12. Tätigkeitsbericht 2004/2005

Eidgenössischer
Datenschutzbeauftragter

Tätigkeitsbericht 2004/2005

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 2004 und 31. März 2005 ab.

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

Vertrieb:

BBL, Verkauf Bundespublikationen, CH-3003 Bern

www.bbl.admin.ch/bundespublikationen

Art.-Nr. 410.012.d/f

Inhaltsverzeichnis

* Originaltext auf Französisch

* Originaltext auf Französisch

* Originaltext auf Französisch

Vorwort

Gelegenheit macht Diebe – weiss der Volksmund. Auf den Datenschutz übertragen könnte man sagen: Jede neue Datenbank weckt den Appetit auf neue Nutzungen. Worin liegt das Problem?

Es besteht die Gefahr, dass dabei wichtige Grundsätze des Datenschutzgesetzes nicht mehr eingehalten werden. Zum Beispiel das Gebot der Zweckbindung. Dieser wichtige Grundsatz verlangt nämlich, dass einmal erhobene Daten nur zu jenem Zweck verwendet werden dürfen, der ursprünglich angegeben wurde. Wer sich beispielsweise mit seinem Leiden einer Ärztin anvertraut, muss nicht akzeptieren, dass seine Adresse ohne Einwilligung einem Pharmabetrieb weiter gegeben wird, der einschlägige Medikamente produziert.

So sehr dieses Prinzip einleuchtet, in der Praxis kann der durch neue Datenbanken geweckte Datenhunger nicht immer erfolgreich abgewendet, können Übergriffe nicht immer verhindert werden. So kommen etwa Kundenkarten von Kaufhäusern regelmässig ins Visier amtlicher Forderungen. Was ist hier erlaubt? Unbestritten ist, dass im Rahmen eines Strafverfahrens der Name eines Karteninhabers offen gelegt werden muss. Datenschutz kann nie Täterschutz sein. Heikler wird es indessen, wenn beispielsweise die Eidgenössische Steuerverwaltung – wie unlängst geschehen – im Zusammenhang mit der Mehrwertsteuer von einem Grossverteiler sämtliche Daten eines Kunden herausverlangt, obwohl diese Informationen sehr wenig über das effektive Einkaufsverhalten des betreffenden Karteninhabers aussagen. Denn die Karte kann zum Beispiel sehr selektiv eingesetzt werden, oder andere Personen können sie verwenden. Deshalb war es richtig, dass das Kaufhaus die Herausgabe verweigerte. Sonst hätte es das Datenschutzgesetz verletzt.

Diese Beispiele deuten darauf hin, dass in Zukunft der Datenhunger von amtlicher Seite zunehmen wird und das Bedürfnis wächst, auf allerlei bestehende Datenbestände zuzugreifen. Ein Blick ins Ausland lässt aufhorchen: In Deutschland beispielsweise ist ohne grosses Aufsehen ein Gesetz in Kraft getreten, das einer Vielzahl von Ämtern (Finanzämter, Erziehungsgeld- und Stipendienämter, Sozial- und Wohnungsämter) den Zugriff auf die Konten jedes Bürgers bzw. jeder Bürgerin ermöglicht. Für diesen Zugriff zahlloser Beamter in einen persönlichen Bereich der Bürger braucht es nicht einmal den Anfangsverdacht eines unredlichen Verhaltens. Man darf gespannt sein, wie das deutsche Bundesverfassungsgericht die Klage zweier Betroffener entscheiden wird.

In den USA ist der Datenfluss zwischen Privatfirmen und dem Staat schon sehr weit fortgeschritten. Ein Bericht des General Accounting Office (einer Art GPK) zeigt, dass bei zahlreichen Projekten private Unternehmen (z.B. Kreditkartenherausgeber und Kreditauskunfteien) den Staat mit Daten beliefern. Die American Civil Liberties Union stellt besorgt fest, dass private Unternehmen (Banken, Airlines, Kreditkartengesellschaften, Autovermieter usw.) ihre Kundendatensammlungen zunehmend der Regierung verkaufen. Zahlreiche grosse professionelle Adresshändler seien heute in der Lage, Listen mit Personen zur Verfügung zu stellen, welche beispielsweise ein Medikament gegen Depressionen einnehmen, an die Bibel glauben, online spielen oder Erotikspielzeuge kaufen. Diese Tendenz hat sich im Zeichen der Terrorismusbekämpfung drastisch verstärkt: Der Patriot Act verpflichtet bestimmte private Firmen zur Lieferung von Daten.

Nicht einmal klar formulierte Gesetze garantieren, dass keine Übergriffe passieren: Kaum war in Deutschland das neue Mautgesetz eingeführt, das die Verarbeitung der erhobenen Daten nur zu spezifischen Zwecken erlaubt, verlangten die Strafverfolgungsbehörden die Daten heraus, um Geschwindigkeitsüberschreitungen zu ahnden. Nur aufgrund der Intervention des deutschen Bundesbeauftragten für den Datenschutz stellte der Gesetzgeber dann klar, dass jede Übermittlung, Nutzung oder Beschlagnahmung nach anderen Rechtsvorschriften unzulässig ist. Was aber, wenn der Gesetzgeber in ein paar Jahren seine Meinung ändert?

Was hat das mit der Schweiz zu tun? Einerseits lehrt die Erfahrung, dass solche Entwicklungen nicht spurlos an unserem Land vorbeiziehen werden. Auch bei uns zeigt sich, dass neue Datenbanken neue Bedürfnisse wecken: Die einmal zusammengestellten Daten lassen sich für viele andere Zwecke verwenden. Ihre Nutzungsmöglichkeiten werden aufgrund verfeinerter Verarbeitungstechnik noch breiter. Andererseits sensibilisiert uns der Blick ins Ausland auf die Probleme, die für uns im transnationalen Datenaustausch entstehen können. Die Frage stellt sich immer wieder sehr konkret, ob im betreffenden Land ein genügendes Datenschutzniveau garantiert und die Übermittlung von Daten unbedenklich ist.

Noch genereller stellt sich indessen die Frage, ob angesichts solcher Entwicklungen die Privatsphäre überhaupt noch zeitgemäss ist. Längst gibt es Stimmen, die das Gegenteil postulieren. David Brin beispielsweise entwirft in seinem Buch «The Transparent Society» die Vision einer Gesellschaft, in der jeder jeden beobachten kann und darf. Dass die Überwachung vielen Menschen nichts ausmacht, zeigt auch die wachsende Zahl der privaten Webcams sowie die in vielen Discos und Lokalen installierten Videokameras, die das Geschehen live ins Netz senden. Mit der «Ich hab nichts zu verbergen»-Mentalität wird die Erstellung einer DNA-Datenbank postuliert, die alle erfassen soll. Der in einem freiheitlichen Staatswesen zentrale Grundsatz der Unschuldsvermutung bleibt dabei auf der Strecke.

Man könnte manchmal den Eindruck erhalten, die westlichen Zivilisationen, die dank dem liberalen und aufklärerischen Geist ihrer Gründerväter eine starke Ausstrahlung hatten, dadurch den autoritären kommunistischen Regimes überlegen waren und sie überlebten, seien der Verteidigung der Freiheitsrechte müde geworden. Zunehmend wird das Heil in mehr Kontrolle und Überwachung gesucht. Wer allerdings die Grundrechte und -freiheiten nicht mehr verteidigt – und der Schutz der Privatsphäre ist eine der zentralen – ist ihrer nicht mehr wert!

Zu guter Letzt wird uns vor Augen geführt, dass auch beim Datenschutz nationale Insellösungen nicht zum Ziel führen; dass also in einer globalisierten Welt mit globalen Datenflüssen die Erarbeitung international gültiger Datenschutzregeln von herausragender Bedeutung ist.

Das ist auch das Hauptziel der 27. Internationalen Konferenz der Datenschutzbeauftragten, die dieses Jahr erstmals in der Schweiz (Montreux, 14. bis 16. September) stattfinden wird. Wir sind hoch erfreut, dass dem Eidgenössischen Datenschutzbeauftragten die Ehre des Gastgebers zuteil wird. Wir haben diese Aufgabe sehr motiviert und mit grossem Engagement in Angriff genommen. Das Motto «Der Schutz von Personendaten und Privatsphäre in einer globalisierten Welt» wird uns genau an diese Fragestellung heranführen. Exakt zum zehnjährigen Geburtstag der EU-Direktive 95/46/EG «zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr» möchten wir Bilanz ziehen. Hat die Direktive das gebracht, was man sich von ihr erhoffte? Wie ist ihr Stellenwert heute im internationalen Kontext? Braucht es eine neue Initiative auf globaler Ebene, um den Datenschutz zu dynamisieren und zu vereinheitlichen? Wir werden an dieser Konferenz eine Schlusserklärung verabschieden, welche Antworten auf diese Fragen gibt.

Hanspeter Thür

Abkürzungsverzeichnis

BAP	Bundesamt für Polizei (heute fedpol)
BAZL	Bundesamt für Zivilluftfahrt
BFF	Bundesamt für Flüchtlinge (heute Bundesamt für Migration BFM)
BJ	Bundesamt für Justiz
BFS	Bundesamt für Statistik
BFU	Büro für Flugunfalluntersuchungen
BSV	Bundesamt für Sozialversicherung
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit
DSG	Bundesgesetz über den Datenschutz
EAN	European Article Number
EDSB	Eidgenössischer Datenschutzbeauftragter
EDSK	Eidgenössische Datenschutzkommission
EPC	European Product Code
FEB	Fachstellen für Früherkennung und Begleitung
GPK	Geschäftsprüfungskommission
GUMG	Bundesgesetz über genetische Untersuchungen beim Menschen
GWG	Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor
IMES	Bundesamt für Zuwanderung, Integration und Auswanderung (heute Bundesamt für Migration BFM)
KVG	Bundesgesetz über die Krankenversicherung
METAS	Bundesamt für Metrologie und Akkreditierung
MGwV	Verordnung über die Meldestelle für Geldwäscherei
RFID	Radio Frequency Identification
SAS	Schweizerische Akkreditierungsstelle
SIS	Schengener Informationssystem

StGB	Strafgesetzbuch
SUVA	Schweizerische Unfallversicherungsanstalt
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
UVG	Unfallversicherungsgesetz
VAG	Bundesgesetz betreffend die Aufsicht von Versicherungsunternehmen
VBS	Departement für Verteidigung, Bevölkerungsschutz und Sport
VOBG	Verordnung über die Offenbarung des Berufsgeheimnisses im Bereich der medizinischen Forschung
VVG	Bundesgesetz über den Versicherungsvertrag
WPISP	Working Party for Information Security and Privacy
ZentG	Bundesgesetz über die kriminalpolizeilichen Zentralstellen des Bundes
ZIS	Zentrales Informationssystem

1 Grundrechte

1.1 Modernisierung des Datenschutzes

1.1.1 Revision des Bundesgesetzes über den Datenschutz

Im Anschluss an zwei parlamentarische Motionen 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 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Die beiden Vorlagen werden gegenwärtig vom Bundesparlament geprüft.

Der Bundesrat unterbreitete 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 grenzüberschreitende Datenübermittlung (BBl 2003 2101) (siehe auch 10. Tätigkeitsbericht, 2002/2003, Ziffer 1.1). Er tat dies als Reaktion auf die Motion 98.3529 der Geschäftsprüfungskommission des Ständerates «Erhöhter Schutz für Personendaten bei Online-Verbindungen» und auf die Motion 00.3000 der Kommission für Rechtsfragen des Ständerates «Erhöhte Transparenz bei der Erhebung von Personendaten». In der Frühjahrssession 2004 beschloss der Nationalrat, zwar auf die Vorlage einzutreten, aber das Geschäft an den Bundesrat zurückzuweisen und ihn zu beauftragen, einen weniger ambitiösen Entwurf vorzubereiten. Die Ratsmehrheit vertrat die Auffassung, der Entwurf des Bundesrates schiesse über die Ziele der beiden Motionen hinaus, und wollte es bei den Motionen und den für die Ratifizierung des Zusatzprotokolls erforderlichen Veränderungen bewenden lassen. Der Ständerat vertrat hingegen die Meinung, der bundesrätliche Entwurf könne von den zuständigen Kommissionen behandelt werden. Schliesslich schloss sich der Nationalrat dieser Auffassung an, so dass die Kommission für Rechtsfragen das Geschäft wieder aufgreifen wird. Wir begrüssen diesen Beschluss, der Verzögerungen des Projekts verhindert. Insgesamt befürworten wir den Revisionsentwurf des DSG und die Ratifizierung des Zusatzprotokolls. Allerdings hätten wir eine weitergehende Revision und eine konsequentere Annäherung an das europäische Recht gewünscht. Unseres Erachtens sollte man in mehreren Etappen vorgehen. Der Entwurf des Bundesrates bildet die Antwort auf die oben erwähnten Motionen und eine unverzichtbare Voraussetzung für die Ratifizierung des Zusatzproto-

kolls. Das Projekt beschränkt sich auf das Wesentliche. Die meisten Bestimmungen ergeben sich direkt aus der Umsetzung der beiden Motionen (Transparenz, Rechte der betroffenen Personen, Anmeldung der Datensammlungen, Aufsicht durch den EDSB, Bearbeitung im Auftrag usw.) bzw. aus der Ratifizierung des Zusatzprotokolls (grenzüberschreitende Datenflüsse, Beschwerderecht des EDSB, Aufsicht durch den EDSB). Die Revision trägt dem Vernehmlassungsverfahren weitgehend Rechnung. Wir begrüssen insbesondere die Einführung der Zertifizierung und des Datenschutz-Qualitätslabels, dank welchem die Autonomie und die Verantwortung der Inhaber von Datensammlungen erhöht und die Selbstregulierung gefördert werden. Dagegen haben wir nach wie vor Vorbehalte gegen die Regelung zu den Pilotprojekten. Wir hoffen, dass diese Frage in den Beratungen wieder aufgegriffen wird.

Zu den kritisierten Punkten des Entwurfs zählt die Informationspflicht. Es wird befürchtet, dass diese Verpflichtung zu weit gehe und eine zusätzliche Verwaltungslast schaffe. Der Gesetzesentwurf verpflichtet zur genauen Information der betroffenen Personen bei der Bearbeitung von besonders schützenswerten Personendaten und von Persönlichkeitsprofilen, wie es die Motion der Kommission für Rechtsfragen des Ständerates verlangt. Darüber hinaus sieht der Gesetzesentwurf vor, dass die Erhebung von Personendaten und die Bearbeitungszwecke für die betroffene Person erkennbar sein müssen. Mit dieser Bestimmung wird der Grundsatz von Treu und Glauben konkretisiert und das Interesse der betroffenen Personen an einem Mindestmass an Transparenz bei der Erhebung von Daten, die nicht als besonders schützenswert eingestuft werden, wiedergespiegelt. Die Transparenz sollte keine übermässigen Kosten verursachen. Der Verhältnismässigkeitsgrundsatz gilt auch in diesem Zusammenhang. Detaillierte Informationen sind nicht für jede einzelne Datenerhebung notwendig. Form und Inhalt der Information hängen von verschiedenen Kriterien ab, insbesondere von Zweck, Bearbeitungsmethoden und -umstände und von der Information, welche die betroffene Person bereits besitzt. Die Information kann in allgemeiner Form (Veröffentlichung, Internet, allgemeine Geschäftsbedingungen, standardisierte Information usw.) angeboten werden. Mehrere Unternehmen halten sich heute bereits an das Transparenzprinzip. Die Transparenz liegt nicht nur im Interesse der betroffenen Person, sondern auch im Interesse der Wirtschaft. Das Parlament hat den Transparenzbedarf in anderen Bereichen bereits anerkannt, so z.B. im Rahmen der Revision des Bundesgesetzes über den Versicherungsvertrag, der eine weitergehende Informationspflicht für die Bearbeitung von Personendaten verankert. Die Kritik, wonach die Informationspflicht zu kostspielig sei und die betroffenen Personen sich nicht für ihre Daten interessieren würden, da nur sehr wenige ihr Auskunftsrecht wahrnehmen, können wir nicht teilen. Wir erhalten täglich Anfragen von Bürgerinnen und Bürgern, die sich nach ihren Rechten erkundigen und Informationen über Bearbeitungen, die

sie betreffen, erhalten möchten. Häufig weiss der Bürger nicht, wer Daten über ihn bearbeitet und welche Rechte er besitzt. Oft hat er zu grossen Respekt vor den Inhabern von Datensammlungen und sieht davon ab, ein womöglich umständliches Verfahren in Gang zu setzen. In anderen Staaten mit einem vergleichbaren Datenschutzgesetz wird der Transparenzgrundsatz auch anerkannt. In diesen Ländern wird die Informationspflicht von den Datenbearbeitern akzeptiert und gilt als Selbstverständlichkeit. Für die Wirtschaft und für die Unternehmen ist es auch vorteilhafter, informierten Kundinnen und Kunden gegenüberzustehen. Die Transparenz fördert ausserdem das Vertrauen zwischen Unternehmen und Kundschaft.

Kritisiert werden am Revisionsentwurf auch die Aufsichtskompetenzen des EDSB im Privatsektor. Es wird befürchtet, der EDSB könnte sich in jeden Einzelfall einmischen. Diese Auslegung würde einerseits Geist und Buchstaben der vorgeschlagenen Bestimmung zuwider laufen; andererseits verfügt der EDSB gar nicht über die erforderlichen Ressourcen, um sich mit jedem Einzelfall zu befassen. Die Änderungsvorschläge sehen zwar eine Vereinfachung des Meldeverfahrens für Datensammlungen vor, statuieren aber keine neuen Befugnisse. Der EDSB kann bereits heute in die Bearbeitung von besonders schützenswerten Daten oder von Persönlichkeitsprofilen eingreifen. Häufig sind Einzelpersonen wegen fehlender Mittel nicht in der Lage, ein Verfahren einzuleiten. Der EDSB muss in Fällen mit besonderem Risiko einer Persönlichkeitsverletzung eingreifen können. Bearbeitungen von besonders schützenswerten Daten oder von Persönlichkeitsprofilen, welche eine grosse Anzahl Personen betreffen, stellen solche Fälle dar.

1.1.2 Vorschlag zum Zertifizierungsverfahren im Rahmen der laufenden Teilrevision des Bundesgesetzes über den Datenschutz

Um eine Selbstregulierung einzuführen, welche die Verantwortung des Inhabers der Datensammlung stärkt und den Wettbewerb ankurbelt, sieht das neue DSG ein Zertifizierungsverfahren für Organisationen und für Produkte vor. Die vom Bundesamt für Justiz revidierte Verordnung über das DSG sollte die wesentlichen Bedingungen verankern, welchen die Zertifizierungsstellen mit Zustimmung der Schweizerischen Akkreditierungsstelle unterliegen. Gleichzeitig arbeiten wir an einem Standardrahmen für die Evaluation des erforderlichen Datenschutzniveaus, um die Mindestanforderungen an Datenschutz-Managementsysteme zu spezifizieren.

Wir befassten uns in Zusammenarbeit mit dem Bundesamt für Justiz (BFJ), welches für die Teilrevision des DSG verantwortlich zeichnet, mit den nächsten erforderlichen Etappen zur Konkretisierung des «Zertifizierungsverfahrens». Mit der Revision des DSG sollte der Selbstregulierungsgrundsatz eingeführt werden, um die Verantwortung des Inhabers der Datensammlung zu stärken, den Wettbewerb zu beleben und den Datenschutz sowie die Datensicherheit zu verbessern. Das Projekt soll Zertifizierungsverfahren für Organisationsstrukturen, Datenverwertungsprozesse und technische Informationssysteme und -programme (d.h. Produkte) fördern; der Akzent liegt jedoch hauptsächlich auf der Zertifizierung von Organisationen, für welche die Attraktivität am grössten sein dürfte. Bei den Vorarbeiten zur Revision der DSG-Verordnung wird in enger Zusammenarbeit mit der Schweizerischen Akkreditierungsstelle (SAS) des Bundesamtes für Metrologie und Akkreditierung (METAS) über die Einführung der wesentlichen Voraussetzungen diskutiert, welchen die Zertifizierungsstellen unterliegen müssen. Hinsichtlich der spezifischeren und praktischen Aspekte des eigentlichen Zertifizierungsverfahrens – d.h. Standard-Evaluationsrahmen für das Datenschutzniveau – prüfen wir die Zweckmässigkeit der Einführung eines Referenzmodells. Das Modell könnte auf den Audit-Standard BS 7799-2:2002 mit den Spezifikationen für die Informationssicherheits-Managementsysteme (ISMS) abgestützt werden, welche auf dem internationalen Standard ISO 17799:2000 und dem Praxiskodex (CoP: 10 Kapitel mit 128 Kontrollen) für das Informationssicherheitsmanagement basieren. Im Rahmen des geplanten Datenschutzmanagementsystems (DMS) sollte der Schwerpunkt auf den Prinzipien und Methoden liegen, die den Datenschutz gewährleisten oder verbessern; dazu gehören besonders solche, die auf von nationalen oder internationalen Instanzen in ähnlichen Verfahren genutzte Modelle oder Referenzmodelle zurückgehen.

1.1.3 Übermittlung von Personendaten durch Luftfahrtgesellschaften an US- und kanadische Behörden

Die US-Behörden bieten der Schweiz die gleichen Datenschutzgarantien wie der Europäischen Union. Diese Garantien sind gegenwärtig in einer diplomatischen Note aufgeführt; sie müssen in einem bilateralen Abkommen verankert werden. Die Passagiere werden informiert, dass Daten über sie an die US-Behörden übermittelt werden. Die kanadischen Behörden gewähren der Schweiz ebenfalls die gleichen Garantien wie der Europäischen Union; diese sind bereits in einem bilateralen Abkommen aufgeführt .

In unserem 11. Tätigkeitsbericht 2003/2004 (Ziffer 1.1.2) erwähnten wir, dass die schweizerischen Behörden beschlossen hatten, Verhandlungen mit den US-Behörden aufzunehmen; Ziel war es, ein Abkommen über die Übermittlung von Passagierdaten auszuarbeiten, das die Flugverbindungen mit den Vereinigten Staaten unter Achtung der allgemeinen Datenschutzgrundsätze garantieren sollte. Im Rahmen dieser Verhandlungen haben die US-Behörden der Schweiz die gleichen Datenschutzgarantien angeboten wie der Europäischen Union. Diese Garantien werden in einem Abkommen zwischen der Europäischen Kommission und der US-Regierung aufgeführt. Für unser Land schlagen die US-Behörden einen diplomatischen Notenwechsel vor. Eine solche Gesetzesgrundlage ist mit Blick auf das DSG unzureichend. Laut Auffassung der interdepartementalen Arbeitsgruppe, in der wir auch vertreten sind, lässt sich jedoch mit dem Vorschlag der Vereinigten Staaten die Verletzung der Persönlichkeit der Passagiere stark verringern. Die Daten werden von den Luftfahrtgesellschaften übermittelt und die US-Behörden haben keinen Zugang zu den Buchungssystemen. Besonders schützenswerte Daten, z.B. über medizinische Behandlungen oder über die gewählte Verpflegung an Bord, werden nicht an die Vereinigten Staaten übermittelt. Die bekannt gegebenen Daten werden nur zur Verhütung und Bekämpfung des Terrorismus, der Verbrechen im Zusammenhang mit dem Terrorismus sowie anderer gravierender Verbrechen, besonders in der organisierten Kriminalität, verwendet. Die Datenaufbewahrung ist auf dreieinhalb Jahre befristet. In der Schweiz wohnhafte Personen können ihre Rechte in den Vereinigten Staaten direkt oder über den EDSB geltend machen. Schliesslich wird die Einhaltung der Garantien von den Behörden der beiden Länder einmal jährlich kontrolliert. Die Passagiere werden in jedem Fall vor dem Besteigen des Flugzeuges informiert, dass den US-Behörden Personendaten übermittelt werden. Wir werden in der interdepartementalen Arbeitsgruppe immer die Position vertreten, dass ein bilaterales Abkommen mit den Vereinigten Staaten ausgearbeitet werden soll, um einen ausreichenden Rechtsrahmen für die Datenübermittlungen zu schaffen.

Die kanadischen Behörden haben der Schweiz die gleichen Garantien angeboten wie der Europäischen Union. Kanada ist ausserdem bereit, ein bilaterales Abkommen mit der Schweiz abzuschliessen. Des weiteren ist zu erwähnen, dass Kanada anders als die Vereinigten Staaten über eine Datenschutzgesetzgebung verfügt, welche der schweizerischen gleichwertig ist.

1.2 Weitere Themen

1.2.1 Personenidentifikator und –register

Bund, Kantone und Gemeinden speichern Personendaten in verschiedenen Registern. Ausgehend von der Harmonisierung der Personenregister bestehen in der Schweiz seit mehreren Jahren Bestrebungen zur Einführung eines Personenidentifikators, der die Verknüpfbarkeit der vorhandenen Register erleichtern soll. Die Auswirkungen des Personenidentifikators wurden bisher jedoch weder genügend durchdacht noch politisch diskutiert. Wir haben mehrfach darauf hingewiesen, dass die mit dem Personenidentifikator zu unterstützenden Abläufe genau definiert und analysiert werden müssen, damit überhaupt sinnvolle Überlegungen zu Sicherheit und Datenschutz gemacht werden können.

Der Personenidentifikator als neu einzuführendes Verknüpfungsmittel zwischen den wichtigsten administrativen Personenregistern in unserem Land ist weiterhin Gegenstand einer Beobachtung unsererseits, insbesondere im Rahmen verschiedener Konsultationsverfahren. Die Bestrebungen, mit einem solchen Identifikator die Verknüpfung von Einträgen in Personenregistern zu erleichtern und zu automatisieren, haben ihren Anfang in der Harmonisierung der Personenregister, die vom Bundesamt für Statistik (BFS) im Hinblick auf die Volkszählung 2010 vorangetrieben wird. Dass sich aus diesen Bestrebungen datenschutzrechtliche Probleme ergeben würden, lag aus zwei Gründen von Anfang an auf der Hand. Einerseits wurden sämtliche Arbeiten im Rahmen der Registerharmonisierung unter der Arbeitshypothese ausgeführt, dass zwecks Verknüpfbarkeit eine Personennummer in die administrativen Personenregister eingefügt werde. Und andererseits wurden die grundlegenden Modelle zur Registerharmonisierung erarbeitet, ohne dass Aspekten des Persönlichkeitsschutzes Rechnung getragen worden wäre.

Schon in unseren ersten Äusserungen im Jahre 2001 hatten wir dem BFS mitgeteilt, dass für Statistikzwecke bei der Registerharmonisierung keine neuen Identifikationsmerkmale in die Administrativregister eingefügt werden dürfen. Vielmehr seien Model-

le mit Pseudonymen oder solche Methoden zu verfolgen, wie sie in der medizinischen Statistik der Krankenhäuser schon erfolgreich erprobt worden sind. Wie alle unsere weiteren Äusserungen wurde auch diese Anregung im Vorhaben Registerharmonisierung nicht berücksichtigt.

In der Zwischenzeit ist das Vorhaben «Personenidentifikator» formell von demjenigen der Registerharmonisierung losgelöst worden. Beide bleiben jedoch sehr eng miteinander verbunden, sowohl inhaltlich, als auch, was den zeitlichen Druck betrifft, unter welchem die beiden im Hinblick auf die näher rückende Volkszählung 2010 voran getrieben werden.

Der im Frühjahr 2004 vom BFS vorgelegte Entwurf gab vor, die Datenschutzprobleme mittels sogenannter «sektorieller» Personenidentifikatoren zu lösen. Nun verhält es sich aber so, dass die dort genannten sechs Sektoren in der Realität der Verwaltungspraxis gar nicht existieren. Zudem ist es auch gar nicht denkbar, derartige voneinander getrennte Sektoren zu schaffen. Einer der Gründe dafür ist, dass ein Grossteil der Personenregister durch die Kantone und Gemeinden nach deren Regeln geführt wird und es unrealistisch ist anzunehmen, der Bund könne von ihnen unter dem Titel «Registerharmonisierung» die Aufspaltung solcher Register verlangen. Es zeigt sich somit, dass die Sektorialisierung keine wirkliche Lösung der datenschutzrechtlichen Probleme darstellt. Daher erstaunt auch nicht, dass die sektoriellen Personenidentifikatoren im Vernehmlassungsverfahren schlechtes Echo bekommen haben und inzwischen wieder aus dem Vorhaben herausgenommen worden sind.

Wir haben dem BFS zur erwähnten Vorlage zwei Stellungnahmen zukommen lassen, welche abgesehen von den Bemerkungen zu den Sektoren weiterhin Gültigkeit behalten. In diesen Stellungnahmen haben wir insbesondere kritisiert, dass auch in der aktuellen Version des Vorhabens – das zu schaffende Verknüpfungsmittel heisst jetzt «Personenidentifikator Bevölkerung» – Überlegungen zu den Risiken, welche mit der Verknüpfbarkeit der Register und mit ihrer elektronischen Vernetzung geschaffen werden, fehlen. Man geht offenbar davon aus, dass gar keine Risiken für den Persönlichkeitsschutz entstehen, weil bloss die «Automatisierung der bestehenden gesetzlich geregelten Datenkommunikationsprozesse» angestrebt werde. Diese Darstellung übersieht jedoch den fundamentalen Unterschied zwischen der traditionellen Papierwelt und der «e-Welt». Denn wenn tatsächlich neue Datenflüsse verhindert werden sollten, müsste vor der Automatisierung die Gesamtheit der betroffenen kantonalen Register genauestens nach Regeln des Bundes entflochten werden. Beispielsweise dürfte es nicht sein, dass ein Kanton Einwohnerregister zusammen mit anderen Registern in derselben Datensammlung führt.

Auf gesetzlicher und verfassungsrechtlicher Ebene haben wir im Wesentlichen drei Punkte kritisiert: Einerseits ist es fraglich, ob ein Personenidentifikator, der für statistische Zwecke geschaffen wird und für den eine ausreichende Verfassungsgrundlage besteht, auch für administrative Zwecke genutzt werden darf. Unserer Meinung nach wird damit auf Bundesebene eine neue Kompetenzordnung geschaffen, welche einer verfassungsmässigen Grundlage bedarf. Mit den vorliegenden Entwürfen würde immerhin ein virtuelles gesamtschweizerisches Bevölkerungsregister geschaffen. Ein zweiter Kritikpunkt liegt darin, dass keiner der bisher entwickelten Entwürfe dem Legalitätsprinzip genügt, weil auf Gesetzesstufe kein ausreichender Grad an Konkretisierung erreicht wird. Es geht aber nicht an, die Analyse und Beschreibung der Abläufe, welche durch elektronische Vernetzung und Personenidentifikator unterstützt werden sollen, zu überspringen und Entscheide von grösster Tragweite einfach an den Verordnungsgeber zu delegieren. Drittens ergeben sich aus dem verfassungsmässigen Persönlichkeitsschutz bestimmte Voraussetzungen für die Einführung eines eidgenössischen Personenidentifikators. Diese hat Prof. Dr. G. Biaggini in einem von uns in Auftrag gegebenen Gutachten (http://www.edsb.ch/d/themen/weitere/epid/gutachten-biaggini.pdf) wie folgt formuliert: «Die Einführung eines koordinierten eidgenössischen Personenidentifikators darf, in Anbetracht der im verfassungsrechtlichen Persönlichkeitsrecht verankerten Schutzanliegen, nicht ohne flankierende Schutzmassnahmen erfolgen, die dafür sorgen, dass die [...] Gefahren soweit möglich gebannt werden. Ein Handlungsbedarf ist um so mehr zu bejahen, als es der Staat selbst ist, der durch Einführung eines Personenidentifikators die fraglichen Gefahren bzw. Gefährdungspotenziale schafft. Da es sich um einen Personenidentifikator handelt, den der Bund einführen will, ist mit ‚Staat' hier in erster Linie der Bund angesprochen. Zwar stehen auch die Kantone und Gemeinden durchaus in der Pflicht, denn Art. 35 BV spricht alle staatlichen Ebenen an. Der Bund als Urheber steht jedoch in einer gesteigerten Verantwortung, der er sich nicht einfach durch ‚Weiterdelegation' an die Kantone oder Gemeinden und deren Organe (Gesetzgeber, andere Behörden) entziehen darf.» Genau dies wird aber in den bisherigen Entwürfen getan, indem den Kantonen durch eine Delegation ohne materielle Schranken die verwaltungsinterne Verwendung des Personenidentifikators gestattet werden soll. Im Übrigen verunmöglicht ein derartiges Vorgehen jegliche Zweckbindung von Anfang an.

Aufgrund des Gesagten bleiben wir bei unserer Beurteilung, wonach hier eine Infrastruktur geschaffen werden soll, welche nebst massiven finanziellen Konsequenzen auch erhebliche Risiken für den Persönlichkeitsschutz mit sich bringt. Angesichts dieser Bedeutung müssen die Projekte zuerst genügend konkretisiert werden, damit eine politische Diskussion und Entscheidungsfindung überhaupt möglich wird.

2 Datenschutzfragen allgemein

2.1 Datenschutz und Datensicherheit

2.1.1 Erforderliche Elemente eines Bearbeitungsreglements

Wir bekommen immer wieder von vielen Seiten die Anfrage, was in einem Bearbeitungsreglement aufgeführt werden muss. Deshalb haben wir ein Musterinhaltsverzeichnis erstellt, aus dem ersichtlich ist, was in ein solches Reglement gehört.

Das Bearbeitungsreglement soll für die notwendige Transparenz im Umfeld sowohl der Systementwicklung als auch der Datenbearbeitung sorgen. Die erste Version des Bearbeitungsreglements ist Ende der Projektplanungsphasen verfügbar und wird während des Systembetriebs nachgeführt. Insbesondere Systemänderungen sowie die Durchführung von Kontrollen sind in der Betriebsphase zu dokumentieren. Das Bearbeitungsreglement ist in möglichst kurzer und verständlicher Form zu führen, so dass das System auch von Nichtexperten verstanden bzw. beurteilt werden kann. Es gilt der Grundsatz: «Soviel wie nötig und so wenig wie möglich». Für detailliertere Informationen ist auf andere Dokumente zu verweisen. Insbesondere der Inhaber der Datensammlung soll sich aufgrund dieses Reglements eine Übersicht über die Systeme oder Anwendungen verschaffen können, die auf die jeweiligen Datensammlungen Zugriff haben. Das Reglement soll ausdrücklich den Zweck des Systems deutlich machen. Ausserdem sind die Informationsflüsse festzuhalten; diese sollen aufzeigen, welche Informationen vom systembetreibenden Organ (Inhaber der Datensammlung) mit anderen Organen wann, wie und in welcher Art ausgetauscht werden. Zusätzlich ist auch die Organisation zu dokumentieren. Einerseits verstehen wir darunter das Organigramm des systembetreibenden Organs sowie die Bereiche – inkl. der Anzahl Mitarbeitenden –, in denen mit dem System gearbeitet wird. Andererseits sollen aber auch die Verantwortlichkeiten festgehalten werden.

Ein weiterer wichtiger Bereich der Dokumentation der Organisation sind die Prozesse bzw. Abläufe. Je sensitiver die Datenbearbeitung ist, um so detaillierter sind die Prozesse aufzuführen. Die Dokumentation der herkömmlichen Aufgabenerfüllungsprozesse beginnt bei der Erhebung der Daten und endet bei ihrer Archivierung oder Löschung.

Im Weiteren sollen auch die Kontrollprozesse sowie die Prozesse der Auskunftserteilung festgehalten werden. Zusätzlich sind noch die Konfiguration der Informatikmittel und die technischen und organisatorischen Datensicherheitsmassnahmen aufzuführen. Bei den Sicherheitsmassnahmen ist festzuhalten, wie diese umgesetzt werden.

Das detaillierte Inhaltverzeichnis eines Bearbeitungsreglements kann von unserer Website heruntergeladen werden (http://www.edsb.ch/d/doku/leitfaeden/tom/bearbeitungsreglement.pdf).

2.1.2 Praktische Erfahrungen mit elektronischen Spuren

Im Anschluss an unsere Darlegung der korrekten Behandlung von elektronischen Spuren am Arbeitsplatz haben wir unsere Arbeiten in diesem Bereich fortgesetzt und die elektronischen Spuren analysiert, welche die Mitarbeiter des EDSB bei am Computer durchgeführten Tätigkeiten hinterlassen. Mit dieser Bestandsaufnahme konnten wir die Nützlichkeit der gesammelten Daten überprüfen und gleichzeitig die Systemadministratoren für die Datenschutzaspekte sensibilisieren.

Elektronische Spuren und besonders Log-Dateien geben Aufschluss darüber, «wer was wann gemacht hat», und machen es möglich, eine Fehlerquelle oder die Herkunft eines Virus zu entdecken oder nach grösseren Pannen (mit einer Sicherheitskopie) den Datenbestand wiederherzustellen. Der Nutzen der elektronischen Spuren steht ausser Zweifel, und die Legitimität der Sammlung der Spuren liegt auf der Hand.

Allerdings wird das Risiko einer durch elektronische Spuren verursachten Persönlichkeitsverletzung gerade am Arbeitsplatz bisweilen ausser Acht gelassen. Die Bearbeitung von elektronischen Spuren, die Personendaten enthalten, unterliegt dem Bundesgesetz über den Datenschutz. Wir haben in Absatz 2.1.3 unseres 11. Tätigkeitsberichts die korrekte Behandlung von elektronischen Spuren beschrieben (siehe auch http://www.edsb.ch/d/themen/sicherheit/technik/elektronische_spuren_d.pdf).

Der nächste Projektschritt bestand darin, die Ratschläge umzusetzen und eine Bestandsaufnahme vorzunehmen. Wir analysierten zunächst die elektronischen Spuren, die im Rahmen unserer eigenen Aktivitäten gesammelt wurden. Wegen der besonderen Organisation unserer Informatik mussten zwei Drittstellen beteiligt werden, die jeweils für einen Teil der gesammelten elektronischen Spuren verantwortlich sind.

Das Experiment zeigte, dass es durchaus möglich ist, die erteilten Ratschläge zu befolgen. Mit vertretbarem Aufwand und dank der Kooperation der zwei Drittstellen konnte eine vollständige Liste der gesammelten elektronischen Spuren erstellt werden.

Der aktuelle Informationsstand führte zur Feststellung, dass einige Spuren nicht wirklich nützlich sind (z.B. die Liste der komprimierten und dekomprimierten Dateien) und dass dagegen andere verwertbare Ereignisse wie beispielsweise die Änderung der Benutzerpasswörter keine Spuren generieren. Wir werden unsere Nachforschungen fortsetzen und versuchen, die festgestellten Mängel zu beheben.

2.1.3 Die Auswirkungen von «Pervasive Computing» auf die Privatsphäre

Das nächste Jahrzehnt wird voraussichtlich im Zeichen des «Pervasive Computing» stehen. Damit steigt die Gefahr von Persönlichkeitsverletzungen. Um eine ausgewogene, realistische und optimale Lösung zu finden, wird die Zusammenarbeit mit Fachleuten dieses Bereichs empfohlen.

«Pervasive Computing» («Ubiquitous Computing») ermöglicht eine Fülle von sehr nützlichen Anwendungen. Mit Technologien wie RFID (Radio Frequency Identification), GPS (Global Positioning System) oder UMTS (Universal Mobile Telecommunications Systems) lassen sich z.B. Applikationen entwickeln, mit denen das Autodiebstahlrisiko verringert oder ein Lager effizienter bewirtschaftet werden kann. «Pervasive Computing» beinhaltet allerdings auch das Risiko von Persönlichkeitsverletzungen. Mit Technologien wie GPS lassen sich z.B. auch die Bewegungen einer Person mitverfolgen bzw. nachvollziehen.

Die beste Prävention von Datenschutzproblemen besteht darin, sie zu begrenzen oder zu vermeiden, indem z.B. die Menge der bearbeiteten Personendaten verringert wird. Dazu ist es wichtig, die erkannten Risiken vorwegzunehmen und möglichst proaktiv zu handeln. Wir haben ein Projekt zur Evaluation der Risiken und Perspektiven dieser Entwicklungen in die Wege geleitet.

In der ersten Projektphase verbesserten wir unser Know-how, indem die verschiedenen existierenden Applikationen entsprechend den verschiedenen verwendeten Technologien klassifiziert wurden. Ausserdem wurden für jede identifizierte Applikation die potenziellen Datenschutzrisiken ermittelt und nach Grad der Persönlichkeitsverletzung analysiert und klassifiziert. Damit möchten wir einen Gesamtüberblick erzielen. In der zweiten Projektphase sollen die Ergebnisse in Zusammenarbeit mit den Fachleuten dieses Bereichs konsolidiert werden. Nur ein multidisziplinärer Ansatz kann zu einer ausgewogenen, rationellen und mithin optimalen Lösung führen.

2.1.4 Verbesserung des Datenschutzes mittels Verschlüsselung von SMS-Kurzmitteilungen

Die bisweilen missbräuchliche Überwachung der Telekommunikationskanäle stellt eine wesentliche Persönlichkeitsverletzung dar. Die Menge der gesendeten SMS hat in den letzten Jahren stark zugenommen, ohne dass den Benutzerinnen und Benutzern Schutzmöglichkeiten zur Verfügung gestellt worden wären. Wir haben in Zusammenarbeit mit einem finnischen Forscher die Experimentierversion einer Anwendung für die Verschlüsselung von SMS-Nachrichten getestet und sind zur Auffassung gelangt, dass sich diese Technik für ein breites Publikum eignet.

Während der letzten fünf Jahre ist die Menge der per SMS übermittelten Personendaten exponentiell angestiegen. In der Folge ist auch das Interesse am Zugriff auf diese Daten und die Gefahr einer Persönlichkeitsverletzung grösser geworden.

Deshalb forschten wir nach Lösungen für das Problem. Wir suchten nach einer Verschlüsselungsanwendung; damit können die Daten in eine für etwaige Hacker unverständliche Form umgewandelt und das Problem an der Wurzel gepackt werden. Nach einigen Nachforschungen entschieden wir uns für eine von finnischen Forschern entwickelte Anwendung. Die Applikation namens «SafeSMS» ist in Java-Programmiersprache geschrieben und mit modernen Mobiltelefonen kompatibel (MIDP 2.0). Die getestete Version ist aber für eine breite Verteilung noch nicht ausgereift, weil zuerst kleinere Fehler behoben werden müssen und die Benutzerfreundlichkeit verbessert werden muss. Mit unseren Tests soll im Wesentlichen bewiesen werden, dass eine robuste Verschlüsselung von SMS in vernünftiger Ausführungszeit (einige Sekunden) möglich ist. Der Verschlüsselungsalgorithmus Blowfish bietet ein ausreichendes Sicherheitsniveau, sofern ein genügend komplexer Schlüssel gewählt wird. Zusätzlich planen die Entwickler eine AES-Version (Advanced Encryption Standard). Da es sich um eine symmetrische Verschlüsselung handelt, müssen sich die beiden Kommunikationspartner auf ein gemeinsames geheimes Passwort einigen. «SafeSMS» ermöglicht es, ein Telefonverzeichnis der Kommunikationspartner mit ihren jeweiligen Passwörtern anzulegen. Das Verzeichnis wird mit einem nur dem Besitzer bekannten Hauptpasswort geschützt. Neben der Geschwindigkeit bietet die symmetrische Verschlüsselung den Vorteil, dass sie keine Public Key Infrastructure (PKI) erfordert, die sehr komplex ist und deshalb kurzfristig nicht in Betracht kommt.

Die Entwicklung solcher Verschlüsselungsanwendungen kann ausgezeichnete Möglichkeiten für den Schutz von Personendaten erschliessen. Wir werden deshalb die Fortschritte in diesem Bereich weiterverfolgen.

2.2 Weitere Themen

2.2.1 Datenschutzrechtliche Probleme bei der Umsetzung der Armee XXI

Im Rahmen der Umsetzung der Armee XXI haben wir das VBS ver-schiedentlich darauf hingewiesen, dass es in zahlreichen Bereichen an hinreichenden gesetzlichen Grundlagen für eine Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen fehlt. Das VBS beabsichtigt auch in Zukunft, sensible Personendaten ohne genügende gesetzliche Grundlagen zu bearbeiten.

In unserem letzten Tätigkeitsbericht haben wir den Einsatz des medizinisch-psychologischen Fragebogens bei der Rekrutierung von Stellungspflichtigen aus dem Blickwinkel des Datenschutzes beurteilt (s. unseren 11. Tätigkeitsbericht 2003/2004; Ziffer 2.2.1). In diesem Jahr haben wir zu verschiedenen Verordnungsentwürfen des VBS (u.a. zur Teilrevision des militärischen Kontrollwesens VmK oder zur Totalrevision der Verordnung über die medizinische Beurteilung der Diensttauglichkeit und Dienstfähigkeit VMBDD) Stellung genommen, die im Rahmen der Umsetzung der Armee XXI dem Bundesrat zur Annahme unterbreitet worden sind.

Dabei zeigten sich aus datenschutzrechtlicher Sicht stets die gleichen Probleme:

Einerseits fehlen für die Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen die vom Datenschutzgesetz geforderten hinreichenden Grundlagen im Militärgesetz (Verstoss gegen das Legalitätsprinzip). Anderseits sind die vom VBS ausgestalteten Verordnungen inhaltlich ungenügend konkretisiert: Die Bestimmungen zur Datenbearbeitung sind jeweils zu ungenau und unvollständig (Verstoss gegen das Legalitäts- und Transparenzprinzip). Unter anderem verzichtet das VBS neuerdings darauf, in den Anhängen zu den Verordnungen einen ausführlichen Datenkatalog, die Zugriffberechtigungen und die Bearbeitungsmodalitäten aufzuführen.

Nachdem wir mehrmals interveniert haben, teilte uns das Generalsekretariat des VBS mit, dass das Departement am gegenwärtigen Vorgehen festhalten und auch in naher Zukunft davon absehen werde, genügende formell-rechtliche Grundlagen für die Bearbeitung von besonders schützenswerten Personendaten zu schaffen. Zudem beabsichtige das VBS, «vorerst *nötigenfalls* auf Verordnungsstufe materiell-rechtliche Grundlagen zu schaffen und *gegebenenfalls* das Militärgesetz im Rahmen der nächsten Revision zu ergänzen.»

Besonders gravierend ist, dass das VBS die Missachtung des Legalitätsprinzips billigt und die Verletzung der Persönlichkeit der Angehörigen der Armee bewusst akzeptiert. Wir haben daher wiederholt gefordert, dass mit der Schaffung von ausreichenden Grundlagen im Militärgesetz nicht bis ins Jahr 2009 zugewartet, sondern umgehend eine vorgezogene Teilrevision des Militärgesetzes durchgeführt wird. Das VBS lehnt dies weiterhin ab. Immerhin hat uns das Generalsekretariat zugesichert, dass künftig die Anhänge zu den Verordnungen wieder einen vollständigen Datenkatalog mit den Bearbeitungsmodalitäten und den Zugriffsberechtigungen aufweisen werden.

2.2.2 Einige Datenschutzaspekte bei der Verwendung von biometrischen Daten im Privatsektor

Die Biometrie hat sich stark verbreitet und hält heute in der ganzen Zivilgesellschaft in automatisierten Authentifizierungs- und Identifizierungsverfahren Einzug: vom Zugang zu Schulkantinen über die Bezahlung von Fahrkarten, Arbeitszeit- und Anwesenheitskontrollen bis zur Zugangskontrolle zu Installationen oder Informatiksystemen. Der Einsatz der Biometrie beinhaltet Risiken für die Grundrechte und -freiheiten und hat sich zu einer grossen Herausforderung für den Datenschutz entwickelt. Der EDSB schlägt verschiedene Prinzipien vor, die im Bereich des Datenschutzes beachtet werden müssen.

In einem Bericht, der anlässlich der 26. Internationalen Konferenz der Datenschutzbeauftragten unterbreitet wurde (siehe Ziffer 9.2.2 und http://www.edsb.ch/d/doku/fachpresse/index.htm), schlugen wir einige Grundsätze vor, die zur Gewährleistung des Datenschutzes bei der Verwendung von biometrischen Daten beitragen sollen. Der Einsatz der Biometrie kann besonders im Zusammenhang mit der Kontrolle von Einzelpersonen und mit der Zusammenführung von Informationen und Dateien erhebliche Datenschutzrisiken beinhalten. Mögliche Vorteile der Biometrie dagegen liegen namentlich in der Sicherung des Datenzugriffs. Die Biometrie könnte sich so zu einem Instrument im Dienst des Schutzes der Privatsphäre entwickeln. Allerdings bildet die Biometrie kein Patentrezept für alle Kontroll- und Verwaltungsprobleme. Biometrische Verfahren weisen hinsichtlich der Verlässlichkeit der Ergebnisse (unrichtige Ablehnung oder Annahme) und der Datensicherheit Fehler und Schwächen auf. Der Einsatz der Biometrie kann ausserdem zu Diskriminierungen führen und die Menschenwürde beeinträchtigen (siehe Ziffer 9.2.2). Deshalb sollten bei der Verwendung von biometrischen Angaben im Privatsektor die folgenden Grundsätze berücksichtigt werden:

- Die Biometrie wird nur eingesetzt, wenn sich das angestrebte Ziel nicht mit weniger einschneidenden Mitteln erreichen lässt.
- Die Biometrie kann zum Ziel des Datenschutzes und der Datensicherheit eingesetzt werden.
- Die Zweckbindung der Bearbeitung muss streng eingehalten werden.
- Die betroffenen Personen müssen klar informiert und in das Bearbeitungsverfahren einbezogen werden.
- Biometrische Daten müssen direkt bei der betroffenen Person bzw. zumindest mit deren Wissen gesammelt werden.
- Zur Vermeidung von Diskriminierungen müssen für Personen, welche nicht in der Lage sind, ein biometrisches System zu benutzen, Alternativen vorgesehen werden.
- Biometrische Daten dürfen nur durch den Vergleich mit einer bei der betroffenen Person erhobenen Probe identifiziert werden.
- Die biometrischen Originaldaten müssen nach der Durchführung des Registrierungsverfahrens vernichtet werden.
- Die Technologien sollten nicht auf der Speicherung von Rohdaten basieren, sondern auf derjenigen von Templates sowie auf der Verwendung von biometrischen Daten, für welche keine Templates in einer Datenbank gespeichert werden müssen, die von einer anderen Bearbeitungsstelle als der betroffenen Person selbst verwaltet wird. Dieses Verfahren wirft grundsätzlich keine Datenschutzprobleme auf, sofern das Template auf einem ausschliesslich von der betroffenen Person verwendeten Medium gespeichert wird (Chipkarte, Mobiltelefon, tragbarer Computer usw.).
- Wenn eine Datenbank von einer anderen Bearbeitungsstelle als der betroffenen Person abgefragt und verwaltet wird, kann das gewählte biometrische Element Konsequenzen für die Grundfreiheiten und -rechte haben. Das ist der Fall, wenn das biometrische Element Spuren hinterlässt (z.B. Fingerabdruck). Der Einsatz solcher Elemente muss einem überwiegenden Sicherheitsinteresse entsprechen.
- Mangels eines solchen Interesses müssen biometrische Elemente eingesetzt werden, die das Missbrauchsrisiko beschränken und keine Spuren hinterlassen (z.B. der Handumriss).

- Beim Einsatz von Elementen, die Spuren hinterlassen und die in einer Datenbank gespeichert sind, muss die Zweckentfremdung mit den erforderlichen Massnahmen vermieden werden. So sollte z.B. das in der Datenbank enthaltene Element mithilfe des Template verschlüsselt werden, so dass die Entschlüsselung nur in Anwesenheit der Person, auf welche sich die biometrische Information bezieht, möglich ist. Das Template muss applikationsspezifisch sein, um die Möglichkeit von Datenverbindungen bzw. des Zugriffs auf verschiedene Applikationen auszuschliessen.

- Die Verwendung der biometrischen Information als universelle Benutzeridentifikation muss mit den erforderlichen Massnahmen vermieden werden.

- Aus biometrischen Daten dürfen sich keine weiteren Angaben zur betroffenen Person, insbesondere über ihren Gesundheitszustand, ableiten lassen.

- In einem Authentifizierungs-(Verifizierungs-)System sollen nur diejenigen Personendaten gesammelt und bearbeitet werden, die zur Authentifizierung erforderlich sind. Bei den gewählten Lösungen sollte die Identität der Person nicht enthüllt werden (anonyme Authentifizierung), ausser wenn der Bearbeitungszweck eine Identifizierung erfordert (Grundsatz der Wirtschaftlichkeit der Bearbeitung).

- In einem Authentifizierungssystem dürfen die biometrischen Daten nicht zu anderen als zu Verifikationszwecken verwendet werden, ausser wenn das Gesetz es ausdrücklich vorsieht (insbesondere im Rahmen einer Strafverfolgung).

- Um die Datensicherheit zu verbessern und das Risiko eines unbefugten Zugriffs – besonders durch die Aneignung der Daten Dritter – zu verringern, muss das biometrische System durch weitere Identifizierungs- oder Authentifizierungsmittel (z.B. Zugangscode) geschützt werden. Ausserdem werden gesicherte biometrische Lesegeräte empfohlen, in welche die befugten Personen ihre Daten direkt eingeben können, bzw. der Einsatz von Systemen, bei denen die biometrischen Daten in einem gesicherten Medium wie z.B. einer Chipkarte integriert sind.

- Biometrische Daten müssen gleich bei der Registrierung verschlüsselt werden, ebenso wie ihre elektronische Übermittlung, insbesondere in einem Netzwerk.

- Die Verlässlichkeit von gespeicherten biometrischen Daten (Templates) muss regelmässig überprüft werden (mittels periodischer Neuregistrierung), da sich die für eine Person erfassten biometrischen Merkmale im Laufe der Zeit verändern können.

- Die Rechte der betroffenen Personen müssen gewährleistet werden. Sie müssen die Nutzung ihrer biometrischen Daten kontrollieren und gegebenenfalls die Vernichtung beantragen können.

- Biometrische Informationssysteme sollten einem Zertifizierungsverfahren und einem Datenschutz-Audit unterliegen. Ausserdem müssen die Systeme vor der Inbetriebnahme auf allfällige Risiken überprüft werden. Dazu sollte ein Schutzkonzept entwickelt werden, welches insbesondere die Bearbeitungsprozesse definiert.

Zur Verwendung von biometrischen Daten im Privatsektor s. auch Ziffer 7.2 des vorliegenden Tätigkeitsberichts.

2.2.3 Gesetzesentwurf über die geografische Information

Im Rahmen der Umsetzung des Gesetzes über die geografische Information und der Ausarbeitung von Vollzugsverordnungen müssen mehrere datenschutzrechtlich wesentliche Aspekte wie z.B. Transparenz der Bearbeitungen, Zweckbindung, klare Regelung der Bekanntgabe von Personendaten oder Garantie der Rechte der betroffenen Personen berücksichtigt werden.

Anlässlich der Vernehmlassung zum Gesetzesentwurf über die geografischen Informationssysteme riefen wir dem Bundesamt für Landestopographie in Erinnerung, dass im Rahmen der Umsetzung des Gesetzes und der Ausarbeitung von Vollzugsverordnungen mehrere datenschutzrechtlich relevante Aspekte berücksichtigt werden müssen. Bei der Realisierung und Nutzung eines geografischen Informationssystems (GIS), das Personendaten umfasst bzw. leicht mit solchen Daten in Verbindung gebracht werden kann, muss das DSG beachtet werden.

Ausserdem muss auf die *Transparenz der Datenbearbeitung* geachtet werden. Dazu müssen die betroffenen Personen über den Zweck des Systems, die Kategorien der bearbeiteten Daten, die Benutzer des Systems und die Empfänger der Informationen informiert werden; die betroffenen Personen müssen ihre Rechte geltend machen können, namentlich über das Auskunftsrecht.

Der *Zweck* des GIS muss *definiert, spezifisch und gerechtfertigt* sein und die Daten müssen diesem Zweck entsprechend bearbeitet werden. So muss ein GIS, das für Anwendungen konzipiert ist, die sich nicht auf bestimmte Personen beziehen, oder das der Allgemeinheit zugänglich sein soll, Mechanismen enthalten, welche die Verknüpfung mit Personendaten begrenzen oder verunmöglichen. Damit kann die Anonymität der Personen bei der Publikation oder Verbreitung der Daten gewährleistet werden.

Der *Katalog der bearbeiteten Daten* muss *definiert* werden. Nur die für den Zweck des GIS notwendigen Daten dürfen gesammelt und bearbeitet werden. Es sollte so weit wie möglich darauf verzichtet werden, Daten zu bestimmten oder bestimmbaren Personen in das System einzuspeisen.

Die *Datenqualität* muss *gewährleistet* sein (Richtigkeit, Aktualisierung, begrenzte Aufbewahrungsdauer).

Die *Bekanntgabe von Personendaten* und insbesondere ihre Verbreitung oder Publikation durch ein Abrufverfahren muss *klar geregelt* sein.

Der rechtliche Rahmen muss von *technischen und organisatorischen Massnahmen* begleitet sein, damit unbefugte Zugriffe vermieden werden bzw. das Risiko einer nicht gerechtfertigten Identifizierung von Personen verhindert wird.

Die *Rechte der betroffenen Personen* müssen *gewährleistet* sein, insbesondere das Recht auf vorgängige Information, das Auskunftsrecht für Daten, welche sie betreffen, und das Recht, sich der systematischen Sammlung und Bearbeitung der Daten zu kommerziellen Zwecken anhand von Bildern der Wohnumgebung zu widersetzen.

Die Grundsätze des Datenschutzes müssen bei der Entwicklung der GIS einbezogen werden. Die Technologien sollten die wirksame Umsetzung der gesetzlichen Erfordernisse fördern. Dies bedingt, dass die Verantwortlichen für die Datenbearbeitung die notwendigen Kenntnisse erwerben, um bei der Realisierung ihrer Projekte die Datenschutzaspekte von Anfang an einbeziehen zu können. Dazu muss ein Datenschutzkonzept für die Entwicklung eines GIS erarbeitet werden.

3 Justiz/Polizei/Sicherheit

3.1 Polizeiwesen

3.1.1 Nachträgliche Information der betroffenen Personen im Polizeibereich

Im Polizeibereich führten wir eine Sachverhaltsabklärung betreffend die gesetzlich vorgesehene nachträgliche Information der Personen, über die Daten bearbeitet werden, durch. Dabei mussten wir feststellen, dass bis zum Zeitpunkt unserer Abklärung noch nie eine nachträgliche Information stattgefunden hatte. In einem Fall muss das Bundesamt für Polizei noch ein Konzept für die Umsetzung der gesetzlichen Bestimmung erarbeiten. In einem zweiten Fall wurden in der Zwischenzeit bereits ein paar Personen informiert.

In unserer Kompetenz als Aufsichtsorgan über die Bundesorgane entschieden wir, betreffend die nachträgliche Information im Polizeibereich beim Bundesamt für Polizei (BAP) eine Sachverhaltsabklärung durchzuführen). Dabei können zwei Fälle unterschieden werden:

Der eine Fall betrifft die Bearbeitung von Personendaten in den Datenbanken JANUS (unter anderem organisierte Kriminalität, illegaler Drogenhandel, Falschmünzerei, Menschenhandel und Geldwäscherei) und GEWA (Datenbank der Meldestelle für Geldwäscherei). Hier muss die Beschaffung von Personendaten durch das BAP für die betroffenen Personen nicht erkennbar sein, sofern der Zweck der Strafverfolgung Geheimhaltung erfordert. Allerdings muss in diesen Fällen die betroffene Person nachträglich darüber informiert werden, sofern nicht wichtige Interessen der Strafverfolgung dem entgegenstehen oder die nachträgliche Mitteilung mit einem unverhältnismässigen Aufwand verbunden wäre. Diese erste Art der nachträglichen Information ist in Art. 14 Abs. 1 ZentG (Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes) geregelt.

Der zweite Fall betrifft ebenfalls die bereits erwähnten Datenbanken JANUS und GEWA sowie zusätzlich die Datenbank ISIS (präventiver Staatsschutz). Dabei geht es um Personen, die ein so genanntes indirektes Auskunftsgesuch gestellt haben und in einem oder in mehreren der erwähnten Informationssysteme registriert waren bzw. sind. Gemäss Gesetz wird beim Dahinfallen der Geheimhaltungsinteressen zur Wahrung der inneren Sicherheit bzw. beim Dahinfallen der Interessen der Strafverfolgung

an der Geheimhaltung, spätestens bei Ablauf der Aufbewahrungsdauer, nach Massgabe des Datenschutzes Auskunft erteilt, sofern dies nicht mit unverhältnismässigem Aufwand verbunden ist. Diese Art der nachträglichen Information der betroffenen Personen ist in Art. 18 Abs. 6 BWIS (für ISIS) und in Art. 14 Abs. 4 ZentG (für JANUS und GEWA) geregelt.

Wir wollten wissen, wie das BAP diese genannten Fälle der nachträglichen Information in die Praxis umsetzt. Wir kündigten dem BAP unsere Sachverhaltsabklärung an und stellten gleichzeitig verschiedene Fragen. Kurze Zeit später führten wir eine Besichtigung vor Ort durch.

Wir haben festgestellt, dass die nachträgliche Information gemäss Art. 14 Abs. 1 ZentG (erster Fall) nie angewendet wurde, da sie gemäss BAP mit unverhältnismässigem Aufwand verbunden gewesen wäre. Ebenfalls wurde niemand gemäss Art. 14 Abs. 4 ZentG und Art. 18 Abs. 6 BWIS (zweiter Fall) nachträglich informiert. Die Begründung betreffend ISIS lautete, das BAP sei der Auffassung gewesen, dass die Geheimhaltungsinteressen noch bestünden; als Begründung betreffend JANUS wurde angeführt, die Bestimmung könne technisch noch nicht umgesetzt werden.

Daraufhin richteten wir Empfehlungen an das BAP. Betreffend Art. 14 Abs. 1 ZentG verlangten wir, dass das BAP ein Verfahren bzw. Konzept ausarbeite, damit die nachträgliche Information gemäss Gesetz in die Praxis umgesetzt werden kann. Zudem forderten wir eine rückwirkende Überprüfung aller Fälle seit Einführung der gesetzlichen Bestimmung. Betreffend Art. 14 Abs. 4 ZentG und Art. 18 Abs. 6 BWIS ersuchten wir das BAP um nochmalige Überprüfung sämtlicher Fälle in den Datenbanken, bei denen eine Person ein indirektes Auskunftsgesuch gestellt hatte und tatsächlich registriert war.

Im Zusammenhang mit der Umsetzung von Art. 14 Abs. 1 ZentG wird das BAP ein Konzept ausarbeiten und uns dieses unterbreiten. In Bezug auf die nachträgliche Information der Personen, die ein indirektes Auskunftsgesuch gestellt haben, hat das BAP unsere Empfehlungen betreffend der entsprechenden Gesetze akzeptiert. Was Art. 14 Abs. 4 ZentG und Art. 18 abs. 6 BWIS anbelangt, so wird die technische Umsetzung aller unserer Forderungen gemäss Angaben des BAP noch etwas Zeit beanspruchen. Allerdings sollte dies noch im Jahr 2005 erfolgen.

3.1.2 Botschaft zum Europol-Abkommen

Wir konnten zum Abkommen zwischen der Schweiz und Europol Stellung nehmen. Dabei bemängelten wir, dass aus der Botschaft nicht ersichtlich ist, aus welchen schweizerischen Datenbanken Daten an Europol weitergegeben werden. Ausserdem muss die Botschaft aufzeigen, ob für jede betroffene Datenbank im Schweizer Recht eine gesetzliche Grundlage bereits besteht oder noch zu schaffen ist. Unbestritten ist, dass der EDSB in Sachen Europol als unabhängige nationale Kontrollinstanz gelten.

Aufgrund der laufenden Verhandlungen zu den Bilateralen II kam es seitens der Europäischen Union zu einer Blockierung des Abkommens zwischen der Schweizerischen Eidgenossenschaft und dem Europäischen Polizeiamt (Europol-Abkommen). Nach einer rund zweijährigen Pause wurde das Abkommen zwischen der Schweiz und Europol am 24. September 2004 unterzeichnet. Anschliessend konnten wir im Rahmen der Ämterkonsultation zur Botschaft zum Europol-Abkommen Stellung nehmen.

Zunächst nahmen wir mit Genugtuung zur Kenntnis, dass nun in der Botschaft ausdrücklich darauf hingewiesen wird, dass im schweizerischen Recht formellgesetzliche Grundlagen geschaffen werden müssen, die die Weitergabe der Personendaten ausdrücklich erlauben. Dies ergibt sich aus dem Wortlaut des Abkommens, der für die Weitergabe auf das nationale Recht verweist. Darauf hatten wir bereits in einer früheren Stellungnahme hingewiesen.

Allerdings bereiteten uns die vorgesehenen gesetzlichen Grundlagen Schwierigkeiten. Es wurde vorgeschlagen, in diesem Zusammenhang einen einzigen Artikel in einem formellen Gesetz neu zu schaffen. Hier stellte sich für uns die Frage, ob darunter sämtliche Weitergaben von Personendaten an Europol subsumiert werden könnten. Um dies beurteilen zu können, mussten wir wissen, aus welchen schweizerischen Datenbanken Daten an Europol weitergegeben werden sollten. Gerade dies ergab sich nicht aus dem Botschaftstext. Darin wurde lediglich erwähnt, dass die Personendaten aus verschiedenen Quellen beschafft werden könnten. In unserer Stellungnahme wiesen wir darauf hin, dass in der Botschaft selbst sämtliche Datenbanken aufgeführt werden müssen, aus denen die Schweiz Personendaten an Europol weitergeben wird. Betreffend jede der betroffenen Datenbanken müsse sodann analysiert werden, ob und wenn ja welches formelle Gesetz die Weitergabe von Daten an Europol erlaubt. Falls es für eine der betroffenen Datenbanken noch keine formelle gesetzliche Grundlage gibt, muss eine solche geschaffen werden. Das Gleiche gilt auch für jede Ausdehnung des Abkommens auf weitere Deliktskategorien.

Weiter verlangten wir, dass unsere Rolle als unabhängige nationale Kontrollinstanz ausdrücklich erwähnt werde.

Wir ersuchten das zuständige Amt, unsere Bemerkungen zu berücksichtigen oder die Divergenz im Bundesratsantrag als Meinungsverschiedenheit zu erwähnen.

3.1.3 Anpassung des Verfahrens betreffend das indirekte Auskunftsrecht gemäss Artikel 14 ZentG und 18 BWIS

Nach einem Beschluss der Eidgenössischen Datenschutzkommission (EDSK) mussten wir unser Verfahren hinsichtlich des indirekten Auskunftsrechts in den Informationssystemen ISIS, JANUS und GEWA des Bundesamtes für Polizei anpassen. Das eigentliche Novum bildet die Erstellung eines Kontrollberichts über die Prüfung des indirekten Auskunftsgesuchs. Dieser Bericht enthält keine polizeilichen Informationen.

Die Eidgenössische Datenschutzkommission (EDSK) empfahl uns in einem Beschluss, unser Verfahren im Bereich des indirekten Auskunftsrechtes anzupassen. Einige Empfehlungen konnten direkt angewandt werden, während andere noch weiterer Klarstellungen bedürfen.

Die EDSK verlangte, dass die Notiz, die bei der Prüfung der Auskunftsgesuche in den Informationssystemen ISIS, JANUS und GEWA des Bundesamtes für Polizei (BAP) erstellt wird, in Form eines detaillierteren Berichts erfolgt. Diese Empfehlung wurde umgehend befolgt. Künftig erstellt der EDSB einen Bericht mit der Liste aller Eintragungen und Dokumente, die vom BAP präsentiert und vom EDSB untersucht werden. Für jede Eintragung oder Unterlage werden im Bericht mehrere Elemente erwähnt (z.B. Referenz, Datum, Verlässlichkeit, Art der Eintragung bzw. des Dokuments, Absender und Empfänger). Es ist zu betonen, dass der Bericht keine polizeiliche Information enthält. Der Bericht erwähnt auch die hinsichtlich Rechtmässigkeit, Verhältnismässigkeit oder Datenrichtigkeit problematischen Eintragungen und Dokumente. Verweise auf von uns erlassenen Empfehlungen werden gegebenenfalls im Bericht angegeben.

Einige Punkte des Beschlusses der EDSK müssen in Zusammenarbeit mit der EDSK und dem BAP noch geklärt werden.

3.2 Weitere Themen

3.2.1 Revision der Verordnung über die Meldestelle für Geldwäscherei

Im Vorentwurf der revidierten Verordnung über die Meldestelle für Geldwäscherei gibt es weiterhin Bestimmungen, die eigentlich in einem formellen Gesetz enthalten sein müssten. Somit wäre es sinnvoll, zunächst die formellgesetzlichen Grundlagen zu revidieren. Ausserdem bestehen praktische Probleme im Zusammenhang mit dem in der Verordnung vorgesehenen indirekten Auskunftsrecht.

Im Rahmen der Ämterkonsultation konnten wir zum Vorentwurf der revidierten Verordnung über die Meldestelle für Geldwäscherei (MGwV) Stellung nehmen. Zunächst ist darauf hinzuweisen, dass das Datenschutzgesetz für die Bearbeitung von besonders schützenswerten Daten durch Bundesorgane eine formellgesetzliche Grundlage verlangt. Diesbezüglich mussten wir feststellen, dass der Vorentwurf MGwV sehr viele Bestimmungen umfasst, die zumindest in ihren groben Zügen in einer formellen Rechtsgrundlage enthalten sein müssten. Aus diesem Grund hielten wir fest, dass es sinnvoll wäre, vor einer Revision der MGwV zunächst die formellen gesetzlichen Grundlagen zu schaffen. Dabei ist zu beachten, dass wir bereits im Zusammenhang mit der Schaffung und der Inkraftsetzung des Bundesgesetzes zur Bekämpfung der Geldwäscherei im Finanzsektor (GwG) darauf hingewiesen hatten, dass die im GwG vorgesehenen formellgesetzlichen Rechtsgrundlagen für die Datenbearbeitungen der Meldestelle für Geldwäscherei nicht genügen würden. Das GwG wurde trotzdem in Kraft gesetzt. Dafür wurde die Geltungsdauer der MGwV befristet und die Erstellung eines Rechenschaftsberichtes vorgesehen (vgl. auch unseren 5. Tätigkeitsbericht 1997/98, Ziffer I 1.3.). Folglich war bereits bei der Schaffung der MGwV klar, dass diese viele Bestimmungen enthält, die in einem formellen Gesetz stehen müssten. Aus diesen Gründen legten wir grossen Wert darauf, dass auch die revidierte MGwV zeitlich befristet bleibe, so lange noch keine formellen gesetzlichen Grundlagen bestünden.

Der Vorentwurf sieht für das Informationssystem der Meldestelle für Geldwäscherei weiterhin das indirekte Auskunftsrecht vor. Abgesehen davon, dass auch hier ein formelles Gesetz nötig wäre, wiesen wir darauf hin, dass das indirekte Auskunftsrecht nicht dem eigentlichen Auskunftsrecht gemäss Datenschutzgesetz entsprechen würde. Die betroffenen Personen haben einzig die Garantie, dass ihr Gesuch von einem Organ ausserhalb des Bundesamtes für Polizei behandelt wird. So ist es uns praktisch nicht möglich, den Wahrheitsgehalt der vorhandenen Einträge zu überprüfen. Damit können die betroffenen Personen ihr Berichtigungsrecht faktisch kaum ausüben.

Zudem sind wir betreffend indirektes Auskunftsrecht immer noch mit verschiedenen verfahrensrechtlichen und juristischen Problemen konfrontiert. Daher schlugen wir vor, das Informationssystem stattdessen dem *direkten* Auskunftsrecht mit seinen Einschränkungsmöglichkeiten gemäss Datenschutzrecht zu unterstellen.

Unsere Anliegen betreffend die mangelnde formellgesetzliche Grundlage und in Bezug auf das indirekte Auskunftsrecht wurden vom zuständigen Bundesamt nicht berücksichtigt. Im Bundesratsantrag wird auf diese Divergenz hingewiesen.

Es bleibt zu hoffen, dass die mangelnden formellgesetzlichen Grundlagen so rasch als möglich entsprechend geschaffen werden.

3.2.2 Revision der Ausländergesetzgebung und der Asylgesetzgebung

Um den allgemeinen Datenschutzprinzipien zu genügen, muss die Weitergabe von Informationen über Strafverfahren an ausländische Behörden eine legitime Zweckbindung aufweisen. Das Ziel, im Rahmen von Verhandlungen über Wiederaufnahme- oder Transitabkommen einen Stillstand zu vermeiden, bildet keine solche Zweckbindung. Ausserdem muss die Aufnahme von Fingerabdrücken und Fotografien von Personen, welche illegal in die Schweiz einreisen, auf einem formalrechtlichen Gesetz beruhen.

Anlässlich der Beratungen der Eidgenössischen Räte zu den Entwürfen der Totalrevision des Ausländergesetzes und der Teilrevision des Asylgesetzes schlug das Bundesamt für Flüchtlinge (BFF, aktuell Bundesamt für Migration) vor, die beiden Gesetze um Bestimmungen zu ergänzen, welche die Bekanntgabe von Informationen über Strafverfahren in der Schweiz an die Behörden der Herkunfts-, Wohnsitz-, Transit- oder Drittstaaten sowie an internationale Organisationen bewilligen. Gemäss dem BFF soll mit der Informationsweitergabe verhindert werden, dass die Verhandlungen über Wiederaufnahme- und Transitabkommen ins Stocken geraten. Die vorgebrachte Zweckbindung – Weitergabe von besonders schützenswerten Daten zur Erleichterung der Verhandlungen mit einem ausländischen Staat – kann nicht als legitim betrachtet werden. Deshalb ist die geplante Datenweitergabe nicht mit den allgemeinen Datenschutzgrundsätzen vereinbar. Die Weitergabe von Informationen über Strafverfahren muss in Übereinstimmung mit der Gesetzgebung über die internationale Rechtshilfe in Strafsachen erfolgen, welche Regeln zum Schutz der Persönlichkeit vorsieht. Die systematische Weitergabe – ausserhalb eines Strafverfahrens im Ausland – würde diese Datenschutzregeln unterlaufen und damit die Personen gravierenden Risiken einer Persönlichkeitsverletzung aussetzen. Ausserdem wäre eine systematische Weitergabe auch an Personen, die solche Informationen gar nicht erhalten sollten (Dritt- oder Transitstaaten, internationale Organisationen), völlig unverhältnismässig.

Um die Abnahme von Fingerabdrücken und das Fotografieren von illegal in die Schweiz eingereisten Personen zu ermöglichen, hat das Bundesamt für Zuwanderung, Integration und Auswanderung (IMES; aktuell Bundesamt für Migration) vorgeschlagen, zwei Verordnungen des Bundesrates zu ändern. Die geplanten Massnahmen bilden eine Persönlichkeitsverletzung der betroffenen Personen und eine Bearbeitung von besonders schützenswerten Daten gemäss DSG. Die Bearbeitung durch ein Bundesorgan ist nur möglich, wenn eine formalrechtliche Gesetzesgrundlage sie ausdrücklich vorsieht. Das IMES hat sich auf eine Bestimmung des Bundesgesetzes über Aufenthalt und Niederlassung der Ausländer berufen, die nicht als ausreichende Gesetzesgrundlage dienen kann. Diese Bestimmung hält eindeutig fest, dass von Ausländern zur Feststellung der Identität Fingerabdrücke und Gesichtsbilder erhoben werden können. Der Fall der Identifikation von Ausländern, die illegal in die Schweiz einzureisen versuchen, wird damit nicht abgedeckt. Da die Bestimmungen von zwei Verordnungen mit Blick auf das DSG nicht als ausreichende Gesetzesgrundlage gelten, forderten wir in unserer Stellungnahme, das Erheben von Fingerabdrücken und Gesichtsbildern von Personen, die illegal in die Schweiz einreisen, in einer formalrechtlichen Gesetzesgrundlage ausdrücklich niederzulegen. Der Bundesrat ist jedoch nicht auf unsere Bemerkungen eingegangen. Die beiden Änderungen sind am 1. Juni 2004 in Kraft getreten.

3.2.3 Veröffentlichung von Personendaten zu Polizeiermittlungen oder Urteilen in der Presse

Bei der Veröffentlichung von Daten zu Polizeiermittlungen oder Urteilen muss das Gebot der Anonymität beachtet werden, ausser wenn die betroffene Person der Veröffentlichung zustimmt, wenn ein Gesetz sie vorsieht oder wenn ein überwiegendes privates oder öffentliches Interesse sie rechtfertigt. Dabei darf die Veröffentlichung keine andere Rechtsvorschrift verletzen. Ein öffentliches Interesse an der Bekanntgabe von Personendaten in der Presse kann insbesondere vorliegen, wenn der Angeklagte oder Verurteilte eine politische Persönlichkeit, ein Richter, eine Person mit einem hohen öffentlichen Amt oder mit aussergewöhnlichen Qualitäten im sportlichen, gesellschaftlichen oder künstlerischen Bereich ist oder war.

Die Veröffentlichung von Informationen in der Presse stellt eine Bearbeitung von Personendaten gemäss DSG dar, sofern sich diese Informationen auf bestimmte oder bestimmbare Personen beziehen. Gemäss dem DSG hat niemand das Recht, Personendaten (d.h. nicht anonyme Daten) ohne Rechtfertigungsgrund Dritten bekannt zu geben. Rechtfertigungsgründe sind die Zustimmung der betroffenen Person, ein über-

wiegendes privates oder öffentliches Interesse oder das Gesetz. Das Vorliegen eines überwiegenden Interesses an der Erhebung von Personendaten für eine Veröffentlichung (journalistische Recherchen vor der Publikation) wird im DSG generell anerkannt. Dieser Rechtfertigungsgrund kann allerdings nicht für die Veröffentlichung von Personendaten in der Presse geltend gemacht werden.

Das DSG schliesst indessen das Vorliegen anderer überwiegender Interessen nicht aus. Dazu zählt insbesondere die Informationspflicht der Medien gegenüber der Öffentlichkeit zu Fragen von allgemeinem Interesse, namentlich zu Angelegenheiten, mit denen sich die Gerichte oder die Polizeiermittler befassen, sofern der öffentliche Informationsbedarf nicht im Widerspruch zum Untersuchungsgeheimnis steht.

Selbst wenn die Veröffentlichung von Personendaten auf einem überwiegenden öffentlichen Interesse beruht, muss sie auch die allgemeinen Grundsätze des DSG, besonders die Prinzipien der Rechtmässigkeit und der Verhältnismässigkeit, erfüllen.

Daneben stellt sich die Frage, ob die Presse im Rahmen von Polizeiermittlungen bzw. eines Urteils ihre Informationen transparent verbreiten darf. Im besonderen Kontext der Polizeiermittlung sind das Fehlen einer Verurteilung des Verdächtigten und die Unschuldsvermutung zu berücksichtigen. Wenn jedoch Name und Fotografie eines Verdächtigten veröffentlicht werden, so gilt dieser in den Augen vieler bereits als schuldig. Der Verdächtigte wird von seinen Mitbürgern verurteilt, obwohl nach Gesetz noch die Unschuldsvermutung gilt; diese Vorverurteilung läuft elementarsten Grundsätzen der Gerechtigkeit zuwider. Im Fall eines Freispruchs ist die Situation besonders bedenklich.

Die Anonymität rechtfertigt sich nicht nur wegen der Unschuldsvermutung, sondern ermöglicht auch eine bessere gesellschaftliche Wiedereingliederung der verdächtigten oder verurteilten Person. Das Gebot der Anonymität ergibt sich aus dem Verhältnismässigkeitsgrundsatz und aus der Unschuldsvermutung. Grundsätzlich dürfen die Medien weder eine verdächtigte noch eine verurteilte Person mit Namen oder mit einem anderen Element, das die Identifizierung ermöglicht, bezeichnen. Identifizierungselemente für eine Person sind Fotografie, Karikatur, Anschrift, Autonummer, Bezeichnung der Funktion oder des Berufs, d.h. alles Elemente, die zweifelsfrei Aufschluss über die Identität der betroffenen Person geben. Die Identität eines Angeklagten oder Täters lässt sich oft nicht hinter Initialen verstecken, so etwa wenn die Initialen besonders originell sind oder wenn die betroffene Person aus einer kleinen Ortschaft stammt, die in vollem Wortlaut angegeben wurde, oder wenn zusätzlich zu den Initialen punktuelle Auskünfte gemacht werden, die zusammen genommen die Person zweifelsfrei bezeichnen (Staatsbürgerschaft, Familienverhältnisse usw.). Das gängige Verfahren, wonach der Vorname gefolgt vom Anfangsbuchstaben des Familiennamens angegeben werden, ist diesbezüglich noch riskanter.

Ausnahmen von der Vorschrift der Anonymität bzw. vom Verbot für die Medien, einen Täter oder einen Verdächtigten mit seinem Namen zu bezeichnen oder ein anderes Element, das zu seiner Identifizierung führt, zu nennen, bilden die *Zustimmung* der betroffenen Person, das *überwiegende private oder öffentliche Interesse* und das *Gesetz.*

Wenn der Angeklagte beispielsweise mit Interviews absichtlich die Aufmerksamkeit auf sich lenkt, ist davon auszugehen, dass er der Bekanntgabe seiner Identität *zugestimmt* hat. In solchen Fällen ist die diese Bekanntgabe grundsätzlich rechtmässig. Allerdings kann die Veröffentlichung des Namens gegen die Verfahrensvorschriften, welche das Ermittlungsgeheimnis garantieren, verstossen. Deshalb müssen die Interessen des Angeklagten, der Richter und der übrigen von den Ermittlungen berührten Personen berücksichtigt werden.

Ein *überwiegendes öffentliches Interesse* an der Veröffentlichung von Personendaten in der Presse kann vorliegen, wenn der Angeklagte oder Verurteilte eine politische Persönlichkeit, ein Richter, eine Person mit einem hohen öffentlichen Verwaltungsamt, mit wichtigen wirtschaftlichen oder sozialen Verantwortungen bzw. mit aussergewöhnlichen Qualitäten im sportlichen, gesellschaftlichen oder künstlerischen Bereich ist bzw. war. Wer wegen seiner Position regelmässig die Neugier der Medien weckt, muss davon ausgehen, dass diese Neugier auch in für ihn ungünstigeren Umständen bestehen bleibt. Das Delikt muss grundsätzlich mit der Stellung, welche die Person innehat und welcher sie ihre Bekanntheit verdankt, in Zusammenhang stehen.

Die Schwere des Deliktes, die Originalität des fraglichen Tatbestands oder der Grad der Perversion des Täters reichen allein nicht aus, um die Veröffentlichung des Namens bzw. anderer Elemente, welche die Identifizierung erlauben, vor oder nach der Verurteilung zu rechtfertigen. Zur Rechtfertigung der Veröffentlichung ist nachzuweisen, dass der Täter ein gravierendes und konkretes Risiko für viele Personen darstellt und dass die Veröffentlichung seines Namens zum Zeitpunkt des Urteils dieses Risiko erheblich verringern kann.

Das *Gesetz* ermächtigt die Gerichtsbehörden, Fahndungsausschreibungen mit dem Namen, der Fotografie oder dem Phantombild der gesuchten Person zu veröffentlichen. Das Bundesgericht erlaubt die Veröffentlichung des Namens eines nicht flüchtigen Angeklagten, wenn dies die Strafverfolgung vorantreiben kann.

Eine Datenbearbeitung ist nicht nur bei Fehlen von Rechtfertigungsgründen unrechtmässig, sondern auch wenn sie bestimmte Rechtsnormen verletzt, besonders im Fall von strafbaren Handlungen wie z.B. der Veröffentlichung amtlicher geheimer Verhandlungen (Artikel 293 Strafgesetzbuch StGB) oder üble Nachrede (Art. 173 StGB).

Der in Art. 293 StGB erfasste Tatbestand liegt vor, wenn ein Journalist infolge von Indiskretionen über vertrauliche Handlungen einer Behörde berichtet. In diesem Fall kann der Journalist grundsätzlich keine Rechtfertigungsgründe geltend machen. Er ist jedoch nicht strafbar, wenn er nach Treu und Glauben annehmen konnte, dass die Person, welche ihm die Dokumente übergeben hatte, im Rahmen ihrer Befugnisse handelte, vor allem wenn die Dokumente nicht als vertraulich eingestuft waren.

Im Fall der Verhütung der üblen Nachrede (Art. 173 StGB) kann der Journalist von jeder Verantwortung befreit werden, wenn er nachweist, dass er eine falsche Aussage für wahr halten musste, weil sie aus einem Polizeibericht oder einer anderen als verlässlich geltenden Quelle stammte. Ausserdem bleibt der Journalist straffrei, wenn er beweist, dass seine Äusserungen der Wahrheit entsprechen. Dagegen wird derjenige nicht zum Exkulpationsbeweis zugelassen, der Äusserungen ohne Wahrung öffentlicher Interessen oder sonst wie begründete Veranlassung vorwiegend in der Absicht verbreitet, jemandem Übles vorzuwerfen.

Zusammengefasst stellt die Veröffentlichung von anonymen Daten in der Presse (d.h. Daten, anhand derer sich die betroffene Person nicht identifizieren lässt) keine Verletzung der Persönlichkeit dar und gehört nicht zum Anwendungsbereich des DSG. Die Veröffentlichung von Personendaten zu Polizeiermittlungen oder Urteilen ist rechtmässig, wenn sie auf einem Rechtfertigungsgrund beruht und keiner Geheimhaltungsvorschrift zuwiderläuft.

4 IT und Telekommunikation

4.1 Datenschutzrechtliche Aspekte beim Einsatz der RFID-Technologie

In immer zahlreicheren Anwendungsgebieten werden Funkchips eingesetzt, die mit Hilfe von Radiowellen (der so genannten Radio Frequency Identification, RFID) berührungslos und ohne Sichtkontakt Daten lesen und speichern können. Während für gewisse Bereiche aus datenschutzrechtlicher Sicht keine Bedenken für die Verwendung von RFID-Chips anzubringen sind, bestehen in anderen erhebliche Risiken für die Privatsphäre der Bevölkerung. Daher müssen beim Einsatz der RFID-Technologie stets Vorkehrungen getroffen werden, um eine widerrechtliche Bearbeitung von Personendaten zu verhindern.

Eine mögliche Anwendung der RFID-Technologie kennen viele Bürgerinnen und Bürger in Form von Diebstahlwarnanlagen in Kaufhäusern. Bei den Ausgängen befinden sich meistens gut ersichtliche Lesegräte, die Funksignale aussenden und empfangen. An oder in den Verkaufsartikeln sind Etiketten mit RFID-Chips (so genannten Transpondern oder Tags) angebracht. Beim Kauf eines Artikels wird der Transponder deaktiviert. Wird ein Artikel mit einem nicht deaktivierten Transponder am Lesegerät vorbeigeführt, wird dies vom Lesegerät erkannt und ein Alarm ausgelöst.

Der Transponder besteht meist aus einem Chip, einer Antenne sowie einem Gehäuse. Gängige Transponder sind z. B. in Glaszylindern, Plastikscheiben und Karten (wie etwa den EC-Karten) untergebracht oder auf Folien aufgetragen. Sie können in jedes Objekt implementiert bzw. an dieses angebracht werden. In der RFID-Technik unterscheidet man zwischen aktiven Transpondern, die über eine eigene Energiequelle (Batterie) verfügen, und passiven Transpondern, welche die benötigte Energie aus den Funkwellen eines Schreib- und Lesegerätes gewinnen. Aufgrund dieser gewonnen Energie sind die passiven Transponder in der Lage, die gespeicherten Daten auszusenden. Angewendet wird die RFID-Technologie u. a. im Bereich der Logistik für die Verfolgung von Waren von der Quelle bis zum Ziel, z. B. bei Paketdiensten, zur Gepäckverfolgung und -identifikation, zur Palettenkennzeichnung, für Lagersysteme und Bestandkontrollen. Auch im Sicherheitsbereich – etwa zur Personen-, Tier- und Fahrzeugidentifikation, Zugangskontrolle, Artikelüberwachung, für Autowegfahrsperren und Türschliesssysteme – sowie im Transportwesen und Ticketing – z. B. für Billete im öffentlichen Verkehr oder bei Grossveranstaltungen und für Skiabonnemente – kommt die RFID-Technologie zum Einsatz.

Zukünftig wird voraussichtlich der auf der RFID-Technologie basierende Elektronische Produkte Code (EPC) Einzug in die Warenhäuser halten. Der EPC ist eine Ergänzung bzw. Erweiterung des heutigen Strichcodes (dem so genannten European Article Number, EAN). Mit der Einführung des EPC kann jedes einzelne Objekt weltweit eindeutig gekennzeichnet werden. Identifiziert sich der Kunde beim Kauf von Produkten z. B. mit einer Kredit- oder Kundenkarte, so können ihm diese eindeutigen Artikelbezeichnungen über eine längere Zeit (sogar lebenslang) zugeordnet werden. Weiter wird inzwischen auch diskutiert, ob Banknoten mit RFID-Chips bestückt werden sollen.

Aus datenschutzrechtlicher Sicht birgt der Einsatz der RFID-Technologie Risiken, da sie es ermöglicht, Daten mit Hilfe von Funkwellen über eine gewisse Distanz zu bearbeiten, ohne dass eine direkte (Sicht-)Verbindung mit dem Chip notwendig ist oder der Betroffene aktiv in einen Prozess eingreifen muss. Es kann also eine Datenbearbeitung erfolgen, ohne dass die Betroffenen dies bemerken. Aus nicht zerstörten oder gelöschten RFID-Transpondern können die gespeicherten Informationen mit Hilfe von (unsichtbaren) Lesegeräten ausgelesen werden. So gewonnene Daten können wiederum miteinander verknüpft werden – auf diese Weise besteht das Risiko, dass Einkaufs- oder Bewegungsprofile erstellt werden.

Auch die Kennzeichnung von Banknoten mittels RFID-Chips ist aus datenschutzrechtlicher Sicht sehr heikel. Wir sind der Ansicht, dass nicht nachvollzogen werden darf, welche Personen welche Banknoten an welchen Geldausgabeautomaten abheben und wo diese Personen welche Waren oder Dienstleistungen einkaufen.

Aufgrund der Vorgaben im Datenschutzgesetz dürfen Personendaten nur bearbeitet werden, wenn die betroffenen Personen ihre Einwilligung für die Datenbearbeitung gegeben haben, sofern nicht öffentliche oder private überwiegende Interessen oder eine gesetzliche Grundlage die Datenbearbeitung rechtfertigen. Die Einwilligung kann nur erfolgen, wenn die Betroffenen darüber informiert sind, welche Daten zu welchem Zweck wann, wo und wie bearbeitet werden. Auch das Prinzip von Treu und Glaube verlangt eine transparente Information der Betroffenen.

Wir empfehlen den Produzenten und Betreibern von RFID-Anwendungen oder -systemen, die erforderlichen Vorkehrungen zu treffen, damit der Einsatz der RFID-Technologie datenschutzkonform erfolgen kann. Insbesondere sind folgende Punkte zu beachten:

- Die Bearbeitung von Personendaten soll möglichst vermieden werden. Ist sie unumgänglich, so sind die Betroffenen in transparenter Weise über den Zweck der Datenbearbeitung wie auch über das Informationssystem aufzuklären. Nebst der Zweckangabe geht es insbesondere darum aufzuzeigen, welche Daten wo erhoben werden und wie sie bearbeitet (z. B. an wen sie weitergeleitet) bzw. wann sie gelöscht werden. Ein erster Schritt zur Transparenz besteht darin, die Kunden darauf aufmerksam zu machen, welche Artikel mit RFID-Transpondern versehen sind.
- Die erhobenen Daten dürfen nur zum angegebenen Zweck bearbeitet werden.
- Das Auskunftsrecht muss gewährleistet sein.
- Die Transponder müssen je nach Anwendung zerstört oder deaktiviert oder aber die gespeicherten Daten gelöscht werden können. Gelangt eine Person durch Kauf oder Weitergabe von Objekten zusätzlich auch in den Besitz von Funk-Chips, so muss sie die Möglichkeit haben, die Daten ganz oder teilweise zu löschen oder löschen zu lassen, so dass diese nicht mehr rekonstruierbar sind. Im Weiteren muss die Person auch die Möglichkeit haben, den Chip zu zerstören oder zerstören zu lassen. Beim Ausleihen von Produkten (z. B. von Büchern aus einer Bibliothek) ist dafür zu sorgen, dass die Transponder beim Ausleihvorgang deaktiviert werden, so dass diese nicht ausgelesen werden können, solange sie im Gebrauch des Benutzers oder der Benutzerin sind. Erst bei der Rückgabe der Ware ist der Transponder wieder zu aktivieren.
- Die Informationssicherheit ist zu gewährleisten: Die Systeme müssen sicher gestaltet werden, so dass insbesondere Vertraulichkeit, Verfügbarkeit und Integrität gewährleistet sind. Die Informationen in den RFID-Transpondern müssen (z. B. mittels Chiffrierverfahren) so geschützt werden, dass sie nur für die dafür vorgesehene Anwendung verfügbar sind. Es darf nicht möglich sein, dass der Besitzer oder die Besitzerin eines Schreib- und Lesegerätes Informationen aus nicht geschützten RFID-Transpondern auslesen kann. Besonders gefährlich wäre zudem, wenn man mit einem Lesegerät feststellen kann, wie viel Geld jemand auf sich trägt.

4.2 Registrierung der Prepaid-SIM-Karten von Mobiltelefonen

Im August 2004 ist in der Schweiz eine Bestimmung in Kraft getreten, die die Mobiltelefonanbieter verpflichtet, die Käufer von vorausbezahlten SIM-Karten zu registrieren. Die Wirksamkeit dieser mit grossem Aufwand verbundenen Massnahme ist allerdings fraglich.

Die eidgenössischen Räte haben im Herbst 2003 eine bereits seit Jahren diskutierte Ergänzung des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs beschlossen. Käufer von Prepaid-SIM-Karten werden durch die neue Bestimmung verpflichtet, ihre Personalien anzugeben. Ziel ist eine verbesserte Kriminalitätsbekämpfung. Die Fernmeldeanbieter werden verpflichtet, diese Daten mindestens zwei Jahre aufzubewahren; Daten, die weder für die Erbringung der Dienstleistung noch für die Rechnungsstellung notwendig sind.

Am 1. August 2004 ist nun die Registrierungspflicht zusammen mit Ausführungsbestimmungen in Kraft getreten. Registriert werden alle Neukunden sowie diejenigen unter den bisherigen Kunden, die ihren Karte nach dem 1. November 2002 aktiviert haben. Ältere Karten können unregistriert weiterverwendet werden. Die Anbieter müssen sicherstellen, dass beim Verkauf von Prepaid-SIM-Karten Name, Vorname, Adresse, Geburtsdatum anhand eines gültigen Reisepasses, einer Identitätskarte oder eines anderen für den Grenzübertritt in die Schweiz zulässigen Reisedokumentes erfasst werden. Ausserdem sind die Art des Ausweises und die Ausweisnummer zu erfassen.

Ein Mobiltelefonanbieter beabsichtigte, die über das Registrierungsformular erhobenen Daten für zusätzliche Zwecke, die von der gesetzlichen Grundlage nicht abgedeckt sind, zu verwenden. Dazu ist jedoch eine vorgängige Einwilligung der betroffenen Person nötig. Da die Entscheidungsmöglichkeit der Kundinnen und Kunden nicht klar war, haben wir interveniert. Das Formular ist daraufhin angepasst worden. Es ist nun klar ersichtlich, welche Daten obligatorisch und welche freiwillig anzugeben sind, beziehungsweise, welche Bearbeitungen vorgenommen werden sollen.

Die Weitergabe der SIM-Karte durch den Erstkäufer an eine andere Person ist nicht meldepflichtig. Dies wäre auch kaum praktikabel. Somit ist die Person, die im Beisitz der Karte ist und diese auch benutzt, nicht unbedingt identisch mit derjenigen, die ursprünglich registriert wurde. Auch ist es nach wie vor möglich, in der Schweiz mit nicht registrierten Prepaid-Karten ausländischer Anbieter zu telefonieren. Dass mit der Registrierung Kriminalität und Terrorismus wirksam bekämpft werden können, ist angesichts dieser Umgehungsmöglichkeiten somit eher zweifelhaft. Die mit hohem Aufwand errichtete Sammlung von Daten hunderttausender von Personen birgt allerdings ein gewisses Risiko an Datenschutzverletzungen.

4.3 Bekanntgabe von Personendaten beim Inkasso von Telekommunikations-Mehrwertdiensten

Mehrwertdienste im Telekommunikationsbereich werden den Kundinnen und Kunden üblicherweise durch den Fernmeldeanbieter in Rechnung gestellt. Damit haben die Anbieter von Mehrwertdienstleistungen keinen Zugriff auf die Kundendaten. Bestreitet der Kunde die Inanspruchnahme der Dienstleistung, stellt sich die Frage, ob und in welcher Form diese Kundendaten an den Mehrwertdienstanbieter weitergegeben werden sollen, um diesem ein direktes Inkasso zu ermöglichen. Wir haben die Frage erörtert, inwiefern eine solche Weitergabe von Kundendaten aus datenschutzrechtlicher Sicht zulässig ist.

Grundsätzlich fordert das Datenschutzgesetz (DSG) einen Rechtfertigungsgrund für die Bearbeitung von Personendaten; dies kann die Einwilligung der betroffenen Person sein, eine gesetzliche Vorschrift oder ein überwiegendes öffentliches oder privates Interesse.

Ein Einspruch gegen die Belastung von Mehrwertdiensten auf der Rechnung könnte als Einwilligung in die Weiterleitung der Personendaten verstanden werden, sofern dieses Vorgehen beispielsweise in den Geschäftsbedingungen des Fernmeldeanbieters ausreichend transparent gemacht wird. Eine solche Einwilligung kommt aber nicht einer freien Wahl gleich, da die einzige Alternative darin besteht, den strittigen Betrag zu bezahlen. Eine gesetzliche Vorschrift, welche die fragliche Übermittlung der Kundendaten an den Mehrwertdienstanbieter fordert oder ausdrücklich zulässt, ist nicht bekannt. Auch überwiegende öffentliche Interessen fallen kaum in Betracht.

Das DSG zählt nun aber in einem nicht abschliessenden Katalog Fälle auf, in denen grundsätzlich von einem überwiegenden Interesse des Datenbearbeiters auszugehen ist. Ein solches ist insbesondere dann gegeben, wenn er in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über den Vertragspartner bearbeitet. Werden Mehrwertdienste in Anspruch genommen, wird sowohl zwischen dem Kunden und dem Telefondienstanbieter als auch zwischen dem Kunden und dem Mehrwertdienstanbieter ein Vertrag geschlossen. Damit ist ein überwiegendes Interesse des Mehrwertdienstanbieters als Datenbearbeiter gegeben.

Dabei müssen aber in jedem Fall die vom DSG aufgestellten allgemeinen Grundsätze der Datenbearbeitung beachtet werden. Insbesondere fordert der Grundsatz der Verhältnismässigkeit, dass eine Datenbearbeitung nur in demjenigen Umfang vorgenommen werden darf, der für den angestrebten Zweck erforderlich ist. Im vorliegenden

Kontext bedeutet dies, dass der Telefondienstanbieter nur diejenigen Daten bekannt geben darf, die der Mehrwertdienstanbieter für das Inkasso benötigt – also Name, Adresse und geschuldeter Betrag.

Wenn die Kundin oder der Kunde jedoch bestreitet, die Dienstleistung wissentlich und willentlich in Anspruch genommen zu haben (z.B. bei so genannten Internet-Dialern), ist das Zustandekommen eines Vertrags zwischen Anrufer und Mehrwertdienstanbieter strittig. In einem solchen Fall klären Kunden und Mehrwertdienstanbieter am besten im direkten Kontakt ab, ob ein gültiger Vertrag und damit eine Zahlungspflicht besteht. Aus dem Interesse der Kunden, das Zustandekommen eines gültigen Vertrags dem Mehrwertdienstanbieter gegenüber bestreiten zu können, lässt sich schliessen, dass der fraglichen Bekanntgabe der Kundendaten aus datenschutzrechtlicher Sicht nichts entgegensteht.

Zu prüfen ist indessen, ob die fragliche Bekanntgabe nach den fernmelderechtlichen Spezialbestimmungen ebenfalls zulässig ist.

Das grundrechtliche, in der Verfassung verankerte Fernmeldegeheimnis schützt in erster Linie Kommunikationsinhalte. Der Schutz umfasst aber auch alle zusätzlichen persönlichen Angaben zur Kommunikation. Das Fernmeldegesetz legt fest, dass Fernmeldedienstanbieter «Dritten» gegenüber keine Angaben über den Fernmeldeverkehr von Kundinnen und Kunden machen dürfen. Als angerufener Gesprächspartner gilt der Mehrwertdienstanbieter als Dritter. Ausnahmen zu diesem Auskunftsverbot für Fernmeldeanbieter können gegeben sein, wenn die Personendaten («Namen und Adres-sen der anrufenden Anschlüsse») zur Ermittlung von missbräuchlich hergestellten Verbindungen (z.B. telefonische Belästigungen) oder, gemäss den Bestimmungen des Strafgesetzbuches betreffend die Verletzung des Post- und Fernmeldegeheimnisses (Art 321ter StGB), zur «Ermittlung des Berechtigten» sowie zur «Verhinderung von Schäden» benötigt werden. In der vorliegenden Konstellation kann, zumindest betreffend den Mehrwertdienstanbieter, keine dieser Ausnahmen geltend gemacht werden.

Somit wäre nach unserer Auffassung die Schaffung einer Rechtsgrundlage im Fernmelderecht erforderlich; zunächst wäre allenfalls noch vertieft zu prüfen, ob eine Gesetzeslücke – eine planwidrige Unvollständigkeit – oder ein qualifiziertes Schweigen des Gesetzgebers vorliegt. Aus datenschutzrechtlicher Sicht steht der Schaffung einer solchen Rechtsgrundlage nichts entgegen.

5 Gesundheit

5.1 Verschiedene Themen

5.1.1 Datenschutzrechtliche Fragen in Zusammenhang mit dem Arzttarif Tarmed

Im Hinblick auf das Inkrafttreten von Tarmed im KVG-Bereich auf den 1. Januar 2004 haben wir zwei Sachverhaltsabklärungen vorgenommen. Die Ergebnisse führen uns zum Schluss, dass die gegenwärtige systematische personenbezogene Datenbearbeitung unverhältnismässig ist. Es liegt an den involvierten Akteuren Lösungen auszuarbeiten, die den datenschutzrechtlichen Anforderungen Rechnung tragen.

Der Tarmed-Rahmenvertrag regelt eine gemeinsame Tarifstruktur und die einheitliche Abwicklung der Leistungsvergütung zwischen Leistungserbringern und Kostenträgern. Mit der Einführung von Tarmed wird – nach einer zweijährigen Übergangsfrist – auf die elektronische Rechnungsstellung zwischen Leistungserbringern und Kostenträgern umgestellt. Die Umstellung von der Papierrechnung zum elektronischen Rechnungsformular vereinfacht systematische Kontrollen. Ohne die erforderlichen Massnahmen nimmt dadurch das Risiko zu, dass der Persönlichkeitsschutz nicht mehr gewährleistet ist. Wir haben in der Vergangenheit bereits mehrfach auf datenschutzrechtliche Gefahren hingewiesen, die die Einführung des Arzttarifs Tarmed mit sich bringt (vgl. 10. Tätigkeitsbericht 2002/2003, Ziffer 5.1.5; 9. Tätigkeitsbericht 2001/2002, Ziffer 5.1.4; 8. Tätigkeitsbericht 2000/2001, Ziffer I 7.5).

Der Leistungserbringer muss dem Schuldner von Gesetzes wegen eine detaillierte und verständliche Rechnung zustellen. Der Versicherer hat die Möglichkeit eine genaue Diagnose oder zusätzliche Auskünfte medizinischer Natur zu verlangen. Ausserdem ist der Leistungserbringer in begründeten Fällen berechtigt und auf Verlangen der versicherten Person in jedem Fall verpflichtet, medizinische Angaben nur dem Vertrauensarzt des Versicherers bekannt zu geben.

Der Gesetzgeber sieht mit den Absätzen 3 und 4 des Artikels 42 des Krankenversicherungsgesetzes (KVG) eine stufenweise Bekanntgabe der Behandlungsdaten durch den Leistungserbringer vor. Der Versicherer kann als Ergänzung zu den bereits erfolgten Angaben zusätzliche Auskünfte verlangen (Abs. 4 als Ergänzung zu Abs. 3). Dadurch schliesst der Gesetzgeber folglich aus, dass bereits in einem ersten Schritt eine systematische Weitergabe von Behandlungsdaten und Diagnosen in detaillierter Form zu erfolgen hat. Die systematische Bekanntgabe von detaillierten Diagnosen bzw. Diag-

nosecodes 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.

Die Sachverhaltsabklärungen (vgl. unseren Bericht «Tarmed und Datenschutz» vom 22. Juni 2004, http://www.edsb.ch/d/themen/gesundheit/tarmed-bericht_d.pdf) haben ergeben, dass die Versicherer von Gesetzes wegen verschiedene Aufgaben wahrnehmen müssen. Geprüft werden muss unter anderem die Leistungspflicht, die Wirtschaftlichkeit der durch die Ärzte erbrachten Leistungen und die zu bezahlende Rechnung. Für diese Aufgaben unterscheiden sich die Datenbedürfnisse. Die Versicherer benötigen jeweils nicht den ganzen personenbezogenen Datensatz. Es muss folglich dafür gesorgt werden, dass zwischen den einzelnen Arbeitsprozessen nur die Daten weitergegeben werden, die für den Folgeprozess zweckmässig und zwingend erforderlich sind. Mit den auf dem Rechnungsformular geforderten Daten stehen aber alle Angaben in ihrer Gesamtheit personenbezogen zur Verfügung. Die Datenbearbeitung in dieser Form ist nicht verhältnismässig.

Die Gesetzgebung schreibt vor, dass ein Bearbeitungsreglement erstellt werden muss, das die technischen und organisatorischen Massnahmen für eine datenschutzkonforme Bearbeitung definiert. Insbesondere werden die Aufbewahrungsfristen, Art und Umfang des Zugriffs der Benutzer der Datensammlung, die Verfahren bei der Berichtigung, Sperrung und Anonymisierung bzw. Pseudonymisierung definiert.

Zusätzlich zum Bearbeitungsreglement ist aus unserer Sicht ein Datenschutzkonzept zu entwickeln, da die systematische Bearbeitung von besonders schützenswerten Patientendaten eine detaillierte Beschreibung der konzeptionellen Massnahmen erfordert, die das Risiko einer Persönlichkeitsverletzung auf ein Minimum reduzieren. Weiter soll das Konzept dazu dienen, den Betroffenen Klarheit über die Datenbearbeitung zu verschaffen. Das Bearbeitungsreglement und das Datenschutzkonzept sind durch den Inhaber der Datensammlung regelmässig auf ihre Anwendung und Aktualität hin zu überprüfen.

5.1.2 Aufsicht über die Einhaltung der Bewilligungsauflagen im Bereich der medizinischen Forschung

Die Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung erlässt Bewilligungen für Forschungsstudien. Aufgabe des EDSB ist es, die Einhaltung der mit den Bewilligungen verbundenen Auflagen zu überprüfen. Wir haben die Einhaltung der Auflagen zweier Bewilligungen kontrolliert und unser Ergebnis der Expertenkommission in einem Bericht mitgeteilt.

Die Aufgabe der Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung ist es, unter gewissen Voraussetzungen Bewilligungen für Forschungsstudien zu erlassen. Die Expertenkommission ist paritätisch zusammengesetzt: Je drei Mitglieder vertreten die Forschung, die Ärzteschaft und die Patientenorganisationen; hinzu kommen zwei Juristinnen oder Juristen. Die Kommission untersteht der Aufsicht des Bundesrates, dem sie periodisch Bericht über ihre Tätigkeit erstattet. Die Einzelheiten sind in der Verordnung über die Offenbarung des Berufsgeheimnisses im Bereich der medizinischen Forschung (VOBG) geregelt.

Die Kommission erlässt Bewilligungen für einzelne Forschungsstudien (Sonderbewilligung), für Spitäler (generelle Bewilligung, auch Klinikbewilligung genannt) wie auch für Medizinalregister im Bereich der medizinischen Forschung, wie z.B. Krebsregister (auch hier eine generelle Bewilligung). Es geht dabei um Datenschutz und insbesondere um die Frage, welche Patientendaten zu Zwecken der medizinischen Forschung weitergegeben und genutzt werden dürfen.

Die Sonderbewilligungen müssen auf das im Gesuch bezeichnete Forschungsvorhaben beschränkt werden. Bei jeder Änderung des Forschungsvorhabens, namentlich des Forschungszwecks, muss eine neue Bewilligung eingeholt werden. Die den Kliniken und medizinischen Universitätsinstituten erteilten generellen Bewilligungen gewähren dem mit betriebsinternen Forschungstätigkeiten betrauten Personal sowie den Doktoratskandidatinnen und -kandidaten Zugriff auf Personendaten, wenn die schutzwürdigen Interessen der Berechtigten nicht gefährdet sind und wenn die Daten zu Beginn der Forschungstätigkeit anonymisiert werden.

Die Expertenkommission kann den Organen, welche für die zu medizinischen Forschungszwecken verwendeten Register (Medizinalregister) verantwortlich sind, generelle Bewilligungen zur Entgegennahme nicht anonymisierter Daten erteilen.

Die Erteilung solcher Bewilligungen unterliegt, wie in Art. 321bis des Strafgesetzbuches (StGB) festgehalten, strikten kumulativen Bedingungen: Die Bewilligung kann nur erteilt werden, wenn die betroffene Person vorgängig über ihre Rechte aufgeklärt worden ist und ihre Einwilligung nicht ausdrücklich verweigert hat, wenn die Forschung nicht mit anonymisierten Daten durchgeführt werden kann, wenn es unmöglich oder besonders schwierig ist, die Einwilligung des Berechtigten einzuholen und wenn die Forschungsinteressen gegenüber den Geheimhaltungsinteressen überwiegen.

Mit der Bewilligungserteilung entsteht keine Pflicht, sondern lediglich ein Recht zur Datenbekanntgabe (vgl. zum bisher gesagten auch unseren 3. Tätigkeitsbericht 1995/1996, Ziffer 6.1, sowie den 5. Tätigkeitsbericht 1997/1998, Ziffer 6.1).

Hat die Kommission die Offenbarung des Berufgeheimnisses bewilligt, so beaufsichtigt der EDSB die Einhaltung der damit verbundenen Auflagen, namentlich in Bezug auf die Datensicherheit.

Wir haben dieses Jahr die Einhaltung der Auflagen einer Sonderbewilligung sowie einer generellen Bewilligung (Klinikbewilligung) überprüft. Bei den Auflagen handelt es sich um Massnahmen zum Schutz und zur Wahrung der Sicherheit der bekannt gegebenen Daten. So sind z.B. die Daten frühestmöglich zu anonymisieren. Ferner sind die nicht anonymisierten Daten, welche auf Papier festgehalten sind, unter Verschluss zu halten und diejenigen, welche auf elektronischen Datenträgern gespeichert sind, durch ein Passwort zu schützen. Dies bestimmt den Kreis der Zugriffsberechtigten. Es dürfen nur die Bewilligungsnehmer und deren Assistenten auf die nicht anonymisierten Daten zugreifen.

Für unsere Abklärung haben wir Bewilligungen der Expertenkommission studiert und zwei davon für unsere Kontrolle ausgewählt. Sodann haben wir Dokumente zur Durchführung des Forschungsprojektes sowie der damit verbundenen Datenbearbeitung bei den Forschern einverlangt. In einem weiteren Schritt haben wir die eingegangenen Dokumente analysiert und einen Fragebogen erstellt. Anschliessend haben wir uns die Datenbearbeitung vor Ort vorführen lassen.

Wie unsere Überprüfung ergeben hat, wurden die Auflagen grundsätzlich eingehalten. Die Ergebnisse unserer Kontrollen haben wir der Expertenkommission in Form eines Berichtes mitgeteilt.

Wir werden auch zukünftig in enger Zusammenarbeit mit der Expertenkommission weitere Kontrollen über die Einhaltung der Auflagen durchführen und die Expertenkommission in datenschutzrechtlichen Fragen beraten.

5.2 Genetik

5.2.1 Bundesgesetz über genetische Untersuchungen beim Menschen

Im Oktober 2004 hat das Parlament das Bundesgesetz über genetische Untersuchungen beim Menschen gutgeheissen. Das Gesetz enthält auch zahlreiche Bestimmungen zum Persönlichkeitsschutz.

Die Referendumsfrist für das Bundesgesetz über genetische Untersuchungen beim Menschen (GUMG) ist am 27. Januar 2005 abgelaufen. Der Bundesrat wird das GUMG inkl. Ausführungsbestimmungen voraussichtlich Mitte des Jahres 2006 in Kraft setzen.

Der Geltungsbereich des GUMG deckt die genetischen Untersuchungen im medizinischen Bereich, im Arbeits-, Versicherungs- und Haftpflichtbereich ab. Ferner regelt das GUMG die Erstellung von DNA-Profilen zur Klärung der Abstammung oder zur Identifizierung von Personen (vgl. auch unseren 10. Tätigkeitsbericht 2003/2003, Ziffer 5.2.2).

Das Gesetz sieht vor, dass niemand wegen seines Erbgutes diskriminiert werden darf. Genetische und pränatale Untersuchungen dürfen nur durchgeführt werden, sofern die betroffene Person frei und nach hinreichender Aufklärung zugestimmt hat. Jede Person soll zudem das Recht haben, die Kenntnisnahme von Informationen über ihr Erbgut zu verweigern (Recht auf Nichtwissen). Die Durchführung genetischer Untersuchungen untersteht der Bewilligung der zuständigen Bundesstelle.

Im Rahmen der genetischen Untersuchungen soll die betroffene Person eine fachkundige Beratung erhalten. Insbesondere soll sie über Zweck, Risiken, mögliche physische und psychische Belastungen informiert werden. Im Sinne des Transparenzprinzips ist eine umfassende Information der betroffenen Personen zu begrüssen.

Für den Arbeits-, Versicherungs-, Haftpflichtbereich sowie für den Zweck der Klärung der Abstammung sind genetische Untersuchungen grundsätzlich verboten. Unter gewissen Voraussetzungen sind aber Ausnahmen vorgesehen. So sind z. B. genetische Untersuchungen für Lebensversicherungen mit einer Versicherungssumme, welche 400'000 Franken übersteigen, im Prinzip zulässig.

Das GUMG ist aus datenschutzrechtlicher Sicht als gelungen zu bezeichnen und trägt auch dem Selbstbestimmungsrecht der betroffenen Personen Rechnung. Ob und wie das Gesetz in der Praxis umgesetzt wird, bleibt abzuwarten. Schliesslich ist zu erwähnen, dass das GUMG auch die Entwicklung auf internationaler Ebene berücksichtigt. Dies gilt insbesondere für das Europarats-Protokoll über genetische Untersuchungen beim Menschen, welches kurz vor dem Abschluss steht. Es handelt sich hier um ein Zusatzprotokoll zum Übereinkommen des Europarates über Menschenrechte und Biomedizin (mehr dazu in unserem 11. Tätigkeitsbericht 2003/2004, Ziffer 11.1.1).

6 Versicherungen

6.1 Sozialversicherungen

6.1.1 Regelungslücken im medizinischen Datenschutz

Wir wurden vom Bundesamt für Sozialversicherung (BSV) erneut eingeladen, zum Bericht über den medizinischen Datenschutz im Sozialversicherungsbereich Stellung zu nehmen. Unsere Anliegen wurden jedoch nur teilweise berücksichtigt.

Ausgangspunkt des vorliegenden Berichts ist das Postulat der Kommission für Rechtsfragen des Nationalrates (99.093), welches einen «umfassenden, alle Sozialversicherungsbereiche umfassenden Bericht über Regelungslücken im medizinischen Datenschutz» verlangt. Dabei ist insbesondere die technologische Entwicklung und die damit zusammenhängende Missbrauchsgefahr zu berücksichtigen. Im Weiteren soll das Patientengeheimnis nach Art. 321 Strafgesetzbuch (StGB) in die Überlegungen einbezogen werden.

Auch in diesem Berichtsjahr wurden wir vom BSV aufgefordert, zum Vorbericht bzw. zum Bericht jeweils unsere Stellungnahme abzugeben (siehe auch 11. unseren Tätigkeitsbericht 2003/2004, Ziffer 6.1.1). Die Meinungsverschiedenheiten zwischen dem BSV und uns konnten jedoch in wesentlichen Punkten nicht aus dem Weg geräumt werden.

In den verschiedenen Stellungnahmen haben wir zum Ausdruck gebracht, dass der Bericht grundsätzlich in die richtige Richtung geht und einen umfassenden Überblick über Regelungslücken im medizinischen Datenschutz gibt. Insbesondere macht der Bericht auf den Vollzugsnotstand aufmerksam. So wurde etwa richtig erkannt, dass die Transparenz der Datenbearbeitung für die versicherten Personen noch verbesserungswürdig ist. In diesem Sinne wurde der EDSB, der schon seit Jahren auf den datenschutzrechtlichen Vollzugsnotstand im Sozialversicherungsbereich hinweist, bestätigt.

Hingegen fehlen im Bericht Lösungsansätze und konkrete Massnahmen, wie die Lücken gefüllt und der Vollzugsnotstand behoben werden könnten. Wir haben dem BSV diesbezügliche Vorschläge gemacht. Denkbar wäre etwa, im Sozialversicherungsbereich Datenschutz-Audits und Zertifizierungsverfahren von Gesetzes wegen einzuführen. Wir haben schliesslich das BSV gebeten, unsere Stellungnahme dem Bundesrat zu unterbreiten.

6.1.2 Die 5. IV-Revision

Im Rahmen der Ämterkonsultation nahmen wir die Gelegenheit wahr, zur 5. IV-Revision Stellung zu nehmen. Durch eine verstärkte Zusammenarbeit aller Beteiligten soll die Zunahme der Neurenten gedämpft werden. Dies wirft jedoch datenschutzrechtliche Fragen auf.

Die Gesetzesrevision sieht u.a. Massnahmen vor, welche den Verbleib von versicherten Personen im Erwerbsleben ermöglichen soll. Dazu gehört eine verstärkte Zusammenarbeit zwischen Arbeitgeber, Krankentaggeldversicherer und IV-Stelle. Neu sollen Fachstellen für Früherkennung und Begleitung (FEB) geschaffen werden. Die FEB haben den Zweck, umfassende Abklärungen im medizinischen, sozialen und beruflichen Umfeld der versicherten Person durchzuführen bzw. durchführen zu lassen. Damit ist auch eine extensive Datenbearbeitung verbunden.

Im Rahmen der Ämterkonsultation haben wir darauf hingewiesen, dass die Bearbeitung von besonders schützenswerten Personendaten (Gesundheitsdaten) eine gesetzliche Grundlage im formellen Sinn erfordert. Insbesondere der Umfang und der Zweck der Datenbearbeitung ist in einer klaren Rechtsgrundlage festzulegen.

Im Weiteren sind die datenschutzrechtlichen Grundsätze zu berücksichtigen. Das Verhältnismässigkeitsprinzip z. B. verlangt, dass nur diejenigen Personendaten bearbeitet werden dürfen, die für den jeweiligen Zweck geeignet und erforderlich sind. Diesbezüglich ist es sehr heikel, wenn Arbeitgeber in die Abklärungen einbezogen werden sollen. Bereits heute besteht die Tendenz, dass der (kranke) Arbeitnehmer nur noch als Kostenfaktor betrachtet wird. Die Gefahr einer Diskriminierung ist vor allem deshalb nicht von der Hand zu weisen, da ein Kündigungsschutz für den vorliegenden Fall weder im Obligationenrecht noch im vorliegenden Gesetzesentwurf explizit vorgesehen ist.

Zudem hat die Datenbearbeitung für die versicherte Person transparent zu erfolgen (vgl. Art. 4 Abs. 2 DSG). Dies gilt insbesondere für die Bearbeitung von sensiblen Daten betreffend den psychischen Gesundheitszustand (gemäss Botschaftsentwurf betrifft die Zunahme der Neurenten vor allem Personen mit psychischen Problemen). Tatsächlich sieht der Gesetzesentwurf vor, dass die FEB die betroffenen Personen vorgängig und umfassend über Zweck und Umfang der Datenbearbeitung informieren müssen.

Ob und inwiefern die geplante Neuregelung die Persönlichkeitsrechte der Arbeitnehmer berücksichtigt, kann zum jetzigen Zeitpunkt nicht abschliessend beurteilt werden. Dies deshalb, weil die Verfahrensabläufe noch nicht in allen Punkten klar sind bzw. viele Fragen offen lassen. Wir werden die Neuerungen der 5. IV-Revision weiterhin begleiten und auf ihre Datenschutzkonformität hin überprüfen.

6.1.3 KVG-Revision

Nach dem Scheitern der 2. KVG-Revision hat der Bundesrat das Geschäft in zwei Revisionspakete unterteilt. Diese Pakete, welche ihrerseits Revisionen mit individuellen Teilbotschaften enthalten, wurden uns zur Stellungnahme unterbreitet. Datenschutzrechtlich von Bedeutung sind dabei die Einführung der Versichertenkarte sowie die Förderung von Managed-Care-Modellen.

Im Oktober 2004 hat das Parlament die gesetzlichen Grundlagen für die Schaffung einer Versichertenkarte verabschiedet. Der Bundesrat kann demnach eine Versichertenkarte für den KVG-Bereich einführen. Im Weiteren ist er für die Datensicherheit besorgt und regelt insbesondere den Umfang der Datenbearbeitung und den Zugriff. Die Versichertenkarte soll nebst administrativen Daten auch die neue Sozialversicherungsnummer enthalten (vgl. auch unseren 10. Tätigkeitsbericht 2002/2003, Ziffer 6.1.3). Zusätzlich können, die Einwilligung der versicherten Person vorausgesetzt, auch Notfalldaten gespeichert werden. Langfristig gibt es Bestrebungen, aus der Versichertenkarte eine Gesundheitskarte zu machen. Gegenwärtig ist der Bundesrat bzw. das Bundesamt für Gesundheit daran, für die Versichertenkarte ein Umsetzungskonzept inkl. Projektorganisation zu erarbeiten. Wir begleiten dieses Projekt in datenschutzrechtlicher Hinsicht.

Im Weiteren sind im zweiten Revisionspaket sogenannte Managed-Care-Modelle vorgesehen. Konkret sollen Versicherungsmodelle mit integrierten Versorgungsnetzen im Gesetz verankert werden. Managed-Care-Modelle sollen den Versicherten eine umfassende Betreuung in guter Qualität garantieren und mithelfen, die Kosten im Gesundheitswesen einzudämmen.

Zu begrüssen ist, dass die versicherte Person freiwillig entscheiden kann, ob sie an diesen neuen Modellen teilnehmen will oder nicht. Dies entspricht dem Recht auf informationelle Selbstbestimmung, wonach es die versicherte Person ist, welche über die Bearbeitung ihrer Daten bestimmen kann.

Auch ist vorgesehen, den Datenaustausch zwischen den involvierten Stellen vertraglich zu regeln. Soweit jedoch Personendaten im Rahmen der Managed-Care-Modelle bearbeitet werden, genügen Verträge grundsätzlich nicht, und es sind die notwendigen gesetzlichen Grundlagen zu schaffen.

Grundsätzlich bleiben im Gesetzesentwurf aber die einzelnen Informationsprozesse unklar; weder im Gesetzesentwurf noch in der Botschaft ist ersichtlich, wie die neuen besonderen Versicherungsformen bzw. die Datenbearbeitungen im Einzelnen aussehen. Eine abschliessende datenschutzrechtliche Beurteilung der Managed-Care-Modelle ist daher zum jetzigen Zeitpunkt nicht möglich.

6.2 Privatversicherungen

6.2.1 Bekämpfung des Versicherungsmissbrauchs und Datenschutz

Privatversicherer, welche Massnahmen gegen den Versicherungsmissbrauch treffen, sind an die Datenschutzgesetzgebung gebunden. In einem Fall führte dies zur einer umfangreichen Abklärung durch den EDSB.

Privatversicherer treffen vermehrt Massnahmen gegen den Versicherungsmissbrauch. Dabei sind aber in jedem Fall die datenschutzrechtlichen Grundsätze zu berücksichtigen. In der Berichtsperiode haben wir unsere Abklärungen betreffend einen Privatversicherer fortgesetzt und schliesslich abgeschlossen (vgl. auch unseren 11. Tätigkeitsbericht 2003/2004, Ziffer 6.2.2).

Konkret ging es um zwei interne automatisierte Datensammlungen eines Privatversicherers, welche beim EDSB zunächst nicht angemeldet wurden (was im Rahmen der Abklärungen des EDSB schliesslich noch nachgeholt wurde). Beide Datensammlungen haben den Zweck, Versicherungsbetrug bzw. -missbrauch zu bekämpfen. Darin aufgeführt sind etwa Falldaten, Bemerkungen, Personalien, Mitbeteiligte und Angaben über Straf- und Zivilverfahren. Die Datensammlungen enthalten somit besonders schützenswerte Personendaten, allenfalls sogar Persönlichkeitsprofile. Sie betreffen einerseits den Privatversicherungsbereich und andererseits den KVG- und UVG-Bereich.

Unsere Abklärungen ergaben folgende Feststellungen bzw. Schlussfolgerungen:

Beide Datensammlungen sind anmeldungspflichtig und hätten unmittelbar bei Inbetriebnahme beim EDSB angemeldet werden müssen. Tatsächlich geschah dies zu spät. Im Weiteren haben wir den Vorschlag gemacht, die Transparenz der Datenbearbeitung für die versicherten Personen zu verbessern. Denkbar wäre z. B. ein Merkblatt im Antragsverfahren, welches die Versicherten ausführlich über die Datenbearbeitung betreffend den Versicherungsmissbrauch informiert. Die erhöhte Transparenz entspricht auch den Tendenzen auf internationaler Ebene; insbesondere sei hier an die Europarats-Empfehlung Rec(2002) 9 über den Schutz von zu Versicherungszwecken beschafften und bearbeiteten Personendaten erinnert (vgl. auch die laufende DSG-Revision sowie die abgeschlossenen Revisionen des VVG und des VAG, siehe dazu unseren 11. Tätigkeitsbericht 2003/2004, Ziffer 6.2.3).

Zudem stellten wir fest, dass die rechtliche Grundlage für die Datensammlung betreffend den KVG- und UVG-Bereich ungenügend ist. Denn besonders schützenswerte Personendaten und Persönlichkeitsprofile dürfen durch Sozialversicherer grundsätzlich nur dann bearbeitet werden, wenn ein formelles Gesetz dies vorsieht (vgl. Art. 17 DSG). Unseres Erachtens gibt es weder im KVG noch im UVG eine genügende Rechtsgrundlage, welche die systematische Führung einer solchen «Betrugsdatenbank» erlauben würde.

Schliesslich haben wir den Privatversicherer gebeten, die einzelnen Informationsprozesse transparent zu machen bzw. ein Bearbeitungsreglement für die oben erwähnten Datensammlungen auszuarbeiten. Tatsächlich erstellte der Privatversicherer ein Bearbeitungsreglement und tat die Absicht kund, ein periodisches Audit unter Beizug des IT-Sicherheitsoffiziers durchzuführen.

7 Arbeitsbereich

7.1 Die Protokollierung der Kassenaktivitäten zur Klärung von Inventurdifferenzen

Systematische Protokollierungen von Kassenaktivitäten dürfen nur unter Einhaltung bestimmter Voraussetzungen durchgeführt werden. Ins-besondere muss das Risiko eines finanziellen Schadens des Arbeitgebers durch Diebstahl, Betrug oder unbeabsichtigte Fehlmanipulation an der Kasse bestehen. Die betroffenen Personen müssen vorgängig informiert werden. Werden zur Feststellung von Missbräuchen und Fehlmanipulationen Kassenaktivitäten durchgekämmt, hat das in pseudonymer Art und Weise zu erfolgen. Liegen kritische Verhaltensmuster vor, können Personen identifiziert werden.

Eine weltweit tätige Firma gelangte mit der Frage nach der Rechtmässigkeit von systematischen Protokollierungen der Kassenaktivitäten ihrer Angestellten an uns. Die Frage zielte insbesondere darauf ab, mögliche Kollisionen mit dem Datenschutzgesetz und der Arbeitsgesetzgebung abzuklären. Als Zweck der Protokollierung gab die Firma in erster Linie an, systematisch Beweise zur Klärung von vorsätzlich oder fahrlässig herbeigeführten Inventurdifferenzen sichern zu wollen. Die gesammelten Informationen sollten nach bestimmten auffälligen Verhaltensmustern durchsucht werden. Bei der Identifizierung einer Unregelmässigkeit sollten genauere Nachforschungen, gegebenenfalls konzentriert auf einzelne Mitarbeiterinnen oder Mitarbeiter, angestellt werden. Detaillierte Analysen würden erst dann erstellt, wenn verdächtige oder unkorrekte Aktivitäten aufgedeckt worden seien.

Wir haben der Firma Folgendes mitgeteilt:

Die mit der Protokollierung bearbeiteten Daten betreffen eine ganze Reihe von Kassenaktivitäten, die von der Bedieneran- und -abmeldung bis hin zu Kreditkartenaktivitäten, Mitarbeiterkäufen oder zum Einlösen von Gutscheinen gehen. Nebst der Leistung (z. B. Geschwindigkeit an der Kasse) und gegebenenfalls dem deliktischen Verhalten können auch Absenzen am Arbeitsplatz, persönliche Einkäufe oder ähnliches eruiert werden. Da die betroffenen Angestellten bestimmt oder bestimmbar sind, stellen die bearbeiteten Informationen Personendaten im Sinne des Datenschutzgesetzes dar. Beweismittel betreffend deliktisches Verhalten sind gemäss DSG besonders schützenswerte Daten (Daten über strafrechtliche Verfolgungen und Sanktionen). Daten über Leistung und Verhalten können in ihrer Gesamtheit betrachtet sogar Persönlichkeitsprofile darstellen.

Eine solche Protokollierung ist grundsätzlich gerechtfertigt, sofern das Risiko eines finanziellen Schadens des Arbeitgebers durch Diebstahl, Betrug oder unbeabsichtigte Fehlmanipulation an der Kasse gegeben ist und weniger einschneidende Schutzmassnahmen nicht zum selben Ziel führen würden. In diesem Zusammenhang ist aus dem Blickwinkel des Verhältnismässigkeitsprinzips insbesondere dafür zu sorgen, dass Missbräuche bzw. unbeabsichtigte Fehlmanipulationen möglichst von Anfang an technisch oder organisatorisch verhindert werden. Es sind ausserdem nur Filterergebnisse personenbezogen auszuwerten, welche auf Missbräuche bzw. Fehlmanipulationen zurückzuführen sind. Das darüber hinaus erfasste berufliche oder private Verhalten (z. B. Absenzen vom Arbeitsplatz, spezielle Einkäufe) soll nicht ausgewertet werden. Das Verhältnismässigkeitsprinzip ist auch bei der Festlegung der Aufbewahrungsdauer zu berücksichtigen; eine Frist von ein bis zwei Monaten scheint zur Eruierung von verdächtigen Praktiken oder von Fehlmanipulationen an der Kasse auszureichen.

Der Dateninhaber muss seine Angestellten vorgängig informieren. Einerseits müssen Zweck und Funktionen der Protokollierung, andererseits die Folgen einer personenbezogenen Datenauswertung, die Zugriffsrechte, die Aufbewahrungsdauer und das Auskunftsrecht erklärt werden.

Was die Datensicherheit anbelangt, so ist der entsprechende Server gegen den Zugriff unberechtigter Personen zu schützen. Die Rechte sind auf Personen zu beschränken, welche mit der Auswertung der Daten beauftragt sind, sowie auf jene Datenkategorien, welche zur Klärung von Inventurdifferenzen unbedingt nötig sind. Ein Datenaustausch mit anderen Servern ist grundsätzlich nicht zulässig. Der Serverraum ist gegen den Zutritt unberechtigter Dritter mit geeigneten technischen und organisatorischen Massnahmen zu schützen.

Das Verbot der gezielten systematischen Verhaltensüberwachung hat zur Folge, dass diese Art von Kontrolle der Kassenaktivitäten grundsätzlich nur mit pseudonymisierten Personendaten erfolgen darf. Personen dürfen nur bei Auffälligkeiten identifiziert werden. Unter diesen Voraussetzung lässt sich somit sagen, dass die Protokollierung von Kassenaktivitäten zwar eine (leichte) Persönlichkeitsverletzung darstellt, mit Blick auf die Verhältnismässigkeit aber als datenschutzkonform betrachtet werden kann.

7.2 Anwesenheitskontrolle mit Hilfe von Fingerabdrücken

Die Anwesenheitskontrolle am Arbeitsplatz wird heute zunehmend mit softwarebasierten Fingerabdruckkontrollsystemen durchgeführt. Die zentrale Speicherung von Fingerabdrücken ist datenschutzrechtlich bedenklich; es ist weit weniger problematisch, nur die Minuzien in Verbindung mit der Identität zu speichern, sofern entsprechende Sicherheitsmassnahmen angewandt werden. Allerdings würde eine von jedem Beschäftigten beim Stempeln vorgewiesene und ausschliesslich von ihm verwendete Chipkarte mit biometrischen Daten eine verhältnismässigere und daher mit dem Datenschutz zu vereinbarende Lösung darstellen.

Ein in der Genfer Region tätiges Unternehmen stellte uns die Frage, ob die Bearbeitung von Fingerabdrücken zwecks Anwesenheitskontrolle mit dem Datenschutz vereinbar sei. Wir sollten insbesondere prüfen, ob der Einsatz der Biometrie mit Blick auf das angestrebte Ziel gerechtfertigt und verhältnismässig ist. Wir gelangten zu den folgenden Ergebnissen:

Die Anwesenheits- und die Zugangskontrolle zum Arbeitsplatz wird heute zunehmend mit Software durchgeführt. Diese Softwareprogramme können in das Büroautomatik-Umfeld integriert werden, so dass die einschlägigen Daten bisweilen sogar mit anderen Softwareprogrammen abgefragt werden können. Die in der Regel passwortgeschützten Anwesenheitskontrollanwendungen können neben klassischen Datenkategorien (Name, Vorname, Abteilung oder Einheit, Adresse, Arbeitszeiten usw.) auch besondere Vorgänge oder Bewegungen (Zugang innerhalb des Betriebs, Benutzung von Fahrzeugen usw.) erfassen. Bestimmte Applikationen ermöglichen die Datenbearbeitung anhand der Fingerabdrücke der Beschäftigten. Dabei wird zuerst ein digitales Bild des Fingerabdrucks erstellt und analysiert, um die Minuzien (d.h. bestimmte Merkmale des Fingerabdrucks, wie Punkte mit einer Gabelung oder einem Linienende und Rillen auf der Fingeroberfläche) herauszufiltern. In der Authentifizierungsphase erlaubt oder verweigert das System je nach Übereinstimmung zwischen den Minuzien der Finger und dem Referenzmuster den Zugang. Grundsätzlich reicht die *Authentifizierung* allein aus, um einer Person, die so anonym bleibt, den verlangten Zugang zu gewähren. Im Fall der Anwesenheitskontrolle ist eine *Identifizierung* der Personen erforderlich. Dazu empfehlen wir, statt des Vergleichs auf Basis einer zentralisierten Sammlung von mit den entsprechenden Identitäten kombinierten Referenz-Minuzien, eine Benutzeridentifizierung, welche die Angestellten beim Stempeln vorweisen.

Bei Fingerabdrücken und daraus extrahierten Minuzien handelt es sich um statische biometrische Daten. Sie sind normalerweise zeitlich unveränderliche und unverwechselbare Wesensmerkmale einer Person, die sich andere Personen nicht aneignen

können. Ohne Verbindung zur Identität stellen die biometrischen Elemente keine Personendaten dar; mit Verbindung zur Identität dagegen bilden die Fingerabdrücke schützenswerte Daten, da sich daraus die Rassenzugehörigkeit rekonstruieren lässt (was für Minuzien nicht der Fall ist). Im letzten Fall wird eine Datenbank gebildet, für welche die Bestimmungen des Bundesgesetzes über den Datenschutz gelten. Biometrische Daten können nur bearbeitet werden, wenn ein Rechtfertigungsgrund vorliegt oder, falls der Inhaber der Datensammlung ein Bundesorgan ist, eine Gesetzesgrundlage die Bearbeitung vorsieht. Mangels eines Rechtfertigungsgrundes bedeutet die Bearbeitung eine rechtswidrige Persönlichkeitsverletzung, da die betroffene Person durch missbräuchliche Handlungen eines Dritten die Kontrolle über ihre eigenen Fingerabdrücke verliert.

Wenn mit der Identität verbundene Minuzien bearbeitet werden, müssen angemessene Sicherheitsmassnahmen wie z.B. die Chiffrierung der bearbeiteten Daten ergriffen werden. Alle Bearbeitungsschritte – das Speichern, der Vergleich und die Übermittlung von Personendaten – müssen geschützt werden. Der Zweck der Datenbearbeitung muss den betroffenen Personen mitgeteilt werden. Ausserdem sollte der Arbeitgeber die Angestellten konsultieren, bevor er solche Massnahmen ergreift.

Die Individualität und die Unveränderlichkeit der Fingerabdrücke lassen in der Regel eine Verwendung durch Dritte nicht zu. Biometrische Authentifizierungs-Systeme schränken so das Risiko des Kopierens, Diebstahls, Vergessens oder Verlusts, welches bei klassischen Stempelkarten oder Badges auftreten kann, stark ein. Diese Systeme bilden sehr effiziente Identifizierungssysteme, auch wenn sie in seltenen Fällen Fotokopien von Fingerabdrücken, Abformungen von Fingern oder tote Finger akzeptieren. Das Ergebnis des Abgleichs der Minuzien beruht auf Wahrscheinlichkeitsrechnungen, so dass eine irrtümliche Authentifizierung nicht ausgeschlossen werden kann. Fällt eine Identifikation irrtümlich negativ aus, ist das problematisch. Noch problematischer ist es indessen, wenn eine Identifikation irrtümlich positiv ausfällt. Dies macht eine zusätzliche Kontrolle durch eine persönliche Identifikationsnummer (PIN) oder ein Passwort erforderlich. Einzelne Fingerabdrücke können z.B. durch Reinigungsmittel oder eine Verletzung vorübergehend oder dauerhaft verändert werden. Aus diesem Grund wird empfohlen, Referenz-Muster von verschiedenen Fingern der gleichen Person zu sammeln, um die Authentifizierung bei Veränderungen eines Fingerabdrucks zu ermöglichen. Die teilweise oder vollständige Rekonstruktion eines Fingerabdrucks auf der Basis der Minuzien kann nicht gänzlich ausgeschlossen werden. Zwar ist das Risiko des Verlusts des Beweiswertes von Fingerabdrücken infolge von Missbrauch gering, aber die Spezialisten plädieren einstimmig für eine sehr restriktive Verwendung der Fingerabdrücke im privaten Bereich.

Im privaten Bereich und besonders bei der Arbeit ist es legitim, Personendaten zu Zwecken der Anwesenheitskontrolle zu bearbeiten. In bestimmten Situationen können diese Daten auch zur Kontrolle von Bewegungen innerhalb des Betriebs dienen (Räumlichkeiten mit Zugangseinschränkungen, die gesichert werden müssen). Der Einsatz der Biometrie ermöglicht so eine zuverlässige Anwesenheitskontrolle; Datenmanipulation durch den Angestellten ist praktisch ausgeschlossen. Auch das Risiko der Zweckentfremdung von Datenbanken mit Fingerabdruck-Minuzien scheint sehr gering. Es ist sehr schwierig, von den Minuzien ausgehend das Bild eines vollständigen Fingerabdrucks zu rekonstruieren. Das Risiko der Verknüpfung von Datenbanken mit biometrischen Daten ist ebenfalls gering, weil die Extraktions-Algorithmen der Minuzien bislang nicht standardisiert sind. Eine solche Verknüpfung würde allerdings mithilfe von mit diesen Daten verbundenen klassischen Identitätselementen relativ leicht fallen. Die einzige Möglichkeit zur Verhinderung von Verknüpfungen, welche zur Erstellung von Persönlichkeitsprofilen führen könnten, ist die Einschränkung der Bewilligung für die Verknüpfung von Datenbanken.

Zusammengefasst kann die zentralisierte Speicherung von Fingerabdrücken datenschutzrechtlich problematisch sein, die zentralisierte Speicherung der (mit der Identität assoziierten) Minuzien jedoch in weit geringerem Masse, sofern die im DSG vorgesehenen Sicherheitsmassnahmen angewandt werden. Die Abnahme eines Fingerabdrucks, die Extraktion von Minuzien und der Abgleich mit dem vom Angestellten vorgewiesenen Referenzmuster (Authentifizierung) stellt offensichtlich die Lösung mit dem geringsten Risiko einer Persönlichkeitsverletzung dar. Mit anderen Worten: Die Bearbeitung des Referenzmusters in einer persönlichen Chipkarte, die jeder Angestellte beim Stempeln vorweist, stellt eine verhältnismässigere und mit der Datenschutzgesetzgebung zu vereinbarende Lösung dar.

Zur Verwendung von biometrischen Daten im Privatsektor s. auch Ziffer 2.2.2 des vorliegenden Tätigkeitsberichts.

7.3 Tonaufnahmen in den Radarräumen der Firma Skyguide

Zur Verbesserung der Flugsicherheit will die Firma Skyguide in ihren Radarräumen umfassende Tonaufnahmen zulassen. Diese Sicherung von akustischen Beweismitteln soll eine genauere Rekonstruktion von Unfällen und schweren Zwischenfällen ermöglichen. Aus datenschutzrechtlicher Sicht muss sich ein solches Vorgehen auf eine gesetzliche Grundlage stützen (was gegenwärtig nicht der Fall ist) und dem Verhältnismässigkeitsgrundsatz genügen. Insbesondere muss die Notwendigkeit einer derartigen Massnahme nachgewiesen werden.

Ende 2003 ersuchte uns die Skyguide AG und der Sicherheitsdelegierte des Eidg. Departements für Umwelt, Verkehr, Energie und Kommunikation (UVEK) um eine datenschutzrechtliche Beurteilung der geplanten Tonaufnahmen in den Radarräumen der Firma Skyguide mittels Ambient Voice Recording Equipment (AVRE). Nach einem Augenschein haben wir eine schriftliche Stellungnahme zu Handen der Skyguide, des Bundesamts für Zivilluftfahrt (BAZL), des Büros für Flugunfalluntersuchungen (BFU) und der Gewerkschaften der Flugverkehrsleiter verfasst.

AVRE ermöglicht die Aufnahme sämtlicher Gespräche im Radarraum. Die Mikrofone sollen am Arbeitsplatz jedes einzelnen Flugverkehrsleiters eingebaut werden und das gesamte akustische Geschehen erfassen.

Die umfassende Sicherung akustischer Beweismittel soll nach Angaben der verantwortlichen Stellen eine genauere Rekonstruktion von Unfällen und schweren Zwischenfällen zulassen.

Das von Skyguide in groben Zügen vorgestellte Projekt sieht vor, dass der Zugriff auf die Aufnahmen mittels eines sogenannten Dual-Code-Systems und nur auf Anordnung des BFU bei Unfällen oder schweren Zwischenfällen geschehen soll. Dabei soll Skyguide den ersten, die Mitarbeitervertretung den zweiten Teil des Zugriffscodes besitzen; beide Teile sollen für den Zugriff auf die Daten erforderlich sein. Die bereinigte Abschrift der Aufnahmen auf Papier soll nur dem BFU und dem BAZL bekannt gegeben werden.

Die bearbeiteten Informationen stellen Personendaten im Sinne des Datenschutzgesetzes dar, da sie mit bestimmten oder bestimmbaren Personen in Verbindung gebracht werden können. Die Aufnahmen können unter Umständen besonders schützenswerte Personendaten oder Persönlichkeitsprofile enthalten.

Aus dem Blickwinkel der Verhältnismässigkeit stellen wir fest, dass die umfassende akustische Beweissicherung von AVRE dazu geeignet ist, die Rekonstruktion von Unfällen und schweren Zwischenfällen zu erleichtern und die Flugsicherheit zu verbessern. Ob das Erreichen dieser Ziele ein solches System erforderlich macht, ist indessen nicht gänzlich erwiesen. Tatsächlich würden auch jene Gespräche aufgenommen, die nicht bereits durch die üblichen Telefon- oder Funkaufnahmen zwischen Flugverkehrsleiter und Piloten im Cockpit des Flugzeuges registriert werden. AVRE erlaubt technisch keine Unterscheidung zwischen geschäftlichen und privaten Gesprächen. Zudem hat gemäss Bundesamt für Zivilluftfahrt bis heute kein anderes Land ein solch umfassendes Aufnahmesystem eingeführt und es wird auch von keiner internationalen Zivilluftfahrt-Organisation empfohlen. AVRE kann aber für die Rekonstruktion von persönlichen Verantwortlichkeiten innerhalb der Skyguide als geeignet betrachtet werden.

Bezüglich des Verhältnismässigkeitsprinzips bedarf es eines vernünftigen Verhältnisses zwischen Bearbeitungszweck und Persönlichkeitsbeeinträchtigung. Einerseits besteht ein berechtigtes Interesse an einer verbesserten Rekonstruierbarkeit von Unfällen und schweren Zwischenfällen, an der Eruierung von persönlichen Verantwortlichkeiten und der Verbesserung der Flugsicherheit. Andererseits kann nicht geleugnet werden, dass bereits das Wissen um solche Aufnahmen negative Gefühle auslösen kann, die nebst einer Verschlechterung der Arbeitsatmosphäre auch einen nicht zu vernachlässigenden psychischen Druck mit gesundheitlichen Konsequenzen zur Folge haben können. Dann wäre die Einschränkung der Freiheit des Angestellten und die daraus resultierende Persönlichkeitsverletzung erheblich und beträfe nicht nur die für einen Unfall oder schweren Zwischenfall verantwortlichen Personen, sondern sämtliche Angestellte in der Flugverkehrsleitung. Die Verschlechterung der Arbeitsleistungen könnte ebenso eine direkte negative Konsequenz von AVRE sein wie auch ein häufigeres Fehlen vom Arbeitsplatz wegen erhöhtem Bedarf an unüberwachten Zeiträumen.

Werden die Angestellten indessen darüber informiert, dass die Aufnahmen grundsätzlich nicht zugänglich sind und nur über das Dual-Code-System ausgewertet werden können, reduziert sich der Eindruck ständiger Überwachung und damit der Eingriff in die Persönlichkeit beträchtlich. Darüber hinaus sind die betroffenen Angestellten detailliert über die Zwecke von AVRE, Gegenstand und Umfang der Aufnahmen, Auswertungsverfahren, Aufbewahrungsdauer und Auskunftsrecht zu informieren.

In jedem Fall sind die Aufnahmen nur bei einem Unfall oder schweren Zwischenfall und erst auf Anordnung des BFU auszuwerten. Das bedeutet, dass die Aufnahmen nur bei Erfüllung kumulativer, restriktiver Voraussetzungen überhaupt zugänglich sind, was einen bedeutenden Unterschied zu einer Abhörung im Sinne einer ständigen Verhaltensüberwachung darstellt.

Da noch kein konkretes Projekt vorliegt, ist es uns zum jetzigen Zeitpunkt unmöglich, die Verhältnismässigkeit von AVRE zu beurteilen. Insbesondere die Frage nach der Notwendigkeit einer solchen Massnahme ist noch offen. Unter diesen Umständen haben wir der Firma Skyguide empfohlen, Massnahmen zu prüfen, die weniger stark in die Persönlichkeit der betroffenen Personen eingreifen.

Selbst wenn sich die Massnahme mit Blick auf die Verhältnismässigkeit als notwendig erweisen sollte, müsste vor deren Einführung eine ausreichende gesetzliche Grundlage dafür geschaffen werden. Natürliche oder juristische Personen, welche wie Skyguide mit öffentlichen Aufgaben des Bundes betraut sind, benötigen für eine Datenbearbeitung eine gesetzliche Grundlage. Der Einsatz von AVRE erfordert eine detaillierte Reglementierung insbesondere über den oder die Zwecke der Datenbearbeitung, die Systemorganisation, die Zugriffsberechtigungen, die gespeicherten Datenkategorien, das Auswertungsverfahren, den oder die Verantwortlichen der Datensammlung und den Kreis der betroffenen Personen. Gegenwärtig existieren für ein solches System indessen weder nationale Regelungen, noch internationale Normen.

8 Handel und Wirtschaft

8.1 Allgemeine Anforderungen für die Bearbeitung von Motor- und Betriebsdaten in Motorfahrzeugen

Moderne Motorfahrzeuge haben zunehmend neue Technologien (GPS, Chips) eingebaut, welche Informationen zu Routen und Fahrverhalten speichern. Das wirft datenschutzrechtliche Bedenken auf. Zunächst gilt es zu klären, ob es sich dabei überhaupt um Personendaten handelt. Wird diese Frage positiv beantwortet, stellt sich die Frage, welche Daten gespeichert und in welchem Umfang und zu welchem Zweck sie bearbeitet werden. Nicht zuletzt ist auch relevant, wie die gespeicherten Daten vor Zugriff geschützt sind.

Gemäss Definition von Artikel 3 des Datenschutzgesetzes (DSG) gelten alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, als Personendaten. Das Kriterium der Bestimmbarkeit ist erfüllt, wenn die Zuordnung einer Information zu einer Person ohne unverhältnismässigen Aufwand möglich ist. Da die Halterin oder der Halter – und in der Regel auch die Fahrerin oder der Fahrer – eines immatrikulierten Fahrzeuges ohne weiteres bestimmbar ist, sind Informationen über dieses Fahrzeug grundsätzlich als Personendaten zu betrachten. Was Motor- bzw. Betriebsdaten eines Fahrzeuges betrifft, so drängt sich eine Unterscheidung auf zwischen Informationen, die sich auf das Fahrverhalten beziehen oder Rückschlüsse darüber zulassen (z.B. Daten betreffend Geschwindigkeit, Drehzahl, Schaltverhalten), und Informationen, die sich ausschliesslich auf den technischen Zustand des Fahrzeuges beziehen (Ölstand, Reifendruck, etc.). Bei letzteren scheint kein genügend enger Zusammenhang mit einer bestimmten Person zu bestehen. Eindeutig als Personendaten zu betrachten sind dagegen Aufzeichnungen von geographischen Navigationsdaten (z.B. GPS-Koordinaten).

Soweit Motor- und Betriebsdaten von Fahrzeugen als Personendaten zu betrachten sind, ist das DSG anwendbar. Solche Daten dürfen nur rechtmässig beschafft und bearbeitet werden, und die Grundprinzipen des Datenschutzes sind zu beachten.

Wer Daten bearbeitet, braucht einen *Rechtfertigungsgrund*. Im vorliegenden Kontext kommt dafür die Einwilligung der Betroffenen oder die Vertragsabwicklung in Frage. Unabhängig davon müssen aber die vorgesehenen Bearbeitungen aus dem jeweiligen Vertrag hinreichend genau hervorgehen, wie es das *Transparenzprinzip* verlangt. Dementsprechend muss dem Fahrzeughalter mitgeteilt werden, zu welchem Zweck welche Daten wo und von wem gespeichert oder abgefragt und welche Auswertungen vorgenommen werden.

Datenbearbeitungen, die zum Zweck von Garantie- oder Serviceleistungen, Unterhaltsarbeiten und Reparaturen vorgenommen werden, stellen aus der Sicht des Datenschutzes kein Problem dar. Geht die Bearbeitung jedoch darüber hinaus – werden also mehr Daten bearbeitet als notwendig oder zu einem anderen als dem angegebenen Zweck – ist sie nur zulässig, wenn die Betroffenen darüber informiert sind und ihre Zustimmung gegeben haben. Wenn immer möglich sollen die Daten aus Gründen der Verhältnismässigkeit in anonymisierter Form bearbeitet werden.

Die Datenbearbeiter sind darüber hinaus auch verpflichtet, die *Datensicherheit* durch angemessene organisatorische und technische Massnahmen zu gewährleisten. Dazu gehören insbesondere Benutzer- und Zugriffskontrollen sowie die Verschlüsselung von Daten.

Gegebenenfalls sind die Anforderungen an eine rechtmässige Übermittlung der Motor- und Betriebsdaten ins Ausland zu berücksichtigen. Diesbezüglich sei darauf hingewiesen, dass in den EU-Ländern grundsätzlich ähnliche Anforderungen an den Datenschutz gestellt werden wie in der Schweiz.

Betrifft die Auswertung von Motor-, Betriebs- oder geographischen Navigationsdaten einen Dienst- oder Firmenwagen, müssen unter Umständen auch die rechtlichen Anforderungen an eine Überwachung von Mitarbeitenden am Arbeitsplatz beachtet werden. Dies könnte etwa der Fall sein, wenn solche Daten mit Bezug auf einzelne Mitarbeitende ausgewertet werden, die für einen wesentlichen Teil ihrer Tätigkeit auf das Fahrzeug angewiesen sind (z.B. Aussendienstmitarbeitende). Eine solche Überwachung ist nur ausnahmsweise und unter bestimmten Voraussetzungen zulässig.

Polizei und Strafverfolgungsbehörden können – im Rahmen der dafür anwendbaren Rechtsgrundlagen – auf Motor- und Betriebsdaten zugreifen. Will hingegen eine Haftpflichtversicherung Motor- oder Betriebsdaten des Fahrzeuges eines Geschädigten auswerten (lassen), so muss sie sich auf die Einwilligung des Geschädigten oder ein überwiegendes öffentliches bzw. privates Interesse stützen können.

Es lässt sich die Tendenz feststellen, einmal gespeicherte Daten für ursprünglich nicht deklarierte Zwecke wie bspw. Marketingaktionen zu verwerten. Auch aus diesem Grund soll wenn möglich auf nicht zwingend erforderliches Speichern von Daten verzichtet werden bzw. sind gespeicherte Daten periodisch zu löschen. Dies entspricht datenschutzrechtlich auch dem Verhältnismässigkeitsgrundsatz und dem sich daraus ergebenden Prinzip der Datenvermeidung bzw. -sparsamkeit. Mit der gleichen Begründung soll eine Bearbeitung nach Möglichkeit in anonymisierter oder wenigstens pseudonymisierter Form vorgenommen werden. Die Diagnoseerstellung in der Garage bzw. beim Hersteller kann ohne weiteres pseudonymisiert erfolgen, während der Fahrzeughalter nur identifiziert wird, wenn dies zwingend notwendig ist, bspw. bei Garantieleistungen.

Grundsätzlich ist es entscheidend, dass die Kundinnen und Kunden klar darüber informiert werden, welche Betriebs- und Fahrzeugdaten im Fahrzeug gespeichert werden, welche Daten zu Unterhaltszwecken von wem (Garagist, Hersteller, Dritte) abgefragt und/oder weitergeleitet werden, und welche zusätzlichen Bearbeitungen vorgenommen werden (z.B. zu Marketingzwecken). Denn nur so wird die Voraussetzung dafür geschaffen, dass die Kundinnen und Kunden bewusst eine Entscheidung darüber treffen können, welche Bearbeitungen sie akzeptieren.

8.2 Bekanntgabe und Verwendung von Kundendaten durch einen Autoimporteur

Muss ein Garagist seine Kundendaten aus dem Abschluss eines Kaufvertrages an seinen Importeur weiterleiten? Für den betroffenen Garagisten mag es unbefriedigend sein, wenn der Importeur die Kunden direkt anschreibt und ihnen vorschlägt, zu einer anderen Garage, die weiterhin die Markenvertretung sicherstellt, zu wechseln. Unter bestimmten Voraussetzungen ist die Verwendung der Kundendaten durch den Importeur zulässig.

Ein Autoimporteur organisierte sein Markenvertreternetz neu. Zu diesem Zweck schrieb er die Inhaber der Markenautos an und informierte sie darüber, dass ihrem bisherigen Garagisten die Markenvertretung entzogen wurde. Gleichzeitig wurde den Autoinhabern ein neuer Markenvertreter vorgeschlagen. Im selben Schreiben wies der Autoimporteur darauf hin, dass sich die Autoinhaber gegen die Weitergabe ihrer Kundendaten an den neuen Markenvertreter aussprechen können. Zahlreiche Garagisten, denen auf diese Weise die Marktenvertretung entzogen wurde, waren der Ansicht, dass das Vorgehen des Autoimporteurs gegen das Datenschutzgesetz verstösst.

Wir führten daraufhin eine Sachverhaltsabklärung fest, die Folgendes ergab:

Der Garagist (bisheriger Markenvertreter) hat mit Zustimmung der betroffenen Autoinhaber deren Kundendaten für Marketingzwecke an den Autoimporteur weitergeleitet.

Für die Bearbeitung von Personendaten – vorliegend die Weitergabe von Kundendaten – verlangt das Datenschutzgesetz stets einen Rechtfertigungsgrund. Ein möglicher Rechtfertigungsgrund ist die Einwilligung der betroffenen Person. Die Einwilligung kann ausdrücklich oder stillschweigend erfolgen. Welchen Anforderungen die Einwilligung der Betroffenen im konkreten Einzelfall genügen muss, bestimmt sich insbesondere nach der Sensibilität der bearbeiteten Personendaten. Vorliegend wurden die Kunden in den allgemeinen Geschäftsbedingungen zum Kaufvertrag darüber infor-

miert, dass die Kundendaten an den Importeur weitergegeben werden. Demzufolge hat der Garagist die von ihm erhobenen Kundendaten datenschutzkonform weitergeleitet.

Der Autoimporteur informierte die betroffenen Autoinhaber über die geplante Weitergabe der Kundendaten und die Zweckänderung in der Datenbearbeitung. Ein Autoinhaber konnte sich der Weitergabe ihrer Daten an den neuen Markenvertreter widersetzen.

Die Weitergabe der Kundendaten durch den Importeur stellt eine Änderung des ursprünglichen Bearbeitungszwecks dar. Der Autoimporteur informierte die betroffenen Autoinhaber schriftlich über die geplante Weitergabe der Kundendaten. Er räumte ihnen die Möglichkeit ein, sich innerhalb eines bestimmten Zeitraums gegen diese Bekanntgabe auszusprechen. Bei den in Frage stehenden Kundendaten handelte es sich nicht um besonders schützenswerte Personendaten. Eine ausdrückliche Zustimmung der Kunden zur Weitergabe ihrer Daten war demnach nicht notwendig. Das Schweigen eines Kunden konnte in diesem konkreten Fall als gültige Einwilligung im Sinne des Datenschutzgesetzes gewertet werden.

Für die Bearbeitung der Kundendaten kann sich der Importeur zudem auf den Rechtfertigungsgrund des überwiegenden Interesses im Zusammenhang mit der Abwicklung eines Vertrags berufen. Er darf die Kunden grundsätzlich direkt kontaktieren, um ihnen mitzuteilen, dass Änderungen im Vertreternetz geplant sind. Dies gilt namentlich, soweit diese Änderungen eine Auswirkung auf das Vertragsverhältnis zwischen einem Garagisten, dem die Markenvertretung entzogen werden soll, und dessen Kunden haben (weil z.B. der Vertrag Garantieleistungen vorsieht, die nur ein Markenvertreter erfüllen kann). Der Importeur darf aber ohne die Zustimmung der Kunden deren Personendaten nicht an andere Garagisten, die weiterhin die Vertretung der betreffenden Marke innehaben, weiterleiten.

Das Datenschutzgesetz verleiht dem bisherigen Garagisten keine Ansprüche auf jene Kundendaten, die dieser datenschutzkonform (d.h. mit Einwilligung der Betroffenen) an den Autoimporteur bekannt gegeben hat.

Nach Datenschutzgesetz stehen nur den Personen, deren Daten bearbeitet werden, Abwehrrechte bezüglich der Bearbeitung dieser Daten zu. An einer Datensammlung Beteiligte – im vorliegenden Fall die Garagisten – können im Hinblick auf die Bearbeitung der von ihnen beschafften und an Dritte weitergeleiteten Daten keine Rechte geltend machen.

Unsere Sachverhaltsabklärung hat somit ergeben, dass die Weitergabe von Kundendaten durch den Importeur mit dem Datenschutzgesetz im Einklang steht.

9 International

9.1 Europarat

9.1.1 Arbeiten des T-PD: Biometrische Daten – Rechte der betroffenen Personen – Internet

Die Schwerpunkte in den Arbeiten des beratenden Ausschusses des Übereinkommens 108 (T-PD) und des Vorstands bildeten die Redaktion eines Berichts über die Anwendung der Grundsätze des Übereinkommens 108 auf die Erhebung und Bearbeitung von biometrischen Daten, die Prüfung der Relevanz der grundlegenden Datenschutzprinzipien, die globalen Telekommunikationsnetze sowie die Analyse der Rechte und Verantwortlichkeiten der betroffenen Personen.

Nach den Strukturveränderungen im Europarat und besonders nach der Auflösung der Projektgruppe für den Datenschutz CJPD (siehe unsere 11. Tätigkeitsbericht 2003/2004, Ziffer 11.1.2) ist der T-PD als einziges Gremium des Europarates für Fragen des Datenschutzes zuständig. Der Ausschuss setzt sich aus den Vertretern aller Staaten zusammen, welche das Übereinkommen 108 ratifiziert haben. Die übrigen Mitgliedsländer des Europarates können als Beobachter an den Arbeiten teilnehmen. Der Ausschuss hat einen Vorstand, bestehend aus 7 Vertretern der Vertragsparteien, darunter der Vertreter der Schweiz, mit der Vorbereitung der Arbeiten betraut.

Der Ausschuss widmete sich vorrangig der Ausarbeitung eines Berichts über die Anwendung der Prinzipien des Übereinkommens 108 auf die Erhebung und Bearbeitung von biometrischen Daten. Der Bericht wurde anlässlich der 20. Plenarversammlung vom 2. – 4. Februar 2005 vom Ausschuss verabschiedet. Das Dokument ist als Zwischenbericht zu sehen. Der Ausschuss hatte nicht die Absicht, eine juristische Urkunde auszuarbeiten, welche einen sich laufend verändernden Bereich regeln sollte, sondern schlug auf der Basis der aktuellen Erkenntnisse Orientierungen vor; gegebenenfalls kann später eine Rechtsurkunde ausgearbeitet werden. In den Schlussfolgerungen hielt der Ausschuss fest, dass die folgenden Grundsätze beim Einsatz von biometrischen Daten besonders berücksichtigt werden müssen:

- Evaluation der Vor- und Nachteile des Einsatzes von biometrischen Daten für die Privatsphäre der betroffenen Personen; Berücksichtigung von Alternativlösungen; Wahl eines Systems, welches möglichst wenig in die Privatsphäre eingreift;
- Befolgung des Zweckbindungsgrundsatzes;

- Befolgung des Verhältnismässigkeitsgrundsatzes; mit einem Datenbearbeitungssystem dürfen nicht mehr Personendaten erhoben und bearbeitet werden, als der Bearbeitungszweck erfordert;
- Lösungen zur Identifizierung von betroffenen Personen sind zu vermeiden, wenn die Verifizierung für die Bearbeitungszwecke ausreicht;
- bei der Verifizierung der Identität der Einzelpersonen sollten die biometrischen Daten vorzugsweise auf einem gesicherten individuellen Speichermedium (z.B. Chipkarte) gespeichert werden;
- Information der betroffenen Personen über die Zweckbindung des Systems, die Identität des für die Bearbeitung Verantwortlichen, die bearbeiteten Daten und die Empfängerkategorien;
- Befolgung des Auskunfts- und des Berichtigungsrechtes;
- Befolgung des Datensicherheitsprinzips;
- Entwicklung von Zertifizierungs- und Kontrollverfahren;
- Vorhandensein eines Verfahrens zur Neuüberprüfung, wenn eine in einem biometrischen System registrierte Person zurückgewiesen wird.

Der Ausschuss prüfte ausserdem die Relevanz der Grundsätze des Übereinkommens 108 für die globalen Telekommunikationsnetze und besonders für das Internet. In diesem Zusammenhang nahm er einen Sachverständigenbericht zur Kenntnis, welcher das Fazit zieht, dass die Prinzipien des Übereinkommens 108 den aktuellen Herausforderungen des Internets und der neuen Technologien entsprechen. Allerdings wird vorgeschlagen, das Übereinkommen um neue Grundsätze zur Förderung der informationellen Selbstbestimmung im aktuellen technologischen Umfeld zu ergänzen: Es handelt sich um die Grundsätze Verschlüsselung, «reversible» Anonymität, Vorteile auf Gegenseitigkeitsbasis, Förderung von datenschutzkonformen Technologielösungen oder solchen, die den rechtlichen Schutz der Personen verbessern, Kontrolle des Betriebs der Endgeräte durch die Benutzer, Gewährung von Schutzmöglichkeiten an die Verbraucher und an die Benutzer bestimmter Informationssysteme. Der Ausschuss hat den Vorstand beauftragt, den Bericht eingehend zu prüfen und künftige Schritte festzulegen.

Im Anschluss an eine Konferenz über die Rechte und Verantwortlichkeiten der von Datenbearbeitungen betroffenen Personen, ausgerichtet vom Europarat und vom Datenschutzbüro der Tschechischen Republik in Prag vom 14. bis zum 15. Oktober 2004, beschloss der beratende Ausschuss, die Sensibilisierung der betroffenen Perso-

nen und der für die Bearbeitung Verantwortlichen zu verbessern (siehe unten, Ziffer 9.1.2). Vor diesem Hintergrund stimmte der beratende Ausschuss dem Vorschlag der Schweiz zu, einen europäischen Tag des Datenschutzes einzuführen, der jedes Jahr am 28. Januar stattfinden soll. Das Ministerkomitee des Europarates muss noch grünes Licht für diese Initiative geben. Schliesslich einigte sich der beratende Ausschuss darauf, unseren Vorschlag, das grundlegende Recht auf Datenschutz in den Urkunden des Europarates zu verankern, weiter zu verfolgen.

9.1.2 Konferenz über die Rechte und Verantwortlichkeiten der von den Daten betroffenen Personen

Am 14. und 15. Oktober 2004 tagte in Prag die vom Europarat und vom Datenschutzbüro der Tschechischen Republik organisierte Konferenz über die Rechte und Verantwortlichkeiten der Personen, über die Daten bearbeitet werden. Die Konferenz legte den Schwerpunkt auf die Notwendigkeit der Sensibilisierung der Einzelpersonen für ihre Rechte und Pflichten im Datenschutz.

Die Hauptthemen der Konferenz waren die Sensibilisierung der von Datenbearbeitungen betroffenen Personen für ihre Rechte und Verantwortlichkeiten, damit sie den Schutz der eigenen Daten selbst in die Hand nehmen, ebenso wie die Information der betroffenen Personen, die Zustimmung und die Umsetzung der Rechte. Die Teilnehmer befassten sich mit der Verbesserung der Kenntnisse der Einzelpersonen im Bereich Datenschutz. Mit der Globalisierung der Informations- und Kommunikationstechnologien (grenzüberschreitende Informationssysteme mit unbeschränkten Kapazitäten) wurde die Kontrolle der Einzelpersonen über ihre eigenen Informationen stark beschnitten. Einerseits wissen die Einzelpersonen nicht ausreichend Bescheid über die Rechte, die ihnen aus den Datenschutzgesetzen erwachsen. Anderseits tendieren die Verantwortlichen für die Datenbearbeitung dazu, sich über diese Gesetze hinwegzusetzen. Deshalb müssen die Gesetze mit Aspekten der Selbstregulierung, mit Zertifizierungsverfahren und Technologielösungen ergänzt werden. Die Sensibilisierung darf nicht allein den Behörden überlassen werden. Auch andere Akteure, insbesondere Dienstleistungsanbieter, Hersteller von Hardware- oder Software-Ausrüstungen sowie Organisationen für die Verteidigung der individuellen Rechte, müssen auf den Plan treten. Die Transparenz bei der Bearbeitung von Personendaten muss erhöht werden; die Einzelnen müssen über das Funktionieren der Informationssysteme orientiert werden, damit sie das eigene Informationsumfeld besser verstehen. Das ist sehr wichtig, weil heute praktisch alle Handlungen und fast jeder Einsatz von Technologie zur Bearbeitung von Personendaten führen. Die Daten-

schutzbehörden sollen ihre Informations- und Aufklärungsarbeit bei den betroffenen Personen und bei den Verantwortlichen für die Datenbearbeitung intensivieren. Sie sollten ein offenes Ohr für die Anliegen der Bürgerinnen und Bürger haben und ihnen benutzerfreundliche Informationen anbieten. Schliesslich müssen die Behörden auch die Kontrolltätigkeiten vertiefen. Dazu brauchen sie entsprechende Mittel und Ressourcen. Sensibilisierung setzt Ausbildung, die Integration des Datenschutzes in die Lehrpläne von Schulen und Universitäten sowie die Einführung von Datenschutz-Lehrgängen voraus.

9.2 Europäische Union

9.2.1 Datenschutz und die Bilateralen II

Die Umsetzung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union (Bilaterale II) hätte zur Folge, dass mehrere schweizerische Erlasse angepasst werden müssten. Davon betroffen wären auch Bestimmungen, die datenschutzrechtliche Inhalte aufweisen. Besondere Bedeutung kommt dem Datenschutz bei den beiden Assoziierungsabkommen Schengen/Dublin zu.

Im Rahmen der Assoziierung der Schweiz an Schengen/Dublin muss jede Bearbeitung von Personendaten in den Bereichen, die unter den ersten Pfeiler der EU fallen (Grenzkontrollen, Visa, Feuerwaffen, Betäubungsmittel und Asyl), den Anforderungen der EU-Datenschutzrichtlinie 95/46/EG genügen. Die Übernahme deren materiellen Gehalts erfordert Anpassungen der entsprechenden schweizerischen Spezialgesetze.

Die Umsetzung der Bilateralen II zieht die Einführung einer materiell identischen Bestimmung für das Bundesgesetz über Aufenthalt und Niederlassung der Ausländer, das Asyl- und das Waffengesetz nach sich. Sie regelt die möglichen Fälle der Datenweitergabe einer Schweizer Behörde in Staaten, die nicht an Schengen beteiligt sind. Gemäss EU-Datenschutzrichtlinie ist diese Datenweitergabe nur zulässig, wenn der Drittstaat ein angemessenes Datenschutzniveau gewährleistet. Fehlt ein angemessenes Datenschutzniveau, soll eine Datenweitergabe unter bestimmten Voraussetzungen trotzdem möglich sein, u.a. wenn der Datenempfänger im Einzelfall ausreichende Garantien für den Persönlichkeitsschutz der betroffenen Personen bietet. Den Umfang der Garantien und die Modalitäten der Garantieerbringung soll dabei der Bundesrat bestimmen. In der Ämterkonsultation zur Botschaft haben wir beantragt, dass der Eidgenössische Datenschutzbeauftragte diese Funktion wahrnehmen soll, da es bei der Bewilligung einer Datenbekanntgabe nicht um eine politische, sondern alleine

um eine datenschutzrechtliche Beurteilung geht. Der EDSB verfügt über die notwendige Sachkenntnis, um festzustellen, welche Garantien für den Persönlichkeitsschutz der Betroffenen ergriffen werden müssen, und ist somit geeigneter als Bundesrat, diese Funktion wahrzunehmen.

Für den Datenschutz in den Bereichen von Schengen, die unter den dritten Pfeiler der EU fallen (polizeiliche Zusammenarbeit und justizielle Kooperation in Strafsachen) und in denen die Datenschutzrichtlinie folglich nicht zur Anwendung kommt, enthält das Schengener Durchführungsübereinkommen spezifische Datenschutzvorschriften, die zu einem grossen Teil direkt anwendbar und somit von den Schweizer Behörden ohne vorgängige Umsetzung ins innerstaatliche Recht unmittelbar berücksichtigt werden müssen. Soweit eine Umsetzung ins schweizerische Recht gleichwohl erforderlich ist, wird im Strafgesetzbuch die notwendige formell-rechtlich Grundlage geschaffen.

Im Rahmen von Schengen/Dublin soll der Datenschutzbeauftragte zusätzliche Funktionen wahrnehmen (national zuständige Kontrollinstanz des nationalen Teils des Schengener Informationssystems SIS, Mitglied der gemeinsamen Kontrollinstanz und Teilnahme Datenschutzgruppe Art. 29 Datenschutzrichtlinie, Ausschuss Datenschutz Art. 31 Datenschutzrichtlinie und Arbeitsgruppe Datenschutz im Bereich des 3. Pfeilers). Diese neuen Aufgaben wird der EDSB nur mit zusätzlichen Ressourcen wahrnehmen können. Mit der Aufgabenerweiterung sind zudem Folgekosten verbunden, die im Budget des EDSB berücksichtigt werden müssen.

9.2.2 Europäische Konferenz der Datenschutzbeauftragten

Die europäische Konferenz der Datenschutzbeauftragten tagte vom 21. – 23. April 2004 in Rotterdam und am 14. September 2004 in Wroclaw. Sie verabschiedete insbesondere die Regeln über die Akkreditierung der Datenschutzbehörden bei der Konferenz.

Auf dieser Konferenz versammelten sich die Datenschutzbeauftragten der 31 europäischen Staaten, welche das Übereinkommen 108 ratifiziert haben, darunter die 25 Mitgliedsstaaten der Europäischen Union. Bosnien-Herzegowina nahm als Beobachterland an der Konferenz teil. Die Delegierten der Kontrollbehörden der europäischen Kommissionen, von Europol, Schengen und Eurojust sowie Vertreter der Europäischen Kommission und des Sekretariats des Europarates beteiligten sich ebenfalls an den Arbeiten.

Die erste Sitzung der Konferenz war der Untersuchung der Rolle der Datenschutzbehörden gewidmet. Gemäss dem Berichterstatter Prof. Colin J. Bennett von der Universität Victoria (Kanada) hat sich die Globalisierung der Gesellschaft auf die Rolle, die

Organisation und die Ansätze der Datenschutzbehörden ausgewirkt. Datenschutzgrundsätze werden je nach Staat unterschiedlich umgesetzt, es existieren mehrere Instrumente nebeneinander: Bewilligungsmodell, Datenschutzbeauftragter, Registrierungsmodell, Selbstkontrolle. Die Rolle der Datenschutzbeauftragten steht im Wandel. Sie erfüllen verschiedene Aufgaben: Mediator, Kontrolleur, Berater, Erzieher, Ausbilder, Verhandlungsführer, Fürsprecher, Botschafter usw. Lösungen werden vermehrt gemeinsam mit den verschiedenen Akteuren gesucht. Die Datenschutzbehörden müssen als unverzichtbare Akteure der Datenschutzinstrumente ihre Präsenz und ihre Zusammenarbeit festigen und sich bewusst werden, dass sie eine wichtige Kraft darstellen. Es wäre wünschenswert, dass die Datenschutzbehörden häufiger Entschliessungen auf internationaler Ebene verabschieden. Ausserdem soll ihre proaktive und allgemeine Rolle gegenüber der reaktiven und spezifischen Rolle überwiegen.

Anlässlich der zweiten Sitzung befasste sich die Konferenz mit der Kommunikationspolitik und der Interaktion der Datenschutzbehörden mit der Aussenwelt. Die Europäische Kommission stellte die Ergebnisse einer umfassenden Erhebung vor, welche in allen EU-Staaten bei den Verantwortlichen für Datenbearbeitungen und bei den Bürgerinnen und Bürgern durchgeführt worden war. Die Umfragen lassen Bedarf an einer Aufstockung der Ressourcen für die Sensibilisierung und Information der Öffentlichkeit erkennen. Die Datenschutzbeauftragten wissen, dass die Information Lücken aufweist. Sie plädieren dafür, den Schwerpunkt auf Sensibilisierung, Ausbildung, Information und Kommunikationspolitik zu setzen.

Die dritte Sitzung war den Fragen der Umsetzung gewidmet. Nach einigen Vorträgen über nationale Systeme sprachen sich die Datenschutzbeauftragten für eine bessere Harmonisierung der operationellen Mechanismen und für gemeinsame Aktionen aus. Dabei rückten sie die Bedeutung des Informationsaustausches in den Vordergrund.

Auf der vierten Sitzung wurden die interne Organisation der Datenschutzbehörden sowie die Verbesserung ihrer Effizienz und ihres Bildes nach aussen behandelt. Nach Auffassung der Datenschutzbeauftragten ist es von grundlegender Bedeutung, die Interessen der Bürger im Auge zu behalten und auf die gesellschaftliche Akzeptanz des Datenschutzes hinzuarbeiten.

Anlässlich der fünften Sitzung setzten sich die Datenschutzbeauftragten mit Fragen der Justizzusammenarbeit in der Europäischen Union auseinander. Dabei betonten sie die Schlüsselrolle des Datenschutzes und plädierten für gemeinsame Regeln. Ausserdem wurden einige Probleme erörtert, die mit dem Rechtsrahmen, den verschiedenen beteiligten Instanzen (internationale Organisationen wie Europol, Schengen, Interpol, Europarat und nationale Organisationen) sowie den verschiedenen Ansätzen zu-

sammenhängen. Mehrere Staaten haben bilaterale Abkommen abgeschlossen, in welchen der Datenschutz unterschiedlich behandelt wird, was den bestehenden Rahmen zu schwächen droht: Im Datenschutzbereich ist ein globalisierter und pragmatischer Ansatz erforderlich.

Die Datenschutzbeauftragten plädieren für die langfristige Zusammenführung der Datenschutzbehörden von Europol, Schengen, Eurodac, Eurojust und der europäischen Kommissionen in eine einzige Behörde. Das setzt künftig institutionelle Veränderungen voraus. Aus dieser Perspektive setzte die Konferenz der Datenschutzbeauftragten eine Arbeitsgruppe ein, die beauftragt wird, Strategie und Zielsetzungen festzulegen und sich mit den von der EU gewünschten Massnahmen zur Terrorismusbekämpfung auseinander zu setzen.

Die Konferenz verabschiedete eine Weisung zur Festlegung ihrer Aufnahmekriterien. So wird die Erweiterung der Konferenz auf alle europäischen Staaten beschlossen, welche das Übereinkommen 108 ratifiziert haben, und zwar in Übereinstimmung mit unseren Vorschlägen anlässlich der Konferenz von Sevilla im Jahr 2003. Die Konferenz setzte einen Akkreditierungsausschuss ein, zu dem Spanien, die Niederlande und Polen gehören.

9.3 OECD

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

Die Arbeitsgruppe beschäftigte sich mit der Umsetzung der revidierten Sicherheitsrichtlinien der OECD, der Erstellung einer Website und eines Online-Ausbildungstools in Sachen Sicherheit. Weitere Themen waren die Verstärkung der Massnahmen zur Erhöhung der internationalen Reisesicherheit, der Stand der Implementierung von Authentifizierungsverfahren in den Mitgliedstaaten und die Transparenzanforderungen bei Datenschutzerklärungen.

Die Arbeitsgruppe erarbeitete einen Fragebogen, mit dem Angaben zur Umsetzung der Sicherheitsrichtlinien bei den einzelnen Mitgliedländern erhoben wurden. Damit sollen die Bereiche definiert werden, bei denen weiterer Handlungsbedarf besteht. Gleichzeitig mit dem Fragebogen wurde ein leicht verständliches Inventar der verschiedenen praktischen Sicherheitsmethoden erstellt, die in den Mitgliedländern zur Anwendung kommen.

Daneben richtete das Sekretariat eine Sicherheitswebsite ein, um jederzeit einen vollständigen Überblick über die Sicherheitsmethoden zu erhalten, die in den Mitgliedstaaten zur Anwendung kommen.

Um die Umsetzung von Sicherheitsmassnahmen bei KMUs und Endbenutzern zu fördern, wurde entschieden, ein Online-Ausbildungstool zur Umsetzung von Sicherheitsmassnahmen zu entwickeln. Das Ausbildungstool soll die verschiedenen Sicherheitsoptionen aufzeigen und die Sensibilität bei Unternehmen und Benutzern erhöhen. Angesichts der knappen Ressourcen der Arbeitsgruppe stellte sich die Frage, ob die OECD ein eigenes Tool entwickelt, oder ob stattdessen ein bereits bestehendes weiterentwickelt bzw. gefördert werden sollte. Zudem wäre im Hinblick auf die unterschiedlichen Betriebssysteme und Unternehmensstrukturen die Erstellung eines einheitlichen Sicherheitstools, das allen nationalen und internationalen Anforderungen genügen sollte, sehr schwer zu realisieren. Es wäre deshalb von Vorteil, stattdessen eher Online-Tools für diverse Sicherheitsanalysen mittels Checklisten anzustreben; diese müssten eine einfache Struktur aufweisen, damit sie auch von KMUs verwendet werden könnten. Dabei ist zu bedenken, dass es schwierig sein wird, solche Checklisten für eine weltweite Benutzung durch KMUs zu entwickeln. Es wäre deshalb denkbar, eine internationale Sicherheitsnorm (z.B. ISO 17799) zu übernehmen, um über diesen Kanal die erste Sicherheitsebene zu überprüfen. Gleichzeitig könnten auch die länderspezifischen Anforderungen (analog zum OECD-Generator für Datenschutzerklärungen) einbezogen werden. Das Sekretariat wird in Zusammenarbeit mit einigen Mitgliedländern eine mögliche Lösung erarbeiten und an der nächsten Sitzung vorstellen.

Ein anderes Thema, das die Arbeitsgruppe beschäftigte, war die internationale Reisesicherheit. Die OECD hat sich zum Ziel gesetzt, die Verifizierung der Identität im Reiseverkehr zu verstärken. Dabei ist auf die Interoperabilität der verschiedenen technischen Lösungen zu achten. Gleichzeitig sollte aber der Reiseverkehr nicht unnötig erschwert werden. Die Gewährleistung eines reibungslosen und sicheren Reiseverkehrs darf aber nicht auf Kosten der Privatsphäre der Passagiere gehen. Deshalb werden nebst dem Einbezug der dafür geschaffenen Expertengruppe des ICAO auch den Arbeiten des Europarats und der EU-Arbeitsgruppe, die in Art. 29 der EU-Datenschutzrichtlinie 95/46/EG vorgesehen ist, Rechnung getragen, welche sich mit den Bereichen Biometrie und Reisesicherheit bereits intensiv auseinander setzen. Die Expertengruppe hat begonnen, an den Prinzipien für die Verwendung von biometrischen Merkmalen zur Verifizierung der Identität von Reisenden zu arbeiten. Dabei werden praktische Informationen zusammengetragen, um eine Richtlinie zu erstellen, die den Datenschutz- und Datensicherheitsanforderungen Rechnung trägt. In einer ersten Phase soll eine Datenbank über gestohlene und verlorene Reisepässe eingerichtet werden.

Die USA gaben klar zu erkennen, dass sie ein grosses Interesse an Biometriedatenbanken haben, namentlich an solchen, die einen ständigen Datenaustausch ermöglichen (crossborder realtime information sharing). Dabei haben sie drei Prioritäten: Datenschutz und -sicherheit, den weltweiten Austausch der Daten und die Überprüfung der technischen Lösungen. Gleichzeitig wurde klar und unmissverständlich erklärt, dass die Arbeiten in diesem Bereich beschleunigt werden müssen.

In Sachen Biometrie wurde auch ein Bericht des Europarates vorgestellt. In diesem sensiblen, technisch hoch komplexen Bereich werden nicht wie üblich von Anfang an Grundprinzipien zur Biometrie erarbeitet. Stattdessen wird an einem so genannten Stufenbericht (Rapport d'étapes) gearbeitet. Darin werden Fragen der Sicherheit – insbesondere der Zugriffssicherheit –, des Zwecks, der Verwendung solcher Daten, der Verifizierung ihrer Authentizität und der Speicherung durch Dritte behandelt. Der Schlussbericht wird im Sinne einer Bestandesaufnahme im Bereich der Biometrie angelegt, worin auch Hinweise auf Risiken, Sicherheitsanforderungen und Interoperabilität enthalten sind und die Fragen der zentralen oder dezentralen Speicherung behandelt werden.

Im Bereich der elektronischen Authentifizierung ist eine Umfrage in allen Mitgliedstaaten im Gange, die zum Ziel hat, Beispiele für die aktuelle Implementierung von Authentifizierungsverfahren aufzuführen. Dazu gehören alle Technologien, die in diesem Zusammenhang zur Anwendung kommen, ebenso wie die (insbesondere technischen) Barrieren, welche die Weiterentwicklung behindern.

Die von der OECD ins Leben gerufenen Task Force in Sachen Spam hat als erklärtes Ziel die Entwicklung eines kompletten Antispam-Tools, das nebst der Erfüllung gesetzlicher Anforderungen und der Bereitstellung technischer Lösungsvarianten auch als Ausbildungs- und Informationsinstrument für die Benutzerinnen und Benutzer dienen soll.

Schliesslich befasste sich die Arbeitsgruppe mit den Informations- und Transparenzanforderungen bei der Bearbeitung von Personendaten (auch Datenschutzerklärungen, privacy notices oder Global multi-layered notices genannt). Die anlässlich der 25. Internationalen Datenschutzkonferenz in Sydney verabschiedete Resolution über Datenschutzerklärungen wurde erläutert. Daneben wurde festgestellt, dass die Datenschutzerklärungen gegenwärtig in der Regel nicht nur zu lang, sondern in den meisten Fällen für die Benutzerinnen und Benutzer auch unverständlich sind. Es besteht unter Datenschutzbehörden und im privaten Sektor Einigkeit darüber, dass Datenschutzerklärungen kurz, klar und verständlich sein müssen. Zudem müssen die Datenschutzerklärungen einer Website leicht auffindbar sein. Zu den üblichen Anforderungen einer Datenschutzerklärung siehe auch unseren 6. Tätigkeitsbericht 1998/99, Ziffer 4.1.

Neu ist bei der Problematik von Datenschutzerklärungen der Vorschlag der US-Organisation e-trust, ein weltweit einheitliches Format (common template) zur Verfügung zu stellen, um damit die Verständlichkeit für die Benutzerin oder den Benutzer zu erhöhen. Die verschiedenen Organisationen, die ein international anerkanntes einheitliches Format und eine kurze, aber informative Datenschutzerklärung begrüssen, befürworten dieses Vorgehen ebenso wie die EU-Gruppe des Art. 29.

Das Sekretariat schlug vor, Arbeiten im Bereich von Datenschutzerklärungen nicht zu duplizieren, sondern die sich im Gange befindenden Bemühungen mitzuverfolgen und gegebenenfalls mitzugestalten. Gesetztes Ziel der OECD ist es, eine derartige Musterdatenschutzerklärung zu erarbeiten, die mittels des OECD-Datenschutzgenerators automatisch erzeugt werden kann.

Ziel einer solchen Musterdatenschutzerklärung ist nicht eine komplette und mit allen nationalen Bestimmungen kompatible Lösung. Vielmehr geht es darum, eine (in Format und Text) uniforme Datenschutzerklärung zu erstellen, die es durch ihre Prägnanz dem Benutzer erlaubt, Unterschiede in der Bearbeitung von Personendaten durch Unternehmen einer gleichen Branche oder eines anderen Landes klar erkennbar zu machen.

Alle Delegationen begrüssten die Arbeiten zur Verbesserung von Datenschutzerklärungen, insbesondere, weil dadurch nicht nur die rechtlichen Transparenzanforderungen erfüllt werden, sondern weil sie auch für den Endbenutzer von unmittelbarem praktischem Nutzen sein werden.

9.4 Weitere Themen

9.4.1 Internationale Konferenz der Datenschutzbeauftragten

Die 26. Internationale Konferenz der Datenschutzbeauftragten tagte vom 14. bis zum 16. September 2004 in Wroclaw. Delegationen aus rund 40 Staaten aus der ganzen Welt nahmen daran teil. Die Konferenz war dem allgemeinen Thema «Das Recht auf Privatsphäre – das Recht auf Würde» gewidmet. Die Datenschutzbeauftragten verabschiedeten eine Entschliessung über das Projekt von ISO-Normen zum Schutz der Privatsphäre.

Die 26. Internationale Konferenz der Datenschutzbeauftragten, welche dem Thema «Das Recht auf Privatsphäre – das Recht auf Würde» gewidmet war, fand auf Einladung der polnischen Datenschutzbehörde in den Räumlichkeiten der Universität von Wroclaw statt. Polen richtete als erstes der mittel- und osteuropäischen Länder die

Internationale Konferenz aus. Die Wahl des Konferenzthemas und der Gaststadt – am Kreuzweg unterschiedlicher historischer Nationen und Kulturen – veranschaulichte, dass die Bearbeitung von Personendaten zur Negierung der Menschenwürde führen kann, wenn die demokratische Kontrolle fehlt. Dabei wurde betont, dass besonders die juristischen Datenschutzinstrumente eine Schlüsselrolle für die Garantie der Menschenwürde spielen. Die Konferenz bot wie üblich Gelegenheit zu einem breiten Gedanken- und Erfahrungsaustausch unter Datenschutzbeauftragten, Vertretern der internationalen Organisationen, der Wirtschaft, der Medien sowie der Universitäts- und Wissenschaftskreise. Dabei wurden nicht nur die Risiken einer Beeinträchtigung der Grundfreiheiten und -rechte erörtert – vor allem wegen der technologischen Entwicklungen und wegen der Universalität der Information – sondern auch die Mittel zum Schutz der Privatsphäre. Diese Themen wurden im Rahmen von Plenarversammlungen und von Parallelveranstaltungen behandelt. Die Konferenz befasste sich mit dem Recht auf Privatsphäre und mit dem Schutz der öffentlichen Sicherheit, mit den RFID-Technologien (Radio-Frequenz-Identifikation, Identifizierung per Funk), mit dem Schutz der Privatsphäre am Arbeitsplatz, mit dem Recht auf Privatsphäre gegenüber den Medien sowie mit E-Demokratie und grenzüberschreitenden Datenflüssen. Die Datenschützer setzten sich mit den Erwartungen der Wirtschaft auseinander und stellten fest, dass der Datenschutz zwar bisweilen hohe Kosten verursacht, sich aber für die Unternehmen als nützlich erweist. Die Konferenz setzte den Schwerpunkt auf die internationale Zusammenarbeit unter den Datenschutzbehörden.

Schliesslich befasste sich die Konferenz mit den Fragen der biometrischen Identifizierung des Menschen. In diesem Zusammenhang präsentierten wir einige Aspekte des Datenschutzes bei der Verwendung von biometrischen Daten im Privatsektor (http://www.edsb.ch/f/doku/fachpresse/index.htm). Der Einsatz der Biometrie beschränkt sich nicht mehr auf besondere Sektoren wie Strafermittlung und -verfolgung, sondern hält generell in zahlreichen Anwendungen des öffentlichen und privaten Sektors Einzug. Die Biometrie lässt sich nicht auf eine Technologie reduzieren, sondern bildet in erster Linie ein Wesensmerkmal jedes Lebewesens. Es existiert eine Tendenz zur Banalisierung von Angaben zu physischen und verhaltensbezogenen Merkmalen. Biometrie ist mit wesentlichen Risiken für die Verletzung der Grundfreiheiten und -rechte verbunden. Bei der Sammlung und Bearbeitung von biometrischen Daten müssen die Datenschutzanforderungen und besonders die grundlegenden Prinzipien (Rechtmässigkeit, Treu und Glauben, Zweckbindung, Verhältnismässigkeit, Sicherheit, Rechte der betroffenen Personen) berücksichtigt werden. Die Biometrie ist kein Allheilmittel für Probleme der Sicherung von Informationssystemen oder sensitiven Anlagen. Bei den möglichen Anwendungen der Biometrie und bei der Auswahl der Technologien ist stets Vorsicht geboten. Im Privatsektor ist der Einsatz der Biometrie als Authentifizierungsmit-

tel meistens ungenügend und sollte nur erfolgen, wenn sich das angestrebte Ziel mit weniger einschneidenden Mitteln nicht erreichen lässt oder wenn die Biometrie zum Datenschutz beiträgt (siehe auch Ziffer 2.2.2 oben).

Im ausschliesslich den Datenschutzbeauftragten vorbehaltenen Konferenzteil wurde eine Resolution über einen Entwurf zu ISO-Normen über den Schutz der Privatsphäre verabschiedet (http://26konferencja.giodo.gov.pl/rezolucje/j/ge/). Die Internationale Organisation für Standardisierung (ISO) entwickelt internationale Normen über die Grundsätze des Schutzes der Privatsphäre. Die Datenschutzbeauftragten begrüssen diese Initiative und möchten aktiv an der Ausarbeitung der Normen beteiligt werden. Diese Normen müssen das Ziel verfolgen, die Umsetzung existierender Gesetzespflichten über den Datenschutz und den Schutz der Privatsphäre zu fördern bzw. Gesetzespflichten zu formulieren, falls sie nicht existieren. Die Konferenz vertritt jedoch die Auffassung, dass sich dieses Ziel mit dem Projekt der ISO nicht erreichen lässt. Die Entwicklung einer internationalen Norm muss insbesondere auf dem Transparenzgrundsatz («Fair Information Practices») sowie auf den Prinzipien der Datensparsamkeit, Datenminimierung und Anonymität beruhen. Damit die Normen effizient sind, müssen sie:

- Analyse- und Evaluationskriterien für die Funktionalitäten des Schutzes der Privatsphäre aller Systeme bzw. Technologien vorsehen, um den Verantwortlichen für die Datenbearbeitung die Übereinstimmung mit den nationalen oder internationalen Rechtsinstrumenten über den Datenschutz zu erleichtern;
- Garantien zu den Anforderungen des Schutzes der Privatsphäre für Technologien und Systeme anbieten, mit denen personenbezogene Informationen verwaltet werden;
- die Anforderungen des Datenschutzes für natürliche Personen unabhängig von der Anzahl der Organisationen, die an der Bearbeitung und am Austausch von Personendaten beteiligt sind, gewährleisten.

Die 27. Internationale Konferenz der Datenschutzbeauftragten wird vom 14. bis zum 16. September 2005 in Montreux, Schweiz, stattfinden (siehe www.privacyconference2005.org). Unter dem Titel «Der Schutz von Personendaten und der Privatsphäre in einer globalisierten Welt: ein universelles Recht unter Achtung der Verschiedenheiten» wird die Thematik früherer Konferenzen fortgesetzt. Die Konferenz soll zur Verabschiedung einer Abschlusserklärung zur Festigung des Datenschutzrechtes auf universaler Ebene führen.

9.4.2 Internationale Arbeitsgruppe Datenschutz im Telekommunikationsbereich

Wir haben am 18. und 19. November 2004 an der 36. Sitzung der Internationalen Arbeitsgruppe Datenschutz im Telekommunikationsbereich in Berlin teilgenommen. Die Gruppe wurde 1983 von Datenschutzbeauftragten verschiedener Länder ins Leben gerufen, um den Datenschutz im Telekommunikations- und Medienbereich zu verbessern.

Abgesehen vom gegenseitigen Austausch über die Entwicklungen im Fernmelderecht der einzelnen Staaten wurde an der Herbstsitzung 2004 unter anderem über datenschutzfreundliche Mittel zur Bekämpfung von Internetbetrug diskutiert. Eine verbesserte Strafverfolgung und Zusammenarbeit der Staaten ist auf diesem Gebiet sicherlich nützlich, bringt aber auch Datenerhebungen und -transfers mit sich, die datenschutzrelevant sein können. Die Arbeitsgruppe betont die positiven Wirkungen von präventiven Techniken, denen im Allgemeinen noch zu wenig Beachtung geschenkt wird. Die Behörden sollen datenschutzfreundliche Mittel wie beispielsweise die digitale Signatur, Treuhanddienste im Internethandel, Auditierungen/Qualitätssiegel etc. in Betracht ziehen, bevor sie Massnahmen ergreifen, die die Privatsphäre der Menschen tangieren. Sie sollen Informationen über solche datenschutzfreundlichen Massnahmen sammeln, Beispiele austauschen und die Öffentlichkeit darüber informieren.

Ein weiteres Thema behandelte die immer präziseren Standortinformationen, die durch Mobilfunkdienste erhoben werden können. Dies führt zum Angebot neuer Dienste, die teilweise von Drittfirmen erbracht werden, welche selber nicht unter das Fernmeldegeheimnis fallen. Aus Datenschutzsicht ist zu fordern, dass in diesem Bereich keine bzw. möglichst wenige Personendaten bearbeitet werden. Eine präzise Lokalisierung soll nur auf Wunsch für die Nutzung spezieller Dienste und nicht standardmässig aktiviert werden. Weiter muss der Benutzer bzw. die Benutzerin bestimmen können, inwiefern präzise Standortdaten über ihn bearbeitet werden. Auch ist die Weitergabe solcher Daten von einer klaren Einwilligung abhängig zu machen.

Weitere behandelte Themen betrafen u.a. Funktechniken im Nahbereich (d.h. die direkte Kommunikation zweier Geräte ohne Fernmeldeanbieter dazwischen, wie z.B. zwischen Headset und Handy mit Bluetooth), Videoüberwachungsanlagen, die von der Norm abweichendes Verhalten registrieren, sowie die Aufbewahrung von Fernmeldedaten zu Strafverfolgungszwecken.

Die verabschiedeten Papiere der Arbeitsgruppe sind zu finden im Internet unter der Adresse: http://www.datenschutz-berlin.de/doc/int/iwgdpt/.

10 Der Eidgenössische Datenschutzbeauftragte

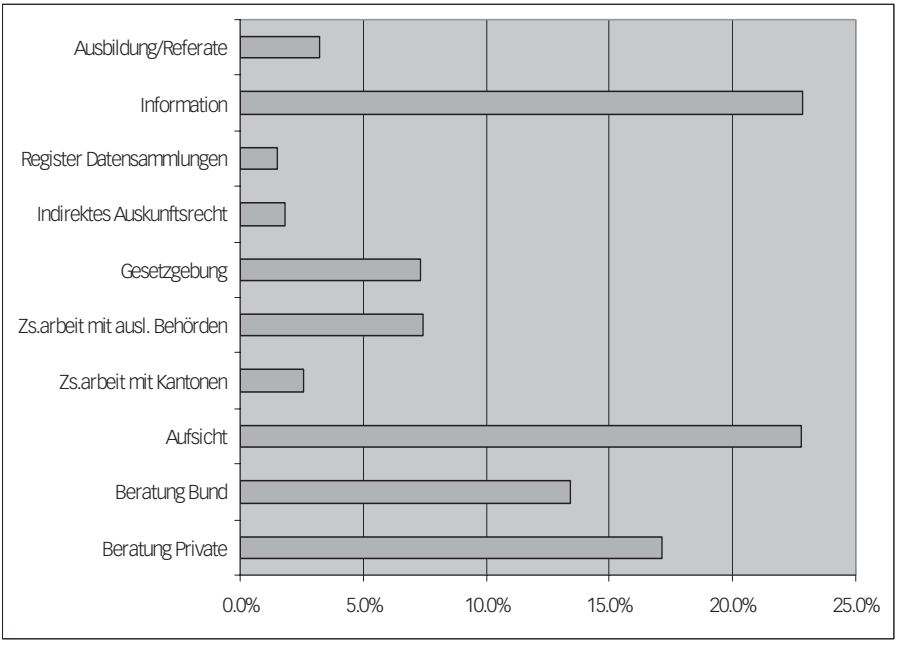
10.1 Publikationen des EDSB – Neuerscheinungen

Unter Spam versteht man unverlangte, zumeist unerwünschte und wiederholte Massen- bzw. kommerzielle E-Mail-Sendungen. In Fachkreisen wird eher von UBE (Unsolicited Bulk E-Mails) beziehungsweise UCE (Unsolicited Commercial E-Mails) gesprochen. Als UCE gelten mit Abstand die meisten Spam-Exemplare, da ihnen kommerzielle Interessen zugrunde liegen. Spam wird aber auch im Vorfeld von Wahlen oder Abstimmungen, zum Versand von Scherzmails und vieles mehr eingesetzt. Es handelt sich hingegen nicht um Spam, wenn Sie von einer Firma, deren Kunde Sie sind, hie und da E-Mails bekommen. Voraussetzung dafür ist jedoch, dass Sie diesen Sendungen zugestimmt haben.

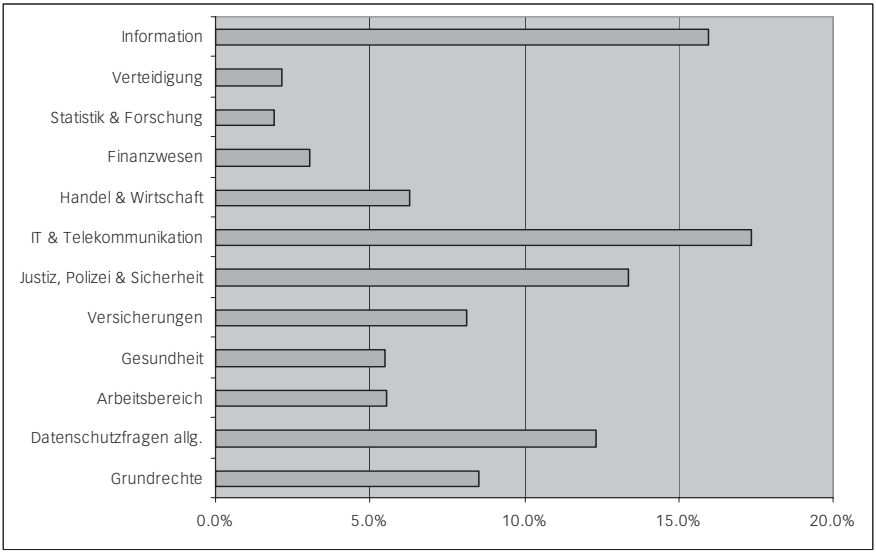
Unser Merkblatt zum Thema Spam erklärt Hintergründe der Spam-Problematik und gibt wertvolle Hinweise zum Schutz vor Spam und für den Umgang mit unerwünschten E-Mail-Sendungen. Das Merkblatt ist im Anhang des vorliegenden Tätigkeitsberichtes (Ziffer 11.1) sowie auf unserer Website (http://www.edsb.ch/d/doku/merkblaetter/spam.htm) zu finden.

10.2 Statistik über die Tätigkeit des Eidgenössischen Datenschutzbeauftragten vom 1. April 2004 bis 31. März 2005

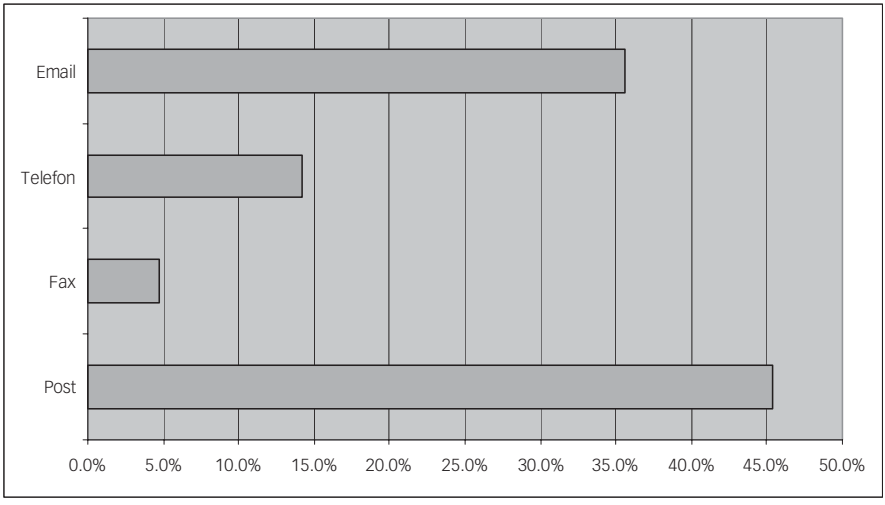
Aufwand nach Aufgabengebiet



Aufwand nach Sachgebiet



Herkunft der Anfragen



10.3 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.
Einheit Beratung und Information:	8 Personen
Einheit Aufsicht:	9 Personen
Kanzlei:	3 Personen

11 Anhang

11.1 Merkblatt über unerwünschte E-Mail-Werbung (Spam)

Unter Spam versteht man unverlangte, zumeist unerwünschte und wiederholte Massen- bzw. kommerzielle E-Mail-Sendungen. In Fachkreisen wird eher von UBE (Unsolicited Bulk E-Mails) beziehungsweise UCE (Unsolicited Commercial E-Mails) gesprochen. Als UCE gelten mit Abstand die meisten Spam-Exemplare, da ihnen kommerzielle Interessen zugrunde liegen. Spam wird aber auch im Vorfeld von Wahlen oder Abstimmungen, zum Versand von Scherzmails und vieles mehr eingesetzt. Es handelt sich hingegen nicht um Spam, wenn Sie von einer Firma, deren Kunde Sie sind, hie und da E-Mails bekommen. Auch der Newsletter, den Sie abonniert haben, stellt kein Spam dar. Voraussetzung dafür ist jedoch, dass Sie diesen Sendungen zugestimmt haben.

Dieses Merkblatt erklärt Hintergründe der Spam-Problematik und gibt wertvolle Hinweise zum Schutz vor Spam und für den Umgang mit unerwünschten E-Mail-Sendungen.

1. Die Beschaffung der E-Mail-Adressen durch den Spammer

Spammer beschaffen sich E-Mail-Adressen mittels leistungsfähiger Suchmaschinen in öffentlichen Räumen und Foren des Internets oder indem sie Adressdateien kaufen. Sie können die Adressen auch selber zusammenfügen, indem sie Namenslisten und häufige Domains kombinieren. Eine E-Mail-Adresse wie z. B. peter.muster@domain.ch ist somit anfälliger als eine zufällig zusammengesetzte (z. B. tr56&&@domain.ch). Die Hersteller von Antiviren-Software halten neuerdings eine Zusammenarbeit von Spammern und Virenschreibern für wahrscheinlich. Das gemeinsame Vorgehen sähe in etwa so aus: Virenschreiber setzen Würmer in Umlauf, die in der Internetverbindung der befallenen PCs eine Hintertür öffnen. Durch diese Hintertür greifen Spammer anschliessend mit den geeigneten Hilfsmitteln auf die befallenen PCs zu und verschicken von da Spam an beliebig viele Empfänger.

2. Die wichtigsten Konsequenzen für die betroffenen Personen

Der Spammer gibt den betroffenen Personen keine Möglichkeit, die unerwünschten Zusendungen abzubestellen. In den meisten Fällen besitzen solche E-Mails überdies keine gültige Absenderadresse, was die Abmeldung sowieso verunmöglicht. Spammer nützen die Anonymität insbesondere dazu, Betroffene mit zweifelhaften kommerziellen Angeboten zu belästigen. Spam belastet das Internet übermässig, verursacht Verbindungskosten, überfüllt den E-Mail-Briefkasten und beansprucht Speicherplatzkapazität auf den betroffenen PCs.

3. Die datenschutzrechtliche Relevanz

3. 1 E-Mail-Adressen stellen Personendaten dar, welche die Identifikation einer Person ermöglichen, sofern ihr Name darin enthalten ist oder die E-Mail-Adresse mit einer bestimmbaren Person assoziiert werden kann. Unter diesen Voraussetzungen untersteht die Bearbeitung von E-Mail-Adressen der Datenschutzgesetzgebung. Gemäss Art. 12 Abs. 3 des Bundesgesetzes über den Datenschutz (DSG, SR 235.1) stellt diese Bearbeitung in der Regel keine widerrechtliche Persönlichkeitsverletzung dar, wenn die E-Mail-Adresse vom Betroffenen allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt wurde. Eine solche Zugänglichmachung liegt beispielsweise vor, wenn eine Person ihre E-Mail-Adresse auf der eigenen Internet-Seite veröffentlicht. Aber auch diese Person kann Werbung ablehnen, und die Nichtbeachtung dieser Ablehnung stellt eine Persönlichkeitsverletzung dar.

3. 2 Wird die E-Mail-Adresse nur für spezifische Zwecke (Teilnahme an Mailing-Listen, Newsgroups, Bestellungen von Waren im Internet) benutzt, liegt keine allgemeine Zugänglichmachung im Sinne von Art. 12 Abs. 3 DSG vor. Die Beschaffung solcher E-Mail-Adressen durch den Spammer stellt eine Zweckentfremdung (Art. 4 Abs. 3 DSG) dar, die ohne Kenntnis (Art. 4 Abs. 2 DSG) und Einwilligung der betroffenen Person (Art. 13 Abs. 1 DSG) erfolgt. Dies ist datenschutzwidrig. Die Persönlichkeitsverletzung ist als gering einzustufen, wenn neben der E-Mail-Adresse keine besonders schützenswerten Personendaten bearbeitet werden. Das Datenschutzgesetz sieht für die betroffenen Personen die zivilrechtlichen Rechtsansprüche gemäss Art. 15 DSG vor (vgl. auch Art. 28ff Zivilgesetzbuch, ZGB, SR 210). Denkbar ist insbesondere eine Feststellungsklage gegen den Spammer. Auch Schadenersatz- und/oder Genugtuungsansprüche können erhoben werden, wobei zu bemerken ist, dass die Persönlichkeitsverletzung in der Regel klein und der Schaden zudem schwer beweisbar ist. Da der Spammer oft versteckt oder aus dem Ausland handelt und die Rechtsverfolgung somit sehr schwierig und meis-tens mit dem (kostspieligen) Beizug eines Anwalts verbunden ist, stellt der Rechtsweg in der Regel eine umständliche und teure Lösung dar.

3. 3 Spammer, welche ihre Adressdateien an Dritte abtreten, müssen dies dem Eidg. Datenschutzbeauftragten melden, wenn die betroffenen Personen davon keine Kenntnis haben (Art. 11 Abs. 3 DSG).

4. Die lauterkeitsrechtliche Relevanz

Die schweizerische Werbebranche hat sich zum Ziel gesetzt, unlautere kommerzielle Kommunikation (u. a. sämtliche Formen von unlauterer Werbung) zu bekämpfen. Zu diesem Zweck unterhält sie eine aus Konsumenten, Medienschaffenden und Werbern paritätisch zusammengesetzte Lauterkeitskommission. Jede Person ist befugt, ihrer Meinung nach unlautere Werbung bei dieser Kommission unentgeltlich zu beanstanden. Die Grundsätze der Kommission über die Lauterkeit in der kommerziellen Kommunikation stellen ethische Standards dar, welche sich die Werbewirtschaft selbst gesetzt hat. Die Kommission stützt sich in ihrer Arbeit auch auf das schweizerische Lauterkeitsrecht (vgl. insb. Bundesgesetz über den unlauteren Wettbewerb, UWG, SR 241) und auf die grenzüberschreitenden Richtlinien der Internationalen Handelskammer. Die betroffenen Personen können aufgrund des UWG insbesondere Schadenersatz- und Genugtuungsansprüche geltend machen (Art. 9 Abs. 3 UWG).

Gemäss Punkt 4.4 der Grundsätze der Schweizerischen Lauterkeitskommission gehören Verkaufsmethoden im Fernabsatz zur kommerziellen Kommunikation, die sich mittels persönlicher Adressierung an individuelle Personen richtet. Dazu gehört auch Spam. Solche Kommunikation, so halten die genannten Grundsätze weiter fest, gilt als aggressiv und damit unlauter, wenn dem Empfänger keine Möglichkeit angeboten wird, die kommerzielle Kommunikation mittels dem gleichen Kommunikationsmittel abzubestellen (z.B. Wahloption auf der Webseite oder wirksamer «unsubscribe»-Link). Bei diesem Lösungsvorschlag, der sogenannten **Opt-Out-Lösung**, ist eine erstmalige Kontaktaufnahme durch den Spammer per E-Mail erlaubt. Möchte die betroffene Person keine weiteren E-Mails erhalten, so meldet sie sich ab. Der Grossteil der Spammer berücksichtigt die Abmeldung jedoch nicht. Mit dem Klick auf den „unsubscribe-Link" bestätigt der Empfänger vielmehr den Erhalt des E-Mails und somit die Gültigkeit der Adresse. Bedenklich bei der Opt-Out-Lösung ist ferner, dass der Spammer ausgerechnet von denjenigen Personen eine E-Mail-Adressliste führen müsste, welche nichts mit ihm zu tun haben wollen.

5. Geplante gesetzgeberische Massnahmen gegen Spam

Der schweizerische Gesetzgeber arbeitet an der Revision zweier Bundesgesetze. Einerseits geht es um eine Ergänzung des Fernmeldegesetzes (FMG, SR 784.10): Anbieterinnen von Fernmeldediensten sollen mit geeigneten und zumutbaren Massnahmen die Übermittlung von Werbemitteilungen an Kundinnen und Kunden verhindern, die nicht schon in einer Geschäftsbeziehung mit dem Absender stehen oder ihre ausdrückliche Zustimmung zum Erhalt der Mitteilungen gegeben haben (Art. 45a FMG).

Anderseits soll das Bundesgesetz über den unlauteren Wettbewerb entsprechend geändert werden. Nach dem Revisionsvorschlag wird also insbesondere unlauter handeln, wer Telekommunikationsmittel zu Werbezwecken bei Personen verwendet, die dies nicht ausdrücklich erlaubt haben oder mit denen er nicht schon in einer Geschäftsbeziehung steht (Art. 3 lit. n UWG neu). Der Absender muss somit vor dem Versand der ersten Kontaktaufnahme die Einwilligung der Kundinnen und Kunden einholen (**Opt-In-Lösung**).

6. Technische und organisatorische Schutzmassnahmen gegen Spam

Seien Sie vorsichtig bei der Bekanntgabe Ihrer E-Mail-Adresse. Sie kann auch ohne Ihre Kenntnis und Einwilligung durch unberechtigte Dritte erfasst werden, sobald sie auf einer Webseite bekannt gegeben wird (z. B. bei der Teilnahme an Diskussionsforen oder Bestellung von Newsletters, bei online-Geschäften oder beim Ausfüllen von Formularen).

Mit folgenden präventiven Massnahmen können Sie sich gegen Spamschützen:

a. Wahl der E-Mail-Adresse

Wählen Sie Ihre E-Mail-Adresse so, dass Ihr Name und Vorname nicht darin erscheinen. Dies erschwert die Erfassung der Adresse durch den Spammer.

b. Transparenz über die Weiterverwendung Ihrer E-Mail-Adresse im Internet

Vergewissern Sie sich vor der Erfassung Ihrer E-Mail-Adresse in einem Internet-Formular, dass die weitere Verwendung der Adresse angegeben wird. Dadurch können Sie das Risiko einer unerwünschten Weiterverwendung Ihrer E-Mail-Adresse (z. B. zu Marketingzwecken) reduzieren. Ausserdem müssen Sie über die weiteren Empfänger Ihrer Daten sowie über das Auskunftsrecht informiert werden.

c. Mehrere E-Mail-Adressen benutzen

Schaffen Sie eine für Ihre Internetgeschäfte, Ihre Teilnahme an Diskussionsforen und Newsletters bestimmte E-Mail-Adresse. Damit können Sie Ihre persönliche E-Mail-Adresse, die Sie ausschliesslich für berufliche oder private Kontakte benutzen, weitgehend vor Spam schützen.

d. Liste der Empfänger Ihrer E-Mail-Adresse

Daten (Einschreibedatum, E-Mail-Inhalt, Passwort), die Sie beim Abonnement von Newsletters, bei der Öffnung von Konten oder online-Zahlungen angeben, sollten Sie ausdrucken und aufbewahren. Es kann bspw. nicht ausgeschlossen werden, dass ein Spammer hinter einem fiktiven Newsletter steckt. Desgleichen sollten Sie eine Liste jener Webseiten führen, auf welchen Sie Ihre E-Mail-Adresse bekannt gegeben haben.

e. Schutz von E-Mail-Adressen Dritter

Wenn Sie ein E-Mail an mehrere Empfänger versenden, benutzen Sie die Funktion „versteckte Kopie" (BCC) Ihrer E-Mail-Software. Damit schützen Sie die Adressen Ihrer Korrespondenzpartner. Verbergen Sie die Adressen auch in Newsgroups und anderen Verteilerlisten.

f. Einwilligung der betroffenen Personen

Geben Sie E-Mail-Adressen von Drittpersonen ohne deren Einwilligung nicht bekannt.

g. Spam-Filter

Der Spam-Problematik lässt sich zur Zeit mittels Inhalts- und Header-Analyse entgegenwirken. Die eingegangenen E-Mails werden nach bestimmten Merkmalen untersucht und gefiltert. Damit sind jedoch nicht alle Probleme beseitigt. Erstens können auch erwünschte Mails im Filter hängen bleiben. Im Allgemeinen rechnet man mit einer Fehlerquote von mindestens 10% (falsch positive und falsch negative Treffer). Zweitens wird das eigentliche Problem nicht gelöst: Spam wird trotzdem verschickt, der Filter erspart Ihnen bloss etwas Arbeit. Immer mehr Internetprovider bieten eigene Spam-Filter an, die die Postfächer direkt auf dem Mailserver durchforsten. Bietet Ihr Mailprovider diesen Dienst an, können Sie den Spam-Filter für Ihr Mailkonto selbst verwalten. Dabei können Sie wählen, ob als Spam erkannte Mails schon bei der Ankunft auf dem Server ohne Ihr Zutun entsorgt oder in einen Spam-Ordner verschoben werden sollen.

h. Öffentliche Verzeichnisse

Vermerken Sie beim Eintrag in ein öffentliches Verzeichnis (z. B. elektronische Telefonverzeichnisse), sofern möglich, dass Sie keine unaufgeforderte Werbung erhalten möchten.

i. Sperrlisten

Eine weitere Möglichkeit ist der Eintrag in Sperrlisten, wobei deren Nutzen von der Beachtung durch die Spammer abhängt. Es besteht zudem die Gefahr, dass der Eintrag in einer Sperrliste als Bestätigung der Gültigkeit einer E-Mail-Adresse gesehen und durch den Spammer missbraucht werden kann.

j. Schwarze Listen

Mittels schwarzer Listen können E-Mail-Provider verifizieren, ob der Server, aus welchem eine Meldung versendet wird, für die Versendung von Spam bekannt ist; gegebenenfalls kann die Meldung abgelehnt werden. Bei der Auswahl Ihres E-Mail-Providers sollten Sie darauf achten, dass er solche Listen führt.

Wenn Sie Spam erhalten haben, sollten Sie sich an folgende Regeln halten:

a. Ungelesen löschen

Am besten löschen Sie Spam-E-Mails, ohne sie zu öffnen. Auf keinen Fall sollten Sie Attachments öffnen oder auf allfällige kommerzielle Angebote eingehen, egal wie interessant das Werbemail aussehen mag.

b. Spam nicht beantworten

Sie sollten Spam nie beantworten. Eine Antwort bestätigt dem Spammer, dass Ihre E-Mail-Adresse gültig ist und benutzt wird. Er kann Ihnen somit weiterhin unerwünschte E-Mails senden und seine Adressdateien weiterverkaufen. Unerwünschte E-Mails sollten nur beantwortet werden, wenn eine Abmeldung möglich ist (Opt-Out) oder wenn Sie eine eigens dafür geschaffene E-Mail-Adresse haben.

c. Keine Überreaktionen

Überfluten Sie den E-Mail-Briefkasten des Spammer nicht mit grossen Dateien. Der Spammer könnte nämlich seine Mails mit falscher Identitätsangabe signiert haben: Entweder existiert die Adresse gar nicht oder sie gehört einem anderen Spam-Opfer. Ausserdem überlasten Sie das Internet unnötig.

d. Hypertext-Links im Spam nicht anklicken

Hypertext-Links im Spam sollten nicht angeklickt werden. Sie riskieren damit, dass Ihre E-Mail-Adresse z.B. via Cookies erfasst wird, womit der Spammer die Bestätigung hat, dass die Adresse benutzt wird.

e. Information an E-Mail- oder Internet-Provider

Informieren Sie den Inhaber des vom Spammer gebrauchten Mail-Servers oder Ihren eigenen Internet-Provider. Die meisten Internet- und E-Mail-Provider haben eigens dafür vorgesehene elektronische Briefkästen geschaffen; sie können gegen den Spammer vorgehen und die Benutzer besser vor ungewollten E-Mail-Sendungen schützen.

f. Software einsetzen

Mittels spezieller Software können Sie den Inhalt Ihres Postfachs direkt auf dem Server des Providers einsehen. Absender, Betreffzeilen und Grösse der E-Mails werden angezeigt. So entsorgen Sie lästige Mails mit wenigen Mausklicks, bevor Sie den restlichen Inhalt Ihres Postfachs mit Ihrem regulären Mailprogramm herunterladen.

g. Drohungen des Spammers melden

Werden Sie durch den Spammer bedroht (z. B. mit der Verbreitung von Botschaften mit pornographischem Inhalt in Ihrem Namen), erstatten Sie Anzeige bei den zuständigen Strafverfolgungsbehörden.

7. Links

Folgende staatliche, überstaatliche und private Organisationen setzten sich mit der Spam-Problematik auseinander:

- http://europa.eu.int/information_society/topics/ecomm/doc/useful_information/library/communic_reports/spam/spam_com_2004_28_fr.pdf
- http://cm.coe.int/ta/rec/1995/f95r4.htm
- http://cm.coe.int/ta/rec/1999/f99r5.htm
- http://www.oecd.org/dataoecd/55/32/31450810.pdf
- http://www2.dcita.gov.au/ie/trust/improving/spam_home
- http://www.cnil.fr/index.php?id=1266
- http://www.datenschutz-berlin.de/jahresbe/03/teil3.htm#3
- http://spamlaws.com
- http://www.siug.ch/positionen/SIUG-Spam.shtml
- http://www.euro.cauce.org
- http://spamcop.net
- http://www.sncd.org/deontologie/index.html
- http://www.imc.org/imc-spam/index.html
- http://spamanti.net
- http://www.caspam.org
- http://www.lauterkeit.ch/pdf/grundsaetze.pdf