Eidgenössischer Datenschutzbeauftragter

Tätigkeitsbericht 2000/2001

Der Eidgenössische Datenschutzbeauftragte hat dem Bundesrat periodisch einen Bericht über seine Tätigkeit vorzulegen (Art. 30 Datenschutzgesetz). Der vorliegende Bericht deckt den Zeitraum zwischen 1. April 2000 und 31. März 2001 ab.

INHALTSVERZEICHNIS

*: Originaltext auf Französisch

*: Originaltext auf Französisch

*: Originaltext auf Französisch

VORWORT

Die vernetzte Informationsgesellschaft und die Nutzung des Internets haben das Risiko für die Privatsphäre steigen lassen. Es liegt den neuen Technologien zu Grunde, wie auch viele Umfragen und Studien zeigen, dass Personendaten unkontrolliert von Dritten missbraucht werden können.

Die gegenwärtigen Rechtsvorschriften und die freiwillige Selbstregulierung reichen heute bei Weitem nicht aus, um bei jeder Übertragung von Personendaten einen ausreichenden Schutz zu gewährleisten. Die aktuelle Konzeption des Datenschutzes nur mit starren rechtlichen Bestimmungen zu agieren, ist keine Antwort für ein sich dynamisch entwickelndes Umfeld der globalen Informationsgesellschaft. Deshalb ist es an der Zeit, technische Lösungsansätze für den Schutz der Privatsphäre in der globalen Informationsgesellschaft anzustreben. Dafür ist es jedoch notwendig, dass Multimediadienste konsequent und systematisch datenschutzrechtliche Anforderungen durch datenschutzintegrierende Systemlösungen technisch umsetzen.

Die Technologie, die dafür sorgt, dass Personendaten gespeichert, genutzt und weitergegeben werden, soll auch für den Schutz der Privatsphäre des Bürgers genutzt werden. Dafür müssen technische Verfahren eingesetzt werden, die das Prinzip der Datensparsamkeit umsetzen, die Verwendung von Anonymisierungs- und Pseudonymisierungsverfahren ermöglichen, die Einwilligung des Benutzers zur Erhebung und Nutzung seiner Daten elektronisch verlangen und die Ausübung des Auskunftsrechts elektronisch ermöglichen.

Überdies können Gütesiegel, welche gemeinsame Prüfungs- und Bewertungskriterien von Informationssystemen definieren, zum Schutz der Privatsphäre beitragen. Dafür ist jedoch eine Diskussion auf internationaler Ebene erforderlich, um einen grenzüberschreitenden und gesamteuropäischen Kriterienrahmen zu schaffen. Gütesiegel mit einer objektiven Umsetzung von datenschutzrechtlichen Anforderungen, verbunden mit einer technisch normierten Zertifizierung können einen wesentlichen Baustein zur technologischen Konkretisierung des Datenschutzes auf nationaler und internationaler Ebene bilden.

Damit aber der technologische Ansatz der Umsetzung des Datenschutzes erfolgreich sein kann, muss er von allen im Datenbearbeitungsprozess beteiligten Akteuren (Benutzer, Unternehmen, Staat) akzeptiert werden, praxistauglich sein, den Schutz der Privatsphäre verbessern und marktwirtschaftlich tragbar sein.

Odilo Guntern

ABKÜRZUNGSVERZEICHNIS

BAP	Bundesamt für Polizei
BKP	Bundeskriminalpolizei
BSV	Bundesamt für Sozialversicherung
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit
DAP	Dienst für Analyse und Prävention
DOSIS	Datenverarbeitungssystem zur Bekämpfung des illegalen Drogenhandels
EDI	Eidgenössisches Departement des Innern
EJPD	Eidg. Justiz- und Polizeidepartement
EMRK	Europäische Menschenrechtskommission
ESBK	Eidgenössische Spielbankenkommission
FAMP	Datenverarbeitungssystem zur Bekämpfung der Falschmünzerei, des Menschenhandels und der Pornografie
FMH	Verbindung der Schweizer Ärzte (Foederatio Medicorum Helveticorum)
FZG	Freizügigkeitsgesetz
GEWA	Datenverarbeitungssystem zur Bekämpfung der Geldwäscherei
GwG	Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor
ISA	Informationssystem Ausweisschriften
ISIS	Staatsschutz-Informations-System
ISOK	Datenverarbeitungssystem zur Bekämpfung der organisierten Kriminalität
IV	Invalidenversicherung
JANUS	Gemeinsames Informationssystem der kriminalpolizeilichen Zentralstellen des Bundes
KKJPD	Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren
KKPKS	Konferenz der kantonalen Polizeikommandanten der Schweiz
KVG	Bundesgesetz über die Krankenversicherung
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
RIPOL	Automatisiertes Fahndungssystem
SRO	Selbstregulierungsorganisation
UNO	Vereinigte Nationen
ZAS	Zentrale Ausgleichkasse
ZentG	Bundesgesetz über die kriminalpolizeilichen Zentralstellen des Bundes

I. AUSGEWÄHLTE THEMEN

1. Polizeiwesen

1.1. Projekt «Neuer Schweizer Pass»

Im Rahmen der Entwicklung des neuen Schweizer Passes wurde der Entwurf eines Bundesgesetzes erarbeitet, das künftig die Rechtsgrundlage für das Informationssystem Ausweisschriften (ISA) bilden soll. Wir beteiligten uns an der «Arbeitsgruppe Recht» sowie am «Projektausschuss» des Projekts Ausweisschriften des Bundesamtes für Polizei und haben uns in verschiedenen Projektphasen eingeschaltet. In unseren Äusserungen gingen wir hauptsächlich auf die Problematik der Zugriffsrechte zum ISA-System ein; wir forderten, dass es sich weiterhin um eine Administrativdatenbank, keine Polizeidatenbank, handeln müsse, und äusserten uns zum Prozess der Personalisierung und der Erstellung der Pässe.

Am 28. Juni 2000 verabschiedete der Bundesrat die Botschaft zum Bundesgesetz über die Ausweise für Schweizer Staatsangehörige. Die Annahme der Botschaft markiert für den Datenschutz eine wichtige Etappe in diesem breit angelegten Projekt. Der dem Parlament unterbreitete Gesetzesentwurf soll künftig die Rechtsgrundlage des Informationssystems Ausweisschriften (ISA) darstellen und die geltenden Verordnungen über den Schweizer Pass und über die Identitätskarte ersetzen.

Zahlreiche Fragen im Rahmen der Vorbereitung der Botschaft berührten direkt den Datenschutz. Wir arbeiteten in der Lösungssuche eng mit dem Bundesamt für Polizei (BAP) zusammen und beteiligten uns insbesondere an der «Arbeitsgruppe Recht» und am «Projektausschuss» des Projekts Ausweisschriften. Nach den ersten Arbeitsschritten sahen wir uns veranlasst, vor der Gefahr zu warnen, das ISA-System könnte sich - wegen bestimmter geplanter Zugriffsrechte für Polizeibehörden - von einer Administrativdatenbank in eine Polizeidatenbank verwandeln. Ausserdem wiesen wir im Mitberichtsverfahren an den Bundesrat bei der Eröffnung des externen Vernehmlassungsverfahrens auf das Problem hin.

Im Laufe der Projektänderungsphase, die auf das externe Vernehmlassungsverfahren folgte, wurde vor allem das Zugriffsrecht abgeändert. Wir äusserten uns zur endgültigen Fassung des Botschaftsentwurfs und betonten, dass die Zugriffsrechte per Abrufverfahren, die dem Grenzwachtkorps, den von den Kantonen bestimmten Polizeidiensten und dem für die Bearbeitung von Identitäts-

kontrollgesuchen aus dem Ausland zuständigen Bundespolizeidienst gewährt werden, nur für klare und gesetzlich verankerte Zielsetzung galten (nämlich nur zur Identitätskontrolle oder zur Registrierung von Ausweisverlusten) und unserer Auffassung nach dem Verhältnismässigkeitsprinzip genügten. Wie aus der Botschaft eindeutig hervorgeht, dürfen die Zugriffsrechte nur im Rahmen der Aufdeckung von Missbräuchen zur alltäglichen Identitätskontrolle ausgeübt werden.

Ausserdem plädierten wir dafür, die Wechselwirkung zwischen dem Informationssystem Ausweisschriften ISA und dem automatisierten Fahndungssystem RIPOL im Gesetz klar zu regeln. Der Gesetzesentwurf sieht denn auch bei Verlust von Identitätsausweisen einerseits die polizeiliche Meldepflicht und Erfassung im RIPOL-System und andererseits die automatische Übermittlung der Verlustanzeige vom RIPOL-System an das ISA-System vor.

Was die Produktion des neuen Schweizer Passes betrifft, befürworteten wir schliesslich den Beschluss des Eidgenössischen Justiz- und Polizeidepartements und des Eidgenössischen Finanzdepartements, den Auftrag zur Gestaltung der Pässe einem Privatunternehmen zu erteilen, aber die Personalisierung und Herstellung des Passes innerhalb der Bundesverwaltung abzuwickeln. Das Unternehmen, das den Auftrag erhält, liefert die verschiedenen Bestandteile des neuen Schweizer Passes (Papier, Einbandmaterial, Sicherheitselemente und Produktionsmaschinen), während das Bundesamt für Bauten und Logistik für die Personalisierung und Ausfertigung der Pässe verantwortlich ist. Diese Lösung garantiert eine unabhängige und fälschungssichere Herstellung der Ausweise innerhalb der Bundesverwaltung, zumal die Personendaten in der Hand der Bundesstellen bleiben und nicht im Outsourcing an eine Privatfirma vergeben werden.

Wir werden unsere Begleit- und Beratungstätigkeiten im Rahmen des Projekts fortsetzen. Dazu werden wir die Verhandlungen im Parlament weiter verfolgen, uns an etwaigen Anhörungen in Kommissionen beteiligen und Stellungnahmen zum Verordnungsentwurf, der derzeit im BAP ausgearbeitet wird, formulieren.

1.2. Reorganisationprojekte Strupol und Usis

Zur Überprüfung der Funktionsstrukturen der schweizerischen Polizeibehörden wurden zwei Projekte entwickelt: Mit dem Projekt «Strupol» erhielt das Bundesamt für Polizei den Auftrag, die Strukturen des Polizeibereichs des Bundes zu überprüfen. Beim Projekt «Usis» soll eine vom Eidgenössischen Justiz- und Polizeidepartement sowie von der Konferenz der Kantonalen Justiz- und Polizeidirektoren beauftragte Projektgruppe das globale System der Inneren Sicherheit Schweiz überprüfen. Da sich beide Projekte

erheblich auf die Datenbearbeitung durch Polizeibehörden auswirken, wurden wir aufgefordert, uns daran zu beteiligen.

Hauptziel der Projektgruppe «*Strupol*» war die optimale Eingliederung der neuen Funktionen in das Bundesamt für Polizei (BAP), vor allem im Rahmen der Überführung der Bundespolizei und des Sicherheitsdienstes der Bundesverwaltung aus der Bundesanwaltschaft in das BAP. Im Laufe dieser Arbeiten waren wir regelmässig beratend tätig und wiesen vor allem auf die rechtlichen Folgen (Änderung von Gesetzen und Verordnungen) hin, die einige zur Diskussion stehende Umstrukturierungsvarianten beinhalteten. Ausserdem betonten wir, dass die Konsequenzen der Projekte für die Datenbearbeitung durch die verschiedenen Polizeieinheiten hinsichtlich der geltenden Gesetzesnormen und der gewährten Zugriffsrechte zu überprüfen seien.

Die Arbeiten mündeten in einer Umstrukturierung zahlreicher Dienststellen innerhalb des BAP sowie in der Überführung verschiedener Einheiten in andere Ämter (so werden z.B. das Strafregister, die Rechtshilfe und die Auslieferung in das Bundesamt für Justiz transferiert). Die Veränderungen erforderten eine Anpassung zahlreicher Verordnungen des Bundesrates, die wir aus datenschutzrechtlicher Sicht prüften.

Auf der Grundlage der Resultate des Projekts «*Strupol*» beschloss das Eidgenössische Justiz- und Polizeidepartement (EJPD), die nachrichtendienstlichen und die kriminalpolizeilichen Aufgaben, welche bislang von der Bundespolizei und den kriminalpolizeilichen Zentralstellen geleistet wurden, neu zu verteilen: Der neue Dienst für Analyse und Prävention (DAP) beschafft - nach den Vorschriften des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit - Informationen insbesondere über Terrorismus, gewalttätigen Extremismus und verbotenen Handel mit Waffen. Er wertet diese Informationen zuhanden der politischen Behörden und der Strafverfolgungsbehörden aus. Die neue Bundeskriminalpolizei (BKP) führt alle gerichtspolizeilichen Vorermittlungs- und Ermittlungsverfahren in Bundeszuständigkeit durch. Die neue Gliederung ist am 1. Januar 2001 in Kraft getreten. Wir werden uns vor allem mit der Verteilung der Datenbearbeitungsaufgaben auf die verschiedenen Polizeistellen noch eingehend auseinander setzen.

Das Projekt «*Usis*» ging über die im BAP ergriffenen Reorganisationsmassnahmen hinaus. Die Projektgruppe «*Usis*» wurde vom EJPD und der Konferenz der Kantonalen Justiz- und Polizeidirektoren (KKJPD) beauftragt, das gesamte System der Inneren Sicherheit Schweiz zu überprüfen. Die Hauptaufgabe besteht in der Untersuchung der Aufgabenverteilung zwischen Bund und Kantonen im Polizeibereich.

Die Arbeitsgruppe untersuchte zunächst die geltende Aufgabenverteilung im Polizeibereich sowie die finanziellen Aufwendungen. Wir verlangten, alle geplanten Veränderungen in der polizeilichen Zusammenarbeit auch im Lichte der Gesetzesgrundlagen für den Austausch von Personendaten unter Polizeibehörden zu prüfen. Ausserdem machten wir das Projektteam «Recht» darauf aufmerksam, dass konkret abgeklärt werden müsse, welche Informatiksysteme der Polizei das Projekt «*Usis»* betreffe. Die Gruppe begann mit der Untersuchung der Polizeikompetenzen auf Bundes- und Kantonsebene, stellte die geltenden Gesetze zusammen und untersuchte, welche Normen insbesondere aus datenschutzrechtlichen Gründen gegebenenfalls revidiert bzw. geschaffen werden müssen.

Parallel zum Projekt «*Usis»* der KKJPD läuft ein Projekt der Konferenz der kantonalen Polizeikommandanten der Schweiz (KKPKS) unter dem Namen «Polizei XXI». Ziel des Projekts ist, die Standpunkte der Kantone zur Zusammenarbeit untereinander, mit dem Bund und mit dem Ausland in Erfahrung zu bringen. Im Laufe des Jahres 2000 wurde der Projektzeitplan von «*Usis»* abgeändert, damit die Ergebnisse des Projekts «Polizei XXI» einbezogen werden können. Wir werden unsere Mitwirkung am Projekt «*Usis»* fortsetzen und die Einhaltung der Datenschutzauflagen in der geplanten Reorganisation des Polizeibereichs im Auge behalten.

1.3. Datenbearbeitungen im Bereich der Glücksspiele und Spielbanken (Casinos)

Bei der Einreichung von Konzessionsgesuchen durch Casinos müssen diese unter anderem detaillierte Angaben über Verwaltungsräte und am Spielbetrieb beteiligtes Personal machen. Da das Bundesgesetz über Glückspiele und Spielbanken erst am 1. April 2000 in Kraft getreten ist, kann im jetzigen Zeitpunkt noch nicht abschliessend beurteilt werden, welche Angaben verhältnismässig sind. Es gilt abzuklären, welche Daten für einen sicheren und transparenten Spielbetrieb notwendig sind. Zudem soll sichergestellt werden, dass mit den Angaben die Kriminalität und die Geldwäscherei in oder durch Spielbanken verhindert wird. In zwei bis drei Jahren sollte eine Evaluation der Sachlage stattfinden.

Am 1. April 2000 ist das Bundesgesetz über Glückspiele und Spielbanken (Spielbankengesetz) in Kraft getreten. Die Spielbanken hatten sechs, resp. zwölf Monate Zeit, um bei der Eidgenössischen Spielbankenkommission (ESBK) zuhanden des Bundesrats ein Konzessionsgesuch einzureichen. Im Zusammen-

hang mit den dafür von der ESBK verlangten Unterlagen und Angaben gelangten einige Anfragen an uns.

In einem Fall war zu überprüfen, welche Angaben eine bei einem Casino angestellte Person im Rahmen des Konzessionsgesuchs machen muss. Bei ihrer Tätigkeit musste diese Person unter anderem Geld zählen, Münzen und Währungen wechseln sowie bei den Spielautomaten Schecks ab Fr. 200.-- auszahlen. Gemäss ESBK galt diese Person als «am Spielbetrieb beteiligtes Personal» und musste gemäss der Spielbankenverordnung einen detaillierten Lebenslauf einreichen und einen ausführlichen Fragebogen der ESBK ausfüllen. Dabei war zu beachten, dass bei der Erteilung einer Konzession überprüft werden muss, ob das Casino einen sicheren und transparenten Spielbetrieb gewährleisten kann und die Verhinderung der Kriminalität und der Geldwäscherei in oder durch Spielbanken sichergestellt ist. Allerdings war und ist es äusserst schwierig festzustellen, welche Unterlagen und Angaben zu einem detaillierten Lebenslauf gehören und/oder für die Gewährleistung der Überwachung des Spielbetriebs und damit auch der Verhinderung der Geldwäscherei nötig und geeignet (Verhältnismässigkeitsprinzip) sind. Dies trifft umso mehr zu, als das Spielbankengesetz erst am 1. April 2000 in Kraft getreten ist und auf diesem Gebiet bisher noch nicht viele Erfahrungen gesammelt werden konnten. Nach Überprüfung der verlangten Angaben und Unterlagen kamen wir zum Schluss, dass diese datenschutzrechtlich grösstenteils in Ordnung waren. Wir wiesen die betroffene Person jedoch auf einige Punkte hin, die unseres Erachtens gewisse Vorbehalte hervorrufen. Trotzdem rieten wir der Person, alles wie verlangt einzureichen. Die ESBK wiesen wir darauf hin, dass nach Ablauf von zwei bis drei Jahren eine erneute Evaluation der Situation angezeigt wäre. Dabei müsse dann überprüft werden, welche Daten für den verfolgten Zweck - insbesondere Bekämpfung der Geldwäscherei - wirklich nötig und geeignet sind.

In einem anderen Fall ging es um die Frage, welche Angaben und Unterlagen bestimmte Personen - wie zum Beispiel Verwaltungsräte - einreichen müssen. Gemäss dem Spielbankengesetz müssen diese Personen einen guten Ruf geniessen und Gewähr für eine einwandfreie Geschäftstätigkeit bieten. Die für den Nachweis des guten Rufs verlangten Dokumente werden sodann in der Spielbankenverordnung aufgeführt. Für die aufgeführten Dokumente bestand und besteht somit eine gesetzliche Grundlage, weshalb wir diesbezüglich keine Einwände hatten. Daneben verlangte die ESBK eine Liste sämtlicher Verwaltungsratsmandate der Verwaltungsratsmitglieder der Spielbanken. Die ESBK hielt fest, dass dies zum Lebenslauf eines Verwaltungsratsmitglieds gehören würde. Dabei stützte sie sich auf die Praxis der Eidgenössischen Bankenkommission. Aus diesen Gründen hatten wir auch gegen die Einreichung der verlangten Dokumente nichts einzuwenden. Wir wiesen die ESBK jedoch auch in diesem Fall darauf hin, dass nach einiger Zeit eine Evaluation der Sachlage stattfinden müsse.

Zu klären war schliesslich, welche Unterlagen die ESBK im Rahmen ihrer Beaufsichtigungsfunktion verlangen darf. Dabei kann die ESBK überprüfen, ob die Spielbank ihrer Meldepflicht nachgekommen ist. Dies kann sie jedoch nur machen, wenn sie die gleichen Unterlagen verlangen kann wie bei einer Konzessionserteilung. Braucht die ESBK zur Wahrnehmung ihrer Beaufsichtigungsaufgaben weitere, weder im Spielbankengesetz noch in der Verordnung vorgesehene Personendaten, müssten dafür die entsprechenden gesetzlichen Grundlagen geschaffen werden.

1.4. Erfahrungen mit dem indirekten Auskunftsrecht

Das «indirekte» Auskunftsrecht ist einerseits im Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit für das Staatsschutz-Informations-System (ISIS) vorgesehen. Andererseits gilt es auch gemäss dem Bundesgesetz über die kriminalpolizeilichen Zentralstellen des Bundes für die Systeme JANUS (bisher DOSIS, ISOK und FAMP) und GEWA. Betreffend das bei dessen Ausübung anzuwendende Verfahren konnten in beiden Fällen weitere Erfahrungen gesammelt werden.

Auch im vergangenen Jahr trafen verschiedene «indirekte» Auskunftsgesuche bei uns ein. Dabei fällt auf, dass die Anzahl der Gesuche gemäss dem Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) für das Staatsschutz-Informations-System ISIS in letzter Zeit leicht abgenommen hat. Dagegen stieg die Anzahl der zu behandelnden «indirekten» Auskunftsgesuche gemäss dem Bundesgesetz über die kriminalpolizeilichen Zentralstellen des Bundes (ZentG) an. Immer häufiger sind zudem diejenigen Personen, die ihr Auskunftsrecht sowohl nach BWIS als auch nach ZentG ausüben.

Im letzten Tätigkeitsbericht (siehe 7. Tätigkeitsbericht 1999/2000, S. 11 ff.) wurde bereits darauf hingewiesen, dass in enger Zusammenarbeit mit den einzelnen Einheiten des Bundesamts für Polizei (BAP) ein klares, einheitliches Verfahren zum Ablauf der Ausübung der «indirekten» Auskunftsrechte erarbeitet worden war. In diesem Zusammenhang konnten mit den betroffenen Stellen unterschiedliche Erfahrungen gesammelt werden. Diesbezüglich ist noch darauf hinzuweisen, dass die Systeme ISOK, DOSIS und FAMP der kriminalpolizeilichen Zentralstellen auf den 1. Juli 2000 in ein einziges Informationssystem namens JANUS zusammengeführt wurden. Auf die Ausübung der Auskunftsrechte hatte dies allerdings keinen Einfluss.

Die Zusammenarbeit mit der Bundespolizei (seit 1. Januar 2001 Dienst für Analyse und Prävention), die für das ISIS-System zuständig ist, verlief rei-

bungslos. Für alle Auskunftsgesuche konnte hier das erarbeitete einheitliche Verfahren angewendet werden.

Im Zusammenhang mit verschiedenen Auskunftsgesuchen nach ZentG verlief die Überprüfung bei der Meldestelle für Geldwäscherei für das System GEWA ohne Hindernisse. Für das System JANUS dagegen mussten wir an die kriminalpolizeilichen Zentralstellen des Bundes eine Empfehlung richten, um einige Unstimmigkeiten berichtigen zu lassen. Dabei ging es unter anderem um ein nicht erfasstes sowie ein nicht auffindbares Dokument. Vor allem aber wiesen wir in der Empfehlung darauf hin, dass auch bei den kriminalpolizeilichen Zentralstellen des Bundes das gleiche Verfahren wie bei der Bundespolizei angewendet werden sollte. Das BAP akzeptierte die Empfehlung, korrigierte die aufgezeigten Unstimmigkeiten und machte eine schriftliche Zusammenfassung des anzuwendenden Verfahrens. Darauf konnten die noch hängigen «indirekten» Auskunftsgesuche überprüft werden.

Beim JANUS-System handelt es sich um ein reines Informationssystem. Dies hat zur Folge, dass nicht alle Papier-Unterlagen in das System aufgenommen werden. Zudem werden verschiedene Informationen direkt von den Kantonen in das System eingegeben, wobei das BAP oft keine Kopie der Unterlagen in Papierform erhält. Unter diesen Bedingungen kann das BAP nicht gewährleisten, dass bei der Behandlung der Gesuche sämtliche Personendaten der betroffenen Person, die durch die kriminalpolizeilichen Zentralstellen des Bundes bearbeitet werden, überprüft werden können. Das im ZentG geregelte indirekte Auskunftsrecht bezieht sich aber sowohl auf das Informationssystem JANUS, als auch auf die Unterlagen in Papierform. Aus diesen Gründen haben wir das BAP darauf hingewiesen, dass es eine Lösung finden müsse, die die vollständige Anwendung des Auskunftsrechts nach dem ZentG erlaubt.

2. Telekommunikation und Post

Telekommunikation

2.1. Staatliche Überwachung von Post- und Fernmeldeverkehr

Das neue Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs, das voraussichtlich noch in diesem Jahr in Kraft treten wird, ist insgesamt mit den generellen Datenschutzgrundsätzen vereinbar. Das Gesetz wird gelten für alle staatlichen Organe, für Einrichtungen, die der Konzessions- oder Bekanntmachungspflicht unterliegen und Post- oder Fernmeldedienste anbieten. Auch ist es anwendbar für Inter-

net Service Provider (ISP), wenn bei Strafverfahren auf Bundes- oder Kantonsebene die Überwachung per Post oder Fernmeldewesen angeordnet und ausgeführt wird.

Die im November 1998 durch die Rechtskommission des Nationalrates eingesetzte Subkommission «Telefonüberwachung» (siehe 6. Tätigkeitsbericht 1998/1999, S. 15-17) hat 1999 einen Bericht vorgelegt, der zum Entwurf des Bundesrates vom 1. Juli 1998 einen Gegenentwurf mit folgenden Schwerpunkten enthielt:

- eingeschränkter Geltungsbereich des Gesetzes; die Überwachung zur Verhütung eines Deliktes fällt weg und die Überwachung des Zahlungsverkehrs der Post ist an die der Banken angeglichen;
- deutlich reduzierter Deliktekatalog für zulässige Überwachungen; in den Katalog aufgenommen wurden nur besonders schwerwiegende Delikte oder solche, bei deren Begehen der Post- oder Fernmeldeverkehr eine Schlüsselrolle spielen;
- restriktivere Voraussetzungen für die Möglichkeit der Überwachung;
- die Einrichtung von Direktanschlüssen wird im Gesetz geregelt; eine derartige Überwachung ist nur zulässig, wenn keine überwiegenden Interessen von Dritten beeinträchtigt werden;
- grundsätzlich ist die Überwachung von Personen mit Zeugnisverweigerungsrecht aufgrund des Berufsgeheimnisses verboten; Ausnahmen werden im Gesetz genau geregelt;
- verstärkte Kontrolle der Behörde, die eine Überwachung anordnet, durch die Genehmigungsbehörde.

Dieser Gegenentwurf fand unsere Zustimmung, da er die schutzwürdigen Interessen der betroffenen Personen besser berücksichtigt.

Im Dezember 1999 wurde der Gegenentwurf der Rechtskommission des Nationalrates von letzterem genehmigt. Bei der Prüfung des Gesetzesentwurfs durch den Ständerat hat dessen Rechtskommission unter anderem die Aufnahme einer neue Vorschrift vorgeschlagen. Diese soll die Anbieter von Fernmeldediensten verpflichten, Teilnehmer ohne Abonnement während mindestens zwei Jahren nach Eröffnung einer Geschäftsverbindung in der Mobiltelefonie zu identifizieren und auf Anfrage die Verkehrs- und Rechnungsdaten zu liefern. Dieser Vorschlag wurde im Juni 2000 durch den Ständerat angenommen. Im September 2000 bekräftigte der Nationalrat seine Position, Benutzer von Mobiltelefonen mit Prepaid-Karten nicht zu registrieren. An dieser unterschiedlichen Auffassung hielten beide Räte weiterhin fest, bis die Schlichtungskonferenz im Oktober 2000 vorschlug, sich der Position des Nationalrates anzuschliessen. Dieser Vorschlag wurde angenommen. Unserer Auffassung nach ist die Identifikation und die Registrierung der Käufer von Prepaid-Karten für die Mobiltelefonie weder notwendig noch geeignet, das erwünschte Ziel - nämlich die Verbrechensbekämpfung - zu erreichen. Eine zusätzliche Datenbearbeitung würde die Gefahr neuer Missbräuche mit sich bringen und verstösst gegen das Ver-

hältnismässigkeitsprinzip. Im Februar 2000 haben wir diesen Standpunkt erneut vor der Subkommission «Telefonüberwachung» der Rechtskommission des Ständerates verteidigt.

Das neue Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs, das voraussichtlich noch in diesem Jahr in Kraft treten wird, tritt an die Stelle der in der Bundesgesetzgebung über die Strafrechtspflege enthaltenen einschlägigen Bestimmungen. Hier ist zu erwähnen, dass das neue Gesetz nicht nur für die im Rahmen eines Bundesstrafprozesses angeordnete und durchgeführte Überwachung des Post- und Fernmeldeverkehrs Anwendung finden wird, sondern ebenfalls im Rahmen kantonaler Strafverfahren. Die zur Ausführung eines internationalen Rechtshilfeantrages in Strafsachen angeordneten und durchgeführten Überwachungen fallen ebenfalls in den Geltungsbereich des neuen Gesetzes, das sowohl für Anbieter von Post- und Fernmeldediensten als auch für Internet Service Provider gilt.

Post

2.2. Die Nachsendeformulare der Post und die Adressaktualisierung (Post/DCL)

Die bereits längere Zeit dauernde Diskussionen um die Problematik der Nachsendeformulare der Post und der Adressaktualisierung kam im letzten Jahr einen Schritt weiter. Die Post hat nun akzeptiert, die via Umzugsformulare erhobenen Daten nur dann Dritten für die Adressaktualisierung zur Verfügung zu stellen, wenn die Postkunden damit einverstanden sind. Kritisiert wurde von uns die enorme Preisdifferenz für Kunden, die einer Adressaktualisierung widersprechen, sowie die teils schwer verständlichen Formulierungen auf den Formularen.

Die schweizerische Post bietet (siehe auch 7. Tätigkeitsbericht 1999/2000, S. 24) für Kunden, die umziehen, den Nachsendeauftrag an. Mit einem Formular werden die geänderten Adressangaben erfasst, um die Postsendungen an die neue Adresse weiterleiten zu können. Das Weiterleiten von Sendungen mit einer alten und nunmehr unrichtigen Adresse verursacht hohe Kosten, weshalb die Post alles daran setzt, dass möglichst viele Absender von Postsendungen möglichst schnell in den Besitz der neuen Adresse kommen und von vornherein korrekt adressieren. Zusammen mit der Firma Data Care AG bietet die Post die Dienstleistung «MAT[CH]move» an, die eine Aktualisierung von Post-Adressen umfasst.

Zu Beginn des Jahres 2001 hat die Post nun neue Formulare eingeführt, bei denen das Recht, eine Adressaktualisierung für Dritte abzulehnen, den Kunden «offiziell» zugestanden wird. Dies haben wir seit längerer Zeit gefordert. Der umziehende Kunde kann nun seine Entscheidung mit einem Kreuz dartun. Wird die Adressaktualisierung für Dritte nicht akzeptiert, bedeutet dies für den Kunden einen finanziellen Mehraufwand.

Im letzten Jahr hat der Bundesrat auf Antrag der Post bzw. des UVEK die Postverordnung geändert. Es ist nun explizit erwähnt, dass die Post Adressen von Kunden Dritten für das Nachführen ihrer eigenen Adressdatensammlungen zur Verfügung stellen kann, sofern die betroffene Person eine Bearbeitung nicht ausdrücklich untersagt hat. Diese Bestimmung gibt der Post allerdings keine zusätzlichen Datenbearbeitungsmöglichkeiten, da lediglich die ohnehin im Datenschutzrecht vorgesehenen Einwilligungserfordernisse beschrieben werden.

Im Sinne einer besseren Transparenz für den Kunden haben wir der Post verständlichere Formulierungen des Kleingedruckten der Formulare vorgeschlagen. Beispielweise wird vom «Absender» gesprochen, der Adressen aktualisieren lassen kann. Die Adressaktualisierung kann jedoch jeder nutzen, unabhängig davon, ob er eine Sendung aufzugeben beabsichtigt oder einen nicht postalischen Zweck verfolgt.

Nicht einverstanden waren wir mit der enormen Preiserhöhung für Kunden, die einer Adressaktualisierung widersprechen. Bezahlten diese bis Ende 2000 10 Franken pro Jahr für die Nachsendung, waren es ab 2001 20 Franken pro Monat, auf ein Jahr gerechnet eine Preissteigerung um das 24-fache oder 2‘300 %. Ein Preisunterschied ist durchaus gerechtfertigt, da in der Regel ein tatsächlicher Mehraufwand der Post erfolgt, falls einer Aktualisierung nicht zugestimmt wird. Eine derart extreme Differenz verletzt allerdings das informationelle Selbstbestimmungsrecht der betroffenen Personen. Wir sahen uns daher gezwungen, in dieser Sache eine Empfehlung gegen die Post zu erlassen. Die Post hat unsere Empfehlung abgelehnt und wir haben diese ans UVEK weitergezogen.

Es bleibt zu erwähnen ist, dass eine Person, die umzieht, der Post nicht unbedingt einen Nachsendeauftrag erteilen muss. Es ist durchaus auch möglich - wenn auch aufwändiger - , Personen, Firmen und Behörden direkt über die neue Adresse zu informieren. Werden trotzdem noch Sendungen an die bisherige Adresse geschickt, werden diese als unzustellbar an den Absender zurückgeschickt.

3. INTERNET und datenschutzfreundliche Technologien

3.1. Datenschutzverletzungen im Internet

Beinahe täglich werden wir mit mehr oder weniger gravierenden Datenschutzverletzungen im Internet konfrontiert. Im Nachfolgenden möchten wir einige Beispiele wiedergeben.

- Bei einem Internetprovider waren die Benutzernamen und Passwörter der E-Mail-Accounts irrtümlicherweise via Internet zugänglich. Dies führte automatisch dazu, dass Suchmaschinen die Daten sammelten und bei Übereinstimmung als Suchresultate ausgaben. Mit den Angaben konnten die elektronische Post nicht nur gelesen werden, sondern es konnten auch Meldungen verschickt oder gelöscht werden. Nachdem das Leck von einem Journalisten entdeckt wurde, behob die betroffene Firma dieses sofort. Grund der Panne war ein simpler, aber folgenschwerer Konfigurationsfehler, der offenbar mehrere Wochen bestand, ohne dass die Firma diesen selbst bemerkte. Dies führte zu einer Überprüfung der technischen und organisatorischen Massnahmen.

- Bankkunden wurden durch Medienberichte aufgeschreckt, ihre Zahlungsinformationen samt Adresse seien im Internet frei zugänglich gewesen. Es handelte sich keineswegs um eine Sicherheitslücke des Online-Banking-Systems der betreffenden Bank. Die Daten waren unabsichtlich in einen Testbereich gespiesen worden, der für fiktive Daten gedacht und daher bewusst nicht geschützt war. Dieser Fall zeigt einmal mehr, dass auch mit den besten technischen Sicherheitsmassnahmen nicht verhindert werden kann, dass sensible Daten in einen Bereich des Netzes gespiesen werden, der ausdrücklich für einen allgemeinen Zugang geschaffen wurde (Testbereich, Newsgroups, Homepages etc.) Irrtümer sind bekanntlich menschlich und sie werden nie gänzlich zu vermeiden sein. Allerdings müssen die Ablaufprozesse so gestaltet sein, dass einzelne Fehlhandlungen nicht zu einem Desaster führen, sondern – falls nötig durch mehrfache Kontrollen – aufgefangen werden.

- Auch in diesem Jahr mussten wir bei Betreibern von Webcams intervenieren. Immer wieder werden auf öffentlichen Strassen oder Plätzen solche Live-Kameras installiert. Da von den betroffenen Personen, die sich an diesen Orten aufhalten, keine Einwilligung verlangt werden kann, müssen die Kameras so konfiguriert werden (Aufnahmewinkel, Auflösung), dass die Personen nicht erkennbar sind.

3.2. P3P – eine technische Grundlage zum Selbstdatenschutz

Der technische Standard «Platform for Privacy Preferences Project (P3P)» ist eine wichtige Grundlage, um den Selbstdatenschutz im Internet zu unterstützen. Mit P3P sollen Browser künftig automatisch überprüfen, ob die vom Nutzer eingegebenen Datenschutzpräferenzen mit der Praxis des Webangebotes übereinstimmen.

P3P ist ein technischer Standard der vom World Wide Web Consortium (W3C) entwickelt wurde. Bei der Implementierung von P3P in Webangebote und Browser können die Benutzer entscheiden, ob und welche Personendaten sie über sich selbst preisgeben möchten. Wenn das Webangebot eine Datenschutzerklärung ausweist, erhält der Nutzer automatisch eine Meldung, wie Personendaten auf diesem Webangebot bearbeitet werden. Zudem erhält der Webnutzer eine Warnmeldung, sofern die Datenbearbeitungen der Website mit seinen Nutzungspräferenzen nicht übereinstimmen.

Grundvoraussetzung für die erfolgreiche Einführung und Nutzung ist die Einbindung dieses Standards durch die Webbetreiber und Dienstleistungsanbieter im Internet. Denn sofern ein Webanbieter sein Angebot nicht P3P-fähig gestaltet hat, funktioniert die automatische Überprüfung nicht. P3P kann ohne passende technische Umgebung nicht funktionieren.

Wir sind der Ansicht, dass P3P eine Hilfe für Internetbenutzer ist. P3P unterstützt den Einzelnen bei der Kontrolle seiner Personendaten, indem er ihm die Möglichkeit gibt zu wissen, welche seiner Daten in welchem Umfang und in welcher Art bearbeitet werden. Somit wird die Bearbeitung von Personendaten für den Einzelnen transparenter und folglich wird auch das Vertrauen der Benutzer gegenüber Internet-Unternehmen gestärkt. Deshalb raten wir Dienstleistungsanbietern im Internet standardisierte maschinenlesbare Datenschutzerklärungen zu erarbeiten, die den Benutzern und potenziellen Kunden eine transparente Information über die Verwendung ihrer Daten geben.

4. Datenschutz und E-Commerce

4.1. Notwendige Elemente für die Vergabe eines Gütesiegels im E-Commerce aus datenschutzrechtlicher Sicht

Der globale Charakter des elektronischen Geschäftsverkehrs (E-Commerce) bringt einen intensiven Austausch von Personendaten mit sich, der unter Umständen die Privatsphäre der betroffenen Personen verletzen kann. Deshalb ist es von grösster Be-

deutung, dass die Grundprinzipien des Datenschutzes auch im Umfeld des E-Commerce Anwendung finden.

Um das Vertrauen der Benutzer in den E-Commerce zu stärken, sollen - wie dies auch vom DSG vorausgesetzt wird - die Anbieter die Kundendaten transparent bearbeiten. Sie müssen die Benutzer informieren, welche Personendaten sie für welchen Zweck bearbeiten möchten. Aufgrund dieser Überlegungen begrüssen wir die Schaffung eines Gütesiegels, das u.a. die datenschutzkonforme Bearbeitung von Personendaten garantiert und somit das Vertrauen der Kunden in den E-Commerce stärkt.

Bei einem Gütesiegelverfahren gilt als Grundvoraussetzung, dass die gesetzlichen Anforderungen für den Schutz der Privatsphäre mittels einer Normierung technisch umgesetzt werden. Für die Wirksamkeit eines Gütesiegels müssen aus datenschutzrechtlicher Sicht folgende Anforderungen und Prüfungskriterien berücksichtigt werden:

Verlässlicher Prozess bei der Vergabe des Gütesiegels

Die Vergabe des Gütesiegels darf nur über einen transparenten Vergabeprozess mit nachvollziehbaren Prüfungskriterien erfolgen. Deshalb muss sichergestellt werden, dass das Verfahren zur Erteilung des Gütesiegels sowie die Prüfungskriterien klar definiert und in einer verbindlichen Norm festgelegt werden. Der somit klar festgelegte Zertifizierungsvorgang hat anschliessend zur Vergabe des Gütesiegels zu führen durch eine dafür geeignete Institution im Rahmen eines Auditverfahrens.

Einhaltung und Umsetzung der gesetzlichen Datenbearbeitungsgrundsätze

Vor der Vergabe des Gütesiegels ist die Einhaltung der gesetzlichen Anforderungen für die Bearbeitung von Personendaten über den Zertifizierungsvorgang zu überprüfen. Deshalb müssen insbesondere folgende Anforderungen geprüft werden:

- Transparente Information an den Benutzer/Kunden (z.B. Privacy Policy).
- Erfüllung der gesetzlichen Anforderungen bei Datenbearbeitungen (wie Kriterien zur Speicherung, Löschung und Weitergabe von Personendaten).
- Gewährung von Auskunfts- und Berichtigungsrecht sowie Klagerechte bei Streitfällen oder Persönlichkeitsverletzungen.
- Gewährung eines Wahlrechts an die Benutzer/Kunden für die Verwendung seiner Daten.
- Gewährung der Datensicherheit durch technisch-organisatorische Massnahmen.

Verbindlicher Kontrollprozess mit Sanktionen und Massnahmen bei Nichteinhaltung der Regeln

Mittels eines verbindlichen und verlässlichen Prozesses muss nach der Vergabe des Gütesiegels die Nachkontrolle, z.B. auf jährlicher Basis, gewährleistet werden. Bei Nichteinhaltung der Anforderungen und Regeln sind schliesslich auch Sanktionen und Massnahmen vorzusehen wie z.B. der Entzug des Gütesiegels.

Berücksichtigung der europäischen Anforderungen in Sachen Datenschutz

Die europäischen gesetzlichen Anforderungen an die Bearbeitung von Personendaten müssen bei der Prüfung einbezogen werden, damit auch die internationale Verlässlichkeit des Siegels erwirkt werden kann.

4.2. Alternative Streitbeilegungsmechanismen bei Online–Transaktionen (E-Commerce)

Auf S. 95 sind die wesentlichen Kriterien für den erfolgreichen Einsatz von alternativen Mechanismen zur online-Streitbeilegung zu finden.

5. Personalwesen

Privatbereich

5.1. Drogentests in der Lehre

Der Eidgenössische Datenschutzbeauftragte hat in Zusammenarbeit mit anderen Fachstellen einen Bericht publiziert (www.edsb.ch), welcher die Voraussetzungen von Drogentests in der Lehre festhält. Falls ein überwiegendes Sicherheitsinteresse sowie die Einwilligung des Lehrlings nicht gegeben sind, dürfen Drogentests nicht angeordnet werden.

Sowohl der Eidgenössische Datenschutzbeauftragte (EDSB) als auch andere Fachstellen wurden seit einigen Jahren vermehrt mit der sich verbreitenden Praxis der Drogentests bei Lehrlingen konfrontiert. Aus diesen Gründen ist eine Arbeitsgruppe mit dem Ziel eingesetzt worden, einheitliche Richtlinien für eine persönlichkeitsschutzkonforme Gestaltung von Prävention und Aufdeckung des Drogenkonsums zu konzipieren. Nebst dem EDSB haben auch die Schweizerische Fachstelle für Alkohol und andere Drogenprobleme, das Staatssekretariat

für Wirtschaft, das Bundesamt für Gesundheit sowie das Bundesamt für Justiz bei der Erarbeitung dieser Richtlinien mitgewirkt. Beigezogen wurden zudem das Institut für Rechtsmedizin in Lausanne, die Berufsbildungsämter sowie Vertreter der Arbeitgeber- und Arbeitnehmerseite. Der Bericht kommt zu folgenden Schlussfolgerungen:

Drogen können die Arbeitssicherheit gefährden, die Leistung reduzieren, das Klima im Unternehmen beeinflussen oder Kosten verursachen. Nicht selten greift der Arbeitgeber zum Schutz seiner Interessen auf Urintests (auch Drogentests genannt) zurück, welche den Drogenkonsum aufdecken sollen. Die ärztliche Massnahme der Urinanalyse stellt jedoch einen Eingriff in die Persönlichkeit der untersuchten Person dar. Nur ein gegenüber dem Persönlichkeitsschutz überwiegendes Sicherheitsinteresse, verbunden mit der Einwilligung des Lehrlings, kann einen Drogentest rechtfertigen. Der Arbeitgeber ist in solchen Fällen berechtigt, einen Drogentest anzuordnen.

Die Vornahme von Drogentests entbindet aber den Arbeitgeber nicht von der Pflicht, die notwendigen Massnahmen der Arbeitssicherheit zu treffen. Drogentests kommt somit nur ein Ergänzungscharakter zu. Die Drogentests sind von einem vom Betrieb unabhängigen Arzt und nach freier Wahl des Lehrlings vorzunehmen. Wird hingegen der Betriebsarzt zur Durchführung der Drogentests beigezogen, hängt dies von der Einwilligung des Lehrlings ab. Willigt der Lehrling dem Beizug des Betriebsarztes nicht ein, so ist er in der Wahl des Arztes frei. Der Lehrling ist über den Zweck und die Folgen von Drogentests vorgängig zu informieren. Bei fehlender Einwilligung zum Drogentest kann der Lehrling nicht dazu gezwungen werden, hat aber mit den vertraglich vorgesehenen Konsequenzen zu rechnen. Zu bemerken ist, dass die Einwilligung frei, spezifisch sowie ausdrücklich sein muss und erst aufgrund der Aufklärung des Lehrlings über Zweck und Folgen der Drogentests als gültig betrachtet werden kann.

Fehlt jedoch ein überwiegendes Sicherheitsinteresse, stellen Drogentests eine unverhältnismässige Massnahme dar. Die Einwilligung alleine stellt keinen gültigen Rechtfertigungsgrund für Drogentests dar, da ohne überwiegendes Sicherheitsinteresse der Persönlichkeitsschutz gegenüber anderen Interessen des Arbeitgebers überwiegt. In Ausnahmefällen kann die Einwilligung alleine einen gültigen Rechtfertigungsgrund darstellen, wenn die Vornahme eines Drogentests im Interesse des Lehrlings liegt. Drogentests würden mangels überwiegendem Sicherheitsinteresse nicht zuletzt deswegen einen unverhältnismässigen Eingriff in die Gesundheitssphäre des Lehrlings darstellen, weil die Sicherheit auch mit anderen Massnahmen effizient gewährleistet werden kann. Der Arbeitgeber darf bei beunruhigenden Auffälligkeiten oder Verhaltensänderungen des Lehrlings Gespräche durchführen, konkrete Ziele und Massnahmen festlegen oder Sanktionen beschliessen für den Fall, dass die vereinbarten Ziele

nicht eingehalten werden. Sofern es zur Besetzung bzw. Weiterbesetzung der Lehrstelle notwendig ist, darf der Arbeitgeber vom Lehrling eine Gesundheitsabklärung verlangen. Die Einwilligung des Lehrlings zur Vornahme der Gesundheitsabklärung ist notwendig. Ob in deren Rahmen ein Drogentest vorgenommen wird bzw. Fragen über den Drogenkonsum gestellt werden, hängt ausschliesslich vom Entscheid des Arztes sowie von der Einwilligung des Lehrlings ab (Beziehung Arzt-Patient). Die Vornahme eines Drogentests im Rahmen der Gesundheitsabklärung darf vom Arbeitgeber weder verlangt noch vorgeschlagen werden.

Der Arzt darf dem Arbeitgeber nur den Befund über die Tauglichkeit für die Weiterbesetzung der Lehrstelle bekanntgeben. Angaben über einen allfälligen Drogenkonsum dürfen dem Arbeitgeber nicht gemacht werden (Arztgeheimnis sowie Verhältnismässigkeits- und Zweckmässigkeitsprinzip).

Es ist einzig der Fall denkbar, dass im Rahmen eines umfassenden Begleitprogramms des Arbeitgebers gewisse andere unabdingbare Informationen vom Arzt weitergegeben werden dürfen, sofern der betroffene Lehrling seine Einwilligung dazu gegeben hat. In einem solchen Fall soll die Angabe über den Drogenkonsum dem Arbeitgeber dazu dienen, Hilfsmassnahmen wie Gestaltung von Präventionsprogrammen, gegebenenfalls Finanzierung einer Drogenentzugstherapie, vorzunehmen. Der Arbeitgeber hat mangels überwiegendem Sicherheitsinteresse seine Aufmerksamkeit nicht lediglich auf das Betäubungsmittel, sondern auf die gesamte Problematik des Drogenkonsums und seine Folgen zu richten. Nur unter diesen Umständen kann von einer erweiterten Fürsorgepflicht des Arbeitgebers für den Lehrling gesprochen werden. Drogentests alleine besitzen einen Repressions- statt Hilfscharakter und stellen keine ganzheitliche Lösung von Drogenproblemen in der Jugend dar. Sie können zu weiteren Problemen wie Diskriminierung des Lehrlings führen.

Willigt der Lehrling dem Drogentest oder der Bekanntgabe der Testresultate an den Arbeitgeber nicht ein und ist ein überwiegendes Sicherheitsrisiko nicht gegeben, so dürfen ihm daraus keine negativen arbeitsrechtlichen Folgen erwachsen. Erst die wiederholte Feststellung, dass die Lehrziele nicht erreicht werden können oder dass der Lehrling den Drogenkonsum nicht unter Kontrolle hat, kann zu den vereinbarten Konsequenzen führen. Der Arbeitgeber hat die im Zusammenhang mit dem Drogenkonsum allenfalls bearbeiteten Daten vertraulich zu behandeln.

Die Situation in der heutigen Arbeitswelt hat sich dem Eidg. Datenschutzbeauftragten in verschiedenen Formen gezeigt: einerseits gestalten bestimmte Arbeitgeber Drogentests im Einklang mit den oben geschilderten Richtlinien (Siehe auch 6. Tätigkeitsbericht 1999/2000, S. 68), andererseits gibt es Hardliner, welche Drogentests ohne einen überwiegenden Sicherheitsgrund

durchführen. Gegen solche Arbeitgeber haben wir eine Empfehlung erlassen (siehe S. 122). Da unsere Empfehlung vom betroffenen Unternehmen abgelehnt wurde, haben wir die Angelegenheit der Eidgenössischen Datenschutzkommission zum Entscheid vorgelegt.

5.2. Die E-Mail- und Internetüberwachung am Arbeitsplatz

Wir haben ein Schema publiziert, das erklärt, unter welchen Umständen die Internet- und E-Mailnutzung am Arbeitsplatz überwacht werden darf. Das Schwergewicht wird auf die technische Prävention gelegt. Personenbezogene Auswertungen der Protokollierungen dürfen nur nach festgestelltem Missbrauch vorgenommen werden. Weitere Voraussetzung der personenbezogenen Auswertung der Protokollierungen ist die vorgängige Information der Arbeitnehmer. Das entsprechende Schema ist auf S. 113 zu finden.

Technische Prävention statt Überwachung: Mit diesem Schlagwort soll der Arbeitgeber auf die eigene Verantwortung zum Schutz seiner Ressourcen hingewiesen werden. Technische Schutzmassnahmen garantieren unter Anderem die Sicherheit von Daten und Anwendungen und schützen den Betrieb vor Systemüberlastungen. Konkrete Massnahmen sind zum Beispiel der Einsatz von Firewalls und Antivirusprogrammen oder die Beschränkung der Speicherkapazität der Nutzer. Spionprogramme, die die Netzwerkaktivität bestimmter Personen überwachen, sind nicht erlaubt. Sowohl Arbeitgeber wie auch Arbeitnehmer haben dafür zu sorgen, dass zum Beispiel keine Viren eingeschleppt oder keine Speicherüberlastungen verursacht werden. Für den Arbeitgeber heisst dies vor allem, dass er für einen passenden technischen Schutz sorgen muss. Die Angestellten sind im Gegenzug dazu verpflichtet, mit der notwendigen Vorsicht vorzugehen, wenn sie auf dem Internet surfen oder E-Mails von Unbekannten bekommen.

In Protokollierungen werden die Aktivitäten der Internetnutzer fortlaufend aufgezeichnet, in Form von Angaben wer, was, wann besucht hat. Durch diese Protokollierungen kann der Benutzer identifiziert werden.

Der Arbeitgeber hat die Arbeitnehmer über die eingesetzten technischen Schutzmassnahmen und Protokollierungen sowie über die Nutzungs- und Überwachungsregelung zu informieren. In der Nutzungsregelung hält der Arbeitgeber fest, ob und wie die Benutzung des Internets und E-Mails erlaubt ist. Er kann die Nutzung vollständig frei geben, einschränken, zum Beispiel auf die Mittagspause, oder gänzlich verbieten. Ob diese Nutzungsregelung eingehalten wird, darf der Arbeitgeber – sofern er ein Überwachungsreglement verfasst hat

– kontrollieren. Wir empfehlen mit Nachdruck eine solche Nutzungsregelung zu erlassen, damit Klarheit darüber herrscht, was erlaubt ist und was nicht.

Das Überwachungsreglement hält seinerseits fest, mit welchen Kontrollen die Arbeitnehmer/-innen rechnen müssen. Es informiert auch darüber, wie die persönlichen Auswertungen den Vorgesetzen mitgeteilt werden und welche Sanktionen diese ergreifen können. Personenbezogene Kontrollen sind nur erlaubt, wenn erstens ein schriftliches Überwachungsreglement vorliegt und zweitens bei einer anonymen Kontrolle ein Missbrauch festgestellt wurde. Eine präventive personenbezogene Kontrolle ist nicht erlaubt. Ein Missbrauch liegt einerseits dann vor, wenn ein Arbeitnehmer die Bestimmungen der Nutzungsregelung missachtet, oder – wenn keine Nutzungsregelung vorhanden ist – gegen die Treuepflicht gegenüber dem Arbeitgeber oder gegen das Prinzip der Verhältnismässigkeit verstösst. Mit Treuepflicht ist die Verpflichtung der Arbeitnehmerschaft gemeint, die Interessen des Arbeitgebers zu wahren. Als unverhältnismässig und als Verstoss gegen die Treuepflicht gilt zum Beispiel überdurchschnittliches Surfen während der Arbeitszeit. In diesen Fällen ist eine personenbezogene Auswertung der Protokollierungen erlaubt – natürlich wiederum nur, wenn ein Überwachungsreglement besteht.

Im Normalfall ist es nicht der Vorgesetzte selber, der die Überwachung durchführt, sondern die Informatikdienste oder spezielle Sicherheitsbeauftragte. Diese geben die Auswertungen den Vorgesetzen ausschliesslich im Rahmen der Überwachungsregelung bekannt.

Wenn ein Missbrauch keine technische Störung zur Folge hat, erfolgt die personenbezogene Auswertung der Protokollierungen aus Gründen der Verhältnismässigkeit erst bei wiederholter Feststellung eines Missbrauchs. Der Arbeitgeber muss deshalb die Arbeitnehmerschaft darüber informieren, dass er einen Missbrauch festgestellt hat und personenbezogen auswerten wird, falls sich dies wiederholt.

Die Inhalte privater E-Mails bleiben für den Arbeitgeber jedoch tabu. Der Inhalt der E-Mails ist Teil der Privatsphäre eines jeden Menschen. Auch wenn der private Gebrauch von E-Mail am Arbeitsplatz verboten ist, darf der Arbeitgeber die E-Mails der Angestellten nicht lesen. Wenn bei einer Stichprobe der Verdacht entsteht, dass ein Arbeitnehmer gegen ein Verbot des privaten E-Mail-Gebrauchs verstossen hat, dann muss dies aufgrund der Adressierung des E-Mails festgestellt werden. Wenn dies nicht möglich ist, muss der Arbeitnehmer direkt gefragt werden, ob ein E-Mail privat ist oder nicht.

Wenn der Arbeitgeber bei einer Überwachung einen konkreten Verdacht schöpft, dass eine Straftat begangen wurde, darf er nur beschränkt ermitteln. Die Strafverfolgung bleibt immer den Strafjustizbehörden vorbehalten, der Ar-

beitgeber darf einzig Beweise sichern, wenn dies zur Anzeige der verdächtigten Person führt. Falls der Verdacht auf eine Straftat besteht, darf der Arbeitgeber selber aus Gründen der Verhältnismässigkeit die Identität der Verdächtigen feststellen, unabhängig davon, ob eine technische Störung vorliegt oder nicht. Weitergehende präventive Überwachungen bleiben im Zuständigkeitsbereich der Strafjustizbehörde. Will er keine Anzeige erstatten, bleiben die Regeln der arbeitsrechtlichen Überwachung und der entsprechenden Sanktionen bestehen.

Wenn ein Arbeitnehmer meint, dass er vom Arbeitgeber auf eine unerlaubte Art kontrolliert worden ist, kann er zivilrechtlich gegen den Arbeitgeber wegen Persönlichkeitsverletzung klagen. Strafrechtlich kann der Arbeitnehmer gegen den Arbeitgeber bei den zuständigen Behörden wegen Verletzung der Privatsphäre oder wegen unbefugtem Beschaffen von Personendaten vorgehen. In der Regel erstattet er Anzeige bei der Polizei.
Zu diesem Thema haben wir einen ausführlichen Leitfaden publiziert (www.edsb.ch).

5.3. Bearbeitung von Gesundheitsdaten durch den Arbeitgeber

Eine Krankenversicherung hat eine CD-ROM zur Kontrolle der Abwesenheiten der Arbeitnehmer herausgegeben, welche gegen die Grundsätze des Datenschutzes verstösst. Unsere Empfehlung wurde formell abgelehnt, in der Tat jedoch umgesetzt.

Die Überprüfung des Sachverhaltes hat ergeben, dass durch die CD-ROM Personendaten wie Name, Vorname, Nationalität, Abwesenheitsgrund, Arzttyp, Diagnose, Bemerkungen, usw. durch den Arbeitgeber systematisch erfasst werden können. Die Auswertung der Daten kann nach Kriterien wie Nationalität, Arzt oder Diagnose bzw. nach festgelegten Zielwerten (Zeitbudget für Krankheiten) erfolgen. Ausserdem ermöglicht die CD-ROM den Datenaustausch mit anderen Datenbanken. Die CD-ROM soll nach Angaben der Versicherung dem Arbeitgeber als Kontrollinstrument über die Abwesenheiten seiner Angestellten dienen. Sie soll zudem den Gesundheitsschutz fördern als auch die Abwesenheiten am Arbeitsplatz reduzieren. Die Versicherung hat im Wesentlichen die Auffassung vertreten, dass der Arbeitgeber berechtigt ist, Krankheitsdiagnosen systematisch zu bearbeiten, um sich einen Überblick über die Absenzen zu verschaffen und um über die Weiterbeschäftigung eines kranken Mitarbeiters entscheiden zu können. Ein Datenaustausch mit Datenbanken der Versicherung finde jedoch in der Praxis nicht statt.

Wir haben uns auf den Standpunkt gesetzt, die CD-ROM stelle eine unverhältnismässige und unzweckmässige Datenbearbeitung dar, da der Arbeitgeber die systematisch erfassten Gesundheitsdaten zur Durchführung des Arbeitsvertrages

nicht braucht. Nach dem Verhältnismässigkeitsprinzip ist es insbesondere unzulässig, dass der Arbeitgeber bzw. sein Personaldienst Arztdiagnosen systematisch erfasst. Die systematische Erfassung von Diagnosen ist weder zur Schaffung von Massnahmen der Gesundheitsprävention oder zur Absenzbewirtschaftung noch zur Entscheidfindung über die Weiterbeschäftigung eines kranken Mitarbeiters notwendig. Nur einzelfallweise, sofern dies zur Abklärung einer speziellen Sachlage erforderlich ist, kann ein Arbeitgeber bzw. die Abteilung Sicherheits- und Gesundheitsprävention des Unternehmens oder der entsprechenden Branche Kenntnis über die Ursachen einer Krankheit einer bestimmten Person erlangen. Ohne ausdrückliche Einwilligung des Arbeitnehmers darf der Arbeitgeber sonst nur einen Arztbefund bearbeiten («krank» oder «geeignet/ungeeignet» für eine Stelle). Zulässig ist hingegen die Erfassung der Anzahl Absenztage wegen Krankheit, ohne weitere Spezifikationen.

Die vorgesehene Datenbearbeitung ist auch deswegen zu beanstanden, weil die Gesundheitsdaten mit weiteren Personendaten, z. B. die Nationalität, kombiniert und verglichen werden können. Daraus können unserer Meinung nach diskriminierende Rückschlüsse gezogen werden. Die systematische Erfassung anderer Abwesenheitsgründe durch den Arbeitgeber (z. B. Ferien, Militär, usw.), welche von der CD-ROM auch ermöglicht wird, wurde von uns nicht beanstandet.

Die CD-ROM ist auch als Gesundheitsmassnahme nicht geeignet. Die Arbeitsgesetzgebung verpflichtet den Arbeitgeber, Massnahmen zu treffen, um Gefahren für die Gesundheit der Arbeitnehmer vorzubeugen. Arbeitsräume, Systeme und Maschinen sind so zu unterhalten, dass deren Benutzung keine Folgen auf die Gesundheit der Arbeitnehmer haben können. Die Erfassung von Informationen über «Schwachstellen» im Unternehmen (Luftzug, gefährliche Substanzen, Rauchen, schlechte Bildschirme, usw.) erfolgt anonym, aufgrund statistischer Angaben. Nur in Ausnahmefällen, sofern es zur Abklärung einer speziellen Sachlage erforderlich ist, darf der Arbeitgeber bzw. die Abteilung Sicherheits- und Gesundheitsprävention des Unternehmens oder der entsprechenden Branche mit den betroffenen Personen Kontakt aufnehmen. Bei der in Frage stehenden CD-ROM handelt es sich hingegen um eine reine Absenzkontrolle.

Das Festhalten eines jährlichen Budgets an Krankheitstagen ist auch unstatthaft, weil dadurch gesundheitlich schwächere Menschen, die öfters abwesend sind, diskriminiert werden können. Die Behauptung der Versicherung, die fragliche Datenbearbeitung sei gegenüber gesundheitlich schwächeren Angestellten nicht diskriminierend, weil für solche Angestellten individuelle «Krankheitsbudgets» geschaffen werden können, widerspricht der Zielsetzung der Absenzenreduktion.

Die Behauptung der Versicherung, ein Datenaustausch zwischen ihr und den Arbeitgebern finde nicht statt, mag zwar in der Tat zutreffen, sie ändert aber an der Tatsache nichts, dass bereits die technische Möglichkeit eines solchen Datenaustausches gesetzeswidrig ist. Weder die Einwilligung der betroffenen Personen noch eine gesetzliche Grundlage, noch ein überwiegendes privates oder öffentliches Interesse sind für den Datenaustausch zwischen der Absenz-Datenbank und anderen Datenbanken gegeben. Ohne Rechtfertigungsgrund würde eine solche Datenbekanntgabe im Übrigen eine Verletzung des Berufsgeheimnisses seitens des Arbeitgebers darstellen.

Aufgrund dieser Erwägungen haben wir der Versicherung empfohlen, die Produktion und der Vertrieb der fraglichen CD-ROM unverzüglich einzustellen und die bereits verteilten CD-ROM zurückzuziehen oder die fraglichen Datenkategorien von der CD-ROM zu entfernen. Die Versicherung hat sich mit unseren Erwägungen nicht einverstanden erklärt, jedoch die CD-ROM datenschutzkonform gestaltet.

6. Versicherungswesen

Sozialversicherungen

6.1. Nachweis eines Gesundheitsschadens in Suchtinstitutionen

Das Bundesamt für Sozialversicherung (BSV) prüft, ob Suchthilfeorganisationen IV-Beiträge erhalten oder nicht. Dafür verlangt es auch Gesundheitsdaten über die Bewohner der Suchtinstitutionen, der Umfang dieser Daten ist jedoch fraglich (vgl. auch 7. Tätigkeitsbericht 1999/2000, S. 41).

Das BSV schliesst mit den Suchthilfeinstitutionen (Leistungsvertragsnehmern) sogenannte Leistungsverträge ab. Damit diese in den Genuss von IV-Beiträgen kommen, müssen bestimmte Voraussetzungen erfüllt sein. Insbesondere müssen 50% der Klienten der Suchtinstitutionen Behinderte im Sinne der IV-Gesetzgebung sein. Das BSV verlangt dafür u.a. Gesundheitsdaten der Klienten. Gesundheitsdaten gehören zu den besonders schützenswerten Personendaten. Wir haben das BSV mehrmals darauf hingewiesen, dass das Beschaffen von besonders schützenswerten Personendaten entsprechende gesetzliche Grundlagen benötigt.

Es gilt zu bedenken, dass es sich bei den Leistungsvertragsnehmern in erster Linie um ambulante Institutionen handelt, die grösstenteils Drogenabhängige oder ehemals Drogenabhängige begleiten und betreuen. Es werden demnach

sehr sensitive Daten bearbeitet. Aufgrund der Sensibilität der Daten sind auch an die Bearbeitungsgrundsätze strengere Anforderungen zu stellen. Insbesondere gilt dies für das Verhältnismässigkeitsprinzip.

Eine Möglichkeit besteht darin, die Personendaten der Betroffenen soweit als möglich zu anonymisieren. Um dies zu ermöglichen, bietet sich die Verwendung von Codes an, mit Hilfe derer die Daten pseudonymisiert werden. Die Pseudonymisierung darf jedoch nicht erst durch den Empfänger erfolgen, sondern ist durch den Leistungsvertragsnehmer z. B. durch Vergabe einer Kundennummer vorzunehmen. Die Angaben, welche in codierter Form übergeben werden, sind auf ein Minimum zu beschränken. Das BSV würde somit Angaben bekommen, die lediglich mit dem vom Leistungsvertragsnehmer verwendeten Code versehen sind. Die Daten wären somit beim Leistungsvertragsnehmer pseudonymisiert. Allenfalls im konkreten Einzelfall und aufgrund einer konkreten Nachfrage wäre der Kunde wieder identifizierbar.

6.2. Pensionskassengelder: Suche nach Anspruchsberechtigten

Die Zentralstelle 2. Säule hat den Zweck, die «vergessenen Pensionskassengelder» den anspruchsberechtigten Arbeitnehmern zukommen zu lassen. Die Suche nach den meist im Ausland lebenden Versicherten erwies sich jedoch als schwierig. Es wurden daher neue Wege gesucht, und die gesetzlichen Grundlagen wurden dementsprechend angepasst.

Nicht alle Arbeitnehmer haben ihre Pensionskassengelder in Anspruch genommen. Es handelt sich dabei vor allem um Arbeitnehmer aus anderen europäischen Staaten, die für diesen Zweck ausfindig zu machen sind. Die im Freizügigkeitsgesetz vorgesehene Regelung war jedoch ungenügend. Insbesondere war es nicht möglich, alle Adressen über die Zentrale Ausgleichskasse (ZAS) herauszufinden. Es wurde daher der Vorschlag gemacht, die fehlenden Adressen bei den ausländischen Sozialversicherungsbehörden zu eruieren. Der EDSB empfahl, die gesetzlichen Grundlagen dementsprechend anzupassen (vgl. auch 7. Tätigkeitsbericht 1999/2000, S. 37).

Für die spanischen Arbeitnehmer wurde für diesen Zweck ein Staatsvertrag (Notenwechsel) zwischen der Schweiz und Spanien ausgearbeitet. Darin wird festgehalten, dass die Zentralstelle 2. Säule einmal jährlich einen Datenträger (Name, Vorname und Geburtsdatum der nicht lokalisierten Berechtigten spanischer Nationalität) an die spanischen Sozialversicherungsbehörden übermittelt. Diese versuchen, die in Spanien wohnhaften Arbeitnehmer ausfindig zu machen und teilen dies der Zentralstelle 2. Säule mit.

Aus unserer Sicht wichtig war, dass die Daten nur für diesen Zweck bearbeitet werden (Zweckbindungsgebot). Im Weiteren haben wir Wert darauf gelegt, dass der Notenwechsel auch Bestimmungen über die Datensicherheit enthält. Insbesondere wird darin ausdrücklich erwähnt, dass die Datenträger verschlüsselt übermittelt werden müssen.

Wir begrüssten diese Regelung und hoffen, dass analoge Lösungen auch mit anderen Ländern gefunden werden.

6.3. Expertenkommission für den Persönlichkeitsschutz in der sozialen und privaten Kranken- und Unfallversicherung

Der Schlussbericht der Expertenkommission für den Persönlichkeitsschutz in der sozialen und privaten Kranken- und Unfallversicherung wurde im Oktober 2000 dem Eidgenössischen Departement des Innern (EDI) vorgelegt. Der Bericht wurde im März 2001 veröffentlicht.

Die Kommission hat ihre Arbeit im März 1998 aufgenommen und insgesamt 17 Sitzungen abgehalten. Die Aufgabe der Arbeitsgruppe bestand insbesondere darin, die Thematik des Persönlichkeitsschutzes in der sozialen und privaten Kranken- und Unfallversicherung zu untersuchen. Konkret ging es darum, Verbesserungsvorschläge und auch vollständig formulierte Gesetzesbestimmungen auszuarbeiten. Aus datenschutzrechtlicher Sicht standen das Verhältnismässigkeits- und das Transparenzprinzip im Vordergrund.

In den obligatorischen Pflegeversicherungen war v.a. abzuklären, welche Datenbedürfnisse sowohl die Krankenversicherer als auch die Unfallversicherer haben. Aus Sicht des EDSB wichtig zu erwähnen ist, dass Gesundheitsdaten nicht auf Vorrat beschafft und gespeichert werden dürfen (Prinzip der Verhältnismässigkeit). Es ist vorher genau abzuklären, welche Daten die Versicherer für welche Zwecke brauchen.

Im Zusatzversicherungsbereich waren insbesondere die Antragsformulare mit den Gesundheitsfragen und den Einwilligungsklauseln ein Thema. Auf jeden Fall dürfen die Fragen des Versicherers die Persönlichkeit des Antragsstellers nicht verletzen und müssen dem Grundsatz der Verhältnismässigkeit entsprechen. Einwilligungsklauseln, welche u.a. den Arzt von der Schweigepflicht entbinden sollen, müssen für die einwilligende Person klar und erkennbar sein (vgl. auch 7. Tätigkeitsbericht 1999/2000, S. 66-67).

Bei der Aufnahme in die Krankentaggeldversicherung sind Gesundheitsfragen grundsätzlich erlaubt. Dies kann zu Diskriminierungen von Arbeitnehmern mit «erhöhten Risiken» führen. Denn Arbeitgeber wie auch Krankentaggeldversicherer haben ein finanzielles Interesse daran, Personen mit ungeeigneten Gesundheitsdispositionen nicht einzustellen bzw. nicht weiterzubeschäftigen. Wir fordern daher, im Bereich der Krankentaggeldversicherungen auf Gesundheitsfragen generell zu verzichten.

Das System der Vertrauensärzte ist bis anhin nur im KVG geregelt. Diskutiert wurden mehrere Modelle, welche die Unabhängigkeit der Vertrauensärzte gegenüber der Versicherungsverwaltung zum Inhalt haben. Im Weiteren wurde der Datenfluss zwischen dem Vertauensarzt und der Versicherungsverwaltung untersucht. Für uns ist wichtig, dass das System der Vertrauensärzte so weit als möglich auf andere Versicherungsformen ausgedehnt wird. Insbesondere ist eine analoge Einrichtung für den Unfallversicherungsbereich ernsthaft zu prüfen.

Der Bericht der Expertenkommission wurde im Oktober 2000 dem EDI unterbreitet und im März 2001 veröffentlicht. Viele unserer Forderungen wurden erfüllt. Insbesondere die Verwendung von getrennten Antragsformularen für die Grund- und Zusatzversicherungen.

Privatversicherungen

6.4. Die Notwendigkeit eines Vertrauensarztes im Privatversicherungsbereich

Das Institut des Vertrauensarztes ist für den Krankenversicherungsbereich geregelt und aus datenschutzrechtlicher Sicht zu begrüssen. Die versicherte Person hat die Möglichkeit, medizinische Angaben nur dem Vertrauensarzt mitzuteilen. Es stellt sich daher die Frage, ein analoges Institut auch für den Privatversicherungsbereich zu schaffen.

Das Krankenversicherungsgesetz (KVG) kennt das System der Vertrauensärzte. Der Vertrauensarzt hat hinsichtlich des Datenflusses eine gewisse «Filterfunktion» zwischen den Versicherten und der Krankenkassenverwaltung. Er berät die Versicherer in medizinischen Fachfragen sowie in Fragen der Vergütung und der Tarifanwendung. Vertrauensärzte überprüfen insbesondere die Voraussetzungen der Leistungspflicht des Versicherers. Im Weiteren sind sie in ihrem Urteil unabhängig.

Es stellt sich generell die Frage, das Institut des Vertrauensarztes auf andere Versicherungsformen auszudehnen und die nötigen gesetzlichen Grundlagen zu schaffen.

Im Privatversicherungsbereich existieren seit rund 15 Jahren Empfehlungen für die Behandlung medizinischer Akten. Eine dieser Empfehlungen wurde zwischen der FMH und der Privatassekuranz ausgearbeitet. Sie sieht u.a. vor, dass medizinische Daten, welche besonders schützenswerte Personendaten enthalten, dem medizinischen Dienst oder beratenden Arzt des Versicherers zugestellt werden können. Im Weiteren kann verlangt werden, dass diese Daten beim Versicherer gesondert aufbewahrt werden. Auch müssen die Versicherer sicherstellen, dass diese Unterlagen nur einem begrenzten Personenkreis zugänglich sind. Zudem müssen die Versicherer auf den Antragsformularen darauf hinweisen, dass besonders schützenswerte Personendaten dem medizinischen Dienst bzw. dem beratenden Arzt (mit dem Vermerk «persönlich») an die Adresse des Versicherers mitgeteilt werden können.

Medizinische Dienste oder Vertrauensärzte sind in der Privatassekuranz demnach nichts Neues und haben sich bewährt. Zu begrüssen wäre allerdings, dass sie gegenüber den Versicherern auch unabhängig wären.

Wir fordern daher, medizinische Dienste bzw. Vertrauensärzte auch für den Privatversicherungsbereich auf Gesetzesstufe zu regeln (Aufgabe, Zweck, Organisation etc.). Vertrauensärzte im Privatversicherungsbereich sind umso wichtiger, da hier Diskriminierungen aufgrund einer ungeeigneten Gesundheitsdisposition nicht auszuschliessen sind. Falls genetische Untersuchungen im Versicherungsbereich - welche der EDSB grundsätzlich ablehnt - eines Tages dennoch möglich sein sollten, wird man um das Institut des Vertrauensarztes im Privatversicherungsbereich nicht herumkommen.

6.5. Blutproben gehören nicht in die Hände von Versicherern

Privatversicherer können grundsätzlich Gesundheitsdaten von den Antragstellern zur Risikobeurteilung beschaffen. Sie sind aber an das Verhältnismässigkeitsprinzip gebunden. Auf keinen Fall darf ein Versicherer Blutproben verlangen.

Eine Person wollte von uns wissen, ob eine Versicherungsgesellschaft im Aufnahmeverfahren in eine Pensionskasse berechtigt sei, auch Blutproben einzufordern.

Eine Versicherungsgesellschaft darf im Aufnahmeverfahren Gesundheitsangaben verlangen, soweit sie tatsächlich erforderlich sind. Im Bereich der berufli-

chen Vorsorge dürfen Gesundheitsangaben nur für den überobligatorischen Teil verlangt werden. Wohl steht es der Versicherungsgesellschaft zu, die notwendigen Gesundheitsinformationen einzuholen (Verhältnismässigkeitsprinzip). Auf keinen Fall darf sie jedoch körperliche Substanzen wie z. B. Blutproben einfordern. Schriftliche Angaben des Antragstellers bzw. des behandelnden Arztes genügen vollends. Der Antragsteller ist zur Wahrheit verpflichtet, ansonsten er eine Anzeigepflichtverletzung begeht. Der Arzt ist zudem an seine ärztliche Sorgfaltspflicht gebunden. Es wäre demnach unverhältnismässig, wenn ein Versicherer nebst den Gesundheitsangaben auch noch Blutproben, Urin etc. vom Antragsteller verlangen würde.

Im Weiteren besteht die Gefahr, dass der Versicherer die Blutproben für andere Zwecke verwendet. Aus Blutproben können etwa genetische Informationen geholt werden. Auch ist unklar, ob die Daten an den ärztlichen Dienst der Versicherung gelangen oder gar an die Versicherungsverwaltung. Eine weitere Frage ist, wer auf diese sensiblen Daten Zugriff haben soll bzw. wo und wie lange die Blutproben aufbewahrt werden. Wir sind zur Zeit daran, die nötigen Abklärungen zu treffen.

6.6. Datenweitergabe an Rückversicherer

Rückversicherer verlangen von den Versicherern Versichertendaten, um den Leistungsanspruch abklären zu können. Dabei sind die Daten der Versicherten soweit als möglich zu anonymisieren.

Eine Rückversicherungsgesellschaft hat uns Reglementsauszüge für die Grossrisikoversicherung zur Stellungnahme unterbreitet. Im Reglement wird festgehalten, dass dem Rückversicherer unter bestimmten Voraussetzungen Kopien und Zeugnisse von versicherten Personen zugestellt werden müssen. Im Weiteren habe der Rückversicherer das Recht, von den Versicherern weitere Unterlagen zu verlangen oder bei diesen einzusehen.

Aus datenschutzrechtlicher Sicht gilt es, die Versichertendaten soweit als möglich zu anonymisieren. Es stellt sich daher die Frage, ob der Rückversicherer die oben erwähnten Angaben in jedem Fall braucht. Denkbar wäre, die Daten mittels Kennziffern (Codes) zu anonymisieren. Die Codes wären im Besitze der Versicherer. Im konkreten Einzelfall könnte der Rückversicherer allenfalls auf die Versichertendaten zugreifen, um Leistungsansprüche näher abklären zu können. Die Versichertendaten wären somit grundsätzlich anonym, könnten aber im Einzelfall wieder bestimmbar gemacht werden (Pseudonymisierung).

Im Weiteren sei noch erwähnt, dass die Bearbeitung von Personendaten eines Rechtfertigungsgrundes bedarf. Bearbeitet ein Rückversicherer Versichertendaten eines Privatversicherers, ist in der Regel eine konkrete Einwilligung der versicherten Personen notwendig. Ist ein Rückversicherer in der sozialen Krankenversicherung tätig, sind die spezifischen Datenbekanntgaberegelungen im KVG zu berücksichtigen.

6.7. Qualitätskontrollen im Zusatzversicherungsbereich

Im Zusatzversicherungsbereich gibt es Bestrebungen der Krankenversicherer, die Qualität der Leistungserbringer verstärkt zu kontrollieren. Für diesen Zweck werden Personendaten bearbeitet. Die datenschutzrechtlichen Grundsätze sind dabei einzuhalten.

Der EDSB wird vermehrt mit Anfragen konfrontiert, welche die Qualitätskontrolle von Leistungserbringern im Zusatzversicherungsbereich betreffen. Insbesondere die Krankenkassen schliessen sich zu Vereinen zusammen, um die Qualität der einzelnen Leistungserbringer im Zusatzversicherungsbereich zu kontrollieren. Für diesen Zweck werden von den Leistungserbringern Personendaten erhoben. Auf Seiten der Leistungserbringer wie z. B. Fitnessstudios werden umfangreiche Daten über Ausbildung, methodische Massnahmen etc. verlangt. Entscheidend ist hier, dass wirklich nur diejenigen Daten bearbeitet werden, die tatsächlich benötigt werden (Prinzip der Verhältnismässigkeit). Aus unserer Sicht unverhältnismässig wären etwa unangemeldete Besuche von Krankenkassenvertretern bei einzelnen Leistungserbringern. Auch ist es nicht notwendig, im Rahmen der Qualitätskontrolle Personendaten von versicherten Personen zu bearbeiten.

Im Weiteren muss die Datenbearbeitung für die Leistungserbringer transparent sein. Sie müssen umfassend informiert werden, was mit ihren Daten geschieht. Wir haben daher vorgeschlagen, den Leistungserbringern ein Merkblatt zum Datenschutz auszuhändigen. Zudem dürfen die Daten nur für den vorliegenden Zweck bearbeitet werden (Zweckbindungsprinzip). Dies gilt insbesondere für Daten, die Geschäftsgeheimnisse der Leistungserbringer zum Inhalt haben. Die Krankenkassen dürfen Personendaten nur bearbeiten, wenn ein Rechtfertigungsgrund vorliegt. Werden Daten von Leistungserbringern im Zusatzversicherungsbereich bearbeitet, ist deren Einwilligung erforderlich. Fraglich bleibt jedoch, ob die Einwilligung des Leistungserbringers frei erfolgen kann. Denn wenn der Leistungserbringer weiterhin von den einzelnen Zusatzversicherungen anerkannt bleiben will, hat er faktisch oft keine andere Wahl, als sich einer solchen Qualitätskontrolle zu unterziehen.

7. Gesundheitswesen

7.1. Call-Center im medizinischen Bereich

Es werden im medizinischen Bereich immer mehr Call-Center eingerichtet, die Bürgern die Möglichkeit bieten, sich im Krankheitsfall telefonisch über die erforderlichen ersten Schritte oder das weitere Vorgehen zu informieren. Im Zusammenhang mit diesen Telefongesprächen werden sehr sensible Daten des Anrufers bearbeitet. Es stellen sich die grundsätzlichen Fragen der Transparenz der Datenbearbeitung, der Einwilligung der Betroffenen sowie der Datensicherheit.

Im letzten Jahr haben sich im medizinischen Bereich viele sogenannte Call-Center auf dem Markt etabliert. Je nach Zielsetzung bieten Call-Center im Krankheitsfalle zum Einen dem spontanen Anrufer die Möglichkeit, sich telefonisch über die ersten erforderlichen Schritte sowie über weiteres Vorgehen zu erkundigen. Zum Anderen werden festen Kunden des Anbieters des Call-Centers z. B. die folgenden Dienstleistungen angeboten: Organisation der ärztlichen Betreuung, Information des medizinischen Personals im Ausland oder Erstellen von längerfristigen Gesundheitsplänen.

Der Grossteil der Kontakte zwischen dem Patienten und dem Call-Center bzw. dessen Anbieter läuft über das Telefon. Um den Patienten beraten zu können, muss dieser den Mitarbeitern des Call-Centers umfangreiche Angaben zu seiner Gesundheit machen, die vom Call-Center bearbeitet werden. Zwar ist dem Anrufer in der Regel bewusst, welche Informationen er dem Call-Center mündlich gibt. Es stellt sich jedoch die Frage, ob dem Anrufer auch bewusst ist, wie und in welchem Umfang das Call-Center die mündlich gemachten Angaben bearbeitet. In der Regel werden die Telefongespräche aufgezeichnet. Zudem setzen Call-Center während des Telefongespräches verschieden detaillierte und komplexe Software-Programme ein, in die die mündlich gemachten Angaben eingegeben werden. Die Programme dienen dazu, den Mitarbeitern des Call-Centers die Beratung zu erleichtern und die Entscheidfindung abzunehmen. Die eingegebenen Daten werden in den Programmen unter anderem zu Zwecken der weiteren Kundenbetreuung oder zu Beweissicherungszwecken eine Zeit lang gespeichert. Es stellt sich die Frage, ob den Anrufern die Aufzeichnung der Telefongespräche sowie die Bearbeitung der mündlich gemachten Angaben mittels Software-Programmen in Form von Auswertung und Speicherung bekannt ist. Nur im Falle der vollumfänglichen Kenntnis kann der Anrufer in die vorgenommenen Datenbearbeitungen rechtsgültig einwilligen. Ist die Einwilligung rechtsgültig, sind die Datenbearbeitungen durch die Call-Center zulässig. Diese kann sicher schriftlich gewährleistet werden, wenn es sich beim Anrufer um

einen festen Kunden des Anbieters des Call-Centers handelt. Fraglich ist jedoch die vollumfängliche vorgängige Information für Spontananrufer. Allein der Hinweis darauf, dass das Telefongespräch aufgezeichnet wird, reicht kaum aus, um dem Anrufer transparent zu machen, wie lange die Aufzeichnungen aufbewahrt werden und welche weitergehenden Datenbearbeitungen im Hintergrund zusätzlich vorgenommen werden.

Zudem stellen sich verschiedene Fragen der Datensicherheit im Zusammenhang mit der Abhörbarkeit des Anschlusses des Call-Centers, Zugriffsberechtigungen und Zugriffsmöglichkeiten von Unbefugten auf die Daten.

7.2. Qualitätsmessungs- und Qualitätssicherungsprojekte im medizinischen Bereich

Aus Kostengründen werden im Gesundheitsbereich sowohl in Spitälern als auch in Heimen vermehrt Qualitätsmessungs- und Qualitätssicherungsprojekte eingesetzt. In diesem Zusammenhang stellen sich Fragen der Notwendigkeit, besonders schützenswerte Personendaten zu bearbeiten, der Zweckbindung, der Transparenz und der Einwilligung in die Datenbearbeitung durch die betroffenen Personen sowie der Datensicherheit.

Nach dem Bundesgesetz über die Krankenversicherung ist der Leistungserbringer zur Wirtschaftlichkeit seiner Leistungen sowie zur Qualitätssicherung verpflichtet. Zu diesen Zwecken setzen Leistungserbringer mit komplexeren Abläufen wie Spitäler oder Heime sogenannte Qualitätsmessungs- und Qualitätssicherungsprojekte ein. Je nach Zielsetzung dienen diese Projekte der Optimierung des Kosten/Nutzen-Verhaltens im Hinblick auf die Betreuung zukünftiger, gegenwärtiger oder sowohl gegenwärtiger als auch künftiger Klienten. Zur Erreichung der Qualitätsmessung und -sicherung werden Gesundheitsdaten der Klienten, Angaben über ihre täglichen Lebensgewohnheiten, Lebenseinstellungen und -philosophien sowie Wünsche detailliert ausgewertet.

Ein Problempunkt in diesem Zusammenhang ist die Rechtmässigkeit der Bearbeitung von Personendaten. Da das Bundesgesetz über die Krankenversicherung nicht ausdrücklich vorsieht, dass zu Zwecken der Qualitätssicherung Personendaten, im Speziellen besonders schützenswerte Personendaten und Persönlichkeitsprofile bearbeitet werden dürfen, stellt sich die Frage, ob die Datenbearbeitung durch eine rechtsgültige Einwilligung der betroffenen Person erlaubt ist. Aus Beweissicherungsgründen ist es sinnvoll und notwendig, wenn die Einwilligung schriftlich erfolgt. Eine rechtsgültige Einwilligung hat gut lesbar, allgemein verständlich und so formuliert zu sein, dass sie den Betrof-

fenen über die Folgen der Einwilligung informiert sowie ihm die Möglichkeit gibt, diese jederzeit zu widerrufen. Dieses jederzeitige Widerrufsrecht impliziert die Freiwilligkeit der Einwilligung. Eine solche ist nicht rechtsgültig, wenn sie aufgrund von irgendwelchen Drucksituationen zustande gekommen ist. Darunter fallen unter anderem der Gruppendruck («alle willigen ein...»), der materielle Druck («Wenn ich nicht einwillige, werden meine Kosten nicht übernommen...») oder der Druck, mit Qualitätsverlust rechnen zu müssen («Wenn Sie nicht einwilligen, können Sie auch nicht an Qualitätsverbesserungen teilhaben...»).

Weiter stellt sich in diesem Zusammenhang unter dem Gesichtspunkt der Verhältnismässigkeit die Frage der Notwendigkeit, Personendaten zu bearbeiten. Unter Personendaten werden alle Angaben über eine bestimmte oder bestimmbare Person verstanden. Die Fragestellung bedeutet damit konkret, ob es für die Auswertung zu Qualitätsmessungs- und Qualitätssicherungszwecken Angaben braucht, die den einzelnen Klienten identifizieren, oder ob mit anonymisierten, allenfalls pseudonymisierten Daten gearbeitet werden kann. Wenn die Qualitätsmessung und die daraus resultierende Qualitätsverbesserung dem einzelnen gegenwärtigen Klienten unmittelbar wieder zugute kommen soll, ist sicher erforderlich, die auszuwertenden Daten und die Resultate wieder derjenigen Person zuordnen zu können, deren Daten ausgewertet wurden. Anders sieht es dagegen aus, wenn die Auswertung der Daten erst in eine künftige Qualitätssicherung und -verbesserung einfliessen soll. In diesem Fall käme die Qualitätsverbesserung nicht mehr derjenigen Person zu gute, deren Daten ausgewertet werden. Unseres Erachtens ist es in diesen Fällen nicht verhältnismässig, die Auswertung anhand von Personendaten vorzunehmen. Vielmehr reicht grundsätzlich die Auswertung anonymisierter Daten aus. Vertritt man jedoch die Auffassung, dass über längere Zeiträume nachvollziehbar sein muss, welche Leistungen ein und derselben Person erbracht wurden, so ist es unserer Meinung nach notwendig, die Daten zu pseudonymisieren. Das bedeutet, dass die die betreffende Person identifizierenden Elemente einem Code zugewiesen werden, die ein und derselben Person erbrachten Leistungen unter dem selben Code abgelegt werden und die Relationsdatenbank, die die Verbindung Code/identifizierende Elemente enthält, getrennt von den Leistungsdaten geführt wird.

Häufig sollen die Auswertungen der Daten zu Zwecken der Qualitätsmessung und –sicherung nicht von der leistungserbringenden Institution vorgenommen, sondern an externe Firmen delegiert werden. Wir sind der Auffassung, dass in diesen Fällen generell so vorgegangen werden sollte, dass an das Drittunternehmen nur anonymisierte Daten oder allenfalls pseudonymisierte Daten bekannt gegeben werden, wobei im letzten Fall das Drittunternehmen keinen Zugriff auf die Relationsdatenbank haben darf. Dies ergibt sich aus dem hohen Schutzbedarf der Gesundheitsdaten, die unter anderem über die strafrechtlich

geregelten beruflichen Schweigepflichten, wie z.B. das Arztgeheimnis, einen zusätzlichen Schutz erfahren. Zu denken ist, dass das EDV-System sofort bei Eingabe der Personendaten einen Code generiert. Das System würde jedes Mal, wenn dieselben identifizierenden Angaben eingegeben würden, denselben Code hervorholen. Auf diese Weise wäre sichergestellt, dass Daten, die zu ein und derselben Person gehören, ein und demselben Code zugewiesen würden. Die Daten würden «anonymisiert» an das Drittunternehmen übermittelt. Die Auswertung erfolgte somit aufgrund dieser pseudonymisierten Daten.

Ein weiterer Aspekt im Zusammenhang mit den Qualitätsmessungs- und Qualitätssicherungsprojekten ist die Frage der Zweckbindung der bearbeiteten Daten. Nach dem Zweckbindungsgrundsatz dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Erfolgt vor der Beschaffung von Daten keine hinreichende Information der Klienten über den Verwendungszweck, scheint die Zweckbindung zweifelhaft. Aber auch in diesem Kontext ist zu differenzieren, ob die Qualitätsmessung und -sicherung dem Klienten unmittelbar wieder zugute kommen soll, dessen Daten ausgewertet werden. Der grundsätzliche Zweck der Bearbeitung von Klientendaten liegt in der Betreuung und/oder medizinischen Behandlung des Klienten. In diesem Fall kann davon ausgegangen werden, dass die Qualitätsmessung und -sicherung einen unmittelbaren Einfluss auf die Betreuung und die Behandlung der betreffenden Person hat. Somit kann bei dieser Konstellation davon ausgegangen werden, dass der Zweckbindungsgrundsatz eingehalten ist. Etwas Anderes gilt unserer Auffassung nach jedoch, wenn die Qualitätsmessung und -sicherung sowie die Auswertung der Daten künftigen Klienten in ähnlichen Situationen zugute kommen sollen. In diesen Fällen wäre die Bearbeitung von Personendaten nicht mehr vom Betreuungs- und Behandlungszweck gedeckt.

Ein weiterer Gesichtspunkt der Verhältnismässigkeit aber auch der Datensicherheit ist die Regelung der Zugriffsberechtigungen auf die entweder auszuwertenden Personendaten oder aber im Falle der Pseudonymisierung auf die Relationsdatenbank. Gerade im Hinblick auf die hohe Sensibilität der Daten sowie die Strafbarkeit der Verletzung des Arztgeheimnisses ist es unserer Ansicht nach erforderlich, zum Beispiel mittels Codierungssystemen und anwenderfreundlicher Software die Abläufe so zu gestalten, dass nur die behandelnden Ärzte oder die zuständigen medizinischen Hilfspersonen die Daten über klar strukturierte, für die Auswertung konzipierte Masken in das EDV-System eingeben. Die pseudonymisierten Daten würden den für die Auswertung zuständigen Personen zur Verfügung gestellt. Auf diese Weise wäre gewährleistet, dass nicht zuständige Personen nicht mit besonders schützenswerten Personendaten arbeiten müssten. Das Arztgeheimnis und die berufliche Schweigepflicht blieben gewahrt. Auf die Relationsdatei, die Auskunft darüber

gibt, welche Person hinter welchem Code steht, hätten Drittpersonen keinen Zugriff.

Im Zusammenhang mit der technischen Umsetzung von Zugriffsberechtigungen zum Beispiel auf die Relationsdatenbank gehen wir in die Richtung, die Verschlüsselung der Datenbank und nicht nur die individuellen Zugriffe der Daten zu vertreten.

7.3. Elektronisches Rezept

Auf dem Markt ist die Idee der Verwendung elektronischer Rezepte am Entstehen. Hier stellen sich Fragen der Einwilligung des Patienten und der Datensicherheit.

Im Computerzeitalter sind der Phantasie hinsichtlich des Einsatzes von EDV zum Zweck der Bearbeitung von Personendaten keine Grenzen gesetzt. So sind Ideen auf dem Markt, das bis anhin gebräuchliche Papierrezept durch ein elektronisches Rezept zu ersetzen. Gedacht ist folgender Ablauf: Der Patient geht zum Arzt. Nach der Untersuchung verschreibt der Arzt ein Medikament. Statt seinen herkömmlichen Rezeptblock an die Hand zu nehmen, greift der Arzt zu einem kleinen Computer in der Grösse des Rezeptblocks. Er gibt in die im Computer gespeicherte Maske sämtliche Angaben ein, die auch bis anhin für das Ausstellen eines Rezeptes erforderlich waren. Er kann das Rezept ausdrucken und in Papierform dem Patienten übergeben. Sinn und Zweck der Idee des elektronischen Rezeptes ist jedoch die elektronische Übermittlung des Rezeptes an die Wunschapotheke des Patienten nach mündlicher Absprache mit diesem. Nach Absenden des Rezeptes trifft dieses auf dem Server eines Verteilers (Drittfirma) ein. Dieser leitet das Rezept entsprechend den Adressaten an den Server der zuständigen Apotheke weiter. Von dem Server der Apotheke wird eine Rückmeldung an den Server des Verteilers geschickt, der wiederum dem verschreibenden Arzt die Übermittlung des Rezeptes bestätigt.

Für Überlegungen im Zusammenhang mit derartigen Vorhaben stehen für uns die Aspekte der Freiwilligkeit der Einwilligung des Patienten in die Übermittlung eines elektronischen Rezeptes sowie der Datensicherheit im Vordergrund.

Damit der Patient eine rechtsgültige Einwilligung abgeben kann, muss er vollumfänglich und in für ihn verständlicher Weise über die technischen und praktischen Folgen eines elektronischen Rezeptes informiert werden und er muss die tatsächliche Freiheit haben, sich für oder gegen das elektronische Rezept zu entscheiden. Dem Patienten muss transparent gemacht werden, wer auf welche seiner Daten Zugriff hat. Das bedeutet insbesondere, dass der Patient

davon Kenntnis haben muss, dass auch der Verteiler (Drittfirma) sogenannte Übermittlungsbestätigungen bearbeitet. Hinsichtlich dieser Bestätigungen ist die inhaltliche, für den Verteiler lesbare Ausgestaltung relevant. Je nach dem werden unmittelbar den Patienten identifizierende Elemente aufgenommen, die vom Verteiler gelesen werden können. Damit hätte der Verteiler Kenntnis davon, dass ein bestimmter Patient bei einem bestimmten Arzt in Behandlung war. Oder aber es wird lediglich eine vom Arzt vergebene Patientennummer aufgeführt, mittels derer der Verteiler den Patienten nicht identifizieren kann. Nur im letzten Fall ist unserer Auffassung nach dem Verhältnismässigkeitsgrundsatz Genüge getan und der Zugriff Unberechtigter auf sehr sensible Personendaten ausgeschlossen.

Ein anderer wesentlicher Aspekt der Datensicherheit ist die geschützte Übermittlung des elektronischen Rezeptes. Da aus dem Rezept Rückschlüsse auf die Krankheit einer bestimmten Person gezogen werden können, es sich mithin um besonders schützenswerte Personendaten im Sinne des Datenschutzes handelt, sind an die Sicherheit der Übermittlung sehr hohe Anforderungen zu stellen, um Zugriffe Unberechtigter zu verhindern (hierzu S. 74).

Wir sind der Auffassung, dass die Unternehmen, die derartige Projekte aufziehen und ihren Kunden – im vorliegenden Fall Ärzten und Apotheken – zur Verfügung stellen wollen, auch Verantwortung zur Umsetzung des Datenschutzes übernehmen müssen. Insbesondere müssen die technischen und organisatorischen Massnahmen dem heutigen Stand der Technik entsprechen.

7.4. Elektronische Abrechnung/Trust-Center

Es gibt verschiedene Projekte, deren Zweck die Realisierung der elektronischen Rechnung ist. Ziel ist, dass die Rechnung vom Leistungserbringer elektronisch an den Kostenträger verschickt wird. Neben einer schleichenden Entmündigung des Patienten bergen diese Projekte aus Sicht des Datenschutzes Probleme wie die Aushöhlung beziehungsweise Aufhebung des informationellen Selbstbestimmungsrechtes, die Frage der Verhältnismässigkeit der bearbeiteten Personendaten sowie Fragen der Datensicherheit.

Es werden zur Zeit von verschiedenen Interessenvertretern unterschiedliche Projekte auf dem Markt lanciert, die der Realisierung der elektronischen Rechnung dienen. Grundgedanke bei allen Projekten ist das Verschicken einer elektronischen Rechnung durch den Leistungserbringer an den Kostenträger (Versicherer).

Wir mussten feststellen, dass die Tendenz besteht, in den elektronischen Rechnungsformularen weit mehr Patientendaten zu bearbeiten als im Papierformat. Geht man davon aus, dass bis anhin dem Versicherer die papiernen Rechnungen mit den darauf enthaltenen Daten zur Kostenrückerstattung eingereicht wurden und dies auch ausreichte, stellt sich die Frage der Verhältnismässigkeit der bearbeiteten Daten bei der elektronischen Abrechnung. Es ist nicht nachvollziehbar, warum die Versicherer für die Kostenrückerstattung jetzt weit mehr Daten benötigen. Es drängt sich der Verdacht auf, dass aufgrund der Tatsache, dass mit den elektronischen Mitteln ohne Probleme weit mehr Daten bearbeitet werden können als in Papierformat, der Wunsch nach mehr Daten geweckt wird. Dies geschieht, obwohl die Datenmengen nicht unbedingt für die Aufgabenerfüllung in Form der Kostenrückerstattung erforderlich sind. Zudem sind wir der Auffassung, dass es hinsichtlich des Inhalts und des Umfangs der bearbeiteten Daten keinen Unterschied machen darf, ob der Schuldner der Patient oder aber die Versicherung ist, an die die elektronische Rechnung geschickt wird. Solange der Inhalt identisch ist, spielt es dagegen keine Rolle, ob in der Papierrechnung Klartext, in der elektronischen Rechnung dagegen für dieselbe Aussage ein Code verwendet wird.

Wie bei anderen Projekten, deren Zweck die Übermittlung von besonders schützenswerten Personendaten ist, ist darauf zu achten, dass die Übermittlung nach dem neusten Stand der Technik erfolgt (hierzu S. 74).

Treten in den Abläufen und Datenflüssen Drittfirmen als Verteiler der übermittelten Daten beziehungsweise als Trustcenter auf, stellen sich folgende Fragen: Welche Aufgaben haben diese Trustcenter konkret? Welche Daten bearbeiten diese Trustcenter, indem sie auf sie zugreifen, lesen oder diese mutieren können? Wie lange werden Daten in den Trustcentern gespeichert? Die Möglichkeiten der zu erfüllenden Aufgaben reichen von einem reinen Verteiler, der keinen Zugriff auf Inhalte der übermittelten Daten hat, bis hin zur Übernahme von Aufgaben des Versicherers im Rahmen eines Outsourcing.

Neben diesen Gesichtspunkten bergen die Projekte auch Probleme grundlegender Art. Der vom Bundesgesetz über die Krankenversicherung statuierte Grundgedanke des «tiers garant», bei dem der Patient der Schuldner ist und im Rahmen seiner Selbstverantwortung im Gesundheitsbereich die Rechnung an den Versicherer weiterleitet, wird schleichend aufgehoben. Darüber hinaus sind die tatsächlich erfolgenden Datenbearbeitungen sowie deren Umfang dem Patienten nicht mehr transparent. Auf diese Weise verliert der Patient die Möglichkeit zur Ausübung seines datenschutzrechtlichen informationellen Selbstbestimmungsrechtes. Er kann nicht mehr regulierend eingreifen, indem ihm die Möglichkeit genommen wird, selber zu entscheiden, welche Daten er an den Versicherer weitergeben will.

In diesem Zusammenhang stellt sich auch die grundlegende Frage der rechtsgenüglichen Einwilligung des Patienten in diese Form der Datenbearbeitung. Sollten sich diese Projekte auf dem Markt durchsetzen, scheint die für die Rechtsgültigkeit der Einwilligung erforderliche Freiwilligkeit zweifelhaft. Die Macht des Faktischen wird dem Patienten keine Möglichkeit mehr lassen, einen freien Entscheid zu fällen. Die rechtliche Zulässigkeit derartiger Bestrebungen werden damit fraglich.

7.5. Der Arzttarif Tarmed

Im Zusammenhang mit Tarmed - dem Arzttarif - sind aus datenschutzrechtlicher Sicht vor allen Dingen die Gesichtspunkte der detaillierten Diagnoseangabe auf dem Rechnungsformular sowie der elektronischen Rechnungsstellung relevant.

Auch beim neuen Arzttarif (Tarmed) ist die Verwendung elektronischer Rechnungen ein umstrittener Diskussionspunkt. Diesbezüglich verweisen wir auf die Ausführungen zur elektronischen Rechnungstellung/Trustcenter (siehe dazu S. 40).

Im Weiteren ist strittig, ob auf den Rechnungen systematisch detaillierte Diagnoseangaben an den Versicherer geschickt werden dürfen oder nicht. Wir sind der Ansicht, dass gemäss Bundesgesetz über die Krankenversicherung die systematische Bekanntgabe einer sogenannten Rahmendiagnose vertretbar und verhältnismässig ist. Demgegenüber halten wir an unserer Auffassung fest, dass systematische Bekanntgaben von detaillierten Diagnoseangaben weder mit dem Bundesgesetz über die Krankenversicherung noch mit dem Verhältnismässigkeitsgrundsatz vereinbar ist. In der Regel geben die Rechnungen keinen Anlass zu Zweifeln, weshalb eine Kostenrückerstattung ohne Probleme erfolgen kann. Dagegen kann der Versicherer in begründeten Einzelfällen detaillierte Diagnoseangaben und weitere Informationen verlangen, wenn ihm eine Rechnungstellung nicht nachvollziehbar ist. Wir wenden uns gegen ein systematisches Beschaffen und Horten von besonders schützenswerten Personendaten.

7.6. Verfahren zur Überprüfung von Wirtschaftlichkeit im Gesundheitsbereich

Im Zusammenhang mit Verfahren zur Überprüfung von Wirtschaftlichkeit wurden von den Versicherern sämtliche Rechnungen mit vollständigen Patientendaten des zu überprüfenden Leistungserbringers an Versicherungsverbände weitergeleitet. Nach dem Grundsatz der Verhältnismässigkeit ist eine Identifizierung des Patienten allenfalls in

Ausnahme- und Einzelfällen vertretbar. Es reicht aus, wenn erkennbar ist, dass erbrachte Leistungen ein und derselben Person zugute gekommen sind.

Nach dem Bundesgesetz über die Krankenversicherung ist der Leistungserbringer (Arzt, Spital, Heim, Therapeut) verpflichtet, seine Leistungen wirtschaftlich zu erbringen. Die Versicherer haben die Wirtschaftlichkeit der Leistungserbringer zu überprüfen. Da in der Regel Versicherer nicht über die nötigen Kapazitäten verfügen, die Wirtschaftlichkeitsüberprüfungen selber vorzunehmen, delegieren sie diese Aufgabe an die kantonalen Versicherungsverbände. Zum Zweck der Überprüfungen werden den Versicherungsverbänden von den Versicherern in der Regel nicht nur allgemeine Angaben über den Leistungserbringer wie Name, Adresse, Leistungserbringernummer, Art und Umfang von Leistungen nach Kategorien übermittelt. Vielmehr werden den Versicherungsverbänden auch systematisch Patientendaten bekannt gegeben. Wir haben uns gegen diese Praxis aus Gründen der Verhältnismässigkeit gewendet. Bei der Wirtschaftlichkeitsüberprüfung geht es ausschliesslich um eine Überprüfung des Leistungserbringers. Wir sind der Ansicht, dass es grundsätzlich ausreicht, wenn zu diesem Zweck erkennbar ist, welche Leistungen ein und derselben Person zugute gekommen sind. Es ist nicht erforderlich, dass für die Versicherungsverbände auch erkennbar sein muss, welche Person diese Leistungen bezogen hat. Die Zuordnung verschiedener Leistungen zu ein und derselben Person liesse sich durch die sogenannte Pseudonymisierung erreichen. Bei dieser würde dem einzelnen Patienten eine Nummer in Form eines Codes gegeben. Die Leistungen würden dieser Nummer und nicht dem Namen und der Adresse des Patienten zugeordnet. An die Versicherungsverbände würden von Versicherern diese pseudonymisierten Daten bekannt gegeben werden.

Da es unter den Versicherungsverbänden keine einheitliche Praxis hinsichtlich der Bekanntgabe von Patientendaten gibt, zum Teil jedoch erkannt wurde, dass die Versicherungsverbände grundsätzlich die Identität des Patienten für die Wirtschaftlichkeitsüberprüfung nicht benötigen, wurde seitens eines Versicherungsverbandes, dem Konkordat Schweizerischer Krankenversicherer, die Bitte unterbreitet, eine für die Schweiz einheitliche, alle Parteien befriedigende Regelung auszuarbeiten.

7.7. Die Herausgabe der Krankengeschichte an die Patienten

Immer häufiger verlangen Patienten von den Ärzten nicht nur die Einsicht in ihre Krankengeschichte, sondern deren Herausgabe. Wir vertreten weiterhin die Ansicht, dass die Krankengeschichte dem Patienten gehört, der Arzt aufgrund Gesetzesbestim-

mungen jedoch zur Aufbewahrung dieser verpflichtet ist. Für diesen Konflikt sind praktikable Lösungsansätze gefragt.

Immer häufiger gelangen Ärzte an uns mit der Problematik, dass Patienten von ihnen nicht nur eine Kopie ihrer Krankengeschichte im Rahmen des datenschutzrechtlichen Auskunftsrechtes, sondern die Herausgabe der Krankengeschichte verlangen. Die Ärzte sehen sich mit dem Konflikt konfrontiert, dass sie einerseits aufgrund kantonaler Gesundheitsgesetze zur Aufbewahrung der Krankengeschichte über mehrere Jahre hinweg verpflichtet sind, dass andererseits aus Sicht des Datenschutzes die Krankengeschichte dem Patienten gehört. Die Aufbewahrungspflicht dient dem Arzt unter anderem dazu, im Falle von Ansprüchen des Patienten gegen ihn aus dem Behandlungsverhältnis auch Beweismittel in der Hand zu haben. Die Herausgabepflicht genügt dagegen dem datenschutzrechtlichen informationellen Selbstbestimmungsrecht, nach dem jede Person das Recht hat, selbst zu bestimmen, wer welche Daten über sie bearbeitet.

Für diesen Konflikt ist eine praktikable Lösung zu suchen und zu finden. Wie bereits in unserem Leitfaden für die Bearbeitung von Personendaten im medizinischen Bereich dargelegt, kann unserer Ansicht nach die Lösung in einem Formular bestehen, mit dem der Patient bei Herausgabe der Krankengeschichte den Arzt ausdrücklich von seinen gesetzlichen und vertraglichen Aufbewahrungspflichten befreit und auf alle Ansprüche gegen den Arzt aus dem Behandlungsverhältnis verzichtet.

7.8. Übertragung medizinischer Daten per Internet

Die Übertragung von medizinischen Daten ist zwar einfach und dementsprechend verlockend, doch sind zur Vorbeugung schwerer Verstösse gegen den Datenschutz gewisse Verhaltensregeln zu beachten. Bei schützenswerten Daten müssen die Vorsichtsmassnahmen über die Übertragung selbst hinausgehen.

Seit einigen Jahren bereits ist eine Zunahme der Übertragung medizinischer Daten per Internet zu beobachten. Der Informationsaustausch findet statt zwischen Patienten und Ärzten, unter Ärzten, zwischen Ärzten und Untersuchungslabors, zwischen Krankenhäusern und Ärzten, zwischen Anbietern von Pflegediensten und Versicherungen, zwischen Versicherten und Versicherungen oder zwischen Arbeitnehmern und Arbeitgebern. Um der Gefahr der Übertragung von besonders schützenswerten Daten an Unbefugte vorzubeugen, sind folgende Regeln zu beachten:

- Rechtmässigkeit der Übertragung prüfen und nur genaue und unbedingt notwendige Daten austauschen;
- So oft wie möglich die Anonymisierung oder mindestens die Pseudonymisierung der Daten vornehmen. Die Verwendung der Initialen möglicherweise zusammen mit dem Geburtsjahr des Patienten stellen nur eine rudimentäre Form der Pseudonymisierung dar, bei der die Identifizierung durch Dritte und vor allem eine falsche Identifizierung durch den Empfänger eine grosse Gefahr darstellt. Sinnvoller wäre daher die Verwendung eines richtigen Pseudonyms wie beispielsweise der für das Bundesamt für Statistik entwic??kelten «anonyme» Verbindungscode;
- Bei der Übertragung von medizinischen Daten über identifizierte oder identifizierbare Personen ausschliesslich sichere Übertragungskanäle verwenden. Für die Verbindung mit Web-Servern sollte das Protokoll HTTPS (mit mindestens 128-Bit-Verschlüsselung während jeder Internet-Sitzung) verwendet werden. Bei der elektronischen Post sind die übertragenen Informationen unbedingt zu verschlüsseln oder gar elektronisch zu signieren. Dies gehört in den Bereich der Public Key Infrastructure, für die heute bereits konkrete, wirksame und wirtschaftliche Lösungen existieren (Zertifizierung Swisskey, web-of-trust «Pretty Good Privacy»...).

Selbstverständlich dürfen sich der Schutz und die Sicherheit nicht nur auf die Übertragung der Daten beschränken. Sie müssen auch nach Ankunft beim Empfänger sicher und vertraulich weiterbehandelt werden. Auf tragbaren Computern oder Personal Digital Assistant sind medizinische Daten unbedingt in verschlüsselter Form zu speichern. Direkt an das Internet angeschlossene Systeme müssen mit angemessenen Schutzwällen ausgestattet sein (Router, Filter, Firewall), um sie gegen Angriffe von aussen abzusichern. Schliesslich müssen die auf einem LAN-Server gespeicherten Daten selbstverständlich derart geschützt sein, dass sie nur für Zugriffsberechtigte zugänglich sind.
In Zukunft sind vermehrt elektronische Dossiers zu erwarten, welche die gesamte Krankheitsgeschichte des Patienten enthalten und völlig transparent verwaltet werden.

8. Genetik

8.1. Gesetz betreffend die Verwendung des DNA-Profils

Die Ausarbeitung eines Gesetzesentwurfs betreffend die Verwendung des DNA-Profils wurde von uns begrüsst, doch bedauern wir den Verzicht auf ein externes Vernehmlassungsverfahren bei den interessierten Kreisen. Bei der Prüfung des Entwurfs haben wir folgende Auffassung vertreten: Die Erhebung genetischen Materials darf nur mit rich-

terlicher Verfügung und nur in den ausdrücklich vom Gesetz vorgesehenen Fällen (Deliktekatalog) stattfinden. Bei Einstellung des Verfahrens oder Freispruch müssen die DNA-Profile automatisch aus der Datenbank gelöscht und das genetische Material vernichtet werden.

Provisorische Rechtsgrundlage für die Bearbeitung genetischer Daten zwecks Strafuntersuchungen und insbesondere für die nationale DNA-Profil-Datenbank bildet die Verordnung über das DNA-Profil-Informationssystem. Aus der Sicht des Datenschutzgesetzes ist diese Rechtsgrundlage unzureichend, da es um die Bearbeitung besonders schützenswerter Daten geht. Ohne das Projekt zu billigen, erklärten wir im März 2000, dass wir diesen Lösungsansatz nicht bekämpfen, unter der Bedingung, dass die Erarbeitung einer formalgesetzlichen Grundlage rasch in Angriff genommen wird (siehe 7. Tätigkeitsbericht 1999/2000, S. 52). Das Eidgenössische Justiz- und Polizeidepartement (EJPD) blieb seinem Engagement treu und unterbreitete dem Bundesrat im Oktober 2000 den Entwurf eines Bundesgesetzes über die Verwendung von DNA-Profilen im Strafverfahren und zur Indentifizierung von unbekannten und vermissten Personen.

Das genetische Material des Menschen und das DNA-Profil sind weit mehr als gewöhnliche Fingerabdrücke oder Fotografien, da es Rückschlüsse auf Krankheiten, Erbkrankheiten und Veranlagungen zulässt. Auch ist nicht auszuschliessen, dass in naher Zukunft aus DNA-Profilen Informationen über Veranlagung oder gar den Gesundheitszustand einer Person abgeleitet werden können. DNA-Profil-Datenbanken und die Aufbewahrung von genetischem Material stellen daher eine reelle Gefahr für die Grundrechte der betroffenen Personen dar. Aus diesem Grunde sind hierfür strengere Vorschriften als für die «gewöhnliche» Identifizierung (Fingerabdrücke und Fotografien) notwendig. Der dem Parlament vorliegende Gesetzesentwurf enthält mehrere problematische Aspekte:

Bei den Diskussionen über die Notwendigkeit eines externen Vernehmlassungsverfahrens wurde insbesondere argumentiert, dass ein solches Verfahren bereits für den Gesetzesentwurf über genetische Untersuchungen beim Menschen stattgefunden habe. Dieser Entwurf betraf jedoch nicht in erster Linie die Verwendung von DNA-Profilen im Rahmen von Strafverfahren. Die minimalen Abschnitte, die dieser Frage gewidmet waren, entsprachen zudem in keiner Weise dem Entwurf, der nun dem Parlament vorliegt. Da es im Zusammenhang mit der Analyse von DNA-Profilen im Rahmen eines Strafverfahrens zahlreiche Unklarheiten gibt und es sich um eine ausserordentlich heikle Frage handelt, sind wird der Auffassung, dass ein externes Vernehmlassungsverfahren notwendig gewesen wäre.

Darüber hinaus böte ein im Gesetz verankerter Deliktekatalog eine Gewähr für die restriktive Verwendung der DNA-Analyse im Rahmen eines Strafverfahrens, während das Modell des EJPD der Polizei die Möglichkeit gibt, sich ohne eindeutigen rechtlichen Rahmen Proben zu beschaffen. Für die Telefon- und Postüberwachung haben wir ebenfalls die Notwendigkeit eines gesetzlichen Deliktekataloges betont. Diesem Vorschlag ist das Parlament bei der Annahme des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs gefolgt.

Die oben erwähnten Risiken und Gefahren rechtfertigen auch das Anrufen des Richters. Die richterliche Anordnung für die Erhebung von genetischem Material stellt keine Behinderung der Polizeiarbeit dar. Ausserdem ist es durchaus denkbar, dass die Polizei in dringenden Fällen selbst über die Erhebung entscheidet. Diese Entscheidung sollte später durch den Richter bestätigt werden.

Wir befürworten ebenfalls die automatische Löschung des Eintrags aus der DNA-Profil-Datenbank und die Vernichtung des genetischen Materials im Falle eines Einstellungsbeschlusses oder eines Freispruchs. Die Möglichkeit der zu unrecht angeklagten Person, sich in derselben Lage wie vor der erkennungsdienstlichen Behandlung wiederzufinden, stellt ein höheres Interesse dar als die vom EJPD zugunsten einer Löschung auf Gesuch der betroffenen Person vorgebrachten Argumente. Insbesondere wird vorgebracht, das Anmeldeverfahren zwischen den Strafverfolgungsbehörden und der für die DNA-Profil-Datenbank verantwortlichen Stelle sei unverhältnismässig.

9. Finanzen

9.1. Geldwäschereigesetz und Anerkennung von Finanzintermediären

Gemäss Geldwäschereigesetz hatten die Finanzintermediäre bis zum 1. April 2000 Zeit, sich einer anerkannten Selbstregulierungsorganisation anzuschliessen, ansonsten sie der direkten Aufsicht durch die Kontrollstelle für die Bekämpfung der Geldwäscherei unterstehen. Dabei mussten wir überprüfen, ob die von einer anerkannten Selbstregulierungsorganisation für diesen Anschluss von den Finanzintermediären verlangten Unterlagen datenschutzrechtlich zulässig waren. Wir machten die Kontrollstelle für die Bekämpfung der Geldwäscherei darauf aufmerksam, dass sich nach Ablauf von zwei bis drei weiteren Jahren eine erneute Evaluation der Situation aufdrängen würde.

Gemäss dem Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (GwG) gelten als Finanzintermediäre auch Personen, die berufsmässig fremde

Vermögenswerte annehmen oder aufbewahren oder helfen, sie anzulegen oder zu übertragen. Diese können sich einer anerkannten Selbstregulierungsorganisation (nachfolgend SRO) anschliessen, die dann den Finanzintermediär beaufsichtigt. Finanzintermediäre, die sich keiner SRO anschliessen, unterliegen der direkten Aufsicht der Kontrollstelle für die Bekämpfung der Geldwäscherei. Die Finanzintermediäre hatten ab dem Inkrafttreten des GwG (1. April 1998) zwei Jahre Zeit, sich einer SRO anzuschliessen, ansonsten sie der direkten Aufsicht durch die Kontrollstelle unterstehen.

Im Zusammenhang mit seinem Gesuch um Aufnahme in eine anerkannte SRO gelangte ein Finanzintermediär an uns. Er vertrat die Auffassung, dass die SRO auf ihren Aufnahmeformularen zu viele persönliche Angaben verlangen würde. Wir stellten zunächst fest, dass gemäss GwG die SRO die Voraussetzungen für Anschluss und Ausschluss von Finanzintermediären in einem Reglement festhalten müssen. Dieses Reglement seinerseits ist von der Kontrollstelle für die Bekämpfung der Geldwäscherei zu genehmigen. Im vorliegenden Fall musste der Finanzintermediär gemäss Reglement der SRO nachweisen, dass alle mit der Geschäftsführung und Verwaltung vertrauten Personen über einen guten Leumund in Bezug auf diese Tätigkeit verfügten. Zudem hatte er aufgrund einer angemessenen Betriebsorganisation die Erfüllung der Pflichten nach GwG sicherzustellen. Die gleichen Voraussetzungen werden gemäss GwG ebenfalls von der Kontrollstelle selbst für die ihr direkt unterstellten Finanzintermediäre verlangt.

Zu prüfen war sodann, ob die von der SRO verlangten Unterlagen verhältnismässig, das heisst für diesen Nachweis des guten Leumunds wirklich nötig und geeignet waren. Unserer Meinung nach konnten im vorliegenden Fall allenfalls der verlangte unterzeichnete Lebenslauf sowie die verschiedenen Referenzschreiben mit dem Verhältnismässigkeitsprinzip in Konflikt stehen. Da uns aber konkrete Anhaltspunkte fehlten, konnten wir die Frage nicht abschliessend beurteilen. Wir wiesen jedoch darauf hin, dass im Bankbereich neue Banken ihren Bewilligungsgesuchen ebenfalls unterzeichnete Lebensläufe sowie Referenzen der mit der Verwaltung und Geschäftsführung betrauten Personen beilegen müssen. Da die Banken ebenfalls als Finanzintermediäre im Sinn des GwG gelten, konnte ein Vergleich nicht ohne weiteres ausgeschlossen werden. Daher hielten wir fest, dass die von der SRO verlangten Unterlagen nicht von vorn herein eine Verletzung des Verhältnismässigkeitsprinzips darstellten. Wir machten den Finanzintermediär darauf aufmerksam, dass er die Wahl habe, sich entweder einer anderen anerkannten SRO oder der Kontrollstelle selbst zu unterstellen.

Wie erwähnt, trat das GwG erst auf den 1. April 1998 in Kraft. Zudem konnten die Finanzintermediäre bis zum 1. April 2000 ein Bewilligungsgesuch einreichen. Aus diesem Grund war es noch zu früh, eine Gesamtüberprüfung der in

diesem Zusammenhang verlangten Personendaten zu machen. Wir wiesen die Kontrollstelle für die Bekämpfung der Geldwäscherei jedoch darauf hin, dass sich nach Ablauf von zwei bis drei weiteren Jahren eine erneute Evaluation der Situation aufdrängen würde. Dies ist notwendig, um insbesondere zu überprüfen, welche Unterlagen für den verfolgten Zweck (Bekämpfung der Geldwäscherei) wirklich nötig und geeignet sind.

10. Werbung und Marketing

10.1. Unerwünschte Werbung und Belästigung schwacher Personen

Aggressive Marketing-Kampagnen, die sich an ältere oder gar kranke Menschen richten, werden immer häufiger. Dem Versandgeschäft kommen geschwächte Menschen sehr gelegen. Da derartige Werbeoffensiven häufig auf internationaler Ebene stattfinden, können sich die Geschädigten nur schwer zur Wehr setzen.

In der Wahrsager-Branche entwickelte sich beispielsweise ein Adresshandelsnetz zwischen Belgien und der Schweiz. Empfänger der Prospekte sind meist in der Schweiz oder in Belgien lebende Senioren, die gelegentlich die Dienste eines Wahrsagers in Anspruch genommen haben. Aus der Schweiz werden via Rotterdam meist inhaltlich ähnliche Sendungen verschickt: Ankündigung glücklicher Ereignisse und hoher finanzieller Gewinne, wenn sich der Empfänger für das Angebot entscheidet. Hingegen wurde grosses Unheil prophezeit, falls das Angebot abgelehnt werden sollte. Mit Hilfe von Fristen wird darüber hinaus der Beantwortungsdruck verstärkt.

Unsere Ermittlungen haben den Ursprung dieser Sendungen aufgedeckt. Durch unser Eingreifen erhielten die Kläger die Bestätigung der Löschung ihrer Daten aus den Datensammlungen. Sie wurden unseres Wissens nicht weiter belästigt.

11. Statistik

11.1. Die Grundsätze zur Bearbeitung von Personendaten zu statistischen Zwecken

Bei der Statistik geht es unter anderem um das Beschaffen und Bearbeiten von Personendaten. Solche Daten sind bei den Akteuren der Gesellschaft, Wirtschaft, Kultur, Politik und Verwaltung heiss begehrt und können für sie äusserst nützlich sein. Dabei besteht die Gefahr, dass Daten zweckentfremdet und für nicht-statistische Belange genutzt werden.

Anonyme aggregierte Statistikresultate könnten analysiert und kombiniert und so nach den Personen, aus der sich die beobachtete Bevölkerung zusammensetzt, erschlossen werden.

Öffentliche Organisationen oder private Stellen, die Personendaten zu statistischen Zwecken beschaffen und bearbeiten, müssen die Datenschutzauflagen befolgen, um die Achtung der grundlegenden Rechte und Freiheiten jedes Einzelnen – vor allem das Recht auf Achtung des Privatlebens – zu gewährleisten. Ausserdem sind Statistiker verpflichtet, höchste Vertraulichkeit zu garantieren, wenn sie Zugriff auf Daten beanspruchen, aus denen sie verlässliche statistische Informationen beziehen. Bei der Suche nach dem richtigen Gleichgewicht zwischen den Anforderungen des Datenschutzes und dem Bedarf der Statistik an Personendaten müssen drei Kriterien beachtet werden:

- Transparenz der Bearbeitung für die betroffenen Personen;
- strikte Befolgung des Zweckbindungsgrundsatzes, wonach zu statistischen Zwecken beschaffte und bearbeitete Daten nicht zu anderen Zwecken verwendet werden dürfen;
- anonyme Datenbearbeitung.

Das Vertrauen in die statistischen Instrumente bildet eine unverzichtbare Voraussetzung für das Funktionieren und die Entwicklung der Statistik. Selbst geringste Zweifel an der Verwendung der zu statistischen Zwecken beschafften Daten beeinträchtigen das Vertrauen und die Verlässlichkeit der statistischen Instrumente. Der Zweckbindungsgrundsatz und das statistische Geheimnis müssen daher uneingeschränkt gewährleistet werden. Zu statistischen Zwecken beschaffte und bearbeitete Daten dürfen nicht mehr zu nicht-statistischen personenbezogenen Zwecken (vor allem für Entscheidungen oder Massnahmen in bezug auf diese Personen) verwendet werden.

In dieser Hinsicht muss die Funktionsweise und die Organisation der Statistik weiter entwickelt werden. Die Ära der grossen Volkszählungen und der erschöpfenden Erhebungen gehört wahrscheinlich der Vergangenheit an. Dagegen werden immer häufiger Daten statistisch verwertet, die zu anderen Zwecken beschafft und bearbeitet wurden. Mitunter wird die Information durch sektorielle Erhebungen auf der Basis von Stichprobenpopulationen (Mikrozensus) ergänzt. Die sekundäre Datenverwendung verlangt eine Harmonisierung der Register und der Bearbeitungen, damit die Daten zu statistischen Zwecken verwendet werden dürfen (ein Bundesgesetz über die Harmonisierung der Register befindet sich in Vorbereitung). Daraus ergeben sich neue Herausforderungen für die Achtung des Privatlebens. Die Harmonisierung darf nicht dazu führen, dass neue, von den Statistikstellen verwaltete zentralisierte Bevölkerungsregister entstehen. Angesichts des (mit Rationalisierung und Effizienz legitimierten)

Drucks auf der Verwaltung ist zu befürchten, Register könnten auch zu nicht-statistischen Zwecken verwendet werden, was heute für existierende Register (Firmen, Gebäude, Wohnungen) bereits der Fall ist. Identifizierungsdaten dürfen nicht länger quasi unbefristet in statistischen Registern aufbewahrt werden, wenn sie nur für bestimmte statistische Bearbeitungsphasen erforderlich sind. Aus diesem Grund fordern wir Folgendes:

- die Statistik sollte die Bearbeitung von Personendaten reduzieren, welche die Beschaffung oder gar Aufbewahrung von Daten, die direkte Rückschlüsse auf den Einzelnen erlauben, voraussetzen;
- die Statistik soll gestützt auf die datenschutzfreundlichen Technologien mit anonymen Einzeldaten arbeiten und insbesondere codierte Identifizierungsdaten oder Pseudonyme benutzen.

Mit solchen Mechanismen lässt sich die Bearbeitung von Personendaten begrenzen. Ausserdem verhelfen sie den datenschutzrechtlichen Anforderungen in der Statistik - insbesondere dem Zweckbindungsgrundsatz - mehr Beachtung. Die Zugriffsrechte der Statistiker auf notwendige Informationen werden nicht eingeschränkt, sondern neu organisiert.

11.2. Der Datenschutz in geografischen Informationssystemen

Das Aufkommen der Informationsgesellschaft und die explosionsartige Verbreitung der Teleinformatik-Technologien bewirken tiefgreifende Umwälzungen des sozialen Umfelds und unseres Umgangs mit Information. Individuelle, gesellschaftliche, berufliche, wirtschaftliche, kommerzielle, politische und kulturelle Entscheidungen hängen von der Qualität der verfügbaren Information sowie von unseren Fähigkeiten und unserem Zugang zu relevanter Information ab. Unter den heute expandierenden Informationstechnologien spielen die geografischen Informationssysteme und die Gebietsinformationssysteme eine wichtige Rolle; sie bilden einen festen Bestandteil der Informationsinfrastruktur.

Bei den Gebietsinformationssystemen handelt es sich um Entscheidungs- und Planungsinstrumente, die auf Informatiksystemen zur Datenerfassung und -verwaltung und zur standardisierten oder spezifischen Datenextraktion beruhen. Ursprünglich waren die Systeme bestimmten Tätigkeiten der öffentlichen Verwaltungen – insbesondere in den Bereichen Raumplanung, Grundbuch, amtliche Vermessungen, Topographie, Umwelt und Statistik – vorbehalten. Heute erfreuen sie sich auch bei anderen öffentlichen Stellen steigender Beliebtheit. Auch im Privatsektor, vor allem im Versicherungswesen, Marketing, in der Kreditberatung, im Transport und im Tourismus gewinnen sie an Popularität.

Die kommerziellen Verwendungszwecke von geografischen Informationssystemen haben stark zugenommen, und digitalisierte Gebäudeaufnahmen werden systematisch vorgenommen. Damit können Datenbanken aufgebaut werden, die den vollständigen Liegenschaftsbestand aufführen. Ausserdem sind solche Informationen immer häufiger für die breite Öffentlichkeit bestimmt.

Obwohl zahlreiche Anwendungen im Zusammenhang mit geografischen Informationssystemen durchaus legitim erscheinen und einem unbestrittenen öffentlichen Interesse entsprechen, lasten die weitreichenden Konsequenzen der Systeme betreffend Technologie und Information den Gestaltern und Benutzern eine schwere gesellschaftliche Verantwortung auf. Die Systeme besitzen neben zahlreichen Vorteilen auch Nachteile, die kontrolliert werden müssen. Eine negative Auswirkung besteht in den realen oder potenziellen Beeinträchtigungen der Persönlichkeitsrechte und den Grundrechten, insbesondere des Rechts auf Privatsphäre.

In der Auseinandersetzung mit dem Problem geografische Informationssysteme hatten wir zunächst den Eindruck, dass die Systeme den Schutz von Personendaten nicht berührten. Ein geografisches Informationssystem betrifft in erster Linie das Gebiet, den Raum und die Umwelt. An sich dürfte es keine Angaben über bestimmte oder bestimmbare Personen enthalten. Räumliche Daten umfassen jedoch nicht nur rein geografische Angaben, sondern auch sogenannte ökonomische oder statistische Attribute, die persönlichen Charakter besitzen können, d.h. sich auf eine identifizierte oder identifizierbare Person beziehen. Geografische Informationssysteme, die sich auf relationale Datenbanken stützen, ermöglichen die Erfassung von geometrischen (geokodierte Daten, Positionen, Koordinaten) und faktischen Daten (Eigenschaften, Attribute). Sie erleichtern die inhaltliche und räumliche Verknüpfung der Daten in einem komplexen logischen Verhältnis. In der Kartographie werden mit den Computertechnologien komplexe Modelle entwickelt, welche sehr genaue Analysen liefern und dadurch Rückschlüsse auf die Personen erleichtern. Mit an die - vor allem satellitengestützte - Fernerkundung gekoppelten geografischen Informationssystemen lassen sich Vorgänge, die durch Beobachten vor Ort schwer erkennbar sind, auf einer Karte problemlos orten. So wird es möglich, Personen in Bezug auf einen Ort, ein Objekt oder ein Gebäude zu identifizieren. Mit solchen Techniken kann z.B. ein Fahrzeug geortet, ein Gebäude lokalisiert, die Verwendung von Agrarsubventionen überwacht oder zur Schadenskontrolle beigetragen werden. Die Systeme stellen also äusserst leistungsfähige Instrumente dar, welche (vor allem durch die Verknüpfung mit der geographischen Lokalisierung, dem sog. Geokodierungsverfahren) eine Datenintegration ermöglichen. In Bereichen wie dem Marketing, dem Versicherungswesen oder der Kreditberatung erweisen sich die Systeme als vielversprechende Technik mit einen ungeahnten Potenzial, Daten über Einzelpersonen, Haushalte und Unternehmen aus verschiedenen Informationsquellen zu kombinieren und zusammen-

zustellen. Tatsächlich lassen sich Informationen aus verschiedenen Datenbeständen - insbesondere aus öffentlichen Registern - miteinander verknüpfen und verschiedenen Benutzern zugänglich machen. In der Kartenherstellung kann das Haushaltsprofil im Massstab einer kleinen Gemeinde, eines Quartiers oder einer Strasse nach Alter, Beruf, Kinderzahl, Einkommens- oder Vermögensstufe, Wohnungstyp usw. abgebildet werden. Geografische Informationssysteme haben sich zu äusserst leistungsfähigen Werkzeugen zur Analyse und Bearbeitung von Personendaten entwickelt. Wegen der Datenintegration und der analytischen Aussagekraft und wegen der lokalen und räumlichen Angaben bieten solche Systeme ein bei anderen Informationssystemen unbekanntes Potenzial, weit in die Privatsphäre des Einzelnen einzudringen.

Die Entwicklung der geografischen Informationssysteme und der Gebietsinformationssysteme muss den Imperativen des Rechtsstaates und der demokratischen Gesellschaft Rechnung tragen. Insbesondere müssen sie die Persönlichkeits- und die Grundrechte beachten. Daher ist es erforderlich, die Einführung und Verwendung solcher Systeme in einen geeigneten Rahmen an Gesetzen und Verordnungen zu stellen, um den Datenschutz zu gewährleisten, gleichzeitig aber überwiegende öffentliche oder private Interessen, welche gegebenenfalls die Bearbeitung von Personendaten rechtfertigen, zu berücksichtigen. Dabei muss insbesondere Folgendes gewährleistet werden:

- *die Transparenz der Bearbeitung von Personendaten in einem geografischen Informationssystem:* Die betroffenen Personen müssen über den Zweck des Systems, die Kategorien der bearbeiteten Daten, die Systembenutzer und die Informationsempfänger unterrichtet werden und ihre Rechte einfordern können.

- *Die Verwendungszwecke des geografischen Informationssystems müssen festgelegt und eingehalten werden.* Bei nicht-personenbezogenen Verwendungszwecken (insbesondere im Rahmen der Statistik) muss das Statistikgeheimnis gewahrt und die Anonymität in der Veröffentlichung oder Verbreitung gewährleistet werden.

- Über die bearbeiteten Daten wird ein Katalog erstellt: *Nur die zum Bearbeitungszweck notwendigen Daten dürfen beschafft und bearbeitet werden*.

- *Gewährleistung der Datenqualität* (Richtigkeit, Aufdatierung, befristete Aufbewahrung).

- Die *Datenbekanntgabe*, vor allem per Abrufverfahren, muss einer *klaren Regelung unterstellt werden.*

- Der Rechtsrahmen muss flankierende *technische und organisatorische Massnahmen* beinhalten. Insbesondere sollte die Entwicklung und Verwendung der sogenannten datenschutzfreundlichen Technologien gefördert werden.

- *Die Rechte der betroffenen Personen müssen gewährleistet werden*. Das gilt namentlich für das Recht auf vorangehende Information, das Auskunftsrecht zu Daten über sie und das Recht, das systematische Beschaffen und Bearbeiten von Bilddaten zum Wohnumfeld zu kommerziellen Zwecken zu verweigern. Die betroffene Person hat das Recht, sich der Datenberbreitung über Internet oder der Speicherung auf CD-Rom zu widersetzen.

11.3. Durchführung der Volkszählung 2000

Als Stichtag der Volkszählung wurde der 5. Dezember 2000 festgelegt. Alle zu diesem Zeitpunkt in der Schweiz wohnhaften Personen mussten einen Fragebogen ausfüllen und haben so an dieser umfassenden Erhebung teilgenommen, die eine soziokulturelle Übersicht des Landes wiedergeben soll. Unsere Aufgabe bestand darin, für die Einhaltung der Vorschriften des Bundes über den Datenschutz zu sorgen. Im Allgemeinen wurden die verschiedenen Phasen der Volkszählung ordnungsgemäss durchgeführt. Dennoch gilt es auch weiterhin, wachsam zu bleiben und unsere Beratungs- und Kontrollfunktion auszuüben.

Die Volkszählung 2000 fand am 5. Dezember 2000 statt. Die Personen-, Haushalts- und Gebäudefragebögen wurden vorgedruckt und an alle in der Schweiz wohnhaften Personen zugestellt. In den Kantonen Luzern und Jura haben die vorgedruckten Daten zu einigen Schwierigkeiten geführt. Durch das Eingreifen der kantonalen Überwachungsbehörden konnten die Fehler berichtigt werden. Anschliessend wurden die ausgefüllten Fragebögen entweder per Post oder per Internet über das System «e-census» an das Bearbeitungszentrum gesandt. Die Internet-Übertragung der Volkszählungsdaten erfolgte mittels einer 128-Bit-Verschlüsselung, die dem heutigen Stand der Technik entspricht und eine hohe Sicherheit gewährleistet. Dem vom Bundesamt für Statistik (BFS) entwickelten Konzept «e-census» schenken wir bei der Ausführung unserer Kontrollaufgaben besondere Aufmerksamkeit, wobei uns das dazugehörende Bearbeitungsreglement von grossem Nutzen sein wird.

Die meisten Kantone und zahlreiche Gemeinden haben die im Zusammenhang mit der Volkszählung anfallenden Aufgaben einem Dienstleistungszentrum übertragen, das vom BFS beauftragt wurde und aus mehreren Unternehmen be-

steht. Die Räumlichkeiten befinden sich in verschiedenen Städten und Kantonen.

Das Verfahren zur Bearbeitung der Fragebögen kann wie folgt zusammengefasst werden: Die von Hand ausgefüllten Fragebögen wurden direkt beim Eintreffen im Briefzentrum in Luzern gescannt. Danach wurde die elektronische Fassung zur Verbesserung der Lesbarkeit an das Unternehmen DCL Data Care AG in Kriens (Kanton Luzern) weitergeleitet.

Für Fragen zu den Formularen wurde ein telefonischer Auskunftsdienst (Hotline) eingerichtet.

Nach Ablauf der Frist für das Einreichen der Fragebögen (12. Dezember 2000) kam ein telefonisches und schriftliches Mahnungssystem zum Einsatz.

Das Dienstleistungszentrum war verpflichtet, alle erforderlichen Massnahmen zur Sicherstellung des Datenschutzes zu treffen. Oberstes Gebot für DCL war die Einhaltung der datenschutzrechtlichen Anforderung im Bundesgesetz über die Volkszählung, in der Vollzugsverordnung über die eidgenössische Volkszählung, in den Richtlinien des BFS über die Arbeiten des Dienstleistungszentrums und in den Verträgen mit dem BFS.

Das Informatiksystem des Dienstleistungszentrums wurde vor Inbetriebnahme durch die Einheit für Informatikstrategie des Bundes und durch unsere Vertreter kontrolliert. Darüber hinaus wurde ein externes Kontrollorgan mit der Erstellung eines Berichtes zum Datenschutz im Dienstleistungszentrum beauftragt.

Im Mai 2000 entstand eine Datenschutz-Kontrollgruppe bestehend aus unseren und kantonalen Vertretern (Zürich, Basel-Landschaft und Freiburg). Diese Gruppe wurde während der Phase des Vordrucks der Volkszählungsformulare tätig. Als Überwachungsorgan hatte die Gruppe für die Einhaltung und Koordinierung der Weisungen in Sachen Datenschutz auf Bundes- und Kantonsebene zu sorgen.

Die in der Kontrollgruppe vertretenen Kantone wünschten ihre Beteiligung ab dem 5. Dezember 2000 zu unterbrechen, d.h. ab Beginn der neuen Phase, zu der vor allem in unseren Zuständigkeitsbereich fallende Bundesaufgaben gehören. Die Verantwortlichen in den Kantonen konzentrieren sich seitdem auf die Datenbearbeitung in Kantonen und Gemeinden. Für Daten, deren Bearbeitung von den Kantonen an DCL delegiert wurde, können sie aber nach wie vor Kontrollen im Dienstleistungszentrum durchführen.

Wir haben im Dezember 2000 und im Januar 2001 Kontrollen in den mit Volkszählungsaufgaben beauftragten Stellen durchgeführt. Unsere Vertreter haben folgende Einrichtungen besucht:

- die Gebäude des Briefzentrums (Schweizer Post) in Luzern, wo die Umschläge mit den Fragebögen eintrafen;
- das Dienstleistungszentrum DCL in Kriens;
- die Hotline und
- das für die Vervollständigung der Fragebögen zuständige Call-Center.

Bei den Besuchen ging es im Wesentlichen darum, die Einhaltung der Datenschutzvorschriften zu überprüfen. Die Räumlichkeiten wurden kontrolliert, um die Gewährleistung der Sicherheit bei Datenzugriff und -aufbewahrung sicherzustellen. Die Mitarbeiter wurden befragt, um festzustellen, ob sie in Sachen Datenschutz ausreichend geschult und sensibilisiert wurden. Die Kommunikationsmittel und Datenträger wurden kontrolliert. Schliesslich wurde ebenfalls die Informatiksicherheit geprüft.

Die Kontrollen haben zu keinerlei Befürchtungen hinsichtlich der Datensicherheit Anlass gegeben. Die für die Kontrollen notwendigen Unterlagen wurden zur Verfügung gestellt und gezielte Stichproben zeigten, dass die Aufgaben ordnungsgemäss von einem über das einzuhaltende Amtsgeheimnis informierten Personal ausgeführt wurden.

Noch anstehende Aufgaben zur Volkszählung sind die Erhebung noch fehlender Daten (Vervollständigung), die Vollzähligkeitserhebung, der Datenrückfluss an Kantone und Gemeinden, die Anonymisierung, die Auswertung der in den eingegangenen Fragebögen enthaltenen Daten und schliesslich die Vernichtung oder Archivierung der für die Volkszählung 2000 verwendeten Datenträger. Wir werden während den einzelnen künftigen Etappen Kontrollen durchführen.

12. Modernisierung des Datenschutzes

12.1. Unterwegs zu einer Modernisierung des Datenschutzes

Nach der Annahme zweier Motionen der Geschäftsprüfungskommission und der Kommission für Rechtsfragen des Ständerates wurde das Bundesamt für Justiz beauftragt, einen Vorentwurf für die Revision des Bundesgesetzes über den Datenschutz vorzubereiten. Der Vorentwurf wird im Jahr 2001 in die Vernehmlassung gegeben. Der Eidgenössische Datenschutzbeauftragte hat an den Arbeiten mitgewirkt.

Acht Jahre nach dem Inkrafttreten des Bundesgesetzes über den Datenschutz (DSG) ist der Bundesrat daran, dem Parlament eine Botschaft zur Teilrevision des DSG zu unterbreiten. Mit der Veränderung soll der Motion 98.3529 der Geschäftsprüfungskommission des Ständerates «Erhöhter Schutz für Personendaten bei Online-Verbindungen» sowie der Motion 00.3000 der Kommission für Rechtsfragen des Ständerates «Erhöhte Transparenz bei der Erhebung von Personendaten» Folge geleistet werden. Gemäss den beiden Motionen betrifft die Revision in erster Linie die Einführung einer Gesetzesbasis, welche die Durchführung von Pilotprojekten mit Zugriff per Abrufverfahren ermöglichen würde. Die Revision wird Mindestvorschriften für Zugriffsrechte, Verwendung und Kontrolle der eidgenössischen Datenbanken festlegen, um die Zusammenarbeit zwischen Bund und Kantonen zu verbessern. Schliesslich wird die Informationspflicht der privaten Personen beim Beschaffen von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen eingeführt. Daneben soll sich die Revision noch auf weitere Aspekte beziehen.

Aus Anlass der Revision möchten wir Bilanz zur Anwendung des DSG ziehen und untersuchen, inwieweit ein Veränderungsbedarf des Gesetzes gegeben ist. Obwohl das DSG erst vor relativ kurzer Zeit verabschiedet wurde, beruht es auf dem Konzept der Datenschutzgesetzgebungen Ende der 70er Jahre. Im Gegensatz zu bestimmten kantonalen und ausländischen Gesetzen verfolgt das DSG jedoch einen nicht-technologischen Ansatz, der eine gewisse Flexibilität bietet und eine bessere Anpassung an die technologische Entwicklung erlaubt. Trotzdem erscheint eine Modernisierung des Datenschutzes sinnvoll, vor allem um der Entwicklung des Europarechts, den Informationstechnologien, der Globalisierung und der Verbreitung des Informationsaustausches Rechnung zu tragen. In diesem Rahmen sind folgende Massnahmen zu treffen:

- den Katalog der Definitionen aktualisieren, um die technologischen Entwicklungen zu berücksichtigen;
- das Anmeldungssystem zu den grenzüberschreitenden Datenflüssen, das der Realität der internationalen Transaktionen (vor allem per Internet) nicht entspricht, überarbeiten;
- das Register der Datensammlungen, das sich als schwerfällig zu handhabendes Instrument von beschränkter Effizienz herausgestellt hat, überarbeiten;
- die Stellung der betroffenen Person, die sich besonders im privaten Sektor wegen der fehlenden Bearbeitungstransparenz und wegen der unzureichenden Verteidigungsmittel in einer heiklen Lage befindet, stärken;
- die Befugnisse des Eidgenössischen Datenschutzbeauftragten ausbauen;
- die Unterschiede im Schutzniveau zwischen öffentlichem und privatem Sektor einebnen. Die Differenzen rechtfertigen sich nicht mehr, nachdem seit einigen Jahren eine Privatisierungspolitik betrieben wird. Die Voraus-

setzungen für das Bearbeiten von schützenswerten Daten und von Persönlichkeitsprofilen im Privatsektor müssen verschärft werden;
- die Verbindung zum Entwurf des Bundesgesetzes über die Transparenz der Verwaltung prüfen und die Zweckmässigkeit einer Zusammenfassung beider Gesetze untersuchen (siehe 7. Tätigkeitsbericht 1999/2000, S. 73 ff.).

Die Gesetzesänderung sollte ausserdem in den Kantonen, die bereits über ein Datenschutzgesetz verfügen, einen Revisionsprozess auslösen und die übrigen Kantone zur Verabschiedung eines solchen Gesetzes veranlassen. Es gilt, die Harmonisierung zwischen Bundes- und Kantonsrecht sicherzustellen und gegebenenfalls die Kompetenzverteilung zwischen Bund und Kantonen zu prüfen, vor allem wenn die Kantone in Anwendung des Bundesrechtes Daten bearbeiten.

Die gegenwärtige Revision dürfte sich daher nicht auf die Umsetzung der beiden Motionen beschränken. Allerdings darf die Modernisierung des Datenschutzes weder in einer Totalrevision des DSG münden noch die grundlegenden Prinzipien des Datenschutzes, die sich aus dem Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108) ergeben, in Frage stellen. Auch die Gliederung des Gesetzes ist beizubehalten. Die Modernisierung des Datenschutzes verfolgt die folgenden Ziele:

- *Stärkung der Position und der Verantwortung der Einzelperson in bezug auf die Bearbeitung ihrer Personendaten*. Die Garantie des Selbstbestimmungsrechts des Einzelnen im Informationsbereich setzt voraus, dass der Einzelne auch in der Lage ist, aktiv zur Entwicklung der Informationsgesellschaft beizutragen und Verantwortung für ihn betreffende Datenbearbeitungen zu übernehmen. Bevor die Daten beschafft oder bekanntgegeben werden, muss er vorher darüber informiert worden sein. Er darf nicht gezwungen werden, unerwünschte Datenbearbeitungen zu dulden, sondern muss sie ohne grössere Hindernisse verweigern können. Ausserdem muss er über (insbesondere technische) Mittel verfügen, um den Schutz des Privatlebens zu verwirklichen und zu bestimmen, welche Personendaten über ihn von wem bearbeitet werden dürfen. Dazu muss das Gesetz den Einsatz von Mechanismen zur Verschlüsselung, zur anonymen Bekanntgabe und zur pseudonymen Verwendung fördern.

- *Mehr Verantwortung der Personen und Stellen, die Personendaten bearbeiten oder bearbeiten lassen.* Die für die Bearbeitung verantwortlichen Personen haben eine bessere Transparenz ihrer Bearbeitungen sicherzustellen. Sie sind verpflichtet, die betroffenen Personen bei der Beschaffung der Daten zu unterrichten. Anders als in der Motion der Kommission für Rechtsfragen des Ständerates vorgesehen, darf sich die Informationspflicht nicht

auf schützenswerte Daten oder Persönlichkeitsprofile beschränken, sondern muss jede Datenbearbeitung unabhängig von der Datenart erfassen. Wie wir feststellten, werden nicht schützenswerte Daten häufig ohne die Kenntnis der betroffenen Personen bearbeitet. Damit werden die Persönlichkeitsrechte beeinträchtigt – mit möglicherweise gravierenden Folgen für die Person, die ihre Rechte nicht geltend machen kann. Das gilt insbesondere für den Finanzsektor. Die Bearbeitungsverantwortlichen müssen ausserdem die Daten transparenter bearbeiten und gründlicher dokumentieren. Das Gesetz sollte deshalb regelmässige Audits zum Datenschutz verlangen und die Schaffung von Datenschutz-Labels fördern. Ausserdem sollte es für Berufsstandesorganisationen und Dachverbände die Möglichkeit vorsehen, Verhaltenskodizes im Datenschutz, welche die Gesetzesanforderungen konkretisieren und ergänzen, zu entwickeln.

- *Anreiz für den Einsatz von Technologien, welche die Achtung des Privatlebens ermöglichen.* Ziel ist, die Datenschutzauflagen bereits bei der Gestaltung und Entwicklung von Personendaten-Bearbeitungssystemen (Hard- und Software) zu berücksichtigen. Die Systeme sind nach dem Grundsatz der Datensparsamkeit zu gestalten. Zudem soll das Gesetz Anonymisierungs- und Pseudonymisierungstechniken erlauben und fördern, sofern dies möglich und zur Gefahr einer Verletzung der Privatsphäre nicht unverhältnismässig ist.

- *Harmonisierung der schweizerischen Gesetzgebung mit dem europäischen Recht*, sofern sich damit vermeiden lässt, dass die Verantwortlichen der Datenbearbeitung, die auch in der Europäischen Union tätig sind, mit unterschiedlichen Datenschutzanforderungen konfrontiert werden.

- *Verwirklichung des Zusatzprotokolls zum Übereinkommen 108*, welches die Verpflichtung der Parteien vorsieht, eine oder mehrere unabhängige Kontrollbehörden einzusetzen. Das Protokoll regelt ausserdem grenzüberschreitende Datenübermittlungen an Empfänger in Staaten, welche die Konvention nicht ratifiziert haben (siehe 7. Tätigkeitsbericht 1999/2000, S. 89, und nachstehend S. 88).

- *Reduzierung der bürokratischen Auflagen des Gesetzes* durch den Verzicht auf die Anmeldepflicht, sofern sie für den Datenschutz keinen Mehrwert bringt. So könnte die Anmeldungspflicht für grenzüberschreitende Datenflüsse aufgehoben werden. Das Register der Datensammlungen, das für die Bearbeitungstransparenz eine Rolle spielen muss, muss geändert werden. Ausserdem wäre es denkbar, die Bearbeitungsverantwortlichen zu verpflichten, eine Liste der Bearbeitungen zu führen und diese allgemein zugänglich zu machen. Das vom EDSB geführte Register der Datensammlungen könnte sich dabei auf Bearbeitungen von schützenswerten Daten und

Persönlichkeitsprofilen oder solche, die eine regelmässige Datenbekanntgabe beinhalten, beschränken.

- *Verstärkte Kontrolle des Datenschutzes*. Das Gesetz sollte Datenschutzberater der Bundesorgane und der Privatpersonen, die für Bearbeitungen verantwortlich sind, institutionalisieren und ihnen Kontrollaufgaben übertragen.

- *Festigung der Beratungs- und Vermittlungsbefugnisse des Eidgenössischen Datenschutzbeauftragten.* Die Vermittlung zwischen dem Bearbeitungsverantwortlichen und den betroffenen Personen ermöglicht der Einzelperson, ihre Rechte ohne Rückgriff auf bisweilen aufwendige und kostspielige Zivil- oder Verwaltungsverfahren einzufordern. Vor allem im Privatsektor lassen sich Einzelpersonen ungern auf ein Verfahren ein, in dem sie dem Bearbeitungsverantwortlichen an Verteidigungsmitteln oft unterlegen sind. Der Eidgenössische Datenschutzbeauftragte wird künftig den Schwerpunkt seiner Arbeit auf die Beratungs-, Vermittlungs-, Ausbildungs- und Informationstätigkeiten setzen müssen. Ausserdem soll er in der Lage sein, sich frühzeitig auf technologische Entwicklungen einzustellen und Ratschläge zur datenschutzkonformen Entwicklung von Bearbeitungssystemen zu erteilen. Kontrollen bleiben nichtsdestotrotz unerlässlich und müssen insbesondere in Situationen durchgeführt werden, in denen die Bearbeitung eine grosse Anzahl Personen gravierend zu beeinträchtigen droht. In dieser Hinsicht muss der Datenschutzbeauftragte auf verstärkte Ermittlungskompetenzen zählen können. Wie bei den Zuständigkeiten der Eidgenössischen Finanzkontrolle müsste dem EDSB die Möglichkeit eingeräumt werden, Bearbeitungen durchzuführen und insbesondere Datenbanken zur Überprüfung ihrer Gesetzeskonformität abzufragen. Der Datenschutzbeauftragte soll ausserdem ein Mittel zur Durchsetzung seiner Empfehlungen besitzen. Insbesondere muss er die an die Bundesstellen gerichteten Empfehlungen der Eidgenössischen Datenschutzkommission vorlegen können (siehe 6. Tätigkeitsbericht 1998/1999, S. 134ff, 181).

II. WEITERE THEMEN

1. Auskunftsrecht

1.1. Auskunftspflicht der Bundesorgane

Beim Auskunftsrecht handelt es sich um ein Grundrecht der betroffenen Person und um das Schlüsselelement des Datenschutzes. Es ist die einzige Möglichkeit für die betroffene Person, ihre Rechte geltend zu machen. Ausser im Falle gegenteiliger Gesetzesbestimmungen ist ein Bundesorgan verpflichtet, die im Bundesgesetz über den Datenschutz festgelegten Vorschriften über das Auskunftsrecht einzuhalten. Bei Verweigerung oder Einschränkung dieses Rechtes hat das Bundesorgan seine Entscheidung zu begründen.

In einem Fall ersuchte eine Privatperson bei einem Bundesamt um Auskunft über sämtliche sie betreffende Dokumente. Das betreffende Amt übermittelte dem Gesuchsteller einen Teil der gewünschten Dokumente, machte jedoch in manchen Akten gewisse Stellen unleserlich, ohne dies zu begründen. Daraufhin wandte sich der Gesuchsteller an das zuständige Departement, indem er den Verstoss gegen das Bundesgesetz über Datenschutz (DSG) und insbesondere gegen die Bestimmungen über das Auskunftsrecht geltend machte. Einige Tage später schilderte er seinen Fall dem Eidgenössischen Datenschutzbeauftragten, um zu erfahren, ob die Praxis des Amtes mit dem DSG im Einklang stehe. Bei Einschränkung des Auskunftsrechtes ist der Inhaber der Datensammlung verpflichtet, die betroffene Person innerhalb von 30 Tagen nach Eingang des Antrages darüber schriftlich in Form eines begründeten Entscheids zu unterrichten. Wir haben daher das betreffende Amt aufgefordert, den Fall im Einklang mit dem DSG zu behandeln, jedoch ohne Ergebnis. Darüber hinaus erwiderte das zuständige Departement dem Gesuchsteller, das DSG käme im vorliegenden Fall nicht zur Anwendung, aus dem einfachen Grunde, weil keine Datensammlung existiere. Eine Datensammlung ist jeder Bestand an Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind. Aus der Tatsache, dass dem Gesuchsteller ihn betreffende Dokumente zugestellt wurden, geht das Bestehen einer Datensammlung und demzufolge die Anwendbarkeit des DSG klar hervor. In einem zweiten Versuch haben wir das Departement daran erinnert, dass das DSG einzuhalten ist. Schliesslich wurde dem Antragsteller eine dem geltenden Recht entsprechende Entscheidung zugestellt, gegen die er gegebenenfalls Rechtsmittel einlegen kann.

Das Bundesorgan, das Inhaber der Datensammlung ist, muss dem Gesuchsteller nicht nur alle über ihn in der Datensammlung vorhandene Daten zukommen lassen, sondern ihm ebenfalls den Zweck und gegebenenfalls die Rechtsgrundla-

gen der Bearbeitung, die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger mitteilen. Das Bundesorgan kann die Auskunft nur verweigern oder einschränken, soweit ein formelles Gesetz es vorsieht: Das ist beispielsweise bei den Datenbanken zur Verbrechensbekämpfung der Fall, für die der Gesetzgeber ein indirektes Auskunftsrecht vorgesehen hat, das durch den Datenschutzbeauftragen ausgeübt wird. Der Inhaber der Datensammlung kann ebenfalls die überwiegenden Interessen eines Dritten geltend machen, wenn z.B. das beantragte Dokument Angaben über die Gesundheit einer Drittperson enthält. Die Einschränkung des Auskunftsrechtes kann ebenfalls wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, erforderlich sein. Ein weiterer Grund für die Verweigerung oder Einschränkung des Auskunftsrechtes liegt vor, wenn die Auskunft den Ablauf eines Untersuchungsverfahrens zu beeinträchtigen droht. Wie wir bereits weiter oben erwähnten, ist bei Verweigerung oder Einschränkung des Auskunftsrechtes immer ein begründeter Entscheid vorzulegen. Der Gesuchsteller kann beim Departement Beschwerde einlegen und dessen Verfügung bei der Eidgenössischen Datenschutzkommission anfechten. Deren Entscheid unterliegt der Verwaltungsgerichtsbeschwerde an das Bundesgericht.

1.2. Verweigerung der Einsichtnahme in Prüfungsnotizen

Grundsätzlich fallen Notizen, die für den persönlichen Gebrauch erstellt werden, nicht in den Anwendungsbereich des Datenschutzgesetzes. Dies gilt allerdings nicht immer: Ein Prüfungskandidat hat Anrecht auf Einsichtnahme in Notizen, welche die Prüfungsexperten während den mündlichen Prüfungen erstellt haben.

Ein Kandidat, der die Höhere Fachprüfung für eidgenössisch diplomierte Verkaufsleiterinnen und Verkaufsleiter absolviert hat, möchte nach Erhalt des negativen Prüfungsentscheids die Prüfungsakten einsehen. Dem Kandidaten werden nur die schriftlichen Prüfungsunterlagen zugänglich gemacht. Die Prüfungskommission, ein Bundesorgan im Sinne des Bundesgesetzes über den Datenschutz, verweigert ihm aber die Einsichtnahme in Notizen, welche die Experten im Verlauf der mündlichen Prüfungen erstellt haben. Die Prüfungskommission stützt sich dabei auf ein Merkblatt des Bundesamtes für Berufsbildung und Technologie. Darin wird das Recht auf Einsichtnahme in persönliche Expertennotizen sogar ausdrücklich ausgeschlossen.

Das Bundesgesetz über den Datenschutz findet grundsätzlich keine Anwendung auf Personendaten, die von einer natürlichen Person ausschliesslich zum persönlichen Gebrauch bearbeitet und nicht an Aussenstehende bekannt gegeben werden. Dieser Grundsatz gilt sowohl für Notizen für den Privatbereich wie

auch für Notizen, die in Ausübung des Berufes angefertigt werden und dabei lediglich als Gedankenstütze oder Arbeitshilfe gedacht sind. Etwas anderes gilt aber für Notizen, die Experten im Verlauf von mündlichen Prüfungen erstellt haben.

Diese Expertennotizen dienen nur in ganz seltenen Fällen einzig und alleine dem persönlichen Gebrauch. So liegt spätestens dann kein persönlicher Gebrauch mehr vor, wenn der Experte seine Notizen anlässlich einer Notenkonferenz öffentlich kund tut oder seine Prüfungsnotizen pflichtgemäss in ein Kandidatendossier ablegt, das von einem Dritten eingesehen werden kann. Ausserdem sind diese Notizen für die spätere Notengebung mitentscheidend und damit mehr als eine blosse Gedankenstütze des Experten. Prüfungsnotizen eines Experten fallen daher klar in den Anwendungsbereich des Datenschutzgesetzes.

Auch die Bezeichnung der Expertennotizen als interne Akten hilft der Prüfungskommission nicht weiter. Als intern werden jene Akten bezeichnet, die lediglich der verwaltungsinternen Meinungsbildung dienen und daher nicht vor der Öffentlichkeit ausgebreitet werden sollen. Das datenschutzrechtliche Auskunftsrecht umfasst - im Gegensatz zum rein verfahrensrechtlichen Akteneinsichtsrecht - auch die internen Akten.

Der Kandidat kann mit dem datenschutzrechtlichen Auskunftsrecht verlangen, dass ihm alle über ihn in der Prüfungsakte vorhandenen Daten mitgeteilt werden, also auch die Expertennotizen. Die Ausnahmen zum Auskunftsrecht werden im Datenschutzgesetz abschliessend aufgeführt. So kann der Inhaber der Datensammlung die Auskunft nur verweigern, einschränken oder aufschieben, wenn ein formelles Gesetz dies vorsieht oder überwiegende Interessen eines Dritten dies erfordern. Ein Bundesorgan wie die vorliegende Prüfungskommission kann die Auskunft zudem verweigern, einschränken oder aufschieben, wenn dies wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, erforderlich ist oder wenn die Auskunft den Zweck einer Strafuntersuchung oder eines anderen Untersuchungsverfahrens in Frage stellt.

Wir sind somit der Ansicht, dass einem Prüfungskandidaten die Einsicht in alle ihn betreffenden Prüfungsunterlagen, auch in die Expertennotizen, gestattet werden muss.

2. Kundenkarte

2.1. Kundenkarten: M-Cumulus

Die Migros darf die Identität des Inhabers einer M-Cumulus-Karte, der im Verdacht steht, gegen das Gemeindereglement zur Abfallentsorgung verstossen zu haben, der Gemeinde nicht bekanntgeben.

In unserem 7. Tätigkeitsbericht 1999/2000, S. 65 wurde die Frage behandelt, ob die Migros einem Untersuchungsrichter Name und Adresse des Inhabers einer M-Cumulus-Karte bekanntgeben darf oder nicht. Die Kassenquittung mit aufgedruckter M-Cumulus-Nummer war in einem Abfallsack aufgefunden worden. Die Frage wurde unter dem Gesichtspunkt des Zeugnisverweigerungsrechtes geprüft. Da die Migros nicht zu den privaten Personen zählt, die von der Pflicht, vor Gericht auszusagen, befreit werden können, wurde die Bekanntgabe als zulässig erklärt. Dem Untersuchungsrichter, der um die Bekanntgabe ersucht hatte, wurde im Rahmen eines hängigen Strafverfahrens die Identität des Karteninhabers mitgeteilt.

Im Jahr 2000 haben wir folgenden Fall behandelt: Die Migros fragte nach, ob sie einem Auskunftsgesuch, diesmal von einer Gemeinde, nachkommen dürfe oder nicht. Die Gemeinde handelte in ihrer Eigenschaft als Ausführungsorgan eines kommunalen Verwaltungsreglements zur Abfallbewirtschaftung.

Wir verneinten diese Frage. Die Erteilung derartiger Auskünfte im Rahmen eines erstinstanzlichen Verwaltungsverfahrens wird durch das Bundesgesetz über den Datenschutz geregelt. Eine solche Bekanntgabe verstösst gegen das Zweckbindungsgebot, auf dessen Grundlage die Personendaten der M-Cumulus-Karten gesammelt werden. Es darf daran erinnert werden, dass sich die Migros verpflichtet, die Daten nur innerhalb der Migros-Genossenschaft zu Marketing- oder Statistikzwecken zu bearbeiten und nicht an aussenstehende Dritte weiterzugeben.

3. Videoüberwachung

3.1. Videoüberwachung im Privatbereich - datenschutzrechtliche Mindestanforderungen

Private Personen dürfen Videoüberwachungssysteme nur einsetzen, wenn die datenschutzrechtlichen Grundprinzipien erfüllt sind. Angesichts der vielen Anfragen hat der EDSB zu diesem Thema ein Merkblatt herausgeben.

Im privaten Bereich werden immer häufiger Videoüberwachungssysteme aufgestellt, um Personen zu schützen und Sachbeschädigungen zu verhindern. Dementsprechend gelangten zu diesem Thema verschiedene Anfragen an uns. Wir haben deshalb ein Merkblatt ausgearbeitet (siehe S. 113), das die allgemeinen Voraussetzungen für den Einsatz von Videoüberwachungssystemen wiedergibt. Die Videoüberwachung am Arbeitsplatz wird darin jedoch nicht behandelt.

Die Benutzung von Videokameras durch private Personen zwecks Überwachung untersteht dem Bundesgesetz über den Datenschutz, sofern sich die gefilmten Bilder auf eine oder mehrere bestimmte oder bestimmbare Personen beziehen, unabhängig davon, ob die Bilder aufbewahrt werden oder nicht. Die vorgenommenen Bearbeitungen (Erfassen, Bekanntgabe, unmittelbares oder nachträgliches Anschauen, Aufbewahrung der Bilder, usw.) müssen im Einklang mit den allgemeinen Grundsätzen des Datenschutzes stehen.

Ein Videoüberwachungssystem darf nur eingesetzt werden, wenn die zwei folgenden Bedingungen erfüllt sind:

- Die Videoüberwachung darf nur eingesetzt werden, wenn dieser Eingriff in die Persönlichkeit durch die Zustimmung der betroffenen Personen, durch ein überwiegendes öffentliches oder privates Interesse oder durch Gesetz gerechtfertigt ist. So kann zum Beispiel ein Bijouteriebesitzer ein überwiegendes Interesse daran haben, dass während seiner Abwesenheit kein Einbruchdiebstahl erfolgt (Rechtmässigkeitsprinzip).
- Die Videoüberwachung muss ein geeignetes und nötiges Mittel sein, um den verfolgten Zweck, d.h. die Sicherheit, insbesondere den Schutz von Personen und/oder Sachen, zu erreichen. Sie darf nur angewendet werden, wenn sich andere Massnahmen, die das Privatleben weniger beeinträchtigen, wie zusätzliche Verriegelungen, Verstärkung der Eingangstüren, Alarmsysteme, als ungenügend oder undurchführbar erweisen. So wird beispielsweise der Einsatz von Videokameras in einer Einstellhalle zur Verhinderung von Vandalismus in der Regel zulässig sein (Verhältnismässigkeitsprinzip).

Bei der Installation und dem Gebrauch eines Videoüberwachungssystems müssen die folgenden Regeln respektiert werden:

- Die für das Videoüberwachungssystem verantwortliche Person muss die Personen, die das Aufnahmefeld der Überwachungskameras betreten, mittels einem sichtbaren Hinweisschild über ein solches System informieren. Sind die aufgenommenen Bilder mit einer Datensammlung verbunden, muss auf diesen Schildern angegeben sein, bei wem das Auskunftsrecht geltend gemacht werden kann, falls sich dies nicht aus den Umständen ergibt. Zum Beispiel muss bei einer Videokamera beim Eingang zu einem Mehrfamili-

enhaus das Hinweisschild für jede eintretende Person gut ersichtlich sein (Prinzip von Treu und Glauben sowie Auskunftsrecht).

- Die für das Videoüberwachungssystem verantwortliche Person muss die Personendaten durch angemessene technische und organisatorische Massnahmen vor jeglichem unbefugten Bearbeiten schützen (z. B. unberechtigten Personen den Zugang zu den Daten verbieten). So muss etwa sichergestellt sein, dass nur berechtigte Personen Zugang zu den Bildschirmen der Videokameras haben. Desgleichen müssen die gespeicherten Daten an einem sicheren Ort, z. B. in einem verriegelten Raum, aufbewahrt werden, wobei nur berechtigte Personen Zugriff zum Schlüssel haben dürfen (Datensicherheit).
- Die Videokamera muss zudem so aufgestellt werden, dass nur die für den verfolgten Zweck absolut notwendigen Bilder in ihrem Aufnahmefeld erscheinen. Beispielsweise darf in einem Mehrfamilienhaus über das Aufnahmefeld der Kamera in der Regel nicht ersichtlich sein, welche Personen in welche Wohnung ein- und ausgehen. (Verhältnismässigkeitsprinzip).
- Die Daten dürfen nur für den Schutz von Personen und Sachen benutzt werden. Sie dürfen nicht für andere Zwecke verwendet werden. So dürfen zum Beispiel Aufnahmen durch eine für die Sicherheit aufgestellte Videokamera nicht für Marketingzwecke verwendet werden (Zweckbindungsprinzip).
- Die mit einer Kamera aufgenommenen Personendaten dürfen nicht bekannt gegeben werden, ausser in den durch das Gesetz vorgesehenen oder erlaubten Fällen, z. B. eine von einem Richter stammende Anfrage. Die aufgenommenen Bilder dürfen auch nicht für Marketingzwecke an Dritte weitergegeben werden (Zweckbindungsprinzip).
- Die mit einer Kamera aufgenommenen Bilder müssen innert möglichst kürzester Zeit gelöscht werden. Sachbeschädigungen oder Personenverletzungen werden in der Regel innerhalb von Stunden seit deren Begehung festgestellt. Eine Aufbewahrungsfrist von 24 Stunden ist somit - angesichts des verfolgten Zwecks - genügend, sofern innerhalb dieses Zeitraums keine Sachbeschädigungen oder Personenverletzungen entdeckt werden. Bei der Videoüberwachung in privaten Räumen, die nicht öffentlich zugänglich sind, kann diese Frist in gewissen Fällen länger sein. So kann beispielsweise eine längere Aufbewahrung aufgrund einer Ferienabwesenheit gerechtfertigt sein. Doch auch hier sind die Aufnahmen nach der Rückkehr so schnell als möglich zu vernichten, wenn keine Sachbeschädigung festgestellt wurde (Verhältnismässigkeitsprinzip).

Informationen zur Videoüberwachung finden Sie auch in S. 86.

3.2. Videoüberwachung im öffentlichen Verkehr - datenschutzrechtliche Mindestanforderungen

Im öffentlichen Verkehr wird vermehrt zur Videokamera gegriffen, um den Vandalismus zu bekämpfen und das Sicherheitsgefühl zu erhöhen. Findet eine Videoüberwachung statt, muss diese für die Passagiere erkennbar sein. Zudem sind die aufgenommenen Bilder in der Regel nach Ablauf von 24 Stunden zu löschen. Handelt es sich beim Transportunternehmen um ein Bundesorgan, braucht es für die Videoüberwachung zudem eine gesetzliche Grundlage.

Im öffentlichen Verkehr zeichnet sich die Tendenz ab, zur Bekämpfung des Vandalismus und zur Wahrung der Sicherheit von Personen Videoüberwachungssysteme einzusetzen. Diesbezüglich unterbreiteten uns die Schweizerischen Bundesbahnen ihr Vorhaben, unbegleitete Nahverkehrszüge mit Videoüberwachungsanlagen zu versehen.

Bei privatrechtlichen Verkehrsbetrieben gelten grundsätzlich die gleichen Voraussetzungen wie bei der Videoüberwachung im Privatbereich (vgl. Ausführungen auf S. 64 über Videoüberwachung im Privatbereich). Erfolgt die Videoüberwachung durch ein Transportunternehmen, das datenschutzrechtlich als Bundesorgan gilt, braucht es zudem eine gesetzliche Grundlage.

Die Videoüberwachung im öffentlichen Verkehr darf grundsätzlich nur für die Erhöhung der Sicherheit von Personen sowie zur Bekämpfung des Vandalismus vorgenommen werden. Zudem muss die Videoüberwachung im öffentlichen Verkehr nötig und geeignet sein, den verfolgten Zweck zu erreichen. Sie ist unzulässig, wenn der Zweck durch eine mildere Massnahme erreicht werden kann. Im Übrigen müssen die betroffenen Personen auf die Videoüberwachung mittels sichtbaren Hinweisschildern – z. B. bei der Tür – orientiert werden. Sind die aufgenommenen Bilder mit einer Datensammlung verbunden, muss auf diesen Schildern angegeben sein, bei wem das Auskunftsrecht geltend gemacht werden kann, falls sich dies nicht aus den Umständen ergibt. Angemessene technische und organisatorische Massnahmen müssen getroffen werden, um die abgespeicherten Daten vor dem Zugriff von unbefugten Dritten zu schützen. Die Videokamera muss zudem so aufgestellt werden, dass nur die für den verfolgten Zweck absolut notwendigen Bilder in ihrem Aufnahmefeld erscheinen. Die Aufnahmen dürfen nur für den verfolgten Zweck verwendet werden. Ferner sind die Aufnahmen, die sich nicht auf einen Vorfall beziehen, spätestens nach 24 Stunden zu vernichten.

Sind alle diese Voraussetzungen erfüllt, ist der Einsatz von Videoüberwachungssystemen datenschutzrechtlich zulässig.

4. Veröffentlichung von Personendaten

4.1. Publikation der nachrichtenlosen Konten

Wir hatten in den vergangenen Jahren mehrmals Gelegenheit, unsere Position im Zusammenhang mit den nachrichtenlosen Vermögenswerten/2. Weltkrieg darzulegen (siehe auch 5. Tätigkeitsbericht 1997/1998, S. 76 und 6. Tätigkeitsbericht 1998/1999, S. 124). Wir äusserten uns im laufenden Jahr eingehend über die Zugriffsmodalitäten auf eine im Internet publizierte Liste, die Angaben zu rund 26'000 Konten enthält.

Die Eidgenössische Bankenkommission hat aufgrund von Empfehlungen des «Independent Committee of Eminent Persons» entschieden, dass schweizerische Banken die im Zusammenhang mit Holocaust-Opfern bestehenden offenen nachrichtenlosen sowie bestimmte geschlossene Konten publizieren müssen. Die Schweizerische Bankiervereinigung beabsichtigte eine Veröffentlichung der rund 26'000 Konten im Internet. Dabei sollten jeweils Name, Vorname und Wohnsitzland des Kontoinhabers sowie ein Hinweis über den Zustand des Kontos und allenfalls dessen Betragshöhe publiziert werden. Die Schweizerische Bankiervereinigung wollte vom EDSB wissen, welche datenschutzrechtlichen Erfordernisse dabei zu beachten seien. Die mit der Durchführung beauftragten amerikanischen Stellen verlangten, dass die gesamte Liste mit allen 26'000 Konten im Internet veröffentlicht wird und dass die Liste vollständig kopiert werden kann, um den Betroffenen einen möglichst einfachen und offenen Zugang zu ermöglichen.

Auch bei einer Publikation im Internet gelten die allgemeinen Grundsätze der schweizerischen Datenschutzgesetzgebung. Die Veröffentlichung der Liste mit allen 26'000 nachrichtenlosen Konten verstösst gegen den im Datenschutz äusserst wichtigen Grundsatz der Verhältnismässigkeit. Eine Abfrage im Internet sollte demnach nur einzelfallweise auf Namen und Vornamen hin erfolgen. In Bezug auf die praktischen Probleme und Risiken von verschiedenen Namensschreibweisen haben wir angeregt, die Suchkriterien hinsichtlich Orthographie und Phonologie von Namen und Vornamen zu verbessern. Ausserdem schlugen wir vor, dass für bestimmte Organisationen ein erweiterter Zugriff (mit Passwortschutz) geschaffen werde. Personen, die über keinen Internetzugang verfügen oder Schwierigkeiten haben, Internet zu benützen, können sich bei der Suche an diese Organisationen wenden. Zudem kann die vollständige Liste in Papierform an diese Organisationen abgegeben werden, um die geforderte volle Einsichtnahme in die gesamte Liste zu ermöglichen.

Die Schweizerische Bankiervereinigung hat die Bearbeitung und Publikation der Daten einer Treuhandgesellschaft übertragen. Wir haben die Schweizerische

Bankiervereinigung darauf hingewiesen, dass sie als Inhaberin der Datensammlung weiterhin die Verantwortung dafür trägt, dass bei der Datenbearbeitung und -publikation die schweizerische Datenschutzgesetzgebung eingehalten wird.

5. Bekanntgabe von Personendaten

5.1. Online-Verzeichnisse von Bundesangestellten (Admin Directory Public)

Im Internet-Zeitalter bekommt der herkömmliche «Eidg. Staatskalender» in Buchform ein elektronisches Pendant. Im Sinne einer transparenten und bürgerfreundlichen Verwaltung sollen Informationen über die Bundesbehörden und ihre Mitarbeiter einfacher und rascher online zugänglich gemacht werden. Dabei sind jedoch die Datenschutzbestimmungen zum Schutz der Betroffenen einzuhalten.

Bei der Publikation von Personendaten im bundesinternen Intranet oder im weltweiten Internet handelt es sich um eine Bekanntgabe im Abrufverfahren, für die ein Bundesorgan nach Datenschutzgesetz eine gesetzliche Grundlage benötigt. Eine Grundlage für die Herausgabe von Verzeichnissen zur Erleichterung der Kommunikation unter den Mitarbeitern der Bundesverwaltung ist in der Organisationsverordnung der Bundeskanzlei enthalten. Insbesondere für die elektronische Publikation von Verzeichnissen können folgende Daten aller Angestellten *bundesintern* zugänglich gemacht werden: Name, Vorname, Funktion, Titel, Anrede, Amtssprache, Telefon-, Fax- und Pagernummer, Post- und E-Mail-Adresse, verwendete Kommunikationsprotokolle und Teile von Verschlüsselungsinformationen. Solche Online-Verzeichnisse existieren bereits seit einigen Jahren im Bundes-Intranet.

Für die vorgesehenen *verwaltungsexternen* elektronischen Verzeichnisse (z.B. Projekt: «Admin Directory Public» des Bundesamtes für Informatik und Telekommunikation) muss der Zugang auf die obengenannten Personendaten derjenigen Mitarbeiter beschränkt bleiben, die als «Ansprechpartner gegenüber Dritten gelten». Diese Einschränkung ist in der Organisationsverordnung der Bundeskanzlei festgeschrieben. Sie folgt den Datenschutzprinzipien der Zweckbindung und der Verhältnismässigkeit.

Wesentlich ist, dass die Dienststellen des Bundes über die Risiken einer Internetpublikation (Abrufbarkeit auch in Ländern mit geringen oder gar keinen Datenschutzbestimmungen, einfache Verknüpfbarkeit mit weiteren Daten-

beständen, fehlende Datensicherheit) informiert werden. Bundesweit sind einheitliche Kriterien bei der Beurteilung, ob eine Person als Ansprechpartnerin gegenüber Dritten anzusehen ist, anzuwenden.

Die bisherigen Kontakte mit den entsprechenden Stellen der Bundeskanzlei und des Bundesamtes für Informatik und Telekommunikation stimmen uns zuversichtlich, dass in dieser Sache eine Lösung gefunden wird, die einerseits die Interessen der Kommunikationspartner des Bundes und andererseits den Datenschutz der Mitarbeiter des Bundes optimal abdeckt.

6. Datenschutz und rechtliche Rahmenbedingungen

6.1. E-Government und Mindestanforderungen für den Schutz der Privatsphäre

Die Cyber-Administration wird für den Bürger bald Realität sein. Unter dem Begriff E-Government sind umfassende Projekte wie Guichet virtuel und E-Voting im Entstehen. Mit dieser ausserordentlichen technologischen Herausforderung stellt sich aber auch verschärft die Frage nach dem Schutz der Privatsphäre. Zwar besteht der Hauptzweck des virtuellen Amtsschalters in der Information des Bürgers, doch werden Kommunikation und Transaktionen vor allem bei der elektronischen Stimmabgabe zunehmen. Für den Erfolg des E-Government wird das Vertrauen des Bürgers in die Cyber-Administration ausschlaggebend sein. Daher müssen diese ambitiösen Projekte hinsichtlich der Wahrung von Datenschutz und -sicherheit mit gutem Beispiel vorangehen. Ausserdem sollten sie innovative Technologien fördern, die einen immer besseren Schutz der Privatsphäre gewährleisten.

Die Bundeskanzlei leitet im Bereich des E-Government zwei Schlüsselprojekte, nämlich die Schaffung eines Guichet virtuel (virtueller Amtsschalter) und die Einführung des E-Voting, d.h. der elektronischen Stimmabgabe. Die im Juni 2000 eingesetzte Arbeitsgruppe Guichet virtuel wurde mit der Beurteilung von Projekten virtueller Amtsschalter in der Schweiz und im Ausland beauftragt. Darüber hinaus wurde im Dezember 2000 die Vereinbarung über die Zusammenarbeit von Bund und Kantonen bezüglich Aufbau eines Guichet virtuel unterzeichnet.

Der Erfolg des anschliessenden Projektes E-Voting wird grösstenteils von der Qualität und Funktionstüchtigkeit des virtuellen Amtschalters abhängen. Daher

sind bereits jetzt die bestmöglichen Voraussetzungen für den Datenschutz zu schaffen.

Ziel des virtuellen Amtsschalters ist die Entwicklung und Umsetzung einer Internetplattform, die einen einfachen und empirischen Zugang zu den Dienstleistungen der Verwaltungsbehörden von Bund, Kantonen und Gemeinden bietet sowie Links zu den Informationen von Kantonen und Gemeinden herstellt. Der Zugang erfolgt themenbezogen (Auto, Steuern, Geburt, Heirat, Scheidung, Ruhestand usw.). Nach einer kurzen Einführung wird der Benutzer direkt zu den Internet-Seiten der jeweils zuständigen Dienststellen des Bundes, der Kantone oder der Gemeinden geleitet.

Die Projektentwickler sollten unbedingt baldmöglichst eine Datenschutzpolitik festlegen und folgende Fragen klären:
- Sollen Datenschutzaufträge dem öffentlichen oder dem privaten Sektor erteilt werden?
- Welche bestehenden Technologien sollen vorrangig eingesetzt werden?
- In welchen Sektoren sind Investitionen zu planen?
- Wo sollen sich die Schnittstellen des Systems befinden?
- Soll zur Entwicklung des Datenschutzkonzeptes ein zentralisierter oder dezentralisierter, schweizerischer oder internationaler Ansatz gewählt werden (Anzahl und geographische Konfiguration der verschiedenen Elemente des Schutzsystems wie Firewalls, Kontroll- und Zertifizierungsbehörden, Funktionen der Verwalter)?

Der rechtliche Rahmen für den virtuellen Amtsschalter ist sorgfältig auszuarbeiten (Gesetze, Verordnungen, Richtlinien, Vereinbarungen und Verträge). Zur Schaffung des geeigneten Rahmens ist sowohl die bestehende Datenschutzgesetzgebung als auch der innovative Charakter des Projektes zu berücksichtigen (dazu gehören ebenfalls neue juristische Begriffe wie z.B. elektronische Zertifizierung und digitale Signatur). Als wichtigste Partner des Projektes werden Kantone und Gemeinden ausserdem durch die Weiterentwicklung der Internet-Technologie unausweichlich mit dem Zentralisierungseffekt konfrontiert. Die Schwierigkeit dieses Unterfangens ist nicht zu unterschätzen. Nur mit einem klaren rechtlichen Rahmen lässt sich die eventuelle Umverteilung von Zuständigkeiten früh genug in Angriff nehmen. Diese Fragen sollten unserer Auffassung nach in einem formellen Gesetz geregelt werden.

Die wichtigsten technischen Optionen müssen in einem Bearbeitungsreglement festgehalten werden. Dies wird von der Verordnung zum Bundesgesetz über den Datenschutz verlangt und legt die Planung und die wichtigsten technischen und organisatorischen Aspekte fest. Das Reglement ist zu Beginn des Projektes auszuarbeiten und anschliessend regelmässig zu aktualisieren. HERMES, das

vom Bundesamt für Informatik und Telekommunikation (BIT) entwickelte Verwaltungsinstrument für elektronische Projekte des Bundes bietet eine nützliche Grundlage für ein solches Bearbeitungsreglement.

Angesichts der Tragweite des Prozesses wäre ein Ausbildungsmodul mit Schwerpunkt Datenschutz angebracht, das sämtliche Beteiligten an dem Projekt zu jedem Zeitpunkt und zu jedem Entwicklungsstadium für diese Fragen sensibilisiert.

Der virtuelle Amtsschalter dient sowohl zur «Information» (an wen wendet man sich und wann, um sich über diverse Alltagsfragen zu erkundigen usw.) als auch zur «Kommunikation» bzw. «Transaktion» (Austausch von Verwaltungsformularen, Zahlungen, Ausstellung diverser Bescheinigungen usw.). Im ersten Fall gilt es vor allem, Fragen zur Verfolgbarkeit zu klären (Personalisierung mittels IP-Nummer, Cookies, Erstellung von Profilen, Aufbewahrung der Daten, usw.). Im zweiten Fall stellen sich neben der Verfolgbarkeit auch Fragen zur Vertraulichkeit, Integrität und Authentifizierung der Vorgänge.

Bei der Einführung von E-Government ist vor allem folgenden allgemeinen Datenschutzgrundsätzen Rechnung zu tragen:

- Verhältnismässigkeit und Zweckbindung: Der Zugang zur Information darf nicht dazu führen, dass mehr Personendaten beschafft oder bearbeitet werden, als zur Beantwortung der Benutzerfragen notwendig sind oder als der Benutzer von Gesetzes wegen bekanntgeben muss (Steuererklärung, Subventionsanträge usw.);
- Konzentration und Zentralisierung der Daten: Die Datenmenge darf nicht unter dem Vorwand der Rationalisierung oder der Harmonisierung ansteigen. Besondere Aufmerksamkeit ist dabei den Risiken bei Datenflüssen zwischen Bund, Kantonen und Gemeinden oder innerhalb einer Verwaltung zu schenken;
- Transparenz: Bei jeder Aufforderung, Personendaten bekanntzugeben, muss der Benutzer frei und bewusst entscheiden können, ob er die gewünschten Daten liefert. Bei jedem Vorgang muss er folgende Informationen erhalten: Zweck, Empfänger, fakultative und notwendige Angaben (unterschiedlich zu kennzeichnen), Inhaber der Datensammlungen und Dauer der Datenaufbewahrung;
- Auskunftsrecht: Der Benutzer muss zu jedem Zeitpunkt die ihn betreffenden Daten überprüfen und ihre Löschung oder Berichtigung verlangen können;
- Anonymer Zugang: Der Benutzer muss auf Wunsch die Verfolgbarkeit (z.B. mittels IP-Nummer oder Cookies) seiner Erkundigungen ausschliessen können. Die Verwendung von Pseudonymen oder von datenschutzfreundlichen Technologien (PET) muss wo immer möglich gefördert werden;

- Bekanntgabe der Daten: Die Bekanntgabe von Personendaten muss immer rechtmässig sein;
- bei Kommunikation und Transaktion müssen Vertraulichkeit, Integrität und Authentifizierung der Daten durch den Einsatz modernster Technologien zur Verschlüsselung, Zertifizierung und digitalen Signatur gewährleistet werden.

6.2. Bekämpfung der Schwarzarbeit

Die Vernetzung (Online-Zugang zu sämtlichen vorhandenen Datensammlungen oder Vergleich von Datensammlungen) von Verwaltungsdaten (Steuer, Sozialversicherungen, Ausländerpolizei und Asylbehörden) muss gemäss den allgemeinen Datenschutzgrundsätzen erfolgen. Durch eine so umfassende Massnahme wie die Vernetzung werden zahlreiche besonders schützenswerte Daten durch Abrufverfahren zugänglich gemacht, was durch ein formelles Gesetz ausdrücklich vorgesehen sein muss.

Der Bundesrat beauftragte eine Arbeitsgruppe, die rechtliche und technische Machbarkeit der Vernetzung von administrativen Daten der Steuer, der Sozialversicherungen (AHV, IV und Arbeitslosenversicherung), der Ausländerpolizei und der Asylbehörden zu untersuchen. Ziel dieser Massnahme ist es, diese Verwaltungsdaten den für die Ermittlung von Fällen der Schwarzarbeit verantwortlichen Überwachungsorganen zugänglich zu machen. Unter Vernetzung versteht man die Möglichkeit, einerseits über ein Abrufverfahren auf die in verschiedenen Datensammlungen enthaltenen Informationen zuzugreifen und andererseits die in allen Registern enthaltenen Daten systematisch zu vergleichen. Im Rahmen dieses Auftrages haben wir erneut daran erinnert, dass jede Bearbeitung von Personendaten im Einklang mit den allgemeinen Grundsätzen des Datenschutzes zu erfolgen hat.

Ob die Bearbeitung von Personendaten dem Verhältnismässigkeitsprinzip entsprach, lässt sich in einem zweistufigen Verfahren überprüfen. Zunächst ist festzustellen, ob die zu bearbeitenden Personendaten notwendig und geeignet sind, das gewünschte Ziel zu erreichen. In diesem Falle geht es um die Bekämpfung der Schwarzarbeit. Wie die Arbeitsgruppe feststellte, sind die verfügbaren Daten aufgrund ihres Inhaltes und zeitlichen Ursprungs kaum zu vergleichen. Darüber hinaus liefern die in den untersuchten Datenbanken enthaltenen Daten keine stichhaltigen Angaben zur Aufdeckung von Schwarzarbeit. Der zweite Schritt besteht in der Abwägung der vorhandenen Interessen, d.h. Ziel der Bearbeitung, insbesondere erwartete Ergebnisse vs. Persönlichkeitsverletzung der betroffenen Personen. Bei einer allgemeinen Vernetzung muss man sich darüber bewusst sein, dass eine Fülle von Personendaten über einen Grossteil der in der Schweiz wohnhaften Bevölkerung bearbeitet würde und die

Datensicherheit damit stärker gefährdet wäre. Die Bearbeitung von besonders schützenswerten Personendaten und von Persönlichkeitsprofilen würde durch mehrere Kantons- und Bundesorgane erfolgen. Diese Daten dürfen nur bearbeitet bzw. durch ein Abrufverfahren zugänglich gemacht werden, wenn ein formelles Gesetz es ausdrücklich vorsieht. In den Rechtsgrundlagen sind der Zweck und der ungefähre Umfang der Bearbeitung, die an der Bearbeitung beteiligten Organe sowie die Kategorien der bearbeiteten Daten festzuhalten. Entsprechende Änderungen werden in der Sozialversicherungs-, Steuer- und Ausländergesetzgebung notwendig sein.

Die Arbeitsgruppe kam zu dem Schluss, dass eine Gesamtvernetzung der bestehenden Datensammlungen die Bekämpfung der Schwarzarbeit nicht wesentlich verbessern würde und dass die geplanten Datenbearbeitungen in keinem Verhältnis zum gesteckten Ziel stehen. Die Arbeitsgruppe schlug daher vor, die Vernetzung auf die Sozialversicherungen zu beschränken (Vergleich der Daten der Arbeitslosenversicherung mit jenen der AHV). In unserer Eigenschaft als Beratungsorgan werden wir die Entwicklung dieses Vorhabens weiter verfolgen und uns zur Anpassung bereits bestehender oder zur Schaffung neuer einschlägiger Gesetzesvorschriften im Rahmen der jeweiligen Vernehmlassungsverfahren äussern.

7. Datenschutz und Datensicherheit

7.1. Chiffrieralgorithmen, die heute als sicher erachtet werden können

Sichere Chiffrierverfahren bzw. Algorithmen sollen veröffentlicht sein, um Transparenz zu gewährleisten. Damit ist auch sicher gestellt, dass Kryptoexperten die veröffentlichten Verfahren testen können. Symmetrische Algorithmen mit einer Schlüssellänge von 128 Bit und asymmetrische mit einer Schlüssellänge von 1024 bzw. 2048 Bit erachtet der Eidg. Datenschutzbeauftragte heute als sicher.

Der Eidg. Datenschutzbeauftragte wird immer wieder angefragt, welche Chiffrieralgorithmen er als sicher erachtet. Grundsätzlich muss dabei festgehalten werden, dass es von Vorteil ist, wenn der Chiffrieralgorithmus veröffentlicht wurde. Dadurch sind andere Chiffrierexperten in der Lage, diese Algorithmen zu testen und auf mögliche Schwachstellen hinzuweisen, und es besteht somit eine möglichst grosse Transparenz. Es existieren sicher auch gute, nicht veröffentlichte Algorithmen. Man muss sich aber dabei die Frage stellen, warum diese Algorithmen nicht veröffentlicht werden und warum man keine Transparenz will. Bei nicht veröffentlichten Algorithmen kann die Gefahr bestehen,

dass gewisse «Hintertüren» eingebaut sind. Dies würde es dann beispielsweise anderen Organen oder Stellen ermöglichen, die chiffrierten Daten zu entschlüsseln. Als sicher bei den symmetrischen Verschlüsselungsverfahren erachtet man heute veröffentlichte Algorithmen mit einer Schlüssellänge von mindestens 90 Bit wie z.B. der IDEA-Algorithmus (International Data Encryption Algorithm), der eine Schlüssellänge von 128 Bit aufweist oder der Triple-DES-Algorithmus (Data Encryption Standard). Bei asymmetrischen Verfahren wie beispielsweise beim RSA-Algorithmus (Rivest, Shamir, Adleman) konnte man den 512 Bit Schlüssel 1999 brechen. Man geht heute davon aus, dass eine Schlüssellänge von 1024 Bit als sicher erachtet werden kann. Wir sind allerdings diesbezüglich immer vorsichtig und empfehlen den Anwendern möglichst lange Schlüssel zu verwenden.

7.2. Sichere Passwörter und andere Authentifizierungsverfahren

Ein Passwort soll eine Länge von mindestens 6 (besser wären 8 oder mehr) Zeichen beinhalten. Diese können mit einfachen Hilfsmitteln kreiert und so aufbewahrt werden, dass das Passwort auch nach längerer Abwesenheit wieder generiert werden kann. Es ist darauf zu achten, dass ein periodischer Wechsel der Passwörter (beispielsweise alle drei Monate) erfolgt. Experten vertreten die Meinung, dass insbesondere im sensitiven Umfeld die Authentifikation durch Wissen (Passwort) zu wenig sicher ist; es sollen zusätzliche Massnahmen wie biometrische Systeme oder Chipkarten eingesetzt werden.

Neben der Benutzeridentifikation (USER-ID) verwendet man heute meistens ein Passwort, um sich beispielsweise bei einem EDV-System anzumelden. Bei der Auswahl des Passworts ist darauf zu achten, dass es mindestens eine Länge von 6-8 Zeichen hat. Heute wird insbesondere in der englischen Sprache auch von Passphrase (Passsatz) gesprochen. Dies weist u.a. darauf hin, dass man aus Sicherheitsgründen nicht nur ein «Wort», sondern eine nichtsaussagende Zeichenkombination gebrauchen sollte, die dann eher einer Länge von beispielsweise 8-12 Zeichen entsprechen würde.

Wichtig bei der Auswahl des Passworts ist es, dass keine Wörter wie Namen, Vornamen, Auto-, Telefonnummern sowie Zeichenkombinationen aufgeführt werden, wie sie etwa in Wörterbüchern aufgeführt sind. Wenn man nun noch die Buchstaben mit Zahlen und Sonderzeichen wie %, & durchmischt, so entsteht ein gutes Passwort. Dieses wird man kaum mit den aus dem Internet frei herunterladbaren «Hackertools» ausfindig machen können.

Eine der wichtigsten Sorgen der Benutzer ist das mögliche Vergessen des Passworts. Durch langzeitigen Nichtgebrauch von Wissen (z. B. bei Ferienabwe-

senheit) kann das am Arbeitsplatz täglich eingesetzte Passwort verloren gehen. Deshalb möchte man das Passwort irgendwo aufschreiben. Man will ja schliesslich nicht diejenige Person sein, die immer wieder den System-Administrator anrufen muss, damit dieser ein neues Passwort kreiert. Grundsätzlich dürfen Passwörter weder an einem frei zugänglichen Ort noch im Klartext festgehalten werden. Es sind die folgenden Lösungen denkbar: Wir schreiben uns einen oder mehrere Sätze auf einen Zettel, die jedoch keinen Bezug zu einem EDV-System haben dürfen. Nun wählen wir einen Satz, der auf dem Zettel festgehalten ist und kreieren daraus unser Passwort. Als Schlüssel halten wir beispielsweise fest (ohne diesen aber auf dem Zettel zu notieren), dass wir die beiden letzten Buchstaben der jeweiligen Worte des Satzes als Passwort verwenden wollen. Dieses ergänzen wir dann noch durch Sonderzeichen und halten zwei Buchstaben in grosser Schrift fest.

Beispiel:
(festgehaltener Satz) ⇒ Geste**rn** war**s** lust**ig** drauss**en** ⇒ Passwort = **rnrsigen**
Dieses ergänzen wir noch durch Sonderzeichen **£rnrsigen$**
und halten die beiden mittleren Buchstaben in Grossschrift fest **£rnrSIgen$**

Eine andere Möglichkeit besteht darin, dass man eine Karte mit beliebigen Zeichen kreiert, aufgrund derer man auch ein Passwort mit Hilfe eines Schlüssels bzw. von Auswahlkriterien erstellt.
Bsp.:

	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*0*
1	*a*	*b*	*h*	*i*	*Z*	*£*	*?*	*P*	*k*	*ö*
2	*C*	*&*	*%*	*I*	*7*	*h*	*F*	*f*	*ä*	*j*
3	*)*	*Q*	*B*	*%*	*n*	*L*	*&*	*8*	*L*	*D*
4	*1*	*4*	*D*	*g*	*g*	*L*	*9*	*3*	*N*	*m*
5	*&*	*#*	*#*	*K*	*K*	*l*	*o*	*g*	*$*	*!*
6	*Z*	*+*	*I*	*9*	*0*	*&*	*L*	*b*	***	*7*
7	*W*	*6*	*!*	*F*	*h*	*B*	*7*	*3*	*v*	*V*
8	*G*	*G*	*K*	*?*	*m*	*k*	*$*	*@*	*A*	*m*
9	*z*	*8*	*h*	*M*	*)*	*ç*	*x*	*K*	*9*	*0*
0	*(*	*¢*	*v*	*7*	*2*	*l*	*K*	*ä*	*m*	*q*

Man merkt sich beispielsweise die Zahl 45 und kreiert aufgrund der Tabelle das Passwort, indem man von der obigen 4 der Tabelle bis zur 5 runter die Zeichen aneinander reiht und dann nach rechts (links/diagonal) weiter die Zeichen festhält, bis man beispielsweise 8 Zeichen für das Passwort zusammengestellt hat ⇒ **Passwort = iI%gKK1o** usw.

Die Aufbewahrung dieser Sätze oder der Karte kann z. B. in der Brieftasche erfolgen. Sollte allenfalls die Brieftasche einmal gestohlen werden, so sind die Passwörter sofort zu ändern und neue Karten oder Sätze zu erstellen.

Einige wenige Passwörter können mit dem obigen Vorgehen verwaltet werden. Bei mehreren Passwörtern ist es sinnvoll, ein Werkzeug einzusetzen, welches die unterschiedlichen Benutzeridentifikationen und Passwörter verwaltet (beispielsweise Single Sign On Systeme).

Ein Passwort soll periodisch geändert werden (in etwa alle drei Monate); dabei ist darauf zu achten, dass nicht wieder das alte Passwort verwendet werden darf.

Einige Experten weisen immer wieder darauf hin, dass ein Passwort selbst, welches eine Authentifikation durch Wissen ermöglicht, insbesondere im sensitiven Umfeld zuwenig sicher ist. In diesem Umfeld ist (zusätzlich) der Einsatz von Biometrischen Systemen (Authentifikation durch Eigenschaften der Person) oder von Chipkarten (Authentifikation durch Besitz) vorzusehen. Das nachfolgende Thema enthält auch Informationen zur Biometrie.

7.3. Zugang zu Informatiksystemen mittels biometrischer Authentifizierung

Die im Auftrag des EDSB von einer Ingenieurschule durchgeführte Studie zeigt, dass Authentifizierungssysteme auf der Grundlage von Fingerabdrücken heute bereits technisch weit entwickelt sind und durchaus die klassische Authentifizierung durch Passwörter ersetzen können. Allerdings bestehen noch einige Sicherheitsmängel bei der Integration in Betriebssysteme. Diese Kinderkrankheiten dürften rasch abklingen, da die neuen biometrischen Authentifizierungssysteme für die zahllosen elektronischen Dienstleistungen auf dem Markt die einzige Hoffnung auf Fortschritt in Sachen Zugangssicherheit darstellen.

Mit zunehmender Informatisierung unserer Gesellschaft muss sich jeder Einzelne eine beeindruckende Anzahl Passwörter, persönlicher Identifikationsnummern (PIN: Personal Identification Number) und anderer magischer Formeln merken. Zur Vorbeugung gegen den Missbrauch durch Personen, die sich die Sicherheitsdaten unrechtmässig beschafft haben, müssen manche Codes ausserdem regelmässig geändert werden. Angesichts dieser anspruchsvollen Aufgabe neigt der Benutzer verhängnisvollerweise zur Vereinfachung und/oder Vereinheitlichung seiner Zugangscodes. Zuweilen notiert er sie gar auf einem Zettel in der Nähe der dazugehörenden Dienstleistung (Passwort unter der Tastatur, PIN auf der Kreditkarte...). Da die Zugangssicherheit der betreffenden Dienste durch dieses Verhalten bedauerlicherweise erheblich beeinträchtigt wird, ist nach überzeugenden Lösungsansätzen zu suchen. Die Verwendung von - teilweise kostenlosen - Programmen zur Verwaltung von persönlichen Codes

in einer verschlüsselten Datenbank stellt gegenüber dem Zettel mit notierten Codes bereits einen grossen Fortschritt dar. Ebenso lässt sich der geheime Bereich des Personal Digital Assistant verwenden, den man im Prinzip immer bei sich trägt.

Dennoch handelt es sich in der Regel um einfache Codes, die in direktem Zusammenhang mit dem Inhaber, seinem Umfeld oder seinen Gewohnheiten stehen und somit von übelwollenden Dritten leicht herauszufinden sind. Diesbezüglich stellt die biometrische Authentifizierung einen erheblichen Fortschritt dar, da sie statt mit einem auswendig gelernten und wiederzugebenden Code mit einem vom Benutzer untrennbaren äusserlichen Merkmal operiert. Die grosse Anzahl verfügbarer äusserlicher Merkmale setzt eine ebenso grosse Vielfalt an komplexen und zuverlässigen Erkennungssystemen voraus. Am häufigsten werden für die biometrische Authetifizierung folgende Körpermerkmale eingesetzt: Fingerabdruck, Stimmenklang, Morphologie der Hand, des Gesichtes oder des Ohrs, Muster der Iris oder der Netzhaut, Aussehen und/oder Dynamik der Unterschrift, Dynamik der Tastenberührung, Blutzusammensetzung, Körpergeruch.

Der Benutzer bevorzugt verständlicherweise Systeme, auf die seine körperliche oder seelische Verfassung keinen Einfluss hat, die keinen Körperkontakt verlangen und hinsichtlich des Datenschutzes keine Gefahren mit sich bringen. Auch stossen manche Systeme instiktiv auf Ablehnung: Der Fingerabdruck wird mit der Polizei in Verbindung gebracht, das Muster der Iris oder der Netzhaut enthält indirekt Informationen über den Gesundheitszustand der authentifizierten Person. Dem zugrunde liegt natürlich immer die Befürchtung des Missbrauchs der persönlichen Merkmale zu unzulässigen Zwecken.

Die biometrischen Authentifizierungssysteme verwandeln das analysierte Körpermerkmal in eine für den Vergleich wesentlich geeignetere Schablone (Template). Auch gibt es keine absolute biometrische Authentifizierungsmethode, da die Erkennung durch eine auf der Wahrscheinlichkeit beruhende Übereinstimmung zwischen der analysierten Schablone und den Refenzschablonen der Datenbank erfolgt. Bei jeder Methode wird daher immer ein gewisser Prozentsatz irrtümlich angenommen (Vertraulichkeit und Integrität sind gefährdet) bzw. abgelehnt (Verfügbarkeit und Zuverlässigkeit sind gefährdet). Dies hängt von der Differenzierbarkeit, der Reproduzierbarkeit und der Beständigkeit der gewählten Körpermerkmale ab, aber auch von externen Faktoren wie Ausrüstungskosten und Grad der Benutzerakzeptanz.

Sieht man vom zuletzt genannten Kriterium ab, ist die Authentifizierung über Fingerabdrücke ohne Zweifel die Methode mit dem besten Preis-Leistungs-Verhältnis, wie es auch das in die Höhe schnellende Angebot dieser Produkte belegt. Die Abbildung des Fingerabdrucks wird in eine Schablone aus einzigar-

tigen Merkmalen (minutien) eines Fingerabdrucks verwandelt, d.h für jeden Fingerabdruck einzigartige und unverwechselbare Punkte (Endungen, Verbindungen, Windungen, Schlaufen, Spiralen...). Um die Zuverlässigkeit des Systems zu steigern, wird der Durchschnitt mehrerer Abbildungen desselben Fingerabdrucks als Schablone gespeichert, die wiederum oft sogar durch Schablonen der Abdrücke anderer Finger des Benutzers ergänzt wird. Fälschungssichere, wärme- und feuchtigkeitsempflindliche Erkennungsgeräte schliessen den Betrug durch Auflegen einer Abbildung aus. Vorstellbar wäre theoretisch der Missbrauch des Systems durch Auflegen einer Art Kunsthaut, in die ein dem Opfer unbemerkt abgenommener Fingerabdruck eingraviert wurde. Allerdings steht der Aufwand eines solchen Unterfangens womöglich in keinem Verhältnis zum erhofften Gewinn.

Die Verwandlung des Fingerabdrucks in eine Schablone stellt einen unumkehrbaren Vorgang dar und schliesst somit die Gefahr der Rekonstruktion des Fingerabdrucks anhand der Schablone aus. Da es ausserdem für die Verwandlung bis heute kein standardisiertes Verfahren gibt, besteht nahezu kein Risiko, dass anhand übereinstimmender Schablonen eine Verbindung zwischen Datenbanken, die eigentlich unabhängig bleiben sollten, hergestellt wird. Um diese Unabhängigkeit und somit das Pseudonym des Benutzers zu gewährleisten, müssen entweder für jede Dienstleistung andere äussere Merkmale verwendet oder aber alle Datenbanken mit Schablonen bzw. Fingerabdrücken einzeln verschlüsselt werden.

Die von uns in Auftrag gegebene Studie konzentrierte sich auf Authentifizierungssysteme mit Fingerabdruck-Erkennungsgeräten, die in die Maus, in die Tastatur oder ein anderes zweckbestimmtes Endgerät integriert sind. Während die Erhebung und Erkennung des Fingerabdrucks kaum Schwierigkeiten bereitete, stellte sich die Integration der Software in die Sicherheitsebene des Betriebssystems in vielerlei Hinsicht als enttäuschend heraus. Die Schablonen-Datenbank muss unbedingt mit der Datenbank für die Passwörter der identifizierten Personen verknüpft werden (z.B. SAM-Datenbank von Windows NT). In einem Fall gelang zwar die Verbindung durch Kopieren der Passwörter, mit dem Ergebnis allerdings, dass diese anschliessend in der Schablonen-Datenbank unverschlüsselt und editierbar erschienen! Dieser Mangel ist umso bedauerlicher, als die automatische Identifizierung (Benutzername braucht nicht mehr eingegeben werden) und der Einsatz von Fingerabdrücken als Chiffrier-Schlüssel für besonders schützenswerte persönliche Dateien zahlreiche Vorteile boten. In einem anderen Fall bestand zwar eine klare Trennung zwischen beiden Datenbanken, doch konnte der Benutzer nach Herstellung der Verbindung die Schablonen anderer Personen durch seine eigene ersetzen und sich dadurch mit der Identität und sämtlichen Privilegien der betrogenen Person Zugang zum System verschaffen. Einzig die Fingerabdruckerkennung mittels zweckbestimmtem Endgerät erlaubte eine sichere und zuverlässige Identifizierung ver-

bunden mit der automatischen Benutzererkennung. Ein Angriff auf die Übertragungsleitung (hier ein USB) zwischen dem Periphäriegerät und dem Computer blieb aufgrund der dynamischen Codierung der übertragenen Fingerabdrücke ohne Erfolg. Zu dem Erkennungsgerät gehört ausserdem eine Software-Erweiterung für NT-Server, mit der die Passwörter vollständig durch die aus den persönlichen Fingerabdrücken abgeleiteten Schablonen ersetzt werden können. Die zentrale Verwaltung der Schablonen erlaubt die Mobilität (Roaming) der Benutzer, da sie an jedem mit einem geeigneten Erkennungsgerät ausgestatteten Arbeitsterminal authentifiziert und identifiziert werden können. Zu der in die Maus integrierten Fingerabdruckerkennung muss leider gesagt werden, dass keines der beiden geprüften Modelle die funktionalen und ergonomischen Eigenschaften aufwies (keine Kugel, zu kurzes Kabel, mangelhafter Tastenkontakt), die man heute von diesen Zeigegeräten erwarten kann. Die Tastaturen werden diesbezüglich weniger kritisiert, da ihre Ergonomie quasi standardisiert und die Qualität der wichtigsten Funktion - nämlich Tippkomfort - nur selten zu beanstanden ist.
Abschliessend zeigte die Studie, dass die Authentifizierung mittels Fingerabdruck heute durchaus machbar ist. Sie bietet gegenüber der Authentifizierung mittels Passwort sowohl in Bezug auf Benutzerfreundlichkeit als auch auf Sicherheit unbestreitbare Vorteile, vorausgesetzt, dass letztere umfassend garantiert wird. Eine generelle Verbreitung biometrischer Authentifizierungssysteme wird zweifelsohne zu niedrigeren Preisen und vor allem zur Verbesserung von Datensicherheit und Datenschutz führen.

7.4. Protokollierung relationaler Daten: Zweckbindung, Schutz, Archivierung und Vernichtung

Seit mehreren Jahrzehnten haben in der Welt der Datenbanken die relationalen Systeme die Vorherrschaft. Die Protokollierung der Bearbeitung dieser Daten bereitet nicht zu unterschätzende technische und organisatorische Schwierigkeiten, selbst wenn sie aus gutem Grunde geschieht. Glücklicherweise erlauben es die mit relationalen Systemen gelieferten Standardwerkzeuge, diese Schwierigkeiten auf zufriedenstellende Weise zu beheben. Protokollierungs-Daten sind äusserst schützenswerte Daten, deren Vertraulichkeit und Integrität durch eine kohärente Archivierungs- und Vernichtungspolitik zu garantieren ist.

In relationalen Datenbanksystemen (weiter unten SGBDR) verwendet die Sprache ISO/SQL (International Standards Organisation, Structured Query Language) den altbekannten Suchbefehl «SELECT FROM WHERE» sowie die Befehle «INSERT, UPDATE, DELETE» zur Ergänzung, Änderung respektive Löschung der Daten in einer relationalen Tabelle. Die Protokollierung besteht

im Wesentlichen darin, für jeden Vorgang die Informationen «Who did What, When» in einer zusätzlichen Tabelle zu speichern, die im Idealfall in einer unabhängigen eigens zu diesem Zweck geführten Datenbank abgelegt ist. Um die Protokollierungstabellen unter Wahrung der Anonymität analysieren zu können, empfiehlt es sich, die Identifizierungsdaten («Who») in verschlüsselter Form zu speichern.

Zur Protokollierung der Datenabfrage muss die Anwendung eine Paraphierung durch Eintrag in dem entsprechenden Protokoll für jeden Lesevorgang ausdrücklich vorsehen. Dieser Sachzwang verlangt die Abklärung des Zwecks des Unterfangens, insbesondere da die Anzahl der täglichen Lesevorgänge mancher Tabellen beeindruckend hoch sein kann.

Zur Protokollierung von Aktualisierungen hingegen erlaubt es der SQL-Standard, «TRIGGERS» zu definieren. Dabei handelt es sich um kleine Hilfsanwendungen zur Aktualisierung, die vor oder nach der Ausführung einer Hauptaktualisierung gestartet werden. Dazu ist lediglich in den betreffenden Tabellen ein TRIGGER für jeden der drei Aktualisierungsbefehle festzulegen [Beispiel: CREATE TRIGGER tr_client_up FOR client AFTER UPDATE AS INSERT INTO log_client SELECT Who, When, ClientNum, PhoneNum... FROM Inserted;], damit die SGBDR automatisch eine von der Anwendung völlig unabhängige Protokollierung vornimmt.

Hinsichtlich der Zugriffsberechtigung zu den Protokollierungstabellen (SQL: GRANT) muss das Hinzufügen von Einträgen natürlich sämtlichen Benutzern offenstehen (SQL: Public), jede spätere Änderung jedoch strengstens verboten sein. Die Verantwortlichen der Datensicherheit hingegen müssen die Möglichkeit haben, die Protokolle einzusehen und nach ihrer regelmässigen Übertragung auf Archivierungsdatenträger zu löschen. Auch die Archivierungsdatenträger sind schliesslich zu vernichten, sobald die maximal vorgeschriebene Aufbewahrungsfrist verstrichen ist.

Wie bei jeder Vernichtung besonders schützenswerter Daten ist das logische Löschen durch marktübliche Vernichtungs-Tools einer physischen Entsorgung vorzuziehen. Für herkömmliche Dateien können Vernichtungs-Tools (file wiping tools) eingesetzt werden, die durch mehrfaches Überschreiben vorgehen. Bei relationalen Datenbanken ist die physische Vernichtung eines Tabelleninhalts aufgrund der automatischen Speicherplatzverwaltung weitaus komplizierter. Manchmal muss die Datenbank reorganisiert, komprimiert oder neu geladen werden, es sei denn, der Befehl DELETE verfügt über eine systemdefinierte Option zur physischen Zerstörung der Daten.

Es ist festzustellen, dass die Managementsysteme von relationalen Datenbanken sämtliche Funktionen zu einer unkomplizierten, autonomen und teilweise von

der Anwendung unabhängigen Protokollierung der ausgeführten Bearbeitungen bieten. Diese Systeme erlauben es ebenfalls, den Zugriff auf Informationen im Einklang mit den datenschutzrechtlichen Anforderungen abzusichern. Zusammen mit einer seriösen Archivierungs- und vor allem Datenvernichtungspolitik gestaltet sich die Protokollierung von relationalen Daten weniger kompliziert und gefährlich, als auf den ersten Blick erscheinen mag.

7.5. EDSB-Office: Ein abgesichertes Geschäftsführungssystem

Nach über einem Jahr Erfahrung mit der internen Public Key Infrastructure liefert der EDSB einige Erkenntnisse über die Machbarkeit, Einführung und Weiterentwicklung eines solchen Systems. Die Ergebnisse in Bezug auf Sicherheit, Leistungsfähigkeit und Benutzerfreundlichkeit zeigen, dass mit der heutigen Technologie eine äussert sichere Umgebung geschaffen werden kann, die den höchsten Anforderungen unseres Datenschutzgesetzes gerecht wird.

Angesichts der Inkompatibilität unseres ehemaligen Systems mit dem Jahr 2000 und mit der erklärten Absicht, die Machbarkeit eines Systems mit Verschlüsselung sämtlicher Arbeitsdokumente zu beweisen, hat der EDSB die Entwicklung einer spezifischen Windows-Anwendung in Auftrag gegeben, die auf der «Office Suite» und einem marktüblichen Managementsystem für relationale Datenbanken basieren sollte. Innerhalb einer heute gängigen Client-Server-Konfiguration erfolgt die Chiffrierung und Dechiffrierung für jeden Client mit Hilfe einer ad-hoc-Software, die sich inzwischen de facto als Standard für die Bearbeitung verschlüsselter E-Mail durchgesetzt hat. Dies erlaubt eine unverletzbare Übertragung besonders schützenswerter Dokumente und Datenfelder zwischen Clients und Datenbankserver, wo sie zum Schutz vor Angriffen auf dieser Ebene verschlüsselt gespeichert werden (Eindringen, Sicherheitskopien...). Für die Ausgabe von Daten an einen Netzdrucker gelten ähnliche Schutzmassnahmen, wobei spezielle Druckerserver die Datenflüsse unmittelbar vor dem eigentlichen Druckvorgang entschlüsseln. Dennoch ist für besonders schützenswerte Dokumente natürlich ein direkt an die Arbeitsstation des Verfassers angeschlossener Drucker vorzuziehen.
Erfahrungsgemäss geschieht die Chiffrierung und Dechiffrierung von Dokumenten, die bis zu mehrere Dutzend Seiten umfassen, in zufriedenstellenden Reaktionszeiten. Nebenbei wird Platz gespart, da die Chiffrierung automatisch zur Komprimierung der Dateien führt. In einer Public Key Infrastructure (PKI) stellte die Verwaltung der Schlüssel einen wesentlichen Aspekt des Projektes dar. Die asymmetrischen Schlüssel (Schlüsselpaar bestehend aus öffentlichem und privatem Schlüssel) werden von den Benutzern selbst hergestellt, um jegliche unrechtmässige Kopie besonders kritischer Daten zu vermeiden. Auf-

bewahrt werden die Schlüssel – paradoxerweise – auf einer gewöhnlichen Diskette, die zwar keinen schnellen Zugriff, aber dafür wegen ihrer Mobilität eine absolute Sicherheitsgarantie zu äusserst geringen Kosten bietet (Laufwerk standardmässig eingebaut und extrem kostengünstiger Datenträger). Natürlich wären auch andere schnellere, verlässlichere und/oder kompaktere, aber auch teurere mobile Datenträger für die Speicherung der Schlüsselbunde (Keyrings) denkbar.

Besonders wichtig ist der Pass-Satz (Passphrase), der den privaten Teil des Schlüssels schützt. Er muss eine gewisse Komplexität besitzen (Länge, Unverständlichkeit, Sonderzeichen...), um gegen eventuelle Angriffe durch Interessierte resistent zu sein. Der öffentliche Teil des Schlüssels kann und soll, wie sein Name sagt, ungehindert an jeden exportiert und übertragen werden können, der ein Dokument verfassen möchte, das anschliessend nur vom Inhaber des entsprechenden privaten Schlüssels gelesen werden kann. In einem Umfeld, in dem sich die beteiligten Personen kennen und häufig sehen, kann der öffentliche Schlüssel einfach auf Diskette weitergegeben werden, ohne dass eine aussenstehende Zertifizierungsbehörde (CA: Certification Authority) hinzugezogen werden muss.

Nachdem der Benutzer den zu seinem privaten Schlüssel gehörenden Pass-Satz eingegeben hat, kann er die Anwendung starten, um all seine persönlichen Dokumente zu bearbeiten und sämtliche mit dem Gruppenschlüssel (Standardmodus) chiffrierten Dokumente zu lesen. Neben dem individuellen und dem Gruppenschlüssel kennt das Programm die Chiffrierung jedes Dokumentes mit einem zusätzlichen Dechiffrierungs-Schlüssel (ADK: Additional Decryption Key). Dieser dient dazu, die gespeicherten Dokumente unter allen Umständen lesen zu können, selbst wenn wegen Verlust, Vergessen, Beschädigung o.ä. die üblichen zur Dechiffrierung notwendigen Elemente nicht zur Verfügung stehen. Diese Funktion ist den Direktionsmitgliedern vorbehalten und wird somit von den Systemverwaltern nicht kontrolliert. Bedauerlicherweise ist eine derartige Aufgabentrennung im Bereich der Datenverwaltung eher die Ausnahme.
Neben der Dokumentenverschlüsselung bietet das System eine weitere bemerkenswerte Funktion: die Möglichkeit, Dokumente aufgrund einer logischen Kombination von Stichwörtern zu suchen (auch Volltextsuche genannt). Zur Vereinfachung der Indexierung und vor allem zur Beschleunigung des Suchvorgangs wurde für die vier Arbeitssprachen (Deutsch, Französisch, Italienisch und Englisch) eine Liste von «unwichtigen» Wörtern erstellt. Das Ergebnis ist beeindruckend: In nur wenigen Sekunden erscheint eine Liste der mit den Suchkriterien übereinstimmenden Dokumenten.

Die Anwendung erlaubt ausserdem das unabhängige Arbeiten mit produktiven oder fiktiven Daten. Damit vermeidet man den unnötigen Zugriff auf produktive Daten bei Vorführungen für Dritte oder Testläufen neuer Software-Versionen.

Die fiktive Datenbank bietet darüber hinaus für neue Mitarbeiter den Vorteil, sich ohne Risiko mit der Anwendung vertraut zu machen. Hinsichtlich der Software-Versionen unterscheiden wir zwischen der Beseitigung von Funktionsstörungen, die so schnell wie möglich vorgenommen werden muss, und der Verbesserung der Funktionen, die eine jährliche oder halbjährliche Planung, Beurteilung und Umsetzung verlangt. Auf diese Weise ist eine wirksame Weiterentwicklung - unter Wahrung der für eine derartige Anwendung unabdingbaren Stabilität - möglich.

Die gewählte Verschlüsselungs-Software erlaubt es ausserdem jedem Benutzer, verschlüsselte E-Mails zu verschicken und sich mit Hilfe einer persönlichen Firewall oder einem Angrifferkennungssystem gegen Cyber-Angriffe zu schützen. In Kombination mit einen Anti-Virus-Programm, dessen Definitionsdateien regelmässig aktualisiert werden, bietet das System ein angemessenes Schutzniveau gegen die Gefahren, denen ein Arbeitsterminal mit Internet-Anschluss ausgesetzt ist.

Schliesslich bietet das Geschäftsführungsprogramm zusätzliche Basisfunktionen für die Weiterleitung von Dokumenten (Workflow), die Arbeitsplanung und das Projektmanagement sowie für die Protokollierung sämtlicher Les- und Schreibvorgänge.

7.6. Umsetzung der Datensicherheit in der Bundesverwaltung

Die Datensicherheit muss bereits in den Planungsphasen eines Projekts (Vorstudie, Konzept) berücksichtigt werden. Die Planung und Realisierung von Projekten hat in der Bundesverwaltung nach dem HERMES-Handbuch zu erfolgen, dessen Vorgaben aber nicht immer eingehalten werden. Dadurch entfallen viele Vorteile, die ein solcher Projektrealisierungs-Standard mit sich bringen würde. Teilt man die Datensicherheit in die drei Bereiche Vertraulichkeit, Verfügbarkeit und Integrität auf, so kann man feststellen, dass die Verfügbarkeit in der Bundesverwaltung recht gut abgedeckt ist. Bei der Vertraulichkeit und der Integrität sind aber noch einige Massnahmen zu ergreifen, damit eine angemessene Datensicherheit ausgewiesen werden kann.

Die Umsetzung der Datensicherheit beginnt schon bei der Planung des Informations- bzw. Informatik-Systems. Für die Führung und Abwicklung von Informatikprojekten in der Bundesverwaltung muss bzw. sollte das HERMES-Handbuch verwendet werden. Dieses Handbuch ist als Standard für die Führung von Projekten einzusetzen. Ziele von Standards können wie folgt umschrieben werden:

- personenunabhängig	- nachvollziehbar	- einheitlich
- Verhinderung von Wildwuchs	- bekannte Qualität	- geringere Kosten
- vollständig	- kompatibel	- revisionsfähig

In einigen Fällen konnten wir feststellen, dass in der Bundesverwaltung nicht nach HERMES vorgegangen wird. Bei solchem Vorgehen geht ein grosser Teil der oben aufgeführten Zielsetzungen verloren. In vielen Fällen werden auch die von HERMES geforderten und zu dokumentierenden Sicherheitsvorgaben (Qualität) nicht berücksichtigt, so dass wir immer wieder nachfassen müssen, soweit wir dazu die notwendigen Kapazitäten haben. In den Ausschreibungen bzw. den Pflichtenheften finden sich in den seltensten Fällen Vorgaben zur Datensicherheit. Wir haben auch schon festgestellt, dass aufgrund von unkonkreten Konzepten, die nicht auf HERMES basierten, Ausschreibungen gemacht wurden, die nicht sehr klar waren. Wie man aufgrund solcher Vorgaben die richtige Wahl treffen kann, ist für uns nicht nachvollziehbar.

Einem Bericht an den Bundesrat entnehmen wir, dass die Kosten für die Informatiksicherheit schwer auszuweisen seien. Dies liege vor allem daran, dass die Sicherheitskosten kaum getrennt von den normalen Informatikkosten verbucht werden könnten. Wir sind zwar ebenfalls der Meinung, dass die Kosten für die Informatiksicherheit überall in einem EDV-System oder Informatik-Projekt auftreten können, dennoch müsste unseres Erachtens schwergewichtig festgelegt werden, in welche Sicherheitsbereiche investiert wurde. Die Feststellung, dass ca. 6% der Ausgaben in der Informatik auf Datensicherheitsmassnahmen entfallen, ist wenig aussagekräftig. Es besteht keine Transparenz, welche Ämter bzw. Departemente in welche Bereiche der Datensicherheit investiert haben. Beim Nachfassen unsererseits wurden wir im Jahre 1999 immer wieder auf die Jahr 2000 Problematik verwiesen. Wir gehen deshalb davon aus, dass diese Mittel insbesondere für die Analyse der bestehenden Systeme und Anwendungen sowie einen unterbruchsfreien Berieb beim Jahreswechsel eingesetzt wurden. Es wurden uns in der vergangenen Zeit auch nur wenige EDV-Projekte unterbreitet. Projekte, die sich schwergewichtig mit Datensicherheitsanliegen auseinander setzen, haben wir keine erhalten.

Ein Teilbereich der Datensicherheit ist die Aufrechterhaltung des Systembetriebs - der Verfügbarkeit der Informatiksysteme und -anwendungen. Die dazu notwendigen Massnahmen wie z. B. die Anschaffung von Cluster-, RAID5-, Shadowing-Systemen im Host- bzw. Serverbereich sollten finanziell nicht mehr den Informatiksicherheitskosten belastet werden, weil solche Systeme schon fast zur Grundausstattung gehören. Die Nichtverfügbarkeit von Systemen wird in den betroffenen Organisationseinheiten sehr rasch erkannt. Aus diesem Grunde sind die Datensicherheitsmassnahmen in diesem Bereich recht gut umgesetzt. Nachholbedarf besteht aber nach wie vor bei den Aspekten

der Datenintegrität und der Vertraulichkeit. Insbesondere in diesem Bereich müssen transparente Steuerungselemente wie beispielsweise die Anmeldung von EDV-Projekten gemäss der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) oder finanzielle Mittel ein- bzw. durchgesetzt werden, um die Informatiksicherheit zu erhöhen.

Diverse Kontrollen haben in den vergangenen Monaten aufgezeigt, dass im Umfeld der Datensicherheit nach wie vor erheblicher Handlungsbedarf besteht; ohne die notwendigen Ressourcen (Personal, finanzielle Mittel) sehen wir auch zukünftig keine grosse Verbesserung der Situation. Einen anderen möglichen Lösungsansatz sehen wir darin, den Kontrollorganen bessere Sanktionsmöglichkeiten zur Verfügung zu stellen.

III. INTERNATIONALES

1. Europarat

- Arbeiten der CJPD: Datenschutz im Versicherungswesen und in der Videoüberwachung

Die Projektgruppe für den Datenschutz (CJPD) tagte vom 9. bis zum 13. Oktober 2000. Sie schloss die Arbeiten im Versicherungsbereich ab und setzte sich weiter mit dem Bereich der Informationstechnologie – mit dem Schwerpunkt auf der Überwachung – auseinander.

Nach der Verabschiedung eines Empfehlungsentwurfs über den Schutz von Personendaten, die zu Versicherungszwecken erhoben und bearbeitet werden (siehe 7. Tätigkeitsbericht1999/2000, S. 88), beendete die CJPD auch den dazugehörenden Begleitbericht. Das Gesamtpaket dürfte im Jahr 2001 vom Ministerkomitee des Europarates angenommen werden.

Die CJPD befasste sich zudem mit einem Sachverständigenbericht über den Schutz des Privatlebens im Zusammenhang mit der Überwachung (http://www.coe.fr/dataprotection) und beschloss, einen Katalog von Leitgrundsätzen zum Schutz der Personen bei der Datenbeschaffung und -bearbeitung per Videoüberwachung auszuarbeiten (siehe auch zum Thema Videoüberwachung S. 64). Ausgehend von der Feststellung, dass immer mehr öffentliche und private Stellen zur Kontrolle des Personen- und Warenverkehrs, des Zugangs zu Privatliegenschaften oder mancher Demonstrationen Überwachungssysteme

einsetzen, befürwortete die CJPD die Festlegung von Leitgrundsätzen. Die Grundsätze sollen die Garantien für betroffene Personen beim Einsatz technischer Videoüberwachungs-Installationen hinsichtlich Beobachten sowie Beschaffen und Speichern von Personendaten (vor allem Verhalten, Bewegungen und Kommunikation einer oder mehrerer Personen) erweitern und klären. Gemäss den Vorschlägen des von der CJPD beauftragten Sachverständigen setzen Überwachungstätigkeiten Folgendes voraus:

- überprüfen, ob und inwieweit die Überwachung auf der Basis geeigneter Rechtsgrundlagen zu legitimen, spezifischen und expliziten Zwecken zugelassen ist und fair durchgeführt wird;
- mittels erforderlicher Massnahmen sicherstellen, dass die Überwachungsaktivität den Grundsätzen des Schutzes von Personendaten genügt;
- Videoüberwachungsgeräte nur dann verwenden, wenn andere Systeme, die das Privatleben weniger stark beeinträchtigen, nicht in Frage kommen;
- im Einzelfall die Grundsätze Selektivität und Verhältnismässigkeit in bezug auf die verfolgten Ziele beachten, um das Privatleben auch im öffentlichen Raum angemessen zu schützen;
- den Grundsatz der Datenrelevanz und -angemessenheit - vor allem in bezug auf die verwendeten technischen Mittel - befolgen;
- die Videoüberwachung einschränken, sofern sie zu Diskriminierung führen kann oder lediglich für bestimmte Personen wegen deren Meinungen, Überzeugungen oder deren Sexualleben angeordnet wurde;
- den Transparenzgrundsatz beachten, d.h. vor allem die betroffenen Personen über eine existierende spezifische Videoüberwachung informieren (mit klaren Auskünften, auch Zusammenfassungen und Schildern, auf denen der Standort der Überwachungsgeräte deutlich signalisiert wird);
- bei spezifischen Risiken für die betroffenen Personen und/oder weiter gehenden Kontrollen (z.B. Verbinden von Bild und biometrischen Daten oder Profildefinition der betroffenen Personen) den Datenschutz verstärken;
- grundsätzlich keine Personendaten an von der Überwachungstätigkeit nicht betroffene Dritte bekanntgeben;
- ad hoc-Bestimmungen für die Ausübung des Auskunftsrechts der betroffenen Personen festlegen;
- den Einsatz der Systeme, welche gezielt die Arbeitsqualität oder die Produktivität am Arbeitsplatz überprüfen sollen, einschränken und für angemessene Information der Beschäftigten sorgen.

Die CJPD prüfte ausserdem den Entwurf des Übereinkommens über Kriminalität im Cyberspace und verabschiedete eine Stellungnahme, in der sie die Bedeutung des Datenschutzes unterstrich und forderte, zumindest einen Verweis auf das Übereinkommen Nr. 108 des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108) in den Konventionsentwurf aufzunehmen. Ausserdem betonte sie, dass

das Übereinkommen 108 einen festen Bestandteil der Normen bildet, welche das «acquis» (Rechtsbestand) des Europarats ausmachten. Schliesslich begann die CJPD mit der Untersuchung eines Empfehlungsentwurfs über den Zugang zu amtlichen Dokumenten.

- Arbeiten des T-PD: Zusatzprotokoll, Vertragsklauseln und Evaluation des Übereinkommens 108

Der Beratende Ausschuss des Übereinkommens 108 (T-PD) hielt vom 6. bis zum 8. Juni 2000 seine 16. Tagung ab. Der Ausschuss nahm die vom 5. April 2000 datierte Stellungnahme Nr. 217 (2000) der Parlamentarischen Versammlung zum Zusatzprotokoll des Übereinkommens 108 betreffend Aufsichtsbehörden und grenzüberschreitende Datenübermittlungen zur Kenntnis (http://www.coe.fr/dataprotection) und beendete die Arbeiten am Text des Zusatzprotokolls. Daneben befasste er sich weiter mit den Vertragsklauseln und begann vor allem vor dem Hintergrund der technologischen Entwicklungen mit der Evaluation des Übereinkommens 108.

Der Beratende Ausschuss prüfte insbesondere, ob der Protokollentwurf verändert werden solle, um die Vorschläge der Parlamentarischen Versammlung aufzunehmen (siehe auch 7. Tätigkeitsbericht 1999/2000, S. 88). Zwar betonte er den positiven Beitrag der Stellungnahme der Parlamentarischen Versammlung, vor allem weil darin der Stellenwert des Datenschutzes im Zeitalter des Internets und der Informationsgesellschaft hervorgehoben wird, griff aber die Vorschläge im Protokollentwurf nicht ausdrücklich auf. Er befolgte die zu Beginn der Arbeiten festgelegte Linie, die darin bestand, sich an Geist und Buchstaben des Übereinkommens 108 zu halten und einen Text zu verfassen, der sich auf die wesentlichen Elemente beschränkt. In diesem Sinn wurden bestimmte Vorschläge der Parlamentarischen Versammlung im erläuternden Bericht übernommen; andere sollen später geprüft werden.

Das Zusatzprotokoll dürfte demnächst vom Ministerkomitee angenommen und den Mitgliedsstaaten zur Unterzeichnung freigegeben werden. Die Schweiz hat an der Ausarbeitung aktiv mitgewirkt und sollte in der Lage sein, es rasch zu ratifizieren. Zu untersuchen ist der Veränderungsbedarf des DSG (siehe dazu das Thema über die Modernisierung des Datenschutzes, S. 56); es geht darum, die Kompetenzen der Kontrollbehörden und die Systeme der grenzüberschreitenden Datenflüsse zu Empfängern, die keinem gleichwertigen Datenschutzsystem unterstellt sind, zu klären und auszuführen. Eine rasche Ratifizierung liegt vor allem aufgrund des Informationsaustausches mit der Europäischen Union im Interesse der Schweiz. Sobald die fünfzehn Mitgliedstaaten das Protokoll unterzeichnet haben, könnte die Europäische Union womöglich

ihre Haltung gegenüber den Vertragsparteien des Übereinkommens 108, die dem Protokoll fernbleiben, überdenken.

Ausserdem beschloss der Beratende Ausschuss, das Übereinkommen 108 angesichts der Entwicklungen in den zwanzig Jahren seit der Annahme und angesichts der neuen Informationstechnologien zu evaluieren. Der Ausschuss wird gestützt auf diese Evaluation entscheiden, ob eine Änderung des Übereinkommens 108 ins Auge gefasst werden muss. Eine allfällige Veränderung darf in keinem Fall die grundlegenden Prinzipien des Datenschutzes in Frage stellen. Dagegen könnten mit Blick auf die Stärkung des Datenschutzes auf internationaler Ebene die Befugnisse des Ausschusses überarbeitet werden.

Ferner befasste sich der Beratende Ausschuss weiter mit der Untersuchung der Vertragsklauseln in bezug auf grenzüberschreitende Datenströme zu Empfängern in Staaten, welche das Übereinkommen 108 nicht ratifiziert haben. Auf der Basis des Sachverständigenberichts (http://www.coe.fr/dataprotection) hat er eine Reihe von Empfehlungen zu erarbeiten, die anlässlich der 17. Tagung verabschiedet werden dürften.

- Entwurf eines Protokolls über genetische Untersuchungen beim Menschen

Eine Arbeitsgruppe des Europarates ist daran, ein Protokoll über genetische Untersuchungen beim Menschen auszuarbeiten. Mit dem Protokoll soll jegliche Diskriminierung einer Person wegen ihres Erbgutes untersagt werden. In der Berichtsperiode wurden v.a. die allgemeinen Bestimmungen des Protokolls diskutiert. Insbesondere ging es um den Geltungsbereich des Protokolls und die genetische Beratung. Ein weiteres Thema war die Einwilligung in die Verwendung von gentechnischen Informationen.

Die Arbeitsgruppe hat zum Ziel, ein Zusatzprotokoll zum Übereinkommen des Europarates über Menschenrechte und Biomedizin (Konvention von Oviedo) auszuarbeiten. Die vierte und fünfte Tagung der Arbeitsgruppe fand vom 5. bis 7. April und vom 17. bis 19. Oktober 2000 statt.

Der Geltungsbereich des Protokolls soll sich nicht nur auf den Gesundheitsbereich, sondern auch auf den Arbeits- und Versicherungsbereich erstrecken. Was die Gliederung des Protokolls im Detail betrifft, verweisen wir auf unseren letzten Tätigkeitsbericht (siehe 7. Tätigkeitsbericht 1999/2000, S. 89-90). Ob und inwiefern genetische Daten im Arbeits- und Versicherungsbereich bearbeitet werden dürfen, wurde noch nicht diskutiert. Aus unserer Sicht ist jedoch die Bearbeitung von genetischen Daten im Arbeits- und Versicherungsbereich

grundsätzlich zu untersagen. Denn eine Diskriminierung aufgrund des Erbgutes ist gerade hier nicht auszuschliessen.

Ebenfalls wurde das Thema der genetischen Beratung behandelt. Die betroffene Person muss vorher und umfassend über die Verwendung der genetischen Daten informiert werden. Dazu gehören u.a. Informationen über Zweck, Art und Aussagekraft der Untersuchung. Zudem müssen allfällige Risiken, die mit der Untersuchung verbunden sind, der betroffenen Person bekannt sein. Zum informationellen Selbstbestimmungsrecht gehört auch das Recht auf Nichtwissen. Dies sind nur einige Kriterien, die zur genetischen Beratung gehören. Eine umfassende Aufklärung ist auch nötig, damit die betroffene Person die Tragweite der Einwilligung erkennen kann. Eine solche Einwilligung in die Verwendung der genetischen Daten hat freiwillig zu erfolgen und muss jederzeit widerrufbar sein. Ob die Bearbeitung und vor allem die Konsequenzen der gentechnischen Untersuchungen den Betroffenen überhaupt jemals transparent gemacht werden können, bleibt jedoch fraglich.

Weitere Themen der Arbeitsgruppe waren genetische Untersuchungen, die systematisch angeboten werden (Reihenuntersuchungen), Forschung und Gentherapien.

2. Beziehungen zur Europäischen Union

- Anerkennung eines angemessenen Datenschutzniveaus für die Schweiz

Die Kommission der Europäischen Gemeinschaften stellte in der Entscheidung vom 26. Juli 2000 (siehe Anhang S. 109) fest, dass die Schweiz über einen angemessenen Schutz von Personendaten verfügt (siehe auch 7. Tätigkeitsbericht, 1999/2000, S. 92).

3. Internationale Konferenz der Beauftragten für den Datenschutz

Die XXII. Internationale Konferenz der Datenschutzbeauftragten fand vom 28. bis zum 30. September 2000 in Venedig statt. An der Konferenz beteiligten sich die Datenschutzbeauftragten von weltweit 25 Staaten, Regierungsexperten, Vertreter internationaler Organisationen, der Industrie, der Informatik, der Forschung und der Wissenschaft. Die Konferenz verabschiedete eine Erklärung, in welcher sie die Notwendigkeit von ge-

meinsamen Prinzipien und Standards im Datenschutz - vor allem angesichts der wachsenden Rolle der Technologien in der Datenberarbeitung, der steigenden Benutzerzahlen und der Verdichtung des Informationsaustausches auf weltweiter Ebene - bekräftigte. Ausserdem äusserte die Konferenz Besorgnis an den unzureichenden Datenschutzbestimmungen im Entwurf des Übereinkommens des Europarates über die Kriminalität im Cyberspace.

Die Konferenz legte den Schwerpunkt auf die Notwendigkeit eines universellen Schutzes des Privatlebens im globalen Umfeld: «One World, One Privacy» (www.garanteprivacy.it). Zur Frage stand die Zweckmässigkeit einer universellen Datenschutzkonvention. In diesem Rahmen wurde betont, dass die grundlegenden Prinzipien des Übereinkommens 108 einen universellen Geltungsanspruch besässen und dass dieses Übereinkommen insbesondere auch Staaten, die nicht Mitglieder des Europarates sind, zum Beitritt offen stehe. Die Konferenz setzte sich eingehend mit den Risiken und den Vorteilen der Informationstechnologien auseinander und bewertete auf der Basis konkreter Projekte die Fortschritte im Sektor der datenschutzfreundlichen Technologien. Die Sachverständigen befassten sich in verschiedenen Workshops mit den Grenzen von Vertragsklauseln im Rahmen der grenzüberschreitenden Datenflüsse. Ferner erörterten sie die Themen Genetikdaten, Videoüberwachung, Chipkarten und globale Dienstleistungen und behandelten die Frage des Schutzes des Privatlebens und der Medien sowie die elektronische Transparenz. Untersucht wurde auch das Problem des Datenschutzes im Bereich der Zusammenarbeit zwischen Gerichten und Polizei. Schliesslich äusserte die Konferenz ihre Besorgnis angesichts der Banalisierung der Privatsphäre, vor allem durch Sendungen wie «Big Brother», welche das wesentliche Konzept des Privatlebens unterhöhlen. Solche Trends erschweren in einer exhibitionistischen Gesellschaft die Achtung des Rechts auf Privatsphäre.

4. Europäische Konferenz der Beauftragten für den Datenschutz

Die Europäischen Datenschutzbeauftragten versammelten sich am 6. und 7. April 2000 zur Frühjahreskonferenz in Stockholm. Wir nahmen als Beobachter daran teil. Die Konferenz verabschiedete eine Erklärung über die Speicherung von Verkehrsdaten durch Internet Service Provider. Ausserdem äusserte sie Bedenken an der drohenden Speicherung und systematischen Aufbewahrung von Verkehrsdaten zu anderen Zwecken als der Rechnungsstellung (vor allem um die Daten den Strafverfolgungsbehörden zugänglich zu machen). Wie die Konferenz betonte, handelt es sich bei einer solchen Aufbewahrung um eine Verletzung der Grundrechte; diese muss einem offen-

sichtlichen Bedürfnis entsprechen und die Datenverwendung muss im Gesetz geregelt sein. Die Daten sollen so kurz wie möglich aufbewahrt werden.

Die Konferenz setzte sich im Lichte der nationalen Erfahrungen mit der Frage der Bearbeitung genetischer und medizinischer Daten auseinander. In Deutschland beispielsweise wurde eine Neuerung in das Gesundheitssystem eingeführt, welche den Informationsfluss zwischen Pflegeeinrichtungen und Krankenversicherungskassen regelt. In diesem System werden anstelle der Identitätsdaten Pseudonyme verwendet. Die genaue Identität kann ohne die Einschaltung des «Trustcenter» nicht offenbart werden. Anschliessend befasste sich die Konferenz mit der Überwachungstätigkeit der nationalen Kontrollbehörden und mit den Klageverfahren. Ferner wurde über gemeinsame Umfragen Spaniens und der Niederlande bei Internet Service Providern berichtet; Frankreich präsentierte eine Studie zur Privatsphäre-Politik der auf den E-Commerce spezialisierten Dienstleistungsanbieter. Die Zusammenarbeit unter nationalen Datenschutzbehörden muss offensichtlich noch verstärkt werden. Ausserdem sind Normen zur Kontrolldurchführung und zur Förderung des Austausches unter den Kontrollbehörden zu ergreifen. Die Konferenz befasste sich mit der Frage, welches Recht bei Streitigkeiten im Rahmen der Bearbeitung von Personendaten im Internet anwendbar sei. Dazu sollte ein integrierter europäischer Ansatz über den Schutz von Online-Daten eingeführt werden (siehe http://europa.eu.int/comm/internal_market/de/media/dataprot/wpdocs/index.htm). Wichtig ist auch, die Gestaltung von Informatikmaterial und Software mit datenschutzkonformer Verwendung zu fördern. Frankreich schlug die Einführung eines europäisches Datenschutz-Labels vor; es könnte an alle Sites vergeben werden, die sich verpflichten, Internet-Benutzer über ihre Rechte zu unterrichten und die in der europäischen Richtlinie verankerten Garantien umzusetzen. Denkbar wäre auch die Schaffung einer europäischen Kontrollbehörde, welche die von den Berufsorganisationen ausgestellten Labels prüft (siehe dazu auch S. 19). Schliesslich zog die Konferenz Bilanz zum Stand der Umsetzung der europäischen Richtlinie in den Mitgliedsstaaten. Der Vertreter der Europäischen Kommission unterstrich nachdrücklich die Bedeutung des Harmonisierungsziels; wie er betonte, legt die Richtlinie klare Voraussetzungen fest, die den nationalen Gesetzgebungen nur einen beschränkten Handlungsspielraum belassen. Die Kommission wird die Lage untersuchen und überprüfen, ob die Zielsetzung der Freizügigkeit unter den Mitgliedsstaaten erreicht wurde und ob die nationalen Gesetzgebungen nach wie vor Unterschiede aufweisen.

5. OECD

- Arbeitsgruppe über die Informationssicherheit und Schutz der Privatsphäre (WISP)

Die Arbeitsgruppe hat sich im vergangenen Geschäftsjahr mit der Finalisierung des Generators für die automatisierte Erstellung von Datenbearbeitungserklärungen im Internet beschäftigt. Daneben suchte sie nach Lösungen, wie in der Zukunft die Privatsphäre im Internet besser geschützt werden kann und nahm die Aktualisierung der Inventare über Authentifizierungsverfahren und Kryptografie an die Hand. Schliesslich entschied sie, mit der Arbeitsgruppe über Genetik zusammenzuarbeiten.

Der Generator für die automatisierte Erstellung von Datenbearbeitungserklärungen im Internet wurde finalisiert und über das Internet allen interessierten Kreisen zur Verfügung gestellt (http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm). Ein direkter Link ist auf der Seite des EDSB in der Rubrik «News and Links» zu finden. Mit Hilfe des Generators können nun Dienstleistungsanbieter im Internet einfacher eine Datenbearbeitungserklärung – eine sogenannte «Privacy Policy» – verfassen und so insbesondere die Bearbeitung von Kundendaten transparent gestalten (detaillierte Informationen zum Generator finden sich auch im 7. Tätigkeitsbericht, 1999/2000, S. 95).

Angesichts des noch mangelnden Vertrauens der Benutzer und Konsumenten in den E-Commerce hat die Arbeitsgruppe konkrete Massnahmen zur Vertrauensbildung vorgeschlagen. So wurde beschlossen, ein Inventar von allen technischen Mitteln, die die Privatsphäre im Internet schützen, zu erstellen. Gleichzeitig entschied sich die Arbeitsgruppe für die Organisierung einer Konferenz über alternative Streitbeilegungsmechanismen im E-Commerce. Die Konferenz fand am 11. und 12. Dezember 2000 in Den Haag statt (Einzelheiten zur Konferenz sind auf S. 94 zu finden).

In den Bereichen Authentifizierungsverfahren und Kryptografie entschied die Arbeitsgruppe, die bestehenden Inventare zu aktualisieren, um diese den aktuellen Entwicklungen anzupassen. Erwähnenswert ist, dass eine starke Lockerung der Exportkontrollen für Kryptografieprodukte zu verzeichnen ist. Sowohl die USA als auch Frankreich haben den Marktzugang zu Kryptoprodukten stark liberalisiert. Allerdings möchte Frankreich weiterhin an Lösungen arbeiten, die den Zugang und Zugriff von Ermittlungsbehörden auf chiffrierte Dokumente gewährleisten. Im französischen Parlament wird an einem Kryptografiegesetz gearbeitet, das den Zugriff von Ermittlungsbehörden regelt. Die Idee besteht darin, dass es als Indiz zu Lasten des Beschuldigten betrachtet wird, wenn dieser in einem Verfahren den Text oder den Schlüssel nicht herausgibt.

Wir werden diese Entwicklung aufmerksam verfolgen, um zu sehen, ob nebst dem durch einen Untersuchungsrichter gewährten Zugriff – was der schweizerischen Praxis entspricht – auch polizeiliche Behörden ohne richterlichen Entscheid Zugriff erhalten.

Verhaltensregeln, die als Alternative zu Gesetzen für den Schutz der Privatsphäre gelten, werden von der Arbeitsgruppe gesammelt und ausgewertet. Ziel ist deren Wirksamkeit genauer zu analysieren. Wir haben allerdings festgehalten, dass Verhaltensregeln keine Alternative zu gesetzlichen Bestimmungen sind, wenn sie die Privatsphäre nicht wirksam schützen können (siehe dazu auch 6. Tätigkeitsbericht 1998/1999, S. 128). Verhaltensregeln können jedoch in bestimmten Branchen dazu beitragen, gesetzliche Verpflichtungen transparenter umzusetzen.

Die Bedeutung der Bearbeitung von genetischen Daten im Zusammenhang mit dem Schutz der Privatsphäre wurde erkannt. Deshalb entschied die Arbeitsgruppe, sich intensiv auch mit dieser Thematik zu befassen um dabei mit der dafür verantwortlichen Arbeitsgruppe zusammenzuarbeiten.

- Alternative Mechanismen zur Konfliktlösung im Umfeld von Online-Transaktionen – Konferenz in Den Haag

Am 11./12. Dezember 2000 fand in Den Haag eine Konferenz der OECD über Mechanismen zur Streitbeilegung zwischen Unternehmen und Konsumenten im Umfeld von Online-Transaktionen statt. Während der Konferenz wurden verschiedene Modelle zur Beilegung von Konflikten und Streitigkeiten in der vernetzen Welt vorgestellt. Es wurde erkannt, dass gemeinsame Kriterien notwendig sind, um die Online-Streitbeilegung weltweit effektiv zu gestalten. Dafür braucht es eine gemeinsame Politik, die mittels einer effektiven und gerechten Online-Streitbeilegung das Vertrauen der Konsumenten in den E-Commerce steigern soll.

Da die heutigen nationalen Gesetze und Regulierungen für Online-Streitigkeiten in der Regel die Grenze ihrer Effektivität an der Staatsgrenze finden, müssen Lösungen gesucht werden, die globale beziehungsweise internationale Wirksamkeit entwickeln können. Es wurde erkannt, dass E-Commerce-Transaktionen das Vertrauern der Konsumenten noch nicht haben, weil insbesondere keine globalen Systeme für die internationale Beilegung von Streitigkeiten existieren. Auch beim Schutz der Privatsphäre stellt sich die gleiche Problematik, denn es fehlen auch hier weitgehend internationale Kriterien, insbesondere für die Beilegung von Streitigkeiten bei Verletzungen der Privatsphäre. Hinzu

kommt, dass die rapide Vermehrung von Verhaltensregeln im E-Commerce für Verwirrung sorgen und dementsprechend auch das Vertrauen der Konsumenten beeinflussen.

Im Hinblick auf die weltweite Stärkung des Vertrauens der Konsumenten in den E-Commerce ist es deshalb wichtig, dass Konfliktlösungsmechanismen an die unterschiedlichen kulturellen Aspekte und an die Bedürfnisse der Konsumenten angepasst werden. Zudem sind auch die verschiedenen Rechtssysteme zu berücksichtigen. Es wird jedoch nicht möglich sein, die verschiedenen Rechtssysteme und -kulturen unter einen weltweit gemeinsamen Nenner zu bringen. Deshalb ist es um so wichtiger, Brücken zwischen den verschiedenen Systemen zu bauen, damit Konsumenten und Unternehmen, wie bei traditionellen Handelstransaktionen, die Möglichkeit haben, Streitigkeiten sinnvoll und effektiv beilegen zu können.

Ein wichtiger Aspekt, der aber oft übersehen wird, ist die Sprache. Es muss dafür gesorgt werden, dass die Sprachbarriere die Effizienz der alternativen Streitbeilegung nicht von Vornherein zunichte macht. Deshalb muss gewährleistet werden, dass sich Konsumenten in ihrer eigenen Sprache beschweren können. Neben dem sprachlichen Aspekt müssen auch die kulturellen Besonderheiten und Werte im Streit berücksichtigt werden. Schliesslich müssen auch die Unternehmen, die im Internet Mechanismen zur Online-Streitbeilegung anbieten, die Konsumenten über die Bedingungen und die Anwendung informieren.

Für den erfolgreichen Einsatz von alternativen Mechanismen zur Online-Streitbeilegung müssen insbesondere folgende Kriterien erfüllt sein:

- Untersuchung und Bewertung aller bereits bestehender Streitbeilegungsmechanismen
- Festlegung von gemeinsamen internationalen Kriterien zur Beilegung von Online-Streitigkeiten
- Transparente Gestaltung der Prozesse
- Einfache Zugänglichkeit der Systeme für die Konsumenten
- Berücksichtigung der verschiedenen kulturellen und sprachlichen Aspekte
- Gewährleistung der Unabhängigkeit bei der Beurteilung von Streitfällen
- Ordentlicher Rechtsweg muss für Streitparteien offen bleiben

In der Zukunft soll jedes Unternehmen, das Dienstleistungen über das Internet anbietet, auch online aussergerichtliche Konfliktlösungsmöglichkeiten anbieten. Der Konsument ist klar und transparent über diese Konfliktlösungsmöglichkeit zu informieren. Für diesen Aspekt der Information wird die Lösung des sprachlichen Problems von entscheidender Bedeutung sein.

Unbestritten ist, dass alternative Möglichkeiten zur Online-Konfliktlösung nicht die geltende Rechtsordnung ersetzen werden. Sie bilden lediglich eine Alternative zur Streitbeilegung, um nicht den beschwerlichen Rechtsweg gehen zu müssen. Anderer Meinung sind Vertreter der US-Wirtschaft, die mittels solcher Streitbeilegungsmechanismen den ordentlichen Rechtsweg gerne ausschliessen würden. Dies würde jedoch auf internationaler Ebene das Vertrauen der Konsumenten in den E-Commerce nicht stärken.

Die EU-Kommission hat angekündigt, dass sie Kriterien für die Anerkennung von alternativen Mechanismen zur Online-Streitbeilegung erlassen werde. Das Ziel ist, soweit als möglich den langwierigen ordentlichen Prozessweg zu vermeiden. Die EU möchte in drei bis vier Jahren software «intelligent agents» entwickeln, die sowohl für den Schutz der Privatsphäre als auch für alternative Konfliktlösungsmechanismen eine Lösungsvariante bilden werden.

Auf jeden Fall darf man nicht aus den Augen verlieren, dass bei Streitigkeiten in der Geschäftswelt der menschliche Kontakt weiterhin eine wichtige Rolle spielt.

6. Safe Harbor Prinzip – Erster Schritt zum Schutz der Privatsphäre in den USA

Nach gut zweijährigen Verhandlungen haben sich im Juli 2000 die EU und die USA grundsätzlich über gemeinsame Standards für den Schutz der Privatsphäre geeinigt. Dieses Abkommen soll den Austausch von grenzüberschreitenden Informationen ermöglichen und so den E-Commerce erleichtern. Obwohl über dieses Abkommen einige wichtige Anforderungen für den Schutz der Privatsphäre (wie Informations- und Widerspruchsrecht des Bürgers) Anwendung finden, ist abzuwarten, ob dieses Abkommen tatsächlich die erhoffte Wirksamkeit entfalten wird.

Mit dem Konzept des Safe Harbor (sicherer Hafen) verpflichten sich US-Unternehmen selbst, einige europäische Datenschutzanforderungen einzuhalten. Allerdings ist das «Einlaufen» im sicheren Hafen freiwillig, d.h. es findet nur auf diese US-Unternehmen Anwendung, die sich in die dafür vom US-Handelsministerium geschaffene öffentliche Liste, (siehe http://export.gov/safeharbor/) eingetragen haben. Dadurch gehen die eingetragenen Unternehmen bindende rechtliche Verpflichtungen ein. Das US-Handelsministerium überwacht die Einhaltung der Prinzipien und es gibt rechtliche Konsequenzen für fehlbare Unternehmen.

Europäische Konsumenten haben ein Recht von einem Unternehmen, das sich dem Safe Harbor Prinzip unterworfen hat, zu wissen, ob und an welche Dritte Personendaten übermittelt werden, was dem europäischen Auskunftsrecht gleichkommt. Zudem dürfen sensible Personendaten nur mit ausdrücklichem Einverständnis der Betroffenen an Dritte weitergegeben werden. Die Einhaltung dieser Anforderungen soll jährlich vom Handelsministerium überprüft werden.

Obwohl mit der Einführung der Safe Harbor Prinzipien ein erster Schritt in die richtige Richtung gemacht wurde, bleibt abzuwarten, ob dadurch auch die Privatsphäre effektiv geschützt wird. Festzuhalten ist insbesondere die Tatsache, dass die Prinzipien des Safe Harbor nicht allen europäischen gesetzlichen Anforderungen genügen und lediglich Grundprinzipien wie die Information und die Zustimmung des Betroffenen berücksichtigen. Zudem sind die Prinzipien des Safe Harbor nicht zwingende Bestimmungen. Unternehmen können sich den Prinzipien freiwillig unterwerfen. Bisher haben sich (Stand Jan. 2001) nur ein Dutzend Unternehmen registrieren lassen. Somit haben die Safe Harbor Prinzipien auf die Mehrheit der US-Unternehmen keine Wirkung.

Aus diesen Gründen empfehlen wir schweizerischen Unternehmen bei der Übermittlung von Personendaten in der USA weiterhin auf der Grundlage von Einzelverträgen den Schutz der übermittelten Daten zu gewähren.

7. EUROPOL-Übereinkommen

Im Meinungsaustausch zu den Voraussetzungen für die Verhandlungen, die auf den Abschluss von Kooperationsabkommen zwischen Europol und bestimmten Drittstaaten abzielen, empfing das Bundesamt für Polizei zwei Europol-Vertreter zu einem Besuch in Bern. Wir wurden ebenfalls zu diesem Treffen eingeladen. Dabei vermittelten wir einen Überblick über die schweizerischen Gesetze und Gepflogenheiten im Datenschutz und hoben vor allem diejenigen Datenschutzaspekte hervor, welche im Hinblick auf künftige Verhandlungen noch untersucht werden müssen.

Das Europäische Polizeiamt Europol wurde durch die im Jahr 1995 von den fünfzehn Mitgliedsstaaten der Europäischen Union abgeschlossene gleichnamige Konvention gegründet. Europol verfolgt das Ziel, die zuständigen Dienststellen der Mitgliedsstaaten effizienter zu gestalten und die Zusammenarbeit vor allem in der Prävention und Bekämpfung des Terrorismus, im illegalen Betäubungsmittelhandel und anderen Formen der internationalen Schwerkriminalität zu verbessern. Zur Erfüllung seiner Aufgaben hat Europol ein Informationssystem eingerichtet, in das die Polizeidienststellen der Mitglieds-

staaten ihre Informationen direkt eingeben. Das Europol-Übereinkommen sieht sehr strenge Vorschriften zur Führung des informatisierten Systems vor. Eine Fülle von Bestimmungen regelt ausserdem den Datenschutz (Schutzniveau, Datenbearbeitung, Zugriffsrechte, Kontrollbehörden, Datensicherheit, ...).

Nach den Informationen des Integrationsbüros und des Bundesamtes für Polizei (BAP) hat der Ministerrat der Europäischen Union im März 2000 eine Entscheidung verabschiedet, welche den Europol-Direktor zur Aufnahme von Verhandlungen zwecks Abschluss von Zusammenarbeitsabkommen mit bestimmten Drittstaaten und -organisationen ermächtigt. Die Entscheidung an sich betrifft im Augenblick nur technische oder strategische Abkommen. Für den Austausch von Personendaten ist ein operatives Abkommen erforderlich, das ein schwerfälligeres Verfahren voraussetzt: Europol müsste dazu einen Bericht über die Gesetzgebung und Verwaltungspraxis des betroffenen Drittstaates im Datenschutzbereich erstellen. Die datenschutzrechtlichen Belange spielen in den Verhandlungen zwischen Europol und Drittstaaten dann auch eine Schlüsselrolle. Beinhaltet die Zusammenarbeit mit einem Drittstaat den Austausch von Personendaten, so ist sie nur dann möglich, wenn die Gesetze und die Praxis des fraglichen Staates den Auflagen des Europol-Übereinkommens sowie der sekundären Gesetzgebung über Datenschutz und -sicherheit genügen.

Im August 2000 empfing das BAP in Bern zwei Vertreter von Europol, die beauftragt sind, die Lage in der Schweiz zu überprüfen und einen Bericht über die Informatiksysteme des BAP und über den Datenschutz zu verfassen. Wir wurden eingeladen, an der Begegnung teilzunehmen, und erläuterten die verschiedenen Kompetenzen, die uns das Bundesgesetz über den Datenschutz erteilt. Ausserdem bezogen wir Stellung zur Angemessenheit der schweizerischen Gesetzgebung angesichts der von Europol eingeführten Datenschutzanforderungen.

Wie wir betonten, erfüllt die Schweiz in bezug auf die einzuführenden Gesetzesnormen die von Europol vorgeschriebenen Kriterien. Zu erwähnen ist insbesondere die Ratifizierung des Übereinkommens Nr. 108 des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und die Annahme der Empfehlung des Europarates R(87) 15 über die Verwendung von personenbezogenen Daten im Polizeibereich. Ausserdem erinnerten wir an die bereits existierenden Bundes- und Kantonsgesetze über den Datenschutz, an die Einrichtung unabhängiger Datenschutzkontrollstellen auf Bundes- und Kantonsebene, an die Ausarbeitung formalgesetzlicher Vorschriften über die Informatiksysteme der Polizei sowie an die Entscheidung der Kommission der Europäischen Union, welche die schweizerische Datenschutzgesetzgebung als angemessen anerkannte.

Als Kontrollorgan betonten wir indessen, dass wir im Augenblick keine Gewähr für einwandfreie Verhältnisse im Datenschutz geben konnten, zumal wir nicht ausreichend detailliert über die ergriffenen Massnahmen bzw. den Stand der Fortschritte in den Verhandlungen zwischen dem BAP und Europol Bescheid wissen. Tatsächlich gilt es noch zahlreiche praktische Punkte zu prüfen, beispielsweise die Informatiksysteme der betroffenen Polizeistellen, die Modalitäten der Ausübung der Zugriffsrechte oder die Kompetenzverteilung unter den Datenschutz-Kontrollstellen.

Wir ersuchten das BAP, uns regelmässig über den Stand und die Fortschritte möglicher Verhandlungen zu unterrichten. Ausserdem wurde vereinbart, dass wir den Vertretern von Europol für sämtliche Fragen zum Datenschutz zur Verfügung stehen würden.

8. Datenschutz im Kosovo

Im Rahmen der OSZE-Mission im Kosovo war ein Mitarbeiter des EDSB vor Ort als Datenschutzbeauftragter tätig. Aus Sicht des Datenschutzes standen vor allem Datensicherheitsfragen im Vordergrund. Im Wesentlichen ging es darum, dass die Personendaten der verschiedenen Volksgruppen im Kosovo nicht in falsche Hände gerieten.

Sowohl die UNO als auch die OSZE waren im letzten Jahr damit beschäftigt, die Bevölkerung im Kosovo zu registrieren. Dies war vor allem nötig, weil ein Teil der Zivilstandsdaten im Krieg entweder gestohlen oder vernichtet wurde. Die Registrierung der Bevölkerung bildete auch die Grundlage für die im Herbst 2000 stattgefundenen Gemeindewahlen. Die Rechtsnormen der UNO sowie die Europäische Menschenrechtskonvention (EMRK) bildeten die Rechtsgrundlage für die Tätigkeit als Datenschutzbeauftragter im Kosovo.

Aus datenschutzrechtlicher Sicht sind grundsätzlich alle Personendaten im Kosovo als besonders schützenswert einzustufen. Denn in aller Regel geben schon Namen klare Hinweise auf die dort lebenden Volksgruppen (Kosovo-Albaner, Serben, Türken etc.). Mit anderen Worten ist bereits eine Adressliste im Kosovo als sensitiv zu bezeichnen.

Insbesondere mussten die Daten der im Kosovo lebenden Minderheiten, die sich registrieren lassen wollten, geschützt werden, denn die Lage zwischen den einzelnen Ethnien war und ist immer noch sehr angespannt. Im Vordergrund stand hier, v.a. die geeigneten technischen und organisatorischen Massnahmen zu treffen (Zugriffskontrolle, Zugangskontrolle, Transportkontrolle etc.). Wichtig war, den ganzen Prozess der Registrierung auf allfällige Sicherheitslücken zu

untersuchen. Zudem wurden die Mitarbeiter der OSZE und der UNO auf die Sensibilität der Daten aufmerksam gemacht.

Im Rahmen der Registrierung wurden sehr viele Personendaten gesammelt. Insbesondere verlangte man von jedem Gesuchsteller einen Fingerabdruck, damit eine doppelte Registrierung nicht möglich war. Hier ging es darum, diejenigen Personendaten, welche für den Zweck der Registrierung nicht mehr benötigt wurden, der Vernichtung zuzuführen (Prinzip der Verhältnismässigkeit). Leider wurde dies nicht überall berücksichtigt.

Während der Wahlperiode mussten vor allem die Daten von denjenigen Personen geschützt werden, die in der Regel einer ethnischen Minderheit angehörten und an den anstehenden Gemeindewahlen teilnehmen wollten. Diese Leute hatten z. T. Angst, ihre Wahlzettel in einer Wahllokalität abzugeben. Es musste daher ein Prozedere ausgearbeitet werden, damit sie zu Hause wählen konnten.

Schliesslich wurde ein Entwurf für ein Datenschutzgesetz für den ganzen Kosovo geschaffen. Der Gesetzesentwurf enthält die wesentlichen europäischen Datenschutzstandards und umfasst die Datenbearbeitung durch die ganze Verwaltung im Kosovo. Ein Gesetz, welches die Persönlichkeitsrechte der Einwohner im Kosovo schützt, ist unabdingbar. Es ist zu hoffen, dass dieses Projekt seine Fortsetzung findet.

IV. DER EIDGENÖSSISCHE DATENSCHUTZBEAUFTRAGTE

1. Publikationen des EDSB – Neuerscheinungen

- Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz

- Ablaufschema über die Voraussetzungen und den korrekten Verlauf der Internet- und E-Mail-Überwachung am Arbeitsplatz

- Merkblatt über die Videoüberwachung durch private Personen

Das Ablaufschema und das Merkblatt sind am Anhang dieses Berichtes zu finden (Seite 113 und 114) und können auch auf der Website www.edsb.ch konsultiert werden.

- Infoblatt des EDSB 2/2000
- Infoblatt des EDSB 1/2001

Die Infoblätter sind auf der Website (www.edsb.ch) zu finden.

2. Statistik über die Tätigkeit des Eidgenössischen Datenschutzbeauftragten Zeitraum 1. April 2000 bis 31. März 2001

Konferenzteilnahmen:

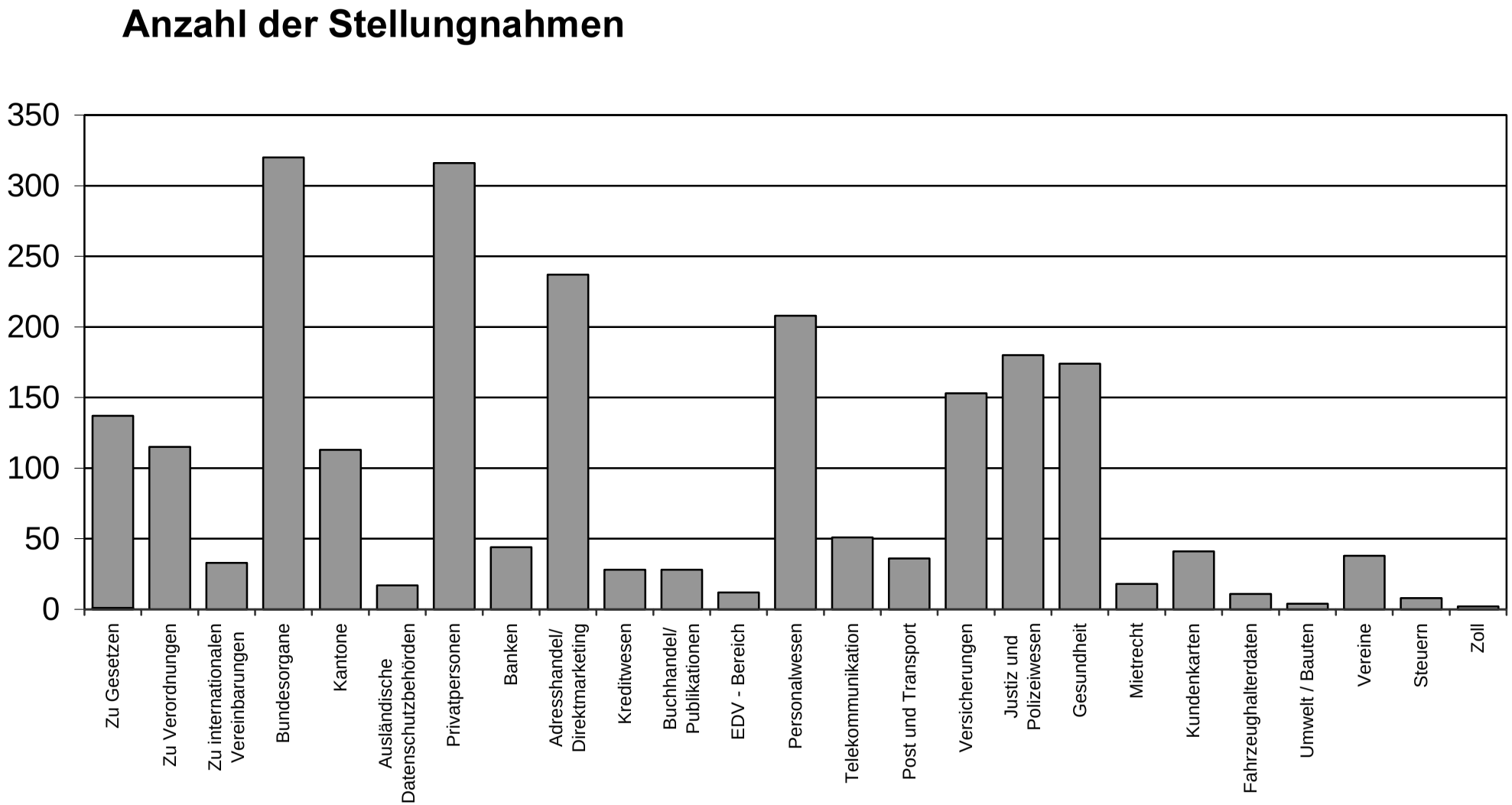
National	International
25	18

Anzahl von Sitzungen

	Bund	Private	Kantone
Intern	293	115	19
Extern	143	75	29
Total	436	190	48

Anzahl der Stellungnahmen

	Eingänge	Schriftliche Stellungnahmen	Empfehlungen des EDSB	Keine Einwendungen
Zu Gesetzen	67	61		9
Zu Verordnungen	52	42		21
Zu internationalen Vereinbarungen	18	9		6
Anfragen aus dem öffentlichen Bereich:				
Bundesorgane	180	136		4
Kantone	61	52		
Ausländische Datenschutzbehörden	10	7		
Anfragen aus dem privaten Bereich:				
Privatpersonen	181	133	2	
Banken	22	19		3
Adresshandel/Direktmarketing	129	108		
Kreditwesen	16	12		
Buchhandel/Publikationen	15	13		
EDV - Bereich	6	6		
Personalwesen	4	204		
Telekommunikation	49	2		
Post und Transport	18	18		
Versicherungen	82	71		
Justiz und Polizeiwesen	91	88	1	
Gesundheit	94	80		
Mietrecht	9	9		
Kundenkarten	21	20		
Fahrzeughalterdaten	5	5	1	
Umwelt / Bauten	2	2		
Vereine	22	16		
Steuern	4	4		
Zoll	1	1		
Total	1159	1118	4	43

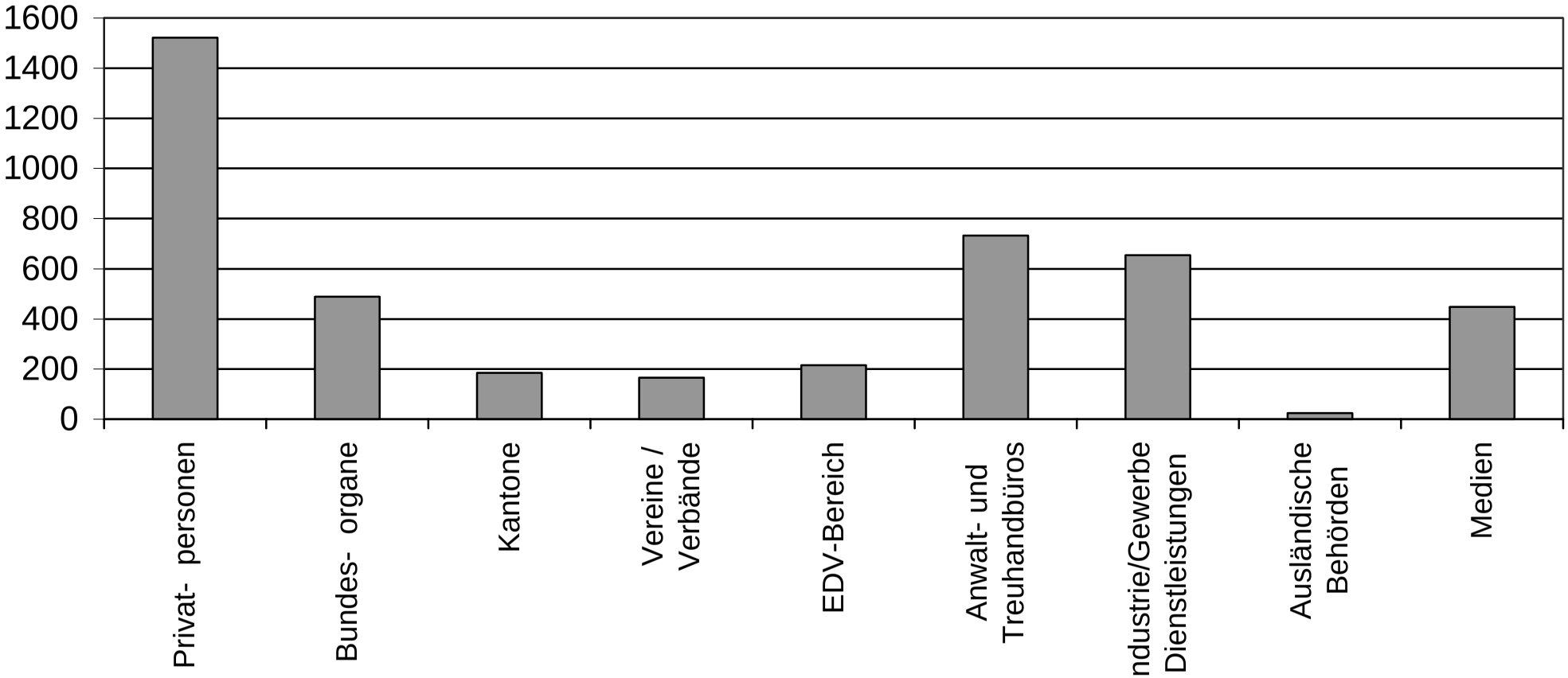

Anzahl der Stellungnahmen
350
300
250
200
150
100
50
0
Zu Gesetzen
Zu Verordnungen
Zu internationalen Vereinbarungen
Bundesorgane
Kantone
Ausländische Datenschutzbehörden
Privatpersonen
Banken
Adresshandel/ Direktmarketing
Kreditwesen
Buchhandel/ Publikationen
EDV - Bereich
Personalwesen
Telekommunikation
Post und Transport
Versicherungen
Justiz und Polizeiwesen
Gesundheit
Mietrecht
Kundenkarten
Fahrzeughalterdaten
Umwelt / Bauten
Vereine
Steuern
Zoll

TELEFONAUSKUNFT

	Privatpersonen	Bundesorgane	Kantone	Vereine / Verbände	EDV-Bereich	Anwalt- und Treuhandbüros	Industrie / Gewerbe / Dienstleistungen	Ausländische Behörden	Medien
Datenschutz allgemein	218	151	38	20	10	131	61	1	68
Auskunftsrecht	108	22	10	21		8	1		7
Anmeldung Datensammlungen	62	16	1	8		47	11		
Datenbekanntgabe	86	19	5	30	5	81	107		42
Übermittlungen ins Ausland	59			7	25	118	61	1	10
Kompatibilität mit E.U. Länder	15	12	4	3	19	57	52	1	21
Arbeitsbereich / Arbeitsvermittlung	237	36	16	1	39	96	154	12	53
Gesundheit / Versicherungen/	307	97	47	2	43	63	16	1	15
Mietrecht / Mietformulare	12			1					
Marketing direkt Werbung	53	2		23	9	8	19	1	29
Banken/Kreditkarten Kreditauskünfte	71	2		7		24	22		33
Statistik	32	18	30			1	11	3	34
Fahrzeughalter Register	3		1					1	2
Videoüberwachung Bildmaterial	30	7	6		10	3	12	1	37
Telefon-Daten	63	3	2	10	4	36	30	2	21
INTERNET	79	15	7	16	8	19	37		30
Datensicherheit Kryptografie	30	29	6	9	25	10	23		14
Polizeiwesen	40	23	11			6			6
Zoll	1	7	1						
Ausländer / Asyl.	3	18		7					1
Steuern	4								
Militär	5	3							
E-Commerce	2	1		1	18	25	38		10
DNA Genetik	2	8							15
Total	1522	489	185	166	215	733	655	24	448

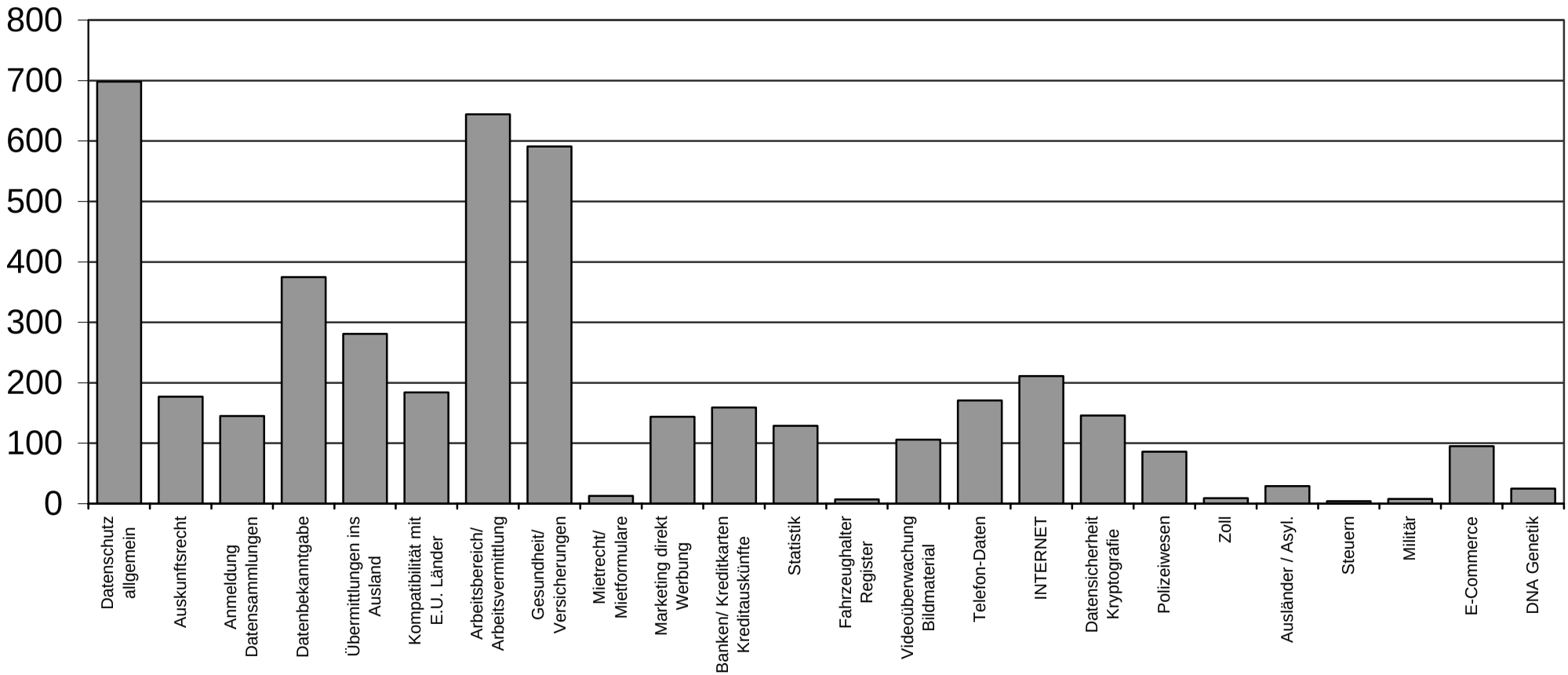
Telefonauskunft

nach Anfragenden



Telefonauskunft

nach Sachgebiet



3. 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.
Informations- und Pressedienst	Eggli Liliane, lic. phil. Tsiraktsopulos Kosmas, lic. iur.
Rechtsdienst:	8 Personen
Informatikdienst:	3 Personen
Kanzlei:	3 Personen

V. ANHANG

1. Entscheid der EU-Kommission zur Angemessenheit des Schutzes personenbezogener Daten in der Schweiz

II

(Nicht veröffentlichungsbedürftige Rechtsakte)

KOMMISSION

ENTSCHEIDUNG DER KOMMISSION

vom 26. Juli 2000

gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz

(Bekannt gegeben unter Aktenzeichen K(2000) 2304)

(Text von Bedeutung für den EWR)

(2000/518/EG)

DIE KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [1], insbesondere auf Artikel 25 Absatz 6,

in Erwägung nachstehender Gründe:

(1) Gemäß der Richtlinie 95/46/EG haben die Mitgliedstaaten vorzusehen, dass die Übermittlung personenbezogener Daten in ein Drittland nur zulässig ist, wenn dieses Drittland vor der Übermittlung ein angemessenes Schutzniveau gewährleistet und die einzelstaatlichen Rechtsvorschriften zur Umsetzung anderer Bestimmungen der Richtlinie beachtet werden.

(2) Die Kommission kann feststellen, dass ein Drittland ein angemessenes Schutzniveau gewährleistet. In diesem Fall können personenbezogene Daten aus den Mitgliedstaaten übermittelt werden, ohne dass zusätzliche Garantien erforderlich sind.

(3) Gemäß der Richtlinie 95/46/EG sollte die Angemessenheit des Schutzniveaus unter Berücksichtigung aller Umstände, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen, und im Hinblick auf die gegebenen Bedingungen beur- teilt werden. Die durch die Richtlinie eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten hat Leitlinien für solche Bewertungen erstellt [2].

(4) Angesichts der verschiedenen Ansätze von Drittländern im Bereich Datenschutz sollte die Beurteilung der Angemessenheit bzw. die Durchsetzung jeder Entscheidung gemäß

[1] ABl. L 281 vom 23.11.1995, S. 31.

[2] Stellungnahme 12/98 der Datenschutzgruppe vom 24. Juli 1998: Übermittlungen personenbezogener Daten an Drittländer. Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU (GD MARKT D/5025/98), verfügbar auf der Website http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

Artikel 25 Absatz 6 der Richtlinie 95/46/EG in einer Form erfolgen, die gegen Drittländer bzw. unter Drittländern, in denen gleiche Bedingungen vorherrschen, nicht willkürlich oder ungerechtfertigt diskriminierend wirkt und unter Berücksichtigung der bestehenden Verpflichtungen der Gemeinschaft kein verstecktes Handelshemmnis darstellt.

(5) Die Schweizerische Eidgenossenschaft verfügt auf Bundes- wie auch auf kantonaler Ebene über verbindliche Rechtsnormen zum Schutz personenbezogener Daten.

(6) Gemäß der am 18. April 1999 durch Volksabstimmung geänderten Bundesverfassung, die am 1. Januar 2000 in Kraft getreten ist, hat jede Person Anspruch auf die Achtung ihrer Privatsphäre und insbesondere auf den Schutz vor Missbrauch der sie betreffenden Daten. Das Bundesgericht hat in seiner Rechtsprechung bereits auf Basis der früheren Verfassung, die keine derartige Bestimmung enthielt, allgemeine Grundsätze für die Verarbeitung personenbezogener Daten entwickelt. Diese beziehen sich vor allem auf die Qualität der verarbeiteten Daten, das Auskunftsrecht der betroffenen Personen und das Recht, die Berichtigung oder Vernichtung der Daten zu verlangen. Diese Grundsätze sind sowohl für den Bund als auch für die Kantone bindend.

(7) Das schweizerische Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 ist am 1. Juli 1993 in Kraft getreten. Durchführungsvorschriften zu einigen Bestimmungen dieses Gesetzes, insbesondere über das Auskunftsrecht der betroffenen Personen, die Anmeldung der Datensammlungen bei einer unabhängigen Kontrollinstanz oder die Übermittlung der Daten ins Ausland, wurden in Verordnungen des Bundesrates geregelt. Das Gesetz gilt für die Bearbeitung personenbezogener Daten durch Bundesorgane, durch den gesamten privaten Sektor sowie durch kantonale Stellen in Erfüllung des Bundesrechts, sofern die Kantone auf diese Datenbearbeitung nicht kantonale Datenschutzbestimmungen anwenden.

(8) Die meisten Kantone haben datenschutzrechtliche Vorschriften für ihren Zuständigkeitsbereich erlassen, die insbesondere öffentliche Krankenhäuser, den Bildungssektor, direkte Steuern der Kantone und die Polizei betreffen. In den übrigen Kantonen wird der Schutz durch Ordnungsvorschriften gewährleistet oder es gelten die in der kantonalen Rechtsprechung festgelegten Grundsätze. Ungeachtet von Herkunft und Inhalt der kantonalen Bestimmungen, aber auch wenn keine derartigen Bestimmungen vorliegen, sind die Grundsätze der Verfassung einzuhalten. In ihrem Zuständigkeitsbereich können die Kantonalbehörden veranlasst werden, personenbezogene Daten an Behörden von Nachbarländern zu übermitteln, hauptsächlich zur Wahrung wichtiger öffentlicher Interessen oder, im Fall öffentlicher Krankenhäuser, zur Wahrung lebenswichtiger Interessen der betroffenen Personen.

(9) Die Schweiz hat am 2. Oktober 1997 das Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108)[3] ratifiziert, mit dem der Schutzpersonenbezogener Daten gestärkt und der freie Verkehr zwischen den Vertragsparteien, vorbehaltlich der Ausnahmen, die diese vorsehen können, sichergestellt werden soll. Das Übereinkommen ist zwar nicht direkt anwendbar, enthält jedoch internationale Verpflichtungen für den Bund und die Kantone. Diese Verpflichtungen betreffen sowohl die Grundsätze des Datenschutzes, die jede Vertragspartei in ihrem innerstaatlichen Recht zu verwirklichen hat, als auch Vorkehrungen zur Zusammenarbeit zwischen den Vertragsparteien. Insbesondere müssen die schweizerischen Behörden den Behörden der übrigen Vertragsparteien auf Ersuchen Auskünfte über Recht und Verwaltungspraxis im Bereich des Datenschutzes sowie Sachauskünfte über eine bestimmte automatische Verarbeitung erteilen. Zudem

[3] Verfügbar auf der Website http://conventions.coe.int/treaty/EN/cadreintro.htm.

haben sie jede im Ausland wohnende Person bei der Ausübung der ihr zustehenden Rechte zu unterstützen, wenn diese Auskünfte darüber verlangt, ob personenbezogene Daten über sie verarbeitet werden, sich diese Daten mitteilen lassen und sie gegebenenfalls berichtigen oder löschen lassen will und wenn sie einen Rechtsbehelf einlegen will.

(10) Die in der Schweiz geltenden Rechtsvorschriften berücksichtigen alle Grundsätze, die notwendig sind, damit ein ausreichender Schutz für natürliche Personen gegeben ist, obwohl sie auch Ausnahmen und Einschränkungen zur Wahrung wichtiger öffentlicher Interessen vorsehen. Um die Anwendung dieser Vorschriften zu garantieren, stehen Rechtsbehelfe zur Verfügung, und unabhängige Stellen, wie der mit Untersuchungs- und Eingriffskompetenzen ausgestattete eidgenössische Datenschutzbeauftragte, stellen die Überwachung sicher. Im Übrigen sind die Bestimmungen des schweizerischen Rechts über die zivilrechtliche Haftung anzuwenden, wenn durch die unerlaubte Verarbeitung ein Schaden verursacht wurde.

(11) Im Interesse der Transparenz und der Gewährleistung der Fähigkeit der zuständigen einzelstaatlichen Behörden, den Schutz von Personen bei der Verarbeitung ihrer personenbezogenen Daten zu gewährleisten, ist es ungeachtet der Feststellung eines angemessenen Schutzniveaus notwendig, in dieser Entscheidung die besonderen Umstände zu nennen, unter denen die Aussetzung bestimmter Datenströme gerechtfertigt ist.

(12) Die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten hat zu dem von dem schweizerischen Recht gewährten Schutzniveau Stellungnahmen abgegeben, die bei der Ausarbeitung der vorliegenden Entscheidung berücksichtigt wurden [4].

(13) Die in dieser Entscheidung vorgesehenen Maßnahmen entsprechen der Stellungnahme des durch Artikel 31 der Richtlinie 95/46/EG eingesetzten Ausschusses —

HAT FOLGENDE ENTSCHEIDUNG ERLASSEN:

Artikel 1

Es wird festgestellt, dass die Schweiz für sämtliche unter die Richtlinie 95/46/EG fallenden Tätigkeiten ein im Sinne des Artikels 25 Absatz 2 der genannten Richtlinie angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die aus der Gemeinschaft übermittelt werden.

Artikel 2

Die vorliegende Entscheidung betrifft nur die Angemessenheit des Schutzes, der in der Schweiz gewährt wird, um die Anforderungen des Artikels 25 Absatz 1 der Richtlinie 95/46/EG zu erfüllen und lässt die Anwendung anderer Bestimmungen der Richtlinie, die sich auf die Verarbeitung personenbezogener Daten in den Mitgliedstaaten beziehen, unberührt.

Artikel 3

(1) Ungeachtet ihrer Befugnisse, tätig zu werden, um die Einhaltung einzelstaatlicher Vorschriften, die gemäß anderen Bestimmungen als den des Artikels 25 der Richtlinie 95/46/EG angenommen wurden, zu gewährleisten, können die zuständigen Behörden in den Mitgliedstaaten ihre bestehenden Befugnisse ausüben, zum Schutz von Privatpersonen bei der Verarbeitung ihrer personenbezogenen Daten die Datenübermittlung an einen Empfänger in der Schweiz auszusetzen, wenn

[4]) Stellungnahme 5/99 der Datenschutzgruppe vom 7. Juni 1999 (GD MARKT 5054/99), verfügbar auf der in Fußnote 2 genannten Website.

a) eine zuständige Schweizer Behörde feststellt, dass der Datenempfänger die geltenden Datenschutzvorschriften nicht einhält oder

b) eine hohe Wahrscheinlichkeit besteht, dass die Schutzvorschriften verletzt werden; wenn Grund zur Annahme besteht, dass die zuständige Schweizer Behörde nicht rechtzeitig angemessene Maßnahmen ergreift bzw. ergreifen wird, um den Fall zu lösen; wenn die fortgesetzte Datenübermittlung den betroffenen Personen einen nicht wieder gutzumachenden Schaden zufügen würde, und wenn die zuständigen Behörden in den Mitgliedstaaten ihre Mitteilungspflichten gegenüber der für die Verarbeitung in der Schweiz zuständigen Stelle unter den gegebenen Umständen in angemessener Weise erfüllt und dieser Gelegenheit zur Stellungnahme gegeben haben.

Die Aussetzung ist zu beenden, sobald sichergestellt ist, dass die Vorschriften befolgt werden und die zuständige Behörde in der Gemeinschaft davon in Kenntnis gesetzt ist.

(2) Die Mitgliedstaaten informieren die Kommission unverzüglich, wenn Maßnahmen gemäß Absatz 1 ergriffen wurden.

(3) Die Mitgliedstaaten und die Kommission informieren einander auch über Fälle, bei denen die Maßnahmen der für die Einhaltung der Vorschriften in der Schweiz verantwortlichen Einrichtungen nicht ausreichen, um die Einhaltung zu gewährleisten.

(4) Ergeben die Informationen nach den Absätzen 1, 2 und 3, dass eine der für die Einhaltung der Vorschriften in der Schweiz verantwortlichen Einrichtungen ihrer Aufgabe nicht wirkungsvoll nachkommt, so informiert die Kommission die zuständige Schweizer Behörde und schlägt, wenn nötig, gemäß dem Verfahren von Artikel 31 der Richtlinie 95/46/EG im Hinblick auf eine Aufhebung oder Aussetzung dieser Entscheidung entsprechende Maßnahmen vor.

Artikel 4

(1) Diese Entscheidung kann jederzeit im Licht der Erfahrungen mit ihrer Anwendung oder aufgrund von Änderungen der Schweizer Rechtsvorschriften angepasst werden. Die Kommission nimmt drei Jahre, nachdem sie die Mitgliedstaaten von dieser Entscheidung in Kenntnis gesetzt hat, anhand der verfügbaren Informationen eine Bewertung ihrer Anwendung vor und unterrichtet den nach Artikel 31 der Richtlinie 95/46/EG eingesetzten Ausschuss über ihre Feststellungen, einschließlich sämtlicher Erkenntnisse, die die Beurteilung in Artikel 1 dieser Entscheidung, wonach die Schweiz ein angemessenes Schutzniveau im Sinne von Artikel 25 der Richtlinie 95/46/EG bietet, berühren könnten, sowie etwaiger Belege dafür, dass die Entscheidung in diskriminierender Weise angewandt wird.

(2) Die Kommission legt erforderlichenfalls gemäß dem Verfahren von Artikel 31 der Richtlinie 95/46/EG Vorschläge für Maßnahmen vor.

Artikel 5

Die Mitgliedstaaten ergreifen binnen 90 Tagen, nachdem sie von der Veröffentlichung der Entscheidung in Kenntnis gesetzt worden sind, alle für ihre Umsetzung erforderlichen Maßnahmen.

Artikel 6

Diese Entscheidung ist an alle Mitgliedstaaten gerichtet.

Brüssel, den 26. Juli 2000

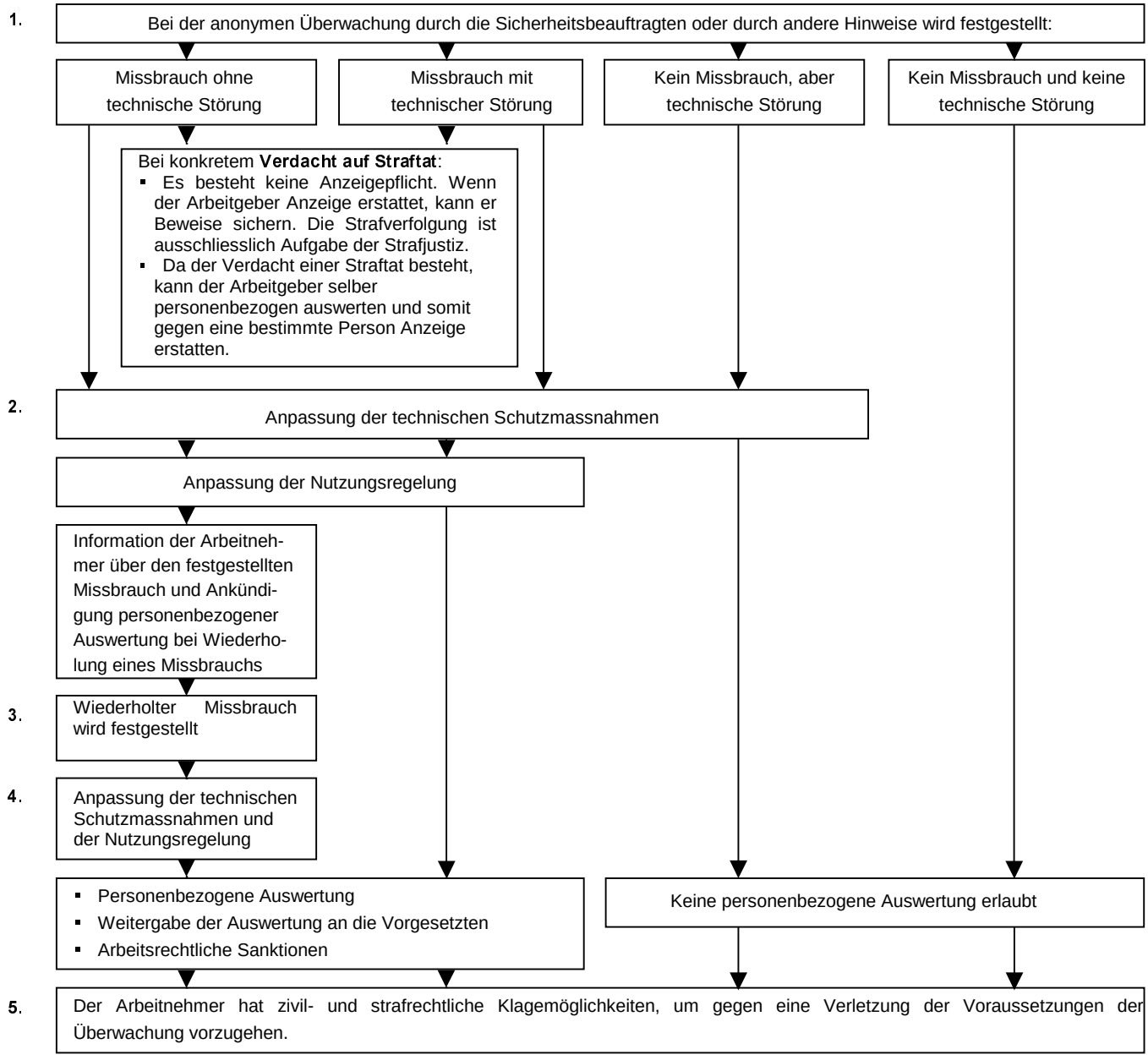
Für die Kommission
Frederik BOLKESTEIN
Mitglied der Kommission

2. Ablaufdiagramm E-Mail- und Internetüberwachung am Arbeitsplatz

A. DIE VORAUSSETZUNGEN DER ÜBERWACHUNG

1. Der Arbeitgeber setzt technische Schutzmassnahmen wie Antivirusprogramme, Firewalls, Diskquotas, Backups usw. ein. Der Einsatz von sogenannten Spionprogrammen beim Benutzer ist verboten. Der Arbeitgeber bestimmt die einzusetzenden Protokollierungen und sorgt dafür, dass einzig der Sicherheitsbeauftragte bei Bedarf darauf Zugriff hat.
2. Der Arbeitgeber informiert die Arbeitnehmerschaft über folgende Punkte:
   - Eingesetzte **technische Schutzmassnahmen** und bestehende Protokollierungen
   - **Nutzungsregelung**
     Dies ist eine schriftliche Weisung, die besagt, ob und wie die Benutzung von E-Mail und Internet erlaubt ist. Eine solche Regelung ist empfehlenswert, da sie Klarheit schafft.
   - **Überwachung**
     Die Sicherheitsbeauftragten führen laufend anonyme Überwachungen der technischen Ressourcen (intrusion and abuse detection) durch und können die Einhaltung der Nutzungsregelung stichprobenweise anonym überprüfen. Ein Missbrauch muss jedoch festgestellt werden, bevor der Arbeitgeber die Protokollierungen personenbezogen auswerten darf. Ein solcher liegt dann vor, wenn gegen die Nutzungsregelung oder gegen die Treuepflicht bzw. gegen die Verhältnismässigkeit verstossen wird. Damit personenbezogen ausgewertet werden darf, ist zudem ein schriftliches Überwachungsreglement zwingend. Darin sind auch die Bekanntgabe der Auswertungen an die Vorgesetzten und die Sanktionen geregelt.
     N.B. - Die Überwachung des E-Mail-Gebrauchs ist von der Technik her immer personenbezogen und nur aufgrund der Vertraulichkeitsangaben (privat, persönlich, vertraulich) oder der Adressierungselemente erlaubt. Wenn die Natur des E-Mails unklar bleibt, muss die betroffene Person gefragt werden.
     - Die Protokollierung der durch die technischen Schutzmassnahmen verhinderten Operationen werden nicht personenbezogen ausgewertet.

B. DER ABLAUF DER ÜBERWACHUNG



3. Merkblatt über die Videoüberwachung durch private Personen

Der Eidgenössische Datenschutz- beauftragte informiert:

MERKBLATT ÜBER DIE VIDEOÜBERWACHUNG DURCH PRIVATE PERSONEN

Wenn private Personen Videokameras einsetzen, beispielsweise um Personen zu schützen oder Sachbeschädigungen zu verhindern, so untersteht dies dem Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG; SR 235.1), wenn sich die gefilmten Bilder auf bestimmte oder bestimmbare Personen beziehen. Dies gilt unabhängig davon, ob die Bilder aufbewahrt werden oder nicht. Die vorgenommenen Bearbeitungen der Bilder – wie Erfassen, Bekanntgeben, unmittelbares oder nachträgliches Anschauen oder Aufbewahren – müssen die allgemeinen Grundsätze des Datenschutzes einhalten.

Dieses Merkblatt betrifft die Videoüberwachung durch private Personen an privaten Örtlichkeiten, egal ob diese öffentlich zugänglich sind oder nicht. Dieses gilt nicht für die Videoüberwachung am Arbeitsplatz. Dazu finden Sie Informationen im 4. Tätigkeitsbericht des Eidgenössischen Datenschutzbeauftragten, Kapitel I, 4.2.

Videoüberwachungssysteme sind nur erlaubt, wenn die folgenden zwei Bedingungen erfüllt sind:

1. Die Videoüberwachung darf nur eingesetzt werden, wenn dieser Eingriff in die Persönlichkeit durch die Zustimmung der betroffenen Personen, durch ein überwiegendes öffentliches oder privates Interesse oder durch ein Gesetz gerechtfertigt ist *(Rechtmässigkeitsprinzip)*.

   Beispiel: Ein Bijouteriebesitzer hat ein privates Interesse daran, dass während seiner Abwesenheit kein Einbruch begangen wird.

2. Die Videoüberwachung muss geeignet und notwendig sein, um den verfolgten Zweck der Sicherheit, insbesondere den Schutz von Personen und/oder Sachen, zu erreichen. Sie darf nur angewendet werden, wenn sich andere Massnahmen, die das Privatleben weniger beeinträchtigen, wie zusätzliche Verriegelungen, Verstärkungen der Eingangstüren oder Alarmsysteme als ungenügend oder undurchführbar erweisen *(Verhältnismässigkeitsprinzip)*.

   Beispiel: Videokameras in einer Einstellhalle sind im Allgemeinen erlaubt, da sie Vandalismus verhindern können.

Die Anforderungen an den Aufbau und Einsatz einer Videoüberwachung sind im einzelnen auf der Rückseite zusammengefasst.

Weitere Informationen zum Datenschutz finden Sie unter www.edsb.ch oder wenden Sie sich bitte direkt an den Eidgenössischen Datenschutzbeauftragten, 3003 Bern, Tel. 031 322 43 95, Fax. 031 325 99 96, info@edsb.ch

Beim Einsatz und Aufbau eines Videoüberwachungssystems müssen die folgenden Regeln eingehalten werden:

1. Die für die Videoüberwachung Verantwortlichen müssen alle Personen, die das Aufnahmefeld der Kameras betreten, mit einem gut sichtbaren Hinweisschild über das Überwachungssystem informieren. Sind die aufgenommenen Bilder mit einer Datensammlung verbunden, muss auch angegeben sein, bei wem das Auskunftsrecht geltend gemacht werden kann, falls sich dies nicht aus den Umständen ergibt. *(Prinzip von Treu und Glauben sowie Auskunftsrecht)*

   Beispiel: Beim Eingang zu einem Mehrfamilienhaus muss das Hinweisschild für jede eintretende Person gut ersichtlich sein.

2. Die verantwortliche Person muss die Personendaten durch angemessene technische und organisatorische Massnahmen vor jeglichem unbefugten Bearbeiten schützen. *(Datensicherheit)*

   Beispiel: Nur berechtigte Personen dürfen die Bildschirme sehen können. Die gespeicherten Daten müssen in einem sicheren, verriegelten Raum aufbewahrt werden, zu dem nur berechtigte Personen den Schlüssel haben.

3. Die Videokamera muss so aufgestellt werden, dass nur die für den verfolgten Zweck absolut notwendigen Bilder in ihrem Aufnahmefeld erscheinen. *(Verhältnismässigkeitsprinzip)*

   Beispiel: Bei einer Überwachung in einem Mehrfamilienhaus darf nicht ersichtlich sein, wer in welche Wohnung eintritt.

4. Die Daten dürfen nur für den Schutz von Personen und Sachen benutzt werden, nicht für andere Zwecke. *(Zweckbindungsprinzip)*

   Beispiel: Ein Verkaufsgeschäft darf Sicherheitsaufnahmen nicht für Marketingzwecke verwenden.

5. Die aufgenommenen Personendaten dürfen nicht bekannt gegeben werden, ausser in den durch das Gesetz vorgesehenen oder erlaubten Fällen, z. B. bei einer von einem Richter stammenden Anfrage. *(Zweckbindungsprinzip)*

   Beispiel: Das Verkaufsgeschäft darf die aufgenommenen Bilder weder an Dritte weitergeben noch -verkaufen.

6. Die mit einer Kamera aufgenommenen Bilder müssen innert kürzester Zeit gelöscht werden. Sachbeschädigungen oder Personenverletzungen werden im Normalfall sofort oder innerhalb von wenigen Stunden festgestellt. Eine Frist von 24 Stunden erscheint angesichts des verfolgten Zwecks als genügend, sofern innerhalb dieses Zeitraums keine nennenswerten Ereignisse entdeckt werden. Bei der Videoüberwachung in privaten Räumen, die nicht öffentlich zugänglich sind, kann diese Frist in gewissen Fällen länger sein.
   (Verhältnismässigkeitsprinzip)

   Beispiel: Bei einer Ferienabwesenheit können Aufnahmen ausnahmsweise länger aufbewahrt werden, müssen aber nach der Rückkehr der verantwortlichen Person so bald wie möglich gelöscht werden.

4. Empfehlungen des EDSB
4.1. Empfehlung in Sachen Absenz-Management

Bern, den 7. Dezember 2000

EMPFEHLUNG

gemäss

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

in Sachen

ABSENZ-MANAGEMENT (CD-ROM CORPORATE WELLNESS) DER SWICA

I. Der Eidg. Datenschutzbeauftragte stellt fest:

1. Der Eidg. Datenschutzbeauftragte (EDSB) wurde im April 2000 auf die Produktion und Vertrieb einer CD-ROM « Absenzmanager » der Gesundheitsorganisation SWICA informiert.
2. Aus den bestehenden Unterlagen sowie aus dem Briefwechsel zwischen EDSB und SWICA hat sich insb. ergeben, dass die CD-ROM die systematische Erfassung von Personendaten wie Name, Vorname, Nationalität, Abwesenheitsgrund, Arzttyp, Diagnose, Bemerkungen, usw. durch den Arbeitgeber und die Auswertung nach Kriterien wie Nationalität, Arzt oder Diagnose (siehe dazu z. B. S. 8 Booklett) bzw. nach festgelegten Zielwerten (Zeitbudget für Krankheiten) ermöglicht. Ausserdem sieht die CD-ROM die Möglichkeit des Datenaustausches mit anderen Datenbanken vor. Die CD-ROM ist nach Angaben der SWICA als Kontrollinstrument des Arbeitgebers über die Abwesenheiten seiner Angestellten konzipiert und soll sowohl den Gesundheitsschutz fördern als auch die Abwesenheiten am Arbeitsplatz reduzieren.
3. Für den EDSB ist die CD-ROM als Gesundheitsmassnahme nicht geeignet. Ausserdem stellt die CD-ROM eine unverhältnismässige und unzweckmässige Datenbearbeitung dar, da der Arbeitgeber die systematisch erfassten Gesundheitsdaten (Diagnose, behandelnder Arzt) zur Durchführung des Arbeitsvertrages nicht braucht (vgl. Schreiben des EDSB vom 31.08.2000). Im übrigen ist die vorgesehene Datenbearbeitung auch deswegen unzulässig, weil die Gesundheitsdaten mit weiteren Personendaten (z. B. die Nationalität) kombiniert und verglichen werden können. Daraus können nach Meinung des EDSB diskriminierende Rückschlüsse gezogen werden. Die systematische Erfassung anderer Abwesenheitsgründe durch den Arbeitgeber (z. B. Ferien, Militär, usw.) wird vom EDSB nicht beanstandet.
4. Die SWICA vertritt im Wesentlichen die Auffassung, dass der Arbeitgeber berechtigt ist, Krankheitsdiagnosen systematisch zu bearbeiten. Gesundheitsdaten seien für den Arbeitgeber auch deswegen wichtig, weil Letzterer über die Weiterbeschäftigung eines kranken Mitarbeiters entscheidet. Ein Datenaustausch mit Datenbanken der SWICA finde in der Praxis nicht statt. Die SWICA behauptet ausserdem, die systematische Erfassung von Gesundheitsdaten sei gegenüber gesundheitlich schwächeren Mitarbeiter nicht diskriminierend, da gerade für solche Angestellten individuelle Krankheitsbudgets geschaffen werden.

II. Der EDSB zieht in Erwägung:

1. Bei der Datenbeschaffung ist der Arbeitgeber am Verhältnismässigkeits- und Zweckmässigkeitsprinzip gebunden (Art. 328b OR). Die durch die fragliche CD-ROM erfassten Daten (u.a. Arztdiagnose, Arzttyp) stellen besonders schützenswerte Personendaten dar. Nach dem Verhältnismässigkeitsprinzip ist es insb. unzulässig, dass der Arbeitgeber bzw. sein Personaldienst Arztdiagnosen systematisch erfasst. Diese sind weder zur Schaffung von Massnahmen der Gesundheitsprävention noch zur Absenzenbewirtschaftung notwendig. Solche besonders schützenswerte Personendaten dürfen per Definition nur durch Personen bearbeitet werden, die dem Arztgeheimnis unterstehen. Einzelfallweise, sofern dies zur Abklärung einer speziellen Sachlage erforderlich ist, kann ein Arbeitgeber bzw. die Abteilung Sicherheits- und Gesundheitsprävention des Unternehmens oder der Unternehmensgruppe Kenntnis über die Ursachen einer Krankheit einer bestimmten Person erlangen. Bagatellfälle (z. B. Grippe) werden vom Arbeitnehmer dem Arbeitgeber meistens bekannt gegeben. Die systematische Erfassung dieser Daten entbehrt jedoch eines Rechtfertigungsgrundes. Ohne ausdrückliche Einwilligung des Patienten darf der Arbeitgeber vom Arzt nur einen Arztbefund bekommen (”krank” oder ”geeignet/ungeeignet” für eine Stelle). Zulässig ist hingegen die Erfassung der Anzahl Absenztage wegen Krankheit (ohne Spezifikationen).
2. Das Festhalten eines jährlichen Budgets an Krankheitstage ist ebenso unzulässig, weil dadurch gesundheitlich schwächerer Menschen, die öfters abwesend sind, diskriminiert werden können. Die Behauptung der SWICA, die fragliche Datenbearbeitung sei gegenüber gesundheitlich schwächeren Angestellten nicht diskriminierend, weil für solche Angestellten individuelle Krankheitsbudgets geschaffen werden können, widerspricht der in der Einführung des Bookletts zur CD-ROM festgehaltenen Zielsetzung der Reduktion der Absenzen. Die vorgesehene Datenbearbeitung ist aber auch deswegen unzulässig, weil Gesundheitsdaten mit weiteren besonders schützenswerten Personendaten wie die Nationalität kombiniert und verglichen werden können. Daraus können auch rassendiskriminierende Rückschlüsse gezogen werden.
3. Die CD-ROM ist auch als Massnahme der Gesundheitsprävention zu beanstanden. Wie wir es bereits in unserer Stellungnahme vom 31. August 2000 festgehalten haben, verpflichtet die Gesundheitsprävention (Art. 328 OR) den Arbeitgeber, Massnahmen zu treffen, um Gefahren für die Gesundheit der Arbeitnehmer vorzubeugen. Arbeitsräume, Systeme und Maschinen sind so zu unterhalten, dass deren Benutzung keine Folgen auf die Gesundheit der Arbeitnehmer haben können. Die Erfassung von Informationen über ”Schwachstellen” im Unternehmen (z. B. Luftzug, gefährliche Substanzen, Rauchen, schlechte Bildschirme, usw.) erfolgt anonym, aufgrund statistischer Angaben (Verhältnismässigkeitsprinzip, Art. 4 Abs. 2 Datenschutzgesetz, DSG, SR 235.1, vgl. dazu auch die auf dem UVG basierende Richtlinie 6508 zur Sicherheits- und Gesundheitsprävention der Eidg. Koordinationskommission für Arbeitssicherheit). Nur in Ausnahmefällen, sofern es zur Abklärung einer speziellen Sachlage erforderlich ist, darf der Arbeitgeber bzw. die Abteilung Sicherheits- und Gesundheitsprävention des Unternehmens oder der Unternehmensgruppe mit betroffenen Personen Kontakt aufnehmen. Bei der in Frage stehenden CD-ROM handelt es sich hingegen u. a. um ein Programm zur systematischen, personenbezogenen Erfassung und Auswertung von Gesundheitsdaten. Die Kenntnis des Bestehens einer personenbezogenen, systematischen Auswertung des Absenzverhaltens könnte dank der bearbeiteten Daten und deren Kombinationen (u. a. Diagnose, Nationalität) und der daraus resultierenden, möglichen Diskriminierungen, einen psychischen Druck auf die Arbeitnehmer ausüben, welcher mit dem ursprünglichen Zweck, nämlich der Gesundheitsprävention, in Widerspruch steht. Gemäss Art. 26 Abs. 2

der Gesundheitsvorsorgeverordnung 3 zum Arbeitsgesetz (SR 822.113) sind aber Überwachungssysteme so zu gestalten, dass die Gesundheit und die Bewegungsfreiheit dadurch nicht beeinträchtigt werden. Gegen das Bestehen einer gesundheitspräventiven Wirkung der CD-ROM sprechen im übrigen auch die Erläuterungen im Booklett, wonach es sich bei der CD-ROM vielmehr um eine reine Absenzenkontrolle handelt. Fehlt bei einer Massnahme der Gesundheitsprävention die gesundheitspräventive Wirkung oder ist Erstere nicht mit dem übrigen Recht vereinbar, ist von ihrer Anwendung abzusehen (weil es u. E. nicht Aufgabe einer Gesundheitsorganisation ist, Absenzkontrollsysteme für Arbeitgeber zu schaffen), oder ist rechtskonform zu gestalten.

4. Für die Datenbearbeitung durch private Personen sind Rechtfertigungsgründe nötig (Art. 13 DSG). Weder die Einwilligung der betroffenen Personen, noch eine gesetzliche Grundlage, noch ein überwiegendes privates oder öffentliches Interesse ist für den Datenaustausch zwischen Absenz-Datenbank und andere Datenbanken gegeben. Ohne Rechtfertigungsgrund stellt eine solche Datenbekanntgabe im übrigen eine gravierende Verletzung des Berufsgeheimnisses seitens des Arbeitgebers dar. Die Behauptung der SWICA, ein Datenaustausch zwischen ihr und dem Arbeitgeber finde nicht statt, mag zwar in der Tat richtig sein, sie ändert aber an der Tatsache nichts, dass bereits die technische Möglichkeit eines solchen Datenaustausches gesetzeswidrig ist.

III. Aufgrund dieser Erwägungen empfiehlt der Eidg. Datenschutzbeauftragte:

1. Die Produktion und der Vertrieb der fraglichen CD-ROM ist unverzüglich einzustellen und die bereits verteilten CD-ROM zurückzuziehen, oder die Datenkategorien ”Diagnose”, ”Arzttyp”, ”Absenzenbudget” und ”Bemerkungen” von der CD-ROM zu entfernen sowie die Kategorie ”Absenzen wegen Politik oder Vereinsmitgliedschaft” durch ”Absenzen privat” zu ersetzen.
2. Die SWICA benachrichtigt den Eidg. Datenschutzbeauftragten innerhalb von dreissig Tagen seit Erhalt der Empfehlung, ob Sie die Empfehlung annimmt oder nicht. Wird die Empfehlung abgelehnt oder stellt der Eidg. Datenschutzbeauftragte nach Ablauf der Frist fest, dass sie nicht eingehalten wird, so kann er die Angelegenheit gemäss Art. 29 DSG der Eidg. Datenschutzkommission zum Entscheid vorlegen.

DER EIDGENÖSSISCHE
DATENSCHUTZBEAUFTRAGTE
Der Beauftragte:

O. Guntern

4.2. Empfehlung in Sachen Nachsendeauftrag der Post

3003 Bern, 19. Februar 2001

EMPFEHLUNG

gemäss

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

in Sachen

Nachsendeauftrag der Schweizerischen Post

I. Der Eidg. Datenschutzbeauftragte stellt fest:

1. Die Schweizerische Post bietet ihren Kundinnen und Kunden den sog. Nachsendeauftrag (Formular 01 «Nachsendeauftrag für Postsendungen / Wohnungswechsel») an. Nach einem Wohnungswechsel werden die Postsendungen, die noch an die ehemalige Anschrift adressiert werden, an das neue Domizil geleitet.
2. Die Schweizerische Post bietet zusammen mit der Firma DCL Data Care AG einen Adressaktualisierungsdienst mit der Bezeichnung «MAT[CH]move» an. Mit Hilfe einer Umzugsdatenbank können Dritte ihre Adressbestände auf den neusten Stand bringen lassen. Insbesondere Firmen nutzen MAT[CH]move, um ihren Kundenstamm aktuell zu halten. Die Adressaktualisierung wird jedem Interessenten angeboten, unabhängig davon ob er eine Postsendung zu verschicken beabsichtigt.
3. Die Umzugsdatenbank wird mit den Angaben des unter Punkt 1 genannten Formulars gespiesen, welches die Umziehenden ausfüllen.
4. In den Formularen, die bis Ende 2000 verwendet wurden, war die Untersagungsmöglichkeit der Adressaktualisierung für Dritte nicht erwähnt. Der Eidg. Datenschutzbeauftragte (EDSB) hat bei der Schweizerische Post wiederholt in dieser Sache interveniert. Nach einer Anzahl von Sitzungen und Briefwechseln mit der Schweizerischen Post, hat der EDSB am 10. November 2000 Änderungsvorschläge zu den Postformularentwürfen gemacht, die die Post dem EDSB am 2. November 2000 zugestellt hatte:

   «Wir schlagen Ihnen beispielsweise folgende Formulierung vor: Darf Ihre neue Postadresse einem Dritten, der bereits im Besitz Ihrer alten Adresse ist, zur Verfügung gestellt werden (Adressaktualisierung) ? Ja/Nein »

   Der EDSB hat sich ebenfalls zu den Tarifen geäussert. Er verlangte, dass die Tarife die freie Wahl der Kundinnen und Kunden, die Adressaktualisierung für die Dritte zu erlauben oder zu untersagen, nicht beeinflussen.

   Am 27. Dezember 2000 hat die Post dem EDSB die definitiven Formulare (gültig ab 1. Januar 2001 / siehe Punkt 5 unten) zur Information zugestellt, die nur einen Teil der Forderungen des EDSB berücksichtigen.

   Am 10. Januar 2001 hat der EDSB von der Post Erklärungen über noch hängige Punkte verlangt (Zugänglichmachung der Daten via das Internet-Portal «Yellowworld» der Post). Des Weiteren hat der EDSB erneut die unpräzisen Formulierungen des Formulars bzw. des Merkblattes kritisiert und Änderungsvorschläge gemacht.

   Am 23. Januar 2001 antwortete die Post dem EDSB, dass sichergestellt ist, dass inskünftig keine Daten aus den Formularen via Yellowworld-E-Mailverzeichnis abrufbar sind. Zu den Änderungsvorschlägen des EDSB schrieb die Post lediglich: *«Ihre Vorschläge für*

eine Änderung der Formulare und des Merkblattes werden wir bei der nächsten Auflage eingehend prüfen und gegebenenfalls einfliessen lassen».

5. Ab dem 1. Januar 2001 hat die Schweizerische Post ihr neues Formular eingeführt, das die Untersagungsmöglichkeit der Adressaktualisierung für Dritte wie folgt erwähnt: *«Darf dem Absender, der noch über Ihre alte Adresse verfügt, die neue Postadresse bekannt gegeben werden ? o Ja o Nein».*
6. Kundinnen und Kunden, die «Ja» wählen, bezahlen den bisherigen Tarif von Fr. 10.- für die Nachsendung der Post während eines Jahres. Wer «Nein» ankreuzt, also eine Adressaktualisierung für Dritte untersagt, hat einen erhöhten Tarif zu bezahlen, nämlich Fr. 20.- pro Monat (also Fr. 240.- pro Jahr). Auf ein Jahr gerechnet entspricht dies dem vierundzwanzigfachen Preis (bzw. einer Steigerung um 2'300 %).

II. Der Eidg. Datenschutzbeauftragte zieht in Erwägung:

1. Die Adressaktualisierung stellt eine Bearbeitung von Personendaten im Sinne des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (DSG, SR 235.1) dar, woraus sich die Legitimation des EDSB zum Erlass einer Empfehlung gemäss Art. 27 Abs. 4 DSG ergibt.
2. Gemäss Art. 13 des Postgesetzes vom 30. April 1997 (PG, SR 783.0) gelten für das Bearbeiten von Personendaten durch die Post die Artikel 12–15 DSG. Die Aufsicht richtet sich nach den Bestimmungen für Bundesorgane (Art. 23 Abs. 2 DSG).
3. Ausgehend vom verfassungsmässig garantierten Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten (Art. 13 Abs. 2 Bundesverfassung) muss jede Person die Herrschaft über die sie betreffenden Informationen ausüben und eine Bearbeitung dieser Daten durch Dritte einschränken können (informationelles Selbstbestimmungsrecht; vgl. BUNTSCHU, in Maurer/Vogt (Hrsg.), Kommentar zum Schweizerischen Datenschutzgesetz, Art. 1, N 14 ff.)
4. Ohne transparente Information durch die Postformulare (inkl. Merkblätter) wird das informationelle Selbstbestimmungsrecht tangiert. Die Tarife müssen so festgelegt sein, dass sie die freie Entscheidung der betroffenen Personen nicht beeinflussen. Daraus folgt:

   4.1. Im **Formular** 01 (212.09) wird vom «Absender» gesprochen, dem die neue Adresse bekannt gegeben werden soll. Der Postkunde nimmt daher an, dass bereits eine Sendung aufgegeben ist oder dies mindestens beabsichtigt wird. Die Adressaktualisierung wird jedoch allen Interessierten angeboten unabhängig davon, ob sie eine Postsendung aufgegeben haben oder sie eine Aktualisierung aus völlig andern Gründen wünschen. Die Formulierung ist daher intransparent und irreführend. Deshalb muss «Darf *dem Absender*, der *noch* über Ihre alte Adresse verfügt ...» z.B. durch «Darf *einer Person*, die über Ihre alte Adresse verfügt ...» ersetzt werden.

   Im **Merkblatt** 212.09.1 zum Formular 01 wird unter «X Ja» erwähnt: «Ihre Adresse wird in keinem Fall an Dritte verkauft oder vermietet, sondern lediglich zur Aktualisierung bestehender Adressdatenbanken verwendet». Unter «X Nein» steht: «Ihre Adresse wird nicht an Dritte weitergegeben». Diese Darstellung gibt dem Kunden den Anschein, die Auswahl habe einen Einfluss auf eine allfällige Bekanntgabe an Dritte, die nicht über die alte Adresse verfügen. Wie die Schweizerischen Post dem EDSB versichert hat, findet weder bei «X Ja» noch bei «X Nein» eine Weitergabe an Dritte statt. Der Eindruck, dass die Post mit verwirrlichen Formulierungen versucht, den Kunden zum Ankreuzen des «X Ja» zu bewegen, kann nicht ganz von der Hand gewiesen werden. Daher muss eine verständliche Aussage (z.B. «Einer Person, die nicht über Ihre alte Adresse verfügt, geben wir keine Ihrer Adressen bekannt») in den ersten Abschnitt des Merkblattes (gültig für «X Ja» und «X Nein») eingefügt werden.

Aussagen über Weitergabe, Verkauf oder Vermietung unter den Titeln «X Ja» und «X Nein» sind zu streichen.

4.2. Die **Preisdifferenz** zwischen den zwei Varianten (Zustimmung oder Untersagung der Adressaktualisierung für Dritte) ist derart hoch, dass sie das informationelle Selbstbestimmungsrecht der betroffenen Personen verletzt. Um die freie Entscheidung der Postkundinnen und –kunden nicht zu beeinflussen, wäre es anzustreben, dass beide Varianten gleich viel kosten. Wer eine Adressaktualisierung für Dritte untersagt, wird die meisten regelmässigen Absender direkt über seine neue Adresse informieren. Trotzdem wird in den meisten Fällen die Anzahl der fehlgeleiteten Sendungen höher sein und damit auch höhere Kosten für die Post verursachen. Daher kommt ein moderater Preisunterschied in Frage, konkret akzeptiert der EDSB maximal die Erhebung des doppelten Preises, falls die Adressaktualisierung für Dritte nicht akzeptiert wird. Beispielsweise (pro Jahr) Fr. 10.- mit Aktualisierung für Dritte und Fr. 20.- ohne Aktualisierung für Dritte.

Der EDSB weist zusätzlich darauf hin, dass es aus der Sicht des Datenschutzes wünschbar wäre, die Untersagung einer Datenbearbeitung (Ausübung des datenschutzrechtlichen Abwehrrechtes) kostenlos anzubieten, wie dies beispielsweise die Deutsche Post AG tut (kostenlose ähnliche Nachsendedienstleistung, mit oder ohne Untersagung einer Adressaktualisierung). Betreffend die Kostenlosigkeit der Ausübung der datenschutzrechtlichen Abwehrrechte siehe auch das Urteil der Eidg. Datenschutzkommission vom 12. März 1999 (ISDN-Rufnummerunterdrückung) in VPB 64.73.

III. Aufgrund dieser Erwägungen empfiehlt der Eidg. Datenschutzbeauftragte:

1. Die Schweizerische Post passt die in II. 4.1. erwähnten missverständlichen Formulierungen (**Formular** 01 und dem dazugehörigen **Merkblatt**) im Sinne des Vorschlages des EDSB umgehend an.
2. Die Schweizerische Post ändert Ihre **Tarife** folgendermassen: Kundinnen und Kunden, die eine Adressaktualisierung für Dritte untersagen, bezahlen für den Nachsendeauftrag für dieselbe Zeitspanne maximal den doppelten Preis gegenüber denjenigen, welche die Adressaktualisierung für Dritte erlauben.
3. Denjenigen Kundinnen und Kunden, die seit dem 1. Januar 2001 einen Nachsendeauftrag ohne Adressaktualisierung erteilt haben, ist der zuviel bezahlte Betrag zurückzuerstatten.
4. Die Schweizerische Post teilt dem Eidg. Datenschutzbeauftragten bis zum 23. März 2001 mit, ob sie diese Empfehlung annimmt oder ablehnt. Wird diese Empfehlung nicht befolgt oder abgelehnt, so kann der Eidg. Datenschutzbeauftragte die Angelegenheit dem Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) zum Entscheid vorlegen. Der Entscheid wird den betroffenen Personen mitgeteilt.
5. Diese Empfehlung wird gemäss Art. 30 Abs. 2 DSG veröffentlicht.
6. Diese Empfehlung wird der Schweizerischen Post sowie dem Generalsekretariat des UVEK mitgeteilt.

DER EIDGENÖSSISCHE DATENSCHUTZBEAUFTRAGTE
Der Beauftragte:

O. Guntern

4.3. Empfehlung in Sachen Drogentests in der Lehre

Bern, den 22. Februar 2001

EMPFEHLUNG

gemäss

Art. 29 Abs. 3 des Bundesgesetzes über den Datenschutz (DSG, SR 235.1)

in Sachen

Drogentests in der Lehre bei Hoffmann-La Roche AG

I. Der Eidg. Datenschutzbeauftragte (EDSB) stellt fest:

1. 1999 sind wir von verschiedenen Seiten auf die Drogentests bei der Hoffmann-La Roche AG aufmerksam gemacht worden. Den entsprechenden Angaben zufolge führt die genannte Firma sowohl bei der Rekrutierung als auch während der gesamten Lehre stichprobenartige Drogentests durch. Mit Schreiben vom 22. Dezember 1999 sind wir an die genannte Firma gelangt und haben von Ihr die Beantwortung von Fragen in Zusammenhang mit der Rechtmässigkeit von Drogentests verlangt. Wir haben uns insb. über Zweck, Freiwilligkeit, Testbedingungen, gesetzliche Grundlagen und Folgen der Verweigerung solcher Tests erkundigen wollen.
2. Mit Schreiben vom 17. Januar 2000 hat die Hoffmann-La Roche AG zu den gestellten Fragen Stellung genommen. Das Drogenkonzept wird im wesentlichen mit dem Bestreben gerechtfertigt, den Auszubildenden eine drogenfreie Lehrzeit anzubieten sowie die Sicherheit und den Gesundheitsschutz an allen Arbeitsplätzen zu gewährleisten. Die Drogentests finden bei der ärztlichen Eignungsuntersuchung im Rahmen der Rekrutierung, bei Lehrbeginn sowie stichprobenartig während der ganzen Lehre statt. Ausserdem führt die Hoffmann-La Roche aus, die Lehrlingen werden beim Antritt der Lehrstelle über die Drogentests informiert. Die Verweigerung eines Drogentests stellt an sich einen Verstoss gegen die vereinbarten Abmachungen dar. Bis heute sind keine Testsverweigerungen vorgekommen. Zum Schluss sichert die Hoffmann-La Roche AG zu, dass Ihre Betriebsärzte dem Arztgeheimnis unterstehen. Letztere dürfen einen positiven Befund eines Drogentests der Lehrlingsleitung mitteilen.
3. In der Folge fand eine Besprechung zwischen der Hoffmann-La Roche AG und uns statt. Die Hoffmann-La Roche erörterte Ihren Standpunkt und ersuchte uns, die Empfehlung zurückzuziehen. Aufgrund der auseinandergehenden Auffassungen bezüglich der Zulässigkeit von Drogentests hielten wir an die Empfehlung fest, beschlossen aber zugleich, Letztere nicht vor Publikation eines ”Berichtes über Drogentests in der Lehre” einer im nachhinein eingesetzten Arbeitsgruppe vor der Eidg. Datenschutzkommission zu bringen. Mit Schreiben vom 31. Mai 2001 gelangte die Hoffmann-La Roche AG nachmals beim EDSB und hob die wichtigsten Punkten der gemeinsamen Diskussion nochmals hervor.
4. Im Rahmen eines Hearings der Arbeitsgruppe ”Drogentests in der Lehre”, bestehend aus der Schweiz. Fachstelle für Alkohol- und andere Drogenprobleme, dem Staatssekretariat für Wirtschaft, dem Bundesamt für Gesundheit, dem Bundesamt für Justiz und dem EDSB

selber, konnte die Hoffmann-La Roche AG Ihre Argumente für die Durchführung von Drogentests nochmals darlegen.

5. Am 16. Februar 2001 hat die genannte Arbeitsgruppe das Bericht über Drogentests in der Lehre publiziert (vgl. Beilage). Dabei wird sowohl der Gesundheitsschutz als auch die Obhutspflicht des Arbeitgebers gegenüber dem Lehrling als Rechtfertigungsgründe für Drogentests ausgeschlossen und das überwiegende Sicherheitsinteresse samt Einwilligung des Lehrlings als einzige Rechtfertigung solcher Tests betrachtet.
6. Nach Neubeurteilung der Fakten wird die Empfehlung vom 30. März 2000 durch die vorliegende Empfehlung ersetzt.

II. Der EDSB zieht in Erwägung:

1. Gegen das Ziel einer Firma, die Sicherheit und Gesundheit am Arbeitsplatz sowie die Unterstützung Auszubildender zu gewährleisten, ist nichts einzuwenden, sofern die Persönlichkeit der betroffenen Personen respektiert wird. Dass Drogenkonsum am Arbeitsplatz gravierende Folgen haben kann, wie z. B. erhöhtes Unfallrisiko, die Gefährdung der öffentlichen Sicherheit oder des Arbeitsklimas, die finanziellen Einbussen des Unternehmens, die Gesundheit der anderen Mitarbeiter, usw., ist unbestritten. Ein Unternehmen ist demzufolge grundsätzlich berechtigt, Massnahmen zu treffen, um ihren Mitarbeitern und Lehrlingen die bestmöglichen Arbeitsbedingungen zu bieten (vgl. Art. 328 des Schweiz. Obligationenrechtes, OR, SR 220). Die ärztliche Massnahme der Urinanalyse stellt jedoch einen Eingriff in die Persönlichkeit der untersuchten Person dar und setzt das Bestehen eines überwiegenden Rechtfertigungsgrundes voraus. Nur ein gegenüber dem Persönlichkeitsschutz überwiegendes Sicherheitsinteresse, verbunden mit der Einwilligung des Lehrlings, kann einen Drogentest rechtfertigen.
2. Störend am Drogenkonzept der Hoffmann-La Roche AG ist zuerst das Fehlen eines überwiegenden Sicherheitsinteresses. Ein überwiegendes Sicherheitsinteresse ist bspw. dann gegeben, wenn die Verletzung einer Sicherheitsnorm zur Gefährdung des Lebens des Lehrlings oder von Dritten führen kann. Die Übertretung von Sicherheitsnormen z. B. im Bereich des Luft- und Zugsverkehrs kann zur Gefährdung des Lebens der Passagiere führen. Zu denken ist auch an Arbeiten auf dem Bau – wie Gerüstbau, Arbeiten auf Dächern oder bei Kranführern – und an den Umgang mit gefährlichen Stoffen. In solche Fällen können Drogentests, sofern sie nur stichprobenartig und im Rahmen eines bestimmten, im Arbeitsvertrag umschriebenen Sicherheitsmassnahmenpakets vorgenommen werden – vom Arbeitgeber präventiv angeordnet werden. Flächendeckende Tests sind hingegen unverhältnismässig. Die Hoffmann-La Roche AG hat ein überwiegendes Sicherheitsinteresse nicht belegt. Sie stützt Ihre Argumentation vor allem auf die erweiterte Fürsorgepflicht des Arbeitgebers, auf die Drogenprävention und auf den Persönlichkeitsschutz. Schon aus diesem Grund sind die flächendeckenden Drogentests bei der Hoffmann-La Roche AG unzulässig. Andere effiziente Sicherheitsvorkehren (z. B. ISO-Normen für die Gewährleistung der Produktqualität, Vorschriften der Arbeitssicherheit) können die Sicherheit ohne Eingriff in die besonders schützenswerte Gesundheitssphäre des Lehrlings gewährleisten (Verhältnismässigkeits- und Zweckmässigkeitsprinzip, Art. 328b OR sowie Art. 4 Abs. 2 und 3 DSG).
3. Unverhältnismässig und unzweckmässig ist auch die Erhebung von Gesundheitsdaten anhand des Fragebogens ”Ärztliche Eignungsuntersuchung für Lehrlinge”, da die meisten dadurch erhobenen Daten mit der Eignung des Lehrlings für das Arbeitsverhältnis oder mit der Durchführung des Lehrvertrages mit der Hoffmann-La Roche AG in keinem Zusammenhang stehen. Daran vermag auch die Tatsache nichts zu ändern, dass der

Fragebogen nicht von der Hoffmann-La Roche AG selber entworfen worden ist. Der Fragebogen wurde scheinbar für die Gesundheitsabklärung sämtlicher möglichen Lehrverhältnisse konzipiert, ohne Berücksichtigung der Unterschiede zwischen verschiedenen Lehrstellen. So kann die Bearbeitung bestimmter Datenkategorien für die Besetzung gewisser Lehrstellen nötig sein, für andere hingegen nicht.

4. Die Einwilligung alleine stellt keinen gültigen Rechtfertigungsgrund für Drogentests dar, da ohne überwiegendes Sicherheitsinteresse der unabänderliche Persönlichkeitsschutz andere Interessen des Arbeitgebers überwiegt (Art. 362 OR). Grundsätzlich gilt, dass die Vornahme von Drogentests ohne überwiegendes Sicherheitsinteresse einen unverhältnismässigen Eingriff in die Persönlichkeit des Lehrlings darstellt und auch nicht bei Einwilligung des Lehrlings gerechtfertigt ist. Die Einwilligung alleine würde ausnahmsweise dann einen genügenden Rechtfertigungsgrund darstellen, wenn die Vornahme von Drogentests zugunsten des Lehrlings erfolgen würde. In solchen Fällen müsste die Einwilligung insbesondere frei sein. Von freier Einwilligung ist dann die Rede, wenn deren Verweigerung keine Folgen für den Lehrling hat. Dies ist im Drogenkonzept der Hoffmann-La Roche AG nicht der Fall, da die Verweigerung der Einwilligung Konsequenzen auf den Abschluss bzw. Weiterführung des Lehrvertrages hat.

5. Der Arzt ist aufgrund des Arztgeheimnisses verpflichtet, dem Arbeitgeber nur einen ärztlichen Befund über die Eignung einer Person zur Besetzung einer bestimmten Lehrstelle bekannt zu geben (”geeignet” bzw. ”nicht geeignet”). Weitergehende Gesundheitsdaten (z. B. die Angabe, ob das Drogentest bei einem Lehrling positiv ausgefallen ist) dürfen dem Arbeitgeber nicht bekannt gegeben werden. Vollmachten, die den Arzt in Zusammenhang mit Urintests vom Arztgeheimnis befreien sollten, sind nichtig. Es ist einzig der Fall denkbar, dass im Rahmen eines umfassenden Begleitprogramms des Arbeitgebers gewisse andere unabdingbare Informationen vom Arzt weitergegeben werden dürfen, sofern der betroffene Lehrling seine Einwilligung dazu gegeben hat.

6. Nicht zu vergessen ist auch die Tatsache, dass der Arbeitsvertrag auf gegenseitiges Vertrauen beruht. Letzteres kann u. a. dadurch tangiert werden, dass der Arbeitgeber ohne jeglichen konkreten Verdacht auf Drogenkonsum präventiv fahndet, indem er besonders schützenswerte Gesundheitsdaten über sämtliche Lehrlinge (auch diejenigen, die keine Drogen konsumieren) systematisch vor und auch während der Lehre mit Fragebögen und Urintests bearbeitet.

7. Drogentests können nicht mit dem Gesundheitsschutz gemäss Art. 328 OR und Art. 6 des Arbeitsgesetzes (ArG, SR 822.11) begründet werden. Die zu treffenden Massnahmen des Gesundheitsschutzes gemäss diesen Bestimmungen sind arbeitsbedingt und bewirken Änderungen im Arbeitsumfeld. Dies ist bei Drogentests nicht der Fall, weshalb sie nicht mit der Pflicht des Arbeitgebers, die Gesundheit des Arbeitnehmers zu schützen, begründet werden können.

8. Obwohl dem Arbeitgeber einer erweiterte Fürsorgepflicht gegenüber Lehrlingen obliegt, kann Letztere nicht als Rechtfertigungsgrund von Drogentests betrachtet werden, wenn bestimmte Voraussetzungen nicht erfüllt sind. Es muss insbesondere eine Abwägung zwischen Arbeitgeber- und Lehrlingsinteressen vorgenommen werden. Bei dieser Abwägung hat der - im Lehrverhältnis besonders wichtige - Persönlichkeitsschutz des Lehrlings den Vorrang und die Problematik des Drogenkonsums im Betrieb muss ganzheitlich betrachtet werden. Dies setzt voraus, dass der Arbeitgeber seine Aufmerksamkeit nicht auf die Drogen und Drogentests fokussiert, sondern konstruktive Hilfsmassnahmen anbietet und Drogenprävention betreibt. Drogentests sind Fahndungs- und Personalbewirtschaftungsinstrumente, welche zur erweiterten Fürsorgepflicht des Arbeitgebers gegenüber Lehrlingen nicht passt.

III. Aufgrund dieser Erwägungen empfiehlt der EDSB:

1. Die Drogentests bei der Hoffmann-La Roche AG sind unverzüglich einzustellen.
2. Die in Zusammenhang mit den Drogentests erhobenen Gesundheitsdaten sind zu vernichten.
3. Die Hoffmann-La Roche AG meldet dem EDSB innert 15 Tagen seit Erhalt dieser Empfehlung, ob Sie die fraglichen Gesundheitsdaten vernichtet hat und ob Sie auf die Urintests verzichten wird.

EIDGENÖSSISCHER DATENSCHUTZBEAUFTRAGTER
Der Beauftragte:

O. Guntern