen oder aber eine spezifische Bestimmung über die Bearbeitung von Daten im Zusammenhang mit der Geldwäscherei im Finanzsektor auszuarbeiten. Wenn das Bundesamt für Polizeiwesen die Daten über das organisierte Verbrechen und diejenigen über die Geldwäscherei zusammen bearbeitet, muss dem sowohl im Hinblick auf die Bekanntgabe der Daten als auch hinsichtlich der Ausübung des Auskunftsrechts Rechnung getragen werden. Die Eidgenössische Finanzverwaltung darf dann nämlich nur Zugriff zu den Daten über die Geldwäscherei haben.

Wir haben auch hervorgehoben, dass die Wahl der Koordinationsstelle Auswirkungen auf den Inhalt der auszuarbeitenden Datenschutzbestimmungen haben wird. Überträgt man diese Aufgabe dem Bundesamt für Polizeiwesen, so müssen, wie dargelegt, Präzisierungen in bezug auf die Datenbearbeitungen im Zusammenhang mit dem organisierten Verbrechen und der Geldwäscherei erfolgen. Wird die Eidgenössische Finanzverwaltung als Koordinationsstelle bezeichnet, so sind ebenfalls spezifische Regelungen notwendig, vor allem in bezug auf die Informationen, die bei dieser Behörde durchgehen, sowie im Zusammenhang mit deren vermutlicher Führung einer Datenbank speziell über die Geldwäscherei. Der Vorentwurf sieht in der Tat vor, dass das Bundesamt für Polizeiwesen der Eidgenössischen Finanzverwaltung alle erforderlichen Daten und Informationen zur Verfügung stellen muss.

Die Art und Weise der Datenbekanntgabe und der Zugang zu den Daten haben uns zu zahlreichen Bemerkungen veranlasst. So muss das Ausmass der besagten Zugänge zu den Daten in Funktion der im Rahmen des Vorprojekts getroffenen Wahl für die Bearbeitung der erhobenen und ausgetauschten Informationen geregelt werden. Verschiedene Bestimmungen setzen nämlich voraus, dass von einer zuständigen Stelle zur anderen Meldungen weitergeleitet, Informationen geliefert und Entscheide - wie etwa die Sperrung einer Transaktion, ein strafrechtlicher Entscheid oder eine Einstellungsverfügung - mitgeteilt werden. So wird in den Erläuterungen zum Vorentwurf in bezug auf das Bundesamt für Polizeiwesen und die Eidgenössische Finanzverwaltung unterstrichen, dass auf jeden Fall eine intensive Zusammenarbeit zwischen diesen beiden Behörden stattfinden muss. Jedoch wird nicht präzisiert, welche Übermittlungsarten in Frage kommen. Wir haben die Eidgenössische

Finanzverwaltung daher darauf aufmerksam gemacht, dass, wenn bestimmte Zugriffe auf die im Besitz der Koordinationsstelle befindlichen Informationen oder ein Austausch von Personendaten zwischen dem Bundesamt für Polizeiwesen und der Eidgenössischen Finanzverwaltung über ein Abrufverfahren (Online-Verbindung) stattfinden sollen, eine spezifische Regelung im Gesetz dies ausdrücklich vorsehen muss.

Schliesslich haben wir hervorgehoben, dass, wenn schon - wie bereits erwähnt - die Datenschutzbestimmungen bei hängigen strafrechtlichen Ermittlungen keine Wirkung haben, eine erfolgreiche Anwendung des Gesetzes von einer engen Zusammenarbeit zwischen dem Bundesamt für Polizeiwesen, der Eidgenössischen Finanzverwaltung und den kantonalen Strafverfolgungsbehörden abhängen wird. Bestimmte identische Informationen werden verschiedenen Rechtsbestimmungen unterstellt sein, je nach Behörde, die für ihre Bearbeitung zuständig ist. So werden die kantonalen Verfahrensbestimmungen auf ein hängiges Strafverfahren Anwendung finden. Diese Bestimmungen regeln insbesondere die Rechte der Betroffenen (Einsichtsrecht) und die Datenbearbeitung durch den Untersuchungsrichter. Wie sieht es aber in bezug auf dieselben Daten aus, wenn sie sich in den Händen der Koordinationsstelle befinden? Wir haben deshalb z. B. gefordert, dass sowohl die Aufbewahrungsdauer der bei der Koordinationsstelle befindlichen Informationen als auch das Recht der Betroffenen auf Einsicht in diese Daten ausdrücklich festgelegt werden. Diese beiden Punkte sind auch dann gesetzlich zu regeln, wenn die Eidgenössische Finanzverwaltung in ihrer Rolle als Übermittlungsstelle bestimmte Daten bearbeitet. Und schliesslich ist festzulegen, ob die auf einem Verdacht beruhenden Meldungen von der Koordinations- und/oder von der Übermittlungsstelle aufbewahrt werden dürfen und, wenn ja, für wie lange, wenn von den zuständigen Strafverfolgungsbehörden letztendlich keine Ermittlung eingeleitet wird.

Im Rahmen der Veröffentlichung der Ergebnisse des Vernehmlassungsverfahrens hat das Eidgenössische Finanzdepartement den Bundesrat über unsere Bemerkungen informiert und ihn darauf hingewiesen, dass die Beschaffung, Aufbewahrung und Bekanntgabe von Daten im Rahmen des neuen Gesetzes unter Berücksichtigung des Bundesgesetzes über den Datenschutz zu regeln sind. Wir begrüssen diese Vorgehensweise. Bei der vom Bundesrat verlangten Überarbeitung des Vorentwurfs müssen unsere Bemerkungen berücksichtigt und klare Datenschutzbestimmungen ausgearbeitet werden.

1.4. Revision Strafregisterverordnung

Gleichzeitig mit dem DSG trat ein Artikel im Strafgesetzbuch in Kraft, der regelt, dass Anfragen von Strafjustizbehörden beim Schweizerischen Zentralpolizeibüro (ZEPO) auf Strafregisterauszug während maximal zwei Jahren gespeichert werden. Die Bestimmung sieht weiter vor, dass das ZEPO der anfragenden Strafjustizbehörde mitteilen darf, bei welcher anderen Strafjustizbehörde ein Verfahren hängig ist.

Das ZEPO speichert während zwei Jahren die im Zusammenhang mit hängigen Verfahren ergangenen Gesuche von Strafjustizbehörden des Bundes und der Kantone um Strafregisterauszüge. Erfasst werden die anfragende Behörde, die Personalien der beschuldigten Person, die Beschuldigung und das Datum der Zustellung des Registerauszuges. Ersucht eine Strafjustizbehörde im Rahmen eines Strafverfahrens um einen Strafregisterauszug, so gibt das ZEPO der Strafjustizbehörde die entsprechenden Daten bekannt. Die Strafjustizbehörde meldet dem ZEPO Freisprüche und Einstellungsverfügungen in Verfahren, für die ein Strafregisterauszug eingeholt wurde. Im

Anschluss daran vernichtet das ZEPO die gespeicherten Daten. Die Einzelheiten, insbesondere die Verantwortung für die Datenbearbeitung, die Verfahrensrechte der betroffenen Personen, die Zusammenarbeit mit den Kantonen und die Behörden, die für die Einsicht in die Daten sowie deren Berichtigung und Vernichtung zuständig sind, müssen auf Verordnungsebene geregelt werden. Zu diesem Zweck soll die Strafregisterverordnung revidiert werden. Zur Zeit liegt der Entwurf, an dessen Ausarbeitung wir beteiligt waren, beim Bundesamt für Polizeiwesen, mit dem in dieser Sache eine gute Zusammenarbeit möglich war.

2. Ausländer- und Asylrecht

2.1. Zentrales Ausländerregister ZAR

Aus dem Zentralen Ausländerregister (ZAR) dürfen die Daten nicht gesuchter Personen (unbeteiligte Dritte) durch Abrufverfahren in der Regel nicht bekanntgegeben und in keinem Fall weiterbearbeitet werden.

Letztes Jahr hatten wir dem Inhaber des ZAR, dem Bundesamt für Ausländerfragen, empfohlen, die Bekanntgabe von Daten über die im ZAR aufgeführten etwa 3,5 Mio. Ausländer im Abrufverfahren (Selbstbedienungsprinzip) oder auch nur in grossen Mengen, etwa an das Bundesamt für Polizeiwesen, zu unterlassen. (Vgl. den 1. Tätigkeitsbericht, Seiten 28 bis 30).Wir erachteten eine Bekanntgabe auf Anfrage hin und im Einzelfall als genügend, insbesondere da alle Polizeibehörden und auch das Bundesamt für Polizeiwesen bereits umfassende Zugriffe auf eigens für die Fahndung und den übrigen Polizeibereich geschaffene Datensammlungen haben, in denen kriminelle Personen, darunter auch Ausländer, verzeichnet sind. Das ZAR ist keine Fahndungsdatei. Mit den heute üblichen Bürokommunikationsmitteln ist es zudem möglich, verschiedene verfügbare Datensammlungen oder Teile davon miteinander zu verknüpfen oder abzugleichen (Rasterfahndung). Dies ist rechtlich unzulässig, weshalb auch von der Systemgestaltung her für das ZAR eine Lösung zu wählen ist, welche von vornherein nur zulässige, erlaubte Datenbearbeitungen gestattet (kein gleichzeitiger Vorzugriff auf das ZAR und die Fahndungsdateien des Polizeibereichs.

Der Bundesrat und das Eidgenössische Justiz- und Polizeidepartement haben in der Folge bei der Revision der ZAR-Verordnung beschlossen, dass die Polizei zwar weiterhin im Abrufverfahren auf das ZAR zugreifen darf, dass aber bestimmte Beschränkungen und Auflagen einzuhalten sind:
Zunächst sind die Abfragen nur zur Personenidentifikation gestattet und nur für wenige Datenfelder zulässig. Sie müssen protokolliert und die Protokolle regelmässig kontrolliert werden. Die Daten nicht gesuchter Personen dürfen grundsätzlich nicht bearbeitet werden. Die Rasterfahndung bleibt verboten. Das Bundesamt für Ausländerfragen muss Sicherheit und Organisation bei der Bearbeitung von ZAR-Daten in Zusammenarbeit mit dem Bundesamt für Informatik überprüfen. Das Bundesamt für Polizeiwesen muss die Aufgabenanalyse der Dienste, die ZAR-Daten abfragen, vervollständigen.
Damit haben die zuständigen Behörden zwar eine andere Gewichtung des Persönlichkeitsschutzes bei Datenbearbeitungen im Polizei- und im Ausländerrecht vorgenommen, als wir, sind aber bezüglich der für diese Datenbearbeitungen erforderlichen Schutzvorkehren in wichtigen Fragen unseren Vorschlägen gefolgt.

Die Revision der ZAR-Verordnung warf neben der Frage der on-line-Zugriffe von Polizeibehörden weitere datenschutzrechtliche Fragen auf:

- Wir vertraten die Auffassung, dass die erhebliche Änderung oder Erweiterung eines grossen EDV-Systems, wie dem ZAR den Vorschriften des DSG und der VDSG ohne Rücksicht auf die in Art. 38 festgelegte Übergangsfrist untersteht. Deshalb ist für die Neueinrichtung von on-line-Anschlüssen der Polizeibehörden, durch die auch besonders schützenswerte Daten abgefragt werden können, eine Grundlage in einem formellen Gesetz erforderlich. Indessen vermochte sich der Bundesrat unserer Sichtweise nicht anzuschliessen.
- Ebensowenig drangen wir mit der Anregung durch, die Zulässigkeit der Bekanntgabe von Asyldaten durch das Bundesamt für Flüchtlinge an das ZAR zur Ausstellung von Flüchtlingsausweisen nicht in Art. 5 Abs. 1 lit. b, sondern in den Übergangsbestimmungen der ZAR-Verordnung zu regeln. Ein auf Dauer angelegter derartiger Datenaustausch läuft nämlich im Ergebnis auf eine aus datenschutzrechtlicher Sicht unzulässige gemeinsame Datenbank hinaus. Sobald das Bundesamt für Flüchtlinge die Flüchtlingsausweise in seinem System selbst ausdrucken kann, muss Art. 5 Abs. 1 lit. b der ZAR-Verordnung aber gestrichen werden.

Bekanntgabe von ZAR-Daten an nicht am ZAR angeschlossene Behörden

Eine kantonale Fremdenpolizeibehörde hat uns angefragt, ob Ausländerdaten mittels sogenannter elektronischer Listen in grösserem Umfang an nicht ans ZAR angeschlossene kantonale oder kommunale Behörden bekanntgegeben werden dürfen. Wir wiesen darauf hin, dass das ZAR gemäss ZAR-Verordnung einer Vielzahl genau bezeichneter kantonaler und kommunaler Behörden zur Verfügung steht, die im Abrufverfahren auf die für sie erforderlichen Ausländerdaten zugreifen können. Zudem bietet das ZAR diesen Behörden viele technische Hilfsfunktionen an, so etwa die Möglichkeit, Personen und Dossiers zu suchen oder eine Geschäftskontrolle zu führen. Damit existiert für die in der ZAR-Verordnung genannten Behörden ein modernes elektronisches Arbeitsinstrument. Die weiten und vielfältigen Möglichkeiten zur Datenbearbeitung bedingen indessen einen entsprechend ausgebauten Datenschutz, wie er im ZAR mit vergleichsweise aufwendigen Massnahmen realisiert wurde. Würden die Ausländerdaten - wie verlangt - in grösserem Umfang das System verlassen und an nicht in der ZAR-Verordnung genannte Behörden abgegeben, so würden dadurch nicht nur die Vorschriften der ZAR-Verordnung und des Datenschutzgesetzes verletzt, sondern die im ZAR ergriffenen Massnahmen zum Datenschutz in Frage gestellt. Nach unserer Auffassung sind derartige Datenübernahmen aus dem ZAR daher unzulässig.

Schweizer und Schweizerinnen im Zentralen Ausländerregister

Wir wurden von privater Seite verschiedentlich darauf aufmerksam gemacht, dass auch Schweizer im ZAR verzeichnet sind und dass deren Daten möglicherweise durch die Polizei über deren automatisiertes Fahndungssystem (RIPOL) abgefragt werden können. Die ZAR-Verordnung sieht verschiedentlich die Bearbeitung von Daten über Schweizer vor:

- So sind gemäss ZAR-Verordnung die Daten der in der Schweiz eingebürgerten Personen nach zwei Jahren im ZAR zu löschen.
- Die kantonalen und kommunalen Arbeitsmarktbehörden melden dem ZAR laufend die Adressen der um eine Bewilligung ersuchenden Arbeitgeber.
- Das Bundesamt für Ausländerfragen erhebt zudem Einladungsschreiben an Ausländer von schweizerischen Gastgebern.
- An die Polizeibehörden werden zudem die für die fremdenpolizeilichen Kontrollaufgaben sowie zur Personenidentifikation erforderlichen Daten be-

kanntgegeben, darunter nach dem Verordnungswortlaut freilich auch die Adresse, die sich im Einzelfall auch auf einen Schweizer oder eine Schweizerin beziehen kann.

Im übrigen finden sich in der ZAR-Verordnung keine Hinweise auf Daten von Schweizern und Schweizerinnen, die im ZAR verzeichnet sind. Eine Ermächtigung zur Bekanntgabe der Namen von schweizerischen Gastgebern an die Polizeibehörden lässt sich nach unserer Auffassung aus diesen Bestimmungen indessen nicht ableiten. Auch scheint es fraglich, ob die Namen der schweizer Gastgeber im ZAR verzeichnet sein dürfen (und müssen). Wir haben eine Abklärung eingeleitet.

2.2. Papierloses Personendossier-Verwaltungssystem (REGI-2)

Grosse EDV-Systeme sind nach Möglichkeit so zu gestalten, dass unzulässige Datenbearbeitungen von vornherein ausgeschlossen sind. Die 'elektronischen Dossiers' sind so aufzubauen, dass die Zugriffe je nach Aufgabe abgestuft gewährt werden können. Das Bundesamt für Ausländerfragen hat sich mit einer entsprechenden Empfehlung unsererseits einverstanden erklärt.

Fragen der Systemgestaltung oder der Architektur grosser EDV-Systeme stellten sich auch beim neu geplanten papierlosen Personendossier-Verwaltungssystem REGI-2 des Bundesamtes für Ausländerfragen (vgl. auch den 1. Tätigkeitsbericht, Seite 29). Der Umstand, dass ein EDV-System einer Vielzahl von Benützern die Bearbeitung grosser Datenmengen gestattet, verlangt eine sorgfältige Einbeziehung datenschutzrechtlicher Aspekte bereits im Zeitpunkt der Entwicklung. Dabei geht es im Wesentlichen darum, mit der konkreten Ausgestaltung des fraglichen Systems die Voraussetzungen dafür zu schaffen, dass sich die Systembenutzer bei ihrer Arbeit datenschutzrechtskonform verhalten. Das System ist also so auszugestalten, dass es von vornherein nur rechtskonforme Datenbearbeitungen zulässt.
Im Einzelnen ist darauf zu achten, dass bei den mutmasslichen Benutzern oder Benutzer-Organisationseinheiten eine Aufgabenanalyse durchgeführt wird. Dabei stellen sich vorab folgende Fragen:

- Ist die Bearbeitung von Personendaten mit elektronischen Mitteln in einem bestimmten Zusammenhang wirklich notwendig und ist sie gesetzlich erlaubt ?
- Müssen dabei besonders schützenswerte Daten oder Persönlichkeitsprofile bearbeitet werden?
- Müssen die Daten auch regelmässig an Dritte bekanntgegeben werden? Gibt es berechtigte entgegenstehende Interessen, und wie sind diese zu bewerten?
- Wie können die Daten wirksam vor Verlust, Veränderung oder unerlaubter Bearbeitung geschützt werden?
- Wie können namentlich Zweckentfremdungen verhindert werden, wenn zum Beispiel bereits eine Zugriffsberechtigung auf verschiedene andere elektronische Datensammlungen besteht?

Diese Fragen waren beim REGI-2 noch nicht alle geklärt und es war auch keine Dokumentation vorhanden, wie sie die Datenschutzverordnung verlangt. Insbesondere war unklar, wie namentlich bei umfangreichen Dossiers sichergestellt werden soll, dass nur die Bekanntgabe der vom Empfänger wirklich benötigten Daten erfolgt, damit dem Zweckbindungs- und dem Verhältnismässigkeitsgrundsatz nachgelebt werden kann. Gleichwohl war beabsichtigt, umfangreiche Datenbearbeitungen im Hinblick auf das REGI-2 zu tätigen (Einlesen bzw. Einscannen der ganzen Dossierbestände des BFA in einen Datenspeicher). Wir empfahlen daher, mit den das REGI-2 vorbereitenden Datenbearbeitungen zuzuwarten, bis die offenen Fragen beantwortet und die Ergebnisse rechtsgenüglich dokumentiert seien. Das BFA hat die Empfehlung akzeptiert und Ende 1994 ein Bearbeitungsreglement vorgelegt, das nun auf seine Datenschutzkonformität überprüft werden kann.

2.3. Automatisiertes Personenregistratursystem AUPER-2

Die Polizei soll auch auf Asyldaten im Automatisierten Personenregistratursystem AUPER-2 des Bundesamtes für Flüchtlinge (BFF) zugreifen können. Bei einer Teilrevision

der AUPER-Verordnung und entgegen einer Empfehlung unsererseits haben sich der Bundesrat und das Eidgenössische Justiz- und Polizeidepartement (EJPD) leider (noch) nicht für einen Schutz der Rechte unbeteiligter Dritter ausgesprochen. Indessen wurde eine Überprüfung des AUPER angeordnet, die zur Zeit im Gang ist.

Letztes Jahr haben wir empfohlen, dass die Daten der im AUPER aufgeführten Asylbewerber und Flüchtlinge nicht im Abrufverfahren oder in grossen Mengen etwa an das Bundesamt für Polizeiwesen (BAP) bekanntgegeben werden dürfen. Wir waren der Meinung, dass eine Bekanntgabe durch das BFF als Inhaber der im AUPER gespeicherten Asyldaten auf Anfrage hin und im Einzelfall genüge. (Siehe 1. Tätigkeitsbericht, Seiten 27 und 28).

Im November des letzten Jahres hat das EJPD dem BAP die vorläufige Weiterführung der bisherigen Bearbeitung von Asylbewerber- und Flüchtlingsdaten aus dem AUPER gestattet, wobei systematische Datenabgleiche mit anderen Datenbanken bzw. Rasterfahndungen weiterhin verboten bleiben und landesrechtliche und völkerrechtliche Übermittlungsverbote von Asyldaten ins Ausland weiterhin zu beachten sind. Gleichzeitig hat das EJPD auf die Notwendigkeit einer umfassenden Sicherheits- und Organisationsanalyse hingewiesen, wie sie kurz zuvor vom BFF beschlossen wurde, und es hat verlangt, deren Ergebnisse seien im Rahmen der anstehenden Totalrevision der AUPER-Verordnung auch in eine definitive Zugriffsregelung umzusetzen. Zur Zeit wird die Trennung des AUPER in einen Bereich Asyl und einen Bereich Polizei geprüft.

In einer vorgezogenen Teilrevision der AUPER-Verordnung hat der Bundesrat zudem den kantonalen Polizeibehörden und den Grenzposten einen on-line-Zugriff auf die Asyldaten des AUPER zugestanden. Entgegen unseren Anträgen wurde darauf verzichtet, wie im übrigen Ausländerbereich auch im Asylbereich Vorschriften für einen angemessenen Schutz namentlich der Rechte unbeteiligter Dritter zu erlassen (beschränkte Datenbekanntgabe bei Suchvorgängen, Verbot der Weiterbearbeitung, Protokollierung der Datenabfragen). Vor dem Hintergrund der aktuellen Entwicklungen im Bereich der Informatik und angesichts der besonderen Gefährdungssituation in ihrer Heimat verfolgter Personen ist dies aus datenschutzrechtlicher Sicht sehr zu bedauern. Dies umso mehr, als offenbar auch die Nationalität unkontrolliert mittels Abrufverfahren und ohne Schutzauflagen bekanntgegeben werden soll. Dadurch werden die betroffenen Personen unnötig einer möglichen zusätzlichen Gefährdung ausgesetzt und es werden zugleich indirekte Hinweise auf die Rassenzugehörigkeit gegeben, welche zu den besonders schützenswerten Daten gehört. Es bleibt zu hoffen, dass der Bundesrat bei der anstehenden umfassenden Revision der AUPER-Verordnung auf seinen Entscheid zurückkommen wird.

In der teilrevidierten AUPER-Verordnung wurden sodann die Grundlagen für eine externe Führung des Sicherheitskontos der Asylbewerber geschaffen, welches im Übrigen im Asylgesetz und in der Asylverordnung 2 geregelt wird. Wir stimmten der beabsichtigten Datenauslagerung in den Bereich der PTT unter strengen Voraussetzungen zu, deren zeitgerechte Erfüllung versprochen wurde. Weil dies bisher leider nicht geschehen ist, haben wir unter Beizug des Bundesamtes für Informatik eine Empfehlung. Danach ist zwischen den zahlreichen beteiligten Stellen ein gesamthaftes Sicherheitskonzept samt einem objektbezogenen Massnahmenkatalog zu schaffen. Die Datenflüsse sind lückenlos zu chiffrieren. Das Konto selber ist im Bereich der PTT von anderen Datenbearbeitungen einwandfrei zu trennen. Es ist ein Bearbeitungsreglement im Sinne der Datenschutzverordnung zu schaffen. Auch im Rahmen dieser Teilrevision haben wir vergeblich darum gebeten, auf einen Datenaustausch zwischen dem AUPER und dem ZAR zu verzichten, welcher den datenschutzrechtlichen Bearbeitungsgrundsätzen zuwiderläuft.

2.4. Revision des Ausländer- und des Asylgesetzes

Die direkten Amtshilfe-Zugriffe auf die Ausländer- und Asyldatenbanken sind zu beschränken und die Daten unbeteiligter Dritter vor unzulässigen 'Suchaktionen' usw. angemessen zu schützen. Datenbekanntgaben ins Ausland sollen nur im Einzelfall und nach einer Interessenabwägung erfolgen. Auch Fingerabdrücke dürfen nur in verhältnismässigem Umfang erhoben werden.

Eine eigentliche 'Auslegeordnung' der bei der Revision des Ausländergesetzes und des Asylgesetzes anstehenden Datenschutzfragen haben wir bereits im 1. Tätigkeitsbericht vorgenommen (vgl. die Seiten 30 bis 32). Zusammenfassend ergeben sich auch heute folgende Kernaussagen:

- Sollen Ausländer- und Asylbewerberdaten etwa den Polizeibehörden im Abrufverfahren zugänglich gemacht werden, so sind Umfang und Zweck dieser Zugriffe in der entsprechenden Rechtsgrundlage hinreichend klar zu umschreiben.
- Soll das ZAR oder das AUPER als (einzige) moderne Möglichkeit zur raschen Identifikation eines Ausländers oder Aslybewerbers eingesetzt werden können, so muss diese Zweckbestimmung aus dem Gesetzestext ersichtlich sein.
- Gleichzeitig muss das Gesetz auch sagen, dass die Daten anderer nicht zu identifizierender Personen (unbeteiligter Dritter) in der Regel nicht bekanntgegeben werden und in keinem Fall weiterbearbeitet werden dürfen. Des weitern muss das Gesetz die hiefür erforderlichen Schutzauflagen, so z.B. die Kontrolle der Abfragen, in den groben Zügen nennen.
- Datenbekanntgaben ins Ausland sollen namentlich im heiklen Asylbereich nur im Einzelfall und nach einer Interessenabwägung möglich sein, weil sonst die Einhaltung landes- und völkerrechtlicher Übermittlungsverbote nicht mehr gewährleistet ist. Abweichungen von diesem Grundsatz zur rascheren Feststellung der Zuständigkeit zur Behandlung eines Asylgesuchs im europäischen Raum müssen ausdrücklich im Gesetz genannt werden, wenn sie sich als wirklich notwendig erweisen.
- Die Erhebung und Weitergabe von Fingerabdrücken nichtkrimineller Ausländer oder Asylbewerber sollen nur als ultima ratio in Frage kommen. Die Aufnahme einer Vorschrift in die Rechtsgrundlage, wonach ausnahmslos bei allen Asylbewerbern, darunter auch Kinder und ältere Menschen, Fingerabdrücke erhoben werden müssen, erachten wir als klar verfassungs- und grundrechtswidrig. Werden Fingerabdrücke erhoben, so sind sie getrennt von Kriminaldaten aufzubewahren und zu bearbeiten.

Staatsverträge

Nach den beiden Rückübernahmeabkommen mit Deutschland und Ungarn betreffend Personen an der Grenze (vgl. 1. Tätigkeitsbericht, Seite 32) konnten in der Berichtperiode auf der gleichen Basis Abkommen mit Rumänien und Bulgarien abgeschlossen werden. Dabei dürfen im Rahmen des Vollzugs dieser Abkommen nur die im Datenkatalog genannten Daten an die ebenfalls im Abkommen genau bezeichneten Behörden weitergegeben werden. Vorbehalten bleiben allfällige Übermittlungsverbote des jeweiligen Landesrechts oder vorrangiger internationaler Abkommen.

Ein weiteres Abkommen mit Deutschland soll den einmaligen Abgleich von Fingerabdrücken einer gewissen Zahl in den beiden Vertragsstaaten aufgenommener Asylbewerber zu statisti-

schen Zwecken gestatten. Wir haben um detaillierte Angaben und Unterlagen gebeten, die uns eine fundierte Würdigung des Vorhabens aus datenschutzrechtlicher Sicht erlauben werden.

3. Telekommunikation

3.1. ISDN / SwissNet 2

Das digitale Kommunikationsnnetz ISDN bringt für die Benutzer und Benutzerinnen eine Menge nützlicher Funktionen. Aus der Sicht des Datenschutzes müssen jedoch insbesondere bei der Rufnummerübermittlung einige Vorbehalte gemacht werden.

Die Telecom PTT hat im Oktober 1992 den kommerziellen Betrieb von ISDN (Integrated Services Digital Network) unter dem Namen «SwissNet 2» aufgenommen. Dabei handelt es sich um ein digitales Kommunikationsnetz, das Dienste wie Sprache, Daten, Fax und Bild integriert. ISDN wird als Primäranschluss (30 Nutzkanäle mit je 64 KBit/s) oder Basisanschluss (2 Nutzkanäle mit je 64 KBit/s) angeboten. Der Basisanschluss kann bereits für Kleinfirmen und private Anwender interessant sein. ISDN bringt den Benutzern viele Vorteile wie bessere Erreichbarkeit, höhere Übertragungsraten, Arbeitserleichterung und dadurch generell mehr Komfort und eine höhere Effizienz in der Kommunikation.

Das digitale Netz erlaubt aber auch die Erfassung und Speicherung von etlichen Kommunikationsdaten, was aus der Sicht des Datenschutzes problematisch sein kann. Aufgrund der Identifikation des Anrufers (Calling Line Identification Presentation, CLIP) erhält der ISDN-Teilnehmer, *bevor* er eine Verbindung entgegennimmt, die Nummer des Anrufers übermittelt. In der Schweiz werden einem ISDN-Teilnehmer auch die Anrufer aus dem herkömmlichen analogen Telefonnetz standardmässig angezeigt, sofern diese an eine digitale Telefonzentrale angeschlossen sind, was heute für die Mehrzahl der Telefonanschlüsse gilt. Verbindet der Angerufene die Rufnummer mit einem elektronischen Verzeichnis, so kann er direkt den Namen und die Adresse des Anrufenden erkennen. Dadurch kann er zwischen wichtigen und unwichtigen Anrufen unterscheiden, aber auch allfällige belästigende Anrufer feststellen. Der Anrufer seinerseits kann sich durch die Rufnummerübermittlung ausweisen.

Allerdings gibt es Fälle, in denen die Identifizierung der Anrufer nicht wünschbar ist. Man denke etwa an anonyme Beratungsdienste (z.B. im medizinischen Bereich) oder an die Möglichkeit, Anrufe bestimmter Personen nicht zu beantworten. Problematisch ist auch, dass der Zugriff auf die Identifikationsdaten nicht in allen Fällen auf den Gesprächsempfänger beschränkt ist (z. B. wenn ein Anschluss von mehreren Personen benützt wird).

Grundsätzlich muss jeder Teilnehmer die Freiheit haben zu entscheiden, ob seine Rufnummer an andere Teilnehmer übermittelt wird. Ideal ist die fallweise Unterdrückung der Rufnummer, das heisst, der Anrufer kann für jeden Anruf erneut entscheiden, ob er seine Nummer übermitteln lassen will oder nicht. Der Angerufene entscheidet ebenso frei, ob er den Anruf entgegennehmen will. Abonnenten, die ihre Nummer beim ISDN-Teilnehmer nicht anzeigen lassen wollen, können diese im heutigen Zeitpunkt gegen eine (einmalige sowie monatliche) Gebühr generell unterdrücken lassen.
Die Telecom PTT realisiert ISDN in Stufen. Das heute verfügbare System (SwissNet 2) erlaubt die fallweise Rufnummerunterdrückung noch nicht. Die nächste nun anstehende

Stufe (SwissNet 3) wird sie aber ermöglichen, allerdings lediglich für die ISDN-Teilnehmer selbst. Nach Angaben der Telecom PTT wird die fallweise Unterdrückung der Rufnummer den Benutzern von analogen Telefonanschlüssen aus technischen und praktischen Gründen nicht gewährt, obwohl eine Realisierung nicht absolut ausgeschlossen wäre.
Aufgrund des dargelegten Sachverhalts haben wir der Telecom PTT folgende Verbesserungsvorschläge unterbreitet:

- Alle Telefonabonnenten sind schriftlich zu informieren, dass ihre Nummer bei ISDN-Teilnehmern angezeigt werden kann und dass die Möglichkeit zur generellen Unterdrückung der Nummer besteht. Diese Information ist so durchzuführen, dass die Kenntnis der Kunden von diesem Sachverhalt vorausgesetzt werden kann. Zum heutigen Zeitpunkt kann keineswegs damit gerechnet werden, dass sich die Telefonabonnenten überhaupt bewusst sind, dass ihre Rufnummern zu jedem ISDN-Teilnehmer übertragen werden.
- Damit der Kunde frei entscheiden kann, darf unseres Erachtens - entgegen der heutigen Regelung - für die Unterdrückung der Rufnummer keine monatliche Gebühr erhoben werden. Höchstens für die Umstellung kann eine bescheidene einmalige Gebühr verlangt werden.
- Weiter sollte für den Anrufer eruierbar sein, ob es sich bei dem gewünschten Anschluss um einen ISDN-Anschluss handelt und somit eine Rufnummerübertragung in Betracht kommt. Aus den für die Kunden zugänglichen Teilnehmerverzeichnissen ist dies bis anhin nicht ersichtlich.

Nebst der automatischen Rufnummererkennung gibt es weitere Funktionen, die insbesondere bei ISDN-Anlagen implementiert sein können und aus datenschutzrechtlicher Sicht problematisch sind:

- Freisprecheinrichtung: Im Telefonapparat befinden sich Lautsprecher und Mikrofon, die es erlauben, freihändig zu telefonieren. Der Gesprächspartner ist dann jedoch auch für andere Personen, die sich im Raum aufhalten hörbar, was ihm unter Umständen nicht bewusst ist.
- Direktes Ansprechen: Hier aktiviert der *Anrufer* Lautsprecher und Mikrofon beim Angerufenen, um diesen direkt ansprechen zu können. Diese Installationen können auch dazu dienen, einen Lauschangriff auf einen Raum durchzuführen. Um Missbräuche zu verhindern, muss am Telefonapparat deutlich erkennbar sein, ob das Mikrofon eingeschaltet ist oder nicht.

3.2. Internet

Beim Internet handelt es sich um das weltweit grösste Computernetz, genauer um ein Netz von Netzen, das eine gigantische Informationsmenge enthält. In letzter Zeit hat sich die Benutzerzahl stark erhöht. Grund genug, Überlegungen aus der Sicht des Datenschutzes anzustellen.

Vorläufer des Internet war ein US-amerikanisches militärisches Netz, das möglichst dezentral aufgebaut sein sollte, um auch bei einem Teilausfall noch funktionsfähig zu sein. Später wurde das Netz vor allem auf den universitären wissenschaftlichen Sektor ausgedehnt. Seit einiger Zeit nutzen immer mehr auch Firmen und private Personen das immense Informationsangebot und stellen selber Informationen im Netz zur Verfügung. Der Internet-Benutzer hat die Möglichkeit, die verschiedensten Anwendungen zu nutzen: Er kann

E-Mails versenden und empfangen, sich an öffentlichen elektronischen Diskussionsforen (sogenannte Newsgroups) beteiligen, bestimmte Dateien von einem entfernten Rechner holen, von seinem Terminal aus auf einem andern Rechner im Internet arbeiten, wie wenn er selbst an Ort und Stelle wäre. Weiter existieren einfach zu bedienende Abfrage-Schnittstellen, wie das sehr verbreitete «World Wide Web», um auf das schier unermessliche Informationsangebot zugreifen zu können. Das Internet hat in letzter Zeit sehr stark an Popularität gewonnen, die Benutzerzahl wird heute auf ungefähr 30 bis 40 Millionen geschätzt und ein Ende des Aufschwungs ist bisher nicht abzusehen.

Aus datenschutzrechtlicher Sicht stösst das Internet auf erhebliche Bedenken:

- Im Internet gibt es keinen Zentralrechner. Ebenso gibt es keine zentrale Kontrollinstanz, die über Verletzungen im Datenschutzbereich wacht. Faktisch kann jeder im Internet machen, was er will. Daher vermittelt es auch den Eindruck eines chaotischen Gebildes. Einen genauen Überblick über die Situation im Internet scheint niemand zu haben.
- Problematisch ist nebst dem Fehlen einer neutralen Kontrollinstanz, dass keine einheitlichen internationalen oder gar globalen datenschutzrechtlichen Regelungen vorhanden sind, aufgrund derer der Datenschutz über die Ländergrenzen hinaus auch für das Internet Gültigkeit hätten. Massgeblich dürfte im jetzigen Zeitpunkt noch immer diejenige Datenschutzregelung sein, welche in dem Land besteht, von dem aus die Daten verschickt oder zum Abruf bereitgestellt werden.
- Ein Grossteil der über Internet angebotenen Informationen ist zum allgemeinen öffentlichen Abruf gedacht. In diesem Zusammenhang ist darauf zu achten, dass nicht Personendaten zum Abruf zur Verfügung gestellt werden, die für sich genommen unproblematisch erscheinen, jedoch durch Verknüpfung mit anderen auch zum allgemeinen öffentlichen Abruf gedachten Personendaten zu Persönlichkeitsprofilen zusammengestellt werden können. Nicht vertrauliche Daten, die zum allgemeinen Abruf gedacht sind, sind nicht problematisch. Die Frage der Vertraulichkeit kommt jedoch ins Spiel, wenn etwa persönliche E-Mails und nicht für die Öffentlichkeit bestimmte Daten über das Netz versandt werden. Standardmässig bestehen keine Massnahmen, welche die Vertraulichkeit garantieren. Ein Internet-E-mail kann auf seinem Weg vom Sender zum Empfänger von vielen Augen gelesen werden.
- Ein weiteres Problem bietet die Überprüfung der Identität eines Kommunikationspartners. Der Empfänger einer Information kann nie sicher sein, ob der Absender auch tatsächlich derjenige ist, den er zu sein vorgibt, da das Internet standardmässig keine technischen Vorkehrungen zur Sicherstellung der Authentizität kennt.
- Durch Aufzeichnung und Analyse der Kommunikationsbeziehungen (beispielsweise im E-Mail-Verkehr) können Kommunikationsprofile entstehen, das heisst, es kann festgestellt werden, mit welchen Partnern eine Person wann und wie oft Informationen austauscht.
- Auch durch die Nutzung von allgemeinzugänglichen Informationen (Informationsseiten, Datenbanken, öffentliche Dateibestände usw.) können Personendaten entstehen. Die Problematik ist vergleichbar mit derjenigen der Nutzung des interaktiven Fernsehens, das an anderer Stelle in diesem Bericht (S. 37) erwähnt ist. Unabhängig von der Aufzeichnung der abgefragten Daten selber können durch die Registrierung der Zeiten, während denen ein Benutzer im Netz «aktiv» ist, Rückschlüsse auf sein Verhalten im Büro (oder auf sein Freizeitverhalten bei privater Nutzung) gezogen werden.
- Im Internet existieren mehrere tausend Newsgroups zu den verschiedensten Themen. Newsgroup-Artikel, die eine bestimmte Person ins Netz speist, können mit einfachen

Programmen systematisch auf bestimmte Stichworte ausgewertet werden. So entstehen unter Umständen umfassende Bilder der Ansichten, Interessen und Aktivitäten der Personen, die Newsgroup-Artikel schreiben. Naheliegend ist der Missbrauch der Daten für geziehlte Werbesendungen. Der Phantasie sind jedoch mit bezug auf die Verwendung kaum Grenzen gesetzt.

Eine Anzahl Risiken können die Benutzer auf eigene Initiative und Verantwortung mit technischen und organisatorischen Massnahmen selbst beschränken. Vertrauliche Informationen können chiffriert, die Authentizität von Dokumenten mit elektronischen Unterschriftsverfahren verbessert werden. Firmeninterne Netze, die mit dem Internet kommunizieren sollen, können mit speziellen Zwischenrechnern abgeschottet werden, um sich vor Angriffen aus dem Internet zu schützen. Es ist wichtig, dass jede Person, die das Internet benutzt, sich über die dabei entstehenden Gefahren und Risiken im Klaren ist. Wer unverschlüsselte Nachrichten verschickt, muss damit rechnen, dass diese grundsätzlich von Dritten gelesen werden können. (Zur Problematik, dass Personen in elektronischen Verzeichnissen Daten über andere Personen zum Abruf zur Verfügung stellen, siehe auch Ziffer 3.3. nachstehend).

Da über Internet Daten international und weltweit verschickt oder zum Abruf bereit gestellt werden, ist darauf hinzuweisen, dass der Datenschutz in den einzelnen Ländern, in welche die Daten gelangen können, unterschiedlich ausgebaut ist. Gemäss DSG darf eine Bekanntgabe von Daten ins Ausland dann nicht erfolgen, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde. Das ist namentlich dann der Fall, wenn ein Datenschutz fehlt, der dem schweizerischen gleichwertig ist. Die meisten aufgezeigten Probleme bestehen nicht nur im Internet, sondern auch bei kommerziellen Online-Diensten (wie z.B. Compuserve) und bei Mailbox-Netzen, die im übrigen oft auch über Schnittstellen zum Internet verfügen.

3.3. Elektronische Verzeichnisse

Werden Personendaten auf elektronischen Netzen national, international oder global durch andere als die betroffenen Personen selbst zum Abruf zur Verfügung gestellt, so stellt aus datenschutzrechtlicher Sicht die Verfügbarkeit und Verknüpfbarkeit der Daten sowie die fehlende Kontrolle darüber, was mit den Daten geschieht, ein grosses Problem dar.

Der Einsatz der elektronischen Datenbearbeitung nimmt immer mehr zu. Ein Beispiel dafür sind die sogenannten elektronischen Verzeichnisse, in denen sich immer öfter Personendaten finden. Zum Teil befinden sie sich in geschlossenen Netzen, so dass nur ein bestimmter Personenkreis auf darin enthaltene Daten zugreifen kann. Dagegen steht eine Unzahl von elektronischen Verzeichnissen in offenen Netzen zum Abruf bereit, was dazu führen kann, dass darin enthaltene Daten national, international oder gar global von jedermann abrufbar sind. Aus datenschutzrechtlicher Sicht ist zwischen solchen Datenbearbeitungen im allgemeinen und denen, die durch den Arbeitgeber vorgenommen werden, zu unterscheiden.

Im allgemeinen

Wer über Datenleitungen Personendaten im Abrufverfahren zugänglich macht, ist an die Grundsätze des Datenschutzgesetzes gebunden. Diese Grundsätze finden Anwendung sowohl auf Angaben über Qualifizierungen, Spezialitäten, Hobbies, Körpermasse usw. einer bestimmten oder bestimmbaren Person, als auch auf die Angabe von Name, Adresse, Telefonnummer, FAX-Nummer, E-Mail-Adresse und anderer Kommunikationsparameter. Je heikler die bearbeiteten Personendaten sind, desto höher sind die Anforderungen an den Datenschutz. Wer Angaben über andere Personen zugänglich macht, hat auch für die Datensicherheit zu sorgen. Dazu gehören insbesondere die Vertraulichkeit, die Verfügbarkeit und die Richtigkeit der Daten. Für den Fall, dass Daten international oder gar global zum Abruf bereit gestellt werden, ist zu beachten, dass Daten nicht ins Ausland bekanntgegeben werden dürfen, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde. Das ist namentlich dann der Fall, wenn in dem betreffenden Land ein Datenschutz fehlt, der mit dem schweizerischen vergleichbar ist. Die fehlenden Datenschutzregelungen können durch vertragliche Vereinbarungen ersetzt werden.

Werden durch private Personen Angaben über andere Personen auf elektronischen Netzen zum Abruf national, international oder global bereitgestellt, so sollte eine schriftliche Einwilligung der betroffenen Person vorliegen. Sie umfasst idealerweise Kenntnisnahme von:

- den bearbeiteten Daten,
- dem Netz, auf dem die Daten verfügbar sind,
- dem Zweck der Bearbeitung auf dem Netz,
- den Möglichkeiten und Risiken des Netzes (Verfügbarkeit, Verknüpfbarkeit),
- einer allfälligen weltweiten Verfügbarkeit,
- dem allfälligen Fehlen einer adäquaten Datenschutzgesetzgebung in bestimmten Ländern, in denen auf die Daten zugegriffen werden kann.

Den betroffenen Personen sollte das Recht eingeräumt werden, die erfassten Daten selber zu bestimmen und ihre Zustimmung zu widerrufen.
Eine entsprechende Einwilligungserklärung kann wie folgt lauten:

Durch den Arbeitgeber
Immer mehr Firmen gehen dazu über, Angaben über ihre Mitarbeiter in einem elektronischen Verzeichnis firmenintern und/oder auch für Dritte zum Abruf bereitzustellen. Auf diesem Weg kann in der Regel auf Name, Adresse und andere Kommunikationsparameter von Mitarbeitern sowie zum Teil auf weitergehende Informationen wie Qualifikationen, Fotos usw. zugegriffen werden. Diese Daten werden - selbst wenn sie wie Name und Adresse öffentlich zugänglich sind - dadurch, dass sie im elektronischen Verzeichnis eines bestimmten Arbeitgebers erscheinen, aus dem neutralen Kontext öffentlicher Abonnentenverzeichnisse herausgenommen und in einen spezifischen Kontext hineinversetzt, aus dem zum Beispiel ersichtlich ist, bei welchem Arbeitgeber eine bestimmte Person tätig ist. Die Verknüpfung von an sich "harmlosen" Personendaten mit einem solchen Kontext kann sogar zu besonders schützenswerten Personendaten führen, etwa wenn bekanntermassen ein Arbeitgeber nur Mitarbeiter einer bestimmten Religionszugehörigkeit oder einer bestimmten politischen, weltanschaulichen oder gewerkschaftlichen Anschauung beschäftigt.

Für das privatrechtliche Arbeitsverhältnis sieht Art. 328b OR vor, dass der Arbeitgeber Daten über den Arbeitnehmer nur bearbeiten darf, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrags erforderlich sind (vgl. im einzelnen S. 44 ff. und 1. Tätigkeitsbericht, S. 53). Diese Bestimmung regelt auch die Bekanntgabe von Personendaten wie Name, Adresse und andere Kommunikationsparameter durch den Arbeitgeber. Die Daten dürfen also nur bekanntgegeben werden, wenn dies für die Durchführung des Arbeitsvertrags erforderlich ist. Dies kann zum Beispiel der Fall sein, wenn bestimmte Arbeitnehmer als Ansprechpartner gegenüber der Öffentlichkeit fungieren.
Ebenso kann die Bekanntgabe der Kommunikationsparameter eines Mitarbeiters gegenüber einem Verhandlungspartner erforderlich sein, wenn der betreffende Mitarbeiter bei den vorvertraglichen oder vertraglichen Verhandlungen als Ansprechpartner auftritt. Von Art. 328b OR nicht abgedeckt ist dagegen ein allgemeines, für jedermann zugängliches Verzeichnis sämtlicher Mitarbeiter, ohne dass eine solche Bekanntgabe zur Durchführung des Arbeitsvertrages erforderlich wäre.
Da Art. 328b OR (einseitig) zwingend ist, darf von ihm weder durch Abrede, noch durch Normalarbeits- oder Gesamtarbeitsvertrag zuungunsten des Arbeitnehmers abgewichen werden. Zugunsten des Arbeitnehmers darf von Art. 328b OR abgewichen werden. Ob das Bekanntgeben von Kommunikationsparametern eines Mitarbeiters sich zuungunsten der betreffenden Person auswirkt, ist eine Frage des Einzelfalles und kann nicht von vornherein allgemein beantwortet werden. Es ist durchaus denkbar, dass die allgemeine Bekanntgabe der Kommunikationsparameter aufgrund des Tätigkeitsbereichs des Arbeitgebers (Sexgewerbe, religiöse oder rassische Einrichtungen, Sekten usw.) nachteilige Auswirkungen für den Arbeitnehmer zur Folge haben kann. Auch in anderen Fällen sind - vielleicht weniger krasse - Benachteiligungen möglich. Von Art. 328b OR darf auch nicht mit Einwilligung des Arbeitnehmers abgewichen werden.

In Fällen, in denen die Voraussetzungen von Art. 328b OR nicht erfüllt sind, ist es daher am sinnvollsten, wenn der Arbeitgeber nach vorheriger eingehender Information seiner Mitarbeiter über die technischen und tatsächlichen Folgen (wie weltweite Abrufbarkeit, Kopierbarkeit) diesen die Plattform des elektronischen Verzeichnisses für die Eingabe und damit für die Bekanntgabe ihrer eigenen Kommunikationsparameter zur Verfügung stellt und ihnen sowohl die Eingabe, als auch den Inhalt und den Umfang der eingegebenen Daten sowie deren Änderung oder Löschung freistellt. An die Freiwilligkeit einer Datenbekanntgabe sind generell hohe Anforderungen zu stellen. Dies gilt erst recht im Verhältnis Arbeitgeber/Arbeitnehmer. Aufgrund des Arbeitsklimas, des Gruppendrucks oder anderer -

vielleicht nur unterschwellig vorhandener - Machtgefälle kann die vordergründige Freiwilligkeit in Wahrheit auf einem starken Druck beruhen und damit faktisch fehlen.

3.4. Detaillierter Taxauszug

Telefon-Abonnenten können einen detaillierten Taxauszug verlangen. Dieser gibt das Datum und die Dauer des Gesprächs, die Höhe der Taxe sowie die um die vier letzten Stellen gekürzte Telefonnummer des Gesprächpartners an. Verschiedentlich gingen bei uns Beschwerden von Privatpersonen ein, die einen Taxauszug mit der vollständigen Telefonnummer des Gesprächspartners wünschten.

Gemäss Fernmeldegesetz (FMG) dürfen die PTT-Betriebe dem Abonnenten eines Anschlusses Auskunft erteilen über Zeitpunkt, Dauer und Entgelt der Verbindungen, die über diesen Anschluss hergestellt wurden. Zudem dürfen sie die Ortszentralen bekanntgeben, mit denen die angewählten Anschlüsse verbunden sind. Die vollständige Rufnummer sowie Name und Adresse der angewählten Abonnenten dürfen nicht mehr bekanntgegeben werden. Der Grund für diese Einschränkung der Datenbekanntgabe liegt im Schutz von Drittpersonen, die vom Apparat des Abonnenten aus telefonieren. Die PTT-Betriebe unterstehen dem Fernmeldegeheimnis. Sie dürfen dem Abonnenten gegenüber keine Angaben darüber machen, welche Drittperson von seinem Anschluss aus mit wem wie lange telefoniert hat, es sei denn, es bestünde dazu eine gesetzliche Verpflichtung. Diese Regelung kann jedoch z.B. in Fällen, in denen der Anschluss ausschliesslich vom Abonnenten selbst benutzt wird, zu stossenden Ergebnissen führen. Die jetzige Fassung wurde vom Parlament im Bewusstsein beschlossen, dass die Regelung einen Kompromiss darstellt zwischen dem Interesse des Abonnenten an einem vollständigen Taxauszug und demjenigen Dritter, die denselben Anschluss benützen und ihrer Gesprächspartner an der Vertraulichkeit ihrer Gespräche.

Im Jahre 1993 wurde eine an den Nationalrat gerichtete Petition, die eine Abänderung der gesetzlichen Grundlagen verlangte, damit die PTT-Betriebe wieder die Möglichkeit hätten, einen vollständigen Taxauszug zu erstellen, von einer Mehrheit der Kommission des Nationalrates abgelehnt. Eine bessere Lösung für Abonnenten, die ihren Anschluss alleine benutzen, kann allenfalls im Rahmen einer Revision des FMG gesucht werden. Entsprechende Revisionsvorhaben werden vorwiegend von der Frage geprägt sein, ob und wie die ausschliessliche Benutzung des Anschlusses durch den Abonnenten bewiesen werden und ob und wie die PTT-Betriebe die entsprechenden Angaben kontrollieren können. Solange nicht eine Lösung gefunden werden kann, die eine einwandfreie Unterscheidung zwischen der Benutzung des Anschlusses durch Dritte (auch mögliche Gäste) und der ausschliesslichen Benutzung durch den Abonnenten erlaubt und damit überprüft werden kann, ob ein Anschluss ausschliesslich vom Abonnenten benutzt wird, hat unseres Erachtens das Interesse des Abonnenten an einem vollständigen Taxauszug hinter dem Interesse der Dritten am Schutz ihrer Persönlichkeit zurückzustehen.

3.5. Verkaufsdatenbank der PTT-Betriebe

Die PTT-Betriebe sind verpflichtet, nach betriebswirtschaftlichen Grundsätzen zu arbeiten. Wie jedes Unternehmen, das nach solchen Grundsätzen geführt wird, sind die PTT-Betriebe daran interessiert, ihre Produkte und Dienstleistungen entsprechend

den Bedürfnissen der Kunden an diese zu verkaufen. Zu diesem Zweck führen sie eine sogenannte Verkaufsdatenbank für Geschäftskunden im Post- und Zahlungsbereich.

Mit dieser Verkaufsdatenbank verfolgen die PTT-Betriebe den Zweck, ihren Geschäftskunden im Post- und Zahlungsbereich ihre Produkte und Dienstleistungen kundenorientiert anbieten zu können. Die PTT-Betriebe sind - wie jedes Bundesorgan - gemäss Art. 20 Abs. 2 VDSG verpflichtet, uns sämtliche Projekte zur automatisierten Bearbeitung von Personendaten unverzüglich, also bereits bei Beginn ihrer Entwicklung, zu melden. Gleichwohl wurden wir von ihnen über das Projekt Verkaufsdatenbank leider erst in einem Zeitpunkt informiert, in dem der Entscheid über die Einrichtung dieser Datenbank bereits gefallen war.

Wir haben zum Projekt dennoch Stellung bezogen und folgende Gesichtspunkte festgehalten:

- Die Bearbeitung von Personendaten in dieser Verkaufsdatenbank durch die PTT-Betriebe bedarf einer gesetzlichen Grundlage. Abgesehen von der gesetzlichen Pflicht zu einer Tätigkeit nach betriebswirtschaftlichen Grundsätzen gibt es keine explizite Rechtsgrundlage, die den Betrieb einer Verkaufsdatenbank vorsieht. Diese Pflicht ist jedoch als Rechtsgrundlage grundsätzlich ausreichend für das Führen einer Verkaufsdatenbank, da zur betriebswirtschaftlichen Führung eines Unternehmens auch das marktorientierte Arbeiten gehört. Dieses setzt das Erarbeiten von Marketingkonzepten und -strategien sowie deren Umsetzung voraus. Um ihre Produkte oder Dienstleistungen den bereits vorhandenen Kunden optimal anbieten und diese optimal betreuen zu können, benötigen die Unternehmen detaillierte, für Marketingzwecke auswertbare Informationen über die bereits vorhandenen Kunden sowie über die von diesen abonnierten Dienstleistungen. Bei den Informationen, die in der Verkaufsdatenbank gespeichert werden sollen, handelt es sich um Angaben über Geschäftskunden, die aufgrund der Datenbank kundenorientiert betreut werden sollen.
- Durch die vorhandene Rechtsgrundlage nicht abgedeckt ist jedoch die Weitergabe der Personendaten an Dritte, unabhängig davon, ob es sich um eine Weitergabe im Einzelfall oder gar durch Abrufverfahren handelt. Als Dritte gelten nicht nur natürliche oder juristische Personen ausserhalb der PTT-Betriebe, wie etwa Geschäftspartner. Vielmehr umfasst der Begriff der Dritten auch die PTT-internen Stellen und Mitarbeiter, welche die betreffenden Personendaten für ihre Aufgabenerfüllung nicht unbedingt benötigen. Die Weitergabe an Dritte ist somit unzulässig, es sei denn, die Daten würden anonymisiert.
- Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Die Verwendung von Kundendaten zu Marketingzwecken ist gemäss Ziffer 2.1 *der Empfehlung Nr. (85) 20 an die Mitgliedstaaten zum Schutz personenbezogener Daten bei der Verwendung für Zwecke der Direktwerbung* grundsätzlich vom ursprünglichen Bearbeitungszweck abgedeckt. Die in der Verkaufsdatenbank Post/Zahlungsverkehr gespeicherten Informationen über Geschäftskunden dürfen jedoch ausschliesslich zu dem Zweck, eine optimale Kundenbetreuung und daraus resultierend eine betriebswirtschaftliche Betriebsführung zu ermöglichen, bearbeitet werden. Eine Verwendung zu weiteren Zwecken ist unzulässig.
- Schliesslich muss die Bearbeitung verhältnismässig sein. Es dürfen also nur diejenigen Daten bearbeitet werden, die zur Erreichung des angestrebten Zweckes absolut erforderlich sind. Insbesondere sind innerhalb der Verkaufsdatenbank

Memofelder zur Eingabe von Freitexten nur zulässig, sofern gar nicht auf sie verzichtet werden kann. In den Freitext dürfen nur die Informationen eingegeben werden, die der Verkaufsberater unbedingt für die Erfüllung seiner Aufgabe - die Beratung des betreffenden Kunden - benötigt. Weitere Informationen über die Geschäftskunden, wie etwa Angaben, die mit den abonnierten Postdienstleistungen oder den abonnierten Dienstleistungen im Zahlungsverkehr in keinem Zusammenhang stehen, dürfen in der Datenbank nicht bearbeitet werden. Darüber hinaus dürfen in die Memofelder nur die Verkaufsberater Informationen eingeben. Ebenso dürfen darauf nur die Personen Zugriff haben, welche die Freitexte abgefasst haben.

- Generell dürfen auf die zu Marketingzwecken gespeicherten Personendaten nur die Personen und Stellen Zugriff haben, welche die Informationen für ihre Aufgabenerfüllung tatsächlich brauchen. Das heisst, dass jeder Verkaufsberater nur auf die Personendaten Zugriff haben darf, welche die ihm zugeordneten Kunden betreffen. Bei der Ausarbeitung von Marketingkonzepten und -strategien reicht der Zugriff auf anonymisierte Daten aus, da dafür die Kenntnis spezifischer Personendaten nicht relevant ist. Auch für diejenigen Personen, die über die Marketingkonzepte entscheiden, ist es nicht erforderlich, Daten einzelner Geschäftskunden einsehen oder gar mutieren zu können. Auch hier rechtfertigt sich einzig der Zugriff auf anonymisierte Daten.
- Die Datenrichtigkeit und das Auskunftsrecht müssen gewährleistet sein.
- Gemäss Ziff. 4.1.i. der erwähnten Empfehlung Nr. (85) 20 hat jede betroffene Person das Recht, zu verbieten, dass ihre Daten zu Marketingzwecken bearbeitet werden. Diesem Erfordernis ist auch im vorliegenden Fall Rechnung zu tragen. Dies setzt voraus, dass die Kunden über den Betrieb der Verkaufsdatenbank durch die PTT-Betriebe informiert werden und ihnen die Möglichkeit gegeben wird, die Bearbeitung der sie betreffenden Personendaten zu untersagen.
- Schliesslich ist die Datensammlung beim Eidgenössischen Datenschutzbeauftragten anzumelden.

3.6. Störungen im Telefonsystem der Bundesverwaltung

Ein Grossteil der Telefonanschlüsse der Bundesverwaltung in Bern wird heute durch eine über zwanzigjährige elektromechanische Telefonzentrale realisiert. Aufgrund des hohen Alters und die grossen Belastung der Zentrale treten vermehrt Störungen auf, die unter anderem aus der Sicht des Datenschutzes Anlass zu Besorgnis geben.

Im Frühjahr 1994 wurden wir von einem Mitarbeiter der Bundesverwaltung darauf aufmerksam gemacht, dass Störungen im Telefonverkehr auftreten. Es wurde berichtet, dass Dritte in das Gespräch zweier Telefonpartner gelangen und dieses mithören können, auch ohne dass die Gesprächspartner dies bemerken. Die Störungen betreffen Verbindungen innerhalb der Bundesverwaltung sowie solche zwischen Anschlüssen der Bundesverwaltung und dem übrigen Telefonnetz. Der Telefondienst der Bundesverwaltung bestätigte auf unsere Anfrage die Störungen; sie kämen jedoch gemessen am hohen Verkehrsaufkommen relativ selten vor.
Bis zum Ersatz der Zentrale durch eine neue digitale Anlage im November 1995 müssen die an die alte Telefonzentrale angeschlossenen Verwaltungseinheiten erhöhte Sorgfalt walten lassen. Der Telefondienst versucht zusätzlich mit vorbeugenden Unterhaltsmassnahmen die Störungen zu begrenzen. Die Telefonteilnehmer wurden übrigens auch vom Sicherheitsdienst der Bundesverwaltung orientiert und angewiesen, vorläufig telefonisch

keine vertraulichen Informationen weiterzugeben. Da die Teilnehmer über die Risiken informiert sind und die Zentrale bis Ende 1995 ersetzt wird, kann der gegenwärtige Zustand aus datenschutzrechtlicher Sicht toleriert werden.

3.7. Verantwortung für den Datentransport über elektronische Leitungen

Werden Personendaten über elektronische Leitungen übertragen (E-Mail) oder zum Abruf bereitgestellt (elektronische Verzeichnisse), so stellt sich die Frage, wer für die Einhaltung des Datenschutzes verantwortlich ist.

Private Personen und Bundesorgane, die Personendaten bearbeiten, haben durch technische und organisatorische Massnahmen die Vertraulichkeit, Verfügbarkeit und Richtigkeit der Daten zu gewährleisten. Überträgt eine private Person die Datenbearbeitung einem Dritten, so hat sie dafür zu sorgen, dass der Dritte die Daten nur so bearbeitet, wie sie selbst es tun dürfte (Art. 14 DSG). Ein Bundesorgan darf durch einen Dritten Personendaten nur bearbeiten lassen, wenn der Datenschutz gewährleistet ist. Es bleibt jedoch für den Datenschutz verantwortlich und hat dafür zu sorgen, dass die Daten auftragsgemäss bearbeitet werden, insbesondere was deren Verwendung und Bekanntgabe betrifft. Untersteht der Dritte dem DSG nicht, so hat sich das verantwortliche Organ zu vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Andernfalls stellt es diesen auf vertraglichem Wege sicher.
Werden Personendaten über elektronische Leitungen übertragen oder zum Abruf zur Verfügung gestellt, so sind für die Vertraulichkeit, Verfügbarkeit und Richtigkeit der Personendaten auch diejenigen Personen mitverantwortlich, die ein Datenkommunikationsnetz zur Verfügung stellen. Hauptverantwortlich bleiben jedoch die Personen oder Organe, welche die Daten verschicken oder zum Abruf bereitstellen. Insbesondere obliegt ihnen die Verantwortung dafür, dass der Datenschutz auch auf den Leitungen und dem Netz gewährleistet ist. Wer ein Datenkommunikationsnetz zur Verfügung stellt, hat aber im Rahmen seiner Möglichkeiten ebenfalls dafür zu sorgen, dass auf dem von ihm zur Verfügung gestellten Netz die Vertraulichkeit, Verfügbarkeit und Richtigkeit der Daten gewährleistet ist.

3.8. Interaktives Fernsehen

Das herkömmliche Fernsehen ist ein Einwegkommunikationsmittel. Alle Zuschauer konsumieren gleichzeitig die angebotenen Programme. Bereits seit einiger Zeit wird über interaktives Fernsehen diskutiert. Es erlaubt dem Zuschauer, selber Signale zurück zur Fernsehanstalt zu senden und auf diese Weise Einfluss auf das Programm nehmen. Dabei entstehen jedoch Personendaten.

Bis jetzt war das Fernsehen grundsätzlich ein Einwegkommunikationsmittel. Der Fernsehzuschauer war passiver Konsument, der lediglich betrachten konnte, was ihm angeboten wurde. Seit geraumer Zeit wird jedoch über das sogenannte interaktive Fernsehen diskutiert. Hierbei kann der Zuschauer aus der Position des passiven Zuschauers in die Rolle des aktiven Fernsehteilnehmers schlüpfen. Die Teilnahme erfolgt aus dem Fernsehsessel von zu Hause aus. Es gibt verschiedene Möglichkeiten: Teilnahme an laufenden Sendungen, Einflussnahme auf die Handlung in Spielfilmen, Teilnahme an Fernsehspielen, Einkaufen am Bildschirm (Teleshopping) usw. Bei "Video on Demand" kann der Zuschauer einen Film aus einem bestimmten Angebot auswählen. Der Film wird dann

sozusagen individuell für diesen Zuschauer gesendet. Er kann auf diese Weise sein eigenes Programm zusammenstellen. Die Realisierung von interaktivem Fernsehen bedingt eine aufwendige Übermittlungstechnik und wird erst durch das Zusammenwachsen der Fernseh- und der Computertechnologie ermöglicht.

Das interaktive Fernsehen birgt erhebliche datenschutzrechtliche Risiken:

- Bei der Benutzung des interaktiven Fernsehens können durch die Aufzeichnung und Auswertung des Verhaltens der Zuschauer Personendaten entstehen. Die Bearbeitung von Personendaten kann sich aus der Benutzung des Angebots selbst ergeben oder für die Gebührenberechnung bei kostenpflichtigen Angeboten erfolgen. Zum Beispiel können Daten über die Nutzungszeiten anfallen: Das heisst, es wird gespeichert, wer zu welchen Zeiten von den Möglichkeiten des interaktiven Fernsehens Gebrauch macht. Aus diesen Angaben über das (Freizeit-)Verhalten einer Person ist erkennbar, ob eine Person tagsüber oder hauptsächlich während der Abend- und Nachtstunden ihre Freizeit vor dem Fernseher verbringt. Daraus können weitere Rückschlüsse auf Arbeitszeiten, Schlaf- und Lebenswandel gezogen werden.
- Sodann werden für die Rechnungsstellung Daten über die genutzten Angebote gespeichert. Durch Erfassung des genutzten Angebotes werden persönliche Präferenzen wie Vorlieben für Sportsendungen und -filme oder sogar für bestimmte Sportarten, kulturelle Sendungen, Sexfilme oder politische Sendungen ersichtlich. Daraus können Persönlichkeitsprofile entstehen.
- Aus der Häufigkeit und dem finanziellen Aufwand der Bestellungen (zum Beispiel bei "Video on Demand") kann auf die finanziellen Verhältnisse einer Person geschlossen werden.
- Aus Daten, die im Zusammenhang mit dem Teleshopping anfallen und gespeichert werden, können Rückschlüsse auf die finanziellen Verhältnisse und die bevorzugten Produkte gezogen werden.

Projekte im Bereich des interaktiven Fernsehens nehmen nun konkretere Formen an. Die Telecom PTT hat in der Schweiz für 1995 in Grenchen und Nyon erste Versuche geplant. Wie schon in anderen Fällen kamen die PTT-Betriebe auch für diese Projekte ihrer gesetzlichen Pflicht, uns bereits bei Beginn der Entwicklung der Projekte zu informieren, nicht nach. Die Projekte können von uns deshalb nicht auf ihre Datenschutzkonformität hin geprüft werden. Im jetzigen Zeitpunkt können wir nur ganz allgemein festhalten, dass lediglich diejenigen Daten bearbeitet und insbesondere aufbewahrt werden dürfen, die nötig sind, um das Angebot technisch zu realisieren und korrekt abzurechnen. Diese Daten dürfen nur von den dafür zuständigen Stellen bearbeitet werden und nicht ohne Einverständnis des Kunden an Dritte bekanntgegeben werden.

3.9. Bargeldlos telefonieren

Nicht zuletzt wegen des um sich greifenden Vandalismus, aber auch um den Telefonkunden das Bereithalten des nötigen Kleingeldes zu ersparen, gehen die Telefongesellschaften vermehrt dazu über, das Telefonieren mit Bargeld in öffentlichen Telefonzellen zugunsten von bargeldlosen Systemen abzulösen. Es existieren unterschiedliche Realisierungen, die aus der Sicht des Datenschutzes auch unterschiedlich zu bewerten sind.

Immer häufiger wird bargeldlos mit Plastikkarten telefoniert. Es gibt verschiedene Arten von Telefon-Plastikkarten:

- Zum einen kann mit sogenannten *Wertkarten* telefoniert werden. Bei den Wertkarten werden die Telefongespräche wie beim Telefonieren mit Bargeld im voraus bezahlt. In der Schweiz erwirbt der Kunde in einer Poststelle eine sogenannte Taxcard. Auf dieser ist ein bestimmter Betrag gespeichert, den der Kunde in der Poststelle bezahlt. Bei jedem Anruf von einer öffentlichen Telefonzelle aus wird der verwendete Betrag abgebucht. Die Wertkarte ist unpersönlich und kann an Dritte weitergegeben werden. Wie beim Telefonieren mit Bargeld erfolgt der Zahlungsverkehr beim Einsatz einer derartigen Wertkarte anonym. Diese Art des bargeldlosen Telefonierens ist aus datenschutzrechtlicher Sicht unbedenklich. Es gibt jedoch auch Wertkarten, die an sogenannten Ladestationen wieder aufgeladen werden können. Handelt es sich um anonyme Wertkarten, die ohne Identifizierungsmerkmale des Besitzers wie einer persönlichen Identifikationsnummer (PIN) mittels Bargeld aufgeladen werden, so bestehen aus datenschutzrechtlicher Sicht ebenfalls keine Bedenken. In anderen Ländern werden jedoch bereits wiederaufladbare Wertkarten eingesetzt, die mit Identifizierungsmerkmalen des Kartenbesitzers (z.B. PIN-Nummern) versehen sind. Bei diesen Karten, die entweder durch Bargeld oder über das Postkonto aufgeladen werden, erfolgt der Zahlungsverkehr für das einzelne Telefonat anonym. Es werden aber die Geldbeträge, die geladen werden, dem Besitzer zugeordnet.
- Von den Wertkarten unterscheiden sich die Systeme, bei denen nicht im voraus bezahlt, sondern der vertelefonierte Betrag nach dem erfolgten Gespräch abgebucht wird. Bei diesem System wird bei jedem Anruf die anrufende Person identifiziert. Es werden aber auch Angaben über den Zeitpunkt, das Datum und die Dauer des Gesprächs sowie die angewählte Telefonnummer gespeichert. Abgebucht wird in diesen Fällen von einem persönlichen Konto des Karteninhabers. In der Schweiz wird von den PTT-Betrieben seit April 1995 das Telefonieren mittels *Postcard* angeboten. Das System basiert - wenigstens vorerst - auf der bereits existierenden und weit verbreiteten Chipkarte «Postcard» der PTT. Die Postkonto-Kunden, die eine Postcard besitzen, können diese dann nicht nur am Postomaten, in den Einkaufszentren, an der Tankstelle usw. verwenden, sondern auch in den dafür eingerichteten öffentlichen Telefonzellen. Die Postcard wird vor dem Telefonieren in das Lesegerät eingeführt; nach Eingabe der PIN können die Anrufe getätigt werden. Die Kosten werden direkt dem Postkonto des Kunden belastet. Aufgrund der zum Zweck der Rechnungstellung über die geführten Gespräche gespeicherten Daten entstehen sogenannte Bewegungsprofile. Diese geben Auskunft darüber, wer sich zu welchem Zeitpunkt an welchen Orten aufgehalten hat. Darüber hinaus kann aus den angewählten Telefonnummern auf die Identität der Gesprächspartner geschlossen werden. Auf diese Weise wird eine Datenspur gelegt, die für den einzelnen Kunden kaum überschaubar und aus datenschutzrechtlicher Sicht nicht unbedenklich ist.
- Im Januar 1995 hat die Telecom PTT unter dem Namen «Swiss Telecom Card» eine sogenannte "*Calling Card*" lanciert. Bei diesem vor allem von US-amerikanischen Telefongesellschaften verwendeten System wählt sich der Anrufer von irgendeinem Land per Gratisnummer in das System des Calling Card-Anbieters ein und kann nach Eingabe seines persönlichen Codes die gewünschten Telefongespräche führen. Dabei spielt es keine Rolle, ob von einem öffentlichen oder privaten Telefonanschluss telefoniert wird. Abgerechnet wird in der Regel über eine Kreditkarte. Bei diesem System werden der Zeitpunkt, die Dauer, die angewählten Nummern sowie der Ort, von dem aus telefoniert wurde, festgehalten. Diese Daten werden dem Kunden auf seiner Rechnung mitgeteilt. Zum Teil erscheinen die angerufenen Nummern direkt auf der

Abrechnung der Kreditkartengesellschaft. Gemäss den von den PTT-Betrieben an ihre Kunden verschickten Kartenanträgen kann der Abonnent für die Rechnungstellung zwischen der Direktbelastung des Postkontos, der monatlichen Rechnung mit Einzahlungsschein und dem Auftrag an seine Bank, die von den PTT-Betrieben eingereichten Rechnungen direkt zu bezahlen, wählen. Der Karteninhaber kann zudem Zusatzkarten abonnieren, die von Dritten wie Familienmitgliedern oder Mitarbeitern verwendet werden können. Für die mittels dieser Zusatzkarten geführten Gespräche werden ihm bei der Rechnungstellung folgende Angaben bekanntgegeben: Zeitpunkt, Dauer und Entgelt der mit Hilfe der Zusatzkarten hergestellten Verbindungen, die Rufnummern der mit Hilfe der Zusatzkarten angewählten Anschlüsse sowie die Rufnummern der Anschlüsse, über welche die Verbindungen hergestellt werden.

Weder im Zusammenhang mit dem Projekt "Telefonieren mittels Postcard" noch im Zusammenhang mit der "Swiss Telecom Card" haben uns die PTT-Betriebe über die vorgesehenen Datenbearbeitungen informiert. Die PTT-Betriebe sind ihren diesbezüglichen Verpflichtungen gemäss Art. 20 Abs. 2 VDSG nicht nachgekommen. Die Projekte sind bereits oder werden in Kürze realisiert, ohne dass sich abschliessende detaillierte Feststellungen über die Datenschutzkonformität der Projekte machen liessen. Dass ein Missbrauch der bei Benutzung solcher Systeme entstehenden "Datenspuren" schwerwiegende Persönlichkeitsverletzungen zur Folge haben kann, dürfte aber feststehen. Umso wichtiger ist deshalb der Einsatz adäquater Sicherungsmassnahmen. Im Zusammenhang mit der Swiss Telecom Card ist sodann zu prüfen, ob die Angaben, die dem Karteninhaber über den Fernmeldeverkehr der Verwender der Zusatzkarten gemacht werden, gegen das im Fernmeldegesetz festgeschriebene Fernmeldegeheimnis oder gegen dessen Bestimmungen über den detaillierten Taxauszug verstossen.

Die hier angesprochene Problematik beschränkt sich nicht nur auf den Telefonbereich. Die gleichen Probleme stellen aus datenschutzrechtlicher Sicht auch andere Zahlungssysteme, wie etwa das bargeldlose Einkaufen, der bargeldlose Bezug von Fahrkarten an Automaten usw.

3.10. Verordnung über die Telefoniedaten der ETHZ

Die Eidgenössische Technische Hochschule Zürich (ETHZ) wollte ein System einführen, mittels dessen die Kosten, die beim Telefonieren anfallen, besser kontrolliert und zugeordnet werden können. Sie gelangte mit der Bitte an uns, die datenschutzrechtlichen Bedingungen für die Verwendung eines solchen Kontrollsystems zu formulieren.

Die Aufzeichnung von Daten im Zusammenhang mit einer konkret zustande gekommenen Telefonverbindung stellt eine Bearbeitung von Personendaten dar. Dies gilt sowohl für die Aufzeichnung von sogenannten Randdaten (Apparat des abgehenden Gespräches, angewählte Telefonnummmer, Datum, Gesprächsdauer, Gesprächstaxe) als auch des Gesprächsinhaltes. Die ETHZ als Bundesorgan darf Personendaten nur bearbeiten, wenn dafür eine genügende Rechtsgrundlage besteht. Die Beschaffung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss zudem für die betroffene Person erkennbar sein. Im vorliegenden Fall sind wir zum Schluss gekommen, dass grundsätzlich eine Verwaltungsverordnung, welche die Einzelheiten im Zusammenhang mit

dem internen Aufzeichnen von Telefoniedaten und deren interne Verwendung regelt, als Rechtsgrundlage ausreicht.

In dieser Rechtsgrundlage war zu regeln:

- welche Daten von welchen Gesprächen aufgezeichnet werden,
- Zweck der Aufzeichnung,
- unter welchen Bedingungen die Weitergabe von Angaben über die pro Anschluss aufgelaufenen Kosten in bestimmten, festzulegenden zeitlichen Abständen erfolgen darf,
- welche Daten eine Detailauswertung umfasst,
- die Voraussetzungen der Weitergabe von Detailauswertungen,
- die Weitergabe von Detailauswertungen an die Leiter von Einheiten der ETHZ,
- Aufbewahrungdauer sowie Vernichtungsfristen der aufgezeichneten Daten.

In der Rechtsgrundlage war auch festzulegen, dass die Aufzeichnung der Telefoniedaten ausschliesslich zum Zweck der Kostenkontrolle erfolgen darf. Eine Verwendung zu anderen Zwecken wie etwa zur Arbeits- und Tätigkeitskontrolle der betreffenden Mitarbeiter wäre nicht zulässig. Des weiteren haben wir festgehalten, dass nur die Daten bearbeitet werden dürfen, die zur Erreichung des Zwecks erforderlich und notwendig sind. Das heisst, die aufzuzeichnenden Telefoniedaten sind auf das für eine effiziente Kostenkontrolle erforderliche Minimum zu reduzieren. Zulässig ist demnach das Aufzeichnen des Anschlusses, von dem das Gespräch ausgeht, Datum und Dauer des Gespräches, die sich daraus ergebenden Gesprächstaxen sowie die angewählte Nummer. Bei der angewählten Nummer sollten jedoch zumindest die letzten vier Ziffern des angerufenen Anschlusses unterdrückt werden, um eine Feststellung der Identität des Angerufenen zu verunmöglichen, da diese für eine Kostenkontrolle nicht erforderlich ist. Zu begrüssen wäre die Beschränkung auf die Angabe der Vorwahl, soweit das sinnvollerweise ausreicht. Vom Zweck der Kostenkontrolle nicht abgedeckt wäre die Aufzeichnung von Daten über eingehende und interne Gesprächen, die der ETHZ keine Telefonkosten verursachen und die Aufzeichnung von Gesprächsinhalten.

Bei Unklarheiten und Unregelmässigkeiten in den Aufzeichnungen sollte unter bestimmten Voraussetzungen die Weitergabe von Detailauswertungen an die Leiter von Einheiten der ETHZ möglich sein. Aus Gründen der Transparenz ist eine möglichst weitgehende Information der Mitarbeiter über die aufgezeichneten Daten vorzunehmen. Diese könnte dadurch erfolgen, dass jedem Mitarbeiter die gültige Verwaltungsverordnung direkt (z.B. als Beilage der Lohnabrechnung) oder aber auf dem Zirkularwege zugestellt wird.

Die ETHZ hat unseren Forderungen in der von ihr erlassen Verwaltungsverordnung vollumfänglich Rechnung getragen. Es handelte sich bei diesem Geschäft um ein sehr positives Beispiel frühzeitiger Zusammenarbeit.

4. Statistik

Volkszählung 2000

Das Bundesamt für Statistik (BFS) hat mit den Vorbereitungen für die Volkszählung 2000 begonnen. Um die erfassten Personen und die Gemeinden nicht unnötig zu belasten will man die Erhebungsvorgänge rationalisieren. Zu diesem Zweck sollen für die Volkszählung die gemeindeeigenen Einwohnerregister beigezogen werden. Wir wurden gebeten, die Datenschutzmassnahmen der Volkszählung zu überprüfen, insbesondere die Weiterverwendung der Volkszählungsdaten zur Ergänzung der gemeindeeigenen Register.

Wie schon im ersten Tätigkeitsbericht (S. 41) erwähnt, bereitet das BFS die nächste Volkszählung vor, die im Jahre 2000 durchgeführt wird. Bei diesem umfangreichen Vorhaben will das BFS die Erhebungsvorgänge rationalisieren, die Zusammenarbeit von kantonalen und Bundesbehörden effizienter gestalten, die optimale Verwendung der Daten für verschiedene statistische Zwecke ermöglichen und die Belastung der erfassten Personen so gering wie möglich halten.

Die Zählung aufgrund kantonaler Register ist das zentrale Instrument, welches sowohl die Zusammenarbeit der Behörden verbessern als auch die Erhebungsvorgänge rationalisieren würde und unter Umständen auch die Belastung der erfassten Personen vermindern könnte. Der Gesetzgeber hat in Art. 4 des neuen Statistikgesetzes die Grundsätze der Datenbeschaffung für statistische Erhebungen festgelegt. Gemäss dieser Bestimmung soll der Bund auf besondere Erhebungen verzichten, falls die zu statistischen Zwecken benötigten Daten bei Organen, die Bundesrecht vollziehen, schon vorhanden sind. Im zweiten Absatz desselben Artikels wird ausdrücklich auf die Möglichkeit der indirekten Erhebung von Daten bei Kantonen und Gemeinden hingewiesen. Vorausgesetzt ist, dass die Daten für die Bundesstatistik notwendig sind. Diese Regelung der Datenbeschaffung könnte auch bei der Volkszählung angewendet werden, soweit daraus für die erfassten Personen keine Nachteile erwachsen.

Bei der Volkszählung 1990 wurde erstmals die Weiterverwendung der Volkszählungdaten für personenbezogene Zwecke ausgeschlossen. Durch die Einführung eines Art. 3a im Bundesgesetz über die Eidgenössische Volkszählung (Volkszählungsgesetz) wurde diese datenschutzkonforme Verwendung der Volkszählungsdaten gesetzlich verankert und damit auch das Vertrauensverhältnis zwischen Bürger und Staat verbessert. Gestützt auf diesen neuen Artikel wurde in die Verordnung über die Eidgenössische Volkszählung 1990 ein Abschnitt über die Sicherstellung des Datenschutzes aufgenommen. Insgesamt sieben Artikel sorgen für eine gesetzeskonforme Bearbeitung der Volkszählungsdaten. Diese Revision hat dem Persönlichkeitsschutz Rechnung getragen und stellt einen grossen Schritt in Richtung eines verbesserten Datenschutzes bei der Durchführung der Volkszählung dar. Auch das BFS hat seine Erfahrungen mit dem Volkszählungsgesetz 1990 positiv bewertet, vorallem aus datenschutzrechtlicher Sicht.

Die vom BFS eingeschlagene Richtung, die Volkszählungdaten vor allem zur Entlastung der Befragten indirekt (also einen Teil der Daten direkt aus den Registern der Gemeinden und Kantone und nicht direkt durch die Befragung der erfassten Personen selbst zu erheben) ist durchaus positiv zu bewerten. Doch auch eine solche indirekte Erhebung der Daten (Registerzählung) muss für die erfassten Personen transparent bleiben und es muss ihnen auch in diesem Fall möglich sein, die Richtigkeit und Erheblichkeit der bearbeiteten Daten zu

überprüfen und gegebenenfalls zu berichtigen. Auf keinen Fall dürfen bei der Volkszählung Daten ohne Wissen der Betroffenen bearbeitet werden. Es ist deshalb vorzusehen, dass zuerst die Registerdaten aufgenommen werden und anschliessend der nicht schon ausgefüllte Teil der Fragebogens von den Betroffenen selbst ausgefüllt wird. Diese Lösung hat den Vorteil, dass die Befragten die indirekt erhobenen Daten kontrollieren können. Nur wenn sie wissen, was mit ihren Daten geschieht, kann von den betroffenen Personen eine Zusammenarbeit auf Vertrauensbasis erwartet werden. Die Erfahrungen der Vergangenheit haben gezeigt, dass eine optimale Kooperation zwischen Befragten und Behörden für den Erfolg einer Volkszählung unerlässlich ist.
Sodann ist bei einer Registererhebung auch der in Art. 3a des Volkszählungsgesetzes konkretisierte Grundsatz der Zweckbindung zu beachten. Eine Registerzählung, die auf eine direkte Befragung nicht verzichtet, darf nicht dazu dienen, Register der kantonalen Verwaltung zu ergänzen. Obwohl das Bedürfnis der Gemeinden, ihre Register mit Personendaten der Volkszählung zu ergänzen, aufgrund der Rationalisierung der Aufgaben der Gemeinden verständlich ist, verstösst diese Weiterverwendung der Daten gegen den Grundgedanken des Volkszählungsgesetzes, der unmissverständlich jede personenbezogene Verwendung der Daten ausschliesst. Eine Verwendung der erhobenen Daten innerhalb der Verwaltung für andere als statistische Zwecke würde aber eine Lossagung von der Konzeption der Abschottung der Statistik von der Verwaltungstätigkeit und einer Lockerung/Änderung der erst anlässlich der Volkszählung 1990 eingeführten Datenschutzbestimmungen bedeuten. Dies setzt zudem eine Änderung des Volkszählungsgesetzes voraus. Sodann stellt die ausschliessliche Verwendung der Daten aus der Volkszählung zu statistischen Zwecken ein wesentliches Element der Vertrauensbildung in der Bevölkerung dar. Die erfassten Personen geben nämlich ihre persönlichen Angaben im Vertrauen darauf bekannt, dass ihnen durch diese Freigabe der Daten zu statistischen Zwecken keine Nachteile erwachsen, beziehungsweise die Daten nicht für Verwaltungszwecke verwendet werden. Solche Nachteile können insbesondere auch entstehen, weil die Summe der bei einer Volkszählung erhobenen Personendaten durchaus zur Bildung von umfangreichen Persönlichkeitsprofilen führt, welche mit amtlichen Einwohnerverzeichnissen nicht erstellt werden können.

Aus dem Vernehmlassungsverfahren zur Änderung des Volkszählungsgesetzes im Vorfeld der Volkszählung 1990 geht klar hervor, dass die bei der Volkszählung erhobenen Personendaten ausschliesslich zu statistischen Zwecken bearbeitet werden dürfen. Vom sogenannten Datenausgleich, das heisst von einer Kontrolle und möglichen Ergänzung der Einwohnerregister durch die Gemeinden mittels Volkszählungsdaten wurde abgeraten.

Die Änderung der geltenden Praxis über die Verwendung dieser Daten würde gegen diese fundamentale Zweckbestimmung des Volkszählungsgesetzes verstossen. Ausserdem könnte eine solche Änderung auf den Widerstand der Bevölkerung stossen, die eine klare Trennung von Statistik und Verwaltung verlangt. Darüber hinaus würde das noch angeschlagene Vertrauensverhältnis zwischen Bürger und Staat einen neuen Rückschlag erleiden. Deshalb sollte der utilitaristische Gedanke der Verwendung der Volkszählungsdaten nicht in die Konzeption der statistischen Verwendung dieser Daten eindringen.

Volkszählung als reine Registerzählung
Bei der Volkszählung 2000 wird die Erhebung der Daten *teilweise* direkt bei den Betroffenen und *teilweise* über die Register erfolgen. Für eine verstärkte Nutzung von Registerdaten oder gar eine vollständige Indirekterhebung ist die Harmonisierung der gemeindeeigenen Register

eine wesentliche Voraussetzung, weil diese nur so für die Volkszählung optimal genutzt werden können. Die Führung der Register liegt im Kompetenzbereich der Kantone und deshalb muss zuerst durch eine Verfassungsänderung eine Bundeskompetenz zur Regelung der Vereinheitlichung geschaffen werden.(siehe dazu 1. Tätigkeitsbericht, S. 42) Ein solcher grundsätzlicher Systemwechsel ist für die Volkszählung 2000 ausgeschlossen und könnte frühenstens für das Jahr 2010 ins Auge gefasst werden.

5. Personalwesen

5.1. Privatbereich - Datenschutz im Arbeitsverhältnis

Anfragen aus dem Bereich des Arbeitsverhältnisses gehören nach wie vor zu den häufigsten im Privatbereich. Schon im ersten Tätigkeitsbericht wurden unsere wichtigsten Stellungnahmen zum Datenschutz im Arbeitsverhältnis im Privatbereich dargelegt (S. 53 f.). Diese und andere, neu dazugekommene, sind nun in einem Leitfaden zusammengefasst, der sich sowohl an Arbeitgeber als auch an Arbeitnehmer richtet und bei uns erhältlich ist. Wir informieren an dieser Stelle kurz über die einschlägigen Bestimmungen und über den Inhalt des Leitfadens. Etwas ausführlicher gehen wir auf den Einsatz von Überwachungs- und Kontrollsystemen am Arbeitsplatz, ein Thema von zunehmender Aktualität, ein.

Rechtslage
Schon nach *Art. 328 Abs. 1 OR* hat der Arbeitgeber im Arbeitsverhältnis die Persönlichkeit des Arbeitnehmers zu schützen und zu achten. Aus dieser Bestimmung wird eine allgemeine Fürsorgepflicht des Arbeitgebers gegenüber den Arbeitnehmern hergeleitet, die das Gegenstück ihrer Treuepflicht (Art. 321a OR) darstellt. Der Arbeitgeber hat alle Eingriffe in die Persönlichkeit der Arbeitnehmer zu unterlassen, die nicht durch den Arbeitsvertrag gerechtfertigt sind, und im Rahmen des Arbeitsverhältnisses entsprechende Eingriffe von Vorgesetzten, Mitarbeitern oder Dritten abzuwehren. Die Fürsorgepflicht (auch umschrieben als Pflicht, alles zu unterlassen, was die berechtigten Interessen der Arbeitnehmer schädigen könnte) führt unter anderem auch zu Einschränkungen hinsichtlich der Bearbeitung von Daten über die Arbeitnehmer durch den Arbeitgeber. Persönliche Verhältnisse, Eigenschaften und Neigungen, die nicht wesentlich die beruflichen Fähigkeiten mitbestimmen, müssen schon gestützt auf Art. 328 OR ausserhalb des Zugriffs des Arbeitgebers bleiben. Aus Art. 328 OR ergibt sich für den Arbeitgeber nicht nur eine Unterlassungspflicht, sondern auch eine Pflicht, die Arbeitnehmer über ihre Rechte zu informieren. Z.B. ist er verpflichtet, die Arbeitnehmer über Voraussetzungen und Umfang betrieblicher Sozialleistungen sowie über die zur Verfügung stehenden Sozialeinrichtungen zu unterrichten. Ebenso hat er sie über die ihnen nach Datenschutzrecht zustehenden Rechte, namentlich das Auskunftsrecht zu informieren.

Gleichzeitig mit dem Datenschutzgesetz trat speziell für das Arbeitsverhältnis *Art. 328b OR* in Kraft. Er lautet: "Der Arbeitgeber darf Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Im übrigen gelten die Bestimmungen des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz." Art. 328b OR geht dem Datenschutzgesetz und anderen allgemeinen Datenschutzbestimmungen vor, wird aber durch die Bestimmungen des Datenschutzgesetzes ergänzt. Er konkretisiert die in Art. 4 DSG enthaltenen allgemeinen Grundsätze der Datenbearbeitung, insbesondere den Grundsatz der

Verhältnismässigkeit. Der Arbeitgeber kann demnach nur in zwei Fällen und nur in einem bestimmten Umfang Daten über Arbeitnehmer/innen bearbeiten:

- Im Vorfeld des Abschlusses eines Arbeitsvertrags dürfen Daten über Bewerber/innen bearbeitet werden, um abzuklären, ob sie für die betreffende Arbeitsstelle geeignet sind.
- Während der Durchführung des Vertragsverhältnisses dürfen diejenigen Daten über Arbeitnehmer/innen bearbeitet werden, die für die Durchführung des Arbeitsverhältnisses erforderlich sind.

Von Art. 328b OR darf unter keinen Umständen, auch nicht mit Einwilligung der Arbeitnehmer/innen, abgewichen werden (Art. 362 OR).
In der neuen *Verordnung 3 zum Arbeitsgesetz* findet sich eine wichtige Bestimmung über die Überwachung von Arbeitnehmern, auf die noch näher eingegangen wird.

Leitfaden für die Bearbeitung von Personendaten im Arbeitsbereich
Im Frühjahr haben wir einen Leitfaden herausgegeben, der die wichtigsten Fragen der Bearbeitung von Personendaten im Arbeitsbereich durch private Personen behandelt. Er übernimmt und vervollständigt die Ausführungen zu diesem Thema im ersten Tätigkeitsbericht (S. 50 ff.). Nach einigen allgemeinen Ausführungen zum Datenschutz und zum anwendbaren Recht behandelt der Leitfaden die datenschutzrechtlichen Fragen, die sich im Verlauf des Arbeitsverhältnisses stellen können in chronologischer Reihenfolge. Hinsichtlich des Bewerbungsverfahrens befasst er sich unter anderem mit der Frage der Zulässigkeit von Stelleninseraten unter Chiffre, den im Bewerbungsverfahren zu machenden Angaben, Einstellungstests, der Bearbeitung von Gesundheitsdaten und der Pflicht zur Rückerstattung oder Vernichtung der Daten bei Nichtanstellung. Sodann wird geprüft, welche Daten während der Dauer des Anstellungsverhältnisses bearbeitet werden dürfen, inwiefern ein Auskunfts- und ein Berichtigungsrecht der betroffenen Person besteht, wann die betreffenden Datensammlungen angemeldet werden müssen und unter welchen Voraussetzungen die Bekanntgabe von Daten an Dritte zulässig ist. Schliesslich werden die zulässige Aufbewahrungsdauer von Personendaten und das Bestehen eines Auskunftsrechts nach Beendigung des Arbeitsverhältnisses behandelt. Bei all diesen Fragen wird den besonderen datenschutzrechtlichen Bestimmungen über die Personalvermittlung und den Personalverleih Rechnung getragen. Ein besonderes Kapitel befasst sich mit Fragen des Einsatzes von Überwachungs- und Kontrollsystemen am Arbeitsplatz. Da dieses Thema zur Zeit von grosser Aktualität ist, wird der entsprechende Auszug aus dem Leitfaden im folgenden praktisch vollständig wiedergegeben. Der Leitfaden ist bei unserem Sekretariat kostenlos erhältlich.

Einsatz von Überwachungs- und Kontrollsystemen am Arbeitsplatz
Überwachungs- und Kontrollsysteme sind alle technischen Systeme, durch welche einzelne oder mehrere Tätigkeiten oder Verhaltensweisen der Arbeitnehmer erfasst werden können. Die Verwendung solcher Systeme ist dem Arbeitgeber schon aus Gründen des Gesundheitsschutzes nicht gestattet, wenn sie der Überwachung des Verhaltens von Arbeitnehmern am Arbeitsplatz dient (Art. 26 der Verordnung 3 zum Arbeitsgesetz). Erlaubt ist der Einsatz von Überwachungs- und Kontrollsystemen aus Sicherheitsgründen und zur Erfassung der Arbeitsleistung (zum Beispiel Registrierung der Anzahl Anschläge pro Tag bei Texterfassungssystemen). Der Arbeitgeber darf jedoch solche Systeme nur einsetzen, wenn die betroffenen Arbeitnehmer vorgängig informiert wurden.

Zu den Überwachungs- und Kontrollsystemen gehören:

- *Telefonzentralen*. Schon kleine, in der Anschaffung nicht sehr aufwendige Telefonzentralen erlauben heute die Registrierung und Anzeige der ein- und ausgehenden Anrufe samt Teilnehmernummern, der Dauer und der Kosten jedes Gesprächs. Häufig ist auch das Abhören der geführten Telefongespräche ohne Wissen der betroffenen Person problemlos möglich. Die Aufzeichnung von Telefondaten darf nicht dem Zweck dienen, das Verhalten der Mitarbeiter zu kontrollieren. Eine Aufzeichnung der Teilnehmernummern der *aus beruflichen Gründen* angewählten Anschlüsse ist zulässig, sofern sie nicht zur Kontrolle des Verhaltens der Arbeitnehmer vorgenommen wird, sondern aus beruflichen Gründen (zum Beispiel, um den Kunden Rechnung zu stellen) und die Arbeitnehmer darüber informiert sind. Die Teilnehmernummern der von den Arbeitnehmer angewählten *privaten Anschlüsse* (oder der von ihnen erhaltenen Anrufe) dürfen unter keinen Umständen aufgezeichnet werden, wenn das Führen privater Telefongespräche nicht generell untersagt ist. Allenfalls dürfen die Ortskennziffern aufgezeichnet werden. Ein Verbot, Privatgespräche zu führen, ist mit anderen Mitteln als durch Überwachung von Telefongesprächen durchzusetzen, z. B., indem Aussenverbindungen durch eine Zentrale vermittelt werden oder nur von bestimmten Anschlüssen aus möglich sind. Wird die *Rufnummer automatisch* angezeigt, so ist dafür zu sorgen, dass die Anzeige bei Bedarf von beiden Teilnehmern abgeschaltet werden kann. Die Weiterleitung eines Anrufs an einen anderen als den gewählten Anschluss ist rechtzeitig zu signalisieren, damit die anrufende Person die Verbindung unterbrechen kann. Der Inhalt von Telefongesprächen darf nur aus Gründen der Leistungskontrolle (zum Beispiel 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 (zum Beispiel durch ein optisches oder akustisches Signal). Unter allen Umständen *unzulässig* sind Kontrollrückrufe zu den angerufenen Teilnehmer. Auch das Abhören der zwischen Arbeitnehmern geführten Gespräche (etwa durch eine entsprechend ausgerüstete Gegensprechanlage) ist auf keinen Fall gestattet. Besteht ein solches Verbot, so muss den Arbeitnehmern die Möglichkeit gegeben werden, in dringenden Fällen und während der Pausen von einem unbeaufsichtigten Anschluss aus zu telefonieren.

- *EDV-Systeme*. Auch bei EDV-Systemen sind zahlreiche Überwachungs- und Kontrollmöglichkeiten vorhanden. Mittels Hardware- oder Softwaremonitoren kann zum Beispiel registriert werden, wann ein Rechner benutzt wird, ob Konfigurationen verändert werden, welche Programme aufgerufen oder verlassen werden, welche Aktivitäten innerhalb bestimmter Programme ausgeführt werden (Mutationen von Datensätzen, Anzahl Anschläge pro Minute bei Textverarbeitung usw.). E-Mail-Botschaften können in der Regel problemlos geöffnet und gelesen werden.

- *Andere Systeme*. Zu beachten ist, dass auch andere Systeme, welche nicht primär der Überwachung des Personals dienen, zu diesem Zweck benützt werden können (zum Beispiel, wenn sie mit einer elektronischen Zugangsberechtigung und einem automatischen Zählwerk ausgestattet sind). Solche Systeme sind zum Beispiel Fotokopiergeräte, FAX-Geräte, Zeiterfassungssysteme, Auftragsabwicklungssysteme, Zugangskontrollen, Zählwerke usw.

Bei Systemen, mit denen eine *Überwachung aus Sicherheitsgründen* durchgeführt wird, ist darauf zu achten, dass eine für die Angestellten möglichst schonende Vorgehensweise gewählt wird. So ist zum Beispiel bei der Diebstahlüberwachung durch Videokameras in

einem Warenhaus möglichst zu verhindern, dass die gewählten Bildausschnitte die Angestellten erfassen. Das gilt auch für Anlagen, welche der Produktionssteuerung dienen. Ist die Überwachung der betroffenen Person selbst aus Sicherheitsgründen notwendig (etwa um in gefährlichen Situationen eingreifen zu können) so sind alternative Möglichkeiten zu prüfen (zum Beispiel das regelmässige Quittieren einer Meldung, ansonsten Alarm ausgelöst wird).

Allgemein gilt, dass der Einsatz solcher Systeme auf möglichst schonende Art und Weise zu erfolgen hat. Folgende Richtlinien* der Internationalen Arbeitsorganisation (IAO) verdeutlichen diesen Grundsatz:

- Arbeitnehmer haben Anspruch auf eine angemessene Privatsphäre am Arbeitsplatz.
- Arbeitnehmer wissen, welche elektronischen Überwachungsmethoden verwendet werden und wie der Arbeitgeber die dabei erhobenen Daten verwendet.
- Der Arbeitgeber verwendet elektronische Überwachungsmethoden oder Durchsuchungen von Datensammlungen, Netzwerkkommunikation oder E-Mail so wenig wie möglich. Dauernde elektronische Überwachung ist nicht gestattet.
- Arbeitnehmer sind an der Entscheidung, wann und wie elektronische Überwachungsmethoden oder Durchsuchungen stattfinden, beteiligt.
- Daten werden nur zu klar definierten, mit der Arbeit zusammenhängenden Zwecken erhoben und verwendet.
- Überwachungen und Durchsuchungen ohne vorgängige Information der Arbeitnehmer werden nur vorgenommen, wenn ernstzunehmende Anhaltspunkte auf kriminelle Tätigkeiten oder andere Missbräuche hinweisen.
- Die Beurteilung der Leistungen der Arbeitnehmer beruht nicht allein auf den Überwachungsergebnissen.
- Arbeitnehmer haben das Recht, die bei der elektronischen Überwachung über sie erhobenen Daten einzusehen, zu kritisieren und zu berichtigen.
- Aufnahmen, die für den Zweck zu dem sie erhoben wurden, nicht mehr länger benötigt werden, sind zu vernichten.
- Überwachungsdaten, durch die individuelle Arbeitnehmer identifiziert werden können, werden nicht an Dritte bekanntgegeben, es sei denn, es bestehe dafür eine gesetzliche Pflicht.
- Arbeitnehmer oder zukünftige Arbeitnehmer können auf das Recht auf Privatsphäre nicht verzichten.
- Vorgesetzte, welche diese Grundsätze verletzen, müssen mit Disziplinarmassnahmen oder Entlassung rechnen.

*Quelle: "A model employment/privacy policy", in Workers' privacy, Part II: Monitoring and surveillance in the workplace, Conditions of work digest, International Labour Office, Geneva 1993, S. 75. Übersetzung: EDSB.

5.2. Bund: Eignungstests (Sigmund Potential) innerhalb der Bundesverwaltung

Die Veränderungen bei der Bearbeitung von Daten über das Personal der Bundesverwaltung zeigen sich nicht nur - wie in unserem ersten Tätigkeitsbericht (S. 59) beschrieben - an der Einführung dezentralisierter elektronischer Bearbeitungssysteme, sondern auch daran, dass immer mehr Ämter bei der Einstellung, aber auch bei der Evaluation von Personal auf automatisierte Eignungstests zurückgreifen oder dies zumindest ins Auge fassen. Eines dieser zur

Personalverwaltung eingesetzten Instrumente stellt der Eignungstest Sigmund Potential dar. Angesichts der Risiken einer Persönlichkeitsverletzung bei der Verwendung solcher Instrumente, muss ihnen ein möglichst strikter Rahmen gesetzt werden. Da ihre Einführung eine Umgestaltung der gesamten Personalverwaltungspolitik bedingt, ist eine gründliche Reflexion sowie eine Absprache bezüglich der Voraussetzungen der Verwendung solcher Systeme von seiten aller für die Verwaltung des Bundespersonals verantwortlichen Personen angebracht.

Es sei zunächst daran erinnert, dass unter "Eignungstests" in erster Linie graphologische Gutachten, psychologische Tests, Persönlichkeitstests, biologische Fragebogen sowie Evaluationssysteme wie Sigmund Potential zu verstehen sind. Die Verwendung von Tests dieser Art ist unserer Auffassung nach mit dem Bundesgesetz über den Datenschutz sowie mit dem Rundschreiben des Eidgenössischen Personalamts zum Datenschutz (Rundschreiben Nr. 318.4/83 C. 2648) vereinbar, wenn folgende Voraussetzungen erfüllt sind:

- vorherige Benachrichtigung des Eidgenössischen Datenschutzbeauftragten sowie des Datenschutzberaters des betreffenden Amtes oder Departements zwecks Überprüfung aus Sicht des Datenschutzes, wenn es um die Verwendung von Produkten wie Sigmund geht;
- Schaffung einer Rechtsgrundlage;
- Wahrung der allgemeinen Grundsätze, wie etwa des Grundsatzes der Zweckbindung und der Verhältnismässigkeit;
- Zuverlässigkeit und Objektivität der Resultate;
- Freiwilligkeit der Teilnahme am Testverfahren;
- Professionalität der Testdurchführung und -auswertung;
- Verständlichkeit für den Kandidaten oder die Kandidatin;
- Anonymisierung von Tests, deren Ergebnisse zum Zwecke der Auswertung an externe Experten oder zur Verbesserung der Qualität des Produkts an den Hersteller gesandt werden;
- Respektierung der Persönlichkeit der Kandidaten bei der inhaltlichen Ausrichtung der Fragen;
- Zugang zu den Testantworten und -ergebnissen nur für den Kandidaten und die auswertende Person;
- gesonderte Aufbewahrung der Ergebnisse; diese dürfen nicht ins Dossier der betroffenen Person kommen;
- möglichst rasche Vernichtung dieser Daten, sobald die auswertende Person den Kurzbericht zu Handen des künftigen Arbeitgebers abgefasst hat, spätestens aber bei Abschluss des Einstellungs- bzw. Evaluationsverfahrens, vorbehaltlich des Wunsches der betroffenen Person, die Ergebnisse aufzubewahren, um sie mit den Resultaten eines eventuellen späteren Tests zu vergleichen;
- Anmeldung der aufgrund der Testergebnisse erstellten Datensammlung beim Datenschutzbeauftragten, falls die Testresultate über den zur Erstellung eines Evaluationsberichts notwendigen Zeitraum hinaus aufbewahrt werden sollen.

Zum aus Frankreich stammenden Produkt Sigmund Potential ist zunächst zu betonen, dass es nicht dazu bestimmt ist, den Begutachter zu ersetzen. Es soll vielmehr das Evaluationsgespräch strukturieren und orientieren. Es handelt sich dabei nicht nur um ein Instrument zur Einstellung und zur internen und externen Selektion von Personal, sondern auch und vor allem um ein Hilfsmittel, das dazu dient, Potentiale aufzudecken, die Laufbahn zu planen oder einen eventuell vorhandenen Aus- oder Weiterbildungsbedarf zu erkennen.

Das Programm Sigmund Potential wird auf einem PC zur Verfügung gestellt. Es umfasst 460 Fragen, die allesamt zu verschiedenen Persönlichkeitskriterien (insgesamt deren 38) in Bezug gesetzt werden. 17 Kriterien betreffen die berufliche Sphäre, 13 den sozialen und 8 den psychologischen Bereich. Die antwortende Person hat für die Beantwortung jeder Frage 9 Sekunden zur Verfügung. Der Fragenkatalog ist zudem den regionalen und kulturellen Eigenheiten des geographischen Raumes, in dem er verwendet wird, angepasst.

Die bewertende Person erhält keine Kenntnis der auf die einzelnen Fragen gegebenen Antworten, da die Auswertung in graphischer Form erfolgt, indem zu jedem Persönlichkeitskriterium eine Bewertung nach Punkten (von 0 bis 20) vorgenommen wird. Ferner wird ebenfalls angegeben, inwieweit die Antworten untereinander übereinstimmen. Eine ungenügende Übereinstimmung macht das Testergebnis für die bewertende Person unbrauchbar.

Die in der Schweiz für Sigmund verantwortliche Person legt sehr viel Wert auf die Einhaltung ethischer Grundsätze bei der Verwendung ihres Produkts, was von uns sehr begrüsst wird. Namentlich wird die Benützung von Sigmund nur denjenigen Kunden gestattet, die sich vertraglich dazu verpflichten, bestimmte Grundsätze, vor allem hinsichtlich der Vertraulichkeit, einzuhalten. Sie empfiehlt sodann die Unterzeichnung eines Benutzungskodexes, durch die sich die bewertende Person unter anderem dazu verpflichtet, die Evaluation auf professionneller Ebene durchzuführen und die Weigerung eines Kandidaten zu respektieren, sich dem Test zu unterziehen.

Aus Sicht des Datenschutzes haben wir folgende Vorteile hervorgehoben:

- der Test wird ständig auf den neuesten Stand gebracht;
- die bewertende Person erhält von den durch die Testperson gegebenen Antworten keine Kenntnis;
- der Test ist nur brauchbar, wenn die Antworten untereinander hinreichend übereinstimmen;
- die Antworten sind nicht in Textform verfügbar, die Raum für Interpretationen lässt, sondern sie werden schematisch dargestellt;
- die Ergebnisse sind nur nützlich, wenn sie mit dem Kandidaten im Gespräch diskutiert werden;
- die Benutzer von Sigmund werden im Hinblick auf den Gebrauch dieses Programms entsprechend geschult;
- die in der Schweiz für Sigmund verantwortliche Person stellt sicher, dass die Benutzer betreut werden, damit keine "Ausrutscher" passieren;
- die evaluierten Personen werden hinreichend informiert, bevor sie den Test machen und sie haben Anspruch auf ein Feedback sowie auf Zugang zu den graphisch dargestellten Testergebnissen;
- die Testergebnisse sind nur für den Kandidaten und die bewertende Person zugänglich.

Wir haben allerdings auch Schwächen festgestellt:

- das Testergebnis wird durch den jeweiligen Zustand des Kandidaten beeinflusst, welcher wiederum davon abhängt, ob die Testperson zum Zeitpunkt der Testdurchführung durch persönliche, berufliche oder familiäre Probleme belastet wird oder nicht;

- die Auslegung der Testergebnisse hängt vor allem von der Persönlichkeit der bewertenden Person ab, aber auch von ihrer Erfahrung, ihrem psychologischem Geschick und ihrem Einfühlungsvermögen;
- verfügt die bewertende Person über ausreichend Erfahrung, so kann sie, wenn sie das Gespräch nicht auf die Auskünfte beschränkt, die notwendig sind, um zu erkennen, ob der Kandidat für einen bestimmten Posten geeignet ist, die Persönlichkeit der Testperson entblössen und, wenn sie nicht über das nötige Taktgefühl verfügt, diese destabilisieren oder gar dauerhaft verunsichern und auf diese Weise ihre Persönlichkeit verletzen;
- die Verwendung von Sigmund ermöglicht die Legitimierung der Zurückweisung von unliebsamen Bewerbungen unter dem Deckmantel der Objektivität;
- die durch Sigmund erteilten Noten können für die betroffene Person negative Auswirkungen haben, wenn es sich bei der bewertenden Person um einen "konventionellen" Typ handelt;
- die von Sigmund durchgeführte Schulung ist nicht ausreichend und kann die erforderliche Professionalität nicht garantieren.

Gestützt auf diese Feststellungen haben wir für die Verwendung von Sigmund bei der Anstellung von Personen gefordert, dass zusätzlich zu den eingangs erwähnten Grundsätzen für die Verwendung von Eignungstests folgende Bedingungen eingehalten werden:

- Wahrung des Grundsatzes der Verhältnismässigkeit, was insbesondere voraussetzt, dass die Verwaltungseinheit zur Erfüllung ihrer gesetzlichen Aufgaben Beamte mit spezifischen persönlichen Eigenschaften einstellen muss, welche anhand der Bewerbungsunterlagen oder der üblichen Einstellungsgespräche nur schwer zu erkennen sind (Gemeinschaftsgeist, Initiative, Verhandlungs- oder Führungsgeschick, natürliche Autorität, Fähigkeit, Niederlagen einzustecken ...) oder dass Direktionsposten oder andere besonders exponierte Stellen neu zu besetzen sind;
- Sicherstellung einer gewissen Objektivität durch Rückgriff auf externe Experten oder durch Schaffung eines Evaluationszentrums, bespielsweise im Eidgenössischen Personalamt. Bei jedem Einsatz von Sigmund würde die bewertende Person vom auswärtigen Experten oder von einem Vertreter dieser Begutachtungsinstanz unterstützt (Vieraugenprinzip). Wird eine solche Instanz ins Leben gerufen, so muss sie von der Firma, welche Sigmund in der Schweiz vertritt, gebührend unterstützt und geschult werden;
- Abschaffung der Notenblätter;
- Anhörung des Personals vor der Einführung von Sigmund, wie dies im Rundschreiben des Eidgenössischen Personalamts zum Schutz der Daten von Bundesbediensteten vorgesehen ist.

Hinsichtlich der Verwendung von Sigmund zur Potentialanalyse haben wir uns für die Unterstützung und Förderung des Einsatzes dieses Systems durch die für die Personalverwaltung verantwortlichen Personen derjenigen Verwaltungseinheiten, die Sigmund verwenden ausgesprochen. Wir haben aber auch darauf hingewiesen, dass solche Tests nur zulässig sind - sofern sie die oben erwähnten Voraussetzungen einhalten - wenn sie auf Anfrage der betroffenen Personen durchgeführt werden.

Der Einsatz von Eignungstests wie Sigmund innerhalb der Bundesverwaltung beinhaltet ernstzunehmende Risiken für die Persönlichkeit der betroffenen Personen. Insofern ist eine möglichst strikte Festlegung des Verwendungsrahmens solcher Tests unerlässlich. Dazu

gehört insbesondere die Verabschiedung detaillierter Richtlinien durch die zuständigen Departemente, die sowohl ethische Grundsätze als auch datenschutzrechtliche Anforderungen berücksichtigen. In einem weiteren Schritt müssen diese Richtlinien dann in die schon in unserem ersten Tätigkeitsbericht (S. 57 f.) angesprochene künftige Verordnung des Bundesrates zum Schutze der Daten von Bundesbediensteten einfliessen. Ob eine formelle gesetzliche Grundlage geschaffen wird, ist allerdings noch offen. Schliesslich kann die Bundesverwaltung aus der Verwendung dieser Evaluationsmittel nur dann wirklich einen Nutzen ziehen, wenn die Personalverwaltungspolitik von Grund auf geändert wird. Dies wiederum bedingt eine grundsätzliche Auseinandersetzung mit der Problematik von seiten der für das Bundespersonal zuständigen Stellen. Die dabei entwickelte einheitliche Linie wird nicht nur einen minimalen rechtlichen Standard im Bereich des Datenschutzes, sondern auch ein befriedigendes ethisches Niveau gewährleisten.

6. Versicherungswesen*

6.1. Sozialversicherungen

Im Sommer 1994 wurden wir aufgefordert, uns zur Rechtsstellung der privatrechtlichen Vorsorgeeinrichtungen - insbesondere hinsichtlich der Pflicht zur Anmeldung von Datensammlungen - zu äussern. Im Anschluss an unsere Intervention hinsichtlich der Analysenliste mit Tarif, von der in unserem ersten Tätigkeitsbericht (vgl. S. 48) die Rede war, wurde eine Arbeitsgruppe ins Leben gerufen. Diese Arbeitsgruppe hat Vorschläge zur Verbesserung der am 15. März 1995 in Kraft getretenen Liste vorgelegt. Wir haben zudem auf die Grundsätze der Amtshilfe zwischen der AHV und den Steuerbehörden hingewiesen. In bezug auf die Frage der Rechtmässigkeit der Statistik des Konkordats der Schweizerischen Krankenkassen haben wir schliesslich darauf hingewiesen, dass die Grundlage dieser Statistik, ohne rechtswidrig zu sein, unbefriedigend ist und die Schaffung eines klaren rechtlichen Rahmens erforderlich ist.

Anwendbare Datenschutzbestimmungen auf die privatrechtlichen Vorsorgeeinrichtungen im Bereich der obligatorischen zweiten Säule.
Welches Datenschutzrecht findet auf die privatrechtlichen Vorsorgeeinrichtungen (im folgenden "Vorsorgeeinrichtungen") im Bereich der obligatorischen zweiten Säule Anwendung ? Wie steht es mit der Pflicht zur Anmeldung dieser Datensammlungen ? Diese offenen Fragen wurden vor allem mit den Vertretern des Schweizerischen Versicherungsverbands (SVV) diskutiert. Der SVV war der Ansicht, dass die Vorsorgeeinrichtungen den Bestimmungen des DSG für den Privatbereich unterstehen. Wir haben hingegen den Standpunkt vertreten, dass die Vorsorgeeinrichtungen für sämtliche im Rahmen der obligatorischen 2. Säule vorgenommenen Datenbearbeitungen im Sinne des DSG Bundesorganen gleichgestellt sind. Dies aus folgenden Gründen:

- die Vorsorgeeinrichtungen erfüllen eine Bundesaufgabe;
- die 2. Säule gehört zum Sozialversicherungsbereich, was der Bundesrat in seiner Stellungnahme vom 17. April 1991 mit dem Titel "Parlamentarische Initiative, Sozialversicherungsrecht" bestätigt hat, die insbesondere den Entwurf eines Bundesgesetzes über den allgemeinen Teil des Sozialversicherungsrechts betraf;
- aus dem Kommentar zu Artikel 34quater der Bundesverfassung geht hervor, dass der Verfassungsgeber in erster Linie aus wirtschaftlichen Gründen beschlossen hat, sich auf bestehende, in den meisten Fällen alte und bereits bewährte Strukturen

abzustützen. Diese Argumentation wurde schon in anderen Bereichen der Sozialversicherungen, wie etwa bei den Krankenversicherungen vertreten, ohne bereits etwas über die rechtliche Stellung der Kassen auszusagen, die laut dem Bundesgesetz über den Datenschutz als Bundesorgane anzusehen sind;

- der Beitritt zu einer Vorsorgeeinrichtung ist obligatorisch;
- die Streitfälle zwischen Vorsorgeeinrichtungen, Arbeitgebern und Anspruchsberechtigten werden nicht im Zivilverfahren, sondern im Verwaltungsverfahren geregelt. So steht auf Bundesebene die Verwaltungsgerichtsbeschwerde ans Eidgenössische Versicherungsrecht offen;
- laut Verordnung über die Errichtung der Stiftung Sicherheitsfonds sind die Zuschüsse, die den Vorsorgeeinrichtungen zukommen, mit Subventionen gleichzusetzen;
- im Rahmen der Arbeiten zum Europäischen Wirtschaftsraum hat die Kommission der Europäischen Gemeinschaften die Ansicht vertreten, dass die obligatorische Mindestvorsorge als integrierender Bestandteil eines Sozialversicherungssystems zu sehen sei. Trotz starker Opposition von seiten der betroffenen Kreise hat das Parlament diesen Standpunkt gestützt.

Dies bedeutet konkret, dass die privaten Vorsorgeeinrichtungen alle Datensammlungen der obligatorischen zweiten Säule bei unserem Sekretariat anmelden müssen.

Die Analysenliste mit Tarif (im folgenden "Liste" genannt)
In unserem ersten Tätigkeitsbericht (vgl. S. 48) hatten wir auf die durch diese Liste aufgeworfenen datenschutzrechtlichen Probleme hingewiesen. Wir warteten damals auf den Entscheid über die Konstituierung einer Arbeitsgruppe mit dem Auftrag, die Liste noch einmal zu überarbeiten und die Problematik des Informationsflusses zu den Versicherungskassen global zu untersuchen.

Die Arbeitsgruppe ADAK wurde durch Verfügung des Eidgenössischen Departements des Innern vom 25. April 1994 ins Leben gerufen. Zwischen dem 24. Juni und dem 15. November 1994 hielt die ADAK vier Sitzungen ab, im Laufe derer Verbesserungsvorschläge für die Liste erarbeitet wurden (die Liste ist am 15. März 1995 in Kraft getreten). Ferner hat die Arbeitsgruppe einen Katalog sämtlicher Probleme im Zusammenhang mit dem Informationsfluss erstellt und Lösungsvorschläge dazu ausgearbeitet. Wir möchten bei dieser Gelegenheit anmerken, dass die Zusammenarbeit innerhalb der Gruppe äusserst fruchtbar war.

Im Laufe der Arbeiten sowie anlässlich der Prüfung des Verordnungsentwurfes über die Krankenversicherung mussten wir allerdings feststellen, dass die Liste als solche, selbst in ihrer verbesserten Form, aus Sicht des Datenschutzes problematisch ist, wie auch andere im Krankenversicherungsbereich verwendete Listen. Trotzdem haben wir die Ansicht vertreten, dass die Verwendung solcher Listen solange zulässig sein muss, wie diese nicht durch andere - gegenwärtig geprüfte - Systeme für die Kostenkontrolle ersetzt worden sind, die sowohl effizienter, als auch aus datenschutzrechtlicher Sicht unbedenklicher sind.

Auskunftspflicht der AHV-Organe gegenüber den Steuerbehörden (Art. 50, Abs. 1bis des Bundesgesetzes über die Alters- und Hinterlassenenversicherung; AHV)
Dieser neue Absatz trat am 1. Januar 1995 gleichzeitig mit dem Bundesgesetz über die direkte Bundessteuer in Kraft. Er hebt die Schweigepflicht der AHV-Organe gegenüber Behörden, die mit dem Vollzug der Steuergesetze betraut sind, auf. Gestützt auf diese Bestimmung hatte die Konferenz der Steuerbeamten die systematische Bekanntgabe bestimmter Informationen verlangt. Wir sind bezüglich der Frage, in welchem Ausmass die

AHV-Organe zur Amtshilfe verpflichtet sind, mehrfach konsultiert worden. Wir kamen zum Schluss, dass diese Bestimmung - abgesehen von ihrem obligatorischen Charakter - auf der Linie der allgemeinen Amtshilfegrundsätze im Verwaltungsbereich liegt. Diese können wie folgt zusammengefasst werden:

- eine gesetzliche Grundlage sieht die Weitergabe von Informationen ausdrücklich vor;
- im Einzelfall wird ein begründeter Antrag eingereicht;
- die Auskünfte sind für den Vollzug der Steuergesetze notwendig;
- die Informationen konnten beim Steuerzahler oder bei seinem Arbeitgeber nicht eingeholt werden.

Statistik des Konkordats der Schweizerischen Krankenkassen (KSK)
Wir haben zunächst darauf hingewiesen, dass die Verwendung des Begriffs "Statistik" sowohl vom Standpunkt des Statistikgesetzes aus, als auch aus Sicht des Datenschutzes ungeeignet ist, solange die Statistik des KSK namentlich (nach den Leistungserbringern) geführt wird und nicht hauptsächlich einen statistischen Zweck verfolgt, sondern eher zur Überprüfung der Wirtschaftlichkeit der Behandlungen dient.

Im Juli 1994 wurden wir von einer Privatperson auf die Rechtmässigkeit der KSK-Statistik angesprochen. Zunächst haben wir angemerkt, dass das Eidgenössiche Versicherungsgericht in seiner ständigen Rechtsprechung den Rückgriff auf diese Methode zum Zwecke der Feststellung einer Überarztung für zulässig erklärt hat. Es ist jedoch auf die Frage der Rechtmässigkeit der KSK-Statistik nicht eingetreten, da es offenbar die Auffassung vertritt, die Bestimmung des Krankenversicherungsgesetzes, welche den Grundsatz der Wirtschaftlichkeit der Behandlungen stipuliert, stelle eine hinreichende Gesetzesgrundlage dar. Nach Überprüfung dieser Bestimmung sowie des Inhalts der KSK-Statistik aus datenschutzrechtlicher Sicht, sind wir zu der Ansicht gelangt, dass der Grundsatz der Rechtmässigkeit nicht verletzt ist, solange die Statistik als Kontrollinstrument bezüglich der Wirtschaftlichkeit der Behandlungen eingesetzt wird.

Wir haben jedoch betont, dass die derzeitige Situation nicht befriedigend ist, da immer mehr potentielle Benutzer auf diese Statistik zurückgreifen möchten, was angesichts des Fehlens eines präzisen rechtlichen Rahmens zu einer Verletzung des Zweckbindungsgrundsatzes führen könnte. Andererseits sind die Krankenkassen und die Aufsichtsbehörden in ihrer Funktion als Bundesorgane für die Einhaltung des Datenschutzes in bezug auf die Daten, die sie bearbeiten oder bearbeiten lassen, verantwortlich. Diese Verantwortung können sie aber nur auf vertraglichem Weg sicherstellen, was unbefriedigend ist. Mit dem für 1996 vorgesehenen Inkrafttreten des neuen Krankenversicherungsgesetzes wird sich die Frage eines Nebeneinanders der KSK-Statistik und anderer Statistiken, wie sie etwa vom Bundesamt für Sozialversicherungen geführt werden sollen, verschärft stellen. Schliesslich kommt die Verantwortung für die KSK-Statistik sowohl Bundesorganen als auch Privatpersonen zu, was die Situation zusätzlich kompliziert. Deshalb sind wir zum Schluss gekommen, dass es vor allem im Interesse der Transparenz und der Rechtssicherheit notwendig ist, so bald als möglich eine spezifische gesetzliche Grundlage für die KSK-Statistik zu schaffen, welche zunächst in einer Vollzugsverordnung zum neuen Krankenversicherungsgesetz und bei einer Revision des Gesetzes in diesem selbst zu verankern ist.

Aus den vorangegangenen Ausführungen geht hervor, dass im Bereich der Sozialversicherungen die Sensibilisierung für Datenschutzfragen wächst und den Anforderungen des Datenschutzgesetzes vermehrt Rechnung getragen wird, obwohl die im

Bericht Jaggi vor mehr als zehn Jahren festgestellten Lücken noch lange nicht geschlossen sind.

6.2. Privatversicherungen - Informationsblatt und Einwilligungsklausel

Die Privatversicherungen sind nach Datenschutzgesetz im Prinzip dazu verpflichtet, ihre Datensammlungen bei uns anzumelden, da für die Bearbeitung der meisten Daten keine gesetzliche Pflicht besteht und die Betroffenen über die Bearbeitung zumeist nicht genügend informiert sind. Die meisten Versicherer zogen es vor, die Betroffenen zu informieren, anstatt ihre Datensammlungen anzumelden. Die Information erfolgte im allgemeinen mit Hilfe eines Merkblattes. Ausserdem wurde die Einwilligungsklausel genauer formuliert. Diese Neuformulierung bezweckte nicht nur mehr Transparenz, sondern sollte es den Versicherern auch ermöglichen, die ärztliche Schweigepflicht aufzuheben, ohne sie zu verletzen. Diese Schriftstücke wurden uns zum grössten Teil vor ihrer Verwendung nicht vorgelegt, und wir haben darin eine gewisse Anzahl Lücken und Ungenauigkeiten festgestellt. Wir haben insbesondere bemängelt, dass die Klausel aufgrund ihrer zu allgemein gehaltenen Formulierung einer Blankovollmacht zugunsten der Versicherungen gleichkommt, was mit den Anforderungen des Datenschutzes nicht zu vereinbaren ist. Ferner haben wir die Ansicht vertreten, dass die von einigen Versicherern gewählte Lösung, nur eine einzige standardisierte Einwilligungsklausel vorzusehen, die für sämtliche Privatversicherungsbereiche verwendet werden kann, dem Datenschutzgesetz zuwiderläuft. Der Umfang und die Häufigkeit des für die Verwaltung eines Dossiers erforderlichen Informationsflusses ist nämlich zum Beispiel bei den Lebensversicherungen ein anderer als bei den Zusatzkrankenversicherungen.

7. Gesundheitswesen

7.1. Kontrollierte Drogenabgabe

Die Versuche mit der kontrollierten Drogenabgabe sind auch aus datenschutzrechtlicher Sicht nicht unumstritten. Im Interesse der Teilnehmer sollten die Versuche anonym durchgeführt werden können. Dies ist denn auch in der entsprechenden Verordnung so vorgesehen. Dagegen wird jedoch von verschiedener Seite Widerstand geleistet. Namentlich wurde gefordert, die Teilnehmer sollten den Führerausweis während der Dauer des Versuchs beim Strassenverkehrsamt hinterlegen.

Der Verzicht auf jegliche Weitergabe der Daten von Testteilnehmern an Dritte, vor allem an Verwaltungsbehörden oder an die Polizei, stiess zum Teil auf grossen Widerstand. So wehrten sich die Strassenverkehrsämter dagegen mit der Begründung, da während der Projektteilnahme aufgrund der damit zusammenhängenden Einnahme von Drogen das Führen eines Motorfahrzeuges nicht zulässig ist, müsse der Führerausweis bei ihnen hinterlegen werden. Werde der Führerausweis nur freiwillig beim Projektleiter hinterlegt, so habe das Lenken eines Fahrzeugs höchstens eine Busse wegen Nichtmitführens des Führerausweis zur Folge, während andernfalls ein disziplinarisches Verfahren stattfinde. Die Hinterlegung des Führerausweises beim Strassenverkehrsamt kommt jedoch in der Wirkung einem Entzug gleich. Eine so einschneidende Massnahme ist in der *Verordnung über die*

Förderung der wissenschaftlichen Begleitforschung zur Drogenprävention und Verbesserung der Lebensbedingungen Drogenabhängiger, welche die Einzelheiten des Versuchs regelt, nicht vorgesehen und kann den Teilnehmern nicht ohne weiteres auferlegt werden.

Zu den Versuchen werden nur Personen zugelassen, welche schriftlich in die Teilnahme am Versuch eingewilligt haben (Einverständnis-Erklärung. vgl. die Einzelheiten dazu im 1. Tätigkeitsbericht, auf S. 44/45). Dieser Einwilligung geht eine eingehende mündliche und schriftliche Information über die Bedingungen der Versuche voraus. Die betreffende Person wird darüber orientiert, dass während der Projektteilnahme das Führen eines Motorfahrzeuges nicht zulässig ist und dass das Führen eines Motorfahrzeuges unter Betäubungsmitteleinfluss strafbar ist. Sie verpflichtet sich, ihren Führerausweis zu Beginn des Projektes beim Projektleiter zu hinterlegen. Sie erklärt sich ferner mit der wissenschaftlichen Auswertung des Projektes einverstanden und erklärt sich ebenso bereit, unter bestimmten, in der Zustimmungserklärung aufgezählten Bedingungen, an den Befragungen und Untersuchungen teilzunehmen. Dazu gehört namentlich die Anonymisierung aller für die wissenschaftliche Auswertung erforderlichen Daten. Durch externe Interviewer erhobene personenbezogene Daten werden nicht weitergegeben, auch nicht an das Projekt. Damit wird ausgeschlossen, dass die Beantwortung der Fragen persönliche Konsequenzen für die betroffenen Personen hat. Damit trotz der Anonymisierung Angaben über die Beschaffungskriminalität erhoben werden können, wird jeweils bei Eintritt in das Projekt und bei Abschluss von der Projektleitung ein Strafregisterauszug eingeholt. Um die Anonymität der Probanden auch in diesem Bereich zu wahren, ist aus der Anfrage beim Zentralstrafregister die Teilnahme an dieser Studie nicht ersichtlich.

Wie sich in der Praxis herausstellte, sind die meisten Teilnehmer gar nicht im Besitze eines Führerausweises. Dennoch dürfte die Aufhebung der Anonymität durch die Hinterlegung des Führerausweises beim Strassenverkehrsamt die Bereitschaft zur Teilnahme an den Versuchen generell reduzieren. Dies wiederum hätte nachteilige Auswirkungen auf die wissenschaftliche Auswertung der Präventions- und Betreuungsmassnahmen und schliesslich auf die Entwicklung neuer Behandlungsmöglichkeiten. Bei einer Abwägung zwischen dem öffentlichen Interesse an der Verkehrssicherheit und demjenigen an der wissenschaftlichen Auswertung der Versuche mit der kontrollierten Drogenabgabe, dürfen sowohl die geringe Teilnehmerzahl (Anfangs 1995 waren lediglich ungefähr 320 Personen, die zumeist keinen Führerausweis besitzen, am Versuch beteiligt) als auch die befristete Projektdauer bis Ende 1996 nicht ausser Acht gelassen werden.

Aufgrund dieser Überlegungen sind wir zum Schluss gekommen, dass der Hinterlegung der Führerausweise während der Dauer der Teilnahme am Versuch bei den Projektleitern gegenüber der Hinterlegung bei den Strassenverkehrsämter namentlich mit Blick auf die sich aus der Aufhebung der Anonymität möglicherweise ergebenden Persönlichkeitsverletzungen der Vorzug zu geben ist.

7.2. Software-Demoversionen

Für Demoversionen von Software sollten Personendaten nur mit dem Einverständnis der Betroffenen verwendet werden. Ansonsten ist die Verwendung offensichtlicher Fantasienamen vorzuziehen, damit sichergestellt ist, dass niemand in seiner Persönlichkeit verletzt wird.

Wir wurden von einem Softwareentwickler angefragt, ob eine Demoversion eines Software-Paketes für Ergo- und Physiotherapeuten mit verwürfelten Patientendaten für Demonstrationszwecke datenschutzkonform sei. Als Stammdaten sollten Name, Vorname, Adresse, Geschlecht, Zivilstand, Geburtsdatum, Telefonnummer, Beruf und Arbeitgeber sowie die Krankenkasse ohne Mitgliedernummer bearbeitet werden. In Verbindung mit medizinischen Diagnosen und verschriebenen Behandlungen sind diese Personendaten als besonders schützenswert zu qualifizieren.
Zunächst befremdete uns, dass im betreffenden Fall der Zugriff auf echte Patientendaten durch einen Softwareentwickler überhaupt möglich war. Gemäss Art. 321 Strafgesetzbuch sind nämlich Ärzte sowie deren Hilfspersonen (wie z.B. Physiotherapeuten) zur Verschwiegenheit verpflichtet, wenn ihnen in Ausübung ihres Berufes ein Geheimnis anvertraut worden ist. Eine Offenbarung dieser Information ist auf Antrag sogar strafbar. Wer vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekanntgibt, von denen er bei der Ausübung seines Berufes, der die Kenntnis solcher Daten erfordert erfahren hat, macht sich strafbar. Dasselbe gilt, wenn die Personendaten bei der Tätigkeit für den Geheimhaltungspflichtigen in Erfahrung gebracht wurden (Art. 35 Abs. 1 und 2 DSG). Aus diesen Gründen ist die Weitergabe von echten Patientendaten durch Physiotherapeuten ohne Einwilligung der betroffenen Personen nicht erlaubt, womit sich die Prüfung der Zulässigkeit der Bearbeitung dieser Daten durch den Softwareentwickler erübrigt, selbst wenn die Daten unkenntlich gemacht werden.
Etwas anderes gälte nur, wenn die betroffenen Personen ihre Daten freiwillig zur Verfügung stellen würden. In diesem Fall stünde einer Bearbeitung nichts im Wege. Die Betroffenen müssten allerdings vorher genau orientiert werden, zu welchem Zweck ihre Daten bearbeitet werden, über welchen Zeitraum die Bearbeitung erfolgt, wie die Weitergabe an Dritte und die anschliessende Vernichtung der Daten vorgesehen ist und dazu ihre ausdrückliche schriftliche Zustimmung geben. Ansonsten ist die Verwendung eindeutiger Fantasienamen oder numerischer Bezeichnungen vorzuziehen.
Werden für die Demoversion echte Krankengeschichten benötigt, so dürfen sie vom Inhaber der Datensammlung erst nach vorgängiger Anonymisierung zur Verfügung gestellt werden. Anonymisiert ist die Krankengeschichte erst, wenn eine Person auch nicht aufgrund einer bestimmten Kombination von Daten (zum Beispiel eines seltenen Krankheitsbildes) bestimmt werden kann.

7.3. Softwarewartung

Für die Wartung eines EDV-Systems durch externe Personen sind besondere Vorkehren zu treffen. Manchmal kann der Zugriff des Lieferanten auf die darin enthaltenen Personendaten unumgänglich sein. Wenn immer möglich sollte aber der Inhaber der Datensammlung Personendaten vor der Wartung aus dem Computer entfernen.

Obwohl das Wartenlassen eines Computers kein Zugänglichmachen von Personendaten im engeren Sinn darstellt, bietet sich dabei Gelegenheit, in die im Computer gespeicherten Daten Einsicht zu nehmen. Wird durch die Wartung Zugang zu besonders schützenswerten Daten verschafft, so ist ein besonderer Schutz erforderlich. Der Schutz ist durch technische und/oder organisatorische Massnahmen zu verwirklichen (wie etwa das Vier-Augen-Prinzip). Zu beachten sind die Strafbestimmungen des DSG. Auf Antrag wird bestraft, wer vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekanntgibt, von denen er bei der Tätigkeit für den Geheimhaltungspflichtigen erfahren hat (Art. 35 Abs. 2 DSG).

Der Inhaber der Datensammlung tut gut daran, mit dem Lieferanten ein "Non-Disclosure-Agreement" abzuschliessen. Am besten bildet eine solche Vereinbarung bereits Inhalt des Supportvertrages.

7.4. Auskunftsrecht der Patienten - Kostenbeteiligung

Jede Person kann vom Inhaber einer Datensammlung Auskunft darüber verlangen, welche Daten über sie bearbeitet werden. Dies gilt auch für die Daten, die der Arzt über seine Patienten bearbeitet. Wir hatten zu prüfen, unter welchen Voraussetzungen der Arzt vom Patienten eine Kostenbeteiligung für die Einsicht in sein Dossier verlangen kann.

Eine Patientin verlangte nach einer über zehnjährigen Therapie von ihrem Arzt eine Kopie ihrer handgeschriebenen Krankengeschichte. Der Arzt war dazu grundsätzlich bereit, wollte jedoch wissen, wozu seine handschriftlichen Einträge benötigt würden und unterbreitete ihr einen Kostenvoranschlag für die Kopien, bei dem er auch den Arbeitsaufwand berücksichtigte. Die Patientin ihrerseits war der Auffassung, das Auskunftsrecht könne unentgeltlich ausgeübt werden und beanstandete den Kostenvoranschlag.
Grundsätzlich kann jede Person vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob und welche Daten über sie bearbeitet werden. Sie muss die Auskunft schriftlich beantragen und sich gegenüber dem Inhaber der Datensammlung über ihre Identität ausweisen. Die Auskunft ist in der Regel schriftlich, in Form eines Ausdrucks oder einer Fotokopie sowie kostenlos zu erteilen. Da die Ausübung des Auskunftsrechtes Ausfluss des Grundrechts der persönlichen Freiheit ist, muss es grundsätzlich unabhängig von der Entrichtung einer Gebühr geltend gemacht werden können.
Die Verordnung zum Datenschutzgesetz sieht eine Ausnahme vom Grundsatz der Kostenlosigkeit vor, wenn der antragstellenden Person in den zwölf Monaten vor dem Gesuch die gewünschten Auskünfte bereits mitgeteilt wurden und kein schutzwürdiges Interesse an einer neuen Auskunftserteilung nachgewiesen werden kann. Ein schutzwürdiges Interesse ist insbesondere gegeben, wenn die Personendaten ohne Mitteilung an die betroffene Person verändert wurden. Eine Kostenbeteiligung kann aber auch erhoben werden, wenn die Auskunftserteilung mit einem besonders grossen Arbeitsaufwand verbunden ist. Dies kann der Fall sein, wenn beispielsweise die Datensammlung manuell und ausschliesslich für interne Zwecke geführt worden ist, und nicht dafür eingerichtet ist, Daten bekanntzugeben. In Zukunft müssen die Inhaber von Datensammlungen dafür sorgen, dass ihre Datensammlungen so organisiert sind, dass sie der betroffenen Person die Ausübung ihres Auskunfts- und Berichtigungsrechts erlauben.
Die Gebühr beträgt maximal 300 Franken. Der Gesuchsteller ist über die Höhe der Beteiligung vor der Auskunftserteilung in Kenntnis zu setzen und kann sein Gesuch innert zehn Tagen zurückziehen. Verlangt werden kann eine "angemessene Beteiligung", nicht aber die reellen Kosten der Operation.
Im vorliegenden Fall haben wir der Patientin geraten, den Arzt anzufragen, ob die Krankengeschichte an Ort und Stelle eingesehen werden könnte. Nebst den geringeren Kosten dieser Vorgehensweise erlaubt diese auch, allfällige Missverständnisse aufzuklären. Ausserdem erübrigt sich das Entziffern von handgeschriebenen Einträgen. Die Auskunft könnte allenfalls auch mündlich erteilt werden, sofern die um Auskunft ersuchende Person damit einverstanden wäre. Bei heiklen Informationen über die Gesundheit der betroffenen Person kann es ratsam sein, dass diese einen neutralen Arzt ihres Vertrauens beizieht, der ihr diese Informationen mitteilt.

7.5. Blutspenden - medizinischer Fragebogen

Wer Blut spenden will, muss zuerst einen medizinischen Fragebogen des Schweizerischen Roten Kreuzes (SRK) ausfüllen, damit die Spendetauglichkeit geprüft werden kann. Aus Sicherheitsgründen stellt dies eine Voraussetzung für die Blutspende dar. Die Beantwortung der zum Teil recht weit in die Intimsphäre vordringenden Fragebogen stösst jedoch manchmal auf Widerstand.

Eine Person, die Blut spenden wollte und einen solchen Fragebogen hätte ausfüllen sollen, war durch die Ausrichtung gewisser Fragen irritiert. Dabei handelte es sich unter anderem um Fragen über sexuelle Beziehungen, Drogenkonsum, Impfungen, Zeckenbisse, Reisen in Malaria-Gebiete, Schwangerschaften und Hormonbehandlungen. Da der Bogen mit weiteren Angaben ergänzt und später archiviert werden sollte, weigerte sich die betreffende Person, den Bogen vollständig auszufüllen und konnte daraufhin kein Blut spenden. Sie hat sich an uns gewandt, um zu erfahren, ob die Fragen und ihre weitere Bearbeitung zulässig seien.
Wie aus einem vor dem Ausfüllen des Fragebogens an die betroffenen Personen abgegebenen Merkblatt hervorgeht, ist sich das SRK bewusst, dass es mit diesen Fragen weit in die Privatsphäre der spendewilligen Personen vorstösst. Der medizinische Fragebogen stellt aber eine wichtige Massnahme dar, um dem Empfänger die bestmögliche Sicherheit der Blutprodukte zu gewährleisten. Vorderhand untersteht das SRK den Bestimmungen über das Bearbeiten von Personendaten durch private Personen. Wer als Privatperson Personendaten bearbeitet, darf die Persönlichkeit der Betroffenen nicht widerrechtlich verletzen. Eine Verletzung der Persönlichkeit kann unter anderem durch Einwilligung des Verletzten gerechtfertigt sein. Indem die spendewillige Person die verlangten Angaben freiwillig liefert, willigt sie in die Überprüfung ihrer Spendetauglichkeit ein. Damit ist die für die Durchführung der Blutspende erforderliche Datenbearbeitung gerechtfertigt.

8. Kreditwesen

Kreditwarnlisten

Verschiedentlich stellen Verbände ihren Mitgliedern ganze Listen über die Kreditwürdigkeit potentieller Kunden zu. Das systematische und globale Bekanntgeben von Kreditwarnlisten an Dritte stellt jedoch aus datenschutzrechtlicher Sicht grosse Probleme. Wir sahen uns gezwungen, über das Bearbeiten solcher Daten eine Empfehlung zu erlassen.

Ein Verband hat sich bei uns erkundigt, inwieweit sich seine Kreditwarnlisten mit dem DSG vereinbaren liessen. Die Mitglieder des Verbands meldeten dem Sekretariat Kunden, die sie betrieben hatten oder solche, die regelmässig mit Zahlungen im Rückstand waren. Das Sekretariat fasste die Namen dieser Kunden und ihre finanzielle Situation auf Kreditwarnlisten zusammen und stellte diese regelmässig allen Verbandsmitgliedern zu.
Wie wir dem Verband mitgeteilt haben, ist die systematische Bekanntgabe von Kreditwarnlisten an die Verbandsmitglieder nicht datenschutzkonform. Vorzuziehen ist die Abgabe solcher Informationen einzelfallweise und lediglich auf Anfrage hin. Die betreffenden Datensammlungen sind ausserdem bei uns anzumelden, weil die betroffenen Personen von der Datenbearbeitung keine Kenntnis haben.

Der Verband hielt daraufhin fest, nach seiner Auffassung seien Kreditwarnlisten als Mittel des Gläubigerschutzes auch nach DSG zulässig und würden keiner Meldepflicht unterliegen. Zudem könne nicht von einer Weitergabe von Personendaten an Dritte gesprochen werden, nur weil den Mitgliedern des Verbandes wirtschaftliche Selbständigkeit zukomme. Die Datenbekanntgabe innerhalb des Verbandes sei nicht anders zu behandeln als die betriebsinterne Datenbekanntgabe. Eine einzelfallweise Behandlung von Anfragen über die Kreditwürdigkeit wäre mit einem enormen Mehraufwand und unzumutbaren Mehrkosten verbunden, womit der interne Kreditschutz geradezu illusorisch gemacht würde. Weiter sehe ein Reglement vor, dass die Listen ausschliesslich für die Überprüfung der Kreditwürdigkeit von potentiellen Kunden benützt werden dürften.
In der Folge haben wir eine Empfehlung erlassen, wonach der Verband ab sofort das systematische und globale Versenden von Kreditwarnlisten mit Name, Adresse, Angaben über die finanzielle Situation und eventuell Schuldbetreibungs- und Konkursdaten potentieller Kunden zu unterlassen habe. Auskünfte seien nur noch auf Anfrage und einzelfallweise zu erteilen. Die betreffende Datensammlung ist bei uns anzumelden.

Der Verband hat aufgrund der Empfehlung von der systematischen Erfassung und Bekanntgabe von Kreditwarnlisten abgesehen und ein EDV-Konzept "Debitorenkontrolle" entwickelt. Dieses Konzept wurde uns unterbreitet und beinhaltet folgende Regelungen:

- Der Verband erstellt ein Reglement, worin die Rahmenbedingungen für die Benützung des EDV-Systems gefordnet werden. Zusätzlich wird mit jedem Systembenützer ein Vertrag abgeschlossen, der ihn verpflichtet, nur die Kreditwürdigkeit von Kunden zu prüfen, mit denen effektiv geschäftliche Beziehungen geknüpft oder Verträge abgeschlossen werden. Aufgrund der vertraglichen Regelung wird davon abgesehen, für jede Anfrage einen Interessennachweis zu verlangen. Die Mitglieder werden verpflichtet, nur richtige Angaben zu liefern und die erhaltenen Auskünfte nicht an Dritte weiterzugeben. Das bisherige System der Kreditwarnlisten wird aufgegeben. Zur Zeit werden die Daten quartalsweise in eine Datenbank überführt. In Zukunft sollen diese Meldungen monatlich erfolgen. Die Aktualität und Richtigkeit der Daten wird durch den Verband gewährleistet.
- Das EDV-System wird technisch so gestaltet, dass nur die einzelfallweise Abfrage möglich ist. Ein Blättern in den Datensätzen wird nicht zugelasssen. Als Suchkriterien dienen dem Benützer nur der Name, die Firma oder die Mehrwertsteuernummer (eindeutige Identifikationsmerkmale) des Kunden.
- Daten, die dem Verbandssekretariat auf Papier zugestellt wurden, werden ein Jahr lang unter Verschluss aufbewahrt und anschliessend vernichtet. Sämtliche Angaben, die im System aufgenommen sind, werden im ersten Jahr alle drei Monate gelöscht und neu überschrieben, danach jeden Monat. Die Herkunft der Informationen über die Kreditwürdigkeit kann durch den Verband jederzeit festgestellt werden, um der Auskunftspflicht nachzukommen. Die Datensammlung wird bei uns angemeldet.

9. Mietrecht

9.1. Anmeldeformulare für Mietinteressenten

Bezüglich der Angaben, die bei der Auswahl eines Mieters oder einer Mieterin vom Vermieter erhoben werden dürfen, haben wir eine Empfehlung erlassen.

Bereits im Dezember 1993 waren uns Anmeldeformulare für MietinteressentInnen zur Begutachtung unterbreitet worden. In der Folge haben wir mit den Interessenverbänden Hearings durchgeführt, eine erste Stellungnahme erarbeitet, diese den Interessenverbänden und anderen interessierten Personen zur Vernehmlassung unterbreitet und eine beträchtliche Anzahl von in der Praxis gebräuchlichen Anmeldeformularen in Hinblick auf die erhobenen Daten untersucht (hierzu auch den 1. Tätigkeitsbericht, S. 61 f.).

Bei dieser Untersuchung hat sich folgendes ergeben:

- Die Bearbeitung von Personendaten bei der Vermietung von Wohnobjekten ist dem Geltungsbereich des DSG unterstellt. Sie stellt keine Bearbeitung von Personendaten ausschliesslich zum persönlichen Gebrauch dar, auf die das DSG keine Anwendung finden würde.
- Nicht jede Datenbearbeitung im Zusammenhang mit der Vermietung von Wohnobjekten ist dadurch gerechtfertigt, dass die Mietinteressenten von der Datenbearbeitung Kenntnis haben oder die Angaben selbst mitgeteilt haben. Datenbearbeitungen, die gegen allgemeine Bearbeitungsgrundsätze verstossen oder die Persönlichkeit der Mietinteressenten auf andere Weise verletzen, sind nur durch Einwilligung gerechtfertigt, wenn die betroffene Person ihre Einwilligung in Kenntnis des Verstosses erteilt hat.
- Ein überwiegendes Interesse des Vermieters an der Datenbearbeitung liegt nicht in jedem Fall vor. Zwar bearbeitet der Vermieter Personendaten in Zusammenhang mit dem Abschluss des Mietvertrags, was grundsätzlich die Datenbearbeitung rechtfertigt. Jedoch gilt dies nur für die Bearbeitung von Daten über den Vertragspartner und in dem Umfang, der für den Abschluss des Vertrags erforderlich ist. Darüber hinaus gehende Datenbearbeitungen, zum Beispiel von Angaben, die für die Auswahl des Mieters gar nicht nötig sind oder bei Personen, die für die Vermietung gar nicht in Betracht kommen, sind dadurch nicht gerechtfertigt. Je zahlreicher die Personen sind, über die im Vorfeld eines Vertragsabschlusses Daten erhoben werden, desto mehr Zurückhaltung ist bei der Erhebung und Bearbeitung von Daten über diese Personen angebracht, da ein unmittelbarer Zusammenhang mit dem Vertragsabschluss vielfach fehlt.
- Das Bestehen gesetzlicher Pflichten, welche die Erhebung von Angaben über den einziehenden Mieter erforderlich machen (zum Beispiel Pflicht zur Meldung an die Einwohnerkontrolle) rechtfertigt nicht, dass diese Angaben schon bei allen Mietinteressenten erhoben werden.
- Die Datenerhebung darf nicht unrechtmässig sein (z. B. Frage nach Bereitschaft zum Abschluss eines Versicherungsvertrags mit der betreffenden Liegenschaftsverwaltung), sie darf nicht gegen Treu und Glauben verstossen (z. B. Erkundigung nach Automarke, um die finanzielle Leistungsfähigkeit abschätzen zu können) und sie darf nicht unverhältnismässig sein. Aus den untersuchten Formularen wurde ersichtlich, dass der Vermieter seine Auswahl primär aufgrund der finanziellen Lage des Mietinteressenten trifft und dann noch abklärt, ob er Lebensgewohnheiten hat, die sich auf die Mitbewohner störend auswirken können. Fragen, die sich nicht

auf diese zwei Bereiche beziehen, sind grundsätzlich als unverhältnismässig und nicht zulässig zu betrachten. Zudem müssen die notwendigen Abklärungen auf für den Mietinteressenten möglichst schonende Art und Weise getroffen werden. So braucht der Vermieter nicht zu erfahren, ob der Mietinteressent verlobt, verheiratet, getrennt, geschieden oder verwitwet ist, um abzuklären, ob die Wohnung als Familienwohnung im Sinne des Eherechts dient. Es reicht, wenn er fragt, ob die Wohnung als Familienwohnung dienen soll.

- Schliesslich dürfen die Daten nicht zu einem anderen Zweck als der Auswahl eines geeigneten Mieters und dem Abschluss des Mietvertrags verwendet werden. Sie dürfen auch nicht an Dritte weitergegeben werden und müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt sein. Nach Abschluss des Auswahlverfahrens sind grundsätzlich alle Daten, ausser denjenigen des ausgewählten Mieters unverzüglich zu vernichten.

Gestützt auf diese Überlegungen kamen wir zum Ergebnis, dass zwischen vier Kategorien von Daten zur unterscheiden ist:

- Daten, die auf jeden Fall erhoben werden dürfen,
- Daten, die nur erhoben werden dürfen, wenn und soweit eine diesbezügliche gesetzliche Pflicht besteht (zum Beispiel Pflicht zur Meldung von ausländischen Mietern an die Fremdenpolizei),
- Daten, die nur unter besonderen Voraussetzungen erhoben werden dürfen (zum Beispiel statutarische Bestimmung, wonach eine Wohngenossenschaft nur an Personen in Ausbildung vermietet),
- Daten, die unter keinen Umständen erhoben werden dürfen (zum Beispiel Bestehen chronischer Krankheiten).

Die Fragen auf den von uns untersuchten Anmeldeformularen haben wir in diese vier Kategorien unterteilt und gestützt darauf eine Empfehlung erlassen, die sich an alle Personen, welche in der Schweiz Wohnungen vermieten, richtet. Diese wurde im Bundesblatt veröffentlicht und den an den Hearings und dem darauffolgenden Vernehmlassungsverfahren beteiligten Verbänden und Personen zugestellt.

In der Folge lehnten mehrere Vermieter die Empfehlung ganz oder teilweise ab. Der Eidgenössische Datenschutzbeauftragte kann in einem solchen Fall die Angelegenheit der Eidgenössischen Datenschutzkommission zum Entscheid vorlegen. Dies geschah im Februar 1995. Über das weitere Vorgehen entscheidet nun die Eidgenössische Datenschutzkommission.

9.2. Bekanntgabe der Vermieter von Invalidenwohnungen

Das Bundesamt für Wohnungswesen hat sich bei uns erkundigt, ob es zulässig sei, dem Schweizerischen Invalidenverband eine gesamtschweizerische Liste von mit Bundeshilfe geförderten Invalidenwohnungen zuzustellen. Die Datenbekanntgabe umfasst die Adresse der betreffenden Liegenschaft, Name und Adresse des Bauherrn, den Mietbeginn und die Anzahl der Invalidenwohnungen.

Soweit die betroffenen Personen über die Datenbekanntgabe informiert sind und die Möglichkeit haben, die Bekanntgabe abzulehnen, ist diese unproblematisch. Wir rieten dem Bundesamt für Wohnungswesen deshalb, in Zukunft bei der Vergabe von Subventionen für

Invalidenwohnungen auf die Möglichkeit der Datenbekanntgabe an einen oder mehrere genau zu bezeichnende Invalidenverbände hinzuweisen und den Betroffenen die Möglichkeit zu geben, sich dieser Bekanntgabe zu widersetzen. Für die bereits bestehenden Wohnungen wäre die Information der betroffenen Personen mit einem sehr grossen Aufwand verbunden gewesen. Da vom Bund subventionierte Invalidenwohnungen nur an Invalide vermietet werden dürfen, kann jedoch davon ausgegangen werden, dass die Vermieter im Prinzip ein Interesse daran haben, dass Kandidaten, welche die Mietvoraussetzungen erfüllen, von der Existenz solcher Wohnungen Kenntnis erhalten. Ausserdem würde eine Bekanntgabe nur der Liegenschaftsadresse interessierte Personen zwingen, verschiedenenorts Erkundigungen über die Person des Vermieters einzuziehen. Dies kann für invalide Personen eine wesentliche Erschwerung darstellen und bedeutet für den Vermieter nicht unbedingt ein schonenderes Vorgehen.
Aus diesen Gründen haben wir im Sinne einer Interessenabwägung einer Bekanntgabe der schon existierenden Wohnungen ohne vorgängige Information der betroffenen Besitzer ausnahmsweise zugestimmt. Dabei haben wir folgende Auflagen gemacht, um die Gefahr einer unerwünschten Bekanntgabe möglichst geringzuhalten:

- Wann immer sich dazu eine Gelegenheit ergibt, sollten die betroffenen Personen auch im Nachgang zur Bekanntgabe noch darüber informiert werden.
- Es dürfen nur die für die Vermietung der betreffenden Wohnungen relevanten Adressen bekanntgeben werden (also gegebenenfalls der Liegenschaftsverwaltung und nicht des Besitzers oder Bauherrns).
- Bei Ablehnung der Bekanntgabe durch eine betroffene Person dürfen die Daten nicht weitergegeben werden oder wenn dies schon geschehen ist, muss dafür gesorgt werden, dass die Invalidenverbände die betreffende Adresse nicht mehr weitergeben und aus ihrer Datensammlung entfernen.
- Die Invalidenverbände dürfen die Adressen nur an Personen, welche als Mieter/innen in Frage kommen und nur für diesen Zweck weitergeben. Damit nicht jedesmal die ganze Adressliste abgegeben werden muss, haben wir zudem geraten, eine Aufteilung in Regionen vorzunehmen.

Vom Erfordernis der Einwilligung der betroffenen Personen entbunden wäre das Bundesamt für Wohnungswesen nur, wenn in der Verordnung zum Wohnbau- und Eigentumsförderungsgesetz eine gesetzliche Grundlage für die erwähnte Datenbekanntgabe geschaffen würde.

II. WEITERE THEMEN

1. Versandhandel

In unseren Briefkästen landen die verschiedensten Postsendungen. Vieles davon ist Werbung, oft mit einer Kaufofferte verbunden. Dieses meist harmlose alltägliche Phänomen kann manchmal recht unangenehme Folgen haben.

Letztes Jahr ist uns folgender Vorfall angezeigt worden: Ein Lehrer erhielt an seiner Schuladresse einen Gutschein für den Kauf von Sexzubehör zugestellt. Abgesehen davon, dass er nie so ein Produkt bestellt hatte, störte er sich daran, dass er an seinem Arbeitsplatz ein solches Angebot erhielt. Ausserdem wurde er auf dem Gutschein fälschlicherweise als

Frau angesprochen. Die ganze Angelegenheit war für ihn äusserst peinlich, deshalb wandte er sich an uns und bat um Rat wie er sich gegen eine solche Zustellung wehren könnte.

Wir empfahlen ihm, sein Auskunftsrecht geltend zu machen, um herauszufinden, weshalb seine Adresse für diesen Zweck verwendet worden war. Das Versandhaus antwortete daraufhin, dass es unter seinem Namen eine Bestellung für ein solches "Gerät" erhalten habe. Es sei jedoch nicht in der Lage, die Herkunft der Bestellung zu überprüfen, weil Bestellungen sowohl brieflich als auch telefonisch entgegengenommen würden. Das Versandhaus war bereit, die Personalien des Lehrers aus seiner Kundenkartei zu streichen. Dieser wollte jedoch wissen, woher das Versandhaus seine Adresse erhalten hatte, damit er seine Adresse auch dort sperren lassen konnte. Er störte sich daran, dass das Versandhaus die Herkunft der Bestellung überhaupt nicht überprüft, insbesondere wenn es sich um Bestellungen "heikler" Art handelt und verwies auf Art. 5 DSG, der den Inhaber einer Datensammlung verpflichtet, sich über die Richtigkeit der Personendaten, die er bearbeitet, zu vergewissern. Eine solche Überprüfung drängt sich vor allem auf, wenn eine Bestellung nicht unterschrieben ist. In Fällen wie dem vorliegenden muss sodann sichergestellt werden, dass nicht Minderjährige solche Produkte bestellen können.

Der betroffene Lehrer brachte die Angelegenheit durch Strafanzeige vor Gericht. Dieses stellte fest, dass die Strafbestimmungen des Datenschutzgesetzes nicht verletzt worden waren, räumte jedoch ein, dass durch die auf Fahrlässigkeit zurückzuführende irrtümliche Bearbeitung seiner Personendaten eine Verletzung seiner Persönlichkeit entstehen konnte. Die Gerichtskosten wurden deshalb dem Versandhaus auferlegt. Gestützt auf dieses Urteil wollte der Betroffene eine Schadenersatzklage erheben. Er verzichtete jedoch schliesslich darauf aus Furcht vor zu hohen Kosten, weil die Zivilprozessordnung seines Wohnsitzkantons eine *obligatorische Rechtsvertretung* vorschreibt. Es ist bedauerlich, dass die Durchsetzung des Rechts des Geschädigten an prozeduralen Bestimmungen scheitern musste. Man sollte vielleicht überlegen, ob in Fällen von Persönlichkeitsverletzungen das Zivilverfahren ähnlich wie bei Klagen zur Durchsetzung des Auskunftsrechts nach Art. 15 Abs. 4 DSG vereinfacht werden könnte.

2. Streichung aus dem 156-PTT-Verzeichnis

Die PTT-Betriebe führen ein öffentlich zugängliches Verzeichnis, in dem sämtliche Anbieter von 156er-Nummern aufgeführt sind. An uns wurde das Problem herangetragen, dass die Privatadressen von Personen, die über eine 156er Nummer Sexdienste anbieten, aus dem 156er-Verzeichnis ersichtlich sind, sofern der Anschluss an ihrer Privatadresse ist.

Die PTT-Betriebe haben sich damit einverstanden erklärt, dass Personen, die solche Dienste von ihrer Privatadresse aus anbieten, gegenüber den PTT-Betrieben ein Sperrecht zum Schutz ihrer Persönlichkeit geltend machen können. Bei Ausübung des Sperrechts wird die betreffende Person nicht in das 156er-Verzeichnis aufgenommen oder, sofern sie schon darin enthalten ist, aus demselben gelöscht.

3. Zustellung von Rechnungen / offener Postversand

Fast jeden Tag finden wir in unseren Briefkästen jede Art von Rechnungen verschiedener Herkunft. Telefon-, Strom,- Miet- und sogar Arztrechnungen werden zum Teil ohne Umschlag für jedermann zugänglich verschickt. Je nach Art des Vertragsverhältnisses kann eine Rechnung verschiedene Personendaten enthalten.

Die meisten Rechnungen enthalten die Personalien der Vertragspartner und die zu begleichende Summe. Einige hingegen offenbaren die Art des Vertragsverhältnisses und verschiedene Vertragseigenschaften, welche Rückschlüsse auf Eigenschaften des Betroffenen zulassen wie z. B. das Verhalten, die Lebensbedingungen, die soziale Zugehörigkeit, die finanzielle Situation und anderes mehr.

Bei uns hat sich eine betroffene Person über die offene Postbeförderung von Prämienrechnungen einer Versicherung beschwert. Die Versicherung hatte sich geweigert, solche Prämienrechnungen verschlossen zuzustellen, weil sie der Auffassung war, dass die Zahlungsbeträge keine datenschutzrechtlich relevanten Daten seien. Dem Anwendungsbereich des DSG unterstehen jedoch alle Daten, die sich auf Personen beziehen. Vorausgesetzt ist nur, dass die Daten sich auf bestimmte oder bestimmbare Personen beziehen. Demzufolge gibt es an sich keine "freien Daten". Im Falle der Prämienrechnungen handelt es sich nicht nur um Zahlungsbeträge, sondern um Rechnungen mit verschiedenen Daten und Beträgen, die unter anderem auch Rückschlüsse auf die Art der Versicherungsleistung erlauben.

Bei solchen Rechnungsstellungen sind die allgemeinen Bearbeitungsgrundsätze des DSG zu beachten. Dazu gehört insbesondere das Prinzip der Verhältnismässigkeit. In diesem Sinne ist es verhältnismässig, wenn derartige Prämienrechnungen in verschlossenen Couverts zugestellt werden. Das Postgeheimnis verpflichtet nur den Postbeamten, es schützt nicht vor unbefugter Einsichtnahme in offen verschickte Prämienrechnungen durch Dritte. Gemäss Art. 7 Abs. 1 DSG sind Personendaten jedoch durch angemessene technische oder organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Die Privatperson hat gemäss Art. 8 Abs. 1 Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG) für die Vertraulichkeit der Daten zu sorgen. Das bedeutet insbesondere einen Schutz gegen unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen (lit. e). Für Bundesorgane gelten gemäss Art. 20 Abs. 1 VDSG dieselben Anforderungen. Die technischen oder organisatorischen Massnahmen haben gem. Art. 8 Abs. 2 VDSG angemessen zu sein. Aus diesen Gründen dürfen unserer Ansicht nach Rechnungen nicht offen verschickt werden, weil das Verschicken von Rechnungen in Umschlägen als angemessene Massnahme zu erachten ist, um den Datenschutz hinreichend zu gewährleisten.
Mehrere Gesellschaften haben eine solche Praxis eingeführt.

4. Amtliche Personendaten in private Register

Der Trend zur automatisierten telefonischen Datenabfrage verbreitet sich immer mehr. Via Telekiosk und Videotex sind die vielfältigsten Informationen erhältlich, vom Kochrezept bis zu Konzerthinweisen. Auf demselben Weg werden von privaten Anbietern aber auch heiklere Informationen zur Verfügung gestellt. Über die Zulässigkeit privater Personenregister haben wir uns in einer Empfehlung ausgesprochen.

Bereits im ersten Tätigkeitsbericht (S. 64) haben wir uns zur Zulässigkeit eines privaten Eigentumsregister für geleaste, gestohlene oder gepfändete Fahrzeuge geäussert. Wir waren zum Schluss gekommen, dass gegen den Betrieb eines solchen Registers unter gewissen Voraussetzungen nichts einzuwenden ist, namentlich weil es nur Personendaten enthält, die von der betroffenen Person im Bewusstsein der weiteren Verwendung eingegeben wurden. Im vergangenen Jahr haben wir überprüft, ob der Betrieb eines automatisch abfragbaren Registers, das Auskünfte über Bestattungen, Bevormundungen und Privatkonkurse enthält, die in Amtsblättern veröffentlicht wurden, zulässig ist. Die im Register enthaltenen Angaben wurden Amtsblättern oder anderen amtlichen Publikationen entnommen und waren jeder interessierten Person ohne Interessennachweis gegen Gebühr zugänglich. Der Betreiber des Register berief sich darauf, dass es sich um veröffentlichte und somit öffentliche Daten handle, deren Weiterverwendung ohne weiteres zulässig sei. Dieser Argumentation konnten wir uns nicht anschliessen. Denn:

- Die Beurkundung des Personenstandes und somit auch von *Todesfällen* ist grundsätzlich Sache des Bundes. Aus Gründen der Rechtssicherheit und des Persönlichkeitsschutzes können neben den zu diesem Zweck geführten öffentlichen (nicht aber offen zugänglichen) Zivilstandsregistern keine privaten, der Öffentlichkeit frei zugänglichen Datenbanken mit Zivilstandsdaten zugelassen werden.
- Es besteht ein berechtigtes Interesse privater Personen, über die Kreditwürdigkeit von Personen, mit denen sie in wirtschaftliche Beziehung treten, informiert zu sein und deshalb auch über allfällige *Konkurseröffnungen* Informationen zu erhalten. Dem trägt das Bundesgesetz über Schuldbetreibung und Konkurs Rechnung, in dem es vorsieht, dass wer ein Interesse nachweist, in die von den Betreibungs- und Konkursämtern geführten Protokolle Einsicht nehmen und sich Auszüge aus denselben geben lassen kann. Auch Eröffnung und Schluss des Konkursverfahrens sind öffentlich bekanntzumachen. Daraus ergibt sich jedoch nicht, dass Konkurs- und Pfändungsdaten der Öffentlichkeit ohne weiteres allgemein zugänglich gemacht werden dürfen. Eine zentralisierte, systematische und automatische Erfassung aller Konkurseröffnungen, eventuell gar mit automatischer Meldung an interessierte Personen, beinhaltet eine viel grössere Gefahr der Persönlichkeitsverletzung, als die gesetzlich vorgesehenen Veröffentlichungen oder die Möglichkeit, aufgrund eines Interessennachweises in die Protokolle der Konkurs- und Betreibungsämter Einsicht zu nehmen. Dies wird gerade im vorliegenden von uns überprüften Fall durch die Tatsache bestätigt, dass die auskunftverlangende Person keinen Interessennachweis erbringen muss und somit eine Nachfrage aus reiner Neugierde oder zur gezielten Kreditschädigung nicht auszuschliessen ist.
- Die *Bevormundung* einer mündigen Person muss, sobald sie rechtskräftig geworden ist, im Amtsblatt ihres Wohnsitzes und ihres Heimatortes veröffentlicht werden. Eine erneute Veröffentlichung der Bevormundung ist bei Wohnsitzwechsel des Bevormundeten vorgesehen. Diese Bestimmungen haben den Schutz gutgläubiger Dritter zum Ziel, da sich unmündige oder entmündigte Personen nur mit Zustimmung ihres gesetzlichen Vertreters durch ihre Handlungen verpflichten können. Ist die Bevormundung wieder aufgehoben, so besteht für gutgläubige Dritte kein Schutzbedarf mehr. Aus dem im vorliegenden Fall überprüften Register ist eine Bevormundung aber auch noch nach Ende der Massnahme ersichtlich, was einen starken Eingriff in die Persönlichkeit der betroffenen Person darstellt, der in allfälligen Drittinteressen keinen Rechtfertigungsgrund findet. Zudem gehören administrative Sanktionen, wie sie die Bevormundung darstellt, zu den besonders schützenswerten Daten, deren Bekanntgabe an Dritte gemäss Art. 12 Abs. 2 lit. c DSG eine Persönlichkeitsverletzung darstellt.

Gerade das in den Werbeunterlagen des Registerbetreibers zitierte Beispiel eines Personalchefs, der auf diesem Weg herausfinden kann, dass ein Bewerber vor einer gewissen Zeit "vermutlich" aufgrund einer Verurteilung zu einer Freiheitsstrafe bevormundet wurde, zeigt nur zu deutlich, wie gross die Gefahr des Missbrauchs und von Persönlichkeitsverletzungen durch die systematische Erfassung und Bekanntgabe solcher Bevormundungsdaten ist. Der (zukünftige) Arbeitgeber darf nämlich gemäss Art. 328b OR Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrags erforderlich sind (siehe S. 44 ff.). Die Abklärung, ob ein Bewerber zu einer Freiheitsstrafe verurteilt wurde, ist also nur zulässig, wenn dies für die Eignung für das Arbeitsverhältnis wesentlich ist. Aber auch in diesem Fall darf der Arbeitgeber die Angaben nicht ohne Zustimmung des Bewerbers einholen, weshalb er allenfalls einen Auszug aus dem Strafregister zu verlangen hat. Dass die Möglichkeit, ohne Interessennachweis von einer Bevormundung zu erfahren, auch in anderen Fällen zu Persönlichkeitsverletzungen führen kann, ist offensichtlich.

Wir sind somit in allen drei Bereichen zum Schluss gekommen, dass die zentralisierte und systematische Erfassung der Daten in Personenregistern, um sie interessierten Personen auf Abfrage oder durch Meldung bekanntzugeben, durch die einschlägigen gesetzlichen Bestimmungen nicht abgedeckt ist, da diese Datenbearbeitungen grundsätzlich staatlichen Eingriffen vorbehalten sind. Deshalb sind die diesbezüglichen Datenbeschaffungen als unrechtmässig und die Bekanntgabe dieser Daten als Zweckentfremdung zu betrachten.
Aufgrund dieser Erwägungen haben wir dem Registerbertreiber empfohlen, die Bearbeitung von Daten über Todesfälle, Konkurs und Bevormundungen in Zukunft zu unterlassen.

5. Familienforschung (Genealogie)

Das Betreiben von Familienforschung (Genealogie) erfordert die Einsichtnahme in zahlreiche amtliche Dokumente bei den verschiedensten Behörden der Kantone und des Bundes. Ob und unter welchen Voraussetzungen eine solche Einsichtnahme zulässig ist, steht oft nicht fest. Seit Inkrafttreten des DSG haben Genealogen vermehrt Mühe, bei den zuständigen Behörden Einblick in die entsprechenden Register zu erhalten. Die Rechtslage ist unterschiedlich, je nachdem, ob in Zivilstandsregister oder andere öffentliche Register des Privatrechtsverkehrs oder in andere amtliche Dokumente Einblick gewünscht wird.

Nachforschungen in Zivilstandsregistern und anderen öffentlichen Registern des Privatrechtsverkehrs
Das DSG findet keine Anwendung auf öffentliche Register des Privatrechtsverkehrs (Art. 2 Abs. 2 lit. d DSG). Dazu gehören auch die Zivilstandsregister, die bei genealogischen Nachforschungen vor allem Verwendung finden. Auf diese kommt die Zivilstandsverordnung zur Anwendung. Diese hält fest, dass für Privatpersonen kein Anspruch auf Einsicht in die Zivilstandsregister besteht. In Ausnahmefällen kann die kantonale Aufsichtsbehörde Privatpersonen die Befugnis einräumen, in die Zivilstandsregister Einsicht zu nehmen, wenn sie das Verlangen nach Einsichtnahme als begründet erachtet. In vielen Kantonen wird Gesuchen um Einsichtnahme in die Zivilstandsregister zu genealogischen Forschungszwecken in der Regel stattgegeben, wobei damit häufig Auflagen verbunden sind. Es empfiehlt sich, ein schriftliches begründetes Gesuch an die Aufsichtsbehörde des Kantons zu richten, in dem Nachforschungen angestellt werden sollen. Verwandte in gerader

Linie sowie Personen, die ein unmittelbares, schutzwürdiges Interesse dartun, können einen Auszug aus den Registereintragungen verlangen. Werden Auskünfte über noch lebende Personen gebraucht, so verlangen am besten die betreffenden Personen selbst einen Auszug oder erteilen der nachforschenden Person eine Vollmacht, dies zu tun. Im übrigen wird im allgemeinen an Drittpersonen keine Auskunft über noch lebende Personen erteilt.

Leider ist die Rechtslage betreffend Nachforschungen zu genealogischen Zwecken in Zivilstandsregistern im Moment noch unbefriedigend, weil dieser Fall in der Zivilstandsverordnung nicht ausdrücklich geregelt ist und es somit den Kantonen überlassen bleibt, nach ihrem Ermessen die gewünschten Auskünfte zu erteilen. Es ist jedoch vorgesehen, in nächster Zeit diesen Fall in der Zivilstandsverordnung ausdrücklich zu regeln.

Nachforschungen in anderen amtlichen Dokumenten
In diesem Fall ist das DSG nur anwendbar auf Daten, die von Bundesorganen bekanntgegeben werden, während die Bekanntgabe von Personendaten durch kantonale Behörden dem kantonalen Datenschutzrecht untersteht. Die Rechtslage in den Kantonen ist unterschiedlich. Nicht alle Kantone verfügen über ein Datenschutzgesetz und die bestehenden Datenschutzgesetze unterscheiden sich zum Teil erheblich voneinander. Wiederum ist es ratsam, bei derjenigen Behörde, von der Informationen verlangt werden, ein schriftliches, begründetes Gesuch um Einsichtnahme zu stellen und sich von ihr über die Rechtslage aufklären zu lassen.

Bezüglich der Auskunfterteilung durch *Bundesorgane* gilt folgendes:

- Ist die betreffende Person verstorben, so sieht Art. 1 Abs. 7 VDSG vor, dass die Auskunft zu erteilen ist, wenn der Gesuchsteller ein Interesse an der Auskunft nachweist und keine überwiegenden Interessen von Angehörigen der verstorbenen Person oder von Dritten entgegenstehen. Ein Interesse wird namentlich durch nahe Verwandtschaft begründet. Gemäss dieser Bestimmung ist also im Normalfall (wenn nicht aus Rücksicht auf Angehörige ein Geheimhaltungsbedürfnis besteht) einem Auskunftsbegehren über verstorbene Verwandte zum Zweck der Familienforschung stattzugeben.
- Ist die betreffende Person nicht verstorben, so richtet sich die Datenbekanntgabe nach Art. 19 DSG (und allenfalls nach den Bestimmungen des Archivrechts). Gemäss dieser Bestimmung dürfen Bundesorgane Personendaten nur bekanntgeben, wenn dies in einer gesetzlichen Grundlage vorgesehen ist. Die Bekanntgabe von Daten lebender Personen zum Zweck der Familienforschung ist aber nirgends gesetzlich vorgesehen und deshalb nicht zulässig. Ausnahmsweise dürfen Bundesorgane auf Anfrage Name, Vorname, Adresse und Geburtsdatum einer Person auch ohne Bestehen einer gesetzlichen Grundlage bekanntgeben, sofern die allgemeinen Grundsätze des Datenschutzgesetzes dadurch nicht verletzt werden. Familienforschung kann eine solche Ausnahme begründen, jedoch kann dies nur aufgrund der Umstände des Einzelfalles abschliessend beurteilt werden. Auch in diesem Fall ist ein Gesuch an die zuständige Behörde zu richten.

6. Die 350 Reichsten und Einflussreichsten in der Schweiz

Die Publikation "Die 350 Reichsten und Einflussreichsten in der Schweiz" ist eine Sammlung von Personendaten, die an Dritte bekanntgegeben wird. Geschieht dies

ohne Kenntnis der betroffenen Personen, so muss die Datensammlung bei uns angemeldet werden.

Die Publikation umfasst Angaben über Name, Adresse, Beruf/Tätigkeit, Eigentum, Branche und Vermögen von 350 Personen. Über die meisten Personen enthält die Publikation zudem Kurzbiographien von ein bis zwei Seiten mit zusätzlichen Daten zur Ausbildung, geschäftlichen und anderen Aktivitäten, Beziehungen, Kontakten zu Kultur, Sport und Hobbies. Dabei werden die folgenden Macht- und Einfluss-Sphären kurz dargestellt: Eigentum, Beteiligungen, Politik/Militär, Verbände, Kultur/Sport, Beratung/Wissenschaft. Zwei Personen, die ohne ihr Wissen in dieser Publikation figurierten, baten uns um Intervention beim Herausgeber der Listen.
Private Personen dürfen besonders schützenswerte Personendaten oder Persönlichkeitsprofile nicht ohne Rechtfertigungsgrund an Dritte bekanntgeben. Unter einem Persönlichkeitsprofil ist eine Zusammenstellung einer grösseren Zahl von Daten über die Persönlichkeitsstruktur, die beruflichen Fähigkeiten und Aktivitäten oder auch ausserberuflichen Beziehungen und Tätigkeiten zu verstehen, die ein Gesamtbild oder ein wesentliches Teilbild der betreffenden Person ergibt. Durch das systematische Zusammenstellen der soeben aufgezählten Daten wird über die betroffenen Personen ein Teilbild erstellt.
In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat. Die in der Publikation enthaltenen Daten wurden der Öffentlichkeit von den Betroffenen nicht ausnahmslos zugänglich gemacht. Da kein überwiegendes öffentliches oder privates Interesse am Erstellen solcher Listen ersichtlich ist, kommt für die Datenbearbeitung kein anderer Rechtfertigungsgrund als die Einwilligung der Betroffenen in Frage. Daher sind neu aufzunehmende Personen vorher ausdrücklich zu informieren, damit sie in die Bearbeitung und Publikation ihrer Daten einwilligen könnten.
In einer Fussnote der Publikation wird jede Gewähr für die Richtigkeit der Angaben abgelehnt. Der Inhaber der Datensammlung hat jedoch die Pflicht, sich über deren Richtigkeit zu vergewissern.
Um seine Datensammlung nicht anmelden zu müssen, berief sich der Inhaber der Datensammlung auf Art. 10 DSG, der die Einschränkung der Auskunftspflicht für Medienschaffende regelt, mit der Anmeldung von Datensammlungen zur Registrierung aber nichts zu tun hat. Datensammlungen sind aber gemäss Art. 4 VDSG nicht anzumelden, wenn sie vom Inhaber ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums verwendet werden und wenn ihre Daten Dritten nicht bekanntgegeben werden, ohne dass die betroffenen Personen davon Kenntnis haben. Dies trifft im vorliegenden Fall jedoch nicht zu.
Hingegen sind private Personen, die regelmässig Persönlichkeitsprofile bearbeiten oder Personendaten an Dritte bekanntgeben verpflichtet, ihre Sammlungen bei uns anzumelden, sofern die betroffenen Personen davon keine Kenntnis haben. Damit die Anmeldungspflicht entfällt, muss den betroffenen Personen die Existenz der Datensammlung, deren Inhaber, eine allfällige Bearbeitung besonders schützenswerter Personendaten oder Persönlichkeitsprofile und eine allfällige Bekanntgabe an Dritte bekannt sein. Eine Anmeldung der Datensammlung würde sich im vorliegenden Fall erübrigen, sofern jeder betroffenen Person der Inhalt sowie allfällige Ergänzungen oder Änderungen des Kurzporträts mitgeteilt würden, und sie ihre ausdrückliche Zustimmung zur Weitergabe an Dritte zu geben hätte. Um seine Datensammlung nicht anmelden zu müssen, hat sich der Herausgeber der Publikation für diese Vorgehensweise entschieden.

7. Hotelmeldeschein

Wer in einem Hotel oder Gasthof übernachten will, muss in der Regel an der Rezeption einen Hotelmeldeschein ausfüllen. Dieser enthält Fragen über Name, Vorname, Beruf, Geburtsdatum, Nationalität, Zivilstand, Kinder und Passnummer, des öfteren aber auch über die verwendeten Verkehrsmittel, Herreiseort, Abreisedatum, Reiseziel usw.

Wir wurden von einer betroffenen Person angefragt, ob alle gestellten Fragen beantwortet werden müssten. Die Bearbeitung von Personendaten durch private Personen wie Hotels hat nach gewissen Grundsätzen zu erfolgen. Die Beschaffung der Daten muss rechtmässig sein, das heisst, sie muss auf einer gesetzlichen Norm beruhen oder durch Einwilligung der betroffenen Person oder ein überwiegendes öffentliches oder privates Interesse gerechtfertigt sein, sie darf nicht gegen Verbotsnormen verstossen und nicht mit unrechtmässigen Mitteln wie Täuschung oder Drohung erfolgen.

Die Beschaffung der aufgezählten Daten durch die Beherberger beruht zum Teil auf gesetzlichen Pflichten:

- So ist für Personen, welche Ausländer gegen Entgelt beherbergen, eine Meldepflicht im Bundesgesetz über Aufenthalt und Niederlassung der Ausländer und in dessen Vollzugsbestimmungen vorgesehen. Der Ausländer seinerseits ist verpflichtet, dem Beherberger zuhanden der Behörde die für die Meldung erforderlichen Angaben wahrheitsgetreu zu machen. Der Beherberger hat in Erfüllung seiner Meldepflicht für die Vollständigkeit und Richtigkeit der Angaben des Ausländers zu sorgen. Zudem ist er verpflichtet, dem Ausländer bei der Ankunft das Ausweispapier abzunehmen und es mit dem Meldezettel der Polizei vorzuweisen. Daraus ergibt sich die Pflicht der Hotels zur Verwendung von Systemen (Meldezettel oder andere), mit deren Hilfe sie die erforderlichen Angaben über ihre Gäste erfassen können. Zwar bezieht sich die in diesen Vorschriften geregelte Meldepflicht nur auf Ausländer. Damit die Hotels jedoch erkennen können, ob es sich um einen Ausländer handelt, benötigen sie die Angaben aller Gäste über den Namen, den Vornamen, die Wohnadresse und die Nationalität.
- Sodann erstellt das Bundesamt für Statistik gestützt auf das Bundesstatistikgesetz eine Hotelstatistik. Diese Statistik enthält monatliche Erhebungen über Ankünfte und Logiernächte der Gäste nach Wohnsitzländern. Das Bundesamt für Statistik ist ermächtigt, die Angaben der Meldepflichtigen notfalls an Ort und Stelle zu prüfen. Auch aus diesen Bestimmungen resultiert eine Pflicht der Beherberger, mit Hilfe eines Kontrollsystems, sei dies nun ein Gästebuch oder ein Meldescheinsystem, über die beherbergten Personen Buch zu führen.
- Schliesslich finden sich in kantonalen Erlassen im Zusammenhang mit dem Gastgewerbe Bestimmungen über die Meldepflicht der Beherberger. Ausserhalb der erwähnten gesetzlichen Bestimmungen steht die Gästekontrolle den Kantonen zu. Somit kann jeder Kanton selbständig festlegen, welche Angaben er von den Beherbergern erhebt.

Sodann kann die Datenerhebung durch ein überwiegendes Interesse des Gastgebers gerechtfertigt sein. Ein solches kommt insbesondere in Betracht, wenn die Daten in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages bearbeitet werden. Dies gilt sicher bei Angaben, die der Gastgeber benötigt, um den Gast, wenn er die Rechnung nicht bezahlt, belangen zu können. Die Bearbeitung von Personendaten muss zudem verhältnismässig sein. Das bedeutet, dass Daten nur in dem

Umfang beschafft werden dürfen, der für die Erfüllung von Pflichten und Aufgaben unbedingt erforderlich ist.

Soweit die Erhebung der Daten durch die Beherberger gesetzlich vorgesehen ist, sind diese berechtigt und verpflichtet, die geforderten Angaben zu verlangen, und der Gast ist verpflichtet, die entsprechenden Fragen vollständig und wahrheitsgetreu zu beantworten. Soweit die verlangten Angaben nicht gesetzlich vorgeschrieben sind, ist der Beherberger an den Grundsatz der Verhältnismässigkeit gebunden. Das bedeutet, er darf nur so viele Informationen verlangen, wie er für die Erfüllung seiner Pflicht zur Gästekontrolle benötigt. Damit der Gastgeber für den Fall, dass der Gast ihm gegenüber seinen Verpflichtungen nicht nachkommt, weiss, wo er ihn ausfindig machen kann, benötigt er zumindest die Angaben über Name, Vorname, Wohnadresse, Nationalität und das Geburtsdatum, da es vorkommt, dass verschiedene Personen denselben Namen haben.

Die Beantwortung der Frage, welche Angaben von den Gastgebern erhoben werden müssen und welche Angaben von den Gästen auszufüllen sind, richtet sich somit zum einen nach den eidgenössischen gesetzlichen Bestimmungen, zum anderen nach den kantonalen Bestimmungen über die Gästekontrolle. Für die Beurteilung, inwieweit die Datenerhebungen durch die Gastgeber aufgrund kantonaler Bestimmungen den datenschutzrechtlichen Grundsätzen entsprechen, sind die kantonalen Datenschutzkontrollorgane zuständig.

8. Parkplatz-Vignette

Viele Firmen und Bundesorgane bieten ihren Mitarbeitern die Möglichkeit, ihre Fahrzeuge auf firmeninternen oder angemieteten externen Parkplätzen abzustellen. Zu diesem Zweck erhalten die Mitarbeiter sogenannte Parkplatz-Vignetten, die als Karten hinter die Windschutzscheibe gelegt oder als Etiketten an die Windschutzscheibe geklebt werden müssen.

Diese Parkplatz-Vignetten sollen bei Kontrollen zeigen, dass der Inhaber des Fahrzeugs zur Benutzung eines bestimmten Parkplatzes berechtigt ist. In Verbindung mit dem Fahrzeug, an dem sie angebracht sind, werden diese Vignetten zu Personendaten, da aus ihnen ersichtlich ist, dass der Fahrzeughalter zur Nutzung des Parkplatzes berechtigt ist. Der Fahrzeughalter lässt sich ja aufgrund des Kontrollschildes leicht eruieren. Die aus der am Fahrzeug angebrachten Vignette ersichtlichen Angaben sind in der Regel jedermann zugänglich.

Wir haben überprüft, ob die Verwendung solcher Vignetten aus datenschutzrechtlicher Sicht zu Beanstandungen Anlass gibt. Insbesondere war zu prüfen, ob der Verhältnismässigkeitsgrundsatz eingehalten ist. Klebe-Vignetten sollen verhindern, dass Nichtberechtigte von Parkausweisen Gebrauch machen können, wie dies der Fall sein kann, wenn die Vignetten lediglich hinter die Windschutzscheibe zu legen sind. Die Verwendung von Klebe-Vignetten ist aus diesem Grund als verhältnismässig anzusehen. Andererseits bezieht sich der Verhältnismässigkeitsgrundsatz auch auf die bearbeiteten Daten und deren Inhalt. Es dürfen also nur die Daten bearbeitet werden, die zur Erreichung des verfolgten Zweckes erforderlich sind. Für die Kontrolle der parkierten Fahrzeuge ist es nicht erforderlich, dass sich auf der Vignette Angaben über den Arbeitgeber befinden, die allgemein verständlich sind. Bei einer Tätigkeit in einem heiklen Umfeld wie z.B. dem Kernenergiebereich, bei pornographischen Unternehmen, bei der Bundesanwaltschaft, in religiösen oder rassischen Einrichtungen können diese Angaben für den Halter des

Fahrzeuges zu Unannehmlichkeiten oder gar Problemen führen. Ein neutrales Signet oder aber eine Buchstaben/Ziffern-Kombination, die firmenintern und für die kontrollierende Person, nicht aber für Aussenstehende verständlich ist, reicht für die Erfüllung des Kontrollzweckes vollkommen aus.

Parkplatz-Vignetten sind somit aufgrund des Verhältnismässigkeitsgrundsatzes (und noch mehr bei privatrechtlichen Arbeitsverhältnissen aufgrund von Art. 328b OR, vgl. dazu die Ausführungen, S. 44) so zu gestalten, dass sie keine für Aussenstehende verständliche Angaben über den Arbeitgeber machen.

9. Erteilung von Auskünften über die Dauer der Arbeit von Taxifahrern

Eine Taxifahrtenzentrale muss der kantonalen Behörde, welche die Einhaltung der von Bund und Kantonen erlassenen Vorschriften bezüglich der Arbeits- und Ruhezeiten von berufsmässigen Fahrern zu überwachen hat, nur soweit die zur Erfüllung der Kontrollfunktionen dieser Behörde notwendigen Auskünfte erteilen, wie eine gesetzliche Bestimmung dies vorsieht.

Wir wurden von einem Kanton angefragt, inwieweit die Taxifahrtenzentralen gegenüber der zuständigen kantonalen Behörde die für Kontrolle der Einhaltung der von Bund und Kantonen erlassenen Vorschriften im Zusammenhang mit der Dauer der Arbeits- und Ruhezeiten der berufsmässigen Motorfahrzeugführer erforderlichen Angaben bekanntgeben müssen. In unserer Antwort haben wir folgendes hervorgehoben:
Die Bekanntgabe von Personendaten an eine kantonale Behörde durch eine Taxifahrtenzentrale untersteht dem Bundesgesetz über den Datenschutz dann, wenn diese Zentrale dem Privatrecht untersteht. Hingegen fallen Bearbeitungen von Personendaten durch kantonale Behörden im Rahmen der Anwendung von Vorschriften des Bundesrechts in den Kompetenzbereich der Kantone. Diese Behörden unterstehen dem Bundesgesetz über den Datenschutz nur, wenn sie beim Vollzug von Bundesrecht Daten bearbeiten und keinen kantonalen Datenschutzbestimmungen unterstehen. Deckt das Datenschutzgesetz eines Kantons beispielsweise nur automatisierte Bearbeitungen ab, so wäre er im Falle einer manuellen Datenbearbeitung dem Bundesrecht unterstellt.
Eine Taxifahrtenzentrale ist nur dann verpflichtet, den kantonalen Behörden Daten über die Taxifahrer und deren Arbeitgeber bekanntzugeben, wenn eine gesetzliche Vorschrift sie dazu zwingt. Sie kann die Auskünfte auch erteilen, wenn die Betroffenen ihre Einwilligung dazu gegeben haben oder wenn sie, im Einzelfall, einen anderen Rechtfertigungsgrund geltend machen kann (überwiegendes privates oder öffentliches Interesse). Die Bundesgesetzgebung über den Strassenverkehr und über die Arbeits- und Ruhezeit der berufsmässigen Motorfahrzeugführer regelt nur die Informationspflicht der Arbeitgeber und der Fahrer. Dasselbe gilt im vorliegenden Fall für die kantonale Gesetzgebung bezüglich der Taxiunternehmen. Insofern beruht die den Taxifahrtenzentralen auferlegte Verpflichtung zur Bekanntgabe von Personendaten auf keiner hinreichenden Gesetzesgrundlage. Aufgrund ihres systematischen und regelmässigen Charakters findet sie auch keine Rechtfertigung in einem überwiegenden öffentlichen oder privaten Interesse oder in einem anderen im Bundesgesetz über den Datenschutz vorgesehen Rechtfertigungsgrund.

10. Elektronische Ortung und Registrierung

Mit Hilfe der Informatik und insbesondere der Mikrochip-Technologie ist es heute möglich, Techniken zu entwickeln, mittels derer Fahrzeuge lokalisiert oder registriert werden können. Diese Techniken werden zum Beispiel eingesetzt, um gestohlene Fahrzeuge wiederzufinden oder um die Erhebung von Gebühren auf Autobahnen oder Alpenpässen zu erleichtern. Die Verwendung dieser Technologien darf nicht auf Kosten des Datenschutzes geschehen. Der Einsatz solcher Systeme muss auf klar definierte Zwecke beschränkt werden (z. B. Aufspürung eines gestohlenen Fahrzeugs, Entrichtung von Strassenbenutzungsgebühren). Die verwendeten Systeme müssen, soweit dies irgend möglich ist, die Anonymität der Verkehrsteilnehmer wahren. Schliesslich haben wir auch darauf aufmerksam gemacht, dass das multifunktionale Potential dieser Technologien gewisse Risiken in bezug auf die Wahrung der Grundrechte der Individuen beinhalten und zum Entstehen einer elektronisch überwachten Gesellschaft führen kann.

Informatik und Telematik halten immer stärkeren Einzug in die Verkehrsführung und in unsere Mobilität allgemein, sei dies, um den Verkehr zu überwachen, für einen stetigen Verkehrsfluss zu sorgen, die Warteschlangen an den Autobahngebührenschaltern zu vermindern, Fahrzeuge anzuhalten, deren Fahrer sich regelwidrig verhalten oder um verunfallte, verschwundene oder gestohlene Fahrzeuge ausfindig zu machen. Auch in der Schweiz treten diese Technologien zunehmend in Erscheinung. Wir wurden aufgefordert, uns zu zwei Systemen zu äussern, deren Einsatz gegenwärtig geprüft wird: die Verwendung eines Informatiksystems für die Gebührenerhebung an Alpenübergängen und der Einsatz von Mikrochips zum Aufspüren von gestohlenen Fahrzeugen.
Nach der Annahme der Alpeninitiative untersucht eine Arbeitsgruppe unter der Leitung des Bundesamtes für Polizeiwesen gegenwärtig die Einführung eines Systems zur Gebühreneintreibung auf Alpenpässen. Die Errichtung und der Betrieb von technischen Mitteln zur Gebührenerhebung unterstehen dem Bundesgesetz über den Datenschutz, soweit sie die Bearbeitung von Personendaten beinhalten. Die Bearbeitung muss sich demnach auf eine genügende gesetzliche Grundlage abstützen; ausserdem sind die allgemeinen Grundsätze der Datenbearbeitung zu beachten, insbesondere die Grundsätze der Verhältnismässigkeit und der Zweckgebundenheit. Es ist also auf ein System zurückzugreifen, das nicht nur die Gebührenerhebung unter Optimierung von Verkehrsfluss und Verkehrssicherheit gestattet und die Einhaltung von Raumplanungs- und Umweltschutzauflagen gewährleistet, sondern das darüber hinaus die Persönlichkeit und die Grundrechte der betroffenen Personen (Fahrzeuginhaber, Fahrzeugführer oder Mitfahrer) möglichst wenig beeinträchtigt. So wird beispielsweise die Prepaid-Karte (Vorauszahlungskarte), welche die Anonymität der Benutzer wahrt, gegenüber der Postpaid-Karten (Nachzahlungskarte), welche die Erhebung und Bearbeitung von Personendaten erfordert, vorzuziehen sein. Sollte dennoch ein System gewählt werden, bei dem die Zahlungen im nachhinein getätigt werden, so muss die Datensammlung einzig auf die für die Gebührenerhebung notwendigen Informationen beschränkt werden (also Identifizierung des Fahrzeugs, Ort, Datum und Zeitpunkt des Passierens, Name und Adresse des Fahrzeuginhabers oder der Person, welche die Gebühr zu entrichten hat, Gebührenbetrag). Die erhobenen Daten sind einzig und allein zu diesem Zweck zu verwenden und zu vernichten, sobald die Gebühr entrichtet worden ist. Die Einführung eines solchen Gebührenerhebungssystems könnte noch durch andere technische Massnahmen (Fotoapparat oder Videokamera) begleitet sein, um diejenigen Fahrzeuge zu registrieren, deren Fahrer ihrer Zahlungspflicht nicht nachgekommen sind. Auch diese Informationen dürfen nicht zu anderen Zwecken verwendet werden und es dürfen keine Informationen über

Personen, die ihre Zahlungspflicht erfüllt haben, gespeichert und aufbewahrt werden. Das System muss so konzipiert sein, dass es nicht unter Umgehung der Datenschutzbestimmungen verwendet werden kann.
Wir haben ein zweites System geprüft, welches erlaubt, gestohlene Fahrzeuge ausfindig zu machen und wiederzufinden sowie eine Fernüberwachung von Autos vorzunehmen. Dieses in Frankreich bereits eingeführte System könnte in der Schweiz noch in diesem Jahr auf den Markt kommen. Es umfasst insbesondere den Einbau ins Fahrzeug eines vorkodierten, praktisch nicht zu entdeckenden elektronischen Mikrochips. Dieser Mikrochip kann eine Verbindung zu einem automatisierten Informatiksystem herstellen. Sodann müssen im Strassennetz an strategischen Stellen (Kreuzungen, Ein- und Ausfahrten von Autowerkstätten oder Tankstellen, Autobahnauffahrten und -ausfahrten usw.) Erkennungspunkte eingerichtet werden. Das Erkennungssystem sollte sich nur einschalten, wenn ein Fahrzeug als gestohlen gemeldet wird. Sobald das Fahrzeug aufgespürt ist, werden die entsprechenden Informationen, nämlich Datum, Uhrzeit, Auffindungsort, vermutetes Fahrziel, Automarke, Modell, Typ, Farbe und Kennzeichen per Fax oder Telefon an die Polizei weitergeleitet, welche dann eingreifen und das Fahrzeug und den Dieb anhalten kann. Wird dieses System in der Schweiz eingeführt, so können die Geheimcodes und die Erkennungsmerkmale der als gestohlen gemeldeten Fahrzeuge auch an Unternehmen weitergeleitet werden, die ein solches System in anderen Ländern betreiben. Diese können die Informationen in ihr eigenes Aufklärungsnetz einspeisen. Die interessierten Personen schliessen mit der für die Betreibung des Systems verantwortlichen Gesellschaft einen Vertrag ab. Dies bedingt die Erhebung und Bearbeitung von Personendaten, wie Name, Vorname, vollständige Adresse, Fahrzeug (Marke, Modell, Kennzeichen, Seriennummer, Nummer der Versicherungspolice, Versicherungsgesellschaft), Zahlungsmodalitäten (Bankkonto, Scheck, Bargeld), Abbuchungsgenehmigung für die Erneuerung des Abonnements (Bankinstitut, Adresse, Kontonummer), Name des Automobilclubs, dem die betroffene Person eventuell angehört, und Name der Kraftfahrzeugversicherung.
Bei der Überprüfung des geplanten Systems haben wir festgestellt, dass dieses keine widerrechtliche Verletzung der Persönlichkeit der Betroffenen zur Folge hat, solange es auf vertraglicher Basis und nur zu dem Zweck der Aufspürung von gestohlenen oder mutmasslich gestohlenen Fahrzeugen (Fernüberwachung) eingesetzt wird und sofern einzig und allein die zur Auffindung des Fahrzeugs und zur Anhaltung des Diebes erforderlichen Daten gegebenenfalls an die Polizei weitergeleitet werden. Jedoch muss die Bearbeitung unter Wahrung der allgemeinen Datenbearbeitungsgrundsätze, insbesondere der Grundsätze der Verhältnismässigkeit, der Zweckbindung und der Datensicherheit erfolgen und hat die Rechte der betroffenen Personen zu wahren. Dies bedeutet namentlich:

- dass die Datenerhebung und -bearbeitung mit ausdrücklicher Einwilligung der betroffenen Person in Kenntnis der Bearbeitungsumstände durchgeführt wird. Die betroffene Person ist über die bearbeiteten Daten, den Zweck der Bearbeitung und das Bestehen von Datensammlungen, die zur Ausführung des Vertrags erforderlich sind, in Kenntnis zu setzen;
- dass nur Daten bearbeitet werden, die für den Vertragsabschluss und die Vertragsausführung benötigt werden. Dieser Datenkatalog ist im konkreten Fall verhältnismässig;
- dass die Daten nicht über den zur Ausführung des Vertrags nötigen Zeitraum hinaus aufbewahrt werden. So ist das Passieren von nicht gestohlenen oder nicht als gestohlen angesehenen Fahrzeugen (Fernüberwachung) nicht zu registrieren. Nach Ablauf des Vertrags und sobald die gesetzliche Aufbewahrungsfrist abgelaufen ist,

werden die Personendaten vernichtet und der Mikrochip wird ausser Kraft gesetzt und, wenn möglich, vom Fahrzeug entfernt;

- dass die Angaben über die gestohlenen Fahrzeuge an die Polizei nur im Interesse einer schnellen Auffindung der Fahrzeuge weitergeleitet und von dieser ausschliesslich zu diesem Zweck verwendet werden. Die betroffene Person wird bei Abschluss des Vertrags, spätestens aber bei Vorliegen eines Diebstahls über diese Bekanntgabe informiert. Bei der Fernüberwachung ist die betroffene Person zu benachrichtigen, wenn ihr Fahrzeug auf verdächtige Weise fortbewegt wird. So kann sie bei Vorliegen eines Irrtums das Verfahren stoppen. Sämtliche anderen Datenbearbeitungen und -bekanntgaben an die Polizei und andere Behörden wären nicht durch den Rechtfertigungsgrund (Ausführung des Vertrags) abgedeckt und würden einen unrechtmässigen Eingriff in den Persönlichkeit der betroffenen Personen darstellen. Eventuelle spätere Verwendungen durch die Behörden oder eine Verallgemeinerung des Systems in Form einer Pflicht müssten auf einer ausreichenden gesetzlichen Grundlage beruhen. Ausserdem müsste derartigen Schritten eine detaillierte Bedürfnisanalyse vorausgehen.

11. Name und Adresse von Fahrzeughaltern über die Nummer 111 und über Videotex

Die Bekanntgabe der Identität von Fahrzeughaltern durch den telefonischen Auskunftsdienst 111 und über Videotex verstösst nicht gegen die Bundesgesetzgebung über den Strassenverkehr, sofern nur eine Auskunft pro Anruf und pro Autokennzeichen erteilt wird und sich diese auf den Namen, den Vornamen und die Adresse des Fahrzeughalters beschränkt. Die bekanntgegebenen Informationen dürfen nur zu Zwecken im Zusammenhang mit dem Strassenverkehr verwendet werden. Die Fahrzeughalter müssen die Bekanntgabe und die Veröffentlichung ihrer Identität untersagen können.

Nicht jede Person, die ein Fahrzeug lenkt, ist für die anderen Strassenverkehrsteilnehmer ohne weiteres identifizierbar. Gemäss der bestehenden Strassenverkehrgesetzgebung muss das Fahrzeug aufgrund des Nummernschildes identifizierbar sein. Andere Fahrzeuginsassen als der Fahrzeughalter sind nicht verpflichtet, sich ohne begründeten Anlass auszuweisen. Auch muss die Identität eines Fahrzeughalters, der ein gesetzeskonformes Verkehrsverhalten an den Tag legt, nicht ermittelt werden. Nur bei Verkehrsstörungen, bei schweren Zwischenfällen und Unfällen stellt sich die Frage der Identifizierung. Selbst als Insasse eines Fahrzeugs, das sich auf öffentlichen Strassen bewegt, hat das Individuum ein Recht darauf, dass seine Privatsphäre unangetastet bleibt. Um zu verhindern, dass eine Datenbekanntgabe nur der Befriedigung der Neugier dient und dass die Daten zu gesetzeswidrigen Zwecken verwendet werden, insbesondere um dem Fahrzeuginhaber oder seinen Angehörigen zu schaden, sollte die Erteilung von Auskünften an den Nachweis eines Interesses gebunden werden (z. B. Verwicklung des Fahrzeughalters in einen Unfall, Verkehrsstörung, Gefahrenverursachung). Dies würde allerdings eine Gesetzesänderung voraussetzen.
Gemäss dem Bundesgesetz über den Strassenverkehr sind die Kantone zuständig für die Erhebung und Bearbeitung der Personendaten, die sich auf die Fahrzeughalter beziehen. Das Gesetz gibt ihnen auch das Recht, eine Liste der Fahrzeughalter zu veröffentlichen. Unabhängig vom Bestehen einer solchen Veröffentlichung geben die kantonalen Strassenverkehrsämter auf Wunsch telefonisch Auskunft über die Identität eines Fahrzeughalters. Aufgrund der Arbeitsüberlastung ihrer Mitglieder und um die Aktualität der

Verzeichnisse zu erhöhen, hat die Vereinigung der Strassenverkehrsämter seit dem letzten Jahr den PTT die Aufgabe übertragen, die gewünschten Auskünfte zu erteilen. Zu diesem Zweck erhalten die PTT von den Kantonen die Fahrzeugschildnummer und Name und Adresse des Fahrzeughalters. Die Auskünfte werden über die Nummer 111 und über Videotex erteilt. Der Entscheid, die Liste der Fahrzeughalter zu veröffentlichen oder auf die PTT zurückzugreifen, obliegt einzig und allein den Kantonen.
Die Veröffentlichung und die Bekanntgabe von Auskünften unterstehen der Bundesgesetzgebung über den Strassenverkehr und den kantonalen Datenschutzgesetzen. Soweit ein Kanton nicht kantonalen Datenschutzbestimmungen unterstellt ist, findet das Bundesgesetz über den Datenschutz Anwendung. Von seiten des Bundesamtes für Polizeiwesen, der Vereinigung der Strassenverkehrsämter und einigen Kantonen um eine Stellungnahme gebeten, haben wir einige Vorbehalte in bezug auf die Notwendigkeit und Zweckmässigkeit der Veröffentlichung von Verzeichnissen der Fahrzeughalter und in bezug auf deren Verbreitung über die Nummer 111 und über Videotex angemeldet. Wir haben betont, dass die gewünschte Information nur gestützt auf das Fahrzeugkennzeichen abgegeben werden darf und dass die einschlägigen Bestimmungen der Bundesgesetzgebung über den Strassenverkehr einzuhalten sind, welche die Bekanntgabe auf Namen, Vornamen und Adresse des Fahrzeughalters beschränken. Sodann darf eine Datenbekanntgabe nur im Einzelfall (eine Auskunft pro Anruf) und nicht systematisch und regelmässig stattfinden und muss die Zwecksetzung der Gesetzgebung über den Strassenverkehr respektieren.
Wir haben auch hervorgehoben, dass es ausgeschlossen ist, über die Nummer 111 oder über Videotex ganze Verzeichnisse abzugeben, andere Ermittlungskriterien als das Fahrzeugkennzeichen zu verwenden oder den Datenkatalog auf das Geburtsdatum, die Staatsangehörigkeit, den Heimatkanton oder Namen und Adresse der Haftpflichtversicherung des Fahrzeughalters auszudehnen.
Allerdings sind die für Strassenverkehrsfragen zuständigen Behörden laut Bundesgesetzgebung berechtigt, auf Anfrage hin die Identität des Versicherers preiszugeben, wenn die um Auskunft ersuchenden Personen in einen Unfall verwickelt sind oder wenn ein Wechsel des Fahrzeughalters vorliegt. Schliesslich dürfen andere, aus dem Führerausweis hervorgehende Informationen auf begründete schriftliche Anfrage hin an Personen abgegeben werden, die im Hinblick auf ein Gerichtsverfahren ein genügendes Interesse an der Bekanntgabe geltend machen können.
Da die Veröffentlichung und die Bekanntgabe von Daten zur Person des Fahrzeuginhabers nicht obligatorisch sind, muss sich dieser gegen die Bekanntgabe und/oder die Veröffentlichung zur Wehr setzen können. Das Sperrecht untersteht dem kantonalen Recht. Wir haben in bezug auf die Anwendung dieses Rechts grosse Unterschiede feststellen müssen. Einige Kantone weigern sich systematisch, die Daten zu sperren oder stellen sehr hohe Anforderungen, wohingegen andere Kantone die Ausübung dieses Rechts an keinerlei Bedingungen knüpfen. Es wäre zu wünschen, dass die Kantone nicht mehr Restriktionen auferlegen als es das Bundesgesetz über den Datenschutz tut und dass sie die Sperrung akzeptieren, sofern der Fahrzeughalter ein legitimes Interesse wahrscheinlich machen kann. Wenn also die Behörde nicht offensichtlich ausschliessen kann, dass die Datenbekanntgabe eine Verletzung der persönlichen Freiheit oder der Persönlichkeit der betroffenen Person nach sich zieht, muss der Einspruch gegenüber der Veröffentlichung oder der Bekanntgabe der Daten angenommen werden.

12. Archivierungssystem der Arbeitslosenkassen

In den letzten Jahren sind die Arbeitslosenkassen mit einem steigenden Arbeitsvolumen konfrontiert worden. Um die sich häufenden Papierdossiers rationell verwalten und vor allem archivieren zu können, haben die Arbeitslosenkassen der Westschweiz in Zusammenarbeit mit dem Bundesamt für Industrie, Gewerbe und Arbeit (BIGA) einen Pilotversuch zur Mikroverfilmung der Dossiers gestartet. Wir haben die Massnahmen geprüft, die für eine datenschutzkonforme Durchführung dieses Versuchs erforderlich sind.

Um den kantonalen Arbeitslosenkassen eine rationelle Verwaltung des beträchtlichen Volumens an archivierten Dossiers zu ermöglichen, hat das BIGA der Gründung eines Mikroverfilmungszentrums zugestimmt. Dieses wird in das Ausbildungszentrum der Arbeitslosenkassen der Westschweiz in La Chaux-de-Fonds integriert. In einer ersten Phase wird ein Pilotversuch laufen, der die Mikroverfilmung der Dossiers aller Arbeitslosenkassen der Westschweiz abdeckt. In einer zweiten Phase soll das Zentrum die archivierten Dossiers aller schweizerischen Arbeitslosenkassen übernehmen können.

Bei diesem Rationalisierungsprozess werden Personendaten bearbeitet, indem sie archiviert und verfilmt werden. Daten über Arbeitslose sind als Massnahmen der sozialen Hilfe gemäss Art. 3 lit. c Ziff. 4 DSG besonders schützenswerte Personendaten. Eine unrechtmässige Bearbeitung dieser Daten würde die Persönlichkeit der betroffenen Personen schwerwiegend gefährden. Das BIGA hat uns gebeten zu prüfen, welche Voraussetzungen erfüllt sein müssen, damit eine datenschutzkonforme Bearbeitung dieser Daten erfolgen kann. Aufgrund einiger Sitzungen haben wir dem BIGA empfohlen, die für die Bearbeitung dieser Daten erforderlichen Rechtsgrundlagen zu schaffen und zu entscheiden, welche technisch-organisatorischen Massnahmen für den Schutz der Daten notwendig sind.

13. Mehrwertsteuer und Berufsgeheimnis

Zwei parlamentarische Interpellationen im Zusammenhang mit der Frage, ob Anwälte dazu verpflichtet seien, die Identität ihrer im Ausland ansässigen Mandanten preiszugeben, um von der Entrichtung der Mehrwertsteuer befreit zu werden, gaben uns Anlass zu einer Stellungnahme. Wir kamen zum Schluss, dass ein Anwalt nur dann die von den Steuerbehörden gewünschten Auskünfte erteilen müsste, wenn seine Mandanten dazu ihre Zustimmung erteilt haben und wenn der Anspruch auf eine Steuerbefreiung nicht auf anderem Wege nachgewiesen werden kann.

Die Gesetzgebung zur Mehrwertsteuer sieht eine Steuerbefreiung für die im Ausland ausgeführten Dienstleistungen vor. Dies betrifft insbesondere die Anwälte, deren Mandanten im Ausland ansässig sind oder dort ihren Firmensitz haben, sofern die erbrachten Dienstleistungen ausschliesslich im Ausland genutzt werden. Um eine Steuerbefreiung beanspruchen zu können, muss der Anwalt seinen Anspruch nachweisen, indem er Buchhaltungsunterlagen und Belege vorlegt. Die Steuerbefreiung kommt sowohl dem Anwalt zugute, der die Dienstleistung erbringt, als auch dem Mandanten, der keine Mehrwertsteuer zu entrichten hat. Der Anwalt muss ausserdem der Steuerbehörde Informationen über den Mandanten bekanntgeben, namentlich dessen Namen und Adresse. In Hinblick auf die Beantwortung zweier parlamentarischer Interpellationen, in denen die Frage aufgeworfen wurde, inwieweit diese Auskunftspflicht der Anwälte mit deren Berufsgeheimnis zu vereinbaren sei, wurden wir um Stellungnahme gebeten.

Wir haben uns folgendermassen geäussert:

Die Bundesgesetzgebung über die Mehrwertsteuer verpflichtet alle Steuerpflichtigen, die Behörden über sämtliche Umstände zu unterrichten, die für die Feststellung der Steuerpflicht oder für die Steuerberechnung von Bedeutung sein könnten. Ebenso sieht sie eine Verpflichtung zur Aufbewahrung bestimmter Unterlagen vor, anhand derer über die Steuerpflicht oder Steuerbefreiung entschieden werden kann. Die Gesetzgebung spricht der Steuerverwaltung eine Kontrollkompetenz zu und ermächtigt sie, Auskünfte bei Dritten einzuholen, insbesondere bei Personen, denen gegenüber eine Dienstleistung erbracht wurde oder die eine solche erbracht haben. Sie enthält jedoch keine Präzisierungen zur Frage, welche Daten über Dritte erhoben werden dürfen. Das Berufsgeheimnis bleibt gewährleistet. Diese Gewährleistung gilt für den Anwalt, der Name und Adresse seines Mandanten angeben soll, welcher der wahre Nutzniesser der Steuerbefreiung ist.
Die Pflicht zur Bekanntgabe von Name und Adresse einer Person, für die eine steuerbefreite Leistung erbracht wurde, beinhaltet eine Bearbeitung von Personendaten durch ein Bundesorgan. Diese untersteht dem Datenschutzgesetz und muss somit insbesondere auf einer gesetzlichen Grundlage beruhen und die allgemeinen Bearbeitungsgrundsätze beachten. Im vorliegenden Fall besteht zwar eine gesetzliche Grundlage, aber die Verordnung zur Mehrwertsteuer reicht für die Aufhebung des durch ein Gesetz im formellen Sinne geschützten Berufsgeheimnisses nicht aus. Die Bekanntgabe der verlangten Angaben durch den Anwalt darf demnach nur mit Einwilligung der betroffenen Person stattfinden. Bevor eine solche Auskunftspflicht verallgemeinert wird, muss zunächst geprüft werden, ob Name und Adresse des Dienstleistungsempfängers im Ausland für den Anspruchsnachweis im Zusammenhang mit der Steuerbefreiung überhaupt notwendig sind, oder ob es ausreichen würde, diese Angaben nur in Zweifelsfällen oder anlässlich einer Kontrolle zu verlangen. Wenn der Anwalt in der Lage ist, den Anspruch auf eine Steuerbefreiung nachzuweisen, ohne Personendaten bekanntzugeben, muss die Auskunftsverpflichtung entfallen. Wenn der Anwalt aufgefordert wird, Auskünfte zu erteilen, sein Mandant aber die Einwilligung dazu nicht erteilt, muss er diesen über die möglichen Konsequenzen seiner Weigerung in Kenntnis setzen, nämlich, dass er damit das Risiko eingeht, die Steuer entrichten zu müssen.

14. Spielbanken - provisorischer Vorentwurf zu einem Bundesgesetz

Das Eidgenössische Justiz- und Polizeidepartement hat eine Expertenkommission "Spielbankengesetz" eingesetzt. Das Bundesamt für Polizeiwesen war mit der Ausarbeitung eines Vorentwurfs zu einem Bundesgesetz über die Spielbanken betraut, welcher der Expertenkommission bei ihren Verhandlungen als Arbeitsgrundlage dienen sollte. Es legte uns im September 1994 ein provisorisches Papier vor und bat uns, dieses vor Eröffnung des offiziellen Vernehmlassungsverfahrens einer summarischen Überprüfung hinsichtlich seiner Vereinbarkeit mit den Anforderungen des Datenschutzes zu unterziehen.

Im Rahmen unserer Stellungnahme haben wir die Experten darauf aufmerksam gemacht, dass bei der Einführung der Gesetzgebung über die Spielbanken ganz allgemein darauf zu achten ist, dass die Grundsätze des Bundesgesetzes über den Datenschutz gewahrt werden. In diesem Stadium, wo nur ein provisorischer Vorentwurf vorlag, war es für uns allerdings äusserst schwierig abzuschätzen, ob diese Grundsätze - insbesondere der Grundsatz der Verhältnismässigkeit - berücksichtigt worden sind. Zu diesem Zeitpunkt war noch kein Kommentar oder Begleitbericht vorhanden, der die Führung der für die Verwaltung der Spielbanken, wie das Personenregister zur Identifizierung der Spieler, das Personenregister über den Ausschluss von Personen, denen das Spielen verboten wurde (Register über die Spielersperre) und das Personenregister über die Transaktionen hätte

erläutern und rechtfertigen können. Wir haben ausserdem darauf hingewiesen, dass auch in bezug auf den Inhalt dieser Register der Grundsatz der Verhältnismässigkeit gewahrt werden muss, um sicherzustellen, dass nur die wirklich zweckdienlichen Personendaten erhoben und gespeichert werden.

Um die Expertenkommission auf einige aus datenschutzrechtlicher Sicht problematische Punkte aufmerksam zu machen, haben wir darüber hinaus verschiedene Bemerkungen zu einigen Bestimmungen des provisorischen Vorentwurfs angebracht. So haben wir insbesondere darauf hingewiesen, dass in bezug auf die Daten zur Identität der Spieler (Personalien) und in bezug auf deren Aufbewahrungsdauer Präzisierungen anzubringen sind. Zusätzlich haben wir empfohlen, die Meldepflicht gegenüber den Strafverfolgungsbehörden und dem Bundesamt für Polizeiwesen mit einer Bestimmung zu verbinden, die es dem Geschäftsführer einer Spielbank untersagt, den Verdacht gegen einen Spieler, den er den Aufsichtsbehörden bereits gemeldet hat, zu speichern.
Wir haben ausserdem betont, dass die betroffene Person ihr Auskunftsrecht in bezug auf die Gesamtheit der zu ihrer Person von seiten des Spielbankenbetreibers erfassten Daten geltend machen kann und dass die Ausübung dieses Rechts im Prinzip kostenlos erfolgt. Die Ausnahmen vom Grundsatz der Kostenlosigkeit sind in der Verordnung zum Bundesgesetz über den Datenschutz aufgeführt. Was die Bekämpfung der Verschuldung anbelangt, so muss die diesbezügliche Bestimmung ergänzt werden, um die Einleitung von Ermittlungen oder eine zu weit gehende Datenerhebung durch die Spielbankenbetreiber im Rahmen der Ausführung dieser Bestimmung mit dem Charakter einer sozialen Massnahme zu verhindern oder zu verbieten. Wir haben ausserdem nahegelegt, die Frage der Bekanntgabe von Spielverboten (Spielersperren) an sämtliche anderen Spielbanken der Schweiz unter den Gesichtspunkten der Zweckmässigkeit und der Verhältnismässigkeit zu prüfen. Eine diesbezügliche Regelung müsste das Bekanntgabeverfahren und eine regelmässige Aktualisierung für den Fall der Aufhebung des Verbots vorsehen.
Wir haben die Experten aufgefordert, unseren Bemerkungen die gebührende Aufmerksamkeit zu schenken, wobei auch der Tatsache Rechnung zu tragen ist, dass unsere Bemerkungen nur auf einer summarischen Prüfung des provisorischen Vorentwurfs basieren. Anlässlich der Ämterkonsultation und sobald der Begleitbericht mit der Kommentierung jeder einzelnen Bestimmung vorliegt müssen bestimmte Bemerkungen noch vertieft oder eventuell überarbeitet werden, und zwar in erster Linie unter dem Blickwinkel des Grundsatzes der Verhältnismässigkeit.
Die Schlussfassung des Vorentwurfs für ein Bundesgesetz über die Spielbanken wurde uns im Rahmen der Ende Januar 1995 eröffneten Ämterkonsultation zugestellt. Wir sind im Hinblick auf eine eventuelle ergänzende Stellungnahme gegenwärtig dabei, diesen Gesetzesentwurf einer erneuten Prüfung zu unterziehen.

15. Anwendbarkeit des Bundesgesetzes über den Datenschutz

Der Dritte, welcher für ein privates Unternehmen oder ein Bundesorgan Personendaten bearbeitet, ist dem Bundesgesetz über den Datenschutz unterworfen.

Eine Dienstleistungsgesellschaft, deren Sitz sich in der Schweiz befindet, bearbeitet für Rechnung von Handels- und Industrieunternehmungen Daten aus der Personal- und Lohnverwaltung dieser Unternehmungen. Die Datenbearbeitung erfolgt zu einem grossen Teil bei einem in Frankreich ansässigen Rechenzentrum. Die Gesellschaft handelt als Beauftragte und ist nicht im Besitz der Personaldatensammlungen ihrer Auftraggeber. Auf

die Frage, ob diese Gesellschaft dennoch den Bestimmungen des Bundesgesetzes über den Datenschutz unterstehe, haben wir folgendes geantwortet:

Jede natürliche oder juristische Person, die in der Schweiz Personendaten bearbeitet, ist den Pflichten, die sich aus dem Bundesgesetz über den Datenschutz ergeben unterworfen, ungeachtet dessen, ob sie als Inhaberin einer Datensammlung, als Beauftragte oder in einer anderen Funktion handelt. Das Gesetz präzisiert insbesondere, dass eine Person, die einen Dritten mit der Bearbeitung von Personendaten beauftragt, dafür zu sorgen hat, dass sich dieser Dritte ebenso an die Vorschriften des Datenschutzes hält, wie sie selbst dies tun müsste. Dies betrifft alle Arten der Bearbeitung, von der Datenbeschaffung bis zur Datenbekanntgabe, aber auch ihre Aufbewahrung und Vernichtung. Der Beauftragte kann dieselben Rechtfertigungsgründe geltend machen wie der Auftraggeber.
Sofern dies nicht ausdrücklich in einer Gesetzes- oder Vertragsbestimmung vorgesehen ist, wird vom Beauftragten allerdings nicht verlangt, dass er allenfalls bestehende Pflichten des Inhabers der Datensammlung zur Anmeldung von Datensammlungen und von Datenbekanntgaben ins Ausland erfüllt. Macht eine betroffene Person ihr Auskunftsrecht geltend und wendet sie sich zu diesem Zweck an den Auftragnehmer, so muss dieser die erwünschten Auskünfte nur erteilen, wenn er die Identität des Inhabers der Datensammlung nicht preisgibt oder wenn letzterer keinen Wohnsitz in der Schweiz hat. Die betroffene Person, die sich in ihrer Persönlichkeit beeinträchtigt fühlt, kann nicht nur den Inhaber der Datensammlung, sondern auch die mit der Datenbearbeitung beauftragte Person gerichtlich belangen.

16. Die Umsetzung von Datensicherheitsmassnahmen in der Bundesverwaltung

Die uns zugestellten Projektunterlagen sind in vielen Fällen unvollständig. Häufig werden die Prozesse (Ablauforganisation) und die Konfiguration der Informatikmittel nicht oder nur unvollständig aufgeführt oder die Datensicherungsmassnahmen sind nicht genügend umschrieben.

Die Erfahrungen bei der Umsetzung der technischen und organisatorischen Massnahmen des Datenschutzes sind sehr unterschiedlich. Während gewisse Organisationseinheiten die Anliegen des Datenschutzes sehr ernst nehmen, ändern andere die Systeme oder entwickeln sogar neue ohne angemessene Berücksichtigung der Rahmenbedingungen. Bei der Neuentwicklung sowie bei der Änderung von Systemen sind die Anliegen des Datenschutzes sogleich zu berücksichtigen und umzusetzen. Die fünfjährige Übergangsfrist (bis 1. Juli 1998) für die Umsetzung der technischen und organisatorischen Massnahmen gilt nur für Systeme, die am 1. Juli 1993 bereits bestanden und an denen keine "grösseren" Änderungen vorgenommen werden.
Technische Vorkehren zum Schutz von Personendaten sind zum Teil mit besonderem Aufwand verbunden. Man darf den Aufwand für die Umsetzung der Datenschutzanliegen insbesondere dann nicht unterschätzen, wenn in der Vergangenheit organisatorische Gesichtspunkte sowie Aspekte der Datensicherheit generell nicht angemessen berücksichtigt wurden. Wichtig ist, dass die Prozesse dokumentiert werden (Ablaufdiagramme) und dass der Organisationsaufbau definiert wird (wer ist für welche Aufgabenerfüllung zuständig?). Diese Forderungen des Datenschutzes sind nicht neu, sondern werden z. B. auch in Hinblick auf die Qualitätssicherung oder aus der Sicht der Organisation gefordert. Die erforderlichen Datensicherungsmassnahmen sind je nach System von unterschiedlicher Komplexität. Die Umsetzung dieser Massnahmen sollte deshalb immer so rasch wie möglich in Angriff genommen werden. Der Entscheid über die notwendigen Datensicherungsvorkehrungen

bedingt einen Überblick über das Gesamtsystem. Dazu muss die Konfiguration der Informatikmittel aufgeführt werden, soweit sie für den Datenschutz oder die Datensicherheit relevant sind. Erst aufgrund dieser Unterlagen kann festgestellt werden, welche Sicherheitsvorkehrungen vorzunehmen sind und ob damit die Risiken angemessen abgedeckt werden können.

Verantwortlich für den Datenschutz und damit auch für die Datensicherheit ist der Inhaber der Datensammlung. Diesem ist es oft nicht möglich, sich mit Informatik, Betriebswirtschaft (Organisation) und Recht, eingehend zu befassen, um beurteilen zu können, welche Massnahmen erforderlich sind. Er ist deshalb auf Beratung durch die Datenschutzberater und die Sicherheitsbeauftragten der Departemente oder Ämter (soweit vorhanden) sowie auf die Sektion Sicherheit des Bundesamtes für Informatik angewiesen. Diese müssen den Inhaber der Datensammlung über die möglichen Massnahmen und ihre Wirkungen und die dafür notwendigen Ressourcen informieren, damit er in der Lage ist, eine angemessene Lösung für das jeweilige System auszuwählen. Angemessen muss die Lösung insbesondere in Bezug auf den Schutz des Betroffenen sein. Die Kosten sind erst in zweiter Linie angesprochen. Der Inhaber der Datensammlung entscheidet über die Angemessenheit und trägt die Verantwortung für den Datenschutz. Einzelheiten zu den möglichen Massnahmen finden sich im *Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes*, der bei unserem Sekretariat kostenlos erhältlich ist. Werden die Anforderungen des Datenschutzes in technischer und organisatorischer Hinsicht zu wenig berücksichtigt, so kann dies eine Empfehlung des Eidgenössischen Datenschutzbeauftragten zur Folge haben. Es bleibt zu hoffen, dass bei der Neuentwicklung und Änderung von Systemen, durch die Personendaten bearbeitet werden, die Anliegen des Datenschutzes vermehrt berücksichtigt werden.

17. Unzulässige Datebekanntgabe an Dritte durch ein Bundesorgan

Gibt ein Bundesorgan unberechtigterweise Daten an Dritte weiter, so können Personen, die dadurch in ihrer Persönlichkeit verletzt werden, vom betreffenden Bundesorgan verlangen, es sei die Widerrechtlichkeit der Bearbeitung festzustellen. Ein negativer Entscheid des betreffenden Bundesorgans kann an die Eidgenössische Datenschutzkommission weitergezogen werden.

Im vorliegenden Fall hatten sich mehr als zwanzig Privatpersonen zusammengeschlossen, um gemeinsam ein Unternehmen zu gründen. Um einem Antrag im Zusammenhang mit der Unternehmensgründung an das zuständige Bundesorgan mehr Nachdruck zu verleihen, wurde ihm eine Liste mit den Unterschriften aller Beteiligten vorgelegt. Beim betreffenden Bundesorgan lagen bereits mehrere ähnliche Anträge von anderen Personen vor. Darunter befand sich auch ein Antrag des Arbeitgebers einer der an der erwähnten Unternehmensgründung beteiligten Privatpersonen. Diesem wurde "im Interesse einer besseren Koordination" die ganze Unterschriftenliste bekanntgegeben. Dies obwohl auf der Unterschriftenliste ihre Bekanntgabe an Dritte ausdrücklich untersagt war. Die beim betreffenden Arbeitgeber angestellte Person verlor daraufhin die Arbeitsstelle. Sie wandte sich mit der Bitte um Beratung an uns.

Grundsätzlich dürfen Bundesorgane Personendaten bekanntgeben, wenn dafür Rechtsgrundlagen im Sinne von Art. 17 DSG bestehen oder wenn die betroffene Person ihre Daten allgemein zugänglich gemacht hat (Art. 19 Abs. 1 lit. c DSG). Im vorliegenden Fall bestand keine Rechtsgrundlage, die eine Weitergabe von Personendaten an Dritte vorsah. Da die betroffenen Personen zudem die Bekanntgabe ihrer Daten an Dritte ausdrücklich

untersagt hatten, war die Bekanntgabe unzulässig und stellte eine widerrechtliche Datenbearbeitung dar. Wir haben das Bundesorgan aufgefordert, derartige Datenbekanntgaben in Zukunft zu unterlassen.
Die betroffene Person kann ihrerseits vom Bundesorgan verlangen, es sei die Widerrechtlichkeit der Datenbearbeitung festzustellen. Ist ein Schaden entstanden, so muss die betroffene Person diesen innert einem Jahr seit Kenntnis ebenfalls geltend machen und beweisen.
Bestreitet das Bundesorgan die Widerrechtlichkeit, so kann die Eidgenössische Datenschutzkommission angerufen werden. Deren Entscheid kann mittels Verwaltungsgerichtsbeschwerde an das Bundesgericht weitergezogen werden.

18. Aushebung von Rekruten - medizinischer Fragebogen

Vor der Aushebung müssen alle Auszuhebenden einen medizinischen Fragebogen ausfüllen. Er enthält nicht nur Fragen zur Gesundheit der betreffenden Person selbst, sondern auch über ihre Angehörigen. Im Rahmen der Armeereform 95 ist zu prüfen, inwieweit all diese Fragen heutzutage noch notwendig und zweckmässig sind.

Der Vater eines Auszuhebenden hat sich in dieser Sache an uns gewandt. Er wollte wissen, ob sämtliche Fragen über die Eltern, die Geschwister und über den Auszuhebenden selbst tatsächlich notwendig sind. Der Fragebogen enthält unter anderem Fragen über deren Geburtsjahr, Krankheiten, Todesursachen und Todesjahr von Eltern und Geschwistern und die Frage nach dem Beruf des Vaters. Gefragt wird auch, wo der Auszuhebende aufgewachsen ist. Der medizinische Fragebogen wird vom Bundesamt für Sanität bei der Aushebung der Rekruten verwendet. Er dient vor allem der Rationalisierung des Verfahrens, da er eine systematische Befragung jedes Einzelnen erspart. Aufgrund der Vorgeschichte, der mitgebrachten medizinischen Dokumentation und der medizinischen Untersuchungsergebnisse soll festgestellt werden, ob die Auszuhebenden für den Militärdienst tauglich sind. Eine gesetzliche Grundlage für die Datenerhebung besteht bis heute nicht. Nach der Aushebung stehen die erhobenen Daten nur den Militärärzten und der Militärversicherung zur Verfügung. Die Daten werden nicht systematisch ausgewertet.

Im Zusammenhang mit der Armeereform 95 ist anlässlich der Revision der Vorschriften und Formulare auch eine Überarbeitung des medizinischen Fragebogens vorgesehen. Dabei wird zu prüfen sein, welche dieser Angaben heute noch zweck- und verhältnismässig sind und ob zum Teil darauf verzichtet werden könnte. Zudem wird eine gesetzliche Grundlage für die Datenerhebung zu schaffen sein.

19. Datenschutz im Bereich des Steuerrechts und Grundbuchs

Auch wenn die Kantone dezentrale Datenbanken führen, dürften sich übergreifende Datenschutz- und Datensicherheitskonzepte in zunehmendem Mass als sinnvoll erweisen. Bei der revidierten Grundbuchverordnung wurde diese Zielsetzung gut erkannt.

Sowohl im Bereich des Steuerrechts als auch des Grundbuchrechts verhält es sich so, dass die (auch) zur Erfüllung von Bundesaufgaben beschafften Daten dezentral von den Kantonen bearbeitet werden. Diese setzen hierbei in zunehmendem Mass EDV-Mittel ein, wozu sie für das Grundbuch durch das revidierte Zivilgesetzbuch und die revidierte

Grundbuchverordnung ausdrücklich ermächtigt werden. Soweit ersichtlich, bestehen vergleichbare Vorschriften im Bereich des Steuerrechts (noch) nicht.

Die Herausforderung dieser Entwicklung besteht darin, eingebettet in die kantonale Vollzugssouveränität datenschutzkompatible Lösungen beim Einsatz von EDV zu wählen, welche den vielfältigen Anforderungen der beteiligten Verwaltungsstellen und weiterer Benützer der in Frage stehenden Datensammlungen auf der einen Seite und dem Persönlichkeitsschutz oder allfälligen berechtigten Geheimhaltungsinteressen der Betroffenen auf der anderen Seite gerecht werden. Von Interesse ist in diesem Zusammenhang speziell das Kapitel der Grundbuchverordnung über das EDV-Grundbuch mit seinen Vorschriften über die Datensicherheit und die Pflicht, Sicherheitskonzepte aufzustellen und einer externen Vorprüfung zu unterziehen sowie über die Zugriffe mittels Abrufverfahren und deren Umfang. Diese oder ähnliche Bestimmungen könnten sich auch für den Bereich des Steuerrechts als sinnvoll erweisen.

III. INTERNATIONALES

1. Internationale Konferenz der Beauftragten für den Datenschutz

Die Instanzen, welche die Aufgabe haben, über die Einhaltung der nationalen Datenschutzbestimmungen zu wachen, haben eine internationale Konferenz ins Leben gerufen, die einmal jährlich auf Einladung eines der Mitgliedstaaten stattfindet. Ziel dieser Konferenz ist es, den Austausch von Informationen unter den Aufsichtsbehörden zu ermöglichen, die Praxis zu festigen und zu harmonisieren und gegebenenfalls gemeinsame Positionen festzulegen und diese in Form von Erklärungen oder Resolutionen abzugeben. Die Konferenz ist teilweise öffentlich und richtet sich an die Vertreter der für die Anwendung der Datenschutzbestimmungen zuständigen Kreise.

Die XVI. Internationale Konferenz der Datenschutzbeauftragten fand vom 6. bis am 8. September 1994 auf Einladung des niederländischen Datenschutzbeauftragten in Den Haag statt. Die Konferenz stand im Zeichen der neuen Informationstechnologien und gab Anlass zur Untersuchung der Frage, welche Vorteile die im privaten Bereich verwendeten Technologien mit sich bringen. Die Konferenz, an der Vertreter aus allen Teilen der Welt teilnahmen, ermöglichte auch eine Standortbestimmung zur internationalen Entwicklung im Bereich des Datenschutzes. Ausserdem fand ein grundlegender Meinungsaustausch über Datenbearbeitungen im Finanz- und und Kreditwürdigkeitsprüfungsbereich statt (Verwendung der Punktzahltechnik, mit Hilfe derer Persönlichkeitsprofile durch Anreicherungen und Abgleichungen von Datensammlungen erstellt und als Entscheidhilfen verwendet werden können). Weitere Themen waren der Gesundheitsbereich und die Entwicklung neuer Informationstechnologien (Multimedia, Datenautobahnen, Internet, Chip-Karten vor allem im Verkehr und im Gesundheitswesen), die keine Grenzen kennen und neue Herausforderungen für den Schutz der Persönlichkeit und der Grundrechte darstellen. In Anbetracht dieser Gegebenheiten kam man zu dem Schluss, dass es notwendig ist, Technologien zu fördern, die den Datenschutz gewährleisten können, wie die Verwendung von Chiffrierungstechniken, Technologien, welche die Wahrung der Anonymität sicherstellen (Karten zur Vorauszahlung) oder den Datenzugriff auf bestimmte Personen und bestimmte Zwecke beschränken. Die Datenschutzbeauftragten haben ausserdem auf die Notwendigkeit hingewiesen, die internationale Zusammenarbeit zu stärken und den Datenschutz besser

bekannt zu machen, insbesondere durch eine verstärkte Informationspolitik zugunsten des Bürgers.
In Ergänzung der einmal jährlich stattfindenden Konferenz arbeiten die Datenschutzbeauftragten unter sich zusammen, zum einen durch bilaterale Kontakte (Informationsaustausch) und zum anderen durch die Bildung von Arbeitsgruppen, in denen man sich mit bestimmten Fragestellungen auseinandersetzt. So wurde zum Beispiel die Arbeitsgruppe Berlin eingerichtet, die zweimal pro Jahr zusammentrifft, um Datenschutzprobleme im Bereich der Telekommunikation und der Medien zu untersuchen. Diese Gruppe befasst sich gegenwärtig mit dem Internet, über welches Personendaten ohne grosse Schwierigkeiten in die ganze Welt verbreitet werden können. Dieses Netz wirft aufgrund des Fehlens genügender gesetzlicher Bestimmungen sowie einer speziellen Aufsichtsinstanz schwerwiegende Datenschutzprobleme auf. Die Arbeitsgruppe analysiert ausserdem Fragestellungen im Zusammenhang mit der Verwendung der Telekommunikation in Arbeitsverhältnissen, Telefonkarten, elektronischen Telefonbüchern und der elektronischen Überwachung von Häftlingen. Letztere stellt eine Alternative zum Gefängnis dar und gibt die Möglichkeit, die Bewegungen der straffällig gewordenen Person zu verfolgen und ihre Tätigkeiten und Fortbewegungen zu begrenzen.

2. Europarat

Die internationale Tätigkeit des Eidgenössischen Datenschutzbeauftragten konzentriert sich zu einem grossen Teil auf die Verfolgung der Arbeiten des Europarats. Der Europarat spielt bei der Entwicklung des Datenschutzrechts in Europa eine zentrale Rolle. Die Europaratskonvention zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108) wurde bereits von 16 Mitgliedstaaten ratifiziert, das heisst von sämtlichen über ein Datenschutzgesetz verfügenden Staaten mit Ausnahme der Schweiz. Im Auftrag des EJPD haben wir im Hinblick auf eine Ratifizierung der Konvention durch die Schweiz die Vorbereitung einer entsprechenden Botschaft in Angriff genommen, und wir hoffen, dass die Schweiz diesem Übereinkommen zu Beginn der nächsten Legislaturperiode beitreten wird.
Die beiden mit datenschutzrechtlichen Fragen betrauten Komitees haben ihre Arbeiten fortgesetzt. So ist die Projektgruppe für Datenschutz (CJ-PD) zweimal zusammengetroffen und hat die Arbeiten an zwei Empfehlungen abgeschlossen. Zunächst einmal die Empfehlung zum Schutze personenbezogener Daten im Bereich der Telekommunikationsdienste (insbesondere bei den Telefondiensten), die vom Ministerkomitee an seiner Sitzung vom 6. und 7. Februar 1995 verabschiedet wurde. Diese Empfehlung enthält insbesondere Bestimmungen, die auf Abonnentenverzeichnisse, die Verwendung von Daten zu Zwecken des Direkt-Marketings, die detaillierte Rechnungstellung, interne Telefonzentralen, die Identifizierung der Rufnummer, die Um- oder Weiterleitung von Anrufen und die Verwendung von Mobiltelephonen Anwendung finden. Die zweite Empfehlung betrifft den Schutz medizinischer Daten. Ihre Verabschiedung durch das Ministerkomitee wurde verschoben, um dem Komitee für Gesundheitswesen Gelegenheit zu geben, Stellung zu beziehen. Diese Empfehlung wird auf jegliche Bearbeitung medizinischer Daten Anwendung finden, sei es im Bereich des Gesundheitswesens oder in einem anderen Zusammenhang, durch einen Arzt oder durch eine andere Person. Sie umfasst auch die medizinische Forschung und die Bearbeitung genetischer Daten. Die Empfehlung enthält insbesondere Bestimmungen, welche die Vertraulichkeit der Bearbeitung von medizinischen Daten verstärken, der betroffenen Person ein Recht auf Information vor jeder Bearbeitung von medizinischen Daten einräumen, die

Bedingungen festlegen, unter denen die Zustimmung der betroffenen Person eingeholt werden muss und und das Auskunftsrecht der betroffenen Person gewährleisten.
Zwei weitere Empfehlungen befinden sich derzeit in Ausarbeitung. Sie sollen die Bearbeitung von Personendaten einerseits zu statistischen Zwecken und andererseits für Privatversicherungszwecke regeln. Bezüglich letzterer haben wir der zweiten Sitzung der Arbeitsgruppe 14 in Strassburg beigewohnt. Dort wurde insbesondere der Inhalt der Einwilligungsklausel behandelt und die Frage diskutiert, ob es sinnvoll ist, Daten, die den Finanzbereich betreffen, den besonders schützenswerten Daten zuzuordnen.
Der durch die Konvention 108 ins Leben gerufene beratende Ausschuss, der insbesondere die Aufgabe hat, Stellungnahmen zur Anwendung der besagten Konvention abzugeben, hat sich näher mit der Definition von personenbezogenen Daten auseinandergesetzt. Er hat dem Einbezug von Stimmen und Bildern in die Definition zugestimmt, sofern diese eine Identifizierung der betroffenen Person ermöglichen. Hingegen hat der Ausschuss die Frage, ob die Bearbeitung von Daten wie Stimmen und Bildern in den Anwendungsbereich des Datenschutzes fallen oder nicht, noch nicht abschliessend entschieden. Diese Frage sollte zumindest für den Fall bejaht werden, dass Bild und Stimme in einem automatisierten System gespeichert werden, das eine Bearbeitung dieser Informationen gestattet. Schliesslich musste der beratende Ausschuss feststellen, dass die Verwendung des in Zusammenarbeit mit der Europäischen Union und der internationalen Handelskammer ausgearbeiteten "Mustervertrags" für grenzüberschreitende Datenflüsse bisher nicht auf das erwartete Echo gestossen ist. Wir selbst haben Unternehmen, die grenzüberschreitend tätig sind, mehrfach nahegelegt, Datenschutzverträge nach diesem Modell abzuschliessen.

3. Organisation für Zusammenarbeit und Entwicklung (OECD) - Datenautobahnen und interaktive Multimediasysteme

Seit der Verabschiedung der Richtlinien über den Schutz der Privatsphäre und den grenzüberschreitenden Fluss von personenbezogenen Daten vom 23. September 1980 hält die OECD regelmässig Ad-hoc-Experten-Sitzungen ab, welche die Einhaltung dieser Richtlinien begutachten und spezifische Problemstellungen hinsichtlich des Datenschutzes behandeln sollen. Eine solche Sitzung fand vom 30. November bis zum 2. Dezember 1994 in Paris statt. Sie war der Infrastruktur von Informationen, insbesondere den Datenautobahnen und den interaktiven Multimediasystemen gewidmet. Anhand konkreter Beispiele konnten wir neben den Vorteilen der neuen Technologien auch die dadurch entstehenden Risiken der Verletzung der Persönlichkeit erfassen. So liessen sich einige pervers anmutende, versteckte Aspekte dieser Technologien ans Licht bringen. Unter dem Vorwand, potentiellen Kunden die Möglichkeit einzuräumen, ihre Lebensmittel- oder gar Kleiderkäufe über ihren PC oder ihren interaktiven Fernsehapparat zu erledigen, ohne dafür ihr Haus verlassen zu müssen, sämtliche Eingaben der betroffenen Person werden in diesem Informationssystem gespeichert. Diese Daten werden anschliessend zur gezielten Steuerung des Angebots ausgewertet. Anhand der vom Kunden vorgenommenen Dateneingaben wird es auf diese Weise möglich, unzählige Informationen über seine Gewohnheiten, Wünsche und Erwartungen zu erhalten. Daraufhin - ohne dass sich die betreffende Person dessen bewusst ist - kann das Produkteangebot entsprechend anpasst und das Kaufverhalten der betreffenden Person beeinflusst werden. Es können daraus Persönlichkeitsprofile enstehen.
Es wurde auch festgestellt, dass sich mit der Einführung von Informatik und Netzwerken in jedem Haushalt und Betrieb der Lebensstil, der Arbeitsrhythmus und die geschäftlichen Transaktionen verändern werden. Diese Netzwerke werden in der Tat öffentliche Verwaltungen, Haushalte, öffentliche Unternehmen und andere Institutionen an ein sehr weites Spektrum interaktiver Dienste anschliessen, wie zum Beispiel an Sozialdienste,

Verwaltungsbehörden, Freizeit-, Bildungs- und kulturelle Einrichtungen, Datenbanken, an den Zahlungs- und Bankverkehr, an Einrichtungen zur Kundenwerbung oder an den elektronischen Handel. Diese Entwicklung darf allerdings nicht auf Kosten der Persönlichkeitsrechte des Individuums vonstatten gehen. In Zusammenarbeit mit den anderen Sitzungsteilnehmern haben wir eine anschauliche, wenn auch keineswegs erschöpfende Bestandesaufnahme der festgestellten Risiken und der schon bestehenden Verletzungsmöglichkeiten vorgenommen, die im Zuge der ersten Erfahrungen mit der Verwendung von Datenautobahnen in verschiedenen Ländern bereits beobachtet werden konnten: missbräuchliche Beschaffungen von Personendaten, unerwünschtes Eindringen in den Privatbereich infolge von Einkäufen über Telenetz, zwischenbehördlicher Austausch von personenbezogenen Informationen, die zu anderen Zwecken als den bei der Beschaffung angegebenen verwendet wurden, widerrechtliches Vorgehen einiger "Televerkäufer", zielgerichtete Werbesendungen, Erstellen von Persönlichkeitsprofilen auf der Basis von Multimedia-Interaktionen der betreffenden Personen oder auch Beobachtung der Lebensstile und -gewohnheiten der Benützer dieser Technologien.
Im Anschluss an die Bestandsaufnahme wurde über die Schritte diskutiert, mit denen diesen Phänomenen zu begegnen ist. Dabei wurde hervorgehoben, dass die neuen Technologien Teil unserer modernen Gesellschaft seien und es keinen Sinn habe, sie zu bekämpfen, sondern dass ihre Mechanismen zu studieren und daraufhin Strategien zu entwickeln seien, welche die Weiterentwicklung dieser Technologien unter gleichzeitiger Beachtung der Persönlichkeitsrechte des Individuums erlaubten. Dabei ist nebst der Schaffung von gesetzlichen Bestimmungen und Regelungen, von Verhaltenskodizes und ähnlichen freiwillig einzuhaltenden Normen oder gar technischen und organisatorischen Lösungen die "Sensibilisierung" und "Erziehung" des einzelnen in Hinblick auf diese Gefahren zentral. Alsdann wird jede Person in der Lage sein, sich in Kenntnis der Problematik in dieser neuen informatisierten Umgebung zu bewegen. An dieser Einsicht orientiert sich unsere Informationspolitik, in der wir eine unserer wichtigsten Aufgaben sehen.
Einige vorwiegend in Kanada durchgeführte Experimente haben im übrigen gezeigt, dass Transparenz nicht nur zur Verbesserung des Datenschutzes beiträgt, sondern auch den wirtschaftlichen Interessen dient. Die Experten haben sodann auf die Bedeutung von Technologien wie Chiffrierverfahren hingewiesen, mit Hilfe derer anonyme Transaktionen vorgenommen werden können. Ausserdem haben sie die komplementäre Rolle der Sicherheitsmassnahmen als Mittel, welche in der Lage sind, den Datenschutz und die Wahrung der Privatsphäre zu garantieren, herausgestellt.

4. Europäische Union

Wie bereits in unserem ersten Bericht (vgl. S. 77) erwähnt, hat die Europäische Kommission im Oktober 1992 eine zweite Fassung des Richtlinienentwurfs zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vorgelegt und sie an den Ministerrat weitergeleitet. Dieser zweite Entwurf war Gegenstand eingehender Diskussionen der Regierungsexperten, wobei er ziemlich verändert wurde. Er wurde am 20 Februar 1995 vom Ministerrat verabschiedet und ans Parlament übermittelt. Die Richtlinie könnte somit Anfang nächsten Jahres in Kraft treten. Der Entwurf einer Richtlinie zum Schutz personenbezogener Daten und der Privatsphäre im Zusammenhang mit den öffentlichen digitalen Telekommunikationsnetzen und insbesondere mit dem dienstintegrierten digitalen Netz (ISDN) sowie den öffentlichen mobilen digitalen Netzen wurde von der Kommission fertiggestellt und könnte dieses Jahr noch verabschiedet werden. Nach der Verabschiedung dieser Richtlinien wird deren Bedeutung und ihre Konsequenzen für die Schweiz zu untersuchen sein, insbesondere bezüglich des grenzüberschreitenden

Datenverkehrs. Weitere Arbeiten sind in bestimmten Bereichen, wie dem Zollwesen, in Gang.

5. Schengen

Das Schengener Abkommen, das von neun Mitgliedstaaten der Europäischen Union (Frankreich, Deutschland, Belgien, Luxemburg, Niederlande, Spanien, Portugal, Italien, Griechenland) unterzeichnet wurde, ist am 26. März dieses Jahres zwischen sieben Staaten in Kraft getreten. Italien und Griechenland erfüllen zur Zeit noch nicht alle rechtlichen und technischen Bedingungen, vor allem hinsichtlich des Datenschutzes, welche für die Anwendung des Abkommens nötig sind. Das Abkommen, das die Aufhebung der Grenzkontrollen in den Staaten des "Schengener Bereichs" vorsieht, regelt insbesondere den Personenverkehr und die polizeiliche, zollamtliche und gerichtliche Zusammenarbeit. Es sieht die Errichtung des umfangreichen computergestützten Schengener Informationssystems (SIS) vor, das einen raschen Informationsaustausch und einen schnellen Zugriff zu den für die Personen-, Fahrzeug- und Sachfahndung angelegten automatisierten Fahndungsdateien gewährleisten soll. Das SIS setzt sich zusammen aus einer für den technischen Unterhalt des Systems zuständigen Zentralstelle und einer nationalen Aussenstelle in jedem Mitgliedstaat. Um den Datenschutzes zu gewährleisten, enthält das Abkommen detaillierte Regelungen, die sich auf die Konvention 108 und auf die Empfehlung des Europarats Nr. (87) 15 abstützen, welche auf eine Regelung der Verwendung von personenbezogenen Daten im Polizeibereich abzielt. Diese Empfehlung ist übrigens Bestandteil des Schengener Abkommens. Die Schweiz ist nicht Mitglied von Schengen und kann dies, da sie nicht zur Europäischen Union gehört, zum jetzigen Zeitpunkt auch nicht werden. Unser Land hat allerdings jedes Interesse, sich diesen Staaten anzunähern, vor allem im Bereich der Bekämpfung des organisierten Verbrechens und des Drogenhandels, aber auch bezüglich Massnahmen zur Einwanderungskontrolle. Wir sind der Ansicht, dass diese Annäherung unter Beachtung der nationalen Datenschutzbestimmungen stattfinden und in gleichlautende Regelungen eingebettet sein sollte, wie sie im Schengener Abkommen vorgesehen sind. In diesem Sinn befürworten wir die Förderung einer institutionalisierten Zusammenarbeit.

IV. REGISTER DER DATENSAMMLUNGEN

1. Bilanz

Die Zahl von 1500 Anmeldungen von Datensammlungen, von der in unserem ersten Bericht die Rede war, ist erreicht und wird demnächst überschritten werden, da uns einige Ämter ihre Anmeldungen noch nicht haben zukommen lassen. Trotz der bestehenden Schwierigkeiten, die in erster Linie auf den Personalmangel sowohl bei den Datenschutzberatern als auch bei uns zurückzuführen sind, sind DATAREG und das Register der Datensammlungen auf dem besten Wege dazu, sich mittelfristig zu einem leistungsfähigen "Werkzeug" zu entwickeln.

Die Schwierigkeiten, auf die wir in unserem ersten Bericht hingewiesen hatten, bestehen weiterhin. Vor allem haben innerhalb der Bundesverwaltung, einige Ämter ihre Datensammlungen entweder noch gar nicht oder nur unvollständig angemeldet. Ausserdem

verfügen wir nicht über genügend Personal, um die Kontrolle der Anmeldeformulare effizient durchführen und das Register der Datensammlungen in der angestrebten Form und innerhalb der vorgesehenen Fristen veröffentlichen zu können. Hinzu kommt, dass die von den Departementen und einigen Ämtern ernannten Datenschutzberater uns nur selten bei der Erfüllung unserer Aufgabe unterstützen können, etwa indem sie das Anmeldeverfahren und die Übersetzungen organisieren. Dies wiederum liegt daran, dass ihnen von seiten der Verwaltungseinheiten, denen sie angehören, im allgemeinen weder die erforderliche Zeit noch die nötigen Mittel zur Verfügung gestellt werden.
Im Privatbereich sind uns Anmeldungen aus den verschiedensten Branchen, wie der Automobilbranche, den Banken, dem Einzelhandel, dem Tumor-Register, den Kirchen, der Telematik, der Presse usw. zugekommen. Die im Rahmen des Anmeldeverfahrens geknüpften Kontakte sind uns nicht nur im Hinblick auf die Erstellung des Registers der Datensammlungen sehr nützlich, sie erlauben uns auch, uns mit den Funktionsweisen dieser Bereiche vertraut zu machen und die privaten Inhaber von Datensammlungen in bezug auf datenschutzrechtliche Anliegen zu informieren, respektive zu sensibilisieren.
Abschliessend möchten wir festhalten, dass DATAREG und damit das Register der Datensammlungen trotz der erwähnten Schwierigkeiten dabei ist, Form anzunehmen und seine "Kinderkrankheiten" zu überwinden, um auf mittlere Sicht für die Betroffenen "der Schlüssel zur Ausübung ihres Auskunftsrechts" zu werden und uns gleichzeitig als effizientes Arbeitsinstrument zu dienen.

2. DATAREG - Verwaltungssystem

Nachdem im Juli 1994 das automatisierte System zur Verwaltung des Registers der Datensammlungen (DATAREG) in Betrieb genommen worden ist, liegen nun die ersten Auswertungen der bereits registrierten Datensammlungen vor.

Am 4. Juli 1994 wurde DATAREG bei uns offiziell in Betrieb genommen. Am 16. Juni 1994 waren 462 Anmeldungen von Datensammlungen durch Bundesorgane eingegangen. Davon waren 16 zur Registrierung und somit zur Eingabe ins DATAREG bereit. Von privaten Personen waren 94 Datensammlungen angemeldet worden. Davon waren 10 für die Eingabe ins DATAREG bereit. Bereit für die Eingabe ins DATAREG ist eine Anmeldung, wenn sie die gesetzlich vorgesehene summarische Prüfung der Rechtmässigkeit durchlaufen hat und in drei Sprachen (Deutsch, Französisch und Italienisch) vorliegt. Bis Ende Januar 1995 sind insgesamt 1'500 Anmeldungen beim EDSB eingetroffen. Davon sind 200 Anmeldungen von privaten Personen.

Die folgenden Ausführungen beziehen sich auf den Stand im Januar 1995:

- Zu diesem Zeitpunkt sind gesamthaft 111 Datensammlungen registriert. Davon stammen 104 von Bundesorganen. Von den 111 registrierten Datensammlungen sollen bis auf zwei alle publiziert werden. Alle Einträge sind in drei Sprachen erfolgt. Bisher wurden gemäss den Angaben auf den Anmeldungen von Datensammlungen 102 *Adressen* (z.B. Inhaber, Auskunftsperson, usw.) in das System aufgenommen.
- Auf den Anmeldeformularen sind 17 Kategorien von bearbeiteten Personendaten zur Auswahl und als Beispiele vorgegeben. Auf den eingegebenen Anmeldungen wurden jedoch 188 verschiedene Kategorien von Personendaten angegeben. Diese Kategorien werden insgesamt 530mal verwendet, was bedeutet, dass pro Anmeldung durchschnittlich fünf Kategorien von bearbeiteten Personendaten bezeichnet wurden.

- Es wurden 143 Kategorien von Datenempfängern aufgenommen. Von diesen sind 41 auch als Beteiligte aufgeführt. Daraus kann geschlossen werden, dass durchschnittlich jede zweite registrierte Datensammlung eine Kategorie von Beteiligten hat sowie in der Regel jede registrierte Datensammlung mindestens einer Empfängerkategorie zugeordnet ist. Aus diesen Datensammlungen werden also Daten an Dritte bekanntgegeben.
- Bei den Anmeldungen durch Bundesorgane wurden jetzt 56 verschiedene Rechtsgrundlagen genannt. Diese werden 154mal verwendet. Das bedeutet, dass pro Anmeldung im Schnitt mehr als eine Rechtsgrundlage (Gesetz/Verordnung) für die Bearbeitung der Datensammlung gemeldet wird.
- Für die Einträge von privaten Datensammlungen wurden bis Januar 1995 vier Branchenkategorien vergeben.
- Nach der Registrierung im DATAREG erhält die meldende Stelle einen Kontrollausdruck mit der Registernummer der Datensammlung und den Angaben, die ins DATAREG aufgenommen wurden.

Am System DATAREG wurden verschiedene Korrekturen und Anpassungen vorgenommen. Diese sind einerseits dadurch bedingt, dass es sich um ein neues Anmeldeverfahren handelt, andererseits durch technische Notwendigkeiten. So mussten zum Beispiel Feldlängen sowie männliche und weibliche Bezeichnungen im Kontrollausdruck des Registereintrags für die meldenden Stellen angepasst werden.

V. DER EIDGENÖSSISCHE DATENSCHUTZBEAUFTRAGTE

1. Aufgabenentwicklung

Auch dieses Jahr steigerte sich das Aufgabenvolumen in fast allen Bereichen. Besonderes Gewicht hatte die Klärung von Fragen bezüglich der Voraussetzungen der Anmeldung von Datensammlungen. Wie auch im letzten Jahr hatten wir zahlreiche Anfragen zum Auskunftsrecht, zu Persönlichkeitsverletzungen und allfälligen Rechtfertigungsgründen, zu Datenübermittlungen ins Ausland, zur Anwendbarkeit von kantonalen Bestimmungen und zu vielen anderen Datenschutzfragen zu beantworten.

2. Information der Öffentlichkeit

Während des ganzen Jahres haben wir an verschiedenen Veranstaltungen (Konferenzen, Tagungen) zum Datenschutz teilgenommen. Dadurch konnte verschiedenen Kreisen das Datenschutzrecht und die Zweckmässigkeit seiner Umsetzung nahegebracht werden und es wurden anstehende Probleme auf diesem Weg gelöst.
Dieses Jahr haben wir an Behörden und Private insgesamt 5000 Broschüren in verschiedenen Sprachen verschickt. Ergänzend zu den bereits vorhandenen Broschüren ist eine neue zum Datenschutz im privaten Arbeitsverhältnis erarbeitet worden.

Folgende Broschüren sind beim EDSB zu beziehen:

- Leitfaden für die Bearbeitung von Personendaten in der Bundesverwaltung
- Leitfaden für die Inhaber von Datensammlungen (Privatbereich)
- Die Rechte der betroffenen Personen bei der Bearbeitung von Personendaten
- Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes
- Leitfaden für die Bearbeitung von Personendaten im Arbeitsbereich (Privatbereich)

Wir nahmen zweimal die Gelegenheit wahr, via Pressecommuniqué über die Problematik der Anmeldeformulare für Mietinteressenten (siehe dazu S. 60) und über die Abfrage von Fahrzeuginhaber über die Nr. 111 (siehe dazu S. 74) zu informieren.

☎Telefondienst des EDSB

Auch dieses Jahr haben wir nicht nur über den offiziellen Korrespondenzweg Anfragen beantwortet. Viele Auskünfte wurden auch telefonisch erteilt.

Die nachfolgende Tabelle auf Seite 94 liefert einen Überblick über die Bereiche, in denen telefonische Anfragen besonders häufig waren.

Auf besonderes Interesse stiessen die Bereiche Anmeldung von Datensammlungen, Übermittlungen ins Ausland und Geltendmachung des Auskunftsrechts. Personen aus dem Privatbereich (Einzelpersonen, Gewerbe/Industrie, Vereine, Anwälte usw.) griffen mit insgesamt 870 Anfragen häufiger zum Telefon als die Bundesbehörden mit 230 Anfragen.

3. Personelle Ausstattung des Sekretariats des EDSB

Im letzten Jahr hat sich der Personalbestand des Sekretariats leicht erhöht, jedoch kann die Fülle unserer Aufgaben auch mit der heutigen Personalkapazität nicht zufriedenstellend bewältigt werden. Eine weitere Erhöhung des Personalbestandes ist in Aussicht. Sie wird uns ermöglichen, unsere Aufgaben im Bereich der Offenbarung des medizinischen Berufsgeheimnisses anzugehen. Zahlreiche andere Tätigkeitsbereiche bleiben jedoch weiterhin unterdotiert.

4. Aus- und Fortbildung

Aufgrund der schnellen Entwicklung des Datenschutz in rechtlicher und technischer Hinsicht besteht ein erhöhter Bedarf an Weiterbildung der Mitarbeiter/innen. Wichtig ist insbesondere die Verfolgung der Entwicklung auf internationaler Ebene, damit wir zeitgerechte Konfliktlösungen für unseren Bereich anstreben können. Doch fehlen zur Zeit vielfach die Mittel und die zeitliche Kapazität, um die erforderlichen Kurse zu besuchen.

5. Statistik über die Tätigkeit des EDSB

Zeitraum 1. April 1994 bis 31. März 1995

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.
Stellvertreter:	Buntschu Marc, lic. iur.
Rechtsdienst:	7 Personen
Informatikdienst:	3 Personen
Informationsdienst:	Tsiraktsopulos Kosmas, lic. iur.
Kanzlei:	3 Personen