Eidgenössischer Datenschutzbeauftragter

Préposé fédéral à la protection des données

1. Tätigkeitsbericht 1993/94

1er Rapport d'activités 1993/94

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

Eidgenössischer Datenschutzbeauftragter

Tätigkeitsbericht 1993/94

Der Eidgenössische Datenschutzbeauftragte hat dem Bundesrat periodisch einen Bericht über seine Tätigkeit vorzulegen (Art. 30 Datenschutzgesetz). Der vorliegende Bericht deckt den Zeitraum zwischen 1. Juli 1993 und 31. März 1994 ab.

INHALTSVERZEICHNIS

*: Originalversion auf Französisch

*: Originalversion auf Französisch

ABKÜRZUNGSVERZEICHNIS

AFIS	Automatisches Fingerabdruck-Identifizierungssystem AFIS: Automatic Fingerprints Identification System
AGIS	Agrarpolitisches Informationssystem
AHV	Alters- und Hinterlassenenversicherung
AIDS	Acquired Immunodeficiency syndrom Erworbenes Abwehrswäche Syndrom
ANAG	Bundesgesetz über Aufenthalt und Niederlassung der Ausländer
AS	Amtliche Sammlung
ASTERIX	Automatisierter Strafregister-Index
AUDIT	Prüfverfahren
AUPER	Automatisiertes Personenregistratursystem
BAKOM	Bundesamt für Kommunikation
BBl	Bundesblatt
BFI	Bundesamt für Informatik
BStatG	Bundesstatistikgesetz
BUR	Betriebs- und Unternehmensregister
BV	Bundesverfassung
BVG	Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge
CJ-PD	Projektgruppe für den Datenschutz im Europarat
DNS	Desoxyribonukleinsäure
DOSIS	(Pilot) Provisorische Datenverarbeitung zur Bekämpfung des illegalen Drogenhandels
DSG	Datenschutzgesetz
EDI	Eidg. Departement des Innern
EDSB	Eidgenössischer Datenschutzbeauftragter
EDV	Elektronische Datenverarbeitung
EJPD	Eidg. Justiz- und Polizeidepartement
EPA	Eidg. Personalamt
FMH	(Foederatio Medicorum Helveticorum) Verbindung der Schweizer Ärzte
HIV	Immundefekt Aids HIV: Human Immunodeficiency Virus
IDK 95	Identitätskarte
ISDN	Dienstintegriertes digitales Netz
ISIS	Provisorische Staatsschutz-Informations-System
MOFIS	Motorfahrzeug-Informationssystem
OECD	Organisation für Zusammenarbeit und Entwicklung
OK	(Organisierte Kriminalität) Datenverarbeitung zur Bekämpfung des organisierten Verbrechens
OR	Obligationenrecht
PERIBU	Personalinformationssystem des Bundes
PIAS	Personalinformations- und administrationssystem des EJPD
PISA	Personalinformationssystem der Armee
PISEDI	Personalinformationssystem des EDI
REGI	Papierlose Personen- und Dossierverwaltung
RIPOL	Automatisierte Fahndungssystem
SEBA	Systeme zur elektronischen Berechnung der Arbeitszeit
SPO	Schweizerische Patienten Organisation
SR	Systematische Sammlung

StGB	Strafgesetzbuch
SUPIS	Sulzer Personalinformationssystem
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
VPB	Verwaltungspraxis der Bundesbehörden
VSKF	Verband Schweizerischer Kreditbanken und Finanzierungsinstitute
ZAN	Zentraler Aktennachweis des Schweizerischen Zentralpolizeibüros
ZAR	Zentrales Ausländerregister
ZEK	Zentralstelle für Kreditinformation

VORWORT

Das Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG) und die dazugehörigen Vollzugsbestimmungen sind am 1. Juli 1993 in Kraft getreten. Damit ist eine wesentliche Lücke in unserer Rechtsordnung geschlossen worden. Das neue Gesetz stellt eine Reihe von Datenbearbeitungsgrundsätzen auf, an welche sich alle Inhaber von Datensammlungen, für die das Gesetz Gültigkeit hat, zu halten haben.
Allein mit materiellen Grundsätzen ist jedoch der Datenschutz nicht zu gewährleisten, weil das Gesetz nicht für die ganze Vielfalt von Datenschutzproblemen der heutigen Zeit eine Antwort bieten kann. Für die Durchsetzung des Datenschutzes ist die Entwicklung eines datenschutzrechtlichen Bewusstseins der Gesellschaft von entscheidender Bedeutung. Den besten Schutz der Privatsphäre gewährleistet eine gut informierte Öffentlichkeit, die im Bewusstsein der Probleme in diesem Bereich ihre Rechte in ihrem eigenen Interesse wahrnehmen kann.

Der erste Tätigkeitsbericht des Eidgenössischen Datenschutzbeauftragten (EDSB) versucht, unter anderem auch zur Entwicklung dieses Datenschutzbewusstseins beizutragen, indem er über die Aktivitäten des EDSB während des ersten Tätigkeitsjahres berichtet.
In diesem ersten Tätigkeitsbericht werden einige Aspekte der datenschutzrechtlichen Situation im privaten Bereich sowie in der Bundesverwaltung in der Schweiz dargestellt. In der Absicht, die informationelle Selbstbestimmung der Bürgerinnen und Bürger zu schützen, wird über Positives sowie über Negatives berichtet. In unserer modernen, komplexen Gesellschaft ist das Recht der Bürgerinnen und Bürger auf Schutz ihrer Privatsphäre immer wieder gefährdet.
Obwohl wir zur Lösung verschiedener Probleme beigetragen haben, wird es auch in der Zukunft nicht ausbleiben, dass bei der Bearbeitung von Personendaten Missstände entstehen. Ebenso wird es immer wieder Stimmen geben, die nach weniger Datenschutz und nach mehr Eingriffskompetenzen für den Staat verlangen werden. Doch ist die zunehmende automatisierte Bearbeitung von Personendaten und die Vernetzung von EDV-Systemen nicht die einzige Lösung für alle Probleme unserer Gesellschaft. Die unverhältnismässige Bearbeitung von Personendaten birgt Risiken in sich, die für das soziale Umfeld nicht immer abzuschätzen sind.

Der Datenschutz trägt massgeblich zum Schutz der Privatsphäre der Bürgerinnen und Bürger bei. Wir sind uns bewusst, dass in der modernen Gesellschaft kein vollständiger Schutz der Persönlichkeit realisierbar ist. Wir werden uns aber immer dafür einsetzen, dass jede Person das Recht behält, mitzubestimmen zugunsten welcher anderen Rechte ihre Privatsphäre eingeschränkt werden kann. Denn das Recht der betroffenen Person auf informationelle Selbstbestimmung muss möglichst vollständig gewahrt werden. Dieses Recht sowie das Recht auf Schutz der Persönlichkeit bei Datenbearbeitung muss sowohl von den Bürgerinnen und Bürgern, als auch von den Behörden wahrgenommen werden. Der Schutz dieses Rechts liegt im Interesse aller, die mit Datenbearbeitungen zu tun haben und es ist erfreulich feststellen zu können, dass die Öffentlichkeit und die Bundesverwaltung mehrheitlich bereit sind, den Datenschutz zu gewährleisten.

Zur Zeit findet eine intensive Diskussion über Themen wie die innere Sicherheit, die Telefonabhörung, die neue Identitätskarte, die Forschung im Gentechnologiebereich statt - um nur einige Beispiele zu nennen - bei denen der Schutz von persönlichen Daten notwendig ist. Wir werden die Entwicklung in diesen Bereichen aufmerksam

mitverfolgen und versuchen, die anstehenden datenschutzrechtlichen Probleme in Zusammenarbeit mit den zuständigen Behörden zu lösen.

I. AUSGEWÄHLTE THEMEN

1. Polizeiwesen

1.1. 1994 "Jahr der inneren Sicherheit"; auch unter der Berücksichtigung des Datenschutzes?

Der in unserer heutigen Gesellschaft immer häufiger zu beobachtende und auf den technologischen Fortschritt zurückzuführende Rückgriff auf die Möglichkeiten der Datenverarbeitung erhöht die Risiken eines Eingriffs in den Persönlichkeitsbereich des Einzelnen auf alarmierende Weise. Besonders auffällig ist dieses Phänomen des "Datenbearbeitungsbooms" auf dem spezifischen Sektor der Polizei.

Obwohl sich diese Tendenz schon vor einigen Jahren abzeichnete, hat die Entwicklung dessen, was man "neue Mittel" der Polizei nennen kann, gerade in den Jahren 1993/94 einen ungeheuren Aufschwung erfahren. Zu erwähnen ist nicht nur die Einrichtung neuer automatisierter Systeme bei der Polizei, wie etwa die Inbetriebnahme des "Provisorischen Staatsschutz-Informations-Systems" (ISIS), sondern auch die Entwicklung einer ganzen Reihe von Informatik-Projekten für verschiedene Polizeibehörden, wie zum Beispiel die "Provisorische Datenverarbeitung zur Bekämpfung des illegalen Drogenhandels" (Pilotprojekt DOSIS), die Datenverarbeitung zur Bekämpfung des Organisierten Verbrechens (OK) oder die zentrale Datenbank in bezug auf die neue Identitätskarte (IDK 95).

Diese Tendenz des immer stärkeren Rückgriffs auf neue polizeiliche Mittel äussert sich nicht nur in der Erstellung von neuen Systemen, sondern auch in der Einrichtung einer immer *grösser werdenden Zahl an Direktverbindungen (online)*, die den Behörden einen unmittelbaren Zugang zu verschiedenen Systemen verschaffen. Wir können - um nur einige Beispiele zu geben - folgende Systeme nennen: das "Automatisierte Fahndungssystem" (RIPOL), das "Zentrale Ausländerregister" (ZAR), das "Automatisierte Personenregistratursystem" (AUPER), den "Automatisierten Strafregister-Index" (ASTERIX), das "Motorfahrzeug-Informationssystem" (MOFIS), den "Zentralen Aktennachweis des Schweizerischen Zentralpolizeibüros" (ZAN) oder das neue "Provisorische Staatsschutz-Informations-System" (ISIS). In diesem Zusammenhang verweisen wir auf den Abschnitt dieses Berichts, der den "neuen Gefahren" gewidmet ist und ein "Schema" enthält, das das Übermass an vorhandenen und möglichen Verbindungen illustriert.

Die Systeme, von denen wir oben einige aufgezählt haben, sind ausserdem manchmal miteinander *verbunden*. Als Beispiel für dieses Phänomen möchten wir auf den "Zentralen Aktennachweis" (ZAN) verweisen, der mit dem "Automatischen Fingerabdruck-Identifizierungssystem" (AFIS), den Informationen des INTERPOL-Dienstes und der künftigen "Provisorischen Datenverarbeitung zur Bekämpfung des illegalen Drogenhandels" (Pilotprojekt DOSIS) verbunden ist. Dazu ist das Zentrale Ausländerregister (ZAR) mit dem "Automatisierten Personenregistratursystem" (AUPER) und dem "Betriebs- und Unternehmensregister" (BUR) verbunden.

Hervorzuheben ist hier noch die Tatsache, dass - parallel zu diesem Phänomen der Expansion technologischer Hilfsmittel für die Polizei - *neue Gesetzestexte* entworfen werden. Diese dienen nicht nur dazu, Regelungen in bezug auf die automatisierten

Systeme der Polizei zu treffen, sondern auch zur Schaffung von Rechtsgrundlagen in bezug auf die innere Sicherheit, die Verbrechensbekämpfung oder die Einrichtung von Zentralstellen und die Beschäftigung von Verbindungsbeamten. Die Ausarbeitung von solchen Gesetzesnormen hat die immer grösser werdende Schwierigkeit aufgezeigt, die Interessen der Polizeibehörden mit den Grundsätzen des Datenschutzes zu vereinbaren. Die systematische Infragestellung des Auskunftsrechts ist ein gutes Beispiel für diese Problematik. Obwohl das Auskunftsrecht fester Bestandteil des Datenschutzgesetzes ist, wird es regelmässig beschnitten, wenn es etwa um die Bekämpfung des organisierten Verbrechens oder um die Erhaltung der inneren Sicherheit geht.

Die oben erwähnten Beispiele machen deutlich, wie sehr der Einsatz der technologischen Errungenschaften im Bereich des Polizeiwesens mit einem *erhöhten Risiko der Beschneidung der Grundrechte* und des Eingriffs in den Persönlichkeitsbereich der Bürgerinnen und Bürger einhergeht. Zusätzlich erhöht werden diese Risiken durch die Ausarbeitung von juristischen Normen, anhand derer eine immer stärkere Beschneidung der Rechte des Einzelnen leicht zu rechtfertigen ist. Im Rahmen eines speziellen Aktionsprogramms hat das Eidgenössische Justiz- und Polizeidepartement das Jahr 1994 zum "Jahr der inneren Sicherheit" erklärt. Es ist in diesem Zusammenhang allerdings darauf zu achten, dass der Aktionsplan nicht auf Kosten des Datenschutzes verwirklicht wird.

1.2. Schutz von polizeilichen Daten: Die "neuen" Gefahren!

Wir haben - entgegen einer weit verbreiteten falschen Vorstellung - schon mehrfach darauf hingewiesen, dass der Datenschutz keineswegs darauf abzielt, Kriminelle auf Kosten der Effizienz polizeilicher Tätigkeiten zu schützen. Der Datenschutz verfolgt das Ziel, einen klar umgrenzten gesetzlichen Rahmen zu schaffen, der die Bedingungen festlegt, unter denen Datenbearbeitungen getätigt werden müssen. Dieser gesetzliche Rahmen muss die Interessen der Polizeibehörden im Hinblick auf die Erfüllung ihrer Aufgaben einerseits und die Wahrung der Grundrechte sowie den Schutz des Persönlichkeitsbereichs der betroffenen Personen andererseits unter einen Hut bringen. Angesichts der Tatsache, dass die technologischen Fortschritte auf dem Polizeisektor und das Aufkommen einer Reihe "neuer Gefahren" das Risiko des Eingriffs in die Persönlichkeitsrechte des Einzelnen erhöhen, haben wir ausdrücklich betont, dass die verschiedenen vorhandenen Interessen auf eine immer sorgfältigere Art und Weise gegeneinander abgewogen werden müssen. Die angesprochenen "neuen Gefahren" bestehen in erster Linie in der kontinuierlichen Ausdehnung der bestehenden Polizeisysteme, in der unbegründeten Schaffung von Rechtsgrundlagen, die alles rechtfertigen können und in der Einrichtung einer immer beeindruckenderen Anzahl an Direktverbindungen zum Netz (online), die einer grossen Zahl verschiedenartigster Behörden einen direkten Zugang zu den Datenbanken der Polizei verschafft. Wir haben schliesslich festgestellt, dass es für einen Bürger oder eine Bürgerin immer schwieriger wird, die echten Risiken und Gefahren zu erkennen, die mit der Schaffung von neuen automatisierten Polizeisystemen verbunden sind.

Schaffung von Rechtsgrundlagen, anhand derer alles gerechtfertigt werden kann und gefährliche Überhandnahme von Direktverbindungen zum System (online): das Beispiel der schematischen Darstellung von bestimmten automatisierten Polizeisystemen.

Das Bundesgesetz über den Datenschutz sieht vor, dass die Bundesorgane Personendaten nur bei Vorhandensein einer entsprechenden Rechtsgrundlage bearbeiten dürfen. Es sagt auch, dass ein Bundesorgan Personendaten durch ein Abrufverfahren (online) nur zugänglich machen darf, wenn dies ausdrücklich vorgesehen ist; ausserdem muss ein formelles Gesetz vorhanden sein, um über eine Direktverbindung Zugang zu besonders schützenswerten Daten und Persönlichkeitsprofilen erhalten zu können.
Wir waren gezwungen, mehrfach darauf hinzuweisen, dass diese Bedingungen in bezug auf jede Bearbeitung von Personendaten respektiert werden müssen. Wir mussten auch mitansehen, wie bestimmte Organe versuchten, von ihnen gewünschte Datenbearbeitungen durch die Schaffung von entsprechenden Rechtsgrundlagen abzusichern. Ausserdem hat der bei zahlreichen Behörden zu beobachtende Drang nach Zugang zu immer mehr Informationssystemen insbesondere zur Folge, dass das Risiko, die Zweckdienlichkeit vieler Systeme zu unterhöhlen, immer grösser wird. Dies ist gerade auf dem spezifischen Gebiet des Polizeiwesens gefährlich, da dort "heikle" Daten bearbeitet werden.

In diesem Zusammenhang haben wir die zuständigen Bundesorgane auf die Tatsache aufmerksam gemacht, dass mit der Befolgung des Grundsatzes der Rechtmässigkeit in erster Linie Transparenz hergestellt werden soll und dass er selbst nicht genügt, um eine Bearbeitung von Personendaten zu legitimieren. Bevor man eine Direktverbindung (online) einrichtet, muss gründlich geprüft werden, ob sie überhaupt nötig ist und ob sie mit den Grundsätzen der Verhältnismässigkeit und der Zweckmässigkeit vereinbar ist. Mit anderen Worten dürfen Datenbearbeitungen und Zugänge zum System nicht nur in gesetzlichen Bestimmungen vorgesehen sein. Sie müssen auch mit den allgemeinen Grundsätzen des Gesetzes über den Datenschutz übereinstimmen. Angesichts des gewaltigen Ausmasses an Direktverbindungen (online) und der Gefahren, die diese mit sich bringen, müssen wir bei der Überprüfung eines Antrags auf Zugang zu einem bestimmten System jeweils darauf achten, dass die gewünschte Verbindung mit den allgemeinen Grundsätzen des DSG vereinbar ist, und dies, bevor die Rechtsgrundlage, die einen solchen Zugang gestattet, ausgearbeitet oder genehmigt wird.

Um die hier angeschnittene Problematik auch anschaulich zu machen, haben wir *ein Schema* entworfen, das für einige der Öffentlichkeit relativ bekannte Informationsysteme der Polizei, die bereits in Betrieb sind oder noch entwickelt werden, repräsentativ ist. Das Schema zeigt das Ausmass an Direktverbindungen (online) auf, die bereits bestehen oder zugunsten von zahlreichen Behörden ins Auge gefasst werden. In diesem Schema ist nur ein kleiner Abschnitt dessen abgebildet, was in der Bundesverwaltung an Systemen tatsächlich vorhanden ist. Diese Anmerkung ist wichtig, denn trotz seiner beeindruckender Wirkung gibt dieses Schema wie gesagt nur "einen Wassertropfen im Informatik-Meer des Bundes" wieder.

Zwei Bemerkungen:

- Die in diesem Schema aufgezeichneten Verbindungen stellen nicht allesamt Direktverbindungen (online) zu sämtlichen Daten eines Systems dar. Viele Verbindungen gewähren - gemäss der entsprechenden Zugangsmatrix - lediglich zu einem Teil der Daten eines Systems Zugang.

- Dieses Schema enthält einige Systeme, welche noch nicht im Betrieb genommen wurden. Alle dargestellten Verbindungen sind indessen einerseits effektiv oder mit entsprechender Zustimmung gemäss den gültigen Gesetzen oder Verordnungen möglich. Andererseits sind einige in verschiedenen publizierten Gesetzesentwürfen vorgesehen (Botschaft des Bundesrates, offenes Ämterkonsultationsverfahren).

Die wahren Risiken und Gefahren, die mit der Schaffung eines neuen Informatiksystems der Polizei verbunden sind: das Beispiel der neuen Identitätskarte (IDK 95)

Im Rahmen seines Vorhabens, eine neue Schweizer Identitätskarte (IDK 95) in Umlauf zu bringen, hat das Bundesamt für Polizeiwesen Anfang des Jahres einen Verordnungsentwurf des Bundesrates zur Ämterkonsultation vorgelegt. In der Verordnung soll nicht nur das Herausgabeverfahren der neuen Identitätskarte geregelt werden; es sollen darin auch die Bedingungen in bezug auf die Bearbeitung der zu diesem Zweck gesammelten Personendaten sehr genau festgelegt werden. Man hat sich in der Entwicklungsphase des Projekts an uns gewandt. Wir haben die Verantwortlichen des Projekts auf die von seiten des Datenschutzes gestellten Bedingungen aufmerksam gemacht, die unserer Ansicht nach in der Verordnung zur Identitätskarte verankert werden sollten. Daraufhin wurde ausdrücklich festgelegt, welche Daten für das Antragsformular gesammelt werden dürfen, welche Daten auf der Identitätskarte festgehalten werden sollen und welche Daten in der durch das Bundesamt für Polizeiwesen verwalteten zentralen Datenbank in Bern zu registrieren sind. Wir haben ausserdem verlangt, dass genau vorgeschrieben wird, durch wessen "Hände" diese Personendaten gehen dürfen (ausstellende Behörde, Hersteller der Karte und Bundesamt für Polizeiwesen). Der Verordnungstext legt im übrigen die von Stelle zu Stelle unterschiedliche Dauer der Datenaufbewahrung fest: sieben Tage bei der Herstellerfirma, zwei Monate bei der ausstellenden Behörde und maximal fünfzehn Jahre in der zentralen Datenbank.

Bei der Überprüfung des Konzepts IDK 95 haben wir ausdrücklich darauf bestanden, dass keine "versteckten" Daten in die Karte eingetragen werden dürfen. Das heisst, dass alle Informationen durch den Karteninhaber lesbar sein müssen und dass die Karte folglich weder Magnetband noch Mikrochips enthalten darf. Diese Forderungen wurden erfüllt. Natürlich sieht das Konzept des Bundesamts für Polizeiwesen die Eintragung von maschinenlesbaren Informationen (MRIDs - Machine Readable Identification Documents) unter der Norm ICAO 9303 (International Civil Aviation Organization) vor. Der "maschinenlesbare Code" wurde von den Verantwortlichen des Projekts als unentbehrliches Element eingeführt, das im Herstellungskonzept einer solchen Identitätskarte nicht fehlen darf. Aber da der besagte Code lediglich die Daten wiedergibt, die ohnehin schon auf der Karte eingetragen sind, ist er für den Karteninhaber ohne Probleme lesbar. Im Rahmen der Ämterkonsultation zur Verordnung bezüglich der Identitätskarte entstand bei den Personen, denen das Projekt zum ersten Mal vorgelegt wurde, grosse Verwirrung. Es wurden Ängste im Hinblick auf die Verwendung des maschinenlesbaren Codes geäussert. Man wies vor allem auf das Risiko hin, dass sich die Polizeibehörden und Zollbeamten mit Hilfe dieses Codes Zugang zum Automatisierten Fahndungssystem (RIPOL) oder zum Zentralen Ausländerregister (ZAR) verschaffen könnten. An dieser Stelle muss deshalb darauf hingewiesen werden, dass der maschinenlesbare Code gemäss der von den verantwortlichen des Projekts gelieferten technischen Informationen einzig und allein den Zweck erfüllt, den Grenzposten die Arbeit zu erleichtern. Dank dem Code, der mit Hilfe eines Leseapparats entschlüsselt werden kann, gelingt den Zollbeamten nämlich eine weitaus schnellere Erledigung ihrer Überwachungsaufgaben. Entgegen allen Befürchtungen räumt der maschinenlesbare Code aber keineswegs das Recht oder die Möglichkeit ein, sich Zugang zu der einen oder anderen Datenbank zu verschaffen. Der Code stellt nämlich in keiner Weise einen Schlüssel zum Eintritt in die verschiedenen Systeme dar. Die Zugänge zum RIPOL oder zum ZAR sind gesetzlich

geregelt. Die Behörden, die in bezug auf diese Systeme zugangsberechtigt sind, haben diese Befugnis demnach aufgrund gesetzlicher Bestimmungen und nicht über die Verwendung der neuen Identitätskarte.

Diese Klarstellungen ändern allerdings nichts an der Tatsache, dass bei der Verwendung dieses maschinenlesbaren Codes äusserste Vorsicht geboten ist. Aus diesem Grunde haben wir darauf bestanden, dass die Verwendung des Codes in der Verordnung klar und einschränkend festgelegt wird, und zwar unter Angabe der nutzungsberechtigten Behörden und unter Aufzählung sämtlicher Fälle, in denen ein Rückgriff auf diesen Code vertretbar ist. Dementsprechend wurde die Verwendung des Codes auf die für Grenzkontrollen zuständigen Behörden beschränkt. Allerdings dürfen selbst diese Behörden nur in bestimmten, genau definierten Situationen auf den Code zurückgreifen.

Die oben dargelegten Befürchtungen in bezug auf die Verwendung des maschinenlesbaren Codes machen deutlich, wie schwierig es ist, die mit der Einführung neuer technologischer Mittel verbundenen Gefahren zu erfassen. Wenn die Verwendung des Codes auch überwacht und klar geregelt werden muss, so gibt es in der Tat noch ein anderes Element, auf das wir hingewiesen haben. Es ist zwar der Öffentlichkeit weniger bekannt, aber deutlich gefährlicher: Zur Verwaltung der neuen Identitätskarten wird in Bern eine *zentrale Datenbank* in Betrieb genommen. In dieser werden alle Identitätsdaten sowie Foto und Unterschrift sämtlicher Identitätskarteninhaber registriert. Mit anderen Worten werden alle Schweizer Bürgerinnen und Bürger, die Inhaber einer Identitätskarte sind, in diesem vom Bundesamt für Polizeiwesen verwalteten Informationssystem registriert. Insofern ist es unbedingt notwendig, strikte Regelungen im Hinblick auf den Gebrauch dieser Datenbank zu treffen. In diesem Sinne haben wir darauf bestanden, dass die Verordnung des Bundesrates unmissverständlich vorschreibt, dass die Registrierung der Daten in diesem Informationssystem nur vorgenommen werden darf, um zu verhindern, dass sich ein und dieselbe Person mehrere Identitätskarten ausstellen lässt und um das Erneuerungsverfahren im Falle des Verlustes der Karte zu beschleunigen. Mit dem Ziel, die Wahrung des Grundsatzes der Zweckmässigkeit sicherzustellen, haben wir ausserdem empfohlen zu präzisieren, dass das Bundesamt für Polizeiwesen nur im Rahmen der Anwendung der Verordnung auf die Daten zurückgreifen darf und nicht etwa, um anderen gesetzlichen Aufgaben der Polizei nachzukommen. Das heisst also, dass die verschiedenen Dienststellen des Bundesamts für Polizeiwesen, wie etwa die Zentralstellen zur Bekämpfung des Drogenhandels, die Sektion RIPOL oder der INTERPOL-Dienst des Schweizerischen Zentralpolizeibüros kein Recht auf Zugang zu dieser Datenbank haben. Aus diesem Grunde wurde präzisiert, dass einzig und allein die dazu befugten Angestellten der Sektion Verwaltungspolizei des BAP, die ausdrücklich mit Verwaltungsaufgaben bezüglich der Identitätskarten und Pässe betraut sind, Zugang haben sollen.

Das Beispiel der neuen Identitätskarte macht auf sehr eindrückliche Weise deutlich, dass die Entwicklung und der Einsatz neuer technologischer Mittel vom Standpunkt der Persönlichkeitsrechte her eine Vielzahl von Gefahren mit sich bringen, von denen die schwerwiegendsten nicht immer auf den ersten Blick erkennbar sind. Insofern sind die zahlreichen Forderungen von seiten des Datenschutzes, die wir im Rahmen dieses Projekts geltend machen konnten, angesichts der Risiken, durch eine zentrale Registrierung aller Schweizer Bürgerinnen und Bürger, die Inhaber einer Identitätskarte sind, gegen die Grundrechte des Individuums zu verstossen, allemal gerecht-

fertigt. Wir hatten insofern Erfolg, als die vom Datenschutz gestellten Anforderungen in den vom Bundesamt für Polizeiwesen ausgearbeiteten Verordnungsentwurf aufgenommen wurden. Jetzt haben wir die Pflicht, darauf zu achten, dass diese Bedingungen auch tatsächlich strikt eingehalten werden. Doch dies reicht nicht aus. Wir müssen ausserdem darüber wachen, dass die datenschutzrechtliche Anforderungen vor allem nicht durch gesetzliche Anpassungen aufgrund neuer Zugangsanträge von seiten bestimmter Behörden abgeschwächt bzw. untergraben werden.

1.3. Bekämpfung des organisierten Verbrechens

Schaffung einer Zentralstelle zur Bekämpfung des organisierten Verbrechens

Wir haben mit einigen Bemerkungen zur Botschaft des Bundesrates vom 12. Januar 1994 bezüglich der Abänderung des Strafgesetzbuchs im Hinblick auf die Schaffung einer Zentralstelle zur Bekämpfung des organisierten Verbrechens Stellung bezogen. Die meisten unserer Bemerkungen, die auf eine strengere Wahrung der Persönlichkeitsrechte abzielten, wurden berücksichtigt. Die Schlussfassung des Projekts enthält allerdings noch zwei Punkte, die grundlegend von unseren Vorstellungen abweichen. Es handelt sich um die Beschränkungen des Auskunftsrechts und um die Einführung einer Generalklausel zur Entwicklung künftiger Informationssysteme "anderer Zentralstellen". Die Überprüfung dieser Punkte im Rahmen der Parlamentsdebatten gibt Gelegenheit, den Spielraum zu bemessen, der den Grundrechten der Bürgerinnen und Bürger angesichts der Ausarbeitung von juristischen Normen, anhand derer sich die immer stärkeren Beschränkungen der Individualrechte rechtfertigen lassen, noch verbleibt.

Seit letztem Jahr hat sich das politische Engagement zugunsten einer stärkeren Gesetzgebung im Hinblick auf eine wirksamere Bekämpfung der neuen Verbrechensformen, insbesondere der Wirtschaftskriminalität und der organisierten Kriminalität, ausserordentlich verstärkt.

Nach Verabschiedung eines ersten "Massnahmenpakets" gegen die organisierte Kriminalität (dieser bestand aus Strafnormen zur Geldwäscherei und zur mangelnden Sorgfalt bei Finanzgeschäften), wurde mit der Botschaft des Bundesrates vom 30. Juni 1993 zur Abänderung des Strafgesetzbuchs und des Militärstrafgesetzbuchs ein zweites "Massnahmenpaket" vorgelegt. Dieses betrifft vor allem das Melderecht des Financiers (Art. 305ter Abs. 2 StGB) und den Begriff der "kriminellen Organisation" (Art. 260ter StGB). Unter demselben Gesichtspunkt wurde am 12. Januar 1994 eine neue Botschaft vom Bundesrat verabschiedet. Sie nimmt auf die Schaffung einer Zentralstelle zur Bekämpfung des organisierten Verbrechens Bezug.

Das Projekt zur Schaffung einer Zentralstelle zur Bekämpfung des organisierten Verbrechens stellt im Grunde genommen eine Reihe von spezifischen Bestimmungen in bezug auf die Datenbearbeitungen bei der Polizei dar. Die einzelnen vorgeschlagenen Strafnormen enthalten unter anderem Bestimmungen in bezug auf die Aufgabe der Zentralstelle, welche vor allem in der Bearbeitung von Informationen über die nationalen und internationalen Verflechtungen von kriminellen Organisationen besteht. Ausserdem legen sie verschiedene andere Punkte fest, wie etwa die Kompetenzen der Verbindungsbeamten, die Informationspflicht bestimmter Behörden, die Bekanntgabe- und Auskunftsbedingungen in bezug auf Daten aus anderen Dienststellen, die Informationsermittlung und -sammlung, die Bearbeitung von

Personendaten, die Einrichtung eines Informationssystems zur Nutzung sachdienlicher Hinweise im Rahmen der Bekämpfung des organisierten Verbrechens, die Bekanntgabe von Personendaten sowie die Ausübung des Auskunftsrechts.

Im Rahmen der Ämterkonsultation wurde das Projekt mehr als zwanzig betroffenen Stellen und Ämtern unterbreitet. Obwohl das Projekt datenschutzrechtliche Fragen aufwarf, hat man uns das Projekt zunächst nicht vorgelegt. Erst nachdem wir ausdrücklich beim Bundesamt für Polizeiwesen nachgehakt hatten, wurden uns die zur Anhörung freigegebenen Texte und die dazugehörige Botschaft zur Stellungnahme übergeben. Wir haben in unserer Stellungnahme vor allem in bezug auf folgende Punkte Vorbehalte angemeldet: Sammlung von Informationen ohne Wissen der betroffenen Personen, Online-Zugang zum Informationssystem durch die für den Schutz der inneren Sicherheit zuständigen Bundesorgane und Beschränkungen des Auskunftsrechts.

Einigen unserer Bemerkungen wurde Rechnung getragen. Dies äusserte sich in erster Linie in der Einführung eines im nachhinein geltend zu machenden Informationsrechts zuhanden der Person, über die ohne deren Wissen Daten gesammelt wurden, sowie in der Beschränkung des Online-Zugangs: die für die Wahrung der inneren Sicherheit zuständigen Bundesbehörden dürfen nur auf die in der Datenbank gespeicherten Kurzpersonalien Zugriff haben. Was allerdings nicht berücksichtigt wurde, waren unsere Bedenken im Zusammenhang mit der Beschneidung des Auskunftsrechts. Schlimmer noch ist allerdings die Tatsache, dass das dem Bundesrat zur Bewilligung vorgelegte überarbeitete Projekt durch eine neue Bestimmung ergänzt wurde, die es "anderen Zentralstellen" erlaubt, Datenverarbeitungssysteme zu unterhalten. Ausserdem hat man vorgegeben, dass wir unser Einverständnis zu diesem Projekt gegeben hätten. Unter Berufung auf die Bestimmungen des Bundesgesetzes über den Datenschutz und der dazugehörigen Verordnung haben wir dem Bundesrat einen Bericht zugesandt, um ihn auf die bei der Ämterkonsultation festgestellten Lücken und auf die im Dossier noch bestehenden materiellen Divergenzen aufmerksam zu machen. Trotz zahlreicher Sitzungen und trotz des wiederholten Austauschs von Vorschlägen, die unserer Intervention gefolgt waren, konnte keine Kompromisslösung zwischen uns und den verschiedenen Vertretern des Eidgenössischen Justiz- und Polizeidepartements gefunden werden.

Was das *Auskunftsrecht* im einzelnen anbelangt, so hat sich das EJPD für die Ausarbeitung eines neuen - weitaus restriktiveren - Reglements stark gemacht. Und dies trotz der durch das DSG ohnehin gebotenen Möglichkeiten, die Gewährung dieses Rechts zu verweigern, einzuschränken oder aufzuschieben. Nach diesem neuen Reglement muss sich die betroffene Person, die ihr Recht ausüben will, auf einen konkreten Sachverhalt beziehen und ein besonderes Interesse an der Auskunft darlegen; ausserdem darf die Beschneidung des Auskunftsrechts ohne Angabe von Gründen erfolgen. Letzteres können wir unter Umständen noch einsehen. Was wir allerdings nicht gutheissen können, sind die anderen zur Ausübung dieses Rechts gestellten zusätzlichen Bedingungen. Die den betroffenen Personen auferlegte Verpflichtung, ein besonderes Interesse geltend zu machen, ist im besonderen Fall der Bekämpfung des organisierten Verbrechens zur Not noch zu rechtfertigen, selbst wenn sie mit der Rechtsprechung des Bundesgerichts kollidiert. Danach heisst es nämlich ausdrücklich, dass der Person, die einigermassen glaubhaft vorgibt, dass die zu ihrer Person registrierten Daten einen Eingriff in ihre persönliche Freiheit ermöglichen, die Einsicht gewährt werden muss, ohne dass die Person verpflichtet ist, noch

ein anderes schutzwürdiges Interesse glaubhaft zu machen. Indem das Projekt auf das entsprechende Recht verweist, ist allerdings sichergestellt, dass jede Anfrage nach dem Interessenabwägungsprinzip und unter Berücksichtigung des Grundsatzes der Verhältnismässigkeit überprüft wird. Es ist in erster Linie die der betroffenen Person auferlegte Bedingung, sich auf einen konkreten Sachverhalt beziehen zu müssen, die unserer Ansicht nach nicht hingenommen werden darf. Diese Bedingung läuft - entgegen der menschlichen Würde - darauf hinaus, jeden Bürger zu zwingen, sich selbst bestimmter Tatbestände zu bezichtigen. Ausserdem ist es für den Bürger, der sich nichts vorzuwerfen hat und der nur sicherstellen möchte, dass er von der Polizei nicht missbräuchlich oder grundlos überwacht wird, in den meisten Fällen unmöglich, diese Bedingung zu erfüllen.

Die Bestimmung, welche "anderen Zentralstellen", die für die Bekämpfung bestimmter Gesetzesübertretungen zuständig sind, die Verwaltung eines Datenverarbeitungssystems gemäss den neuen Strafnormen zum organisierten Verbrechen gestattet, ist ebenfalls auf Kritik von unserer Seite gestossen: Abgesehen von der Tatsache, dass die Bestimmung ungenau ist, entspricht sie im Grunde einer Generalklausel für alle zukünftigen Datenbanken, die im Rahmen der Bekämpfung von noch nicht definierten Gesetzesübertretungen angelegt und von noch unbestimmten Zentralstellen verwaltet werden. Angesichts der Tatsache, dass die Zahl der neuen Informationssysteme zuhanden der Polizei ständig wächst und immer mehr Verbindungen aufgebaut werden, dank derer verschiedene Behörden Zugang zu diesen Systemen haben, kann eine solche Generalklausel nicht hingenommen werden. Sie steht den Bestimmungen des Gesetzes über den Datenschutz entgegen. Bevor ein System entwickelt wird, muss geprüft werden, ob dieses notwendig, zweckmässig und verhältnismässig ist. Ausserdem muss sich die Entwicklung eines Systems auf eine ihr angemessene Rechtsgrundlage stützen können. Dieses Prinzip wird unter anderem noch dadurch bekräftigt, dass die Bundeskammern eine Bestimmung in das DSG aufgenommen haben, die besagt, dass die verschiedenen Direktverbindungen (online), die Zugang zu besonders schützenswerten Daten gewähren - wie etwa zu den Daten in den Informationssystemen der Polizei -, durch ein formelles Gesetz ausdrücklich vorgesehen sein müssen. Das in der Botschaft vorgebrachte Argument, das die Schaffung der Generalklausel im Hinblick auf die endgültige Einrichtung der Datenbank DOSIS zur Bekämpfung des internationalen Drogenhandels zu rechtfertigen sucht, ist nicht treffend. Damit deren Online-Verbindungen ausdrücklich erwähnt werden können, muss spezifisch für diese Datenbank über den Drogenhandel unter allen Umständen und auf jeden Fall eine formelle Gesetzesnorm ausgearbeitet werden. Das Pilotprojekt DOSIS war in bezug auf diesen Punkt übrigens immer sehr klar, wenn man bedenkt, dass es für seine Endphase eine Abänderung von Art. 29 des Bundesgesetzes über die Betäubungsmittel vorgesehen hat.

Der Vorschlag zur Abänderung des Strafgesetzbuchs im Hinblick auf die Schaffung einer Zentralstelle zur Bekämpfung des organisierten Verbrechens wurde vom Bundesrat in seiner Sitzung vom 12. Januar 1994 genehmigt. Wir konnten bei der Lektüre der veröffentlichten Botschaft feststellen, dass einige unserer Forderungen verwirklicht wurden. Die beiden verbleibenden Divergenzen, die die Beschränkungen des Auskunftsrechts beziehungsweise die Einführung einer Generalklausel im Hinblick auf künftige Informationssysteme "anderer Zentralstellen" betreffen, wurden als solche in der Botschaft des Bundesrates nicht erwähnt. Dort heisst es kurz und knapp: "Die vorgeschlagene strenge Regelung beachtet die geltende Datenschutzgesetzgebung des Bundes; sie ist denn auch mit dem Eidgenössischen Daten-

schutzbeauftragten besprochen worden". Es besteht kein Zweifel, dass die Regelung im Rahmen von Parlamentssitzungen erneut debattiert wird. Insofern ist es angebracht, sich zu fragen, welchen Platz man den Grund- und Persönlichkeitsrechten der Bürgerinnen und Bürger einräumen will. Diese Frage ist angesichts der Ausarbeitung von juristischen Normen zur Rechtfertigung immer stärkerer Beschränkungen der Individualrechte durchaus berechtigt.

Das Pilotprojekt DOSIS

DOSIS stellt ein Pilotprojekt dar, das von den zuständigen Dienststellen des Eidgenössischen Justiz- und Polizeidepartements im Rahmen der Einrichtung einer zentralen Drogendatenbank ausgearbeitet wurde. Das System wird von der Zentralstelle des Bundesamtes für Polizeiwesen zur Bekämpfung des unerlaubten Betäubungsmittelverkehrs verwaltet. Sie hat hauptsächlich die Funktion, über eine Online-Verbindung die Zusammenarbeit mit den Betäubungsmitteldiensten der kantonalen Polizeikorps sicherzustellen. In seiner Sitzung vom 23. März 1994 hat der Bundesrat die Verordnung DOSIS verabschiedet. Die Verordnung wurde vom Bundesamt für Polizeiwesen in Zusammenarbeit mit uns ausgearbeitet. Sie enthält eine besondere Bestimmung zum Auskunftsrecht, die wir im Rahmen einer Anhörung zu einem ähnlichen Projekt als mit dem DSG "nicht vereinbar" bezeichnet hatten. Die Einführung einer solchen allgemeinen Beschränkung des Auskunftsrechts auf Verordnungsstufe verletzt die gesetzlichen Vorschriften des Datenschutzes. Dabei wurden diese in Form eines formellen Gesetzes vom Parlament verabschiedet.

Das Projekt wurde als prioritär eingestuft und nach einem Verwirklichungskonzept in drei Phasen ausgearbeitet. Die erste Phase, die man offiziell am 15. Januar 1993 in Angriff nahm und "interne Phase" nannte, wurde auf eine interne Bearbeitung innerhalb der Zentralstelle für Rauschgift beim Bundesamt für Polizeiwesen beschränkt, ohne mit den Kantonen in Verbindung zu treten: die Zusammenarbeit zwischen Bundes- und kantonalen Behörden, die für die Bekämpfung des Drogenhandels zuständig sind, wird noch heute durch Kantonsangestellte sichergestellt, die sich zu diesem Zweck nach Bern begeben. Für die zweite Phase ("externe Phase" genannt) ist der Aufbau von Online-Verbindungen einiger Kantone zum Informationssystem vorgesehen. Was die dritte Phase anbelangt, so ist sie der Inbetriebsetzung der endgültigen Drogendatenbank gewidmet, an die sämtliche Kantone angeschlossen werden sollen.

Die Dringlichkeit der Einrichtung einer Bundesdrogendatenbank und die Notwendigkeit, diese Datenbank auf der Basis konkreter Erfahrungen zu verankern, haben das Bundesamt für Polizeiwesen dazu bewogen, sich für eine Verwirklichung in mehreren Etappen mit einer externen Versuchsphase zu entscheiden. Seit Beginn der Ausarbeitung des DOSIS-Konzepts hat man sich an uns gewandt, und wir haben das Entwicklungsverfahren in drei Phasen gutgeheissen. Allerdings haben wir verlangt, dass in der zweiten Phase, die einen externen Versuch beinhaltete, nur acht klar festgelegten Kantonen eine Online-Verbindung zugeteilt würde. Im weiteren bestanden unsere Forderungen darin, die zweite Phase ausdrücklich zeitlich zu begrenzen, sie erst mit Inkrafttreten einer entsprechenden Verordnung beginnen zu lassen und sie unter Anwendung der im Bundesgesetz über den Datenschutz enthaltenen Bestimmungen durchzuziehen. Mit der letzten dieser Bedingungen soll insbesondere die Einhaltung der im DSG vorgesehenen Bestimmung zum Auskunftsrecht sichergestellt werden. Was die dritte Phase anbelangt, so haben wir darauf hingewiesen, dass sie gemäss DSG die Schaffung einer formellen Rechtsgrundlage erfordert, die

den Rückgriff auf Direktverbindungen durch die kantonalen Betäubungsmitteldienste der Polizeikorps ausdrücklich vorsieht. Man hat beschlossen, nach Auslaufen der Versuchsphase eine Abänderung des Art. 29 des Bundesgesetzes über die Betäubungsmittel auszuarbeiten, um die endgültige Datenbank gesetzlich verankern und die Online-Verbindungen zuhanden der kantonalen Betäubungsmitteldienste in den Polizeikorps aller Kantone festlegen zu können.

Die Arbeiten im Zusammenhang mit der Ausarbeitung des Verordnungsentwurfs DOSIS wurden vom Bundesamt für Polizeiwesen in Zusammenarbeit mit unserem Dienst ausgeführt. Die Verordnung legt unter anderem die mit dem Informationssystem DOSIS verfolgten Zielsetzungen fest. Ferner bestimmt bzw. regelt sie die Untersysteme, die Art der darin zu bearbeitenden Daten, die Benutzer des Systems und deren Zugriff, die Datenberarbeitung, die Datenerfassung und -qualitätskontrolle, die Datenbekanntgabe, die Dauer der Datenaufbewahrung und die Datenlöschung sowie die nötigen Sicherheitsmassnahmen.

Am Rande der Arbeiten im Zusammenhang mit der Ausarbeitung der Verordnung DOSIS hat uns das Bundesamt für Polizeiwesen gebeten, uns in bezug auf zwei Fragestellungen zu äussern, die von einigen an einer Teilnahme am Projekt interessierten Kantonen aufgeworfen wurden:

Die erste dieser Fragestellungen betrifft die Anwendung des Bundesgesetzes über den Datenschutz auf das System DOSIS. Sie konnte eindeutig beantwortet werden: DOSIS ist ein System des Bundes, das vom Bundesamt für Polizeiwesen in Zusammenarbeit mit den Kantonen verwaltet wird. Im Rahmen der externen Versuchsphase, für die Online-Verbindungen der Kantone vorgesehen sind, muss die Zentralstelle zur Bekämpfung des unerlaubten Betäubungsmittelverkehrs beim Bundesamt für Polizeiwesen die in das System DOSIS eingeführten Daten untersuchen, um sich zu vergewissern, dass sie mit den Zielsetzungen des Systems übereinstimmen. Ferner muss die Zentralstelle die provisorisch erfassten Daten überprüfen und deren definitive Registrierung im Rahmen eines Konzepts zur Kontrolle der Daten bestätigen. In dieser Hinsicht ist DOSIS in seiner Eigenschaft als System des Bundes also dem Bundesgesetz über den Datenschutz und folglich der Kontrolle des Eidgenössischen Datenschutzbeauftragten unterstellt. Der Kontrolle unterzogen wird allerdings nur das System DOSIS und nicht die Polizeiakten der Kantone. Die Kontrolle bewegt sich auch nur innerhalb der Grenzen, die uns durch das Bundesgesetz über den Datenschutz gesteckt sind. Der juristische Rahmen des Systems DOSIS und insbesondere die Anwendung des DSG wurde also für alle Projektteilnehmer deutlich festgesetzt. Die nachträgliche Entscheidung des Kantons Zürich, sich vom Pilotversuch DOSIS zurückzuziehen, hat technische Gründe. Sie hängt mit dem Projekt zusammen, deutet also nicht auf Datenschutzprobleme hin.

Der zweite von verschiedenen Kantonen hervorgehobene Punkt bezieht sich auf das Auskunftsrecht. Die Kantone haben in bezug auf die Bestimmungen des Bundesgesetzes über den Datenschutz Bedenken geäussert, die die Ausübung des Auskunftsrechts garantieren. Sie haben gefragt, inwieweit Massnahmen zur Ausschliessung oder wenigstens zur Beschränkung dieses Rechts ergriffen werden können. Diese Tendenz, die Ausübung des Auskunftsrechts in bezug auf Daten, die in den Datenbanken der Polizei registriert sind, zu begrenzen, greift immer stärker um sich. Sie wurde im Rahmen der Botschaft des Bundesrates bezüglich der Abänderung des Strafgesetzbuchs im Hinblick auf die Schaffung einer Zentralstelle zur Bekämpfung

des organisierten Verbrechens noch konkreter sichtbar. Hier heisst es: *"Im Hinblick auf die Frage des Einsichtsrechtes hat die Konferenz der kantonalen Justiz- und Polizeidirektoren in ihrer Stellungnahme vom 8. September 1993 gefordert, dass die blinde Anwendung des Datenschutzrechtes nicht zu einer Vereitelung der Strafverfolgung führen darf. Dieser Forderung wird mit dem Wortlaut von Artikel 351 quindecies StGB Rechnung getragen".*

Wir haben, was uns anbelangt, im Rahmen der Ausarbeitung der Verordnung DOSIS daran erinnert, dass das DSG nicht nur die Ausübung des Auskunftsrechts regelt, sondern dass es auch ausdrücklich Möglichkeiten zur Verweigerung, Beschränkung oder Aufschiebung der Ausübung dieses Rechts vorsieht. Im Zuge der Verabschiedung des DSG war sich das Parlament deutlich der Notwendigkeit bewusst gewesen, solche Ausnahmen vorzusehen, vor allem im Hinblick auf die Tätigkeiten der Polizei. Diese Bestimmungen zur Beschränkung der Ausübung des Auskunftsrechts kommen den Forderungen von seiten der Polizeibehörden insofern bereits entgegen. Das Pilotprojekt DOSIS in seiner externen Versuchsphase, die auf einer Verordnung des Bundesrates basiert, kann unter Einhaltung der im Bundesgesetz über den Datenschutz enthaltenen Bestimmungen zur Ausübung und Beschränkung des Auskunftsrechts also sehr wohl verwirklicht werden.

Jedoch hat man entgegen den oben dargestellten Überlegungen eine besondere Bestimmung zum Auskunftsrecht in die vom Bundesrat in seiner Sitzung vom 23. März 1994 verabschiedete Verordnung DOSIS aufgenommen. Diese Bestimmung sagt aus, dass "*Das Einsichts- und Auskunftsrecht im "DOSIS" wird bis zum Inkrafttreten der Änderung vom ... des Schweizerischen Strafgesetzbuches (Schaffung einer Zentralstelle zur Bekämpfung des Organisierten Verbrechens), längstens aber bis zum 31. Dezember 1995 aufgeschoben"*. In unserer Stellungnahme zum Entwurf einer gleichartigen Bestimmung, um die uns das Bundesamt für Polizeiwesen im Dezember 1993 gebeten hatte, erklärten wir diese Bestimmung noch als *"unvereinbar mit dem DSG*". Wir haben die Verantwortlichen des DOSIS-Projekts insbesondere auf die Tatsache aufmerksam gemacht, dass sie auf der Stufe einer Verordnung unmöglich eine allgemeine Beschränkung des Auskunftsrechts festlegen könnten. Bei dieser Gelegenheit haben wir daran erinnert, dass die Polizeibehörden nach dem gegenwärtigen Stand der Gesetzgebung und der Rechtsprechung des Bundesgerichts die Auskunft verweigern, einschränken oder aufschieben können, wenn einerseits ein formelles Gesetz es vorsieht oder Interessen Dritter es verlangen (Art. 9 Abs. 1 DSG), und andererseits aufgrund eines überwiegenden öffentlichen Interesses oder wenn das Risiko der Beeinträchtigung eines Ermittlungsverfahrens besteht. Zuerst aber müssen von Fall zu Fall die vorhandenen Interessen konkret gegeneinander abgewogen und der Grundsatz der Verhältnismässigkeit gewahrt werden (Art. 9 Abs. 2 DSG; BGE 113 1a 262).

Das Bundesamt für Polizeiwesen hat diese Ausnahmeregelung unter Berufung auf Artikel 9 Absatz 1 Ziffer a DSG für DOSIS beibehalten. Diese Bestimmung legt dabei ausdrücklich fest, dass es möglich ist, das Auskunftsrecht einzuschränken, soweit ein formelles Gesetz dies vorsieht. Dieser Artikel des DSG wurde von den Bundeskammern verabschiedet, um zu vermeiden, dass schwerwiegende Verstösse gegen die Grundrechte des Individuums ohne Zusimmung des Parlaments gestattet werden können. Die Aufnahme einer solchen allgemeinen Einschränkung des Auskunftsrechts auf der Stufe einer einfachen Bundesratsverordnung ist also offensichtlich mit

dem DSG *nicht vereinbar*. Sie *verletzt* die gesetzlichen Datenschutzvorschriften, die in Form eines formellen Gesetzes vom Parlament verabschiedet worden sind!

In diesem Zusammenhang ist es angebracht, auf die Ergebnisse der durch das Parlament vorgenommenen Überprüfung der Botschaft des Bundesrates bezüglich der Schaffung einer Zentralstelle zur Bekämpfung des organisierten Verbrechens einzugehen. Die Botschaft sieht die Aufnahme einer neuen Bestimmung zur Einschränkung des Auskunftsrechts in Fällen der organisierten Kriminalität vor, diesmal allerdings auf der Ebene eines Bundesgesetzes (im vorliegenden Fall des Strafgesetzbuchs) (vgl. Kommentar im Kapitel über die Schaffung einer Zentralstelle zur Bekämpfung der organisierten Kriminalität). Durch die Aufnahme einer Bestimmung über die künftigen automatisierten Systeme "anderer Zentralstellen" soll mit diesem Projekt ausserdem die endgültige Nutzung der Drogendatenbank DOSIS geregelt werden. In diesem Zusammenhang muss also darüber nachgedacht werden, welche Abänderungen man in bezug auf Art. 29 des Bundesgesetzes über die Betäubungsmittel noch vornehmen sollte, wie dies in der Antwort des Bundesrates auf die einfache Anfrage Rechtsteiner vom 28. April 1993 zu eben dem Pilotprojekt DOSIS bestätigt worden war.

1.4. Innere Sicherheit

Das System ISIS und der Entwurf des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit

ISIS ist das Informationssystem der Bundesanwaltschaft zur Datenbearbeitung bezüglich des Staatsschutzes. Es wurde als provisorisches System angelegt und befindet sich nun auf dem Wege der Verwirklichung. Was die juristische Seite anbelangt, so wurden die von seiten des Datenschutzes gestellten Bedingungen in einer Verordnung des Bundesrates detailliert festgesetzt. Nach Ablauf dieser provisorischen Phase müssen die Bestimmungen der Verordnung, insbesondere diejenigen, die die Aufbewahrungsdauer und das Löschen der Daten regeln, neu bewertet werden. Dabei ist es wichtig, auch die Ergebnisse der Parlamentsdebatten zu berücksichtigen, die anlässlich der Prüfung des Entwurfs des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit geführt wurden. Der besagte Bundesgesetzentwurf ist am 14. März 1994 vom Bundesrat verabschiedet worden.

Bei ISIS handelt es sich um das provisorische Staatsschutz-Informations-System. Um der Genauigkeit willen muss hervorgehoben werden, dass die neue Terminologie auf die "Wahrung der inneren Sicherheit" Bezug nimmt. Das System ISIS wird von der Bundesanwaltschaft verwaltet und ist darauf ausgerichtet, die Durchführung von gerichtpolizeilichen Ermittlungen bei Fällen, die der Bundesgerichtsbarkeit unterstehen, zu erleichtern. ISIS soll ausserdem die Anwendung von Präventivmassnahmen im Bereich des eidgenössischen Staatsschutzes erleichtern. Diese Massnahmen zielen in erster Linie auf die Verhinderung und Bekämpfung von Terrorismus, verbotenen Nachrichtendienstes und gewalttätigen Extremismus ab. Das System ISIS setzt sich aus fünf Datenbanken zusammen (Staatsschutz; nicht-staatschutzrelevante Strafverfahren; Verwaltung; Dokumentation; Nummer-System). Man ist derzeit dabei, ISIS fertigzustellen. Im Dezember 1993 wurden zwei Untersysteme in Betrieb genommen. Dabei handelt es sich um die beiden Datenbanken "Verwaltung" und "Dokumentation". Die anderen Untersysteme werden voraussichtlich im Laufe des Jahres 1994 in Betrieb gesetzt werden.

Bei der Einführung des Systems ISIS wurden die Forderungen von seiten des Datenschutzes vor allem in juristischer Hinsicht vertreten. So wurde eine ausführliche Verordnung des Bundesrates ausgearbeitet, die klar festlegen sollte, zu welchem Zweck das System eingerichtet wird, welche Daten darin bearbeitet werden dürfen, wer die Benutzer des ISIS sind und zu welchen Daten diese Zugriff haben dürfen. Die Verordnung regelt ausserdem die Datenerfassung und die Qualitätskontrolle der Daten, die Bekanntgabe der Daten, das Verfahren der periodischen Gesamtbeurteilung, das Löschen der Daten und deren Aufbewahrungsdauer, die Ausübung des Auskunftsrechts der betroffenen Personen, die Sicherheitsmassnahmen und die verschiedenen Kontrollvorgänge in bezug auf die Benutzung des Systems. Da uns kein genaues Informatikkonzept zur derzeit laufenden technischen Verwirklichung des Systems vorliegt, haben wir die Bundesanwaltschaft daran erinnert, dass ISIS nur in hundertprozentiger Übereinstimmung mit der entsprechenden Verordnung des Bundesrates benutzt werden darf.

Nach Auskunft des Eidgenössischen Justiz- und Polizeidepartements wurde dieses System als Inselsystem angelegt. Das heisst, dass es mit keinem anderen Informationssystem verbunden ist und dass es einzig und allein durch die derzeitige Bundespolizei der Bundesanwaltschaft (in Zukunft: Bundesamt für innere Sicherheit) genutzt werden darf. Es muss allerdings hervorgehoben werden, dass die Verordnung ISIS die Möglichkeit vorsieht, bestimmten Beamten des Bundesamtes für Polizeiwesen den Zugang zu gewissen Daten des Systems zu gewähren. Darüber hinaus ist im Entwurf des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit vorgesehen, dass Personen, die den Sicherheitsorganen des Bundes und der Kantone angehören und Aufgaben zu erfüllen haben, die in diesem Gesetz festgelegt sind, einen Direktzugriff (online) zu diesem Informationssystem haben sollen. Unabhängig von diesem Gesetzentwurf hat uns die Bundesanwaltschaft beauftragt, die juristischen Bedingungen im Hinblick auf die baldige Einrichtung von Online-Verbindungen zu prüfen, welche den Kantonen den Zugang zum provisorischen System ISIS gewähren sollen.

ISIS wurde als provisorisches System entwickelt. Die entsprechende Verordnung gilt bis zur Inbetriebnahme des definitiven ISIS, längstens aber bis zum 31. Dezember 1996. Wir haben im Laufe der verschiedenen Entwicklungsphasen des ISIS-Systems regelmässig darauf hingewiesen, dass im Hinblick auf die Inbetriebnahme eines definitiven Informationssystems überprüft werden muss, inwieweit das Datenlöschverfahren funktioniert und wie genau die unterschiedlichen Aufbewahrungsfristen eingehalten werden. Ausserdem ist es unserer Meinung nach wichtig, die Bedingungen für einen Online-Anschluss der kantonalen Sicherheitsorgane zum System festzulegen.

Was das Auskunftsrecht der betroffenen Personen anbelangt, so entspricht die in der ISIS-Verordnung vorgesehene Regelung, die derzeit in Kraft ist, den Bestimmungen des Bundesgesetzes über den Datenschutz. Dennoch sollten die Ergebnisse der Parlamentsdebatten beachtet werden, die anlässlich der Prüfung des Entwurfs des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit geführt worden sind. Dieser Bundesgesetzentwurf, der am 14. März 1994 vom Bundesrat verabschiedet wurde, sieht - genau wie der Gesetzesentwurf bezüglich der Schaffung einer Zentralstelle zur Bekämpfung des organisierten Verbrechens - in bezug auf das Auskunftsrecht die Einführung einer restriktiveren Bestimmung vor. Der Vorentwurf, der uns zehn Monate vorher zur Stellungnahme unterbreitet wurde, enthielt eine entsprechende Bestimmung, die in bezug auf die Ausübung des Aus-

kunftsrechts auf das Bundesgesetz über den Datenschutz verwies. Obwohl das Auskunftsrecht den Eckstein des Datenschutzes bildet, ist man im Hinblick auf die Einführung einer neuen, restriktiveren Bestimmung in den Gesetzentwurf nicht an uns herangetreten. Und dies trotz unserer wiederholten Anfragen und unserer Befürchtungen, dass die getroffene Wahl für die organisierte Kriminalität zugunsten der inneren Sicherheit zurückgenommen werden könnte.

Wie bereits im Kapitel über die Schaffung einer Zentralstelle zur Bekämpfung des organisierten Verbrechens erwähnt, legt diese restriktive Norm zum Auskunftsrecht - zunächst einmal unter Verweis auf das DSG - fest, dass jeder Antrag nach dem Interessenabwägungsprinzip und unter Wahrung des Grundsatzes der Verhältnismässigkeit geprüft werden muss. Im Anschluss daran sieht die Bestimmung allerdings eine Reihe von Ausnahmen in bezug auf das DSG vor. Für die Fälle, in denen die Verbreitung von Auskünften das Ziel beeinträchtigen könnte, das mit Hilfe des Einschänkungsentscheids erreicht werden soll, sehen wir ein, dass es wichtig ist, die Möglichkeit zu haben, eine Beschränkung des Auskunftsrechts nicht begründen zu müssen. Die Verpflichtung, ein besonderes Interesse darlegen zu müssen, ist im spezifischen Rahmen der Massnahmen zur Wahrung der inneren Sicherheit noch gerade zu vertreten, obwohl sie mit der Rechtsprechung des Bundesgerichts kollidiert. Diese sieht nämlich vor, dass der Person, die einigermassen glaubhaft vorgibt, dass die zu ihrer Person registrierten Daten geeignet sind, in ihre persönliche Freiheit einzugreifen, die Einsicht gewährt werden muss, ohne dass die Person verpflichtet ist, noch ein anderes schutzwürdiges Interesse glaubhaft zu machen. Hingegen ist die der betroffenen Person auferlegte Bedingung, sich auf einen konkreten Sachverhalt beziehen zu müssen, unserer Ansicht nach inakzeptabel. Diese Bedingung läuft nämlich darauf hinaus - entgegen der menschlichen Würde - jeden Bürger zu zwingen, sich selbst bestimmter Tatbestände zu bezichtigen. Ausserdem ist es in den meisten Fällen für den Bürger, der sich nichts vorzuwerfen hat und der nur sicherstellen möchte, dass er von der Polizei nicht missbräuchlich oder grundlos überwacht wird, unmöglich, diese Bedingung zu erfüllen. Wir sind insofern der Ansicht, dass diese letzte Bedingung im Hinblick auf die Wahrung der Grundrechte und des Persönlichkeitsbereichs des Individuums gestrichen werden müsste. Die Entscheidung darüber liegt beim Parlament.

Es scheint uns noch wichtig zu erwähnen, dass die Autoren des Bundesgesetzentwurfs über Massnahmen zur Wahrung der inneren Sicherheit die Einführung einer derart restriktiven Regelung bezüglich des Auskunftsrechts durch einen Hinweis aufs deutsche Recht zu rechtfertigen suchen. Dementsprechend heisst es in der Botschaft zu diesem Gesetzentwurf, dass *"Diese Lösung, die wir ebenfalls für das Informationssystem der Zentralstelle für die Bekämpfung der organisierten Kriminalität vorgeschlagen haben (Botschaft vom 12. Januar 1994), hat sich im übrigen als Regel des deutschen Rechts für die Auskunftserteilung des Bundesamtes für Verfassungsschutz bewährt"*. Es muss allerdings darauf hingewiesen werden, dass gerade diese Lösung, die in Deutschland im Dezember 1990 in Kraft getreten ist, bei ihrer Verabschiedung ebenfalls auf starke Opposition in Deutschland stiess. Und selbst nachdem man einige Jahre mit dieser Regelung gelebt hat, steht sie immer noch im Kreuzfeuer der Kritik! So hat sich - man erinnere sich in diesem Zusammenhang auch an die von uns vorgebrachten Bedenken - der deutsche Bundesbeauftragte für den Datenschutz in seinem 13. und 14. Tätigkeitsberichts von 1991 und 1993 sowohl in bezug auf das Prinzip selbst als auch in bezug auf dessen zu restriktive Anwendung, sehr kritisch gegenüber dieser Lösung geäussert.

Was die anderen Bemerkungen angeht, die wir in bezug auf den uns vorgelegten Vorentwurf des Gesetzes gemacht haben, so muss hervorgehoben werden, dass einige auf ein positives Echo gestossen und aufgenommen worden sind. Wir haben z. B. gefordert, dass die Online-Zugriffe einiger Behörden zum Informationssystem ausdrücklich im Gesetz festgeschrieben werden sollen, dass sie dem Grundsatz der Verhältnismässigkeit Rechnung tragen müssen und dass sie einzig und allein auf die Behörden zu beschränken sind, denen der Zugang wirklich Nutzen bringt und die die Daten mit der gleichen Zielsetzung bearbeiten, mit der sie die Daten gesammelt haben. Insofern wird - gemäss dem Gesetzentwurf - die Datenbank bezüglich der Massnahmen zur Wahrung der inneren Sicherheit nicht für jede beliebige Bundes- oder kantonale Behörde zugänglich sein, sondern nur für die Sicherheitsorgane des Bundes und der Kantone, die bestimmte, im Gesetz über die innere Sicherheit festgeschriebene Aufgaben innehaben. Deshalb muss im Detail geprüft werden, wer sich hinter diesen Sicherheitsdiensten verbirgt.

2. Ausländer- und Asylrecht

2.1. Automatisiertes Personenregistratursystem AUPER-2

Wenige Monate vor Beginn der Berichtperiode, das heisst am 1. Januar 1993, wurde das automatisierte Personenregistratursystem AUPER-2 in Betrieb genommen, das unter anderem dem Bundesamt für Flüchtlinge und den kantonalen Fremdenpolizeibehörden zur Bearbeitung der heiklen Asylbewerber- und Flüchtlingsdaten dient. Es steht aber auch anderen Behörden zur Verfügung, darunter solchen, die vorab mit Fahndungsaufgaben betraut sind. Aus datenschutzrechtlicher Sicht musste wiederholt auch während der Berichtperiode beanstandet werden, dass das AUPER-2 mit seiner weiten Zugriffsregelung Datenbearbeitungen ermöglicht, für die eine ausreichende gesetzliche Grundlage fehlt und die geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen. Leider wurde die Arbeit des Datenschutzes durch eine ungenügende Kooperation der Systemverantwortlichen in verschiedener Hinsicht ernsthaft in Frage gestellt. Als erste Massnahme muss dringend der unklare Ist-Zustand des ständig in Weiterentwicklung begriffenen Systems aufgenommen werden. Hernach müssen für das AUPER-2 verbindliche Vorgaben zur Verbesserung und Weiterentwicklung auch des Datenschutzes formuliert und umgesetzt werden.

Am 30. Januar 1992 beschloss die Projektoberleitung des AUPER-2 auf Anregung des Datenschutzes die Abfassung eines Sicherheitsberichts zur Abklärung von Sicherheitsfragen und zur Erarbeitung verbesserter Grundlagen für eine zu erlassende AUPER-Verordnung. Wir wurden mit der Redaktion betraut. Dieser Bericht wurde nach eingehenden Gesprächen mit den Systemverantwortlichen und nach mehreren Hearings bei den Systembenutzern am 7. Oktober 1992 fertiggestellt und anschliessend der Projektoberleitung vorgelegt. Der Bericht erhob zwar nicht den Anspruch einer abschliessenden Bestandesaufnahme und Würdigung von Sicherheitsfragen beim kurz vor der Inbetriebnahme stehenden AUPER-2. Dazu wäre der Beizug externer Experten erforderlich gewesen, was auch seitens der Projektoberleitung anerkannt und im Bericht festgehalten wurde. Dennoch konnten verschiedene, zum Teil schwerwiegende Mängel festgestellt und Vorschläge zu deren Behebung unterbreitet werden. Im Vordergrund stand dabei eine konsequente Trennung von (fahndungs-) polizeilichen und Asylbewerber-Daten im AUPER-2 bei der Speicherung und bei der Gewährung der Zugriffsrechte, so dass die Asylbewerber-Daten nicht von vornherein

unkontrolliert zusammen mit den Fahndungsdaten für jegliche Art der Polizeiarbeit im In- und Ausland verwendet werden könnten. Dies umso mehr, als heute die meisten Benutzer von zentralen EDV-Systemen wie dem AUPER-2 über eigene Bürokommunikationssysteme und "Mail"-Anschlüsse auch für das Ausland verfügen. Ebenso sollten nur die zur Aufgabenerfüllung unerlässlichen Asylbewerber-Daten elektronisch bearbeitet und zur Verfügung gestellt werden, was (gemäss den Ergebnissen der Hearings) beim AUPER-2 nicht überall der Fall ist. Diese und einige weitere Mängel wurden auch anlässlich der Ämterkonsultation für die AUPER-Verordnung vom 18. November 1992 im einzelnen aufgeführt. Unser Einverständnis wurde von deren Behebung vor oder kurz nach der Inbetriebnahme des AUPER-2 bzw. der Inkraftsetzung der AUPER-Verordnung abhängig gemacht. Nachdem die Projektoberleitung die Behebung dieser Mängel versprochen hatte, stimmte der Dienst für Datenschutz der Inbetriebnahme des AUPER-2 sowie der AUPER-Verordnung zu. Die aufgezeigten Mängel wurden aber in der Folge nicht behoben, sondern stattdessen die Weiterentwicklung des AUPER-2 forciert.
Wir haben daher neben einer umfassenden und verbindlichen Erhebung des aktuellen Zustands des AUPER-2 empfohlen, die Asylbewerber- und Flüchtlingsdaten konsequent von den übrigen (Personen-) Daten des AUPER-2 zu trennen und die Bearbeitung von Asylbewerber- und Flüchtlingsdaten durch Polizeistellen auf ein absolutes Minimum zu reduzieren. Das Verfahren ist noch hängig.

2.2. Zentrales Ausländerregister ZAR

Im Zentralen Ausländerregister ZAR des Bundesamts für Ausländerfragen sind die verschiedensten Daten von etwa 3,5 Mio Ausländern gespeichert, die sich in der Schweiz aufgehalten haben oder noch aufhalten. Eine Vielzahl von Behörden des Bundes, der Kantone und der Gemeinden arbeiten mit diesen Daten. Das System ist in ständiger Entwicklung begriffen. Wiederholt ist es dabei leider vorgekommen, dass Online-Zugriffe von Polizeibehörden bekannt geworden sind, ohne dass für diese Zugriffe eine Erlaubnis bzw. eine Rechtsgrundlage bestanden hätte, so auch in jüngster Zeit. Zudem scheint es sich so zu verhalten, dass die bearbeiteten Daten vielfach auch sonst ungenügend geschützt sind und zum Teil nicht à jour gehalten werden (können). Es ist daher ebenfalls beim ZAR notwendig, den heutigen Zustand umfassend und verbindlich abzuklären und hernach die erforderlichen Massnahmen zur Verbesserung und Weiterentwicklung des Datenschutzes bei diesem System zu formulieren und umzusetzen.

Im Frühjahr 1992 wurde bekannt, dass die Grenzposten und die Polizeibehörden der Kantone über einen Online-Zugriff auf das ZAR verfügen, ohne hierzu berechtigt zu sein. Mit Änderung der ZAR-Verordnung erteilte der Bundesrat am 25. März 1992 die ausdrückliche Erlaubnis zum direkten Zugriff der genannten Behörden auf das ZAR für die Erfüllung genau umschriebener ausländerrechtlicher Aufgaben. Der Datenschutz wurde mit Passwörtern und Zugriffsprofilen geregelt. In der Folge wurde das ZAR einer sog. Audit-Prüfung unterzogen, damit derartige Pannen nicht mehr vorkämen. Wir erhielten ein Exemplar des Schlussberichts dieser Untersuchung zugestellt, der aus datenschutzrechtlicher Sicht keinen Anlass zu sofortigem Einschreiten seitens des Dienstes für Datenschutz gab. Immerhin gelangte das Bundesamt für Ausländerfragen als Datenherr des ZAR mit der Bitte an uns, ihn in Fragen des Datenschutzes betreffend das ZAR zu unterstützen bzw. zu verschiedenen Fragen und Massnahmen Stellung zu nehmen. Im Rahmen dieser Tätigkeit, die bis in die Berichtperiode hinein dauerte, erstellten wir zahlreiche Rechtsgutachten zu Daten-

schutzfragen und nahmen unter Beizug eines Informatik-Spezialisten an verschiedenen Besprechungen der Systemverantwortlichen und der Systembenutzer teil. Hierbei wurden auch Datenbearbeitungen vorgeführt. Da das ZAR in ständiger Weiterentwicklung begriffen ist, war es dabei leider nicht möglich, einen einigermassen gesicherten Sachverhalt zu erstellen und diesen gesamthaft zu würdigen. Weil auch die erwähnte Audit-Prüfung wichtige Datenschutzprobleme beim ZAR nachweislich nicht erkannt hat (vgl. hiezu die Ausführungen am Ende des nachfolgenden Abschnitts), scheint eine systematische Aufnahme des Ist-Zustands und dessen Würdigung aus datenschutzrechtlicher Sicht nunmehr als unerlässliche und dringend notwendige Massnahme.

Im Rahmen der erwähnten Beratertätigkeit wurden verschiedene Gutachten zu Grundsatzfragen der Ausgestaltung ("Architektur") eines grossen EDV-Systems wie des ZAR verfasst. Ein Gutachten äusserte sich dabei speziell auch zur Frage der Protokollierungspflicht bei unerlässlichen Polizeizugriffen auf zivile Daten. Ein anderes Gutachten behandelte Fragen der Datensicherheit in Rechenzentren des Bundes und der Kantone, namentlich wenn Daten aus vielen Sammlungen an einer zentralen Stelle mit denselben Geräten und unchiffriert bearbeitet und übermittelt werden. Ein weiteres Gutachten betraf Fragen des Verbunds von EDV-Systemen des Bundes mit solchen der Kantone, zumal wenn heikle "Bundes-Daten" in eine kantonale Umgebung mit einer vergleichsweise largen Zugriffsregelung übermittelt werden sollen. - Ein zweiter Schwerpunkt der Gutachtertätigkeit betraf die amtshilfeweise Weiterleitung von umfangreichen Ausländer-Datenbeständen an die Polizei- oder Registerbehörden des Auslands sowie von Visumunterlagen an die Kantonspolizeien oder von Ausländer- bzw. von Arbeitslosenversicherungsdaten an die Steuerbehörden der Kantone. Als dritter Schwerpunkt kristallisierte sich die Frage des Umfangs und der Erforderlichkeit von Datenbearbeitungen mit elektronischen Mitteln heraus. Aus datenschutzrechtlicher Sicht als problematisch musste die Aufbewahrung und Verwaltung grosser Bestände zumal unstrukturierter Dossiers mit elektronischen Mitteln bezeichnet werden, wie dies mit dem EDV-System REGI-2 offenbar für den gesamten Dossierbestand des Bundesamts für Ausländerfragen vorgesehen ist. Bereits bei der elektronischen Eingabe können Fehler nicht ausgeschlossen werden. Weiter können die so gespeicherten besonders schützenswerten Daten und Persönlichkeitsprofile in bisher ungekanntem Ausmass mit den vielfältigsten elektronischen Mitteln bearbeitet und ausgewertet werden. Weil heute die Chiffrierung vielfach als zu aufwendig erachtet wird, entstehen zudem erhebliche Sicherheitsrisiken, die zu umfangreichen Haftungen führen könnten. Ebenso bildete die Frage der Zulässigkeit der sog. Freitexte bzw. "Memofelder" und der Bemerkungscodes im ZAR Gegenstand einer datenschutzrechtlichen Beurteilung. Offenbar konnten die dabei gemachten Anregungen bereits in die Praxis umgesetzt werden, so dass im ZAR nur noch standardisierte, datenschutzrechtlich "unbedenkliche" Freitexte und vergleichsweise wenige und meist wertungsfrei aufgeschlüsselte Bemerkungscodes verwendet werden. Der Umfang der Datenbearbeitung mit dem ZAR bildete zudem den Gegenstand verschiedener Gespräche mit Benutzer-Organisationseinheiten. Dabei ergab sich, dass die getroffenen Zugriffsregelungen in den wenigstens Fällen auf einer eigentlichen Aufgabenanalyse basieren und daher möglicherweise zu weit ausgefallen sind. Bei den Gesprächen mit dem Bundesamt für Polizeiwesen Ende 1993/Anfang 1994 stellte sich heraus, dass dieses Amt offenbar seit mehreren Jahren über zahlreiche Zugriffe auf das Zentrale Ausländerregister verfügt, ohne hierzu berechtigt zu sein. Um eine sachgerechte Abwägung der Interessen der betroffenen Personen und der Sicherheit vornehmen zu können, müsste auf Unterlagen gegriffen werden können, wie sie bei

einer Aufgabenanalyse im umschriebenen Sinn angefertigt werden. Solche Unterlagen fehlen auch hier. Wir haben daher empfohlen, die Bearbeitungen von ZAR-Daten im Bundesamt für Polizeiwesen auf ein absolutes Minimum zu reduzieren und sogleich eine Aufgabenanalyse durchzuführen. Das Verfahren ist noch hängig.

2.3. Revision des Asyl- und Ausländergesetzes; Datenschutz bei der Rechts- und Amtshilfe

In die Berichtperiode fielen zudem die verwaltungsinternen Vorarbeiten für eine Änderung des Asylgesetzes und des Bundesgesetzes über Niederlassung und Aufenthalt der Ausländer, an denen wir auch teilnahmen. Nach den Bestimmungen des DSG bedürfen heikle Datenbearbeitungen, wie sie namentlich im Asylbereich, aber auch im Bereich des übrigen Ausländerrechts vorkommen, einer demokratisch abgestützten Rechtsgrundlage. Aus datenschutzrechtlicher Sicht ist es zu begrüssen, wenn nunmehr die bisher fehlenden Bestimmungen im Asyl- und übrigen Ausländerbereich geschaffen werden. Diese sollten sich dabei weitestmöglich an den Zielen des DSG orientieren. Verfehlt wäre es, wenn umstrittene Praktiken bei der Datenbearbeitung ohne sorgfältige Güterabwägung im Gesetz festgeschrieben würden, um den formellen Anforderungen zu genügen. Eine gewisse Gefahr hierzu scheint im Asyl- und übrigen Ausländerbereich insofern zu bestehen, als sehr vielen Behörden "einfachheitshalber" direkte (Online-) Zugriffe auf die vielfach heiklen Daten gewährt werden oder gewährt werden sollen, ohne dass dafür wirklich eine Notwendigkeit bestünde. Aus datenschutzrechtlicher Sicht als problematisch erscheint dabei auch der unkontrollierte Austausch namentlich von Asylbewerber-Daten mit dem Ausland etwa im Rahmen von INTERPOL. Weiter muss aus Gründen des Persönlichkeits- und des Datenschutzes eine diskriminierende Behandlung der Asylbewerber durch ein unverhältnismässiges Vorgehen bei der Erhebung von Fingerabdrücken abgelehnt werden.

Bundesorgane sind zur gegenseitigen *Amtshilfe* verpflichtet. Das DSG ermächtigt sie denn auch ausdrücklich in Art. 19 zur amtshilfeweisen Bekanntgabe von Personendaten, wenn dafür eine Rechtsgrundlage besteht oder die Daten für den Empfänger im Einzelfall zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich sind. Sie müssen die Bekanntgabe jedoch ablehnen, einschränken oder mit Auflagen verbinden, wenn höherrangige Interessen oder gesetzliche Geheimhaltungspflichten sowie besondere Datenschutzvorschriften dies verlangen. Erhält indessen jemand den direkten Zugriff auf die elektronischen Datenbanken eines Bundesorgans, kann ab diesem Zeitpunkt nicht mehr geprüft werden, ob die einzelnen Datenabfragen auch wirklich notwendig oder zulässig sind oder ob sie vom Bundesorgan nicht vielmehr verweigert oder zumindest eingeschränkt werden müssten. Solche Online-Zugriffe sind daher nur zulässig, wenn der Datenbekanntgabe von vornherein keine höherrangigen Interessen, gesetzlichen Geheimhaltungspflichten oder besonderen Datenschutzvorschriften entgegenstehen können. Das ist sehr selten der Fall. Um ganz sicher zu sein, dass dieses datenschutzrechtliche Grundanliegen nicht leichtfertig ausser Acht gelassen wird, verlangt das DSG für solche Online-Zugriffe eine ausdrückliche gesetzliche Erlaubnis, bei der Weitergabe heikler Daten gar eine ausdrückliche Erlaubnis in einem formellen Gesetz. Kann, was der Regelfall sein dürfte, ein solcher Online-Zugriff nicht gewährt werden, ist gleichwohl in den allermeisten Fällen die einzelfallweise Amtshilfe möglich, d.h. wenn die erforderliche Güterabwägung und die Rechtslage im konkreten Fall dies gestatten.

Unter grossem Zeitdruck und mit den oben im Abschnitt über das AUPER-2 geschilderten Vorbehalten stimmten wir Ende 1992 dem Begehren verschiedener Poli-

zeibehörden des Bundes nach einem Online-Zugriff auf die Asylbewerber-Daten des AUPER-2 zu. Diese Behörden machten im Wesentlichen geltend, rasch ersehen zu müssen, ob eine interessierende Person ein Asylgesuch gestellt hat. In der Zwischenzeit wurde aber bekannt, dass diesen Behörden offenbar auch sog. "Endlos-Suchmasken" und Asylbewerber-Daten in einem Umfang zur Verfügung stehen, welcher über die angegebene Datenbearbeitung hinaus eine eigentliche Rasterfahndung ermöglicht. Ferner erhielten diese Behörden in der Zwischenzeit moderne Büroautomatisationen, die unkontrolliert weitere Datenbearbeitungen und auch den Datenversand ins Ausland gestatten. Ähnliche Zugriffe bestehen nach dem Gesagten beim Zentralen Ausländerregister oder sollen neu ermöglicht werden. Es besteht zudem offenbar die Auffassung, dass INTERPOL-Abfragen auch bei den Asylbewerber- oder Ausländer-Daten keine Güterabwägung im umschriebenen Sinn erheischen, sondern dass die erfragten Daten gemäss den INTERPOL-Statuten vielmehr in jedem Fall bekanntgegeben werden müssen und zwar auch an Länder ohne ausreichenden Datenschutz. Unter all diesen Umständen sind die erwähnten Online-Zugriffe aus datenschutzrechtlicher Sicht strikte abzulehnen. Formellgesetzliche Bestimmungen, wie sie im Rahmen der anstehenden Revisionen vorgeschlagen werden könnten und die auf derart undifferenzierte Weise den Umgang zumal mit den hochsensiblen Flüchtlingsdaten gestatten würden, könnten aus verfassungs- und datenschutzrechtlichen Ueberlegungen in keiner Weise gutgeheissen werden. Diesen Standpunkt haben wir während der Berichtperiode in verschiedenen Eingaben deutlich gemacht und auch eine Anpassung der AUPER-Verordnung verlangt. Wir haben konkrete Vorschläge unterbreitet, wonach in wenigen Fällen Online-Zugriffe zu - auch inhaltlich beschränkten - Einzelabfragen ohne Verwendung von Endlos-Suchmasken ermöglicht und Zweckentfremdungen der abgefragten Daten namentlich unbeteiligter Dritter mittels Protokollierung festgestellt werden könnten. Diese Vorschläge wurden bisher vollumfänglich abgelehnt.

Beim *internationalen Datenaustausch* muss ein gleichwertiger Datenschutz im Empfängerstaat gewährleistet sein. Gleichwertig ist der Datenschutz namentlich dann, wenn der Grundsatz der Zweckbindung bzw. Zweckbeschränkung bei der Datenbearbeitung eingehalten wird und wenn generell die übermittelten Daten in ausreichender Weise gesichert sind. Mit anderen Worten muss von vornherein feststehen, welche ausländische Behörde für die Entgegennahme der übermittelten Daten zuständig ist und dass diese die übermittelten Daten nicht in unzulässiger Weise zweckfremd verwendet oder weiterleitet. Diese Grundsätze gelten auch gemäss Art. 15 des sog. Dubliner Erstasylabkommens von 1992, welches im Wesentlichen die innereuropäische Zuständigkeit bei der Behandlung von Asylgesuchen und den damit verbundenen Datenaustausch regelt, und dem die Schweiz im Rahmen eines Parallelabkommens beitreten möchte. Zudem werden in diesem Abkommen die zu übermittelnden Daten genau festgelegt (Datenkatalog), was es beim Erlass von Landesrecht in diesem Bereich zu berücksichtigen gilt, wenn nicht Abweichungen in Kauf genommen werden sollen. Das Abkommen verlangt auch die Protokollierung des Datenaustausches. Bei verschiedenen Gelegenheiten haben wir daher angeregt, sowohl Vorschriften über die Zweck- und Behördenbindung im umschriebenen Sinn als auch einen Katalog der Asylbewerber-Daten, die ans Ausland übermittelt werden dürfen, vor allem ins revidierte Asylgesetz aufzunehmen. - In diesem Zusammenhang sind ebenfalls die (für den Asylbereich praktisch gleichlautenden) Bestimmungen des sog. Schengener Zusatzabkommens von 1990 von Bedeutung. Nach diesem Abkommen dürfen im neu zu schaffenden Schengener Informationssystem neben den Daten aus dem Polizeibereich keine Daten aus dem Asylbereich be-

arbeitet und aufbewahrt werden. Darin ist eine auch für das schweizerische Recht wichtige Konkretisierung des erwähnten Grundsatzes der Zweckbindung zu sehen. Die Übermittlung der - üblicherweise im Bereich der polizeilichen Fahndung verwendeten - Fingerabdrücke ist im hier besprochenen internationalen Flüchtlingsrecht nicht geregelt. Aus datenschutzrechtlicher Sicht erscheint sie als nicht unproblematisch (Intensität des Eingriffs und diskriminierende Wirkung sowie Schutzwürdigkeit der Daten). Wir haben von einer Übermittlung solcher Daten nicht krimineller Asylbewerber ins Ausland abgeraten. Sollte sich eine Uebermittlung in Ausnahmefällen als unumgänglich erweisen, müssten die Daten gut geschützt und an eine Asylbehörde bekanntgegeben werden, welche sie nicht zusammen mit Strafdaten aufbewahrt.

Mit dem *revidierten Asylgesetz* soll offenbar die bisherige Uebergangsregelung ins ordentliche Recht aufgenommen werden, wonach bei ausnahmslos allen Asylbewerbern die Fingerabdrücke erhoben und im Fingerabdruck-Identifikationssystem AFIS der Bundesanwaltschaft und des Bundesamts für Polizeiwesen gespeichert werden müssen. Wir haben mehrfach und mit Nachdruck darauf hingewiesen, dass die Erhebung der Fingerabdrücke nur als ultima ratio in Frage kommt. Deshalb sei im Asylgesetz eine mit Art. 351quinquies StGB vereinbare Formulierung zu wählen. Ferner werde eine gemeinsame Aufbewahrung von Asylbewerber-Daten mit Kriminellen-Daten aus den oben dargelegten datenschutzrechtlichen Gründen strikte abgelehnt. Anlässlich einer Vorführung des AFIS ergab sich zwar, dass die Fingerabdruckbogen nur mit personenunabhängig vergebenen Hinweisnummern versehen werden, doch dass die Zugriffs- und Bearbeitungsberechtigungen wie auch die Sicherheitsvorkehren keineswegs datenschutzrechtskonform ausgestaltet sind, so dass die geäusserten datenschutzrechtlichen Einwände vollumfänglich aufrechterhalten werden müssen.

2.4. Weitere Aktivitäten im Bereich des Asylrechts und des übrigen Ausländerrechts

In die Berichtperiode fielen auch die Stellungnahmen zu den *Rückübernahmeabkommen betreffend Personen an der Grenze mit Deutschland und Ungarn* sowie zum sog. Schengen-Polen Uebereinkommen gleichen Inhalts. Hier wurden wir leider regelmässig sehr spät über entscheidende Schritte informiert. Gleichwohl konnten die bereits im vorstehenden Abschnitt näher umschriebenen zentralen Grundsätze betreffend die Zweck- und Behördenbindung beim internationalen Datenaustausch und die Aufnahme eines verbindlichen Datenkatalogs in die beiden Verträge mit Deutschland und Ungarn angeregt werden. Im Falle des Abkommens mit Deutschland führten wir zudem eine Erhebung über die Datenbearbeitungen an der Grenze und in den schweizerischen Flughäfen durch, die die tatbeständliche Grundlage unserer Stellungnahme bildete. In anderem Zusammenhang bot sich zudem die Gelegenheit, ein erstes Mal einlässlich Datenschutzfragen im Gesundheits- und Fürsorgebereich des Asylwesens aufzugreifen und abzuhandeln (Mitbericht zum EDV-Projekt LIFAS).

3. Telekommunikation

3.1. X.500-Directory: ein weltweites Informationssystem

Beim X.500-Directory handelt es sich um ein weltweites Informationssystem, mittels dessen weltweit von Personen und Institutionen, die an das Directory angeschlossen sind, Informationen abgerufen werden können, die im Directory gespeichert sind. Zur Zeit läuft ein Pilotprojekt, an dem bereits über 30 Länder mit über 1 Million Einträgen beteiligt sind. Die weltweite Verfügbarkeit und mögliche Verknüpfbarkeit von Personendaten durch das X.500-Directory wirft aus datenschutzrechtlicher Sicht grosse Probleme auf.

Jegliche Kommunikation beruht auf dem Austausch von Informationen. Für jeden Informationsaustausch benötigt der Absender einer Mitteilung die Adresse des Empfängers. Bei der Adresse kann es sich etwa um eine Postadresse oder auch um eine Telefonnummer handeln. Übertragen wir diesen Sachverhalt auf die Welt der elektronischen Datenübertragung, so wird deutlich, dass auch hier Informationen notwendig sind, um einen Kommunikationspartner adressieren zu können. Die in diesem Bereich verwendeten Adressen und Informationen sind jedoch nicht immer so leicht verständlich und geläufig wie die Verwendung einer Postadresse.

Heute gibt es eine Vielzahl von Verzeichnissen (z.B.: Telefonnummern, Telefaxnummern, X.25 Adressen, X.400 Adressen,...), in denen oft redundante Daten vorhanden sind. Ebenso sind diese Verzeichnisse in den vielfältigsten Systemumgebungen und auf verschiedendsten Medien vorhanden. Ändert sich eine Information, so müssen sämtliche Verzeichnisse, in denen diese Information enthalten ist, angepasst werden. Ein Beispiel dafür ist ein Umzug. Hier ist es allein schon ein ziemlich grosser Aufwand, alle Adressänderungen zu veranlassen, was noch immer keine Garantie für den Erfolg ist. Immer wieder treten bei diesem Vorgang Fehler auf. Denkt man an die elektronische Datenübertragung, so wird deutlich, dass ein Fehler in diesen Bereichen gravierende Auswirkungen haben kann. Dies war auch eine der Hauptmotivationen, sich ein Verzeichnis zu wünschen, das immer aktuell, leicht zu pflegen und für alle Beteiligte verfügbar ist.
So wurde ein Directory-Standard ausgearbeitet, mit dessen Hilfe die leichte Pflege und Aktualität der verzeichneten Informationen bewerkstelligt werden soll.
Dieser Directory-Standard wurde vom CCITT (Comité Consultatif International Télégraphique et Téléphonique) und der ISO (International Organisation for Standardization) ausgearbeitet und beschrieben. Die Standards werden als X.500 und folgende für CCITT, sowie ISO - 9594 - 1 bis 8 für ISO bezeichnet.

Dieser Dienst (X.500 oder ISO 9594) ermöglicht es, Informationen über verschiedenartige Objekte in einer verteilten Kommunikationsumgebung (Personen, Organisationen, andere Dienste oder Rechner etc.) global zugänglich zu machen. Der Directory-Dienst nach X.500 regelt im wesentlichen anwendungsunabhängig die Abbildung von Informationen in einer Directory Information Base (DIB) sowie deren logische Struktur. Ebenso werden die Regeln zum Unterhalt und den Zugriff auf diese Informationen unter Verwendung von standardisierten Zugriffsprotokollen festgelegt. Jeder Eintrag in der DIB wird durch einen Namen identifiziert. Jeder Eintrag in einer DIB muss weltweit eindeutig bezeichnet werden können. Für die Namensgebungsinstanzen muss es klar abgrenzbare Zuständigkeitsbereiche geben.
Da mit X.500 die logische Struktur der Daten festgelegt werden kann, ist es möglich, beinahe jede Art von Information so zu verwalten. Es können sowohl Informationen

zur Adressierung als auch zum Informationsgewinn gespeichert werden. Beispiele hierfür wären die Abbildung eines Telefonbuches (weisse und gelbe Seiten), wie auch die Abbildung eines Versandhauskataloges. Je nach technischen Voraussetzungen können die abgebildeten Informationen neben Text auch Bild und Ton enthalten. Die Daten können verteilt gespeichert und administriert werden. Der Zugriff auf die Daten erfolgt über Suchanfragen. Es bestehen Möglichkeiten der individuellen Zugriffsbeschränkung zu Objekten.

In der Schweiz beschäftigt sich das SDF (Swiss Directory Forum) mit dem Einsatz des Directory-Services nach X.500. Hier interessiert die Frage nach der weltweiten Einbindung ebenso wie der Einsatz in der Schweiz. Die Bestimmung und Regelung der Zuständigkeiten von Namensgebungsinstanzen und die Definition der DIT-Struktur (Directory Information Tree) für die Schweiz sind derzeit Themen in diesem Forum. Wir haben seit Ende 1993 die Gelegenheit zur Mitarbeit. Von zentraler Bedeutung ist die Frage, welche Informationen im Swiss-Directory zugänglich gemacht werden sollen, sowie die Beurteilung, welche Punkte unter dem Aspekt des Datenschutzes von Bedeutung sind und geregelt werden müssen.

Die dem X.500-Directory zugrundeliegende Idee war, Firmen zu ermöglichen, ihren Geschäftspartnern weltweit Namen, Adressen, Telefon- und Telefaxnummern sowie die E-Mail-Identifikationen ihrer Mitarbeiter jederzeit abrufbar zur Verfügung zu stellen. Wie es oft geschieht, entwickelte auch dieses Projekt eine gewisse Eigendynamik mit der Folge, dass über X.500 heute nicht mehr nur die Telekommunikationsangaben von Firmen verfügbar sind. Dadurch, dass auch Einzelpersonen Interesse an der Nutzbarmachung des X.500 für ihre Zwecke zeigten, ist heute über X.500 im Grunde genommen alles, gleichgültig welchen Inhaltes und in welcher Form in den Ländern, die bereits angeschlossen sind, abrufbar: normale Textpassagen zu wissenschaftlichen Zwecken, Namen, Adressen, Telefon- und Telefaxnummern, E-Mail-Identifikationen, Berufe, Funktionen, Bilder - seien es Abbildungen von Gegenständen, Portraits von Personen oder Fingerabdrücke -, Klangfolgen wie Musik, aber auch Stimmen, Hobby, Haarfarbe, Lieblingsgetränke, Körpermasse und andere mehr.

Aus datenschutzrechtlicher Sicht stellt sich die *weltweite Verfügbarkeit* von Personendaten über ein Computersystem als äusserst problematisch dar, da in der Regel das, was ins System eingegeben wurde, grundsätzlich von jedermann, der am X.500 angeschlossen ist, abgerufen werden kann. Die im System verfügbaren Daten können also nicht nur in der Schweiz und somit im Geltungsbereich des schweizerischen Datenschutzgesetzes abgerufen werden, sondern auch in anderen europäischen oder gar aussereuropäischen Ländern, die nicht über eine dem schweizerischen Datenschutzgesetz vergleichbare Datenschutzgesetzgebung verfügen. Das hat zur Folge, dass der Personenschutz in den verschiedenen Ländern nicht den Anforderungen des schweizerischen DSG entspricht, was vor allen Dingen bei der Verfügbarkeit von sehr sensiblen Daten, besonders schützenswerten Personendaten sowie Persönlichkeitsprofilen schwerwiegende Folgen für die betroffene Person haben kann.

Ein weiterer wesentlicher Gesichtpunkt aus der Sicht des Datenschutzes ist die *Verknüpfbarkeit der Daten*. Diese Problematik bezieht sich nicht nur auf besonders schützenswerte Personendaten und Persönlichkeitsprofile, die im System direkt zur Verfügung gestellt werden können. Vielmehr werden von ihr auch andere "normale"

Personendaten, die mit Hilfe des Computers unkontrollierbar verfügbar und verknüpfbar werden, erfasst. Dadurch können aus "normalen" Personendaten ganze Persönlichkeitsprofile von Personen zusammengestellt und zu irgendwelchen, nicht kontrollierbaren Zwecken weiterverarbeitet werden. Zwar sind bereits heute in öffentlichen, in der Regel gedruckten Verzeichnissen Personendaten verfügbar, die für sich in dem jeweiligen Verzeichnis nicht besonders schützenswert oder gar Persönlichkeitsprofile sind. Die Verknüpfung dieser Daten der einzelnen Verzeichnisse zu Persönlichkeitsprofilen würde jedoch einen immensen Aufwand bedingen oder wäre gar unmöglich. Dagegen kann mittels X.500 die Verknüpfung der darin verfügbaren Daten mit enormer Geschwindigkeit vorgenommen werden, ohne dass es eines beträchtlichen Arbeitsaufwandes bedürfte. Ansatzweise liesse sich das Problem der Verknüpfbarkeit aus technischer Sicht durch Zugriffsberechtigungen angehen.

Um die verschiedenen Probleme wenigstens ansatzweise in den Griff zu bekommen, ist es erforderlich, einerseits für die schweizerischen Informationsanbieter soweit wie möglich einheitliche Regelungen auszuarbeiten und anzubieten, andererseits auf internationaler oder zumindest europäischer Ebene gemeinsame Richtlinien für den Gebrauch von X.500 zu erarbeiten.
Im schweizerischen Rechtsraum wären folgende Lösungsansätze denkbar:
Für die *privaten Informationsanbieter* wird eine Art Vertrag ausgearbeitet, in dem die Bedingungen und Umstände des Zur-Verfügung-Stellen von Personendaten sowie weitere Verantwortlichkeiten festgelegt würden, wie etwa welche Personendaten zugänglich gemacht werden dürfen, dass von Firmen keine besonders schützenswerten Personendaten und Persönlichkeitsprofile ihrer Mitarbeiter zur Verfügung gestellt werden dürfen, dass das Zugänglichmachen von Personendaten Dritter (Mitarbeiter etc.) nur nach vorgängiger schriftlicher Einwilligung der betroffenen Person zulässig ist, Hinweise auf einen allfälligen ungenügenden Persönlichkeitsschutz in anderen Ländern und Staaten, Rechtsfolgen usw. Dieses Reglement wäre von jedem, der an X.500 an geschlossen ist, zu unterschreiben.

Da auch *Bundesorgane* sowohl über sich, als auch über Dritte (Mitarbeiter usw.) Personendaten zur Verfügung stellen können, sollte die Ausarbeitung eines für alle Bundesorgane verbindlichen Gesetzes an die Hand genommen werden, in dem festzulegen ist, welche Personendaten unter welchen Bedingungen (Einwilligung, technische Voraussetzungen usw.) im X.500 zugänglich gemacht werden dürfen.

Es wäre jedoch auch denkbar, für alle, die einen Anschluss an das X.500 vom BAKOM erhalten, unabhängig von der Art des X.500-Beteiligten (sei es Privatperson, Bundesorgan oder kantonales Organ) verbindliche Bedingungen auszuarbeiten, die diese als Voraussetzung für den Zugang zum X.500 unterzeichnen und damit anerkennen müssen.

3.2. Frequenzüberwachung

Aufgrund einer Intervention von unserer Seite nach vorgängiger Information durch die Presse wurde eine Arbeitsgruppe eingesetzt, die mit der Schaffung einer hinreichenden Rechtsgrundlage für die von den PTT-Betrieben durchgeführten Frequenzüberwachungen, im Rahmen derer die Inhalte von über schnurlose Telefone geführte Gespräche mitgehört und aufgezeichnet werden, beauftragt wurde.

Nach Abklärung des Sachverhaltes aus datenschutzrechtlicher und verfassungsrechtlicher Sicht gelangten wir mit der Feststellung, dass sich diese Praxis auf keine hinreichende Rechtsgrundlage in Form eines formellen Gesetzes stützen könne, an die Medien. In der Folge konstituierte sich eine Arbeitsgruppe, die den Auftrag hat, eine solche Rechtsgrundlage zu erarbeiten.
Zielsetzung für die zu erarbeitende(n) Bestimmung(en) ist aus unserer Sicht: festzulegen, zu welchem Zweck eine Frequenzüberwachung erfolgen darf, die Bedingungen zu definieren, unter denen ein Mithören und/oder Aufzeichnen der über die Frequenz geführten Gesprächsinhalte zulässig ist, die Regelung der Weitergabe von mittels der Frequenzüberwachung ermittelten Personendaten an das BAKOM bzw. an die Strafverfolgungsbehörden des Bundes etc.

In der Arbeitsgruppe sind das Bundesamt für Kommunikation, die Generaldirektion der PTT-Betriebe, das Bundesgericht und wir vertreten. Mittlerweile wurde die von uns vertretene Auffassung hinsichtlich des Fehlens einer hinreichenden Rechtsgrundlage durch ein internes Arbeitspapier, das vom Vertreter des Bundesgerichtes ausgearbeitet wurde, bestätigt.

3.3. Telefonüberwachung/Observation zu Zwecken der Strafverfolgung

Aufgrund eines Berichtes der Geschäftsprüfungskommission des Nationalrates sowie der dazu erfolgten Stellungnahme des Bundesrates wurde per Verfügung durch Bundesrat Koller eine Studiengruppe Telefonüberwachung eingesetzt, die mit der Ausarbeitung von restriktiveren, die Persönlichkeit weitergehend schützenden, auch für die Kantone geltenden Regelungen zur Telefonüberwachung sowie von neuen Bestimmungen zur Regelung von Observation und Einsatz von V-Leuten beauftragt wurde. Unter den 14 Mitgliedern gibt es nur ein Mitglied von Seiten des Persönlichkeitsschutzes/Datenschutzes.

Die Geschäftsprüfungskommission des Nationalrates (GPK Nationalrat) erstellte am 9. November 1992 einen Bericht "Telefonüberwachung im Bund" an den Bundesrat, mit dem sie die Schaffung von strikteren Regelungen für die Telefonüberwachung zu Zwecken der Strafverfolgung sowie von neuen, den Regelungen der Telefonüberwachung entsprechenden Bestimmungen für den Einsatz von V-Leuten und die Observation verlangte. Zu diesem Bericht erfolgte eine Stellungnahme des Bundesrates vom 17. Februar 1993. Aufgrund der erfolgten Ausführungen erliess der Vorsteher des Eidgenössischen Justiz- und Polizeidepartementes, Bundesrat Koller, am 15. Oktober 1993 die Verfügung über die Einsetzung der Studiengruppe Telefonüberwachung. Mit dieser Verfügung wurde die Studiengruppe beauftragt,

- die Frage der Veröffentlichung von nichtpublizierten Angaben über Abonnementsverhältnisse abzuklären;
- den Gesetzgebungsbedarf abzuklären, wie er sich aus der Stellungnahme des Bundesrates vom 17. Februar 1993 zum Bericht der GPK Nationalrat ergibt;
- einen Vernehmlassungsentwurf zu erarbeiten, der auf den Ergebnissen der Beratung in den Räten (93.3205, Motion der GPK Nationalrat vom 24. Mai 1993. Telefonüberwachung) beruht;
- abzuklären, ob der Revision des Schweizerischen Strafgesetzbuches sowie weiterer Bundesgesetze die Erarbeitung eines separaten Erlasses ("Bundesgesetz über die Einschränkung des Fernmeldegeheimnisses") vorzuziehen sei;

- abzuklären, ob den Kantonen von Bundesrechts wegen prozessuale Vorschriften gemacht werden sollen;
- zu prüfen, wieweit ein Bedürfnis für eine Regelung der Telefonüberwachung im Rahmen von Rechtshilfeverfahren besteht.

Laut Motion 93.3205 der GPK Nationalrat vom 24. Mai 1993, die vom Bundesrat am 14. Juni 1993 gutgeheissen wurde, wurden für die Revision Inhalte vorgegeben, wie die Schaffung eines restriktiven Deliktskataloges, dessen Ergänzung durch eine Generalklausel, der verbesserte Schutz von Drittpersonen, insbesondere solcher mit Zeugnisverweigerungsrecht, eine nachträgliche Wirksamkeitskontrolle und das Verfahren für die Anordnung von Observationen und den Einsatz von Verbindungsleuten.
Nach dem in der Verfügung vorgesehenen Zeitplan soll die Studiengruppe bis Ende März 1994 ihren Entwurf vorlegen. Wenn man bedenkt, dass erst Ende Oktober 1993 eine erste verwaltungsinterne Vorbereitungssitzung stattfand, muss man feststellen, dass der vorgegebene Zeitraum viel zu kurz und knapp bemessen ist, um eine derart wichtige und heikle Materie zufriedenstellend in den Griff zu bekommen.
Zwar werden durch die Revision des StGB für die Kantone und den Bund verbindliche Regelungen bezüglich Voraussetzungen und Verfahren der Telefonüberwachung geschaffen. Mit den ausgearbeiteten Entwürfen, die in gleicher Weise wie die Telefonüberwachung den Einsatz technischer Überwachungsmassnahmen regeln, besteht jedoch die Gefahr, dass der Kerngehalt von Grundrechten in unzulässigem Masse berührt wird, wenn nicht wenigstens in den Erläuterungen die zulässigen und unzulässigen Massnahmen - etwa im Zusammenhang mit dem Implementieren von Sendern auf dem Körper einer Person gegen deren Willen, der Verwanzung von Wohnungen, der Installation von versteckten Kameras in Wohnungen -aufgezählt werden.
Darüber hinaus muss eine befriedigende Regelung von Observation und V-Mann-Einsatz an die Hand genommen werden. Die weitere Entwicklung wird man abwarten müssen.

3.4. Datenschutz im Telekommunikationsbereich

Der Telekommunikationsbereich umfasst eine Unmenge von technischen Einrichtungen, die der Kommunikation von Menschen mit Mensch, Mensch mit Rechner, und Rechner mit Rechner dienen. Mit zunehmender Technisierung und Komplexität der Vernetzungen werden immer mehr Angebote, Konstellationen und Situationen deutlich, die aus Sicht des Datenschutzes problematisch sein können und überprüft werden müssen.

Im folgenden soll nur auf eine kleine Anzahl von Möglichkeiten, die im täglichen Leben aktuell sind, hingewiesen werden.

ISDN-Telefon

Von den PTT-Betrieben wird das ISDN-Telefon angeboten, das über eine Display-Anzeige verfügt. Über diese Anzeige kann der Angerufene erkennen, von welchem Anschluss (Telefonnummer) er angerufen wird, gleichgültig, ob er den Anruf entgegennimmt oder nicht. Die Anzeige des Anschlusses erfolgt, wenn der Anrufende ebenfalls am Swissnet angeschlossen ist, aber auch dann, wenn der Anrufende über ein analoges Gerät verfügt, die Verbindung aber über eine digitalisierte Zentrale der PTT-Betriebe weitergeleitet wird.

Der Anrufende, der selbst an Swissnet angeschlossen ist, weiss, dass die Anschlussnummer auf dem Empfangsapparat angezeigt wird. Der Anrufende aber, der einen analogen Telefonapparat benutzt, hat in der Regel keine Kenntnis davon, dass bei seinem möglichen Gesprächspartner die Anschlussnummer auf dem Display erscheint. Die Display-Anzeige mag für den Angerufenen viele Vorteile aufweisen, denen jedoch aus datenschutzrechtlicher Sicht einige, nicht von der Hand zu weisende Bedenken gegenüberstehen:

Für bestimmte Institutionen ist die Anonymität des Anrufers eine wesentliche Grundlage ihrer Arbeit. Dies gilt insbesondere für Behörden der inneren Sicherheit, Telefonseelsorge, AIDS- und Drogenberatung etc.

Der Angerufene kann die Rufnummern speichern und kommerziell auswerten.

Über das Display kann der Anrufer Dritten im Bereich des Angerufenen gegen seinen Willen offenbart werden.

Aus datenschutzrechtlicher Sicht muss durch technische Vorkehrungen sicher gestellt werden, dass die Rufnummern-Anzeige individuell durch den Anrufer unterdrückt werden kann. Zur Zeit besteht diese Möglichkeit noch nicht, ist aber nach Aussage der PTT-Betriebe auf 1995 zu erwarten.

Aufzeichnung von Telefongesprächen mittels firmeninterner Hauszentralen

Immer mehr Unternehmungen richten aus Kostengründen firmeninterne Computergesteuerte oder manuelle Hauszentralen ein, mittels derer die entweder nur abgehenden Telefongespräche der Mitarbeiter oder aber ab- und eingehende Telefongespräche aufgezeichnet werden.

Die Aufzeichnung von Teilnehmernummern kann durch die daraus möglichen Rückschlüsse auf telefonische Kontakte einer Person zu Persönlichkeitsverletzungen führen. Sie darf deshalb nur vorgenommen werden, wenn ein Rechtfertigungsgrund besteht. Ein solcher kann sich insbesondere für den Arbeitgeber aus betriebsinternen organisatorischen Gründen ergeben.

Damit eine Aufzeichnung von Teilnehmernummern innerhalb eines Betriebs vorgenommen werden darf, ist zusätzliche Voraussetzung, dass die dadurch betroffenen Personen über die vorgesehene Aufzeichnung umfassend informiert werden.

Im weiteren ist die Verhältnismässigkeit der Datenbearbeitung in Hinblick auf die jeweils aufgezeichneten Daten zu überprüfen:

Aus unserer Sicht mögen Aufzeichnungen in gewissem Rahmen verständlich und vertretbar sein. Unbedenklich ist im allgemeinen im Zusammenhang mit abgehenden Gesprächen das Festhalten von Datum, Apparatnummer des abgehenden Gespräches, Zeitdauer sowie angewählter Anschluss, soweit ein Rückschluss auf die angerufene Person unmöglich ist. Das kann angenommen werden, wenn die letzten 4 Ziffern des angerufenen Anschlusses unterdrückt werden. Von unserer Seite zu begrüssen wäre die Beschränkung auf die Angabe der Vorwahl, soweit das sinnvollerweise ausreicht.

Die vollständige Teilnehmernummer des Gesprächsempfängers darf hingegen nur aufgezeichnet werden, wenn die für die Sperrung notwendigen Massnahmen unzumutbar sind und der durch die Aufzeichnung der Teilnehmernummer entstandene Eingriff in die Persönlichkeit des Arbeitnehmers durch den Zweck des Eingriffs gerechtfertigt ist.

Eine Aufzeichnung der Teilnehmernummern des Arbeitnehmers und des Empfängers der im Betrieb geführten privaten Gespräche zu Kontrollzwecken stellt einen Eingriff in die Persönlichkeit des Arbeitnehmers dar. Sie darf nur erfolgen, wenn ihr eine Weisung des Arbeitgebers vorgegangen ist, wonach private Gespräche im Betrieb nicht oder nur in einem bestimmten Umfang erlaubt sind, und wenn es keine scho-

nendere Möglichkeit gibt, die Einhaltung dieser Weisung zu durchzusetzen (insbesondere die nur teilweise Aufzeichnung der Empfängernummer). In diesem Fall müssen die Arbeitnehmer die Möglichkeit haben, in dringenden Fällen oder während der Pausen von einem nicht überwachten Apparat aus zu telefonieren. Ausserdem sind die Arbeitnehmer über die vorgesehene Aufzeichnung umfassend zu informieren.
Eine Aufzeichnung solcher Daten nur bei beruflichen Gesprächen stellt einen weniger grossen Eingriff in die Privatsphäre der Arbeitnehmer dar. Dennoch sind sie über die Aufzeichnung vorgängig zu informieren. Ausserdem muss der Arbeitnehmer selbst die Möglichkeit haben, die Aufzeichnung der privaten Gespräche zu sperren.
Im Falle inhaltlicher Aufzeichnungen abgehender Gespräche sowie der Aufzeichnung eingehender Gespräche müssen die Gesprächsteilnehmer im voraus über die Aufzeichnung des Gespräches informiert werden. Unserer Meinung nach gilt das auch für sog. Schwedengespräche im Bank-Bereich (z. B. telefonische Börsenaufträge).
Es ist immer dafür zu sorgen, dass die aufgezeichneten Daten nur den für ihre Auswertung zuständigen Personen zugänglich sind. Dieser Personenkreis ist so klein wie möglich zu halten. Insbesondere ist zu verhindern, dass die Daten an einem allgemein zugänglichen Ort ausgedruckt werden.
Selbst wenn Aufzeichnungen nach den oben dargestellten Grundsätzen zulässig sind, müssen sie nach Ablauf einer bestimmten Zeitspanne vernichtet werden. Falls die Aufzeichnung zu Kontrollzwecken vorgenommen wird, hat der Arbeitgeber sie regelmässig zu überprüfen und die sich daraus ergebenden Massnahmen zu ergreifen und sodann die Aufzeichnungen zu vernichten.

Code und Passwörter im Zusammenhang/156-Nummer
Im Bereich der "erotischen" 156-Nummern wurden aus Gründen des Jugendschutzes Codes und Passwörter eingeführt. Das ist grundsätzlich sehr zu begrüssen. Es ist jedoch darauf hinzuweisen, dass die Frage des Codes bzw. Passwortes je nach technischer Ausgestaltung und Handhabung aus datenschutzrechtlicher Sicht zu Problemen führen kann.

4. Statistik

4.1. Das neue Bundesstatistikgesetz (BStatG)

Das neue Bundesstatistikgesetz hat die bisher bestehende Vielfalt der Anordnungskompetenzen in der Statistik einheitlich geregelt. Die dazugehörende Verordnung vom 30. Juni 1993 über die Durchführung von statistischen Erhebungen des Bundes zählt nun alle statistische Erhebungen in einem Anhang abschliessend auf und legt fest, von wem und wie welche Erhebung durchgeführt wird. In diese Rechtsgrundlage wurden nun auch die notwendigen datenschutzrechtlichen Bestimmungen eingegliedert. Insbesondere wurde die Eingriffsmöglichkeit des Staates in die Privatsphäre durch die Einholung von Auskünften gesetzlich geregelt und somit auch transparent gemacht.

Statistiken, die vom Bundesamt für Statistik aus den von Behörden und Privaten gelieferten Daten erstellt werden, erhalten immer grössere Bedeutung, da die amtliche Statistik in einer demokratischen Industriegesellschaft eine wichtige Voraussetzung für Informationen über Bevölkerung, Wirtschaft, Gesellschaft und Umwelt ist.
Wie alle staatliche Aufgaben muss auch die amtliche Statistik auf eine zeitgemässe Rechtsgrundlage abgestützt sein. Die bis anhin gültige Rechtsgrundlage (das Bundesstatistikgesetz vom 23. Juli 1870!) war sehr allgemein. Sie regelte lediglich die

Anordnungskompetenzen und die Kostenbeteiligung der Kantone sowie die Möglichkeit, die Kantone zur Mitarbeit bei der Erstellung der Bundesstatistik zu verpflichten. Das neue Bundesstatistikgesetz hat die bisher bestehende Vielfalt der Anordnungskompetenzen im statistischen Bereich einheitlich geregelt, indem die Befugnisse auf Verordnungsebene abschliessend geregelt wurden. Die Verordnung vom 30. Juni 1993 über die Durchführung von statistischen Erhebungen des Bundes zählt alle statistische Erhebungen in einem Anhang auf und legt fest, von wem und wie welche Erhebung durchgeführt wird.
In diese Rechtsgrundlage wurden nun auch die notwendigen datenschutzrechtlichen Bestimmungen eingegliedert. So wurde die Eingriffsmöglichkeit des Staates in die Privatsphäre durch die Einholung von Auskünften gesetzlich geregelt und damit auch transparenter gemacht. Auf diese Weise wurde Klarheit über die Rechte und Pflichten der befragten Personen bei der Erteilung von Auskünften für statistische Zwecke geschaffen.
Ausserdem ist im neuen Bundesstatistikgesetz ein Kapitel über den Datenschutz und die Datensicherheit integriert worden. Erwähnenswert ist noch, dass nach den neuen Bestimmungen Daten, die zu statistischen Zwecken erhoben wurden, *ausschliesslich für statistische Zwecke verwendet werden dürfen. Für andere administrative Zwecke dürfen sie nur dann verwendet werden,* wenn dies in einem Bundesgesetz ausdrücklich vorgesehen ist oder wenn die betroffene Person einer solcher Verwendung *schriftlich* zugestimmt hat.

4.2. Die Revision der Verordnung des Betriebs- und Unternehmensregisters (BUR)

Dieses Register dient aufgrund seiner Vollständigkeit seit längerer Zeit nicht nur Zwecken der Bundesstatistik. Ein genau bezeichneter Teil der BUR-Angaben darf von anderen Bundes- und kantonalen Stellen für Verwaltungsaufgaben verwendet werden. Deshalb wurde es notwendig, die Verwendung der Daten des Systems für nichtstatistische Zwecke bzw. für Verwaltungszwecke in einer gesetzlichen Grundlage festzulegen. Dieser Verwendungszweck der BUR-Daten wurde in Art. 10 Abs. 3 BStatG geregelt.

Nach der Betriebszählung im Jahre 1975 wurde das BUR-Register aufgebaut. Es enthält Namen und Adressen und weitere wichtige Merkmale, wie etwa die Anzahl der beschäftigten Personen, die Rechtsform, Datum des Eintrags im Handelsregister, das Grundkapital der Aktiengesellschaften aller in der Schweiz registrierten Betriebe und Unternehmen. Die revidierte Verordnung zählt die heute im Register gespeicherten Daten abschliessend auf.
Das BUR-Register diente ursprünglich als Adressgrundlage für Betriebszählungen und andere statistische Erhebungen des Bundes und war vorerst in der Verordnung vom 12. Dezenber 1988 über die Führung eines Betriebs- und Unternehmensregisters rechtlich verankert. Diese Rechtsgrundlage war jedoch bis Ende des Jahres 1993 zeitlich befristet. Aus diesem Grund drängte sich eine Revision der Verordnung auf.
Die Revision wurde aber auch notwendig, weil dieses Register dank seiner Vollständigkeit seit längerer Zeit nicht nur Zwecken der Bundesstatistik diente. Ein genau bezeichneter Teil der BUR-Angaben darf von anderen Bundes- und kantonalen Stellen für *Verwaltungsaufgaben* verwendet werden. Gemäss Art. 14 BStatG sind die zu statistischen Zwecken erhobene Daten nur dann für andere Zwecke zu verwenden, wenn ein Bundesgesetz eine andere Verwendung anordnet oder die betroffene Person schriftlich zustimmt.

Deshalb musste die Verwendung der BUR-Daten für nichtstatistische Zwecke bzw. für Verwaltungszwecke in einer gesetzlichen Grundlage festgelegt werden. Dies geschah in Art. 10 Abs. 3 BStatG. Zusätzlich wurde die revidierte Verordnung des BUR-Registers den Anforderungen des neuen BStatG und des neuen DSG angepasst. Aufgrund unserer Vorschläge wurden folgende Änderungen vorgenommen:

- Die Quellen sowie der Inhalt des BUR wurden neu festgelegt.
- Die Verwendung der Daten wurde detalliert geregelt.
- Die Erfassung, Mutation und Archivierung der Daten wurden in neuen Bestimungen festgelegt.
- Die Verbindungen zu anderen Informationssystemen und deren Zugriff auf die Daten wurden im Anhang der Verordnung abschliessend festgelegt.

4.3. Die Volkszählung 1990

Vor einiger Zeit wurde die statistische Auswertung der Erhebungsunterlagen abgeschlossen. Wie in Art. 25 der Verordnung vom 26. Oktober 1988 über die Eidgenössische Volkszählung vorgesehen, mussten diese Unterlagen datenschutzkonform vernichtet werden. Wir haben die vom Bundesamt für Statistik gewählte Aktenvernichtungsanlage in Bern besucht und uns über die Sicherheitsmassnahmen für die datenschutzkonforme Vernichtung der Erhebungsunterlagen ein Bild gemacht.

Im Jahre 1990 wurde die letzte eidgenössische Volkszählung durchgeführt. Nachdem vor einiger Zeit die statistische Auswertung der Erhebungsunterlagen abgeschlossen worden war, mussten diese Unterlagen, die auch besonders schützenswerte Personendaten enthielten, wie in Art. 25 der Verordnung vom 26. Oktober 1988 über die Eidgenössische Volkszählung vorgesehen, datenschutzkonform vernichtet werden.
Zuerst wurden die im Auftrag des Bundesamtes für Statistik beim Bundesamt für Informatik automatisiert gespeicherten Personenfragebogen der Volkszählung 1990 am 14. Mai 1993 definitiv gelöscht. Danach mussten die noch auf Papier vorhandenen Personendaten (Haushaltumschläge, Personenfragebogen, Zwischenmaterial, Gebäudefragebogen u.a.) datenschutzkonform vernichtet werden. Die zuständigen kantonalen Stellen hatten, wie vorgesehen, die Erhebungspapiere dem Bundesamt für Statistik abgeliefert, damit dieses die Vernichtung zentral vornnehmen konnte.
Wir hatten in der Folge die vom Bundesamt für Statistik gewählte Aktenvernichtungsanlage in Bern besucht und uns über die Sicherheitsmassnahmen zur datenschutzkonformen Vernichtung der Erhebungsunterlagen vergewissert.
Bis zum 2. November 1993 wurden in dieser Anlage die Erhebungsunterlagen effizient und ohne Probleme datenschutzkonform vernichtet. Vom Erhebungsmaterial der Volkszählung 1990 verbleiben noch die Gebäudefragebogen, deren Vernichtung voraussichtlich Mitte dieses Jahres erfolgen wird.

4.4. Volkzählung 2000

Damit das Bundesamt für Statistik für die nächste Volkszählung im Jahre 2000 die notwendigen Daten indirekt erheben kann, müssen die Datensammlungen der Kantone und der Gemeinden als vollständiger oder teilweiser Ersatz von Direkterhebungen herangezogen werden. Dem Bund fehlt zwar die verfassungsmässige Kompetenz, um neue Bundesvorschriften über die Führung von kommunalen und kantonalen Registern erlassen zu können. Eine indirekte Erhebung der Volkszählungsdaten muss jedoch die Grundsätze des Datenschutzes respektieren. Deshalb muss eine Indirekter-

hebung bzw. eine Registerzählung von Massnahmen begleitet werden, welche die Transparenz der Datenbearbeitung garantieren. Ausserdem müssen die notwendigen Vorkehrungen getroffen werden, damit die durch Verbindung der kantonalen Register ermittelten Daten nur für Volkszählungszwecke verwendet werden und nicht für andere Verwaltungsaufgaben des Bundes und der Kantone genutzt werden.

Nach dem Inkrafttreten des neuen Bundesstatistikgesetzes besteht nur eine einzige Ausnahme vom Prinzip, einzelne Statistiken auf Verordnungsstufe zu regeln. Diese Ausnahme betrifft die Volkszählung. Das Volkszählungsgesetz vom 3. Februar 1860 das im Jahr 1988 revidiert wurde, sieht die 10-jährige Periodizität der Zählung vor und enthält Bestimmungen über das Durchführungsjahr, die Aufgaben- und Kostenteilung zwischen Bund und Kantonen und über den Datenschutz. Neben diesen spezifischen Regelungen des Volkszählungsgesetzes finden auf die Volkszählung auch die Bestimmungen des BStatG Anwendung. Man wollte aber das Volkszählungsgesetz nicht in das neue BStatG integrieren.

Gemäss Art. 4 BStatG soll der Bund, soweit er über die notwendigen Daten verfügt, auf besondere Erhebungen bei der Bevölkerung verzichten, um den betroffenen Personen wiederholte Befragungen zu ersparen.
Ein zweites Instrument zur Entlastung der Befragten ist die sogennante Indirekterhebung, d.h. die Beschaffung der Daten über Dritte aus Datensammlungen der Kantone und der Gemeinden oder bei Organen, die dem BStatG nicht unterstellt sind, aber Bundesrecht vollziehen.
Das Bundesamt für Statistik möchte nun für die nächste Volkszählung im Jahre 2000 die notwendigen Daten zum Teil indirekt erheben. Das heisst, dass Datensammlungen der Kantone und der Gemeinden als vollständiger oder teilweiser Ersatz von Direkterhebungen herangezogen werden müssen. Für die indirekte Erhebung der für die Volkszählung notwendigen Daten müssten aber die Vorschriften über die Führung von Einwohnerregistern und sonstigen kantonalen Registern geändert werden, um eine zweckmässige Nutzung dieser Daten für statistische Zwecke zu erlauben. Um die Datenübernahme rationell zu gestalten, müssten ausserdem neue Rechtsvorschriften über die automatisierte Verbindung dieser Register erlassen werden. Mit anderen Worten müssten *neue Bundesvorschriften* über die Führung von kommunalen und kantonalen Registern erlassen werden, um diese Register zu harmonisieren.
Die Führung der obenerwähnten Register liegt jedoch im Kompetenzbereich der Kantone, der Gemeinden und deren Organe. Bundesorgane können aber im Hoheitsbereich der Kantone nur dann gesetzgeberisch tätig werden, wenn in der Verfassung eine solche Kompetenz ausdrücklich vorgesehen ist. Eine solche verfassungsmässige Grundlage fehlt jedoch und müsste durch eine Verfassungsänderung geschaffen werden.

Schliesslich ist zu erwähnen, dass eine indirekte Erhebung der Volkszählungsdaten die allgemeinen Grundsätze des Datenschutzes, insbesondere das Prinzip der Verhältnismässigkeit, respektieren muss. Obwohl die Notwendigkeit und Zweckmässigkeit von Indirekterhebungen unbestritten ist, muss die Bearbeitung von Personendaten bei der Volkszählung transparent sein. Denn bei der Indirekterhebung von Daten können traditionelle Informationsschranken beseitigt werden, die den einzelnen Bürgerinnen und Bürgern erlauben, selbst zu bestimmen, wie sie sich vor den Behörden darstellen wollen, und ihnen ermöglichen, die erhobenen Daten zu überprüfen und gegebenenfalls unrichtige Daten zu berichtigen. Bei einer direkten Erhebung ist die Gefahr geringer, dass unrichtige Daten ohne ihr Wissen bearbeitet werden.

Deshalb muss eine Indirekterhebung bzw. eine Zählung mittels Registern von solchen Massnahmen begleitet werden, welche die Transparenz der Datenbearbeitung garantieren. Dazu gehört namentlich, dass die betroffenen Personen über die Bearbeitung ihrer Daten im voraus informiert werden.
Weiter ist zu beachten, dass die Vernetzung der kantonalen Register nicht dazu dienen darf, dass die Daten über den Zweck ihrer Beschaffung (Statistik, Volkszählung) hinaus für andere Zwecke bearbeitet werden (Zweckentfremdung). Deshalb müssen die notwendigen Vorkehrungen getroffen werden, damit die durch die Verbindung der kantonalen Register ermittelten Daten nur für Volkszählungszwecke verwendet werden und *nicht für andere Verwaltungsaufgaben des Bundes und der Kantone genutzt werden.*

Aus diesen Gründen müssen die durch die Vernetzung verschiedener Register erhobenen Daten den betroffenen Personen bekannt gemacht werden, damit sie die ihre Person betreffenden Daten wie bei einer direkten Vollerhebung kennen. Nur wenn die Bürgerinnen und Bürger wissen, welche Daten über sie bearbeitet werden, können sie von den im Datenschutzgesetz statuierten Rechte (Auskunftsrecht, Berichtigung der Daten u.a.) Gebrauch machen.

5. Gesundheitswesen

Die Daten über den Gesundheitszustand einer Person geniessen einen besonders starken Rechtsschutz, vor allem wenn sie durch Bundesorgane bearbeitet werden. Im folgenden möchten wir beispielhaft auf zwei Fragestellungen eingehen, bezüglich derer man sich an uns gewandt hat: auf die Verordnung zu HIV-Studien und auf die Einführung eines Programms zur kontrollierten Drogenabgabe im Rahmen einer Auswertung von Projekten zur Verhütung von Rauschgiftsucht. Information (Transparenz), Einwilligung der betroffenen Personen, Respektierung ihres Willens und schnellstmögliche Anonymisierung ihrer Daten - dies sind einige Eckpfeiler des Datenschutzes. Die Wahrung dieser Grundsätze bildet unter anderem das Fundament für das Vertrauen, das ein unentbehrliches Element für den guten Verlauf jeglicher Studie darstellt, die im Bereich des Gesundheitswesens durchgeführt wird.

Die Daten über den Gesundheitszustand einer Person werden laut Bundesgesetz über den Datenschutz (DSG) als besonders schützenswerte Daten angesehen. Der Gesetzgeber hat sie deshalb einem besonderen Rechtsschutz unterstellt. In bezug auf die beiden unten darzustellenden Problembereiche hat man uns um Stellungnahme gebeten. Die Studien über AIDS werden bereits durchgeführt, während sich die Studien im Zusammenhang mit der kontrollierten Drogenabgabe noch in Planung befinden und erst in Form eines Projekts vorliegen.

AIDS
Diese Krankheit stellt vor allem wegen der unbegründeten Ängste, die diese Krankheit in der Bevölkerung auslöst, das heikelste Thema dar, das man sich vorstellen kann. Arbeitgeber und Versicherer können sich ebenfalls dazu hinreissen lassen, nachteilige Massnahmen für die Personen zu ergreifen, die Virusträger oder bereits krank sind. Aus diesem Grund haben wir zu grösster Vorsicht aufgerufen, als das Bundesamt für Gesundheitswesen uns über sein Projekt in Kenntnis setzte, in unserem Land Studien über die Prävalenz und die Inzidenz des Immundefekts AIDS (HIV)

durchzuführen. Unsere Mitarbeit hat zur Verabschiedung einer Verordnung des Bundesrates geführt, die am 1. August 1993 in Kraft trat:
"Verordnung vom 30. Juni 1993 über epidemiologische Studien zur Erfassung von Daten über den Human Immunodeficiency Virus (Verordnung über HIV-Studien)"

Im Hinblick auf *anonyme Studien* sieht die Verordnung insbesondere vor, die für die Entnahme von Proben zuständigen Stellen zu verpflichten, die Teilnehmer klar und verständlich aufzuklären. Wenn der Spender sich nämlich nicht offiziell gegen die Suche von HIV-Antikörpern in der ihm entnommenen Probe wehrt, wird seine diesbezügliche Zustimmung automatisch vorausgesetzt. Im Falle der Verweigerung der Teilnahme muss der Wille des Spenders respektiert werden. Eine allgemeine Verpflichtung zur Aufklärung der Öffentlichkeit ist ebenfalls vorgesehen, wenn eine anonyme Studie durchgeführt werden soll. Ausserdem dürfen Proben nicht ausschliesslich zum Zweck von anonymen HIV-Studien entnommen werden. Und schliesslich müssen die Proben in den Entnahmezentren anonymisiert werden und dürfen nur in dieser Form an die Analyselabors weitergereicht werden.

Für Studien mit Hilfe von Freiwilligen (unter Angabe ihres Namens) sind die Information und die Zustimmung der getesteten Personen ebenfalls erforderlich. Die Testpersonen müssen im übrigen darauf hingewiesen werden, dass sie ihre Zustimmung verweigern oder jederzeit zurückziehen können. Die gesammelten Daten gelangen nicht in die Teststellen, sondern werden direkt an die für die Studie verantwortliche Zentralstelle gesandt. Der Studienbericht muss so abgefasst werden, dass die Testteilnehmer nicht identifiziert werden können. Die Verordnung sieht schliesslich Normen zur Schweigepflicht, zur Aufbewahrung der Daten und zum Auskunftsrecht vor. Ebenso ermöglicht sie den Testpersonen, auf eine Vermittlung durch den Studienbeauftragten zurückzugreifen.

Diese zur Sicherung eines optimalen Persönlichkeitschutzes der Versuchsteilnehmer ergriffenen Massnahmen zielen ebenfalls darauf ab, das Vertrauen der Bevölkerung beziehungsweise der "Risikogruppen" zu gewinnen. Dieses Ziel soll vor allem auch durch eine grösstmögliche Transparenz (Information) und die Gewährleistung einer gewissen Entscheidungsfreiheit (Einwilligung der Spender) erreicht werden.

Kontrollierte Drogenabgabe
Eine am 15. November 1992 in Kraft getretene Verordnung des Bundesrates mit Wirkung bis zum 31. Dezember 1996 legt den Rahmen für eine Beurteilung von Massnahmen fest, die zur Verhütung der Drogensucht, zur Verbesserung des Gesundheitszustands und der Lebensbedingungen der Drogenabhängigen, zur Wiedereingliederung in die Gesellschaft und zur Eindämmung der Beschaffungskriminalität getroffen worden sind:
"Verordnung vom 21. Oktober 1992 über die Förderung der wissenschaftlichen Begleitforschung zur Drogenprävention und Verbesserung der Lebensbedingungen von Drogenabhängigen"

Zu diesem Zweck sind Versuche mit Gruppen von je 50 Drogenabhängigen vorgesehen, die unter Aufsicht des Bundesamts für Gesundheitswesen durchgeführt werden sollen. Im Zusammenhang mit diesen Versuchen ist eine kontrollierte Abgabe von Drogen wie Heroin, Morphium oder Methadon geplant. Gegenwärtig ist man dabei, einen Gesamtversuchsplan in bezug auf die Studie auszuarbeiten, der auch Durchführungsbestimmungen enthält. Ausserdem wird derzeit insbesondere ein Entwurf zu

einer "Einverständniserklärung" erstellt, die jeder Versuchsteilnehmer unterzeichnen muss. Im Januar 1994 hat uns das Bundesamt für Gesundheitswesen diese beiden Schriftstücke zur Stellungnahme vorgelegt.

Wir haben dem Bundesamt für Gesundheitswesen nahelegt, alles zu veranlassen, damit die Auswertung in einem Klima des Vertrauens stattfinden kann. Ein Vertrauensklima ist unserer Ansicht die Bedingung sine qua non für die Erzielung von zufriedenstellenden Resultaten. Diesem Ziel folgend, haben wir folgende Punkte hervorgehoben:

- sämtliche Bearbeitungen von Personendaten, die im Rahmen der Auswertung stattfinden, werden unabhängig von der Frage, welches Organ die Datenbearbeitungen vornimmt, dem Bundesgesetz über den Datenschutz unterstellt;

- die für die Versuchsdurchführung verantwortlichen Personen sind verpflichtet, darauf zu achten, dass die Testpersonen ihre Zustimmung zur Teilnahme an den Versuchen trotz ihres Abhängigkeitszustands frei und ausdrücklich geben können;

- wenn eine Zustimmung gegeben wurde, so bezieht sie sich nur auf eine zeitlich begrenzte Dauer und auf einen im voraus genau festgelegten Inhalt. Damit eine Eingrenzung in bezug auf den Inhalt der gegebenen Zustimmung sichergestellt werden kann, muss die "Einverständniserklärung" so abgefasst werden, dass die betroffene Person nicht gezwungen ist, eine globale Zustimmung zu geben. Sie muss die Möglichkeit haben, zu jeder vorgesehenen Massnahme ihre Zustimmung im einzelnen zu geben, je nachdem, ob man sie zum Beispiel fragt, ob sie einverstanden ist, sich einem HIV-Test zu unterziehen, dass jeweils am Anfang und am Ende des Versuchs ein Auszug aus ihrem Strafregister angefordert wird oder dass die Ärzte oder deren Hilfskräfte von der Schweigepflicht entbunden werden;

- die für die Untersuchung verantwortlichen Organe sind verpflichtet, jegliche Weitergabe von Daten der Testteilnehmer an Dritte, vor allem an Verwaltungsbehörden oder an die Polizei, zu verhindern. Dies gilt unabhängig von der Frage, ob die betroffenen Personen ihre Einwilligung zur Datenweitergabe gegeben haben oder nicht. Einerseits sprechen die allgemeinen Grundsätze des Datenschutzes gegen eine Bekanntgabe der Daten (Grundsätze der Verhältnismässigkeit und der Zweckmässigkeit). Andererseits könnte der Verlauf der Auswertung unter einer Datenbekanntgabe leiden.

In Anbetracht all dieser Faktoren haben wir dem Bundesamt für Gesundheitswesen geraten, den Gesamtversuchsplan und folglich die "Einverständniserklärung" dementsprechend noch einmal zu überprüfen.

6. Genetik

Nach Inkrafttreten von Art. 24novies der Bundesverfassung (BV) wurden wir aufgefordert, uns in Anbetracht des jetzigen Gesetzesstands über die Zulässigkeit des Rückgriffs auf die DNS-Analyse (Methode Jeffrey) zur Feststellung oder zum Ausschluss der Vaterschaft zu äussern. Wir sind der Ansicht, dass die Methode Jeffrey derzeit die geeignetste ist, da sie die allgemeinen Grundsätze des Datenschutzes respektiert, insbesondere die Grundsätze der Verhältnismässigkeit und der Richtigkeit.
Was die Bearbeitung von entnommenen Proben insbesondere in der Humanforschung anbelangt, so haben wir die Ansicht vertreten, dass sie angesichts der aus den Proben ablesbaren individuellen Eigenheiten die Ausarbeitung von spezifischen Datenschutznormen erforderlich macht. Damit die festzulegenden Normen für alle Teile zufriedenstellend ausfallen, haben wir deutlich gemacht, wie wichtig es für uns ist, in die derzeit laufenden Reflexionsarbeiten miteinbezogen zu werden.

Am 17. Mai 1992 trat Art. 24novies der Bundesverfassung zur Genetik und Fortpflanzungshilfe in Kraft. Die in Art. 24novies enthaltenen Bestimmungen zielen darauf ab, den Menschen und seine Umwelt gegen Missbräuche der Fortpflanzungs- und Gentechnologie zu schützen. Art. 24novies berechtigt den Bund, Vorschriften zur Sicherung des Persönlichkeitsschutzes zu erlassen. Der Artikel sieht unter anderem vor, dass "das Erbgut einer Person nur mit ihrer Zustimmung oder aufgrund gesetzlicher Anordnung untersucht, registriert oder offenbart werden darf". Im Herbst 1992 begann das Bundesamt für Justiz mit seinen Untersuchungen. Es hat mit uns Kontakt aufgenommen und uns um Stellungnahme in bezug auf die Analyse des genetischen Fingerabdrucks de lege lata (DNS-Analyse) in der Vaterschaftsforschung und die Auswirkungen von Art. 24novies BV auf die bestehenden rechtlichen Forschungsprinzipien gebeten. Wir haben uns folgendermassen geäussert:

DNS-Analyse und Vaterschaftsforschung: Im Gegensatz zur Blutanalyse, die noch viele andere Informationen als diejenigen, die zum positiven oder negativen Nachweis der Vaterschaft nötig gewesen wären, preisgab, ist die sogenannte "Jeffrey-Methode" weniger "geschwätzig". In der Tat ist es nach dieser Methode für die Vaterschaftsforschung nicht nötig, die fünf Prozent der DNS zu untersuchen, die Code-Sequenzen (Erbfaktoren) enthalten. Es genügt, in den DNS-Abschnitten ohne Code-Sequenzen zu arbeiten, die auf ganz bestimmten Teilstücken der Chromosen angelegt sind. Dank der Längenunterschiede, die zwischen diesen Segmenten bestehen (Längenpolymorphie), ist eine Individualisierung möglich. Es scheint ausserdem, dass diese Methode für den Nachweis der Nichtvaterschaft zu hundert Prozent sicher ist. Zur (positiven) Feststellung der Vaterschaft ist der Zuverlässigkeitsgrad überdies höher als die vom Bundesgericht geforderten 99,8 Prozent. Wir haben insofern den Schluss gezogen, dass die Methode Jeffrey vom Standpunkt der allgemeinen Datenschutzgrundsätze und insbesondere von den Grundsätzen der Verhältnismässigkeit und der Richtigkeit her die bis zum heutigen Tage geeignetste Analysemethode darstellt.

A*rt. 24novies BV und Humanforschung:* Art. 321bis des Strafgesetzbuchs (StGB) ist zum gleichen Zeitpunkt wie das DSG in Kraft getreten. Dieser Artikel sieht vor allem die Bildung einer "Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung" (nachfolgend "Kommission" genannt) vor. Diese Kommission hat im Januar 1994 ihre Arbeit aufgenommen. Wenn die Bedingungen dieser strafrechtlichen Bestimmung (Art. 321bis) erfüllt werden, hat die Kommission die Entscheidungskompetenz über die Erteilung oder Nichterteilung der Erlaubnis, Personenda-

ten zu Forschungszwecken in den Bereichen der Medizin und des Gesundheitswesens bekanntzugeben. Obwohl Art. 321bis StGB sowohl auf den privaten als auch auf den öffentlichen Bereich und sowohl auf kantonaler Ebene als auch auf Bundesebene anwendbar ist, haben wir die Ansicht vertreten, dass er nicht ausreicht, um alle Forschungssituationen abzudecken, von denen in Art. 24novies BV die Rede ist. Andererseits haben wir daran erinnert, dass der Anwendungsbereich der Datenschutznormen mit Ausnahme der Bestimmungen zur Datenbeschaffung nicht ohne weiteres auf die zu genetischen Forschungszwecken entnommenen Proben ausgeweitet werden kann. Zum einen stellt die entnommene Probe in gewisser Hinsicht eine unerschöpfliche Informationsquelle dar, über die der Einzelne praktisch keinen Überblick mehr hat. Zum anderen kann sie nicht nur Informationen über die betroffene Person, sondern auch über deren Vorfahren und Nachkommen liefern. Aus diesem Grund ist es notwendig, spezifische Normen zur Bearbeitung von entnommenen Proben - einschliesslich Normen zur Aufbewahrung, Weitergabe und Vernichtung der Proben - zu erlassen. Hierfür bildet Art. 24novies BV in bezug auf die zu genetischen Forschungszwecken entnommenen Proben die Verfassungsgrundlage. Wir haben sowohl das Bundesamt für Justiz als auch das Eidgenössische Departement des Innern auf die Notwendigkeit aufmerksam gemacht, uns an den Tätigkeiten sämtlicher auf der Grundlage von Art. 24novies BV gegründeten Arbeitsgruppen zu beteiligen, sofern es um Personendaten oder menschliche Probeentnahmen geht. Nur so können die Anforderungen, die der Datenschutz an uns stellt, auf harmonische Weise in neue Normen zur Genetik und Fortpflanzungshilfe einfliessen.
Wir stehen gegenwärtig erst am Anfang unserer Ermittlungen im Zusammenhang mit den Datenschutzfragen, die durch die Genetik aufgeworfen werden und sich in so verschiedenen Bereichen wie der Forschung, der Sozial- und Privatversicherungen und des Arbeitsrechts stellen. Anstatt direkt in ein derartig heikles Gebiet einzugreifen, sollte man erst einmal Behutsamkeit und Umsicht walten lassen. Insofern können wir an dieser Stelle nur wiederholen, dass praktikable Lösungen, die gleichzeitig die Persönlichkeitsrechte wahren, nur gefunden werden können, wenn wir von Anfang an bei den auf diesem Gebiet zu leistenden Reflexionsarbeiten mitwirken können.

7. Versicherungswesen

7.1 Sozialversicherungen

Genau wie im Gesundheitswesen greift man auch im Versicherungsbereich auf die Bearbeitung von besonders schützenswerten Daten und Persönlichkeitsprofilen zurück. Für diese Art von Daten enthält das DSG erhöhte Schutznormen, so wie dies der "Bericht Jaggi" von 1984 gefordert hatte. Auf dem Gebiet der Sozialversicherungen müssen noch zahlreiche Lücken geschlossen werden, zumal das Problem der Bekanntgabe medizinischer Daten, vor allem an die Krankenkassen, bis heute nicht geregelt ist (vgl. beispielsweise die neue Analysenliste mit Tarif, die am 1. Januar 1994 in Kraft getreten ist). Im Gegensatz zu den Sozialversicherungen, die meistens mit spezifischen materiellen Datenschutznormen ausgestattet sind, untersteht der Privatversicherungssektor gänzlich den Bestimmungen des DSG, welche auf den Privatsektor anwendbar sind. Insbesondere im Zusammenhang mit der Anmeldepflicht von Datensammlungen haben wir nach Inkrafttreten des Gesetzes erste Kontakte zu der einen oder anderen Versicherungsgesellschaft hergestellt. Auf europäischer Ebene hat der Europarat eine Arbeitsgruppe eingerichtet, in der wir mitarbeiten. Diese hat den Auf-

trag, einen Empfehlungsentwurf zum Schutze von Personendaten auszuarbeiten, die zu Zwecken der Privatversicherung gesammelt und bearbeitet werden.

Bereits im Februar 1984 zeichnete eine vom Bundesamt für Justiz eingesetzte Kommission in ihrem Bericht mit dem Titel "Datenschutz im Medizinalbereich" (Bericht Jaggi) ein eher düsteres Bild in bezug auf das Problem der Bearbeitung (und insbesondere der Bekanntgabe) von medizinischen Daten vor allem bei Sozial- und Privatversicherungen. Der Bericht kam unter anderem zu dem Schluss, dass es unbedingt notwendig sei, derartige Daten besser zu schützen. Diese Forderung wird durch das DSG erfüllt.
Einerseits sind die Tätigkeiten der Sozialversicherungen im Prinzip durch spezifische materielle Datenschutznormen geregelt. Andererseits bereitet der Datenschutz - wenn das DSG zur Anwendung kommt - vor allem den Pensions- und Verbandsausgleichskassen eine Reihe von Problemen, so z. B. in bezug auf die Frage der Anmeldung von Datensammlungen beim Datenschutzbeauftragten. Der folgende Abschnitt enthält unsere Antwort auf diese Problematik. Auf die neue Analysenliste mit Tarif, deren Herausgabe Gegenstand einer am 1. Januar 1994 in Kraft getretenen Verordnung des Eidgenössische Departements des Innern ist, wird im darauffolgenden Abschnitt eingegangen. Anhand dieser Liste wird deutlich, dass die meisten im Bericht Jaggi hervorgehobenen Mängel bezüglich des Datenschutzes noch bis heute nicht ausgeräumt sind, vor allem was das Problem der Weitergabe von medizinischen Daten angeht. Mit einigen Überlegungen hinsichtlich der Privatversicherungen soll dieser kurze Überblick abgeschlossen werden.

Auf die kantonalen Ausgleichskassen und die Verbandsausgleichskassen anwendbares Datenschutzrecht - betrachtet vor allem unter dem Gesichtspunkt der Anmeldepflicht von Datensammlungen

Um den kantonalen Ausgleichskassen und den Verbandsausgleichskassen in bezug auf die Anmeldung von Datensammlungen jeden Zweifel zu nehmen, haben wir ihnen gegenüber folgendes präzisiert:
Wenn eine Ausgleichskasse in Anwendung des kantonalen Rechts - beispielsweise zum Zwecke des Familienausgleichs - Datensammlungen mit Personendaten führt, muss sie diese Datensammlungen bei den kantonalen Datenschutzbehörden anmelden, sofern der jeweilige Kanton über ein derartiges Gesetz verfügt.
Falls für eine Kasse (wie zum Beispiel für die AHV) Bundesrecht gilt, so hat sie die von ihr geführten Datensammlungen bei den kantonalen Datenschutzbehörden anzumelden, sofern in dem entsprechenden Kanton ein Datenschutzgesetz besteht. In den Kantonen, die noch nicht über ein solches Gesetz verfügen, wird die Anmeldung beim kantonalen Kontrollorgan vorgenommen, das laut DSG von den Kantonen als solches geschaffen werden muss.
Was die Verbandsausgleichskasse als Privatperson (Urlaubsfonds) angeht, so untersteht sie der Anmeldepflicht nur in den Fällen, die vom DSG vorgesehen sind. Bezüglich der Datensammlungen, die die Verbandsausgleichskasse in ihrer Eigenschaft als Bundesorgan führt (obligatorische berufliche Vorsorge, BVG), ist die Verbandsausgleichskasse wie alle anderen Bundesorgane stets zur Anmeldung verpflichtet.
Die neue Analyseliste mit Tarif (im folgenden "Liste" genannt)

Über das Bestehen dieser Liste wurden wir durch die Verbindung der Schweizer Ärzte (FMH) und die Schweizerische Patienten-Organisation (SPO) in Kenntnis gesetzt.

Die FMH und die SPO haben uns auf die neuen Datenschutzprobleme aufmerksam gemacht, die durch das Inkrafttreten der überarbeiteten Liste entstehen könnten.
Da wir nicht im Besitz des Listentextes waren und uns die Art des Gebrauchs der Liste durch die Analyselabors unbekannt war, haben wir dem Bundesamt für Sozialversicherung am 15. Dezember 1993 eine *Empfehlung* unterbreitet, in der wir nahelegten, das Datum des Inkrafttretens der Liste solange zu verschieben, bis wir die Liste unter dem Blickwinkel des Datenschutzes untersucht hätten. Angesichts der Dringlichkeit der Situation haben wir dem Präsidenten der Eidgenössischen Datenschutzkommission am 20. Dezember 1993 einen *Antrag für provisorische Massnahmen* vorgelegt, in dem wir ihn darum baten, das Datum des Inkrafttretens der Liste zu verschieben. Am 23. Dezember 1993 wurden wir vom Generalsekretär des Eidgenössischen Departements des Innern eingeladen. Vertreter des Bundesamts für Sozialversicherung versicherten uns, dass es technisch schwer möglich wäre, das Inkrafttreten der Liste hinauszuschieben, da sämtliche Analyselabors ihre Informatiksysteme im Hinblick auf die Einführung der neuen Liste bereits umgestellt hätten (diese Information erwies sich im nachhinein als unrichtig, zumindest was die meisten privaten Labors anbelangte). Dass es in bezug auf die Liste Datenschutzprobleme gab, hat man unter anderem eingesehen. Das Bundesamt für Sozialversicherung erhielt den Auftrag, eine Arbeitsgruppe ins Leben zu rufen. Diese soll die Liste zunächst noch einmal überprüfen und sie den Erfordernissen des Datenschutzes anpassen. Der zweite Aufgabenbereich der Arbeitsgruppe besteht darin, die Gesamtproblematik des Informationsflusses in die Hände von Versicherungskassen zu untersuchen. Am 24. Dezember 1993 haben private Analyselabors - unterstützt von öffentlichen Labors - beim Bundesrat *Beschwerde* eingereicht beziehungsweise *Anzeige* erstattet. Sie forderten die provisorische Aufhebung des Inkrafttretens der Liste. Wie dieses Verfahren ausging, ist uns bis heute nicht bekannt. Am 17. Januar 1994 lehnte der Präsident der Eidgenössischen Datenschutzkommission (ohne formellen Entscheid des Eidgenössischen Departements des Innern) die von der FMH und der SPO eingereichten Beschwerden ab. Er sprach der FMH die Berechtigung ab, eine Beschwerde einzureichen und erachtete vor allem die von der SPO vorgebrachten Elemente als nicht hinreichend geeignet, eine Aufhebung der Liste zu rechtfertigen. Am 25. Januar 1994 haben wir zu einem Entscheidsentwurf bezüglich der Einrichtung der obengenannten Arbeitsgruppe Stellung bezogen. Seitdem warten wir auf einen neuen Vorschlag. Am 23. Februar 1994 führte uns der Datenschutzbeauftragte des Kantons Bern seinerseits die Problematik im Zusammenhang mit der neuen Liste vor Augen.

Einige Probleme im Zusammenhang mit der Liste: Ausgehend von den Informationen, die aus verschiedenen beschwerdeführenden Kreisen an unsere Adresse gelangt sind, haben wir festgestellt, dass die neue Liste sowohl vom Standpunkt des Datenschutzes her als auch aus der Perspektive der ärztlichen Schweigepflicht neue Schwierigkeiten mit sich bringt, von denen wir hier nur die offensichtlichsten erwähnen möchten:

- Die neue Liste sieht die Erwähnung der analysierten Probe und des Analyseergebnisses auf der Rechnung vor;
- Nach der neuen Liste sind kleinste Detailabrechnungen vorgesehen, auch in bezug auf so heikle Tests wie Tests zur Feststellung von AIDS, Hepatitis B oder krebsartigen Tumoren;
- Der Empfänger der Rechnung ist über das positive oder negative Resultat der jeweiligen Analyse informiert, da die Anzahl der in Rechnung gestellten Punkte vom Resultat abhängt.

In Anbetracht dieser Tatsachen sind die Ärzte nicht mehr in der Lage, ihren Patienten ein Minimum an ärztlicher Schweigepflicht zu garantieren, und die Analyselabors, die auf die neue Liste zurückgreifen müssen, brechen ihre im DSG verankerte Schweigepflicht.
Eine Weitergabe von derart detaillierten Informationen an die Krankenkassen ist schlussendlich problematisch. Bei den meisten Kassen sind die Analyseresultate für das Verwaltungspersonal ohne weiteres zugänglich. Es fehlt an einem "Filter" durch den Vertrauensarzt. Wenn es sich um eine kleine Filiale mit ein oder zwei Angestellten handelt, die die Versicherten persönlich kennen, besteht das Risiko von Indiskretionen oder einer Anhäufung von nicht miteinander zu vereinbarenden Funktionen.

7.2. Privatversicherungen

In den letzten Jahren weht bei den Privatversicherungen in der Schweiz ein Wind der Dereglementierung, durch die die entsprechende Gesetzgebung "eurokompatibel" gemacht werden soll.
Diese Lockerung der staatlichen Aufsicht hat hingegen keine direkten Auswirkungen auf den Persönlichkeitsschutz der Versicherten, da der Bereich der Privatversicherungen seit 1. Juli 1993 gänzlich durch das DSG geregelt wird. Auf nationaler Ebene haben wir seit Inkrafttreten des DSG mit der einen oder anderen grösseren Versicherungsgesellschaft erste Kontakte geknüpft, hauptsächlich im Hinblick auf deren Anmeldepflicht von Datensammlungen. Was die europäische Ebene anbelangt, so haben wir im Februar 1994 an der ersten Sitzung der Arbeitsgruppe 14 teilgenommen. Die Arbeitsgruppe 14 ist damit betraut worden, einen Empfehlungsentwurf des Europarats zum Schutze von personenbezogenen Daten auszuarbeiten, die zu Zwecken der Privatversicherung gesammelt und bearbeitet werden.

8. Archivwesen

8.1. Ein neues Archivgesetz

Aufgrund der Entwicklungen in den letzten Jahren auf nationaler und internationaler, vor allen Dingen europäischer Ebene entstand das Bedürfnis nach einer Neuregelung des Archivbereichs durch ein Gesetz. Diese Neuregelung des Archivbereichs auf Gesetzesebene wurde vor allen Dingen aufgrund von Durchsetzungsproblemen der Abgabepflicht im Zusammenhang mit personenbezogenen, sensiblen und elektronisch gespeicherten Informationen erforderlich. Darüberhinaus statuiert das DSG, dass für das Bearbeiten von besonders schützenswerten Personendaten und Persönlichkeitsprofilen durch Bundesorgane ein formelles Gesetz als Rechtsgrundlage vorhanden sein muss. Aus diesem Grund nehmen wir an einer interdepartementalen Arbeitsgruppe zur Schaffung eines neuen Archivgesetzes teil.

Bundesorgane müssen Personendaten, die sie nicht mehr benötigen, anonymisieren oder vernichten, soweit die Daten nicht Beweis- oder Sicherungszwecken dienen oder dem Bundesarchiv abzuliefern sind.
Nach dem zur Zeit noch geltenden Reglement für das Bundesarchiv vom 15. Juli 1966 sind die Mitglieder, Beamten und Angestellten der Bundesversammlung und deren Kommissionen, des Bundesrates sowie von Amtsstellen und Anstalten der allgemeinen Bundesverwaltung, der Verwaltungs-, Experten- und sonstigen ausserpar-

lamentarischen Kommissionen, deren Sekretariat von der allgemeinen Bundesverwaltung besorgt wird, sowie der selbständigen Anstalten des Bundes, die sich auflösen oder die wichtige Akten ausscheiden wollen, verpflichtet, ihre offiziellen Akten dem Bundesarchiv abzuliefern.
Darüberhinaus verwahrt das Bundesarchiv hinterlegte, geschenkte, hinterlassene oder sonstwie erworbene Aktenbestände zur Geschichte der Schweiz seit 1798 sowie verschiedene Sammlungen von Abschriften, Photokopien, Mikrofilmen, Registern und Inventaren zur Schweizergeschichte aus anderen Archiven und Bibliotheken.
Das führt dazu, dass im Bundesarchiv Unmengen von Personendaten, besonders schützenswerten Personendaten und Persönlichkeitsprofilen lagern.
Neben dem Bedürfnis nach einer Neuregelung im Rahmen der Beratung und Betreuung der Schriftgut- und Informationsverwaltung der Bundesorgane sowie der Archivierungs- und Abgabepflichten zeigte sich die Notwendigkeit einer Neuregelung des Archivbereiches vor allen Dingen aufgrund von Durchsetzungproblemen der Abgabepflicht im Zusammenhang mit personenbezogenen, klassifizierten bzw. sensiblen und elektronisch gespeicherten Informationen. Darüberhinaus statuiert das DSG, dass für das Bearbeiten von besonders schützenswerten Personendaten und Persönlichkeitsprofilen durch Bundesorgane ein formelles Gesetz als Rechtsgrundlage vorhanden sein muss.
Aus diesen Gründen wurde im Laufe des Jahres 1993 eine aus mehrerer Interessenvertretern der Bundesverwaltung zusammengesetzte interdepartementale Arbeitsgruppe eingesetzt, deren Aufgabe die Ausarbeitung eines Entwurfs für ein neues Bundesarchivgesetz ist. In dieser Arbeitsgruppe ist der Datenschutz ebenfalls vertreten.
Zielvorgaben für das Gesetz von unserer Seite sind:

- aus Gründen der Transparenz die Schaffung eines einheitlichen, den Archivbereich umfassend regelnden Erlasses, so dass - so weit möglich - auf Sonderregelungen in Spezialbereichen ausserhalb des Archivgesetzes verzichtet werden kann;
- aus Gründen der Transparenz und der Einheitlichkeit eine klare Kompetenzausscheidung zugunsten des Schweizerischen Bundesarchivs nach Ablieferung von Akten an das Bundesarchiv, damit es in Zweifels- und Streitfällen nur einen Ansprechpartner gibt, der für die Entscheidfällung zuständig ist, und auf diese Weise eine gewisse Einheitlichkeit in der Entscheidfindung gewährleistet wird;
- aus Gründen der besseren Kenntnis der Bereiche, in denen ursprünglich die Personendaten bearbeitet wurden, die Festlegung einer Pflicht des Bundesarchivs, die abgebenden Bundesstellen in Zweifels- und Streitfällen vor der Entscheidfällung zu konsultieren;
- aus Gründen der Rechtssicherheit die Schaffung klarer Regelungen des Bearbeitens von sehr sensiblen und besonders schützenswerten Personendaten sowie von Persönlichkeitsprofilen, insbesondere durch Festlegen von Schutzfristen im Zusammenhang mit der Einsichtgewährung in Dossiers mit sehr sensiblen oder besonders schützenswerten Personendaten und Persönlichkeitsprofilen.

8.2. "Kinder der Landstrasse"

Die Tätigkeit des Hilfswerks "Kinder der Landstrasse" hat in den 80er Jahren die Öffentlichkeit stark beschäftigt. Im Nachgang zu den Ereignissen hat sich die Frage gestellt, inwiefern den Betroffenen und Dritten (etwa zu Forschungszwecken) Einblick in

die sehr umfangreichen Akten des Hilfswerks gegeben werden soll. Obwohl die Akten grösstenteils nicht dem Anwendungsbereich des DSG unterstehen, haben wir auf entsprechende Anfragen hin zum Problem einer Einsichtsregelung für Betroffene und Drittpersonen Stellung bezogen.

Von 1926 bis 1973 führte die Stiftung Pro Juventute das Hilfswerk "Kinder der Landstrasse", das zum Ziel hatte, die "Vagantität" durch Trennung jenischer Kinder von ihren Eltern zu bekämpfen. Dabei wurden über 600 Kinder bei Pflegeeltern, in Kinderheimen, Waisenhäusern, psychiatrischen Kliniken und Strafanstalten untergebracht. Unterstützt wurde das Hilfswerk von kantonalen Behörden, aber auch vom Bund. Über die Betroffenen und ihre Angehörigen wurden umfangreiche, zum Teil sehr heikle und besonders schützenwerte Daten erhoben. 1973 stellte das Hilfswerk seine Tätigkeit ein. Ab 1985 wurden gegenüber den betroffenen Personen Wiedergutmachungsbestrebungen aufgenommen, die zur Gründung zweier Kommissionen führten. Die Aktenkommission "Kinder der Landstrasse" prüfte zuhanden der betroffenen Kantone, ob und in welchem Umfang den betroffenen Personen Einsicht in ihre Akten gewährt werden könne. Die Fondskommission kümmerte sich um die Frage der Entschädigung der Betroffenen. Im Rahmen der Tätigkeit der Aktenkommission, die 1993 aufgelöst worden ist, wurde etwa 240 Personen Einsicht in ihre Akten gewährt.

Sowohl zur Klärung der Verantwortlichkeiten als auch in Hinblick auf die Wiedergutmachung des von den Betroffenen erlittenen Unrechts wurde von den Betroffenen selbst, von der Öffentlichkeit, aber auch von Pro Juventute und vom Bund eine wissenschaftliche Aufarbeitung des Geschehenen gefordert. Dabei stellte sich die Frage, inwieweit die Betroffenen bezüglich der Gestaltung dieser Aufarbeitung über ein Mitspracherecht verfügen und - datenschutzrechtlich relevant - ob zu Forschungszwecken in die Akten der Betroffenen ohne deren Zustimmung Einsicht gewährt werden dürfe.

Da die Verfügungsgewalt über die Akten bei den Kantonen liegt, findet das DSG grundsätzlich keine Anwendung. Dennoch wurden wir gebeten, zur Frage der Einsichtnahme zu Forschungszwecken und zu einer generellen Einsichtsregelung für die Betroffenen sowohl bezüglich der Akten der Pro Juventute als auch bezüglich der neu entstandenen Akten der Akten- und der Fondskommission Stellung zu nehmen.

Zum ganzen Fragenkomplex haben wir mehrere Stellungnahmen abgegeben. Diese sind allerdings, soweit das DSG nicht Anwendung findet (also betreffend die Akten, die der Verfügungsgewalt der Kantone unterstehen), unverbindlich.

Für die wichtigste Frage, nämlich eine Einsichtsregelung für die Betroffenen und für Forschungszwecke und die Handhabung des Berichtigungsrechts, ergab sich dabei folgendes:

Obwohl die verschiedenen Aktenarten unter der Verfügungsgewalt verschiedener Organe stehen und damit auch unterschiedlichen Rechtsnormen unterworfen sind, ist im Interesse der Betroffenen eine einheitliche *Einsichtsregelung*, für die zudem nur eine Behörde zuständig ist, wünschenswert. Entgegen dem von verschiedener Seite geäusserten Wunsch können wir nicht die für die Gewährung des Einsichtsrechts zuständige Behörde sein, da wir sonst in Konflikt mit unserer Aufsichtsfunktion im Datenschutzbereich kämen. Die Einsichtsregelung selbst sollte sich nach unserer Auffassung an der im Datenschutzgesetz getroffenen Regelung des Auskunftsrechts orientieren. Sie sollte im einzelnen festhalten, wer einsichtsberechtigt ist, in welchem Umfang Einsicht gewährt wird und aus welchen Gründen die Einsicht im Einzelfall beschränkt werden kann.

Da von Seite der Betroffenen mehrfach darauf hingewiesen wurde, dass sie bezüglich der *Einsichtnahme* in ihre Akten durch Drittpersonen zu Forschungszwecken ein Mitspracherecht oder eine Entscheidkompetenz fordern, kann nicht von ihrer still-

schweigenden Einwilligung ausgegangen werden. Daher ist vor der Einsichtnahme in die Akten betroffener Personen zu Forschungszwecken deren ausdrückliche Zustimmung einzuholen. Von dieser Zustimmung könnte nur auf der Grundlage einer ausdrücklichen Regelung in einem formellen Gesetz abgesehen werden. Es ist ebenfalls klarzustellen, ob allenfalls Drittpersonen auch zu anderen als Forschungszwecken Einsicht gewährt werden kann. Ein solches Einsichtsrecht sollte erst gewährt werden, wenn sichergestellt ist, dass keine der betroffenen Personen mehr lebt oder sich an der Einsicht stören könnte. Die in Art. 7 des Reglementes für das Bundesarchiv vorgesehene Sperrfrist von 35 Jahren dürfte dafür nicht genügen.
Die betroffenen Person haben mehrfach zum Teil die Vernichtung der in den Akten über sie enthaltenen falschen Daten und zum Teil einfach deren *Berichtigung* gefordert. Gemäss Datenschutzgesetz hat jede Person, die Daten bearbeitet, sich über die Richtigkeit dieser Daten zu vergewissern. Jede betroffene Person kann verlangen, dass unrichtige Daten berichtigt werden. Ein Anspruch auf Vernichtung falscher Daten und ihren Ersatz durch korrekte Daten besteht insoweit, als die falsche Angabe bei zukünftigen Datenbearbeitungen der betroffenen Person schaden kann. Die ebenfalls zum Teil verlangte Herausgabe der Akten an die Betroffenen ist im DSG nicht vorgesehen.
Abgesehen von der Vernichtung des ganzen Aktenbestandes, die dem Interesse der Betroffenen an der Aufklärung ihrer persönlichen Vergangenheit und der Öffentlichkeit an der historischen Aufarbeitung der Aktion "Kinder der Landstrasse" zuwiderlaufen würde, kommt eine Vernichtung der "falschen" Daten schon aus praktischen Gründen nicht in Frage. Ausserdem handelt es sich bei den falschen Daten in der Mehrzahl um negative Werturteile (Qualifikation der betroffenen Person als schwachsinnig, arbeitsscheu usw.). Diese sind zwar für die Betroffenen sehr schmerzhaft und haben ihnen in der Vergangenheit viel Schaden zugefügt, könnten ihnen aber in Zukunft höchstens im Rahmen einer Forschungsarbeit schaden, wenn die mit der Forschungsarbeit betraute Person von diesen Werturteilen nicht genügend Abstand nehmen kann.
Deshalb sollte den betroffenen Personen in Anlehnung an Art. 15 Abs. 2 VDSG, der für beim Bundesarchiv hinterlegte Personendaten einen Vermerk über den strittigen oder unrichtigen Charakter der Daten vorsieht, die Gelegenheit gegeben werden, eine Berichtigung zu den Akten zu geben, in der auf die Ungültigkeit dieser Werturteile aufmerksam gemacht wird. In diesem Zusammenhang ist es wohl ebenso wichtig, bei einer zukünftigen Forschungsarbeit ausdrücklich die Entkräftung dieser Werturteile und die Darstellung des objektiven Sachverhalts zu verlangen.
Unserer Meinung nach empfiehlt es sich, den ganzen Fragenkomplex der Akten des Hilfswerk "Kinder der Landstrasse" in einem formellen Gesetz zu regeln, damit sichergestellt ist, dass eine Regelung gefunden wird, die die Interessen der Betroffenen wahrt, und damit diese die Möglichkeit haben, in einem rechtsstaatlichen Gesetzgebungsakt auf die Wahrung ihrer Interessen Einfluss zu nehmen.

9. Personalwesen

9.1. Privatbereich

Das Arbeitsverhältnis gibt Anlass zu einer häufig sehr umfangreichen und manchmal langandauernden Bearbeitung von Personendaten der Arbeitnehmerinnen und Arbeitnehmer durch den Arbeitgeber. In Anbetracht der rechtlichen und tatsächlichen Abhängigkeit der Angestellten vom Arbeitgeber ist auf diesem Gebiet dem Datenschutz

ein besonderes Augenmerk zu schenken und darauf zu achten, dass die Persönlichkeit der Angestellten durch den Umgang des Arbeitgebers mit ihren Daten nicht beeinträchtigt wird. Bei der Prüfung datenschutzrechtlicher Aspekte der Bearbeitung von Bewerbungsunterlagen und Personaldossiers, der Bekanntgabe von Daten an Dritte und des Berichtigungsrechts von Arbeitnehmern und Arbeitnehmerinnen bezüglich unrichtiger Angaben in Qualifikationen und Zeugnissen steht der neue Artikel 328b des Obligationenrechts im Vordergrund.

In Anbetracht der Tatsache, dass die Bearbeitung von Personaldaten in jeder Firma, die über Angestellte verfügt, vorkommt, erstaunt es nicht, dass Fragen über den Datenschutz im Arbeitsverhältnis zu den im Bereich der Datenbearbeitung durch Privatpersonen am häufigsten gestellten gehören. Seit Inkrafttreten des DSG wurden in diesem Bereich etwa 10 Stellungnahmen geschrieben. Die Antworten auf die häufigsten Fragen wurden in Merkblättern zusammengefasst, die an zahlreiche interessierte Personen verschickt wurden. Ausserdem wurden telefonisch sehr viele Auskünfte erteilt.
Gleichzeitig mit dem Datenschutzgesetz trat Art. 328b OR in Kraft. Er lautet: "Der Arbeitgeber darf Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrags erforderlich sind. Im übrigen gelten die Bestimmungen des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz."
Art. 328b OR ist eine Spezialnorm, die für den Bereich des privatrechtlichen Arbeitsvertragsrechts eine besondere Datenschutzbestimmung für die Bearbeitung von Personendaten des Arbeitnehmers durch den Arbeitgeber aufstellt. Der Grund dieser Spezialnorm liegt zum einen darin, dass das Arbeitsverhältnis Anlass zu einer häufig sehr umfangreichen und langandauernden Bearbeitung von Daten über Arbeitnehmerinnen und Arbeitnehmer gibt, zum anderen in der rechtlichen und tatsächlichen Abhängigkeit der Arbeitnehmer und Arbeitnehmerinnen vom Arbeitgeber, die einen verstärkten Schutz erforderlich macht. Art. 328b OR geht dem Datenschutzgesetz und anderen allgemeinen Datenschutzbestimmungen vor, wird aber durch die Bestimmungen des Datenschutzgesetzes ergänzt. Er konkretisiert die allgemeinen Grundsätze der Datenbearbeitung, insbesondere den Grundsatz der Verhältnismässigkeit, indem er vorsieht, dass der Arbeitgeber nur in zwei Fällen und nur in einem bestimmten Umfang Daten über Arbeitnehmerinnen und Arbeitnehmer bearbeiten darf: Er darf im Vorfeld des Abschlusses eines Arbeitsvertrags Daten über Bewerberinnen und Bewerber bearbeiten, um abzuklären, ob sie für die betreffende Arbeitsstelle geeignet sind. Und er darf während der Durchführung des Vertragsverhältnisses diejenigen Daten über Arbeitnehmerinnen und Arbeitnehmer bearbeiten, die für die Durchführung des Arbeitsverhältnisses erforderlich sind.
Für die Bearbeitung von Personendaten im Arbeitsverhältnis sind nebst Art. 328b OR und den allgemeinen Bearbeitungsgrundsätzen vor allem die Grundsätze für Datenbearbeitungen durch Private und die Rechtfertigungsgründe für eine Persönlichkeitsverletzung von Bedeutung.

Im folgenden werden in chronologischer Reihenfolge des Ablaufs eines Arbeitsverhältnis die wichtigsten bisher behandelten Fragen dargestellt.

Bewerbungsverfahren
Datenschutzrechtliche Fragen stellen sich schon bei der *Inserierung* von Stellenangeboten. Es kommt vor, dass ein Stellenangebot ohne Bezeichnung des Arbeitgebers oder der Personalrekrutierungsfirma nur unter Chiffre ausgeschrieben wird. Kennen aber die Bewerber und Bewerberinnen die Identität des Inserenten nicht, so

können sie ihr Auskunftsrecht ihm gegenüber nicht geltend machen. Dies kann unangenehm sein, wenn z.B. abgewiesene Bewerber und Bewerberinnen in Erfahrung bringen möchten, ob ihre Bewerbungsunterlagen aufbewahrt werden. Wenn der Inhaber einer Datensammlung Daten durch Dritte bearbeiten lässt, bleibt grundsätzlich er auskunftspflichtig. Allerdings ist der Dritte auskunftspflichtig, wenn er die Identität des Inhabers nicht bekanntgibt. Weder der Verleger der Zeitung noch eine Inserierungsfirma können bezüglich eines Chiffre-Inserats vollständig Auskunft geben, da sie im allgemeinen nur über den Inseratstext verfügen und die eingegangenen Antworten direkt weiterleiten. Deshalb müssen sie einer Bewerberin oder einem Bewerber auf Anfrage die Identität des Chiffre-Inserenten preisgeben, damit diese ihr Auskunftsrecht geltend machen können.
Im Zusammenhang mit Stellenbewerbungen darf der Arbeitgeber nur Unterlagen verlangen oder Fragen stellen, die von ihm zur *Abklärung der Eignung* der Bewerberin oder des Bewerbers für das Arbeitsverhältnis benötigt werden.
Dies gilt auch für die Einholung von *Auskünften bei Dritten* über die Bewerberinnen und Bewerber. Hierfür ist ausserdem die Zustimmung der betroffenen Person erforderlich. Es dürfen zum Beispiel keine Auskünfte beim bisherigen Arbeitgeber eingeholt werden, ohne dass der Bewerber oder die Bewerberin dazu das Einverständnis erteilt hat. Grundsätzlich haben die Arbeitnehmer und Arbeitnehmerinnen nämlich bezüglich ihrer Personendaten ein Selbstbestimmungsrecht. Dies lässt sich schon aus Art. 330a OR schliessen, wonach Arbeitnehmer und Arbeitnehmerinnen selbst entscheiden können, ob sie ein Vollzeugnis oder eine einfache Arbeitsbestätigung erhalten wollen. Daraus ergibt sich zumindest implizit eine Schweigepflicht des Arbeitgebers. In diesem Sinn äussert sich auch die Botschaft zum DSG. Das gesetzlich eingeräumte Recht der Arbeitnehmer und Arbeitnehmerinnen zur Informationsbegrenzung darf nicht hinter ihrem Rücken unterlaufen werden.
Selbst wenn der Arbeitnehmer oder die Arbeitnehmerin der Auskunfterteilung zugestimmt hat, darf sich die Auskunft *nur auf für die betreffende Tätigkeit wesentliche Informationen* beziehen. Sie darf sich nur auf Leistung und Verhalten der Arbeitnehmer und Arbeitnehmerinnen während des Arbeitsverhältnisses erstrecken. Unzulässig ist insbesondere die Gewährung der Einsichtnahme in die Personalakte der Arbeitnehmer und Arbeitnehmerinnen sowie die Bekanntgabe der Bedingungen des Arbeitsvertrags, da dadurch die Position des Bewerbers oder der Bewerberin erheblich geschwächt werden kann. Der potentielle neue Arbeitgeber darf selbstverständlich keine Auskünfte über die Bewerber und Bewerberinnen einholen, die er nach Gesetz nicht von diesen persönlich fordern dürfte.
Auch die Erstellung *graphologischer Gutachten* über Stellenbewerber und -bewerberinnen ist nur mit deren ausdrücklicher Zustimmung zulässig. Graphologische Gutachten entsprechen in der Regel der Definition von Persönlichkeitsprofilen (Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt) und enthalten häufig aufschlussreiche Aussagen über die betroffene Person. Die übliche Praxis, von allen Bewerbern und Bewerberinnen eine handschriftliche Bewerbung zu verlangen, um allenfalls ein Gutachten erstellen lassen zu können, genügt den Anforderungen des Datenschutzgesetzes nicht.
Aus Art. 328b OR und dem Grundsatz der Verhältnismässigkeit ergibt sich im weiteren, dass die Unterlagen der nicht berücksichtigten Bewerber und Bewerberinnen ihnen zurückgegeben und allfällige Kopien sogleich nach Abschluss des Anstellungsverfahren vernichtet werden müssen.

Während der Dauer des Arbeitsverhältnisses
Für die Dauer des Arbeitsverhältnisses wird über den Arbeitnehmer oder die Arbeitnehmerin in aller Regel ein Personaldossier geführt. Diese Personaldossiers dürfen gemäss Art. 328b OR nur Daten enthalten, die für die Durchführung des Arbeitsverhältnisses erforderlich sind.
Eine *Registrierungspflicht* besteht für Personaldossier nur unter bestimmten Voraussetzungen. Soweit in Personaldossiers nur Daten enthalten sind, für deren Bearbeitung durch den Arbeitgeber eine gesetzliche Pflicht besteht, die Bearbeitung der Daten dem Arbeitnehmer oder der Arbeitnehmerin bekannt ist oder nicht regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet oder an Dritte bekanntgegeben werden, sind diese Personaldatensammlungen nicht meldepflichtig.
Im Zusammenhang mit der *Qualifikation* von Arbeitnehmerinnen und Arbeitnehmern (aber auch in bezug auf die Ausstellung von Zwischen- und Endzeugnissen) und mit der Auskunftserteilung an den neuen Arbeitgeber stellt sich die Frage, ob Meinungsäusserungen über Arbeitnehmerinnen und Arbeitnehmer Personendaten darstellen und ob ein Anspruch auf Berichtigung (Art. 5 Abs. 2 DSG) solcher Äusserungen besteht. Bei Meinungsäusserungen handelt es sich, sobald sie mit einer bestimmten oder bestimmbaren Person in Verbindung gebracht werden oder werden können, um Personendaten. Solche Äusserungen sind auf ihre Richtigkeit hin zu überprüfen und nötigenfalls zu berichtigen. Es sind drei Fälle zu unterscheiden:
- Rein subjektive Wertungen ("Diese Person ist mir unsympathisch", usw.). Diese können nicht auf ihre Richtigkeit überprüft werden, haben aber grundsätzlich ihren Platz nicht in einer Personalakte, da sie für die Beurteilung der betreffenden Person nicht zweckdienlich sind.
- Subjektive Beurteilungen, die auf objektiven Kriterien beruhen ("der Arbeitnehmer erfüllt die geforderten Leistungen nicht, ist unzuverlässig, tüchtig", usw.). Hier bleibt die Beurteilung zwar subjektiv, jedoch kann überprüft werden, ob sie auf objektiven Kriterien beruht und für Dritte nachvollziehbar ist. Wenn ja, ist sie als richtig einzustufen. Wenn nicht, ist sie zu berichtigen.
- Beurteilungen, deren Richtigkeit oder Unrichtigkeit nicht immer dargelegt werden kann (bspw. "könnte mehr leisten"). Hier ist in analoger Anwendung von Art. 15 Abs. 2 DSG ein Vermerk über die Strittigkeit anzubringen. Noch besser, aber nicht gesetzlich vorgeschrieben ist es, die "Gegendarstellung" der betroffenen Person zu den Akten zu nehmen.

Es stellt sich auch die Frage, ob und inwiefern Arbeitnehmer und Arbeitnehmerinnen das Recht auf *Auskunft* über die im Personaldossier enthaltenen Unterlagen oder gar ein *Einsichtsrecht* bezüglich dieser Unterlagen haben:
Aus Art. 8 DSG ergibt sich, dass Arbeitnehmerinnen und Arbeitnehmer grundsätzlich ein *umfassendes Recht zur Auskunft über den Inhalt ihres Personaldossiers* haben. Die Beschränkung des Auskunftsrechts darf nur ausnahmsweise und in begründeten Fällen erfolgen. Insbesondere ist die systematische Beschränkung der Einsicht in Qualifikationen nicht zulässig. Personaldossiers müssen so geführt sein, dass den Arbeitnehmern und Arbeitnehmerinnen grundsätzlich über alles Auskunft erteilt werden kann und die Beschränkung des Auskunftsrechts nur aufgrund aussergewöhnlicher Umstände ausnahmsweise erforderlich ist. Zulässig ist die Beschränkung der Auskunft, um die überwiegende Interessen von Drittpersonen zu schützen (zum Beispiel durch Abdeckung des Namens der Verfasserin eines graphologischen Gutachtens).
Schliesslich fragt sich, inwieweit der Arbeitgeber Daten über Arbeitnehmer und Arbeitnehmerinnen *an Dritte bekanntgeben* darf.

- Der Arbeitgeber darf sicherlich Daten aufgrund einer gesetzlichen Pflicht bekanntgeben. In anderen Fällen kann die Bekanntgabe von Personendaten durch den Arbeitgeber an Dritte aufgrund seiner Fürsorgepflicht dem Arbeitnehmer oder der Arbeitnehmerin gegenüber schnell zu einer Verletzung der Persönlichkeit führen und ist mit Vorsicht zu handhaben.
- Die weitverbreitete Praxis, an Dritte (bspw. Vermieter und Vermieterinnen, Kreditkartenorganisationen) ohne das Bestehen einer gesetzlichen Pflicht Auskünfte über das Einkommen eines Arbeitnehmers oder einer Arbeitnehmerin zu erteilen, ist bedenklich. Solche Auskünfte sind von den Dritten grundsätzlich direkt bei Arbeitnehmer oder bei der Arbeitnehmerin selbst einzuholen. Auf jeden Fall dürfen sie vom Arbeitgeber nur mit der Einwilligung der Arbeitnehmerin oder des Arbeitnehmers erteilt werden.
  (Zur Frage, ob der Arbeitgeber Daten an einen potentiellen neuen Arbeitgeber bekanntgeben darf, vgl. oben).

Nach Beendigung des Arbeitsverhältnisses
Ist das Arbeitsverhältnis beendet, so stellt sich für den Arbeitgeber primär die Frage, was mit den von ihm über den Arbeitnehmer oder die Arbeitnehmerin bearbeiteten Daten zu geschehen hat.

- Gemäss Art. 328b OR darf er nur diejenigen Daten weiterhin aufbewahren, die auch nach Beendigung des Arbeitsverhältnisses zu dessen ordnungsgemässer Durchführung erforderlich sind. Dazu gehören Daten, die er aufgrund einer gesetzlichen Pflicht aufzubewahren hat, und Daten, deren Aufbewahrung im Interesse des Arbeitnehmers oder der Arbeitnehmerin liegt (bspw. für die Ausstellung eines Zeugnisses erforderliche Unterlagen, sofern nicht schon bei Beendigung des Arbeitsverhältnisses ein Zeugnis ausgestellt wurde). Daten, die unter keinen Umständen nochmals benötigt werden, sind sofort zu vernichten (dies gilt schon während der Dauer des Arbeitsverhältnisses).
- Für andere Daten, die eventuell noch gebraucht werden, ist die Aufbewahrungsdauer je nach Datenkategorie einzeln festzulegen. Für den Regelfall empfiehlt sich eine Aufbewahrungsfrist von 5 Jahren, die in Ausnahmefällen, bspw. wenn das Gesetz dies vorsieht, auf 10 Jahre verlängert werden kann.

9. 2. Bund

Das Datenbearbeitungssystem bezüglich des Personals der Bundesverwaltung wird derzeit völlig umgewandelt. Man ist dabei, das PERIBU (Personalinformationssystem des Bundes) umzustrukturieren und gleichzeitig Projekte zur dezentralisierten elektronischen Datenbearbeitung bezüglich des Personals sowie zur elektronischen Berarbeitung der Arbeitszeiten zu prüfen. In einigen Ämtern sind diese Systeme sogar schon im Einsatz. Die "Papierakten" werden dabei allerdings nicht ganz verschwinden. Es ist insofern dringend an der Zeit, Regelungen in bezug auf die Tatsache des "Nebeneinander-Bestehens" all dieser Datenbearbeitungssysteme zu treffen und den betroffenen Personen einen einheitlichen Datenschutz zu gewähren. Um dies zu erreichen, wird derzeit eine Verordnung des Bundesrates zum Schutze der Daten bezüglich der Bundesbediensteten ausgearbeitet. Diese Regelung wird das Rundschreiben des Eidgenössischen Personalamts vom 16. Januar 1984 zum Schutze der Daten von Bundesbediensteten ablösen.

Mit Inkrafttreten des DSG wurden die Richtlinien des Bundesrates vom 16. März 1981 bezüglich der Bearbeitung von Personendaten in der Bundesverwaltung aufge-

hoben. Gleichzeitig hätte auch das Rundschreiben des Eidgenössischen Personalamts (EPA) vom 16. Januar 1984 zum Schutze der Daten von Bundesbediensteten (im folgenden "Rundschreiben" genannt) hinfällig werden müssen. Das EPA war aber sehr richtig der Ansicht, dass es besser wäre, dieses Rundschreiben solange in Kraft zu lassen, bis eine spezifische Verordnung des Bundesrates zum Schutze der Daten von Bundesbediensteten verabschiedet ist. Eine solche Verordnung mit dem Titel "Verordnungsentwurf zum Schutze der Daten von Bundesbediensteten" (im folgenden mit "Verordnung" abgekürzt) wird derzeit ausgearbeitet. Das System PERIBU (Personalinformationssystem des Bundes) wird gerade neu strukturiert. Sowohl im Eidgenössischen Justiz- und Polizeidepartement (EJPD) als auch im Eidgenössischen Departement des Innern (EDI) ist man gegenwärtig dabei, Entwürfe zur elektronischen Datenvearbeitung (EDV) bezüglich des Personals und zur elektronischen Berarbeitung der Arbeitszeiten (z. B. Muri 10) zu prüfen, wobei in einigen Ämtern einige Systeme schon in Betrieb sind. Bei den mit Hilfe dieser Systeme bearbeiteten Daten handelt es sich meistens um besonders schützenswerte Daten oder um Persönlichkeitsprofile. Aus diesem Grunde ist ein erhöhter Persönlichkeitsschutz der betroffenen Bediensteten erforderlich. Die meisten der Informationen, die gegenwärtig noch in den "Papierakten" der entsprechenden Personalabteilungen enthalten sind, werden in die EDV-Systeme wie PIAS (EJPD) oder PISEDI (EDI) übernommen. Das erhöht die Risiken eines Eingriffs in den Persönlichkeitsbereich der Bundesbediensteten entsprechend. Die Verordnung muss demzufolge so vollständig wie möglich ausfallen und vor allem allgemeine Datenschutznormen enthalten (sie könnte unter anderem die im Rundschreiben vorhandenen Bestimmungen übernehmen). Ausserdem wäre es angebracht, spezifische Normen in bezug auf die Personalakten und die EDV-Systeme in die Verordnung aufzunehmen. Mit Hilfe dieser Normen muss es auch gelingen, eine Regelung im Hinblick auf das "Nebeneinander-Bestehen" all dieser Systeme herbeizuführen. Im weiter unten folgenden Abschnitt legen wir unsere Ansichten dar, die wir sowohl im Anschluss an die Untersuchung der ersten Version der Verordnung als auch nach der Analyse der uns vorgelegten EDV-Entwürfe vertreten haben.

Aufbewahrung der Daten von ehemaligen Stellenbewerbern: In einigen mit eigenen EDV-Systemen ausgestatteten Personalabteilungen ist es aufgrund der starken Personalschwankungen üblich, die Daten der Stellenbewerber, denen man eine Absage erteilt hat, zu registrieren und aufzubewahren. Dieses Verfahren wird für den Fall angewendet, dass der entsprechende Kandidat sich ein zweites oder gar drittes Mal um eine Stelle am gleichen Ort bewirbt. Dieses Vorgehen steht im Gegensatz zu den grundlegenden Prinzipien des DSG (Rechtmässigkeit, Verhältnismässigkeit ...) und dem Inhalt des Rundschreibens. Wir haben geraten, ein derartiges Vorgehen zu unterlassen und es in der Verordnung ausdrücklich zu untersagen.

Gleichbehandlung von Bediensteten, die den Bund verlassen, und von solchen, die in eine andere Verwaltungseinheit überwechseln: Verlässt ein Bediensteter den Bund, so wird vor einer Weiterleitung der ihn betreffenden Daten (Daten des PERIBU oder Daten seiner Personalakte) an seinen neuen Arbeitgeber seine Zustimmung zu diesem Schritt eingeholt. Dies geschieht jedoch nicht, wenn ein Bediensteter in eine andere Verwaltungseinheit überwechselt. Die PERIBU-Daten werden der neuen Einheit ohne weiteres unmittelbar zugänglich gemacht. In bezug auf Bedienstete, die innerhalb eines Departements lediglich das Amt wechseln, ist in einigen EDV-Projekten dieselbe Praxis vorgesehen. Demgegenüber werden die "Papierakten" keinesfalls an den neuen Arbeitgeber weitergeleitet, ob er nun auch beim Bund oder

sogar in demselben Departement ist oder nicht. In Übereinstimmung mit den allgemeinen Grundsätzen des Datenschutzes und eines gesunden Verwaltungswesens haben wir in bezug auf den obigen Fall ein einheitliches Vorgehen empfohlen. Wir sind der Meinung, dass in bezug auf die Bediensteten, die den Bund ganz verlassen, und diejenigen, die in eine andere Verwaltungseinheit des Bundes überwechseln, dasselbe Verfahren angewandt werden sollte. Die Zustimmung der betroffenen Person muss in jedem Fall eingeholt werden, bevor deren Daten an Dritte weitergeleitet werden, ob die Informationsbearbeitung nun über EDV erfolgt oder nicht. Es dürfen nur die Informationen (zum Beispiel PERIBU-Daten) weitergeleitet werden, die unbedingt notwendig sind. Um den Grundsatz der Gleichbehandlung zu wahren, haben wir empfohlen, in den Anhang der Verordnung das Muster eines Formulars aufzunehmen, mit Hilfe dessen die betroffene Person schriftlich ihre Zustimmung zu einer späteren Bekanntgabe ihrer Daten geben kann, gleichgültig, ob sie den Bund verlässt oder in eine andere Verwaltungseinheit wechselt.

Bestimmungen, die auf die von den Verwaltungseinheiten des Bundes dezentralisiert verwalteten EDV-Systeme anwendbar sind: In der Absicht, in allen Personalabteilungen des Bundes den gleichen Datenschutz zu gewährleisten, haben wir nahegelegt, Bestimmungen in die Verordnung aufzunehmen, die auf alle bestehenden und künftigen EDV-Personalsysteme anwendbar sind. Wir haben bezüglich sämtlicher Systeme auf die Notwendigkeit hingewiesen, folgende Grundsätze zu wahren:

- Erstellung von Inselsystemen;
- Strikte Beschränkung des Zugangs zu den Systemen auf die Angestellten der entsprechenden Personalabteilung, die dazu ermächtigt sind, Änderungen vorzunehmen;
- periodische Aushändigung (beispielsweise alle zwei Jahre) eines verständlichen Auszugs zuhanden der betroffenen Person. Der Auszug muss die entsprechenden Personendaten enthalten, die durch das System bearbeitet werden. Auf Verlangen hin müssen die Bediensteten ihr Auskunftsrecht geltend machen können;
- Möglichst kurze Aufbewahrungsdauer der Daten nach Ausscheiden des entsprechenden Bediensteten;
- Weitergabe nur der absolut notwendigen Daten an den neuen Arbeitgeber. Diese Regel gilt auch, wenn der Bedienstete innerhalb desselben Departements, das mit demselben EDV-System ausgestattet ist, lediglich die Einheit wechselt. Für die informatisierten Personalakten gelten in bezug auf die Datenweitergabe die gleichen Bestimmungen wie für die "Papierakten". Letztere werden allerdings an den neuen Arbeitgeber, wer auch immer dies ist, nicht weitergeleitet;
- An das Schweizerische Bundesarchiv werden nur Daten von historischer Bedeutung weitergegeben. In bezug auf die Personaldaten muss allerdings neu definiert werden, was mit "historischer Bedeutung" gemeint ist.

Auf PERIBU anwendbare Bestimmungen: Wir haben dem EPA nahegelegt, die Bestimmungen des Abschnitts der Verordnung, die PERIBU betreffen, durch folgende Punkte zu ergänzen:

Erwähnung der Systeme, mit denen PERIBU verbunden ist (online) und mit denen ein Datenaustausch stattfindet (beispielsweise das System SUPIS der Eidgenössischen Versicherungskasse) und Nennung der ausgetauschten oder eingesehenen Daten;

Aufnahme des Katalogs der im PERIBU bearbeiteten Daten in den Anhang der Verordnung, und zwar in der Weise, wie es für das System PISA des Militärdepartements erfolgt ist;
Verpflichtung für alle Organe, die PERIBU-Daten kopieren oder übernehmen, diese auf dem neuesten Stand zu halten und die Daten, zu denen das EPA ihnen den Zugang entzogen hat, aus ihren EDV-Systemen zu entfernen (vor allem bei Weggang oder Tod eines Bediensteten).

Systeme zur elektronischen Berechnung der Arbeitszeit (SEBA): Hierbei haben wir auf folgende Punkte hingewiesen:

Verpflichtung, die SEBA als Inselsysteme anzulegen, die weder mit dem PERIBU noch mit anderen elektronischen Berarbeitungssystemen verbunden sind. Einzige zulässige Ausnahme: Wenn ein Amt eine grosse Anzahl von Personen anstellt, die stundenweise bezahlt werden, könnte eine Verbindung zum PERIBU ins Auge gefasst werden, um die Verwaltung der Gehältern dieser Personen zu erleichtern;
Wahl einer im Sinne des Datenschutzes nichtsprechenden Erkennungsnummer für die Legitimationskarte und Gebrauch dieser Karte als Stechkarte;
strikte Beschränkung des Zugangs zu das SEBA auf Angestellte des Personalamts, die die Aufgabe haben, die Operationen im Zusammenhang mit dem Stechuhrsystem zu überwachen und gegebenenfalls Änderungen an das SEBA vorzunehmen;
Aufbewahrung der Daten im System während einem Jahr; dann Entfernung der Daten aus dem System und Lagerung derselben während zwei Jahren auf Magnetbändern; nach Ablauf dieser Frist Löschung der Daten.

Mitsprache des Personals: Wir haben festgestellt, dass die für die Anlegung von Personalakten zuständigen Organe diesen Grundsatz bis jetzt fast nie befolgt haben. Dabei ist er sowohl im Rundschreiben als auch in der Empfehlung des Europarats zum Schutz personenbezogener Daten für Beschäftigungszwecke verankert. Wir haben die Personalabteilungen, zu denen wir Kontakt hatten, auf diese Regel hingewiesen und ausserdem geraten, sie mit folgenden Worten in der Verordnung festzuschreiben:
"Für eine Anlegung und Verwendung von manuellen oder automatisierten Datensammlungen, müssen die Bediensteten, deren Daten registriert und bearbeitet werden sollen, oder auch deren Vertreter angehört werden."

"Papierakten": Diesbezüglich haben wir die Ansicht vertreten, dass für die anzulegenden Dossiers ein Standardinhalt festgelegt werden sollte. Darüber hinaus haben wir empfohlen, in die Verordnung den Grundsatz aufzunehmen, dass jedes Dokument eines Bediensteten in seiner Akte festgehalten werden sollte, wobei dem betreffenden Bediensteten systematisch eine Kopie des Eintrags ausgehändigt werden muss. Einzige Ausnahme: das Beurteilungsschreiben, das - von einem Streitfall einmal abgesehen - nur dem betroffenen Bediensteten selbst und seinem direkten Vorgesetzten zugänglich ist. Das bedeutet, dass von dem Beurteilungsschreiben kein Exemplar - also weder das Original noch eine Kopie - in die Akte des Bediensteten übergehen darf. Wir haben festgestellt, dass die Aufbewahrungsdauer bezüglich der Dossiers der Bediensteten zu lang ist, und sind der Meinung, dass sie von zehn auf fünf Jahre nach Beendigung des Arbeitsverhältnisses gekürzt werden sollte. Was die systematische Übergabe der Dossiers an das Schweizerische Bundesarchiv nach Ablauf dieser Frist anbelangt, so haben wir hervorgehoben, dass dieses Vorgehen

weder mit dem Sinn des Reglements des Schweizerischen Bundesarchivs noch mit den Bestimmungen des Datenschutzes vereinbar ist.

Rolle des Eidgenössischen Datenschutzbeauftragten: Angesichts der Tatsache, dass die Vermittlerrolle des Eidgenössichen Datenschutzbeauftragten nicht mehr klar aus dem DSG hervorgeht, haben wir aus Gründen der Transparenz vorgeschlagen, den schon im Rundschreiben enthaltenen Gedanken, der in folgende Worte gefasst werden könnte, in die Verordnung zu übernehmen. "Die Bediensteten können den Eidgenössischen Datenschutzbeauftragten um Beratung oder Vermittlung ersuchen"

Die zunehmende Informatisierung in bezug auf die Berarbeitung von Personaldaten in der Bundesverwaltung kennzeichnet für die mit der Verwaltung dieser Daten betrauten Bediensteten den Anfang einer neuen Ära. Die Technik legt ihnen Instrumente für eine optimale Rationalisierung ihrer Aufgaben in die Hände. Die Versuchung, sich einzig dieser technischen Möglichkeiten zu bedienen, ist gross und geht auf Kosten der Persönlichkeit der betroffenen Bediensteten. Die Bundesverwaltung fühlt sich hingegen verpflichtet, ihr Hauptaugenmerk auf den Schutz der Daten der betroffenen Personen zu legen, auch wenn sie dadurch womöglich auf bestimmte technologische Arbeitsinstrumente, die in technischer Hinsicht vieles erleichtern würden, aber für ein gesundes Verwaltungswesen nicht unbedingt notwendig sind, verzichten muss. Aus dieser Grundauffassung heraus lassen sich bestimmte Entscheidungen der Bundesverwaltung erklären, die von Anfang an getroffen werden müssen, wie etwa die Entscheidung für die Einrichtung und Verwendung von Inselsystemen.

10. Mietrecht

Anmeldeformulare für Mietwohnungen

Aufgrund von Äusserungen unsererseits in einer Radiosendung im Dezember 1993 und der darauf erfolgten Reaktionen haben wir eine schriftliche Stellungnahme zuhanden von Vermietern und Vermieterinnen verfasst, in der die gebräuchlichen Fragen auf Anmeldeformularen für Mietwohnungen Punkt für Punkt aus datenschutzrechtlicher Sicht analysiert werden. Dabei hat sich ergeben, dass auf den meisten gebräuchlichen Anmeldeformularen zu viele und zum Teil für die Auswahl des Mieters oder der Mieterin nicht erforderliche Angaben erhoben werden.

Wer sich für eine Wohnung interessiert, muss in der Regel ein Anmeldeformular zuhanden der Vermietung oder der Liegenschaftsverwaltung ausfüllen. Diese Formulare enthalten vor allem Fragen zur Person der Mieterin oder des Mieters, zu ihren Lebensgewohnheiten, ihren finanziellen Verhältnissen und ihrer vorherigen Wohnsituation. Die Fragen sollen der Vermietung ermöglichen, unter mehreren Bewerbern oder Bewerberinnen für eine Wohnung eine Auswahl zu treffen. Die Anzahl der gestellten Fragen und ihre Ausrichtung ist in der Praxis sehr unterschiedlich.
Wir haben die in den Anmeldeformularen gestellten Fragen auf ihre Vereinbarkeit mit dem DSG hin geprüft.
Gemäss Art. 13 Abs. 2 lit. a DSG dürfen Privatpersonen in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über ihren Vertragspartner oder ihre Vertragspartnerin bearbeiten. Die Vermietung hat also das Recht, im Hinblick auf den Abschluss eines Mietvertrags von den Mietin-

teressenten Angaben zu ihrer Person zu verlangen, die es ihr ermöglichen zu entscheiden, ob sie mit dem Mietinteressenten oder der Mietinteressentin einen Mietvertrag abschliessen will. Diese Angaben dürfen aber erst verlangt werden, wenn feststeht, dass die betreffende Person wirklich an dem konkreten Mietobjekt interessiert ist. Es wäre unverhältnismässig, von den Mietinteressenten zu verlangen, dass sie das Anmeldeformular ausfüllen, bevor sie die zu vermietende Wohnung gesehen haben.
Die Bearbeitung von Personendaten im Zusammenhang mit einem Vertragsabschluss ist nur zulässig, sofern dabei die allgemeinen Grundsätze des Datenschutzgesetzes respektiert werden. Zu erwähnen sind insbesondere der Grundsatz der Verhältnismässigkeit und der Zweckbindung der erhobenen Daten.
Die Erhebung von Daten von Mietinteressenten auf Anmeldeformularen ist somit grundsätzlich erlaubt. In bezug auf den zulässigen Umfang der Erhebung von Daten auf Anmeldeformularen für Mietwohnungen sind wir zu folgendem Ergebnis gelangt:
Die Vermietung darf von den Mietinteressenten nur diejenigen Angaben verlangen, die sie für die Auswahl einer geeigneten Mieterin oder eines geeigneten Mieters nach objektiven Kriterien benötigt. Sie hat die Pflicht, die von ihr benötigten Angaben auf die Art und Weise in Erfahrung zu bringen, die für die Mietinteressenten die geringste Persönlichkeitsbeeinträchtigung darstellt. Ist die Vermietung verpflichtet, bestimmten Behörden Angaben über ihre Mieterinnen und Mieter zu machen, so darf sie diese Angaben erst beim Abschluss des Mietvertrags erheben. Schliesslich hat sie sicherzustellen, dass die Daten nur denjenigen Personen zugänglich sind, die die Auswahl der Mieterin oder des Mieters treffen, dass keine unbefugten Datenbearbeitungen möglich sind und dass die nicht mehr benötigten Daten sofort vernichtet werden.
Aufgrund dieser Erwägungen haben wir eine Liste der Angaben, die im Normalfall (d.h. wenn keine besonderen objektiven Voraussetzungen gegeben sind) erhoben werden dürfen, erarbeitet. Diese Liste ist zur Zeit bei den Interessenverbänden in Vernehmlassung. Aufgrund der Ergebnisse dieser Vernehmlassung werden wir eine definitive Liste erarbeiten und die Vermieter und Vermieterinnen auffordern, sich bei der Erarbeitung ihrer Anmeldeformulare auf die in dieser Liste enthaltenen Angaben zu beschränken, es sei denn, sie könnten einen objektiv feststellbaren Bedarf nach weiteren Angaben darlegen. Eventuell werden wir sodann eine Empfehlung in diesem Sinne herausgeben.

II. WEITERE THEMEN

1. Verordnung über die Erhebung und Bearbeitung von landwirschaftlichen Betriebsdaten

Ein erfreuliches Beispiel von Kooperation im Bereich des Datenschutzes zwischen der Bundesverwaltung und uns ist aus dem Bundesamt für Landwirtschaft zu berichten. Seit mehreren Jahren hat das Bundesamt für Landwirtschaft an der Erstellung eines Informationssystems zur rationellen Verwaltung von Agrardaten gearbeitet. Das System bearbeitet u.a. auch Personendaten wie Name, Adresse und Beruf des Bewirtschafters, Art der landwirtschaftlichen Nutzungsfläche, Anzahl der Beschäftigten. Diese Datenbearbeitung fand ihre gesetzliche Grundlage in der Verordnung über die Erhebung und Bearbeitung von landwirschaftlichen Betriebsdaten. Die Rechtsgrundlage gewährleistet die datenschutzkonforme Bearbeitung der betreffenden Personendaten.

Das EDV-System ermöglicht eine einheitliche Verarbeitung einzelbetrieblicher Agrardaten (wie u.a. Adresse und Standort des Betriebes, Organisationsform, Produktionszone, Name, Adresse und Beruf des Bewirtschafters, Art der landwirtschaftlichen Nutzungsfläche, Anzahl der Beschäftigten) im Bundesamt für Landwirtschaft, um administrative und statistische Datenerhebungen zu koordinieren. Diese Daten liefern Informationen über alle landwirtschaftlichen Betriebe der Schweiz. Sie führen alleine oder zusammen mit anderen Agrardaten zur Identifikation des Betriebes oder des Bewirtschafters.

Das Bundesamt für Landwirtschaft schuf in Zusammenarbeit mit uns die notwendigen Rechtsgrundlagen. Die Verordnung, die den Betrieb des Informationssystems (Agrarpolitisches Informationssystem AGIS) regelt, wurde so gestaltet, dass sie den Grundsätzen des Datenschutzes entspricht. Insbesondere ging es darum, die Voraussetzungen für die Übermittlung von Personendaten an andere Behörden und für den Zugriff auf die Daten mittels anderen angeschlossenen EDV-Systemen festzulegen und generell alle Datenbearbeitungen, die mittels des Systems getätigt werden, für den Bürger und die Bürgerin transparent in der Verordnung zu regeln.

2. Projekt "Armee 95"

Seit Juli 1993 wurden uns durch das Eidgenössische Militärdepartement verschiedene Entwürfe zur Revision von Gesetzesakten zur Überprüfung vorgelegt, unter ihnen der Gesetzentwurf über die Armee und die Militärverwaltung. In diesem Entwurf wurden die Rechtsgrundlagen für die Tätigkeiten des Nachrichtendienstes und des Dienstes für militärische Sicherheit geschaffen. Die Rechtsgrundlage vom PISA (Personalinformationssystem der Armee) wurde dahingehend ergänzt, dass die Organe, die Online-Zugriff zu diesem System haben, explizit erwähnt werden müssen.

3. ZEK (Zentralstelle für Kreditinformation)

Die ZEK wurde als "Vereinigung zur Verwaltung einer Zentralstelle für Kreditinformation" gegründet. Bei dieser Datenbank handelt es sich um eine globale Zentralstelle zur Sammlung von Informationen über die Schuldner, die den Mitgliedern des Verbandes "Schweizerischer Kreditbanken und Finanzanstalten" (VSKF) zur Verfügung steht. Die Datenbank gibt Auskunft über die Kreditwürdigkeit der Antragsteller und Empfänger von Konsumkrediten und Verbrauchsgüterleasing.
Seit Inkrafttreten des DSG stehen wir mit dem Sekretariat des VSKF vor allem wegen der Fragen bezüglich der Anmeldung der ZEK-Datensammlung und der Art und Weise, wie die betroffenen Personen ihr Auskunftsrecht geltend machen können, in Verbindung. Am 9. März 1994 haben wir den Sitz der AC Automation AG besucht, die ihr Rechenzentrum verschiedenen Kunden, u. a. den Inhabern der ZEK-Datensammlung, zur Verfügung stellt. Bei diesem ersten Zusammentreffen haben wir eine globale Überprüfung der Umgebung der ZEK vorgenommen und ausserdem kontrolliert, inwieweit eine Datensicherung gewährleistet wird.

4. Kreditauskunfteien

Einige dieser Kreditauskunfteien, darunter Creditreform, stehen schon seit mehreren Jahren mit unserem Dienst in Verbindung. Seit Inkrafttreten des DSG arbeiten wir mit Creditreform in bezug auf die Fragen der Anmeldepflicht von Datensammlungen und des grenzüberschreitenden Datenflusses zusammen. Gegenstand unserer Zusammenarbeit bildet auch die Frage, auf welche Weise die Personen, deren Daten bearbeitet werden, ihr Auskunftsrecht geltend machen können. Creditreform liefert regelmässig Kreditauskünfte ins Ausland, wobei die Informationen meistens an Empfänger in solchen Ländern gelangen, die noch über keine Gesetzgebung zum Datenschutz verfügen (zum Beispiel Italien) oder in denen das Gesetz auf juristische Personen nicht anwendbar ist (wie im Falle Deutschlands) oder in denen es Datenschutznormen nur in bezug auf bestimmte Bereiche gibt (wie in den Vereinigten Staaten). Wir haben Creditreform darauf aufmerksam gemacht, dass sie gemäss DSG auf dem Vertragswege sicherstellen muss, dass ihre Kunden in bezug auf die ihnen gelieferten Daten ein Ausmass an Datenschutz garantieren, das demjenigen in unserem Land gleichkommt.

5. Private Eigentumsregister

Wir haben überprüft, inwiefern die Abfrage privater Eigentumsregister für geleaste, gestohlene oder gepfändete Fahrzeuge durch Telekiosk oder Videotex nach DSG zulässig ist, und sind zum Schluss gekommen, dass, sofern gewisse Voraussetzungen beachtet werden, solche Abfragen aus datenschutzrechtlicher Sicht zulässig sind.
Via Telekiosk oder Videotex werden heute Abfragen privater Eigentumsregister angeboten. Interessant sind solche Abfragen insbesondere für Autokäufer, die sicherstellen wollen, dass das ihnen zum Kauf angebotene Fahrzeug nicht geleast, verpfändet oder gestohlen ist. Wir wurden vom Betreiber eines solchen Eigentumsregisters um eine Stellungnahme aus datenschutzrechtlicher Sicht gebeten. Das betreffende Eigentumsregister enthält nach Angaben des Betreibers nur Personendaten (Telefonnummer und Initialen des Fahrzeugeigentümers), die von den betroffenen Personen im Bewusstsein der weiteren Verwendung eingegeben worden sind. Es werden keine Personendaten über Drittpersonen (bspw. einen Leasingnehmer) bearbeitet, da die Kontrolle der Fahrzeuge mittels Fahrzeuggestellnummer erfolgt. Wir sind der Meinung, dass in diesem Rahmen die Zurverfügungstellung der im Eigentumsregister enthaltenen Personendaten aus datenschutzrechtlicher Sicht unbedenklich ist, sofern für die Vertraulichkeit, die Verfügbarkeit und die Richtigkeit der bearbeiteten Daten gesorgt wird. Anders verhielte es sich jedoch, wenn Zusammenstellungen der eingegangenen Abfragen nach Person, Fahrgestellnummer, Inhalt der Abfrage oder ähnlichem erstellt würden. Die Überprüfung weiterer Register, insbesondere von Personenregistern zur Verhinderung von Debitorenverlusten, wird demnächst erfolgen.

6. Technische und organisatorische Massnahmen des Datenschutzes

Ein wesentlicher Teil des Datenschutzes besteht aus technischen und organisatorischen Massnahmen, die erforderlich sind, um die Umsetzung des Datenschutzes in des Praxis zu gewährleisten. Im folgenden werden diese Massnahmen näher erläutert und die von uns in diesem Zusammenhang im Umfeld der Bundesverwaltung gesammelten Erfahrungen dargelegt.

In Art. 7 DSG ist festgehalten, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden müssen. Obwohl schon in den Richtlinien für die Bearbeitung von Personendaten in der Bundesverwaltung vom 16. März 1981 in Ziffer 6 für die Bundesorgane die Anliegen der Datensicherheit aufgeführt waren, mussten wir vor allem in der Bundesverwaltung leider feststellen, dass dem Gesichtspunkt der Datensicherheit in vielen Fällen zuwenig Beachtung geschenkt wurde. In der Vollzugsverordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 14. Juni 1993 wurde diesem Umstand in Abschnitt 4 Rechnung getragen.

Datenschutz setzt ein System kontrollierter Informationsbearbeitung voraus, wie sie eigentlich von jeder Organisationseinheit oder Unternehmung gewünscht wird. Jeder Aufgabenträger, jede Organisationseinheit oder Unternehmung soll aus Gründen des Datenschutzes (aber auch im Interesse einer effizienten Aufgabenerfüllung) nur diejenigen Personendaten erhalten und bearbeiten, welche für die Erfüllung ihrer Aufgaben notwendig sind.
Bei der Systemgestaltung geht es darum, die Interessen der Fachabteilungen, der Systembetreiber und des Datenschutzes in angemessener Weise zu berücksichtigen. Je sensibler die Datenbearbeitung, desto umfangreicher ist den Anliegen des Datenschutzes Rechnung zu tragen.

Für den Datenschutz stellen sich bei der Systemgestaltung (-veränderung) namentlich die folgenden Fragen:

Welche Aufgaben sollen mit welchen Informatik-Mitteln gelöst werden?
Diese Frage kann beantwortet werden, indem man eine Organisationsanalyse (Aufgabenanalyse, Informationsbedarfs- und Informationsflussanalyse, ...) erarbeitet, aus der unter anderem der Bedarf an personenbezogenen Daten abgeleitet werden kann.
Jedes Informationssystem soll die Aufgabenträger bei der Erfüllung ihrer Aufgaben unterstützen. Aus diesem Grunde sind die Aufgaben und die für die Aufgabenerfüllung notwendigen organisatorischen Abläufe zu dokumentieren. Je sensitiver ein Informationssystem ist, um so detaillierter ist die Aufbau- und Ablauforganisation festzuhalten.

Welche technischen und organisatorischen Massnahmen (Datensicherheit) bedingt eine solche Bearbeitung von Personendaten?
- Bei der Umsetzung von Schutzmassnahmen ist es wichtig, dass man die Risiken oder Gefahren vor allem mit präventiven Massnahmen abdecken kann (z. B. Entflechtung von Personendaten und anderen Daten; Abschottung von Personendaten und Programmen; Zugriff und Operationsmöglichkeiten nur auf denjenigen Daten (Datenfelder), welche im Minimum für die Aufgabenerfüllung notwendig sind; Verschlüsselung, ...).
- Die präventiven Massnahmen reichen leider nicht immer aus für die Gewährleistung des Datenschutzes aus. Aus diesem Grunde muss der laufende Betrieb in denjenigen Bereichen festgehalten werden, in denen die vorbeugenden Massnahmen den Anforderungen des Datenschutzes nicht genügen können.
- Im weiteren muss festgehalten werden, welcher Systemzustand zum jeweiligen Zeitpunkt vorhanden war.

Ist die Bearbeitung von Personendaten mit Hilfe eines Informatik-Systems rechtmässig?
- Bei der Systemgestaltung müssen die rechtlichen Rahmenbedingungen so in das System implementiert werden, dass eine Umgehung der Vorschriften verunmöglicht bzw. minimiert wird. Dabei sind zwingende technische Massnahmen den organisatorischen Vorkehrungen vorzuziehen, weil sie in den meisten Fällen eine Umgehung der Vorschriften verunmöglichen.

Die Bundesverwaltung hat für die Umsetzung der technischen und organisatorischen Massnahment bei bestehenden Systemen eine fünfjährige Uebergangsfrist. Bei der Neugestaltung von Systemen ist den Anliegen des Datenschutzes *von Beginn an* Rechnung zu tragen. Dies führt zu kostengünstigeren datenschutzkonformen Systemen, als wenn man die Datenschutzmassnahmen (technische und organisatorische Vorkehrungen) im nachhinein in ein System implementieren muss.

Die Erfahrungen, die wir innerhalb der Bundesverwaltung sammeln konnten, zeigen, dass den Anliegen des Datenschutzes bei der Systemgestaltung in vielen Fällen noch zuwenig Rechnung getragen wird. Angaben in den Planungsunterlagen der Informatik-Projekte wie "die einschlägigen Vorschriften des Datenschutzes werden eingehalten" können seit der Inkraftsetzung des Datenschutzgesetzes nicht mehr akzeptiert werden, weil in der Verordnung zum Bundesgesetz über den Datenschutz in Abschnitt 4 Zielsetzungen aufgeführt sind, die konkret darauf hinweisen, wie man Systeme datenschutzkonform gestalten und betreiben muss. Um sich von der Datenschutzkonformität des jeweiligen Systems überzeugen zu können, ist festzuhalten, wie die Systemgestalter oder -betreiber den in Art. 20 VDSG aufgeführten Gesichtspunkten sowie insbesondere den in Art. 9 Abs. 1 der VDSG aufgeführten Zielsetzungen gerecht werden. Die Systemgestalter haben festzuhalten, welche möglichen Massnahmen sie für die jeweiligen Zielsetzungen vorsehen. Die verschiedenen Massnahmen mit ihren Wirkungen und den dafür notwendigen Ressourcen sind aufzuzeigen. Erst aufgrund dieser transparenten Informationen kann der Inhaber der Datensammlung entscheiden, welche Vorkehrungen er für das System vorsehen soll. Wir legen Wert auf eine nachvollziehbare Entscheidungsfindung.

Wir müssen immer wieder feststellen, dass die *organisatorischen Aufgaben in der Bundesverwaltung vernachlässigt werden*. Dies ist recht erstaunlich, weil man bei der Rationalisierung von Aufgaben oder Aufgabenerfüllungsprozessen primär von den organisatorischen Gesichtspunkten ausgehen muss. Erst in der nächsten Stufe müssen dann - wenn insbesondere eine kostengünstigere oder qualitativ bessere Lösung erreicht werden kann - die Aufgabenerfüllungsprozesse mit den notwendigen Informatik-Mitteln unterstützt werden. Leider sind die organisatorischen Gesichtspunkte auch bei sensitiven Systemen in der Bundesverwaltung in vielen Fällen nicht genügend dokumentiert, so dass wir vom Datenschutz nur sehr mühsam oder überhaupt nicht nachvollziehen können, welche Aufgaben man bei den jeweiligen Stellen oder Organisationseinheiten erfüllt. Die ungenügende "Pflege" und Dokumentation der organisatorischen Belange ist nicht nur ein Problem des Datenschutzes, sondern auch ein Problem zwischen den Fachabteilungen und der Informatik. Wenn die Fachabteilungen nicht in der Lage sind, ihre Bedürfnisse für die Unterstützung ihrer Aufgaben zu formulieren, so ist die Gefahr gross, dass die Informatik ein System entwickelt, welches den Aufgabenerfüllungsprozessen der Fachabteilungen nur ungenügend Rechnung trägt. Weil in den meisten Fällen ein grosser Teil der Dokumentation der Organisation fehlt, gehen wir momentan so vor, dass wir die wichtigsten Informatio-

nen in den jeweiligen Organisationseinheiten erheben. Leider mussten wir bis heute schon mehrmals feststellen, dass auf gleiche Fragen immer wieder anders geantwortet wird, so dass *ein gute Datenschutzanalyse bis heute ohne die notwendige Dokumentation der Organisation nur ungenügend möglich war.*

Daraus folgt, dass die Systemgestalter und -betreiber die Rahmenbedingungen des Datenschutzes besser berücksichtigen müssen.
Die Verantwortlichkeit für den Datenschutz liegt beim Inhaber der Datensammlung. Dieser hat sich immer wieder die folgenden Fragen zu stellen:

Ist die Bearbeitung rechtmässig?

Ist das System transparent und damit kontrollierbar gestaltet (Bearbeitungsreglement VDSG)? Sind insbesondere die Organisation (Aufbau- und Ablauforganisation) sowie die Informatikmittel dokumentiert?

Sind die notwendigen technischen und organisatorischen Massnahmen der Datensicherheit, die den Datenschutz gewährleisten sollen, geplant worden (Allgemeine -, besondere Massnahmen, Protokollierung VDSG)? Haben die Verantwortlichen nachvollziehbar entschieden, welche Massnahmen zu treffen sind, und hat man diese Entscheide auch umgesetzt?

Ist die Zweckbindung der Datenbearbeitung gewährleistet?

7. Bekanntgabe von Personendaten

7.1. Bekanntgabe von Adressen durch Bundesorgane (Art. 19 Abs. 2 DSG)

Die Bundesorgane werden des öfteren mit Anfragen von seiten privater Personen, Vereinigungen und Unternehmen konfrontiert, die den Namen, den Vornamen und die Adresse von bestimmten Personen zu erhalten wünschen. Einige fragen nach Daten zu einer einzelnen Person, anderen wiederum geht es um die Herausgabe ganzer Listen. Ferner kann es sich um eine einmalige Anfrage oder um den Wunsch nach regelmässiger und systematischer Datenbekanntgabe handeln. Die Gründe für diese Anfragen sind unterschiedlich. Sie können ideeller, geschäftlicher (vor allem zu Zwecken gezielter Werbekampagnen) oder auch wissenschaftlicher Art sein. Wir wurden mehrfach aufgefordert, uns zu diesen Anfragen zu äussern und haben schliesslich einige Richtlinien ausarbeiten können.

Art. 19 Abs. 2 DSG regelt die Bekanntgabe des Namens und Vornamens, der Adresse und des Geburtsdatums einer Person. Die in Art. 19 Abs. 2 DSG enthaltene Bestimmung berechtigt die Bundesorgane, derartige Daten auf Anfrage bekanntzugeben, auch wenn die Voraussetzungen von Art. 19 Abs. 1 DSG nicht erfüllt sind. Diese Ausnahmeregelungen lauten folgendermassen:
Die Bekanntgabe ist in einer Rechtsgrundlage vorgesehen, sie ist für den Empfänger im Einzelfall zur Erfüllung seiner Aufgabe unentbehrlich, die betroffene Person hat im Einzelfall eingewilligt, oder ihre Einwilligung darf nach den Umständen vorausgesetzt werden, der Empfänger macht glaubhaft, dass die betroffene Person die Einwilligung hinsichtlich der Datenbekanntgabe verweigert, um dem Empfänger die Durchsetzung von Rechtsansprüchen zu verwehren, oder die betroffene Person hat ihre Daten allgemein zugänglich gemacht. *Es handelt sich für das um Auskunft gebetene Bundesorgan nicht um eine Verpflichtung, sondern eben um eine Befugnis.* Das Bundesorgan bleibt in der Tat frei, zu entscheiden, ob es die gewünschten Daten bekanntgibt oder nicht. Es muss aber darauf achten, den Grundsatz der Gleichbehandlung einzuhalten, nicht in Willkür zu verfallen und die Rechte der betroffenen Personen zu

wahren. Das Bundesorgan muss insbesondere davon absehen, Daten bekanntzugeben, die Rückschlüsse auf andere Informationen über die betroffenen Personen, vor allem auf besonders schützenswerte Personendaten, zulassen. Ebenso bleibt die Bekanntgabe dieser Daten durch ein Abrufverfahren, besonders durch Online-Zugriffe, den Bestimmungen von Art. 19 Abs. 3 DSG unterworfen, welcher die Notwendigkeit einer ausdrücklichen Gesetzesgrundlage vorsieht. Schliesslich darf die Bekanntgabe nicht stattfinden, wenn die betroffene Person sich ihr widersetzt hat. Allerdings muss diese ein schutzwürdiges Interesse an der Nichtbekanntgabe glaubhaft machen. Das Bundesorgan darf die Sperrung der Bekanntgabe nur aufheben, um einer Rechtspflicht nachkommen oder um seine gesetzliche Aufgabe erfüllen zu können. Das verantwortliche Bundesorgan muss hinreichend grosszügig sein, wenn es um die Anerkennung des Interesses einer Person an der Nichtbekanntgabe ihres Namens, Vornamens, ihrer Adresse und ihres Geburtsdatums geht. Das um Auskunft gebetene Bundesorgan *kann* die Bekanntgabe übrigens nicht nur ablehnen, sie *muss* es sogar, wenn ein wesentliches öffentliches Interesse oder ein offensichtlich schutzwürdiges Interesse der betroffenen Person dies verlangt oder wenn eine gesetzliche Geheimhaltungspflicht oder eine besondere Datenschutzvorschrift es erforderlich macht (Art. 19 Abs. 4 DSG).
Die Bekanntgabe von Name, Vorname, Adresse und Geburtsdatum kann nur auf Anfrage und im Einzelfall erfolgen, und zwar einzeln oder in Form einer Liste. Demgegenüber sind eine regelmässige und systematische Bekanntgabe von Adressenlisten oder eine Veröffentlichung derartiger Listen durch Art. 19 Abs. 2 nicht abgedeckt.

7.2. Direktmarketing

Die Verwendung von Adressen zu Werbezwecken ohne Zustimmung der betroffenen Personen kommt in der Schweiz täglich tausendfach vor. So sehr es die einen schätzen, unbestelltes Werbematerial zu erhalten, so sehr stören sich die anderen an diesem "unerwünschten Eindringen in ihre Privatsphäre". Wir haben uns mit diesem Phänomen bisher leider nur am Rande befassen können, werden uns aber in nächster Zeit vertieft damit auseinandersetzen und versuchen, in Zusammenarbeit mit den Branchenverantwortlichen praktikable Lösungen zu erarbeiten.

Die Verwendung von Adressen zu Werbezwecken stösst bei vielen betroffenen Person auf Widerstand und Ablehnung. Zwar hat die Adresse keinen besonders schützenswerten Charakter und ihre Bearbeitung gilt als zulässig, solange die betroffene Person sie nicht ausdrücklich untersagt hat. Die Beeinträchtigung der Persönlichkeit durch unerwünschte Werbesendungen ist jedoch möglich und kann sogar schwerwiegend sein (man denke etwa an die unerwünschte Zustellung von Werbematerial mit pornographischem Charakter an eine mit einem Partner zusammenlebende Person).

Ein besonderes Problem stellt die *Unüberschaubarkeit* und damit einhergehend, die *Unkontrollierbarkeit* der Datenbearbeitung dar. Da Adressen über die verschiedensten Kanäle (PTT, Gemeinden, Versandhäuser, Adressbroker, Kundenlisten von Firmen, usw.) erhältlich sind, ist es oft nicht möglich, den Ursprung einer Adressbearbeitung zu eruieren. Insbesondere reichen die bestehenden Möglichkeiten (Robinsonliste, Adressblockierung durch die PTT) nicht aus, um die unerwünschte Zustellung von Werbesendungen zu unterbinden.

In einer diesbezüglichen Stellungnahme haben wir Verantwortliche der Direktmarketingbranche aufgefordert zu prüfen, wie es für die betroffene Person möglich gemacht werden kann, die Daten aufgrund der verwendeten Adresse bis zum Inhaber der Datensammlung (bspw. durch einen Identifikationscode) zurückzuverfolgen, damit sie ihr Auskunftsrecht geltend machen und allenfalls die Berichtigung verlangen oder die Weiterverwendung untersagen kann. Schon heute ist bei der Bearbeitung von Adressen zu Werbezwecken sicherzustellen, dass die betroffene Person dagegen nichts einzuwenden hat (bspw. durch einen Hinweis auf Anmeldeformularen, Information über Adressenverkauf durch die Gemeinden, usw.).

Wir haben uns auch zu der Frage geäussert, wann die Weitergabe von Adressen durch Privatpersonen zu Werbezwecken zulässig ist. Dies ist der Fall, wenn die Datenbearbeitung nach den allgemeinen Grundsätzen des DSG insbesondere dem Grundsatz der Zweckbindung, wonach Daten nicht für Werbezwecke verwendet werden dürfen, wenn sie zu anderen Zwecken erhoben wurden und die betroffenen Personen nicht über die vorgesehene Weiterverwendung informiert wurden, erfolgt und die betroffene Person die Weitergabe nicht untersagt hat.

In nächster Zukunft werden wir mit den betroffenen Kreisen Verbindung aufnehmen, um den ganzen Problembereich Direktmarketing zu analysieren und nach gangbaren Lösungswegen zu suchen.

7.3. Bekanntgabe von Personendaten aus dem Register der Fahrzeuginhaber

Wir wurden um Stellungnahme zum Änderungsentwurf eines kantonalen Datenschutzgesetzes gebeten, der dahin tendiert, eine Bestimmung einzuführen, die insbesondere die Weitergabe von Personendaten aus dem Register der Fahrzeuginhaber und Autofahrer an bestimmte in der gezielten Werbung tätige Unternehmen des Kantons erlaubt. Wir waren der Ansicht, dass der Entwurf die Handels- und Gewerbefreiheit beeinträchtigt und den Grundsätzen der Zweckmässigkeit und der Verhältnismässigkeit sowie den Bestimmungen der Bundesgesetzgebung über den Strassenverkehr zuwiderläuft.

Laut Bundesgericht schützt Art. 31 der Bundesverfassung jede private wirtschaftliche Tätigkeit, die auf Erzielung eines Gewinns ausgerichtet ist und beruflich ausgeübt wird, d. h. jede von einer Person entfaltete gewinnbringende Tätigkeit. Art. 31 BV beinhaltet das Recht auf freie Wahl und freie Ausübung jeglicher privaten gewinnbringenden Tätigkeit, und zwar an sämtlichen Orten der Schweiz. Laut Art. 31 Abs. 2 BV können die Kantone die Handels- und Gewerbefreiheit einschränken. Allerdings müssen diese Beschränkungen auf einer Rechtsgrundlage beruhen, sich durch ein überwiegendes öffentliches Interesse rechtfertigen lassen, den Grundsatz der Verhältnismässigkeit wahren, sich dem Grundsatz der Gleichbehandlung von wirtschaftlichen Konkurrenten unterordnen und dürfen den wesentlichen Inhalt der Handels- und Gewerbefreiheit nicht beeinträchtigen. Die Beschränkungen dürfen nicht Ausdruck von wirtschaftspolitischen Massnahmen sein. Folglich sind alle Massnahmen untersagt, die in den freien Wettbewerb eingreifen, um einzelne Wirtschaftszweige und Betriebsformen zu erhalten oder zu fördern und die dahin tendieren, das Wirtschaftsgeschehen nach einem festen Plan lenken zu wollen. Was unseren Fall anbelangt, so scheint die beabsichtigte Massnahme, nämlich bestimmten Unternehmen Zugang zu gewissen Daten aus dem Register der Autofahrer zu gewähren, ganz klar von dem wirtschaftspolitischen Interesse herzurühren, einen bestimmten Wirtschafts-

zweig, nämlich den der gezielten Werbung, zu unterstützen. Die Zugangsgenehmigung ist ausserdem auf ein oder zwei in dem Kanton ansässige Unternehmen dieser Branche beschränkt. Diese Massnahme zur Erhaltung oder Förderung eines Gewerbes greift in den freien Wettbewerb ein. Der Eingriff steht der Rechtssprechung des Bundesgerichts allerdings entgegen. Die besagte Tätigkeit kann ausserdem nicht als Tätigkeit öffentlichen Interesses angesehen werden. Selbst das Vorliegen eines öffentlichen Interesses würde einen Eingriff in das System des freien Wettbewerbs zum Schutze bestimmter Wirtschaftszweige oder Betriebsformen vor Konkurrenz oder zu deren Erhaltung nicht gestatten. Eine solche Massnahme stünde im Gegensatz zum Prinzip der Gleichbehandlung und würde den Grundsatz der Verhältnismässigkeit untergraben.

Wir haben in unserer Stellungnahme betont, dass die beabsichtigte Massnahme, selbst wenn man sie als vereinbar mit der Handels- und Gewerbefreiheit und mit dem Prinzip der Gleichbehandlung ansähe, mit anderen Grundsätzen kollidieren würde. Hierbei handelt es sich um Datenschutznormen und insbesondere um dem Grundsatz der Zweckmässigkeit sowie das Bundesgesetz über den Strassenverkehr. Letzteres regelt im besonderen die Beschaffung von Daten über Fahrzeuginhaber und Autofahrer. Derartige Informationen werden von den Kantonen unter Anwendung von Bundesrecht gesammelt und müssen entsprechend der Zweckbestimmung, für die das Bundesgesetz über den Strassenverkehr eine derartige Massnahme erlaubt, bearbeitet oder bekanntgegeben werden. Die Informationen dürfen nicht zu Zwecken verwendet werden, die mit diesem Gesetz nichts zu tun haben oder die mit ihr nicht vereinbar sind (zum Beispiel zum Zwecke direkter Werbung oder zu anderen als KfZ-Steuerzwecken). Die Register mit den Fahrzeughaltern und Autofahrern stellen Verwaltungsregister dar, die der Verwaltung in erster Linie als Arbeitsinstrumente dienen sollen. Sie sind nicht öffentlich. Sicher erlaubt das Strassenverkehrsrecht unter bestimmten Umständen die Bekanntgabe von Personendaten. Es gestattet den Kantonen auch die Veröffentlichung des Registers der Fahrzeughalter. Die betroffenen Personen verfügen aber über das Recht, eine Veröffentlichung der sie betreffenden Daten und folglich deren Bekanntgabe an Dritte zu sperren, wenn sie ein legitimes Interesse an der Nichtveröffentlichung geltend machen können (die Anforderungen, um ein solches Interesse geltend machen zu können, sind nicht so hoch anzusetzen). Wir haben übrigens daran erinnert, dass diese Möglichkeit der Veröffentlichung unter dem Blickwinkel des Datenschutzes fragwürdig ist.
Wir haben schliesslich betont, dass für den Fall, dass ein Kanton das Register veröffentlicht, der Zweck des Puplizierens mit dem Zweck des Datensammelns vereinbar sein muss. Das schliesst aus, dass die Daten zu gezielten Werbezwecken regelmässig und systematisch an einen bestimmten Empfänger weitergegeben werden können.

8. Grenzüberwachung mittels Videokamera

Im Bereich der inneren Sicherheit spielt die Kontrolle von Personen, die die Grenze passieren, eine wichtige Rolle. Diese Kontrollfunktion wird von den Grenzschutzbeamten und der jeweiligen Kantonspolizei ausgeübt. In der Absicht, den Kampf gegen die illegale Einwanderung und gegen Schlepperbanden effizienter zu gestalten, sieht die Eidgenössische Zollverwaltung vor, die Kontrollen an der grünen Grenze zu verstärken. Dies soll vor allem durch die Installierung von festen oder beweglichen Kameras erreicht werden. Diese Kameras sollen an den Stellen eingerichtet werden, an denen

unerlaubte Grenzüberschreitungen häufig vorkommen und wo es nicht möglich ist, auf Dauer Grenzpersonal zu stationieren.

Überwachungssysteme mit Videokameras sind in unserem Leben seit einigen Jahren täglich anzutreffen, dies sowohl in privaten Gebäuden (Banken, Geschäften, Restaurants, Arbeitsorten etc.) als auch an öffentlichen Orten (Strassen, Grenzen, öffentlichen Plätzen und Gebäuden, Stadien und anderen Sport- und Kultureinrichtungen). Der Rückgriff auf die Videoüberwachung gestattet eine Beobachtung des Verhaltens von Zuschauern oder Teilnehmern einer sportlichen oder sonstigen Veranstaltung. Durch die Videoüberwachung kann ein unliebsamer Kunde in einem Geschäft entlarvt, ein Verkehrssünder, ein Einbrecher oder eine Person, die illegal die Grenze passiert, ausfindig gemacht werden. Dieses technische Mittel wird ausserdem für die Überwachung von Kranken, für die Sicherheit auf den Strassen, in Parkhäusern und anderen Einrichtungen oder für die Produktionsüberwachung in einem Betrieb eingesetzt. Der Rückgriff auf eine Videoüberwachung ist in bezug auf solche Zwecke meistens legitim. Wenn man es allerdings versäumt, bestimmte Richtlinien zu beachten, kann mit einer derartigen Überwachung - wie im Falle des Abhörens von Telefongesprächen - auch ein schwerer Eingriff in den Persönlichkeitsbereich und die Grundrechte der beobachteten Personen verbunden sein. Wir haben bereits darauf hingewiesen, dass die Videoüberwachung ein anonymes, manchmal hinterlistiges technisches Mittel darstellt, dessen Folgen für den Einzelnen gravierender sein können als eine einfache visuelle Überwachung durch Personen, die zu diesem Zweck eingestellt wurden. Wir haben ebenfalls darauf aufmerksam gemacht, dass ein Bild von einer Person oder ein Bild, das deren Identifizierung gestattet, den Personendaten zuzurechnen ist. Insofern stellt das Einholen und die Aufbewahrung solcher Informationen, und wenn es auch nur für einen kurzen Zeitraum ist, eine Bearbeitung von Personendaten im Sinne des DSG dar, welche den allgemeinen Grundsätzen dieses Gesetzes unterliegt.

Videoüberwachung an Grenzposten: Die Eidgenössische Zollverwaltung hat uns über ihre Absicht in Kenntnis gesetzt, auf dieses technische Mittel zurückzugreifen. Wir haben sie in diesem Zusammenhang auf folgende Punkte aufmerksam gemacht:

Rechtmässigkeit der Aufnahme: Als Bundesorgan muss die Zollverwaltung den Rückgriff auf eine Videoüberwachung auf eine hinreichende Gesetzesgrundlage abstützen können. Wir haben eine Verordnung des Bundesrates in dem Masse als ausreichend angesehen, als die Installierung nicht die Aufzeichnung und die Aufbewahrung der Daten (über einige Tage hinaus) beinhaltet und die Videoüberwachung nicht ohne Wissen der betroffenen Personen vorgenommen wird. Hingegen erfordert die Aufbewahrung über mehrere Wochen, Monate oder gar Jahre hinweg, die eine Verwendung der Daten über den eigentlichen Grenzüberwachungszweck hinaus, insbesondere in Form einer Weitergabe der Daten an andere eidgenössische oder kantonale Behörden erlaubt, eine Rechtsgrundlage in Form eines formellen Gesetzes. Eine derartige Aufbewahrung oder mehrfache Verwendung dürfte nur dann gestattet werden, wenn sie unbedingt notwendig wäre.

Informationsbearbeitung nach dem Prinzip von *Treu und Glauben:* Die gefilmten Personen müssen im Prinzip in bezug auf die Massnahme der Videoüberwachung Kenntnis haben. Die Kameras müssten so sichtbar angebracht sein, dass die betroffene Person die Möglichkeit hat, ihr Verhalten der Situation anzupassen und gegebenenfalls darauf verzichten zu können, eine mit einem derartigen Überwachungssystem ausgestattete Einrichtung zu betreten. Wenn die Information nicht im voraus

gegeben werden kann, so mindestens im nachhinein. Im Einzelfall haben wir es der Eidgenössischen Zollverwaltung hingegen genehmigt, ihre Kameras aus strategischen Gründen versteckt anzubringen. Was den Gebrauch von mobilen Anlagen anbelangt, so haben wir uns dem Standpunkt der Eidgenössischen Zollverwaltung angeschlossen. Denn schliesslich könnten sich auch die Zollbeamten selbst verstecken, um die grüne Grenze zu beobachten. Wichtig ist für uns nur, dass die auf diese Weise gesammelten Informationen nicht länger als 24 Stunden aufbewahrt werden, sofern keine Festnahme erfolgt ist. Hingegen sind wir der Ansicht, dass die festen Anlagen sichtbar bleiben sollten, so wie auch die Zollbeamten am Grenzposten sichtbar sind. Für den Fall, dass dennoch unsichtbare Kameras verwendet werden sollen, haben wir dazu geraten, die betroffenen Personen in Form von Warnschildern darüber in Kenntnis zu setzen, dass das Grenzgebiet mit Videokameras überwacht wird.

Wahrung des Grundsatzes der *Verhältnismässigkeit:* Auf das Mittel der Videoüberwachung sollte nur zurückgegriffen werden, wenn das gesteckte Ziel nicht anders erreicht werden kann und wenn eine Überwachung durch Methoden, die weniger in den Persönlichkeitsbereich und die Grundrechte eingreifen, als nicht hinreichend wirksam erachtet wird. Das Einholen und die Aufbewahrung der Informationen ist nur über die Zeitspanne hinweg zulässig, die zur Erledigung der Aufgaben mit Hilfe der Videoüberwachung benötigt wird. Die infolge der Videoüberwachung an den Grenzen entstandenen Aufnahmen dürften nicht aufbewahrt werden, wenn direkt keine Gesetzesübertretung oder keine sonstigen ungewöhnlichen Vorkommnisse festgestellt werden können. In diesem Sinne betrachten wir die vom Schweizer Zoll vorgesehene Frist von 24 Stunden als angebracht.

Vereinbarkeit der Videoüberwachung mit dem Grundsatz der *Zweckmässigkeit:* Das Mittel der Videoüberwachung darf nur zur Erledigung einer von vornherein klar bestimmten Aufgabe eingesetzt werden. Unzulässig ist es hingegen, auf diese Möglichkeit zurückzugreifen, um zu undefinierten Zwecken unbegrenzt Daten zu sammeln. Was den Zoll anbelangt, so haben wir dazu geraten, die Videoüberwachung auf die Kontrolle des Grenzverkehrs zu beschränken, sie insbesondere mit dem Ziel einzusetzen, illegale Einwanderungen zu verhindern und Schlepperbanden zu bekämpfen.

III. DIE ANWENDBARKEIT DES DATENSCHUTZGESETZES AUF KANTONALER EBENE

Das eidgenössische Datenschutzgesetz gilt für die Bearbeitung von Personendaten durch Privatpersonen und Bundesorgane. Grundsätzlich keine Gültigkeit hat das eidgenössissche Datenschutzgesetz für das Bearbeiten von Personendaten durch kantonale Organe. Etwas anderes gilt jedoch gemäss Art. 37 DSG, wenn die Kantone Bundesaufgaben vollziehen, soweit keine kantonalen Datenschutzvorschriften bestehen. In diesem Zusammenhang stellt sich die Frage, welchen Anforderungen die kantonalen Datenschutzvorschriften hinsichtlich formeller Qualität und materiellem Inhalt zu genügen haben, damit das eidgenössische Datenschutzgesetz nicht zur Anwendung gelangt.

Da der Datenschutz Ausfluss von verfassungsmässigen Rechten, insbesondere des ungeschriebenen Rechts der persönlichen Freiheit sowie des Rechtsgleichheitsgebo-

tes von Art. 4 Bundesverfassung ist, sind den Kantonen verfassungsrechtliche Mindestanforderungen vorgegeben, denen sie im Rahmen ihrer Verwaltungstätigkeit hinsichtlich der Bearbeitung von Personendaten zu genügen haben. Im übrigen verfügen die Kantone jedoch im Bereich der kantonalen Verwaltungstätigkeit grundsätzlich über die Organisationsautonomie. Das bedeutet, dass die Kantone grundsätzlich frei sind, Regeln über den Umgang mit Personendaten in der öffentlichen und kommunalen Verwaltung zu erlassen. Weil die Kantone durch ihre Verwaltungstätigkeit aber nicht nur eigene Angelegenheiten ausführen, sondern auch Bundesrecht vollziehen, besteht die Gefahr, dass Divergenzen zwischen dem Datenschutz beim Vollzug von Bundesrecht durch die Kantone und dem Datenschutz auf Bundesebene entstehen.

Um einen einigermassen einheitlichen Datenschutz für die Tätigkeit von Bundesorganen und die Verwaltungstätigkeit der Kantone beim Vollzug von Bundesrecht zu erreichen und vor allem auch im Hinblick auf eine mögliche Ratifizierung des Übereinkommens Nr. 108 des Europarates zum Schutze des Menschen bei der automatisierten Verarbeitung von personenbezogenen Daten wurde in das Datenschutzgesetz Art. 37 DSG aufgenommen.

Art. 37 DSG kann nur zum Tragen kommen, wenn die Kantone Bundesrecht vollziehen. Die Abgrenzung, wann die Kantone noch Bundesrecht und wann sie kantonales Recht vollziehen, ist nicht immer ganz einfach vorzunehmen. Hierfür lassen sich vor allen Dingen zwei Gründe anführen:

- Die Grenze zwischen dem Vollzug von noch kantonalem Recht, d.h. wann die Kantone noch eine originäre Aufgabe erfüllen, und dem Vollzug von schon Bundesrecht kann fliessend sein.
- Kantonale Organe nehmen teilweise, etwa im Steuerbereich, gleichzeitig kantonale und eidgenössische Vollzugsaufgaben wahr. Die Erfüllung von Bundes- und kantonalen Aufgaben erfolgt teilweise im gleichen Verfahren und gestützt auf die gleichen Unterlagen. Praktisch alle übernommenen und verarbeiteten Daten sind sowohl für den Vollzug von Bundesgesetzen als auch für den Vollzug kantonaler Gesetze von Bedeutung. Es muss dann abgegrenzt werden, ob nun das Datenschutzrecht des Bundes oder das des Kantons zur Anwendung gelangt. Kantonale Verwaltungen werden dann hinsichtlich ein und derselben Amtshandlung verschiedenen Datenschutzgesetzgebungen unterstellt.

Grundlegend im Zusammenhang mit Art. 37 Abs. 1 DSG ist sodann die Beantwortung der Frage, was unter "kantonalen Datenschutzvorschriften" zu verstehen ist. Hinsichtlich der *formellen Qualität* der kantonalen Vorschriften ergeben sich aus dem Gesetz unmittelbar keine Anhaltspunkte. Der Gesetzgeber hat davon Abstand genommen, definitiv festzulegen, ob es sich bei den kantonalen Datenschutzvorschriften um ein Gesetz im formellen Sinne zu handeln habe oder ob die Form einer Verordnung ausreiche. Er wollte die Kantone nicht zwingen, dem eidgenössischen Datenschutzgesetz gleichwertige Rechtsnormen zu schaffen. In den Beratungen war man sich jedoch einig, dass die kantonalen Datenschutzvorschriften rechtssetzenden Charakter haben müssen. Die Normen müssen die Wirkung von für den Richter massgebenden Regelungen haben. Sie müssen Aussenwirkung entfalten. Gerade im Hinblick auf die Europaratskonvention und die Grundrechtsproblematik sind wir der Ansicht, dass es sich bei "kantonalen Datenschutzvorschriften" im

Sinne von Art. 37 Abs. 1 DSG um Erlasse in der Form eines *Gesetzes im formellem Sinne* zu handeln habe.

Auch in bezug auf den *materiellen Inhalt der kantonalen Vorschriften* hat der Gesetzgeber darauf verzichtet, den Kantonen Vorgaben zu machen, so dass etwa hinsichtlich der Rechte der betroffenen Personen zwischen dem eidgenössischen Datenschutzgesetz und den kantonalen Vorschriften erhebliche Divergenzen auftreten können. Da es sich beim Datenschutz jedoch um Persönlichkeits- und Grundrechtsschutz handelt sind zum einen zumindest die durch die reichhaltige Rechtsprechung des Bundesgerichtes - insbesondere zu dem Grundrecht der persönlichen Freiheit und zu Art. 4 BV - erfolgten Vorgaben als Mindestinhalte der kantonalen Vorschriften zu verstehen. Zum anderen ist das eidgenössische Datenschutzgesetz vor allen Dingen in materieller Hinsicht als Richtlinie oder Massstab heranzuziehen. Auch im Hinblick auf die Europaratskonvention müssen die kantonalen Vorschriften gewisse Minimalstandards enthalten, wie sie auch in dem von der Konferenz der kantonalen Justiz- und Polizeidirektoren 1983 vorgelegten Muster-Datenschutzgesetz vorgesehen sind.

Gemäss Art. 37 Abs. 2 DSG bestimmen die Kantone ein Kontrollorgan, das für die Einhaltung des Datenschutzes sorgt. Die Artikel 27, 30 und 31 sind sinngemäss anwendbar. Es wird die Ansicht vertreten, Abs. 2 komme nur zum Tragen, wenn das Bundesgesetz ersatzweise für die Vollzugsaufgaben zur Anwendung gelange, d.h. wenn keine kantonalen Datenschutzvorschriften im Sinne von Art. 37 Abs. 1 DSG bestünden. Erst dann müssten die Kantone ein eigenes Datenschutzkontrollorgan einrichten. Diese Meinung trifft zu, wenn man davon ausgeht, dass die kantonalen Datenschutzvorschriften gewisse minimale Inhalte regeln müssen, insbesondere ein Kontrollorgan vorzusehen haben, wie es von Art. 37 Abs. 2 DSG gefordert wird. Es ist jedoch denkbar, dass zur Zeit bestehende kantonale Datenschutzvorschriften entweder gar kein Kontrollorgan vorsehen oder aber Regelungen über Aufsichtsorgane enthalten, die in keiner Weise den Anforderungen an ein Kontrollorgan im Sinne von Art. 37 Abs. 2 DSG genügen. Von daher besteht unseres Erachtens für die Kantone unabhängig vom Vorhandensein kantonaler Datenschutzvorschriften die Verpflichtung, ein Kontrollorgan im Sinne des Art. 37 Abs. 2 DSG einzusetzen.

Beim Kontrollorgan gemäss Art. 37 Abs. 2 DSG muss es sich unserer Meinung nach um eine *neutrale und unabhängige Instanz* handeln, an die die Beteiligten - Inhaber der Datensammlungen, betroffene Personen - in Streitfällen gelangen können. Um darüberhinaus auch die Einheitlichkeit der Kontrolle zu gewährleisten, kommt nach unserer Auffassung für das Kontrollorgan nur eine *einzige, zentrale Instanz* in Betracht, die objektiv die Einhaltung der Datenschutzregeln überwacht.

Auf das zu schaffende Kontrollorgan sind die Art. 27, 30, 31 DSG bezüglich seiner *Kompetenzen und Aufgaben* sinngemäss anzuwenden. Das bedeutet, dass eine Anlehnung an die Bestimmungen des DSG geboten, aber nicht zwingend ist. Vielmehr ist in jedem Einzelfall zum einen auf die kantonalen Umstände und Bedingungen bzw. auf das kantonale System, d.h. auf die Struktur und die Organisation jedes einzelnen Kantons Rücksicht zu nehmen. Zum anderen ist immer von der grundsätzlich gültigen kantonalen Organisationsautonomie auszugehen. Die in den Art. 27, 30, 31 sind somit nicht als Mindeststandard zu verstehen. Schaffen die Kantone aus Eigeninteresse ähnliche Bedingungen, wie es das DSG vorsieht, etwa in Art. 31 Abs. 2 DSG, so wären das zu begrüssende Bestrebungen.

IV. INTERNATIONALES

Die mit dem Datenschutz verbundenen Problemstellungen machen vor den nationalen Grenzen nicht halt. In einer Welt mit einer immer grösser werdenden gegenseitigen Abhängigkeit und einer ständig ansteigenden technologischen Leistungsfähigkeit ist der Austausch von Informationen - insbesondere von personenbezogenen Informationen - über die nationalen Grenzen hinaus zu einer Leichtigkeit geworden. Ein solcher Austausch von Informationen entspricht den Bedürfnissen verschiedenster Bereiche wie der Wirtschaft, der Wissenschaft, der Kultur, der Tourismusbranche, des Verwaltungswesens oder der Polizei. Die internationale Dimension des Flusses von Personendaten kann das nationale Datenschutzsystem schwächen und macht eine Harmonisierung in rechtlicher Hinsicht sowie eine internationale Zusammenarbeit unbedingt notwendig.

Im DSG ist ausdrücklich vorgesehen, dass unsere Aufgaben vor allem darin bestehen, mit den für den Datenschutz zuständigen Behörden im Ausland zusammenzuarbeiten und zu untersuchen, inwieweit der im Ausland gewährte Datenschutz dem schweizerischen entspricht. Angesichts der Tatsache, dass die meisten Tätigkeiten, die eine Bearbeitung von Personendaten erfordern, über die nationalen Grenzen hinaus stattfinden und die Datenschutzprobleme sich nicht auf eine Region oder einen bestimmten Staat beschränken, ist eine internationale Zusammenarbeit nicht mehr wegzudenken. Sie ermöglicht vor allem einen Informationsaustausch zwischen den Datenschutzbehörden und eine gemeinsame Erarbeitung von Lösungen. Eine internationale Zusammenarbeit gestattet ausserdem eine bessere Beratung von Personen und Organen, die mit der Bearbeitung von Personendaten betraut sind. Darüber hinaus kann dadurch betroffenen Personen bei der Ausübung ihrer Rechte im Ausland effizienter geholfen werden. Die Zusammenarbeit erfolgt auf verschiedenen Ebenen: durch bilaterale Kontakte, durch die internationale Konferenz der Beaufragten für Datenschutz und über internationale Organisationen (vor allem Europarat und OECD).

1. Internationale Konferenz der Beauftragten für Datenschutz

Die Kontrollinstanzen, die laut den verschiedenen nationalen Gesetzgebungen zum Zweck der Überwachung des Datenschutzes eingerichtet werden, haben eine internationale Konferenz ins Leben gerufen. Diese findet auf Einladung je eines Mitgliedstaates einmal jährlich statt. Die Zielsetzung dieser Konferenz besteht darin, den Austausch von Informationen unter den Kontrollbehörden zu ermöglichen. Ausserdem soll sie den Kontrollbehörden die Gelegenheit geben, ihre Vorgehensweisen zu festigen und aufeinander abzustimmen und gegebenenfalls gemeinsame Positionen einzunehmen (Beschluss der Konferenz).
Die XV. Internationale Konferenz der Beauftragten für Datenschutz fand auf Einladung von "Data Registrar" (Vereinigtes Königreich) vom 27. bis 30. September 1993 in Manchester statt. Anlässlich der Konferenz konnte die internationale Entwicklung des Datenschutzes dargestellt werden. Die Konferenz bot ausserdem Gelegenheit zu einem vertieften Meinungsaustausch über folgende Problembereiche und Fragestellungen: Sammlung von aus öffentlichen Datensammlungen stammenden Personendaten und deren Nutzung für geschäftliche Zwecke, Wahrung der Privatsphäre und der Meinungsäusserungsfreiheit, Rückgriff auf Erkennungsmerkmale (Identifikationsnummer, Genmarkierung), Volkszählung, Überwachung mit Hilfe von Videokameras oder auch Sicherheit im Bereich der Informatik. Angesichts der neuen Forschungs-

und Untersuchungsmöglichkeiten, die uns die moderne Technologie zur Verfügung stellt (Genforschung, Videoüberwachung, elektronische Überwachung ...) haben die Beauftragten für Datenschutz auf der Notwendigkeit bestanden, ein echtes Gleichgewicht zwischen dem Informationsbedarf einerseits und der Wahrung der Grundrechte und vor allem des Privatlebens andererseits zu finden. Sie hielten es für angebracht, sorgfältig abzuwägen zwischen dem Nutzen, den diese modernen Möglichkeiten mit sich bringen, und den Einschränkungen in bezug auf die Rechte des Individuums sowie den Folgen dieser Einschränkungen für unsere demokratische Gesellschaft.

2. Europarat

Seit über zwanzig Jahren beschäftigt sich der Europarat mit der Frage nach der Harmonisierung des Datenschutzrechts in Europa und unternimmt diverse Arbeiten in diesem Sinne. 1981 hat er ein Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten verabschiedet (Konvention 108) und diese seinen Mitgliedstaaten zur Unterzeichnung vorgelegt. Die Konvention wurde von fünfzehn Staaten ratifiziert (Österreich, Belgien, Dänemark, Finnland, Frankreich, Deutschland, Island, Irland, Luxemburg, Niederlande, Norwegen, Portugal, Spanien, Schweden und Vereinigtes Königreich). Sechs weitere Staaten (Zypern, Griechenland, Ungarn, Italien, Slowenien und die Türkei) haben sie ebenfalls unterzeichnet. Bis zum Inkrafttreten des DSG war unser Land nicht imstande, die Konvention zu unterzeichnen und zu ratifizieren. Obwohl noch nicht alle Kantone ein Gesetz über den Datenschutz verabschiedet haben, sind wir der Meinung, dass der Moment für unser Land gekommen ist, diesen Text zu ratifizieren. Am 14. Juni 1993 hat der Bundesrat dem EJPD den Auftrag erteilt, diesbezüglich eine Botschaft vorzubereiten.
Innerhalb des Europarats sind zwei Komitees mit den Fragen des Datenschutzes betraut. Dabei handelt es sich in erster Linie um die "Projektgruppe für Datenschutz im Europarat" (CJ-PD), an der wir aktiv beteiligt sind und die zweimal jährlich im Plenum zusammentrifft. Die CJ-PD arbeitet vor allem Empfehlungen aus, die die allgemeinen Grundsätze der Konvention 108 in bezug auf einzelne Bereiche konkretisieren und präzisieren. Acht Empfehlungen wurden seit 1981 verabschiedet (medizinische Datenbanken, wissenschaftliche und statistische Forschung, direktes Marketing, soziale Sicherheit, Polizei, Arbeitswesen, öffentliche Datensammlungen, Zahlungsvorgänge und ähnliche Vorgehensweisen). Vier weitere Empfehlungen sind derzeit in Vorbereitung. Dabei geht es um Telekommunikation, medizinische Daten (vor allem medizinische Forschung, Genetik), Statistik und Versicherungen. Ausserdem überprüft die CJ-PD, ob es nützlich ist, die Empfehlung bezüglich der Polizei zu überarbeiten und zu vervollständigen, um hauptsächlich den grenzübergreifenden Informationssystemen (z. B. den Systemen Shengen oder Europol) Rechnung zu tragen.
Das zweite Komitee ist ebenfalls in Sachen Datenschutz aktiv. Es handelt sich hierbei um den beratenden Ausschuss, dessen Einführung in der Konvention 108 vorgesehen war. Dieses Komitee hat den Auftrag, Stellungnahmen bezüglich der Umsetzung der genannten Konvention abzugeben. Die Mitglieder des beratenden Komitee, in dem wir als Beobachter vertreten sind, kommen ein- bis zweimal pro Jahr zusammen. 1993 hat sich das Komitee in erster Linie damit beschäftigt, ein Mustervertragsprojekt im Bereich des grenzüberschreitenden Datenflusses zu Ende zu bringen. Dieses war in Zusammenarbeit mit der Europäischen Union und der internationalen Handelskammer ausgearbeitet worden. Das Ziel der Klauseln besteht darin,

auf dem Vertragswege sicherzustellen, dass die Grundsätze der Konvention 108 im Falle eines Datentransfers in Staaten, die die Konvention nicht unterzeichnet haben, eingehalten werden. Das Komitee hat darüber hinaus angeregt, sich Gedanken über die Frage zu machen, ob auch Informationen über verstorbene Personen oder Bild und Stimme von natürlichen Personen durch den Datenschutz beziehungsweise die Konvention 108 abgedeckt sind. Das Komitee ist diesbezüglich bislang noch zu keinem endgültigen Schluss gelangt. Es überprüft die Bedingungen, unter denen die Europäische Union ihrer Absicht nachkommen kann, die Konvention 108 zu ratifizieren.

3. Organisation für die Zusammenarbeit und Entwicklung OECD

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung ist ebenfalls in Sachen Datenschutz aktiv. Die OECD hat am 23. September 1980 Richtlinien über den Schutz der Privatsphäre und den grenzüberschreitenden Fluss von personenbezogenen Daten verabschiedet. Im Sinn der Konvention 108 des Europarates zielen diese Richtlinien - vor allem im Hinblick auf einen freien Informationsfluss - darauf ab, das Datenschutzrecht zu vereinheitlichen. Der Datenschutz ist fortlaufend Gegenstand von Ad hoc-Zusammenkünften zwischen Experten der verschiedenen Mitgliedstaaten. Diese Zusammenkünfte bieten Gelegenheit, in bezug auf die Entwicklung des Datenschutzrechts in den verschiedenen Mitgliedstaaten Bilanz zu ziehen und bestimmte einzelne Problemstellungen zu untersuchen (zum Beispiel: grenzüberschreitenden Datenfluss, Telekommunikation, Kreditkarten, Videoüberwachung ...). So haben sich die Experten 1993 zusammengesetzt, um sich mit den Fragen des Datenschutzes in bezug auf Krankendossiers und medizinische Forschung auseinanderzusetzen. Die Zusammenkunft gab Gelegenheit zu einem breiten Gedankenaustausch über die je nach Land unterschiedlichen Vorgehensweisen bei der Bearbeitung von medizinischen Daten. Die schweizerische Lösung, eine Expertenkommission bezüglich des Berufsgeheimnisses im Rahmen der medizinischen Forschung einzurichten, stiess bei den anderen anwesenden Delegationen auf ein grosses Echo. Nach der schweizerischen Lösung sollte dieser Expertenkommission die Aufgabe zukommen, Bewilligungen in bezug auf die Bekanntgabe medizinischer Daten zu erteilen. Die schweizerische Lösung wurde in den Empfehlungsentwurf des Europarats aufgenommen, welcher derzeit von der CJ-PD diskutiert wird. Unter den bei dem Zusammentreffen vorgebrachten Anregungen gingen einige Vorschläge in die Richtung, medizinische Forschung betreiben zu lassen, ohne dass die Forscher Kenntnis von der Identität der betroffenen Personen haben (Anonymisierung, Möglichkeiten der Chiffrierung von Informationen, Kodierung der Identifizierungsmerkmale, Verwendung von Pseudonymen).

4. Europäische Union

Die Kommission der Europäischen Gemeinschaft hat im September 1990 einen Richtlinienentwurf zum Personenschutz im Hinblick auf die Bearbeitung von Personendaten vorgelegt. Nachdem man bei den gemeinschaftlichen Institutionen, den Mitgliedstaaten, den Beauftragten für Datenschutz und in den betroffenen privaten Kreisen ausgiebig Rat eingeholt hatte, wurde im Oktober 1992 ein zweiter, überarbeiteter Entwurf vorgelegt. Über diesen wird gegenwärtig im Rat der Europäischen Union diskutiert. Daneben untersucht die Europäische Union zurzeit einen Richtlinien-

entwurf zum Schutz personenbezogener Daten und der Privatsphäre im Zusammenhang mit den öffentlichen digitalen Telekommunikationsnetzen, insbesondere dem dienstintegrierten digitalen Netz (ISDN) und den öffentlichen mobilen digitalen Netzen.

5. Bilaterale Kontakte

In der Einführungsphase des Gesetzes haben wir uns wiederholt an die Datenschutzbehörden verschiedener europäischer Staaten gewandt, um Auskünfte über deren Organisation zu erhalten. Wir haben uns ausserdem in bezug auf verschiedene Fragestellungen, vor allem was das Polizeiwesen, das Abhören von Telefongesprächen und neue Technologien (ISDN, X.500) betrifft, von ihnen beraten lassen. Darüber hinaus sind wir Deutschland und Frankreich - auf deren Anfrage hin - in zwei Fällen, die sich auf direktes Marketing bezogen, zu Hilfe gekommen. Im ersten Fall ging es um eine Werbekampagne über Fax, die Gegenstand einer Anklage seitens einer Privatperson in der Bundesrepublik Deutschland war. Der Bundesdeutsche Beauftragte für Datenschutz hat uns um Hilfe gebeten, um herauszufinden, auf welche Weise die Schweizer Firma, die die Kampagne gestartet hatte, in den Besitz der Daten der Klägerin gekommen war und welche - die Klägerin betreffenden - Informationen die Firma bearbeitete. Unsere Ermittlungen haben zu der Feststellung geführt, dass die besagte Firma lediglich ein Verzeichnis mit Faxnummern benutzt hatte und keine weiteren Informationen über die Personen besass, denen sie ihre Werbeschriften zustellte.
Der zweite Fall befindet sich noch in Bearbeitung. Die französische Nationale Kommission für Informatik und Freiheitsrechte hat sich aufgrund einer Klage von seiten einer französischen Firma an uns gewandt, welche zu Werbezwecken Rechnungen für einen Eintrag in ein internationales Telefonbuch erhalten hatte.

V. REGISTER DER DATENSAMMLUNGEN

Das Register der Sammlungen von Personendaten erfüllt in erster Linie den Zweck, die Öffentlichkeit über die Bearbeitung von Personendaten durch Bundesorgane und private Personen zu informieren. Das DSG verlangt von den Bundesorganen, dass sie uns sämtliche ihrer Datensammlungen, die Personendaten enthalten, anmelden. Von den Inhabern privater Datensammlungen verlangt das DSG, dass sie diejenigen ihrer Datensammlungen anmelden, die die vom DSG vorgesehenen Bedingungen erfüllen. Nach einer summarischen Überprüfung der Anmeldeformulare durch uns werden die auf diese Weise gesammelten Informationen in das elektronisches Verwaltungssystem des Registers der Datensammlungen eingegeben (DATAREG). Diese System gestattet die regelmässige Veröffentlichung des Registers, dient uns als Überwachungsinstrument und den Personen, die ihr Auskunftsrecht ausüben wollen, als Informationsquelle. Es werden an die 1500 Anmeldungen von Datensammlungen erwartet.

Gemäss den Richtlinien des Bundesrates für die Bearbeitung von Personendaten in der Bundesverwaltung vom 16. März 1981 wurde das Register zum letzten Mal 1991 veröffentlicht. Es enthielt nur die Datensammlungen mit Personendaten, die von Ämtern der Bundesverwaltung geführt worden waren. Seit 1. Juli 1993 müssen sich auch private Personen, deren Datensammlungen die im DSG enthaltenen Bedingun-

gen erfüllen, der Anmeldepflicht unterziehen. Die Anmeldung muss bis zum 30. Juni 1994 bei uns vorliegen. Eine kleine Arbeitsgruppe überprüft global den Inhalt der Anmeldung. Die Entwicklung des elektronischen Verarbeitungssystems für das Register der Datensammlungen (DATAREG) wird gerade abgeschlossen. Dank dieses Instruments müsste es uns gelingen, die rund 1000 Anmeldungen aus der Bundesverwaltung und die etwa 500 Deklarationen, die wir von seiten privater Kreise erwarten, effizient zu verwalten.

1. Zweck des Registers

Das Register der Datensammlungen erfüllt den Zweck, die Öffentlichkeit über die Bearbeitung von Personendaten durch Bundesorgane und private Personen zu informieren. Es ist ein Instrument, das die Publizität der Datensammlungen gewährleisten soll, um insbesondere die Ausübung des Auskunftsrechts durch die betroffenen Personen zu erleichtern. Das Register gibt an, wer in welcher Weise Daten bearbeitet. Es bezeichnet in bezug auf jede veröffentlichte Datensammlung die zuständige Stelle, bei der ein Auskunftsgesuch eingereicht werden kann. Das Register dient uns ausserdem als Hilfsmittel zur Erfüllung unserer Beratungs- und Überwachungsaufgabe.

2. DATAREG - Verwaltungssystem des Registers der Datensammlungen

Das *bisherige Register* der Sammlungen von Personendaten enthält rund 600 Einträge über die Sammlungen von Personendaten in der Bundesverwaltung. Ziel dieses Registers war, die Ausübung des Auskunftsrechtes zu erleichtern. Es wurde als reine Textdatei in den Sprachen Deutsch, Französisch und Italienisch geführt. Änderungen wurden nicht nachgeführt.

Nach dem DSG müssen sämtliche Datensammlungen der Bundesorgane angemeldet werden. Unter bestimmten Voraussetzungen sind neu auch Datensammlungen privater Personen meldepflichtig. Das bedeutet, dass es zukünftig je zwei Register der Datensammlungen in den Sprachen Deutsch, Französisch und Italienisch geben wird: eins für Datensammlungen der Bundesorgane und eins für private Personen. Die Anmeldungen erfolgen mittels von uns abgegebenen Formularen. Die Entgegennahme der Anmeldung sowie die Aufnahme der Datensammlung in das Register sagt nichts über die Zulässigkeit der Datenbearbeitung in der betreffenden Datensammlung aus.

Für *die Verwaltung der Einträge* wurde eine Software mit der Bezeichnung DATAREG entwickelt. Die Applikation basiert auf einer relationalen Datenbank. Damit wird eine einfache Pflege der Einträge in das Register der Datensammlungen gewährleistet. Die Einträge werden immer auf dem neuesten Stand gehalten. Mit DATAREG werden die Registereinträge erfasst, wobei automatisch eine Registernummer vergeben wird. Alle Angaben vom Anmeldeformular für Datensammlungen werden zwar ins DATAREG übertragen. Es werden jedoch nicht alle Angaben veröffentlicht. Die Erfassung erfolgt dreisprachig. Aus dem Sprachcode der Registereinträge ist die Sprache ersichtlich. Logisch bilden die drei Einträge eine Einheit. Durch Verwendung von dreisprachigen Begriffskatalogen wird sowohl der Arbeitsaufwand für die Erfassung als auch die Fehlermöglichkeiten reduziert. Auf diese

Weise wird auch sichergestellt, dass für einen Begriff immer dasselbe Wort als Übersetzung benutzt wird. Ebenso ist gewährleistet, dass die Übersetzung mit dem Original übereinstimmt und Fehler möglichst ausgeschlossen werden. Werden einzelne Angaben zu den Registereinträgen verändert, werden sämtliche von der Veränderung betroffene Registereinträge automatisch auf den aktuellen Stand gebracht. Dabei wurde darauf geachtet, dass Redundanzen möglichst vermieden werden. Weiter sind verschiedene Such- und Auswertungsfunktionen integriert. Diese werden den Bedürfnissen entsprechend noch erweitert.

Die Register der Datensammlungen werden veröffentlicht. Die Veröffentlichung mit den Daten aus dem DATAREG soll möglichst ohne manuellen Aufwand erfolgen.
Die dafür benötigten Funktionen sollen bis Anfang 95 bereitstehen. Bis zu diesem Zeitpunkt sollten auch alle Anmeldungen im Verwaltungssystem erfasst sein. Die Publikation der Einträge für Bundesorgane wird in seiner Form dem heutigen Register der Sammlungen von Personendaten entsprechen. Das Register der Einträge für private Personen wird alphabetisch nach Branchen und innerhalb der Branchen nach Firmennamen geordnet.

Angepasst an die Häufigkeiten und Erfahrungen der nächsten Publikation könnte zukünftig der Einsatz zusätzlicher Medien für die Anmeldung von Datensammlungen und die Publikation des Registers der Datensammlungen vorgesehen werden. Dafür in Frage kämen sowohl elektronische Speichermedien als auch Datenübertragungseinrichtungen sowie Dienste der Telekommunikation.

3. Anmeldeformulare

Wir haben folgende vier Arten von Formularen erstellt, von denen zwei dem Register der Datensammlungen zugeführt werden sollen:

Anmeldeformular für die Datensammlungen der Bundesorgane: Für die herkömmlichen Anmeldungen wird das gleiche Formular verwendet wie für die vereinfachten oder globalen Anmeldungen. Dieses Formular enthält vor allem den Namen und die Adresse des verantwortlichen Bundesorgans, den Namen oder die Bezeichnung der Datensammlung, die zuständige Stelle, bei der das Auskunftsrecht geltend gemacht werden kann, die gesetzliche Grundlage und den Zweck der Datensammlung, die Kategorien der bearbeiteten Daten, der Datenempfänger und der an der Datensammlung Beteiligten sowie den Kreis der betroffenen Personen und deren ungefähre Anzahl.

Anmeldeformular für Datensammlungen, die von privaten Inhabern geführt werden: Mit Ausnahme der Gesetzesgrundlage und des betroffenen Personenkreises inklusive ungefährer Anzahl der betroffenen Personen sind die geforderten Angaben dieselben wie die für Bundesorgane.

Anmeldeformular für die Übermittlung von Daten durch Bundesorgane ins Ausland: Dieses Formular wird nicht zu Zwecken der Veröffentlichung ausgefüllt, sondern damit wir im Falle einer Übermittlung von Daten ins Ausland überprüfen können, ob im Empfängerland eine unserem Land gleichwertige Datenschutzgesetzgebung besteht.

Anmeldeformular für die Übermittlung von aus privaten Datensammlungen stammenden Daten ins Ausland: Dieses Formular verfolgt denselben Zweck wie das vorherige.

4. Erste Erfahrungen

Im März 1994 sind bei uns etwa hundert Anmeldungen eingetroffen, von denen ein Drittel aus privaten Kreisen stammt. Die Bundesorgane haben Schwierigkeiten, das Anmeldeverfahren in bezug auf ihre Datensammlungen effizient zu organisieren. In nahezu 90 Prozent der Fälle müssen die Anmeldeformulare der Bundesorgane zur Korrektur oder zum Zwecke einer Ergänzung zurückgeschickt werden. Was den Bereich der Sozialversicherungen angeht, so sind insbesondere die Versicherungskassen, die das DSG als Bundesorgane ansieht, da sie eine Bundesaufgabe vollziehen, erstmalig der Anmeldepflicht unterstellt. Diese Kassen wissen in einigen Fällen nicht, ob sie den kantonalen Datenschutzbehörden oder uns gegenüber meldepflichtig sind.
Was den Privatsektor anbelangt, so stammen die Anmeldungen bis jetzt zum grossen Teil von Unternehmen, die im Versand (direktes Marketing) tätig sind. Auch hier müssen die Formulare zum Zwecke einer Ergänzung häufig zurückgeschickt werden. Auch aus anderen Tätigkeitsbereichen hat man sich im Hinblick auf künftige Anmeldungen an unser Sekretariat gewandt. Es handelt sich dabei in erster Linie um Kreditauskunfteien und Versicherungsgesellschaften. Wir möchten abschliessend betonen, dass die privaten Inhaber von Datensammlungen ihre gesetzlichen Verpflichtungen willig erfüllen.

Das Register der Datensammlungen ist ein nicht mehr wegzudenkendes Hilfsmittel für die durch eine Bearbeitung ihrer Daten betroffenen Personen, wenn es darum geht, das Auskunftsrecht geltend zu machen. Das Register erleichtert ebenfalls die Erfüllung unserer gesetzlichen Aufgaben. Um leistungsfähig sein zu können, muss das Register allerdings so zuverlässig und vollständig wie möglich sein. Es erfordert deshalb sowohl von den Inhabern der Datensammlungen als auch von uns eine sorgfältige Arbeit, für die ein langer Atem nötig ist. Aus diesem Grund kann die neue Version des Registers der Datensammlungen erst 1995 veröffentlicht werden.

VI. DER EIDGENÖSSISCHE DATENSCHUTZBEAUFTRAGTE

Um sich kurz die Lage des Sekretariats des EDSB zu vergegenwärtigen, ist es von Nutzen, sich ein Bild über seine verschiedenen Aufgaben zu machen. Das Sekretariat muss gemäss Datenschutzgesetz alle Bundesorgane im Lande, d.h. mehrere tausend Mitarbeiter, in allen Fragen des Datenschutzes beraten und kontrollieren. Das bedeutet Beratung und Kontrolle in bezug auf alle Rechtssetzungsvorhaben sowie bei allen EDV-Projekten der Bundesorgane. Zudem muss auch der gesamte Privatbereich, d.h. all diejenigen Privatpersonen, die in der Schweiz in irgendeinerweise Personendaten bearbeiten, beraten und beaufsichtigt werden. Schliesslich muss auch die direkte Beratung der Bürgerinnen und Bürger gewährleistet werden, weil sich jede betroffene Person sich an den EDSB wenden kann, wenn sie bezüglich des Umgangs von Bundesorganen oder von Privatpersonen mit ihren Daten Probleme

oder Fragen hat. Weitere Aufgaben des EDSB sind: Informationstätigkeit (Referate halten, Tagungen und Konferenzen organisieren und durchführen, Informationsmaterial wie Merkblätter, Leitfäden und Broschüren für die Bearbeitung von Personendaten ausarbeiten und zur Verfügung stellen); das Verfassen des Tätigkeitsberichtes; das Erstellen, Führen und Publizieren des Registers der Datensammlungen; die Zusammenarbeit mit in- und ausländischen Datenschutzbehörden; die Begutachtung der Gleichwertigkeit ausländischer Datenschutzgesetze; die Vertretung der Schweiz in internationalen Gremien (Europarat); die Beratung der Sachverständigerkommission für das Berufsgeheimnis in der medizinischen Forschung, die Überprüfung der Entscheide dieser Kommission sowie Information der Patienten über ihre Rechte.
Für all diese Aufgaben stehen dem EDSB jedoch nur 9,3 Stellen (2 zusätzliche wurden für April dieses Jahres bewilligt) zu Verfügung. Eine sorgfälltige oder nur zufriedenstellende Erledigung aller Aufgaben ist mit so beschränkten Personalressourcen unmöglich.

1. Aufgabenentwicklung

Seit dem Inkrafttreten des DSG steigt die Zahl der Beschwerden und Beratungswünsche ständig an. Sowohl bei den Bundesorganen als auch im privaten Bereich besteht ein grosses Interesse an datenschutzrechtlichen Fragen.
In den Bundesorganen konzentrieren sich die Anfragen, abgesehen von den bereichsspezifischen Fragen, auf die Voraussetzungen der rechtmässigen Weitergabe von Personendaten und der Anmeldung von Datensammlungen.
Im privaten Bereich war ein reges Interesse an der Handhabung von Personendaten im Arbeitsverhältnis (Führung von Personaldossiers, Erteilung von Auskünften usw.) festzustellen. Auch die Frage, wann eine Datensammlung anzumelden ist und wann wegen "Kenntnisnahme" der betroffenen Personen die Anmeldung der Datensammlung nicht notwendig ist, wurde häufig gestellt.
Ein weiterer Punkt von allgemeinem Interesse war die Meldepflicht von Datenübermittlungen ins Ausland.
Von besonderer Bedeutung ist die Tatsache, dass sowohl Dienststellen des Bundes als auch Private öfters telefonisch Auskunft verlangen. Bei diesen Anfragen handelt es sich mehrheitlich um Fragen über die Auslegung des Gesetzes, die Modalitäten des Auskunftsrechts, die Anmeldung und Registrierung von Datensammlungen, Rechtfertigungsgründe für Datenbearbeitungen im privaten Bereich, die Frage der Anwendbarkeit des Gesetzes in den Kantonen und viele andere mehr.

2. Information der Öffentlichkeit

Die Öffentlichkeitsarbeit ist einer der Schwerpunkte der Tätigkeit des EDSB. Die Mitarbeiterinnen und Mitarbeiter und der EDSB selbst haben an verschiedenen Veranstaltungen Referate über den Datenschutz gehalten. Es war erfreulich festzustellen, dass ein grosses Interesse für die Anliegen des Datenschutzes besteht. Leider konnten wir infolge der knappen Personalmittel, die uns zur Verfügung stehen, nicht an allen Veranstaltungen teilnehmen. Doch wir werden uns auch in Zukunft bemühen, soweit wie möglich an solchen Veranstaltungen mitzuwirken.
Am 1. Juli 1993 wurde an einer Pressekonferenz die Öffentlichkeit über das Inkrafttreten des Datenschutzgesetzes informiert.

Am 8. Oktober 1993 veranstaltete unser Sekretariat die erste schweizerische Konferenz der Datenschutzbeauftragten. Es nahmen 29 Vertreterinnen und Vertreter von 19 kantonalen Datenschutzbehörden, ein Vertreter der Schweizerischen Informatikkonferenz und das Sekretariat des EDSB teil. Nach einem Überblick über die Organisation des EDSB und einer Einführung in das DSG fand ein Meinungsaustausch zwischen den Teilnehmern der Konferenz statt. Bei der Veranstaltung wurde der Nutzen eines regelmässigen Erfahrungsaustausches und der Zusammenarbeit zwischen Bundes- und kantonalen Behörden erkannt. Die Teilnehmerinnen und Teilnehmer der Konferenz haben deshalb beschlossen, diese Veranstaltung zu institutionalisieren und jährlich zu veranstalten, um den Datenschutz auf gesamtschweizerischer Ebene zu koordinieren.
Am 4. März 1994 wurde schliesslich das erste Informationstreffen für Organe des Bundes organisiert, welches einen ersten Erfahrungsaustausch zwischen den Bundesbehörden und dem EDSB ermöglichte.
Im Rahmen der allgemeinen Informationstätigkeit wurden zudem vier Broschüren über die Bearbeitung von Personendaten erarbeitet; nämlich: "Die Rechte der betroffenen Personen bei der Bearbeitung von Personendaten", "Leitfaden für die Inhaber von Datensammlungen", "Leitfaden für die Bearbeitung von Personendaten in der Bundesverwaltung"und "Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes". Die ersten drei davon sind bereits publiziert.
Zur Verordnung zum Datenschutzgesetz wurde ein erklärender Kommentar verfasst.
Es ist vorgesehen, in nächster Zukunft weitere Broschüren, Merkblätter und Leitfäden zu verschiedenen Datenschutzthemen zu erarbeiten und zu veröffentlichen.

3. Personelle Ausstattung des Sekretariats des EDSB

Wir haben versucht, die obenerwähnten gesetzlichen Aufgaben sowie die Anfragen von Privatpersonen und aus der Verwaltung schnellstmöglich zu erledigen, doch es gelang uns nicht, allen Tätigkeitsbereichen die notwendige Beachtung zu schenken. Im Gegenteil, infolge der Arbeitsüberlastung der Mitarbeiter haben sich längst Rückstände gebildet. Wir sahen uns daher gezwungen, Prioritäten zu setzen: das Register der Datensammlungen, die Beratung und die Information.
Trotz dieser Massnahmen ist es uns nicht möglich, unsere Aufgaben ohne zusätzliches Personal zufriedenstellend zu erfüllen.

4. Aus- und Fortbildung

Um den Datenschutz umzusetzen, braucht es nebst dem grundsätzlichen Verständnis der Materie sowohl juristische wie auch technisch-organisatorische Spezialkenntnisse. Dies bedeutet, dass Aus- und Weiterbildungen unerlässlich sind.
Die Mitarbeiterinnen und Mitarbeiter des EDSB versuchen, in ihren Wirkungsbereichen einen gewissen Grundbedarf zu decken. Es ist aber unbestritten, dass ein grosser Nachholbedarf besteht, um in diesem komplexen Wirkungsgebiet sachgerechte Lösungen finden zu können.

5. Statistik über die Tätigkeit des Eidgenössischen Datenschutzbeauftragten Zeitraum 1. Juli 1993 bis 30. März 1994

Anzahl der Sitzungen

Arbeitssitzungen	(extern)	264
Konferenzteilnahmen	national	12
	international	5

Anzahl der Stellungnahmen

	Eingänge	Keine Bemerkungen	keine Einwendungen	Beratung/ schriftliche Stellungnahme
Zu Gesetzen	24		1	23
Zu Verordnungen	50	4	1	45
Zu internationalen Vereinbarungen	26		4	22
Zu Anfragen aus dem privaten Bereich	81	1		80
Zu Anfragen aus dem öffentlichen Bereich	180	32		148

6. Das Sekretariat des Eidgenössischen Datenschutzbeauftragten

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

Sekretariat:

Leiter:	Walter Jean-Philippe, Dr. iur.
Stellvertreter:	Buntschu Marc, lic. iur.
Rechtsdienst:	7 Personen
Informatikdienst:	2 Personen
Informationsdienst:	Tsiraktsopulos Kosmas, lic. iur.
Kanzlei:	2 Personen