10. Tätigkeitsbericht 2002/2003

Eidgenössischer
Datenschutzbeauftragter

Tätigkeitsbericht 2002/2003

des Eidgenössischen Datenschutz-beauftragten

Der Eidg. Datenschutzbeauftragte hat dem Bundesrat periodisch einen Bericht über seine Tätigkeit vorzulegen (Art. 30 DSG). Der vorliegende Bericht deckt den Zeitraum zwischen 1. April 2002 und 31. März 2003 ab.

Dieser Bericht ist auch über das Internet (www.edsb.ch) abrufbar

Inhaltsverzeichnis

* Originaltext auf Französisch

* Originaltext auf Französisch

* Originaltext auf Französisch

* Originaltext auf Französisch

Vorwort

Der 11. September 2001 war das zentrale Thema meines letztjährigen Vorwortes. Im Zentrum meiner Überlegungen stand die Frage, wie ein freiheitlich demokratischer Rechtsstaat dieser Herausforderung begegnen kann, ohne das eigene Fundament in Frage zu stellen.

Wo stehen wir ein Jahr später? Die Hoffnung, dass die Welt mit der nötigen Umsicht auf die neuen Gefahren reagieren wird, hat sich leider noch nicht bestätigt. Zwar hat sich im nationalen Rahmen aus Sicht des Persönlichkeitsschutzes bis heute keine unverhältnismässige Reaktion manifestiert. Der Druck kommt von aussen: Im Kampf gegen die «Achse des Bösen» sucht die Bush-Administration nach Hegemonie auf allen Ebenen. Zunehmend werden nationale Gesetzgebungen ausgehebelt, indem die Vereinigten Staaten versuchen, die übrige Welt ihrem Rechtssystem zu unterwerfen. Jüngstes Beispiel: Die Vereinigten Staaten verlangen ab 5. März 2003 von allen Fluggesellschaften die Herausgabe von personenbezogenen Daten ihrer Passagiere, von Religion und Essgewohnheiten bis hin zu Kreditkartennummer. Das ist nicht nur aufgrund der Sensibilität der verlangten Daten brisant, sondern vor allem angesichts der Art und Weise, wie dieses Datenbedürfnis international durchgesetzt wird. Die US-Behörden verlangen in einem Gesetz von den Fluglinien, dass ihnen die Daten aller anreisenden Passagiere im Voraus übermittelt werden. Bei Zuwiderhandeln drohen Strafen, die bis zum Entzug der Landerechte reichen. Mit den schweizerischen Behörden wurde diesbezüglich bis anhin kein Abkommen getroffen. Mangels eines solchen Abkommens wird die Fluggesellschaft Swiss gezwungen, Daten unter Umständen in Verletzung des nationalen Rechts weiterzugeben. Denn unsere Gesetzgebung verlangt, dass eine Datenweitergabe an ein anderes Land nur erlaubt ist, wenn das betreffende Land über einen vergleichbaren Datenschutz verfügt. Das ist in den USA gerade nicht der Fall, weshalb diese Datenbekanntgabe grundsätzlich nach unserem Recht nur erlaubt wäre, wenn gleichzeitig zwischen den USA und der Schweiz eine Vereinbarung abgeschlossen würde, welche mit Bezug auf diese Daten Schutzbestimmungen festlegt, die mit unserer Gesetzgebung vergleichbar wäre.

Die beschriebene amerikanische Vorgehensweise ist kein Einzelfall. Zunehmend werden wir uns mit der Tatsache auseinander setzen müssen, dass die USA unter dem Deckmantel der Terrorismusbekämpfung versuchen wollen, die Souveränität in der Gesetzgebung der Länder ohne Verhandlung durch einseitiges Diktat zu unterlaufen.

Dass dieser Versuch der Einflussnahme durchaus ernst zu nehmen ist und auch eine sehr akute Gefährdung unserer liberalen Ordnung darstellt, wird sichtbar, wenn zur Kenntnis genommen wird, wie die Bush-Administration im eigenen Land Terrorbe-

kämpfung betreibt: Mit dem so genannten Patriot Act geht die USA längst den Weg in eine repressive Ordnung, welche vom Schutz der Persönlichkeit nicht mehr viel hält. Dieses Gesetz wurde kurz nach dem 11. September 2001 eingeführt, um terroristische Aktivitäten frühzeitig aufzudecken. Das Gesetz erlaubt den Behörden unter anderem sogar, Bibliotheksbenützer zu überwachen, auch wenn nicht der geringste Hinweis auf ein kriminelles Vorgehen vorhanden ist. So erlaubt es den FBI-Mitarbeitern ohne Information des Betroffenen, sämtliche Unterlagen wie Bücher, Dokumente, Zeitungen oder Festplatten von Computern einzufordern. Telefon- und Internetüberwachung wurde vereinfacht. Auch ohne Tatverdacht kann das FBI Personen ausforschen. Die Bush-Regierung will dieses Gesetz noch verschärfen, um sogar US-Bürger heimlich inhaftieren zu können. Mit dem «Total Information Awareness» will das Pentagon ausserdem in einer Datenbank medizinische, finanzielle, steuerliche und andere Aufzeichnungen von Bürgern speichern. Amerikanische Bürgerrechtler warnen vor einer gefährlichen Entwicklung in den USA. Der Direktor der amerikanischen Bürgerrechtsunion (ACLU), Barry Steinhardt, sagte kürzlich in einem Interview: «Eine Kombination aus blitzschnellen technischen Innovationen und der Erosion des Schutzes der Privatsphäre droht Big Brother von einer oft zitierten, aber weit entfernten Gefahr zu einem realen Bestandteil des amerikanischen Alltags werden zu lassen.» Der von dieser Union im Januar 2003 publizierte Bericht trägt den Titel: «Grösseres Monster, schwächere Ketten: Das Wachstum der amerikanischen Überwachungsgesellschaft.»

Massnahmen, die dem Kampf gegen den Terrorismus dienen, sollen selbstverständlich auch von der Schweiz unterstützt werden. Aber es müssen auch Schranken gesetzt werden, denn inzwischen ist der Punkt erreicht worden, wo der Kampf gegen den Terror nicht nur mit dem Datenschutz kollidiert, sondern langsam zur Gefahr für unseren Rechtsstaat wird. Zu befürchten ist, dass die USA diese Überwachungsmentalität auch bei uns mit direktem oder indirektem Druck durchsetzen.

Angesichts dieser Fakten müssen wir am 10-jährigen Jubiläum unseres Datenschutzgesetzes ein ernüchterndes Fazit ziehen: Zwar hat im nationalen Rahmen dank dieses Gesetzes das Bewusstsein und die Sensibilität für die grossen Gefährdungspotentiale der technologischen Entwicklung auf die Persönlichkeitsrechte der Bürger erfreulich zugenommen. Was nützt es aber, wenn am Ende diese Errungenschaften durch eine nach Hegemonie strebende Weltmacht, welche sich mit Bezug auf Daten- und Persönlichkeitsschutz auf dem Niveau eines Entwicklungslandes befindet, schleichend ausser Kraft gesetzt werden?

Diese Feststellung darf indessen nicht zur Annahme verleiten, dass wir keine hausgemachten datenschutzrechtlichen Probleme mehr zu lösen hätten und persönlichkeitsgefährdende Entwicklung ihren Ursprung letztlich im Ausland haben. Da würden wir uns tatsächlich in falscher Sicherheit wiegen. Unabhängig von amerikanischem

Druck grassiert auch bei uns der zunehmende Hang, an jeder Ecke eine Videokamera zu installieren, in der Hoffnung, damit mehr Sicherheit zu erhalten. Auch wenn nicht in Abrede gestellt werden kann, dass diese Technik unter bestimmten Umständen sehr wohl nützliche Dienste leistet, muss festgestellt werden, dass sie oft überflüssig, unzweckmässig und unverhältnismässig ist und zuweilen gar eine falsche Sicherheit vorgaukelt: Ein Parkhaus wird für Frauen nicht deshalb sicherer, weil Kameras montiert sind. Man kann sich ja der Identifizierung durch Verhüllung des Gesichts entziehen. Sicherer wird es nur, wenn es durch Menschen überwacht und kontrolliert wird. Location based services (Benützung des Mobiles durch Marketingfirmen zu Werbezwecken) und pervasive computing (kleine, meist unsichtbare Sender, die überall, bis hin zu den Kleidern und Nahrungsmitteln, eingebaut werden können, um Daten zu liefern) sind Phänomene, welche primär Werber und Marketingleute interessieren, deren persönlichkeitsverletzendes Potential aber immens ist. Oder wie es die deutsche Rechtsprofessorin, Marie-Theres Tinnenfeld anfangs Jahr formulierte: «Heute nun ist zu befürchten, dass eine staatliche Überwachung ohne Mass und eine grenzenlose Datenjagd der Wirtschaft die Privatsphäre zerstören könnten.»

Hanspeter Thür

Abkürzungsverzeichnis

AGX	Arbeitsgruppe Gesundheit
AHV	Alter- und Hinterlassenenversicherung
BASPO	Bundesamt für Sport
BFS	Bundesamt für Statistik
BJ	Bundesamt für Justiz
BSV	Bundesamt für Sozialversicherung
CHOP	Schweizerische Operationsklassifikation
CIRCA	Communication & Information Resource Centre Administrator
EDI	Eidgenössisches Departement des Innern
EO	Erwerbsersatz
FMH	Verbindung der Schweizer Ärztinnen und Ärzte (Foederatio Medicorum Helveticorum)
GUMG	Bundesgesetz über genetische Untersuchungen beim Menschen
ICD-10	International Classification of Diseases, 10th revision
IDA	Interexchange of Data between Administrations (Informationsaus tausch zwischen öffentlichen Verwaltungen)
IKO	Informationsstelle für Konsumkredit
IV	Invalidenversicherung
KKG	Bundesgesetz über den Konsumkredit
KVG	Bundesgesetz über die Krankenversicherung
NDS	Nationale Datenbank für Sport
RAI/RUG	Resident Assessment Instrument/Ressource Utilisation Groupes
StGB	Strafgesetzbuch
SVV	Schweizerischer Versicherungsverband
Tarmed	Tarif Medizin (Tarifwerk des Schweizer Gesundheitswesens)
UVG	Unfallversicherungsgesetz
VDNS	Verordnung über die nationale Datenbank für Sport

1. Grundrechte

1.1 Modernisierung des Datenschutzes

Im Anschluss an zwei parlamentarische Motionen legte der Bundesrat den Eidgenössischen Räten eine Botschaft vor, in der er eine Teilrevision des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG) sowie die Ratifizierung des Zusatzprotokolls zum Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108) beantragte. Der dem Parlament unterbreitete Entwurf des Öffentlichkeitsgesetzes wird ebenfalls zu einer Änderung des DSG führen. Schliesslich könnte sich je nach Verlauf der bilateralen Verhandlungen zwischen der Schweiz und der Europäischen Union bald eine substanziellere Revision des DSG als notwendig erweisen. Der EDSB ist insgesamt mit den beantragten Veränderungen einverstanden, bedauert indessen, dass keine weiter gehende Revision angestrebt wird.

Revision des Bundesgesetzes über den Datenschutz

Als Antwort auf die Motion 98.3529 der Geschäftsprüfungskommission des Ständerates «Erhöhter Schutz bei Online-Verbindungen» sowie auf die Motion 00.3000 der Kommission für Rechtsfragen des Ständerates «Erhöhte Transparenz bei der Erhebung von Personendaten» unterbreitete der Bundesrat den Eidgenössischen Räten am 19. Februar 2003 die Botschaft «zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitender Datenübermittlung» (BBl 2003 2101).

Der Revisionsentwurf stärkt durch die Einführung der Transparenzpflicht bei der Erhebung von Personendaten die Position der betroffenen Personen. Jegliches Beschaffen von Daten soll in Zukunft für die betroffene Person erkennbar sein. Die betroffene Person muss zumindest die Zwecke der Bearbeitung kennen. Wenn besonders schützenswerte Daten und Persönlichkeitsprofile beschafft werden, muss der Verantwortliche für die Datenbearbeitung die betroffenen Personen mindestens über die Identität des Inhabers der Datensammlung, über den Zweck der Datenbearbeitung und wenn die Daten bekannt gegeben werden sollen über die Kategorien der Datenempfänger aktiv informieren. Allerdings kann die Information der betroffenen Person wie beim Auskunftsrecht unter bestimmten Voraussetzungen eingeschränkt werden. Die be-

troffenen Personen müssen auch ausdrücklich informiert werden, wenn eine Entscheidung, die Rechtsfolgen für sie zeitigt oder sie wesentlich betrifft, einzig auf der Grundlage einer automatisierten Datenberarbeitung, die bestimmte Persönlichkeitsaspekte einschätzen soll, gefasst wird. Im privaten Sektor wird das Recht, sich der Bearbeitung zu widersetzen, wirksamer gestaltet, indem der Verantwortliche für die Datenbearbeitung aufgefordert wird, zu den Gesuchen von betroffenen Personen Stellung zu nehmen.

Der grenzüberschreitende Datenverkehr wird ebenfalls überarbeitet. Die Meldepflicht wird aufgehoben. Das Übermittlungsverbot bei gravierender Gefährdung der Persönlichkeitsrechte der betroffenen Personen wird beibehalten. Der Entwurf sieht jedoch Ausnahmeregelungen vor, vor allem wenn der Verantwortliche für die Datenbearbeitung angemessene Garantien (Rückgriff auf vertragliche Datenschutzklauseln, Datenschutzreglement für Unternehmensgruppen) anbietet. Diese Garantien sind dem EDSB zu melden, welcher dann gegebenenfalls einschreitet. Allerdings sollen Ausnahmen von der Meldepflicht im Gesetz verankert und das Meldeverfahren vereinfacht werden: In absehbarer Zukunft wird der Inhaber einer Datensammlung auch die Möglichkeit haben, seine Register online anzumelden. Das Register der Datensammlungen wird im Internet veröffentlicht, was die Einsicht erleichtert. Im Gesetzesentwurf wird neu die Zertifizierung der Produkte und der Personendaten-Bearbeitungssysteme (Audit, Datenschutz-Gütesiegel) als Anreizmassnahme eingeführt. Ausserdem kann der EDSB im Rahmen seiner Befugnisse nachprüfen, ob zum einen die zertifizierten Unternehmen die Datenschutzauflagen beachten und zum anderen die für die Zertifizierung und Labelerteilung verantwortlichen Unternehmen datenschutzkonform arbeiten. Der EDSB kann künftig den Evaluationsrahmen festlegen und gegebenenfalls Empfehlungen formulieren.

Ausserdem wird im Entwurf die Regelung zur Datenbearbeitung im Auftrag, d.h. wenn insbesondere Bundesstellen Daten durch Dritte bearbeiten lassen, präzisiert. In diesem Fall können die Bundesorgane Kontrollen bei diesen Dritten durchführen. Als Antwort auf die Motion «Online-Verbindungen» wird dem Bundesrat ermöglicht, während einer zeitlich beschränkten Versuchsphase die automatisierte Bearbeitung von besonders schützenswerten Daten oder Persönlichkeitsprofilen im Rahmen von «Pilotversuchen» zu bewilligen, bevor die diesbezügliche formellgesetzliche Grundlage in Kraft tritt. Ferner legt der Revisionsentwurf Minimalanforderungen fest, denen die kantonale Gesetzgebung genügen muss, wenn ein Kanton im Vollzug von Bundesrecht Daten bearbeitet. Schliesslich kann der EDSB gegenüber Verfügungen eines Departements bzw. der Bundeskanzlei bei der Eidgenössischen Datenschutzkommission Beschwerde einlegen, wenn die Verfügung nicht auf eine an ein Bundesorgan gerichtete, von diesem abgelehnte oder nicht befolgte Empfehlung eintritt. Die Interven-

tionsbefugnis des EDSB im privaten Sektor wird gestärkt: Künftig kann er Ermittlungen zu Bearbeitungen von besonders schützenswerten Daten oder Persönlichkeitsprofilen sowie zu regelmässigen Datenbekanntgaben unabhängig davon durchführen, ob die bearbeitungsrelevanten Datensammlungen aufgrund der Erfassung im Register der Datensammlungen der Meldepflicht unterliegen.

Zusatzprotokoll zum Übereinkommen 108

Das erste Zusatzprotokoll zum Übereinkommen 108 wurde vom Ministerkomitee des Europarates am 23. Mai 2001 unterzeichnet und den Staaten am 8. November 2001 zur Unterschrift vorgelegt. Bislang haben drei Vertragsparteien des Übereinkommens 108 das Zusatzprotokoll ratifiziert, 18 weitere haben es unterzeichnet. Nach den positiven Ergebnissen des Vernehmlassungsverfahrens hat die Schweiz das Protokoll am 17. Oktober 2002 unterzeichnet. Ziel des Protokolls ist es, die Umsetzung der Grundsätze im Übereinkommen 108 zu stärken und dabei insbesondere die Zunahme der grenzüberschreitenden Datenflüsse an Empfänger in Ländern, die das Übereinkommen nicht unterzeichnet haben, zu berücksichtigen. Das Protokoll regelt zunächst die Verpflichtung der Vertragsparteien, eine bzw. mehrere Behörden für die Überwachung der Einhaltung der nationalen Datenschutzbestimmungen einzusetzen. Diese Behörden handeln unabhängig und verfügen über Untersuchungs- und Interventionsbefugnisse; sie bilden einen festen Bestandteil des Datenschutzkontrollsystems einer demokratischen Gesellschaft. Angesichts der internationalen Dimension des Transfers von Personendaten und zur Verbesserung der Harmonisierung der Datenschutzlösungen werden die Kontrollbehörden der Vertragsstaaten aufgefordert, Informationen auszutauschen und zusammenzuarbeiten, sofern dies für die Aufgabenerfüllung erforderlich ist.

Des Weiteren regelt das Protokoll den grenzüberschreitenden Datenfluss in Drittländer. Die Weitergabe von Personendaten an einen Datenempfänger, der vom Übereinkommen 108 nicht betroffen ist, kann nur erfolgen, wenn der Empfängerstaat bzw. die Empfängerorganisation ein für die fragliche Übermittlung geeignetes Schutzniveau gewährleistet. Das Protokoll sieht indessen Ausnahmen vom Erfordernis des angemessenen Schutzniveaus vor. So kann der Transfer beispielsweise bewilligt werden, wenn er im innerstaatlichen Recht des Vertragsstaates, aus welchem die Daten weitergegeben werden, im spezifischen Interesse der betroffenen Person oder aus legitimen, gegenüber jenen der betroffenen Person überwiegenden Interessen vorgesehen ist. Möglich ist der Transfer auch dann, wenn der Verantwortliche auf Vertragsklauseln beruhende Garantien anbietet. Die Garantien müssen die relevanten Aspekte des Datenschutzes enthalten und die Rechte der betroffenen Personen wahren. Ausserdem müssen die zuständigen Datenschutzbehörden sie für ausreichend befunden haben.

Der DSG-Revisionsentwurf trägt dazu bei, die Bundesgesetzgebung mit den Anforderungen des Zusatzprotokolls in Einklang zu bringen, und erlaubt der Schweiz, dieses zu ratifizieren. Die Ratifizierung des Protokolls spielt für die Schweiz insbesondere wegen der zahlreichen Informationsaustauschvorgänge mit den Mitgliedsstaaten der Europäischen Union eine Schlüsselrolle. Die Befolgung der Auflagen des Übereinkommens 108 und des Zusatzprotokolls soll künftig bei der Beurteilung des angemessenen Schutzniveaus von Drittstaaten mit den Ausschlag geben. Die Kantone müssen ihre Gesetze ebenfalls anpassen bzw. zum Teil die Befugnisse und die Unabhängigkeit der Kontrollbehörden stärken.

Bilaterale Verhandlungen II zwischen der Schweiz und der Europäischen Union

Die Schweiz und die Europäische Union haben neue bilaterale Verhandlungen in die Wege geleitet. Diese Verhandlungen betreffen insbesondere die Dienstleistungen, die Besteuerung der Zinserträge, die Schengener Abkommen und das Dubliner Übereinkommen über Asylfragen. Falls die Verhandlungen in ein Abkommen münden, muss die Schweiz einen Teil des europäischen «acquis» (gemeinschaftlicher Besitzstand) übernehmen. Dazu gehört 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. Die Übernahme des «acquis» zieht eine weiter gehende Revision des DSG nach sich als jene, die der Bundesrat unterbreitet hat. Die Hauptunterschiede gegenüber dem Europarecht betreffen die Definitionen und die verwendete Terminologie, den Geltungsbereich (die Richtlinie geht weiter als das DSG), das Konzept der besonders schützenswerten Daten, welches im Europarecht für den privaten Sektor strikter geregelt wird, die für sämtliche Arten von Personendaten geltende ausdrückliche Information der betroffenen Personen bei der Datenerhebung, das (in der schweizerischen Gesetzgebung fehlende) Recht, keiner automatisierten individuellen Verfügung unterstellt zu werden, sowie das Auskunftsrecht, das in der europäischen Richtlinie ebenfalls breiter definiert wird. Auch das Anmeldungssystem der Bearbeitungen im europäischen Recht unterscheidet sich hinsichtlich der zu liefernden Informationen, der Tragweite der Anmeldung und der vorherigen Prüfung riskanter Bearbeitungen vom Schweizer Recht. Schliesslich sieht die europäische Richtlinie umfassendere Kompetenzen und Befugnisse für die Datenschutz-Kontrollbehörden vor. Die Gesetzgebungen mehrerer Mitgliedsstaaten der Europäischen Union verleihen den Datenschutzbehörden Entscheidungs- und Sanktionsbefugnisse. Auch die schweizerischen Kantone werden ihre Gesetze überarbeiten müssen. Dabei fragt sich, ob der Bund die Kompetenz erhalten sollte, das DSG – mangels eines angemessenen Datenschutzes – zumindest ersatzweise auf sämtli-

che von Kantons- oder Gemeindeorganen durchgeführten Datenbearbeitungen anzuwenden.

Die Umsetzung der europäischen Richtlinie wäre für die Schweiz nicht nachteilig: Selbst wenn eventuell zunächst mit negativen Reaktionen der Privatwirtschaft zu rechnen ist, dürften die in Europa tätigen Schweizer Unternehmen erhebliche Vorteile aus der umfassenderen Harmonisierung unseres Rechts mit dem Europarecht ziehen. Dank der Umsetzung der Richtlinie liessen sich die Hindernisse im Datenverkehr mit den europäischen Staaten beseitigen. Ausserdem würden die betroffenen Personen ein gleichwertiges Schutzniveau und identische Rechte wie die Staatsbürger der Europäischen Union geniessen. Die Umsetzung der Richtlinie würde die Einheitlichkeit der Praktiken und Rechtsprechungen verbessern und eine Mitwirkung an der Entwicklung des Europarechts ermöglichen. Ausserdem dürfte sie uns erlauben, in der durch die europäische Richtlinie eingesetzten Arbeitsgruppe mitzuwirken.

Entwurf eines Bundesgesetzes über die Öffentlichkeit der Verwaltung

Der Bundesrat verabschiedete am 12. Februar 2003 die Botschaft zum Bundesgesetz über die Öffentlichkeit der Verwaltung (BBl 2003 1963) und legte sie den Eidgenössischen Räten vor. Der Gesetzesentwurf soll der Öffentlichkeit Zugang zu amtlichen Dokumenten gewähren und die Transparenz der Verwaltung fördern. Der Zugang zu amtlichen Dokumenten bezieht sich auch auf Personendaten. Im Regelfall werden diese Dokumente anonymisiert, bevor sie den Gesuchstellern übermittelt werden. Eine Anonymisierung ist jedoch nicht immer möglich. Unter Umständen könnte die Verwaltung veranlasst werden, Personendaten an Dritte zu übermitteln. In solchen Fällen findet das DSG Anwendung; die Rechtmässigkeit des Zugangs richtet sich nach den Bestimmungen über die Weitergabe von Personendaten. Die betroffene Person kann verlangen, vor der Weitergabe der angeforderten Daten informiert zu werden; betrifft das Gesuch schützenswerte Daten oder Persönlichkeitsprofile, so ist die Information Pflicht. Der Gesetzesentwurf sieht für etwaige Konflikte zwischen Verwaltung und Bürgern wegen eines Zugangsgesuchs eine Schlichtungsstelle vor. Diese Schlichtung wird vom EDSB gewährleistet, der damit neue Aufgaben übernimmt. Dieses System entspricht dem Standpunkt, welchen der EDSB im Vernehmlassungsverfahrens vertrat (siehe 7. Tätigkeitsbericht, Kapitel II.7). Das Öffentlichkeitsgesetz sieht ausserdem eine Änderung des DSG vor: Personendaten, die im Rahmen der Information der Öffentlichkeit von den Behörden von Amtes wegen oder aufgrund des Öffentlichkeitsgesetzes zugänglich gemacht werden, dürfen weitergegeben werden, falls sie mit der Erfüllung öffentlicher Aufgaben in Zusammenhang stehen und falls ein überwiegendes Interesse an der Datenbekanntgabe besteht. Die Daten können ausserdem im

Internet veröffentlicht werden. Die Verbreitung im Internet kommt auch in Betracht, wenn eine Gesetzesgrundlage die Veröffentlichung der Daten vorsieht. Allerdings dürfen die Daten nicht allein wegen der Veröffentlichung oder der allgemeinen Zugänglichkeit automatisch ins Internet gestellt werden; der Grundsatz der Verhältnismässigkeit ist zu beachten. Ferner müssen die Daten gelöscht werden, sobald das im öffentlichen Interesse liegende Ziel, das die Veröffentlichung rechtfertigte, erreicht ist. Damit soll insbesondere das Recht auf Vergessen gewährleistet werden. In bestimmten Fällen ist der Datenzugang durch die Einschränkung der Datensuchfunktionen zu begrenzen.

Stellungnahme des EDSB zur DSG-Revision

Insgesamt unterstützt der EDSB die in den beiden erwähnten Botschaften erläuterten Änderungsvorschläge des DSG. Wie wir bereits in unserem 8. Tätigkeitsbericht erwähnten (Kapitel I.12), hätten wir eine weiter gehende Revision des DSG und eine konsequentere Annäherung an das Europarecht befürwortet. Wir begrüssen die Einführung der Zertifizierung und des Datenschutz-Gütesiegels, welche die Autonomie und die Verantwortung der Inhaber von Datensammlungen weiter stärken. Ausserdem weisen wir darauf hin, dass im Öffentlichkeitsgesetz ein Gleichgewicht zwischen dem Zugang zu amtlichen Dokumenten und den Anforderungen an den Schutz des Privatlebens gefunden wurde. Dagegen melden wir Vorbehalte an der Einführung einer Bestimmung an, die dem Bundesrat erlaubt, die automatisierte Bearbeitung von besonders schützenswerten Daten oder von Persönlichkeitsprofilen vor dem Inkrafttreten eines formellen Gesetzes zu gestatten. Unseres Erachtens geht diese Bestimmung zum einen über die Motion «Online-Verbindungen» hinaus, welche eine Gesetzesgrundlage einzig für den Online-Zugang forderte. Zum anderen halten wir zwar eine Anpassung des Gesetzmässigkeitsprinzips auch für notwendig – namentlich um die Komplexität der Personendaten-Bearbeitungssysteme und die Entwicklungen bei der Aufgabenerfüllung der Bundesorgane zu berücksichtigen – , aber wir hätten eingehendere Überlegungen zu den Anforderungen des Gesetzmässigkeitsgrundsatzes und zu den Modalitäten der Umsetzung gewünscht. Wie in einigen europäischen Gesetzen könnten so bestimmte Bearbeitungsvorgänge der vorherigen Bewilligung durch den Eidgenössischen Datenschutzbeauftragten unterstellt werden. In einer späteren Phase sind unseres Erachtens die Stärkung der Rechte der betroffenen Person und die Erleichterung des Verfahrens im privaten Sektor unerlässlich, damit die Einzelpersonen ihre Rechte besser geltend machen können. Ausserdem soll der Einsatz von datenschutzfreundlichen Technologien gefördert werden beispielsweise mit der Pflicht für die Datenbearbeitungsverantwortlichen, Instrumente bereitzustellen, damit die Privatpersonen bei der Nutzung von Online-Dienstleistungen ihre Rechte

ausüben können. Auch die Selbstregulierung könnte stärker entwickelt werden. Die grössere Autonomie der Verantwortlichen für die Datenbearbeitung muss indessen die Einführung von präventiven und im Missbrauchsfall repressiven Kontrollmitteln nach sich ziehen. Das bedeutet, dass der EDSB künftig eine aktivere Rolle spielt. Es gilt zu vermeiden, dass Einzelpersonen völlig schutzlos sind, wenn Daten über sie bearbeitet werden. Deshalb muss eine Politik entwickelt werden, welche die Anerkennung und die Achtung der Datenschutzgrundsätze fördert und den betroffenen Personen die effektive Ausübung ihrer Rechte erlaubt. Der EDSB hat darauf zu achten, dass die Regeln befolgt und in die Datenbearbeitungsabläufe integriert werden. Dieser Ansatz erfordert eine Überarbeitung der Befugnisse des EDSB. Der EDSB soll die Befolgung der Gesetzesauflagen nicht nur kontrollieren, sondern bei Verletzung auch die angemessenen Massnahmen ergreifen und gegebenenfalls Sanktionen verhängen können. Die Effizienz der Überwachung setzt (heute unzureichende) Ressourcen und Entscheidungsbefugnisse voraus (siehe auch Abschnitt 12.1 des vorliegenden Berichtes). Ähnlich wie andere Datenschutzbehörden in Europa und sonstige Überwachungsbehörden in der Schweiz, z.B. die Eidgenössische Wettbewerbskommission, sollte auch der EDSB ermächtigt werden, Sanktionen zu verhängen. Ausserdem könnte ein Beschwerderecht gegen Verfügungen von Bundesstellen (ähnlich wie im Datenschutzgesetz des Kantons Glarus vorgesehen) eingeführt werden.

1.2 E-Government

1.2.1 Bestrebungen zur Einführung eines schweizerischen Personenidentifikators

Eine lebenslänglich gleich bleibende Nummer für alle Schweizer Bürger und Einwohner bewirkt Effizienzsteigerungen bei Verknüpfung und Austausch von Informationen der Betroffenen. Dieselbe Effizienzsteigerung kann a priori sowohl für positiv zu wertende als auch für gefährliche oder gar missbräuchliche Tätigkeiten genutzt werden. Aus diesem Grund fordern wir ebenso wie der Verfassungsrechtler G. Biaggini klare Definitionen der Verwendungszwecke eines allfälligen Personenidentifikators.

Im 9. Tätigkeitsbericht (Abschnitt 10.2) haben wir erwähnt, dass die Einführung eines Personenidentifikators im Zusammenhang mit Registerharmonisierung gemäss Art. 65 Abs. 2 BV die für den Datenschutz zentrale Frage darstellt. Unsere Kritik richtet sich dabei nicht gegen die Einführung einer Nummer an sich, sondern gegen die Unbestimmtheiten ihrer geplanten Verwendungszwecke und insbesondere gegen die Tatsache, dass eine im Rahmen eines Statistikprojektes geschaffene Nummer in Register

eingefügt werden soll, welche definitionsgemäss administrativen Zwecken dienen.

Seit dem letztjährigen Tätigkeitsbericht ist zwar gemäss den federführenden Instanzen auf politischer Ebene mit Bezug auf einen Personenidentifikator nichts entschieden worden.

Diese scheinen aber an einer politischen Diskussion auch nicht sonderlich interessiert zu sein, denn im Pressecommuniqué zur Vernehmlassung betreffend das Bundesgesetz über die Harmonisierung der Personenregister wird der Personenidentifikator mit keinem Wort erwähnt. Demgegenüber – und das erscheint uns stossend – wird im Begleitschreiben an die interessierten Organisationen folgende Frage formuliert: «Welche Art eines Personenidentifikators würden Sie grundsätzlich bevorzugen: einen für administrative Zwecke verwendbaren Identifikator im Einwohnerbereich aus den E-Government Projekten des Bundes, den die Statistik mitbenutzen könnte, oder einen separaten Identifikator der Statistik, der ausschliesslich für statistische Zwecke verwendet werden dürfte?»

In faktischer Hinsicht verhält es sich demgegenüber so, dass in diversen Projekten des so genannten eGovernment eine «Arbeitshypothese» gilt, wonach ein koordinierter Eidgenössischer Personenidentifikator in Administrativregister eingeführt werden soll. Aufgrund dieser Annahme werden in diversen Projekten des administrativen Bereichs (Stichwort eGovernment) Weichenstellungen vorgenommen und damit letztlich auch Sachzwänge geschaffen. Welche Auswirkungen die so entstehende Infrastruktur dabei für den Persönlichkeitsschutz hat, ist in keiner Weise geklärt, eine Technikfolgeabschätzung wurde in dieser Hinsicht von den federführenden Organen auch nicht unternommen.

Die Tatsache, dass ein rein statistischer Personenidentifikator überhaupt nicht in die Administrativregister gehört, scheint ebenso vergessen wie die Aussage des Bundesamts für Statistik selbst, dass die Verknüpfung der Administrativregister über einen PIN «nicht der politischen Kultur in der Schweiz» entspreche.

Ein von uns bei Giovanni Biaggini (Professor für Staats- und Verwaltungsrecht an der Universität Zürich) in Auftrag gegebenes Gutachten betreffend die verfassungsrechtlichen Schranken für einen allfälligen Personenidentifikator kommt zum Schluss, dass die Verhältnismässigkeit der Verwendung eines solchen Codes nur anhand von näher bestimmten Zielen geprüft werden kann. Dementsprechend darf ein Personenidentifikator nur dann in bestimmte Administrativregister eingefügt werden, wenn dies durch konkrete Begründung im Rahmen administrativer Geschäftsfälle gerechtfertigt ist. Denn ob allfällige Effizienzgewinne im Administrativbereich die Gefahren für den Persönlichkeitsschutz überwiegen, kann nur im Zusammenhang mit konkreten und näher bestimmte Zielen geprüft werden.

1.2.2 Guichet Virtuel, e-Voting und Registerharmonisierung

Im Bereich des sogenannten eGovernment sieht sich der Datenschutzbeauftragte einer Vielzahl von Projekten gegenüber, von denen manche unpräzise und andere gar fragwürdige Ziele verfolgen. Für den Datenschutz besteht ein zentrales Problem darin, dass in den betreffenden Projektgremien datenschutzbezogenes Know-how und entsprechende Sensibilität fehlen.

Im 9. Tätigkeitsbericht (Abschnitt 1.1) haben wir darauf hingewiesen, dass die Anforderungen von Datenschutz und Datensicherheit erst dann formuliert werden können, wenn klar ist, welche Geschäftsfälle zwischen welchen Akteuren über den virtuellen Amtsschalter abgewickelt werden sollen. In der Zwischenzeit ist in dieser Hinsicht soweit wir sehen nicht mehr Klarheit erreicht worden. Die unter dem modernen Titel «Web Services» vorangetriebenen drei Teilprojekte namens Authentication, Tracking und Payment betreffen aber Elemente, welche in dieser Hinsicht äusserst präzise Basis in ihren jeweiligen Spezifikationen finden sollten. Im übrigen ist angesichts der Grössenordnung und Sensibilität des Projekts Guichet Virtuel selbstverständich, dass das erforderliche Know-how auf dem Gebiete des Datenschutzes innerhalb der Projektorganisation selbst organisiert werden muss. Nur so kann die Projektleitung ihre Verantwortung wahrnehmen und gewährleisten, dass anlässlich der zahlreichen Arbeitsgruppensitzungen die sensiblen Punkte erkannt und die richtigen Weichenstellungen vorgenommen werden.

Zum e-Voting haben wir im 9. Tätigkeitsbericht (Abschnitt 1.1) festgehalten, dass die technischen Herausforderungen, die sich aus dem Spannungsverhältnis zwischen Stimmgeheimnis und Nachvollziehbarkeit ergeben, heute nicht als gelöst betrachtet werden können. Grundsätzlich ist zu sagen, dass im gesamten schweizerischen Umfeld des e-Voting bisher keine gründliche Risikoanalyse durchgeführt worden ist. Es mag mit der technischen Komplexität des e-Voting zusammenhängen, dass risikobezogene Überlegungen ausschliesslich im technischen Bereich angestellt wurden. Risiken für die Demokratie an sich, welche mit dem Vertrauen der Bürger in funktionierende Institutionen und Abläufe zu tun haben, wurden nicht untersucht. Dem Thema Vote électronique wurde im übrigen die diesjährige Tagung «Informatik und Recht» gewidmet. Im entsprechenden Tagungsband (Tagung 2002 für Informatik und Recht, Muralt Müller Hanna, Auer Andreas, Koller Thomas (Hrsg.) Bern 2003, ISBN 3-7272-2162-3) sind verschiedene Aspekte des e-Voting teils auch kritisch beleuchtet. Da sich das e-Voting zur Zeit noch in einer frühen Versuchsphase befindet, ist eine grossflächige Harmonisierung der Stimmregister, wie sie in diesem Zusammenhang von verschiedenen Stellen angestrebt wird, aus datenschutzrechtlicher Sicht äusserst problematisch.

2. Datenschutzfragen allgemein

2.1. Datenschutz und Datensicherheit

2.1.1 Systemsicherheit ohne die Veröffentlichung des Quellcodes (Open Source Software / freie Software)

In einem Umfeld, in dem die Anforderungen an den Datenschutz und die Datensicherheit hoch sind, ist es unabdingbar, dass der Quellcode einsehbar ist bzw. veröffentlicht wird. Jeder Datenbearbeitungsschritt muss nachvollzogen werden können, und mögliche Risiken oder Gefahren sind zu minimieren bzw. auszuschliessen.

Beim grössten Teil der heute eingesetzten Standardsoftware (Anwendungen und Betriebssysteme) wird der Quellcode (Source Code) nicht veröffentlicht. Die Anwender sind nur im Besitze des kompilierten Programms ohne zu wissen, wie dieses im Einzelnen geschrieben bzw. programmiert wurde. Für den Produzenten hat dies sicher den Vorteil, dass er gegenüber den Mitbewerbern nicht aufzeigen muss, wie die Software aufgebaut ist. Man kann sich damit einen nicht unerheblichen Know-how-Vorsprung sichern. Für die Datensicherheit und somit auch für den Datenschutz hat aber diese Intransparenz Nachteile. Bis heute vertraut man diesen Produkten mehr oder weniger. Man kann aber nie ganz sicher sein, ob beispielsweise in der Software nicht noch irgendeine Hintertüre (Backdoor) eingebaut ist, welche Funktionen ausführt, die dem Anwender bzw. Betreiber nicht bekannt sind. Im Weiteren kann man das Programm auch nicht umfassend auf mögliche Fehler überprüfen. Um den Datenschutz und die Datensicherheit zu erhöhen, geht man heute deshalb in vielen Fällen so vor, dass man die Software von einem Hersteller auswählt, aber nicht dessen Chiffriersoftware, sondern eine andere Verschlüsselungssoftware, deren Quellcode veröffentlicht wurde, einsetzt. Ein Vorteil von Open Source Software (freier Software) besteht darin, dass der Source Code offen gelegt ist und von jedem Sachverständigen analysiert werden kann. Fehler können durch diese Veröffentlichung viel schneller entdeckt werden, sofern der veröffentlichte Source Code auch wirklich analysiert wurde. Man muss sich allerdings auch bewusst sein, dass die Menge der Codezeilen oft enorm ist, so dass man nicht zwingend davon ausgehen darf, dass die Programme vollständig analysiert wurden. Es ist aber sicher davon auszugehen, dass Produzenten eher dazu neigen, den Quellcode nicht offen zu legen, wenn Hintertüren im Programm eingebaut sind. Umfangreichere Informationen und Definitionen zu Open Source Software (freier Software) können u. a. den folgenden Internetseiten entnommen werden:

http://www.opensource.org; http://www.ifross.de/

Wir haben bereits bei den Verschlüsselungsverfahren darauf hingewiesen, dass aus Datenschutz- und Sicherheitsgründen ein veröffentlichtes Chiffrierverfahren einzusetzen ist. Dasselbe gilt auch für den Einsatz anderer Software. Ohne die Offenlegung des Quelltexts kann der Datenschutz nicht gewährleistet werden, was insbesondere in einem sensitiven Umfeld höchst problematisch ist. Dies wird einem u. a. dann bewusst, wenn man beabsichtigt, elektronische Abstimmungssysteme (e-Voting) datenschutzkonform zu realisieren. Einerseits haben die Abstimmungsberechtigten das Recht, ihre Stimmen anonym abzugeben, andererseits muss aber festgestellt werden können, ob der jeweilige Abstimmungsberechtigte bereits abgestimmt hat und somit seine Stimme nicht erneut abgeben kann. Ferner muss gewährleistet sein, dass eine abgegebene Ja-Stimme vom System immer als solche interpretiert wird. Deshalb ist es wichtig, dass der Quellcode offen gelegt wird, damit dieser von Sachverständigen analysiert werden kann. Es kann in besonderen Fällen durchaus auch sinnvoll sein, dass gewisse Teile des Source Codes nur von einigen Personen analysiert werden, weil eine Veröffentlichung im grossem Umfang wiederum zu Sicherheitsproblemen führen könnte. Durch die Offenlegung des Source Codes kann man verfolgen, welche Funktionen das System durchführt und welcher Informationsfluss entsteht. Hintertüren (Backdoors), die beispielsweise Manipulationen an abgegebenen Stimmen ermöglichen könnten, können bei einem solchen Vorgehen mit grösster Wahrscheinlichkeit ausgeschlossen werden. Datenschutz- und Datensicherheitsfragen sind bei solch sensitiven Systemen Kernfragen bzw. absolute Muss-Zielsetzungen, ohne deren Einhaltung bzw. Umsetzung ein System nicht in Betrieb genommen werden darf.

2.1.2 Physikalisches Löschen von Daten auf magnetischen Datenträgern

Werden auf einem Datenträger Daten mit den Bordmitteln der Betriebssysteme gelöscht, können sie mit mehr oder weniger hohen Aufwand wiederhergestellt werden. Das gilt auch dann, wenn der Datenträger formatiert wird. Aus datenschutzrechtlicher Sicht ist das – zumal im Bereich der Bundesverwaltung – problematisch, schreibt doch das DSG vor, dass nicht mehr benötigte Personendaten zu vernichten sind. Einige Softwarehersteller bieten Lösungen an, die eine physikalische Löschung der Daten garantieren.

Gemäss dem Bundesgesetz über den Datenschutz sind insbesondere in der Bundesverwaltung die nicht mehr benötigten Personendaten zu anonymisieren oder zu vernichten, soweit die Daten nicht für Beweis- oder Sicherungszwecke aufzubewahren oder dem Bundesarchiv abzuliefern sind. Sowohl eine herkömmliche Löschung der Daten als auch eine Formatierung der Datenträger erfüllt die Forderungen bezüglich der Löschung gemäss Datenschutzgesetzgebung nicht. Unter Löschung versteht man

die Vernichtung der Personendaten, so dass diese im nachhinein nicht mehr rekonstruiert werden können. Die herkömmlichen Löschbefehle der Informatikmittel löschen die Daten lediglich logisch, so dass diese mit verhältnismässig einfachen Werkzeugen wieder rekonstruiert werden können, sofern der gelöschte Teil des Speichermediums nicht bereits überschrieben wurde. Der «format»-Befehl kann beispielsweise durch den «unformat»-Befehl rückgängig gemacht werden und darf u. a. deshalb auch nicht als sicher betrachtet werden. Bei der Low Level-Formatierung (Format /U) von DOS werden Sektoren und Spuren auf der Festplatte neu angelegt und mit einem Bitmuster einmal überschrieben. Bezüglich dieser Löschqualität gehen die Meinungen auseinander. Während die einen behaupten, dass damit alle Daten unwiderruflich gelöscht werden, halten andere fest, dass es Programme gibt, welche die ursprünglichen Daten wieder herstellen können. Insbesondere im Umfeld der Betriebssysteme DOS und Windows gibt es heute Werkzeuge, die es erlauben Dateien zu löschen, so dass diese nicht mehr hergestellt werden können. Sie überschreiben den gelöschten Bereich eines Disks mit einem oder mehreren Bitmustern, so dass die ursprünglichen Daten nicht mehr aufbereitet werden können. Für die Überschreibung werden beispielsweise beim Produkt Pretty Good Privacy (PGP) folgende Angaben gemacht:

- 3 Überschreibungsdurchläufe bei privater Nutzung
- 10 Überschreibungsdurchläufe bei geschäftlicher Nutzung
- 18 Überschreibungsdurchläufe bei militärischer Nutzung
- 26 Überschreibungsdurchläufe für maximale Sicherheit

Professionellen Firmen, die sich mit der Wiederherstellung von Daten befassen, ist es gelungen, Daten zu rekonstruieren, die neun mal überschrieben wurden. Bei der Überschreibung scheint das Bitmuster eine nicht unerhebliche Rolle zu spielen. Es ist auch zu berücksichtigen, dass für die Mehrfachüberschreibungen die notwendige Zeit einzuplanen ist. Wie bereits weiter oben festgehalten, existieren solche Werkzeuge insbesondere im Bereich von DOS- und Windows-Systemen. Bei anderen Betriebssystemen müssen z. T. andere Verfahren angewendet werden. Es gibt namentlich noch die Möglichkeiten der Löschung der Daten mit grossen magnetischen Feldstärken oder die mechanische Zerstörung der Datenträger. Beide Vorgehen führen aber – im Vergleich zu den oben beschriebenen Massnahmen – meist zu erheblichen Mehrkosten. Bei Projekten ist deshalb bereits im Pflichtenheft zu fragen, mit welchen Verfahren oder Massnahmen die Lösungsanbieter gedenken, die «garantierte» physikalische Löschung der Daten zu gewährleisten. Muss man im nachhinein (nach den Projektplanungsphasen und nach der Projektausschreibung) nach Lösungen für die physikalische Datenvernichtung suchen, so kommt eine Lösung meist teurer zu stehen, als wenn man diese bereits am Anfang des Projektes berücksichtigt hätte.

2.1.3 Auswertung von Web-Server Log-Dateien

Ein Grundsatz des Datenschutzes ist, dass die Datenbearbeitung auf das für die Aufgabenerfüllung notwendige Minimum zu beschränken ist. Für die Auswertung von Protokolldateien (Webserver-Logdateien) ist es normalerweise nicht notwendig, dass die IP-Nummer (ein bestimmbares Personendatum) verwendet wird. Durch die Pseudonymisierung dieser Nummer können der direkte Personenbezug eliminiert und die Logdateien in anonymisierter Form den Auswertenden zur Verfügung gestellt werden.

Heute stellen viele Organisationseinheiten bzw. Firmen der Öffentlichkeit über das Internet Informationen zur Verfügung. Für den Informationsanbieter ist sicher von Interesse, welche Informationen von den Interessierten abgefragt werden bzw. wurden und allenfalls in welcher Reihenfolge oder auf welchem Weg man zu den gewünschten Informationen gelangt ist. Dazu benötigt man aber nicht Informationen wie beispielsweise die IP-Adressen, mit welchen man unter Umständen die abfragenden Personen oder die Provider bestimmen könnte. Aus datenschutzrechtlicher Sicht genügt es nicht, wenn die Organisationseinheit, welche die Internetprotokolle aufzeichnet, und die Stelle, welche die Informationen im Internet zur Verfügung stellt, vertraglich festhalten, dass die Protokolle nur zum jeweiligen Zweck ausgewertet werden dürfen. Die Systeme sind technisch und organisatorisch so zu gestalten, dass mögliche Missbräuche oder zweckfremdes Handeln verunmöglicht werden.

Grundsätzlich geht der Datenschutz davon aus, dass nur ein Minimum der für die Aufgabenerfüllung notwendigen Personendaten für die jeweilige Datenbearbeitung zur Verfügung zu stellen ist. Einen guten Lösungsansatz sehen wir im vorliegenden Fall darin, dass man die Log-Dateien anonymisiert oder allenfalls pseudonymisiert. Sofern der Web-Systembetreiber die Log-Dateien in dieser Form an die Organisationseinheiten (Fachbereiche) weitergibt, haben wir aus der Sicht des Datenschutzes keine Einwendungen. Ist eine Identifikation für die zeitliche Nachvollziehbarkeit der Bearbeitung notwendig, so kann man beispielsweise die IP-Adressen durch jeweils gleichbleibende nicht sprechende Zeichenfolgen ersetzen, so dass diese Protokolle keine Rückschlüsse mehr auf die Personendaten erlauben. Selbstverständlich müsste der Algorithmus so aufgebaut sein, dass eine Ein-, aber nicht eine Eineindeutigkeit vorhanden ist. Dies bedeutet, dass dieselbe Quelle immer dasselbe Ziel ergibt, vom Ziel aber nicht auf die Quelle zurückgeschlossen werden kann. Ideal wäre es, wenn die Systeme direkt pseudonymisierte Nummern vergeben, so dass die Protokolle direkt in dieser Form geschrieben werden, und nicht im nachhinein noch eine Pseudonymisierung der identifizierenden Daten durchgeführt werden muss. Im Einzelfall soll aber auch eine Depseudonymisierung der Nummern möglich sein. Diese darf aber nur

über ein Mehraugenprinzip (Funktionstrennung) erfolgen. Es gilt zu beachten, dass ein sicheres Pseudonym nur entstehen kann, wenn die Ausgangsbasis der Daten als sicher betrachtet werden kann. IP-Adressen kann man bekanntlich sehr einfach verändern, so dass das Aufsetzen auf diese Datenbasis nicht unbedingt sinnvoll ist.

2.1.4 Datenschutzprobleme bei modernen Kopiergeräten und Druckern

In letzter Zeit haben sich Fotokopierer zu eigentlichen Multifunktionsgeräten mit viel eigener «Intelligenz» entwickelt. Dadurch sind auch Datenschutzrisiken entstanden. Werden die Dokumente digital gescannt, liegen sie für eine gewisse Zeit in einem Speicher vor. Das Gerät kann auch in ein EDV-Netz integriert sein. Grund genug, um diese Geräte aus der Sicht des Datenschutz näher unter die Lupe zu nehmen.

Vielen Benutzern ist völlig unbekannt, dass der moderne Digitalkopierer, den sie täglich nutzen, von jedem Dokument eine digitale Kopie erstellt und diese womöglich längere Zeit verfügbar hält. So können sich Unmengen von vertraulichen Dokumenten anhäufen. Das Risiko eines unbefugten Zugriffes ist daher nicht zu unterschätzen.

Digitalkopierer duplizieren die Dokumente nicht nur, sie scannen diese erst ein, was zu diversen Nachbearbeitungsmöglichkeiten dient. Die Geräte können auch in ein Firmennetz integriert sein; zudem sind sie allenfalls gleichzeitig auch mit Faxfunktionen ausgerüstet. Diese Zusatzfunktionen bedingen die digitale Zwischenspeicherung der Dokumente im RAM (flüchtiger Speicher) und oft auch auf Festplatten.

Je nach Gerät und Einstellungen werden die Daten nach jedem Druckauftrag, nach jedem Neustart des Gerätes oder nach einer vordefinierten Zeit oder auch gar nie automatisch gelöscht. Teilweise besteht eine manuelle Löschmöglichkeit durch den Benutzer. Bereits eine Funktion, vom letzten verarbeiteten Dokument eine Kopie zu ziehen, kann verheerende Auswirkungen haben.

Unbefugte dürfen keine Möglichkeit haben, Datenträger (in der Regel Harddisks), die kopierte/gescannte Dokumente enthalten, aus dem Gerät zu entfernen. Beim Austausch von Festplatten durch Servicepersonal sind dieselben Sicherheitsmassnahmen zu beachten wie bei jedem Rechner: Die Daten sind unwiderruflich zu löschen, bevor der Datenträger die Firma verlässt.

Ein weiteres Risiko ist der Netzzugriff auf das Gerät (falls vorhanden) von einem entfernten Arbeitsplatz her. Hier sind strikte Zugriffsregelungen zu implementieren. Einige Hersteller bieten optionale Lösungen an, die eine erhöhte Sicherheit bieten. Unabdingbar ist, dass alle Mitarbeiter, die mit digitalen Kopiergeräten arbeiten, über die Funktionen und die Risiken instruiert werden, damit sie sich entsprechend verhalten.

Bereits bei der Evaluation von digitalen Kopiergeräten ist darauf zu achten, dass sie hardware- und softwaremässig so betrieben werden können, dass die Datenschutz- und Datensicherheitsbedürfnisse der Firma vollumfänglich abgedeckt werden können. Die Betreiberin ist als Inhaberin der Datensammlung denn auch dafür verantwortlich: Das Datenschutzgesetz verlangt ausdrücklich, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Benutzer sollten sensible Dokumente nicht auf einem Gerät fotokopieren, von dem sie nicht wissen, wie die Daten bearbeitet werden, und insbesondere, welche Zugriffsmöglichkeiten bestehen.

2.1.5 Trusted Computing Platform Alliance (TCPA) und Datenschutz

Die Begriffe Sicherheit (security) und Vertrauen (trust) werden von Herstellern und Dienstleistern der IT-Branche in der Marketing-Kommunikation sehr häufig verwendet. Dass diese sehr positiv klingenden Ausdrücke kaum einen fassbaren Inhalt aufweisen, wenn sie nicht präzisiert werden, schadet leider der Klarheit.

Unter dem Titel TCPA wird seit Jahren von einer grossen Zahl der wichtigsten Hersteller von Hardware und Betriebssoftware für PCs ein Projekt vorangetrieben, dessen präzises Ziel zumindest auf den ersten Blick nicht vollständig klar erscheint. Seine verschiedenen Aspekte sowie die Tatsache, dass nebst den angesprochenen Herstellern in erster Linie die Unterhaltungsindustrie der Bereiche Musik und Film an TCPA interessiert sind, lassen darauf schliessen, dass ein Hauptziel des Vorhabens in der Steigerung technischer Möglichkeiten für den Kopierschutz von urheberrechtlich geschützten Werken liegt. Bei erster Betrachtung liegt hier nicht hauptsächlich ein Datenschutzthema vor, ein genauerer Blick zeigt jedoch, dass Datenschutz von dieser Entwicklung durchaus stark betroffen sein könnte. Wir können hier nicht auf die potentiell enormen Überwachungsfolgen eingehen, welche durch das für TCPA zentrale so genannte Digital Rights Management geschaffen würden. Wir müssen jedoch darauf hinweisen, dass nach all den bisher vorliegenden Informationen zu TCPA den Benutzern in Zukunft eine Infrastruktur verkauft werden soll, deren Sicherheitsfunktionen sie selbst weder steuern noch im Detail nachvollziehen können. Damit wird nicht nur ein Zustand von Intransparenz geschaffen, sondern auch letztlich die informationelle Selbstbestimmung der Benutzer verunmöglicht. Dementsprechend haben die deutschen Datenenschutzbeauftragten des Bundes und der Länder in einer Entschliessung ihrer 57. Konferenz (http://www.lfd.m-v.de/beschlue/ent57.html) gefordert, dass die Hersteller von Informations- und Kommunikationstechnik Hard- und Software in einer Art und Weise entwickeln und herstellen, welche Anwendern und

unabhängigen Dritten ermöglicht, sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen zu überzeugen. Dieser Forderung können wir uns anschliessen.

In einer der frühesten und bisher gründlichsten Analysen (vgl. http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html) von TCPA / Palladium (die TCPA-Version von Microsoft) hat Ross Anderson – ein weltweit führender Experte für Sicherheitstechnologie – eine zentrale Frage sehr schön auf den Punkt gebracht: Er stellt die rhetorische Frage, ob denn bessere Sicherheit für PCs nicht eine gute Sache sei. Als «Antwort» darauf stellt er gleich anschliessend die eigentliche Kernfrage: «Sicherheit für wen?». Einige Elemente von Andersons Antwort darauf lauten folgendermassen: Weder Virenprobleme noch das Problem der Überflutung mit unerwünschter Werbung per Mail (Spam) werden durch TCPA gelöst. Und auch die Verletzung von Persönlichkeitsrechten bzw. des Datenschutzes schränkt die Technologie nicht ein. Die Sicherheitsinteressen, welche durch TCPA in erster Linie geschützt werden, sind nicht diejenigen der PC-Benutzer, sondern die der PC-Verkäufer, der Softwarelieferanten und der so genannten Content-Industrie (Musik, Film, Spiele).

2.1.6 Weiterbildung der Informatiksicherheitsbeauftragten des Bundes im Bereich technischer Datenschutz

Für die Informatiksicherheitsbeauftragten des Bundes (ISBO) gibt es jetzt einen Weiterbildungskurs über technische und organisatorische Datenschutzmassnahmen. Behandelt werden vor allem Themen wie Pseudonymisierung/Anonymisierung von Personendaten, deren Verschlüsselung ab Erfassung, Bearbeitungsbedingungen von Protokollierungsdateien sowie Anmeldungspflicht und Ausübung des Auskunftsrechts. Durch diesen speziellen Ansatz lassen sich die gängigen Datensicherheitsmassnahmen erweitern.

Die Informatiksicherheitsbeauftragten der Organisationseinheiten (ISBO) des Bundes haben die Möglichkeit, regelmässig an Weiterbildungstagen über Neuerungen im Bereich Informatiksicherheit teilzunehmen. Wir haben vorgeschlagen, dieses Angebot durch Informationen mit dem Schwerpunkt technische und organisatorische Datenschutzmassnahmen zu ergänzen. Ausgegangen wird von der Tatsache, dass die Grundsätze der Verhältnismässigkeit und der Zweckbindung Methoden zur Datenvermeidung bzw. -sparsamkeit verlangen, die zugleich zur Verringerung des Umfangs und der Komplexität von Anwendungen und Datenbanken beitragen. Betont wird dabei, dass die Unmenge von Protokollierungsdateien, die auf quasi unkontrollierte Weise am Rande der Anwendungen und Informatiksysteme produziert werden, diesen Grundsätzen unbedingt entsprechen müssen. Anschliessend werden die verschiedenen Varianten und Möglichkeiten der Pseudonymisierung und Anonymisierung von

Daten vorgestellt und ausführlich erklärt. Betont wird vor allem die Verschlüsselung besonders schützenswerter Daten ab ihrer Erfassung und nicht erst bei ihrer Speicherung oder Weitergabe. Der Vorteil besteht darin, dass die Daten damit ab ihrer Erfassung beispielsweise gegenüber Systemadministratoren und auf den Archivierungsdatenträgern geschützt sind. Die notwendige Verfügbarkeit der verschlüsselten Daten führt sodann zur eminent wichtigen Frage der zentralen Aufbewahrung des verwendeten Chiffrierschlüssels und des zusätzlichen Standardschlüssels zur Entschlüsselung. Die genaue Abklärung des Zwecks solcher Massnahmen, die nur mit absoluter Transparenz gegenüber den betroffenen Personen ergriffen werden dürfen, erlaubt es in der Regel festzustellen, ob sie gerechtfertigt sind. Schliesslich wird an andere besondere Grundsätze des Datenschutzes erinnert, wie beispielsweise die Notwendigkeit einer Abfrageroutine als Voraussetzung für die Ausübung des Auskunftsrechts durch die betroffenen Personen, oder die Anmeldungspflicht des Inhabers der Datensammlung. Wichtig ist es zu verstehen, dass sich die Datensicherheits- und -schutzmassnahmen zwar gegenseitig ergänzen, eine hohe Datensicherheit aber nicht unbedingt einen guten Datenschutz gewährleistet (z.B. die missbräuchliche Beschaffung von Personendaten, die in chiffrierter Form gespeichert werden), wohingegen ohne optimale Datensicherheit (Kennwort, Virusscanner, Firewalls, usw.) kein hohes Datenschutzniveau zu erreichen ist. Auch sei daran erinnert, dass die Sicherheit von Informationen aus einem Gleichgewicht zwischen physischer, technischer, organisatorischer und menschlicher Sicherheit besteht. Die Erfahrungen im Laufe des ersten Jahres der Zusammenarbeit haben deutlich gemacht, dass die ISBO an datenschutzspezifischen Methoden interessiert sind, da sie damit ihre unbestrittenen Kompetenzen in Sachen Datensicherheit ergänzen können.

2.2 Weitere Themen

2.2.1 Die nationale Datenbank für Sport

Das Bundesamt für Sport hat im Rahmen der Neuorganisation der Institution Jugend+Sport (J+S) eine nationale Datensammlung für Sport (NDS) geschaffen. Sie enthält Angaben zu den Kursleitern und erlaubt zudem eine gesamtschweizerisch einheitliche Verwaltung und Abrechnung der von J+S angebotenen Kurse.

Das Bundesamt für Sport BASPO hatte die Aufgabe, eine Gesamtüberprüfung der Institution «Jugend+Sport» (J+S) vorzunehmen, um den heutigen Anforderungen besser begegnen zu können. Dazu gehörte auch die Schaffung einer nationalen Datenbank für Sport (NDS), dank der die Bereiche der Jugendausbildung sowie der Kaderbildung

von J+S gesamtschweizerisch einheitlich elektronisch verwaltetet und die J+S-Kurse abgerechnet werden können. Die NDS ersetzt die bisher in den Kantonen angewandten, unterschiedlichen Informatikprogramme.

Wir haben das BASPO bei der Schaffung der gesetzlichen Grundlage für die nationale Datenbank unterstützt. Zusammen mit dem BASPO haben wir besonderen Wert darauf gelegt, dass die Verantwortlichkeit der Datenbearbeitung, die zahlreichen Zugriffsberechtigungen und der Bearbeitungsumfang klar und transparent geregelt wurden. Im Anhang der Verordnung werden der gesamte Datenkatalog detailliert aufgeführt und die Zugriffsberechtigungen der einzelnen Organisationseinheiten abschliessend geregelt.

Die Verordnung regelt nicht nur klar, welchen Behörden und Organisatoren von Sportveranstaltungen die Personendaten im Abrufverfahren zugänglich gemacht werden, sondern hält ebenso deutlich fest, unter welchen Voraussetzungen Personendaten aus dem Bereich von J+S an Dritte herausgegeben werden dürfen.

2.2.2 Eingangskontrolle mittels Fotos in einem Fitnesscenter

Nur wer bereit war, ein Foto von sich machen zu lassen, konnte ein Abonnement für ein Fitnesscenter erwerben. Unklar blieb dabei, zu welchen Zwecken das Fitnesscenter die Fotos verwendet. Wir haben gegen diese Praxis eine Empfehlung erlassen, die von der Betreiberin des Fitnesscenters angenommen worden ist. Den Text der Empfehlung finden Sie Abschnitt 13.7.1.

In einem Fitnesscenter konnte man nur dann ein Abonnement lösen, wenn man bereit war, sich fotografieren zu lassen. Diese Foto wurde in eine Mitgliederkartei aufgenommen, die gemäss Aussage des Fitnessclubs zu Identifikations- und Kontrollzwecken dienen sollte. In den allgemeinen Geschäftsbedingungen hiess es dazu lediglich, dass der Betroffene zur Kenntnis nehmen müsse, dass eine Fotografie von ihm erstellt werde, und dass diese internen Zwecken diene. Unhaltbar dabei war, dass das Fitnesscenter die Einzelheiten der Datenbearbeitung nicht klar offen legte. So blieb unbestimmt, in welcher Art und Weise die Fotografie eingesetzt wird, wie lange die Daten aufbewahrt werden und welche Zwecke mit dieser Datenbearbeitung nebst der visuellen Kontrolle noch verfolgt werden.

Als wir das Fitnesscenter darauf aufmerksam gemacht haben, dass eine derartige Praxis nicht datenschutzkonform sei, hielt es uns mit Verweis auf die allgemeinen Geschäftsbedingungen entgegen, dass die Fotos mit ausdrücklicher Einwilligung der betroffenen Personen erstellt worden seien. Zudem berief es sich auf den Rechtfertigungsgrund des überwiegenden Interesses an der Bearbeitung von Personendaten in

unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags.

Wir haben dem Fitnesscenter in einer Empfehlung dargelegt, dass eine betroffene Person nur dann rechtsgültig einwilligen kann, wenn sie offen und umfassend über die Einzelheiten der Datenbearbeitung informiert worden ist. Aus einer unbestimmt formulierten Klausel in den allgemeinen Geschäftsbedingungen lässt sich aber nicht eine Einwilligung ableiten. Weiter haben wir aufgezeigt, weshalb selbst bei Vorliegen eines Vertrages nicht jede Bearbeitung von Personendaten zulässig ist. So verlangt der Grundsatz der Verhältnismässigkeit, dass nur jene Datenbearbeitung erfolgen darf, die für die Erreichung eines bestimmten Zwecks objektiv tatsächlich notwendig ist und die zur Persönlichkeitsbeeinträchtigung in einem vernünftigen Verhältnis steht.

Somit reicht es aus, wenn sich das Mitglied zusätzlich zu seinem Abonnement mittels eines amtlichen und mit einer Fotografie versehenen Ausweises, z.B. Identitätskarte, legitimiert. Denkbar ist auch, dass den Mitgliedern ein Abonnement ausgehändigt wird, auf der eine Fotografie des Berechtigten angebracht ist und die dann bei Eintritt vorgewiesen werden muss. Beide Massnahmen ermöglichen eine eindeutige Identifikation des Berechtigten und greifen im Vergleich zur Fotokartei weniger stark in die Persönlichkeitssphäre der betroffenen Personen ein.

Wir haben das Fitnesscenter in der Empfehlung aufgefordert, die Betroffenen vor Vertragsabschluss in adäquater Form ausdrücklich und umfassend auf den Zweck und Umfang der Datenbearbeitung hinzuweisen oder aber ihnen die Möglichkeit anzubieten, Abonnemente zu lösen, ohne dass dabei die Fotografie der Betroffenen in eine Fotokartei aufgenommen wird.

Das Fitnesscenter hat unsere Empfehlung angenommen und klärt die Mitglieder nun in den überarbeiteten allgemeinen Geschäftsbedingungen transparent und umfassend über die Bearbeitung der Personendaten auf.

2.2.3 Selbstbedienungsprinzip im Fotoladen ist unzulässig

Immer öfter gilt beim Abholen von entwickelten Fotos das Selbstbedienungsprinzip. Dabei können problemlos fremde Fotos angeschaut oder sogar die Bilder entwendet werden. Der Fotohändler muss mit organisatorischen Massnahmen dafür sorgen, dass nur berechtigte Personen auf die Fototaschen zugreifen können.

Uns erreichen immer wieder Anfragen von Personen, die ihre Filme zum Entwickeln zu einem Grossverteiler, Detaillisten oder in ein Fotofachgeschäft gebracht haben. Beim

Abholen der entwickelten Fotos stellen die Kundinnen und Kunden erstaunt fest, dass man die Fototasche mit den eigenen Fotos selber aus einer Vielzahl von anderen Fototaschen heraussuchen muss. Auf jeder Fototasche steht der Name und die Adresse der berechtigten Person, und sie enthält die Fotos sowie den entwickelten Film. Für Neugierige ist es somit ein Leichtes, sich irgendeine Fototasche herauszuzupfen, sie zu öffnen und sich die fremden Fotos anzuschauen bzw. die Bilder sogar zu entwenden. Tests der Stiftung für Konsumentenschutz haben gezeigt, dass in einigen Fällen sogar ganze Fototaschen von Unberechtigten «gekauft» werden konnten.

Der Name, die Adresse und die Bilder sind Personendaten im Sinne des Datenschutzgesetzes. Der Fotohändler, der die entwickelten Fotos für die Kundschaft bereit hält, muss dabei die Grundsätze des Datenschutzes berücksichtigen und die ihm anvertrauten Personendaten vertraulich behandeln. So muss er durch angemessene organisatorische Massnahmen dafür sorgen, dass die Personendaten gegen unbefugtes Bearbeiten geschützt sind. Der Händler missachtet diese Vorschrift, wenn er einfach die Fototaschen samt Inhalt in einer Selbstbedienungskiste im Laden aufstellt. Damit verletzt er widerrechtlich die Persönlichkeit seiner Kundinnen bzw. Kunden und verstösst so gegen den Datenschutz.

Somit gilt: Das Selbstbedienungsprinzip beim Abholen von entwickelten Fotos ist unzulässig. Der Händler hat dafür zu sorgen, dass die Fototaschen in einem für die Kundschaft nicht frei zugänglichen Bereich aufbewahrt werden und dass nur das dazu berechtigte Verkaufspersonal Zugriff auf die Fototaschen hat. Das Personal muss sich bei der Herausgabe der entwickelten Fotos auch vergewissern, ob die Kundin bzw. der Kunde tatsächlich die eigenen Fotos abholt, indem es überprüft, ob der vorgewiesene Kontrollbeleg mit der Nummer auf der Fototasche übereinstimmt.

2.2.4 Umfrage des TCS bei seinen Mitgliedern

Eine Mitgliedschaft in einem Verein verpflichtet nicht dazu, dem Vereinsvorstand alle Angaben über seine Person bekannt zu geben. Stehen die verlangten Personendaten nicht in direktem Zusammenhang mit dem Vereinszweck, so muss der Vorstand die Mitglieder vorgängig darüber informieren, zu welchem Zweck er die Daten verwendet, und dass die Bekanntgabe der Personendaten – da kein unmittelbarer Bezug zum Vereinszweck besteht – freiwillig ist.

Der TCS hat seine Mitglieder ohne grosse Zusatzinformationen dazu aufgefordert, einen Fragebogen auszufüllen. Dieser enthielt unter anderem Fragen zur Partnerin bzw. zum Partner (Name, Vorname, Geburtsdatum, Nationalität), zu unterhaltspflichtigen Kindern, zum jährlichen Brutto-Haushaltseinkommen, zu Hobbies usw. Zahlreiche

TCS-Mitglieder haben sich an uns gewandt und wollten wissen, ob die Art und Weise der Informationsbeschaffung durch den TCS zulässig sei.

Der TCS erhält durch die ausgefüllten und retournierten Fragebogen detaillierte Angaben zu den einzelnen Mitgliedern. Er bearbeitet damit Personendaten und muss dabei das Datenschutzgesetz beachten. Wir haben dem TCS ausführlich dargelegt, weshalb sein Vorgehen in verschiedener Hinsicht nicht datenschutzkonform ist. So verlangt beispielsweise das Transparenzprinzip (Grundsatz von Treu und Glauben) eine offene und umfassende Information über den Zweck und Umfang der bearbeiteten Personendaten. Dazu gehört auch, dass den Befragten mitgeteilt wird, ob ihre Personendaten an Drittunternehmen weitergegeben werden und – sofern dies der Fall ist – an wen und zu welchem Zweck dies geschieht. Das Verhältnismässigkeitsprinzip erlaubt nur die Bearbeitung jener Personendaten, die zur Zweckerreichung tatsächlich benötigt werden. Die Zweckbindung wiederum verpflichtet den Datenbearbeiter, die Personendaten nur zu dem Zweck zu bearbeiten, der bei der Beschaffung angegeben worden ist.

Der TCS erhält mit dieser Umfrage-Aktion von seinen Mitgliedern umfassende Informationen, die für die Zweckerreichung des Vereins nicht direkt erforderlich sind. Er muss daher die Mitglieder vorgängig auf diesen Umstand aufmerksam machen und ausdrücklich darauf hinweisen, dass die Teilnahme an der Umfrage freiwillig ist.

Nach unserer Intervention war der TCS schliesslich damit einverstanden, das Versäumte nachzuholen, und er hat sich bereit erklärt, in seiner Club-Zeitschrift über alle Einzelheiten im Zusammenhang mit der durchgeführten Umfrage zu informieren (z.B. Sinn und Zweck der Umfrage, Umfang der Datenbearbeitung, allfällige Weitergabe an Dritte, Aufbewahrungsdauer, Widerrufsrecht, Verantwortlichkeit für die Umfrage usw.).

Der TCS hat auch versichert, in Kürze ein Datenschutzkonzept auszuarbeiten. Damit möchte er jederzeit einen datenschutzkonformen Umgang mit den Personendaten seiner Mitglieder sicherstellen.

3. Justiz/ Polizei/ Sicherheit

3.1 Polizeiwesen

3.1.1 Biometrische Daten in Ausweispapieren

Die Aufnahme von biometrischen Daten in Ausweispapiere muss die allgemeinen Datenschutzgrundsätze – insbesondere die Zweckbindung und die Verhältnismässigkeit – beachten. Das bedeutet, dass die verfolgten Ziele klar definiert werden müssen und dass alle anderen Mittel, mit denen sie sich erreichen lassen, zu prüfen sind. Falls die Einführung von biometrischen Daten sich als notwendig und zur Zielerreichung geeignet erweist, müssen die biometrischen Daten, die in Ausweispapiere aufgenommen werden, entsprechend dem Risiko einer Persönlichkeitsverletzung ausgewählt werden.

Nach den tragischen Ereignissen vom 11. September 2001 drängen die Vereinigten Staaten die übrigen Länder, die Pässe mit mechanisch lesbaren biometrischen Daten zu versehen. Die Bürger von Staaten, deren Ausweispapiere keine biometrischen Daten enthalten, werden (wahrscheinlich ab Ende 2004) nicht mehr ohne Visum in die Vereinigten Staaten reisen können. Im Rahmen der Einführung des neuen Schweizer Passes und der neuen Schweizer Identitätskarte stellte sich auch die Frage der biometrischen Daten. Es handelt sich um einen Vorgang, der eine Änderung des Gesetzes über die Identitätsdokumente sowie technische Anpassungen erfordern würde.

Bevor neue biometrische Daten in Ausweispapieren aufgenommen werden – Lichtbild, Körpergrösse und Unterschrift stellen bereits biometrische Angaben dar – , müssen unbedingt die Zweckbestimmungen der geplanten Bearbeitungen definiert werden: Identifizierung des Dokumenteninhabers, Vergleichen mit einer Suchdatenbank, Speicherung der Kontrolle bzw. der Einreisedaten in einer Datensammlung. Anschliessend muss die Verhältnismässigkeit der geplanten Massnahmen sorgfältig untersucht werden. Dabei sind alle Mittel zu prüfen, mit welchen sich die Zielsetzungen erreichen lassen. Es kommen nur die Möglichkeiten in Betracht, welche die Persönlichkeit der betroffenen Personen am wenigsten beeinträchtigen (d.h. beispielsweise keine schützenswerten Daten enthalten oder keine Erstellung von Persönlichkeitsprofilen erlauben). Sollte sich die Einführung von biometrischen Daten letztlich als notwendig erweisen, so müssten jene ausgewählt werden, welche die Persönlichkeit am wenigsten gefährden. Biometrische Daten, aus denen sich Hinweise zur Gesundheit oder zur Intimsphäre ableiten lassen, sind ausgeschlossen.

Der Verlauf der internationalen Diskussion zur Nutzung von biometrischen Daten – insbesondere in den Bereichen Luftfahrt und Terrorismusbekämpfung – wird für den Standpunkt der Schweiz entscheidend sein.

3.1.2 Geplante Massnahmen betreffend Hooliganismus/Rassismus und Extremismus/Terrorismus

Im Zusammenhang mit den geplanten Massnahmen gegen Rassismus und Hooliganismus soll unter anderem eine so genannte «Hooliganismusdatenbank» geschaffen werden. Zum entsprechenden Gesetzesentwurf konnten wir Stellung nehmen. Weitere Massnahmen sind im Bereich Terrorismus/Extremismus geplant.

Der Bundesrat hat beschlossen, die betreffend Rechtsextremismus anstehenden Rechtssetzungsvorhaben in zwei Pakete aufzuteilen: Einem ersten Paket Rassismus/Hooliganismus und einem zweiten Paket Terrorismus/Extremismus.

Betreffend das erste Paket konnten wir im Rahmen der Ämterkonsultation zum Bundesgesetz über Massnahmen gegen Rassismus und Hooliganismus Stellung nehmen. Dieses Gesetz sieht als Massnahme gegen den Rassismus unter anderem die Möglichkeit vor, Propagandamaterial zu beschlagnahmen. Als Massnahme gegen den Hooliganismus soll mit diesem Gesetz zudem ein Informationssystem geschaffen werden, in dem Daten über Personen aufgenommen werden sollen, die sich an Publikumsveranstaltungen, namentlich an Sportveranstaltungen, gewalttätig verhalten. Diesbezüglich stellten sich für uns verschiedene datenschutzrechtliche Fragen. Den Erläuterungen zum Gesetzesentwurf konnten wir unter anderem entnehmen, dass spontane Gewaltausschreitungen nicht von der vorliegenden Gesetzesvorlage erfasst werden sollten, da diese keine Befassung durch die Staatsschutzbehörden rechtfertigen würden. Dem stimmten wir zu, wiesen aber darauf hin, dass für die Abgrenzung zwischen spontaner und organisierter Gewalt klare Kriterien gefunden werden müssten. Weiter hielten wir fest, dass im Gesetz klar umschrieben werden müsse, welche Personendaten im neuen Informationssystem bearbeitet werden könnten. Aus diesem Grund lehnten wir einen Teil der entsprechenden Formulierung im Gesetzesentwurf als viel zu vage und unklar ab. Auch das Informationssystem muss in der gesetzlichen Grundlage klar umschrieben sein. Dementsprechend verlangten wir, dass die Datenkategorien sowie die Behörden, die auf das Informationssystem Zugriff erhalten sollen, im Gesetz selbst aufgeführt werden müssten. Im Gesetzesentwurf ist sodann vorgesehen, dass die Organisatoren unter bestimmten Voraussetzungen Daten aus der neuen Datenbank erhalten sollen. Hier ist es wichtig dafür zu sorgen, dass diese Daten von den Organisatoren nach der Publikumsveranstaltung wieder gelöscht wer-

den, damit diese mit den betreffenden Personendaten keine eigenen Hooligansdatenbanken aufbauen können.

Betreffend das Paket Terrorismus/Extremismus liegen noch keine konkreten Gesetzänderungsvorschläge vor. Wir hatten Gelegenheit, diesbezüglich zu einem Aussprachepapier an den Bundesrat Stellung zu nehmen. Unsere diesbezüglichen Äusserungen fielen angesichts der Tatsache, dass noch keine fassbaren Vorschläge vorliegend, auch sehr allgemein aus. Wir behielten uns ausdrücklich vor, ausführlicher Stellung zu nehmen, sobald uns konkrete Gesetzesvorschläge unterbreitet würden.

3.1.3 Erfahrungen mit dem indirekten Auskunftsrecht

Die Behandlung der indirekten Auskunftsgesuche im Zusammenhang mit der inneren Sicherheit und der Bekämpfung der Geldwäscherei verlief ohne Hindernisse. Diejenige betreffend organisierte Kriminalität, illegalem Drogenhandel, Falschmünzerei, Menschenhandel und Pornographie dagegen bereitete aufgrund der Natur des Informationssystems JANUS weiterhin Schwierigkeiten. Einige Gesuche wurden zudem vor die Datenschutzkommission gebracht.

Nachdem für den Zeitraum 2001/2002 ein deutlicher Anstieg der Anzahl Auskunftsgesuche gemäss dem Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) in das Staatsschutz-Informationssystem ISIS verzeichnet werden konnte, war die Anzahl der Gesuche im Zeitraum 2002/2003 wieder rückläufig. Der Anstieg war damals hauptsächlich auf die Behandlung von Personendaten durch den Dienst für Analyse und Prävention (DAP) des Bundesamtes für Polizei (BAP) im Rahmen des G8-Gipels in Genua zurückzuführen. Nun beträgt die Anzahl Gesuche wieder etwa gleich viel in den Zeiträumen 2000/2001 und 1999/2000. Dagegen nahm die Anzahl der indirekten Auskunftsgesuche gemäss Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes (ZentG) relativ stark zu. Dies ist vermutlich darauf zurückzuführen, dass nun mehr Leute Kenntnis von dieser Datenbank haben. Insgesamt ist die Anzahl der indirekten Auskunftsgesuche leicht zurückgegangen.

Betreffend die Behandlung der Gesuche hat sich an der Situation, wie wir sie in unserem letzten Tätigkeitsbericht beschrieben haben (9. Tätigkeitsbericht 2001/2002, Abschnitt 3.1.1), wenig geändert. So verlief die Überprüfung der Gesuche betreffend das System ISIS nach wie vor reibungslos. Das Gleiche gilt für die Gesuche nach ZentG betreffend das System GEWA bei der Meldestelle für Geldwäscherei. Auch betreffend die Auskunftsgesuche in JANUS hat sich seit unserem letzten Tätigkeitsbericht wenig verändert. Dem BAP ist es noch nicht gelungen, die in unseren Empfehlungen erwähnten Unstimmigkeiten zu korrigieren.

Schliesslich ist noch darauf hinzuweisen, dass in mehreren Fällen (sowohl betreffend ISIS als auch betreffend JANUS und GEWA) einige betroffene Personen ihren Fall vor die Eidgenössische Datenschutzkommission brachten.

3.2 Weitere Themen

3.2.1 Revision des Ausländergesetzes

Die Verwendung von genetischen Untersuchungen zur Identifizierung einer Person oder im Rahmen der Familienzusammenführung soll künftig im Bundesgesetz über genetische Untersuchungen beim Menschen geregelt werden. Da der Bedarf noch immer nicht nachgewiesen ist, läuft die Verwendung solcher Analysen dem Grundsatz der Verhältnismässigkeit zuwider. Der Einsatz der Videoüberwachung oder von Erkennungssystemen zur Identifizierung von Personen, die mit einem Einreiseverbot in die Schweiz belegt wurden und für die die Luftfahrtgesellschaften, welche sie befördert haben, aufkommen müssen, verstösst wegen der geringen Anzahl betroffener Personen gegen das Verhältnismässigkeitsprinzip. Der Einsatz derselben Mittel zu Zwecken, die nicht in das Ausländerrecht fallen, muss vertieft geprüft werden und bei nachgewiesener Notwendigkeit in Bestimmungen zur Polizei oder zur inneren Sicherheit geregelt werden.

Im Gegensatz zum ersten Entwurf des Ausländergesetzes ist in der Vorlage, die dem Parlament unterbreitet wurde, vom Einsatz genetischer Untersuchungen zur Identifizierung einer Person bzw. im Rahmen der Familienzusammenführung nicht mehr die Rede. Der Bundesrat verzichtet zwar nicht auf die genetischen Untersuchungen, aber sie werden künftig im Bundesgesetz über genetische Untersuchungen beim Menschen geregelt. Die Notwendigkeit genetischer Untersuchungen zur Erfüllung von Aufgaben im Ausländerrecht ist nicht nachgewiesen. Deshalb läuft der Einsatz von genetischen Untersuchungen in diesem Kontext dem Verhältnismässigkeitsgrundsatz zuwider. Gleiches gilt für den Entwurf des Asylgesetzes, der dem Parlament vorliegt (siehe unseren 9. Tätigkeitsbericht 2001/2002, Abschnitt 3.2.1).

Der Gesetzesentwurf sieht ebenfalls die Nutzung von biometrischen Daten zur Identifizierung vor. In der Vollzugsverordnung soll die abschliessende Liste dieser Daten verankert werden. Was die Gefahr der Beeinträchtigung der Persönlichkeit wegen der Verwendung biometrischer Daten anbelangt, wird auf Abschnitt 3.1.1 des vorliegenden Berichts verwiesen.

Den problematischsten Punkt des Gesetzesentwurfs bildet der geplante Einsatz von Videoüberwachungs- oder Erkennungssystemen (einschliesslich des Vergleichs mit Suchsystemen) nicht nur zur Identifizierung von Personen, die mit einem Einreiseverbot in die Schweiz belegt wurden und für die die Luftfahrtgesellschaften, die sie befördert haben, aufkommen müssen, sondern auch zu anderen Zwecken, wie z.B. zur Verbesserung der Sicherheitsmassnahmen oder zum Informationsaustausch. Bezüglich der ersten Zweckbestimmung stellt sich angesichts der geringen Anzahl Personen, die so identifiziert werden können, die Frage nach der Verhältnismässigkeit der geplanten Massnahme. Für die übrigen Zweckbestimmungen ist der Einsatz der genannten Mittel zur Erfüllung von nicht definierten Gesetzesaufgaben im Rahmen des aktuellen Gesetzesentwurfs nicht zu rechtfertigen. Die Massnahmen sollten einerseits Gegenstand einer vertieften Überprüfung bilden, die das Gleichgewicht zwischen den Rechten der Einzelpersonen und der Einführung von verhältnismässigen Sicherheitsmassnahmen berücksichtigt; andererseits müssen sie bei nachgewiesenem Bedarf in der Gesetzgebung zum Polizeiwesen bzw. zur inneren Sicherheit, und nicht im Ausländergesetz, niedergelegt werden.

3.2.2 Datenschutzbestimmungen in den Rückübernahme- und Transitabkommen

Im Rahmen von Rückübernahme- und Transitabkommen mit Staaten ohne Datenschutzgesetzgebung wird die Bekanntgabe von Hinweisen zur Art des Ausweisungsbeschlusses bzw. der Behörde, die den Beschluss erlassen hat, den Grundsätzen der Zweckbindung und der Verhältnismässigkeit nicht gerecht. Die Bekanntgabe stellt kein notwendiges und zur Zielerreichung geeignetes Mittel dar d.h. zur Unterrichtung der Behörden, dass die von der Rückübernahme bzw. vom Transit betroffene Person ein konkretes und aktuelles Risiko für ihre eigene Sicherheit und für diejenige der ersuchten Behörden oder der Begleitpersonen bedeutet.

In den letzten Monaten wurden wir um Stellungnahmen zu Rückübernahme- und Transitabkommen zwischen der Schweizerischen Eidgenossenschaft und Staaten, die nicht über eine gleichwertige Datenschutzgesetzgebung verfügen (insbesondere asiatische und afrikanische Staaten), gebeten. In solchen Fällen muss der Datenschutz im Abkommen ausdrücklich geregelt werden. Anlässlich der Ämterkonsultation beurteilten wir die spezifischen Datenschutzbestimmungen als mit dem Schweizer Recht vereinbar. Diese Bestimmungen entsprechen im übrigen weitgehend den bereits geltenden Vorschriften. Der Anhang des vorliegenden Berichts enthält dazu eine Mindestdatenschutzklausel (siehe Abschnitt 13.4). Dagegen stellten wir fest, dass andere Bestimmungen nicht datenschutzrechtkonforme Bearbeitungen von Personendaten

vorsahen: Es handelt sich insbesondere um die Weitergabe von Hinweisen zur Art des (gerichtlichen oder administrativen) Ausweisungsbeschlusses bzw. zur verfügenden Behörde. In den Abkommensentwürfen und in den erläuternden Berichten werden das oder die Ziele der - unter Missachtung des Zweckbindungsgrundsatzes vorgesehenen - Bekanntgabe generell nicht erwähnt. Bisweilen hiess es, die Bekanntgabe verfolge das Ziel, den ersuchten Behörden mitzuteilen, dass die von der Rückübernahme oder vom Transit betroffene Person ein konkretes und aktuelles Risiko für ihre eigene Sicherheit und diejenige des ersuchten Staates oder der Begleitpersonen bedeute. Unseres Erachtens stellt die Bekanntgabe der Art des Ausweisungsbeschlusses oder der verfügenden Behörde kein notwendiges und geeignetes Mittel dar, um eine Rückübernahme bzw. einen Transit unter optimalen Sicherheitsbedingungen zu gewährleisten. Folglich verstösst eine solche Bekanntgabe gegen den Verhältnismässigkeitsgrundsatz. Dagegen ist die Warnung, die betroffene Person stelle möglicherweise eine Gefahr für die öffentliche Sicherheit, die Behörden der beiden Länder (insbesondere die Begleitpersonen) oder sich selbst dar, durchaus als angemessenes Mittel für die Zielerreichung zu betrachten. Ausserdem wird betont, dass die ersuchten Behörden unrichtige Schlüsse zur betroffenen Person ziehen könnten, wenn sie sich ausschliesslich auf die Art des Ausweisungsbeschlusses abstützen.

3.2.3 Videoüberwachung der SBB im Hauptbahnhof Zürich

Die Kontrolle der Videoanlagen der SBB im Hauptbahnhof Zürich, die wir bereits im Oktober 2001 durchführten, hat Mängel aufgezeigt und dazu geführt, dass Verbesserungen beim Datenschutz an die Hand genommen wurden. Auch werden für die Videoanlagen der SBB nun generell die nötigen gesetzlichen Grundlagen geschaffen. Einige Fragen sind jedoch immer noch offen.

Unsere Kontrolle der Videoanlagen im Hauptbahnhof Zürich (siehe auch 9. Tätigkeitsbericht, Abschnitt 3.2.2) hat gezeigt, dass die verschiedenen Videoüberwachungsinstallationen offensichtlich ohne genaues Konzept entstanden waren. Auch bei den SBB selbst schien niemand einen klaren Überblick über alle Überwachungsmassnahmen zu haben. Die Kontrolle hat diese Probleme ans Licht gebracht und bei den SBB das Bewusstsein für die Problematik geschärft. Nun sind Bestrebungen im Gange, die Videoüberwachung sauber zu regeln: Die SBB haben einerseits den Bundesrat um eine Rechtsgrundlage ersucht; andererseits wurde SBB-intern eine Arbeitsgruppe einberufen, um die bestehenden Ausführungsbestimmungen zum Einsatz der Videoüberwachung zu überarbeiten. Weiter soll ein Register aller Videoanlagen der SBB erstellt werden, damit bei internen und externen Anfragen zeitgerecht und kompetent Auskunft gegeben werden kann.

Die getroffenen und geplanten Massnahmen weisen in die richtige Richtung und müssen weitergeführt werden. Wir haben verlangt, insbesondere über den Stand der Arbeiten in folgenden Punkten informiert zu werden:

- Information der betroffenen Personen über die Videoüberwachung;
- Darlegung der Effizienz und der Wirksamkeit der Anlagen für die Beurteilung der Verhältnismässigkeit der Datenbearbeitung;
- Realisierung einer klaren Verantwortungstrennung zwischen den SBB, der Kantonspolizei Zürich und der Securitrans AG für die Anlage «Knoten Zürich»;
- Strikte Löschung der Aufzeichnungen bei der Anlage «Bahnreisezentrum (BRZ)» nach 24 Stunden, falls kein Ereignis eintritt (Überschreibungsprozess).

3.2.4 Arbeitsgruppe zur Gewalt bei Sportveranstaltungen

Eine interdepartementale Arbeitsgruppe untersucht, welche Massnahmen zur Verhinderung von Gewalt bei Sportveranstaltungen eingesetzt werden können. Die vorgeschlagenen Massnahmen greifen stark in die Persönlichkeit jedes Einzelnen ein. Für die Umsetzung solcher Sicherheitsmassnahmen müssen daher klare gesetzliche Grundlagen geschaffen werden.

Wir wirken in einer interdepartementalen Arbeitsgruppe «Gewalt bei Sportveranstaltungen» mit. Ziel der unter der Leitung des BASPO stehenden Arbeitsgruppe ist es, sich über die Recht- und Zweckmässigkeit von Massnahmen zur Verhinderung von Gewalt und Hooliganismus bei Sportveranstaltungen auszusprechen. Dabei handelt es sich um Massnahmen wie Videoüberwachung, Austausch von Informationen über Hooligans, Erstellung einer Hooliganismus-Datensammlung, Verhängung von schweizweit geltenden Stadionverboten usw. Da jede der vorgeschlagenen Massnahmen in erheblichem Masse in die Persönlichkeit jedes Einzelnen eingreift, müssen verschiedene datenschutzrechtliche Aspekte bei der Beurteilung beachtet werden.

Bei einer künftigen Umsetzung dieser Massnahmen dürfte speziell der Umstand besondere Probleme bereiten, dass unterschiedliche Datenbearbeiter (Bundesbehörden, kantonale Behörden, Private wie Stadionbetreiber oder Fussballvereine) involviert sind, dabei aber nicht für alle Beteiligten die gleichen Datenschutzgesetze zur Anwendung gelangen. Bundesorgane und Private müssen sich an das DSG halten, die kantonalen Behörden (z.B. Polizeistellen) haben sich nach ihren kantonalen Datenschutzgesetzen zu richten. Allen Datenschutzgesetzen ist aber gemeinsam, dass sie Rahmengesetze sind, die lediglich die Grundzüge für eine rechtmässige Datenbearbeitung festhalten. Die Details für eine konkrete Datenbearbeitungsform (z.B. Schaf-

fung einer Hooligan-Datensammlung oder besonderer Strafbestimmungen betreffend Hooligans) müssen in den entsprechenden Spezialgesetzen geregelt werden.

Zum gegenwärtigen Zeitpunkt sind im Projekt «Gewalt bei Sportveranstaltungen» noch zu viele Grundsatzfragen offen. Zusammenfassend lässt sich zumindest eines mit Sicherheit festhalten: Die heutigen gesetzlichen Grundlagen erlauben keine sofortige Umsetzung der vorgeschlagenen Massnahmen. Da unter anderem auch besonders schützenswerte Personendaten betroffen sind, ist die Schaffung einer formellen gesetzlichen Grundlage unumgänglich. Erst wenn bekannt ist, welche konkreten Massnahmen die Behörden gegen die zunehmende Gewalt bei Sportveranstaltungen ergreifen wollen, kann eine detaillierte datenschutzrechtliche Beurteilung vorgenommen werden.

4. IT und Telekommunikation

4.1 Datenschutz in der Telekommunikation

Zu verschiedensten Datenschutzfragen in der Telekommunikation erhalten wir täglich mehrere Anfragen, sei es von betroffenen Personen, sei es von Inhabern von Datensammlungen. Einen Teil von Antworten zu häufigen Fragen haben wir zusammengefasst und publizieren sie fortlaufend auf unserer Internetseite. Eine Auswahl von Fragen und Antworten finden Sie auch im Anhang (Abschnitt 13.2).

4.2 Mindestdatenschutzklausel für allgemeine Geschäftsbedingungen der Fernmeldedienstanbieterinnen

Mehrere Anbieter von Fernmeldedienstleistungen (Festnetz- und Mobiltelefonie) haben ihre allgemeinen Geschäftsbedingungen geändert. Wir wurden von den Anbietern selbst oder von den Kunden um Stellungnahmen zur Gültigkeit der Datenschutzklauseln ersucht. Wie wir feststellten, werden bestimmte Klauseln den gesetzlichen Bedingungen über den Datenschutz – besonders den allgemeinen Grundsätzen der Zweckbindung und der Transparenz sowie den Vorschriften zur Information und Einwilligung der betroffenen Personen – nicht gerecht. Die Kunden müssen in der Tat über die Möglichkeit informiert werden, sich einer Datenbearbeitung zu widersetzen, insbesondere wenn sie für die Leistungserbringung nicht erforderlich ist (z.B. Datenbearbeitung zu Marketingzwecken). In diesem Rahmen haben wir eine Mindestdatenschutzklausel ausgearbeitet, die sich im Anhang des vorliegenden Berichts befindet (siehe Abschnitt 13.1).

4.3 Nachsendeformulare der Post und die Adressaktualisierung – Der Entscheid des UVEK

Durch einen Entscheid des UVEK vom April 2002 konnte die von uns seit mehreren Jahren kritisierte Praxis der Post im Zusammenhang mit den Nachsendeaufträgen nun datenschutzkonform gestaltet werden. Die Post hat die Gebühren für Kunden, die auf eine Aktualisierung verzichten, nach unserer Intervention massiv reduziert. Auch wurden unklare Formulierungen in den Formularen verbessert. Dies hatten wir bereits in unserer Empfehlung gefordert.

Ein Nachsendeformular füllt aus, wer sich seine noch an die alte Adresse gerichteten Sendungen nach einem Umzug an die neue Adresse weiterleiten will. Die Nachsendungen sind aufwändig, weshalb die Post zusammen mit der Firma DCL einen Adressaktualisierungsdienst anbietet wird. Firmen können so ihren Adressbestand auf den neusten Stand bringen und auf diese Weise die Zahl der Fehladressierungen klein halten. Jeder Person, die einen Nachsendeauftrag stellt, steht es jedoch frei, diese Adressaktualisierung für Dritte zu untersagen. Dies hatte die Post nach unseren Interventionen auch veranlasst, jedoch dafür ab 2001 eine 24fache Gebühr (auf ein Jahr gerechnet) verlangt. Da dies die freie Entscheidung massiv beeinträchtigte, haben wir am 19. Februar 2001 eine Empfehlung erlassen, die von der Post verlangte, höchstens die doppelte Gebühr zu erheben, wenn eine Aktualisierung für Dritte untersagt wird. Zudem haben wir unklare Formulierungen im Formular und im zugehörigen Merkblatt der Post gerügt und eine Anpassung verlangt. Die Empfehlung kann unter http://edsb.ch/d/doku/empfehlungen/postsendung_d.pdf abgerufen werden. Da die Post unsere Empfehlung ablehnte, haben wir uns am 27. April 2001 zu einem Weiterzug der Angelegenheit ans UVEK entschlossen. Am 25. April 2002 hat das Departement über unsere Empfehlung entschieden (siehe Anhang Abschnitt 13.3) und unsere Forderungen (mit Ausnahme unseres Begehrens auf Rückerstattung bereits bezahlter Gebühren) vollumfänglich gestützt. Die Post hat den Entscheid des UVEK umgesetzt und verlangt nun seit Juni 2002 für die Nachsendung der Post 15 Franken pro Jahr, falls die Adressaktualisierung für Dritte erlaubt wird, und 30 Franken pro Jahr, falls der Kunde darauf verzichtet (vorher 20 Fr. pro Monat!).

4.4 Revision des Fernmeldegesetzes und des Radio- und Fernsehgesetzes

Sowohl das Fernmeldegesetz als auch das Radio- und Fernsehgesetz befinden sich zur Zeit in Revision. Im Rahmen beider Ämterkonsultationen mussten wir feststellen, dass die entsprechenden Datenschutzbestimmungen viel zu vage formuliert sind.

Zur geplanten Teilrevision des Fernmeldegesetzes, der Fernmeldedienstverordnung sowie der Verordnung über die Adressierungselemente im Fernmeldebereich konnten wir im Rahmen der Ämterkonsultation Stellung nehmen. In datenschutzrechtlicher Hinsicht interessierten uns dabei vor allem die Bestimmungen über die Datenbearbeitung sowie über die Amtshilfe. Das Datenschutzrecht verlangt für die Datenbearbeitung durch Bundesbehörden eine gesetzliche Grundlage. Wir mussten feststellen, dass diese Artikel betreffend die Datenbearbeitung viel zu vage formuliert sind und somit keine genügende gesetzliche Grundlage bilden. Wir verlangten, dass insbesondere die Datenkategorien, die bearbeitet werden sollten, die Zwecke der Datenbearbeitungen sowie die beteiligten Organe im Gesetz selbst aufgeführt würden. Ausserdem forderten wir, dass die Informationssysteme, deren Zweck sowie die Zugriffe darauf klar umschrieben würden. Betreffend die Amtshilfe wiesen wir darauf hin, dass diese nur im Einzelfall und auf begründete Anfrage hin gewährt werden könne. Wir schlugen daher vor, auf die im Rahmen der Amtshilfe vorgesehene Lieferung von Listen zu verzichten. Ferner hielten wir fest, dass die vorgesehene Meldepflicht punkto mitzuteilende Daten und betroffene Behörden präzisiert werden müsste. Schliesslich begrüssten wir, dass neu das Versenden von unerwünschten Mitteilungen (Spamming) geregelt werden soll.

Kurze Zeit darauf konnten wir ebenfalls im Rahmen der Ämterkonsultation zur Totalrevision des Radio- und Fernsehgesetzes Stellung nehmen. Diesbezüglich ist darauf hinzuweisen, dass diese Totalrevision ebenfalls Anpassungen des Fernmeldegesetzes vorsieht, darunter auch die oben erwähnten Bestimmungen des Fernmeldegesetzes. Mit anderen Worten sind diese Bestimmungen in beiden Revisionen enthalten. In unserer Stellungnahme zur Revision des Radio- und Fernsehgesetzes wiesen wir unter anderem darauf hin, dass die Bestimmung betreffend den Datenschutz viel zu vage formuliert ist. Wir verlangten, dass mindestens der Zweck und das Ausmass der Datenbearbeitung, die beteiligten Organe sowie die Datenkategorien enthalten sein müssten. Betreffend die Bestimmungen aus dem Fernmeldegesetz wiederholten wir im Grossen und Ganzen unsere anlässlich der Teilrevision des Fernmeldegesetzes gemachten Äusserungen.

Daraus folgt, dass insbesondere betreffend das Fernmeldegesetz die Anliegen des Datenschutzes zu wenig berücksichtigt wurden.

5. Gesundheit

5.1 Verschiedene Themen

5.1.1 Technische Grundanforderungen an das elektronische Patientendossier

Im Zuge der Digitalisierung von Patientendossiers haben wir versucht, für diese offenbar unausweichliche Entwicklung einige Grundanforderungen bzw. Empfehlungen zu formulieren, ganz gleich, welches Verfahren für die physische Speicherung der Dossiers (zentral, dezentral, Patient, Karte ...) verwendet wird. Dabei kann es durchaus sein, dass angesichts der zahlreichen Modelle und Projekte, die derzeit in unserem Land entwickelt werden, manche unserer Aussagen aufgrund der Erfahrungen in diesem Bereich anzupassen oder zu nuancieren sein werden.

Um einen klaren Rahmen abzustecken, ist es wichtig, die verschiedenen Modelle für die Aufbewahrung von elektronischen Patientendossiers zu beschreiben:

1. Dezentralisierte oder verteilte Aufbewahrung, d.h. die medizinischen Daten bleiben bei den Anbietern von Gesundheitsdiensten und es wird ein virtuelles Dossier mit dem «öffentlichen Teil jeder Episode» erstellt, falls notwendig über ein gemeinsames Netzwerk aller Beteiligten. Für ein solches virtuelles Dossier stellt sich natürlich in erster Linie die Frage, ob dieses in seinem vollen Umfang zur Verfügung stehen soll, und ob nicht trotz allem bestimmte Personendaten zentral aufbewahrt werden müssen.

2. Zentrale Speicherung bei einem Dritten, d.h. alle oder ein Teil der von einem Anbieter von Gesundheitsdiensten erstellten medizinischen Daten werden in ein von einer staatlichen (Kanton, Bund) oder privaten Einrichtung (Dienstanbieter) verwaltetes Zentralregister kopiert. Die mit diesem Modell einhergehenden Fragen betreffen das Vertrauen in das Zentralorgan sowie dessen Angreifbarkeit.

3. Zentrale Speicherung beim Patienten selbst, d.h. alle oder ein Teil der von einem Anbieter von Gesundheitsdiensten erstellten medizinischen Daten werden auf einen von der betroffenen Person verwahrten Datenträger (Chipkarte, CD…) kopiert. Die betroffene Person hätte somit die alleinige Kontrolle über ihre Daten, wobei eine Sicherheitskopie des Datenträgers bei einem Vertrauensarzt hinterlegt werden könnte.

Diese drei theoretischen Modelle lassen sich in der Praxis unterschiedlich kombinieren. So könnte man sich die Patientenkarte als reines Identifikationsmittel vorstellen (Versichertennummer, Name, ...), als Speichermedium für administrative Daten und/oder Angaben für den Notfall, als kryptographischen Zugangschlüssel zu den eigentlichen medizinischen Daten oder schliesslich als Speichermedium für das gesamte Patientendossier.

Unabhängig davon, welches Speicherungsmodell verwendet wird, sind zur Zeit folgende Vorkehrungen bezüglich des Datenschutzes vorstellbar:

- Unterscheidung zwischen administrativen und medizinischen Daten. Unter den medizinischen Daten eine feinere Unterscheidung zwischen objektiven Daten (Untersuchungen, …) und subjektiven Daten (Diagnose,…), Medikation und Angaben für Notfälle. Für letztere ist der Zugriff gesondert zu regeln, da es sich immer um kritische Situationen handelt.

- Speicherungs- und Codierungsformat sämtlicher Daten, um den langfristigen Bestand und die nationale oder gar internationale Interoperabilität sicherzustellen (Erfassung/Konvertierung gegenwärtiger Daten).

- Vorrangige Verwendung von Pseudonymisierungs- und Anonymisierungsverfahren (siehe 9. Tätigkeitsbericht, Abschnitt 2.2.1), um die Gefahr von Datenlecks so weit wie möglich zu begrenzen, jedoch die Nutzung der gesammelten medizinischen Daten zu epidemiologischen oder statistischen Zwecken so weit wie möglich zu erlauben.

- Verschlüsselte Speicherung besonders schützenswerter Personendaten: die Episoden im Dossier können nur von Personen gelesen und/oder bearbeitet werden, die einen gültigen Dechiffrierungsschlüssel besitzen. Dabei kann jede medizinische Episode jeweils unabhängig verschlüsselt werden, und der Patient (oder eventuell sein Vertrauensarzt) sollte grundsätzlich in der Lage sein, die betreffenden Daten zu entschlüsseln. Dazu muss allerdings eine nicht ganz unkomplizierte Public Key Infrastucture (PKI) eingerichtet werden.

- Mögliche provisorische Abdeckung jener medizinischer Daten, die einer mündlichen Erläuterung durch den betreffenden spezialisierten Anbieter von Gesundheitsdiensten bedürfen.

- Systematische Identifizierung und starke Authentifizierung sämtlicher Beteiligter des Gesundheitswesens mit Zugang zum System.

- Ausführliche und von der betroffenen Person jederzeit abrufbare Protokollierung über sämtliche Zugriffe und sämtliche Änderungen von schützenswerten Daten.

- Gewährleistung und regelmässige Überprüfung der Vertraulichkeit, Integrität und Verfügbarkeit der Daten.
- Digitale Signatur aller Dateneingaben, um ihre Integrität und Unabstreitbarkeit sicherzustellen.
- Unterschiedliche Sichtbarkeit der Daten (logische Ansicht) je nach Berechtigtem.
- Gesonderter und den jeweiligen Bedürfnissen angepasster Informationskanal zu den Versicherungen, welche die Angaben zu Rechnungen möglicherweise in einer vereinbarten verschlüsselten Form erhalten (siehe Abschnitt 5.1.2 des vorliegenden Berichts).
- Ebenfalls getrennte Lösung für Rezepte und Zugang der Apotheker.

5.1.2 Versichertenkarte und Gesundheitskarte

Der Bundesrat hat entschieden, im Rahmen der obligatorischen Krankenversicherung eine Versichertenkarte einzuführen. Die Versichertenkarte wird obligatorisch sein, eine Identifikationsnummer tragen, eine Benutzerschnittstelle besitzen und für die elektronische Abrechnung von Versicherungsleistungen eingesetzt werden. Sie bietet zudem die Möglichkeit, freiwillig weitere Informationen abzuspeichern (Notfalldaten). Die Datenschutzrisiken solcher Karten sind abhängig von Inhalt, Verwendungszweck und Einsatzbereich der Karte.

In unserem letzten Tätigkeitsbericht haben wir die Mindestanforderungen für die Einführung einer Gesundheitskarte festgehalten (9. Tätigkeitsbericht 2001/2002, Abschnitt 5.1.1). Zu jenem Zeitpunkt war noch nicht klar, ob eine Versicherungskarte zu rein administrativen Zwecken oder eine eigentliche Gesundheitskarte angestrebt wird. Letztere wird als elektronischer Schlüssel propagiert, der den Zugang zu sämtlichen Gesundheitsdaten einer Person (elektronisches Patientendossier) ermöglicht. Die datenschutzrechtlichen Risiken der beiden Karten sind unterschiedlich hoch. Die administrative Versicherungskarte kann unter der Voraussetzung, dass ihr Inhalt und ihre Verwendungszwecke klar definiert sind, für obligatorisch erklärt werden. Eine Gesundheitskarte aber, auf der medizinische Informationen abgespeichert werden bzw. die Zugriff auf die gesamte lebenslange Krankengeschichte gibt, ist datenschutzrechtlich wesentlich heikler. Besitz und Verwendung einer solchen Karte muss freiwillig sein. Der Kartenbesitzer muss die alleinige Datenherrschaft behalten und frei darüber entscheiden können, wem, wann und in welchem Umfang er Einblick in seine Gesundheitsdaten geben will. Die lebenslange Krankengeschichte ist eine spezielle Datensammlung, die naturgemäss nicht möglichst wenig, sondern eben möglichst

viele Daten enthält. Das ist unproblematisch, solange die Datensicherheit gewährleistet ist und der Zugriff auf den Betroffenen und die von ihm bestimmten Arztpersonen beschränkt bleibt. Natürlich werden aber schnell einmal Dritte ein lebhaftes Interesse an bestimmten Daten aus diesen lebenslangen elektronischen Gesundheitsdatensammlungen bekunden. Es ist absehbar, dass mit dem Vorhandensein elektronischer Krankengeschichten auch der Druck auf den Einzelnen zunehmen wird, in gewissen Situationen Informationen über seine Gesundheit preiszugeben, so z.B. bei Stellenbewerbungen oder beim Abschluss von Versicherungen.

Im August 2002 hat der Bundesrat entschieden, vorerst eine Versichertenkarte im Rahmen der obligatorischen Krankenversicherung einzuführen. Die Versichertenkarte soll zwei Zwecke erfüllen: zum einen die eindeutige Identifizierung des Versicherten mittels einer Identifikationsnummer, zum andern die elektronische Abrechnung von Leistungen nach KVG.

Als Identifikationsnummer könnte die neue AHV-Nummer eingesetzt werden (vgl. Abschnitt 6.1.3). Diese soll zu einer eigentlichen Sozialversicherungsnummer ausgebaut werden. Dem steht grundsätzlich nichts entgegen, solange die Verwendung der Sozialversicherungsnummer ausschliesslich nach eindeutigen, im Gesetz geregelten Bedingungen erfolgt, d.h.

- sie nur für klar im Gesetz umschriebene Zwecke verwendet werden darf;
- sie nur im Bereich der Sozialversicherungen eingesetzt werden darf.

Die Verwendung von Identifikationsnummern ist datenschutzrechtlich deshalb heikel, weil sie die Verknüpfbarkeit von Daten wesentlich vereinfacht. Wird die gleiche Nummer – oder mehrere einander zuordenbare Nummern – zu unterschiedlichen Zwecken in unterschiedlichen Bereichen verwendet, können die Daten aus diesen verschiedenen Lebensbereichen einer Person miteinander verknüpft und zur Erstellung von Persönlichkeitsprofilen verwendet werden. Deswegen muss die Verwendung von Identifikationsnummern auf klar definierte Sektoren begrenzt und detailliert gesetzlich geregelt werden. Dass dies nötig ist, zeigt die Erfahrung mit der heutigen AHV-Nummer, die sich in der Praxis rasch und unkontrolliert verbreitet hat und inzwischen von unzähligen Stellen zu den unterschiedlichsten Zwecken verwendet wird. Bei der zukünftigen Sozialversicherungsnummer muss eine solch ungeregelte Verwendung zum vornherein verhindert werden. Dies um so mehr, als sich mit den modernen elektronischen Kommunikationsmitteln die Verknüpfungsmöglichkeiten noch um ein Vielfaches erhöht und vereinfacht haben (siehe dazu auch Abschnitt 6.1.3).

Die Versichertenkarte wird eine sogenannte «Karte mit Benutzerschnittstelle» sein. Ein «kleiner Computer» ermöglicht den Zugriff auf die Identifikationsdaten und die Verwaltung der persönlichen Daten des Versicherten auf der Karte. Nach Einführung

der Versichertenkarte wird die Abrechnung obligatorisch nur noch über das Versichertenkartensystem (elektronisch) möglich sein.

Die Einführung der elektronischen Abrechnung ist mit dem Projekt Tarmed verbunden, in welchem nach wie vor wichtige Fragen hinsichtlich des Datenschutzes offen sind (vgl. Abschnitt 5.1.5). Die Leistungsabrechnung enthält bereits heute ausführliche Informationen über die Gesundheit des Betroffenen. Nach Einführung des Tarmed werden die Rechnungen einen noch höheren Detaillierungsgrad erreichen als bisher. So wird z.B. der umstrittene ICD-10-Diagnosecode auf den Rechnungen erscheinen. Die Angaben werden zudem, da elektronisch vorhanden, einfacher und vielfältiger auswertbar sein als bisher. Wir stellen uns daher auf den Standpunkt, dass vor Einführung der elektronischen Abrechnung die Fragen des Datenschutzes geregelt werden müssen. Dazu ist es nach unserer Ansicht nötig, dass

- der Datenverkehr zwischen Leistungserbringer und Versicherer überdacht und auf eine zweckmässige und minimale Datenmenge beschränkt wird;
- die generelle Wirtschaftlichkeits- und Leistungskontrolle mit pseudonymen Daten vorgenommen wird, weil es um eine Kontrolle der Leistungserbringer geht und dafür keine patientenbezogenen Daten notwendig sind;
- die Wirtschaftlichkeits- und Leistungskontrolle im Einzelfall zwingend über den Vertrauensarzt (oder ein allenfalls neu einzuführendes neutrales Institut) erfolgt;
- die Daten, welche der Wirtschaftlichkeits- und Leistungskontrolle im Einzelfall dienen, nach Abschluss dieser Kontrollen gelöscht werden, weil sie ihren Zweck erfüllt haben und eine andere Verwendung gegen das Zweckbindungsprinzip verstossen würde;
- das Instrument des Vertrauensarztes, das zurzeit lediglich in der obligatorischen Krankenversicherung vorgesehen ist, verstärkt und ausgeweitet wird;
- eine unabhängige Kontrollinstanz gewährleistet, dass sensitive Daten (medizinische Informationen und Diagnosen) beim Vertrauensarzt verbleiben;
- die Einführung von unabhängigen Auditierungs- und Zertifizierungsinstanzen ins Auge gefasst wird.

Bei der Einführung der elektronischen Abrechnung dürfen die bestehenden Probleme im Bereich der Leistungsabrechnung nicht einfach übernommen, sondern müssen praktisch und annehmbar gelöst werden.

Ob obligatorische Versicherungskarte oder freiwillige Gesundheitskarte: Die Kartensysteme müssen in jedem Falle so konfiguriert werden, dass die datenschutzrechtlichen Prinzipien der Verhältnismässigkeit, der Transparenz und der zweckgebundenen

Datenbearbeitung eingehalten sind. Verantwortlich für die Umsetzung dieser Grundprinzipien sind diejenigen Stellen, welche die Systeme einführen. Für das elektronische Abrechnungssystem bedeutet dies, dass die Versicherten vollständig, klar und nachvollziehbar darüber informiert werden müssen, welche Datenbearbeitungen die Abrechnung mit sich bringt. Dazu gehören auch Informationen darüber, welche Daten für die Abrechnung minimal notwendig sind, wem welche Daten bekannt gegeben, für welchen Zweck diese Daten verwendet und wie lange sie aufbewahrt werden sowie welche Datensicherheitsvorkehren vorgesehen sind.

5.1.3 Versichertenbefragungen durch Institute

Werden zur Durchführung freiwilliger Umfragen Dritte beauftragt, so muss die Datenweitergabe für die Durchführung der Umfragen unter Einhaltung des Verhältnismässigkeitsprinzips erfolgen, d.h. es dürfen nur jene Daten weitergegeben werden, welche für die Durchführung der Umfrage auch notwendig sind. Der Auftraggeber muss daher zuerst feststellen, wer an der Umfrage überhaupt teilnehmen will. Die Weitergabe des gesamten Adressverzeichnisses ist unverhältnismässig.

Für die Durchführung von Umfragen werden in der Praxis immer häufiger externe Institute beigezogen. So beauftragte im letzten Jahr eine Versicherung ein Institut mit der Durchführung einer Versichertenbefragung. Dazu gab sie dem Institut die Adressen sowie den Namen des behandelnden Arztes einer grossen Anzahl ihrer Versicherten bekannt.

Viele der angeschriebenen Versicherten waren überrascht und erstaunt, Post von einem ihnen fremden Institut zu erhalten, welche eine schützenswerte Information, nämlich den Namen des sie behandelnden Arztes, enthielt. Sie beschwerten sich in der Folge bei uns.

Die allgemeinen Datenübermittlungsgrundsätze des Datenschutzgesetzes – wie der Grundsatz von Treu und Glauben, das Verhältnismässigkeitsprinzip, das Gebot der Zweckbindung – gelten immer, auch bei einer an und für sich erlaubten Beauftragung eines Dritten. Die Teilnahme an Befragungen ist in der Regel freiwillig. Der ausgewählte Versicherte muss also – bevor seine Daten weitergegeben werden – die Möglichkeit haben, die Teilnahme und damit auch die Datenweitergabe zu verweigern. Die Versicherung hätte also vor der Weitergabe der Daten an das Institut die von ihr ausgewählten Versicherten anfragen müssen, ob sie an der Befragung überhaupt teilnehmen wollen und ob sie mit der Weitergabe der für diese Umfrage notwendigen Daten an das Institut einverstanden sind. Es handelte sich in diesem Falle zudem nicht nur

um die Adresse, sondern auch um eine besonders schützenswerte Information, nämlich den Namen des behandelnden Arztes, aus dem unter Umständen auch gewisse Schlüsse gezogen werden können, so z.B. wenn es sich dabei um einen Spezialisten handelt (Psychiater, Onkologe). Auf die Freiwilligkeit der Umfrage muss selbstverständlich sowohl beim Einholen der Einwilligung wie auch auf dem Fragebogen selber ausdrücklich hingewiesen werden. Wäre die Versicherung so vorgegangen, hätte das Institut nur die Daten jener Versicherten erhalten, die auch bereit waren, an der Umfrage teilzunehmen. In der Folge wären auch nur diese angeschrieben worden.

Eine einfache Möglichkeit, bei solchen Umfragen die Einwilligung der Betroffenen einzuholen und das Verhältnismässigkeitsprinzip einzuhalten, besteht darin, dass die Versicherungen die Fragebogen selber verschicken, gleichzeitig die Versicherten ausführlich über die Ziele und das Vorgehen bei der Befragung informieren und sie anweisen, den ausgefüllten Fragebogen direkt an das Institut zurückzusenden, wo die Daten anonym ausgewertet werden können.

5.1.4 Transparenzmängel und unverhältnismässiges Datensammeln beim System RAI/RUG

Seniorenorganisationen haben sich an den Verband der Schweizer Datenschutzbeauftragten gewandt, um das System RAI/RUG unter dem Aspekt des Datenschutzes beurteilen zu lassen.

Das System wird in verschiedenen Kantonen zur systematischen Erfassung der Pflegebedürftigkeit von Altersheimbewohner/innen und zu deren Einstufung in Pflegeaufwandgruppen verwendet. Innerhalb des Verbandes wurde die Arbeitsgruppe Gesundheit (AGX) mit der Prüfung dieses Beurteilungsinstrumentes beauftragt. Sie kommt in ihrem Bericht zum Schluss, dass das System für die Heimbewohner kaum durchschaubar ist. Neben diesem Mangel an Transparenz rügt die AGX, dass viel zu viele Daten systematisch erhoben und gespeichert werden, was nicht mehr mit dem Verhältnismässigkeitsprinzip zu vereinbaren ist.

Die detaillierten Überlegungen und Schlussfolgerungen der AGX sind zusammen mit einer Liste von notwendigen Anpassungen unter der Internetadresse www.dsb-cpd.ch abrufbar. Sie sind auch im Anhang dieses Tätigkeitsberichtes (Abschnitt 13.5) zu finden.

5.1.5 Der Arzttarif Tarmed

Im Verlaufe der letzten Jahre haben wir immer wieder auf heikle Datenschutzfragen im Zusammenhang mit Tarmed hingewiesen. Inzwischen steht der Einführungstermin für den Tarmed fest. Trotzdem sind wir bisher nicht offiziell über das gewählte System und die darin vorgesehenen Datenschutz- und Datensicherheitsmassnahmen informiert worden. Eine Beurteilung, ob die datenschutzrechtlichen Fragen befriedigend gelöst wurden, ist daher nicht möglich. Wir können also vorläufig betreffend Datenschutz im Tarmed noch keine Entwarnung geben.

Der Arzttarif Tarmed tritt für die Bereiche Unfallversicherung, Militärversicherung und Invalidenversicherung auf den 1. Mai 2003, für den Bereich Krankenversicherung auf den 1. Januar 2004 in Kraft. Mit diesem neuen Tarifsystem wird gesamtschweizerisch eine einheitliche Tarifstruktur geschaffen. Die Vereinbarungen der Tarifpartner (FMH, santésuisse, H+) halten fest, dass die gesetzlichen Bestimmungen des Datenschutzes einzuhalten sind. Die praktische Umsetzung dieser Bestimmungen und damit die praktische Ausgestaltung des Datenschutzes liegt in der Verantwortung jener, welche die vorgesehenen Systeme einführen.

Wir wirken seit Jahren darauf hin, dass bei der Einführung des Tarmed die Persönlichkeitsrechte der Versicherten gewahrt bleiben. Obschon die Einführung kurz bevorsteht, haben uns die Verantwortlichen des Projektes trotz mehrmaliger Nachfrage nicht darüber informiert, was nun konkret geplant ist. Eine datenschutzrechtliche Beurteilung können wir aber erst vornehmen, wenn bekannt ist, welche konkreten Massnahmen ergriffen wurden.

Die Datenschutzfragen sind also immer noch offen. Die zwei Hauptproblemfelder bilden dabei die detaillierten Diagnose- und Operationscodes (ICD-10 und CHOP) auf den Abrechnungen sowie die mit dem Tarmed und der Versichertenkarte (vgl. Abschnitt 5.1.2) obligatorisch werdende elektronische Abrechnung von Versicherungsleistungen.

Wir haben unsere Position in den Diskussionen mit den Beteiligten im Projekt Tarmed bereits mehrfach dargelegt. Darüber hinaus haben wir auch im jährlichen Tätigkeitsbericht unsere Haltung publiziert (vgl. 9. Tätigkeitsbericht 2001/2001, Abschnitt 5.1.4; 8. Tätigkeitsbericht 2000/2001, Kapitel I. 7.5; 6. Tätigkeitsbericht 1998/1999, Kapitel I. 8.3). Nachstehend nochmals die wichtigsten Grundaussagen:

- Die systematische Bekanntgabe von detaillierten Diagnosen, Diagnosecodes und anderen damit kompatiblen Codes an die Versicherer verstösst sowohl gegen das im Datenschutzgesetz verankerte Verhältnismässigkeitsprinzip als auch gegen

Art. 42 KVG. Das Verhältnismässigkeitsprinzip erlaubt nur das Einholen von tatsächlich erforderlichen und für den vorgesehenen Zweck geeigneten Daten; gerade bei besonders schützenswerten Daten muss diesem Grundsatz erhöhte Bedeutung beigemessen werden. Das Verhältnismässigkeitsprinzip gilt auch im Rahmen der Datenerhebung nach Art. 42 KVG. Zulässig ist somit einzig die systematische Bekanntgabe einer Rahmendiagnose, d.h. einer allgemeinen Diagnose, wie sie zur Bearbeitung eines durchschnittlichen Normalfalles erforderlich ist.

- Wenn in begründeten Einzelfällen die Rahmendiagnose nicht ausreicht, kann der Versicherer nachträglich noch eine detaillierte Diagnose oder zusätzliche medizinische Informationen einholen. Aus datenschutzrechtlicher Sicht müssten diese Informationen zwingend über den Vertrauensarzt des Versicherers eingeholt werden. Das KVG sieht in Art. 42 Abs. 5 zwar immerhin vor, dass der Versicherte verlangen kann, dass diese zusätzlichen Informationen nur dem Vertrauensarzt bekannt gegeben werden. Dazu muss er aber selber aktiv werden, was aus datenschutzrechtlicher Sicht unbefriedigend ist.
- Das Transparenzprinzip verlangt, dass die Datenbedürfnisse und die Datenberarbeitungsverfahren im Zusammenhang mit der Abrechnung – unabhängig davon, ob sie elektronisch erfolgt oder nicht – dem Versicherten klar und nachvollziehbar kommuniziert werden.
- Im elektronischen Abrechnungssystem müssen die heute verfügbaren datenschutzfreundlichen Technologien eingesetzt werden: Anonymisierungs- und Pseudonymisierungsverfahren, Verschlüsselungsverfahren, digitale Signatur usw.
- In Bezug auf Datensicherheit muss der heutige Stand der Technik umgesetzt werden.

Der Datenschutz will weder die elektronische Abrechnung noch die unbestrittenermassen notwendigen Abrechnungskontrollen verhindern. Aber die geplanten Systeme müssen dem Datenschutz Rechnung tragen, indem sie datensparsam und datenschutzfreundlich konfiguriert werden und dem Versicherer ermöglichen, Kontrollen so vorzunehmen, dass dabei das Patientengeheimnis gewahrt bleibt. Dies kann z.B. durch Verwendung von Pseudonymisierungsverfahren erreicht werden. Für die Überprüfung, ob die Leistungserbringer wirtschaftlich arbeiten, genügt eine generelle Wirtschaftlichkeitsprüfung gestützt auf pseudonyme Daten. Die versichertenbezogene Wirtschaftlichkeitsprüfung im Einzelfall muss ebenfalls möglich sein; sie müsste aber nach unserer Ansicht durch den Vertrauensarzt oder durch eine andere neutrale Stelle vorgenommen werden.

5.2 Genetik

5.2.1 Datenschutz verbietet heimliche Vaterschaftstests

Unternehmen, die in der Schweiz Vaterschaftstests vertreiben wollen, müssen Vorkehren treffen, um sicher zu stellen, dass die schriftliche Einwilligung aller betroffenen Personen vorliegt. Sie müssen die Rechtsgültigkeit der vorgelegten Einwilligungen in einem wirksamen Verfahren überprüfen. Nur so kann verhindert werden, dass Gewebeproben von Kindern heimlich entnommen und Vaterschaftstests ohne Wissen des Partners durchgeführt werden.

Im vergangenen Jahr haben private Firmen damit begonnen, in der Schweiz aussergerichtliche Vaterschaftstests anzubieten. Die Durchführung solcher Tests untersteht bis auf weiteres weder einer Bewilligungspflicht noch sonstigen behördlichen Auflagen. Eine gesetzliche Regelung wird erst mit Einführung des Bundesgesetzes über genetische Untersuchungen beim Menschen (GUMG) erfolgen.

In der Art und Weise, wie die Vaterschaftstests angeboten werden, erfüllen sie die Vorschriften des Datenschutzes nicht. Die Durchführung eines Vaterschaftstests stellt eine Bearbeitung von Personendaten im Sinne des Datenschutzgesetzes dar. Wird ein solcher Test nicht durch ein Gericht angeordnet, so darf er nur durchgeführt werden, wenn die betroffenen Personen ihre schriftliche Einwilligung erteilen. Wenn die Unternehmen, die Vaterschaftstests anbieten, nicht überprüfen, ob die notwendigen Unterschriften vorliegen und ob sie tatsächlich von den betroffenen Personen stammen, ist es ohne weiteres möglich, sogenannt heimliche Vaterschaftstests in Auftrag zu geben. Heimliche Tests verletzen aber nicht nur die Persönlichkeitsrechte des betroffenen Kindes, sondern auch jene des Partners, hinter dessen Rücken der Test durchgeführt wird.

Wir haben zwischen Oktober 2002 und Januar 2003 gegen drei Firmen Empfehlungen erlassen (siehe Abschnitt 13.7.2). Darin haben wir die Unternehmen aufgefordert, bei der Durchführung von Vaterschaftstests die Vorschriften des Datenschutzgesetzes einzuhalten und die Rechtsgültigkeit der vom Auftraggeber vorgelegten Einwilligungen wirksam zu überprüfen. Insbesondere müssen die Unternehmen sicherstellen, dass bei Kindern die Einwilligung des gesetzlichen Vertreters vorliegt. In der Regel bedeutet dies, dass beide Eltern ihre schriftliche Zustimmung zum Test geben müssen. Zur Rechtsgültigkeit der Einwilligung gehört ferner, dass sich die Betroffenen über die Tragweite des Tests im Klaren sind. Hier haben die Unternehmen eine spezielle Informationspflicht. Sie müssen ihren Kunden fachmännische Aufklärung und

Beratung anbieten. Weil bei Vaterschaftstests mit besonders schützenswerten Personendaten gearbeitet wird, müssen selbstverständlich auch wirksame Datensicherheitsvorkehren ergriffen werden.

5.2.2 Bundesgesetz über genetische Untersuchungen

Der Bundesrat hat im September 2002 die Botschaft zum Bundesgesetz über genetische Untersuchungen beim Menschen verabschiedet. Die Vorlage geht somit in die parlamentarische Beratung.

Nach mehreren Vernehmlassungen bzw. Ämterkonsultationen liegt das Bundesgesetz über genetische Untersuchungen beim Menschen (GUMG) inklusive Botschaft nun vor (BBl 2002 VII 7361). Das GUMG hat zum Ziel, die Menschenwürde zu schützen, Missbräuche zu verhindern und die Qualität der Untersuchungen zu sichern. Ob eine Diskriminierung aufgrund des Erbgutes mit diesem Gesetz tatsächlich verhindert werden kann, bleibt jedoch fraglich; zu viele Punkte in diesem höchst sensiblen Bereich sind noch ungeklärt. Betreffend die generellen Anforderungen an genetische Untersuchungen verweisen wir auf den letzten Tätigkeitsbericht (vgl. 9. Tätigkeitsbericht 2001/2002, Abschnitt 5.2.1).

Der Geltungsbereich des Gesetzesentwurfes umfasst genetische Untersuchungen im medizinischen Sektor, im Arbeits-, im Versicherungs- und im Haftpflichtbereich. Im Weiteren soll es die Erstellung von DNA-Profilen zur Klärung der Abstammung oder zur Identifizierung von Personen regeln. Zu begrüssen ist die Tatsache, dass der Geltungsbereich des GUMG – im Gegensatz zu früheren Entwürfen – abschliessend geregelt sein soll. Die Bearbeitung von genetischen Daten, welche zu den besonders schützenswerten Personendaten gehören, bedarf einer klaren und abschliessenden gesetzlichen Grundlage. Zukünftige genetische Untersuchungen für neue Zwecke sollen nur dann möglich sein, wenn das Gesetz entsprechend angepasst wird.

Für den Arbeits-, Versicherungs- und Haftpflichtbereich sollen präsymptomatische genetische Untersuchungen grundsätzlich verboten werden (Präsymptomatische genetische Untersuchungen sind Untersuchungen mit dem Ziel, Krankheitsveranlagungen vor dem Auftreten klinischer Symptome zu erkennen). Unter gewissen Voraussetzungen sind allerdings Ausnahmen vorgesehen. Ob sich eine Diskriminierung von Menschen mit «schlechten» Erbanlagen dadurch verhindern lässt, bleibt daher offen. Es ist gut vorstellbar, dass insbesondere im Arbeitsbereich die vorgesehenen Ausnahmen bestimmte Mitarbeiter oder gar Volksgruppen mit spezifischen genetischen Eigenschaften benachteiligen werden (mehr dazu in Abschnitt 7.6).

Neu ist im GUMG auch geregelt, unter welchen Voraussetzungen DNA-Profile zur Klärung der Abstammung ausserhalb eines behördlichen Verfahrens zulässig sein sollen. Dazu gehören auch die Vaterschaftstests, welche bereits heute schon von verschiedenen Labors angeboten werden (vgl. auch Abschnitt 5.2.1). Unter anderem sollen Vaterschaftstests nur dann möglich sein, wenn die betroffenen Personen ihre schriftliche Einwilligung dazu geben; hingegen sieht der Gesetzesentwurf vor, dass ein urteilsunfähiges Kind, dessen Abstammung von einer bestimmten Person geklärt werden soll, von dieser nicht vertreten werden kann.

Das Bundesgesetz über genetische Untersuchungen dürfte in absehbarer Zeit im Parlament beraten werden.

6. Versicherungen

6.1 Sozialversicherungen

6.1.1 Herausgabepflicht der Leistungserbringer nach UVG

Leistungserbringer (Ärzte und Spitäler) müssen den Unfallversicherern für die im UVG vorgesehen Zwecke die notwendigen Informationen liefern. Die Unfallversicherer beharren jedoch auf eine umfassende und systematische Herausgabepflicht der Leistungserbringer. Dieser Umstand führt in der Praxis oftmals zu Problemen mit dem Datenschutzgesetz.

Das Unfallversicherungsgesetz (UVG) sieht vor, dass der Leistungserbringer dem Versicherer eine detaillierte und verständliche Rechnung zustellen muss. Er muss ihm auch alle Angaben machen, die er benötigt, um die Leistungsansprüche zu beurteilen und um die Berechnung der Vergütung und die Wirtschaftlichkeit der Leistung überprüfen zu können. Die Auskunftspflicht der Leistungserbringer ist explizit in Art. 54a UVG geregelt (in Kraft seit 1. Januar 2001).

Die Unfallversicherer machen geltend, dass in der obligatorischen Unfallversicherung das Naturalleistungsprinzip gelte, wonach die Leistungserbringer im Auftrag der Unfallversicherer tätig seien. Im Weiteren müsse der Unfallversicherer den Sachverhalt von Amtes wegen abklären (Untersuchungsgrundsatz). Ihrer Ansicht nach sei das Informationsbedürfnis daher als umfassend zu verstehen. Zudem wird von Versichererseite kritisiert, dass das Merkblatt der Schweizerischen Datenschutzbeauftragten über die Austritts- und Operationsberichte für den UVG-Bereich nicht praktikabel sei. Das Merkblatt stellt Kriterien auf, wann welche Informationen betreffend Spitalaustritten und Operationen an die Versicherer weitergeleitet werden dürfen (mehr dazu im 9.

Tätigkeitsbericht 2001/2002, Abschnitt 6.1.3). Die Unfallversicherer beharren jedoch darauf, in jedem Fall vollständige Austritts- und Operationsberichte von den Spitälern einfordern zu dürfen.

Aus datenschutzrechtlicher Sicht ergeben sich vorliegend vor allem deshalb Probleme, weil die Unfallversicherer dem Verhältnismässigkeitsprinzip zu wenig Beachtung schenken. Oftmals werden etwa umfassende Patientendossiers bzw. Austritts- und Operationsberichte eingefordert. Von Spitalseite kam zudem der Vorwurf, dass die Versicherer systematisch vollständige Berichte verlangen. Aufgrund des Verhältnismässigkeitsprinzips ist jedoch in jedem Fall – ausgehend vom jeweiligen Zweck – abzuklären, welche Daten notwendig und geeignet sind. Eine systematische Weitergabe von Berichten an die Unfallversicherer ist – für welchen Zweck auch immer – weder mit dem Verhältnismässigkeitsprinzip noch mit dem Patientengeheimnis nach Art. 321 StGB vereinbar. Auch ist eine Datenbeschaffung auf Vorrat in jedem Fall zu vermeiden.

Austrittsberichte z. B. enthalten in erster Linie Informationen für den nachbehandelnden Arzt und sind nicht für die Leistungsabklärung gedacht. Geht es etwa für den Unfallversicherer darum, die Wirtschaftlichkeit der Leistung überprüfen zu können, ist es auch nicht notwendig, die Namen der Versicherten zu kennen. Eine möglichst weitgehende Pseudonymisierung der Versichertendaten – wie sie auch für den Krankenversicherungsbereich diskutiert wird – ist für diesen Zweck anzustreben. Der Grundsatz der Verhältnismässigkeit ist denn auch explizit in Art. 54a UVG erwähnt. Dazu gehört auch, dass die Datenbedürfnisse der Versicherer begründet werden müssen; der Hinweis der Versicherer, dass die Berichte «zur Vervollständigung der Akten» notwendig seien, genügt nicht.

Zur Zeit finden Gespräche mit den involvierten Kreisen statt, damit die vorliegende Problematik einer Lösung zugeführt werden kann. Aus unserer Sicht ist es jedoch unabdingbar, dass die Informationsprozesse in den Spitälern, den Arztpraxen und bei den Versicherern etc. transparent gemacht werden. Nur so lassen sich diese auf ihre Datenschutzkonformität hin überprüfen und können sie an die Datenschutzgesetzgebung angepasst werden. Die Schweizerischen Datenschutzbeauftragten haben daher die Unfallversicherer aufgefordert, ihre Datenbedürfnisse konkret zu nennen bzw. entsprechende Standards zu schaffen. Insbesondere soll definiert werden, welche Daten zu welchem Zweck von den Spitälern verlangt werden dürfen.

6.1.2 Regelungslücken im medizinischen Datenschutz

Mit einem Postulat wurden der Bundesrat und wir eingeladen, dem Parlament einen Bericht über Regelungslücken im medizinischen Datenschutz vorzulegen. Er soll den gesamten Sozialversicherungsbereich umfassen. Der Bericht soll im Laufe des Jahres 2003 veröffentlicht und den interessierten Kreisen zur Vernehmlassung unterbreitet werden.

Die Kommission für Rechtsfragen des Nationalrates fordert vom Bundesrat und uns einen umfassenden Bericht über den medizinischen Datenschutz im gesamten Sozialversicherungsbereich (vgl. auch Postulat 00.3178). Der Bericht soll nicht nur allfällige bestehende Regelungslücken im medizinischen Datenschutz aufzeigen, sondern auch die technologische Entwicklung berücksichtigen (dazu mehr im 9. Tätigkeitsbericht 2001/2002, Abschnitt 6.1.1).

Die Arbeiten des beauftragten Instituts für Gesundheitsrecht der Universität Neuenburg kamen planmässig voran. Insbesondere wurde den einzelnen Sozialversicherern ein umfangreicher Fragebogen unterbreitet. Dabei wurden Versicherer in der Westschweiz und in der Deutschschweiz berücksichtigt. Ziel dieses Fragebogens war es u. a., die Informationsprozesse transparenter zu machen. Begleitet wurden die Untersuchungen durch Gespräche vor Ort. Des Weiteren wurden für den Bereich der Medizininformatik spezialisierte Informatiker beigezogen. Auch wurden Abklärungen bei ausländischen Institutionen gemacht, damit rechtsvergleichende Aspekte Eingang in die Studie finden. Es ist vorgesehen, die Ergebnisse des Berichts im Laufe des Jahres 2003 zu veröffentlichen. Gleichzeitig werden auch Änderungsvorschläge den interessierten Kreisen zur Vernehmlassung unterbreitet, dies im Hinblick auf die Erarbeitung des bundesrätlichen Berichts.

6.1.3 Die neue AHV-Nummer

Die AHV-Nummer soll durch eine neue Versichertennummer abgelöst werden. Im Gegensatz zur geltenden AHV-Nummer soll die neue Nummer keine Rückschlüsse auf die Person mehr zulassen. Hingegen soll die neue Nummer Anwendung auf den gesamten Sozialversicherungsbereich finden.

Die bis anhin geltende AHV-Nummer ist eine «sprechende» Identifikationsnummer, da sie Aufschluss über die Nationalität, das Geschlecht, das Geburtsdatum und in beschränktem Masse auch über den Namen gibt. Die AHV-Nummer ist obligatorisch für die Sozialversicherungen AHV, IV und EO. Zudem dürfen Verwaltungen und andere Institutionen die AHV-Nummer zu eigenen Zwecken benützen.

Schon seit mehreren Jahren ist geplant, die bisherige AHV-Nummer aus verschiedenen Gründen durch eine neue «nichtsprechende» Nummer abzulösen. Aus datenschutzrechtlicher Sicht ist es nämlich unbefriedigend, dass die geltende AHV-Nummer die Person zu einem gewissen Grad bestimmbar macht. Im Gegensatz zur bestehenden AHV-Nummer soll neu dieselbe Nummer ein Leben lang verwendet werden.

Das Bundesamt für Sozialversicherung (BSV) hat uns schliesslich einen Projektentwurf vorgestellt, welcher eine neue nicht sprechende Versichertennummer vorsieht. Zudem soll die neue Nummer als Sozialversicherungsnummer für den gesamten Sozialversicherungsbereich verwendet werden. Insbesondere könnte die Nummer für die im KVG geplante Versichertenkarte Anwendung finden (siehe Abschnitt 5.1.2).

Aus datenschutzrechtlicher Sicht zu begrüssen ist die Tatsache, dass die neue Versichertennummer keine Rückschlüsse mehr auf die Person zulassen wird. Wir sprechen uns daher grundsätzlich auch nicht gegen die Einführung einer Sozialversicherungsnummer aus. Jedoch haben wir das BSV gebeten zu prüfen, ob in den einzelnen Sozialversicherungen sektoriell andere Nummern verwendet werden können; dies, nachdem die Sozialversicherungsnummer generiert wurde. Dank der heutigen Technologie wäre dies durchaus umsetzbar. Die Verwendung der Sozialversicherungsnummer ausserhalb des Sozialversicherungsbereichs (Steuerbehörden, Banken, Vereine etc.) – wie heute mit der AHV-Nummer möglich – ist in jedem Fall zu untersagen. Würde man die Sozialversicherungsnummer in anderen Bereichen auch verwenden, so bestünde durch die Verknüpfbarkeit die Gefahr, dass umfassende Persönlichkeitsbilder oder gar Persönlichkeitsprofile erstellt werden könnten. Eine solche Zweckänderung gilt es zu vermeiden. Die Sozialversicherungsnummer hat sich daher auf die Sozialversicherungsgesetzgebung zu beschränken. Ferner ist anzustreben, dass die Bearbeitung der Sozialversicherungsnummer in einer klaren Rechtsgrundlage geregelt wird. Schliesslich haben wir noch die Ausarbeitung eines Bearbeitungsreglements vom BSV verlangt.

Wir werden im Rahmen unserer Möglichkeiten das vorliegende Projekt weiterhin begleiten und auf seine Datenschutzkonformität hin überprüfen.

6.2 Privatversicherungen

6.2.1 Die Beschaffung von Personendaten durch Haftpflichtversicherer

Die Frage, unter welchen Voraussetzungen Haftpflichtversicherer Personendaten beschaffen dürfen, beschäftigte uns auch in diesem Berichtsjahr. Die involvierten Kreise wurden eingeladen, ihre Meinung zu diesem Problem darzulegen. Wir sind zur Zeit daran, die notwendigen Mindeststandards für die Datenbeschaffung durch Haftpflichtversicherer aufzustellen.

Haftpflichtversicherer holen bei Psychiatern, Biomechanikern etc. zum Teil ohne Einwilligung der Geschädigten Gutachten über sie ein. Die Geschädigten werden auch nicht immer darüber informiert. Dies führt in der Praxis insbesondere im Zusammenhang mit HWS-Fällen (Schleudertrauma) zu Problemen. Wir haben daher die involvierten Kreise (Versicherungsbranche, Geschädigtenanwälte und Gutachter) eingeladen, um die einzelnen Standpunkte besser kennen zu lernen.

Aus unserer Sicht dürfen Gutachten durch die Haftpflichtversicherer grundsätzlich nur dann eingeholt werden, wenn als Rechtfertigungsgrund die Einwilligung der Geschädigten vorliegt. Aufgrund des informationellen Selbstbestimmungsrechts entscheidet der Geschädigte in erster Linie selber über seine Daten; solange die Einwilligung möglich ist, hat dieser Rechtfertigungsgrund grundsätzlich Vorrang vor anderen möglichen Rechtfertigungsgründen (dazu mehr im 9. Tätigkeitsbericht 2001/2002, Abschnitt 6.2.2). Zudem liegt ein Gutachten des Bundesamtes für Justiz (BJ) zur strafrechtlichen Frage vor. Das Gutachten des BJ geht grundsätzlich davon aus, dass psychiatrische Gutachten, welche neue Erkenntnisse enthalten, dem Patientengeheimnis nach Art. 321 StGB unterstehen. Die Weitergabe solcher Gutachten an die Haftpflichtversicherer sei somit nur mit Einwilligung der Geschädigten möglich. Dagegen ist die Weitergabe von anonymisierten Gutachten in jedem Fall erlaubt.

Demgegenüber sind Vertreter der Versicherungsbranche der Meinung, dass das Beschaffen von Gutachten durch Haftpflichtversicherer auch ohne Einwilligung der Geschädigten erlaubt sei. Insbesondere seien die Abklärungen notwendig, um Versicherungsbetrug zu verhindern und die Versichertengemeinschaft zu schützen. Ausserdem müssten die Gutachten möglichst schnell erstellt werden, da der Faktor Zeit eine wichtige Rolle spiele. Der Rechtfertigungsgrund des überwiegenden privaten Interesses sei somit gegeben.

Die Geschädigtenanwälte beharren jedoch darauf, dass Haftpflichtversicherer Gutachten über Geschädigte nur mit deren Einwilligung einholen dürfen. Es würden vorliegend besonders schützenswerte Daten bearbeitet, und der einzige Rechtferti-

gungsgrund sei die Einwilligung der Geschädigten. Diese hätten auch Mitwirkungsrechte, welche es zu berücksichtigen gelte. Im Weiteren sei es der Geschädigte, der die Ansprüche zu beweisen hat, und nicht der Haftpflichtversicherer.

Aus Sicht der Gutachter ist es wichtig zu wissen, unter welchen rechtlichen Voraussetzungen diese die Gutachten erstellen dürfen; es könne nicht an den Gutachtern liegen zu prüfen, ob sie nun rechtmässig handeln würden oder nicht; insbesondere sei unklar, ob und bei wem eine Einwilligung einzuholen ist. Für die Gutachter sei die gegenwärtige Situation vor allem auch deshalb unbefriedigend, weil ihnen z. T. mit Strafanzeigen gedroht worden sei.

Trotz der kontroversen Ansichten wird von allen Seiten anerkannt, dass die Transparenz der Datenbeschaffung für die Geschädigten verbessert werden muss.

Wir sind gegenwärtig daran, Mindeststandards für die Beschaffung von Personendaten durch Haftpflichtversicherer aufzustellen.

6.2.2 Die Rolle des medizinischen Dienstes der Privatversicherer

Zur Zeit finden zwischen der Verbindung der Schweizer Ärztinnen und Ärzte (FMH) und dem Schweizerischen Versicherungsverband (SVV) Gespräche zum Thema Datenschutz statt. Unter anderem wird auch die Rolle des medizinischen Dienstes der Privatversicherer genauer analysiert.

Ausser im Krankenversicherungsgesetz (KVG) ist das Institut des Vertrauensarztes (bzw. medizinischen Dienstes) in keinem anderen Gesetz geregelt. Der Vertrauensarzt nach KVG ist gegenüber der Versicherungsadministration unabhängig; zudem kommt ihm eine gewisse Filterfunktion zu. Insbesondere gehen medizinische Angaben direkt an den Vertrauensarzt (und nicht an die Kassenverwaltung), wenn der Versicherte dies wünscht. Dies kommt den Persönlichkeitsrechten der Versicherten entgegen und entspricht insbesondere dem datenschutzrechtlichen Verhältnismässigkeitsprinzip.

Es stellt sich daher die Frage, ob die Einrichtung des Vertrauensarztes nicht auch für andere Versicherer gelten soll. Wir fordern schon seit Langem, die bestehenden medizinischen Dienste (Kreisärzte, beratende Ärzte etc.) der anderen Versicherer auch in diesem Sinne zu nutzen bzw. solche einzuführen (mehr dazu im 8. Tätigkeitsbericht 2000/2001 Kapitel I. 6.4). Auch wenn – mit Ausnahme des KVG – keine spezifischen datenschutzrechtlichen Normen für den medizinischen Dienst bestehen, sind die datenschutzrechtlichen Grundsätze immer einzuhalten. Dies gilt vor allem für besonders schützenswerte Daten wie etwa Gesundheitsdaten.

Tatsächlich ist der medizinische Dienst bzw. der beratende Arzt in der Privatassekuranz an sich nichts Neues. Es sei diesbezüglich auf eine Empfehlung der Versicherungswirtschaft und der FMH aus dem Jahre 1986 verwiesen. Gestützt auf diese Empfehlung besteht die Möglichkeit, dass medizinische Angaben an den medizinischen Dienst der Versicherungsgesellschaft adressiert werden können und ausschliesslich dort aufzubewahren sind.

Die Rolle des medizinischen Dienstes in der Privatassekuranz ist denn auch eines der Themen, welches die FMH und der SVV gegenwärtig einer Analyse unterziehen. Diesbezüglich soll auch geprüft werden, ob der Datenfluss in der von den Privatversicherern durchgeführten obligatorischen Unfallversicherung noch datenschutzkonform ist. So wird z. B. diskutiert, ob sehr sensitive Informationen zuerst an den medizinischen Dienst (bzw. den beratenden Arzt) und nicht direkt an die Versicherungsverwaltung gelangen sollen. Heikle Angaben wie z. B. Aids, psychiatrische Diagnosen oder Suchtkrankheiten können bei den Versicherten zu einer Stigmatisierung bzw. Diskriminierung führen. Deren Bearbeitung, muss daher – soweit dies möglich ist – auf ein Minimum beschränkt werden (Prinzip der Datensparsamkeit und der Datenvermeidung).

Wir begrüssen die Initiative der FMH und des SVV, denn wir erachten es als notwendig, den gesamten Privatversicherungsbereich auf seine Datenschutzkonformität hin zu überprüfen. Es bleibt jedoch abzuwarten, ob tragfähige und vor allem datenschutzkonforme Lösungen für die gesamte Privatassekuranz gefunden und umgesetzt werden.

7. Arbeitsbereich

7.1 Weitergabe von Informationen durch den betrieblichen Vertrauensarzt

Bei krankheits- oder unfallbedingten Abwesenheiten kann der Arbeitgeber den Arbeitnehmer durch den Vertrauensarzt der Firma untersuchen lassen. Der Vertrauensarzt untersteht für seine ärztliche Tätigkeit der ärztlichen Schweigepflicht. Diese gilt auch gegenüber dem Arbeitgeber. Der Arzt darf diesem lediglich seine medizinischen Schlussfolgerungen mitteilen.

Während der Dauer des Arbeitsverhältnisses darf der Arbeitgeber diejenigen Daten seiner Arbeitnehmer bearbeiten, die für die Durchführung des Arbeitsverhältnisses erforderlich sind. Bei krankheits- oder unfallbedingten Abwesenheiten hat der Arbeitgeber das Recht, den Arbeitnehmer durch den Vertrauensarzt untersuchen zu lassen. Der Vertrauensarzt untersteht für seine ärztliche Tätigkeit dem Berufsgeheimnis, der

sogenannten ärztlichen Schweigepflicht. Diese Schweigepflicht gilt auch gegenüber dem Arbeitgeber. Der Vertrauensarzt darf dem Arbeitgeber nur seine medizinischen Schlussfolgerungen mitteilen, und zwar so weit, wie diese für die Abwicklung des Arbeitsverhältnisses notwendig sind. In der Regel handelt es sich dabei um Aussagen über die Arbeitsfähigkeit bzw. Arbeitsunfähigkeit des Arbeitnehmers, z.B. ob er voll, teilweise oder gar nicht arbeitsfähig ist, ob die Arbeitsunfähigkeit die Folge einer Krankheit oder eines Unfalles ist, wie lange die Arbeitsunfähigkeit voraussichtlich dauern wird u.Ä. Solche Informationen sind für die ordnungsgemässe Durchführung des Arbeitsverhältnisses notwendig, da der Arbeitgeber bei längerer Abwesenheit beispielsweise für Ersatzpersonal sorgen muss. Medizinische Informationen darf der Vertrauensarzt hingegen nicht ohne die Einwilligung des Arbeitnehmers weiterleiten. Dies gilt ganz besonders für die Mitteilung von Diagnosen.

7.2 Spionprogramme aus der Sicht des Datenschutzes

Spionprogramme erlauben neben der Aufnahme sämtlicher ein- und ausgehenden E-Mails die Aufzeichnung der Bildschirminhalte sowie die detaillierte Aufnahme sämtlicher Tastenschläge und Surftouren. Arbeitgeber, die diese Mittel zur Kontrolle ihrer Angestellten einsetzen, verstossen gegen gesetzlich vorgegebene Persönlichkeitsschutzbestimmungen und machen sich somit strafbar.

Überwachungsprogramme werden in der Regel ohne Wissen der betroffenen Personen eingesetzt und ermöglichen eine permanente und detaillierte Überwachung sämtlicher Aktivitäten des Arbeitnehmers an seinem elektronischen Arbeitsplatz. Insbesondere gestatten sie die Einsicht in E-Mails, indem sie diese registrieren und anschliessend an eine Drittadresse weiterleiten. Auch das «Fotografieren» bzw. «Kopieren» des Bildschirms mit seinem gesamten Inhalt (z. B. Internetseiten) in regelmässigen Zeitabständen (recurrent screenshots) gehört zu den Funktionalitäten von Spionprogrammen. Ausserdem können solche Programme sämtliche Tastenanschläge erfassen, eingegebene Passwörter aufzeichnen, sämtliche aktive Anwendungen anzeigen, auf die Festplatte des PC zugreifen, abgespielte Audiodateien am PC abhören usw. Überwachungsprogramme ermöglichen auch die Speicherung der aufgezeichneten Aufnahmen und Informationen. Eine weitere Bearbeitung dieser Daten, z. B. in Form einer Datenbekanntgabe an Dritte, ist möglich. Es handelt sich somit um ein leistungsstarkes System zur heimlichen Überwachung des Verhaltens von Angestellten am Arbeitsplatz und stellt sowohl eine Verletzung des Verhaltensüberwachungsverbotes als auch des Grundsatzes von Treu und Glaube dar. Das Aufnehmen, Beobachten, Analysieren, Speichern und Weiterbearbeiten von Informationen und Aktivitäten aller Art am PC ohne Einwilligung der betroffenen Person stellt nach unserer Auf-

fassung ausserdem eine Verletzung des Geheim- oder Privatbereiches durch Aufnahmegeräte im Sinne des Strafgesetzbuches dar. Dadurch, dass der PC mit Überwachungs- und Aufnahmefunktionen dotiert wird, wird er zum Aufnahmegerät. Die Privatsphäre am Arbeitsplatz wird sowohl arbeitsrechtlich als auch durch das verfassungsmässige Fernmeldegeheimnis (vgl. BGE 126 I 50) geschützt. Aufgrund der vielfältigen Funktionen und Programmierungsmöglichkeiten der Überwachungsprogramme kann der Eingriff in die Persönlichkeit des Arbeitnehmers unter Umständen noch tiefgreifender sein als durch den Einsatz einer Videokamera. Das Bundesgericht hat über elektronische Überwachungssoftware noch kein Urteil gefällt.

7.3 Die E-Mail-Verwaltung während Abwesenheiten und beim Verlassen der Firma

Für einen reibungslosen Ablauf der Geschäftsverwaltung ist es erforderlich, dass der Ein- und Ausgang von Geschäftsunterlagen systematisch registriert und nachvollzogen werden kann. Weil eine äussere Unterscheidung von privaten und geschäftlichen E-Mail nicht immer ohne weiteres möglich ist, kann die Verwaltung der elektronischen Post von Arbeitnehmern während deren Abwesenheit datenschutzrechtliche Probleme bewirken. Wird für die geschäftliche Korrespondenz anstelle einer namen- eine funktionsbezogene Adressierung verwendet, können diese Probleme umgangen werden.

Im E-Mail-Bereich bestehen – analog zur herkömmlichen postalischen Geschäftskorrespondenz – zwei Adressierungsmodi: Die namentliche (z. B. hans.meier@firma.ch oder hans.meier@verkauf.firma.ch) und/oder die namenlose, funktionelle (z. B. info@firma.ch, verkauf@firma.ch, oder verkaufsleiter@firma.ch) Adressierung. Heutzutage ist die namentliche Adressierung weit verbreitet.

Bei der namentlichen Adressierung ist die Mailverwaltung während Abwesenheiten des betroffenen Arbeitnehmers und bei seinem Verlassen der Firma mit der Schwierigkeit der Unterscheidung zwischen privaten und geschäftlichen E-Mails verbunden. Wenn kein Unterscheidungsvermerk zwischen privaten und beruflichen E-Mails besteht und die private Natur eines E-Mails aufgrund der Adressierungselemente nicht erkennbar und nicht anzunehmen ist, darf der Arbeitgeber – analog zu den klassischen Postsendungen – davon ausgehen, dass das E-Mail beruflich ist. Bestehen berechtigte Zweifel an der Natur eines E-Mails, so hat der Arbeitgeber dies mit dem Arbeitnehmer abzuklären. Die Einsicht in den Inhalt des fraglichen E-Mails ist in diesem Fall nicht gestattet, unabhängig davon, ob private E-Mails erlaubt sind oder nicht.

Was die vorhersehbaren Abwesenheiten (z. B. Ferien, Urlaub, Militärdienst) betrifft, bestehen hauptsächlich drei Verwaltungsarten:

- Im E-Mail-Programm wird eine Antwort definiert, die beim Eingang einer Nachricht automatisch an den Absender versandt wird und die Abwesenheitsmeldung und Notfallkoordinaten enthält.
- Das E-Mail-Programm wird so eingerichtet, dass jede Eingehende Nachricht an einen zuvor definierten Stellvertreter weitergeleitet wird. Diese Lösung ist mit dem Risiko verbunden, dass auch private E-Mails an den gewählten Stellvertreter gelangen.
- Es wird ein Stellvertreter mit abgestufter Berechtigung zur Einsicht und eventuellen Weiterbearbeitung der eingehenden geschäftlichen E-Mails festgelegt. Die als privat gekennzeichneten E-Mails sind für den Stellvertreter nicht sichtbar. Dadurch bleibt die Privatsphäre des abwesenden Mitarbeiters geschützt.

Für den Fall von unvorhersehbaren Abwesenheiten (z. B. Krankheit, Unfall) sollten im Voraus Stellvertreter bestimmt werden.

Die namenlose Adressierung ist für die nicht persönliche geschäftliche Korrespondenz geeignet, da sie die oben erwähnten Schwierigkeiten der namentlichen Adressierung umgeht. Die namentliche Adressierung sollte für den rein persönlichen geschäftlichen Informationsaustausch (z. B. für Personalangelegenheiten oder persönliche Mitteilungen) verwendet werden.

Vor dem Austritt hat ein Mitarbeiter die noch hängigen Geschäfte wie E-Mails intern weiterzuleiten. Der Arbeitnehmer hat die Übergabe sämtlicher Geschäftsdokumente an die Firma zu bestätigen. Er hat die Möglichkeit, seine privaten E-Mails und andere private Dokumente auf private Datenträger zu speichern und aus den Servern der Firma zu löschen.

Beim Austritt ist spätestens am letzten Arbeitstag sein E-Mail-Account (wie übrigens auch alle anderen EDV-Accounts) zu sperren und sein Briefkasten (wie alle anderen persönlichen Datenträger) zu löschen. Der Arbeitgeber sollte sich dazu schriftlich verpflichten. Absender, welche E-Mails an die gesperrte E-Mail-Adresse schicken, werden automatisch informiert, dass die Empfängeradresse nicht mehr gültig ist.

7.4. Schutz der Privatsphäre bei der Benutzung des persönlichen Laufwerks

Arbeitnehmer verwenden ihre persönlichen Laufwerke (Homedrive) im Firmennetz häufig auch für rein private Zwecke. Dadurch wird natürlich Speicherplatz beansprucht, was – besonders wenn die verwendete Speichermenge gross ist – die Arbeitgeber oft veranlasst, die private Nutzung der persönlichen Laufwerke zu untersuchen.

Grundsätzlich soll der persönliche Homedrive nur für geschäftliche und persönlich-geschäftliche Dokumente verwendet werden. Private Dokumente sind hingegen auf private Datenträger zu übertragen. Dadurch kann sich der Angestellte gegen den unberechtigten Zugriff Dritter schützen. Der Zugriff auf persönliche und geschäftliche Dokumente im persönlichen Homedrive durch Vorgesetzte oder Informatiker soll nur im Bedarfsfalle und unter der Voraussetzung, dass ein Rechtfertigungsgrund sowie eine Zugriffsregelung besteht, zulässig sein.

Analog wie im Bereich der E-Mail-Nutzung am Arbeitsplatz empfiehlt es sich auch im Zusammenhang mit dem persönlichen Homedrive, eine an die jeweiligen persönliche Bedürfnisse der Mitarbeiter angepasste Speicherplatzbeschränkung (Diskquota) festzusetzen. Diskquotas verhindern den unmässigen Zuwachs der Speicherplatzbeanspruchung und die unverhältnismässig lange Aufbewahrungsdauer von Dokumenten. Der PC-User wird durch Diskquotas gezwungen, seinen persönlichen Speicherplatz zu verwalten und unnötige Dokumente in regelmässigen Zeitabständen zu löschen bzw. auf andere Datenträger (z. B. Diskette) zu übertragen.

7.5 Datenschutzaspekte bei der Benutzung des elektronischen Terminplaners am Arbeitsplatz

Die elektronische Agenda am Arbeitsplatz kann Probleme aufwerfen. Private Daten werden mit beruflichen Informationen vermischt und mit dem PC am Arbeitsplatz abgeglichen. Eine Schwierigkeit bilden die Zugriffsregelungen auf diese Daten.

Die PC-Agenda steht aufgrund interner Zugriffsregelungen in der Regel einer grösseren Anzahl von Personen – meistens Sekretärinnen oder Vorgesetzten, oft aber auch sämtlichen Mitarbeitern – zur Verfügung. In der Agenda können aber auch Informationen festgehalten sein, welche Dritten nicht ohne weiteres zugänglich sein sollen. Angesprochen ist nicht nur die Privatsphäre des Angestellten, sondern auch seine beruflich-persönlichen Informationen oder private Informationen über Dritte (z. B. Geburtstage). Die Privatsphäre wird in der Regel nur einem beschränkten Bekanntenkreis bzw.

einer beschränkten Anzahl Zugriffsberechtigten zugänglich gemacht. Die betroffene Person hat das Recht, selber zu bestimmen, mit wem sie ihre Privatsphäre teilen möchte (informationelles Selbstbestimmungsrecht). Privates muss als solches ausdrücklich gekennzeichnet werden, um es vor der Einsicht von Arbeitskollegen oder Vorgesetzten zu schützen. Der Vermerk «privat» schützt den Inhalt des privaten Eintrags gegenüber Dritten. Die Tatsache aber, dass ein Arbeitnehmer Privates eingetragen hat, bleibt trotzdem ersichtlich.

Fehlt die Einwilligung der betroffenen Person, so dürfen private Agenda-Daten betreffend Dritte nur dann zugänglich gemacht werden, wenn ein überwiegendes privates oder öffentliches Interesse besteht.

7.6 Genetische Untersuchungen am Arbeitsplatz

Ärztliche Untersuchungen, wozu auch genetische Untersuchungen (sogenannte präsymptomatische Untersuchungen) gehören, können von Bedeutung sein, wenn Gesundheitsschutz- und Sicherheitsvorschriften in Arbeitsbranchen mit erheblichem Gesundheits- oder Sicherheitsrisiko ausgearbeitet werden. Die Bearbeitung genetischer Daten am Arbeitsplatz wird im Entwurf eines Bundesgesetzes über genetische Untersuchungen beim Menschen geregelt. Die Sammlung genetischer Informationen kann eine widerrechtliche Persönlichkeitsverletzung darstellen.

Genetische Untersuchungen dienen der Abklärung einer möglichen arbeitsrelevanten genetischen Veranlagung von Angestellten oder Bewerbern.

Genetische Überwachungen sehen regelmässige genetische Untersuchungen vor. Der Zweck einer genetischen Überwachung liegt darin, das Risiko des Ausbruchs einer Krankheit vorauszusehen oder frühe Stadien von genetischen Schäden (z. B. genetische Mutationen) zu erkennen. Es werden Arbeitnehmer genetisch überwacht, die regelmässig besonderen Substanzen oder Gefahren am Arbeitsplatz ausgesetzt sind.

In Ländern, wo genetische Untersuchungen bereits praktiziert werden, werden genetische Informationen zu verschiedenen Zwecken gebraucht. Sie werden beispielsweise zur Ablehnung von «genetisch ungünstig veranlagten» Bewerbern oder zur Versetzung von Angestellten an weniger riskante Arbeitsstellen verwendet. Ein Beispiel kann die genetische Untersuchung auf Asthma-Anfälligkeit für Bewerber sein, die in einem verstaubten Arbeitplatz (etwa in einer Bäckerei) arbeiten müssen. Oft geht es auch darum, Produktivitätsverluste zu vermeiden, die z. B. durch Krankheitsabwesenheiten verursacht werden können. Genetische Daten werden auch zu

Identifikationszwecken benutzt. In England etwa werden die genetischen Daten von Polizeibeamten oder -anwärter mit den an Tatorten vorgefundenen genetischen Spuren verglichen, um mögliche spätere Kontaminationen der Beweismitteln zu vermeiden. In den USA werden genetische Proben zur Identifikation von Kriegsgefallenen verwendet. Die Angehörigen der Armee können die Vernichtung ihrer genetischen Proben verlangen, sobald sie die Armee verlassen haben. Der Arbeitgeber nutzt genetische Informationen auch dazu, die Gesundheit und die Sicherheit von Dritten zu schützen.

Verschiedene Kreise haben bereits Kritik an den genetischen Untersuchungen geäussert. Die Benutzung von genetischen Informationen kann erstens dazu führen, dass Arbeitnehmer, bei denen bestimmte genetische Veranlagungen festgestellt werden, von gewissen Arbeitsbranchen ausgeschlossen werden. Eine genetische Veranlagung bedeutet aber nicht automatisch, dass bei der betreffenden Person die entsprechenden Symptome auch wirklich auftreten werden. Weitere Diskriminierungen durch andere Arbeitgeber oder Versicherer werden möglich, wenn ihnen die genetischen Informationen bekannt gegeben werden (Verlust der Kontrolle über die eigenen genetischen Daten). Dies könnte statt zu einer Entlastung eher zu einer Belastung des Gesundheits- und Sozialversicherungswesens führen (insbesondere der Arbeitslosenversicherung). Es besteht aber ein öffentliches Interesse, sowohl die Person in Bezug auf Ihr Recht auf Arbeit als auch das Gesundheits- und Sozialversicherungswesen zu schützen.

Die Bearbeitung von genetischen Daten kann auch ein Risiko für die Persönlichkeit darstellen. Einerseits stellen genetische Tests eine einschneidende Massnahme dar, welche die körperliche Integrität verletzen kann. Andererseits kann die Sammlung genetischer Informationen einen Eingriff in die informationelle Privatsphäre der betroffenen Person und ihrer Familie darstellen. Der Schutz der Privatsphäre ist in diesem Zusammenhang als öffentliches Interesse zu verstehen. Während die Privatsphäre in der Regel als individuelles Recht verstanden wird, hat der Eingriff auf die Privatsphäre einer grösseren Anzahl von Personen einen Einfluss auf die ganze Gesellschaft. Weiter gilt es zu bedenken, dass aufgrund des Abhängigkeitsverhältnisses des Arbeitnehmers gegenüber dem Arbeitgeber nicht ohne weiteres davon ausgegangen werden kann, dass eine allfällige Einwilligung von der betroffenen Person wirklich freiwillig erteilt worden ist. Eine genetische Untersuchung könnte auch das Recht verletzen, die eigene genetische Veranlagung zu ignorieren. Möglich ist auch ein fehlender Zusammenhang zwischen ausgeübter Arbeit und Ausbruch einer bestimmten Krankheit. Somit ist nicht sicher, ob genetische Daten bessere Hinweise als gewöhnliche Gesundheitschecks liefern können. In den meisten Fällen ist es sinnvoller, die Gefahren- und Risikoquellen zu eliminieren, statt unnötige genetische Untersuchun-

gen durchzuführen. Der Arbeitgeber sollte vermeiden, ein kostspieliges Gentestprogramm einführen, ohne dass Klarheit über den Wert der erlangten Informationen besteht. Ferner besteht die Gefahr, dass genetische Untersuchungen die üblichen arbeitsrechtlichen Gesundheits- und Sicherheitsvorschriften ersetzen. Uns sind noch keine konkrete Fälle von genetischen Untersuchungen am Arbeitsplatz in der Schweiz gemeldet worden. Die Bearbeitung genetischer Daten am Arbeitsplatz wird aber bereits im Entwurf des Bundesgesetzes über genetische Untersuchungen beim Menschen geregelt. Dabei werden Diskriminierungen aufgrund des Erbguts ausdrücklich verboten. Der Entwurf macht die Durchführung von genetischen Tests am Arbeitsplatz ausserdem von strengen Voraussetzungen abhängig; so bedarf diese der Einwilligung durch die betroffene Person und darf nur vorgenommen werden, wenn andere Methoden (z. B. die Erhebung von Daten über die Krankengeschichte der Familienmitglieder) die benötigten Informationen nicht liefern können (Verhältnismässigkeitsprinzip). Der Entwurf des Bundesgesetzes sieht auch vor, dass präsymptomatische Untersuchungen nur durchgeführt werden dürfen, wenn am Arbeitsplatz die Gefahr einer Berufskrankheit oder einer schweren Umweltschädigung oder aber ausserordentliche Unfall- oder Gesundheitsgefahren für Dritte vorliegen. Hinzu kommt, dass genetische Untersuchungen nur statthaft sind, wenn andere Massnahmen des Unfallversicherungsgesetzes oder anderer gesetzlichen Bestimmungen nicht ausreichen, die entsprechenden Gesundheits- oder Unfallgefahren auszuschliessen. Der Arbeitsplatz wird ausserdem durch Verfügung der Schweizerischen Unfallversicherungsanstalt oder aufgrund rechtlicher Vorschriften der arbeitsmedizinischen Vorsorge unterstellt sein müssen. Der Gesetzesentwurf legt zudem fest, dass die Untersuchungsart von einer Eidgenössischen Kommission für genetische Untersuchungen für sicher und zuverlässig bezeichnet werden soll. Der Gesetzgeber hat die Bearbeitung von genetischen Daten dem Berufsgeheimnis unterstellt und dessen Verletzung mit strafrechtlichen Konsequenzen verbunden.

8. Handel und Wirtschaft

8.1 Unzulässige Werbung per Mail (Spam)

Werbemails machen heute einen bedeutenden Teil des Verkehrs von elektronischer Post aus. Wer solche Werbebotschaften nicht wünscht, hat es oft nicht leicht, den Versand durch bestimmte Werbetreibende für seine Adresse zu stoppen.

Unverlangte und damit zum Teil unerwünschte Werbung per Mail stellt vor allem deshalb ein Massenphänomen dar, weil der Versender dabei mit minimalen Kosten und Aufwand eine enorm grosse Zahl an Empfänger erreicht. Die problematische Seite

des Ganzen besteht darin, dass Aufwand und Kosten bei den Empfängern anfallen – Verbindungsgebühren, Durchsicht und Löschung der Mails, Speicherplatz –, von denen zumindest ein Teil die Werbung jedoch nicht will.

Gemäss aktueller Rechtslage in der Schweiz müssen mindestens die folgenden zwei Voraussetzungen erfüllt sein, damit die ungefragte Zustellung von Werbemails als rechtmässig bezeichnet werden kann: Erstens dürfen nur rechtmässig gesammelte Adressen verwendet werden. Das bedeutet insbesondere, dass nebst denjenigen Adressen, deren Inhaber explizit einer Verwendung zu Werbezwecken durch bestimmte Werbetreibende oder für bestimmte Interessengebiete zugestimmt haben, nur noch diejenigen öffentlichen Verzeichnisse in Betracht kommen, deren Benutzungsregeln die Verwendung zu Werbezwecken nicht ausschliesst. Als nicht rechtmässig gesammelt müssen dagegen diejenigen Adressen bezeichnet werden, deren Inhaber die Benutzung zu Werbezwecken nicht wünscht und dies explizit oder implizit kundtut. Als Beispiel expliziter Äusserung ist z.B. ein Vermerk wie «keine Werbung» oder «no address grabbing» auf einer Webseite zu werten. Impliziter Widerspruch ist wohl überall dort anzunehmen, wo der Verwendungszweck der Adresse ein spezifischer und nicht werbebezogener ist. Zweitens muss den Empfängern von Werbemails jederzeit eine einfache Möglichkeit zur Ausübung ihres Löschungsrechts gegeben werden. Sicher besteht die einfachste und dem Medium angemessene Möglichkeit darin, im Werbemail selbst eine Mail-Adresse anzugeben, über welche dies geschehen kann. Diese Anforderung wird auch in den Grundsätzen – insbesondere Grundsatz 4.4 – der Schweizerischen Lauterkeitskommission statuiert (http://www.lauterkeit.ch/pdf/grundsaetze.pdf). Gerade dieser Forderung nach einer einfachen Löschungmöglichkeit kommen jedoch bekannte Versender von Werbemails öfters nicht nach. Wir haben in unserer Empfehlung vom 24. Januar 2003 den schon im 9. Tätigkeitsbericht erwähnten in Zürich wohnhaften Werbetreibenden formell aufgefordert, seine Geschäftstätigkeit und Datenbearbeitung den gesetzlichen Vorschriften anzupassen. Die Empfehlung ist im Anhang zu diesem Bericht (Abschnitt 13.7.3) publiziert.

In der Schweiz sind die rechtlichen Möglichkeiten derjenigen welche sich gegen unerwünschte Werbung wehren wollen, (noch) gering (vgl. zu den Möglichkeiten unser Merkblatt Spam auf www.edsb.ch). Gegenüber Werbetreibenden des privaten Sektors muss der mühselige – weil oft teure und bezogen auf den Ausgang unsichere – Zivilrechtsweg beschritten werden. Der Bundesrat hat vor 3 Jahren eine Motion (vgl. Motion 00.3393) zum Thema entgegengenommen, welche eine Änderung der Rechtslage verlangt. Es ist vorgesehen, im Rahmen der Revision des Fernmeldegesetzes (FMG) einen entsprechenden Artikel im Bundesgesetz gegen den Unlauteren Wettbewerb (UWG) aufzunehmen. Die Rechtslage im umliegenden Ausland sieht etwas anders aus.

Frankreich kennt beispielsweise ein bedeutend strengeres Regime. Dort müssen zunächst die Datensammlungen mit Adressen der Aufsichtsbehörde CNIL (Commission Nationale de l'Informatique et des Libertés) gemeldet werden, und ein Verstoss gegen die Regeln rechtmässigen Beschaffens oder Weitergebens von Adressen kann strafrechtliche Folgen haben (bis 5 Jahre Gefängnis und 300'000 Euro Busse). Weitere Informationen finden sich auf der Webseite der CNIL (http://www.cnil.fr). Die EU hat in ihrer Richtlinie 2002/58/EG das Prinzip der vorgängigen Einwilligung zur Regel gemacht, und ihre Mitgliedsstaaten müssen dieses bis zum 31. Oktober 2003 ins Landesrecht umgesetzt haben. In einigen Ländern (Österreich, Dänemark, Finnland und Italien) gilt dieses Prinzip schon gemäss älteren Regelungen.

9. Finanzen

9.1 Informationsstelle für Konsumkredit

Das Konsumkreditgesetz sieht die Schaffung einer Informationsstelle für Konsumkredit vor. Sie führt eine elektronische Datensammlung mit Angaben zu Personen, die einen Konsumkredit erhalten haben. Die Informationsstelle kann die Datenbearbeitung nicht einfach in ihren Statuten regeln, sondern muss dafür wie jedes andere Bundesorgan über ausreichende gesetzliche Grundlagen verfügen. Dazu gehört auch eine transparente Information über den Datenumfang und den Kreis der Datenbearbeiter.

Das neue Bundesgesetz über den Konsumkredit ist auf den 1. Januar 2003 in Kraft getreten. Darunter fallen nicht nur Barkredite und Teilzahlungsverträge (z.B. Leasingverträge), sondern auch Kunden- und Kreditkarten sowie Überziehungskredite, sofern damit die Möglichkeit verbunden ist, den Saldo in Raten zu begleichen. Das Gesetz kommt nur zur Anwendung, wenn die Kreditgeberin gewerbsmässig Konsumkredite gewährt und die Konsumentin oder der Konsument den Kredit für private, also nicht für berufliche oder gewerbsmässige Zwecke beansprucht.

Für Konsumkreditgeberinnen besteht einerseits die gesetzliche Verpflichtung, vor Abschluss eines Geschäftes die Kreditfähigkeit jeder gesuchstellenden Person zu überprüfen; anderseits müssen sie alle gewährten Konsumkredite einer zentralen Stelle melden. Aus diesen Gründen haben sich die Kreditgeberinnen zu einen Verein mit dem Namen «Informationsstelle für Konsumkredit (IKO)» zusammengeschlossen. Die IKO fasst alle gemeldeten Angaben in einer elektronischen Datensammlung, dem sogenannten Informationssystem über Konsumkredite, zusammen. Es handelt sich dabei um die Personalien der Konsumentin oder des Konsumenten (Vorname, Name, Geburtsdatum, Wohnadresse) sowie um Angaben zum Konsumkredit (wie Kreditart,

Vertragsbeginn und -ende, Anzahl Raten, Bruttobetrag des Kredits, Höhe der Tilgungsraten usw.). Die Kreditgeberinnen können auch in einem Abrufverfahren – beispielsweise im Rahmen der Kreditfähigkeitsprüfung – auf die Angaben zugreifen.

Die IKO ist zwar ein privater Verein, laut Konsumkreditgesetz ist sie aber auch ein Bundesorgan im Sinne des Datenschutzgesetzes. Aufgrund dieser Konstellation war es immer wieder nötig darauf hinzuweisen, dass die IKO für die Datenbearbeitung eine ausreichende gesetzliche Grundlage benötigt. Die Statuten eines privaten Vereins reichen dazu nicht aus. Wir haben uns dafür eingesetzt, dass die IKO die gleichen Regeln für die Datenbearbeitung beachten muss wie die übrigen Bundesorgane. Es ist uns schliesslich gelungen durchzusetzen, dass die Einzelheiten zur Datenbearbeitung in der Verordnung zum Konsumkreditgesetz klar festgehalten werden und im dazugehörigen Anhang der vollständige Datenkatalog, der Umfang des Zugriffs und die Berechtigung zur Datenbearbeitung umfassend aufgeführt werden. Darüber hinaus muss die IKO eine Liste der zum Abrufverfahren zugelassenen Kreditgeberinnen führen, diese Liste auf dem neusten Stand halten und allgemein zugänglich machen. Auf unsere Anregung hin hat sich die IKO zudem bereit erklärt, die Statuen sowie das «Reglement betreffend die Abwicklung des Geschäftsverkehrs mit der IKO» zu veröffentlichen.

Die Inhaberin des Informationssystems über Konsumkredite ist die IKO. Somit ist sie gemäss Datenschutzgesetz dafür verantwortlich, dass keine falschen Angaben publiziert und die Einträge nach Rückzahlung des Konsumkredits umgehend gelöscht werden.

Das Eidgenössische Justiz- und Polizeidepartement hat die Statuten der IKO und das erwähnte Reglement genehmigt. Wir haben dazu einen Vorbehalt angebracht, da eine abschliessende datenschutzrechtliche Beurteilung der Datenbearbeitung durch die IKO erst möglich ist, wenn uns das vom Datenschutzgesetz geforderte Bearbeitungsreglement vorliegt.

9.2. Einwilligungsklauseln in Kreditkartenanträgen

Einwilligungsklauseln in AGBs sind ein Dauerthema des Datenschutzes, weil sie oft von Informationsbeschaffung und –weitergabe handeln. Nebst denjenigen in Versicherungsanträgen und im Fernmeldeverkehr geben in jüngster Zeit vor allem diejenigen in Kreditkartenanträgen Anlass zur Sorge.

Wir haben mehrere Beschwerden von Betroffenen zu den Einwilligungsklauseln der allgemeinen Geschäftsbedingungen im Kreditkartenbereich erhalten. Verschiedene Versionen von AGBs zeigen in der Tat bedenkliche Elemente. Viele dieser Klauseln

enthalten äusserst intransparente Formulierungen, welche die rechtliche Gültigkeit einer entsprechenden Einwilligung als zweifelhaft erscheinen lassen. Schliesslich kann eine Einwilligung nur soweit gültig sein, wie ihre konkrete Tragweite für die betroffene Person auch absehbar ist. Wenn sich jedoch eine Kundin damit einverstanden erklären soll, dass Ihre Daten durch nicht näher bezeichnete Dritte bearbeitet werden mit dem Zwecke, Dienstleistungen zu entwickeln, an denen sie interessiert sein könnte, so ist das aus datenschutzrechtlicher Sicht alles andere als befriedigend. Beklagenswert ist, dass die verschiedenen Klauseln sich im Laufe der vergangenen Jahre weiter in Richtung Intransparenz entwickelt haben und bei den unterschiedlichen Issuers auch nicht dasselbe Mass an (Un-)Klarheit aufweisen. Wir sind der Auffassung, dass bei den verschiedenen Issuer – welche ja miteinander im Wettbewerb stehen – dieselben Regeln gelten müssen.

10. Statistik und Forschung

10.1 Weitergabe von Statistikdaten an andere Verwaltungsstellen

Die Verwendung von Statistikdaten zu Aufsichtszwecken ist erlaubt, wenn eine Bestimmung in einem Bundesgesetz es ausdrücklich vorsieht oder wenn die schriftliche Zustimmung der Betroffenen vorliegt. Werden Daten für statistische Zwecke und Daten für Aufsichtszwecke zusammen erhoben, verlangt das Transparenzprinzip, dass klar ist, welche Daten auch oder ausschliesslich Aufsichtszwecken dienen und an andere Ämter weitergegeben werden. Für die Weitergabe von Daten aus der Statistik der Leistungserbringer vom BFS an andere Ämter, insbesondere an das BSV, sind nach unserer Ansicht die gesetzlichen Grundlagen zu wenig präzis. Ein Gutachten des Rechtsdienstes des EDI kommt diesbezüglich zum gegenteiligen Schluss und erlaubt die Weitergabe.

Das BFS erstellt zahlreiche Statistiken im Gesundheitsbereich, unter anderem auch die Statistik der Leistungserbringer (Spitäler). Seit Einführung des Krankenversicherungsgesetzes (KVG) werden diese Daten auch für Aufsichtszwecke im Rahmen des Vollzuges des KVG verwendet. Die Verwendung von Statistikdaten zu Aufsichtszwecken ist allerdings gemäss Statistikgesetz nur möglich, wenn eine Bestimmung in einem Bundesgesetz dies ausdrücklich erlaubt oder wenn die schriftliche Zustimmung der Betroffenen für eine Bearbeitung zu anderen Zwecken vorliegt. (vgl. 4. Tätigkeitsbericht 1996/97, Kapitel I. 6.2; 5. Tätigkeitsbericht 1997/98, Kapitel II. 8.6; 6. Tätigkeitsbericht 1998/99, Kapitel I. 8.3)

Die Regelungen im KVG und in der Krankenversicherungsverordnung decken nach unserer Ansicht nur eine direkte Datenerhebung durch das BSV ab. Für eine Datenweitergabe vom BFS zum BSV sind sie zu wenig präzis; insbesondere halten sie nicht fest, ob aus den vom BFS übermittelten Daten das einzelne Spital bestimmbar sein darf oder nicht. Da bei Erhebungen des BFS Daten für statistische Zwecke und Daten für Aufsichtszwecke zusammen erhoben werden, muss aus Gründen der Transparenz für die Datenlieferanten (Spitäler) klar sein, welche Daten auch oder ausschliesslich Aufsichtszwecken dienen und anschliessend in nicht anonymisierter Form ans BSV oder andere Ämter weitergegeben werden.

Aus datenschutzrechtlicher Sicht müssten also entweder die gesetzlichen Grundlagen angepasst oder aber eine schriftliche Einwilligung der betroffenen Spitäler für die Datenweitergabe eingeholt werden.

Nach langwierigen Diskussionen zwischen uns und den diversen Ämtern hat nun der Rechtsdienst des Generalsekretariates des EDI ein Gutachten erstellt und darin festgehalten, dass die vorhandenen gesetzlichen Grundlagen für die Datenweitergabe ausreichend seien, und zwar für die Datenweitergabe sowohl gegenüber dem BSV wie auch gegenüber anderen mit der Durchführung, der Kontrolle oder Beaufsichtigung der Durchführung des KVG betrauten Organe (z.B. Preisüberwacher). Wir halten an unserer Position fest.

11. International

11.1 Europarat

11.1.1 Arbeiten der CJPD: Videoüberwachung, Chipkarte, Polizeidaten und gerichtliche Daten in Strafsachen

Die Projektgruppe für den Datenschutz (CJPD) tagte vom 7. bis zum 9. Oktober 2002 und verabschiedete einen Entwurf zu Leitgrundsätzen über den Datenschutz im Rahmen der Videoüberwachung.

Die CJPD verabschiedete anlässlich ihrer 40. Tagung einen Entwurf zu Richtlinien über den Datenschutz im Rahmen der Videoüberwachung. Darin werden die Grundsätze aufgeführt, welche beim Einsatz von Videoüberwachungs-Tätigkeiten durch öffentliche Behörden oder durch private Personen zu berücksichtigen sind. Ausserdem werden die Garantien für die betroffenen Personen definiert. Die CJPD verabschiedete zudem einen Bericht über die Auswirkung der Datenschutzgrundsätze betreffend gerichtliche Daten in Strafsachen sowie einen Bericht über die dritte Auswertung der

Empfehlung R (87) 15, welche die Verwendung von Personendaten im Polizeiwesen regeln soll. Die beiden Berichte beschreiben den Inhalt der Grundprinzipien des Datenschutzes in den jeweiligen Sektoren. Daneben setzte die CJPD die Arbeiten für die Annahme von Richtlinien über die Verwendung von Chipkarten fort. Schliesslich befasste sie sich mit den eigenen Arbeitsstrukturen und -methoden.

11.1.2 Arbeiten des T-PD: Vertragsklauseln – Evaluation des Übereinkommens 108

Der Beratende Ausschuss des Übereinkommens 108 (T-PD) hielt vom 9. bis zum 11. Oktober 2002 seine 18. Tagung ab. Der Ausschuss verabschiedete einen Leitfaden über die Vertragsklauseln im Bereich der grenzüberschreitenden Datenflüsse. Daneben vertiefte er die Arbeit an der Evaluation des Übereinkommens.

Der T-PD nahm unter schweizerischem Vorsitz einen Leitfaden betreffend die Vertragsklauseln im Bereich der grenzüberschreitenden Datenflüsse an. Dabei handelt es sich um ein wichtiges Instrument mit Blick auf die Datenübermittlung in Staaten, die kein angemessenes Datenschutzniveau gewährleisten. Der Leitfaden ergänzt den Mustervertrag, welchen der T-PD im Jahr 1992 angenommen hatte; er enthält Vorgaben zur Ausarbeitung von Vertragsklauseln, stellt aber kein rechtlich verbindliches Instrument dar. So soll der Leitfaden Exporteuren, die in einem Land wohnen, welches das Übereinkommen 108 ratifiziert hat, erlauben, mit den Auflagen des Übereinkommens 108 und des Zusatzprotokolls übereinstimmende Datenschutz-Vertragsklauseln abzufassen. Die Vertragsklauseln sollen insbesondere Garantien zur Achtung der Rechte von Personen, deren Daten an Drittstaaten ohne befriedigendes Datenschutzniveau übermittelt werden, enthalten. Der T-PD wird das Instrument je nach den künftigen Entwicklungen ergänzen.

Ausserdem genehmigte der T-PD die Resultate der Evaluationskonferenz zum Übereinkommen 108, welche im November 2001 in Warschau tagte (siehe 9. Tätigkeitsbericht, Abschnitt 11.1.2). Nach Auffassung des T-PD bleiben die Grundsätze des Übereinkommens 108 nach wie vor relevant; die Errungenschaften der Konvention sollen nicht in Frage gestellt werden. Dagegen wird vorgeschlagen, die Untersuchung der Grundsätze fortzusetzen und zu prüfen, inwiefern sie den Fragen, welche die technologische Entwicklung aufwirft, gerecht werden. Das Hauptaugenmerk gilt den Rechten der betroffenen Personen, der Untersuchung der grenzüberschreitenden Datenflüsse, den Folgen der neuen Technologien und der Prüfung der legitimen Ausnahmen von bestimmten Grundprinzipien des Datenschutzes gemäss Artikel 9 des Übereinkommens. Schliesslich befasste sich der T-PD mit den Strukturen des Datenschutzes im Europarat sowie mit den Arbeitsmethoden.

11.1.3 Konferenz über die Herausforderungen und Probleme für die neuen Datenschutzbehörden

Vom 12. bis zum 13. Dezember 2002 fand in Madrid die vom Europarat und der spanischen Datenschutzagentur ausgerichtete Konferenz über die Herausforderungen und Probleme der neuen Datenschutzbehörden statt. Wir haben daran teilgenommen und einen Bericht über die Herausforderungen des grenzüberschreitenden Personendatenverkehrs vorgestellt.

Als Antwort auf eine Anfrage der Mitgliedsstaaten des Europarates, die vor kurzem ein Datenschutzgesetz verabschiedet und eine Datenschutzbehörde eingesetzt haben, organisierten der Europarat und die spanische Datenschutzagentur eine Konferenz über die Herausforderungen und Probleme, mit denen die neu geschaffenen Datenschutzbehörden konfrontiert sind. An dieser Konferenz beteiligten sich die Vertreter der neuen Kontrollbehörden aus 15 mittel- und osteuropäischen Staaten, Zypern und Malta sowie die Vertreter der Datenschutzbehörden Frankreichs, Spaniens, Italiens, Portugals, der Niederlande, Québecs und der Schweiz (ESDB und Datenschutzbeauftragter von Zug). Auch die OECD und die Europäische Kommission nahmen an den Arbeiten teil. Die Konferenz bot Gelegenheit zu einem nützlichen und konstruktiven Meinungsaustausch zwischen den Behörden, die langjährige Erfahrungen mit der Anwendung von Datenschutzvorschriften besitzen, und den neu geschaffenen Behörden. Erörtert wurden Fragen wie der Umsetzungsmechanismus der Datenschutzgrundsätze, Kompetenzen und Rolle der Kontrollbehörden sowie Organisation, Unabhängigkeitsgrad und -bedingungen der Kontrollbehörden. Es wurde daran erinnert, dass die Unabhängigkeit eine entscheidende Voraussetzung für die Aufgabenerfüllung der Datenschutzbehörden bildet, welche ja zur Verteidigung der Menschenrechte bei der Bearbeitung von Personendaten eingesetzt wurden. Die Unabhängigkeit betrifft nicht nur die Aufgabe, sondern das eigentliche Wesen der Behörde; sie beschränkt sich nicht auf autonomes Handeln, sondern misst sich auch an der Ausstattung der Behörde mit (insbesondere budgetären) Mitteln und am Handlungsspielraum bei der Mittelverwaltung. Die Konferenz erörterte ausserdem die Probleme, auf welche die Behörden in den Beziehungen mit dem Datenschutzverantwortlichen bisweilen stossen, sowie die Rolle der Kontrollbehörden in den Bundesstrukturen; zu diesem Thema steuerte der Datenschutzbeauftragte des Kantons Zug einen Beitrag bei. Schliesslich befasste sich die Konferenz mit den Herausforderungen des grenzüberschreitenden Datenverkehrs. In diesem Zusammenhang unterbreiteten wir einen Bericht über die Regelung des Übereinkommens 108 und des Zusatzprotokolls betreffend den grenzüberschreitenden Datenverkehr und über die nationalen Regelungen im Lichte der Gesetzgebung bestimmter Übereinkommensparteien. Ausserdem setzten wir uns mit der Rolle der Datenschutzbehörden im Zusammenhang mit dem

grenzüberschreitenden Datenverkehr auseinander (der Bericht ist auf unserer Website www.edsb.ch sowie auf der Website des Europarates www.coe.int/dataprotection abrufbar). Wir forderten insbesondere, dass die Kontrollbehörden künftig eine aktivere Rolle spielen und sich bemühen müssen, die betroffenen Personen und die Datenbearbeitungsverantwortlichen für Risiken zu sensibilisieren, die mit dem grenzüberschreitenden Datenfluss zusammenhängen. Dazu wurde anlässlich der Konferenz erneut auf die Bedeutung der internationalen Zusammenarbeit unter nationalen Datenschutzbehörden hingewiesen, um die Herausforderungen einer globalisierten Gesellschaft zu bewältigen.

11.1.4 Entwurf eines Protokolls über genetische Untersuchungen beim Menschen

Eine Arbeitsgruppe des Europarates ist daran, das Protokoll über genetische Untersuchungen beim Menschen auszuarbeiten. Ein Teil des Protokolls wurde fertig gestellt und soll den interessierten Kreisen zur Stellungnahme unterbreitet werden.

Zum Übereinkommen des Europarates über Menschenrechte und Biomedizin (Konvention von Oviedo) sind verschiedene Zusatzprotokolle vorgesehen. Das Protokoll über genetische Untersuchungen ist eines davon. Es hat zum Ziel, genetische Untersuchungen für den medizinischen Bereich sowie den Arbeits- und Versicherungsbereich zu regeln (vgl. auch 9. Tätigkeitsbericht 2001/2002, Abschnitt 11.1.4).

Die Arbeitsgruppe hat sich im Berichtsjahr mit der Frage auseinander gesetzt, ob gewisse Teile des Protokolls vorher veröffentlicht werden sollen. Sie kam zum Schluss, Kapitel I (allgemeine Bestimmungen) und Kapitel II (medizinischer Bereich) des Protokolls nochmals zu überarbeiten und den interessierten Kreisen zur Vernehmlassung zu unterbreiten. Auch soll der dazugehörende Begleitbericht zur Diskussion gestellt werden. Die Arbeitsgruppe kommt somit den Wünschen des Ministerkomitees des Europarates entgegen.

Wichtige Themen in den erwähnten Kapiteln sind u. a. die Einwilligung der betroffenen Personen, Qualitätsstandards für genetische Untersuchungen, die genetische Beratung, die Aufbewahrung von biologischem Material (inkl. genetische Daten) und die allfällige Weitergabe von genetischen Daten an Familienmitglieder. Ausserdem wurden Regeln für genetische Reihenuntersuchungen sowie die Gentherapie aufgestellt. Auch wird festgelegt, unter welchen Voraussetzungen genetische Untersuchungen bei urteilsunfähigen Personen durchgeführt werden dürfen. Die Arbeitsgruppe wird in den folgenden Sitzungen den Arbeits- und Versicherungsbereich, welche zum Geltungsbereich des Protokolls gehören, näher untersuchen.

11.2 Europäische Union

11.2.1 Bilaterale Verhandlungen II zwischen der Schweiz und der Europäischen Union

Wir verfolgen die Verhandlungen über die Dienstleistungen sowie jene über den Beitritt zu den Abkommen von Schengen und Dublin aufmerksam mit. Im Fall einer Einigung würde eine Übernahme des europäischen «acquis» über den Datenschutz erforderlich. Die Dienststellen der Europäischen Kommission haben eine vergleichende Untersuchung des Europarechts und der Schweizer Gesetzgebung in die Wege geleitet (siehe auch Abschnitt 1.1).

11.2.2 Europäische Konferenz der Beauftragten für den Datenschutz

Die Europäischen Datenschutzbeauftragten versammelten sich am 25. und 26. April 2002 in Bonn und am 9. September 2002 in Cardiff. Wir nahmen als Beobachter daran teil. Die Konferenz verabschiedete eine Erklärung über die systematische und obligatorische Speicherung von Telekommunikations-Verkehrsdaten.

Die Mitglieder der Europäischen Konferenz der Datenschutzbeauftragten sind die Datenschutzbeauftragten der Länder der Europäischen Union, Norwegens und Islands. Ungarn, Polen, die Tschechische Republik und die Schweiz besitzen einen Beobachterstatus. Die Konferenz ermöglicht einen vertieften Austausch über die Entwicklung der Datenschutzgesetzgebungen in Europa und über technologische Entwicklungen, insbesondere über die datenschutzfreundlichen Technologien und Praktiken der Kontrollbehörden. Daneben erarbeitet sie gemeinsame Lösungen und verabschiedet Erklärungen zu aktuellen Themen.

Die Bonner Konferenz bot Gelegenheit, um die Bilanz der Massnahmen zu ziehen, die nach den Attentaten vom 11. September 2001 ergriffen worden waren. Die Datenschutzbeauftragten begrüssten es, dass insgesamt keine unverhältnismässigen und unbedachten Massnahmen ergriffen wurden, kamen aber überein, dass weiterhin Wachsamkeit geboten sei, da einschlägige Gesetze in mehreren Staaten in Vorbereitung sind. Die Datenschutzbeauftragten stellten fest, dass die Staaten in der Verwendung der Biometrie zu Polizeizwecken einen ähnlichen Ansatz verfolgten, dass die verabschiedeten Gesetze zeitlich befristet waren und dass sie evaluiert werden sollten. Die Datenschutzbeauftragten nahmen die technischen Entwicklungen im Bereich der biometrischen Identifizierung zur Kenntnis; die Technologie erlaubt ihres Erachtens ermutigende Durchbrüche zum Schutz der Privatsphäre der Einzelpersonen.

So können heute Videoüberwachungseinrichtungen verwendet werden, welche die Anonymität der gefilmten Personen so lange gewährleisten, wie keine Identifizierung erforderlich ist.

Daneben nahm die Konferenz die – hauptsächlich deutschen und niederländischen – Projekte betreffend die Zertifizierung und die «Datenschutz-Gütesiegel» zur Kenntnis. Sie plädierte dafür, gemeinsame Strategien auszuarbeiten, welche in einem europäischen Zertifizierungskonzept münden könnten. Schliesslich führten die Datenschutzbeauftragten einen Meinungsaustausch zu in verschiedenen Mitgliedsstaaten aktuellen Themen durch, darunter insbesondere E-Government und Nutzung der universellen Personennummer (PIN).

Am Rande der internationalen Konferenz der Datenschutzbeauftragten in Cardiff (siehe Abschnitt 11.4.1) verabschiedeten die europäischen Datenschutzbeauftragten eine Erklärung über die systematische und obligatorische Speicherung von Telekommunikations-Verkehrsdaten (siehe Abschnitt 13.6). So wird insbesondere betont, dass für die Aufbewahrung von Verkehrsdaten ein Bedarf nachzuweisen ist. Die Aufbewahrungsfrist soll möglichst kurz sein. Ausserdem muss die Praxis klar im Gesetz festgelegt werden, um den illegalen Zugang oder sonstige Missbräuche zu vermeiden. Die ein Jahr oder länger dauernde systematische Aufbewahrung jeglicher Verkehrsdaten wäre eindeutig unverhältnismässig und demzufolge unannehmbar.

11.2.3 Europäische Arbeitsgruppe über die Behandlung von Klagen und über den Informationsaustausch

Wir haben erneut an den Arbeiten dieser Arbeitsgruppe mitgewirkt, die im Rahmen der Europäischen Konferenz der Beauftragten für den Datenschutz eingesetzt wurde, um die Möglichkeiten der Zusammenarbeit unter den Datenschutz-Kontrollbehörden auszuloten, namentlich hinsichtlich der Untersuchung von Klagen und der Durchführung von Inspektionen. In den Arbeiten ging es vor allem um den Vergleich der jeweiligen nationalen Kontrollkompetenzen sowie um die Regelungen zum grenzüberschreitenden Datenverkehr.

Wir setzten unsere Tätigkeit in der europäischen Arbeitsgruppe «Complaints handling Workshop» fort und beteiligten uns an den Tagungen der Gruppe im Frühjahr und Herbst 2002 in Dublin bzw. in Berlin. Die Arbeitsgruppe soll gemäss dem von der Europäischen Konferenz der Datenschutzbeauftragten erteilten Mandat die unterschiedlichen Behandlungsmethoden für Klagen, die bei den Datenschutzbehörden erhoben werden, prüfen und die gegenseitige Zusammenarbeit fördern.

Anlässlich der beiden Tagungen beendete die Arbeitsgruppe die vergleichende Untersuchung der Kontrollverfahren der verschiedenen Datenschutzbehörden, die sie im Jahr 2001 in Lissabon in Angriff genommen hatte. Anhand dieser Arbeiten wurde ein zusammenfassender Bericht erstellt, der die Methoden auflistet, welche die Behörden zur Durchführung ihrer Überwachungstätigkeiten anwenden, und die verschiedenen gesetzlichen Kompetenzen der einzelnen Behörden vergleicht. Diese Arbeiten erlauben uns, uns an den Lösungen anderer Staaten zu orientieren, und vermitteln einen Einblick in die Untersuchungsbefugnisse der ausländischen Kollegen im Fall von Rechtshilfegesuchen bei Klagen und Ermittlungen im Zusammenhang mit Datenbearbeitungen über die nationalen Grenzen hinaus. Wir beteiligten uns in der Arbeitsgruppe auch an der Erstellung von vergleichenden Tabellen über die zahlreichen nationalen Regelungen zum grenzüberschreitenden Datenverkehr.

Im Laufe des Berichtsjahres hat sich das CIRCA (Communication & Information Resource Centre Administrator) für die Arbeiten der Arbeitsgruppe zu einem äusserst effizienten Kooperationsinstrument entwickelt. Über dieses gesicherte Extranetsystem, das mit dem IDA-Programm (Interexchange of Data between Administrations, Informationsaustausch zwischen öffentlichen Verwaltungen) der Europäischen Kommission verknüpft ist, konnten wir zahlreiche Informationen über die nationalen Lösungen, die für ähnliche Datenschutzprobleme gefunden wurden, übermitteln, die Ergebnisse der durchgeführten Kontrollen mitteilen und mit anderen Datenschutzbehörden nützliche Erfahrungen austauschen.

Anlässlich der Tagung in Dublin wurde von zahlreichen Teilnehmern nachdrücklich gefordert, den Informationsaustausch nicht nur auf die Mitglieder der Europäischen Union zu beschränkten, sondern das CIRCA-Informationsaustauschsystem und die Beteiligung in der Arbeitsgruppe auch anderen Staaten mit einem gleichwertigen Schutzniveau zugänglich zu machen. Im Sinne dieser Öffnung tagte die Arbeitsgruppe in Berlin unter Beteiligung der Vertreter der Datenschutzbehörden der Europäischen Union und der Schweiz sowie der neuen Teilnehmer wie Tschechien, die Slowakei, Slowenien, Litauen und Polen.

11.3 OECD

11.3.1 Arbeitsgruppe über die Informationssicherheit und den Schutz der Privatsphäre (WPISP)

Die Arbeitsgruppe beschäftigte sich mit der Revision der Richtlinien über die Informationssicherheit, der elektronischen Authentifizierung, der Privatsphäre im E-Commerce, der Relation zwischen selbstregulierenden Mechanismen und gesetzlichen Bestimmungen, der Notwendigkeit, die Kryptographierichtlinien zu revidieren, und der Rolle der Biometrie zum Schutz der Privatsphäre.

Neben dem symbolischen Aspekt der Veröffentlichung von neuen Richtlinien zu Sicherheitsfragen im Rahmen der Terrorbekämpfung stand vor allem die Schaffung einer «Sicherheitskultur» (culture of security) und zu diesem Zweck die Festlegung von Richtlinien zur Informationssicherheit im Vordergrund. Da schliesslich die Richtlinien relativ allgemein formuliert wurden, kam es zu keinen fundamentalen Meinungsverschiedenheiten zwischen den Mitgliedstaaten. Somit wurden die Prinzipien, die die Informationssicherheit der modernen Netzwerke prägen müssen, gutgeheissen.

Nach der Veröffentlichung der Richtlinien haben die Mitgliedstaaten und das Sekretariat Vorkehrungen getroffen, um sie weitmöglichst in der Öffentlichkeit zu streuen. Daneben haben verschiedenen Mitgliedstaaten auch an der Umsetzung der Sicherheitsprinzipien gearbeitet. Es bestand Einigkeit darüber, dass für die konkrete Umsetzung der Prinzipien durch die breite Öffentlichkeit insbesondere praktische Hinweise für die Sicherheit am PC zur Verfügung gestellt werden müssen. In diesem Sinne haben wir auf unserer Website unter der Rubrik «Themen» ein Kapitel zur Sicherheit eingefügt und darin – fürs Erste – eine Auswahl von relevanten Informationen für die Sicherheit am PC publiziert. Viele Mitgliedstaaten haben ähnliche Vorkehrungen getroffen.

Darüber hinaus hat die deutsche Delegation die Notwendigkeit einer international harmonisierten Sicherheitspolitik hervorgehoben und vorgeschlagen, auch die Arbeiten der EU im Bereich Sicherheit mit zu berücksichtigen. Die von der EU finanzierte Studie über technische Risiken und Abhängigkeiten zeigte schliesslich auf, dass technische Mindeststandards erforderlich sind, die aber auch gesetzlich abgestützt werden müssen. Wegen der bekannten Stellung der OECD zu gesetzlichen Regulierungen wurde die Studie kontrovers aufgenommen.

Bei der elektronischen Authentifizierung wurde ein Dokument erstellt, das die verschiedenen Modelle und die begleitenden Rechtsbestimmungen zusammenführt. Anhand dieser Auflistung wurden die zentralen rechtlichen Anforderungen erläutert. Zusätzlich wurde die Frage der Interoperabilität der Systeme erneut aufgeworfen, weil in den vergangenen vier Jahren auf diesem Gebiet wenig erreicht wurde. Die Pläne der italienischen Regierung, eine digitale Signatur, einen PIN und eine medizinischen Karte zusammenzuführen, stiessen auf grosses Interesse.

Während im Bereich der elektronischen Authentifizierung weiter gearbeitet wird, wird die Revision der Kryptographierichtlinien für vier Jahre auf Eis gelegt.

Der vorgestellte Bericht über die Umsetzung von Massnahmen zum Schutz der Privatsphäre im Bereich des E-Commerce nach der Konferenz in Ottawa (1999) hält fest, dass die Effektivitätsgrenze nur wegen der begrenzten Wirkung der gesetzlichen Bestimmungen zum Schutz der Privatsphäre erreicht wurde. Im Gegenzug wurden im Bericht Selbstregulierungsmechanismen – ohne dass dies überprüft und belegt wurde – als die einzigen Massnahmen für einen wirksamen Schutz der Privatsphäre vorgelegt. Wir verlangten die Streichung oder die Ergänzung des betreffenden Absatzes. Denn obwohl wir überzeugt sind, dass Selbstregulierung eine wichtige Rolle im E-Commerce zu spielen hat, sind wir der Ansicht, dass es dafür nebst nationalen gesetzlichen Bestimmungen auch international anerkannte Standards braucht, welche den Selbstregulierungsmechanismen die notwendige Wirksamkeit verleihen können.

Bei den Diskussionen, die die Arbeitsgruppe für das Arbeitsprogramm der nächsten zwei Jahren führte, wurde von verschiedenen Mitgliedländern vorgeschlagen, Marktanalysen über die Gründe des Misstrauens im E-Commerce zu führen. Dabei stellte sich heraus, dass die Studie die Wirtschaftlichkeit von Massnahmen zum Schutz der Privatsphäre untersuchen sollte (wann lohnt sich der Schutz der Privatsphäre?). Wir unterstrichen, das der Einsatz von Mitteln zum Schutz der Privatsphäre nicht ausschliesslich unter den ökonomischen Aspekt untersucht werden darf. Insbesondere darf nicht nur der Aspekt der wirtschaftlichen Rentabilität über den Einsatz von Massnahmen zum Schutz der Privatsphäre entscheidend sein, den in den meisten Mitgliedländern ist Datenschutz ein verfassungsmässiges Grundrecht. Demnach geht es nicht nur um wirtschaftliche Rentabilität, sondern auch um die Einhaltung von verfassungsmässigen Verpflichtungen von Staat und Wirtschaft.

Auch der Nutzen des Einsatzes der Biometrie (dazu gehören auch DNA-basierte erkennungsdienstliche Verfahren) wird analysiert werden. Gleichzeitig wird auch die Einführung eines PIN (Personal Identification Number) mit berücksichtigt. Diese Arbeiten sollen nebst der Identifikation im Rahmen der Terrorismusbekämpfung auch den möglichen Einsatz der Kontrolle der Bevölkerungsbewegungen untersuchen.

11.4 Weitere Themen

11.4.1 Internationale Konferenz der Beauftragten für den Datenschutz

Die XXIV. Internationale Konferenz der Datenschutzbeauftragten fand vom 9. bis zum 11. September 2002 in Cardiff statt. An der Konferenz beteiligten sich Delegationen aus weltweit 40 Staaten. Die Konferenz bot Gelegenheit, um die Bilanz der technologischen Entwicklungen zu ziehen und die Kontakte zwischen den Datenschutzbeauftragten und den Verantwortlichen für die Datenbearbeitungen – insbesondere transnationalen Unternehmen – auszubauen.

Den Beginn der Konferenz markierte eine den Datenschutzbeauftragten vorbehaltene Sitzung, während der ein Überblick über die Entwicklungen seit den tragischen Ereignissen vom 11. September 2001 vermittelt wurde. Die meisten Staaten setzten der Schwerpunkt auf den Kampf gegen den Terrorismus und die Geldwäscherei. Mehrere Kommissare betonten, dass jeder übermässige Eingriff in die Freiheiten der Bürger einen Sieg für den Terrorismus bedeutete. Es ist zentral wichtig nachzuweisen, dass eine Massnahme notwendig ist, und zu untersuchen, ob sie sich für die Lösung des jeweiligen Problems eignet (Achtung des Verhältnismässigkeitsgrundsatzes). Die Datenschutzbeauftragten üben ausserdem bei der Einführung biometrischer Erkennungsmassnahmen grosse Zurückhaltung. Wenn biometrische Daten zu Identifizierungszwecken in einem Ausweispapier aufgenommen werden, müssen sie nicht in einer zentralisierten Datenbank gespeichert werden: Die Identität lässt sich bereits anhand des Dokuments überprüfen. Schliesslich dürfen die geplanten Massnahmen nicht allein die Angelegenheit der Exekutive bleiben, sondern müssen demokratisch diskutiert werden. Daneben führten die Datenschutzbeauftragten einen Meinungsaustausch zu den Bereichen durch, welche sie vorrangig beschäftigen. Mehrere Datenschutzbeauftragte verwiesen auf die anhaltende Zunahme der Klagen im Zusammenhang mit der Nutzung des Internet. Die Nachforschungen werden mit der Globalisierung des Internet nicht erleichtert; deshalb müssen die Sensibilisierungskampagnen bei den Internet-Usern verstärkt werden. Auch das Thema Spamming weckt Besorgnis. Die Datenschutzbehörden werden von einer Lawine diesbezüglicher Klagen überrollt. Grosse Aufmerksamkeit wurde ferner den Themen Videoüberwachung, Überwachung am Arbeitsplatz, Genetik und Speicherung von Verkehrsdaten im Telekommunikationssektor gewidmet.

Der zweite Teil der Konferenz richtete sich an die Vertreter der Verwaltungen, der Industrie, der Dienstleistungen und sonstiger interessierter Kreise. Die Konferenz stand unter dem allgemeinen Motto «Das Recht auf Information im 21. Jahrhundert:

Eine Demystifizierung». Aus diesem Anlass wurden die Fragen des Informationszugangs und des Datenschutzes geprüft. Die Teilnehmer gingen der Frage nach, inwiefern der Datenschutz den Geschäftsverkehr der Verwaltungen bzw. der Unternehmen behindert, indem insbesondere die Weitergabe von Auskünften verhindert wird. Wichtig ist, die Probleme pro-aktiv zu betrachten und die Vor- und Nachteile des Informationszugangs bzw. der Verweigerung von Informationen unter Berücksichtigung aller Beteiligten, einschliesslich der betroffenen Personen, abzuwägen. Die Achtung der Privatsphäre stellt so kein Hindernis für die Online-Verwaltung dar, aber es muss unbedingt ein System eingerichtet werden, welches eben diese Achtung gewährleistet. Die Technologie bietet in diesem Zusammenhang Möglichkeiten, um Personendaten zu schützen und gleichzeitig den Informationsaustausch zu gestatten. Das Recht auf Anonymität ist für den Schutz der Privatsphäre von zentraler Bedeutung. Grundsätzlich sollten Personen ihre Identität nur dann preisgeben müssen, wenn dies für die Abwicklung einer bestimmten Transaktion durch eine Verwaltung oder ein Unternehmen zwingend erforderlich ist. Die Konferenz beschäftigte sich ausserdem mit der Rolle der Datenschutzbehörden in einer globalisierten Welt, mit dem Beitrag der Selbstregulierung sowie mit dem Verhältnis zwischen Datenschutz und Informations- und Meinungsäusserungsfreiheit.

12. Der Eidgenössische Datenschutzbeauftragte

12.1. Informationssitzung der Subkommission 2 der Finanzkommission des Nationalrates beim EDSB im September 2002

Am 6. September 2002 stattete uns die Subkommission 2 der Finanzkommission des Nationalrates einen Besuch ab. Die Subkommission interessierte sich insbesondere für unsere Organisation, unsere Tätigkeiten und für die Schwierigkeiten, die auf die zu knappen Ressourcen und Mittel zurückzuführen sind. Die Subkommission überzeugte sich von der ungenügenden personellen Ausstattung und von der Unmöglichkeit, die uns anvertrauten Gesetzesaufgaben zu erfüllen. Anlässlich der Wintersession beschloss der Nationalrat, die Problematik im Rahmen der Beratungen zur Teilrevision des Bundesgesetzes über den Datenschutz im Jahr 2003 zu erörtern.

In der Pressekonferenz vom 1. Juli 2002 anlässlich der Veröffentlichung des 9. Tätigkeitsberichtes wiesen wir nachdrücklich darauf hin, dass die Ressourcen für die Erfüllung unserer gesetzlichen Aufgaben nicht ausreichten. Die Subkommission 2 der Finanzkommission des Nationalrates wünschte nähere Information zum Thema und führte im Rahmen der Beratungen zur Festlegung des Voranschlages des Bundes für 2003 am 6. September 2002 einen Besuch bei unserem ständigen Sekretariat durch.

Anlässlich dieses Besuchs haben wir eine Bilanz unserer Tätigkeiten gezogen und unsere künftigen Perspektiven vorgestellt. Die Subkommission interessierte sich insbesondere für unsere Organisation, die uns anvertrauten gesetzlichen Aufgaben, die Zunahme unserer Tätigkeiten und für die Schwierigkeiten, die sich aus den knappen Ressourcen ergeben.

Auf Fragen nach den Mitteln, die wir zur Erfüllung der gesetzlichen Aufgaben besitzen, antworteten wir, dass dem Eidgenössischen Datenschutzbeauftragten ein mit 16,2 Stellen dotiertes ständiges Sekretariat zur Seite steht. Mit diesem Personalbestand müssen wir die Anwendung der eidgenössischen Datenschutzbestimmungen durch Bundesstellen und Privatpersonen überwachen. Dazu stellen wir von Amtes wegen oder auf Gesuch von Dritten Sachverhalte fest und empfehlen gegebenenfalls die Veränderung bzw. Einstellung der Bearbeitung. Unsere Aufgaben liegen in den Bereichen Beratung, Kontrolle, Gesetzgebung und Information. Wir wiesen darauf hin, dass wir mit dem aktuellen Personalbestand nicht in der Lage sind, alle uns anvertrauten Gesetzesaufgaben – vor allem im Kontrollbereich – zu erfüllen und mit den neuen technologischen Entwicklungen fertig zu werden.

Auf der Basis der Erläuterungen wünschte die Subkommission konkretere Beispiele zu bestimmten Tätigkeiten und den zur Durchführung eingesetzten Mitteln. So erklärten wir, dass beispielsweise im Bereich Sicherheit und Verbrechensbekämpfung die Mittel der Bundesbehörden aufgestockt würden, was zu einer Zunahme der Datenbearbeitungsvorgänge durch Bundesorgane führe. Diese Tendenz wurde mit der Notwendigkeit der Stärkung der inneren Sicherheit und der Verbrechensbekämpfung nach den Ereignissen von September 2001 noch verstärkt. Die Zunahme der Bundesaufgaben im Polizeiwesen und in der Strafverfolgung führte insbesondere beim Bundesamt für Polizei zu einer deutlichen Personalaufstockung. Bei uns dagegen blieb eine entsprechende Mittelerhöhung für die Durchführung der erforderlichen Kontrollen und für die Begleitung der Entwicklung von Informatikprojekten aus.

Ausserdem wiesen wir die Subkommission darauf hin, dass die Kostenexplosion im Gesundheitswesen eine Rationalisierung der Bearbeitung von Gesundheitsdaten und eine bessere Koordination der Tätigkeiten unter den verschiedenen Akteuren des Gesundheitswesens erfordert. Diese Entwicklungen dürfen die Rechte der Patienten und der Versicherten – insbesondere das Recht auf Schutz der Privatsphäre – jedoch nicht beeinträchtigen. Die aktuelle Tendenz bewirkt, dass wir bei der Begleitung bestimmter Projekte (Gesundheitskarte, elektronisches Patientendossier, Datenaustausch unter Gesundheitsanbietern und Versicherern usw.) immer stärker beansprucht werden. Wegen der fehlenden Mittel können zahlreiche Projekte nicht geprüft werden. So waren wir insbesondere im Bereich der medizinischen Forschung nie in der Lage, unsere gesetzlichen Aufgaben zu erfüllen und die Einhaltung der Voraussetzungen für die

Bewilligungserteilung durch die Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung zu untersuchen.

Schliesslich verwiesen wir die Subkommission auf Projekte im Zusammenhang mit den Entwicklungen der Informationstechnologien, namentlich E-Government (Guichet Virtuel und E-Voting): Für dieses Projekt stellte die Bundesverwaltung erhebliche Mittel frei, ohne jedoch unsere Ressourcen für die Beantwortung von Gesuchen um Begleitung des wichtigen Projekts zu erhöhen. Gleiches gilt für die Einführung des eidgenössischen Personenidentifikators, die elektronische Identitätskarte, die Harmonisierung der Verwaltungsregister oder für Projekte des Privatsektors namentlich im Bereich E-Commerce, E-Banking, E-Learning oder E-Marketing (insbesondere das Problem Spamming).

Die Mitglieder der Subkommission äusserten ihr Erstaunen über die im Vergleich zu den Aufgaben beschränkten Mittel und fragten, was zur Behebung dieses Missstands unternommen worden war. Wie wir erklärten, haben wir einige Rationalisierungsmassnahmen ergriffen und insbesondere das Geschäftsmanagementsystem «EDSB-Office» eingeführt, mit welchem sich die Prioritäten und die Zielsetzungen besser planen und mit verfolgen lassen. Trotz dieser Massnahmen reicht aber unser Personalbestand nicht aus, um alle gesetzlichen Aufgaben zu erfüllen. Zu dieser Schlussfolgerung war im übrigen bereits die Geschäftsprüfungskommission des Ständerates gelangt, die in ihrem Bericht vom 19. November 1998 über die Einführung von Online-Verbindungen im Polizeiwesen Folgendes betonte: «Die Geschäftsprüfungskommission teilt allerdings die Einschätzung des Datenschutzbeauftragten, dass ihm für die Erfüllung seiner gesetzlichen Kontrollaufgaben die Mittel und namentlich das Personal fehlen. Auf diese Problematik wurde bereits im Rahmen der Inspektion zur Einführung der Informatik in der Bundesverwaltung eingegangen. Die Kommission stellt fest, dass diese Situation immer noch aktuell ist» (BBl 1999 5895). Der Bundesrat anerkannte in seiner Antwort vom 1. März 1999 auf die einfache Anfrage Widmer «Datenschutz» (98.1185) die Stichhaltigkeit der Bemerkungen der Geschäftsprüfungskommission betreffend das Ressourcendefizit beim EDSB: «Der Bundesrat ist sich dieses Problems bewusst und bereit zu prüfen, wie die Mittel des Datenschutzbeauftragten – im Rahmen der geplanten Personalausgaben – verstärkt werden können» (Amtliches Bulletin 1999 I 594). Diese Feststellungen haben jedoch noch nicht zu einer Personalaufstockung geführt, die uns in die Lage versetzen würde, unseren gesetzlichen Auftrag zu erfüllen.

Gegenüber den Datenschutzbehörden anderer Länder ist das ständige Sekretariat des EDSB mit 16,2 Stellen für einen vergleichbaren Aufgabenbereich schlechter ausgestattet als die ausländischen Kollegen. Die Niederlande z.B. verfügen über 56 Mitarbeiter, Belgien, Griechenland und Dänemark über 22, 24 resp. 26 Personen. Die

schwedische Behörde beschäftigt ein 42-köpfiges Team. Die slowakische Republik zählt rund 80 Mitarbeiter. In Italien, Polen und in Tschechien ist die jeweilige nationale Datenschutzbehörde mit einem Team von 100 Personen ausgestattet. Der deutsche Datenschutzbeauftragte, der nur für den öffentlichen Bereich auf Bundesebene zuständig ist, verfügt über ein Sekretariat mit 63 Beschäftigten, zu denen noch das Personal der Datenschutzbehörden der Bundesländer mit jeweils 30 bis 40 Personen zu zählen ist. Die «Commission Nationale de l'Informatique et des Libertés» in Frankreich (CNIL; 17köpfige Datenschutzkommission) wird von einem Sekretariat mit 76 Mitarbeitern unterstützt. Gemäss einer Erhebung der Europäischen Beauftragten für den Datenschutz besitzen die Datenschutzbehörden aller 15 Mitgliedsstaaten der Europäischen Union insgesamt 586 Vollzeitstellen. Das entspricht einem Durchschnitt von 40 Stellen pro Staat.

Zum Abschluss des Besuchs hoben die Mitglieder der Subkommission die mangelhafte Personalausstattung des ständigen Sekretariats des EDSB hervor und betonten, dass der gesetzliche Auftrag unter diesen Voraussetzungen nicht erfüllt werden könne. Das Problem wurde der Finanzkommission des Nationalrates unterbreitet und am 26. November 2002 in der Wintersession des Nationalrates während der Beratungen zum Voranschlag des Bundes für 2003 erörtert. Dabei wurde beschlossen, den Beratungen zu diesem Geschäft nicht vorzugreifen, zumal eine Diskussion bei der Behandlung der Teilrevision des Bundesgesetzes über den Datenschutz im Laufe des Jahres 2003 ansteht; der Bundesrat könnte diese Gelegenheit ergreifen, um zusätzliche Mittel zu beantragen. Schliesslich aber hat der Bundesrat entschieden, die Frage der Ressourcen nicht im Rahmen der Gesetzesrevision, sondern innerhalb der Budgetdiskussionen 2004 zu behandeln.

12.2. Die neunte schweizerische Konferenz der Datenschutzbeauftragten

Die neunte Konferenz der schweizerischen Datenschutzbeauftragten fand am 22. November 2002 in Zug statt. Im Zentrum der Diskussionen standen der von der Bundesverwaltung geplante Eidgenössische Personenidentifikator (EPID), biometrische Verfahren zur automatisierten Gesichtserkennung sowie die Entwicklungen auf dem Gebiet der inneren Sicherheit.

Die Bundesverwaltung plant unter der Federführung des Bundesamtes für Statistik die Einführung eines Eidgenössischen Personenidentifikators, welcher die gesamte schweizerische Bevölkerung einheitlich durchnummerieren würde. Für die Einführung einer solchen Nummer spricht eine effiziente Verwaltungsführung. Die Diskussion zwischen den Vertretern des Bundesamtes für Statistik sowie des Bundesamtes

für Justiz und den Datenschutzbeauftragten zeigte jedoch, dass die Privatsphäre der Bürger massiv tangiert würde, weil dadurch Informationen aus den verschiedensten Verwaltungsbereichen miteinander verknüpft und ausgewertet werden könnten. Zudem steigt die Gefahr von Missbräuchen. Aus Gründen des Schutzes der Privatsphäre verbietet denn beispielsweise die portugiesische Verfassung eine solche einheitliche Durchnummerierung der Bevölkerung. Der Eidgenössische Datenschutzbeauftragte stellte klar, dass ein Eidgenössischer Personenidentifikator nicht ohne breite demokratische Diskussion eingeführt werden kann (vgl. dazu auch Abschnitt 1.2.1).

Der Vertreter einer Softwarefirma aus Deutschland erläuterte die Verfahren zur automatisierten Gesichtserkennung. Ähnliche Verfahren anderer Hersteller werden übrigens wohl nächstens im Flughafen Kloten zur Überprüfung von Einreisenden zum Einsatz kommen. Es zeigte sich, dass es möglich ist, solche Techniken datenschutzfreundlich auszugestalten, indem die Software erlaubt, aufgezeichnete Gesichter unkenntlich zu machen – eine Entschlüsselung könnte auf richterliche bzw. untersuchungsrichterliche Anordnung erfolgen.

Der Zuger Landammann und Sicherheitsdirektor verneinte in seinem Referat, dass der Gesetzgeber der Polizei zusätzliche Instrumente zur Überwachung geben müsse. Das Ausschöpfen der vorhandenen Instrumente genüge. Eine flächendeckende Informationsbeschaffung, wie sie nun die Regierung in den USA anstrebe, sei klar abzulehnen. «Ein liberaler Staat kann nur um den Preis seiner eigenen Seele seinen Bewohnerinnen und Bewohnern die totale Sicherheit versprechen.» Da wir in einer Risikogesellschaft leben, liessen sich Risiken heute nie ganz ausschliessen.

12.3 Publikationen des EDSB – Neuerscheinungen

- Newsletter des EDSB 2/2002
- Newsletter des EDSB 1/2003

Website des EDSB

Wir sind laufend daran, das Informationsangebot auf unserer Website zu erweitern. Die wichtigsten Neuerungen betreffen die Schaffung zweier neuer Rubriken: Unter «Fragen und Antworten» finden sich kurze Antworten zu häufig gestellten Fragen betreffend Datenschutz. Die Fragen und Antworten sind nach Kategorien geordnet und werden laufend ergänzt. Unter der Rubrik «Publikationen» werden neu Beiträge aufgeführt, die die Expertinnen und Experten des EDSB in der Fachpresse veröffentlicht haben («Publikationen - In der Fachpresse»). Demnächst werden wir unter «Gesetze

und Kommentare» eine Liste von Gesetzestexten, die in datenschutzrechtlicher Hinsicht von Interesse sind, erstellen. Daneben wird der Bereich «Themen», in dem Texte zu ausgewählten Themen an einer Stelle zusammengefasst sind, fortlaufend erweitert und ergänzt.

Neue Informationen in folgenden Bereichen:

- Genetische Vaterschaftstests

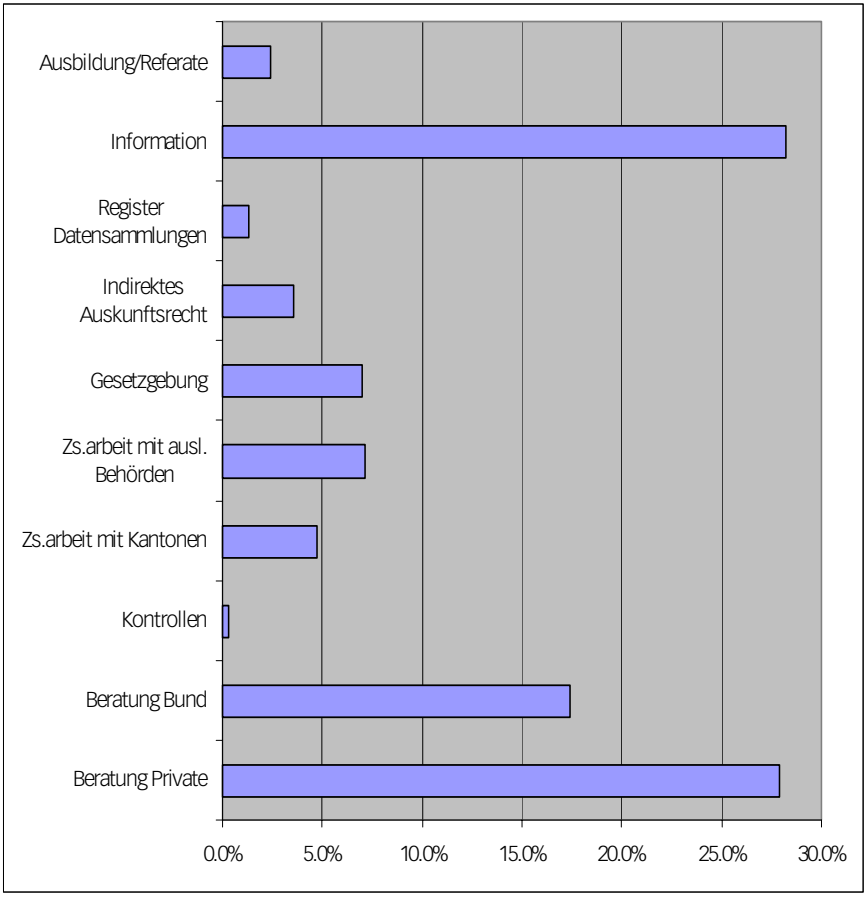
  (http://www.edsb.ch/d/themen/weitere/index.htm)
- Fragen und Antworten zum Bereich Telekommunikation

  (http://www.edsb.ch/d/fragen/index.htm)
- Fragen und Antworten zum Bereich Gesundheit

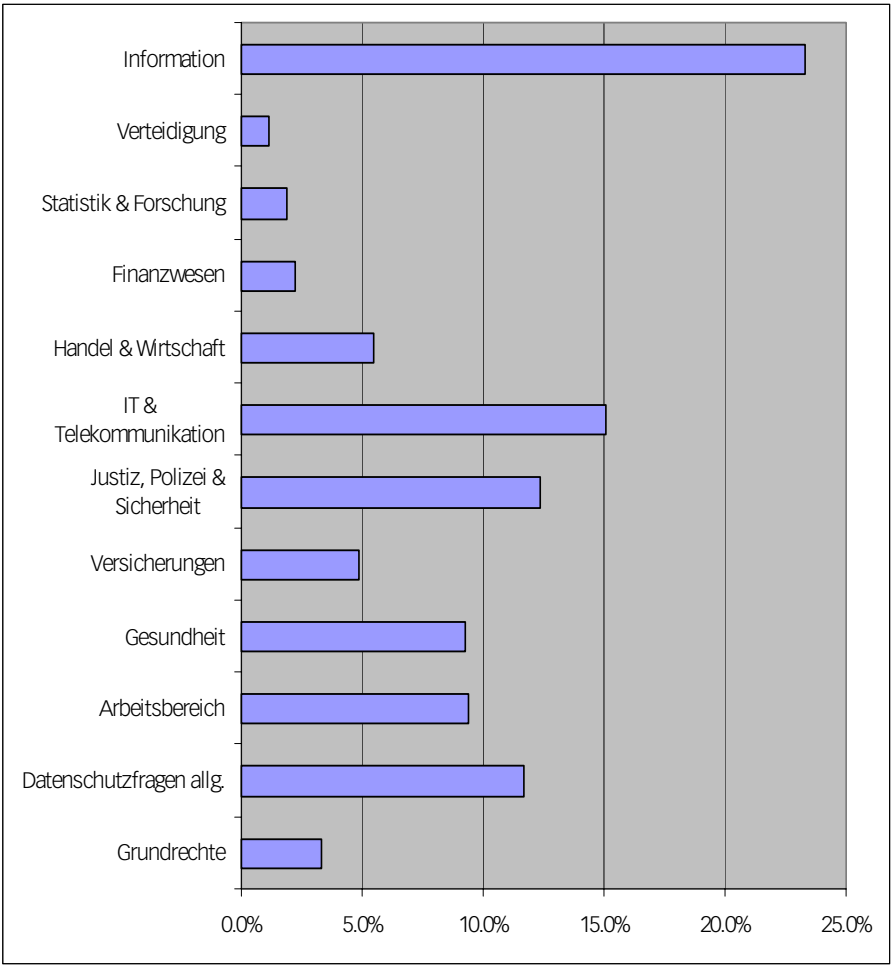
  (http://www.edsb.ch/d/fragen/index.htm)

12.4 Statistik über die Tätigkeit des Eidgenössischen Datenschutzbeauftragten vom 1. April 2002 bis 31. März 2003

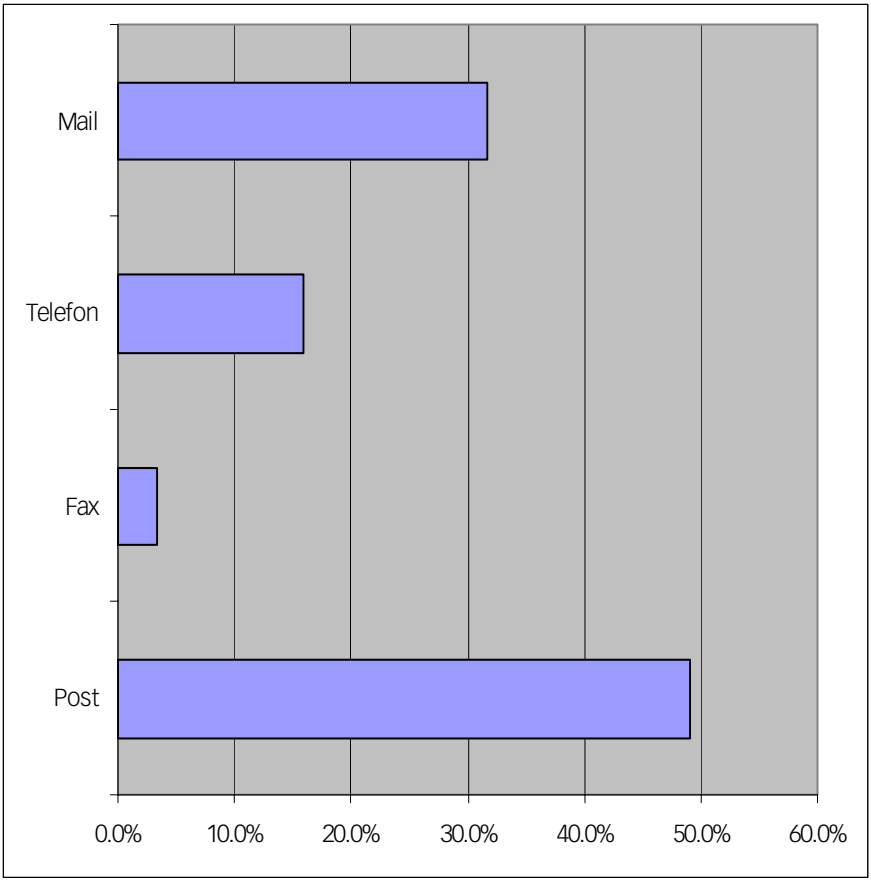
Aufwand nach Aufgabenbereich



Aufwand nach Sachgebiet



Herkunft der Anfragen



12.5 Das Sekretariat des EDSB

Eidgenössischer Datenschutzbeauftragter:	Thür Hanspeter, Fürsprecher
Stellvertreter:	Walter Jean-Philippe, Dr. iur.

Sekretariat:

Leiter:	Walter Jean-Philippe, Dr. iur.
Stellvertreter:	Buntschu Marc, lic. iur.
Informations- und Pressedienst:	Menna Daniel, lic. phil. Tsiraktsopoulos Kosmas, lic. iur.
Rechtsdienst:	7 Personen
Informatikdienst:	5 Personen
Kanzlei:	3 Personen

13. Anhang

13.1 Mindestdatenschutzklausel für allgemeine Geschäftsbedingungen der Fernmeldedienstanbieterinnen (FDA)

1.1 Im Rahmen der Bearbeitung von Personendaten, die für den Abschluss oder die Abwicklung eines Vertrags notwendig sind, kann FDA X mit Behörden sowie mit Unternehmen, die mit der Schuldeintreibung und der Kreditauskunft betraut sind, Daten austauschen um einerseits die Kreditwürdigkeit zu überprüfen sowie andererseits den Zahlungsverkehr abzuwickeln.

1.2 Erbringt FDA X zusammen mit einem Dritten eine Leistung, oder verlangt der Kunde über das Netz von FDA X Leistungen von einem Dritten, kann FDA X diesen Dritten Daten betreffend den Kunden bekannt geben, soweit diese Bekanntgabe für die Erbringung und Rechnungsstellung dieser Leistungen notwendig ist.

1.3 Unter Einhaltung der Datenschutzgesetzgebung, insbesondere unter Gewährleistung eines der schweizerischen Gesetzgebung gleichwertigen Datenschutzniveaus, kann FDA X im Rahmen der Abwicklung des internationalen Verkehrs (Roaming), der Lieferung von Informationen (Call Center) und der Rechnungsstellung Daten ins Ausland bekannt geben.

2.1 Der Kunde, der sich nicht ausdrücklich dagegen widersetzt, akzeptiert, dass FDA X

Version 1 folgende Personendaten … [z.B. Name, Vorname, Adresse…]

Version 2 Personendaten (die Liste der Daten kann an folgender Adresse bezogen werden …)

zur Entwicklung von personenbezogenen Leistungen und zur Ausarbeitung von massgeschneiderten Angeboten (kundenbezogene Werbung) bearbeitet.

2.2 Der Kunde, der sich nicht ausdrücklich dagegen widersetzt, akzeptiert ebenfalls, dass die oben erwähnten Daten für die gleichen Zwecke den Handelspartnern von FDA X

Version 1 d.h. …

Version 2 (die Liste der Partner kann an folgender Adresse bezogen werden …)

bekannt gegeben werden können.

Bemerkungen:

Betreffend das Widerspruchsrecht (vgl. Ziffer 2.1 und 2.2 oben), empfehlen wir den FDAs entweder im Vertrag selber oder auf einem separaten Formular eine spezielle Rubrik vorzusehen, wie beispielsweise:

o Ich widersetze mich dagegen, dass FDA X meine Personendaten zur Entwicklung von personenbezogenen Leistungen oder zur Ausarbeitung von massgeschneiderten Angeboten (kundenbezogene Werbung) bearbeitet.

o Ich widersetze mich dagegen, dass FDA X meine Personendaten für die gleichen Zwecke ihren Handelspartnern bekannt gibt.

13.2 Auswahl Fragen und Antworten im Telekommunikationsbereich

Muss ich mich im Verzeichnis eines Fernmeldedienstanbieters eintragen lassen?

Nein, seit 1998 können Sie selber entscheiden, ob Sie im Verzeichnis eingetragen werden sollen oder nicht. Sie können ausserdem bestimmen, welche Daten im Verzeichnis aufgeführt werden. Allerdings ist die Wahlmöglichkeit der im Verzeichnis aufgeführten Daten sehr begrenzt. Jeder Eintrag besteht mindestens aus folgenden Angaben:

- Name und Vorname oder Firmenname
- Vollständige Adresse
- Rubrik, unter der Teilnehmenden aufgeführt werden möchten
- Telefonnummer (E.164-Nummer)
- Kennzeichen, mit dem die Teilnehmenden bekannt geben können, dass sie keine Werbemittelungen erhalten möchten und dass ihre Daten zu Zwecken der Dirketwerbung nicht weitergegeben werden dürfen.

Kann ich auf eine detaillierte Rechnung verzichten ?

Handelt es sich um einem Anschluss, den mehrere Personen benutzen (z.B. eine Familie) möchten Sie womöglich auf eine detaillierte Rechnung verzichten um zu verhindern, dass der Rechnungsempfänger in Erfahrung bringen kann, welche Anschlüsse angerufen worden sind. Dies kann beispielsweise heikel sein, wenn sich um Ärzte, Beratungsstellen oder Anwälte handelt.

Sie haben das Recht, die Rechnung ohne Details zu erhalten. Wenden Sie sich in diesem Fall an Ihre Anbieterin. Sie wird Ihnen die Rechungen künftig ohne Randdaten ausstellen. Einige Anbieterinnen bieten Ihnen die Möglichkeit, die von Ihnen angerufenen Nummern um einige Stellen gekürzt zu erhalten. Dies erlaubt es Ihnen immer noch, die Rechnung zu kontrollieren, schützt aber die Privatsphäre der Benutzer des Anschlusses. Fragen Sie Ihre Anbieterin nach dieser Möglichkeit.

Ich habe das Gefühl, mein Telefon werde von Dritten abgehört; was kann ich tun ?

Falls Sie begründete Anhaltspunkte haben, Ihr Anschluss werde von unbefugten Dritten abgehört, können Sie gestützt auf 179bis StGB (Abhören und Aufnehmen fremder Gespräche) Strafanzeige erheben.

Ihre Fernmeldeanbieterin informiert Sie über Abhör- und Eingriffsrisiken, die die Benutzung ihrer Dienste mit sich bringt. Sie bietet oder nennt Ihnen geeignete Hilfsmittel zur Beseitigung dieser Risiken. [Art 64 FDV]

13.3 Entscheid des UVEK in Sachen Nachsendeauftrag der Schweizerischen Post

Das Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK)

hat

in der Datenschutzsache

zwischen

Eidg. Datenschutzbeauftragter, Feldeggweg 1, 3003 Bern

und

Die Schweizerische Post, Generalsekretariat, Viktoriastrasse 21, 3030 Bern

betreffend

Empfehlung des Eidg. Datenschutzbeauftragten vom 19. Februar 2001 in Sachen Nachsendeauftrag der Schweizerischen Post 2

festgestellt:

A. Die Schweizerische Post bietet ihren Kundinnen und Kunden den sogenannten 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.

B. Die Schweizerische Post bietet zusammen mit der Firma DCL Data Care AG einen Adressaktualisierungsdienst mit der Bezeichnung „MAT[CH]move" an. Die DCL Data Care AG ist eine Tochtergesellschaft der Schweizerischen Post. Mit Hilfe einer Umzugsdatenbank können Dritte ihre Adressbestände auf den neuesten 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. - Die Umzugsdatenbank wird mittels der Angaben des vorerwähnten Formulars 01 aktualisiert, welches die Umziehenden für die Postnachsendung ausgefüllt haben.

C. In den bis Ende 2000 verwendeten Formularen 01 wurden die Kundinnen und Kunden der Post nicht auf ihre Möglichkeit hingewiesen, die Adressaktualisierung für Dritte zu untersagen. Der Eidg. Datenschutzbeauftragte hat bei der Schweizerischen Post wiederholt in dieser Sache interveniert. Am 2. November 2000 hat er der Post nachstehende Änderungsvorschläge zu den Postformularentwürfen gemacht:

„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 „

Im Weiteren hat sich der Eidg. Datenschutzbeauftragte zu den Tarifen geäussert. Er verlangte, dass die Tarife die freie Wahl der Kundinnen und Kunden, die Adressaktualisierung für Dritte zu erlauben oder zu untersagen, nicht beeinflussen dürfen.

Am 27. Dezember 2000 hat die Post dem Eidg. Datenschutzbeauftragten die ab 1. Januar 2001 gültigen Formulare zur Kenntnisnahme zugestellt. Diese berücksichtigen indessen seine Forderungen nur teilweise. Am 10. Januar 2001 hat der Eidg. Datenschutzbeauftragte deshalb von der Post Erklärungen über noch hängige Punkte verlangt (Zugänglichmachung der Daten via das Internet-Portal „Yellowworld" der Post). Er kritisierte zudem erneut die Formulierungen des Formulars bzw. des Merkblattes als unpräzis und unterbreitete der Post Änderungsvorschläge.

Mit Schreiben vom 23. Januar 2001 antwortete die Post, es sei sichergestellt, dass künftig keine Daten aus den Formularen via Yellowworld-E-Mailverzeichnis abrufbar seien. Zu den Änderungsvorschlägen bemerkte sie, dass sie diese bei der nächsten Auflage von Formular und Merkblatt eingehend prüfen gegebenenfalls berücksichtigen werde.

D. Das seit dem 1. Januar 2001 von der Schweizerischen Post verwendete Formular 01 (212.09) erwähnt nun erstmals die Untersagungsmöglichkeit der Adressaktualisierung für Dritte, und zwar in folgender Formulierung:

„Darf dem Absender, der noch über Ihre alte Adresse verfügt, die neue Postadresse bekannt gegeben werden ? o Ja o Nein".

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, bzw. Fr. 240.— pro Jahr. Im Vergleich zum Tarif von Fr. 10.— entspricht dies für einen Nachsendeauftrag über 12 Monate einem um das Vierundzwanzigfache erhöhten Betrag bzw. einer Steigerung von 2'300 %.

E. Am 19. Februar 2001 hat der Eidg. Datenschutzbeauftragte der Schweizerischen Post eine „Empfehlung" gemäss Artikel 27 Absatz 4 des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (Datenschutzgesetz [DSG]; SR 235.1) eröffnet. Darin fordert er dazu auf, die missverständlichen Formulierungen im Formular 01 und dem dazugehörigen Merkblatt gemäss den von ihm unterbreiteten Vorschlägen anzupassen sowie die Tarife so zu ändern, dass für die untersagte Adressaktualisierung maximal der doppelte Preis gegenüber der erlaubten Adressaktuali-

sierung für dieselbe Zeitspanne zu bezahlen sei. Sodann hielt er die Post dazu an, jenen Kundinnen und Kunden, welche seit dem 1. Januar 2001 einen Nachsendeauftrag ohne Adressaktualisierung erteilt haben, den zuviel bezahlten Betrag zurückzuerstatten. Schliesslich setzte er der Schweizerischen Post eine Frist bis zum 23. März 2001 für die Mitteilung, ob sie diese Empfehlung annehme oder ablehne.

F. Mit Schreiben vom 22. März 2001 hat die Schweizerische Post dem Eidg. Datenschutz-beauftragten mitgeteilt, dass sie seine Empfehlungen ablehnt.

G. Mit Eingabe vom 27. April 2001 hat der Eidg. Datenschutzbeauftragte die Angelegenheit gemäss Artikel 27 Absatz 5 DSG dem Eidgenössischen Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) zum Entscheid vorgelegt.

Die Rechtsbegehren des Eidg. Datenschutzbeauftragten in seiner Eingabe an das UVEK entsprechen dem Inhalt seiner Empfehlungen vom 19. Februar 2001 an die Schweizerische Post. Auch die zugehörige Begründung stimmt mit den Erwägungen des Eidg. Da-tenschutzbeauftragten in seinen Empfehlungen an die Schweizerische Post überein.

H. Das mit der Instruktion des Verfahrens vom dem UVEK befasste Generalsekretariat hat die Schweizerische Post vor dem Entscheid angehört.

Auf die für den Entscheid relevanten Ausführungen der Post wird in den nachstehenden Erwägungen eingegangen.

Das Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation hat

in Erwägung gezogen

I.

1. Bei der von der Schweizerischen Post abgelehnten Empfehlung des Eidg. Datenschutzbeauftragten handelt es sich nicht um eine Verfügung nach Artikel 5 des Bundesgesetzes über das Verwaltungsverfahren vom 20. Dezember 1968 (Verwaltungsverfahrensgesetz [VwVG]; SR 172.021). Die Empfehlung zählt zu den nicht auf Rechtswirkungen gerichteten Verwaltungstätigkeiten, welche als sogenanntes schlichtes oder tatsächliches Verwaltungshandeln bezeichnet werden (Häfelin/Müller, Grundriss des Allgemeinen Verwaltungsrechts, 2. Auflage, Zürich 1993, Rz 602i). Demzufolge gelangen die Vorschriften desVwVG erst mit der vorliegenden Entscheidung zur Anwendung (BGE 117 Ib 481 E. 4b/aa; 113 Ib 90 E.2d/aa).

2. Die Schweizerische Post ist heute eine selbständige Anstalt des öffentlichen Rechts mit eigener Rechtspersönlichkeit; sie befindet sich zu 100% im Besitze des Bundes.

Mit dem Inkrafttreten des Postgesetzes vom 30. April 1997 (PG; SR 783.0) am 1. Januar 1998 (BRB vom 30. April 1997; AS 1997 2457) richten sich die Rechtsbeziehungen der Post zu ihrer Kundschaft neu nach dem Privatrecht. Somit gelten gemäss Artikel 13 PG für das Bearbeiten von Personendaten durch die Post die Artikel 12 – 15 DSG. Ungeachtet ihrer rechtlichen Selbständigkeit bleibt die Post ein Bundesorgan im Sinne von Artikel 3 Buchstabe h DSG. Deshalb richtet sich die Aufsicht nach den Bestimmungen für Bundesorgane (Art. 23 Absatz 2 DSG). Gemäss Artikel 27 Absatz 4 DSG klärt demzufolge der Eidg. Datenschutzbeauftragte ab, ob Datenschutzvorschriften verletzt werden. Kommt er zum Schluss, dass dies der Fall sei, empfiehlt er dem verantwortlichen Bundesorgan, das Bearbeiten der Daten zu ändern oder zu unterlassen. Er orientiert das zuständige Departement über seine Empfehlung.

Die Empfehlung des Eidg. Datenschutzbeauftragten vom 19. Februar 2001 an die Post ist auch dem UVEK zugegangen.

3. Aufgrund von Artikel 5 Absatz 2 Buchstabe b der Organisationsverordnung für das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation vom 6. Dezember 1999 (OV-UVEK; SR 172.217.1) ist das Generalsekretariat des UVEK verantwortlich für die hoheitlichen Aufgaben gemäss Postgesetz vom 30. April 1997 und Postorganisationsgesetz vom 30. April 1997. Zudem besorgt gemäss Artikel 5 Absatz 1 Buchstabe e OV-UVEK das Generalsekretariat des UVEK die Rechtsanwendung, Rechtsprechung und Rechtsberatung auf Departementsstufe und begleitet die Rechtsetzungsarbeiten, die im Departement vorgenommen werden.

Daraus folgt, dass das UVEK zur Behandlung und Entscheidung in der Angelegenheit zuständig ist.

1. Nach Artikel 49 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997 (RVOG; SR 172.010) kann der Departementsvorsteher seine Unterschriftsberechti-gung in zum Voraus bestimmten Fällen auf den Generalsekretär oder dessen Stellvertreter übertragen. Die hierzu ermächtigten Beamten unterschreiben im Namen des Depar-tementsvorsteher. Mit Verfügung vom 1. November 1995 hat Herr Bundesrat Moritz Leuenberger entsprechende Anordnungen getroffen.

II.

1. Gemäss Artikel 3 Buchstabe e DSG bedeutet Bearbeiten (von Personendaten): „jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten „. Dadurch dass die Post

von ihr im Rahmen von Nachsendeaufträgen erfasste Adressänderungen von Kundinnen und Kunden ihrer Tochtergesellschaft DCL Data Care AG weitergibt, damit diese ihren Interessenten einen Adressdatenabgleich anbieten kann, werden Personendaten im Sinne der erwähnten Bestimmung bearbeitet.

Im weiteren legen Buchstabe h und Buchstabe i der vorerwähnten Gesetzesbestimmung fest, dass als Bundesorgane gelten: „Behörden und Dienststellen des Bundes sowie Personen, soweit sie mit öffentlichen Aufgaben des Bundes betraut sind „ bzw. dass als *Inhaber der Datensammlung* gelten: „private Personen oder Bundesorgane, die über den Zweck und den Inhalt einer Datensammlung entscheiden „. Wie in Ziffer I./2. der Erwägungen erwähnt wird, ist die Schweizerische Post aufgrund ihrer im Rahmen des „service public" zu erfüllenden Aufgaben ein Bundesorgan.

Aufgrund der vorstehenden Ausführungen ergibt sich zweifelsfrei, dass vorliegend die Bestimmungen des Datenschutzgesetzes zur Anwendung gelangen. Dies wird denn auch seitens der Schweizerischen Post nicht bestritten.

2. Nach Artikel 12 Absatz 1 DSG darf durch die Bearbeitung von Personendaten die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzt werden. Sodann verlangt Absatz 2 Buchstabe b der erwähnten Gesetzesbestimmung, dass insbesondere nicht ohne Rechtfertigungsgrund Daten einer Person gegen deren ausdrücklichen Willen bearbeitet werden.

Gemäss Art. 12 Abs. 3 DSG liegt „in der Regel" keine Persönlichkeitsverletzung vor - und ist deshalb auch kein besonderer Rechtfertigungsgrund für die Datenbearbeitung nötig -, „wenn die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat."

Aus den Materialien zu Art. 12 Abs. 3 DSG geht hervor, dass der Gesetzgeber davon ausging, Adressen seien in der Regel „allgemein zugänglich" (Amtl. Bull. Ständerat, 1990, S. 142/143).

Gemäss Art. 12 Abs. 3 DSG kann die betroffene Person diese Vermutung jedoch umstossen, indem sie die Bearbeitung der sie betreffenden Daten ausdrücklich untersagt.

Für den hier interessierenden Fall der Adressaktualisierung hat der Bundesrat das im DSG angelegte „informationelle Selbstbestimmungsrecht" der Postkundschaft in Art. 12 der Postverordnung vom 29. Oktober 1997 (VPG; SR 783.01) durch folgende Bestimmung konkretisiert: „Die Post kann die Postadressen von Kundinnen und Kunden Dritten für das Nachführen ihrer eigenen Adressdatensammlungen zur Verfügung stellen, sofern die betroffene Person eine Bearbeitung nicht ausdrücklich untersagt hat."

3. Damit die Kundinnen und Kunden der Post ihr Selbstbestimmungsrecht über die sie betreffenden Daten effektiv ausüben können, müssen sie von der Post in klarer und fairer Weise über die vorgesehene Datenbearbeitung informiert werden.

Diesbezüglich gehen die Auffassungen des Eidg. Datenschutzbeauftragten und der Schweizerischen Post auseinander.

a) Die Schweizerische Post ist der Auffassung, wonach die von ihr gewählte Formulierung auf dem Formular 01 (212.09) *„Darf dem Absender, der noch über Ihre alte Adresse verfügt, die neue Postadresse bekanntgegeben werden ? o Ja o Nein"* den Anforderungen des informationellen Selbstbestimmungsrechtes durchaus genüge. Sie begründet dies damit, dass es kaum eine Rolle spiele, ob eine Firma, die ihre Adressen aktualisieren lässt, im Moment der Aktualisierung einen Versand tätigt oder dies womöglich erst eine Woche, einen Monat oder ein Jahr später tun will. Massgeblich sei in diesem Fall doch vielmehr, ob der von der Firma beabsichtigte Verwendungszweck erlaubt ist oder nicht. Diese Frage stelle sich aber bereits bei der Erfassung der Adresse(Tätigkeit der Firma), und nicht erst bei der späteren Aktualisierung der Adresse (Tätigkeit der Post). Es sei klar, dass ein Unternehmen wissen will, wo seine Kunden derzeit wohnen. Dabei verstehe sich von selbst, dass dieses Anliegen eines jeden Unternehmens dem Bedürfnis nach Verschicken von Postsendungen jederzeit vorgeht. Es dürfe davon ausgegangen werden, dass diese Sachlage jedem Kunden bzw. Konsumenten bewusst ist. Nichts ändern daran dürfte der Umstand, dass nun im Formular - bei sonst identischem Text - der Begriff „Absender" anstelle „Dritter" verwendet wird (vgl. Stellungnahme der Schweizerischen Post vom 22. März 2001, S. 2 f.).

b) Demgegenüber vertritt der Eidg. Datenschutzbeauftragte die Auffassung, dass aufgrund des Begriffes „Absender" der Postkunde annehme, dass bereits eine Sendung aufgegeben sei oder dies mindestens beabsichtigt werde. Weil die Adressaktualisierung allen Interessierten angeboten werde, unabhängig davon, ob sie eine Postsen-dung aufgegeben haben oder eine Aktualisierung aus völlig anderen Gründen wünschten, sei die Formulierung daher intransparent und irreführend. Er fordert somit die entsprechende textliche Anpassung (vgl. Eingabe des Eidg. Datenschutzbeauftragten an das UVEK vom 27. April 2001, Ziffer I./1., S. 1 und Ziffer IV./4.1., S. 3 f.).

c) Nach Auffassung des UVEK sind tatsächlich Zweifel angebracht, ob durch die Verwendung des Begriffs „Absender" die betroffenen Kundinnen und Kunden der Post hinlänglich klar und fair informiert werden. Sodann ist die Auffassung der Post in Frage zu stellen, ob aufgrund der Adressenbestände, welche sich bei den Interessenten für eine Adressaktualisierung befinden, tatsächlich und stillschwei-

gend davon auszugehen sei, dass es sich um bestehende Kundenbeziehungen handle. In diesem Zusammenhang kann offengelassen werden, ob ein Interessent für eine Adressaktualisierung die bei ihm befindlichen Adressen ohne Verletzung datenschutzrechtlicher Bestimmungen erhalten hat. Entscheidend ist allein die Wahrung des informationellen Selbstbestimmungsrechts des Postkunden, welcher das Formular für den Nachsendeauftrag ausfüllt. Es stellt sich mithin die Frage, weshalb es der Post nicht möglich ist, auf dem Formular 01 eine mit der Gesetzesbestimmung von Artikel 12 VPG kongruente Wortwahl zu treffen. Ihre diesbezüglichen Darlegungen vermögen nicht zu überzeugen. **Das UVEK erkennt deshalb, dass die Schweizerische Post die Formulierung auf dem Formular 01 im Sinne dieser Erwägungen und in Folgegebung der Forderung des Eidg. Datenschutzbeauftragten anzupassen hat.**

4. Gemäss Artikel 13 Absatz 2 der Bundesverfassung vom 18. April 1999 (BV; SR 101) hat jede Person Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

Daraus fliesst das Recht ein jeder Person, die Herrschaft über die sie betreffenden Infor-mationen ausüben und eine Bearbeitung dieser Daten durch Dritte einschränken zu können (sogenanntes informationelles Selbstbestimmungsrecht; vgl. Buntschu, in: Maurer/Vogt (Hrsg.), Kommentar zum Schweizerischen Datenschutzgesetz, Artikel 1, N 14 ff.).

Auch in dieser Hinsicht weichen die Auffassungen des Eidg. Datenschutzbeauftragten und der Schweizerischen Post bezüglich des Merkblattes zum Formular 01 (212.09) voneinander ab.

a) Die Schweizerische Post stellt sich auf den Standpunkt, dass jene Firmen, die nicht unmittelbar mit den Adressen Sendungen verschicken, die aktualisierten Adressen auch gegen den Willen der betroffenen Personen rechtmässig bearbeiten dürfen, sofern es sich - wie in Ziffer I/2 der Empfehlung erwähnt - um Unternehmen handle, welche Daten von aktiven Kunden bearbeiten. Die Post wiederum dürfe diesen die Daten gemäss der Sonderregel von Artikel 12 VPG ohne weiteres mitteilen. Schliesslich sei an dieser Stelle die Frage zu stellen, weshalb jemand überhaupt für die Aktualisierung von Adressen Geld bezahlen sollte, wenn er diesen Kunden keine Post zustellen will (Stellungnahme der Schweizerischen Post vom 22. März 2001, Ziffer 3, S. 3). Im Merkblatt 212.09.1 zum Formular 01 erwähnt sie darum unter „X Ja": *„Ihre Adresse wird in keinem Fall an Dritte verkauft oder vermietet, sondern lediglich zur Aktualisierung bestehender Adressdatenbanken verwendet."* Unter „X Nein" steht indessen: *„Ihre Adresse wird nicht an Dritte weitergegeben."* Die unterschiedliche Formulierung begründet die Post damit, dass es ihr gutes und legitimes Recht sei, dass ihre Kundschaft im Formular ein „Ja" ankreuzt.

b) Der Eidg. Datenschutzbeauftragte sieht in der unterschiedlichen Formulierung eine mögliche Irreführung der betreffenden Kundinnen und Kunden, welche das Formular 01 benützen. Die von der Post gewählte Darstellung erwecke den Anschein, die Auswahl zwischen „JA" und „NEIN" habe einen Einfluss auf eine allfällige Bekanntgabe an Dritte, die nicht über die alte Adresse verfügen. Demgegenüber habe die Schweizerische Post versichert, dass weder bei „X Ja" noch bei „X Nein" eine Weitergabe an Dritte stattfinde (vgl. Schreiben der Schweizerischen Post vom 27.12.99 an den Eidg. Datenschutzbeauftragten, Ziffer I, *„…weder die Post noch deren Tochtergesellschaft DCL Adressdaten an Dritte verkauft."*).

c) Nach Massgabe des verfassungsmässig garantierten Rechts auf informationelle Selbstbestimmung ist das UVEK der Auffassung, dass in der Tat die von der Post gewählten unterschiedlichen Formulierungen im Merkblatt 212.09.1 dem Gebot einer klaren und fairen Information nicht entsprechen. Für die Post ist vorab ihre Beziehung zu jenem Kunden massgeblich, welcher den Nachsendeauftrag veranlasst. Dessen Recht, selber zu bestimmen, ob seine (neue) Adresse dem vermeintlichen Absender bekanntgegeben werden soll, ist aus datenschutzrechtlicher Sicht ungeschmälert zu belassen. Daran vermögen die recht ausführlichen Darlegungen der Post bezüglich ihrer Kostenstruktur nichts zu ändern. Zu Recht hat der Eidg. Datenschutzbeauftragte auf das Beispiel der Deutschen Post AG hingewiesen, welche die Nachsendedienstleistung, mit oder ohne Untersagung einer Adressaktualisierung, unterschiedslos anbietet. Es ist zwar durchaus verständlich, dass die Post die Bejahung der Aktualisierung seitens der Nachsende-Auftraggeber bevorzugt, weil sie dadurch ihre Adressaktualisierungs-Dienstleistung als attraktiven Service auch in Zukunft anbieten kann. Dass dieser Service für die Post ein geldwertes Interesse darstellt, wird von ihr auch nicht verneint. Nur kann dieses (privatwirtschaftliche) Interesse nicht höhergewichtig sein gegenüber dem informationellen Selbstbestimmungsrecht. Der Auffassung des Eidg. Datenschutzbeauftragten ist deshalb zuzustimmen, wonach im ersten Abschnitt des Merkblattes unter Hinweis auf Artikel 12 VPG zu erwähnen sein wird, dass eine Adressaktualisierung durch Dritte nur dann möglich sei, wenn diese bereits über die (alte) Adresse verfügten. Sodann ist unmissverständlich auszuführen, dass „X Ja" als *Einverständnis* zur Adressaktualisierung gelte, wohingegen „X Nein" die *Untersagung* der Adressaktualisierung bedeute. Alle übrigen Aussagen über Weitergabe, Verkauf oder Vermietung unter den Titeln „X Ja" und „X Nein" sind wegzulassen. **Das UVEK erkennt deshalb, dass die Schweizerische Post die Formulierungen im Merkblatt zum Formular 01 im Sinne dieser Erwägungen und in Folgegebung der Forderung des Eidg. Datenschutzbeauftragten anzupassen hat.**

5. Gemäss Artikel 14 Absatz 1 PG legt die Post die Preise für ihre Dienstleistungen nach wirtschaftlichen Grundsätzen fest. Aufgrund dieser Bestimmung muss die Post für ihre Dienstleistungen einen mindestens kostendeckenden Preis verlangen. Dieser Grundsatz gilt sowohl für den Universaldienst (reservierte und nicht reservierte Dienste) wie auch für den Wettbewerbsbereich.

Der genannte Grundsatz unterliegt indessen den allgemeinen Schranken des Datenschutzgesetzes. Für die Frage der Preisfestsetzung ist dabei die Zuweisung der Dienstleistung „Nachsendeauftrag" zum Universaldienst oder zum Wettbewerbsbereich unerheblich. Somit erweist sich der Einwand der Post, wonach der Nachsendeauftrag zum Wettbewerbsbereich gehöre, als unbehelflich für die Frage, ob der für die betreffe Dienstleistung erhobene Preis zulässig ist. Das UVEK ist allerdings der Auffassung, dass der Gesetzgeber mit seinem Auftrag an die Post vorab einen ausreichenden Universaldienst sicherstellen wollte. Er hat deshalb einen Katalog von Grundleistungen definiert, es aber der Post überlassen, das Angebot im einzelnen festzulegen. Hierbei hat die Post Rücksicht auf die Bedürfnisse von Bevölkerung und Wirtschaft sowie auf die technische Entwicklung zu nehmen. Anderseits ist auch dem Umstand Rechnung zu tragen, dass die Bestrebungen, den europäischen Postmarkt weiter zu liberalisieren, ihren Fortgang nehmen. Aus regulatorischer Sicht besteht daher das Bedürfnis, dass seit langem eingeführte Dienste auch weiterhin dem Konsumenten angeboten werden. Dies kann grundsätzlich mit der Zuweisung einer Dienstleistung zum Universaldienst sichergestellt werden, sofern die Dienstleistung nach Marktbedingungen nicht erbracht würde. Der Nachsendeauftrag gehört zu den seit langem eingeführten Diensten, welche seit jeher im Leistungsangebot der Schweizerischen Post enthalten waren (vgl. Artikel 9 i.V. mit Artikel 4 Postverkehrsgesetz vom 2. Oktober 1924 [PVG], aufgehoben durch das Postgesetz vom 20. April 1997; J. Buser, Das Schweizerische Postverkehrsgesetz, 2. Auflage, Zürich 1930, S. 146 f.). Das UVEK wird daher die Frage, ob der Nachsendeauftrag explizit dem Universaldienst zuzuweisen ist, noch vertieft prüfen.

Vorliegend kann diese Frage allerdings offengelassen werden, weil die Preisfestsetzung der Post für den Nachsendeauftrag aus anderen Gründen nicht haltbar ist.

a) Unter Berufung auf ihre Kostenstruktur bei der Dienstleistung Nachsendeauftrag macht die Post geltend, dass ihr für eine Nachsendung ohne Adressberichtigung während 3 Monaten durchschnittliche Kosten von Fr. 72.— entstünden. In Berücksichtigung des von ihr verlangten Preises von Fr. 20.— pro Monat resultiert somit ein Verlust von Fr. 12.— . Es ist deshalb nach ihrer Meinung gerechtfertigt, für eine Nachsendung mit Adressberichtigung während eines Jahres lediglich Fr. 10.— zu verlangen.

b) Demgegenüber hält der Eidg. Datenschutzbeauftragte dafür, dass durch diese stark unterschiedliche Preisfestsetzung das informationelle Selbstbestimmungsrecht der betroffenen Personen verletzt werde, weil dadurch die freie Entscheidung der Postkundinnen und –kunden beeinflusst werde. Wer eine Adressaktualisierung für Dritte untersage, werde die meisten regelmässigen Absender direkt über seine neue Adresse informieren. Weil jedoch in diesen Fällen die Anzahl der fehlgeleiteten Sendungen höher sei und damit auch höhere Kosten für die Post verursacht würden, sei ein moderater Preisunterschied, d.h. maximal der doppelte Ansatz, zu akzeptieren.

c) Hinsichtlich der Preisfestsetzung für den Nachsendeauftrag ist das UVEK der Auffassung, dass die Post diesbezüglich nicht absolut frei ist und in jedem Fall Schranken zu beachten hat. Die Post hat bei ihrer Preisfestsetzung in jedem Fall das informationelle Selbstbestimmungsrecht angemessen zu berücksichtigen. Dies bedeutet, dass im Maximum eine Preisfestsetzung möglich ist, welche im Verhältnis zwischen erlaubter und untersagter Adressaktualisierung das Doppelte nicht überschreitet. Aufgrund dieser Darlegung gelangt das UVEK deshalb zur Auffassung, dass die Post mit ihrer prozentual massiv erhöhten Preisfestsetzung für den Nachsendeauftrag mit untersagter Adressaktualisierung in der Tat das informationelle Selbstbestimmungsrecht der betroffenen Personen verletzt. Klarerweise wird damit die freie Entscheidung nachhaltig beeinflusst. **Das UVEK erkennt deshalb im Sinne dieser Erwägungen und in Folgegebung der Forderung des Eidg. Datenschutzbeauftragten, dass die Schweizerische Post für den Nachsendeauftrag mit untersagter Adressaktualisierung im Maximum den doppelten Preis festsetzen darf, wie er für den Nachsendeauftrag mit erlaubter Adressaktualisierung gilt.**

6. Der Eidgenössische Datenschutzbeauftragte hatte der Post empfohlen, die „zuviel verlangten" Gebühren für Nachsendeaufträge zurück zu erstatten.

Nachdem die Post es abgelehnt hat, diese Empfehlung zu befolgen, formulierte er in seiner Eingabe vom 27. April 2001 an das UVEK folgendes Begehren: „Das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation entscheidet über eine Rückerstattung der seit dem 1. Januar 2001 zuviel bezahlten Gebühren."

Zur Begründung führte er aus (S. 5 unten): „Wie die Post schreibt, hat der EDSB kein Recht, eine verbindliche Anweisung über eine Gebührenrückerstattung zu erlassen. Allerdings ist im Entscheid des UVEK eine Rückerstattung der seit dem 1. Januar 2001 zu viel bezahlten Gebühren zu beschliessen. Denn gemäss dem Prinzip von Treu und Glauben, müssen die unrechtmässig erhobenen Gebühren an die Kunden zurückgeben [recte: zurückgegeben; Anm. UVEK] werden."

Der Nachsendeauftrag ist ein Vertrag, der wechselseitige Leistungen und Gegenleistungen stipuliert. Wie in Ziff. 5 Bst. c hiervor begründet, basierten jene Nachsendeaufträge, welche die Post mit dem Formular 01 (212.09) entgegen nahm, auf einer Tarifstruktur, die das UVEK unter dem Gesichtspunkt des Datenschutzes als nicht rechtmässig beurteilt. Das UVEK weist deshalb die Post im Dispositiv seines Entscheides an, die bisherige Tarifstruktur im Sinne der Empfehlungen des Eidg. Datenschutzbeauftragten zu ändern.

Das Begehren des Eidg. Datenschutzbeauftragten betreffend die Rückzahlung unterstellt, dass das UVEK den neuen, datenschutzkonformen Tarif selber festlegt. Dazu ist Folgendes festzuhalten:

- Es ist Sache der Post, die Preise für ihre Dienstleistungen in dem durch das Postgesetz (Art. 14 f.) und das DSG bestimmten Rahmens festzulegen.
- Stellt das UVEK im Rahmen seiner Aufsicht fest, dass sich ein von der Post festgelegter Tarif nicht an diesen Rahmen halten, verfügt es über Folgende aufsichtsrechtlichen Mittel:
  - bei (neuen) genehmigungspflichtigen Preisen: die Nichtgenehmigung –
  - bei anderen Preisen: die Anweisung an die Post, den Tarif so zu ändern, dass er den rechtlichen Vorgaben entspricht.

Dass das UVEK in seiner Eigenschaft als Aufsichtsbehörde über das datenschutzechtlich relevante Verhalten der Post den Preis für einen bestimmten postalischen Tarif gleich selber festlegen würde, käme einzig dann in Frage, wenn sich die Post weigern würde, einer aufsichtsrechtlichen Weisung (zeitgerecht) Folge zu leisten, so dass die Vorausset-zungen für eine „Ersatzvornahme" gegeben wären. Diese Voraussetzung ist im hier interessierenden Fall nicht erfüllt.

Weil sich die aufsichtsrechtliche Kompetenz des UVEK im hier zu beurteilenden Fall dar-auf beschränkt, von der Post eine Änderung des bisherigen Tarifs zu verlangen, kann das UVEK auch nicht beurteilen, ob jenen Postkundinnen und -kunden, die der Post auf Grund des bisherigen Tarifs Nachsendeaufträge erteilten, im Lichte des neuen Tarifs ein (zivil-)rechtlicher Anspruch auf Rückerstattung erwächst. Zuständig für diese Beurteilung ist zudem nicht die Aufsichtsbehörde: Würde eine Postkundin oder ein Postkunde einen solchen Anspruch gegenüber der Post behaupten und die Post ihn bestreiten, läge eine jener „Streitigkeiten zwischen der Post und der Kundschaft" vor, die gemäss Art. 17 des Postgesetzes von den Zivilgerichten zu beurteilen sind.

Aus diesen Gründen gibt das UVEK dem Begehren des Eidg. Datenschutzbeauftragten, wonach in diesem Verfahren über eine Rückerstattung der seit dem 1. Januar 2001 zuviel bezahlten Gebühren zu entscheiden sei, keine Folge.

7. Gemäss Art. 27 Abs. 5 (Satz 2) DSG wird der Entscheid des Departementes über eine nicht befolgte oder abgelehnte Empfehlung des Eidgenössischen Datenschutzbeauftrag-ten „den betroffenen Personen" mitgeteilt.

Vom vorliegenden Entscheid sind betroffen:

- der Eidg. Datenschutzbeauftragte
- die Post als Adressatin der hier zu beurteilenden Empfehlung des Eidg. Datenschutzbeauftragten
- jene Postkundinnen und -kunden, die der Post Nachsendeaufträge unter Verwendung des seit dem 1. Januar 2001 gültigen Formulars 01 (212.09) erteilt und dafür jenen Preis bezahlt haben, welchen die Post auf Grund jenes Tarifs bestimmte, auf den sich die Empfehlung des Eidg. Datenschutzbeauftragten vom 19. Februar 2001 bezieht.

Der Post und dem Eidg. Datenschutzbeauftragten kann der Entscheid direkt eröffnet werden.

106 Laut Art. 36 Bst. d VwVG kann die Behörde ihre Verfügung „in einer Sache, in der sich die betroffenen Parteien ohne unverhältnismässigen Aufwand nicht vollständig bestimmen lassen, durch Veröffentlichung in einem amtlichen Blatt eröffnen." Mit Bezug auf die vom Entscheid betroffenen Kundinnen und Kunden der Post ist diese Voraussetzung im vorliegenden Fall erfüllt: Das UVEK könnte diesen Personenkreis nur mit hohem Aufwand - und selbst dann kaum vollständig - ermitteln. Das Dispositiv des Entscheids ist deshalb im Bundesblatt zu publizieren, verbunden mit dem Hinweis, dass der vollständige Entscheid während der Rechtsmittelfrist beim Generalsekretariat (Rechtsdienst) des UVEK eingese-hen bzw. bezogen werden kann.

8. Gemäss Art. 33 Abs. 1 Bst. b DSG ist gegen Entscheide des zuständigen Departementes über Verfügungen von Bundesorganen in Datenschutzfragen (ausgenommen solche des Bundesrates) die Beschwerde an die Eidg. Datenschutzkommission zulässig. Der Entscheid des Departementes über eine nicht befolgte oder abgelehnte Empfehlung des Eidgenössischen Datenschutzbeauftragten ist eine solche Verfügung (VPB 64.73, Erwägung 1.b). Gegen den vorliegenden Entscheid steht folglich die Beschwerde an die Eidgenössische Datenschutzkommission offen.

Demgemäss wird vom UVEK

erkannt:

1. Die Schweizerische Post hat die Formulierung auf dem Formular 01 im Sinne der Erwägungen und in Folgegebung der Forderung des Eidg. Datenschutzbeauftragten anzupassen.
2. Die Schweizerische Post hat die Formulierungen im Merkblatt zum Formular 01 im Sinne der Erwägungen und in Folgegebung der Forderung des Eidg. Datenschutzbeauftragten anzupassen.
3. Die Schweizerische Post darf für den Nachsendeauftrag mit untersagter Adressaktualisierung im Maximum den doppelten Preis für einen Nachsendeauftrag mit erlaubter Adressaktualisierung verlangen.
4. Auf das Begehren des Eidg. Datenschutzbeauftragten betreffend die Rückerstattung wird nicht eingetreten.
5. Gegen diesen Entscheid kann innerhalb von 30 Tagen seit Eröffnung Beschwerde bei der Eidgenössischen Datenschutzkommission in Bern erhoben werden. Die Beschwerde ist mindestens im Doppel einzureichen. Sie hat die Begehren, deren Begründung mit Angabe der Beweismittel und die Unterschrift der Beschwerdeführenden zu enthalten. Die angefochtene Verfügung und die als Beweismittel angerufenen Unterlagen sind beizulegen, soweit die Beschwerdeführenden sie in Händen haben. Ferner sollte die Vollmacht einer allfälligen Vertreterin oder eines allfälligen Vertreters beigelegt werden.
6. Das Dispositiv des Entscheids wird im Bundesblatt publiziert.

Eidgenössisches Departement für
Umwelt, Verkehr, Energie, Kommunikation
Der stellv. Generalsekretär
André Schrade

Mitteilung an:
Eingeschrieben:

- Eidg. Datenschutzbeauftragter, Feldeggweg 1, 3003 Bern
- Die Schweizerische Post, Generalsekretariat, Viktoriastrasse 21, 3030 Bern

13.4 Standardklausel Datenschutz in Rückübernahme- und Transitabkommen

Siehe Abschnitt 13.4 im französischen Teil des Berichtes.

13.5 Bericht der Arbeitsgruppe AGX zum System RAI/RUG an das Büro DSB+CPD.CH

I. Allgemeines

1. Unsere Arbeitsgruppe setzt sich aus folgenden Mitgliedern zusammen: BL, FR, ZH, BE und EDSB. Den Vorsitz hat FR.

2. Unsere Arbeitsgruppe hatte den Auftrag, die Frage zu untersuchen und gegebenenfalls zu beantworten, ob das System RAI/RUG unter dem Aspekt des Datenschutzes zulässig ist.

3. Zum Vorgehen unserer Gruppe:

   Es wurden 5 Sitzungen abgehalten. An einer dieser Sitzungen wurde das Heim St. Johann in Basel besichtigt, an einer anderen fand ein Treffen mit vier Vertretern von VASOS und des Neuen Panther Clubs statt (Frau Ruth Banderet, Frau Alice Liber, Herr Ernst Widmer und Herr Hansruedi Sigg), und an einer dritten gab es Informationen von Dr. Markus Anliker, Q-Sys. Die Gruppe AGX traf sich auch mit unserem Kollegen Jean-Louis Wanner, Datenschutzbeauftragter BS, der in seinem Kanton eine offizielle Stellungnahme zu diesem System verfasst hat.

   Die Gruppe erhielt ausserdem Unterlagen zu anderen von Alters- und Pflegeheimen in der Schweiz genutzten Systemen (BESA, vom FR Kantonsarzt ausgearbeitetes Schema).

4. Unsere Gruppe hat beschlossen, aus Mangel an Geldmitteln einerseits die anderen in der Schweiz verwendeten Systeme nicht zu untersuchen, und sich andererseits auf eine allgemeine Analyse des oben genannten Systems zu beschränken, um so mehr da eine vergleichende Studie der Gesetzesvorschriften in den Kantonen notwendig wäre. Sollte eine genaue Prüfung notwendig sein, schätzt die Gruppe AGX, dass das Büro einen Auftrag erteilen müsste, der etwa einem Monat Arbeit in Vollzeit entspräche.

   Dieser Bericht wurde unserem Kollegen aus BS vorgelegt und berücksichtigt seine Anmerkungen.

5. Im Vorfeld möchte die Arbeitsgruppe festhalten, dass sie sich einer Grundsatzfrage gegenübergestellt sah, nämlich, ob die Behandlung von Bewohnern und Bewohnerinnen von Altersheimen mittels einer systematischen Aufnahme der geringsten Details zur Person, zu ihren Handlungen und ihrem Benehmen, noch mit den Persönlichkeitsrechten zu vereinbaren ist. Die Gruppe beschränkte sich jedoch darauf, Fragen zum Datenschutz zu untersuchen.

II. Untersuchung des Systems

1. RAI/RUG bedeutet RESIDENT ASSESSMENT INSTRUMENT/RESSOURCE UTILIZATION GROUP. Dieses System wurde in den USA entwickelt und wird in der Schweiz von der Firma Q-SYS AG, St. Gallen, vertrieben. Der Teil RAI umfasst einen Fragebogen, Minimum Data Set (MDS) genannt, der dazu dient, die Bedürfnisse jedes Heimbewohners, jeder Heimbewohnerin durch eine systematische Beschreibung seiner/ihrer Stärken und Schwierigkeiten zu bestimmen. Dies sollte als Grundlage für Pflege und Begleitung dienen, welche sich nach den Bedürfnissen des Heimbewohners, der Heimbewohnerin richten.

   Anmerkung : Gemäss Herrn Dr. Anliker (Q-SYS) ist das Hauptziel des Systems die Qualitätssteigerung der langfristigen Pflege.

   Das Zusatzmodul RUG dient einer differenzierten Tarifgestaltung, zum Beispiel in 12 Kategorien.

   Anmerkung : Nach Meinung der Arbeitsgruppe AGX ist der Hauptgrund für die Nutzung des Systems in der Praxis die Klassifizierung der Heimbewohner und nicht die Verbesserung der Qualität; in Basel-Stadt wird auch eine Qualitätskontrolle angestrebt, um dadurch in Sonderfällen die Dienstleistungen zu verbessern.

   Das System Q-SYS zeigt die folgenden Hauptfunktionen des Systems RAI/RUG auf (siehe auch http://www.qsys.ch>RAI/RUG):

- MDS : Bewohner-Assessment und Dokumentation (MDS dient als Ausgangspunkt für die anderen Ziele)
- Pflegeplanung (Abklärungshilfen)
- Ressourcenmanagement (Case Mix, Stellenplanung)
- Qualitätsmanagement (Indikatoren, Outcomermessung)
- Tarife/Finanzierung (Pflegeaufwandgruppen)

Allgemein gesehen umfasst das System 250 Fragen (MDS) (siehe Anhang 1), die im Prinzip obligatorisch sind; der Kanton Basel-Stadt hat jedoch eine Sonderbehandlung erhalten, welche die obligatorischen Fragen auf ungefähr 210 Fragen reduziert, während die anderen fakultativ sind*. Das System ermöglicht eine Klassifizierung der Bewohner in 12 Kategorien, von denen jede noch weitere Unterteilungen umfasst (hier ist anzumerken, dass das System BAK, das vorher vor allem im Kanton BS verwendet wurde, 4 Kategorien umfasst).

Die Fragen sind wie folgt aufgeteilt: Der erste Teil betrifft administrative Daten (wie zum Beispiel AHV-Nummer, Geburtsdatum), aber auch demographische Daten (Berufsausbildung, vorheriger Wohnsitz, Sprache) und Fragen zu Lebensgewohnheiten. Danach werden verschiedene Fähigkeiten untersucht (kognitive, visuelle, körperliche Fähigkeiten; Kontinenz...). Der Fragebogen fährt mit Krankheiten fort und berücksichtigt den Ernährungs- und Hautzustand usw. Die täglichen Aktivitäten sowie die Medikation, spezielle Messungen und Behandlungen der vergangenen Woche werden erfasst. Der Fragebogen schliesst mit durchlaufenen Therapien und der Fortbewegungsfähigkeit.

Die Fragen auf den ersten drei Seiten sind in BS fakultativ, das heisst diejenigen, die Informationen über die Person, ihre individuelle Geschichte und Gewohnheiten liefern. Die demographischen Daten sind für die Pflege nicht relevant.

Anmerkung : Aus der Diskussion mit Herrn Dr. Anliker geht hervor, dass die demographischen Daten für die Statistik nicht verwendet werden. Nach Meinung der Arbeitsgruppe AGX dürften sie deshalb nicht exportiert werden. Das System muss so installiert werden, dass die notwendigen Daten nur vollständig anonymisiert exportiert werden können. Das Heim hat kein Recht, die Seite 11 des Fragebogens, welche die Diagnose der Krankheiten betrifft, direkt zu übermitteln.

Kurz zusammengefasst: Diese 250 Fragen betreffen Identifikationsdaten, medizinische Daten und Daten zu sozialen Gewohnheiten und Verhaltensweisen.

2. Die durchgeführte Untersuchung führt uns zu folgenden Bemerkungen:

2.1 Gesetzliche Grundlagen: Art. 104a Abs. 2 des Bundesgesetzes vom 18. März 1994 über die Krankenversicherung (KVG), der auf Art. 49 und 50 KVG verweist (siehe Anhang 2). Die Informationsbroschüre für Heimbewohner zitiert folgende juristischen Grundlagen: gesetzliche Grundlage für die Feststellung der Daten sind Art. 25, 32 und 33 des Bundesgesetzes vom 18. März 1994 über die Krankenversicherung (KVG), Art. 33 der Verordnung vom 27. Juni 1995 über die Krankenversicherung (KVV) und Art. 7 und 8 der Verordnung vom 29. September 1995 über Leistungen in der obligatorischen Krankenpflegeversicherung (Krankenpflege-Leistungsverordnung, KLV).

2.2 Allgemeine Grundsätze:

Aus den uns vorliegenden Informationen geht Folgendes hervor:

2.2.1 Es zeigt sich, dass dieses System mehrere Ziele verfolgt:, nämlich die Qualität der Pflege und die Verwaltung des betroffenen Heims, die Klassifizierung der Bewohner/innen, die darauf ausgelegt ist, staatliche Subventionen zu erhalten, die entsprechende Rückzahlung der Versicherungen, Statistiken, die grundsätzlich das entsprechende Heim betreffen und für dieses bestimmt sind.

2.2.2 Andere Ziele scheinen ebenfalls beabsichtigt oder möglich, insbesondere die qualitative Verbesserung der Leistungen, der Vergleich zwischen den Heimen, was vor allem die Behörden interessiert (Subventionen), wobei das Ganze sich kostensenkend auf die Heime auswirken sollte, für die Versicherung wie für die Behörden.

2.2.3 Nach Prüfung der gesetzlichen Grundlage scheinen diese Ziele durch die Bestimmungen des KVG abgedeckt zu sein. Die Frage dagegen, ob diese Ziele tatsächlich in Zusammenhang im Sinne von Art. 4 Abs. 3 DSG und den entsprechenden kantonalen Verordnungen (zum Beispiel Art. 5 des freiburgischen Datenschutzgesetzes) stehen, erscheint uns problematisch. Die Ziele sind nicht unbedingt klar und kompatibel untereinander. Ist die beste Kostenverwaltung mit der Verbesserung der Qualität zu vereinbaren? Müssen alle Ziele von einem einzigen System, zum Beispiel RAI-RUG, abgedeckt werden? Die Beziehung zwischen Cardex und dem System RAI/RUG muss noch geklärt werden, so dass die bereits in Cardex verfügbaren Informationen genutzt werden können. Es muss hier auch erwähnt werden, dass das System gemäss Aussage von Nutzern erheblichen Mehraufwand bei der Einführung und beim Betrieb verursacht. Die für das System RAI/RUG Verantwortlichen werden hier sicher betonen, dass diese Kombination von Zielen gerade die Bedingung für eine gute Qualität der Ergebnisse sei. Nach Meinung der Arbeitsgruppe AGX ist es unzulässig, Daten für mehrere Zwecke zu sammeln, auch wenn diese eine juristische Grundlage haben und der Nutzen der Informationen für alle Ziele gegeben ist oder wenn daraus nur eine beschränkte entsprechende Bearbeitung erfolgt.

Das System muss so installiert werden, dass für jedes Datenfeld bestimmt wird, zu welchem Zweck es verwendet wird und dass eine Nutzung zu diesem Zweck nur mit dem vorher definierten Datenfeld möglich ist.

Zudem muss von einem Hauptziel ausgegangen werden: die Dokumentation über die Bewohnerinnen und Bewohner sowie die Tarifierung und die Finanzierung. Die zu diesem Zweck erforderlichen Daten müssen gespeichert werden. Die weiteren Ziele (Planung, Qualitätsmanagement) sind davon abgeleitete Ziele und müssen sich primär mit den verfügbaren Daten begnügen.

2.2.4 Was den Grundsatz von Treu und Glauben angeht, können wir einerseits festhalten, dass die Information des Bewohners und der Bewohnerin (beziehungsweise der Familie und der Angehörigen) im Allgemeinen lückenhaft erscheint, oder sogar aufgrund der Komplexität des Fragebogens als undurchführbar angesehen wird, und andererseits, dass eine Zustimmung der betroffenen Person in den meisten Fällen nicht als „aufgeklärt" oder freiwillig gegeben betrachtet werden kann, da die Gefahr besteht, die Rückerstattung der Versicherung nicht zu erhalten oder schlimmstenfalls gar keinen Heimplatz zu bekommen. Das System ist schon für den Anwender (Heim) undurchsichtig und um so mehr für den Heimbewohner.

2.2.5 Der Fragebogen ist sehr ausführlich (siehe Anhang 1), wenn nicht sogar perfektionistisch. Die Fragen beziehen sich auf sensible Daten über die Gesundheit, die Privat- und sogar Intimsphäre. Das Ganze ergibt ein richtiges Persönlichkeitsprofil. Zum jetzigen Informationsstand sind wir nicht von der Notwendigkeit all dieser Fragen für jeden von den Heimen behandelten, individuellen Fall überzeugt. Das Prinzip der Datensparsamkeit wird gar nicht beachtet. Mehr noch: Wir sind der Meinung, dass das System das Verhältnismässigkeitsprinzip nicht respektiert. Zum Beispiel die Informationen über die Berufsausbildung (Teil AB), den regelmässigen Kirchenbesuch oder die Konsumierung eines alkoholischen Getränks mindestens einmal pro Woche (Teil AC) oder die morgendliche schlechte Laune (Teil E) und ob es spirituelle/religiöse aktivitäten gibt (Teil N), sind für die Ziele des Systems RAI-RUG nicht notwendig. Ausserdem ist das Beantworten der Fragen obligatorisch; das System lässt die weitere Nutzung nicht zu, wenn nicht auf jede Frage eine Antwort eingegeben wird.

2.3 Kommunikation

Gemäss unseren Informationen sollten die persönlichen Daten im Heim bleiben. Das Erstellen der Statistiken ist jedoch eine der Dienstleistungen, die das Unternehmen Q-Sys auf Anfrage erbringt. Die Informationen müssten in absolut anonymisierter Form an Q-Sys weitergeleitet werden, was nach unseren Feststellungen nicht der Fall ist. Einerseits erhalten die Heime keine Anweisungen über die Art, wie sie ihre Daten liefern müssen; andererseits könnten sie gar keine Wahl mehr

haben, falls die Behörden entscheiden sollten, dass alle Daten geliefert werden müssen, oder wenn der Druck der Versicherer stark genug werden sollte.

In folgenden Punkten hat unsere Arbeitsgruppe bereits Probleme festgestellt: Wie sollen die Fragebögen anonymisiert werden (wenn der Jahrgang bestehen bleibt, wenn es sich um seltene Krankheiten handelt oder um kleine Heime usw. kann die Anonymität nicht garantiert werden)? Zudem dürften nach dem Verhältnismässigkeitsprinzip nur jene Teile des Fragebogens weiter geleitet werden, die zu statistischen Zwecken verwendet werden können, was nicht für alle 250 Fragen der Fall ist. Wenn Teile des Fragebogens freiwillig sind, dürften sie nicht an Dritte weiter geleitet werden.

Schliesslich muss berücksichtigt werden, dass das Heim dem Berufsgeheimnis oder sogar der ärztlichen Schweigepflicht untersteht, was dazu verpflichtet, nur anonymisierte Daten zu liefern oder vorher die Aufhebung der Schweigepflicht zu erreichen.

2.4 Technischer Ebene

- Unter dem Gesichtspunkt der Aufbewahrung und Vernichtung der Informationen haben wir festgestellt, dass es das System nicht zulässt, Daten zu löschen. Es bietet nur die Möglichkeit anzugeben, ob eine Person gestorben ist oder das Heim verlassen hat. Zudem speichert das System die Daten auf unbegrenzte Zeit, womit die Bestimmungen zur Archivierung nicht eingehalten werden.

- Was die Sicherheit und den Datenschutz anbelangt, haben wir festgestellt, dass Daten ungeschützt auf Computern vorhanden waren (Access DB). Beim Datenexport werden die Daten nicht anonymisiert und nur mangelhaft geschützt. Ein geplanter oder unabsichtlicher Zugriff auf sensible Daten kann zum jetzigen Stand der technischen Möglichkeiten nicht ausgeschlossen werden. Zudem ist die Dokumentation des Systems schlecht. Es fehlen Informationen zu den Sicherheitsanforderungen, die das System erfüllen müsste und die Bedingungen dazu; ausserdem gibt es kein Datenschutzkonzept.

- Der Informatiker in unserer Gruppe konnte sich mangels Informationen keine Vorstellung davon machen, wie das System zu einer Klassifizierung kommt.

III. Schlussfolgerungen

Unsere Arbeitsgruppe ist zu folgenden Schlussfolgerungen gekommen:

1. Zur Zeit findet eine Entwicklung der Systeme zur Beurteilung von Bewohnern und Bewohnerinnen von Alters- und Pflegeheimen statt, die neue Proportionen annimmt. Probleme, die diese neuen Systeme mit sich bringen, sind die Erfassung

und die Sicherheit der Daten, die Kommunikation und die Aufbewahrung der Informationen, sowie die Anonymisierung, in Verbindung mit der Schweigepflicht.

2. Einerseits ist der wirtschaftliche Aspekt bedeutend (Entwicklung des Systems von Q-SYS); andererseits versuchen die Beteiligten (Staat, Versicherungen), Kosten zu senken. Wir sind uns der Interessen, die auf dem Spiel stehen, bewusst; diese müssen jedoch die Grundrechte berücksichtigen, vor allem wenn es sich um die Rechte einer Bevölkerungsschicht handelt, die eines besonderen Schutzes bedarf.

3. Die Versicherer üben schon heute starken Druck auf gewisse Heime aus (insbesondere im Kanton FR), um vollständige persönliche Informationen zu erhalten, die eine Klassifizierung der Bewohner und Bewohnerinnen ermöglichen. Man kann ohne grosses Risiko sich zu täuschen, prognostizieren, dass die Versicherer sich mit einem solch ausgeklügelten System noch mehr dafür interessieren werden, die Informationen zu erhalten, um prüfen zu können, ob die Klassifizierung richtig und die Heimführung zufriedenstellend ist. Unserer Meinung nach fehlen zur Zeit klare gesetzliche Grundlagen, welche die systematische Kommunikation von persönlichen Daten zulassen.

4. Für die Heimbewohner und -bewohnerinnen ist das System zu einem grossen Teil undurchsichtig.

5. Die Daten werden systematisch erfasst, unabhängig von den Pflegebedürfnissen des Bewohners oder der Bewohnerin. Dies führt zu einer Sammlung von Daten „auf Vorrat", die mit dem Verhältnismässigkeitsprinzip nicht zu vereinbaren ist. Auch wenn man eine systematische Erfassung von gewissen Informationen zulässt, muss diese auf eine vernünftige Menge beschränkt werden.

6. Zum derzeitigen Stand der Dinge schlägt die Arbeitsgruppe AGX vor, sich auf ein kurz gefasstes Vorgehen zu beschränken. Das heisst, wir streben vor allem zwei Ziele an:

- Beseitigung der Mängel
- Reduktion der Anzahl der obligatorischen Fragen

Im Namen der Arbeitsgruppe AGX
Dominique Nouveau Stoffel
Präsidentin

Freiburg, 17 Juli 2002/12 November 2002/DNS

Liste der notwendigen Anpassungen im System RAI/RUG

Die nachstehende Liste enthält Anpassungen, welche die Arbeitsgruppe Gesundheit (AGX) gestützt auf die ihr zur Verfügung stehenden Informationen als minimal notwendig erachtet. Vorbehalten bleiben weitergehende, nach kantonalem Recht notwendige Anpassungen.

A. Zweckmässige Datenerhebung

1. Beschränkung der Datenerhebung auf eine verhältnismässige Menge: Festlegen und begründen des minimalen Datenbedarfs für den vorgesehenen Zweck: Pflegeplanung und Finanzierung (Einstufung in Pflegeaufwandgruppen).
2. Allfällige weitere Zwecke sind in erster Linie mit den für den Hauptzweck gesammelten Daten zu verfolgen.
3. Daten dürfen nur für effektiv verfolgte Zwecke erhoben werden und nicht für weitere vom System her mögliche Zwecke.
4. Das System muss technisch so eingerichtet werden, dass für jedes Datenfeld festgelegt ist, welchem Zweck es dient. Auswertungen dürfen nur für den festgelegten Zweck möglich sein.

B. Minimum Data Set (MDS)

1. Ausgehend vom minimalen Datenbedarf muss das MDS auf ein verhältnismässiges Mass reduziert werden: weniger Fragen und Überprüfung des Detaillierungsgrades der einzelnen Fragen.
2. Die Anzahl der obligatorischen Fragen muss auf das absolute Minimum beschränkt werden. Die Beantwortung der übrigen Fragen ist freiwillig.
3. Jede Frage muss als obligatorische oder freiwillige Frage erkennbar sein.
4. Das System muss technisch so eingerichtet werden, dass es möglich ist, Fragen unbeantwortet zu lassen.

C. Datenexport zu Statistikzwecken

1. Festlegen der zur Erstellung von Statistiken notwendigen Daten.
2. Das System muss technisch so eingerichtet werden, dass nur die für Statistikzwecke notwendigen Daten exportiert werden (z. B. kein Export demographischer Daten, kein Export von Krankheitsdiagnosen).

3. Die Daten dürfen das Heim nur vollständig anonymisiert verlassen. Die Anonymisierung muss definierten Minimalanforderungen entsprechen.

D. Datensicherheit

1. Die Daten dürfen nicht ungeschützt gespeichert werden, sondern müssen mit den heute zur Verfügung stehenden technischen Mitteln geschützt werden (z.B. abgestufte Zugriffsrechte, Anwendung von Verschlüsselungstechnologien für Ablage und Übermittlung der Daten, digitale Signaturen). Da es sich um besonders schützenswerte Daten handelt, sind die Anforderungen an die Datensicherheitsmassnahmen entsprechend hoch.

E. Verbesserung der Transparenz

1. Es muss nachvollziehbar sein, welche Daten wie, wo und wie lange im System aufbewahrt werden.
2. Das System muss die Archivierung von Daten ermöglichen.
3. Nicht mehr benötigte Daten müssen vollständig gelöscht werden (inkl. Archiv und Back-up).
4. Eine maximale Aufbewahrungsfrist muss festgelegt werden.

F. Dokumentation

1. Erarbeitung einer schriftlichen Information für die Heimbewohner und ihre Angehörigen, welche die Datenbearbeitung durchschaubar und nachvollziehbar darstellt.
2. Erarbeitung eines Datenschutzkonzeptes, welches die Umsetzung der Grundsätze des Datenschutzes beschreibt.

Bern, 20. August 2002

13.6 Erklärung der europäischen Datenschutzbeauftragten

Erklärung der europäischen Datenschutzbeauftragten auf der Internationalen Konferenz in Cardiff (9. - 11. September 2002) zur obligatorischen systematischen Aufbewahrung von Verkehrsdaten im Bereich der Telekommunikation

Die europäischen Datenschutzbeauftragten nehmen mit Besorgnis zur Kenntnis, dass im Bereich der „dritten Säule" der Europäischen Union Vorschläge erwogen werden, die eine obligatorische systematische Aufbewahrung von Verkehrsdaten in Bezug auf alle Arten der Telekommunikation (d.h. Einzelheiten über Zeit, Ort und gewählte Nummern im Telefon-, Telefax- oder E-Mail-Verkehr und jeder sonstigen Nutzung des Internet) über einen Zeitraum von einem Jahr und länger zur Folge hätten, um einen möglichen Zugang durch Strafverfolgungs- und Sicherheitsorgane zu gestatten.

Die europäischen Datenschutzbeauftragten äussern schwerwiegende Zweifel hinsichtlich der Legitimität und Rechtmässigkeit derartiger allgemeiner Massnahmen. Darüber hinaus weisen sie auf die übermässigen Kosten hin, die damit für die Telekommunikations- und Internetbranche verbunden wären, und verweisen darauf, dass in den Vereinigten Staaten keine derartigen Massnahmen angewandt werden.

Die europäischen Datenschutzbeauftragten haben mehrfach betont, dass eine derartige Aufbewahrung eine unzulässige Beeinträchtigung der Grundrechte darstellen würde, die natürlichen Personen durch Artikel 8 der Konvention des Europarates zum Schutz der Menschenrechte und Grundfreiheiten zugesichert sind, wie dies auch vom Europäischen Gerichtshof für Menschenrechte ausgeführt wird (siehe Stellungnahme 4/2001 der Artikel 29-Datenschutzgruppe gemäss Richtlinie 95/46/EG und Erklärung von Stockholm, April 2000).

Der Schutz von Daten im Telekommunikationsverkehr ist nunmehr auch in Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Amtsblatt L 201/37) geregelt, der zufolge die Verarbeitung von Verkehrsdaten grundsätzlich zum Zwecke der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen erlaubt ist. Nach langer und eingehender Diskussion gelangen die europäischen Datenschutzbeauftragten zu dem Schluss, dass bei der Aufbewahrung von Verkehrsdaten für Zwecke der Strafverfolgung die Bedingungen von Artikel 15 Absatz 1 der Richtlinie strikt einzuhalten sind, d.h. in jedem Einzelfall ist die Aufbewahrung nur während einer begrenzten Zeit und wenn dies in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismässig ist, zulässig.

Wenn in besonderen Fällen Verkehrsdaten aufbewahrt werden sollen, muss eine beweisbare Notwendigkeit vorliegen und die Zeitdauer der Aufbewahrung muss so kurz

wie möglich sein; weiterhin muss die diesbezügliche Praxis gesetzlich in einer Weise klar geregelt sein, die ausreichenden Schutz gegen unrechtmässigen Zugang und anderweitigen Missbrauch bietet. Die systematische Aufbewahrung aller Arten von Verkehrsdaten über einen Zeitraum von einem Jahr und länger würde eindeutig gegen den Grundsatz der Verhältnismässigkeit verstossen und wäre somit in jedem Fall inakzeptabel.

Die europäischen Datenschutzbeauftragten erwarten, dass die Artikel 29-Datenschutzgruppe zu Massnahmen, die sich aus den Gesprächen im Bereich der „dritten Säule" ergeben, vor deren Annahme konsultiert wird.

13.7 Empfehlungen des EDSB

13.7.1 Empfehlung in Sachen Fitnesscenter

EMPFEHLUNG

gemäss

Art. 29 Abs. 3 des

Bundesgesetzes über den

Datenschutz vom 19. Juni 1992

in Sachen

Fotokartei mit Mitgliedern der Fitnesscenter der Betreiberin X

I. Der Eidg. Datenschutzbeauftragte stellt fest:

1. Die Fitnesscenter der Betreiberin X bieten zahlreiche Sport-, Fitness- und Wellnessangebote an. Personen, die davon profitieren möchten und ein Abonnement (Abonnemente für 10 Eintritte oder für das ganze Jahr) lösen möchten, müssen sich damit einverstanden erklären, dass von ihnen eine Fotografie erstellt wird. Diese wird in die Mitgliederkartei aufgenommen und soll fortan Identifikations- und Kontrollzwecken dienen.

2. Der Eidg. Datenschutzbeauftragte (EDSB) hat die X mit einem Schreiben vom 6. September 2001 darauf aufmerksam gemacht, dass das von den Fitnesscenter angewandte Vorgehen gegen das Prinzip der Verhältnismässigkeit von Art. 4 des Bundesgesetzes über den Datenschutz (DSG; SR 235.1) verstosse. Der EDSB wies darauf hin, dass es bei der Eintrittskontrolle andere Mittel gebe, die eine eindeutige Identifikation der Berechtigen ermöglichen und dabei die Persönlichkeit der Betroffenen weniger beeinträchtigen würden. Der EDSB bat um eine Stellungnahme.

3. Im Schreiben vom 7. November 2001 vertrat die X die Ansicht, dass es zur Verhinderung des Missbrauchs der teuren Jahresabonnemente keine mildere Massnahme gebe. Des Weiteren führte die X aus, dass diese Fotos mit der ausdrücklichen Einwilligung der betroffenen Personen erstellt würden, „weshalb der Rechtfertigungsgrund gemäss Art. 13 Abs. 1 DSG gegeben ist. Zudem handelt es sich um die Abwicklung einer längerdauernden Vertragsbeziehung; das Foto wird somit aus einem begründeten Anlass erstellt und anschliessend in der Mitgliederkartei abgelegt (Art. 13 Abs. 2 Bst. a DSG).“

II. Der Eidg. Datenschutzbeauftragte zieht in Erwägung:

1. Das Bundesgesetz über den Datenschutz (DSG, SR 235.1) regelt unter anderem die Bearbeitung von Daten natürlicher und juristischer Personen durch private Personen (Art. 2 Abs. 1 DSG). Das Erstellen einer Fotografie von Mitgliedern der Fitnesscenter und in der Folge einer Fotokartei ist eine Bearbeitung von Personendaten im Sinne von Art. 3 Bst. e DSG. Die X ist eine private Person und fällt daher unter die Bestimmungen des DSG (Art. 2 Abs. 1 DSG).

2. Gemäss Art. 29 DSG klärt der EDSB im Privatbereich von sich aus oder auf Meldung Dritter Sachverhalte näher ab, namentlich wenn die Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler, Art. 29 Abs. 1 Bst. a DSG). Die Eidgenössische Datenschutzkommission hat in ihrem Entscheid vom 21. November 1996 in S. Mietwesen (VPB 1996, 62.42B) festgestellt, „dass die Empfehlungsbefugnis des EDSB nach Art. 29 Abs. 1 Bst. a DSG weiter zu interpretieren und nicht bloss auf Fehler von Informationssystemen der EDV zu beschränken sei." Mit anderen Worten ist von einem „Systemfehler" im Sinne der genannten Bestimmung auch dann zu sprechen, „wenn die Bearbeitung von Daten inhaltlich rechtswidrig, d.h. die Bearbeitung als solche so angelegt ist, dass sie geeignet ist, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen." Das beschriebene Vorgehen der Fitnesscenter (Anlegen einer Fotokartei aller Mitglieder) ist geeignet, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen.

3. Das Verhältnismässigkeitsprinzip ist gegeben, wenn eine Massnahme geeignet ist, das angestrebte Ziel zu erreichen (Zwecktauglichkeit), und sie zugleich diejenige ist, welche die privaten Interessen am meisten schont (geringstmöglicher Eingriff) (Maurer, Hrsg., Kommentar zum Schweizerischen Datenschutzgesetz, Art. 4, N 10).

4. Gemäss Art. 12 Abs. 1 DSG darf derjenige, der Personendaten bearbeitet, die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen. Art. 12 Abs. Abs. 2 Bst. a DSG bezeichnet eine Bearbeitung von Personendaten entgegen dem Verhältnismässigkeitsprinzip von Art. 4 Abs. 2 DSG als Persönlichkeitsverletzung, sofern sich der Bearbeiter nicht auf einen Rechtfertigungsgrund nach Art. 13 Abs. 1 DSG berufen kann.

5. Die X geht bei der Einrichtung der Fotokartei zum einen von der „ausdrückliche(n) Einwilligung der betroffenen Personen" aus, zum andern verweist sie für die Datenbearbeitung auf den Rechtfertigungsgrund des überwiegenden Interesses in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags (Art. 13 Abs. 2 Bst. a DSG).

5.1 Die Einwilligung stellt nur dann einen Rechtfertigungsgrund dar, soweit sie die betreffende Persönlichkeitsverletzung abdeckt. Eine Datenbearbeitung, welche gegen den Grundsatz der Verhältnismässigkeit oder andere allgemeine Bearbeitungsgrundsätze verstösst, kann nur durch die Einwilligung der betroffenen Person gerechtfertigt sein, wenn diese ihre Einwilligung in Kenntnis des Verstosses gegen den Bearbeitungsgrundsatz erteilt hat. Soweit also die X Daten in einer Art und Weise erhebt, die für den Vertragsabschluss nicht unbedingt erforderlich sind, so kann sie nur dann davon ausgehen, dass ein künftiges Mitglied eines Fitnesscenters mit dieser Datenbearbeitung einverstanden ist, wenn die X explizit auf diesen Umstand hingewiesen hat.

In den allgemeinen Geschäftsbedingungen der X heisst es dazu unter Punkt 6, dass der Betroffene zur Kenntnis nehmen müsse, dass eine Fotografie vom ihm erstellt werde und dass diese internen Zwecken diene.

Alleine aus diesem Hinweis kann keine wirksame Einwilligung des Verletzten abgeleitet werden. Zudem legt die X auch die Einzelheiten der Datenbearbeitung nicht klar offen. So bleibt zu unbestimmt, in welcher Art und Weise die Fotografie eingesetzt wird, wie lange die Daten aufbewahrt werden und welche Zwecke mit dieser Datenbearbeitung nebst der visuellen Kontrolle noch verfolgt werden. Auch der Begriff 'intern' sorgt für weitere Ungewissheit, da unklar bleibt, ob sich diese Datenbearbeitung nur auf die dort aufgeführten Fitnesscenter beschränkt, sich auf alle Fitnesscenter der X in der Schweiz ausdehnt oder gar auf andere Tätigkeitsbereiche der X bezieht.

Aufgrund des Ausgeführten kommt der EDSB zum Schluss, dass *keine wirksame Einwilligung* der Betroffenen für das Aufnehmen ihrer Fotografie in einer Kartei der Fitnesscenter vorliegt.

5.2 Des Weiteren beruft sich die X auf den Rechtfertigungsgrund des überwiegenden Interesses an der Bearbeitung der Personendaten in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages (Art. 13 Abs. 2 Bst. a DSG). Der EDSB bestreitet nicht, dass die X in diesem Rahmen grundsätzlich Personendaten bearbeiten darf. In vorliegendem Fall lässt die X jedoch völlig ausser Acht, dass selbst bei Bestehen eines Vertrages nicht jede Form der Datenbearbeitung erlaubt ist; auch hier gilt es die allgemeinen Datenschutzgrundsätze nach Art. 4 ff. DSG zu beachten.

Es ist nachvollziehbar, dass sich die Fitnesscenter vor einer missbräuchlichen Verwendung der Abonnemente durch Nichtberechtigte schützen möchten und entsprechende Vorsichtsmassnahmen ergreifen. Die von den Fitnesscenter angewandte Bearbeitungsform trägt dem Verhältnismässigkeitsprinzip jedoch keine Rechnung.

Der Grundsatz der Verhältnismässigkeit sieht vor, dass ein Datenbearbeiter nur diejenigen Daten bearbeiten darf, die er für einen bestimmten Zweck objektiv tatsächlich benötigt und die mit Blick auf den Bearbeitungszweck und die Persönlichkeitsbeeinträchtigung in einem vernünftigen Verhältnis stehen (BBl 1988 II 450).

Der angestrebte Zweck ist, gemäss eigenen Angaben der X, die eindeutige Identifikation des aus dem Abonnement Berechtigten. Dies kann bereits dadurch erreicht werden, dass sich das Mitglied zusätzlich zu seinem Abonnement mittels eines amtlichen und mit einer Fotografie versehenen Ausweises, z.B. Identitätskarte, legitimiert. Denkbar ist auch, dass den Mitgliedern ein Abonnement ausgehändigt wird, auf der eine Fotografie des Berechtigten angebracht ist und die dann bei Eintritt vorgewiesen werden muss. Beide Massnahmen ermöglichen eine eindeutige Identifikation des Berechtigten und greifen im Vergleich zur Fotokartei weniger stark in die Persönlichkeitssphäre der betroffenen Personen ein.

Der EDSB ist der Meinung, dass der *Rechtfertigungsgrund gemäss Art. 13 Abs. 2 Bst. a DSG* für das Erstellen und Führen einer Fotokartei mit den Mitgliedern der Fitnesscenter *nicht gegeben* ist, da die von der X angewandte Form der Datenbearbeitung nicht die schonendste Massnahme darstellt und daher *gegen das Verhältnismässigkeitsprinzip im Sinne von Art. 4 Abs. 2 DSG verstösst*.

III. Aufgrund dieser Erwägungen empfiehlt der Eidg. Datenschutzbeauftragte:

1. Die X schafft für Benutzer und Mitglieder der Fitnesscenter die Möglichkeit, Abonnemente zu lösen, ohne dass dabei die Fotografie der Betroffenen in eine Fotokartei aufgenommen wird, oder sie weist die Betroffenen vor Vertragsabschluss in adäquater Form ausdrücklich und umfassend auf den Zweck und Umfang dieser Datenbearbeitung hin.
2. Die X teilt dem Eidg. Datenschutzbeauftragten innerhalb von 30 Tagen seit Erhalt dieser Empfehlung mit, ob er die Empfehlung annimmt oder ablehnt. Wird diese Empfehlung nicht befolgt oder abgelehnt, so kann der Eidg. Datenschutzbeauftragte die Angelegenheit der Eidg. Datenschutzkommission zum Entscheid vorlegen.
3. Diese Empfehlung wird der X und der betroffenen Person mitgeteilt.

DER EIDGENÖSSISCHE
DATENSCHUTZBEAUFTRAGTE
Der Beauftragte:

Hanspeter Thür

13.7.2 Empfehlung in Sachen Vaterschaftstest

Empfehlung
gemäss
Art. 29 Abs. 3 Bundesgesetz über den

Datenschutz vom 19. Juni 1992

in Sachen

Vaterschaftstest

angeboten durch die Firma X

I. Der Eidgenössische Datenschutzbeauftragte stellt fest:

1. Die Firma X hat den Eidgenössischen Datenschutzbeauftragten (EDSB) über die Tatsache informiert, dass sie in Zusammenarbeit mit sechs Fachlabors aus den USA ab sofort einen Vaterschaftstest in der Schweiz vertreiben will.

2. Die Firma X informiert in ihrem Schreiben den EDSB summarisch über die vorgesehenen Datenbearbeitungen und hält fest, dass,

- die zur Abklärung der Vaterschaft benötigten Speichelproben in ihren Partnerlabors in den USA analysiert werden,
- ausschliesslich das Vorhandensein bzw. der Ausschluss einer vermuteten Vaterschaft überprüft wird,
- die DNA-Profile darüber hinaus nicht weiter bearbeitet werden,
- die DNA-Profile insbesondere nicht Dritten zugänglich gemacht werden,
- die DNA-Profile ein Jahr nach Bekanntgabe der Untersuchungsresultate vernichtet werden,
- die Speichelproben mit Namen, Vornamen Geburtsdatum und Herkunftsregion der Testpersonen versehen übermittelt werden
- und
- meldet beim EDSB gestützt auf Art. 6 und Art. 11 des Bundesgesetzes über den Datenschutz (DSG; SR 235.1) sowie Art. 3 und 5 der Verordnung zum Bundesgesetz über den Datenschutz (VDSG; SR 235.11) die entstehende Datensammlung zur Registrierung an.

3. Die Firma X legt der Anmeldung zusätzlich ein Formular „Vaterschaftsnachweis" bei, das der Auftraggeber zusammen mit der Speichelprobe einschicken muss

und auf dem die Personalien und Unterschriften der zu testenden Personen aufzuführen sind. Das Formular enthält zudem folgende Klausel:

„Mit meiner persönlichen Unterschrift bestätige ich, dass ich Erziehungsberechtigter aller zu testenden Kinder bin und mit der Speichelentnahme keine Persönlichkeitsrechte der Kinder verletze. Als Frau benötige ich zudem die Einwilligung der zu testenden möglichen Väter, um deren Speichel für den Vaterschaftsnachweis zu entnehmen. Hierfür übernehme ich als Auftraggeber/in die alleinige Verantwortung."

II. Der Eidgenössische Datenschutzbeauftragte zieht in Erwägung:

1. Bezüglich datenschutzrechtlicher Fragen im Zusammenhang mit Vaterschaftstest, die von privaten Firmen angeboten werden, kommen die Bestimmungen des DSG zur Anwendung (Art. 2 Abs. 1 lit. a DSG).

2. Das für den Abstammungsnachweis herangezogene DNA-Profil ist eine für das einzelne Individuum spezifische Information, die mit Hilfe molekulargenetischer Techniken aus Gewebeproben gewonnen wird. Es handelt sich dabei um eine genetische Untersuchung.

3. Bei den DNA-Profilen und den hieraus resultierenden Testergebnissen handelt es sich um besonders schützenswerte Personendaten gemäss Art. 3 lit. c DSG. Die eingesandten Speichelproben beinhalten spezifische Informationen, welche im Rahmen des Vaterschaftstests ausgewertet werden.

4. Der EDSB hat gemäss Art. 29 Abs. 1 VDSG vor Registrierung einer bei ihm angemeldeten Datensammlung die Rechtmässigkeit der vorgesehenen Datenbearbeitungen summarisch zu prüfen.

5. Verstösst die zu registrierende Datensammlung gegen Vorschriften des Datenschutzes, kann der EDSB gestützt auf Art. 29 Abs. 3 DSG empfehlen, die vorgesehene Datenbearbeitung zu ändern, einzustellen oder zu unterlassen.

6. Die Durchführung eines Vaterschaftstests - welcher mit der Entnahme der Gewebeproben (im vorliegenden Fall Speichelproben) beginnt - stellt eine Bearbeitung von Personendaten im Sinne des DSG dar und bedarf eines Rechtfertigungsgrundes. Art. 13 Abs. 1 DSG sieht als mögliche Rechtfertigungsgründe die Einwilligung des Verletzten, ein überwiegendes öffentliches oder privates Interesse oder das Gesetz vor. Im Falle eines freiwilligen, d.h. ausserhalb eines behördlichen Verfahrens durchgeführten Tests zur Abklärung der Abstammung kommt einzig die Einwilligung der betroffenen Personen in Betracht.

7. Die datenschutzrechtliche Einwilligung muss gewisse Anforderungen erfüllen. Selbst wenn das Gesetz in der Regel keine besonderen Formerfordernisse für Ein-

willigungen vorsieht, muss angesichts der besonderen Sensibilität der hier in Frage stehenden Daten die Einwilligung für die Durchführung eines Vaterschaftstests stets **schriftlich** vorliegen. Entscheidend für die Rechtsgültigkeit der Einwilligung ist weiter, dass die einwilligende Person **freiwillig** handelt. Auf die Freiwilligkeit der Einwilligung muss im Einwilligungsformular schriftlich hingewiesen werden. Sofern die betroffene Person eine Bedenkzeit wünscht, muss ihr diese gewährt werden. Damit sich die einwilligende Person der Tragweite ihrer Einwilligung bewusst ist (sog. „**aufgeklärte** Einwilligung"), muss sie in Kenntnis der Sachlage und der möglichen Folgen einwilligen. Eine solche aufgeklärte Einwilligung ist nur möglich, wenn die betroffene Person vorgängig alle Informationen erhalten hat, die sie benötigt, um die möglichen Folgen ihres Handelns abzuschätzen.

8. Ein Vaterschaftstest kann für alle Betroffenen weitreichende Auswirkungen (z.B. psychische Belastungen), Komplikationen und Entscheide unterschiedlichster Art nach sich ziehen. Ohne hinreichende fachmännische Aufklärung und Beratung wird man in den seltensten Fällen davon ausgehen können, dass die Tragweite eines solchen Tests - beispielsweise die Folgen eines unerwarteten Testresultates - auch tatsächlich erkannt wurden. Zudem muss die einwilligende Person auch über den Zweck und den Ablauf des Tests an sich und die damit verbundenen Datenbearbeitungen und Datensicherheitsvorkehren informiert werden (Übermittlung, Speicherung, Vernichtung der Daten, Schutz vor unbefugtem Zugriff Dritter, Pseudonymisierungs- oder Anonymisierungsmassnahmen etc.).

9. Schliesslich muss darauf hingewiesen werden, dass die Einwilligung jederzeit **formlos widerrufbar** ist. Ein mündlich oder schriftlich mitgeteilter Widerruf hat zur Folge, dass ein noch nicht begonnener Vaterschaftstest nicht durchgeführt wird, allenfalls bereits abgegebene Speichelprobe vernichtet und alle im Zusammenhang mit dem Vaterschaftstest erhobenen Daten gelöscht werden müssen.

10. Die Firma, die den Vaterschaftstest anbietet und durchführt oder durch Dritte durchführen lässt, ist dafür verantwortlich, dass das Probematerial rechtmässig erlangt wurde. Die rechtmässige Beschaffung des Probematerials ist aus datenschutzrechtlicher Sicht zentral. Die Vaterschaftstests anbietende Firma trifft daher eine **spezielle Aufklärungs- und Überprüfungspflicht**. Sie muss für die fachmännische Beratung und für die wirksame Überprüfung der vom Auftraggeber vorgelegten Einwilligungen aller betroffenen Personen (mutmasslicher Vater, Mutter, Kind) besorgt sein. Bei urteilsunfähigen Kindern muss die Einwilligung des gesetzlichen Vertreters vorliegen, wobei dies in der Regel beide Eltern bzw. derjenige Elternteil ist, der allein sorgeberechtigt ist.

11. Die Verantwortung für das Vorliegen rechtsgültiger Einwilligungen kann nicht auf den Auftraggeber abgewälzt werden, wie dies in der oben zitierten Klausel des Formulars „Vaterschaftsnachweis" vorgesehen ist. Ohne wirksame Überprüfung der vorgelegten Einwilligungen können z.B. ohne weiteres auch sogenannt „heimliche" Vaterschaftstests in Auftrag gegeben werden. Solche Vaterschaftstests, die mit Proben durchgeführt werden, die ohne Vorliegen rechtsgültigen Einwilligungen durchgeführt werden, sind unrechtmässig. Sie verletzen die Persönlichkeitsrechte des betroffenen Kindes und des nicht informierten Partners in erheblichem Masse.

12. Aufgrund der vorstehenden Ausführungen, ist der EDSB bei seiner summarischen Prüfung der Rechtmässigkeit der Datenbearbeitung gemäss Art. 29 Abs. 1 VDSG zum Schluss gelangt, dass die Vorschriften des Datenschutzes bei der geplanten Vorgehensweise nicht eingehalten werden. Die Persönlichkeitsrechte der betroffenen Personen scheinen ernstlich gefährdet, weil grundlegende Anforderungen für die Rechtsgültigkeit der Einwilligung nicht erfüllt sind; insbesondere fehlt die hinreichende Aufklärung der betroffenen Personen sowie eine wirksame Überprüfung der Rechtsgültigkeit der vom Auftraggeber vorgelegten Einwilligungserklärungen.

13. Schliesslich ist die Datenbekanntgabe in die USA, wohin die Proben zur Analyse eingesandt werden, in der Form, wie sie in der Anmeldung beschrieben wird, nicht zulässig. In den USA fehlt ein Datenschutz, der dem schweizerischen gleichwertig ist. In solchen Fällen muss der Schutz der übermittelten Daten einerseits zwingend vertraglich abgesichert werden, andererseits ist die Bekanntgabe von Personendaten wie Name, Vorname, Geburtsdatum, nicht nötig, weil im vorliegenden Falle ohne weiteres mit einem Pseudonymisierungscode gearbeitet werden kann. Diese relativ einfache Massnahme macht die Übermittlung von Personendaten wie Name, Vorname, Geburtsdatum überflüssig und erhöht den Schutz der aus der Analyse resultierenden besonders schützenswerte Personendaten erheblich.

14. Gestützt auf die vorangehenden Erwägungen kommt der EDSB zum Schluss, dass die Registrierung der angemeldeten Datensammlung im jetzigen Zeitpunkt nicht erfolgen kann, weshalb die Registrierung bis auf weiteres sistiert wird.

III. Aufgrund dieser Erwägungen empfiehlt der Eidgenössische Datenschutzbeauftragte:

1. Die Firma X verschiebt den Vertrieb des Vaterschaftstests bis die damit verbundenen Datenbearbeitungen den datenschutzrechtlichen Anforderungen gemäss DSG genügen.

2. Die Firma X kommt ihrer Aufklärungs- und Informationspflicht im Hinblick auf eine aufgeklärte Einwilligung ihrer Kunden nach, indem sie durch geeignete Massnahmen sicherstellt, dass diese eine fachmännische Aufklärung und Beratung erhalten. Dies kann beispielsweise durch Abgabe eines durch Fachleute ausgearbeiteten ausführlichen Informationsblattes geschehen, dessen Kenntnisnahme der Kunde auf dem Einwilligungsformular schriftlich bestätigt. Zudem stellt die Firma X ihren Kunden eine Fachperson zur Verfügung, an die sich diese mit allfälligen Fragen jederzeit schriftlich oder mündlich wenden können.

3. Die Firma X passt das Formular „Vaterschaftsnachweis" entsprechend den Ausführungen in den Ziff. 7 bis 11 der Erwägungen an.

4. Die Firma X kommt ihrer Überprüfungspflicht nach, indem sie die von den Kunden vorgelegten Einwilligungen aller durch den Vaterschaftstest betroffenen Personen wirksam überprüft, z.B. durch telefonische Rückfrage oder durch andere geeignete Massnahmen.

5. Liegt eine Einwilligungserklärung eines urteilsfähigen Unmündigen vor, muss die Firma X die Rechtsgültigkeit dieser Einwilligung mit besonderer Sorgfalt überprüfen. In Zweifelsfällen holt die Firma X zusätzlich die Einwilligung des gesetzlichen Vertreters ein, d.h. beider Eltern bzw. im Ausnahmefall des allein sorgeberechtigten Elternteils.

6. Bestehen Zweifel an der rechtmässigen Probenentnahme, so ordnet die Firma X eine erneute Probenentnahme an und führt diese entweder selber durch oder beauftragt damit eine neutrale Drittperson.

7. Die Firma X pseudonymisiert die Speichelproben vor deren Übermittlung in die USA und schliesst mit ihren US-amerikanischen Partnern einen Datenschutzvertrag ab, der für die übermittelten und für die aus der Analyse resultierenden Daten einen dem schweizerischen analogen Datenschutz garantiert. Sofern ein solcher Vertrag bereits abgeschlossen wurde, ist er dem EDSB vorzulegen.

8. Die Firma X informiert den EDSB im Einzelnen über die im Verfahren des Vaterschaftstests getroffenen Datenschutz- und Datensicherheitsvorkehren.

9. Die Firma X weist alle ihre Mitarbeiter und Hilfspersonen schriftlich auf die Schweigepflicht gemäss Art. 35 DSG hin.

Die Firma X teilt dem EDSB innerhalb von 10 Tagen nach Erhalt dieser Empfehlung mit, ob sie die Empfehlung annimmt oder ablehnt. Wird diese Empfehlung abgelehnt oder nicht befolgt, so kann der EDSB die Angelegenheit der Eidgenössischen Datenschutzkommission vorlegen.

Die vorliegende Empfehlung wird der Firma X eingeschrieben zugestellt und gestützt auf Art. 30 Abs. 2 DSG publiziert.

DER EIDGENÖSSISCHE DATENSCHUTZBEAUFTRAGTE
Der Beauftragte:

Hanspeter Thür

13.7.3 Empfehlung in Sachen SPAM

Empfehlung
gemäss
Art. 29 Abs. 3
Bundesgesetz über den
Datenschutz vom 19. Juni 1992
in Sachen
unerwünschte Werbung per Mail
F
und
HBC

I. Der Eidgenössische Datenschutzbeauftragte stellt fest:

1. Seit einiger Zeit erhält EDSB regelmässig Zuschriften von Privatpersonen und Unternehmen, worin sich diese über die Geschäftspraktiken von F – insbesondere seiner Firma „XY" – beklagen. Dabei formulieren die Betroffenen folgende Vorwürfe:

- F stelle ihnen per e-Mail unerwünschte Werbung zu,
- ihre datenschutzrechtlichen Löschungsbegehren würden nicht befolgt,
- der Versand der unerwünschten Mails höre auch nach Abmahnung bzw. Löschungsbegehren gemäss Art. 15 Abs. 1 des Bundesgesetzes über den Datenschutz (DSG) nicht auf und
- auf ihre Begehren gemäss Art. 8 DSG erhielten sie keine bzw. unvollständige Auskunft.

2. F hat mindestens bis im Jahr 2000 per e-Mail potentiellen Kunden angeboten, einen Probeauszug aus seiner Sammlung von Mail-Adressen zuzustellen, damit sich diese von der Qualität der Adressen überzeugen können.

3. F versendet unverlangte und teils unerwünschte Werbemails nicht bloss unter seinem Namen „XY", sondern auch unter den Namen HBC.

II. Der Eidgenössische Datenschutzbeauftragte zieht in Erwägung:

1. F ist eine Privatperson, seine Datenbearbeitungen fallen gemäss Art. 2 Abs. 1 lit. a DSG in den Anwendungsbereich des DSG. Aus demselben Grund ist die Zuständigkeit des EDSB zu Abklärungen und Empfehlungen gemäss Art. 29 DSG gegeben. Der Begriff der privaten Person in Art. 2 Abs. 1 lit. a DSG erfasst nebst den natürlichen auch die juristischen Personen (vgl. Marc Buntschu, in Kommentar zum

schweizerischen Datenschutzgesetz, Urs Maurer, Nedim Peter Vogt – Basel; Frankfurt am Main: Helbing und Lichtenhahn, 1995 , N 21 zu Art. 2). Für die privatrechtliche HBC gilt daher mit Bezug auf Anwendbarkeit des DSG und Zuständigkeit des EDSB dasselbe wie für die Person F.

2. F begründet die Nichtberücksichtigung der Willensäusserungen der betroffenen Personen damit, dass Mail-Adressen keine Personendaten seien, weil sie für ihn keinen Personenbezug hätten. Ein solcher sei allenfalls für Dritte wie Internet Service Providers oder die Polizei gegeben. Dementsprechend sei das Datenschutzgesetz nicht anwendbar und es gebe auch keine datenschutzrechtlichen Verpflichtungen. Diese Aussage kann in ihrer allgemeinen Form – und darauf kommt es für die Frage der Anwendbarkeit des Bundesgesetzes über den Datenschutz (DSG) an – keinesfalls aufrechterhalten werden. Vielmehr ist ein grosser Teil der Mail-Adressen so aufgebaut, dass die betroffene Person leicht bestimmbar ist. Dies zeigt z.B. ein Blick auf das weit verbreitete Muster für den Aufbau von Mail-Adressen <vorname>.<name>@<arbeitgeber>. Aus der Optik der betroffenen Personen ist betreffend den Personenbezug festzuhalten, dass sie die unerwünschte Werbung in ihre Mailboxen geliefert erhalten; aus deren Sicht scheint klar, dass mit der Zustellung der unerwünschten Werbung Personenbezug hergestellt wird.

Dementsprechend sind E-Mail-Adressen grundsätzlich als Personendaten zu betrachten und die Anwendbarkeit des Datenschutzgesetzes ist mit Bezug auf ihre Bearbeitung gegeben.

3. Die Tatsache, dass die Löschungsbegehren nicht befolgt werden und diejenigen, welche sie gestellt haben, weiterhin unerwünschte Werbung erhalten, widerspricht der Aussage von F im Schreiben vom 17.10.2001 an den EDSB worin er uns mitteilt, wie er auf Auskunfts- und Löschungsbegehren antworte („... Auf Anfrage lösche ich selbstverständlich die E-Mail Adressen aller Personen, die keine Werbung mehr wünschen. ..."). Diese Aussage hat F in Beantwortung des Schreibens vom 16.10.2001 des EDSB in Sachen „Sachverhaltsabklärung gemäss Art. 29 DSG" gemacht. Gemäss den beim EDSB vorliegenden Beschwerden ist das Nichtbefolgen der Löschungsbegehren sowohl für den Zeitraum vor dem 17.10.2001 als auch für denjenigen danach belegt. Damit hat F dem EDSB eine falsche Auskunft in der Abklärung des Sachverhalts gegeben. Auch in subjektiver Hinsicht liegen keine Indizien dafür vor, dass die Aussage gegenüber dem EDSB nicht wissentlich im gleichen Zusammenhang gemacht wurde, in welchem der EDSB Beschwerden von Betroffenen erhalten hat.

4. Für all diejenigen Fälle, in welchen F den Löschungsbegehren nicht Folge leistet, tut er dies entgegen dem ausdrücklichen Willen der betroffenen Personen. Soweit

– was unten zu prüfen sein wird – Mail-Adressen als Personendaten zu betrachten sind, ist darin gemäss Art. 12 Abs. 2 lit. b DSG dann eine Verletzung der Persönlichkeit dieser Personen zu erblicken, wenn F keinen Rechtfertigungs-grund geltend machen kann. Von den drei im Art. 13 Abs. 1 DSG aufgezählten möglichen Rechtfertigungsgründen fällt weder die Einwilligung des Verletzten noch die Rechtfertigung durch Gesetz in Betracht. Auch ein überwiegendes privates Interesse scheint angesichts der Aufzählung von Art. 13 Abs. 2 DSG ausgeschlossen.

Bei der Prüfung der Frage, ob Mail-Adressen als Personendaten zu betrachten sind, ist zu unterscheiden:

a) Das obenerwähnte sehr gebräuchliche Muster für den Aufbau von Mail-Adressen (<vorname>.<name>@<arbeitgeber>) stellt den einfachsten Fall dar. Hier ist nur in denjenigen Ausnahmefällen keine einfache Bestimmung einer betroffenen Person möglich, nämlich dort wo die Elemente vor und hinter dem „@" sehr wenig diskriminatorische Kraft haben, d.h. in den Fällen von Arbeitgebern mit vielen Angestellten und für sehr häufige Namen und Vornamen.

b) In all denjenigen Fällen, in welchen die Bestimmbarkeit der betroffenen Personen nicht derart offensichtlich ist, hilft ein Rückgriff auf den Begriff der Personendaten weiter. Für die Frage, ob eine Person bestimmbar ist, ist gemäss Kommentar zum DSG nicht entscheidend, „ob derjenige, der die Daten bearbeitet den für eine **Identifizierung** erforderlichen Aufwand treiben kann oder will, sondern ob damit gerechnet werden muss, dass ein Dritter, der ein Interesse an diesen Angaben hat, bereit ist, eine Identifizierung vorzunehmen" (vgl. Urs Belser, in Kommentar zum schweizerischen Datenschutzgesetz, Urs Maurer, Nedim Peter Vogt – Basel; Frankfurt am Main: Helbing und Lichtenhahn, 1995 , N 6 zu Art. 3, Hervorhebung im Original). Das bedeutet im vorliegenden Falle nichts anderes, als dass sämtliche von einem Internet Service Provider zur Verfügung gestellten Mail-Adressen als Personendaten zu betrachten sind, sofern der Provider sie im Auftrag von bestimmten Personen einrichtet.

c) Man kann sich sogar fragen, ob nicht sämtliche Mail-Adressen als Personendaten zu betrachten sind. Wenn man davon ausgeht, dass „Bestimmbarkeit" bzw. „Identifizier-barkeit" dadurch gegeben ist, dass die Zuordnung einer Information zur Person mit der Zustellung eines e-Mails geschieht.

5. Aus dem Gesagten ergibt sich, dass F dann die Persönlichkeit der betroffenen Personen verletzt, wenn er ihre Mail-Adressen entgegen ihrem Willen bearbeitet und insbesondere indem er sie für den Versand von Werbemails benutzt. Davon sind nicht bloss diejenigen Personen betroffen, von denen der EDSB Reklamationen erhalten hat. Es kommen dazu noch denjenigen, die sich nur an F, aber nicht

an den EDSB gewendet haben, sowie diejenigen, die F vergeblich zu erreichen versuchten.

6. In den Fällen, in welchen potentielle Kunden von Fs Angebot zur Sichtung von Teilen der Adressliste Gebrauch machten, wurden Personendaten an Dritte bekanntgegeben. Die betroffenen Personen hatten davon jeweils keine Kenntnis – bzw. erst im Nachhinein bei Eingang von Werbung eine beschränkte Kenntnis erhalten. Daher wäre F gemäss Art. 11 Abs. 3 und 4 DSG verpflichtet gewesen, seine Datensammlung dem EDSB anzumelden. Dieser Verpflichtung ist F nicht nachgekommen, was gemäss Art. 34 Abs. 2 Buchstabe a DSG eine Strafe in Form von Haft oder Busse nach sich ziehen kann.

7. Dem EDSB wurden mehrere Fälle gemeldet, in welchen Inhaber von E-Mail-Adressen von Herrn F. ihr Auskunftsrecht nicht korrekt gewährt wurde. Die von Herrn F. verwendete Standardantwort ist derart verwirrend formuliert, dass sogar ein Fall von unvollständiger Auskunft gemäss Art. 34 Abs. 1 DSG nicht ausgeschlossen scheint. Das bedeutet, dass im Falle eines Strafantrages durch eine betroffene Person strafrechtliche Folgen in Form von Haft oder Busse zumindest nicht von Anfang an auszuschliessen sind.

III. Aufgrund dieser Erwägungen empfiehlt der Eidgenössische Datenschutzbeauftragte:

1. F erteilt denjenigen Personen, welche dies bisher verlangt haben, vollständige Auskunft über die Personendaten – seien es Mail-Adressen oder andere Informationen –, welche er über sie bearbeitet.

2. F löscht unverzüglich die Mail-Adressen all derjenigen Personen, welche dies bisher von ihm verlangt haben.

3. F ermöglicht künftig allen Empfängern seiner Mails, auf einfache Art ihr Recht auf ein Opting Out geltend zu machen. Er löscht in Zukunft diejenigen Adressen umgehend aus seiner Datensammlung, für welche das von den betroffenen Personen verlangt wird.

4. F gibt ab sofort keine Personendaten in Form von E-Mail-Adressen mehr an Dritte bekannt oder er meldet seine Datensammlung ordnungsgemäss beim EDSB an.

F teilt dem EDSB innerhalb von 30 Tagen nach Erhalt dieser Empfehlung mit, ob er die Empfehlung annimmt oder ablehnt. Wird diese Empfehlung abgelehnt oder nicht befolgt, so kann der EDSB die Angelegenheit der Eidgenössischen Datenschutzkommission vorlegen.

Die vorliegende Empfehlung wird F eingeschrieben zugestellt und gestützt auf Art. 30 Abs. 2 DSG publiziert. Daneben erhalten diejenigen Betroffenen die Empfehlung, welche sich beim EDSB beschwert haben.

DER EIDGENÖSSISCHE DATENSCHUTZBEAUFTRAGTE
Der Beauftragte:

Hanspeter Thür