Eidgenössischer Datenschutzbeauftragter

Préposé fédéral à la protection des données

3. Tätigkeitsbericht 1995/96

3ème Rapport d'activités 1995/96

© by EDSB
Alle Urheberrechte und Vertragsrechte vorbehalten
Vertrieb: Eidg. Drucksachen- und Materialzentrale, 3003 Bern

Eidgenössischer Datenschutzbeauftragter

Tätigkeitsbericht 1995/96

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 1995 und 31. März 1996 ab.

INHALTSVERZEICHNIS

*: Originalversion auf Französisch

*: Originalversion auf Französisch

*: Originalversion auf Französisch

*: Originalversion auf Französisch

ABKÜRZUNGSVERZEICHNIS

ADAK	Arbeitsgruppe Datenschutz und Analysenliste / Krankenversicherung
ADMAS	Register der Administrativmassnahmen
AFIS	Automatisiertes Fingerabdruck-Identifizierungssystem
AHV	Alters- und Hinterlassenenversicherung
AUPER	Automatisiertes Personenregistratursystem
BAP	Bundesamt für Polizeiwesen
BFF	Bundesamt für Flüchtlinge
BVPLUS	Personalinformationssystem der Bundesverwaltung (neu)
DOSIS	Provisorisches Datenverarbeitungssystem zur Bekämpfung des illegalen Drogenhandels (Pilot)
DSG	Datenschutzgesetz
EDSB	Eidgenössischer Datenschutzbeauftragter
EDSK	Eidgenössische Datenschutzkommission
EDV	Elektronische Datenverarbeitung
EJPD	Eidg. Justiz- und Polizeidepartement
EVK	Eidgenössische Versicherungskasse
FABER	Fahrberechtigungsregister
FMH	(Foederatio Medicorum Helveticorum) Verbindung der Schweizer Ärzte
MOFIS	Motorfahrzeug-Informationssystem
OECD	Organisation für Zusammenarbeit und Entwicklung
OR	Obligationenrecht
PERIBU	Personalinformationssystem der Bundesverwaltung
PIAS	Personalinformations- und administrationssystem des EJPD
PISEDI	Personalinformationssystem des EDI
REGI	Papierlose Personen- und Dossierverwaltung
RIPOL	Automatisiertes Fahndungssystem
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
VPB	Verwaltungsplaxis der Bundesbehörden
ZAN	Zentraler Aktennachweis des Schweizerischen Zentralpolizeibüros
ZAR	Zentrales Ausländerregister

I. AUSGEWÄHLTE THEMEN

1. Polizeiwesen

1.1. Organisiertes Verbrechen - Das System DOSIS

DOSIS ist ein Datenberarbeitungssystem zur Bekämpfung des unerlaubten Betäubungsmittelverkehrs. Als Pilotprojekt konzipiert, wird es von der Zentralstelle für die Bekämpfung des unerlaubten Betäubungsmittelverkehrs des Bundesamts für Polizeiwesen verwaltet. Die Funktion von DOSIS besteht insbesondere darin, die Zusammenarbeit mit den Betäubungsmittelbekämpfungsdiensten der kantonalen Polizeikorps über eine Online-Verbindung sicherzustellen. Die auf acht Kantone beschränkte externe Versuchsphase wurde durch eine zeitlich befristete Verordnung des Bundesrates geregelt. Mit dem Inkrafttreten des Bundesgesetzes über kriminalpolizeiliche Zentralstellen des Bundes am 15. März 1995 wurde das System DOSIS auf eine neue rechtliche Grundlage gestellt, insbesondere was die Bearbeitung von Personendaten anbelangt. Das Bundesamt für Polizeiwesen hat im Anschluss daran einen Entwurf für eine neue DOSIS-Verordnung ausgearbeitet und uns zur Begutachtung vorgelegt.

Indem der Bundesrat dem Vorschlag des Eidgenössischen Justiz- und Polizeidepartements zustimmte, unterstützte er die Einleitung der externen Versuchsphase für das Datenberarbeitungssystem zur Bekämpfung des unerlaubten Betäubungsmittelverkehrs DOSIS. Dieses Informatiksystem, das als Pilotversuch konzipiert wurde und auf einer zeitlich befristeten Verordnung beruht, wird von der Zentralstelle für die Bekämpfung des unerlaubten Betäubungsmittelverkehrs des Bundesamtes für Polizeiwesen verwaltet. Der Zweck von DOSIS besteht in erster Linie darin, über eine Online-Verbindung die Zusammenarbeit mit den Betäubungsmittelbekämpfungsstellen der kantonalen Polizeikorps sicherzustellen.

Die zeitlich befristete Verordnung wurde vom Bundesamt für Polizeiwesen in Zusammenarbeit mit unserem Dienst ausgearbeitet. Sie beschränkt die externe Versuchsphase auf acht Kantone und legt insbesondere die mit dem Informatiksystem DOSIS verbundenen Zielsetzungen fest. Im weiteren legt sie die Untersysteme, die zu bearbeitenden Daten, die Kategorien der Benutzer des Systems und deren Zugriffsrechte fest. Geregelt werden auch die Datenbearbeitung, insbesondere die Datenerfassung und die Kontrolle ihrer Qualität, die Weitergabe der Daten, die Dauer ihrer Aufbewahrung, die Löschung und die Sicherheitsmassnahmen.

Parallel zu dieser externen Versuchsphase für das System DOSIS trat am 15. März 1995 das Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes in Kraft. Dieses Gesetz regelt in erster Linie die Aufgaben der Zentralstellen des Bundesamtes für Polizeiwesen bei der Bekämpfung des organisierten Verbrechens. Es regelt den Einsatz von Polizeiverbindungsleuten im Ausland, die Zusammenarbeit mit den Strafverfolgungsbehörden und Polizeidienststellen der Kantone und des Auslandes 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.

Mit dem Inkrafttreten des Bundesgesetzes über kriminalpolizeiliche Zentralstellen des Bundes wurde das System DOSIS auf eine neue rechtliche Grundlage gestellt, insbesondere was die Bearbeitung von Personendaten anbelangt. Dies machte eine

Anpassung der zeitlich befristeten Verordnung erforderlich.

Eine erste Teilrevision der Verordnung wurde bereits am 15. März 1995 vorgenommen, um darin einen Hinweis auf die Bestimmungen über die Ausübung des Auskunftsrechts im Bundesgesetz über kriminalpolizeiliche Zentralstellen zu verankern. Trotz unserer Vorbehalte (vgl. unseren 2. Tätigkeitsbericht, S. 10 ff.) wurde abweichend von den Bestimmungen des Bundesgesetzes über den Datenschutz eine Sonderregelung verabschiedet, die für das System DOSIS ein indirektes Auskunftsrecht vorsieht.

In der Folge wurde vom Bundesamt für Polizeiwesen ein Entwurf für eine vollständige Revision der DOSIS-Verordnung ausgearbeitet, um das definitive Datenbearbeitungssystem zur Bekämpfung des unerlaubten Betäubungsmittelverkehrs festzulegen. Das Bundesamt für Polizeiwesen zog dabei Nutzen aus den Erfahrungen während der externen Versuchsphase für das System DOSIS und aus den Bestimmungen im Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes für die Bearbeitung von Personendaten. Um eine Stellungnahme gebeten, haben wir den Entwurf aus datenschutzrechtlicher Sicht geprüft, wobei wir uns auf die uns zur Verfügung gestellten Informationen und Unterlagen, die Ergebnisse von Arbeitssitzungen und die Systemvorführungen abstützten. Wir haben uns ausserdem dafür eingesetzt, dass einerseits die vorgeschlagenen Bestimmungen den rechtlichen Rahmen des Bundesgesetzes über kriminalpolizeiliche Zentralstellen respektieren und andererseits die zahlreichen Datenbearbeitungen, die bei der Benutzung des Systems DOSIS ausgeführt werden, klar umschrieben sind.

Verschiedenen Punkten des Verordnungsentwurfs konnten wir zustimmen. Dies gilt insbesondere für die Bestimmung über die Online-Anschlüsse der Betäubungsmittelbekämpfungsstellen der kantonalen Polizeikorps und der Mitarbeiter der Zentralstelle für die Bekämpfung des unerlaubten Betäubungsmittelverkehrs. Bei einigen Punkten des Verordnungsentwurfs haben wir jedoch auch Vorbehalte angebracht, wobei wir jedesmal gleichzeitig konkrete Lösungsvorschläge formulierten. Diese Punkte betreffen insbesondere die Erarbeitung von Sonderbewertungen und die Erstellung von grafischen Darstellungen sowie die Möglichkeit, Elemente für den Vergleich mit Drittpersonen hervorzuheben. Vorbehalte wurden auch angebracht in bezug auf das Abfrageverfahren für die Unterfelder des Systems, die Übertragung von gewissen DOSIS-Daten in den zentralen Aktennachweis (ZAN) des Bundesamtes für Polizeiwesen sowie bezüglich der Dauer der Datenaufbewahrung und ihrer Löschung.

Ausserdem ist auf eine Uneinigkeit hinzuweisen, die auf der Auslegung einer Bestimmung des Bundesgesetzes über kriminalpolizeiliche Zentralstellen des Bundes beruht. In diesem Gesetz ist ausdrücklich festgehalten, dass innerhalb des Datenbearbeitungssystems die Verwendung der erhobenen Daten vor der Eröffnung eines Strafverfolgungsverfahrens getrennt von der Verwendung der Strafverfahrensdaten des Bundes und der Kantone ablaufen muss. Die Umsetzung dieser Bestimmung im Verordnungsentwurf wird gegenwärtig unter Mithilfe des Bundesamtes für Justiz noch geprüft.

Schliesslich haben wir Erläuterungen zur Abwicklung der externen Versuchsphase für das System DOSIS verlangt. Wir mussten nämlich feststellen, dass wir über die Erteilung von on-line-Anschlüssen an gewisse kantonale Polizeidienststellen, die in der zeitlich befristeten Verordnung nicht erwähnt sind und deshalb an diesem Pilot-

versuch nicht teilnehmen dürfen, weder informiert noch um Stellungnahme gebeten wurden. Wir haben auch darauf hingewiesen, dass der Vorschlag an den Bundesrat für die Verabschiedung der neuen Verordnung in jenem Teil, welcher der Abwicklung der externen Versuchsphase gewidmet war, keinen Hinweis auf diese Anschlüsse enthielt. Wir bedauern, dass wir nicht angefragt wurden, und verlangen, dass der dem Bundesrat unterbreitete Vorschlag sowie der Schlussbericht über den Pilotversuch DOSIS dementsprechend ergänzt werden.

1.2. Geldwäscherei - Entwurf eines Bundesgesetzes

Aufgrund der Ergebnisse des Vernehmlassungsverfahrens (vgl. unseren 2. Tätigkeitsbericht, S. 16 ff.) hat der Bundesrat beschlossen, dass der Vorentwurf des Bundesgesetzes zur Bekämpfung der Geldwäscherei im Finanzsektor vollständig überarbeitet werden muss. Wir haben diesen Entscheid begrüsst, da der Vorentwurf trotz der zahlreichen vorgesehenen Datenbearbeitungen keine einzige Datenschutzbestimmung enthielt. Für den neuen Gesetzesentwurf hat die Eidgenössische Finanzverwaltung Bestimmungen über die Datenbearbeitung verfasst. Bei der Prüfung dieser internen Vorschläge haben wir darauf hingewiesen, dass in bezug auf die Datenbearbeitungen durch die Zentralstelle für die Bekämpfung des organisierten Verbrechens beim Vollzug dieses Gesetzes noch genauere Bestimmungen aufgestellt werden müssen.

In unserem 2. Tätigkeitsbericht (S. 16 ff.) haben wir betont, dass wir die Eidgenössische Finanzverwaltung anlässlich des Vernehmlassungsverfahrens zum Vorentwurf des Bundesgesetzes zur Bekämpfung der Geldwäscherei im Finanzsektor darauf hingewiesen haben, dass die Anwendung dieses Gesetzes für verschiedene betroffene Stellen erhebliche Datenbearbeitungen mit sich bringen werde. Dennoch wurden Datenschutzfragen im Verlauf der Arbeiten am Entwurf von der departementsübergreifenden Arbeitsgruppe nicht erörtert. Angesichts der noch bestehenden Unsicherheiten und offenen Optionen wurden in den Erläuterungen zum Vorentwurf in bezug auf den Datenschutz keine Überlegungen angestellt, und in den Vorentwurf keine datenschutzspezifischen Bestimmungen aufgenommen.

Nach der Veröffentlichung der Ergebnisse des Vernehmlassungsverfahrens entschied der Bundesrat, dass der Vorentwurf vollständig überarbeitet werden müsse.

Im Juli 1995 hat uns die Eidgenössische Finanzverwaltung einen neuen Gesetzesentwurf zur Stellungnahme unterbreitet, der sich noch im Stadium der internen Ausarbeitung befand. Nachdem wir festgestellt hatten, dass wiederum keine Datenschutzbestimmungen in diesen Entwurf aufgenommen worden waren, wiederholten wir unsere Vorschläge und Bemerkungen, die wir zum Teil noch ergänzten. Da im Entwurf keine Bestimmungen über die Art der Datenübertragung enthalten waren, haben wir erneut darauf hingewiesen, dass ein allfälliger Austausch von Daten zwischen der Zentralstelle, dem Kontrollorgan und den kantonalen Behörden mit Hilfe eines Abrufverfahrens (on-line-Verbindungen) auf Gesetzesebene ausdrücklich vorgesehen werden muss. Da der Entwurf auf das neue Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes verweist, das am 15. März 1995 in Kraft getreten ist, haben wir ausserdem darauf hingewiesen, dass den darin enthaltenen speziellen Bestimmungen über die Bearbeitung von Personendaten besondere Beachtung geschenkt werden muss. Dies gilt insbesondere für jene Normen, die in das Bundesgesetz zur Bekämpfung der Geldwäscherei integriert werden müssen, und für jene Normen, die in einer Verordnung enthalten sein können.

Im Oktober 1995 wurde uns eine neue Version des Gesetzesentwurfs vorgelegt, in die Bestimmungen über die Bearbeitung von Personendaten aufgenommen worden waren. Diese Bestimmungen, die in einem besonderen Abschnitt des Gesetzes zusammengefasst wurden, sind in Form von Vorschlägen von der Eidgenössischen Finanzverwaltung ausgearbeitet und im Anschluss daran unter Mitarbeit unseres Dienstes überarbeitet worden. In unserer Stellungnahme vom Dezember 1995 haben wir bestätigt, dass die Bestimmungen im “Abschnitt 6: Bearbeitung von Personendaten” eine gute Grundlage für die Regelung der umfangreichen Bearbeitung von Daten bilden, die aus der Anwendung dieses Gesetzes für die verschiedenen betroffenen Stellen resultieren wird. Wir denken dabei insbesondere an die Beschaffung, die Erfassung in verschiedenen Registern, die Aufbewahrung, die Bekanntgabe und an den Austausch von Personendaten sowie an die Einschränkungen in bezug auf die Ausübung des Auskunftsrechts.

Wir haben jedoch ebenfalls darauf hingewiesen, dass sowohl auf Gesetzes- als auch auf Verordnungsebene noch gewisse Präzisierungen vorgenommen werden müssen. Sodann besteht die bedeutendste Lücke in diesem Gesetzesentwurf unserer Ansicht nach darin, dass in bezug auf die Datenbearbeitungen, die durch die “Meldestelle” vorgenommen werden, noch zahlreiche Unklarheiten bestehen. Im Gesetzesentwurf wird diese Aufgabe der Zentralstelle für die Bekämpfung des organisierten Verbrechens des Bundesamtes für Polizeiwesen übertragen und somit auf das Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes verwiesen. Im Botschaftsentwurf wird im übrigen darauf hingewiesen, dass die Modalitäten der Verwaltung des künftigen Datenbearbeitungssystems zur Bekämpfung der Geldwäscherei des Bundesamtes für Polizeiwesen noch nicht genau festgelegt sind. Wir haben daher verlangt, dass in der Botschaft präzisiert wird, wie dieses Amt die Informationen zu bearbeiten hat, die ihm im Rahmen der Anwendung des Bundesgesetzes zur Bekämpfung der Geldwäscherei im Finanzsektor mitgeteilt werden. Diese Präzisierungen sind entscheidend im Hinblick darauf, welche Normen noch in dieses Gesetz zu integrieren sind und welche auf Verordnungsebene ausgearbeitet werden können.

Beim gegenwärtigen Stand des Entwurfs haben wir in Übereinstimmung mit der Eidgenössischen Finanzverwaltung keine weiteren Bemerkungen angebracht, da wir diese Bestimmungen als einen ersten Wurf betrachten, der das Ergebnis der Zusammenarbeit zwischen unseren Diensten darstellt. Wir werden den gesamten Entwurf anlässlich des Vernehmlassungsverfahrens prüfen, das im Laufe des Jahres 1996 eingeleitet wird. Wir werden dann Gelegenheit haben, definitiv Stellung zu beziehen, insbesondere in bezug auf die Datenbearbeitungen durch die Zentralstelle für die Bekämpfung des organisierten Verbrechens im Rahmen der Anwendung dieses Gesetzes, sowie bezüglich der sich daraus ergebenden rechtlichen Folgen.

1.3. Innere Sicherheit - Debatten in den Eidgenössischen Räten

Nachdem der Entwurf des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit am 13. Juni 1995 vom Ständerat behandelt worden war, wurde er an die Kommission für Rechtsfragen des Nationalrats überwiesen. Dieser Gesetzesentwurf enthält aus datenschutzrechtlicher Sicht zahlreiche problematische Aspekte. Wir haben uns insbesondere zu den Bestimmungen bezüglich der Ausübung des Auskunftsrechts und zur speziellen Informationsbeschaffung mit Hilfe von technischen Überwachungsgeräten kritisch geäussert.

Der Entwurf eines Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit, der vom Bundesrat im März 1994 ausgearbeitet wurde, wird gegenwärtig in den Eidgenössischen Räten beraten. Als uns der Vorentwurf des Gesetzes zur Stellungnahme unterbreitet worden war, hatten wir eine Reihe von Vorbehalten und Vorschlägen angebracht. Anlässlich der Beratungen in der Kommission für Rechtsfragen des Ständerats hatten wir Gelegenheit, uns insbesondere zur Bestimmung bezüglich der Ausübung des Auskunftsrechts durch die betroffenen Personen zu äussern.

In seiner Plenarsitzung vom 13. Juni 1995 entschied der Ständerat trotz unserer Vorbehalte, dem Vorschlag seiner Kommission zu folgen und in den Gesetzesentwurf eine Bestimmung über das Auskunftsrecht aufzunehmen, die gleichlautet, wie die Bestimmung im Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes, das am 15. März 1995 in Kraft getreten ist. In der gleichen Sitzung beschloss der Ständerat ausserdem einen neuen Artikel über die Beschaffung von speziellen Informationen. Diese Norm soll bei Präventivermittlungen im Polizeibereich die Überwachung des Briefverkehrs und die Abhörung von Telefongesprächen sowie den Einsatz von technischen Überwachungsgeräten ermöglichen.

Anlässlich einer Anhörung durch die Kommission für Rechtsfragen des Nationalrates im Oktober 1995, zeigten wir die Gefahren auf, die mit der Einführung einer solchen Bestimmung verbunden sind. Die Einsatzbedingungen dieser Bestimmung, welche viel weniger restriktiv sind, als diejenigen des Strafverfahrens sowie die Anwendung dieser Bestimmung bei Präventivermittlungen im Polizeibereich haben wir als kritisch eingestuft. Im Januar 1996 entschied die Kommission, dem Vorschlag des Ständerats nicht zu folgen und die entsprechende Norm zu streichen. Ausserdem hatte die Kommission schon im November 1995 beschlossen, auch den Begriff des organisierten Verbrechens zu streichen, da sie der Auffassung war, dass diese Aufgabe nicht im Zusammenhang mit der inneren Sicherheit steht.

Angesichts der zahlreichen Aspekte dieses Gesetzesentwurfs, die mit dem Datenschutz im Zusammenhang stehen, wurden wir gebeten, an der Sitzung der Kommission für Rechtsfragen des Nationalrates teilzunehmen, die im Februar 1996 stattfand. Der Entwurf wird anschliessend im Nationalrat behandelt.

1.4. Das automatische Fingerabdruck-Identifizierungssystem AFIS

Aufgrund der Entwicklung im Bereiche der Personenidentifikation hat sich eine Neustrukturierung der Sektion Identifikation des BFF und der Sektion Erkennungsdienst des BAP als unausweichlich erwiesen. Mit dem neuen Konzept AFIS-Service soll eine einzige Anlaufstelle für alle AFIS-Dienstleistungen geschafft werden. AFIS-Service soll insbesondere die Aufgabe der Fingerabdruckidentifizierung und der Bekanntgabe von Kurzpersonalien wahrnehmen. Amtsspezifische Kompetenzen und Zuständigkeiten von BAP und BFF sollen weiterhin getrennt wahrgenommen werden.

Das System AFIS verfolgt den Zweck der Personenidentifikation anhand von Fingerabdrücken. Es stellt eine gemeinsame Fingerabdruckdatenbank für die Bereiche Polizei und Asyl dar. AFIS wirft die Frage nach seiner Konformität mit dem zentralen datenschutzrechtlichen Gebot der Zweckgebundenheit auf. Anlässlich der ersten Realisierungsetappe wurde unsererseits das Projekt AFIS-Service im Lichte des genannten Gebotes geprüft. Dabei hielten wir fest, dass bei der Projektrealisierung und

in den vorgesehenen Gesetzesänderungen auf die Trennung von Asyl- und Polizeidaten zu achten ist, sowohl in struktureller Hinsicht als auch bezüglich Zugriffsberechtigungen von BAP und BFF. Insbesondere wurde die Notwendigkeit einer Interessenabwägung vor der Bekanntgabe von Flüchtlingsdaten in den Polizeibereich betont. So dürfen Kurzpersonalien von Flüchtlingen in den Polizeibereich nur bei Vorliegen eines genügenden polizeilichen Grundes bekanntgegeben werden. Eine auf diese Art erfolgte Identitätsbekanntgabe darf nur mit Zustimmung des BFF oder der mit Aufgaben nach dem Asylgesetz beauftragten Behörden ins Ausland weitergegeben werden. Diese Lösung trägt insbesondere dem asylrechtlichen Verbot der Bekanntgabe von Flüchtlingsdaten ins Ausland Rechnung. Sie gilt auch für das System Rapid Response AFIS. Eine umfangreichere Datenbekanntgabe kann nur amtshilfeweise und nach gründlicher Interessenabwägung erfolgen.

Zur Diskussion stand auch die Möglichkeit der Ausdehnung des Systems Rapid Response AFIS (RRA) auf andere Kantone. RRA ist ein dem Kanton Zürich aufgrund der dortigen besonderen Drogensituation zur Verfügung stehendes Fingerabdruck-Identifizierungssystem. Es charakterisiert sich durch elektronische, innert kurzer Zeit erfolgende Bekanntgabe der Kurzpersonalien und des Datenbesitzers. Ansonsten unterscheidet es sich vom üblichen System AFIS kaum. Insbesondere untersteht es den gleichen datenschutzrechtlichen Regeln. RRA stellt als solches das Modell für das Projekt AFIS-Service dar.
Den Einbezug weiterer Kantone ins System RRA machten wir von der Schaffung einer Rechtsgrundlage auf Ebene Bundesratsverordnung abhängig.

1.5. Vollautomatisiertes Strafregister

Das Projekt vollautomatisiertes Strafregister VOSTRA wird in verschiedene Realisierungseinheiten aufgeteilt und während der Periode 1996-1998 schrittweise entwickelt. Die Schaffung einer formellgesetzlichen Grundlage ist frühestens für Anfang 1998 geplant. Eine Übergangsverordnung als gesetzliche Grundlage für die Zeitspanne 1996-1998 ist aus datenschutzrechtlichen Gründen nicht möglich.

Das Projekt vollautomatisiertes Strafregister VOSTRA automatisiert die Verwaltung der Urteils- bzw. Strafregisterauszüge im Bundesamt für Polizeiwesen. Es stellt den Datenaustausch mit anderen Amtsstellen von Bund und Kantonen von Papier auf elektronische Medien um. In der ersten Realisierungsetappe geht es hauptsächlich darum, den Strafregisterauszug einer Person ohne Angabe der Strafen durch Abrufverfahren (on-line) bekanntzugeben. Die zweite Etappe sieht die on-line-Bekanntgabe des Strafregisterauszuges mitsamt Strafen vor. Die schrittweise Realisierung der genannten Etappen findet grösstenteils vor 1998 statt, während die Regelung im Strafgesetzbuch erst für 1998 vorgesehen ist. Die Realisierung des Systems gestützt auf eine Übergangsverordnung ist aufgrund des datenschutzrechtlichen Erfordernisses einer formellgesetzlichen Grundlage nicht möglich. Deshalb muss für die Bearbeitung von Strafregisterdaten und deren Bekanntgabe durch Abrufverfahren die erforderliche Rechtsgrundlage geschaffen werden.

1.6. Revision des Strassenverkehrsgesetzes

Eine Reihe von parlamentarischen Vorstössen hat zur Notwendigkeit einer Revision des Strassenverkehrsgesetzes geführt. Unsere anlässlich der Ämterkonsultation vor-

gebrachten datenschutzrechtlichen Anliegen betreffen hauptsächlich die Regelungsdichte. Wir schlugen ausserdem vor, auf die Publikation des Verzeichnisses der Fahrzeughalter zu verzichten. Eine gleichlautende Forderung wurde mit parlamentarischer Initiative gestellt.

Im Bereich des Strassenverkehrs wird der Bund verschiedene automatisierte Datenbearbeitungssysteme führen. Dabei handelt es sich einerseits um das Register der Administrativmassnahmen ADMAS, das Fahrberechtigungsregister FABER, das Fahrzeug- und Halterregister MOFIS, andererseits das Register über die Unfallstatistik. Diese Register enthalten zum Teil besonders schützenswerte Personendaten, weshalb bei einer Automatisierung der Bearbeitung hohe Anforderungen an die gesetzlichen Grundlagen zu stellen sind. Anlässlich der Ämterkonsultation stellten wir eine ungenügende Regelungsdichte der entsprechenden Gesetzesgrundlagen fest. Diese müssen insbesondere den Zweck der Datenbearbeitung, die zur Bearbeitung ermächtigten Behörden und ihre Aufgaben, die Datenempfänger, die verwendeten Mittel, den Kreis der betroffenen Personen, die bearbeiteten Personendaten, die Datenweitergabe und den Schutz vor Missbräuchen mit hinreichender Bestimmtheit regeln.

Um das Risiko von Persönlichkeitsverletzungen zu entschärfen, schlugen wir im Rahmen der Ämterkonsultation ausserdem vor, auf die Publikation des Verzeichnisses der Fahrzeughalter zu verzichten. Dadurch soll insbesondere verhindert werden, dass Informationen über Fahrzeughalter in öffentliche Informationskanäle gelangen. Eine Initiative gleichen Inhaltes wurde auch parlamentarisch eingeleitet. Sie wird zur Zeit von der Kommission für Rechtsfragen des Nationalrates geprüft.

2. Ausländer- und Asylrecht

2.1. Zugriff von Polizeistellen auf das Zentrale Ausländerregister ZAR

In einer Beschwerde an die Eidg. Datenschutzkommission haben wir die immer noch ungelösten Probleme beim Zugriff von Polizeistellen auf das ZAR und bei der Bearbeitung von Ausländerdaten aus dem ZAR mittels Büroautomation kritisiert. Es geht darum, die Polizeizugriffe auf ein sinnvolles Mass zu reduzieren und die Büroautomationssysteme in eine DSG-konforme Sicherheitsarchitektur einzubinden.

Erstens legten wir der EDSK die Frage vor, ob die beim Bundesamt für Polizeiwesen (BAP) verwendeten Mittel der Büroautomation eine sichere und vertrauliche Bearbeitung der Ausländerdaten gewährleisten. Die dem BAP zugänglich gemachten Ausländerdaten dürfen nicht mit den Fahndungsdaten des BAP zu neuen Datensätzen oder -sammlungen verbunden oder mit den Fahndungsdatensammlungen des BAP abgeglichen werden. Ebensowenig dürfen sie unbefugt an Dritte im In- und Ausland bekanntgegeben werden (vgl. hierzu auch den ersten und den zweiten Tätigkeitsbericht, S. 23f. und S. 20ff.). Nach unserer Auffassung bieten die bisher beim BAP verwendeten Sicherheitsmassnahmen keine ausreichende Gewähr dafür, dass Fehlleistungen und Pannen mit hinreichender Sicherheit ausgeschlossen oder ihr Eintritt zumindest als unwahrscheinlich gewertet werden könnte. Die in der Verordnung vom 10. Juni 1991 über den Schutz der Informatiksysteme und -anwendungen in der Bundesverwaltung vorgeschriebene Risikobeurteilung, bei welcher die Sicherheitsspezialisten des Bundesamtes für Informatik beizuziehen wären, steht jedenfalls

noch aus. Ein blosses Bearbeitungsverbot haben wir vor dem Hintergrund der vorhandenen technischen Bearbeitungsmöglichkeiten als klar ungenügend beurteilt und verlangt, dass an den Anwendungen selbst Sicherheitsvorkehren getroffen werden, wie sie heute ohne weiteres möglich sind und auch zum internationalen Standard gehören.

Das zweite zentrale Problem betraf die Frage, ob und unter welchen Voraussetzungen den verschiedenen z.T. mit Fahndungsaufgaben betrauten Dienststellen im BAP die zu zivilen Zwecken beschafften ZAR-Daten im Abrufverfahren zugänglich gemacht werden dürfen. Als erste unabdingbare Voraussetzung hiefür erachteten wir den ausreichenden Schutz dieser Daten, welcher indessen - wie vorstehend dargelegt - trotz wiederholten Mahnungen nicht oder ungenügend ausgewiesen wurde. Zweite unabdingbare Voraussetzung zur Einrichtung eines Abrufverfahrens ist, dass ein solches für die Aufgabenerfüllung im konkreten Fall wirklich erforderlich ist, und dass nicht andere, weniger einschneidende Formen der amtshilfeweisen Datenbekanntgabe ausreichen würden. Eine interne Abklärung beim BAP hat ergeben, dass nur wenige Dienststellen dieser Behörde die ihnen zur Verfügung stehenden Online-Zugriffe auf das ZAR häufig gebrauchen. Für einige Abfragen pro Tag oder pro Woche würden in den meisten Fällen einzelfallweise (EDV-gestützte) Datenübermittlungen genügen. Aus datenschutzrechtlicher Sicht müssen die nach dem "Selbstbedienungsprinzip" und ohne vorgängige Interessenabwägung erfolgenden Online-Datenübermittlungen namentlich im heiklen Polizeibereich als einschneidend betrachtet werden. Sie sind wo immer möglich zu vermeiden. Dies ergibt sich aus dem Verhältnismässigkeitsgrundsatz und - mit Blick auf eine allfällige informationelle Schlechterstellung der Ausländer gegenüber den Schweizern - wohl auch aus dem Gleichbehandlungsgebot. Mit ähnlichen Fragen beschäftigen sich auch Behörden und Gerichte des Auslands, so etwa zur Zeit das deutsche Bundesverfassungsgericht.

2.2. Kleine Teilrevision der ZAR-Verordnung

In einer kleinen Teilrevision der ZAR-Verordnung wurde dem Umstand Rechnung getragen, dass während einer kurzen Übergangszeit jeweils auch die Namen der Pflegeeltern ausländischer Kinder im ZAR erfasst werden müssen. Ausserdem dürfen Flüchtlingsdaten, die dem ZAR zum Ausdruck von Ausweisen gemeldet werden, nicht im ZAR gespeichert werden.

Bei Bekanntwerden der Namen der Kinder sind die Namen der Pflegeltern zu löschen und spätestens einen Monat nach der Adoption auch die Namen der Kinder. Bei dieser Gelegenheit hat der Bundesrat auch festgehalten, dass die dem ZAR vom Bundesamt für Flüchtlinge zum Ausdruck von Ausweisen gemeldeten *Personendaten aus dem AUPER nicht im ZAR gespeichert werden dürfen.* Damit ist uns der Bundesrat entgegengekommen. Das Zweckbindungsgebot würde einer auch nur teilweisen Zusammenlegung der Asylbewerberdaten mit den übrigen Ausländerdaten klar entgegenstehen. Hinzu kommt, dass die hochsensiblen Asylbewerberdaten weitreichende Sicherheitsanforderungen an eine Datensammlung stellen, welche sich bei einer auch nur teilweisen Zusammenlegung mit einer anderen Datensammlung auf diese "vererben" würden. Wegen der verzweigten Struktur und der Grösse des ZAR würden sich daraus für diese Datensammlung weitere erhebliche Probleme ergeben.

2.3. Schweizer und Schweizerinnen im Zentralen Ausländerregister

Wir wurden von privater Seite angefragt, ob im Zentralen Ausländerregister ZAR aufgeführte Schweizerinnen und Schweizer auch über das Fahndungssystem RIPOL abgefragt werden können.

Gemäss ZAR-Verordnung sind im ZAR schweizer Arbeitgeber und Arbeitgeberinnen (oftmals Firmen) ausländischer Arbeitnehmer und Arbeitnehmerinnen verzeichnet, ferner schweizer Gastgeberinnen und Gastgeber sowie während einer Übergangszeit von zwei Jahren neu in der Schweiz eingebürgerte Personen. Hinzu kommen, wie vorstehend dargelegt, die Pflegeeltern ausländischer Kinder. Von den Polizei- und Grenzbehörden sind über die RIPOL-Leitung im ZAR nur wenige Datenfelder abrufbar, welche mit dem Namen einer Ausländerin oder eines Ausländers verknüpft sein müssen. Darunter befinden sich freilich auch die Datenfelder "Arbeitgeber" und "Adresse" der Ausländerinnen und Ausländer. Der Zugriff auf schweizer "Gastgeber" steht demgegenüber nur dem Bundesamt für Ausländerfragen, dem Beschwerdedienst des EJPD, den schweizer Auslandvertretungen und den Fremdenpolizeibehörden der Kantone offen, nicht jedoch der Polizei. Ebensowenig darf das Datenfeld "Pflegeeltern" über die RIPOL-Leitung aus dem ZAR abgerufen werden. Hier ist zudem geplant, die Zugriffe der zuständigen kantonalen Behörden (i.d.R. Fremdenpolizei) auf die im eigenen Kanton ansässigen Pflegeeltern zu beschränken, was aus datenschutzrechtlicher Sicht rasch erfolgen sollte. Eine weitere Verbesserung der Vertraulichkeit würde namentlich im sensitiven Bereich der Adoption zweifellos auch eine Chiffrierung bringen.

Somit können grundsätzlich nur die seit weniger als zwei Jahren in der Schweiz eingebürgerte Personen und die schweizer Arbeitgeberinnen und Arbeitgeber ausländischer Staatsangehöriger durch die Polizei bzw. über die RIPOL-Leitungen aus dem ZAR abgefragt werden. Unsere Abklärungen haben aber ergeben, dass die neu eingebürgerten Schweizerinnen und Schweizer zum Teil über die zulässige Dauer von zwei Jahren hinaus im ZAR verzeichnet waren. Die zuständigen Stellen im EJPD haben hierauf die vor mehr als zwei Jahren eingebürgerten Schweizerinnen und Schweizer im ZAR gelöscht. Weiter hat sich beim Datenfeld "Adresse" ergeben, dass zur Zeit im ZAR mit technischen Mitteln die Eingabe von *schweizer Gastgeberinnen und Gastgebern anstelle der ausländischen Gäste* nicht verhindert werden kann. Es lässt sich also nicht mit Bestimmtheit ausschliessen, dass unter Umständen auch schweizer Gastgeberinnen und Gastgeber von ausländischen Staatsangehörigen unter dem Datenfeld "Adresse" den Polizeibehörden über die RIPOL-Leitung bekanntgegeben werden können, obwohl dies gegen die ZAR-Verordnung verstossen würde. Offenbar besteht leider zur Zeit - anders als bei den neu eingebürgerten Personen - kein effizientes (elektronisches) Verfahren zur nachträglichen Kontrolle des ZAR auf derartige mögliche Fehleintragungen von Schweizerinnen und Schweizern im ZAR. Das Bundesamt für Ausländerfragen hat zwar in einem Rundschreiben die zuständigen kantonalen Behörden auf die Rechtslage hingewiesen und sie an ihre Sorgfaltspflichten erinnert. Wir sind jedoch der Meinung, dass in dieser Hinsicht beim ZAR unbedingt auch *wirksame Kontrollverfahren* eingerichtet werden müssen, wie dies die Datenschutzverordnung ausdrücklich in den Bestimmungen über das Bearbeitungsreglement vorschreibt. Im Rahmen des Erlasses eines Bearbeitungsreglementes für das ZAR ist daher den Kontrollen die nötige Aufmerksamkeit zu schenken. Wir stehen in Kontakt mit dem Bundesamt für Ausländerfragen und behalten uns vor, allenfalls eine entsprechende Empfehlung zu erlassen.

2.4. Höchstzahl Tänzerinnen pro Betrieb

Um Missbräuchen bei der Anstellung ausländischer Tänzerinnen besser entgegenwirken zu können, wurde den kantonalen Fremdenpolizeibehörden im Zentralen Ausländerregister ZAR neu die Funktion "Höchstzahl Tänzerinnen pro Betrieb" zur Verfügung gestellt.

Solange dabei keine Personendaten bekanntgegeben werden, ist hiefür keine Anpassung der ZAR-Verordnung nötig. Wir haben der Aufnahme der erwähnten Funktion zugestimmt. Gleichzeitig haben wir darauf hingewiesen, dass eine Funktion zur Online-Abfrage von "Namenslisten sämtlicher Ausländer pro Betrieb" ohne Anpassung der ZAR-Verordnung unzulässig wäre. Zudem müssten technische Schutzmassnahmen ergriffen werden, falls sich eine generelle Einführung derart weitgehender Datenbearbeitungen im Ausländerrecht nicht von vornherein als verfassungswidrig erwiese (vgl. zu dieser Frage den Bericht über unsere Beschwerde bei der EDSK, S. 16).

2.5. Suchabfragen im ZAR

In vielen Fällen stehen den Behörden, die auf das Zentrale Ausländerregister ZAR greifen wollen, genaue Angaben über die aufzurufende Person zur Verfügung. Insofern erübrigt sich eine Suchabfrage im ZAR.

Das ist etwa der Fall, wenn eine bestehende Aufenthaltsbewilligung verlängert werden muss und die Personenkennung anhand des Dossiers eingegeben werden kann. In anderen Fällen, wo der abfragenden Behörde kein Dossier vorliegt oder wo keine Ausweise vorgezeigt werden, muss mit den vorhandenen, nicht immer hinreichend genauen Angaben gearbeitet werden. Hiefür besteht im ZAR ein eigenes Instrumentarium, das aufgrund von Suchkriterien und programmgesteuerten Mehrfachabfragen auf dem Bildschirm die Abfrage von Daten einer Auswahl von Personen erlaubt, auf welche die Angaben möglicherweise zutreffen. Zu den aufgerufenen Personen können weitere Daten abgerufen werden, welche eine genauere Zuordnung erlauben.

Bei einer Vorführung der Funktion haben wir festgestellt, dass die zur Verfügung stehenden Suchkriterien zum Teil ausserordentlich weit gefasst sind und deshalb die Abfrage einer zu grossen Auswahl von Personen bewirken. Wir haben daher erhebliche Einschränkungen der Suchfunktionen verlangt, welche uns zugesichert wurden. Allgemein geht es darum, denjenigen Behörden, die nicht mittels eindeutigen Personenkennungen auf ihren Dossiers das ZAR abfragen, möglichst präzise Suchkriterien zur Verfügung zu stellen. Dabei sind persönlichkeitsverletzende Suchkombinationen zu vermeiden, selbst wenn sie in einem bestimmten Fall möglicherweise genauer sind als andere Kombinationen. Bei den ZAR-Abfragen der Polizei über RIPOL-Leitungen haben wir keine persönlichkeitsverletzenden Suchkombinationen festgestellt.

2.6. Provisorische Weisungen betreffend die Protokollierung im ZAR

Reichen präventive Massnahmen in einem bestimmten Bearbeitungszusammenhang nicht aus, um unzulässige Zweckentfremdungen mit hinreichender Sicherheit auszu-

schliessen, müssen die Datenbearbeitungen protokolliert werden.

Dies entspricht international anerkannten Sicherheitsanforderungen und wird auch in Art. 10 VDSG vorgeschrieben. In Ausführung dieser Bestimmung erliess das EJPD am 2. November 1994 "Provisorische Weisungen über die Protokollierung über die Abfrage von Daten des Zentralen Ausländerregisters mittels eines Abrufverfahrens". Danach müssen die Bekanntgaben von Daten durch das ZAR mittels RIPOL-Abfragemaske protokolliert werden. Festgehalten werden dabei Amtsbezeichnung, Benutzer und Benutzer-Nummer, Datum und Zeit der Abfrage sowie die verwendeten Suchbegriffe. Das Rechenzentrum des EJPD stellt ein Auswertungsprogramm für die Protokollierungsdatei zur Verfügung und speichert die Protokollierungsdaten während einem Jahr. Die Datenschutzberater des EJPD überprüfen die Protokolle periodisch und klären namentlich ab, ob die jeweiligen Abfragen zur Erfüllung einer gesetzlichen Aufgabe notwendig sind und ob die Daten von unbeteiligten Dritten weiterverwendet werden. Sie erstatten dem Generalsekretariat jährlich Bericht.

Diese Weisungen sind aus datenschutzrechtlicher Sicht zu begrüssen. Sie sollten nunmehr rasch in ein Definitivum überführt werden. Dabei sollte die Gelegenheit zu den sich aus heutiger Sicht aufdrängenden Anpassungen genutzt werden. So fehlen etwa Vorschriften über den Mitarbeiterschutz, was die Akzeptanz der Weisungen herabsetzen dürfte. Auch sollten einige zusätzliche Auswertungskriterien eingefügt werden, um dem gesetzlichen Auftrag wirkungsvoller nachkommen zu können. Bei mehreren Vorf
ührungen der Protokollierung im Rechenzentrum des EJPD hat sich zudem ergeben, dass die Auswertung mit den bis anhin zur Verfügung gestellten Mitteln zeitraubend und mühsam ist. Heute leicht erhältliche Standardlösungen und möglicherweise die in der Betriebssoftware selber bereits vorhandenen Ressourcen werden nicht oder zu wenig genutzt. Wir werden den zuständigen Stellen im EJPD konkrete Vorschläge unterbreiten.

2.7. Papierloses Personendossier-Verwaltungssystem REGI-2

Beim papierlosen Personendossier-Verwaltungssystem REGI-2 des BFA wurden wichtige Datenschutzforderungen erfüllt. Die Dokumente werden so gespeichert, dass sie nicht mehr verändert werden können. Volltextsuchen sind nicht möglich. Die Zugriffsregelung erfolgt anhand standardisierter Indexe, nach denen die einzelnen Dokumente auch aufgesucht werden können. Es wurde ein Bearbeitungsreglement erlassen. Gleichwohl bestehen noch mehrere Datenschutz-Pendenzen, die möglichst rasch erledigt werden sollten.

Auf unsere Empfehlung hin (vgl. 2. Tätigkeitsbericht S. 24 f.) hat das Bundesamt für Ausländerfragen für dieses neue EDV-System ein Bearbeitungsreglement und eine dazugehörende Dokumentation vorgelegt. Aus diesen Unterlagen ergibt sich im Wesentlichen, dass das REGI-2 zur papierlosen Archivierung der in diesem Amt bearbeiteten Personendossiers dient. Dabei werden die einzelnen Dokumente so gespeichert, dass sie nicht mehr verändert und dass darin auch keine Volltext-Suchen durchgeführt werden können. Indessen werden die Dokumente mit einem Indexfeld versehen, welches nach einem vordefinierten Standard vergeben wird. Dieses Indexfeld gestattet ein rasches Auffinden des interessierenden Dokuments und eine aufgabenbezogene Zugriffsvergabe bzw. eine aufgabenbezogene Bekanntgabe mit elektronischen Mitteln an Dritte. Die Datenbearbeitungen werden protokolliert.

Mit der gewählten Lösung sind wichtige datenschutzrechtliche Anforderungen erfüllt worden. Gleichwohl verbleiben einige ungelöste Probleme. So ist unklar, wie, von wem und in welchem Verfahren die in der VDSG vorgeschriebenen periodischen amtsinternen Kontrollen durchzuführen sind. Ebenso wurde offenbar bisher keine Risikobeurteilung durchgeführt. Dies ist mit Blick auf die bearbeiteten besonders schützenswerten Daten und Persönlichkeitsprofile jedoch gesetzlich vorgeschrieben. Zu dieser Risikobeurteilung sind gemäss der Verordnung vom 10. Juni 1991 über den Schutz der Informatiksysteme und -anwendungen in der Bundesverwaltung die Informatik-Sicherheitsspezialisten der Bundesverwaltung beizuziehen. Weil die Ergebnisse dieser Analyse auch für den Datenschutz bedeutsam sein können (Massnahmenkatalog), fehlen uns zur Zeit wichtige Elemente für eine gesamthafte Beurteilung. Wir haben uns deshalb vorerst nur zu formellen Fragen äussern können (Vollständigkeit des Bearbeitungsreglements und der gemäss VDSG verlangten Unterlagen).

2.8. Automatisiertes Personenregistratursystem AUPER-2

In einer Beschwerde an die EDSK haben wir - ähnlich wie beim ZAR - die immer noch ungelösten Probleme beim Zugriff von Polizeistellen auf die Asylbewerberdaten im AUPER und bei der Bearbeitung von Asylbewerberdaten mittels Büroautomation kritisiert. Es geht darum, die Polizeizugriffe auf ein sinnvolles Mass zu reduzieren und die Büroautomationssysteme in eine DSG-konforme Sicherheitsarchitektur einzubinden. Unhaltbar ist, dass heute immer noch die Asylbewerberdaten des Bundesamtes für Flüchtlinge und wesentliche Datenbestände des Bundesamtes für Polizeiwesen in ein und derselben Datenbank des AUPER gespeichert werden. Unabhängig von dieser Beschwerde haben wir klargestellt, dass auch bei der Asylbewerber-Kontoführung durch die PTT eine saubere Trennung von anderen Datenbearbeitungen und eine gute Sicherung der Asylbewerberdaten nötig ist.

Auch bezüglich des AUPER-2 haben wir (wie beim ZAR, vgl. vorne S. 16) der EDSK die Frage des Einsatzes von Büroautomationsmitteln unter Wahrung der Vertraulichkeit der heiklen Asyldaten unterbreitet. Gegenüber dem Zentralen Ausländerregister ZAR stellen sich diese Fragen beim AUPER-2 akzentuiert. Einmal geht es bei der Gewährleistung einer vertraulichen Bearbeitung von Asyldaten auch um die Einhaltung von völkerrechtlichen Verpflichtungen. Die in unserem Land um Asyl nachsuchenden Personen sollen nicht durch Informationspannen weiteren Nachteilen ausgesetzt werden. Solche Informationspannen können in einem vergleichsweise weit verzweigten System, wie es das AUPER darstellt, nicht ausgeschlossen werden, wenn nicht die erforderlichen Anstrengungen für eine in jeder Hinsicht kontrollierte und gesicherte Datenbearbeitung unternommen werden.

In verfahrensrechtlicher Hinsicht gilt es zudem, sogenannte Nachfluchtgründe zu vermeiden. Nachfluchtgründe können entstehen, wenn Informationen über eine Person bekanntgegeben werden, welche die Wahrscheinlichkeit ihrer Verfolgung im Heimatland erheblich vergrössern könnten. Müssen in einigen Fällen anderen als Asylbehörden Online-Zugriffe auf die Asyldaten gewährt werden, weil sich diese Zugriffe zur Aufgabenerfüllung als absolut notwendig erweisen, ist diesen Behörden die Weitergabe der erhaltenen Daten verboten und die Einhaltung dieses Verbots mit technischen Vorkehren zu gewährleisten. Zudem sind die Suchvorgänge auf ein sinnvolles Mass zu beschränken.

Datenbearbeitungen müssen als unverhältnismässig bezeichnet werden, wenn bei der gewählten Bearbeitungsmethode von vornherein in Kauf genommen wird, dass bei jeder Bearbeitung die Daten einer Vielzahl unbeteiligter Dritter "mitbearbeitet" werden, obwohl sich dies mit einem vertretbaren Aufwand vermeiden liesse. Die heute im AUPER-2 eingerichtete Suchfunktion für die Polizeistellen des Bundes (und wohl auch der Kantone) genügt den Anforderungen des DSG nicht.

In die gleiche Richtung zielte auch unser Vorbringen bei der EDSK, wonach die im AUPER-2 gespeicherten Asyldaten von den in der gleichen Datensammlung gespeicherten Polizeidaten des Bundesamtes für Polizeiwesen (BAP) zu trennen sind, was leider immer noch nicht geschehen ist (vgl. 1. Tätigkeitsbericht S. 27 f. und 30 f. und 2. Tätigkeitsbericht S. 24 ff.). Heute erhält unter Umständen ein Sachbearbeiter des BAP bei der Abfrage von Polizeidaten des BAP im AUPER ungewollt auch eine unbestimmte Anzahl von Asyldaten "mitgeliefert", was als absolut unhaltbar bezeichnet werden muss. Wir haben mit allem Nachdruck darauf hingewiesen, dass dieser bedauerliche Fehler im System, den wir schon früher kritisierten, nunmehr raschestmöglich behoben werden muss. Es bleibt zu hoffen, dass das hängige Verfahren vor der EDSK sowie die parallel dazu verlaufende Risikobeurteilung von Datenbearbeitungen im BFF und im BAP, welche zur Zeit in Zusammenarbeit mit dem BFI und einer schweizerischen Universität erfolgt, diese datenschutzrechtliche Muss-Forderung einer Lösung zuführen wird. Dabei ist auch *das Rechenzentrum des EJPD einzubeziehen*, welches übergreifend die Voraussetzungen für eine datenschutzrechtskonforme Lösung zu schaffen hat.

2.9. Konto für Sicherheitsleistungen der Asylbewerber ("Sicherheitskonto")

Gemäss Asylverordnung 2 müssen Asylbewerber einen bestimmten Anteil ihres Erwerbseinkommens in der Schweiz zur Sicherung allfälliger Fürsorgeleistungen oder Rückführungsmassnahmen in einem Konto hinterlegen, das zur Zeit von den schweizerischen PTT-Betrieben in Zusammenarbeit mit dem Bundesamt für Flüchtlinge (BFF) geführt wird. Dabei entstehen zahlreiche Datenflüsse zwischen den beiden Bundesorganen.

In einer Empfehlung haben wir verlangt, dass ein übergreifendes Sicherheitskonzept mit einem objektbezogenen Massnahmenkatalog für den Austausch und für die Bearbeitung der sensiblen Asylbewerber-Daten bei den PTT sowie ein Bearbeitungsreglement gemäss VDSG erstellt werden. Weiter haben wir in der Empfehlung verlangt, dass die heiklen Asylbewerber-Daten chiffriert übermittelt und bei den PTT von den dort vorhandenen anderen Daten logisch und physisch getrennt bearbeitet werden. An einer gemeinsamen Sitzung mit allen beteiligten Stellen am 28. April 1995 wurde die Empfehlung angenommen. Danach unterbreiten die Informatik-Sicherheitsspezialisten des BFI Vorschläge für die Chiffrierung und das BFF, die PTT und das BFI erarbeiten im Rahmen der beim BFF hängigen Risikobeurteilung und in Zusammenarbeit mit einer schweizerischen Universität einen objektbezogenen Massnahmenkatalog. BFF und PTT erlassen gestützt hierauf ein Bearbeitungsreglement.

2.10. Liegenschafts- und Fürsorgekostenabrechnungssystem LIFAS

Bei einer Besprechung des Vorprojekts für dieses neue EDV-System Ende 1994 hatten wir die verantwortlichen Stellen darauf hingewiesen, dass aus datenschutzrechtlicher Sicht eine möglichst "personenunabhängig" geführte Buchhaltung angestrebt werden sollte. In der Zwischenzeit hat sich der Bundesrat für das Modell einer weitgehend pauschalen Kostenabrechnung mit den Kantonen entschieden, was nicht nur eine Vereinfachung der Buchführung, sondern auch eine "Entschärfung" der Datenschutzprobleme mit sich bringt. Zudem wurde der Fürsorgeteil aus dem Projekt ausgeklammert, so dass keine besonders schützenswerten Gesundheits- und Fürsorgedaten anfallen werden. Das definitive Projekt wird uns zu gegebener Zeit vorgestellt werden.

2.11. Revision des Ausländer- und des Asylgesetzes

Bei diesen Gesetzesrevisionen schlägt der Bundesrat den eidgenössischen Räten auch die Aufnahme von Datenschutzbestimmungen vor. Damit werden - wie es das DSG vorsieht - die wichtigsten Datenbearbeitungen, ihre Zwecke und ihr Umfang sowie der Schutz vor unerlaubten Datenbearbeitungen im Gesetz selber umschrieben. Zwei Differenzen zum bundesrätlichen Entwurf betreffen den Umfang der Online-Zugriffe und den Umfang der Bearbeitung von Fingerabdrücken nichtkrimineller Personen.

In die Berichtperiode fiel die Verabschiedung der Revision des Ausländer- und des Asylgesetzes durch den Bundesrat zu Handen der eidgenössischen Räte. In die Revisionsvorlagen aufgenommen wurden auch die gemäss DSG erforderlichen Bestimmungen über die Datenbearbeitung und den Datenschutz. Die Zusammenarbeit zwischen Verwaltung und EDSB darf als gut bezeichnet werden. Wie im ersten und zweiten Tätigkeitsbericht dargelegt (1. Tätigkeitsbericht S. 30ff. und 2. Tätigkeitsbericht S. 26f.), haben wir schwerpunktmässig folgende Anliegen unterbreitet: Eine hinreichende Umschreibung der Bearbeitungen besonders schützenswerter Personendaten namentlich mittels Abrufverfahren sowie der Bearbeitungszwecke; eine sorgfältige Prüfung der vorgesehenen Datenbearbeitungs-Vorschriften unter dem Blickwinkel der Verhältnismässigkeit/Erforderlichkeit und der Rechtsgleichheit; eine hinreichende Umschreibung spezifischer Schutzmassnahmen, insbesondere des Schutzes unbeteiligter Dritter bei polizeilichen Datenbearbeitungen und des Grundsatzes der separaten Aufbewahrung der Asyldaten von den Polizeidaten; ferner eine hinreichende Umschreibung des Schutzes vor unzulässigen Übermittlungen von Asyldaten ins Ausland und in den Heimatstaat, insbesondere die genaue Umschreibung der (ausnahmsweise) zulässigen Übermittlungen und der Pflicht zur einzelfallweisen Güterabwägung *vor* der Übermittlung; eine Beschränkung der Bearbeitung von Fingerabdrücken auf das absolut Notwendige durch den Gesetzgeber.

Erfreulicherweise konnten die meisten dieser wichtigen Anliegen in der einen oder anderen Form bei der gesetzgeberischen Arbeit berücksichtigt werden. Die verbleibenden Differenzen betreffen folgende Fragen: Anzahl der Behörden, die zur Aufgabenerfüllung wirklich einen Online-Zugriff auf die zentralen Ausländer- und Asyldatensammlungen benötigen und denen die erforderlichen Daten nicht auf andere Weise (einzelfallweise oder paketweise und u.U. anonymisiert) bekanntgegeben werden können; Regel, dass bei der Einreise in unser Land grundsätzlich *allen* Asylbewerbern die Fingerabdrücke abgenommen werden müssen, so dass auf unter-

schiedliche Verhältnisse nicht oder zu wenig Rücksicht genommen werden kann; Dauer der Aufbewahrung der im System gespeicherten Daten nach Abschluss eines ausländer- oder asylrechtlichen Verfahrens. Wir sehen den vom Parlament in diesen wichtigen Fragen zu treffenden Entscheiden mit grossem Interesse entgegen.

Staatsverträge mit Deutschland und Kroatien
Ein erstes Abkommen mit Deutschland, welches am 27. November 1995 unterzeichnet wurde, betrifft den *einmaligen Abgleich von 3000 Fingerabdruckblättern von Asylbewerbern* der deutschen Behörden aus dem Jahr 1993 mit der schweizerischen, EDV-gestützten Fingerabdruck-Datensammlung AFIS. Der einmalige Abgleich erfolgt nach dem Wortlaut des Abkommens ausschliesslich zu statistischen Zwecken und soll über die vermutete Tendenz näheren Aufschluss geben, wonach Asylbewerber gleichzeitig in verschiedenen Ländern Asylgesuche einreichen.
Wir haben uns bei unserer Stellungnahme auf rein datenschutzrechtliche Gesichtspunkte beschränkt, welche im Abkommen vollumfänglich berücksichtigt wurden. Im einzelnen gilt soweit hier interessierend Folgendes: Die deutschen Daten dürfen nicht im AFIS gespeichert werden; sie werden paketweise elektronisch in einen Arbeitsspeicher eingelesen und nach dem Abgleich eines Pakets sogleich wieder gelöscht. Allfällige "Treffer" bzw. Übereinstimmungen werden der Asylbehörde *nicht* mitgeteilt, sondern anonym ausgewertet. Der Abgleich wird von den mit dem Betrieb des AFIS betrauten Beamten des BFF, nicht aber von den für das Asylverfahren zuständigen Beamten durchgeführt. Der EDSB überwacht den Abgleich, der ihm vorgängig gemeldet wird. Die Fingerabdruckblätter werden gut gesichert in die Schweiz versandt und gelangen nach dem Abgleich wieder an die zuständige deutsche Behörde (wir hätten uns auch eine sofortige Vernichtung der Papierkopien nach dem Abgleich in der Schweiz vorstellen können).

Schliesslich wurde uns der Entwurf zu einem Durchbeförderungsabkommen mit Kroatien unterbreitet, welches den formellen datenschutzrechtlichen Anforderungen entspricht. Wir haben die zuständigen Stellen im EJPD auf mögliche Umsetzungsprobleme hingewiesen und unsere Zustimmung von einer periodischen Orientierung und unserer Beiziehung in kritischen Fällen abhängig gemacht. Gleichzeitig haben wir die Ergänzung der im Visumabkommen von 1993 enthaltenen Rückübernahmeklausel im Sinne des DSG und des Durchbeförderungsabkommens angeregt.

3. Telekommunikation

3.1. Internet - Die Datenschutzleitplanken auf dem Datahighway sind noch butterweich

Wenn sich auch bei einzelnen Benutzern, nicht zuletzt wegen den zeitweiligen Netzüberlastungen, bereits eine gewisse Ernüchterung einstellt, ging die rasante Entwicklung des Internet im Berichtsjahr ungebrochen weiter. Mit einem geschärften Bewusstsein für die Auswirkungen der Netzaktivitäten und geeigneten Massnahmen können die nach wie vor beträchtlichen Datenschutzrisiken eingeschränkt werden.

Das Internet ist - wie heute beinahe allgemein bekannt - der grösste weltweite Verbund von Computernetzen. Doch es ist mehr als nur einfach ein Netz von Netzen: das Internet bildet mit seinen Benutzern einen Kommunikationsraum, der nicht untreffend etwa als «global village» bezeichnet wird, als Dorf also, in dem sich die Ein-

wohner elektronische Post und ganze Dateien zusenden, via elektronische Anschlagbretter diskutieren, alle erdenklichen Informationen zum Abruf zur Verfügung stellen, Produkte und Dienstleistungen anbieten, für ihre Interessen werben usw.
Das Internet kann als die erste realisierte Stufe, sozusagen als Hauptschlagader der «Global Information Infrastructure» betrachtet werden.

Die Wurzeln des heutigen Internet reichen zurück in die sechziger Jahre, als das US-Verteidigungsministerium ein Datennetz realisierte, das so konzipiert war, dass es unmöglich sein sollte, das Netz mit einer gezielten punktuellen Zerstörung ausser Gefecht zu setzen. Später fand das Netz bei Universitäten, Forschungseinrichtungen und Behörden Verbreitung. Immer mehr Teilnehmer erkannten den Nutzen der durch das Netz gebotenen Kommunikationsmöglichkeiten, sodass sich immer mehr Institutionen in immer mehr Ländern ankoppelten. Ein regelrechter Boom setzte ein. Von einer breiteren Öffentlichkeit wurde das Internet erst anfang der neunziger Jahre wahrgenommen, als sich vermehrt Firmen anschlossen und bald auch die Möglichkeit bestand, mit dem heimischen PC an der globalen Kommunikation teilzunehmen.

Das Internet bietet den Benutzern, seien sie Informationsanbieter oder -bezüger, als modernes interaktives Kommunikationsmittel enorme Vorteile. Rasch und zu niedrigen Verbindungskosten können Informationen stets aktuell zur Verfügung gestellt werden und weltweit jederzeit abgerufen werden. Für alle erdenklichen Interessensgebiete finden sich Datenmaterial und Diskussionspartner; kaum ein anderes Medium ermöglicht einen derart freien weltweiten Meinungsaustausch.

Wie oben erwähnt, waren die Nutzer das weltweiten Computernetzes bis vor einigen Jahren zum grossen Teil Wissenschafter und Mitarbeiter in Behörden, Universitäten und Forschungsstätten. Der Datenaustausch erfolgte gewissermassen unter Insidern, unter denen ein weitgehendes kollegiales Vertrauensverhältnis herrschte.
Damit ist es nun endgültig vorbei. Durch den Internet-Boom, ausgelöst durch vielfältige Angebote und leicht bedienbare graphische Benutzeroberflächen, die in ihrer Funktionalität dauernd weiterentwickelt werden, ist das Netz nun für breite Kreise attraktiv geworden.
Die Benutzer haben sehr unterschiedliche Möglichkeiten und Motivationen, sich der Internet-Dienste zu bedienen. Da das frühere gegenseitige Vertrauen unter den Netzteilnehmern und damit eine weitgehende Selbstregulierung abnimmt, treten auch Schattenseiten unserer Gesellschaft im Netz in Erscheinung. Dadurch hat es das Internet in den Medien - teilweise auch durch Übertreibung der Zustände - bisweilen zu zweifelhafter Berühmtheit gebracht.
Zu Diskussionen Anlass gegeben haben insbesondere ungeklärte Fragen des Urheberrechts, generell die Publikation von in Papierform verbotenen Schriften (z.B. des Buches «Le Grand Secret» in Frankreich), die Verbreitung von pornographischem Material in Form von Text, Bild und Ton, die Verbreitung von volksverhetzender politischer Propaganda, die Veröffentlichung von Anleitungen zum Begehen von Straftaten u.s.w.

Unerwünschte Aktivitäten sind mit den gegenwärtigen, weitgehend auf nationale Territorien beschränkten Rechtssystemen, nicht mehr adäquat zu erfassen. Häufig weiss der Benutzer nicht einmal, in welchem Staat die Daten, die er gerade abruft, gespeichert sind.
Da bei der Benutzung des Netzes Personendaten anfallen, die in beträchtlichem Masse auch als Inhaltsdaten übermittelt werden, ergeben sich Datenschutzrisiken für die betroffenen Personen:

Zugang zum Internet bieten sogenannte Service-Provider. Konnte ihre Zahl vor kurzer Zeit noch an einer Hand abgezählt werden, sind heute über dreissig Firmen von unterschiedlicher Grösse und Angebotspalette auf dem schweizer Markt tätig. Auch Online-Dienste, wie Compuserve, America Online, Swiss Online (Videotex) etc. bieten ihren Kunden mittlerweile neben ihren eigenen Angeboten auch Zugriff zum Internet an.
Dem Provider ist es technisch möglich, das Kommunikationsverhalten seiner Kunden (von denen er aufgrund der Geschäftsbeziehung zusätzliche Daten kennt) weitgehend zu erfassen. Er kann feststellen, zu welchen Zeiten ein Benutzer im Netz aktiv ist, welche Dienste er nutzt, mit welchen andern Internetbenutzern er elektronisch in Kontakt tritt sowie welche Informationen er von welchen Servern abruft. In diesem Zusammenhang ist die Entstehung von Persönlichkeitsprofilen - d.h. Zusammenstellungen von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben - möglich. Die Bearbeitung von Personendaten ist jedoch lediglich in dem Masse statthaft, wie es für die Aufgabenerfüllung (Abrechnung etc.) des Providers notwendig ist.
Der Kunde sollte über die vom Provider getroffenen technischen und organisatorischen Massnahmen informiert werden, damit er die Risiken möglichst gut einschätzen und sein Verhalten anpassen kann.

Der Benutzer kann den Datenschutz mit folgenden (nicht abschliessenden) Massnahmen und Verhaltensweisen erheblich verbessern:

- Wer Personendaten (eigene oder von Drittpersonen) ins Netz einzuspeisen beabsichtigt, hat sich über die Konsequenzen im Klaren zu sein. Beispielsweise sind die im Internet auftauchenden elektronischen Fragebogen oft sehr umfangreich und erfragen sensible Daten. Sie sollten mit grosser Vorsicht und Zurückhaltung ausgefüllt werden.
- Durch die enormen im Internet zugänglichen Datenmengen ist das Problem der Verknüpfbarkeit besonders aktuell. Mehrere unabhängige Bestände von Personendaten (z.B. Verzeichnisdienste) können zusammengeführt, systematisch ausgewertet und abgespeichert werden, was für die betroffenen Personen nicht abschätzbare Risiken bergen kann. Die öffentlich zugänglichen Internet-Daten können mit sehr leistungsfähigen sogenannten Suchmaschinen durchforstet werden. Sind die Personendaten einmal im Netz verfügbar, hat der Betroffene kaum mehr eine Kontrolle über die Verwendung.
- Das Internet kennt keine nationalen Grenzen: Es ist zu bedenken, dass Personendaten in Länder fliessen können, die lediglich geringere oder überhaupt keine Datenschutzbestimmungen kennen.
- Gute Chiffrierverfahren sind heute allgemein verfügbar und sollten auf jeden Fall dann eingesetzt werden, wenn besonders schützenswerte Personendaten oder Persönlichkeitsprofile übertragen werden (z.B. per E-Mail und Filetransfer). Weiter ist es möglich, mit elektronischen Unterschriftsverfahren die Integrität der übertragenen Daten sowie die Authentizität des Absenders zu prüfen.
- Viele Firmen, aber auch Verwaltungen, wollen vom Informations- und Kommunikationspotential profitieren, das ihnen das Internet eröffnet. Sie haben daher vermehrt das Bedürfnis, ihre eigenen internen Netze ans Internet anzukoppeln. Um die internen Daten vor unberechtigtem Zugriff von aussen zu schützen, ist jegliche Kommunikation zwischen den beiden Netzen über einen Zwischenrechner (sog. Firewall) zu führen. Dort wird die Zugriffsberechtigung überprüft. Eine Protokollierung ermöglicht die rasche Erkennung potentieller Angriffe.

Im übrigen haben die Internet-Teilnehmer in der Schweiz die Bestimmungen des DSG einzuhalten. Die in der Verordnung zum DSG aufgeführten technischen und organisatorischen Massnahmen sind umzusetzen.

Eine kommerzielle Nutzung (direkte Bestellung, Bankgeschäfte etc.) des Internet in grösserem Stil ist ohne umfassende Sicherheitsmechanismen undenkbar. Diese sind auch dem Datenschutz sehr dienlich. Bereits sind zahlreiche Lösungen für bestimmte Anwendungen verfügbar. Das künftige «Internet Protocol Next Generation (IPng)» wird bereits Sicherheitsdienste enthalten.

Ausserdem ist zu prüfen, ob die am Internet-Kommunikationsprozess Beteiligten sich in einem Ehrenkodex auf Einhaltung eines für ihren Einflussbereich bestimmten Datenschutz-Minimalstandards verpflichten könnten. Die Massnahmen dürfen aber keinesfalls zu einer Zensur des freien Datenflusses ausarten; es geht vielmehr darum, bestimmte Verkehrsregeln aufzustellen, die einer missbräuchlichen Verwendung des Netzes Einhalt gebieten.

3.2. Die Revision des Fernmeldegesetzes

Im Hinblick auf die Aufhebung der letzten Monopole des Telekommunikationssektors im europäischen Raum wurde die Revision des PTT-Organisationsgesetzes sowie des Fernmeldegesetzes an die Hand genommen. Im Rahmen der Ämterkonsultation nahmen wir dazu Stellung.

Bis spätestens 1998 werden im europäischen Raum die noch verbleibenden Monopole der nationalen Telekomgesellschaften abgeschafft. Damit die Telecom - PTT konkurrenzfähig bleibt, wird auch ihr Monopol aufgehoben. Der dann freiwerdende Markt soll durch eine Revision des Fernmeldegesetz (FMG) an einheitliche Bedingungen geknüpft werden.

In der ersten Ämterkonsultation konnten wir mit der federführenden Stelle einige bestehende Differenzen bezüglich des Entwurfes begleichen. Wir hatten vertreten, dass Regelungen über die Verwendung der Daten über den Fernmeldeverkehr, die Identifikation des anrufenden Anschlusses sowie die Sicherheit der Fernmeldedienste gegen unbefugte Abhörung und Eingriffe in das Gesetz aufgenommen werden sollten. Mit dem Argument, es handle sich um ein Marktgesetz wurde diese Forderung abgelehnt. Man konnte sich jedoch darauf einigen, dass im Gesetz der Bundesrat verpflichtet werden soll, insbesondere für diese Punkte Regelungen zu schaffen.

Für zwei andere Bereiche konnte jedoch keine Einigung erzielt werden.

Die PTT vertraten die Ansicht, dass aus Gründen der Qualitätssicherung ein Aufzeichnen und Abhören von Funksprüchen und Telefongesprächen erforderlich sei. Da hierbei Gesprächsinhalte aufgezeichnet werden, führt das zu weitreichenden Eingriffen in das Fernmeldegeheimnis und damit in die Persönlichkeit. Wir sind der Ansicht, dass für derartige Massnahmen im Gesetz die einzelnen Voraussetzungen aufzulisten sind. Desweiteren kann die Aufzeichnung und Überwachung von Gesprächsinhalten nur zulässig sein, wenn im Gesetz ein Bewilligungsverfahren festgelegt wird. Das Bewilligungsverfahren muss zumindest vorsehen, dass nach einem bestimmten Zeitraum die Überwachung einer höheren Instanz zur Bewilligung vorzulegen ist. Auch die Dauer der Massnahme und die Häufigkeit der Wiederholungen

sind zu regeln.

Desweiteren vertraten wir im Zusammenhang mit den detaillierten Taxauszügen die Ansicht, dass grundsätzlich an der im heutigen FMG bestehenden Regelung festzuhalten ist. Diese statuiert, dass nur die Ortszentralen bekanntgegeben werden dürfen, während die letzten Stellen der angewählten Abonnentennummer fehlen. Es sollten jedoch Ausnahmeregelungen für Beweiszwecke in einem hängigen Verfahren sowie für die Glaubhaftmachung eines schutzwürdigen Interesses durch den Kunden geschaffen werden.

3.3. Das neue Postverkehrsgesetz

Die Aufhebung des Monopols der PTT-Betriebe im Telekommunikationsbereich führt auch zu einer Veränderung der Stellung der Post auf dem Markt. Um diesen Änderungen Rechung zu tragen, muss das bestehende Postverkehrsgesetz revidiert werden. Im Rahmen der ersten Ämterkonsultation haben wir Stellung genommen.

Nach den uns vorgelegten Entwürfen soll die Post über eine Zwitterstellung verfügen. So sollen die Tätigkeitsbereiche der Post in Universaldienst und Wettbewerbsdienst aufgeteilt werden. Der Universaldienst wird in reservierte und nicht reservierte Dienste unterteilt. Es ist vorgesehen, dass die Post die nicht reservierten Dienste des Universaldienstes sowie die Wettbewerbsdienste in Konkurrenz zu privaten Anbietern erbringt. Demgegenüber verbleibt der reservierte Dienst des Universaldienstes im Monopol der Post. Somit verbleibt der Post das ausschliessliche Recht, adressierte Briefpostsendungen und Pakete bis 2 kg zu befördern. Postsendungen über 2 kg würde die Post in Konkurrenz zu privaten Anbietern befördern.

Aus der Unterscheidung zwischen reserviertem und nicht reserviertem Universaldienst bei den Postsendungen folgt, dass für die Bearbeitung der Kundendaten unterschiedliche Datenschutzbestimmungen Anwendung finden. Für das Bearbeiten von Daten von Kunden, die Postsendungen bis zu 2 kg durch die Post zustellen lassen, finden die Bestimmungen des DSG über das Bearbeiten durch Bundesorgane Anwendung. Verschickt dagegen ein Kunde ein Paket mit einem höheren Gewicht, so finden die Bestimmungen des DSG für die Bearbeitung durch Private Anwendung.
Eine Differenzierung der anzuwendenden Bestimmungen anhand des Gewichtsunterschiedes - ist die Postsendung noch 2 kg schwer oder bereits 2,1 kg - ist kaum praktikabel. Auch aufgrund der Tatsache, dass sich die Rechtsbeziehungen zwischen der Post und ihren Kunden neu nach Privatrecht richten sollen, hat man sich darauf geeinigt, für das Bearbeiten von Kundendaten die Bestimmungen des DSG über das Bearbeiten von Personendaten durch Privatpersonen für anwendbar zu erklären. Hingegen soll sich die Aufsicht nach den Bestimmungen für Bundesorgane richten.

Differenzen bestanden bezüglich der inhaltlichen Anforderungen der Regelung. Wir hatten gefordert, dass auf Gesetzesebene Regelungen geschaffen werden müssten:
- über die Weitergabe von Kundendaten an Dritte;
- über das Recht der Kunden, die Weitergabe der Daten zu untersagen;
- über das Recht der Kunden, nach vorheriger Information das Bearbeiten von Daten, die nicht für die Vertragserfüllung notwendig sind, zu untersagen.

Wie beim Entwurf für das Fernmeldegesetz hat man sich auch hier darauf geeinigt, dass die Einzelheiten nicht im Gesetz, sondern vom Bundesrat auf Verordnungsebene zu regeln sind.

3.4. Rechtsgrundlage für das Bereitstellen von Mitarbeiter-Daten durch die Bundesverwaltung im Abrufverfahren

Immer mehr Arbeitgeber gehen dazu über, Angaben über ihre Mitarbeiter elektronisch oder auf andere Weise zum Abruf zur Verfügung zu stellen. Auch in der Bundesverwaltung nimmt diese Tendenz zu.

Auch in der Bundesverwaltung nimmt der Wunsch der Organisationseinheiten zu, Angaben über ihre Mitarbeiter etwa im X.500-Directory oder im WWW im INTERNET zum Abruf zur Verfügung zu stellen.

Das DSG verlangt für das Zugänglichmachen von Personendaten im Abrufverfahren eine ausdrückliche Rechtsgrundlage, für besonders schützenswerte Personendaten und Persönlichkeitsprofile sogar eine Rechtsgrundlage in einem formellen Gesetz. Dieses Erfordernis wurde unsererseits mit dem Bundesamt für Informatik (BFI) im Zusammenhang mit dem Pilotprojekt X.500 sowie mit der Bundeskanzlei, welche den Staatskalender im Abrufverfahren zur Verfügung stellen will, diskutiert. Das BFI rief eine Arbeitsgruppe ins Leben, deren Ziel die Ausarbeitung einer genügenden Rechtsgrundlage ist. In der Arbeitsgruppe sind die Bundeskanzlei, das BFI und wir vertreten. Diese Arbeitsgruppe soll eine für die gesamte Bundesverwaltung gültige Rechtsgrundlage ausarbeiten.

Dabei stellte sich die Frage, welche Personendaten zu welchen Zwecken in Abrufverfahren zugänglich gemacht werden dürfen. Die Angaben sollen die Kommunikation mit den Staatsangestellten erleichtern. Dementsprechend sind wir der Auffassung, dass nur diejenigen Angaben bekanntgegeben werden dürfen, die für die Herstellung der Kommunikation mit dem betreffenden Mitarbeiter erforderlich sind. Allenfalls könnten auf Wunsch des einzelnen Mitarbeiters weitergehende Daten aufgenommen werden, sofern sich dies auf Angaben beschränkt, die in unmittelbarem Zusammenhang mit seiner Aufgabenerfüllung stehen.

3.5. Meldung von Postfachadressen an städtische Einwohnerkontrolle durch die PTT

Die PTT- Betriebe gaben bis vor kurzem regelmässig Namen und Adressen jener Postkunden an die Einwohnerkontrolle der Stadt Bern bekannt, die ein Postfach eröffneten oder aufgaben. In diesem Zusammenhang stellte sich die Frage nach der Zulässigkeit der Bekanntgabe.

Durch die regelmässige Weitergabe mittels Mutationslisten erhielt die Einwohnerkontrolle nach dem uns bekannten Sachverhalt auch die neuen Postfachadressen von Personen, die zwar in der Stadt wohnten, sich jedoch nicht bei der Einwohnerkontrolle angemeldet hatten, sowie von Personen, die nicht in der Stadt Bern wohnten.

Für die Bekanntgabe von Personendaten wie neuen und geänderten Postfach-

adressen durch ein Bundesorgan bedarf es einer Rechtsgrundlage. Gemäss der Verordnung zum Postverkehrsgesetz dürfen die PTT-Betriebe den Absendern auf Verlangen Adressänderungen von Empfängern gegen eine in den Ausführungsbestimmungen festzusetzende Taxe mitteilen. Adressänderungen dürfen mithin nur an die Absender einer Postsendung bekanntgegeben werden, wenn der Empfänger bereits über eine Postzustelladresse verfügt, die sich jedoch in der Zwischenzeit geändert hat.
Mit den Mutationslisten erhielt die Einwohnerkontrolle auch Postfachadressen von Personen, die nicht in der Stadt Bern wohnen und somit nicht bei der Einwohnerkontrolle gemeldet sind. Für diese Personen verfügte die Einwohnerkontrolle nicht bereits über eine Postzustelladresse. Die betreffende Bestimmung in der Verordnung zum Postverkehrsgesetz konnte somit nicht als Rechtsgrundlage für die Weitergabe dieser Daten herangezogen werden.

Die Weitergabe von Postfachadressen von Personen, die nicht bei der Einwohnerkontrolle gemeldet sind, ist somit unzulässig.

3.6. Elektronische Post und Verzeichnisdienste

Der EDSB hatte 1995 Gelegenheit auf zwei Arbeitsplätzen ein mit Sicherheitsfunktionen versehenes Mailsystem sowie einen Verzeichnisdienst der Bundesverwaltung zu testen.

Die elektronische Post (E-Mail) wird heute in vielen Firmen und Behörden als flexibles und effizientes Kommunikationsmittel rege genutzt. Normalerweise werden kaum Sicherheitsfunktionen implementiert, sodass nicht ausgeschlossen werden kann, dass die übertragenen Meldungen unbefugt gelesen oder auch verändert werden können. Weiter können falsche Kommunikationspartner vorgetäuscht werden.
Immer populärer werden Verzeichnisdienste, die es ermöglichen, Kommunikationsadressen, sowie allenfalls weitere Angaben über potentielle Kommunikationspartner abzurufen.

Anlässlich eines mehrmonatigen Testbetriebs eines Mailsystems mit Verzeichnisdienst des Bundesamtes für Informatik konnte sich der EDSB überzeugen, dass Produkte verfügbar sind, die es erlauben, folgende Sicherheitsfunktionen (basierend auf kryptographischen Methoden) zu nutzen:
- Vertraulichkeit der Nachricht auf dem Übertragungsweg
- Integrität der Nachricht, d.h. keine unbefugte Abänderung
- Überprüfbarkeit der Authentizität des Erstellers der Nachricht (elektronische Unterschrift)

Wie wir feststellen konnten, sind die heute allgemein in der Büroautomation verwendeten Rechner genügend leistungsfähig, um die Ver- und Entschlüsselung der elektronischen Meldungen ohne nennenswerte Verzögerungen auszuführen. Zudem sind die Anwendungen einfach zu bedienen.

Die erwähnten Sicherheitsfunktionen können nur verwendet werden, wenn Sender *und* Empfänger mit der entsprechenden Ausrüstung versehen sind, insbesondere muss das Schlüsselmanagement geregelt sein (Stichwort: Trusted Third Party).

4. Personalwesen

Privatbereich

Gemäss Art. 328b OR darf der Arbeitgeber Personendaten über die Arbeitnehmer nur bearbeiten, soweit sie deren Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind (vgl. zu dieser Thematik auch den 1. Tätigkeitsbericht, S. 53 ff. und den 2. Tätigkeitsbericht, S. 44 ff.):

4.1. Führen von Listen mit privaten Adressen der Mitarbeiter

Der Arbeitgeber darf nur dann eine allen Mitarbeitern zugängliche Liste mit den privaten Adressen der Mitarbeiter führen, wenn dies für die Arbeit unumgänglich ist.

Eine Privatperson hat sich bei uns erkundigt, ob der Arbeitgeber eine Liste mit den privaten Adressen der Mitarbeiter führen und diese Liste den anderen Mitarbeitern zugänglich machen darf. Er darf dies nur, wenn es für die Arbeit notwendig ist, zum Beispiel, weil immer wieder Angestellte privat kontaktiert werden müssen. Ebenso darf der Arbeitgeber die Liste den anderen Angestellten nur zur Verfügung stellen, wenn dies für die Arbeit wirklich notwendig ist. Wenn es aber genügt, dass zum Beispiel die Zentrale die Angestellten privat erreichen kann, so darf der Arbeitgeber die Liste nur an die Zentrale abgeben. Wenn die privaten Adressen der Angestellten für die Arbeit überhaupt nicht benötigt werden, so darf der Arbeitgeber keine solche Adressliste erstellen.

4.2. Überprüfung akademischer Titel durch den Arbeitgeber

Eine kantonale Universität, das Bundesamt für Gesundheitswesen und die Schweizerische Rektorenkonferenz können und müssen auf eine Anfrage eines Arbeitgebers bezüglich der Überprüfung des Berufsabschlusses einer bei ihm angestellten Ärztin verschieden reagieren, da sie unterschiedlichen gesetzlichen Bestimmungen Anwendung unterstehen.

Ein Arbeitgeber, der in seinem Betrieb eine Ärztin beschäftigt, wollte sich vergewissern, ob die von der Ärztin bei der Anstellung gemachten Angaben betreffend ihren Berufsabschluss zutreffend seien. Zu diesem Zweck gelangte er nacheinander an die Ausbildungsstätte, eine kantonale Universität, welche ihm die Auskunft ohne von der betroffenen Person unterzeichnete Einwilligungserklärung verweigerte; an das Bundesamt für Gesundheitswesen, welches die Anfrage nur auf schriftlichen Antrag mit Begründung beantworten wollte und an die Schweizerische Rektorenkonferenz, welche die gewünschte Auskunft bereitwillig telefonisch erteilte. Der Arbeitgeber war von diesen unterschiedlichen Reaktionen sehr befremdet und bat uns um Stellungnahme.

Die unterschiedlichen Reaktionen auf das Auskunftsgesuch des Arbeitgebers erklären sich daraus, dass die verschiedenen auskunfterteilenden Stellen verschiedenen gesetzlichen Bestimmungen unterworfen sind. Die Universität ist als kantonale Lehranstalt dem kantonalen Datenschutzgesetz unterworfen, während das Bundesamt für Gesundheitswesen den Bestimmungen des Datenschutzgesetzes über Bundesorgane untersteht und die Schweizerische Rektorenkonferenz den Bestimmungen des Datenschutzgesetzes über private Personen unterworfen ist. Die Überprüfung

der Auskunfterteilung, bzw. -verweigerung durch die Universität lag demnach nicht in unserem Kompetenzbereich. Hingegen konnten wir feststellen, dass die Reaktion des Bundesamtes für Gesundheitswesen den diesbezüglichen Bestimmungen in der Medizinalprüfungsverordnung entsprach und somit korrekt war. Inwiefern die Auskunfterteilung durch die Schweizerische Rektorenkonferenz zulässig war, liess sich aufgrund der vorliegenden Angaben nicht beurteilen. Es hätte im Einzelfall überprüft werden müssen, ob durch die Datenbekanntgabe keine Verletzung der Persönlichkeit der betroffenen Person erfolgt war. Dies ist jedoch Sache des Zivilrichters. Sie verstiess aber auf jeden Fall nicht grundsätzlich gegen die Bestimmungen des DSG für Datenbearbeitungen durch private Personen.

4.3. Bekanntgabe von Lohndaten an ausländische Steuerbehörden

Art. 328b OR steht einer Datenbekanntgabe durch eine Zweigniederlassung in der Schweiz an den Hauptsitz im Ausland nicht entgegen, wenn sie zur Erfüllung gesetzlicher Pflichten des Hauptsitzes nach dem Recht des betreffenden Landes erforderlich ist.

Die belgischen Steuerbehörden verlangten von einer Firma mit Hauptsitz in Belgien und Niederlassung in der Schweiz Auskünfte über ihre Angestellten in der Schweiz. Sie verlangten namentlich eine Liste mit den Namen der Grenzgänger und den an diese bezahlten Löhnen, um der deutschen und der französischen Steuerverwaltung im Zusammenhang mit der Abklärung von Doppelbesteuerungsfragen Auskünfte erteilen zu können.

Nachdem geklärt war, dass die in Frage stehenden Arbeitsverträge nach dem Bundesgesetz über das Internationale Privatrecht (IPR) grundsätzlich schweizerischem Arbeitsrecht unterstehen, musste die Zulässigkeit der Datenbekanntgabe im Lichte von Art. 328b OR untersucht werden. Die Datenbekanntgabe an Behörden im Rahmen gesetzlicher Pflichten des Arbeitgebers ist als Datenbearbeitung anzusehen, welche zur Durchführung des Arbeitsvertrags erforderlich ist. Somit steht Art. 328b OR einer solchen Datenbekanntgabe nicht entgegen.
Hingegen kann die Niederlassung in der Schweiz durch die belgischen Behörden nicht zur Bekanntgabe dieser Daten gezwungen werden. Ein solcher Zwang kann nur durch die schweizerischen Behörden in der Folge eines Rechtshilfegesuchs ausgeübt werden.
(Die Stellungnahme wurde mit Erwägungen zum IPR und zum Doppelbesteuerungsrecht im Volltext in der VPB 1995 II, S. 254 ff. abgedruckt).

4.4. Auskunftsrecht der Arbeitnehmer - Recht auf Herausgabe graphologischer Gutachten

Der Arbeitnehmer hat grundsätzlich Anrecht auf Herausgabe einer Kopie eines über ihn erstellten graphologischen Gutachtens, nicht aber auf Herausgabe des Originals, da dieses dem Arbeitgeber gehört. Bei Nichtanstellung und nach Beendigung des Arbeitsverhältnisses ist das graphologische Gutachten zu vernichten.

Grundsätzlich hat jede Person ein Anrecht, vom Inhaber einer Datensammlung zu erfahren, welche Daten über sie in einer Datensammlung enthalten sind. Die Auskunft ist in der Regel schriftlich, in Form eines Ausdrucks oder einer Fotokopie zu

erteilen. Im Einvernehmen mit dem Inhaber der Datensammlung oder auf dessen Vorschlag hin, kann die betroffene Person ihre Daten auch an Ort und Stelle einsehen. Aber auch dann muss die betroffene Person die Möglichkeit haben, Kopien zu verlangen. Dieses Vorgehen kann insbesondere für die Einsicht in die eigene Personalakte von Bedeutung sein. Beschränkt werden kann das Recht auf eine Kopie nur im Rahmen von Art. 9 DSG, also insbesondere wegen überwiegender Interessen Dritter oder eigener überwiegender Interessen. Somit haben betroffene Personen grundsätzlich Anrecht auf eine Kopie des graphologischen Gutachtens, hingegen kann der Arbeitgeber z. B. den Namen des Gutachters abdecken.

Ein Anspruch auf Herausgabe besteht sicherlich bezüglich Aktenstücken, welche dem Arbeitnehmer gehören (Bewerbungsunterlagen mit Ausnahme des Bewerbungsschreibens selbst, Sozialversicherungsausweis usw.). Bei Aktenstücken, welche dem Arbeitgeber gehören, besteht hingegen kein Anspruch auf Herausgabe des Originals. Da ein graphologisches Gutachten in der Regel vom Arbeitgeber in Auftrag gegeben wird und somit ihm "gehört", besteht kein Anspruch auf Herausgabe des Gutachtens.

Bei Nichtanstellung hat der Bewerber das Recht, die Vernichtung sämtlicher ihn betreffender Unterlagen, welche nicht an ihn herausgegeben werden müssen, zu verlangen. Dazu gehören die graphologischen Gutachten. Während der Dauer einer Anstellung kann das graphologische Gutachten als Teil der Personalakte aufbewahrt werden, sollte aber nicht innerhalb der Akten offen zugänglich sein. Nach Beendigung des Arbeitsverhältnisses schliesslich darf der Arbeitgeber nur diejenigen Daten aufbewahren, deren er für die ordnungsgemässe Auflösung des Arbeitsverhältnisses und die Erfüllung allfälliger nachvertraglicher Pflichten (z. B. Zeugnis- oder Buchführungspflicht, sozialversicherungsrechtliche Pflichten) bedarf. Alle anderen bearbeiteten Daten sind zu vernichten. Dazu gehören auch graphologische Gutachten und Eignungstests.

4.5. Überwachung von Arbeitnehmern - Gerät zur elektronischen Zählerstandserfassung

Ein Gerät zur elektronischen Zählerstandserfassung kann auch zur Überprüfung der Arbeitsleistung verwendet werden, solange daraus nicht eine systematische und generelle Überwachung der Stromableser resultiert.

Vor einiger Zeit haben verschiedene Elektrizitätswerke neue Geräte für das Stromablesen eingeführt, welche jeweils den genauen Zeitpunkt der Zählerstandserfassung durch jeden Zählerableser erfassen. Das Gerät erlaubt es den zugriffsberechtigten Sachbearbeitern, bei der Energieverrechnung im Einzelfall für Kundenrückfragen im System festzustellen, welche konkrete Bezugsstelle an welchem Datum von welchem Ableser abgelesen wurde. Gleichzeitig besteht die Möglichkeit, Datum und Zeit der einzelnen Bezugsstellenablesungen auszuwerten. Daraus kann ersehen werden, in welchem Rhythmus der betreffende Ableser gearbeitet hat. Ein Angestellter eines Elektrizitätswerkes wandte sich an uns, um zu erfahren, ob dies datenschutzkonform sei.
Rückfragen beim betreffenden Elektrizitätswerk ergaben, dass das neue Gerät im Prinzip nicht zur Überwachung der Ableser benützt und die Angaben grundsätzlich nicht personenbezogen ausgewertet werden. Bei der Einführung des Geräts seien alle Ableser über das neue Gerät und den Verwendungszweck informiert worden

und hätten die Zusicherung erhalten, dass nicht generell personenbezogen ausgewertet werde. Ab Februar 1994 seien aufgrund von konkreten Ungereimtheiten in wenigen Einzelfällen Stichproben vorgenommen worden. An einer Sitzung im Mai 1994 sei über die Stichproben informiert worden und danach sei nur noch in einem Fall über einige Wochen eine Auswertung vorgenommen worden.

Der Arbeitgeber darf Überwachungs- und Kontrollsysteme nur aus Sicherheitsgründen oder zur Erfassung der Arbeitsleistung einsetzen. Als Überwachungs- und Kontrollsysteme sind alle technischen Systeme zu verstehen, durch welche einzelne oder mehrere Tätigkeiten oder Verhaltensweisen der Arbeitnehmer/innen erfasst werden können. Dazu gehören auch die beschriebenen Geräte zur elektronischen Zählerstandserfassung. Diese werden jedoch im vorliegenden Fall grundsätzlich verwendet, um die Rechnungsstellung zu erleichtern und dienen nur in begründeten Einzelfällen zur Überprüfung der Arbeitsleistung. Die betroffenen Personen wurden über die Verwendungsmöglichkeiten des Geräts informiert und der beabsichtigte Verwendungszweck wurde präzisiert. Damit ist aus datenschutzrechtlicher Sicht im vorliegenden Fall nichts gegen einen derartigen Einsatz des Geräts zur elektronischen Zählerstandserfassung einzuwenden. Hingegen könnte die systematische, andauernde Überwachung der Ableser mit Hilfe dieses Geräts schon aus gesundheitsschutzrechtlicher aber auch aus datenschutzrechtlicher Sicht nicht zugelassen werden.

Bundesverwaltung

Die Bearbeitung von Arbeitnehmerdaten durch Bundesorgane untersteht nicht nur den - im Vergleich zur Privatwirtschaft restriktiveren - Bestimmungen des DSG, sondern auch dem Beamtengesetz samt Vollzugsbestimmungen (Rundschreiben des Eidgenössischen Personalamtes vom 16. Januar 1984).

4.6. Ersatz von PERIBU durch BVPLUS und Blockierung der Projekte für eine dezentralisierte Bearbeitung von Personaldaten

Seit mehreren Jahren wird die Frage diskutiert, ob PERIBU durch das neue System BVPLUS ersetzt werden soll (vgl. unseren 1. Tätigkeitsbericht, S.57 ff.). Erst im Januar 1996 haben uns jedoch die Verantwortlichen von PERIBU mitgeteilt, dass dieses System demnächst in Betrieb gesetzt und bereits ab 1997 in einigen Ämtern getestet wird.

Im Rahmen der Prüfung des Entwurfs der Verordnung zum Schutze der Daten von Bundesbediensteten und von Projekten für eine dezentralisierte Bearbeitung von Personaldaten wie PIAS und PISEDI haben wir insbesondere auf die folgenden Punkte hingewiesen (vgl. unseren 1. Tätigkeitsbericht, S. 57 ff.):

- Notwendigkeit bzw. Verpflichtung zur Zusammenarbeit mit dem Eidg. Datenschutzbeauftragten ab Beginn der Ausarbeitung eines Projekts, damit den Erfordernissen des Datenschutzes sofort Rechnung getragen werden kann;
- Koordination zwischen den Verantwortlichen von PERIBU/BVPLUS und den Verantwortlichen der dezentralisierten Projekte;
- Anhörung des Personals und/oder seiner Vertreter.

Im Hinblick auf den Datenschutz und die Datensicherheit haben wir im weiteren die

Entwicklung von dezentralisierten Systemen zur Bearbeitung von Personaldaten unterstützt, wobei das System PERIBU/BVPLUS nur mehr der Lohnverwaltung hätte dienen sollen.
Anlässlich der wenigen Kontakte mit dem Verantwortlichen von PERIBU/BVPLUS (insbesondere anlässlich einer Sitzung im Februar 1992) haben wir die Notwendigkeit von Transparenz betont und verlangt, dass wir regelmässig über die weitere Entwicklung des Dossiers auf dem laufenden gehalten werden.

Dennoch wurden uns erst im Januar 1996 die Datensammlung BVPLUS angemeldet und Dokumentationsunterlagen zugestellt. Aus diesen geht hervor, dass das Projekt so weit fortgeschritten ist, dass es vom nächsten Jahr an in einigen Ämtern getestet werden soll. Wir haben ausserdem erfahren, dass die Entwickler der dezentralisierten Systeme angewiesen worden sind, ihre Arbeiten einzustellen.

Ende Januar 1996 haben wir mit der für BVPLUS zuständigen Stelle Verbindung aufgenommen, um ihr ihre gesetzlichen Verpflichtungen in Erinnerung zu rufen und um die gesamte mit dem Projekt im Zusammenhang stehende Dokumentation zu verlangen.

4.7. Umfang der Verpflichtung eines Mitarbeiters des Bundes, zwecks Aufnahme in eine Pensionskasse Angaben über seinen Gesundheits zustand zu machen

Eine Mitarbeiterin des Bundes, die von ihrer neuen Pensionskasse nur mit einem Vorbehalt aufgenommen worden war, hat uns um Vermittlung gebeten. Die Pensionskasse hatte die betroffene Person gebeten, im Zusammenhang mit der Aufnahme einen Fragebogen auszufüllen, und die Bundesangestellte hatte sich geweigert, die Frage "Wurde bei Ihnen ein positiver AIDS-Test erhoben?" zu beantworten.

Wir haben zunächst festgestellt, dass der erste Teil des Formulars, der den Gesundheitszustand der Eltern und Geschwister der betroffenen Person betrifft, die Bestimmungen des DSG verletzt, weil er sich auf Drittpersonen bezieht. Abgesehen davon war die betroffene Person nicht unbedingt in der Lage, diese Fragen korrekt zu beantworten.

Im weiteren haben wir betont, dass die Frage bezüglich einer allfälligen HIV-Infektion unverhältnismässig ist. Die wissenschaftlichen Erkenntnisse in bezug auf die Auswirkungen einer Seropositivität auf die Entwicklung des Gesundheitszustandes reichen nicht aus, um eine Konzentration auf AIDS, eher als auf andere Krankheiten wie beispielsweise Malaria zu rechtfertigen. Aus diesem Grund ist es nicht gerechtfertigt, wenn Personen, welche die oben angeführte Frage bejahen oder eine Beantwortung dieser Frage verweigern, systematisch mit einem fünfjährigen Vorbehalt in die Pensionskasse aufgenommen werden.

Die Pensionskasse hat unterdessen den gegen die betroffene Person verhängten Vorbehalt aufgehoben und verwendet eine allfällige HIV-Infektion nicht mehr als Aufnahmekriterium. Der Inhalt des Fragebogens, der von den künftigen Mitgliedern der Pensionskasse auszufüllen ist, wird gegenwärtig überarbeitet.

4.8. Begriff der ausschliesslich zum persönlichen Gebrauch bestimmten Daten

Die Mitarbeiterin eines Amtes hat uns um Vermittlung gebeten. Sie hat uns mitgeteilt, dass ihr Vorgesetzter ihren Terminkalender eingesehen und Auszüge daraus kopiert hat. Diese Kopien wurden dem Personaldienst des betreffenden Amtes übergeben. Die Betroffene wurde auch unter Druck gesetzt, damit sie die fotokopierten Seiten vernichtet. Diese Seiten enthielten Informationen über das Kommen und Gehen gewisser Mitarbeiter sowie Bemerkungen zu diesen Personen.

Zunächst haben wir festgehalten, dass gemäss den allgemeinen Regeln des Persönlichkeitsschutzes niemand berechtigt ist, den Terminkalender einer anderen Person einzusehen und erst recht nicht, Fotokopien davon zu erstellen oder die Vernichtung gewisser Seiten zu verlangen. Dem Inhaber eines Terminkalender steht es im übrigen frei, darin alles zu notieren, was er will.

Im weiteren haben wir festgehalten, dass der betreffende Terminkalender nicht eine Datensammlung im Sinne des DSG darstellt, da er nicht so strukturiert ist, dass die darin enthaltenen Informationen nach Personen gesucht werden können. Ausserdem haben wir die von dieser Angelegenheit betroffenen Personen darauf hingewiesen, dass der betreffende Terminkalender nicht dem DSG untersteht, da die darin enthaltenen Daten von einer natürlichen Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden. Damit das Merkmal “ausschliesslich zum persönlichen Gebrauch bestimmt” erfüllt ist, dürfen jedoch die Informationen nicht ausserhalb des privaten und familiären Kreises benutzt werden, was insbesondere voraussetzt, dass sie nicht den Arbeitskollegen mitgeteilt werden.

4.9. Frageblatt zum ärztlichen Zeugnis für die Bewerber um eine Stelle

Die betroffene Person war im Anschluss an eine längere krankheitsbedingte Abwesenheit entlassen worden, weil sie auf dem medizinischen Frageblatt verschiedene Spitalaufenthalte nicht angegeben hatte, die vor der Anstellung stattgefunden hatten. Wir wurden gebeten, aus datenschutzrechtlicher Sicht zu der Tatsache Stellung zu nehmen, dass sowohl für die Anstellung als auch für die Aufnahme in die Eidgenössische Versicherungskasse (EVK) nur ein Fragebogen verwendet wird.

Es wurde uns eine veraltete Version des Frageblatts zur Prüfung eingereicht. 1989 wurde ein neues Formular ausgearbeitet. Unsere Bemerkungen sind daher ausschliesslich für jene Mitarbeiter relevant, deren medizinische Untersuchung “nach der alten Regelung” erfolgte.

Nach einer längeren krankheitsbedingten Abwesenheit der Betroffenen hatte das Departement, bei dem sie angestellt war, über die Freigabe ihrer Stelle für eine andere Person zu entscheiden und musste überdies entscheiden, ob die betroffene Person invalid erklärt werden soll. Der Personalchef, der mit der Regelung dieses Falls beauftragt war, wurde vom ärztlichen Dienst darüber informiert, dass die Mitarbeiterin bei der Anstellung frühere Spitalaufenthalte verschwiegen hatte, weil sie befürchtete, andernfalls nicht angestellt zu werden. Er entschied sich daher zunächst, die betroffene Person für das Verschweigen der Wahrheit mit einer Entlassung aus eigenem Verschulden zu bestrafen, was die Leistungen der Eidgenössischen Versicherungskasse erheblich reduziert hätte.

Von der Rechtsvertreterin der betroffenen Person zu diesem Fall angefragt, hielten wir fest, dass die frühere Praxis des Bundes, für zwei verschiedene Zwecke (Abklärung der Eignung für eine Stelle und Aufnahme in die EVK) den gleichen medizinischen Fragebogen zu benutzen, gegen die im DSG verankerten Verhältnismässigkeits- und Zweckbindungsgrundsätze verstiess. Abgesehen davon stand der Stellenbewerber vor einem Dilemma: gegenüber einem zukünftigen Arbeitgeber ist sein “Notwehrrecht der Lüge" anerkannt, gegenüber der Pensionskasse hingegen nicht.

Was den ärztlichen Dienst anbelangt, haben wir festgehalten, dass dieser, wenn von ihm Berichterstattung an ein Departement verlangt wird, nur seine Schlussfolgerungen in bezug auf die Arbeitsfähigkeit bzw. den Grad und die Dauer der Arbeitsunfähigkeit der betroffenen Person mitteilen darf. Das Departement entscheidet auf der Grundlage dieser Schlussfolgerungen über eine allfällige Invaliditätserklärung der betroffenen Person bzw. über eine Ausschreibung ihrer Stelle.
Wir sind zum Schluss gekommen, dass das Departement in einem derartigen Fall *einen objektiven Entscheid fällen muss* und dass es nicht befugt ist, einen Mitarbeiter in einem solchen Fall aus eigenem Verschulden zu entlassen oder die EVK über ihm bekannte Lücken zu informieren.

Da der Personalchef des Departements der EVK zum Zeitpunkt unserer Intervention die ersten Schlussfolgerungen bereits mitgeteilt hatte, konnte er nurmehr einen Teil unserer Vorschläge befolgen, indem er beim Entscheid über die Arbeitsfähigkeit der betroffenen Person eine objektivere Formulierung wählte.

4.10. Verzeichnen von Abwesenheitsgründen im Wochenprogramm

Die Bekanntmachung der detaillierten Abwesenheitsgründe bei Krankheit (Arzt, Kur, Krank, Rekonvaleszent, Therapie) in einem Wochenprogramm, das nicht nur der unmittelbaren Arbeitsumgebung der betroffenen Person, sondern einer grösseren Anzahl von Personen zugänglich ist, ist nicht datenschutzkonform.

Die Bekanntmachung der Abwesenheitsgründe bei Krankheit von Arbeitnehmern gegenüber Dritten kann in der Tat eine Verletzung der Persönlichkeit der betroffenen Person zur Folge haben. Gemäss dem Grundsatz der Verhältnismässigkeit sollen Daten nur in dem Umfang und in der Weise bearbeitet werden, die zur Erreichung des angestrebten Zieles erforderlich sind. Das bedeutet, dass Daten über die Gesundheit der Arbeitnehmer vom Arbeitgeber nur in dem Umfang erhoben werden dürfen, zudem sie für die Abwicklung des Arbeitsverhältnisses erforderlich sind (namentlich Lohnfortzahlung und Arbeitsplanung während krankheitsbedingter Abwesenheiten). Ebenso dürfen solche Angaben vom Arbeitgeber innerhalb des Betriebs nur an diejenigen Personen bekanntgegeben werden, welche diese aufgrund ihrer Tätigkeit benötigen (Personaldienst, Vorgesetzte und unmittelbare Mitarbeiter der betroffenen Person). Bei anderen Personen genügt in der Regel die Mitteilung, dass die betreffende Person während einer bestimmten Zeit abwesend ist.
Deshalb ist es ratsam, im Wochenprogramm nur die Abwesenheit ohne Angabe von Gründen zu verzeichnen, wobei darauf zu achten ist, dass nicht schon aus der gewählten Umschreibung hervorgeht, dass ein gesundheitliches Problem vorliegt. Wird zum Beispiel in allen anderen Fällen der Abwesenheitsgrund angegeben, so weist schon das Fehlen des Grundes darauf hin, dass die Abwesenheit krankheitshalber erfolgt. Es empfiehlt sich deshalb, im Wochenprogramm nur berufsbedingte Abwesenheiten zu spezifizieren, während Abwesenheiten aus anderen Gründen (Krank-

heit, Ferien, Urlaub usw.) unter einer einheitlichen Bezeichnung eingetragen werden.

4.11. Pflicht der Angestellten des Auskunftsdienstes 111 der Telecom-PTT, ihren Vornamen zu nennen

Die Teleoperatricen des Auskunftsdienstes der Telecom-PTT können ohne entsprechende gesetzliche Grundlagen nicht gezwungen werden, sich zusätzlich zum Namen auch noch mit dem Vornamen zu melden.

Eine bei der Kreisdirektion Genf angestellte Person erkundigte sich, ob sie gezwungen werden könne, sich bei der Auskunfterteilung mit Namen und Vornamen zu melden. Dies wurde von der Kreisdirektion unter Hinweis auf die Verbesserung des Dienstes am Kunden und die Praxis in der Privatwirtschaft verlangt. Die Teleoperatricen fühlten sich von der Pflicht, den Vornamen zu sagen, in ihrer Privatsphäre beeinträchtigt und befürchteten Belästigungen von Seiten der Kunden. Eine bei der Kreisdirektion Genf durchgeführte Kontrolle (Einzelheiten, S. 63) ergab, dass die Vornamensnennung keinen konkreten Nutzen zeitigt und dass sie verschiedentlich zu Vertraulichkeiten seitens der Kunden geführt hat. Wir vertraten deshalb die Auffassung, ohne ausdrückliche diesbezügliche gesetzliche Grundlage könne von den Teleoperatricen die Nennung des Vornamens nicht verlangt werden. Die Kreisdirektion Genf informierte daraufhin die Angestellten entsprechend.

4.12. Empfehlungen des Eidgenössischen Personalamtes zur Anwendung von Einzel- und Gruppen-Testverfahren

Aufgrund der zunehmenden Anwendung von verschiedenen Einzel- und Gruppen-Testverfahren zur Personalselektion innerhalb der Bundesverwaltung hat das Eidgenössische Personalamt Empfehlungen zur Anwendung dieser Testverfahren ausgearbeitet und uns zur Stellungnahme unterbreitet.

In der Tat erfreuen sich Einzel- und Gruppen- Test-Verfahren wie graphologische Gutachten, psychologische Leistungs-, Intelligenz- oder Persönlichkeitstests, biographische Fragebogen und andere Beurteilungssysteme (Assessment, Assessment-Center) immer grösserer Beliebtheit als Hilfsmittel zur Evaluation von gegenwärtigen oder künftigen Mitarbeiter/innen. Bereits im 2. Tätigkeitsbericht (S. 47 ff.) hatten wir zu einem automatisierten Persönlichkeitstest (Sigmund Potential) Stellung genommen und die Voraussetzungen für den datenschutzrechtlich korrekten Umgang mit den bearbeiteten Daten aufgezeigt. Gestützt auf diese Stellungnahme sowie auf den Leitfaden für die Bearbeitung von Personendaten im Arbeitsbereich durch private Personen erliess das Eidgenössiche Personalamt Empfehlungen zum Umgang mit solchen Testverfahren und unterbreitete sie uns zur Begutachtung. Die Empfehlungen stellen verschiedene Grundsätze auf, von denen wir im folgenden nur diejenigen hervorheben, die nicht bereits im 2. Tätigkeitsbericht dargelegt wurden.

- Nehmen mehrere Personen desselben Bundesamtes oder -betriebes an einem Testverfahren teil, bei dem die Anonymität nicht gewahrt werden kann, sind sie darüber im voraus zu informieren.
- Die Testergebnisse müssen der Testperson nach Abschluss des Verfahrens im Original ausgehändigt und die übrigen Unterlagen (inkl. Kopien) vernichtet werden.

- Die Testperson muss in jedem Fall die Möglichkeit zur persönlichen Stellungnahme in bezug auf ihre Testresultate und deren Interpretation erhalten.
- Testverfahren dürfen nicht als einziges oder wichtigstes Instrument eingesetzt werden; sie ersetzen keineswegs das persönliche Auswertungs-, Selektions- oder Fördergespräch und die Entscheidung.
- Der Anwendung von Testverfahren muss eine genaue Analyse der gewünschten Anforderungen vorausgehen; die Testergebnisse müssen in bezug auf diese Anforderungen aussagekräftig sein.
- Anzahl und Umfang der verschiedenen Testverfahren und die zu erwartenden Ergebnisse müssen der Stelle angepasst und aufeinander abgestimmt sein; persönlicher, finanzieller und zeitlicher Aufwand sind im Vergleich mit den zu erwartenden Ergebnissen kritisch abzuwägen.
- Testverfahren gehören ausschliesslich in die Hände von ausgebildeten Fachleuten.
- Den Testergebnissen gegenüber muss eine kritische Haltung bewahrt werden.
- Einzelresultate sind in Bezug zur gesamten Persönlichkeit, und den gesamten Fähigkeiten der getesteten Person zu setzen.
- Gegenüber der Testperson ist ein faires und transparentes Verhalten an den Tag zu legen; es sind ihr alle Testergebnisse unter Gelegenheit zur Stellungnahme vorzulegen.
- Es ist zu klären, welches Menschen- oder Persönlichkeitsbild dem verwendeten Testverfahren zugrundeliegt; dieses sollte nicht unkritisch übernommen werden.
- Es ist zu prüfen, welche Testverfahren der Amts-, respektive Betriebskultur und der zu prüfenden Funktion am besten entsprechen.
- Die Interpretation der Testergebnisse ist immer subjektiv. Es ist darauf zu achten, dass man nicht versucht, diese Subjektivität mit der scheinbaren Objektivität der Testergebnisse zu legitimieren; man sollte zur persönlichen Interpretation stehen und diese der Testperson gegenüber erkennbar machen, damit sie sich dazu äussern kann.

5. Versicherungswesen

Sozialversicherungen

5.1. Systematische Bekanntgabe der Diagnose an die Krankenkassen

Mit dem Inkrafttreten des neuen Krankenversicherungsgesetzes wurde eine Frage wieder aktuell, die von den betroffenen Partnern schon seit mehreren Jahren diskutiert wird: die systematische Bekanntgabe der Diagnose an die Krankenkassen. Wir wurden aufgefordert, uns zur Rechtmässigkeit dieser Bekanntgabe zu äussern.

Die Frage des Grundsatzes der Bekanntgabe der Diagnose an die Krankenkassen, die von den betroffenen Partnern bereits seit mehreren Jahren diskutiert wird, gewann mit dem Inkrafttreten des neuen Krankenversicherungsgesetzes (KVG; siehe auch S. 59) wieder an Aktualität. Wir wurden aufgefordert, uns zur Rechtmässigkeit der systematischen Bekanntgabe der Diagose, wie sie im Entwurf der Verordnung über die Krankenversicherung (KVV) vorgesehen war, zu äussern.

Art. 42 Abs. 4 KVG lautet: “Der Versicherer *kann* eine genaue Diagnose oder zusätz-

liche Auskünfte medizinischer Natur *verlangen*". Aus dem Wortlaut dieser Bestimmung geht hervor, dass eine Anfrage des Versicherers im Einzelfall erforderlich ist. Art. 63 Abs. 1 des KVV-Entwurfs (Fassung vom Januar 1995) verlangte jedoch, dass die Leistungserbringer ihre Diagnose systematisch bekanntgeben. Wir haben zum einen festgehalten, dass dieser Begriff definiert werden müsste, um den Meinungsverschiedenheiten in bezug auf seine Auslegung ein Ende zu setzen. Zum anderen haben wir betont, dass diese Verpflichtung zur Bekanntgabe der Diagnose widerrechtlich war, da sie über den durch das KVG festgelegten Rahmen hinausging und unverhältnismässig war. Wir haben schliesslich empfohlen, für jene Fälle, in denen auf die Diagnose zurückgegriffen werden muss, eine Liste mit Diagnose-Codes zu benutzen, die für die ganze Schweiz gültig ist. Damit könnten die Unterschiede zwischen den Kantonen abgebaut werden, und zudem würde sichergestellt, dass alle Versicherten in der Schweiz dem gleichen Datenschutzniveau unterständen.

Die neue Fassung des KVV-Entwurfs wurde uns nicht mehr zur Stellungnahme unterbreitet, bevor sie vom Bundesrat am 27. Juni 1995 verabschiedet wurde und am 1. Januar 1996 in Kraft trat. Unsere Vorschläge wurden indessen zu einem Grossteil in einen (Art. 59) aufgenommen, der folgendermassen lautet:

[1]Die Leistungserbringer haben in ihren Rechnungen folgende Angaben zu machen:

a. Kalendarium der Behandlungen;

b. erbrachte Leistungen im Detaillierungsgrad, den der massgebliche Tarif vorsieht;

c. Diagnosen im Rahmen von Absatz 2.

[2]Versicherer und Leistungserbringer können in den Tarifverträgen vereinbaren, welche Angaben und Diagnosen in der Regel nur dem Vertrauensarzt oder der Vertrauensärztin des Versicherers nach Artikel 57 des Gesetzes bekanntzugeben sind. Im übrigen ***richtet sich die Bekanntgabe der Diagnose nach Artikel 42 Absätze 4 und 5 des Gesetzes****. Das Departement kann auf gemeinsamen Antrag der Versicherer und der Leistungserbringer einen gesamtschweizerisch gültigen, einheitlichen Diagnose-Code festlegen.*

[3]Die von der obligatorischen Krankenpflegeversicherung übernommenen Leistungen sind in der Rechnung von anderen Leistungen klar zu unterscheiden.

Die Auslegung von Buchstabe c des ersten Absatzes dieser Bestimmung muss in erster Linie vor dem Hintergrund des im zweiten Absatz fettgedruckten Satzes erfolgen. Die darin erwähnte Bestimmung des KVG wird jedoch auf unterschiedliche Weise ausgelegt, von denen wir nachfolgend die gängigsten aufführen:

- Die meisten Versicherer sind der Auffassung, dass sie aufgrund dieser Rechtsgrundlagen berechtigt sind, von den Leistungserbringern die systematische Bekanntgabe der detaillierten Diagnose zu verlangen;

- Gewisse Leistungserbringer (darunter jene aus dem Kanton Genf, für die das Inkrafttreten der neuen Bestimmungen mit einem radikalen Wechsel der bisherigen Praxis im Bereich der Rechnungsstellung verbunden ist) sind der Auffasssung, dass die Bekanntgabe der Diagnose grundsätzlich ausgeschlossen ist und nur in Einzelfällen auf eine entsprechende Anfrage hin erfolgen kann;

- Eine dritte Gruppe vertritt folgende vermittelnde Auffassung: Da im Gesetz

vorgesehen ist, dass dem Versicherer **alle Angaben gemacht werden müssen, die er benötigt**, um die Berechnung der Vergütung und die Wirtschaftlichkeit der Leistung überprüfen zu können, sei auch die Diagnose systematisch bekanntzugeben. Darunter sei eine Rahmen-Diagnose - im Gegensatz zur detaillierten Diagnose - zu verstehen, deren Detaillierungsgrad zwischen den betroffenen Partnern vertraglich vereinbart werden müsse. Eine detaillierte Diagnose könne nur in Einzelfällen und auf eine entsprechende Anfrage hin bekanntgegeben werden.

Nach der Prüfung der Botschaft zum KVG haben wir uns der zweiten “Schule” angeschlossen, da diese Auffassung am besten mit dem Datenschutz zu vereinbaren ist. Wir sind darüber hinaus zum Schluss gelangt, dass die KVV nur innerhalb dieser Schranken als rechtmässig betrachtet werden kann. Zudem haben wir festgehalten, dass man beim gegenwärtigen Stand der Wissenschaft in diesem Bereich nicht davon ausgehen kann, dass die systematische Bekanntgabe der Diagnose - so detailliert diese auch sein mag - ein zufriedenstellendes Kriterium für die Überprüfung der Vergütungen und der Wirtschaftlichkeit der Leistungen darstellt.

5.2. Analysen- und Tarifliste

An ihrer letzten Sitzung vom 31. Mai 1995 hat die Arbeitsgruppe ADAK einen Berichtsentwurf mit dem Titel Bericht der Arbeitsgruppe “Datenschutz und Analysenliste / Krankenversicherung” (im folgenden ADAK-Bericht) verabschiedet, der eine Zusammenfassung der Datenschutzprobleme, die sich besonders im Bereich der Krankenversicherung stellen und entsprechende Lösungsvorschläge enthält (vgl. unsere beiden ersten Tätigkeitsberichte, S. 48 bzw. 52). Die Mitglieder der Arbeitsgruppe haben betont, dass der ADAK-Bericht aufgrund seiner Auswirkungen auf das Sozial- und Privatversicherungsrecht sowie auf das Arbeitsrecht und das Recht im Bereich der Gentechnologie so schnell als möglich veröffentlicht werden muss. Dieser Bericht wird voraussichtlich auch der parlamentarischen Kommission als Reflexionsgrundlage dienen, die am Entwurf für ein Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts arbeitet.
Leider müssen wir jedoch feststellen, dass das Eidgenössische Departement des Innern den ADAK-Bericht noch immer nicht veröffentlicht hat.

5.3. Umfang der Verpflichtung der Ärzte zur Zusammenarbeit mit den Unfallversicherungen

Ein Arzt hat Bedenken in bezug auf die Vereinbarkeit des Übereinkommens zwischen den Unfallversicherern und der FMH mit dem DSG geäussert. Einige Bestimmungen sehen nämlich eine systematische Weiterleitung von Kopien der ärztlichen Berichte an die Versicherungen vor.

Wir haben zunächst betont, dass eine Weiterleitung von Informationen nur innerhalb der durch das DSG vorgegebenen Schranken - insbesondere der allgemeinen Grundsätze wie beispielsweise dem Verhältnismässigkeitsprinzip - erfolgen darf, auch wenn das Unfallversicherungsrecht Bestimmungen enthält, wonach die Ärzte zur Bekanntgabe der von den Versicherern verlangten Informationen verpflichtet sind. Dies bedeutet, dass ein Versicherer nur jene medizinischen Daten verlangen und bearbeiten darf, die zur Regelung des Schadenfalls erforderlich sind. Da die von

uns geprüften vertraglichen Bekanntgabeklauseln diesen Grundsatz nicht berücksichtigen, sind wir zum Schluss gekommen, dass sie unrechtmässig sind.

Privatversicherungen

5.4. Merkblatt und Einwilligungsklausel

Im Anschluss an unsere Bemerkungen über die in den Merkblättern und bei der Einwilligungsklausel noch bestehenden Lücken (vgl. unseren 2. Tätigkeitsbericht, S. 54) wurden uns von den Versicherern neue Formulierungsvorschläge für diese Dokumente zur Stellungnahme unterbreitet. Wir haben bei dieser Gelegenheit an die Notwendigkeit zur Transparenz erinnert und haben am Beispiel der Lebensversicherung differenzierte Einwilligungsklauseln vorgeschlagen.

Die Zusammenarbeit für eine bessere Formulierung der Merkblätter und der Einwilligungsklauseln wird sowohl mit den Personen- als auch mit den Sachversicherern weitergeführt. In diesem Zusammenhang haben uns die Versicherer neue Formulierungsvorschläge unterbreitet. Wir haben eine Verbesserung der Transparenz der Merkblätter festgestellt, wobei insbesondere bei den Abschnitten über die Einwilligung (die jederzeit widerrufen werden kann) und über das Auskunftsrecht noch gewisse Ergänzungen angebracht werden müssen.

Was die Einwilligungsklausel anbelangt, haben wir festgestellt, dass die Formulierung namentlich in bezug auf Dritte, die konsultiert werden können, sowie bezüglich der Zwecke des geplanten Datenaustausches jetzt genauer ist. Wir haben hingegen daran erinnert, dass eine einzige Standard-Generalklausel für eine wirksame Einwilligung der betroffenen Person nicht genügt, und dass sich die Einwilligung nicht sowohl auf die Bearbeitung von Daten im Zusammenhang mit dem Abschluss eines Versicherungsvertrages als auch auf alle weiteren Entwicklungen des Vertrags - einschliesslich des Marketings - beziehen kann. Wir haben betont, dass eine solche Klausel von Rechts wegen als nichtig zu betrachten ist.

Wir haben deshalb empfohlen, zwischen den *notwendigen* und den *subsidiären Klauseln* zu unterscheiden, wobei es sich bei den ersteren um jene Vertragsbestimmungen handelt, die von der betroffenen Person unterschrieben werden müssen, damit der Vertrag abgeschlossen und durchgeführt werden kann. Der Versicherer möchte, dass auch die subsidiären Vertragsbestimmungen unterzeichnet werden, damit er beispielsweise ermächtigt ist, die entsprechenden Daten zu Marketingzwecken zu verwenden. In solchen Fällen ist der Versicherer jedoch nicht berechtigt, den Abschluss des Versicherungsvertrags von der Unterzeichnung einer solchen Klausel abhängig zu machen.

Ausserdem haben wir vorgeschlagen, zwischen den *vorvertraglichen* und den *vertraglichen Beziehungen* zu unterscheiden und für jede Versicherungsbranche eigene Vertragsbestimmungen zu verabschieden. Eine Sachversicherung (beispielsweise für ein Gebäude) setzt für ihre Verwaltung nicht die Bearbeitung gleichvieler Personendaten voraus, wie eine Personenversicherung. Auch innerhalb der Personenversicherungen gibt es Unterschiede: so sind die Häufigkeit und der Umfang des Informationsflusses bei einer Lebensversicherung und bei einer Krankenversicherung unterschiedlich. Am Beispiel der Lebensversicherung haben wir folgende Lösungen vorgeschlagen:

- Im vorvertraglichen Stadium ist die Vereinbarung einer Einwilligungsklausel

erforderlich, deren Wirkung auf das Ende der vorvertraglichen Beziehung begrenzt werden kann. Wenn kein Vertrag zustande kommt, hat dies abgesehen von gewissen Ausnahmen (gesetzliche Pflicht zur Aufbewahrung der Daten, notorisch schlechte Zahlungsmoral des Betroffenen, strafrechtlich relevante Fälle) die Löschung aller bearbeiteten Personendaten zur Folge. In den Ausnahmefällen kommt eine Aufbewahrung der Daten je nach den Umständen während fünf bis zehn Jahren in Betracht.
Falls die betroffene Person zu diesem Zeitpunkt eine subsidiäre Klausel unterzeichnet, die sich spezifisch auf das Marketing bezieht, kann der Versicherer die dafür erforderlichen Daten aufbewahren;

- Während der Durchführung des Vertrags ist keine Einwilligungsklausel erforderlich, wenn die Datenbearbeitung innerhalb der durch die allgemeinen Grundsätzen des DSG gesetzten Schranken bzw. im für die Verwaltung eines Lebensversicherungsvertrags erforderlichen Umfang bearbeitet werden (objektiv zweckmässige Datenbearbeitung).
  Die *Einwilligung* des Versicherten muss jedoch immer dann eingeholt werden, wenn im Zusammenhang mit einem spezifischen Ereignis - wie beispielsweise dem Eintritt eines Schadens - eine über den im vorhergehenden Abschnitt beschriebenen üblichen Rahmen hinausgehende Datenbearbeitung erforderlich ist. Falls der Versicherte nicht in der Lage ist, seine Einwilligung zu geben, oder falls er verstorben ist, muss die Einwilligung seines gesetzlichen Vertreters eingeholt werden;

- Für das im Marketing praktizierte Cross-Selling ist die Unterzeichnung einer spezifischen subsidiären Klausel erforderlich. Die betroffene Person muss die Möglichkeit haben, sich dem Cross-Selling zu widersetzen, ohne dass dies Auswirkungen auf den Versicherungsvertrag hat.

Schliesslich haben wir begrüsst, dass die Versicherer ihrerseits eine Klausel unterzeichnen, in der sie sich verpflichten, ihre Geheimhaltungspflicht und die im Merkblatt umschriebenen Modalitäten der Datenbearbeitung zu beachten. Wir haben verlangt, dass diese Klausel durch folgende Rubriken ergänzt wird:

- Zusicherung, dass wenn kein Vertrag abgeschlossen wird, die dadurch nutzlos gewordenen Daten gelöscht werden (vorbehältlich der vorgängig erwähnten speziellen Umstände);

- Bei Zustandekommen des Vertrags Gewährleistung der Information der betroffenen Person und Einräumung einer genügenden Frist, wenn von einem Dritten stammende Daten negative Auswirkungen für die betroffene Person haben könnten. Sie könnte diesfalls ein Recht auf Anhörung geltend machen;

- Zusicherung, dass in den Fällen, in denen die Datenbearbeitung über den durch das DSG vorgegebenen Rahmen hinausgeht (beispielsweise im Schadensfall), die Zustimmung des Versicherten oder seines gesetzlichen Vertreters eingeholt wird

5.5. Automobil-Versicherung

Als Folge der Deregulierung bzw. Liberalisierung des Wettbewerbs, die in diesem Be-

reich vor kurzem eingeführt wurde, versuchen die Versicherer möglichst viele Informationen über betroffene Personen zu erhalten, um ihre Produkte bestmöglich dem Markt anpassen zu können. In diesem Zusammenhang hat uns eine Privatperson ein Antragsformular zugesandt, um es aus datenschutzrechtlicher Sicht prüfen zu lassen.

Wir haben zunächst in Erinnerung gerufen, dass die gesamte Tätigkeit der Versicherer dem DSG und seinen allgemeinen Grundsätzen untersteht, zu denen auch das Verhältnismässigkeitsprinzip gehört. Wir haben im weiteren darauf hingewiesen, dass das Inkrafttreten des DSG unter anderem auch eine Einschränkung der Tragweite der allgemeinen Norm über die Anzeigepflicht des Antragstellers im Bundesgesetz über den Versicherungsvertrag zur Folge hat. Es darf nicht länger allein aufgrund der Tatsache, dass eine Frage im Antragsformular enthalten ist, angenommen werden, dass sie wichtig ist. Aus datenschutzrechtlicher Sicht ist eine Frage nämlich nicht schon dann zulässig, wenn ihre Beantwortung für den Versicherer *bequem* ist, sondern erst, wenn die Antwort für den Versicherer *erforderlich* ist, um über den Antrag entscheiden zu können.

Wir haben festgestellt, dass der Inhalt des Antragsformulars die obenerwähnten Kriterien nur zum Teil erfüllte, da die gestellten Fragen nicht immer in einem direkten Zusammenhang mit dem Abschluss des Versicherungsvertrags standen.

Die im Antragsformular enthaltene Bestimmung, mit welcher der Antragsteller der Bekanntgabe von ihn betreffenden Personendaten an Dritte zustimmt, ist aufgrund ihres viel zu allgemeinen Charakters unrechtmässig.

Gegenwärtig sind Gespräche im Gang, um eine Lösung zu finden, die praktikabel ist und gleichzeitig die Anforderungen des Datenschutzes erfüllt.

6. Gesundheitswesen

6.1. Die Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung

Diese seit dem 27. Januar 1994 bestehende Kommission bewilligt unter bestimmten Voraussetzungen medizinischen Forschungsprojekten das Arbeiten mit Personendaten. Bis zu diesem Zeitpunkt hätte von Rechts wegen bei allen medizinischen Forschungsprojekten mit Personendaten die Einwilligung sämtlicher betroffenen Personen eingeholt werden müssen. Ein solches Vorgehen war in einer Vielzahl von Fällen derart unpraktikabel, dass viele medizinische Forschungsprojekte mit faktischen Verstössen gegen das Arztgeheimnis verbunden und damit illegal waren. Die Einsetzung einer Expertenkommission, welche Bewilligungen der angesprochenen Art erteilen kann, stellt den Versuch des Gesetzgebers dar, diesen unhaltbaren Zuständen ein Ende zu setzen.

Die Kommission beruht auf Art. 321bis des Schweizerischen Strafgesetzbuchs (StGB), der am 1. Juli 1993 gleichzeitig mit dem DSG in Kraft getreten ist. Sie besteht aus insgesamt elf vom Bundesrat eingesetzten Mitgliedern, welche paritätisch die interessierten Gruppen (Forscher, Patienten, Ärzte) vertreten. Dementsprechend setzt sie sich zusammen aus drei Vertretern der Forschung, drei praktizierenden Ärzten und drei Vertretern von Patientenrechtsorganisationen. Darüberhinaus müssen

zwei Mitglieder Juristen sein. Das Sekretariat der Kommission wird vom Bundesamt für Gesundheitswesen geführt, wo zur Zeit eine juristische Mitarbeiterin voll für diese Aufgabe tätig ist. Abgesehen von der administrativen Zuordnung zum Eidgenössischen Departement des Inneren ist die Kommission unabhängig.

Von insgesamt 29 als Gesuche entgegengenommenen Schreiben - vorwiegend für Medizinalregister und für einzelne Forschungsprojekte - hat die Kommission bisher 21 bewilligt und deren 2 abgelehnt. (Allerdings hatte die Ablehnung des Gesuchs nur im einen Fall zur Folge, dass das Forschungsprojekt nicht durchgeführt werden konnte. Im anderen Fall verhielt es sich so, dass gar keine Bewilligung erteilt zu werden brauchte, weil das Forschungsprojekt das Arztgeheimnis nicht verletzt). 6 Gesuche sind noch hängig.

Für Forschungsprojekte, welche nicht mit anonymisierten Daten durchgeführt werden können und bei denen die Einwilligungen der Betroffenen nicht oder nur mit unverhältnismässigem Aufwand eingeholt werden könnten, kann die Kommission die Aufhebung des Arztgeheimnisses im folgenden Sinne bewilligen: Einerseits wird behandelnden Ärzten erlaubt, Patientendaten für das bestimmte Forschungsprojekt zur Verfügung zu stellen. Andererseits wird den Forschern erlaubt, bei behandelnden Ärzten um Patientendaten nachzufragen, ohne dass dadurch eine Verpflichtung der behandelnden Ärzte zur Bekanntgabe begründet würde.
Zusätzlich wägt die Kommission ab, ob die Forschungsinteressen gegenüber den Geheimhaltungsinteressen überwiegen.

Die Expertenkommission erteilt einerseits sogenannte *Sonderbewilligungen* für genau spezifizierte Forschungsprojekte, wobei die Bearbeitung derselben Daten im Rahmen eines anderen Projektes einer neuen, besonderen Bewilligung bedarf. Auf der anderen Seite werden *generelle Bewilligungen* an Organe erteilt, welche Medizinalregister führen (Registerbewilligungen), sowie an Kliniken, welche regelmässig Forschungsprojekte durchführen (Klinikbewilligungen). Mit den erteilten Bewilligungen verbindet die Kommission Auflagen zur Sicherung des Datenschutzes. Dabei handelt es sich um Anweisungen betreffend die Aufbewahrung der sensiblen Daten, betreffend die Regelung der Zugriffsberechtigungen sowie allenfalls betreffend die Zerstörung der Papierdossiers und Datenträger. Der EDSB hat die Aufgabe, die Einhaltung dieser Auflagen zu überwachen. Anlässlich der Aufnahme dieser Tätigkeit im Bereich der epidemiologischen Krebsregister hat sich gezeigt, dass neben der gesetzlich vorgeschriebenen “Überwachungstätigkeit” von den verantwortlichen Forschern auch eine gewisse Hilfestellung bei der Interpretation der Bewilligungsentscheide benötigt wird.

Der Vollständigkeit halber sollen noch die drei weiteren im DSG vorgesehenen Aufgaben des EDSB im Bereich der medizinischen Forschung erwähnt werden: Zunächst geht es hierbei um die Beratung der Expertenkommission. Sodann soll der EDSB darauf hinwirken, dass die Patienten über ihre Rechte informiert werden. Und schliesslich kann er Bewilligungsentscheide mit Beschwerde bei der Eidgenössischen Datenschutzkommission anfechten.

6.2. Die Anwendbarkeit des DSGs auf kantonale Krankenhäuser

Bei der Bearbeitung von Patientendaten durch kantonale Spitäler ist von Fall zu Fall zu untersuchen, ob ein Arzt - Patientenverhältnis auf dem privaten oder dem öffentli-

chen Recht beruht und ob man sich im Rahmen des Rechts des Bundes oder der Kantone bewegt. Die Krankenbetreuung in öffentlichen Spitälern, von Ärzten in amtlicher Eigenschaft ausgeübt, gilt nach bundesgerichtlicher Rechtsprechung nicht als gewerbliche Tätigkeit des Gemeinwesens.

Eine private Person fragte uns an, ob auf öffentliche Spitäler im Kanton Zürich das DSG oder das kantonale Datenschutzgesetz anwendbar sei. Das Datenschutzgesetz des Kantons Zürich gilt nicht, wenn ein Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei nicht hoheitlich handelt (Paragraph 3 lit. a Datenschutzgesetz des Kantons Zürich). In diesem Zusammenhang wurden verschiedene Arzt-Patientenverhältnisse geprüft, und insbesondere untersucht, ob die öffentlich-rechtlichen Krankenhäuser hoheitlich handeln.

Wenn ein Patient von seinem Arzt aufgrund eines privatrechtlichen Auftragsverhältnisses in einem (öffentlich-rechtlichen) Spital behandelt wird, basiert dessen Tätigkeit auf dem Obligationenrecht. Somit wird der Arzt in diesem Teilbereich als private Person betrachtet, womit die privatrechtlichen Bestimmungen des DSG anwendbar sind.

Der Datenschutz in kantonalen Spitälern ist eine Aufgabe der kantonalen Verwaltungsorganisation, weshalb die Kantone Regeln über den Umgang mit Personeninformationen in der öffentlichen kantonalen und kommunalen Verwaltung erlassen müssen. Auf die öffentlich-rechtlichen Spitäler findet daher das jeweilige kantonale Datenschutzgesetz Anwendung. Für den Kanton Zürich stellte sich die Frage, ob die öffentlich-rechtlichen Krankenhäuser hoheitlich handeln. Nach der bundesgerichtlichen Rechtsprechung gilt die Krankenbetreuung in öffentlichen Spitälern, soweit sie von Ärzten in amtlicher Eigenschaft ausgeübt wird, als hoheitliche, nicht als gewerbliche Tätigkeit des Gemeinwesens (BGE 102 II 47 und 101 II 183, bestätigt in BGE 115 Ib 179 E. 2). Demnach handeln die öffentlich-rechtlichen Spitäler hoheitlich und nehmen nicht am wirtschaftlichen Wettbewerb teil, womit das kantonale Datenschutzgesetz zur Anwendung gelangt.

6.3. Das Auskunfts- und Einsichtsrecht der Patienten

Das Auskunftsrecht ist ein zentrales Element des Datenschutzrechts, welches grundsätzlich jedem Patienten ermöglicht, seine Gesundheitsdaten inklusive Krankengeschichte einzusehen. In Ausnahmefällen können auch andere Personen (Dritte) Einsicht in die Krankengeschichte eines Patienten nehmen.

Das Auskunftsrecht ist grundsätzlich von der betroffenen Person selbst auszuüben (höchstpersönliches Recht) und niemand kann darauf verzichten. Wenn ein Patient aus physischen oder psychischen Gründen nicht in der Lage ist, sein Auskunftsrecht geltend zu machen, treten seine gesetzlichen Vertreter (beispielsweise Eltern oder ein Vormund) an seine Stelle. Das Auskunftsrecht kann unabhängig von einem Verfahren (beispielsweise Zivil- oder Strafprozess) geltend gemacht werden.

Wenn ein Dritter (beispielsweise ein Angehöriger) Einsicht in eine Krankengeschichte nehmen möchte, muss der Patient den Arzt vorher von seiner ärztlichen Schweigepflicht entbinden und seine Einwilligung in die entsprechende Bekanntgabe erteilen. Erst danach kann eine Krankengeschichte einem Dritten zur Einsicht vorgelegt werden. Eltern oder anderen gesetzlichen Vertretern steht kein Recht auf Ein-

sicht zu, wenn ein noch nicht mündiges aber urteilsfähiges Kind in einer ärztlichen Besprechung war und die Einwilligung zur Bekanntgabe der Diagnose an die Eltern nicht erteilen will.
Dem Einsichtsrecht kommt besonders in hängigen Prozessen und Verfahren eine bedeutende Rolle zu. Denn Parteien oder ihre Vertreter haben Anspruch auf Akteneinsicht. Für die Annahme eines das Einsichtsrecht überwiegenden öffentlichen oder privaten Interesses bedarf es immer "greifbarer wesentlicher Anhaltspunkte. In jedem Fall ist eine konkrete, sorgfältige und umfassende Abwägung der entgegenstehenden Interessen nach pflichtgemässem Ermessen vorzunehmen, wobei der Grundsatz der Verhältnismässigkeit zu beachten ist" (BGE 115 V 301f). Das heisst, in jedem Fall sind die besonderen Umstände und Interessen zu berücksichtigen.

Dritte können auch ohne Einwilligung der betroffenen Person Einsicht in Gesundheitsdaten von Verstorbenen erlangen, sofern
- der Gesuchsteller ein Interesse an der Einsicht nachweist und
- keine überwiegenden Interessen von Angehörigen der verstorbenen Person oder von Dritten (nahe Verwandtschaft oder Ehe) entgegen stehen (Art. 1 Abs. 7 VDSG).

Nach dem Tod des Patienten wird seine Krankengeschichte Dritten grundsätzlich nicht einfach zugänglich gemacht. Vorausgesetzt ist, dass zwischen dem Verstorbenen und der einsichtverlangenden Person eine enge Verbundenheit bestanden hat und ein Interesse an der Einsicht nachgewiesen wird (ohne entgegenstehende Interessen Dritter). Dann steht einer Einsichtsgewährung nichts entgegen.

6.4. Bekanntgabe-, Speicher- und Benutzerkontrolle im medizinischen Bereich

Damit der Datenschutz in der medizinischen Praxis wirksam umgesetzt werden kann, sind bestimmte technische Vorkehrungen unabdingbar. Dazu gehören Bekanntgabe-, Speicher- und Benutzerkontrollen. Die besten technischen Massnahmen nützen jedoch nur etwas, wenn sie von den Benutzern auch angewendet werden.

Die Bekanntgabekontrolle

Der Absender von Gesundheitsdaten muss gewährleisten, dass diese ausschliesslich an den berechtigten Empfänger gelangen. In jedem Fall muss nachträglich rekonstruierbar sein, wer, wem welche Daten zu welchen Zwecken bekanntgegeben hat. So kann zum Beispiel verhindert werden, dass Analyselabors die Resultate von HIV-Tests an unberechtigte Empfänger bekanntgeben.

Bei der Datenübermittlung per Fax ist nicht auszuschliessen, dass das Dokument an ein anderes als das gewünschte Ziel gelangt. Der Absender trägt die Verantwortung für die Übermittlung, weshalb er ein Interesse hat, dass die Informationen nicht in falsche Hände geraten. Bei besonders schützenswerten Personendaten empfiehlt es sich, den Empfänger zuvor zu unterrichten, damit der Zugang datenschutzgerecht sichergestellt werden kann. Die Übermittlung sollte verschlüsselt (chiffriert) erfolgen und das Faxgerät so aufgestellt sein, dass nur berechtigte Personen Einsicht in die empfangenen Dokumente nehmen können.
Falls irrtümlicherweise ein Fax einem falschen Empfänger zugestellt wird, sollte der Absender vom falschen Empfänger darüber orientiert werden. Auf dem Fax kann beispielsweise zusätzlich eine Klausel mit folgendem Inhalt angebracht werden: "Sofern Sie nicht der in der Adresse angeschriebene Empfänger sind, bitten wir Sie, den

Absender unverzüglich telefonisch zu benachrichtigen und anschliessend den Fax zu vernichten".

Speicherkontrolle

Damit gespeicherte Gesundheitsdaten nicht unbefugt verändert oder gelöscht werden können, müssen sich die Benützer durch Benützernachweis (User-ID) und Passwort über ihre Berechtigung ausweisen. Zum Schutz der Gesundheitsdaten vor Verlust sind zudem regelmässig Sicherungskopien zu erstellen, die in einem Tresor verwahrt werden sollten. Im übrigen muss verhindert werden, dass Gesundheitsdaten unerlaubterweise auf einen Datenträger - etwa eine Diskette - kopiert werden können. Dazu sind beispielsweise die Disketten-Laufwerke zu sperren.
Schriftliche Unterlagen haben einen hohen Beweiswert (beispielsweise bei haftpflichtrechtlichen Streitigkeiten), weil spätere Änderungen, Radierungen und Ergänzungen meist erkennbar sind. Bei elektronischen Aufzeichnungen ist das anders: Ein späteres Löschen, Hinzufügen und Korrigieren im System ersetzt bei den meisten Speichertechnologien das Bestehende, ohne Spuren zu hinterlassen. Damit die Beweiskraft der elektronischen Dokumentation erhöht wird, sollten Systeme verwendet werden, die ein Überschreiben einmal erfasster Daten und Texte ausschliessen und spätere Ergänzungen in einem Dokument als solche kennzeichnen. Auch die automatische Angabe des Datums jeder neuen Eingabe steigert die Fälschungssicherheit.

Benutzerkontrolle

Es ist zu verhindern, dass Unberechtigte via Einrichtungen zur Datenübertragung Zugriff zu Gesundheitsdaten erhalten. Die Systeme sind insbesondere so zu gestalten, dass die Vertraulichkeit und Integrität der Daten durch Einrichtungen zur Fernwartung sowie durch öffentlich zugängliche Netze nicht tangiert wird.

6.5. Arztgeheimnis bei der Evaluation der Arbeitsbelastung Kranken- und Pflegeheime im Kanton Waadt

Bei dieser Studie geht es dem Kanton Waadt darum, die Subventionen an Kranken- und Pflegeheime im Kanton möglichst gerecht zu verteilen. Sie wird in Zusammenarbeit mit den erwähnten Heimen nach einer in Québec entwickelten Methode vorgenommen. Wir wurden von den Verantwortlichen dieser Untersuchung gebeten, die datenschutzrechtlichen Fragen abzuklären, welche sich bei der Bekanntgabe von Daten an die Projektkoordinationsstelle in Lausanne sowie an die Datenerfassungszentrale in Montréal stellen.

Der Ablauf der Studie kann für jedes der teilnehmenden Heime in etwa folgendermassen beschrieben werden:

- Im Heim füllt das Pflegepersonal pro Heimbewohner einen Fragebogen aus, wobei unter den gelieferten Angaben auch besonders schüztenswerte Personendaten betreffend die körperliche und geistige Gesundheit des Heimbewohners figurieren.
- Die Fragebogen gehen über die Koordinationsstelle in Lausanne zur Datenerfassung und Kontrolle nach Québec. Während der Erfassung und im Anschluss daran wird jeder Fragebogen auf Vollständigkeit und bestimmte Plausibilitätskriterien geprüft.

- Um die dabei auftauchenden Fehler und Unvollständigkeiten beseitigen zu können, müssen die Datenkontrolleure aus Québec mit einer Person aus dem Pflegepersonal des betreffenden Heims Kontakt aufnehmen können, welche den Heimbewohner kennt, um den es beim betreffenden Fragebogen geht.

Die einfachste Variante, die Rückfragen über den Namen des betroffenen Heimbewohners abzuwickeln, würde nun aber eine Verletzung des Berufsgeheimnisses bedeuten. Es galt also, eine Möglichkeit zu finden, welche einerseits den Datenerfassern in Québec erlaubt, vom betroffenen Heim Auskünfte bezüglich bestimmter Bewohner zu erhalten. Andererseits musste sichergestellt werden, dass nur im Heim selbst die Verbindung zwischen bestimmten Personen und deren Krankheitsbildern oder Behandlungen verfügbar ist. Anschliessend wird die gefundene Lösung dargestellt, welche beide Anforderungen erfüllt:

- Das Heim erstellt eine Liste, worin jeder Person eine Nummer zugeteilt wird (Liste der Bewohner).
- Bevor die Fragebogen das Heim verlassen, werden die Namen darauf unkenntlich gemacht und durch die entsprechende Nummer ersetzt.
- Die datenbearbeitenden Personen in Québec können sich bei Rückfragen an das aus dem Fragebogen ersichtliche Heim wenden, müssen aber Informationen betreffend einen Bewohner über die auf dem Fragebogen angegebene Nummer verlangen.

6.6. Die Sondervorschrift betreffend das Auskunftsrecht bei Gesundheitsdaten - Interpretation

Artikel 8 Absatz 3 des DSG bestimmt, dass der Inhaber einer Datensammlung Daten über die Gesundheit der betroffenen Person durch einen von ihr bezeichnenden Arzt mitteilen lassen *kann*. Der Sinn dieser vielfach missverstandene Bestimmung und die sich daraus ergebende Interpretation sollen im folgenden kurz dargestellt werden.

Das Auskunftsrecht ist deshalb ein zentrales Element des Datenschutzes, weil niemand ein Begehren auf Richtigstellung oder Löschung ihn betreffender Daten verlangen kann, wenn er nicht weiss, welche Daten der Inhaber einer Datensammlung über ihn bearbeitet. Aus diesem Grund ist das Auskunftsrecht im DSG und in der VDSG eingehend geregelt, wobei grundsätzlich ein Anspruch auf schriftliche und kostenlose Auskunft vorgesehen ist. Die Sondervorschrift von Artikel 8 Absatz 3 DSG lautet: “Daten über die Gesundheit kann der Inhaber einer Datensammlung der betroffenen Person durch einen von ihr bezeichneten Arzt mitteilen lassen.”

Diese Ausnahmebestimmung zur Regel der direkten schriftlichen Auskunft hat einen sehr begrenzten Anwendungsbereich. Es geht dabei um Fälle, wo der um Auskunft ersuchenden Person aus unvorbereiteter und direkter Auskunft ein sogenannter Aufklärungsschaden entstehen könnte. Dass die Vorschrift eng auszulegen ist, ergibt sich einerseits aus der in ihr durchschimmernden nicht mehr zeitgemässen Bevormundungstendenz. Andererseits spricht auch die Tatsache für eine enge Auslegung, dass der Gesetzgeber die Formulierung *kann* und nicht *muss* gewählt hat. Hingegen darf aus der Kann-Formulierung nicht geschlossen werden, dass der Inhaber der Datensammlung das Recht hat, die Auskunft über einen Arzt erteilen zu lassen. Vielmehr muss der Inhaber der Datensammlung diesen Weg vorschlagen, wenn die Wahrscheinlichkeit einer gravierenden Schädigung durch direkte Auskunfterteilung hoch ist. In allen anderen Fällen hat eine direkte schriftliche Auskunft an die betrof-

fene Person zu erfolgen.

6.7. Aushändigung eines ärztlichen Zeugnisses an die Erben des Verstorbenen

Das Auskunftsrecht gemäss Artikel 8 DSG steht nur der betroffenen Person zu. Artikel 1 Absatz 7 VDSG regelt die Einsicht in Daten von verstorbenen Personen und ist daher streng genommen kein Anwendungsfall des Auskunftsrechts. Die Frage, ob der Ehefrau eine Kopie des ärztlichen Zeugnisses auszuhändigen sei, welches das behandelnde Krankenhaus über den Todesfall ihres Ehemannes ausgestellt hat, haben wir bejaht.

Im konkreten Fall hatte eine Versicherung der Witwe die Herausgabe einer Kopie des ärztlichen Zeugnisses verweigert, welches das behandelnde Krankenhaus über den Todesfall ihres Mannes angefertigt hatte. Als Begründung wurde angegeben, ohne Vollmacht des Arztes dürften keine medizinischen Unterlagen an Dritte weitergegeben werden. Die von der Witwe diesbezüglich ans Bundesamt für Sozialversicherung gerichtete Anfrage wurde von diesem an uns weitergeleitet mit der Bitte, zur Problematik aus datenschutzrechtlicher Sicht Stellung zu nehmen.

Wir kamen zum Schluss, dass dem Begehren der Witwe stattgegeben werden kann. Zwar steht das Recht auf Auskunft gemäss Artikel 8 DSG ausschliesslich der betroffenen Person zu und ist nicht übertragbar, weder unter Lebenden noch durch Verfügung von Todes wegen. Abgesehen von Fällen, wo die betroffene Person nicht urteilsfähig ist und daher beispielsweise die Eltern als gesetzliche Stellvertreter das Auskunftsrecht geltend machen können, weil sie ihr Kind gegen aussen vertreten, steht das Auskunftsrecht selbst Verwandten nicht zu. Diese können höchstens ein eigenes Auskunftsrecht ausüben, wenn ein solches gegeben ist. Artikel 1 Absatz 7 VDSG verleiht nahen Verwandten von verstorbenen Personen grundsätzlich ein solches Einsichtsrecht, das aber durch allfällige überwiegende Interessen von Angehörigen der verstorbenen Person oder von Dritten begrenzt wird. Als Dritter kommt in solchen Fällen auch der behandelnde Arzt in Frage, weshalb nicht von vornherein auszuschliessen ist, dass das Einsichtsrecht in dessen überwiegenden Interessen seine Grenze findet. Die Abwendung von allfälligen Schadenersatzansprüchen kann ein solches überwiegendes Interesse aber jedenfalls nicht begründen.
In die Interessenabwägung miteinzubeziehen ist darüberhinaus der Schutz der Privatsphäre der verstorbenen Person. So hat das Bundesgericht in einem Entscheid vom 26. April 1995 bestätigt, dass die Einsicht in medizinische Akten einer Verstorbenen deren Sohn nur über einen Arzt zu gewähren sei. Zur Begründung führte es insbesondere an, dass diese Vorgehensweise erlaube, einerseits dem Sohn Einsicht zu erteilen, soweit dies gerechtfertigt sei, andererseits die Vertraulichkeit der medizinischen Daten zu wahren. Daraus ist unter anderem zu schliessen, dass - wenn auch nahe Verwandtschaft gemäss Artikel 1 Absatz 7 VDSG ein Interesse begründet - der Zweck des Einsichtsbegehrens im Rahmen einer detaillierten Interessenabwägung ebenfalls zu berücksichtigen ist. Im vorliegenden Fall wurde - anders als im angesprochenen Bundesgerichtsentscheid - bloss die Herausgabe der Kopie eines einzelnen Arztzeugnisses und nicht Einsicht in die gesamte Krankengeschichte verlangt. Daher muss auch die Abwägung der Interessen nicht gleichermassen detailliert ausfallen und dem zu beurteilenden Auskunftsbegehren steht nichts entgegen.

6.8. Die Entwicklung des Systems MediData

Die MediData AG hat sich zum Ziel gesetzt, den elektronischen Datenaustausch zwischen allen Partnern im schweizerischen Gesundheitsmarkt zu fördern. Anstelle des Verkehrs von gedruckten Rechnungen und Gutsprachen sollen sogenannte UN/EDIFACT-Nachrichten ausgetauscht und die Geschäftsabwicklung rationalisiert werden. Aus datenschutzrechtlicher Sicht negativ zu bewerten ist die Tatsache, dass zu den Partnern zwar die Versicherer und die Leistungserbringer, nicht aber die Versicherten selbst zählen. Positiv ist zum im Aufbau stehenden System zu sagen, dass der Frage der Vertraulichkeit der Daten bei der Übertragung Beachtung geschenkt wird.

Die UN/EDIFACT-Norm ermöglicht den elektronischen Austausch von standardisierten Nachrichten. Mit diesem z.B. im internationalen Handel schon in grossem Umfang eingesetzten Verfahren können Routineabläufe rationeller abgewickelt werden. Derartige Rationalisierungseffekte auch auf dem “Gesundheitsmarkt” zu erreichen, ist Ziel der MediData AG, deren Aktien hauptsächlich von Versicherungsgesellschaften gehalten werden. Eine Möglichkeit, Zeit und Kosten zu sparen besteht aber nur dort, wo ähnlich strukturierte Nachrichten mit einer bestimmten Häufigkeit ausgetauscht werden. Daher ist der elektronische Nachrichtenaustausch auch nur zwischen Versicherern und Leistungserbringern vorgesehen. Vor allem für Nachrichten, die medizinische Daten über Patienten beinhalten, ist es datenschutzrechtlich unbefriedigend, dass der Betroffene nicht in den Kreislauf miteinbezogen wird.
Bezüglich des im Aufbau begriffenen Systems wird der EDSB insbesondere drei Punkte beobachten:

- Aus Sicht des Datenschutzes ist beim angestrebten elektronischen Nachrichtenaustausch die Frage nach dem Ausmass der medizinischen Daten zentral, welche jede elektronisch vom Leistungserbringer zur Versicherung übermittelte Rechnung begleiten. Es ist klar und auch im Bundesgesetz über die Krankenversicherung (KVG) vorgesehen, dass bestimmte für die routinemässige Rechnungsprüfung unentbehrliche Angaben immer übermittelt werden müssen. Ebenso eindeutig ist aber, dass die Bekanntgabe von genauen Diagnosen an den Versicherer nur im Einzelfall und auf Anfrage hin erfolgen darf (siehe dazu auch S. 39 über die systematische Bekanntgabe der Diagnose an Krankenkassen).
- Das im KVG vorgesehene Recht der Versicherten zu verlangen, dass medizinische Angaben nur dem Vertrauensarzt der Versicherung bekanntgegeben werden, darf nicht ausgehöhlt werden.
- Weil die Mehrheit der Benützer Bundesorgane sind, sollte untersucht werden, ob die notwendigen Rechtsgrundlagen vonhanden sind, die eine solche Datenbearbeitung mittels eines solchen Systems (MediData) legitimieren.

7. Kreditwesen

7.1. Die Datenbearbeitung bei Kreditkartenanträgen

Wer eine Kreditkarte beantragt, willigt in die Überprüfung seiner Angaben und in die Bekanntgabe an bestimmte Stellen ein. Eine Bekanntgabe dieser Informationen an weitere Dritte ohne Orientierung des Antragstellers erfolgt ohne Rechtfertigungsgrund.

Eine private Person gelangte wegen einer unrichtigen Angabe auf ihrer neu ausgestellten Kreditkarte an den Eidgenössischen Datenschutzbeauftragten und ersuchte um Abklärung. In der Folge wurden der Ablauf des Antragsverfahrens, das Antragsformular und die Allgemeinen Geschäftsbedingungen der betreffenden Kreditkartenunternehmung einer näheren Prüfung unterzogen.
Auf dem Kreditkartenantrag erhebt die betreffende Kreditkartenunternehmung folgende Kundendaten: Name, Vorname, Adresse, Geburtsdatum, Nationalität, Zivilstand, Beruf, berufliche Stellung, Einkommen, Bankverbindungen, Benützung anderer Kreditkarten, Zahlungsmodalitäten und die Unterschrift des Gesuchstellers. Auf Zusatzkartenanträgen werden Name, Vorname, Geburtsdatum und Heimatort der Zusatzperson erhoben.
Der Antragsteller bestätigt mit seiner Unterschrift die Richtigkeit der gemachten Angaben und gestattet der Kreditkartenunternehmung, diese jederzeit zu überprüfen. Gleichzeitig stimmt er den Allgemeinen Geschäftsbedingungen zu und die Kreditkartenunternehmung sichert die vertrauliche Behandlung aller Angaben zu.

Die Daten werden zur Überprüfung der Personalien und der Bonität des Antragstellers sowie für die anschliessende Geschäftsführung erhoben. Die Richtigkeit der Personalien wird anhand des elektronischen Telefonverzeichnisses geprüft. Sofern der Kunde dort nicht vermerkt ist, wird die Einwohnerkontrolle seiner Wohngemeinde angefragt. Die Bonität des Antragstellers wird elektronisch beim Verein zur Führung einer Zentralstelle für Kreditinformation (ZEK) geprüft. Bei besonders unsicheren finanziellen Verhältnissen wird zudem die Vereinigung der Kartenherausgeber der Schweiz (KARTAC) angefragt, die Informationen über die Zahlungsfähigkeit der Kunden in der Schweiz führt. Je nach Situation werden bei der Einwohnerkontrolle, bei den Schuldbetreibungs- und Konkursämtern oder bei der Steuerbehörde zusätzliche Informationen eingeholt. Bevor weitere Dritte angefragt werden, wird mit dem Antragsteller Rücksprache genommen.

Die betreffende Kreditkartenunternehmung ist Miglied der KARTAC, welche ihrerseits Mitglied der ZEK ist. Die Kreditkartenunternehmung gibt der KARTAC Finanzdaten der betroffenen Personen wie Betreibungen, Gründe für Kartensperrungen (beispielsweise Privatkonkurs), Zahlungsmoral und Zahlungsfähigkeit bekannt, welche wiederum von anderen Mitgliedern weiterverwendet werden können.
Indem der Antragsteller den Allgemeinen Geschäftsbedingungen zustimmt, ermächtigt er die Kreditkartenunternehmung, *"alle erforderlichen Auskünfte zur Beurteilung der Kartenbestellung einzuholen. Das heisst, er willigt in die Übermittlung der Daten im erforderlichen Umfang ein, die sich aus den Auftragsunterlagen oder allgemein zugänglichen Dokumenten im Verlaufe der Vertragsdurchführung ergeben oder an durch die Kreditkartenunternehmung bestimmte Dritte (beispielsweise Zentralstellen) zur Beurteilung des Risikos und zur Abwicklung des Vertrages nötig sind. Den Zentralstellen ist es ausdrücklich gestattet, diese Daten anderen Mitgliedern der jeweiligen Zentralstelle zugänglich zu machen. Diese Einwilligung gilt auch für entsprechende Prüfungen bei anderweitig beantragten Kreditkarten und bei künftigen Bestellungen".* Mit diesen Angaben wird der Kunde vage über die Bekanntgabe seiner Daten informiert, aber er weiss nicht, wer hinter den Zentralstellen und ihren Mitgliedern steht und welche Daten bekanntgegeben werden.

Eine Verletzung der Persönlichkeit ist nicht widerrechtlich, wenn sie durch Einwilligung des Verletzten (betroffene Person) gerechtfertigt ist. Damit die betroffene Person ihre Einwilligung wirksam erteilen kann, muss sie jedoch umfassend über die Bearbeitung ihrer Personendaten und den Zweck orientiert werden. Wer einen Kre-

ditkartenantrag unterzeichnet, gibt stillschweigend sein Einverständnis zur Bearbeitung seiner Personendaten durch den Vertragspartner, auch zur Speicherung und späteren Verwendung, nicht aber zur Bekanntgabe an nicht klar bestimmte Dritte. Da der Kunde seine Einwilligung zur Bearbeitung und Überprüfung erteilt, sollten seine Angaben nicht unbestimmten Dritten zu unbekannten Zwecken bekanntgegeben und damit von anderen Unternehmungen weiterverwendet werden können, weshalb der Rechtfertigungsgrund der Einwilligung nicht erfüllt ist.
Die Überprüfung und Bearbeitung der Kreditkartenanträge durch die Kreditkartenunternehmung selbst erfolgt in unmittelbarem Zusammenhang mit der Abwicklung eines Vertrages, womit ein überwiegendes Interesse durchaus zu bejahen und die Bearbeitung der Personendaten intern gerechtfertigt ist.
Angesichts der zahlreichen Kreditkartenanträge (Massengeschäft), die vom betreffenden Kreditunternehmen täglich geprüft werden, ist eine minimale Fehlerquote (unrichtiges Datum auf neu ausgestellter Kreditkarte) nicht vermeidbar.
Da die effektiv vorgenommene Bearbeitung der Personendaten weder aus dem Antrag noch aus den Allgemeinen Geschäftsbedingungen vollständig und klar hervorgeht, sind für den Antragsteller weder der Zweck, noch die genauen Empfänger und deren weitere Bearbeitung ersichtlich. Dies bedeutet, er weiss nicht hinreichend, wozu er einwilligt (kein genügendes Selbstbestimmungsrecht über seine Daten) beziehungsweise, er kann eine Datenbearbeitung nicht verweigern. Aus diesem Grund sind der Antrag und die Allgemeinen Geschäftsbedingungen für eine Kreditkarte zu präzisieren. Jeder Antragsteller muss erkennen können, an wen seine Personendaten zur Prüfung bekanntgegeben werden und wozu er die Einwilligung sonst noch erteilt. Bevor der Kunde ein Vertragsverhältnis eingeht, ist ihm Gelegenheit zu geben, sich umfassend über folgende Punkte zu informieren (beispielsweise in einem Merkblatt oder den Allgemeinen Geschäftsbedingungen):

- Wer ist Inhaber der Datensammlung?
- Worin besteht der Zweck der Datenbearbeitung?
- Bei welchen Stellen/Behörden werden Daten überprüft?
- Welche Daten werden wem und zu welchen Zwecken bekanntgegeben (bei juristischen Personen sind die Empfänger oder Mitglieder näher zu präzisieren) ?
- Wie erfolgt die Art und Weise der Bekanntgabe (on-line oder auf Papier) und Aufbewahrung?

In der Folge wurde die Kreditkartenunternehmung gebeten, die Anträge für Kreditkarten und/oder die Allgemeinen Geschäftsbedingungen entsprechend zu revidieren.

7.2. Auskunftserteilung bei abgelehnten Kreditkartenanträgen

Obwohl in den Allgemeinen Geschäftsbedingungen einer Kreditkartenunternehmung steht, über abgelehnte Kreditkartenanträge werde keine Korrespondenz geführt, muss das Auskunftsrecht gewährt werden. Ein Passus im Kreditkartenantrag oder in den Allgemeinen Geschäftsbedingungen, der jegliche Auskunft ausschliesst, ist ungültig.

Eine Kreditkartenunternehmung muss einer Person, die Auskunft verlangt, grundsätzlich kostenlos alle über sie in der Datensammlung vorhandenen Daten mitteilen. Zudem sind der Zweck und die Kategorien der bearbeiteten Personendaten, sowie an der Sammlung Beteiligte und die Datenempfänger anzugeben. Die schriftliche Auskunft oder der begründete Entscheid über die Beschränkung des Auskunftsrechts muss innert dreissig Tagen seit dem Eingang des Auskunftsbegehrens erteilt

werden. Ansonsten hat der Inhaber der Datensammlung dem Gesuchsteller die Frist mitzuteilen, innerhalb derer die Auskunft erfolgen wird. Die Auskunft kann nur verweigert, eingeschränkt oder aufgeschoben werden, wenn ein formelles Gesetz dies vorsieht, oder wenn es wegen überwiegender Interessen eines Dritten, oder aus überwiegenden eigenen Interessen erforderlich ist und die Personendaten nicht an Dritte bekanntgegeben werden. Falls der Inhaber der Datensammlung die Auskunft verweigert, einschränkt oder aufschiebt, muss er den Grund angeben. Ein Vermerk im Kreditkartenantrag oder in den Allgemeinen Geschäftsbedingungen, welcher das Auskunftsrecht ausschliesst, ist nicht gültig, da das Auskunftsrecht höchstpersönlich und unverzichtbar ist.
Sofern die Auskunft verweigert wird, steht der betroffenen Person die Möglichkeit offen, gegen die Kreditkartenunternehmung eine Klage zum Schutz der Persönlichkeit einzureichen. Klagen zur Durchsetzung des Auskunftsrechts können am Wohnsitz des Klägers oder der Beklagten eingereicht werden.

7.3. Schutzlose Gläubiger wegen Datenschutz?

Ein Gläubiger, der von seinem Schuldner einen Verlustschein erhalten hat, muss sich bei zweifelhaften Angaben an das zuständige Schuldbetreibungs- und Konkursamt wenden und nicht an die Steuerbehörde oder den Arbeitgeber.

Ein Gläubiger hatte einen Verlustschein erhalten, dessen Inhalt ihm zweifelhaft erschien. Darauf wollte er bei den Steuerbehörden und beim Arbeitgeber überprüfen, ob die Angaben den effektiven Verhältnissen entsprachen. Die Steuerbehörde und der Arbeitgeber beriefen sich auf den Datenschutz und erteilten keine Auskünfte. Der Gläubiger sah sich in seinen Rechten als freier Bürger beschnitten und beschwerte sich bei uns.
Verlustscheine sind öffentliche (betreibungsrechtliche) Urkunden, die volle Gültigkeit haben, solange nicht deren Unrichtigkeit nachgewiesen wird. Die Richtigkeit der Angaben auf einem Verlustschein muss von den zuständigen Betreibungsbeamten oder der Aufsichtsbehörde des Betreibungsamtes geprüft werden. Weder die Steuerbehörde, noch der Arbeitgeber dürfen einem Gläubiger Auskunft über die Richtigkeit beziehungsweise Unrichtigkeit der Angaben auf einem Verlustschein erteilen. Schuldbetreibungs- und Konkursregister werden vom Geltungsbereich des DSG gar nicht erfasst, da sie besonderen, strengen Regeln unterstehen. Deshalb kann nicht gesagt werden, dass die Gläubiger aufgrund datenschutzrechtlicher Bestimmungen benachteiligt werden.

8. Direktmarketing

8.1. Allgemeine Problematik

Immer wieder wird uns von betroffenen Personen mitgeteilt, dass sie trotz Sperrung ihrer Adresse für Werbezwecke und sogar ausdrücklicher Abmahnung einer bestimmten Firma von dieser adressiertes Werbematerial erhalten. Wir suchen seit längerem nach Wegen, um solche Fälle zu vermeiden.

Bereits im ersten Tätigkeitsbericht haben wir auf die Problematik hingewiesen (S. 68 f.). Wir haben damals festgehalten, dass die Unüberschaubarkeit und Un-

kontrollierbarkeit der Datenbearbeitungen ein besonderes Problem darstellt, da es oft nicht möglich ist, den Ursprung einer Adresse zu eruieren und die bestehenden Möglichkeiten der Adresssperrung (PTT und Robinsonliste) nicht ausreichen, um die unerwünschte Zustellung von adressiertem Werbematerial zu unterbinden. Seither haben wir regelmässig Beanstandungen von Personen erhalten, die trotz Sperrung ihrer Adresse und vielfach trotz ausdrücklichem Verbot weiterer Werbesendungen an eine bestimmte Firma, weiterhin Werbematerial zugestellt erhielten.
Wir haben daraufhin im Frühjahr 1995 eine Umfrage bei den Branchenverbänden gemacht. Diese Umfrage enthielt einen allgemeinen Teil zuhanden der Dachverbände, worin die Problematik der fehlenden Transparenz, der wirksamen Adresssperrung, des Verstosses gegen allgemeine Grundsätze der Datenbearbeitung (insbesondere gegen den Zweckbindungsgrundsatz) und schliesslich das besondere Problem der Telefon- und Faxwerbung angesprochen wurde. Zu jedem Problemkreis wurden Lösungsvorschläge präsentiert und die Dachverbände gebeten, dazu Stellung zu beziehen. In einem besonderen Teil zuhanden der Firmen, die Direktmarketing betreiben, wurden Angaben zum Tätigkeitsbereich, zu den bearbeiteten Personendaten, zur Bearbeitungsweise, zu den Rechten der betroffenen Personen und zur internen Organisation (Verantwortung für Datenbearbeitung, getroffene Sicherheitsmassnahmen usw.) erbeten. Dieser Teil konnte auch anonym ausgefüllt werden.

Leider erhielten wir nur wenige Antworten auf unsere Umfrage. Verschiedene Dachverbände unter Federführung der Schweizer Werbewirtschaft verlangten eine Besprechung mit uns und sistierten bis dahin die Beantwortung der Umfrage durch ihre Mitglieder. An der Besprechung, die am 18. Oktober 1995 stattfand, waren der Schweizerische Verband für Direktmarketing, der Verband des Schweizerischen Versandhandels und die Schweizer Werbewirtschaft vertreten. Sie teilten uns mit, dass die Branche bereits einen hohen Grad an Selbstregulierung mittels verschiedener Ehrenkodices habe und sehe sich nicht veranlasst, im Bereich Datenschutz spezifisch tätig zu werden.
Aufgrund dieser mangelnden Unterstützung durch die Dachverbände haben wir die für uns dringend notwendigen Informationen über die Datenbearbeitungen der Direktmarketingsfirmen nicht erhalten. Wir haben deshalb beschlossen, im Verlaufe dieses Jahres bei mehreren Direktmarketingsfirmen aus verschiedenen Tätigkeitsbereichen Kontrollen durchzuführen und uns über die Datenbearbeitungen vor Ort ein Bild zu machen, um aufgrund der erhaltenen Kenntnisse eine Beurteilung aus datenschutzrechtlicher Sicht zu jedem Problembereich zu erstellen.

8.2. Weitergabe von Sternchen in privaten Abonnentenverzeichnissen

Personen, die keine Werbesendungen zu erhalten wünschen, können bei den PTT ihre Adresse oder Faxnummer für Werbezwecke sperren lassen. Sie erscheint dann im Telefonbuch mit einem Stern (*). Die PTT dürfen solche Adressen zur Herstellung privater Abonnentenverzeichnisse weitergeben. Dabei wird die Sperrung nicht immer übernommen, was zum Erhalt zahlreicher Werbeanschriften führen kann.

Zu dieser Problematik erhielten wir im letzten Jahr gleich mehrere Anfragen. Einerseits erkundigte sich ein Adressbearbeiter, unter welchen Voraussetzungen er Adressen aus Telefonbüchern, regionalen Verzeichnissen oder elektronischen Verzeichnissen zu kommerziellen Zwecken verwenden dürfe. Andererseits beschwerten sich verschiedene Personen darüber, dass sie trotz Sperrung der Adresse oder Faxnummer für Werbezwecke bei den PTT Werbeanschriften oder -anrufe erhielten.

Schliesslich machte uns ein kantonaler Datenschutzbeauftragter darauf aufmerksam, dass verschiedene elektronische Verzeichnisse auf Datenträger die Sperrungen nicht übernähmen.
Die Verordnung über die Fernmeldedienste sieht vor, dass Daten von Abonnenten, die keine Werbung wünschen, nur zur Herstellung privater Abonnentenverzeichnisse weitergegeben werden dürfen. Die PTT haben die Bedingungen für die Weitergabe festzulegen und dabei die Vorschriften über den Datenschutz zu beachten. Der Verkauf von PTT-Kundenadressen an Dritte ist in einer dienstlichen Weisung geregelt. Diese sieht vor, dass die Weitergabe von Daten zur Herstellung privater Abonnentenverzeichnisse auch dann erlaubt ist, wenn der Kunde keine Werbung wünscht und "die Adresse zur Weitergabe gesperrt hat". Für den Verkauf gesperrt sind die Adressen von Telefon- und Telefax-Abonnenten, welche die Weitergabe ihrer Adresse untersagten. Diese Adressen werden jedoch zur Herstellung privater, lokaler Telefonverzeichnisse und von CD-ROMs geliefert. In den gedruckten Verzeichnissen erscheint der Stern vor der Rufnummer und auf Bildschirmausgaben ab CD-ROM der Hinweis "Wünscht keine Werbung" (die Sperrmöglichkeiten existieren heute für die Verzeichnisse des Telefon- und Telefaxdienstes, aber nicht für das Videotex- und Telexverzeichnis). Ein gleichlautender Passus findet sich in den Bedingungen für die Lieferung von Adressen aus dem Bestand der Telecom-PTT Verzeichnisse, wobei präzisiert wird, dass insbesondere das Weiterverarbeiten solcher Einträge für Direct Mailings nicht statthaft ist. Handelt der Käufer diesen Lieferungsbedingungen zuwider, so kann die Telecom-PTT die Datenlieferungen unverzüglich, nötigenfalls endgültig, einstellen.

Die Generaldirektion der PTT hat uns gegenüber bestätigt, dass die PTT einen Hersteller von Abonnentenverzeichnissen, der fälschlicherweise die Sperrung für Werbezwecke nicht weitergibt, auf seine Pflicht hinweisen und bei weiteren Zuwiderhandlungen die Adresslieferung einstellen würden. Abklärungen bei verschiedenen Herstellern von Datenträgern, die das Elektronische Telefonverzeichnis wiedergeben, ergaben, dass die Sperrungen zwar ursprünglich nicht übernommen worden waren (in der Regel aufgrund technischer Schwierigkeiten) aber in der Folge dann berücksichtigt wurden.

9. Statistik

9.1. Volkszählung 2000

Die Vorbereitungen für die Volkszählung 2000 sind in vollem Gange. Die Arbeiten für die Einführung einer anderen Erhebungsmethode konzentrieren sich jetzt auf die Probleme der technischen Durchführbarkeit und auf die rechtlichen Rahmenbedingungen, die eine Volkszählung mittels Registern (indirekte Erhebung) erlauben würden. In der Zwischenzeit hat die Geschäftsprüfungskommission des Nationalrates den Bundesrat beauftragt, neue Lösungen für die Erhebungsmethode der Volkszählung zu prüfen.

Wir haben schon im zweiten Tätigkeitsbericht (S. 42) dargelegt unter welchen datenschutzrechtlichen Rahmenbedingungen die Erhebungsmethode der Volkszählung geändert werden kann.
Eine Volkszählung mittels Registern (indirekte Erhebung) ist einer Erhebung mittels

Fragebogen (direkte Erhebung) aus verschiedenen Gründen vorzuziehen. Die Hauptgründe sind:

- der Aufwand von Gemeinde-, Kantons- und Bundesbehörden kann kostengünstiger gestaltet werden;
- die Effizienz bzw. die Aussagekraft der Volkszählungdaten kann mit weniger Aufwand gesteigert werden (Rationalisierung der Erhebungsvorgänge);
- die Akzeptanz der Volkszählung in der Bevölkerung kann gesteigert werden, indem die Belastung der Befragten verringert wird.

In diesem Sinn hat die Geschäftsprüfungskommission des Nationalrates den Bundesrat beauftragt, zwei Aspekte zu prüfen:

Die Vereinfachung der Volkszählung 2000
Im Rahmen der heutigen Möglichkeiten soll eine vereinfachte und kostengünstigere Erhebungsmethode angewendet werden. Um diese Zielsetzung zu unterstützen, ist auch die Harmonisierung der verwaltungstechnischen Datenregister von Bund, Kantonen und Gemeinden zwecks statistischer Ziele zu prüfen. Dazu sollen auch die Massnahmen zur Förderung der Zusammenarbeit von Bund, Kantonen und Gemeinden im Bereich der Harmonisierung der regionalen Datenregister geprüft werden.

Die Neuausrichtung der Volkszählung 2010
Damit die Volkszählungsdaten mittels Register erhoben werden können (Registererhebung), soll der Bundesrat die notwendigen verfassungsmässigen und gesetzlichen Grundlagen schaffen, welche auch die Harmonisierung der Register der Kantone und Gemeinden ermöglichen.

Wie wir schon im zweiten Tätigkeitsbericht erwähnt haben, ist eine Revision der Erhebung der Volkszählungsdaten durchaus positiv zu bewerten. In diesem Zusammenhang muss der Zweckbindungsgrundsatz des Datenschutz- und des Statistikgesetzes respektiert werden. Das heisst, dass Personendaten grundsätzlich nur für den ursprünglichen Erhebungszweck verwendet werden dürfen. Das Volkszählungsgesetz schliesst sogar jede nichtstatistische Verwendung der Volkszählungsdaten aus.

Wir sind nach wie vor der Auffassung, dass Daten, die für statistische Zwecke (Volkszählungsdaten) erhoben wurden, nicht gleichzeitig oder nachträglich für Verwaltungszwecke verwendet werden dürfen. Auch die Daten einer registergestützten Erhebung sollen nur für statistische Zwecke verwendet werden. Das Bundesstatistikgesetz sieht zwar eine Bestimmung vor, welche die Verwendung von Personendaten, die ursprünglich für statistische Zwecke erhoben wurden, zu anderen Zwecken erlaubt. Diese ist jedoch nur für Ausnahmefälle gedacht und bedarf einer formellen gesetzlichen Grundlage.
Im Gegensatz zum schweizerischen Bundesstatistikgesetz verbietet die europäische Gesetzgebung (Europäische Union und Europarat) jede nichtstatistische Verwendung von Personendaten, die ursprünglich zu statistischen Zwecken erhoben wurden.

9.2. Der Aufbau von gesamtschweizerischen Datenbearbeitungssystemen

Der Aufbau von zentralen Datenbearbeitungssystemen, welche Personendaten über

die gesamte Schweizer Bevölkerung für statistische Zwecke bearbeiten, kann aus der Sicht des Datenschutzes problematisch werden.

Die Aufgaben der amtlichen Statistik sind in der heutigen Zeit von grosser Bedeutung, insbesondere weil mittels statistischer Informationen die Öffentlichkeit aufgeklärt wird, die Betriebe ihre Unternehmenspolitik planen, der Staat Entscheide trifft und Ziele definiert. Damit gesamtschweizerische statistische Werte erzielt werden können, müssen Personendaten der gesamten Bevölkerung erfasst und bearbeitet werden. Die Bearbeitung einer grossen Menge von Daten ist effizienter, wenn die Daten über zentrale Register verwaltet werden.
Die für die Statistik notwendigen Personendaten werden entweder direkt in der Bevölkerung oder indirekt über Register der kantonalen Verwaltungen und der Bundesverwaltung erhoben. Für die Verwaltung oder Auswertung der erhobenen Daten, und um zeitraubende kostspielige periodische Erhebungen zu verringern, können sogenannte Hilfsdatensammlungen eingesetzt werden. Hilfsdatensammlungen beinhalten Merkmale oder Daten, welche verschiedene andere Datensammlungen miteinander verknüpfen können. In einigen Fällen sind diese Merkmale Personendaten (Adresse, Wohnort usw.) oder können die Identifikation von Personen ermöglichen. Aus der Sicht des Datenschutzes sind solche Datensammlungen nicht problematisch, soweit sie ausschliesslich statistischen Zwecken (Kombination von Resultaten, Erleichterung von Erhebungen) dienen.

Bis vor einiger Zeit war die Erstellung von zentralen Registern (sei es für administrative oder statistische Zwecke) wegen der föderalistischen Struktur der Schweiz nicht einfach. Die Kantone führen eigene, ihren Bedürfnissen angepasste Register und gleichzeitig haben die zuständigen Bundesbehörden Register, welche Daten auf gesamtschweizerische Ebene bearbeiten. Damit die Koordination zwischen kantonalen und Bundesaufgaben an Effizienz gewinnt und vor allem, um die Kosten von Datenbearbeitungen zu senken, wird die Erstellung von zentralen gesamtschweizerischen Registern bevorzugt und gefördert. Unabhängig von den bestehenden rechtlichen Problemen, die dem Aufbau und der gemeinsamen Erstellung von zentralen Registern im Wege stehen, hat die zentrale Datenbearbeitung aus der Sicht des Datenschutzes sowohl Vorteile als auch Nachteile.

Vor allem wegen der Effizienzsteigerung und der Kostensenkung ist die Führung von zentralen Datenbearbeitungssystemen vorteilhaft. Diese Art der Bearbeitung birgt aber Gefahren, die unter bestimmten Umständen das Risiko einer Persönlichkeitsverletzung erhöhen. Die zentrale Datenbearbeitung erhöht aus organisatorischer Sicht die Gefahr, dass die Daten unrechtmässig bearbeitet werden. Hinzu kommt, dass die betroffenen Personen die Übersicht über die unzähligen Datenbearbeitungen, die mit ihren Daten gemacht werden, schlicht verlieren. So gesehen gewährleisten lokale kleinere Systeme eine bessere Übersicht und sind kleineren Gefahren ausgesetzt.

Wir sind nicht gegen die Schaffung zentraler Datenbearbeitungssysteme. Grundsätzlich teilen wir die Auffassung anderer Behörden der Kantone und des Bundes, dass die effiziente und kostengünstige zentrale Datenbearbeitung von Personendaten notwendig ist. Sie soll aber für den Einzelnen übersichtlich und transparent gestaltet werden. Das heisst, der Bürger soll jederzeit wissen, von welchen Behörden und für welche Zwecke seine Daten bearbeitet werden.
Insbesondere dürfen Personendaten oder Datensammlungen, die ausschliesslich für statistische Zwecke erhoben oder erstellt wurden, nicht für Verwaltungszwecke ver-

wendet werden. Die Effizienz- und Kostenfrage darf nicht als Argument für eine Zweckentfremdung dienen.

Wir werden diese Entwicklung aufmerksam verfolgen müssen, weil die Vergangenheit gezeigt hat, dass zentrale Register, die ursprünglich für statistische Zwecke erstellt wurden, schon nach wenigen Jahren für Kontroll- und Verwaltungsaufgaben verwendet werden.

9.3. Kriterien für die Anonymisierung von Personendaten ?

Im letzten Geschäftsjahr wurden wir mehrmals aufgefordert, uns zum Begriff der anonymen Daten zu äussern. Man nimmt offenbar an, dass eine generelle Regel existiert, die für alle Fälle der Anonymisierung von Personendaten angewendet werden kann. Die Merkmale, welche die Identifikation einer Person ermöglichen, sind jedoch nicht abschliessend zu definieren. Deshalb müssen die Kriterien der Anonymisierung von Personendaten für jeden Einzelfall besonders definiert werden.

Personendaten gelten als anonymisiert, wenn diejenigen Daten entfernt werden, welche die Identifizierung der betroffenen Person ermöglichen. Wird der Bezug von Daten zu einer bestimmten Person aufgehoben, verlieren sie den Charakter von Personendaten. Welche Identifikationsmerkmale im Einzelfall entfernt werden müssen, um die Bestimmbarkeit des Betroffenen auszuschliessen, hängt jeweils vom Einzelfall ab. Häufig genügt die Löschung von Name und Adresse. Falls aber besondere Merkmale die Identifizierung des Betroffenen ermöglichen, gelten die betreffenden Daten nicht als anonymisiert. Um eine Anonymisierung derartiger Datenbestände zu gewährleisten, ist es unabdingbar, zusätzliche Massnahmen zu treffen (beispielsweise spezielle Merkmale zusätzlich zu verschlüsseln oder zu verallgemeinern). Gemäss Botschaft vom 23. März 1988 zum Bundesgesetz über den Datenschutz wird unter Anonymisierung jede Massnahme verstanden, die bewirkt, dass die Identität der betroffenen Personen nicht mehr oder nur noch mit ausserordentlichem Aufwand festgestellt werden kann (faktische Anonymisierung). Nötig ist ein Aufwand, den vernünftigerweise niemand auf sich nehmen wird, um die Identität bestimmter Personen festzustellen. Ob ein Datenbestand als «anonymisiert» bezeichnet werden kann, lässt sich nicht abstrakt, sondern nur konkret feststellen, da dies von den übrigen Rahmenbedingungen abhängig ist.

10. Mietrecht

Anmeldeformulare für Mietwohnungen

Die Empfehlung betreffend den bei Interessenten für Mietwohnungen erhobenen Daten wurde von verschiedenen Vermietern abgelehnt. Wir haben die Angelegenheit der Eidgenössischen Datenschutzkommission zum Entscheid vorgelegt.

Bereits im 1. und 2. Tätigkeitsbericht wiesen wir auf die Problematik hin (S. 61 ff. und 60 ff.). Im November 1994 formulierten wir eine Empfehlung zuhanden aller Vermieter in der Schweiz. Die Empfehlung wurde den Vermietern, welche bereits am vorhergehenden Vernehmlassungsverfahren teilgenommen hatten, zugestellt und gleichzeitig im Bundesblatt publiziert. In der Folge lehnten verschiedene Vermieter

die Empfehlung ab. Wir legten daraufhin im Februar 1995 die Angelegenheit der Eidgenössischen Datenschutzkommission zum Entscheid vor. Nach einem Schriftenwechsel mit unserer Stelle über die Frage der Parteiqualität der Personen, welche die Empfehlung abgelehnt hatten, entschied die Eidgenössischen Datenschutzkommission im Dezember 1995, sie trete nur auf den Weiterzug gegenüber einer Partei, einem der grössten Vermieter in der Schweiz, ein. Demnächst sollte nun der materielle Entscheid ergehen.

II. DIE KONTROLLEN DES EDSB

1. Die neue Identitätskarte ID 95

Die neue schweizerische Identitätskarte, ein plastifizierter Ausweis im Kreditkartenformat, ist seit dem 1. Juli 1994 erhältlich. Eine Verordnung des Bundesrates regelt ihre Ausstellung und legt ausserdem strikte Bedingungen an die damit zusammenhängende Bearbeitung von Personendaten fest. Wir haben beschlossen, die Einhaltung dieser Anforderungen im Bereich des Datenschutzes zu kontrollieren. Die Kontrolle begann im Oktober 1995 und wird gegenwärtig im Bundesamt für Polizeiwesen durchgeführt.

Die Verordnung des Bundesrates über die neue schweizerische Identitätskarte “ID 95” ist am 1. Juli 1994 in Kraft getreten. Diese Verordnung regelt nicht nur das Verfahren für die Ausstellung des neuen plastifizierten Ausweises im Kreditkartenformat, sondern legt auch sehr genau die Bedingungen für die Bearbeitung der Personendaten fest, welche zu diesem Zweck beschafft werden. Im weiteren enthält sie auf unser Ersuchen hin zahlreiche restriktive Bestimmungen im Bereich des Datenschutzes.

Im Rahmen unserer Überwachungskompetenzen haben wir beschlossen, eine Kontrolle der Einhaltung dieser Bedingungen durchzuführen. Zu diesem Zweck haben wir mit der Sektion Verwaltungspolizei des Bundesamtes für Polizeiwesen Kontakt aufgenommen, welche für die Datenbank im Zusammenhang mit der neuen Identitätskarte verantwortlich ist.

Die Kontrolle begann im Oktober 1995 und ist gegenwärtig noch im Gange. Sie bezieht sich insbesondere auf den Inhalt und den isolierten Charakter der vom Bundesamt für Polizeiwesen verwalteten Datenbank, auf die Zugriffsberechtigungen zu diesem System, auf die Datenerfassung, auf die Weitergabe der Daten an den Kartenhersteller und an das Bundesamt für Polizeiwesen, auf die Datenbearbeitung, auf die Löschung der Daten nach Ablauf der Aufbewahrungsdauer, auf die Verwendung des maschinenlesbaren Codes sowie auf die Informationen, die auf der Identitätskarte selbst enthalten sind.

2. Das Informationssystem des Schweizerischen Instituts für Berufspädagogik

Das Schweizerische Institut für Berufsausbildung führt ein Datenbearbeitungsystem, welches die Kursadministration, die Grundausbildung und die Organisation von Seminaren und Kolloquien für Berufslehrer verwaltet. Wir haben dieses System kontrolliert, um zu prüfen, ob die notwendigen Massnahmen zur datenschutzkonformen Datenbearbeitung und die notwendigen Datensicherheitsmassnahmen getroffen wurden.

Das Bundesgesetz über die Berufsbildung und die Verordnung über das Schweizerische Institut für Berufspädagogik sind die Rechtsgrundlagen, welche die Führung einer EDV-Applikation zur rationellen Verwaltung der Berufsbildung erlauben. Im System werden Personendaten von etwa fünftausend Personen (Kursteilnehmer, Dozenten, Referenten, Absolventen, Lehrer) erfasst. Die verschiedenen Datenbearbeitungen werden hauptsächlich zur optimalen Abwicklung der fortlaufenden Aus- und Weiterbildung von haupt- und nebenamtlichen Berufslehrern eingesetzt.

Wir haben die verschiedenen Arbeitsabläufe des Systems, die verschiedenen Datenbearbeitungsmöglichkeiten (Archivierung, Bekanntgabe usw.) und die Datensicherheitsmassnahmen für den Zugang und den Zugriff zu den Daten kontrolliert.
Dabei haben wir festgestellt, dass keine widerrechtlichen Datenbearbeitungen zu beanstanden sind und die Massnahmen zur Gewährleistung der Datensicherheit ausreichend sind.

3. Datensammlung über Journalisten in Zermatt

Vom Presserat des Schweizer Verbandes der Journalistinnen und Journalisten wurden wir darauf aufmerksam gemacht, dass in Zermatt eine Journalistenkartei geführt wird und haben die notwendigen Abklärungen vogenommen. Wir haben geprüft, ob die entsprechenden Datenbearbeitungen die Persönlichkeit einer grösseren Anzahl von Personen gefährden können und ob die Datensammlung registriert werden muss. Wir sind zum Schluss gekommen, dass die Datensammlung die Bestimmungen des Bundesgesetzes über den Datenschutz nicht verletzt. Die Existenz einer schwarzen Liste konnte nicht festgestellt werden.

Der Kur- und Verkehrsverein der Gemeinde Zermatt führt eine Datenbank, in der Daten über ungefähr 4'500 Journalisten gespeichert sind. Der Zweck dieser Datensammlung besteht in der Optimierung der Kontakte mit den Medien. Die Datenbank ermöglicht die Speicherung der folgenden Daten: “Name”, “Vorname”, “Adresse”, “Geburtsdatum” (nicht verwendet), “Staatszugehörigkeit”, “Spezialgebiet”, “Art der journalistischen Tätigkeit” (TV, Radio, Printmedien...), “Status des Journalisten” (freier Journalist, Redaktor, ...), “Datum des Aufenthalts in Zermatt”, “War er in Begleitung und falls ja, von wem?”, “Welcher Mitarbeiter des Verkehrsbüros hat ihn betreut?”, “Welche Unterstützung erhielt er während seines Aufenthalts?”, “Wurde er zum Essen eingeladen?”, “Wo und welches Menü hat er gegessen?”, “Hat er eine Freikarte erhalten?”, “Hat er ein Geschenk erhalten?”, “Wer hat das Hotelzimmer reserviert?” und “Wer hat die Rechnung bezahlt?”, “Hat er über Zermatt geschrieben?”, “War der Artikel positiv für Zermatt?", “Wurde ihm gedankt?”, “Welche Informationen hat er verlangt?” und “Welche Unterlagen wurden ihm überreicht?”. Diese Informationen beziehen sich ausschliesslich auf die journalistische Tätigkeit während des Aufenthalts in Zermatt und betreffen das Privatleben des Journalisten nicht. Die

Daten über das Restaurant und das Menü werden nur erhoben, um zu vermeiden, dass ein Journalist zweimal in das gleiche Restaurant eingeladen wird oder dass ihm zweimal das gleiche Menü angeboten wird. Dasselbe gilt für allfällige kleine Geschenke, die das Verkehrsbüro hin und wieder an Besucher verteilt. Die Informationen über die Reservation des Hotelzimmers, über die Bezahlung der Rechnung oder eine allfällige Begleitung während des Aufenthalts in Zermatt sind rein administrativer Natur (Logistik, Buchhaltung). Jeder Artikel und jede Reportage kann vom Verkehrsbüro mit einer Note zwischen 1 und 5 bewertet werden (ausgezeichnet, gut, durchschnittlich, Zermatt nicht erwähnt, für Zermatt wertlos). Diese Noten beziehen sich weder auf die Qualität des Artikels oder der Reportage noch sind sie Ausdruck eines positiven oder negativen Urteils. Sie sind lediglich ein Gradmesser für die Auswirkungen, die ein Artikel für das Tourismuszentrum Zermatt hat, und stellen keine Qualifizierung des Journalisten als Person dar.

Die gespeicherten Daten werden nicht bekanntgegeben, und das Einsichtsrecht der betroffenen Journalisten ist gewährleistet.

Soweit die allgemeinen Grundsätze für die Bearbeitung von Personendaten eingehalten werden, kann das Verkehrsbüro Rechtfertigungsgründe für die Bearbeitung von Daten über jene Journalisten geltend machen, die mit ihm Kontakt pflegen. Gestützt auf unsere Wahrnehmungen und die Informationen, die uns zur Verfügung stehen, haben wir festgestellt, dass die Beschaffung und Bearbeitung der entsprechenden Daten rechtmässig ist, da die Umstände der Datenbearbeitung dem verfolgten Zweck entsprechen und die betroffenen Journalisten Kenntnis von der Datenbearbeitung haben.

Aus diesen Gründen sind wir zum Schluss gekommen, dass die Journalistendatensammlung des Verkehrsbüros Zermatt das Bundesgesetz über den Datenschutz nicht verletzt und dass die Datensammlung nicht zur Registrierung angemeldet werden muss. Wir haben dem Verkehrsbüro Zermatt jedoch empfohlen, auf die Richtigkeit und Aktualität der gespeicherten Daten zu achten, namentlich indem die Journalistendaten spätestens fünf Jahre nach ihrem letzten Kontakt mit Zermatt gelöscht werden. Dem Verkehrsbüro wurde ausserdem nahegelegt, die Journalisten ausdrücklich über die Existenz der Datensammlung und ihr Auskunftsrecht zu informieren.

4. Videoüberwachung an Grenzposten

Die Überwachung der grünen Grenze mit Hilfe von Videogeräten wird durch eine Verordnung des Bundesrates geregelt. Die Video-Aufnahmen sind notwendig für die Sicherung der Grenze, die Erhebung von Zollgebühren sowie für die Überwachung des Grenzübertritts. Die Aufnahmen müssen innerhalb von 24 Stunden gelöscht werden. Wir haben eine Kontrolle einer Video-Installation an der Grenze vorgenommen.

Ende 1991 wurden an dem von uns kontrollierten Grenzposten zwei Videokameras installiert. Diese Kameras ermöglichen die Überwachung von zwei Brücken, die Tag und Nacht zu Fuss oder mit dem Fahrrad überquert werden können. Der Grenzübergang ist zulässig, sofern die betroffenen Personen einen gültigen Identitätsausweis auf sich tragen und nicht mehr Waren mit sich führen, als gesetzlich vorgeschrieben ist. Der Grenzübergang ist bezeichnet, insbesondere durch ein Fahrverbot. Die Überwachungskameras sind versteckt, und es gibt keinen Hinweis darauf, dass die

Zone mit Videokameras überwacht wird. Die lokale Bevölkerung ist jedoch informiert. Die beiden Videokameras sind dauernd in Betrieb, filmen jedoch die beiden Grenzübergänge nur, wenn ein Grenzgänger oder ein Tier eine der beiden Brücken überquert. Es werden zwei verschiedene Installationen getestet. Die eine ist mit einem Videorecorder gekoppelt und ermöglicht die Aufnahme jedes Grenzübertritts auf einer Videokassette. Wenn die Aufnahmekapazität der Kassette erschöpft ist, werden die Aufnahmen gelöscht, und die Kassette wird bis zur endgültigen Abnutzung weiterverwendet. Zuletzt wird sie zerstört und durch eine neue Kassette ersetzt. Bevor die Aufnahmen gelöscht werden, können sie abgespielt werden. Dies bezieht sich in der Regel auf die Aufnahmen der letzten paar Minuten, kann aber auch maximal auf die zwei bis drei letzten Aufnahmestunden zurückgehen. Darüber hinaus ist das Abspielen der gemachten Aufnahmen sinnlos. Die zweite Kamera ist mit einer Festplatte verbunden. Dieses System ermöglicht nur die Speicherung der jeweils letzten beiden Aufnahmen, die bei einem weiteren Grenzübertritt automatisch gelöscht werden. Es ist mit beiden Systemen nicht möglich, die gemachten Aufnahmen zu drucken oder Fotos zu entwickeln. Im Grenzposten wurden zwei Überwachungsmonitoren installiert, die es den Zollbeamten ermöglichen, alle Grenzübertritte zu überwachen und gegebenenfalls einzuschreiten.

Die Videoüberwachung ist in der Verordnung über die Geländeüberwachung mit Videogeräten vom 26. Oktober 1994 geregelt. Danach ist es zulässig, Videokameras zu installieren, um die Sicherung der Grenze und die Einziehung von Zollgebühren sicherzustellen und um die Grenzübertritte zu überwachen. Die Verwendung der kontrollierten Kameras entspricht diesem Zweck. Die Bezeichnung des Grenzübergangs auf den Brücken ist in Anbetracht der lokalen Gegebenheiten ausreichend und ermöglicht den Grenzgängern zu wissen, dass sie die Grenze überqueren und deshalb mit einer Kontrolle rechnen müssen. Was die auf 24 Stunden begrenzte Aufbewahrungsdauer der Aufnahmen anbelangt, haben wir festgestellt, dass diese gesetzliche Anforderung durch das Festplatten-System erfüllt wird, da die Aufnahmen automatisch gelöscht werden, wenn weitere Grenzübertritte erfolgen. Das System, das mit einer Videokassette arbeitet, erfüllt diese Anforderung hingegen nicht, da die Löschung der Aufnahmen frühestens 36 Stunden nach der 1. Aufnahme erfolgt. Hinsichtlich der Arbeitseffizienz der Zollbeamten sowie unter Berücksichtigung der Anzahl aufgenommener Grenzgänger ist das System mit Videokassette jedoch vorzuziehen. Die Löschung der Aufnahmen muss jedoch innerhalb von 24 Stunden erfolgen, damit dieses System den Vorschriften im Bereich des Datenschutzes entspricht. In bezug auf die Datensicherheit haben wir keine besonderen Mängel festgestellt.
Im Anschluss an unsere Kontrolle haben wir den Zollbehörden vorgeschlagen, Videokassetten mit kürzerer Laufdauer zu verwenden, damit die Löschung der Aufnahmen innerhalb von 24 Stunden gewährleistet ist. Dieser Vorschlag wurde angenommen.

5. Auskunftsdienst 111 der Telecom-PTT Genf

Im Januar 1996 führten wir beim Auskunftsdienst der Telecom Genf eine Kontrolle durch. Wir prüften einerseits, ob den Angestellten die Nennung des Vornamens bei der Auskunftserteilung freigestellt wird und andererseits, ob die Durchführung von Verhaltensbeurteilungen mittels Abhörung datenschutzkonform ist.

Wir prüften zunächst, ob im Anschluss an eine dahingehende Intervention unse-

rerseits (vgl. S. 38) den Angestellten des Auskunftsdienstes die Nennung des Vornamens tatsächlich freigestellt wird. Die befragten Angestellten sagten aus, sie fühlten sich frei, den Vornamen nicht zu nennen und seien froh, dass keine diesbezügliche Pflicht mehr bestehe.
Sodann untersuchten wir auch die Durchführung von Verhaltensbeurteilungen mittels unangemeldeter Abhörung durch die Vorgesetzten. Die Durchführung der Beurteilungen ist in einer Weisung der Generaldirektion PTT detailliert geregelt. Die Auskunfterteilung durch die Teleoperatricen wird jährlich ein- oder mehrmals während ca. 45 Minuten von den Vorgesetzten aufgezeichnet und die Aufzeichnung danach mit der betroffenen Person besprochen. Dabei sollen Fehler in der Auskunfterteilung erkannt und behoben werden, die Freundlichkeit und Schnelligkeit der Auskunfterteilung überprüft und gute Leistungen anerkannt werden. Diesen Zwecken werden die Abhörungen sowohl nach Aussagen der Teleoperatricen als auch nach Angaben der Vorgesetzten gerecht. Problematisch ist aus datenschutzrechtlicher Sicht einerseits das Fehlen einer gesetzlichen Grundlage für die Abhörungen, andererseits, dass die Abhörungen unangemeldet vorgenommen werden. Von den befragten Teleoperatricen wird denn auch die vorgängige Ankündigung der Abhörung gewünscht. Die Kontrolle hat gezeigt, dass die Abhörung sich auf die Auskunfterteilung beschränkt, dass also private Gespräche zwischen den Teleoperatricen nicht aufgezeichnet werden. Die Abhörungen verlaufen zudem im Grossen und Ganzen gemäss den Vorgaben in der Weisung der Generaldirektion (Auswertung der Abhörung zusammen mit der betroffenen Person, Ausfüllen eines Beurteilungsblattes, das bis zur nächsten Qualifikation aufbewahrt und sodann vernichtet wird, Löschung der Aufzeichnung sofort nach Beendigung der Beurteilung). Die Weisung verlangt allerdings die Löschung im Beisein der betroffenen Person, was in Genf nicht so geschieht und die Information des Personals über den Zweck und die Durchführung der Arbeitsbeurteilung, was nicht immer geschieht. Wir haben der Telecom Genf also geraten, das Personal bei Anstellung und Schulung systematisch über Zweck, Inhalt und Durchführung der Arbeitsbeurteilung zu informieren, die Abhörung vorgängig anzukünden und die Löschung systematisch im Beisein der betroffenen Person vorzunehmen. Gleichzeitig haben wir bei der Generaldirektion PTT interveniert, um zu klären, inwiefern die Schaffung einer gesetzlichen Grundlage in Hinblick auf die bevorstehende Privatisierung der Telecom notwendig und sinnvoll ist.

III. WEITERE THEMEN

1. Datenschutzrechtliche Rahmenbedingungen

1.1. Umsetzung von Anforderungen des DSG bei der Gesetzgebung

Gemäss DSG müssen für bestehende Datensammlungen mit besonders schützenswerten Personendaten oder Persönlichkeitsprofilen bis zum 1. Juli 1998 formellgesetzliche Grundlagen geschaffen oder angepasst werden. Auf Anfrage des Generalsekretariats des EJPD haben wir in einem Gutachten dargelegt, was für Bestimmungen im einzelnen erlassen werden sollten.

Nach Art. 38 Abs. 3 DSG müssen Bundesorgane für bestehende Datensammlungen mit besonders schützenswerten Personendaten oder mit Persönlichkeitsprofilen bis zum 1. Juli 1998 formellgesetzliche Grundlagen schaffen. Für die Neuschaffung oder

erhebliche Erweiterung solcher Datensammlungen müssen sie die erforderlichen Rechtsgrundlagen umgehend schaffen. Die Frage, was im einzelnen wie zu regeln ist, bildete Gegenstand eines Gutachtens, das der EDSB nach Absprache mit dem Bundesamt für Justiz im Herbst 1995 erstellt hat, und welches zur Publikation in der Verwaltungspraxis der Bundesbehörden (VPB) vorgesehen ist. Insbesondere sind folgende Punkte festzuhalten:

- Werden besonders schützenswerte Personendaten oder Persönlichkeitsprofile regelmässig bearbeitet, muss dies in einem formellen Gesetz gesagt werden. Dabei müssen Zweck und Umfang der Datenbearbeitung, die verwendeten Mittel sowie die zur Bearbeitung befugte(n) Behörden(n) hinreichend bestimmt sein.
- Wird ein grosses und verzweigtes EDV-System ("verwendete Mittel") bei der Datenbearbeitung eingesetzt, in welchem in erheblichem Umfang und von verschiedenen Behörden Personendaten, namentlich besonders schützenswerte Personendaten und Persönlichkeitsprofile bearbeitet werden, muss dies in einem formellen Gesetz ausdrücklich gesagt sein.
- Sollen unter verschiedenen Behörden und zu verschiedenen Bearbeitungszwecken regelmässig Personendaten, namentlich besonders schützenswerte Personendaten oder Persönlichkeitsprofile, ausgetauscht werden, muss dies im formellen Gesetz ausdrücklich gesagt sein. Erhalten einzelne Behörden im Abrufverfahren Zugriff auf diese Daten, muss auch dieser Umstand ausdrücklich erwähnt und die ermächtigte Behörde genannt werden. Erfolgt der Austausch regelmässig mit Behörden des Auslandes, muss dies ebenfalls ausdrücklich geregelt werden.
- Erweisen sich gewisse Grundrechtseingriffe im Zusammenhang mit der Datenbearbeitung nur zusammen mit konkreten, bereichsspezifischen Schutzauflagen als grundrechtskonform, sind auch diese Schutzauflagen bzw. die Grenzen der vorgesehenen Eingriffe formellgesetzlich zu regeln. Beispiele solcher Vorschriften sind die Bestimmungen über die Massnahmen der Personenüberwachung mit technischen Mitteln und deren Begrenzung bzw. Kontrolle im Bundestrafprozess (Art. 65 ff. BStP) oder die Bestimmungen über den Schutz der Daten unbeteiligter Dritter bei Personenabfragen aus dem Zentralen Ausländerregister zu Identifikationszwecken bei der Strafverfolgung (Art. 7 Abs. 3 ZAR-Verordnung, dessen Inhalt in den vom Bundesrat verabschiedeten Entwurf eines revidierten ANAG aufgenommen wurde).

Nachdem dieses Gutachten vorliegt, wird es in einer nächsten Phase darum gehen, die nötigen Gesetzgebungsarbeiten in die Wege zu leiten, sofern dies nicht bereits geschehen ist. Auf Anfrage und in Zusammenarbeit mit dem Bundesamt für Justiz werden wir den betroffenen Bundesorganen im Rahmen unseres gesetzlichen Auftrages dabei beratend zur Seite stehen.

1.2. Der Entwurf zu einem Bundesgesetz über Waffen, Waffenzubehör und Munition

Wir wurden im Lauf der Ausarbeitung dieses Gesetzesentwurfs mehrmals um eine Stellungnahme ersucht und haben immer wieder darauf hingewiesen, dass für die zahlreichen Bearbeitungen von Personendaten, die sich aus der Anwendung dieses Gesetzes ergeben werden, eine genauere Regelung aufgestellt werden muss. Das Bundesamt für Polizeiwesen hatte eine Vielzahl von Bestimmungen in den Entwurf aufgenommen, die eine Delegation von Kompetenzen an den Bundesrat vorsahen. Es

folgte schliesslich unserem Vorschlag, auch speziell für die Datenbearbeitung eine Kompetenzdelegation vorzusehen.

Wir haben im Rahmen des Vernehmlassungsverfahrens zum Entwurf für ein Bundesgesetz über Waffen, Waffenzubehör und Munition im Mai 1995 auf die umfangreichen Datenbearbeitungen hingewiesen, welche sich für die verschiedenen Beteiligten ergeben werden. Wir haben insbesondere verlangt, dass in den Gesetzesentwurf Präzisierungen in bezug auf die Beschaffung von Informationen aufgrund der Verpflichtung zur Überprüfung der Identität, in bezug auf die Führung einer Buchhaltung und in bezug auf die Gewährung von Bewilligungen aufgenommen werden. Ausserdem haben wir gefordert, dass für die zahlreichen Datenbekanntgaben und Datenaustausche, die zwischen den privaten Verkäufern und den zuständigen kantonalen und Bundesbehörden sowie den entsprechenden ausländischen Stellen vorgesehen sind, klare Bestimmungen erarbeitet werden.

Aus der Veröffentlichung der Ergebnisse dieses Vernehmlassungsverfahrens im September 1995 ging hervor, dass die Stellungnahmen der betroffenen Ämter - insbesondere unsere Anmerkungen - berücksichtigt worden sind. Als wir jedoch im November 1995 erneut um eine Stellungnahme zum überarbeiteten Gesetzesentwurf und seinem Botschaftsentwurf ersucht wurden, stellten wir fest, dass unsere Bemerkungen und Vorschläge zur Beschaffung, Bekanntgabe und Bearbeitung von Daten nur am Rande oder gar nicht berücksichtigt worden waren. Zudem enthält der neue Gesetzesentwurf zwar zahlreiche Bestimmungen, die eine Delegation von Kompetenzen an den Bundesrat vorsehen, davon betrifft jedoch keine unzweideutig den Datenschutz.

In unserer Stellungnahme zu diesem neuen Entwurf nahmen wir davon Kenntnis, dass keine Bekanntgabe von besonders schützenswerten Daten oder Persönlichkeitsprofilen durch ein Abrufverfahren (on-line-Verbindung) vorgesehen ist. Wir haben in Erinnerung gerufen, dass jede Bekanntgabe von Personendaten mit Hilfe eines Abrufverfahrens gegebenenfalls ausdrücklich in der Ausführungsverordnung aufgeführt sein muss. Überdies haben wir in bezug auf die Bearbeitung von Personendaten festgehalten, dass die Delegation der Kompetenzen an den Bundesrat aus dem vorliegenden Gesetzesentwurf nicht deutlich genug hervorgeht. Wir haben daher verlangt, dass eine allgemeine Bestimmung über die Delegation von Kompetenzen im Bereich des Datenschutzes in den Gesetzesentwurf aufgenommen wird. In dieser Bestimmung ist vorzusehen, dass der Bundesrat die Modalitäten von Datenbearbeitungen im Zusammenhang mit der Anwendung des Gesetzes sowie die Gewährung von Zugriffsberechtigungen und die Aufbewahrungsdauer auf dem Verordnungsweg regelt. Unserem Vorschlag folgend hat das Bundesamt für Polizeiwesen die verlangte Norm über die Kompetenzdelegation erarbeitet und in die Endfassung des Gesetzesentwurfs einfliessen lassen. Dieser wurde im Januar 1996 vom Bundesrat verabschiedet und dem Parlament zur Beratung vorgelegt.

1.3. Vorentwurf für ein Bundesgesetz über die medizinisch unterstützte Fortpflanzung und eine nationale Ethikkommission - Vernehmlassung bei den betroffenen Kreisen

Im Rahmen des Vernehmlassungsverfahrens bei den betroffenen Kreisen haben wir dem Bundesamt für Justiz eine erste Stellungnahme unterbreitet. Wir betonten insbesondere die Notwendigkeit, die Einwilligungsverfahren im Zusammenhang mit der

medizinisch unterstützten Fortpflanzung für die zukünftigen Eltern zu erleichtern. Wir haben sodann Zweifel angemeldet, ob es sowohl aus wissenschaftlicher Sicht als auch hinsichtlich des Wohls des werdenden Kindes, sinnvoll ist, die Möglichkeit einer Selektion des Spenderspermas aufgrund der körperlichen Ähnlichkeit des Spenders mit dem zukünftigen Vater vorzusehen. Wir haben auch die Auffassung vertreten, dass Informationen über den Zivilstand, die Religionszugehörigkeit, den Beruf und die Ausbildung des Spenders einem Kind, das seine biologische Herkunft abklären möchte, unserer Ansicht nach nicht bekannt sein müssen. Abschliessend haben wir darauf hingewiesen, dass die vorgesehene Aufbewahrungsdauer der Daten von 80 Jahren zu lange ist.

2. Bekanntgabe von Personendaten

2.1. Die Bekanntgabe von Personendaten an Dritte im Sinne von Art. 11 Abs. 3 DSG

Private Personen, die Personendaten an Dritte bekanntgeben, müssen die betreffende Datensammlung beim Eidgenössischen Datenschutzbeauftragten anmelden, wenn für das Bearbeiten keine gesetzliche Pflicht besteht oder die betroffenen Personen davon keine Kenntnis haben. Im Einzelfall muss überprüft werden, ob der Empfänger der Daten als Dritter im Sinne von Art. 11 Abs. 3 DSG gilt.

Eine private Person erkundigte sich, ob Kundendaten, die sie durch eine Druckerei im Auftrag bearbeiten lässt, bei uns angemeldet werden müssten. Diese Frage kann nicht generell beantwortet werden, da es für die Beantwortung der Frage, ob eine Datenbekanntgabe an Dritte im Sinne von Art. 11 Abs. 3 DSG vorliegt, im Einzelfall darauf ankommt, welche Personendaten unter welchen Umständen bekanntgeben werden. Als Bekanntgabe ist das Zugänglichmachen von Personendaten wie die Gewährung der Einsicht, die Weitergabe oder die Veröffentlichung zu verstehen. Dabei gilt es insbesondere zu prüfen:

- welche Art von Personendaten bearbeitet werden;
- ob der Dritte eine unabhängige Person ist oder ob er in einem Subordinationsverhältnis zum Inhaber der Datensammlung steht;
- zu welchem Zweck die Daten an Dritte bekanntgegeben werden;
- wie die Daten durch Dritte bearbeitet werden, namentlich ob der Dritte die Personendaten an weitere Personen bekanntgibt;
- ob der Empfänger primär am Inhalt der Daten interessiert ist, oder die Daten nur technisch bearbeitet, und danach dem Inhaber der Datensammlung wieder vollumfänglich zurückgibt.

Wenn ein Inhaber einer Datensammlung beispielsweise eine Druckerei beauftragt, Formulare für die Erteilung von Zahlungsaufträgen zu drucken, werden der Druckerei Personendaten bekanntgegeben. In diesem Fall erhält die Druckerei die Kundendaten jedoch nur für eine technische Bearbeitung und darf die Daten nur auftragsgemäss bearbeiten. Nach dem Drucken der Zahlungsaufträge ist die Bearbeitung der Personendaten durch die Druckerei abgeschlossen, weshalb sie dem Auftraggeber vollumfänglich zurückgegeben werden. Die Bekanntgabe der Daten dient in diesem Zusammenhang lediglich als Mittel zum Zweck, damit der Auftraggeber seine weiteren Aufgaben erfüllen kann. Damit ist die Druckerei nur Empfängerin der Personen-

daten, aber nicht Dritte im Sinne von Art. 11 Abs. 3 DSG, weshalb die Sammlung bei uns nicht angemeldet werden muss.

2.2. Bekanntgabe von Daten über ausländische Stipendienbezüger

Die Schaffung einer Datenbank durch eine Bundesstelle zum Zwecke der Bekanntgabe und Veröffentlichung von Daten über ausländische Stipendienbezüger muss auf einer ausreichenden gesetzlichen Grundlage beruhen, auf die mit der Veröffentlichung der Daten beabsichtigten Zwecke beschränkt bleiben und das Recht der betroffenen Personen berücksichtigen, die Veröffentlichung oder Bekanntgabe zu verweigern.

Was die Gewährung von Stipendien an ausländische Studenten und Künstler anbelangt, haben wir betont, dass eine Bundesstelle diesbezügliche Daten nur im Einzelfall auf ein Gesuch hin bekanntgeben darf, solange keine gesetzliche Grundlage besteht, welche die Schaffung und die Verwaltung einer Datenbank vorsieht, auf die Dritte Zugriff haben und die Bekanntgabe nicht gesetzlich geregelt ist. Zudem bedarf es der Zustimmung der betroffenen Person, es sei denn, dass nur der Name, der Vorname, die Adresse sowie das Geburtsdatum der betroffenen Person mitgeteilt werden. Eine Bekanntgabe der entsprechenden Daten ist auch möglich, wenn die betroffene Person selbst ihre Daten jedermann zugänglich gemacht hat.

Für die systematische und regelmässige Bekanntgabe von Daten, in Form von Listen, durch die Veröffentlichung von Broschüren oder durch ein Abrufverfahren (Online-Zugang) muss zuerst eine ausreichende gesetzliche Grundlage geschaffen werden. Wenn der Zugriff zu den Daten über ein Abrufverfahren erfolgen soll, muss dies in einer gesetzlichen Grundlage ausdrücklich so vorgesehen sein. Die Bekanntgabe von Daten über Stipendienbezüger muss sodann freiwillig sein. Jeder Stipendienbezüger muss die Möglichkeit haben, die Aufnahme seiner Daten oder ihre Bekanntgabe zu untersagen. Schliesslich dürfen nur jene Daten jedermann zugänglich gemacht werden, die zur Erreichung des mit der Veröffentlichung oder der Verbreitung verfolgten Zwecks erforderlich sind.

2.3. Amtshilfe durch die Bekanntgabe von Listen in den Bereichen Subventions-, Steuer- und Umweltschutzrecht

Bundesorgane dürfen Personendaten zu beschaffungsfremden Zwecken mittels Listen nur bekanntgeben, wenn dafür Rechtsgrundlagen bestehen. In zwei uns unterbreiteten Fällen waren diese Voraussetzungen nicht erfüllt, weshalb wir den beabsichtigten Datenbekanntgaben nicht zustimmen konnten.

In zwei Gutachten haben wir uns zur amtshilfeweisen Bekanntgabe umfangreicher Listen mit Personendaten geäussert. Im ersten Fall ersuchte die Eidgenössische Steuerverwaltung das Bundesamt für Landwirtschaft um die Bekanntgabe sämtlicher Empfänger von Betriebsstillegungsbeiträgen. Im zweiten Fall bat eine ausländische Handelskammer die Interdisziplinäre Schweizerische Kommission für biologische Sicherheit in Forschung und Technik um die Bekanntgabe der gemäss Störfallverordnung gemeldeten genforschenden Betriebe.

Weder das Landwirtschaftsrecht, noch das Steuerrecht oder das Umweltschutzrecht

sehen die anbegehrten umfangreichen Datenbekanntgaben zu beschaffungsfremden Zwecken an Drittbehörden oder an Private vor. Zu beschaffungsfremden Zwecken dürfen die Daten daher nur im Einzelfall bekanntgegeben werden. Konkret hätte im Steuerfall zudem ein rechtsmissbräuchliches Verhalten der Betroffenen glaubhaft gemacht und im Fall der genforschenden Betriebe deren Einverständnis nachgewiesen werden müssen. Diese Voraussetzungen waren ebenfalls nicht erfüllt, weshalb unsere Antwort negativ ausfiel.

3. Datenübermittlungen ins Ausland

Grenzüberschreitende Datenübermittlungen innerhalb multinationaler Unternehmen und Anmeldepflicht

Während des letzten Geschäftsjahres wurden wir von vielen Gesellschaften angefragt, unter welchen Bedingungen sie ihre Daten ins Ausland übermitteln dürfen. Es handelte sich meistens um multinationale Unternehmen, welche im Rahmen von weltweiten Restrukturierungen, Nachfolgeplanung oder effizienter konzerninterner Stellenbesetzung Mitarbeiterdaten an den sich ausserhalb der Schweiz befindenden Hauptsitz oder an das Mutterhaus übermittelten.

Damit multinationale Unternehmen ihren Betrieb rational und effizient gestalten können, müssen Daten unter den verschiedenen Zweigstellen ausgetauscht werden. Von Bedeutung ist vor allem die Übermittlung der Daten der Mitarbeiter der Zweigstellen/Tochtergesellschaften an den Hauptsitz/Muttergesellschaft. Diese werden für die effiziente Einsetzung der im Unternehmen vorhandenen personellen Resourcen und für die optimale Nachfolgeplanung eingesetzt. Meistens handelt es sich um Personendaten des mittleren und höheren Kaders.

Grenzüberschreitende Datenflüsse können für die Persönlichkeit der betroffenen Personen, Gefahren bergen, insbesondere wegen der Unübersichtlichkeit der Übermittlungen ins Ausland. Wenn die Daten einmal im Ausland sind, kann die betroffene Person ihre Rechte auf Einsicht oder Korrektur kaum mehr geltend machen, vor allem in Staaten ohne gleichwertigen Datenschutz und somit steigt die Gefahr, dass beispielsweise durch eine unerlaubte Datenbearbeitung oder durch die Bearbeitung von unkorrekten Daten eine Persönlichkeitsverletzung geschieht.

Aus diesen Gründen weisen wir auf die wesentliche Elemente hin, die bei Datenübermittlungen ins Ausland zu beachten sind:

Wer trägt die Verantwortung bei Datenübermittlungen ins Ausland ?

Das schweizerische Datenschutzgesetz sieht kein eigentliches Bewilligungsverfahren für Datenübermittlungen ins Ausland vor. Grundsätzlich dürfen Personendaten ins Ausland übermittelt werden, wenn dabei die Persönlichkeit der betroffenen Personen nicht schwerwiegend gefährdet wird. Der Gesetzgeber hat bewusst dem Übermittler die Verantwortung und die Beurteilung der Risiken einer Bekanntgabe von Personendaten ins Ausland überlassen.
Die für gewisse Übermittlungen ins Ausland vom Gesetz statuierte Meldepflicht befreit den Inhaber einer Datensammlung nicht von seiner Verantwortung für die Einhaltung der materiellen Regeln des Gesetzes. Der Inhaber muss genau gleich wie

bei einer nicht meldepflichtigen Datensammlung das Risiko einer Persönlichkeitsverletzung selbst beurteilen.

Zweck der Meldepflicht

Mit der Meldung von Übermittlungen ins Ausland wird die Transparenz der Datenbearbeitung bezweckt. Der EDSB nimmt die Rechte der Personen, deren Personendaten ins Ausland übermittelt werden, ad interim wahr. Deshalb entfällt die Meldepflicht, wenn die betroffenen Personen von der Datenübermittlung Kenntnis haben.

Wann besteht die Pflicht zur Meldung einer Übermittlung ins Ausland?

- Wenn die *Datensammlung** das Hoheitsgebiet der Schweiz verlässt, oder
- Daten vom Ausland aus abgerufen werden können, oder
- Daten an einen Dritten übermittelt werden, der beauftragt ist, die Daten für Rechnung des Übermittlers zu bearbeiten.

*Als *Datensammlung* gilt jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind.

Wesentlich ist, dass die Daten das Hoheitsgebiet der Schweiz verlassen und nicht, ob die Daten innerhalb einer Gesellschaft oder eines Konzerns übermittelt werden.

Wann muss eine Übermittlung nicht gemeldet werden ?

- Wenn eine gesetzliche Pflicht für die Bekanntgabe besteht, oder
- die betroffenen Personen von der Datenübermittlung *Kenntnis** haben.

*Die *Kenntnisnahme* der betroffenen Personen ist gegeben, wenn mindestens der Inhaber der Datensammlung, die übermittelten Daten, der Zweck der Übermittlung an Dritte und das Land, in das die Daten übermittelt werden bekannt sind.

Ausnahmen von der Meldepflicht

- Übermittlungen von Daten für nicht personenbezogene Zwecke (Statistik, Planung, Forschung) sind nicht meldepflichtig, sofern die Veröffentlichung der Resultate eine Identifizierung der betroffenen Personen nicht zulässt.
- Übermittlungen von Daten in Länder mit einer gleichwertigen Datenschutzgesetzgebung sind nur dann nicht meldepflichtig, wenn es sich nicht um besonders schützenswerte Personendaten oder *Persönlichkeitsprofile** handelt.

*Bei den Übermittlungen zwischen Betrieben und Konzernen zwecks effizienter Einsetzung der personellen Ressourcen handelt es sich um aussagekräftige Informationen, welche oft *Persönlichkeitsprofile* bilden.

Das Meldeverfahren

Falls eine Übermittlung ins Ausland meldepflichtig ist, müssen folgende Angaben gemacht werden (das notwendige Formular ist beim Sekretariat des ESDB kostenlos zu beziehen) :

- Name und Adresse der Person, welche die Personendaten bekanntgibt;
- Name und Adresse des Datenempfängers;
- Name und vollständige Bezeichnung der Datensammlung;

- Kategorien der bekanntgegebenen Personendaten;
- Kreis und ungefähre Anzahl der betroffenen Personen;
- Zweck der Datenbearbeitung durch den Empfänger;
- Art und Häufigkeit der Bekanntgabe;
- Datum der ersten Bekanntgabe.

Im Gegensatz zu den anmeldungspflichtigen Datensammlungen werden gemeldete Übermittlungen ins Ausland nicht registriert und nicht veröffentlicht.

Bei Datenübermittlungen ins Ausland beachten Sie insbesondere folgende Punkte :

- Ermitteln Sie zuerst die Rechtslage im Empfängerland.
  Konsultieren Sie zuerst die Liste der Staaten mit einem dem schweizerischen gleichwertigen Datenschutz, welche der EDSB führt. Falls das Empfängerland nicht über einen gleichwertigen Datenschutz verfügt oder Unklarheit über die Rechtslage besteht, dann empfiehlt es sich, mit dem Empfänger eine vertragliche Vereinbarung zu treffen, um ein dem schweizerischen gleichwertiges Datenschutzniveau zu gewährleisten. In einer solchen Vereinbarung sollte mindestens folgendes geregelt werden:
- Verbindliche und präzise Definierung des Verwendungszwecks;
- Auskunftsrechte der betroffenen Personen;
- Regelung der Datensicherheit anhand der Sensibilität der Daten
- Folgen für den Fall, dass der Empfänger seine Verpflichtungen nicht einhält. (Schadenersatzpflicht oder Konventionalstrafe).

- Vergewissern Sie sich, dass die Daten, die Sie übermitteln, richtig sind

- Treffen Sie die notwendigen übermittlungstechnischen Massnahmen (Datensicherheit), um die Daten vor dem Zugriff Unbefugter oder vor Verlust zu schützen.

Der Europarat hat einen Mustervertrag erarbeitet, welcher für die Regelung des grenzüberschreitenden Datenverkehrs verwendet werden kann (siehe Anhang S. 106).

4. Datenschutz und Datensicherheit

4.1. Datenschutzanforderungen an die Büroautomation

Vernetzte, leistungsfähige Rechner bieten zusammen mit entsprechender Software völlig neue Möglichkeiten der Büroautomation, die zu wesentlichen Erleichterungen der Ablaufprozesse führen können. Die Vorsichtsmassnahmen beim Umgang mit Personendaten dürfen dabei jedoch nicht ausser Acht gelassen werden.

Büroautomation unterstützt die Büroarbeit, d.h. das Erstellen, Verändern, Ar-

chivieren, Wiederauffinden und Verteilen von Informationen in Form von Text, Daten, Bildern und Sprache. Büroarbeitsplätze werden zunehmend vernetzt und mit immer leistungsfähigeren Rechnern ausgerüstet; so sind weitreichende Datenbearbeitungen möglich, von der einfachen Textverarbeitung bis zur komplexen Groupwareapplikation.

Im Rahmen einer Arbeitsgruppe, die sich mit der Sicherheit im Umfeld der Büroautomation der Bundesverwaltung befasste, haben wir auf die Hauptanforderungen hingewiesen, die es aus der Sicht des Datenschutzes zu beachten gilt, wovon wir hier einige zusammenfassen:

- Der Grundsatz, dass für die Bearbeitung von Personendaten durch Bundesorgane eine gesetzliche Grundlage erforderlich ist, gilt insbesondere auch in der Büroautomation.
- Geeignete Kontrollmechanismen müssen garantieren, dass sich keine unbefugten Änderungen von Dokumenten vornehmen lassen. Änderungen müssen nachvollziehbar sein.
- Bestimmte Daten dürfen nur zu dem für die konkrete Aufgabenerfüllung erforderlichen bzw. dem in den Rechtsgrundlagen festgehaltenen Zweck abgefragt werden.
- Büroautomationssysteme können Zugriff auf Daten aus mehreren unterschiedlichen (einzeln unproblematischen) Quellen bieten. Durch technische Massnahmen ist sicherzustellen, dass nicht unrechtmässig eine automatisierte Verknüpfung vorgenommen werden kann, denn solche Verknüpfungen können zur Entstehung von Persönlichkeitsprofilen führen.
- Die Weitergabe von Dokumenten, in welcher Form auch immer, muss kontrolliert erfolgen. Absender und Empfänger müssen eruierbar sein. Die Dokumente sind angemessen gegen Verletzung der Integrität und Vertraulichkeit zu schützen.
- Nicht mehr benötigte Personendaten müssen anonymisiert oder vernichtet werden, soweit sie nicht Beweis- oder Sicherungszwecken dienen oder dem Bundesarchiv abzuliefern sind.

Gerade bei der Büroautomation ist es aufgrund der Funktionalität und Flexibilität der Systeme schwierig, diese Anforderungen lediglich mit technischen Mitteln zu erfüllen. Eine sinnvolle und wirksame Massnahme ist jedoch die Protokollierung der Datenbearbeitung. Eine unbefugtes Bearbeiten kann zwar damit nicht direkt unterbunden werden; im Nachhinein kann jedoch die Rechtmässigkeit der Bearbeitung, vor allem die Zweckbindung, überprüft werden. Daneben sind auf das konkrete Umfeld zugeschnittene organisatorische Massnahmen zu treffen.
In der Regel ist nicht von vornherein bekannt, Daten welcher Sensibilität mittels Büroautomationssystemen verarbeitet werden; daher ist im Zweifelsfall bei der Wahl der zu treffenden Massnahmen der ungünstigste Fall ins Auge zu fassen.

4.2. Online-Registrierung von Software

Wenn Softwareanbieter die Online-Registrierung eines Softwareprodukts ermöglichen, muss gewährleistet sein, dass der Kunde von allen übertragenen Daten Kenntnis hat. Es muss technisch möglich sein, die Übertragung zu unterbinden.

Mehrere Softwareprodukte im PC-Bereich erlauben anstelle einer Registrierung auf

dem Postweg eine Online-Registrierung via Modem. Diese Möglichkeit steht auch Käufern des PC-Betriebssystems Windows95 der Firma Microsoft offen, das im letzten Jahr auf den Markt kam. Mehrere Medienberichte sowie Privatpersonen, die sich an uns wandten, äusserten die Befürchtung, dass die Firma Microsoft bei der Registrierung möglicherweise Daten vom PC des Kunden überträgt, ohne dass dieser darüber informiert ist. Wir entschlossen uns, den Sachverhalt näher abzuklären, da die Bearbeitungsmethoden eventuell geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen.

Unsere Abklärungen zu diesem Thema waren bei Redaktionsschluss dieses Berichtes noch nicht abgeschlossen. Folgende grundsätzliche Aussagen allgemeiner Natur können jedoch schon heute gemacht werden:

Die rechtmässige Beschaffung von Personendaten sowie deren Bearbeitung nach Treu und Glauben sind fundamentale Datenschutzgrundsätze. Daraus ergibt sich, dass keinesfalls Personendaten eines PCs zu einem Anbieter, Softwarehersteller etc. übertragen werden dürfen, ohne dass der Benutzer davon weiss oder dies annehmen kann. Er muss wissen, welche Personendaten übertragen werden und die Möglichkeit haben, deren Übertragung ganz oder teilweise zu unterbinden.

4.3. Die Verantwortlichkeit des Auftraggebers und der Servicefirma bei Serviceleistungen im EDV-Bereich

Wenn eine defekte Festplatte, die Personendaten enthält, dem Händler für die Reparatur ausgehändigt werden muss, ist vor allem auf Datensicherheitsmassnahmen zu achten, welche die Vertraulichkeit gewährleisten; dies insbesondere dann, wenn die Festplatte ins Ausland gesandt wird. Auch bei der (Fern-)Wartung von EDV-Anlagen sind geeignete technische und organisatorische Massnahmen zu treffen.

Daten aus dem persönlichen Umfeld oder sensible Informationen werden nicht gerne aus der Hand gegeben, wenn nicht davon ausgegangen werden kann, dass diese auch vertraulich behandelt werden.

Der Inhaber der Datensammlung muss dafür besorgt sein, dass die Daten durch Dritte nur so bearbeitet werden, wie er es selbst tun dürfte. Die Übertragung von Datenbearbeitungen an Dritte ist zudem nur zulässig, wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. Eine vertragliche Wegbedingung von Datenschutzbestimmungen gegenüber dem Kunden ist unwirksam.

Bei der Reparatur bzw. beim Austausch von Festplatten besteht die Möglichkeit, dass Daten unkontrolliert eingesehen oder gar weitergegeben werden. Dieser Unsicherheit kann entgegengewirkt werden, indem die Daten auf der Festplatte verschlüsselt abgelegt werden. Entscheidend ist jedoch, dass gute, bewährte Chiffrieralgorithmen mit hinreichenden Schlüssellängen eingesetzt werden.
Liegen die Daten im Klartext auf der Festplatte, kann die Vertraulichkeit mit einer Löschung erreicht werden. Wichtig ist, dass eine physikalische Löschung erfolgt. Die meisten Betriebsysteme löschen normalerweise lediglich logisch und erlauben so eine einfache Wiederherstellung der Daten. Mit speziellen Hilfsprogrammen (mehrfache Überschreibung mit verschiedenen Werten etc.) kann eine dauerhafte Löschung erzielt werden. Nicht mehr ansprechbare Datenträger können mit starken magnetischen Wechselfeldern behandelt werden. Es ist zu beachten, dass Spezia-

listen unter Ausnutzungen von Restmagnetisierungen etc. eine nicht fachgerechte Löschung rückgängig machen können.

In diesem Zusammenhang sei erwähnt, dass das Anlegen von gut verwahrten Sicherheitskopien (Backups) eine Selbstverständlichkeit sein muss. Der Defekt einer Festplatte kann ansonsten zu einem unwiederbringlichen Datenverlust bzw. zu enormen Wiederbeschaffungskosten führen.

Defekte Festplatten werden häufig ins Ausland (z.B. an den Hersteller) gesandt. Die genannten Massnahmen zur Gewährleistung der Vertraulichkeit sind insbesondere in diesem Fall umzusetzen. Datensammlungen, die ins Ausland übermittelt werden, müssen dem Eidgenössischen Datenschutzbeauftragten gemeldet werden, wenn für die Bekanntgabe keine gesetzliche Pflicht besteht oder die betroffenen Personen davon keine Kenntnis haben. Die Übermittlung ist nicht meldepflichtig, wenn sie Staaten betrifft, die über eine gleichwertige Datenschutzgesetzgebung verfügen, es sei denn, die Datensammlungen beinhalten besonders schützenswerte Personendaten oder Persönlichkeitsprofile, oder eine Weiterleitung in ein Drittland ohne gleichwertige Gesetzgebung sei vorgesehen.

Bei der (Fern-)Wartung bzw. der Behebung von Fehlern im EDV-System durch die Liefer- oder Servicefirma muss theoretisch auch von einer unkontrollierten Einsichtnahme oder von einem unkontrollierten Datenabgang ausgegangen werden. Die hohen Privilegien, die dem Wartungspersonal für die Aufgabenerfüllung im EDV-System eingeräumt werden müssen, erlauben es diesem, eine grosse Anzahl von Systemfunktionen auszuführen. In vielen Fällen besteht zwischen der Servicefirma und dem Auftraggeber ein Vertrag mit einer Verschwiegenheitsklausel. Dies ist sicher ein guter Ansatz; es müssen aber zusätzlich Datensicherheitsvorkehrungen getroffen werden, die eine Umgehung dieser Verträge bzw. der Gesetzesvorschriften verunmöglichen, einschränken oder im nachhinein aufzeigen. Mögliche Datensicherheitsmassnahmen sind in diesem Umfeld die Chiffrierung der Daten und die Protokollierung der Eingriffe, die vom Servicepersonal vorgenommen werden. Wie bei allen Sicherheitsmassnahmen gilt natürlich auch in diesem Fall der Grundsatz der Angemessenheit. Bei der Bearbeitung von besonders schützenswerten Personendaten, Persönlichkeitsprofilen oder bei sensiblen Zwecken der Datenbearbeitung ist der Stand der Technik bei den Sicherheitsvorkehrungen umzusetzen. Aufgrund heutiger Erfahrungen kann man festhalten, dass namhafte Unternehmungen rund 10-15% der gesamten IT-Kosten in Datensicherheitsmassnahmen investieren.

4.4. Datensicherheitsaspekte bei der Planung von EDV-Projekten

Bei der Entwicklung von EDV-Systemen ist der Datensicherheit ein besonderes Augenmerk zu schenken. Abhängig von der Sensibilität der bearbeiteten Daten sind entsprechende Sicherheitsmassnahmen vorgesehen. Der Inhaber der Datensammlung als Verantwortlicher für die Datensicherheit ist auf kompetente Beratung durch die Sachverständigen angewiesen.

Die Einschätzung der möglichen Risiken für die betroffenen Personen ist ein massgebendes Kriterium für die Bestimmung der zu treffenden Datensicherheitsmassnahmen. Im Leitfaden des EDSB zu den technischen und organisatorischen Massnahmen werden drei (bzw. vier) Sicherheitsstufen unterschieden, die von “keine besondere Beeinträchtigung” bis zu “Gefahr für Leib und Leben” für die

Betroffenen reichen. Sie dienen den Systementwicklern als Orientierungshilfe für die Ergreifung der Massnahmen. Detaillierte Aussagen können jedoch nur bei Kenntnis eines Projekt im konkreten Umfeld gemacht werden

Die höchste Sensibilität ist ab Stufe 3 gegeben. Hier ist der Stand der Technik umzusetzen. Die Risiken bzw. Gefahren für die Bearbeitung von Daten der Stufe 3 (und höher) werden wie folgt aufgeführt:

Stufe 3: / Hoch
Personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen kann, bzw. die einem besonderen Amtsgeheimnis unterliegen, z. B.

- Patientenkarteien
- Personaldaten,
  insbesondere aber auch diejenigen Daten, welche im Bundesgesetz über den Datenschutz (DSG) unter
- Art. 3 lit. c besonders schützenswerte Personendaten
  lit. d Persönlichkeitsprofil
  aufgeführt sind.

(Stufe 4: / Sehr hoch)
Personenbezogene Daten, deren Missbrauch für den Betroffenen Gefahren für Leib und Leben bedeutet, z. B.

- Adressen von polizeilichen V-Leuten
- Adressen von Zeugen in bestimmten Strafverfahren
- Adressen von Personen, die aufgrund ihrer Meinungsäusserungen bedroht sind.

Es ist erstaunlich, wie oft wir auch heute noch feststellen müssen, dass in den Planungsunterlagen von sensitiven EDV-Projekten keine angemessenen Datensicherungsmassnahmen aufgeführt sind. Wie erwähnt, muss ab der Sicherheitsstufe 3 der Stand der Technik bei den Sicherheitsvorkehrungen realisiert werden. Bei der Datenübermittlung beispielsweise ist eine Chiffrierung auf Applikationsebene anzustreben um die Vertraulichkeit zu garantieren. Sollte dies nicht möglich sein, so ist aufzuführen, warum diese Massnahme nicht umgesetzt werden kann (Beurteilung der Angemessenheit). Diesbezüglich muss allerdings festgehalten werden, dass immer mehr Produkte am Markt verfügbar sind, die eine umfassenden Datensicherheit bereitstellen.

Gesetzliche Vorgaben sind MUSS-Zielsetzungen für die Systementwicklung. Aus diesem Grunde müssen die Datensicherheitsüberlegungen ab Projektbeginn in die Planung einfliessen. Verantwortlich für den Datenschutz ist der Inhaber der Datensammlung d.h. die privaten Personen oder die Bundesorgane, die über Zweck und Inhalt der Datensammlung entscheiden. Diese sind darauf angewiesen, dass die Sachverständigen nachvollziehbar aufzeigen, welche Massnahmen realisierbar sind, welche Wirkungen sie haben und welche Ressourcen benötigt werden. Erst aufgrund dieser transparenten Darstellung wird es dem Inhaber der Datensammlung möglich sein, seiner Verantwortung gerecht zu werden.

5. Nachrichtendienst

Pflicht des militärischen Nachrichtendienstes zur Anmeldung seiner Datensammlungen

Das neue Bundesgesetz über die Armee und die Militärverwaltung sieht die Schaffung eines Nachrichtendienstes vor. Es ermächtigt den Bundesrat, Ausnahmen von der Pflicht zur Registrierung von Datensammlungen nach DSG vorzusehen. Damit ist der Nachrichtendienst jedoch nicht von der Pflicht zur Anmeldung dieser Datensammlungen bei uns entbunden.

Der Nachrichtendienst der Armee hat zur Aufgabe, sicherheitspolitisch bedeutsame Informationen über das Ausland zu beschaffen, auszuwerten und zu verbreiten. Der Bundesrat wird im neuen Bundesgesetz über die Armee und die Militärverwaltung ermächtigt, diesbezüglich Ausnahmen von den datenschutzrechtlichen Vorschriften über die Registrierung von Datensammlungen vorzusehen. Ausgehend von dieser Bestimmung entbindet aber die Verordnung über den Nachrichtendienst diesen nicht nur von der Registrierungspflicht, sondern auch von der Pflicht zur Anmeldung von nachrichtendienstlichen Datensammlungen.

Das Bundesgesetz über den Datenschutz (DSG) unterscheidet klar zwischen Anmeldungs- und Registrierungspflicht.
Die Anmeldung gewährleistet dem EDSB die Aufsicht über die vom Nachrichtendienst geführten Datensammlungen. Bundesorgane sind nach DSG verpflichtet, ihre Datensammlungen anzumelden. Ausnahmen von der Anmeldungspflicht müssen gesetzlich ausdrücklich vorgesehen werden.

Die vom Bundesrat schlussendlich gewählte Lösung entspricht nicht ganz den Bestimmungen des DSG betreffend Anmeldung der Datensammlungen. Das Militärgesetz sieht keine Ausnahme von der datenschutzrechtlichen Anmeldungspflicht vor und entbindet den Nachrichtendienst nur von der Registrierungspflicht. Die bundesrätliche Verordnung sieht jedoch die Anmeldung der Datensammlungen des Nachrichtendienstes nur dann vor, wenn dadurch keine Gefährdung der Informationsbeschaffung entsteht. Aber auch wenn die Informationsbeschaffung nicht gefährdet wird, ist eine ordentliche Anmeldung der Datensammlung nicht vorgesehen. Der Eidgenössische Datenschutzbeauftragte soll in solchen Fällen nur in allgemeiner Form über das Bestehen solcher Datensammlungen informiert werden.

6. Steuern

Datenschutzklauseln in Steuererlassen - Mehrwertsteuergesetz und Militärpflichtersatzverordnung

In internationalen und in nationalen Steuererlassen wird den Anforderungen an den Datenschutz heute regelmässig mit spezifischen Datenschutzbestimmungen Rechnung getragen. Dabei zeichnet sich die Herausbildung eines normativen Standards ab.

Gemäss DSG müssen für gewisse Datenbearbeitungen formellgesetzliche Grundlagen geschaffen werden. Im Rahmen der hängigen Gesetzgebungsverfahren haben

wir uns von der Eidgenössischen Steuerverwaltung die bei der Mehrwertsteuer und beim Militärpflichtersatz anfallenden Datenbearbeitungen erläutern lassen. Dabei hat sich ergeben, dass in beiden Bereichen formellgesetzliche Grundlagen für die Datenbearbeitung geschaffen werden müssen. Für das Mehrwertsteuergesetz haben wir daher im Rahmen des Vernehmlassungsverfahrens einen ausgearbeiteten Ergänzungsvorschlag eingebracht. Desgleichen haben wir bei der Revision der Militärpflichtersatzverordnung Vorschläge unterbreitet, welche von der Eidg. Steuerverwaltung übernommen wurden. Eine Anpassung des Militärpflichtersatzgesetzes ist für die kommende Revision vorgesehen. Bei dieser Gelegenheit können diese Vorschläge von der Verordnung in ein formelles Gesetz übergeführt werden.

Im einzelnen geht es darum, die wichtigen Datenbearbeitungen und die zur Verwirklichung des Steuergeheimnisses und des Datenschutzes erforderlichen organisatorischen und technischen Vorkehren in den groben Zügen zu umschreiben. Anders als bei der Mehrwertsteuer führt die Eidgenössische Steuerverwaltung beim Militärpflichtersatz keine zentrale Datensammlung, sondern überlässt den Vollzug den Kantonen. Aus diesem Grund ist es hier besonders wichtig, dass landesweit ein minimaler Sicherheitsstandard gewährleistet ist. Dies umsomehr, als im Rahmen des Militärpflichtersatzes regelmässig heikle Gesundheitsdaten bearbeitet werden. Erfreulicherweise wurde in die Militärpflichtersatzverordnung daher eine Bestimmung aufgenommen, wonach die Eidgenössische Steuerverwaltung Weisungen über die Anforderungen an die Datensicherheit erlassen und gemäss den Empfehlungen des Bundesamtes für Informatik für die Koordination sorgen kann (vgl. zur erheblichen Bedeutung solcher koordinierender Vorschriften unsere Ausführungen im 2. Tätigkeitsbericht S. 81f.)

Im Rahmen der OECD berät eine Arbeitsgruppe gegenwärtig die Aufnahme einer spezifischen Datenschutzklausel in das Musterabkommen zur Vermeidung der Doppelbesteuerung. Wir haben den schweizer Vertretern in dieser Arbeitsgruppe unsere Befürwortung dieses Vorhabens signalisiert.

7. Banken

Pflicht zur Offenlegung von Bankverbindungen für Anlage- und Handelsgeschäfte durch Bankangestellte

Eine Bank darf allen Angestellten die Offenlegung ihrer Bankverbindungen betreffend Handels- und Anlagegeschäfte vorschreiben, wenn dies für die Beachtung ihrer Sorgfaltspflicht und die Verhinderung von Insidergeschäften erforderlich ist.

Eine private Person machte uns auf das "Reglement für Anlage- und Handelsgeschäfte" einer Bank aufmerksam, welches die Offenlegung sämtlicher Bankverbindungen betreffend Handels- und Anlagegeschäfte aller Mitarbeiter und Mitarbeiterinnen verlangt. Werden Anlage- und Handelsgeschäfte über nicht bewilligte Konti bei Drittbanken abgewickelt, so gilt dies als grober Verstoss gegen das Reglement und kann arbeitsrechtliche Konsequenzen haben (bis hin zur fristlosen Kündigung).

Zweck des Reglementes für die Offenlegung von Anlage- und Handelsgeschäften ist einerseits die Verhinderung von Insidergeschäften, andererseits der Schutz der Mit-

arbeiter, die durch Handelsgeschäfte in Konflikt mit eigenen Interessen, den Interessen der Kunden oder denjenigen der Bank kommen könnten. Zudem unterstehen die Banken der Aufsicht durch die Eidgenössische Bankenkommission und haben im Rahmen ihrer Sorgfaltspflicht diese Bankverbindungen zu überprüfen.

Da der Arbeitgeber Daten über den Arbeitnehmer grundsätzlich nur bearbeiten darf, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind, stellte sich die Frage, inwiefern es für die Bank erforderlich ist, die Bankverbindungen für Anlage- und Handelsgeschäfte jener Angestellten zu kennen, welche in ihrer Tätigkeit nicht mit Informationen im Finanzbereich zu tun haben. Wie unsere Abklärungen ergeben haben, bestehen zwischen den verschiedenen Abteilungen der betreffenden Bank sehr enge Verknüpfungen, weshalb (fast) jeder Mitarbeiter mit Informationen im Finanzbereich in Berührung kommen kann.

Aus diesen Gründen wurde die Erhebung der Bankverbindungen für Handels- und Anlagegeschäfte sämtlicher Angestellter im vorliegenden Fall als zulässig qualifiziert.

8. Videoüberwachung

Videoüberwachung bei Kehrichtsammelstelle

An einer öffentlichen Kehrichtsammelstelle soll von einer privaten Firma eine Videokamera installiert werden, um den Bereich um die aufgestellten Container, die Benutzer der Sammelstelle, das benutzte Auto sowie das Nummernschild desselben aufzuzeichnen. Zweck der Videoüberwachung soll die Identifizierung von Personen sein, die die Sammelstelle zweckentfremden und missbräuchlich benutzen. Die Container befinden sich auf dem Werkhof der Gemeinde.

Eine private Sicherheitsfirma, die Überwachungsgeräte installieren soll, ist eine private Person im Sinne des DSG. Erteilt jedoch eine Gemeinde einer privaten Firma den Auftrag zur Installation einer Videokamera und damit zur Aufzeichnung der Bewegungsabläufe auf dem Werkhofareal, so handelt es sich um eine Datenbearbeitung im Auftrag. Verantwortlich für die Einhaltung des Datenschutzes ist der Auftraggeber, hier die Gemeinde. Die Gemeinde ist jedoch weder Bundesbehörde noch private Person. Aus diesem Grunde fällt sie nicht unter das DSG, sondern unter die Datenschutzbestimmungen des betreffenden Kantons.

Die Problematik der Videoüberwachung durch Private stellt sich aus unserer Sicht allgemein wie folgt dar:
Personendaten im Sinne des DSG sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Unter Bearbeiten wird jeder Umgang mit Personendaten verstanden, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten. Wenn mittels Kamera die Benutzer der Kehrichtsammelstelle gefilmt werden, so enthalten die Filmaufnahmen Angaben über diese Personen. Sie können etwa anhand der Gesichter oder der Autokennzeichen identifiziert und damit bestimmt werden. Beim Aufzeichnen von Bewegungsabläufen von Personen handelt es sich um einen Eingriff in die Persönlichkeit, der gerechtfertigt sein kann, um Missbräuchen vorzubeugen bzw. dieselben ahnden zu

können.
Auch wenn ein Rechtfertigungsgrund für die Aufzeichnung vorliegt, müssen die datenschutzrechtlichen Bearbeitungsgrundsätze der Verhältnismässigkeit und der Zweckgebundenheit beachtet werden. Das bedeutet, dass die Aufzeichnungen nur erstellt und ausgewertet werden dürfen, um Missbräuche zu verhindern bzw. ahnden zu können. Anderweitige Verwendungen der Aufzeichnungen wären nicht zulässig.
Der Grundsatz der Verhältnismässigkeit verlangt zudem, dass nur diejenigen Daten, die für die Erfüllung des Zweckes erforderlich sind, aufgezeichnet werden dürfen. Die Aufzeichnungen dürfen nur während möglichst kurzen Zeiträumen, etwa in der Nacht erstellt werden, wenn tagsüber keine Missbräuche erfolgen. Darüber hinaus müssen die Aufzeichnungen über Bewegungsabläufe, die nachweislich nicht auf Missbräuche hinweisen, sofort vernichtet werden.

9. Verschiedenes

9.1. Das Handelsregister als elektronische Datenbank

Neueinträge im Eidgenössischen Handelsregister wurden bisher im Schweizerischen Handelsamtsblatt (SHAB) publiziert. Das Eidgenössische Amt für das Handelsregister prüft zur Zeit die Einführung der elektronischen Führung des Handelsregisters, um die darin enthaltenen Daten der Öffentlichkeit einfacher zugänglich zu machen.

Das Eidgenössische Amt für das Handelsregister ersuchte uns um Beratung in Hinblick auf die Automatisierung des Handelsregisters. Die Datenbearbeitung im Rahmen öffentlicher Register ist nach sehr detaillierten und formellen Vorschriften geregelt. Bedeutsam für das Handelsregister sind insbesondere die Bestimmungen des Obligationenrechts (OR) und der Handelsregisterverordnung (HRegV). Aus Gründen der Rechtssicherheit sollen diese Vorschriften durch das DSG nicht geändert werden, weshalb das Handelsregister als öffentliches Register des Privatrechtsverkehrs vom Geltungsbereich des DSG ausgenommen ist. Dies schliesst jedoch bei neuen Datenbearbeitungen die Schaffung besonderer Datenschutzbestimmungen im OR und in der HRegV nicht aus. Dabei können die im DSG und der VDSG sowie in der Empfehlung Nr. R (91) 10 des Ministerkomitees des Europarates an die Mitgliedstaaten für die Übermittlung der von öffentlichen Stellen gespeicherten personenbezogenen Daten an Dritte vorgesehenen Lösungen herangezogen werden.

Vor diesem Hintergrund haben wir in einem ersten Schritt vorgeschlagen, die Kategorien der bearbeiteten Personendaten und den Zweck der elektronischen Bearbeitung zu definieren. Ferner ist die für die Datensammlung verantwortliche Stelle zu bezeichnen, welche die Auswahlkriterien und Bedürfnisnachweise für den Zugriff auf die Daten festlegt.
Obwohl das Register einen öffentlichen Charakter hat, bedeutet dies nicht, dass die Daten unbeschränkt zugänglich gemacht und verwendet werden dürfen. Das Zweckbindungsgebot ist nämlich auch auf öffentlich zugängliche Daten anwendbar. Dies bedeutet, Daten dürfen nicht an Dritte übermittelt werden, wenn die Bekanntgabe mit dem Zweck unvereinbar ist, für den sie erhoben wurden. Damit betroffene Personen sich gegen eine Bearbeitung ihrer Daten wehren können, muss auch das Auskunftsrecht gewährleistet sein. Im Interesse der Datensicherheit müssen zudem sämtliche vorgenannte Kriterien mit den technischen und organisatorischen Massnahmen abgestimmt werden.

9.2. Reiseteilnehmerlisten bei Gruppenreisen

Reiseunternehmen, die bei der Durchführung von Gruppenreisen Adresslisten der Teilnehmer erstellen und bekanntgeben, sollten die betroffenen Personen zuvor über die Erstellung dieser Listen orientieren. Wer auf der Liste nicht aufgeführt werden möchte, sollte dies dem Reiseunternehmen, wenn möglich bei Vertragsabschluss, mitteilen können.

Ein Reiseunternehmen erstellte seit Jahren für die Teilnehmer von Gruppenreisen Adresslisten (bestehend aus Anrede, Name, Vorname, Adresse und Nationalität). Der Zweck dieser Listen bestand darin, die Teilnehmer vor Antritt der Reise übereinander zu informieren, damit allenfalls gemeinsame Hin- und Rückreisen organisiert und nach der Reise die geknüpften Kontakte aufrechterhalten werden konnten. Aufgrund von Reklamationen stellte die Reiseunternehmung das Erstellen dieser Listen und wandte sich an uns, um abzuklären, ob die Verwendung solcher Adresslisten erlaubt sei.

Grundsätzlich können Personendaten für die Erstellung von Listen verwendet werden, wenn die betroffenen Personen davon Kenntnis haben. Die Errichtung von Teilnehmerlisten wird erst problematisch, wenn die betroffenen Personen dies nicht wissen. Die Adressdaten werden vom Reiseunternehmen nämlich für die Abwicklung des Vertragsverhältnisses (Buchung der Reise und Rechnungsstellung) beschafft. Die weitere Bearbeitung für Adresslisten, die Dritten (anderen Reiseteilnehmern) bekanntgegeben werden, erfordert deshalb die Einwilligung der Betroffenen. Daher sollte der Kunde vorgängig entsprechend informiert werden, damit er die Möglichkeit hat, der weiteren Bearbeitung seiner Daten zuzustimmen oder sie abzulehnen.

9.3. Das Antragsformular für die Miete eines Fahrzeuges

Ermächtigungsklauseln in Antragsformularen für die Miete von Personenwagen dürfen nicht so allgemein verfasst sein, dass der Vermieter Erkundigungen bei irgend jemandem einholen kann. Für den Mieter muss klar ersichtlich sein, bei wem welche Abklärungen über ihn eingeholt werden sollen und wozu er die Einwilligung erteilt.

Eine private Person gelangte mit der Frage an uns, ob es üblich sei, dass bei der Miete eines Personenwagens Erkundigungen bei den PTT eingeholt würden. Eine Überprüfung des Antragformulars ergab, dass neben dem Namen und der Adresse der Beruf, der Arbeitgeber und dessen Adresse sowie die Dauer der Anstellung anzugeben waren. Gleichzeitig wurde der Fahrzeugvermieter ermächtigt, "sämtliche Angaben überprüfen zu können". Wenn eine Ermächtigungsklausel derart allgemein gehalten ist, kann der Kunde nicht kontrollieren, bei welchen Stellen und Organisationen weitere Nachforschungen über ihn angestellt werden. Aus datenschutzrechtlicher Sicht ist eine derartige Einwilligung ungültig, da der Mieter nur in einen klar bestimmten Sachverhalt einwilligen kann.
Die betroffene Unternehmung hat in der Folge ihr Antragsformular datenschutzkonform revidiert und die Ermächtigungsklausel lautet neu: "Der Mieter ermächtigt den Vermieter, diese Angaben beim Arbeitgeber beziehungsweise den angegebenen Referenzadressen zu überprüfen".

9.4. Akteneinsichtsgesuch des Historischen Lexikons der Schweiz beim Schweizerischen Bundesarchiv bezüglich Chefbeamte

Das Historische Lexikon der Schweiz (HLS) möchte über Chefbeamte jeweils zehn Zeilen umfassende biographische Artikel verfassen. Um die nötigen Informationen über die nicht mehr amtierenden Chefbeamten zu erhalten, hat sich das HLS an das Schweizerische Bundesarchiv (BAR) mit der Bitte gewandt, in die beim BAR lagernden Personaldossiers der betreffenden Chefbeamten Einsicht nehmen zu dürfen. Mit einer generellen Einsichtgewährung konnten wir uns aus Datenschutzgründen nicht einverstanden erklären.

Bei den betreffenden Beamten handelt es sich zum Teil um zur Zeit noch lebende und zum Teil um bereits verstorbene Personen. Es stellt sich die Frage, ob es zulässig ist, Personaldossiers, die besonders schützenswerte Personendaten oder Persönlichkeitsprofile enthalten, Drittpersonen zugänglich zu machen, damit diese biographische Artikel im Umfang von 10 Zeilen über die betreffende Person veröffentlichen können. Die Bekanntgabe von Personendaten durch das BAR unterliegt zur Zeit noch einem Reglement des BAR. Dessen Bestimmungen sind jedoch datenschutzkonform auszulegen.
Gemäss dem Reglement dürfen Personendaten nach 35 Jahren bedingungslos der Öffentlichkeit zugänglich gemacht werden, sofern keine öffentlichen oder privaten Interessen beeinträchtigt werden. Das bedeutet, dass in jedem Einzelfall geprüft werden muss, ob die Einsichtgewährung in ein beim BAR lagerndes Personaldossier private Interessen beeinträchtigt. Dabei sind die verschiedenen sich gegenüberstehenden Interessen gegeneinander abzuwägen.
Personaldossiers enthalten im allgemeinen besonders schützenswerte Personendaten (wie etwa Krankengeschichten, Arztzeugnisse). Oder aber es ergibt sich aufgrund der im Personaldossier enthaltenen Dokumente (wie Qualifizierungen, Beurteilungsgespräche, Lebensläufe, Informationen über Familienverhältnisse) ein Persönlichkeitsprofil der betreffenden Person. Lebt diese noch, so ist grundsätzlich davon auszugehen, dass die Einsichtgewährung ihre privaten Interessen beeinträchtigen kann. Demzufolge dürfen solche Personendaten auch nach 35 Jahren nicht der Öffentlichkeit zugänglich gemacht werden, es sei denn, die betroffene Person ist mit der Einsichtgewährung einverstanden.

Einsicht in Personaldossiers von verstorbenen Personen ist nur dann zu gewähren, wenn der Gesuchsteller ein Interesse nachweist und der Einsichtnahme keine überwiegenden Interessen von Angehörigen der verstorbenen Person oder von Dritten entgegenstehen.
Sowohl bezüglich noch lebender als auch bei verstorbenen Personen rechtfertigt sich die Gewährung der Einsicht im vorliegenden Fall aus Gründen der Verhältnismässigkeit nicht. Es ist unverhältnismässig, einer Drittperson Dokumente mit besonders schützenswerten Personendaten oder Dokumente, aus denen sich Persönlichkeitsprofile ergeben können, zugänglich zu machen, wenn dies nur dazu dient, Eckdaten für einen zehnzeiligen biographischen Artikel zu sammeln.

9.5. Aufnahme von wissenschaftlichen Interviews

Die Schweizerische Landesphonothek führt mit dem Bundesamt für Kommunikation wissenschaftliche Interviews mit Zeitzeugen zur Rolle der Schweiz ab den dreissiger Jahren durch. Die Aufnahmen sollen anschliessend in einer Datenbank dokumentiert

und der wissenschaftlichen Forschung zugänglich gemacht werden.

Die Schweizerische Landesphonothek führt mit dem Bundesamt für Kommunikation eine Reihe von wissenschaftlichen Interviews mit Zeitzeugen zur Rolle des Radios in der Schweiz ab den dreissiger Jahren durch. Dies betrifft einerseits Radiopioniere, andererseits aber auch damalige Radiohörer. Die Aufnahmen werden anschliessend in einer Datenbank dokumentiert und der wissenschaftlichen Forschung zugänglich gemacht.

Die Schweizerische Landesphonothek hat sich an uns gewandt, da sie Wert darauf legt, dass dieses wissenschaftliche Projekt vollumfänglich den gesetzlichen Vorgaben entspricht. Zu diesem Zweck hat sie uns den Entwurf eines Reglementes für die Datenaufnahme und die nachherige Bearbeitung und Nutzung der Daten durch Dritte zur Stellungnahme vorgelegt.
Wir vertraten die Ansicht, dass das Reglement grundsätzlich allen befragten Personen vor dem Interview zugänglich gemacht werden sollte und dass grundsätzlich alle Dokumente bzw. Kopien bis auf zu regelnde Ausnahmen der Öffentlichkeit nur anonymisiert zugänglich gemacht werden dürfen. Desweiteren wiesen wir die Landesphonothek darauf hin, dass sie als Dateninhaberin für die Einhaltung des Datenschutzes verantwortlich sei. Im übrigen konnten wir uns mit dem uns vorgelegten Entwurf einverstanden erklären. Unseren Forderungen wurde vollumfänglich Rechnung getragen.

9.6. Adoptionen und Aufenthaltsnachforschungen

Nachforschungen nach den leiblichen Eltern werden immer häufiger von privaten Vermittlungsstellen vorgenommen. Dabei werden oft Behörden um die Bekanntgabe von Adressen angefragt. Es ist jedoch Aufgabe der zuständigen Adoptionsbehörde, bei Anfragen von Personen, die ihre leiblichen Eltern suchen, nach einer entsprechenden Abklärung und Interessenabwägung die Adressen der leiblichen Eltern bekanntzugeben, sofern diese damit einverstanden sind.

Die Einwohnerkontrolle einer Gemeinde wurde von verschiedenen Vermittlungsinstitutionen für Adoptivkinder nach den Adressen der leiblichen Eltern gefragt. Die Vermittlungsstellen sind im Gegensatz zu den Amtstellen nicht verpflichtet, die Adoptionsakten nach der Adoption zu vernichten und haben so die Möglichkeit, aufgrund des früheren Wohnsitzes der leiblichen Eltern nach der aktuellen Adresse zu suchen. Die Einwohnerkontrolle erkundigte sich bei uns, inwiefern die Beantwortung solcher Anfragen mit dem Adoptionsgeheimnis vereinbar sei.
Einwohnerkontrollen sind Gemeindeorgane, die den kantonalen Datenschutzbestimmungen unterstehen. Soweit keine kantonalen Datenschutzvorschriften bestehen, gelten für das Bearbeiten von Personendaten durch kantonale Organe beim Vollzug von Bundesrecht gewisse Bestimmungen des DSG. Im vorliegenden Fall vollziehen die Einwohnerkontrollen als kantonale Organe Bundesrecht, weshalb gewisse Bestimmungen des DSG in Kantonen ohne kantonales Datenschutzgesetz Anwendung finden. Diese Kantone bestimmen ein Kontrollorgan, welches für die Einhaltung des Datenschutzes sorgt.
Da die Kenntnis der Abstammung ein wichtiges Element für die persönliche Entwicklung eines Menschen bildet, stellt sich die Frage, wer mit dem Adoptionsgeheimnis geschützt werden soll. In erster Linie soll es das Kind schützen. Die leiblichen Eltern des Kindes sollen nicht die Möglichkeit haben, sich durch weiteren Kontakt mit dem

Kind in dessen Erziehung einzumischen und dadurch das Gelingen der Adoption zu gefährden. Die durch Adoption begründete Familie soll sich gleich wie die auf der leiblichen Abstammung basierende unabhängig von äusseren Einflüssen entwickeln können. Aus diesem Grund darf die Identität der Adoptiveltern ohne ihre Zustimmung den leiblichen Eltern des Kindes nicht bekanntgegeben werden. Die soziale Integration des Kindes in seine neue Familie als Hautpzweck des Adoptionsgeheimnisses verlangt indessen nicht, dass die Geheimhaltungspflicht für immer aufrecht erhalten bleibt.
Wir sind der Auffassung, wenn das Kind den Wunsch hegt, seine leiblichen Eltern kennenzulernen, muss eine Interessenabwägung vorgenommen werden. Es sollte von den Adoptionsbehörden und nicht von privaten Vermittlungsstellen geprüft werden, ob tatsächlich ein überwiegendes Interesse der betroffenen Person an der Datenbekanntgabe besteht und inwiefern die übrigen Beteiligten (Adoptiveltern und leibliche Eltern) zur Bekanntgab der Identität bereit sind oder ob anderweitige stichhaltige Interessen entgegenstehen. Die Verantwortung für die Entscheidfindung im Einzelfall liegt freilich stets bei der betreffenden Behörde.

9.7. Arbeitsgruppe der Kantone

Die Zusammenarbeit mit den kantonalen Datenschutzbehörden gehört zu den gesetzlichen Aufgaben des Eidgenössischen Datenschutzbeauftragten. Diese Zusammenarbeit ist von grosser Bedeutung, namentlich in Hinblick auf die zahlreichen Datenbearbeitungen und Informationssysteme zwischen Bund und Kantonen. Diese Zusammenarbeit erfolgt insbesondere durch die Schweizerische Konferenz der Datenschutzbeauftragten (siehe auch S. 89) und durch unsere Beteiligung an einer Arbeitsgruppe, die von den kantonalen Datenschutzbeauftragten der Kantone Zürich, Bern, Basel-Land, Freiburg und Luzern gebildet wurde.

Der Zweck dieser informellen Arbeitsgruppe besteht darin, den Informationsaustausch zwischen den Kantonen über gemeinsame Fragen zu verstärken. Die Arbeitsgruppe steht allen kantonalen Datenschutzbehörden offen, sofern sie dabei sein möchten und bereit sind, aktiv mitzuarbeiten. Die Arbeitsgruppe möchte auch die Zusammenarbeit mit dem Eidgenössischen Datenschutzbeauftragten verstärken und hat ihn zu diesem Zweck an ihre Sitzungen eingeladen. Wir haben uns bereit erklärt, in Funktion der behandelten Themen teilzunehmen, sofern daraus keine Nachteile für die anderen Kantone und die Schweizerische Konferenz der Datenschutzbeauftragten entstehen. Wir haben bisher an drei Sitzungen teilgenommen, an denen die folgenden Themen behandelt wurden: Information zwischen den Kantonen und dem Bund, Datensicherheit in Netzen und Daten über die Gesundheit.

IV. INTERNATIONALES

1. Internationale Konferenz der Beauftragten für den Datenschutz

Die 17. Internationale Konferenz der Datenschutzbeauftragten fand auf Einladung des dänischen Datenschutzbeauftragten vom 6. bis 8. September 1995 in Kopenhagen statt. An dieser Konferenz trafen die Datenschutzbeauftragten von 25 Staaten mit Regierungsexperten und Vertretern der Europäischen Union, der Wirtschaft, der

Wissenschaft und Vertretern des Diensleistungssektors zusammen. Die Schweiz war durch den stellvertretenden Eidgenössischen Datenschutzbeauftragten und den Datenschutzbeauftragten des Kantons Zürich vertreten. An der Konferenz wurden die jüngsten internationalen Entwicklungen und insbesondere die EU-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr erörtert. Die Konferenz ermöglichte auch einen vertieften Informationsaustausch über den Schutz der Privatsphäre im Arbeitsbereich (Problematik der automatisierten Überwachung am Arbeitsplatz: Überwachung der beruflichen Tätigkeit und insbesondere automatische Erfassung der Arbeitszeit, Abhörung von Telefongesprächen zur Kontrolle der Arbeitseffizienz und -qualität, Überwachung von Netzen, Videoüberwachung und die Erscheinung des “elektronischen Vorarbeiters”; Verwendung von genetischen Daten im Arbeitsbereich; Information der betroffenen Personen über ihre Rechte). Die Konferenzteilnehmer befassten sich ausserdem mit Datenschutz-Problemen im Bereich der Forschung und der Statistik, insbesondere am Beispiel der skandinavischen Länder und der Arbeiten des Europarates. Besprochen wurden auch die technologischen Entwicklungen, aus denen sich neue Risiken für die Privatsphäre und den Datenschutz ergeben (insbesondere durch die Multiplikation von elektronischen Spuren, ohne dass die betroffene Person in der Lage ist, den Überblick oder die Kontrolle über alle individuellen Verbindungen, die sie herstellt, zu behalten, ebenso Multifunktionalität und Multimedia, Digitalisierung, Bearbeitung von Bild und Ton). Nach Ansicht der Datenschutzbeauftragten müssen der Datenschutz und die Datensicherheit angesichts dieser neuen Technologien dringend ausgebaut werden. Durch diese neuen Technologien ergeben sich im Bereich der Datenbearbeitung nämlich tiefgreifende Veränderungen, insbesondere durch die Möglichkeit, Ton, Bild und Text zu kombinieren sowie durch die Möglichkeit einer weiträumige Verbreitung von Informationen und wegen der unbegrenzten Kombinationsmöglichkeiten. Erforderlich ist vor allem die Einschränkung der Verwendung von Personendaten durch die Anwendung anonymer Verfahren (anonyme Bezahlung, anonymer Verbindungsaufbau usw.) sowie durch die Beschränkung der Zugriffe auf Daten entsprechend dem jeweils verfolgten Zweck. Die Kontrollverfahren müssen verbessert werden, namentlich indem spezielle Datenschutz-Programme entwickelt und angewendet werden. Ausserdem ist es unerlässlich, bei der Konzeption und Entwicklung von Informationssystemen Technologien zu berücksichtigen, welche die Privatsphäre schützen (Chiffrierungstechniken, Anonymisierung durch den einmaligen Einsatz einer Pseudo-Identität). Zudem betonten die Datenschutzbeauftragten einmal mehr die Bedeutung der Information der Öffentlichkeit für die Sensibilisierung der verschiedenen Beteiligten bezüglich der Risiken der neuen Technologien, was zu einer erhöhten Wachsamkeit und zur Ermutigung der betroffenen Personen, ihre Rechte wahrzunehmen, führt.

2. Europarat

Die Projektgruppe für Datenschutz des Europarates ist unter dem Vorsitz der Schweiz zweimal zusammengetreten. Sie hat insbesondere ihre Arbeit im Zusammenhang mit der Verabschiedung einer Empfehlung zum Schutze medizinischer Daten sowie einer Empfehlung zum Schutze von Personendaten, die zu statistischen Zwecken erhoben und bearbeitet werden, fortgesetzt. Diese beiden Instrumente sollten dieses Jahr zum Abschluss gebracht und im Verlauf des Jahres 1997 vom Ministerkomitee verabschiedet werden. Ausserdem haben wir uns an den Arbeiten der Arbeitsgruppe 14 beteiligt, die beauftragt ist, einen Entwurf für eine Empfehlung zum Schutze von Personendaten vorzubereiten, die für Privatversicherungszwecke erho-

ben und bearbeitet werden. Schliesslich hat eine neue Arbeitsgruppe ihre Arbeiten im Zusammenhang mit den neuen Informationstechnologien, insbesondere mit den Datenautobahnen (Internet) und Multimedia aufgenommen.

Der durch die Konvention 108 geschaffene beratende Ausschuss, der namentlich damit beauftragt ist, Stellungnahmen zur Anwendung des besagten Übereinkommens abzugeben, hat seine Arbeiten im Zusammenhang mit der Definition von personenbezogenen Daten, insbesondere hinsichtlich des Einbezugs von Ton und Bild sowie des Begriffs des ”ungeborenen Kindes”, fortgesetzt. Er hat eine Stellungnahme zur “Kompatibilität von Daten” abgegeben und akzeptiert, dass die Verwendung von Personendaten, die ursprünglich zu anderen Zwecken erhoben wurden, zu statistischen Zwecken grundsätzlich mit dem ursprünglichen Zweck der Bearbeitung vereinbar ist, sofern gewisse Garantien abgegeben werden. Ausserdem hat er den Antrag eines Unterzeichnerstaates auf Ausarbeitung eines Zusatzprotokolls zur Konvention 108, das die internationale Unterstützung von betroffenen Personen verstärken sollte, zurückgewiesen. Auf unser Ersuchen hin hat er zu den Bedingungen für die Ratifizierung der Konvention 108 Stellung genommen. Darin hat er betont, dass unser Land die im Übereinkommen geforderten Kriterien für die Ratifizierung erfüllt. Somit enthält das schweizerische Recht ausreichende Garantien, die mit den Anforderungen des Übereinkommens übereinstimmen, um eine Ratifizierung des Übereinkommens durch die Schweiz zu ermöglichen, obwohl einige Kantone bislang über kein eigenes Datenschutzgesetz verfügen.

Das Europäische Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (STE Nr. 108) ist ein wichtiger Schritt in Richtung einer Harmonisierung der nationalen Gesetzgebungen und der Weiterentwicklung der internationalen Zusammenarbeit. Dadurch kann im Bereich des Datenschutzes ein hohes Niveau sichergestellt und zugleich der freie Datenaustausch gewährleistet werden. Es gilt für alle Datensammlungen und automatisierten Bearbeitungen von Personendaten im öffentlichen und privaten Bereich, sofern diese Daten sich auf identifizierte oder identifizierbare natürliche Personen beziehen. Es legt die Grundsätze und Grundlagen für den Datenschutz fest, welche die Vertragsstaaten in ihren innerstaatlichen Gesetzgebungen konkretisieren müssen. Einschränkungen in bezug auf den grenzüberschreitenden Datenaustausch zwischen den Vertragsstaaten werden im Übereinkommen grundsätzlich ausgeschlossen. Es regelt die Zusammenarbeit zwischen den Staaten für die praktische Umsetzung des Übereinkommens sowie insbesondere die Unterstützung, die ein Vertragsstaat betroffenen Personen leisten muss, die ihren Wohnsitz im Ausland haben. Dieses Übereinkommen wurde von 17 Vertragsstaaten ratifiziert, vier weitere haben es unterzeichnet. Mit Ausnahme der Schweiz und von Ungarn verfügen alle Staaten, die das Übereinkommen noch nicht ratifiziert haben, noch nicht über eine Gesetzgebung, welche die Anforderungen des Übereinkommens erfüllt.

Im Auftrag des EJPD haben wir die Arbeiten hinsichtlich der Ratifizierung der Konvention 108 fortgesetzt. Der Bundesrat wird seine Botschaft an das Parlament voraussichtlich im Laufe des Sommers verabschieden; damit sollte eine Ratifizierung in der ersten Hälfte dieser Legislaturperiode möglich werden. Die Ratifizierung der Konvention stellt in einer immer stärker vernetzten Welt eine politische und rechtliche Notwendigkeit dar. Sie wird letztlich zu einer Erhöhung des Rechtsschutzes des Individuums bei der Bearbeitung von Personendaten führen und gleichzeitig eine Vereinfachung des Informationsaustausches zwischen der Schweiz und den anderen Vertragsstaaten ermöglichen.

3. Europäische Union

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Europäischen Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr wurde am 24. Oktober 1995 verabschiedet. Die Mitgliedstaaten der Europäischen Union und des Europäischen Wirtschaftsraums haben drei Jahre Zeit, um diese Richtlinie in ihrem innerstaatlichen Recht umzusetzen.
Der Zweck dieser europäischen Richtlinie besteht darin, den Bürgern aller Mitgliedstaaten einen ausreichenden Schutz ihrer Privatsphäre zu gewährleisten und gleichzeitig den freien Austausch von Personendaten innerhalb der Europäischen Union und des Europäischen Wirtschaftsraums zu ermöglichen. Ausserdem zielt sie darauf ab, Wettbewerbsverzerrungen und das Risiko von Produktionsauslagerungen abzubauen. Die Richtlinie bezieht sich auf die Bearbeitung von Personendaten im öffentlichen und im privaten Bereich, soweit diese Datenbearbeitungen in den Zuständigkeitsbereich der Europäischen Union fallen. Sie gilt somit nicht für die Datenbearbeitung im Bereich der öffentlichen Sicherheit, der Verteidigung und der Staatssicherheit. Zwischen dem öffentlichen und dem privaten Bereich wird kein Unterschied gemacht. Die Richtlinie legt die Voraussetzungen fest, unter denen eine automatisierte oder nicht automatisierte Bearbeitung von Personendaten zulässig ist und zählt die Rechte der betroffenen Personen auf (insbesondere das Recht auf Information, das Auskunftsrecht, das Berichtigungsrecht, das Recht, eine Datenbearbeitung zu verweigern, sowie das Beschwerderecht). Sie bestimmt, welche Eigenschaften Personendaten aufweisen müssen (insbesondere Richtigkeit, rechtmässige und nicht gegen Treu und Glauben verstossende Beschaffung, rechtmässiger und sinnvoller Bearbeitungszweck, Vereinbarkeit, Verhältnismässigkeit), die Vertraulichkeit und die Bearbeitungssicherheit, die Bekanntgabe der Datenbearbeitungen und die Überwachung (unabhängige Kontrollbehörde mit Entscheidungsbefugnis und dem Recht, Klage einzureichen). Die Richtlinie nimmt, ausser bezüglich manueller Datenbearbeitungen, nicht mehr auf Datensammlungen Bezug, sondern auf die Datenbearbeitung. Geregelt wird schliesslich auch der grenzüberschreitende Datenaustausch, der innerhalb der Europäischen Union nicht behindert werden darf. Der Datenaustausch mit Drittstaaten dagegen ist grundsätzlich nicht zulässig, wenn diese nicht über eine als genügend beurteilte Datenschutzgesetzgebung verfügen. Ein Zweck der Richtlinie besteht im weiteren darin, die in der Europarat-Konvention 108 enthaltenen Grundsätze zu präzisieren und auszubauen. Wir haben zuhanden des Vorstehers des EJPD einen ersten Bericht über die Konsequenzen der Richtlinie für die Schweiz ausgearbeitet. Wir sind darin zum Schluss gekommen, dass das Bundesgesetz über den Datenschutz nicht in allen Punkten der europäischen Richtlinie entspricht. Unsere Gesetzgebung entspricht jedoch den Anforderungen der Konvention 108 und bietet in bezug auf die in der Richtlinie festgelegten Anforderungen ein ausreichendes und angemessenes Schutzniveau. Eine Anpassung des Gesetzes erscheint vor diesem Hintergrund gegenwärtig nicht notwendig. Es kann indessen nicht ausgeschlossen werden, dass eine Anpassung zu einem späteren Zeitpunkt notwendig wird, um unser Recht eurokompatibel zu gestalten. Bevor wir eine solche Anpassung in Betracht ziehen, sollten wir jedoch die Umsetzung der Richtlinie durch die Mitgliedstaaten in ihrem jeweiligen innerstaatlichen Recht abwarten. Die wichtigsten Lücken betreffen die Voraussetzungen für die Einwilligung, die Anforderungen in bezug auf den Zweck der Datenbearbeitung, die Bearbeitung von besonders schützenswerten Daten, das Recht auf Information der betroffenen Personen, den Umfang des Auskunftsrechts, die individuellen automatisierten Entscheidungen, die Haftung, die Bekanntgabe von Datenbearbeitungen (insbesondere im privaten Bereich) sowie die Entscheidungsbefugnisse der unabhängigen Kontrollbehörde.

V. REGISTER DER DATENSAMMLUNGEN

1. Bilanz

Trotz der Schwierigkeiten, auf die wir in unseren beiden ersten Tätigkeitsberichten hingewiesen haben (S. 78 und 86), wurden die Kontrolltätigkeit und die Registrierungsarbeiten fortgesetzt. Eine teilweise Veröffentlichung des Registers der Datensammlungen im Bundesblatt erfolgt demnächst.
Die Kontrolle und Registrierung der Anmeldungen von Datensammlungen und Meldungen von Datenbekanntgaben ins Ausland wurde fortgesetzt. Auf den kommenden Sommer ist die Veröffentlichung eines Teils der Datensammlungen aus dem öffentlichen Bereich sowie aller Datensammlungen aus dem privaten Sektor, die uns angemeldet wurden, vorgesehen.

2. DATAREG - Verwaltungssystem

Nachdem das Verwaltungssystem des Registers der Datensammlungen gut ein Jahr in Betrieb ist und das System aufgrund der gemachten Erfahrungen optimiert wurde, können anhand der aufgenommenen Registereinträge erste Aussagen zu Ausprägungen und Eigenschaften der Einträge gemacht werden.

Während das Jahr 1994 im Zeichen der offiziellen Inbetriebnahme von DATAREG stand, wurden 1995 erste Erfahrungen mit dem System gesammelt und ausgewertet und Optimierungen am System vorgenommen. So wurden unter anderem Anregungen der meldenden Stellen aufgenommen, die Kontrollausdrucke neu überarbeitet und gestaltet, Felder neu aufgeteilt, Längen angepasst, die Benutzeroberfläche optimiert.

Die nachfolgenden Ausführungen und Kennzahlen zu den registrierten Datensammlungen beziehen sich auf den Stand des Registers im Januar 1996.

Es wurden insgesamt 710 Datensammlungen registriert. Davon wurden 18 Einträge auf Hinweis der anmeldenden Stelle bereits wieder gelöscht. 605 Einträge stammen von Bundesorganen, 87 von Privaten. Von den 692 zur Zeit erfassten Registereinträgen werden bis auf vier alle publiziert.

Auf den Anmeldeformularen sind siebzehn Kategorien von bearbeiteten Personendaten zur Auswahl und als Beispiel vorgesehen. Insgesamt wurden im Register bis jetzt aber schon 685 Kategorien von bearbeiteten Personendaten aufgenommen. Diese Kategorien werden von den Einträgen 5187mal verwendet. Die Hitliste der Kategorien von bearbeiteten Personendaten wird angeführt von Adresse, Beruf, Nationalität/Heimatort, vor Identität und AHV-Nummer.

Es wurden 567 Kategorien von Datenempfängern und Beteiligten aufgenommen, welche 1578mal als Empfänger sowie 389mal als Beteiligte aufgeführt werden.

Bei den Einträgen für Bundesorgane wurden bis jetzt 286 verschiedene Rechtsgrundlagen genannt. Diese werden 880mal verwendet.

Bisher wurden 666 Adressen von anmeldenden Stellen in das System aufgenommen. Für die Einträge von Privaten wurden bis jetzt 16 Branchenkategorien ver-

geben.

VI. DER EIDGENÖSSISCHE DATENSCHUTZBEAUFTRAGTE

1. Auslagerung des Sitzes des EDSB vom Zentrum der Stadt Bern nach Zollikofen

Der Sitz des EDSB und seines Sekretariates befindet sich seit März 1993 an der Monbijoustrasse 5, im Zentrum der Stadt Bern. Das Eidgenössische Justiz- und Polizeidepartement entschied am 2. April 1996, dass aufgrund von Sparmassnahmen der EDSB neu in Zollikofen, mit öffentlichen Verkehrsmitteln 25 Minuten vom Zentrum der Stadt Bern entfernt, seinen Sitz begründen müsse. Mit diesem Entscheid wird die Erfüllung der vom Datenschutzgesetz vorgeschriebenen Aufgaben erheblich erschwert werden.

Im Hinblick auf die besonderen Aufgaben des EDSB hatte der Bundesrat bereits 1992 als Sitz des EDSB Bern bestimmt (Art. 30 Abs. 1 der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz). Damit der EDSB seine Funktion als Beratungs- und Kontrollstelle für die Einhaltung des Datenschutzes wahrnehmen kann, müssen mit Bundesstellen, privaten Inhabern von Datensammlungen und mit Privatpersonen regelmässig Kontakte gepflegt werden (Sitzungen, Kontrollen, Augenscheine, Seminarien, Konferenzen usw.). Die Wahrnehmung dieser Tätigkeiten erfordert somit eine nicht zu unterschätzende Mobilität des ganzen Sekretariates des EDSB.
Bereits vor Inkrafttreten des Datenschutzgesetzes stand das Eidgenössische Justiz- und Polizeidepartement vor dem Entscheid, den EDSB ausserhalb der Stadt Bern anzusiedeln. Damals wurde die Notwendigkeit der zentralen Örtlichkeiten - bundesintern und für die ganze Schweiz - jedoch erkannt und der Entscheid über den schon damals vorgesehenen Umzug nach Zollikofen revidiert. In der Folge wurden wir an der Monbijoustrasse untergebracht.

Der Entscheid vom 2. April 1996 des Eidgenössischen Justiz- und Polizeidepartementes scheint unwiderruflich. Durch die Verlagerung des Sekretariates wird es erhebliche Einbussen an Arbeitszeit der Mitarbeiter geben. Von diesem Umstand ebenso betroffen werden sämtliche ratsuchenden Personen (Private und Bundesbehörden), die bei uns eine Konsultation wünschen. Abgesehen von der Erhöhung der Reisekosten, werden durch den unvermeidlichen Zeitverlust auch grössere administrative Kosten verursacht.

2. Aufgabenentwicklung

Einen besonderen Zuwachs hatten wir in den Aufgabenbereichen der Telekommunikation, des Gesundheitswesens und des Personalwesens. Die Überprüfung von angemeldeten Datensammlungen und die Entwicklung des Registers der Datensammlungen haben einen erheblichen Teil der Kapazitäten unserer Stelle beansprucht. Zudem erhalten wir vermehrt Anfragen aus der Bevölkerung, insbesondere zu Problemen der Überwachung am Arbeitsplatz, zum Einsatz der neuen Kommuni-

kationstechnologien, zum Bereich der Wirtschaftsauskunfteien und zu Fragen des Direktmarketings, um nur einige der Anfragenbereiche zu nennen.

3. Information der Öffentlichkeit

Auch während des vergangenen Geschäftsjahres haben der EDSB und seine Mitarbeiter an verschiedenen Informationsveranstaltungen, Konferenzen und Kolloquien Referate über Problembereiche des Datenschutzes gehalten.

Über die in Zermatt verwaltete Datensammlung über Journalisten, über Datenschutzprobleme des INTERNET, und über die zweite schweizerische Konferenz der Datenschutzbeauftragten haben wir mittels Pressemitteilung die Öffentlichkeit informiert.
In übrigen haben wir auch dieses Jahr eine beträchtliche Anzahl von Informationsbroschüren an Private und Behörden verschickt.

Telefondienst des EDSB

Nebst den Anfragen, die bei uns schriftlich (siehe dazu auch Tabelle auf S. 91, 92) eingegangen sind, haben wir auch eine beträchtliche Anzahl von Anfragen telefonisch beantwortet.
Die Tabellen (vgl. S. 93 - 95) gibt die verschiedenen telefonischen Anfragen nach Themen strukturiert wieder.

4. Zweite schweizerische Konferenz der Datenschutzbeauftragten 1995

Am 20. Oktober 1995 fand in Bern unter reger Beteiligung von Vertreterinnen und Vertretern von kantonalen Datenschutzaufsichtsstellen die vom EDSB organisierte zweite schweizerische Konferenz der Datenschutzbeauftragten statt.

Folgende Themen wurden schwerpunktmässig behandelt: Das Auskunftsrecht im Gesundheitswesen, Vor- und Nachteile einer persönlichen Identifikationsnummer, Zugriff der Kantone auf Bundesanwendungen, EDV-Sicherheit Bund-Kantone, Volkszählung 2000, Verbesserung des Informationsaustausches zwischen kantonalen Datenschutzstellen und dem EDSB, die Tätigkeit der Eidgenössischen Datenschutzkommission sowie die Bekanntgabe der Identität von Fahrzeughalterdaten über den Auskunftsdienst 111 und Swiss Online (Videotex). Zu diesem Thema wurde eine Resolution verabschiedet, die fordert, dass alle Fahrzeughalter das Recht haben, die Veröffentlichung und Bekanntgabe ihrer Identität zu untersagen, ohne dies durch ein besonderes Interesse begründen zu müssen.
Aufgrund der positiven Erfahrungen soll nun jährlich eine schweizerische Konferenz der Datenschutzbeauftragten stattfinden. Der Datenschutzbeauftragte des Kantons Zürich hat sich bereit erklärt, 1996 die Organisation zu übernehmen.

5. Statistik über die Tätigkeit des Eidgenössischen Datenschutzbeauftragten

Zeitraum 1. April 1995 bis 31. März 1996

Konferenzteilnahmen:

National	International
25	15

Anzahl von Sitzungen:

	Bund	Private	Kantone
Intern	101	35	1
Extern	194	22	1
Total	295	57	2

Anzahl der Stellungnahmen

Anzahl der Stellungnahmen

Telefonauskunft

Telefonauskunft nach Anfragenden

Telefonauskunft nach Sachgebiet

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.
Delegierter für Information und Presse	Tsiraktsopulos Kosmas, lic. iur.
Rechtsdienst:	9 Personen
Informatikdienst:	3 Personen
Kanzlei:	4 Personen

VII. ANHANG

EUROPARAT

MINISTERKOMITEE

EMPFEHLUNG NR. R (95) 4

DES MINISTERKOMITEES AN DIE MITGLIEDSTAATEN

ZUM SCHUTZ PERSONENBEZOGENER DATEN IM BEREICH DER FERNMELDEDIENSTE, NAMENTLICH IM HINBLICK AUF DIE TELEFONDIENSTE

(angenommen vom Ministerkomitee am 7. Februar 1995, an der 528. Sitzung der Ministerdelegierten)

Das Ministerkomitee, gestützt auf Artikel 15.b der Satzung des Europarates,

In Erwägung, dass es das Ziel des Europarates ist, eine engere Verbindung zwischen seinen Mitgliedstaaten herzustellen;

Im Bewusstsein der zunehmenden Verwendung der Informatik im Bereich der Fernmeldedienste und der Vorteile, die der Benutzer aus den technologischen Entwicklungen insbesondere im Bereich der Telefondienste zieht;

Eingedenk, in diesem Zusammenhang, der Entwicklung in Richtung Digitalisierung der Netze sowie der damit verbundenen Vorteile für die Benützer der Fernmeldedienste;

In der Meinung jedoch, dass die technologische Entwicklung im Bereich des Fernmeldeverkehrs, besonders der Telefondienste, unter Umständen für das Privatleben des Benutzers Risiken sowie Einschränkungen seiner Kommunikationsfreiheit beinhalten kann;

In dieser Hinsicht bezugnehmend auf verschiedene neue Leistungsmerkmale, namentlich im Bereich der Telefondienste, beispielsweise die Anzeige der Rufnummer des Anrufers anzeigen, die Anrufumleitung und die Mobiltelefone sowie die Vorrichtungen zur Identifizierung böswilliger Anrufe und die automatischen Anrufbeantworter;

Auch in der Feststellung der Risiken für das Privatleben und die Kommunikationsfreiheit, die durch Telefonrechnungen mit Angabe der angerufenen Nummern verbunden sind;

In Anerkennung, dass die Bestimmungen des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Strassburg, 1981; S.T.E. 108) auf die Tätigkeiten automatisierter Datenverarbeitung durch Netzbetreiber und jede weitere Person, die Fernmeldedienste anbietet, anwendbar sind;

In der Meinung jedoch, dass es nötig ist, die allgemeinen Bestimmungen des Übereinkommens zu präzisieren, um sie der Erhebung und der Verarbeitung von personenbezogenen Daten durch Netzbetreiber und jede weitere Person, die Fernmeldedienste anbietet, anzupassen.

In der Feststellung des weiteren, dass bei den neuen Entwicklungen bei den Fernmeldediensten der Achtung des Privatlebens und des Briefverkehrsgeheimnisses wie in Artikel 8 der Europäischen Menschenrechtskonvention garantiert, unterworfen sind;

Empfiehlt den Mitgliedstaaten:

- im innerstaatlichen Recht und in der innerstaatlichen Praxis die Grundsätze zu berücksichtigen, die im Anhang zu dieser Empfehlung aufgeführt sind;

- jede Behörde, die bei der Umsetzung einer nationalen Datenschutz- und Fernmeldeverkehrspolitik mitwirkt, auf diese Empfehlung aufmerksam zu machen;
- sich zu vergewissern, dass die Netzbetreiber, die Anbieter von Fernmeldediensten, die Hersteller von Hardware- und Software, die Unternehmen, welche den Fernmeldeverkehr für Zwecke der Direktwerbung benützen, sowie die Organe, welche sie vertreten, und die Konsumentenorganisationen auf die Bestimmungen dieser Empfehlung aufmerksam gemacht wurden;

- die Bestimmungen dieser Empfehlung innerhalb der verschiedenen internationalen Fernmeldeorgane zu fördern;

Anhang zur Empfehlung Nr. R (95) 4

1. *Anwendungsbereich und Definitionen*

1.1. Die Grundsätze in dieser Empfehlung sind auf die Netzbetreiber und Diensteanbieter anwendbar, die in ihrer Tätigkeit personenbezogene Daten erheben und verarbeiten.

1.2. Diese Grundsätze sind auf personenbezogene Daten anwendbar, die automatisiert verarbeitet werden.

Die Mitgliedstaaten können die in dieser Empfehlung erwähnten Grundsätze auf personenbezogene Daten, die manuell verarbeitet werden, erweitern.

1.3. Die Mitgliedstaaten können die in dieser Empfehlung erwähnten Grundsätze auf die Erhebung und die Verarbeitung von personenbezogenen Daten juristischer Personen erweitern.

1.4. Im Sinne dieser Empfehlung bedeuten die Ausdrücke:

- "personenbezogene Daten": jede Information über eine bestimmte oder bestimmbare natürliche Person (betroffene Person); eine natürliche Person gilt nicht als "bestimmbar", wenn die Feststellung ihrer Identität einen unverhältnismässig hohen Aufwand an Zeit und Arbeitskraft erfordert;

- "Fernmeldedienste": die verschiedenen angebotenen Dienstleistungen mittels Fernmeldenetzen, welche den Benützern ermöglichen, miteinander zu kommunizieren oder mündlich, schriftlich, über Bild oder Datenübermittlung zu korrespondieren;

- "Netzbetreiber": jede öffentliche oder private Stelle, welche die Benutzung eines Fernmeldenetzes verfügbar macht;

- "Diensteanbieter": jede öffentliche oder private Stelle, die unter Verwendung eines von einem Netzbetreiber zur Verfügung gestellten Netzes oder ihres eigenen Netzes Fernmeldedienste anbietet und verwaltet.

2. *Achtung der Privatsphäre*

2.1. Die Fernmeldedienste und insbesondere die in Entwicklung befindlichen Telefondienste sollen unter Achtung der Privatsphäre der Benützer, des Briefsgeheimnisses und der Kommunikationsfreiheit angeboten werden.

2.2. Die Netzbetreiber und die Diensteanbieter sowie die Anbieter von Hardware- und Software sollen die Informationstechnologie dahingehend nutzen, Netze, Hardware und Software herzustellen und zu betreiben, die eine Wahrung der Privatsphäre der Benützer gewährleisten.

Es sollen anonyme Systeme für den Zugang zu Fernmeldenetzen und -diensten zur Verfügung gestellt werden.

2.3. Sofern dazu keine Bewiligung aus Gründen der technischen Speicherung oder Übermittlung, anderen rechtmässigen Gründen oder zur Erfüllung eines Dienstleistungsvertrags mit einem Teilnehmer vorliegt, soll jede Einmischung in den Inhalt der Mitteilung durch Netzbetreiber oder Diensteanbieter untersagt sein. Unter Vorbehalt des Grundsatzes 4.2. dürfen die den Inhalt der Mitteilung betreffenden Daten, die bei einer solchen Einmischung erhoben werden, nicht an Dritte weitergegeben werden.

2.4. Die Einmischung der öffentlichen Behörden in den Inhalt einer Mitteilung, einschliesslich die Verwendung von Mithör- und Aufzeichnungseinrichtungen oder anderer Überwachung- oder Abhörvorrichtungen ist nur zulässig, wenn dies durch Gesetz vorgesehen ist und eine in einer demokratischen Gesellschaft notwendige Massnahme ist:

a. zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit, der Währungsinteressen des Staates oder zur Bekämpfung von Straftaten;

b. zum Schutz der betroffenen Person und der Rechte und Freiheiten Dritter.

2.5. Im Falle der Einmischung öffentlicher Behörden in den Inhalt einer Mitteilung sollen im innerstaatlichen Recht festgelegt werden:

a. die Ausübung der Auskunfts- und Berichtigungsrechte durch die betroffene Person;

b. die Voraussetzungen, unter denen die zuständigen öffentlichen Behörden be-

rechtigt sind, der betroffenen Person Auskünfte zu verweigern oder die Erteilung dieser Auskünfte aufzuschieben;

c. die Aufbewahrung oder die Vernichtung dieser Daten.

Wenn ein Netzbetreiber oder Diensteanbieter von einer öffentlichen Behörde mit einer Einmischung beauftragt ist, so dürfen die so erhobenen Daten nur der in der Genehmigung für diese Einmischung bezeichneten Stelle mitgeteilt werden.

2.6. Das innerstaatliche Recht soll die Voraussetzungen und Garantien festlegen, unter denen die Netzbetreiber berechtigt sind, technische Mittel zur Lokalisierung von böswilligen oder missbräuchlichen Anrufen einzusetzen.

3. *Erhebung und Verarbeitung von Daten*

3.1 Die Erhebung und Verarbeitung personenbezogener Daten im Bereich des Fernmeldeverkehrs soll im Rahmen einer Datenschutzpolitik vorgenommen und entwickelt werden und die Bestimmungen des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, insbesondere den Grundsatz der Zweckbindung, berücksichtigen.

Unbeschadet anderer in dieser Empfehlung vorgesehenen Zwecken sollen die personenbezogenen Daten von den Netzbetreibern und den Diensteanbietern nur zu Zwecken des Netzanschlusses und der Zurverfügungstellung eines bestimmten Fernmeldedienstes, zu Rechnungszwecken und zur Zahlungsüberprüfung sowie zur Sicherstellung der optimalen technischen Umsetzung und der Entwicklung des Netzes und des Dienstes erhoben und verarbeitet werden.

3.2. Die Netzbetreiber und die Diensteanbieter sollen die Abonnenten der Fernmeldedienste in geeigneter Form über die Kategorien der sie betreffenden erhobenen und verarbeiteten personenbezogenen Daten, über die rechtliche Grundlage der Erhebung, über die Zweckbestimmung der Erhebung und der Bearbeitung sowie über die Verwendung und Aufbewahrungsdauer informieren.

4. *Bekanntgabe der Daten*

4.1. Die personenbezogenen Daten, die von den Netzbetreibern oder den Diensteanbietern erhoben und verarbeitet werden, sollen nicht bekanntgegeben werden, oder ausser wenn der betroffene Abonnent schriftlich nach Belehrung seine ausdrückliche Zustimmung gegeben hat und die angerufenen Abonnenten nicht aufgrund der mitgeteilten Information bestimmbar sind.

Der Abonnent kann seine Zustimmung jederzeit, jedoch nicht rückwirkend, widerrufen.

4.2. Die von den Netzbetreibern oder den Diensteanbietern erhobenen und verarbeiteten personenbezogenen Daten können den öffentlichen Behörden bekanntgegeben werden, wenn diese Bekanntgabe vom Gesetz vorgesehen ist und eine in einer demokratischen Gesellschaft notwendige Massnahme ist:

a. zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit, der Wäh-

rungsinteressen des Staates oder zur Bekämpfung von Straftaten;

b. zum Schutz der betroffenen Person und der Rechte und Freiheiten Dritter.

4.3. Im Falle der Bekanntgabe personenbezogener Daten an öffentliche Behörden soll das innerstaatliche Recht festlegen:

a. die Ausübung der Auskunfts- und Berichtigungsrechte durch die betroffene Person;

b. die Bedingungen, unter denen die zuständigen öffentlichen Behörden berechtigt sind, der betroffenen Person die Auskunft zu verweigern oder die Erteilung der Auskunft aufzuschieben;

c. die Aufbewahrung oder die Vernichtung dieser Daten.

4.4. Die Listen der Abonnenten, die personenbezogene Daten enthalten, können von den Netzbetreibern oder den Diensteanbietern nur an Drittpersonen bekanntgegeben werden, wenn eine der nachstehenden Bedingungen erfüllt ist:

a. der Abonnent hat schriftlich nach Belehrung seine ausdrückliche und klare Zustimmung gegeben; oder

b. der Abonnent hat, nachdem er über die vorgesehene Bekanntgabe informiert worden ist, keinen Einwand geäussert; oder

c. die mit dem Datenschutz beauftragte Behörde hat die Bekanntgabe bewilligt; oder

d. die Bekanntgabe ist im innerstaatlichen Recht vorgesehen.

Der Abonnent kann seine Zustimmung jederzeit aber nicht rückwirkend widerrufen

4.5. Die Bekanntgabe von personenbezogenen Daten unter Netzbetreibern und Diensteanbietern ist erlaubt, wenn diese Bekanntgabe zu Betriebs- und Rechnungszwecken erforderlich ist.

5. *Auskunfts- und Berichtigungsrechte*

5.1. Jeder Abonnent soll auf Gesuch und in verhältnismässigen Abständen, ohne übermässige Frist oder Kosten alle ihn betreffenden Daten, die von Netzbetreibern oder Diensteanbietern erhoben und verarbeitet werden, erhalten können und sie berichtigen oder löschen lassen, wenn sie unrichtig, nicht stichhaltig oder übermässig sind, oder wenn sie während einer unver-hältnismässig langen Zeit aufbewahrt wurden.

5.2. Das Eingehen auf gemäss Grundsatz 5.1. formulierte Gesuche kann verweigert, einge-schränkt oder aufgeschoben werden, wenn das Gesetz dies erlaubt und wenn dies in einer demokratischen Gesellschaft eine notwendige Massnahme ist:

a. zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit, der Wäh-

rungsinteressen des Staates oder zur Bekämpfung von Straftaten;

b. zum Schutz der betroffenen Person und der Rechte und Freiheiten Dritter.

6. *Sicherheit*

6.1. Die Netzbetreiber und die Diensteanbieter sollen alle geeigneten technischen und organisatorischen Massnahmen ergreifen, um die physische und logische Sicherheit des Netzes, der Dienste und der von ihnen erhobenen und verarbeiteten Daten sicherzustellen, und jede unerlaubte Einmischung und jedes unerlaubte Abfangen von Mitteilungen verhindern.

6.2. Die Abonnenten der Fernmeldedienste sollen über die Risiken der Verletzung der Netzsicherheit informiert werden sowie über die Art, wie sie diese Sicherheitsrisiken bei ihren Mitteilungen begrenzen können.

7. *Anwendung der Grundsätze*

a. Verzeichnisse

7.1. Die Abonnenten sollen kostenlos und ohne Begründung das Recht haben, abzulehnen, dass ihre personenbezogenen Daten in einem Verzeichnis aufgeführt werden.

Wenn jedoch das innerstaatliche Recht fordert, dass bestimmte Daten in einem Verzeichnis enthalten sind, soll der Abonnent seine Daten mit Begründung ausschliessen können.

Wenn das innerstaatliche Recht von einem Abonnenten eine Zahlung fordert, damit seine Daten nicht in einem Verzeichnis erscheinen, soll diese Zahlung einen angemessenen Betrag darstellen und in keinem Fall vom Gebrauch dieses Rechts abhalten.

7.2. Wenn ein Abonnent möchte, dass die Mitbenützer seines Endgerätes in einem Verzeichnis eingetragen sind, soll er vorgängig deren Zustimmung erhalten haben.

7.3. Unter Vorbehalt von Fällen, in denen der Abonnent zusätzliche ihn betreffende Daten im Eintrag wünscht, sollen die personenbezogenen Daten, die im Verzeichnis aufgeführt werden, auf die zur angemessenen Festlegung eines einzelnen Abonnenten und zur Begrenzung von Verwechslungen zwischen oder unter verschiedenen im Verzeichnis aufgenommenen Abonnenten notwendigen Daten begrenzt werden.

7.4. Bei der Einsicht in ein elektronisches Teilnehmerverzeichnis sollen technische Mittel geschaffen werden, um Missbräuchen, insbesondere dem unerlaubten Fernladen, vorzubeugen.

Das Zusammenstellen von in einem elektronischen Teilnehmerverzeichnis enthaltenen Daten mit anderen Daten oder anderen Datensammlungen soll verboten sein, ausser wenn das innerstaatliche Recht dies erlaubt oder wenn es für die Netzbetreiber oder die Diensteanbieter zu Betriebszwecken notwendig ist.

7.5. Die in einem Verzeichnis enthaltenen Daten können von den Netzbetreibern oder den Diensteanbietern zu Zwecken der Verwaltung eines Auskunftsdienstes für punktuelle Anfragen verwendet werden. Alle Auskünfte sollen auf die Bekanntgabe von im Verzeichnis enthaltenen Daten beschränkt werden. Es sollen Massnahmen zur Bekämpfung von Missbräuchen getroffen werden. Der Auskunftsdienst soll keine Information über Abonnenten erteilen, die nicht im Verzeichnis eingetragen sind, ausser mit deren schriftlich nach Belehrung gegebener Zustimmung.

7.6. Die Verwendung von im Verzeichnis eingetragenen Daten ist zudem durch die betreffenden Grundsätze der Empfehlung Nr. R (91) 10 über die Übermittlung der von öffentlichen Stellen gespeicherten personenbezogenen Daten an Dritte geregelt.

b. Verwendung der Daten für Zwecke der Direktwerbung

7.7. Die Grundsätze der Empfehlung Nr. R (85) 20 zum Schutz personenbezogener Daten bei der Verwendung für Zwecke der Direktwerbung sind auf die Verwendung von Abonnentendaten für Zwecke der Direktwerbung durch Dritte anwendbar.

7.8. Das innerstaatliche Recht soll geeignete Garantien aufstellen und die Bedingungen festlegen, unter denen die Abonnentendaten von Netzbetreibern, Diensteanbietern und Dritten für Zwecke der Direktwerbung mittels Telefon oder anderer Telekommunikationsmittel verwendet werden dürfen.

7.9. Die Erarbeitung von Verhaltenskodizes soll gefördert werden, um sicherzustellen, dass die verwendete Praxis den Abonnenten keine Unannehmlichkeiten bereitet. Insbesondere sollen das innerstaatliche Recht oder die Verhaltenskodizes die Zeit, in der Telefonwerbung betrieben werden kann, die Natur der Meldungen und die Art ihrer Übermittlung behandeln.

7.10. Die Direktwerbung mittels Telefon oder anderer Telekommunikationsmittel kann gegenüber keinem Abonnenten ausgeübt werden, der den Wunsch geäussert hat, keine Werbemeldungen erhalten zu wollen. Zu diesem Zweck sollen geeignete Mittel zur Bestimmung der Abonnenten entwickelt werden, die keine Werbemeldungen am Telefon erhalten möchten.

7.11. Die automatischen Anrufbeantworter für die Übermittlung von vorregistrierten Werbemeldungen können nur an die Abonnenten übermittelt werden, die gegenüber den Anbietern dieser Dienste dazu nach Belehrung ihre ausdrückliche Zustimmung gegeben haben. Der Abonnent kann seine Zustimmung jederzeit widerrufen.

c. Detaillierte Rechnung

7.12. Die Netzbetreiber und die Diensteanbieter sollen die Rechnungen mit detaillierter Angabe der Nummern der angerufenen Abonnenten nur auf Gesuch eines Abonnenten zur Verfügung stellen. Es soll die Privatsphäre der Mitbenützer und der Sprechpartner geschützt werden.

7.13. Die für die Rechnungstellung notwendigen Daten sollen von den Netzbetreibern oder den Diensteanbietern nicht länger aufbewahrt werden, als es hinsichtlich

Zahlungsfristen unbedingt notwendig ist. Dabei bleibt zu berücksichtigen, dass Daten während einer angemessenen Zeit für den Fall von mit Rechnungen verbundenen Beschwerden aufbewahrt werden müssen oder dass gesetzliche Bestimmungen eine längere Aufbewahrung dieser Daten verlangen können.

d. Interne Fernsprechsysteme

7.14. Grundsätzlich sollen die Personen mit geeigneten Mitteln darüber informiert werden, dass die mit der Verwendung eines Telefons verbundenen Daten vom Inhaber der Linie erhoben und verarbeitet werden. Die Daten sollen unmittelbar nach der Begleichung der Rechnung gelöscht werden.

7.15. Die Grundsätze der Empfehlung Nr. R (89) 2 zum Schutz personenbezogener Daten für Beschäftigungszwecke sind auf die Verwendung durch Arbeitgeber von automatischen Teilnehmervermittlungsanlagen am Arbeitsplatz anwendbar.

e. Anzeige der Rufnummer des Anrufers

7.16. Die Einführung eines technischen Merkmals, das die Sichtbarmachung der Telefonnummer eines eingehenden Anrufs auf dem Endgerät des angerufenen Abonnenten ermöglicht, sollen alle Abonnenten darüber informiert werden, dass bestimmte Abonnenten über dieses Merkmal verfügen können und es deshalb möglich ist, dass ihre Telefonnummer dem angerufenen Abonnenten enthüllt wird.

Die Einführung dieses Merkmals soll für den anrufenden Abonnenten von der Möglichkeit begleitet sein, durch ein einfaches Mittel die Anzeige seiner Telefonnummer auf dem Endgerät des angerufenen Abonnenten zu unterdrücken.

7.17. Das innerstaatliche Recht soll die Bedingungen und Garantien festlegen, nach denen die Netzbetreiber berechtigt oder verpflichtet sind, die Entscheidung des Anrufenden, dass die Anzeige seiner Nummer auf dem Bildschirm des Angerufenen unterdrückt wird, zu übergehen.

f. Anrufumleitung

7.18. Es soll die Möglichkeit von Mechanismen geprüft werden, die es einem Drittabonnenten ermöglichen, im Falle von Uneinigkeit die Annulierung einer Anrufumleitung zu erlangen.

7.19. Sofern die Überwachung oder das Abhören von eingehenden und abgehenden Anrufen eines Abonnenten in Übereinstimmung mit den Bestimmungen des Grundsatzes 2.4. über das Abhören von Übermittlungen erlaubt ist, sollen die Überwachungs- und Abhörmassnahmen nicht alle beim Endgerät des Drittabonnenten eingehenden Anrufe betreffen, sondern lediglich diejenigen, die Gegenstand einer Umleitung sind.

g. Mobiltelefone

7.20. Was das Angebot und die Betreibung eines Mobiltelefondienstes betrifft, so sollen die Netzbetreiber und die Diensteanbieter die Abonnenten über die mit der Verwendung von Mobiltelefonnetzen verbundenen Risiken der Verletzung des

Briefverkehrsgeheimnisses informieren, besonders, wenn der Funk nicht verschlüsselt ist. Es sollen Mittel geschaffen werden, die es den Abonnenten von Mobiltelefondiensten ermöglichen, ihre Mitteilungen zu verschlüsseln, oder sonst gleichwertige Garantien bieten.

7.21. Es sollte beachtet werden, dass es zur Rechnungstellung für die Verwendung eines Mobiltelefons nicht erforderlich ist, Daten zu speichern, die eine allzu genaue Lokalisierung des Abonnenten oder der angerufenen Partei zum Zeitpunkt der Verwendung enthüllen.

Mustervertrag für die Sicherstellung eines gleichwertigen Datenschutzes im Rahmen des grenzüberschreitenden Datenverkehrs*

(Modellklauseln für die Einfügung in einen Standardvertrag)

gemeinsam erarbeitet von den folgenden Instanzen:

Europarat
Kommission der Europäischen Gemeinschaften
Internationale Handelskammer

Der Zedent und der Zessionar vereinbaren die Abtretung des Nutzungsrechts an Personendaten gegen die Entrichtung eines Betrags in Höhe von ....

Die Vereinbarung zwischen den Parteien untersteht den nachstehenden Bedingungen:

1. <u>Verpflichtung des Zedenten</u>

Der Zedent bestätigt und gewährleistet dem Zessionar, dass die Datenübertragung an den Zessionar rechtmässig ist und dass die Daten in Übereinstimmung mit dem innerstaatlichen Recht

a. in zulässiger und rechtmässiger Weise erhoben und bearbeitet wurden;

b. zu bestimmten, gesetzlich vorgesehenen Zwecken erfasst wurden und nicht in einer Weise verwendet werden, die sich nicht mit diesen Zwecken vereinbaren lässt;

c. für die Zwecke, zu denen sie abgetreten werden, angemessen, relevant und verhältnismässig sind;

d. genau sind und sich auf dem neuesten Stand befinden;

e. über eine Aufbewahrungsbewilligung für die Dauer von ... verfügen.

2. <u>Verpflichtungen des Zessionars</u>

Der Zessionar erklärt und gewährleistet seinerseits, die Daten nur in einer Weise zu nutzen, welche die Grundsätze in den Erklärungen und Garantien des Zedenten in allen Punkten respektiert, und auf jegliche Bearbeitung oder Nutzung der Daten zu verzichten, die im Widerspruch zum Vertrag steht. Zu diesem Zweck sagt der Zessionar zu, insbesondere die folgenden Verpflichtungen einzuhalten, wobei die nachstehende Aufzählung nicht abschliessend ist:

a. der Zessionar benutzt die Daten ausschliesslich zu den nachstehend aufgeführten Zwecken; alle anderen Zwecke sind ausgeschlossen: (*Aufzählung der*

*Der erläuternde Bericht zu diesem Mustervertrag kann in französischer oder englischer Sprache beim Sekretariat des Eidgenössischen Datenschutzbeauftragten bezogen werden.

zulässigen Zwecke);

b. der Zessionar verzichtet darauf, Personendaten zu bearbeiten, welche die Rassenzugehörigkeit, die politische Zugehörigkeit, die religiösen oder andere Überzeugungen, die Gesundheit, das Sexualleben oder das Strafregister betreffen, es sei denn, diese Bearbeitung werde durch dieselben Garantien geschützt, die auch kraft des innerstaatlichen Rechts des Zedenten zur Anwendung gelangt wären;

c. vorbehältlich allfälliger in seinem innerstaatlichen Recht vorgesehenen und ausdrücklich aufgeführten Verpflichtungen nutzt der Zessionar die Daten ausschliesslich zum eigenen Gebrauch und übermittelt sie weder unentgeltlich noch gegen ein Entgelt an andere natürliche oder juristische Personen;

d. der Zessionar berichtigt, löscht oder aktualisiert die Daten unverzüglich, sobald ihm der Zedent dahingehende Anweisungen erteilt. Der Zessionar verpflichtet sich insbesondere, die Gesamtheit oder einen Teil der Daten zu berichtigen, zu ergänzen oder zu löschen, falls sich diese Massnahmen aufgrund des im Staat des Zedenten geltenden Rechts oder aufgrund von neuen Umständen im Staat des Zedenten als erforderlich erweisen; der Zedent teilt dem Zessionar diese Umstände mit und begründet sie, sobald sie im Staat des Zedenten in die Gesetzgebung aufgenommen wurden.

Der Zessionar verpflichtet sich, den betroffenen Personen unter den gleichen Bedingungen, wie sie im innerstaatlichen Recht des Zedenten vorgesehen sind, das Recht auf Auskunft über ihre Daten sowie das Recht auf Berichtigung und Löschung dieser Daten zu gewähren.

Falls der Zessionar den betroffenen Personen das Recht auf Auskunft über ihre Daten oder die von der betroffenen Person verlangte Berichtigung oder Löschung verweigert, wird der Zedent:

- den Vertrag gemäss den Bedingungen und mit den in Klausel 5 vorgesehenen Folgen auflösen, oder

- das Verfahren zur Bestimmung eines Schiedsrichters einleiten, das in Klausel 4 vorgesehen ist.

3. <u>Haftung und Entschädigung</u>

Der Zessionar haftet für die Nutzung der Daten, die durch den Zedenten übermittelt wurden.

Der Zessionar verpflichtet sich, den Zedenten für jede Nichterfüllung seiner Verpflichtungen aus dem vorliegenden Vertrag sowie für jedes Verschulden und jede offenkundige Fahrlässigkeit im Zusammenhang mit der Erfüllung des Vertrags zu entschädigen.

4. <u>Beilegung von Streitigkeiten</u>

Auszüge aus dem erläuternden Bericht:

37. Die Parteien eines Mustervertrags oder eines Vertrags mit Modellklauseln müssen ein geeignetes System für die Beilegung der Streitigkeiten vorsehen, die aus der Erfüllung des Mustervertrags oder der Modellklauseln entstehen können.

Sie können ihre Streitigkeiten einem Schiedsgericht oder einem Sachverständigen vorlegen.

38. Falls die Vertragsparteien beschliessen, sich für die Beilegung ihrer Streitigkeiten an ein Schiedsgericht zu wenden, können sie sich auf die Schiedsregeln der CNUDCI oder der ICC beziehen und die Modellregeln dieser Organisationen anwenden.

Schiedsklausel (CNUDCI):
"Alle Rechtsstreitigkeiten, Meinungsverschiedenheiten oder Beanstandungen, die aus dem vorliegenden Vertrag entstehen oder die im Zusammenhang mit dem Vertrag oder mit einer Verletzung, der Auflösung oder der Nichtigkeit des Vertrags stehen, werden durch ein Schiedsgericht gemäss dem zur Zeit geltenden Schiedsreglement der CNUDCI entschieden."

Schiedsklausel (ICC):
"Alle Rechtsstreitigkeiten aus dem vorliegenden Vertrag werden gemäss dem Schlichtungs- und Schiedsreglement der Internationalen Handelskammer endgültig durch einen oder mehrere Schiedsrichter entschieden, die in Übereinstimmung mit diesem Reglement ernannt werden."

Es empfiehlt sich, diese Schiedsklausel-Modelle mit zusätzlichen Elementen zu ergänzen:

- *der im Schiedsverfahren verwendeten Sprache*
- *dem Ort des Schiedsverfahrens*
- *der Zahl der Schiedsrichter.*

Falls der Vertrag jedoch nur den grenzüberschreitenden Datenverkehr zum Inhalt hat, können die Parteien für die Bestimmung der Schiedsrichter das nachstehende Verfahren festlegen:

"Jede Vertragspartei ernennt einen Schiedsrichter, welche ihrerseits gemeinsam einen dritten Schiedsrichter aus einer Liste von Personen auswählen, die vom beratenden Ausschuss des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten erstellt wurde[*]*. Dieser dritte Schiedsrichter führt den Vorsitz des Schiedsgerichts. Falls sich die von den Vertragsparteien ernannten Schiedsrichter nicht innerhalb von dreissig Tagen über die Ernennung des dritten Schiedsrichters einigen können, wird dieser von der ICC (oder von der Ernennungsinstanz, welche die Vertragsparteien für das Schiedsverfahren gewählt haben) in Übereinstimmung mit ihren Schiedsregeln bestimmt."*

Gegebenenfalls kann diese Klausel auch in gemischten Verträgen benutzt werden.

39. Falls der Vertrag Klauseln über den grenzüberschreitenden Datenverkehr enthält, sich jedoch nicht auf diesen Gegenstand beschränkt, können die Ver-

[*] Die Liste der Schiedsrichter kann beim Sekretariat des Europarats bezogen werden.

tragsparteien während des Hauptverfahrens vor dem Schiedsgericht für diesen Bereich einen Sachverständigen hinzuziehen.

Für diesen Fall können die Vertragsparteien vorsehen, dass der zu bestimmende Sachverständige aus einer Liste ausgewählt wird, die vom beratenden Ausschuss des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten erstellt wurde. Dieser Sachverständige erstellt ein Gutachen zuhanden des Schiedsgerichts.

5. Auflösung des Vertrags

Falls der Zessionar bei der Erfüllung des Vertrags gegen Treu und Glauben verstösst oder falls er sich insbesondere weigert, sich dem Entscheid der Schiedsrichter zu beugen, behält sich der Zedent das Recht vor, den Vertrag - unbeschadet einer allfälligen Schadenersatzforderung - per eingeschriebenen Brief mit Empfangsbestätigung oder durch ein anderes, gleichwertiges Mittel aufzulösen.

Im Zeitpunkt der Auflösung des Vertrags löscht der Zessionar die Daten endgültig und teilt dies dem Zedenten mit.

Bei Nichtbeachtung dieser Klausel verpflichtet sich der Zessionar zur Bezahlung eines Betrags in Höhe von ... an den Zedenten.

Anwendbares Recht (Auszug aus dem erläuternden Bericht)

25. Den Vertragsparteien steht es frei, das auf den Vertrag zwischen dem Zedenten und dem Zessionar anwendbare Recht zu bestimmen. Sie sollten in jedem Fall ausdrücklich angeben, welches Recht sie gewählt haben. Falls das anwendbare innerstaatliche Recht einen besseren Schutz der Personendaten sicherstellt, wird dem Zedenent empfohlen, zu überprüfen, ob die Klauseln entsprechend ergänzt werden müssen.