14. Tätigkeitsbericht 2006/2007

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Tätigkeitsbericht 2006/2007
des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten

Der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte hat dem Bundesrat periodisch einen Bericht über seine Tätigkeit vorzulegen (Art. 30 DSG).
Der vorliegende Bericht deckt den Zeitraum zwischen 1. April 2006 und 31. März 2007 ab.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Vertrieb:

BBL, Verkauf Bundespublikationen, CH-3003 Bern

www.bbl.admin.ch/bundespublikationen

Art.-Nr. 410.014.d/f

Inhaltsverzeichnis

* Originaltext auf Französisch

* Originaltext auf Französisch

* Originaltext auf Französisch

Vorwort

Allzu häufig steckt man als Datenschützer in der Rolle des Sisyphos, jener tragischen Figur aus der griechischen Mythologie, welche den Stein immer wieder einen Berg hinaufstossen musste, obwohl dieser sogleich wieder den Berg hinunterdonnerte: Kaum glaubt man ein Datenschutzproblem gelöst, taucht es in etwas anderer Form gleich wieder auf. So geschehen nach dem langen Seilziehen zwischen dem EDÖB und dem Bundesrat wegen der fehlenden gesetzlichen Grundlagen beim Einsatz von Aufklärungsdrohnen im Dienste des Grenzwachtkorps. Nach diversen Motionen von Parlamentariern scheint nun der Bundesrat trotz anfänglicher Weigerung bereit, den Mangel im Rahmen einer Teilrevision der Militärgesetzgebung zu beheben. Doch das Thema wird uns weiterhin beschäftigen: Mit wachsendem Druck drängen miniaturisierte ferngesteuerte oder gar GPS-programmierbare Kleinstflugzeuge (Helikopter, Drohnen, usw.), ausgerüstet mit hochauflösenden Aufnahmegeräten, für allerlei „legale" und vielleicht auch andere Zwecke auf den Markt und verunsichern zunehmend Bürgerinnen und Bürger. Diese Entwicklung Richtung Miniaturisierung der Überwachungstechnologie stellt in Zukunft für den Schutz der Privatsphäre eine grosse Herausforderung dar. Wir werden uns dieser Problematik zusammen mit andern involvierten Stellen mit der nötigen Intensität annehmen.

Überhaupt bleibt das Thema der zunehmenden Überwachung in mannigfaltiger Ausgestaltung ein Dauerbrenner: Nicht nur auf nationaler Ebene, wo die Revision der Bundesgesetzes über die Wahrung der inneren Sicherheit (BWIS), welche einen radikalen Ausbau der Eingriffsmöglichkeiten der Staatsschützer in die Privatsphäre von Bürgerinnen und Bürger zum Ziel hat, in die heisse Phase der parlamentarischen Beratung kommt. Auch auf internationaler Ebene wird der Spielraum für die persönliche Freiheit immer enger. Mit unseren europäischen Datenschutzkollegen werden wir die Entwicklung in Europa zu einer verstärkten polizeilichen und justiziellen Zusammenarbeit in Strafsachen aufmerksam verfolgen und alles daran setzen, um ein hohes Datenschutzniveau zu gewährleisten.

Ins gleiche Kapitel gehen die Datenlieferungen der Swift-Zentrale in Brüssel an US-Behörden im Zeichen der Terrorbekämpfung, die uns im Berichtsjahr stark beschäftigten (vgl. Ziff 1.8.1). Kritisiert wurde von unserer Seite, dass die Finanzdienstleister in der Schweiz die Kundendaten an die Zentrale in Belgien lieferten, ohne ihre Kundinnen und Kunden zu benachrichtigen. Leider sind bis heute nach wie vor nicht alle Schweizer Bankinstitute der von uns geforderten Transparenzpflicht nachgekommen. Handlungsbedarf besteht seitens der Schweiz auch in Bezug auf die Aushandlung

eines Abkommens, das Datenschutzregeln für die Lieferung solcher Daten an die USA festschreibt (denn bekanntlich verfügen die USA nach wie vor nicht über Datenschutzbestimmungen, die denen der Schweiz vergleichbar sind). Hier ist die Politik gefordert. Erfreulich ist, dass – wie Ende März 2007 bekannt wurde – die Swift-Zentrale selber auf Druck der belgischen Datenschutzbehörde bereit ist, sich den Regeln des so genannten Safe-Harbour-Systems zu unterwerfen. Ob damit allerdings bereits ein ausreichender Schutz gewährleistet und somit eine Schweizer Initiative nunmehr überflüssig ist, ist zu bezweifeln. Wir werden die Entwicklung aufmerksam verfolgen. Interessant ist in diesem Zusammenhang, dass bei datenschutzrechtlich heiklen Fragestellungen oft noch andere höchst brisante Probleme mitschwingen können: Neu wurde die Swift jedenfalls Ende März 2007 von deutschen Banken auch deshalb attackiert, weil sie befürchten, dass europäische Überweisungsdaten von den US-Geheimdiensten auch zur Wirtschaftsspionage missbraucht würden. Ein schlagendes Beispiel dafür, dass die Wirtschaft durchaus ein eminentes Interesse an einem funktionierenden Datenschutz haben müsste.

Das Gesundheitswesen ist weiterhin eine datenschützerische Grossbaustelle, die nach wie vor viele Kräfte absorbiert. Stichworte sind, um nur die wichtigsten zu nennen: Gesundheitskarte, Versichertenkarte, elektronisches Patientendossier, DRG, Einführung der Elektronik beim vertrauensärztlichen Dienst. Gerade im Gesundheitswesen mit seinen höchst sensiblen Daten sind im Zeitalter der voll entfalteten Elektronik Datenschutz-GAUs im grösseren Stil zu befürchten, weil der EDÖB aufgrund seiner Ressourcen in diesem Bereich höchstens stichprobenweise oder bei einer bereits eingetretenen Datenschutzverletzung intervenieren und dann lediglich Empfehlungen abgeben kann. Das Bundesamt für Gesundheit (BAG) muss hier seiner Verantwortung als Aufsichtsbehörde mit Weisungsrecht nachkommen.

Mit dem Mitte letzten Jahres in Kraft getretenen Öffentlichkeitsgesetz ist uns eine neue Aufgabe zugewiesen worden. Die im Gesetz vorgesehenen Mediationsverfahren zwischen Bürgern und Verwaltung in strittigen Fällen mussten in den ersten sechs Monaten dreimal durchgeführt werden. Obwohl wir diese Verfahren – wie angekündigt – ausserordentlich schlank durchführen, so dass von einer eigentlichen Mediation unter fachlichen Kriterien kaum gesprochen werden kann, sind die Verfahren wegen der umfangreichen Dossiers und der oft sehr komplexen Fragestellungen höchst aufwändig, bis von unserer Seite eine rechtlich haltbare Empfehlung abgegeben werden kann. Immerhin muss diese, wird sie von den Parteien nicht akzeptiert, in einem gerichtlichen Verfahren den juristischen Härtetest bestehen. In den ersten drei Monaten des Jahres 2007 sind bei uns bereits 13 weitere Gesuche eingetroffen. Bis heute hat der Bundesrat an seinem Entscheid festgehalten, für diese Aufgabe die ursprünglich

in Aussicht gestellten zusätzlichen Stellen nicht zu bewilligen. Der bisherige Aufwand, der noch in diesem Jahr deutlich ansteigen dürfte, konnte nur bewältigt werden, weil die Bundeskanzlerin uns eine zeitlich befristete Stelle aus ihrem Etat zur Verfügung stellte. Trotz dieser Massnahme ist aber zu befürchten, dass die hängigen Gesuche nicht in der vom Gesetz vorgesehenen Frist abgewickelt werden können.

Bereits letztes Jahr habe ich darauf hingewiesen, dass mir der im internationalen Vergleich ausserordentlich bescheidene Stellenetat Sorge bereite, zumal wir aufgrund der Sparmassnahmen und der stetig wachsenden Aufgaben zusätzlich unter Druck stehen.

Angesichts der Tatsache, dass auf politischer Ebene keine Anzeichen auszumachen waren, die in absehbarer Zeit eine grundsätzliche Änderung versprachen, haben wir im Rahmen einer rigorosen Verzichtsplanung geprüft, wie wir den gesetzlichen Auftrag mit den vorhandenen Mitteln dennoch glaubwürdig erfüllen können. Im Zuge dieser Überprüfung haben wir entschieden, dass wir uns künftig nur noch Datenschutzfragen mit einer grossen Tragweite für die Privatsphäre einer beachtlichen Anzahl von Personen widmen können. Konkret bedeutet dies, dass wir Anfragen von Privatpersonen nicht mehr individuell beantworten werden. Wir wollen aber weiterhin als Klagemauer zur Verfügung stehen und haben deshalb einen täglichen Telefondienst von 10.00 bis 12.00 Uhr eingerichtet. Ausserdem können schriftlich oder per Email Beanstandungen bei uns deponiert werden, die wir dann gemäss ihrer Wichtigkeit und den uns zur Verfügung stehenden Ressourcen bearbeiten werden. Gleichzeitig haben wir unsere Internetseite als Informationsplattform ausgebaut und hoffen so, jenen rund 1500 Personen, die bei uns bisher jedes Jahr eine individuelle Antwort erhielten, eine einigermassen akzeptable Alternative zu offerieren.

Hanspeter Thür

Abkürzungsverzeichnis

AHVG	Bundesgesetz über die Alters- und Hinterlassenenversicherung
ATSG	Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts
BAG	Bundesamt für Gesundheit
BASPO	Bundesamt für Sport
BAV	Bundesamt für Verkehr
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung
BJ	Bundesamt für Justiz
BKP	Bundeskriminalpolizei
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs
BV	Bundesverfassung
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit
CNIL	Commission nationale de l'informatique et des libertés
DAP	Dienst für Analyse und Prävention
DRG	Diagnosis-related group
DSG	Bundesgesetz über den Datenschutz
EDA	Eidgenössischen Departement für auswärtige Angelegenheiten
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖK	Eidgenössische Datenschutz- und Öffentlichkeitskommission
EFD	Eidgenössisches Finanzdepartement
EMRK	Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten
EPA	Eidgenössisches Personalamt
ESBK	Eidgenössische Spielbankenkommission

EVG	Eidgenössisches Versicherungsgericht
fedpol	Bundesamt für Polizei
GEWA	Datenverarbeitungssystem zur Bekämpfung der Geldwäscherei
GWG	Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor
HFG	Bundesgesetz über die Forschung am Menschen
HOOGAN	Hooliganismus-Informationssystem
IPAS	Informatisiertes Personennachweis-, Aktennachweis- und Verwaltungssystem
ISB	Informatikstrategieorgan Bund
ISIS	Staatsschutz-Informations-System
JANUS	Gemeinsames Informationssystem der kriminalpolizeilichen Zentralstellen des Bundes
KVG	Bundesgesetz über die Krankenversicherung
RHG	Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister
RIPOL	Automatisiertes Fahndungssystem
SAMW	Schweizerische Akademie der Medizinischen Wissenschaften
SBG	Bundesgesetz über Glücksspiele und Spielbanken
SECO	Staatssekretariat für Wirtschaft
SIS	Schengener Informationssystem
StGB	Strafgesetzbuch
UVG	Unfallversicherungsgesetz
UWG	Bundesgesetztes gegen den unlauteren Wettbewerb
VBS	Departement für Verteidigung, Bevölkerungsschutz und Sport
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
VDSZ	Verordnung über Datenschutzzertifizierungen

VOBG	Verordnung über die Offenbarung des Berufsgeheimnisses im Bereich der medizinischen Forschung
VOSTRA	Automatisiertes Strafregister
VWIS	Verordnung über Massnahmen zur Wahrung der inneren Sicherheit
ZEMIS	Zentrales Migrationsinformationssystem
ZentG	Bundesgesetz über die kriminalpolizeilichen Zentralstellen des Bundes

1 Datenschutz

1.1 Grundrechte

1.1.1 Verordnungsentwurf für die Datenschutzzertifizierung

Aufgrund ihres Geltungsbereichs, ihrer Tragweite und ihrer relativ komplexen Ausgestaltung sind die Zertifizierungsanforderungen in einer spezifischen Verordnung (VDSZ) zusammengestellt worden. Die Zertifizierung von Organisationen richtet sich für ihr Datenschutz-Managementsystem weitgehend nach der ISO-Norm 27001, während sich die Produktzertifizierung auf den seit einigen Jahren im Bundesland Schleswig-Holstein geltenden Anforderungskatalog für die Begutachtung von IT-Produkten stützt.

Im Rahmen der Ausführung des im März 2006 von der Bundesversammlung angenommenen neuen Artikels 11 des DSG haben wir unsere Zusammenarbeit mit dem Bundesamt für Justiz und der Schweizerischen Akkreditierungsstelle fortgesetzt mit dem Ziel, die Mindestvoraussetzungen und -anforderungen für die Erlangung einer Datenschutz-Zertifizierung zu bestimmen. Die Idee der Ausarbeitung einer spezifischen Zertifizierungsverordnung (VDSZ) drängte sich wegen der zahlreichen besonderen Anforderungen betreffend die Organisationen/Verfahren wie auch die Produkte/Systeme ziemlich rasch auf. Die ersten Artikel der VDSZ definieren die allgemeinen Voraussetzungen für die Erlangung, Verwendung, Gültigkeit und Anerkennung dieser Datenschutz-Zertifizierungen, sowie die jeweiligen Aufgaben der verschiedenen betroffenen Partner. Bekanntlich geht man vom Grundsatz aus, dass bei einem zum Zeitpunkt des Audits als regelkonform anerkannten Datenschutzniveau und einem aktiven und dokumentierten Entwicklungsmanagement eine Datenschutzzertifizierung für die Dauer einiger Jahre ausgestellt werden kann (vgl. Ziffer 1.1.1 in unserem 13. Tätigkeitsbericht 2005/2006).

Für die Zertifizierung von Organisationen haben wir unseren Entwurf für ein Referenzmodell einer Arbeitsgruppe vorgelegt, die sich aus mehreren schweizerischen Firmen für die Zertifizierung von Organisationen gemäss den Managementsystemen ISO 9001:2000 (Qualität) und 27001:2005 (Informationssicherheit) zusammensetzte. Anhang 1 der VDSZ enthält eine Anpassung und Erweiterung der Anforderungen von ISO 27001 entsprechend den auf dem DSG beruhenden Bedingungen, so dass damit ein eigentlicher Anforderungskatalog für die Datenschutz-Managementsysteme (DSMS)

vorliegt. Kapitel 3 umfasst insbesondere die folgenden zehn Datenschutz-Prinzipien oder -Anforderungen: Rechtmässigkeit – Transparenz – Verhältnismässigkeit – Zweck – Richtigkeit – Bekanntgabe ins Ausland – Datensicherheit – Bearbeitung durch Dritte – Liste der Datensammlungen – Zugriffsrecht.

Nach dem Beispiel der Zertifizierung ISO 27001, die vollumfänglich auf dem Leitfaden ISO 17799:2005 für das Management der Informationssicherheit beruht (11 Bereiche, 39 Zielsetzungen und 133 Massnahmen) werden wir einen ergänzenden Leitfaden für das Management und die Zertifizierung des Datenschutzes veröffentlichen und aktualisieren. Dieser wird ausschliesslich dem Datenschutz und der Vertraulichkeit der Personendaten gewidmet sein (ursprüngliche generische Massnahme 15.1.4 der Norm 17799:2005) und soll mit Hilfe von rund zwanzig spezifischen, genau nach den ISO-Empfehlungen strukturierten Massnahmen die Verwirklichung der oben genannten zehn Datenschutzziele ermöglichen. Für die Produktzertifizierung haben wir uns – in Ermangelung wirklich geeigneter und anerkannter internationaler Normen – für den Anforderungskatalog für die Begutachtung von IT-Produkten im Rahmen des in Schleswig-Holstein geltenden Zertifizierungsverfahrens entschieden. Die Gliederung der Anforderungen in vier verschiedene logische Komplexe (Technikgestaltung – Zulässigkeit – technische und organisatorische Massnahmen – Rechte der betroffenen Person) hat uns besonders überzeugt, ebenso wie die Tatsache, dass ein getrenntes Anforderungsprofil für die Randdaten (logdata) vorgesehen ist. Diese stellen nämlich zusätzliche Datensammlungen dar, deren Zweckbestimmung und Bearbeitungsbedingungen grundsätzlich anders sind als für die Hauptdatensammlung. Anhang 2 der VDSZ sollte somit eine Anpassung dieses in Norddeutschland bereits bewährten Anforderungskatalogs an das schweizerische Recht enthalten.

Schliesslich umfasst die VDSZ auch einen Anhang 3, der den Anforderungen an die Qualifikation des Personals der Zertifizierungsunternehmen gewidmet ist, sowie einen Anhang 4, in dem die Qualitätszeichen aufgeführt werden, die der Bund für die vollständige oder teilweise Zertifizierung von Organisationen und für die Produktzertifizierung vorschlägt. Die Verwendung und Anerkennung von privaten Qualitätszeichen werden ebenfalls in der Verordnung geregelt. Das externe Vernehmlassungsverfahren zu diesen Verordnungen wurde Ende Februar 2007 durch das BJ eröffnet. Sehr zu unserem Erstaunen und Bedauern haben wir kurz vor Redaktionsschluss des vorliegenden Berichts erfahren, dass die Anhänge 1, 2 und 4 gestrichen wurden.

1.1.2 Harmonisierung amtlicher Personenregister und Verwendung der neuen AHV-Versichertennummer als Personenidentifikator

Die neue AHV-Versichertennummer wird als Sozialversicherungsnummer und administrative Personenidentifikationsnummer in den harmonisierten Registern verwendet werden. So hat es das Parlament entschieden. Auch in den Kantonen soll diese Nummer eine systematische Verwendung finden.

Das Bundesamt für Statistik (BFS) hat im Bereich Personenidentifikator bereits mehrere Projekte ausgearbeitet, die jedes Mal Konsultationen unterzogen wurden (vgl. hierzu unseren 13. Tätigkeitsbericht 2003/2004, Ziffer 1.2.1). Nun hat das Parlament entschieden: Das Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister (RHG) sowie die Revision des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG) sehen vor, dass die neue AHV-Versichertennummer einerseits als Sozialversicherungsnummer, andererseits aber auch als administrative Personenidentifikationsnummer verwendet werden soll. Die Gesetze wurden am 23. Juni 2006 verabschiedet.

Wir haben im Rahmen von Ämterkonsultationen und anlässlich von parlamentarischen Sitzungen zu den Gesetzesentwürfen Stellung genommen und eine alternative Lösung aufgezeigt. Dabei standen folgende Überlegungen im Vordergrund:

Die Vermischung von Statistik und Verwaltungsanliegen ist aus Sicht des Persönlichkeitsschutzes besonders heikel. Die Statistik braucht pseudonymisierte Daten aus möglichst vielen Quellen bzw. Registern. Die Verwaltung hingegen braucht möglichst genaue, personenbezogene Daten. Die Einführung einer registerübergreifenden Personenidentifikationsnummer (in Form der neuen AHV-Versichertennummer) erleichtert die Verknüpfbarkeit von personenbezogenen Daten aus verschiedenen Registern. Durch diese Verknüpfbarkeit ist die Erkennbarkeit der Datenbearbeitung für die Betroffenen nicht mehr gewährleistet.

Das österreichische Modell
(abrufbar unter: http://www.cio.gv.at/egovernment/umbrella/)

verwendet aus einer verschlüsselten Stammzahl abgeleitete bereichsspezifische Personenkennzeichen. Ein solches Modell bringt klare Vorteile für ein zukünftiges E-Government in der Schweiz. Deshalb braucht es unseres Erachtens eine technische Infrastruktur, die es erlaubt, statistische und administrative Zwecke klar zu trennen, und die gleichzeitig dafür sorgt, dass ein nicht vorgesehener Datenaustausch innerhalb der Verwaltung auch technisch ausgeschlossen werden kann. Das österreichische Modell wurde während den parlamentarischen Arbeiten zum RHG und AHVG von uns vorgestellt und erläutert, jedoch leider nicht als Lösung für die Schweiz berücksichtigt.

Nachdem die Gesetze nun verabschiedet wurden, folgt die Erarbeitung der Ausführungsbestimmungen sowie die Umsetzung der Registerharmonisierung in den Kantonen. Der Kanton Bern hat in diesem Zusammenhang eine Vorreiterrolle eingenommen. Der Grosse Rat hat das Gesetz über die Harmonisierung amtlicher Register (RegG) am 28. November verabschiedet. In seinem Artikel 9 sieht das Gesetz die systematische Verwendung der Versichertennummer nach AHVG vor.

Nachdem auch in anderen Kantonen Gesetzesvorhaben zur Registerharmonisierung bereits vorliegen oder vorliegen werden, haben wir zusammen mit „privatim - die schweizerischen Datenschutzbeauftragten", einem Zusammenschluss der kantonalen und kommunalen Datenschutzbeauftragten, eine Stellungnahme zur Verwendung der AHV-Versichertennummer in den Kantonen abgegeben. Aus Sicht des Datenschutzes ist die Verwendung der AHV-Versichertennummer in den Kantonen als genereller Personenidentifikator durch eine sorgfältige Gesetzgebungsarbeit demokratisch zu legitimieren. Denn eine generelle Ermächtigung in einem Gesetz für die Verwendung der AHV-Versichertennummer in der gesamten kantonalen Verwaltung ist unzulässig. Die Ausbreitung der AHV-Versichertennummer als Universalnummer birgt hohe Risiken für die Privatsphäre der Bürgerinnen und Bürger, weil sie unerwünschte Verknüpfungen ermöglicht. Auch das Bundesamt für Sozialversicherung hat sich in diesem Sinne geäussert. Bereits im Dezember 2002 haben wir bei Prof. Giovanni Biaggini ein Gutachten eingeholt zum Thema „Ein Personenidentifikator im Lichte des verfassungsrechtlichen Persönlichkeitsschutzes (Art. 13 BV)". Diese Stellungnahmen und Gutachten sind abrufbar unter:

http://www.edoeb.admin.ch/themen/00794/00819/01081/index.html?lang=de).

1.1.3 Öffentliche Bekanntgabe von Informationen durch ein Bundesamt

Ein Bundesamt ist berechtigt, selbst ohne Einwilligung des Betroffenen persönliche Daten im Rahmen der behördlichen Öffentlichkeitsinformation bekannt zu geben. Voraussetzung ist allerdings, dass diese Informationen mit der Erfüllung öffentlicher Aufgaben zusammenhängen und dass die Bekanntgabe einem überwiegenden öffentlichen Interesse entspricht. In jedem Einzelfall ist auf die Einhaltung der allgemeinen Datenschutzgrundsätze, insbesondere des Verhältnismässigkeitsprinzips, zu achten.

Ein Bundesamt gelangte mit der Frage an uns, ob ihm aufgrund der Datenschutzgesetzgebung gestattet sei, von der Presse übernommene Fehlinformationen zu einem Einzeldossier durch Bekanntgabe gewisser Elemente dieses Dossiers zu berichtigen, um die Öffentlichkeit über den tatsächlichen Sachverhalt aufzuklären.

Die von einem Bundesorgan vorgenommene Richtigstellung von Fehlinformationen, die von den Medien verbreitet und übernommen wurden, bildet, soweit diese Informationen eine bestimmte Person nennen oder auf deren Identität schliessen lassen, eine Bekanntgabe von Personendaten im Sinne von Art. 19 DSG und muss innerhalb des gesetzlichen Rahmens erfolgen.

Laut Art. 19 DSG dürfen Bundesorgane Personendaten nur bekannt geben, wenn dafür eine Rechtsgrundlage besteht oder in ganz bestimmten, im DSG ausdrücklich vorgesehenen Fällen, namentlich wenn die betroffene Person ihre Einwilligung dazu gegeben ihre Daten allgemein zugänglich gemacht hat. Seit dem 1. Juli 2006 ist der rechtliche Rahmen von Art. 19 DSG erweitert worden, so dass die Bundesorgane nunmehr im Rahmen der behördlichen Information der Öffentlichkeit von Amtes wegen oder gestützt auf das Öffentlichkeitsgesetz auch Personendaten bekannt geben dürfen, wenn die betreffenden Daten im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen und an deren Bekanntgabe ein überwiegendes öffentliches Interesse besteht.

In jedem Einzelfall ist zu beurteilen, ob und in welchem Masse die Bekanntgabe von Personendaten im Rahmen der behördlichen Information der Öffentlichkeit gerechtfertigt ist. Es muss namentlich auf die Einhaltung der allgemeinen Datenschutzgrundsätze geachtet werden, insbesondere des Prinzips der Verhältnismässigkeit: die Personendaten müssen beispielsweise so weit wie möglich anonymisiert werden; es dürfen lediglich die für die Information der Öffentlichkeit unbedingt notwendigen Personendaten bekannt gegeben werden.

1.1.4. Vote électronique: Papierausdruck elektronischer Stimmen (Paper Trail)

Ein heikler Punkt im Zusammenhang mit Vote électronique ist die Frage der Nachvollziehbarkeit der Stimmabgaben. Wir haben die Problematik mit den involvierten Bundesstellen erörtert. Sie soll nun in der Arbeitsgruppe Vote électronique besprochen werden.

Die Bundeskanzlei führt seit mehreren Jahren gemeinsam mit den Kantonen Genf, Neuenburg und Zürich Pilotprojekte zur elektronischen Stimmabgabe (vote électronique) durch. Sie hat im Mai 2006 dem Bundesrat zu Handen des Parlaments einen Bericht über die Ergebnisse der Evaluation dieser Pilotprojekte unterbreitet. Sie zieht grundsätzlich eine positive Bilanz und wünscht einen Ausbau des Vote électronique. Ein heikler Punkt in diesem Zusammenhang ist die Frage der Nachvollziehbarkeit der Stimmabgaben und der Forderung eines Papierausdrucks der elektronischen Stimmen (Paper Trail; vgl. dazu auch unseren 9. Tätigkeitsbericht 2001/2002, Ziffer 1.1). Die Bundeskanzlei hat Vertreter des EDÖB und des Informatikstrategieorgans Bund (ISB) zu einer Besprechung eingeladen, um die Aspekte Stimmgeheimnis, Datenschutz und Informatiksicherheit einerseits und die Forderung nach einem Paper Trail andererseits zu erörtern.

Das detaillierte Verfahren zur Behandlung der Problematik des Paper Trail und der Nachvollziehbarkeit soll in der Arbeitsgruppe Vote électronique besprochen werden.

1.1.5 E-Government und Datenschutz

Im Rahmen einer in Bellinzona organisierten Tagung zum Thema E-Government waren wir eingeladen worden, einen Beitrag zu den Diskussionen einzubringen. Die Tagung war Teil der Veranstaltung „Tecnologia e Diritto" (Technologie und Recht), die jedes Jahr von der Höheren Fachschule für Wirtschaftsinformatik Bellinzona durchgeführt wird.

E-Government ist ein strategisches Ziel des Bundes. Es ist ein typischer Fall einer multidisziplinären Materie, die sowohl mit Recht als auch mit Informatik zu tun hat und Herausforderungen für den Datenschutz mit sich bringt.

Die E-Government-Projekte könnten theoretisch den gesamten Verkehr zwischen den Behörden (Bund, Kanton und Gemeinden) und den Bürgerinnen und Bürgern abdecken; ihr Ziel ist eine Optimierung der verschiedenen Dienste. Ein klassisches Beispiel ist die Anmeldung eines Wohnsitzwechsels; dieser Vorgang könnte über Internet abgewickelt werden und den Betroffenen ein persönliches Erscheinen bei den verschiedenen Gemeindekanzleien ersparen. Diese Art Projekte bringt nicht nur Vorteile, sie birgt auch datenschutzbedingte Risiken (im erwähnten Fall muss zum Beispiel vermieden werden, dass die fraglichen Daten von unbefugten Dritten abgefangen werden können).

Um die Diskussion und das Verständnis für diesen Bereich zu verbessern und zu vervollständigen, beschloss die Höhere Fachschule für Wirtschaftsinformatik Bellinzona, ihre jährliche Veranstaltung „Tecnologia e Diritto" (Technologie und Recht) im Jahr 2006 dem Thema E-Government zu widmen und eine Delegation des EDÖB einzuladen, welche die Risiken für den Datenschutz auf diesem Gebiet erläutern sollte. Wir nahmen diese Gelegenheit wahr, um auch die neuesten Entwicklungen betreffend die Einführung einer persönlichen Einheitsnummer (vgl. Ziffer 1.1.2) sowie die österreichische Lösung vorzustellen (vgl. unseren 13. Tätigkeitsbericht 2005/2006, Ziffer 1.2.1).

1.1.6. Publikation von Bundesgerichtsentscheiden im Internet

Urteile des Bundesgerichtes (sowie des fusionierten Eidgenössischen Versicherungsgerichtes) werden inzwischen bis zurück ins Jahr 1954 im Internet publiziert. Die Entscheide sind teilweise nicht anonymisiert und können sensible Personendaten enthalten. In solchen Fällen empfiehlt es sich, eine Anonymisierung der Online-Publikation zu verlangen.

Die grundsätzliche datenschutzrechtliche Problematik der Publikation von Bundesgerichtsurteilen haben wir bereits in unserem 9. Tätigkeitsbericht 2001/2002 (Ziffer 2.3.3) behandelt. Damals ging es um die Urteile, die ab 2000 ins Netz gestellt wurden.

Hier soll ein spezieller Punkt angesprochen werden, nämlich die älteren Urteile, die gefällt wurden, als noch niemand an eine spätere elektronische Publikation dachte. Auch solche Urteile des Bundesgerichtes bzw. des Eidgenössischen Versicherungsgerichtes (EVG) werden mittlerweile im Internet (www.bger.ch) publiziert.

Eine Person hat festgestellt, dass bei der Eingabe ihres Namens und Vornamens in Internetsuchmaschinen innert Kürze ein Urteil des EVG aus den 80er-Jahren im Volltext gefunden wurde. In diesem Urteil wurden äusserst sensible Daten insbesondere über den Gesundheitszustand dieser Person publiziert. Das Urteil war zwar in Papierform veröffentlicht worden und ist somit der Allgemeinheit zugänglich. Die Internetpublikation hat nun aber eine neue Qualität gebracht: Eine Suche ist mit geringstem Aufwand in kurzer Zeit und weltweit möglich.

Die betroffene Person hat sich an das Gericht gewandt und um die Anonymisierung des Urteils gebeten. Diese konnte erfreulicherweise auch erreicht werden. Zu beachten ist, dass ein Entscheid des Bundesgerichts bzw. des EVG auch dann nicht zwingend aus dem Netz verschwindet, wenn er in der offiziellen Internetpublikation anonymisiert wird. Denn es gibt andere Organisationen, die Urteile publizieren und diese in einer eigenen Datenbank verwalten. Eine Anonymisierung ist also gegebenenfalls auch direkt bei diesen Anbietern zu verlangen.

1.2 Datenschutzfragen allgemein

1.2.1 Verhaltenskodex im Bereich Pervasive Computing

Im Laufe des ersten Halbjahrs 2006 beteiligten wir uns an einem multidisziplinären Gedankenaustausch zum Thema Pervasive Computing, zu dem sich neben Datenschutzexperten auch Vertreter von Konsumentenschutzverbänden, Universitäten und privaten Organisationen oder Firmen zusammengefunden hatten. Dank der Zusammenarbeit dieser Vielzahl von Personen aus verschiedenen Fachrichtungen konnten allgemeine Orientierungen für die Verwendung der Technologien für Pervasive Computing und spezifische Regeln in drei möglichen Anwendungssektoren festgelegt werden.

Auf Initiative der Organisationen Stiftung Risiko-Dialog, Stiftung für Datenschutz und Informationssicherheit und ICT Switzerland kam es im Verlauf des ersten Halbjahrs 2006 zu einem multidisziplinären Dialog im Bereich Pervasive Computing. Die an uns gerichtete Einladung zur Teilnahme an diesen Gesprächen haben wir angesichts des in diesen neuen Technologien liegenden Potenzials für eine Beeinträchtigung der Privatsphäre gerne angenommen. Ziel dieses Gedankenaustausches waren namentlich die Analyse der mit diesen Anwendungen verbundenen Auswirkungen und Risiken und die Festlegung von allgemeinen Orientierungen auf diesem Gebiet sowie von spezifischen Regeln für bestimmte Sektoren wie etwa den medizinischen Bereich, den Detailhandel oder den Transportbereich.

Wir wirkten in der Arbeitsgruppe mit, die sich mit dem Sektor Einzelhandel befasste. Die Hauptanwendung von Pervasive Computing in diesem Bereich wird aller Wahrscheinlichkeit nach die Etikettierung sämtlicher Produkte mit RFID-Chips sein. Mit einer solchen Anwendung wird es möglich sein, jedes Produkt eindeutig zu lokalisieren und zu identifizieren, ohne dass dafür Sichtkontakt erforderlich ist. Dies wird namentlich ein neues Instrument in der Diebstahlbekämpfung darstellen. Für die Unternehmen beschränken sich die Vorteile jedoch nicht darauf: so wird beispielsweise die Ladeninventur dadurch verbessert und vereinfacht. Überdies können die von den Kunden innerhalb des Geschäfts zurückgelegten Wege leicht nachvollzogen und damit die Anordnung der zum Verkauf angebotenen Produkte optimiert werden.

In einigen Ländern haben Unternehmen bereits Versuche mit der Einführung einer derartigen Anwendung begonnen; aufgrund heftiger Proteste der Kundschaft gegen diese als übermässige Beeinträchtigung der Privatsphäre empfundene Neuerung sahen sie sich jedoch gezwungen, diese wieder rückgängig zu machen.

Dank der Diskussionen zwischen den verschiedenen Partnern war es möglich, nützliche, ausgewogene und befriedigende Orientierungen für den Einsatz solcher Anwendungen zu geben.

Initiativen dieser Art sind zu begrüssen und bieten eine gute Gelegenheit, potenzielle Probleme im Zusammenhang mit einer Verletzung der Privatsphäre möglichst proaktiv zu vermindern. Obwohl die Ergebnisse dieses Gedankenaustausches noch zu wenig konkret sind, als dass sie einen eigentlichen Verhaltenskodex bilden könnten, ist dieses Vorgehen unseres Erachtens ein erster Schritt in die richtige Richtung. Eine Fortsetzung der Bemühungen auf diesem Gebiet wäre für die Zukunft wünschenswert.

1.2.2 Der Einsatz von Aufklärungsdrohnen

Der Bundesrat hat den Einsatz von Aufklärungsdrohnen und mit Infrarot-System ausgerüsteten Helikoptern zugunsten des Grenzwachtkorps gutgeheissen. Nun muss die rechtliche Grundlage für den Einsatz militärischer Aufklärungsmittel zu zivilen Zwecken geschaffen werden.

Bereits im letzten Jahr haben wir uns mit dem Einsatz von Aufklärungsdrohnen beschäftigt: Auf Begehren der Zollverwaltung sollten Aufklärungsdrohnen der Armee für die Luftaufklärung im Grenzraum zugunsten des Grenzwachtkorps eingesetzt werden (s. unseren 13. Tätigkeitsbericht 2005/2006; Ziffer 2.2.1). Wir sind der Meinung, dass weder das Militärgesetz noch das Zollgesetz eine hinreichende gesetzliche Grundlage für den Drohneneinsatz beinhalten. Wir sprechen uns nicht grundsätzlich gegen einen solchen aus, verlangten aber, dass der Bundesrat zum einen den Überwachungseinsatz bewilligt und zum andern die notwendigen gesetzlichen Grundlagen zuhanden des Parlaments ausarbeiten lässt. Demgegenüber stellte sich das Eidgenössische Finanzdepartement (EFD) auf den Standpunkt, dass das Zollgesetz eine genügende gesetzliche Grundlage darstelle, und weigerte sich schliesslich, einen entsprechenden Bundesratsantrag auszuarbeiten.

In der Folge nahm sich das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) der Angelegenheit an und bereitete in Absprache mit uns einen entsprechenden Bundesratsantrag vor. Im Juli 2006 erteilte der Bundesrat die Bewilligung zum Einsatz von Aufklärungsdrohnen und mit einem speziellen Infrarot-System ausgerüsteten Helikoptern (so genannter FLIR Super Puma) zur Überwachung der Landesgrenze. Mit dem Infrarot-System können Wärmequellen erkannt werden, was das Auffinden und Verfolgen von Personen ermöglicht. Gemäss Bundesrat sollen die beiden Überwachungsmittel nur punktuell eingesetzt werden. Zudem dürfen gemäss Bundesratsbeschluss bis zum Inkrafttreten des neuen Zollgesetzes und der revidierten Verordnung über die Geländeüberwachung mit Videogeräten keine Daten aufgezeichnet werden. Gestützt auf diese Bewilligung haben das Grenzwachtkorps und die Armee eine Leistungsvereinbarung unterzeichnet, welche die Abläufe, Verantwortlichkeiten und Einsätze regelt.

In derselben Angelegenheit wurde eine Motion (05.3805) eingereicht, mit welcher der Bundesrat beauftragt werden sollte, dem Parlament eine Gesetzesgrundlage im formellen Sinne für den Einsatz von Drohnen im Dienste des Grenzwachtkorps zu unterbreiten. In einem Mitbericht zuhanden des Bundesrates haben wir aufgezeigt, dass bis anhin keine gesetzlichen Grundlagen für den Drohneneinsatz vorliegen. In

seiner Stellungnahme vom Mai 2006 vertrat der Bundesrat die Ansicht, dass für den Einsatz technischer Überwachungsmittel eine explizite formell-gesetzliche Grundlage im neuen Zollgesetz besteht. Des Weiteren führte er aus, dass er im Rahmen der Ausführungsbestimmungen die Verwendung präzisieren und so sicherstellen werde, dass der Einsatz verhältnismässig erfolge.

Inzwischen scheint der Bundesrat sein Meinung insofern geändert haben, als er sich bereit erklärt hat, im Rahmen der Teilrevision der Militärgesetzgebung (resp. im neu zu schaffenden Bundesgesetz über die militärischen Informationsmittel) eine formell-gesetzliche Grundlage für den Einsatz von Aufklärungsmitteln für zivile Zwecke zu schaffen (s. Ziffer 1.2.3). Die Frage, wann, wo und wie derartige Überwachungsgeräte der Armee auch zu zivilen Zwecken eingesetzt werden können, wird uns in Zukunft wohl immer öfters beschäftigen: Der Bundesrat hat den Einsatz von Aufklärungsdrohnen und des FLIR Super Pumas im Rahmen der EURO 08 gutgeheissen (s. Ziffer 1.3.5).

1.2.3 Revision des Militärgesetzes

Der Bundesrat hat den Entwurf zum Bundesgesetz über die militärischen Informationssysteme in die Vernehmlassung geschickt. Wir konnten unsere Anliegen überwiegend einbringen; eine grosse Differenz besteht indessen noch bei den Überwachungsmitteln.

Das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) hat die vom Bundesrat geforderte Teilrevision des Militärgesetzes im Berichtsjahr fortgesetzt (s. dazu auch unseren 13. Tätigkeitsbericht 2005/2006; Ziffer 2.2.2). Zu diesem Zweck sollten laut VBS die den Datenschutz betreffenden Bestimmungen im Militärgesetz angepasst werden. Zusammen mit dem Bundesamt für Justiz haben wir die Ansicht vertreten, dass die verschiedenen Informationssysteme der Armee und der Militärverwaltung in einem eigenen Gesetz zusammengefasst werden sollten. Das VBS schloss sich dieser Sichtweise an und legte schliesslich einen Entwurf zum Bundesgesetz über die militärischen Informationssysteme vor. Dieses Gesetz soll künftig die formellrechtliche Grundlage für die einzelnen militärischen Informationssysteme bilden. Entsprechend der Forderung des Datenschutzgesetzes nach einer hinreichenden gesetzlichen Grundlage muss dieses Gesetz für jedes einzelne Informationssystem den Bearbeitungszweck und den Umfang der Datenbearbeitung in groben Zügen festhalten sowie die am Informationssystem Beteiligten (Datenbearbeiter, allfällige Datenempfänger) ausdrücklich bezeichnen. Soweit in den Informationssystemen besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet werden, müssen die Kategorien der bearbeiteten Daten im Bundesgesetz aufgeführt werden.

Nach langen Diskussionen konnten wir uns mit dem VBS in den meisten Punkten auf datenschutzkonforme und für beide Seiten annehmbare Lösungen einigen. Eine grosse Differenz besteht in Bezug auf den Einsatz von Überwachungsmitteln (wie Drohnen, Wärmebildkameras, Infrarotsuchgeräte). Wir haben uns gegen einen Wortlaut gewehrt, der lediglich festhält, dass „mobile oder fest installierte, boden- oder luftgestützte, bemannte oder unbemannte Überwachungsgeräte und -anlagen" eingesetzt werden können. Damit würde unseres Erachtens eine Generalklausel für jede Form der staatlichen Überwachung ohne jegliche Einschränkungen geschaffen.

In einem liberal-demokratischen Rechtsstaat ist jede Form der staatlichen Überwachung ein schwerwiegender Eingriff in grundrechtlich geschützte Bereiche seiner Bürgerinnen und Bürger. Schwerwiegende Eingriffe müssen demokratisch legitimiert und daher in einem Gesetz im formellen Sinne vorgesehen und konkretisiert sein. Das Bundesgesetz muss die Art der Überwachung spezifizieren und ihre Rahmenbedingungen regeln. Mit andern Worten müssen die eingesetzten Überwachungsgeräte benannt und Art sowie Zweck der Überwachung im Bundesgesetz aufgeführt werden. Zudem muss ebenso klar festgehalten werden, welche Behörden zur Überwachung berechtigt sind, und ob sie Überwachungen auch zugunsten anderer Behörden oder sogar Privaten vornehmen dürfen. Diese Anforderungen sind keineswegs utopisch. So sind sie etwa im Bereich der Überwachung des Post- und Fernmeldeverkehrs unbestritten: Der Gesetzgeber hat im gleichnamigen Bundesgesetz (Überwachung des Post- und Fernmeldeverkehrs BÜPF) die Zulässigkeit und die Modalitäten der Überwachung ausführlich geregelt. Gleiches fordern wir auch für die militärischen Überwachungsgeräte.

Das VBS hat den Entwurf zum Bundesgesetz über die militärischen Informationssysteme dem Bundesrat vorgelegt, der ihn in einer Vernehmlassung der breiten Öffentlichkeit zur Diskussion unterbreitet hat. Wir gehen davon aus, dass die Frage des verdeckten oder offenen Einsatzes von militärischen Überwachungsmitteln zu militärischen oder zivilen Zwecken spätestens bei der Behandlung des Bundesgesetzes über die militärischen Informationssysteme im Parlament viel zu reden geben wird.

1.2.4 Revision der Zollverordnung

Biometrische Daten sind grundsätzlich besonders schützenswerte Personendaten. Darum muss in einem Gesetz festgelegt werden, welche biometrischen Daten zu welchem Zweck von einer Behörde bearbeitet werden dürfen. Im Rahmen der Revision der Zollverordnung haben wir insbesondere darauf geachtet, dass die biometrischen Daten wie auch die zulässigen Bearbeitungsmodalitäten zumindest im Ausführungserlass aufgeführt werden.

Biometrische Daten haben in den letzten Jahren stark an Bedeutung gewonnen. Es hat in diesem Bereich eine Entwicklung gegeben, welche vor einigen Jahren noch nicht absehbar war (z.B. Aufnahme biometrischer Daten im Schweizer Pass, DNA-Profil-Datenbank). Wir haben bereits in der Ämterkonsultation zum Ausweisgesetz auf diese noch nicht vollends abgeschlossene Entwicklung in der Biometrie hingewiesen und den äussert sensiblen Charakter biometrischer Daten hervorgehoben. Daher vertraten wir die Meinung, dass in der Regel in einem formell-rechlichen Erlass, d.h. in einem Bundesgesetz, festgehalten werden muss, welche biometrischen Daten von Behörden bearbeitet werden dürfen.

Konsequenterweise haben wir im Rahmen der Vorarbeiten zur Revision der Zollverordnung darauf hingewiesen, dass die in Art. 226 dieser Verordnung festgehaltenen biometrischen Merkmale eigentlich im Zollgesetz hätten aufgeführt werden müssen. Da das vor kurzem revidierte Zollgesetz aber lediglich davon spricht, dass der Bundesrat festlegt, welche biometrischen Daten abgenommen werden dürfen, forderten wir, dass die einzelnen biometrischen Daten und die zulässigen Bearbeitungsmodalitäten (inkl. eine allfällige Datenweitergabe und die Dauer der Aufbewahrung) biometrischer Daten in der Zollverordnung genau umschrieben und festgelegt werden. Nach längeren Diskussionen konnten wir uns mit der Zollverwaltung darauf einigen, welche biometrischen Daten zur Feststellung der Identität von Personen an der Grenze bearbeitet werden dürfen. Es sind dies Finger- und Handballenabdrücke, das DNA-Profil und Gesichtsbilder. Wir haben Wert darauf gelegt, dass dabei diejenigen Bundesgesetze aufgeführt werden, welche die Bearbeitung biometrischer Daten ausführlich regeln. Wir haben uns gegen das Sammeln auf Vorrat des Irismusters durch die Zollbehörden ausgesprochen. Zum heutigen Zeitpunkt besteht in der Schweiz unseres Wissens keine Irismusterdatensammlung, und weder die EU noch die USA verlangen, dass dieses biometrische Datum im Pass aufgeführt wird. Ein Sammeln ist daher nicht zweckmässig und verstösst gegen das Datenschutzgesetz.

Gemäss Zollgesetz müssen Verkehrsunternehmen der Zollverwaltung Einsicht in alle Unterlagen und Aufzeichnungen gewähren, die für die Zollprüfung von Bedeutung sein können. Dies erlaubt den Zollbehörden, von den Unternehmen Passagier- und Warenlisten herauszuverlangen. Wir haben durchgesetzt, dass diese Listen nicht wie von der Zollverwaltung gewünscht während drei Wochen, sondern lediglich während 72 Stunden aufbewahrt werden dürfen.

1.2.5 Die Teilrevision des Betäubungsmittelgesetzes

Im Rahmen der laufenden Teilrevision des Betäubungsmittelgesetzes haben wir darauf hingewirkt, dass die Datenbearbeitung auf der Grundlage dieses Erlasses exakter beschrieben wird. Auch hinsichtlich der neu vorgesehenen Meldebefugnis bei suchtbedingten Störungen sind gesetzgeberische Anstrengungen zur Präzisierung des Datenflusses notwendig.

Nachdem eine umfassende Revision des Betäubungsmittelgesetzes im Jahr 2004 gescheitert war, will eine parlamentarische Initiative nun jene Punkte umsetzen, die sich damals als mehrheitsfähig erwiesen haben. Die Vorlage will insbesondere den Jugendschutz, die Prävention und die Koordinationsrolle des Bundes stärken.

Der Erlassentwurf beinhaltet – wie vom Datenschutzgesetz gefordert – eine ausdrückliche gesetzliche Regelung der Personendatenbearbeitung. In ihrer Urfassung war die Bestimmung allerdings sprachlich derart breit gefasst, dass aus ihr nur ungenügend deutlich wurde, in welchen Fällen im Betäubungsmittelkontext Personendaten bearbeitet werden sollen. Unser diesbezüglicher Befund hatte einen bundesrätlicher Präzisierungsantrag zur Folge, gemäss dessen Fassung nun der Zweck der Datenbearbeitung, deren Umfang und die an ihr Beteiligten präziser umschrieben werden. Ergänzend ist festzuhalten, dass auf der Grundlage des Betäubungsmittelgesetzes weder ein Abrufverfahren noch eine regelmässige Datenbekanntgabe mittels Listen vorgesehen sind.

Bedeutsam ist aus Sicht des Datenschutzes ausserdem ein neu vorgesehenes, präventives Instrument der Drogenpolitik bei suchtbedingten Störungen, nämlich die Meldebefugnis bestimmter Amtsstellen und Fachleute zugunsten der zuständigen Behandlungs- und Sozialhilfestellen. Ungünstig ist, dass das Gesetz offen lässt, in welchen Fällen von einer suchtbedingten Störung auszugehen ist. Ein solches System bedeutet zwangsläufig eine Datenbearbeitung auf der Grundlage von Verdachtsmomenten, namentlich weil das Meldesystem auch bereits bei drohenden Suchtstö-

rungen greifen soll. Im Hinblick auf den Grundsatz der Datenrichtigkeit ist dies ein heikler Vorgang. Dies insbesondere, weil die der Datenbearbeitung zugrunde gelegte Vermutung im vorliegenden Fall durchaus stigmatisierend ist. Wir werden uns weiterhin dafür einsetzen, dass der Ermessensanteil beim Entscheid zur Datenbearbeitung durch gesetzgeberische Anstrengungen (mindestens auf Verordnungsstufe) auf ein Minimum reduziert wird.

1.2.6 Biometrische Zutrittskontrollen für Sport- und Freizeitanlagen

Die Prüfung der Datenschutzpraktiken bei den „KSS Sport- und Freizeitanlagen Schaffhausen" (nachstehend KSS) hat ergeben, dass die Verwendung biometrischer Daten für die Zutrittskontrolle zu den Anlagen nicht ganz den Datenschutzvorschriften entsprach. Wir haben uns insbesondere dafür eingesetzt, dass die biometrischen Daten nicht mehr zentralisiert gespeichert werden. Ausserdem muss Kundinnen und Kunden, die mit der Erfassung ihrer Fingerabdrücke nicht einverstanden sind, eine Alternativlösung angeboten werden. Wir sind der Auffassung, dass sich diese Empfehlungen analog auf andere private Anlagen desselben Sektors, soweit sie für ihre Zutrittskontrollsysteme biometrische Daten benutzen, anwenden lassen.

Die KSS verwenden seit Januar 2005 ein neues System, um die missbräuchliche Benutzung von persönlichen Halbjahres- oder Jahresabonnements für den Zutritt zum Schwimmbad und zu den Wellness-Anlagen zu bekämpfen. Neben den üblichen persönlichen Daten des Kunden werden auch seine Fingerabdrücke in Form von biometrischen Vorlagen (Templates) erfasst. Um in die Anlage zu gelangen, muss der Kunde seine Abonnentenkarte in ein mit der Zugangsschranke verbundenes Lesegerät einschieben. Danach muss der Abonnementsinhaber mit seinem Finger über einen in das Kartenlesegerät eingebauten Scanner streichen, damit das Gerät ein Prüftemplate des auf diese Weise digitalisierten Fingerabdrucks erstellen kann; diese Vorlage wird mit dem Referenztemplate abgeglichen. Die Zugangsschranke wird erst im Falle einer erwiesenen (über einem festgelegten Mindest-Schwellenwert liegenden) Übereinstimmung der beiden biometrischen Templates entsperrt. Vorgesehen war die Speicherung der Templates in einer zentralisierten Datenbank.

Angesichts der relativ hohen Schutzwürdigkeit der für die Zutrittskontrolle in einer Sport- und Freizeitanlage erhobenen Daten, und aufgrund der negativen Reaktionen mancher Kunden, die sich weigerten, in einem solchen Kontext ihre biometrischen Daten erfassen zu lassen, beschlossen wir, eine Kontrolle durchzuführen. Im Rahmen unseres Schlussberichts haben wir insbesondere empfohlen, den Abonnenten, die sich einer Erfassung ihrer biometrischen Daten widersetzten, eine Ersatzlösung zum gleichen Preis anzubieten; für die Kunden, die nichts gegen das Verfahren einzuwenden hätten, empfahlen wir die Speicherung ihrer biometrischen Daten in einem Chip in der Abonnentenkarte an Stelle einer zentralisierten Aufbewahrung. Wir betonten auch die Notwendigkeit, Fristen für die Löschung der persönlichen Daten und biometrischen Templates betreffend ehemalige Kunden festzulegen. Zudem verwiesen wir auf die Wichtigkeit einer Anonymisierung der durch das System erfassten Besucherdaten („wer hat die Anlage wann betreten?"). Unseres Erachtens dürfen die identifizierbaren Kundenbesuchsdaten nicht im Zentralsystem gespeichert werden. Für die Ausführung der erweiterten Funktionen der Zutrittskontrolle ist die Speicherung der identifizierbaren Daten auf der Smartcard des Abonnenten völlig ausreichend; die Zentralisierung der Kundenbesuchsdaten, die zu statistischen Zwecken erfasst werden, muss in anonymer Form erfolgen. Die KSS haben sich bereit erklärt, ihr System binnen nützlicher Frist allen unseren Empfehlungen anzupassen und die meisten unserer Verbesserungsvorschläge zu befolgen. Darüber hinaus haben wir die KSS ersucht, uns nach der Einführung sämtlicher Massnahmen zu informieren, damit wir überprüfen können, ob sie den abgegebenen Empfehlungen auch wirklich entsprechen.

Der vollständige Bericht über diese Kontrolle sowie eine Zusammenfassung und eine Medienmitteilung sind auf unserer Website veröffentlicht worden. Dem Schlussbericht wurde ein Anhang beigefügt; dieser gibt die Meinungen und Antworten der KSS zu der durchgeführten Kontrolle sowie unsere Schlussbeurteilung wieder.

1.2.7 Identitätskontrolle bei Spielbankenbesuchern

Die eidgenössische Spielbankenkommission (ESBK) hat uns angefragt, ob und in welchem Ausmass eine Spielbank Informationen betreffend die Besucher ihrer Einrichtung erfassen, aufbewahren und verwerten kann, um spielsuchtgefährdete Personen frühzeitig zu erkennen. Wir waren der Auffassung, dass die geltende Gesetzgebung eine derartige Datenbearbeitung nicht gestattet. Eine Rechtsgrundlage ist im Prinzip wünschenswert. Allerdings könnten die Spielkasinos einen anderen Rechtfertigungsgrund geltend machen, etwa ein überwiegendes privates oder öffentliches Interesse. In jedem Fall ist ein Datenschutzkonzept ausdrücklich vorzusehen.

Die eidgenössische Spielbankenkommission (ESBK) hat sich mit der Frage an uns gewandt, ob und in welchem Ausmass eine Spielbank Informationen betreffend die Besucher der Einrichtung erfassen, aufbewahren und verwerten können, um spielsuchtgefährdete Personen frühzeitig zu erkennen. Es sollte insbesondere geprüft werden, ob die zu anderen Zwecken (Marketing, Bekämpfung der Geldwäscherei) beschafften Informationen auch im Rahmen der Erstellung eines Sozialkonzepts verwendet werden könnten.

Die Erhebung, Aufbewahrung und Auswertung von Informationen über Spielkasinobesucher stellen eine Bearbeitung von Personendaten im Sinne des Bundesgesetzes über den Datenschutz (DSG) dar. Als Privatpersonen müssen die Kasinos sich auf einen der Rechtfertigungsgründe nach Art. 13 DSG berufen können, nämlich die Einwilligung des Betroffenen, ein überwiegendes privates oder öffentliches Interesse oder eine gesetzliche Grundlage. Um den Spielkasinos eine solche Datenbearbeitung vorschreiben zu können, muss sich die ESBK – als Bundesorgan – ihrerseits unbedingt auf eine Rechtsgrundlage stützen können (Art. 17 DSG).

Wir überprüften daher zunächst, ob in diesem Fall die geltende Gesetzgebung eine solche Datenbearbeitung vorsieht. Wir stellten fest, dass das Bundesgesetz über Glücksspiele und Spielbanken (SBG) die Spielbanken zur Erstellung eines Sozialkonzepts verpflichtet; wie die Vollzugsverordnung zu diesem Gesetz ausführt, müssen die Spielbanken Massnahmen gemäss im Voraus festgelegten Beobachtungskriterien ergreifen. Wir sind jedoch der Ansicht, dass die von den Spielbanken durchgeführten Datenbearbeitungsmassnahmen zur Vorbeugung gegen die sozial schädlichen Auswirkungen des Spiels ausdrücklich in einer formellgesetzlichen Grundlage vorgesehen sein müssen. Bei den erhobenen Informationen, die die Gesundheit betreffen, handelt es sich um besonders schützenswerte Daten im Sinne des DSG.

Die Spielbanken verfügen über Informationen, die in Ausführung des Bundesgesetzes zur Bekämpfung der Geldwäscherei (GwG) erfasst werden. Für die Verwendung von Personendaten im Rahmen der Durchführung des Sozialkonzepts zu anderen Zwecken als zur Bekämpfung der Geldwäscherei können sich die Spielbanken bzw. die ESBK jedoch nicht auf diese Rechtsgrundlagen berufen. Die Spielbanken haben auch die Möglichkeit, die Daten ihrer Kunden für Marketingzwecke zu registrieren, soweit die Betroffenen ihre Einwilligung dazu geben. Gemäss dem Grundsatz der Zweckbestimmung dürfen die erhobenen Daten indessen nur für Marketingzwecke verwendet werden, und nur dann, wenn der Betroffene seine Einwilligung nach freien Stücken und in Kenntnis der Sache erteilt hat. Folglich ist festzuhalten, dass die ESBK und die Spielbanken über keine genügend präzise Rechtsgrundlage verfügen, um andere als die in der Spezialgesetzgebung ausdrücklich erwähnten Datenbearbeitungen rechtfertigen zu können.

Die Spielbanken als private Einrichtungen könnten sich ihrerseits auf einen anderen Rechtfertigungsgrund berufen, und zwar die Einwilligung des Betroffenen oder ein überwiegendes privates oder öffentliches Interesse, und die verfügbaren Daten im Zusammenhang mit dem Sozialkonzept verwenden. Eine derartige Datenbearbeitung unterliegt indessen den allgemeinen Datenschutzprinzipien, insbesondere den Grundsätzen der Zweckmässigkeit, der Verhältnismässigkeit und der Transparenz.

Auf jeden Fall sind wir der Ansicht, dass eine neue Rechtsgrundlage wünschenswert wäre, um die vorhandenen Instrumentarien zur Früherkennung von spielsüchtigen Personen verwenden zu können. Die besondere Schutzwürdigkeit der im Rahmen des Sozialkonzepts bearbeiteten Daten und das verfolgte öffentliche Interesse sind einschlägige Gründe für eine klare gesetzliche Grundlage. Überdies könnte mit der Festlegung eines rechtlichen Rahmens die Gewähr geboten werden, dass sämtliche Spielbanken das Sozialkonzept gleich wirksam umsetzen.

Abschliessend haben wir darauf hingewiesen, dass die Spielbanken in jedem Fall ein Konzept für die in ihren Einrichtungen vorgenommenen Datenbearbeitungen vorsehen müssen. Sie haben insbesondere die erhobenen Daten, ihre Zweckbestimmung sowie ihre Aufbewahrungsdauer festzulegen; ebenso muss der allfällige Zugriff durch Behörden oder Dritte geregelt werden, und gemäss dem Grundsatz der Transparenz ist auch eine Information der Betroffenen zwingend notwendig.

1.2.8 Elektronische Zugangssysteme in den Skigebieten und Datenschutz

Die Kontrolle des Zutritts zu den Skigebieten erfolgt mit immer höher entwickelten Systemen, die für den Datenschutz problematisch sein können. Beim Erwerb eines Abonnements muss der Skifahrer seine Personalien bekannt geben und eine Fotografie vorlegen. Bei der Erfassung und Verwendung dieser Personendaten muss die Datenschutzgesetzgebung eingehalten werden. Die Betreiber von Wintersportanlagen können sich nicht auf ein überwiegendes privates Interesse berufen, um die Personendaten der Abonnementsinhaber öffentlich anzuzeigen. Die Prüfung der Gültigkeit der Abonnemente und die Vermeidung von Missbräuchen sind auch mit anderen, dem Schutz der Privatsphäre besser angepassten Mitteln möglich.

Beim Kauf eines Abonnements muss der Skifahrer eine Fotografie vorlegen sowie Angaben zu seiner Person machen. Die Erhebung und Verwendung dieser Personendaten bilden eine Datenbearbeitung im Sinne des Datenschutzgesetzes (DSG), dessen Bestimmungen somit zur Anwendung kommen. Die Betreiber von Wintersportanlagen setzen zunehmend elektronische Systeme für die Zugangskontrolle ein. An manchen Wintersportorten erscheint das Foto des Abonnementsinhabers auf einem Bildschirm, sobald der Benutzer die Schranke passiert. Mit einem solchen System soll einerseits kontrolliert werden, ob der Inhaber des Abonnements mit dem Benutzer identisch ist, und andererseits soll die Gültigkeit des Abonnements festgestellt werden. Im Allgemeinen wird die Kontrolle durch das Personal der Wintersportanlagen vorgenommen; in manchen Skigebieten ist der Bildschirm jedoch auch für Dritte sichtbar, die sich in der Nähe der Kontrollstelle befinden. Die Personendaten des Abonnementsinhabers erscheinen dann auf dem Bildschirm und bleiben dort sichtbar, bis der nächste Kunde die Schranke passiert, was mehrere Minuten dauern kann. Mehrere Personen haben sich bei uns über die öffentliche Anzeige ihrer Personendaten beschwert. Wir haben daher die Konformität dieses Verfahrens mit dem DSG überprüft.

Jedermann hat Anspruch auf Achtung seiner Privatsphäre und ist insbesondere berechtigt, seine Identität gegenüber Dritten, einschliesslich im Rahmen seiner Freizeitaktivitäten, abzuschirmen. Andererseits kann eine Privatperson für die Bearbeitung von Personendaten einen Rechtfertigungsgrund geltend machen: das kann ein Gesetz sein, ein überwiegendes privates oder öffentliches Interesse oder auch die Einwilligung der Betroffenen. Die allgemeinen Datenschutzprinzipien sind selbst bei Bestehen eines Rechtfertigungsgrundes einzuhalten.

Verfügt der Betreiber einer Wintersportanlage über einen Rechtfertigungsgrund, der es ihm gestattet, die Daten der Inhaber eines Skiabonnements in einer auch für Dritte sichtbaren Form auf dem Bildschirm anzuzeigen? Ein Gesetz gibt es auf diesem Gebiet nicht, und es kann auch kein öffentliches Interesse geltend gemacht werden. Es bleiben somit, als mögliche Rechtfertigungsgründe, nur ein überwiegendes privates Interesse oder die Einwilligung der Betroffenen.

Der Betreiber einer Wintersportstation hat natürlich ein legitimes Interesse daran, die Gültigkeit der Abonnemente zu prüfen und sich zu vergewissern, dass nicht übertragbare Abonnemente nicht missbräuchlich von Dritten benutzt werden. Zu diesem Zweck hat er das Recht, elektronische Systeme für die Zutrittskontrolle einzurichten. Dabei muss er aber auch die allgemeinen Datenschutzgrundsätze einhalten, insbesondere die Prinzipien der Zweckbestimmung, der Verhältnismässigkeit und der Transparenz. Im vorliegenden Fall bezweifeln wir, dass eine öffentliche Anzeige die Prüfung der Gültigkeit der Abonnemente ermöglicht. Es ist nicht Sache der anderen Kunden, sich an Stelle des Personals zu vergewissern, dass kein Missbrauch vorliegt. Es hat vielmehr den Anschein, dass der Einsatz solcher Systeme etwaige Schwarzfahrer abschrecken soll; im Falle eines Missbrauchs werden aber nicht die Personendaten des Skifahrers angezeigt, sondern die Daten des Abonnementsinhabers, der von dem Missbrauch nicht unbedingt Kenntnis hat und damit zu Unrecht angeprangert wird.

Ausserdem empfiehlt es sich, entsprechend dem Grundsatz der Verhältnismässigkeit, so weit wie möglich Massnahmen anzuwenden, mit der die Privatsphäre am besten geschützt bleibt. Die öffentliche Anzeige von Personendaten bedeutet einen nicht geringfügigen Eingriff in die Privatsphäre der Betroffenen. Im vorliegenden Fall entspricht eine solche Massnahme nicht dem Verhältnismässigkeitsprinzip, denn es gibt andere Kontrollmittel, die wirksam sind und zugleich den Erfordernissen des Datenschutzes gerecht werden, beispielsweise systematisch oder stichprobenweise von Angestellten durchgeführten Kontrollen; einzig das Personal darf Einblick auf die Bildschirme haben.

In Anbetracht dieser Erwägungen können die Betreiber von Wintersportanlagen kein überwiegendes privates Interesse an der öffentlichen Anzeige von Personendaten geltend machen. Der einzige verbleibende Rechtfertigungsgrund wäre die Einwilligung der Betroffenen. Dieses Einverständnis muss frei und in Kenntnis der Sachlage erteilt werden: der Kunde muss sich der Bearbeitung seiner eigenen Daten widersetzen können, ohne dass ihm daraus irgend ein Nachteil entsteht. Die öffentliche Anzeige der Personendaten müsste somit fakultativ sein, was technisch möglich wäre, der Kontrollabsicht der Betreiber aber nicht entsprechen würde.

Wir sind zum Schluss gekommen, dass die öffentliche Anzeige der Fotografie und der Identität der Benutzer von Wintersportanlagen zu Kontrollzwecken nicht der Datenschutzgesetzgebung entspricht. Die Bekanntgabe von Personendaten an Dritte ist in der Tat unnötig und widerspricht dem Grundsatz der Verhältnismässigkeit. Es können auch mit anderen Mitteln, die den Schutz der Privatsphäre besser gewährleisten, die Gültigkeit der Abonnemente überprüft und Missbräuche vermieden werden, beispielsweise durch systematische oder sporadische Kontrollen, wie sie in den öffentlichen Verkehrsmitteln üblich sind. Wir haben die betroffenen Personen auf ihr Klagerecht gemäss von Art. 15 DSG aufmerksam gemacht.

1.2.9 Kontrolle des Bearbeitungsreglements für das Informationssystem AVAM

Bei den von uns kontrollierten Bearbeitungsreglementen sind in vielen Fällen noch Mängel in der Umsetzung der technischen und organisatorischen Massnahmen festzustellen. Sie betreffen insbesondere die Verschlüsselung und die Protokollierung, aber auch die Kontrollverfahren und die Dokumentation der Prozesse (Abläufe). Vorgaben zum Inhalt eines Bearbeitungsreglements sind auf unserer Website aufgeführt.

Das Informationssystem AVAM des Staatssekretariats für Wirtschaft (SECO) wird für die Arbeitsvermittlung und die Arbeitsmarktstatistik eingesetzt. Für ein solches System ist ein Bearbeitungsreglement zu erstellen. Dieses wurde vom SECO gemäss den Vorgaben, die wir auf unserer Website publiziert haben, erstellt (www.edoeb.admin.ch, Dokumentation – Datenschutz – Leitfäden – Technische und organisatorische Massnahmen).

Wir haben das Reglement kontrolliert und einige Punkte als verbesserungswürdig erachtet.

Bei der Schnittstellenbeschreibung, die u. a. den Informationsfluss zwischen dem AVAM (SECO) und den vom System betroffenen Organisationseinheiten aufzeigt, wurden nicht überall die in der Folge aufgeführten Datenfelder umschrieben: VON (von wo stammen die Daten, z.B. AVAM/SECO); NACH (wohin werden die Daten übertragen, z.B. an die regionalen Arbeitsvermittlungszentren); Zweck (was soll mit der Datenübertragung erreicht werden?); DATENART (welche Daten(arten) werden übertragen?); PERIODIZITÄT (in welcher Regelmässigkeit werden die Daten übertragen?); AUSLÖSER (wer löst die Datenübertragung aus?); MEDIUM (mit Hilfe welcher Kommunikationsmittel werden die Daten übertragen?)

Im Weiteren wird nur grob festgehalten, welche Projekt- und Systemdokumente in etwa erstellt wurden. Es fehlt indessen eine abschliessende Liste der Dokumente, die für die Systemplanung und -realisierung sowie den Systembetrieb erstellt wurden. Damit wäre aber eine gewisse Transparenz und Nachvollziehbarkeit gewährleistet.

Die Abläufe bzw. die Prozessgruppen wurden im Reglement festgehalten. Für detailliertere Informationen wurde auf das Intranet verwiesen. Dabei stellte sich aber heraus, dass gewisse Daten, insbesondere die grafischen Abläufe, nicht abgerufen werden konnten und gewisse Prozessbeschreibungen wie z.B. die Kontrollprozesse fehlten (der Datenschutz unterscheidet zwischen den herkömmlichen Aufgabenerfüllungsprozessen, den Kontrollprozessen sowie den Prozessen für die Wahrnehmung des Auskunftsrechts).

Bei den Kontrollverfahren ist festzuhalten, welche Kontrollen in der Planungs- und Realisierungsphase durchlaufen wurden und welche Kontrollverfahren für die Betriebsphase vorgesehen sind. Im Verlaufe der Betriebsphase ist dann auch festzuhalten, welche Kontrollen durchgeführt wurden. Kontrollverfahren sind u. a. auch Protokollauswertungen. Es ist zu dokumentieren, wer wann welche Protokolle auswertet.

Wir haben dem SECO die Verbesserungsvorschläge unterbreitet. Im Weiteren haben wir um Nachführung und Neuzustellung des Reglements gebeten.

Aufgrund der bis heute gemachten Erfahrungen werden wir vermehrt Bearbeitungsreglemente begutachten.

1.3 Justiz/Polizei/Sicherheit

1.3.1 Hooliganismusbekämpfung

Auch in der Schweiz ist gewalttätiges Auftreten von so genannten Hooligans im Rahmen von Sportveranstaltungen seit einiger Zeit zu beobachten. Um diesem Problem entgegenzuwirken, wurden im Jahr 2002 entsprechende Gesetzgebungsarbeiten auf Bundesebene eingeleitet. Die daraus resultierenden Bestimmungen im Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) und der dazugehörigen Verordnung (VWIS) sind am 1. Januar 2007 in Kraft getreten.

Mit den neuen Bestimmungen zur Bekämpfung des Hooliganismus wird einerseits eine Datenbank geschaffen, worin Daten über Personen aufgenommen werden, die sich anlässlich von Sportveranstaltungen „gewalttätig verhalten haben" (Artikel 24a Absatz 1 BWIS). Andererseits werden dadurch verschiedene Massnahmen wie Rayonverbot, Ausreisebeschränkung, Meldeauflage und Polizeigewahrsam vorgesehen. In datenschutzrechtlicher Hinsicht haben sich in diesem Zusammenhang zwei heikle Punkte herauskristallisiert.

Zunächst geht es um Unklarheiten betreffend die Voraussetzungen für die Aufnahme in die Datenbank. Zwar scheint die oben erwähnte Formulierung des Gesetzes BWIS recht klar, diese Klarheit wird aber durch die Artikel 21a und 21b der Verordnung gleich mehrfach verwischt. Art. 21a zählt eine Anzahl von Straftatbeständen auf, bei deren Vorliegen ein gewalttätiges Verhalten gegeben sein soll. Diese Aufzählung ist der Klarheit nicht förderlich, weil sie mit dem Ausdruck „namentlich" eingeleitet wird und damit als nicht abschliessend gekennzeichnet ist. Art. 21b der Verordnung weicht die Grenzen weiter auf, indem er bestimmt, dass gewalttätiges Verhalten auch dann als nachgewiesen betrachtet wird, wenn jemand von einem Sportverein ein Stadionverbot erhalten hat (Art. 21b Abs. 1 Buchstabe c). Für die betroffenen Personen kann sich diese Regelung als problematisch erweisen, weil solche Stadionverbote durchaus willkürlich ausgesprochen werden können und dagegen auch keine Rechtsmittel zur Verfügung stehen.

Der zweite datenschutzrechtlich heikle Punkt liegt in der Unbestimmtheit der Regelungen betreffend Datenweitergaben an Private (z.B. Sportstadienbetreiber) und betreffend Datenbearbeitungen durch diese. Schon allein die Tatsache, dass Daten aus einer staatlichen Datenbank regelmässig und in beträchtlichem Umfang auch an Private weitergegeben werden, ist nicht unproblematisch. Deshalb hat der Gesetzgeber vorgesehen, dass der Bundesrat regeln soll, „wie die Daten durch die Empfänger und durch Dritte bearbeitet werden" (Art. 24a Abs. 8 BWIS). Dieser gesetzliche Auftrag wird jedoch in der Verordnung nicht erfüllt. Stattdessen wird die Angelegenheit auf eine tiefere Normstufe verschoben. Art. 21k der Verordnung bestimmt nämlich, dass der Dienst für Analyse und Prävention (DAP) die Verwendung und Bearbeitung der Daten durch die Organisatoren von Sportveranstaltungen im Bearbeitungsreglement des Informationssystems regelt. Im Bearbeitungsreglement selbst werden jedoch die erforderlichen Regeln ebenfalls nicht definiert. Vielmehr sagt dessen Art. 27 Abs. 3, der DAP erlasse „in enger Zusammenarbeit mit den Sportveranstaltern Richtlinien über die Einzelheiten der Datenweitergabe durch die Sportveranstalter". Diese Bestimmung gibt Anlass zu Kritik, weil damit die Kaskade der Sub-Delegationen weitergeführt wird, ohne dass inhaltliche Klarheit erreicht würde. Sie schafft vielmehr noch weitere Unklarheiten, indem darin von einer Datenweitergabe durch Sportveranstalter die Rede ist. Es ist bis heute nicht absehbar, wie die beschriebenen offenen Fragen geklärt werden können und wann dies geschehen wird.

1.3.2 Pilotprojekt für einen nationalen Polizeiindex

Die Einführung eines Pilotprojekts für einen nationalen Polizeiindex ist erst mit dem vorgezogenen Inkrafttreten von Artikel 17a des Datenschutzgesetzes möglich geworden. Wir haben für diesen Fall eine positive Stellungnahme abgegeben und angekündigt, dass wir bei den verschiedenen Benutzern einen Augenschein vor Ort vornehmen werden, um zu überprüfen, ob die für diesen Pilotversuch festgelegten Bedingungen eingehalten werden.

Das Bundesamt für Polizei (fedpol) konsultierte uns im Sommer 2006 zur Einführung eines Pilotprojekts für einen nationalen Polizeiindex. Da die geltend gemachten gesetzlichen Grundlagen nicht ausreichend waren und der neue Artikel 17a des Bundesgesetzes über den Datenschutz (DSG) betreffend Pilotprojekte noch nicht in Kraft war, erklärten wir fedpol, dass ein derartiges Pilotprojekt nicht durchgeführt werden könne. Das fedpol schlug daraufhin eine vorgezogene Inkraftsetzung des neuen Artikels 17a DSG vor. Der Vorschlag enthielt auch ein Gutachten des Bundesamtes für Justiz, dem zufolge eine einzige Bestimmung durchaus vor der Gesamtheit der revidierten Normen eines Gesetzes in Kraft treten kann. Die Verordnung über den Pilotbetrieb des nationalen Polizeiindexes und die Verordnung über die vorgezogene Inkraftsetzung von Artikel 17a DSG sind seit dem 15. Dezember 2006 in Kraft. Nachdem wir aufgrund der von fedpol erteilten Auskünfte festgestellt hatten, dass die in dieser neuen Bestimmung für die Einführung des Pilotprojektes aufgestellten Bedingungen erfüllt waren, gaben wir eine positive Stellungnahme ab. Wir erinnerten das Bundesamt daran, dass es dem Bundesrat spätestens zwei Jahre nach Inbetriebnahme der Versuchsphase einen Evaluationsbericht vorzulegen habe. Wir betonten, dass das Pilotprojekt für einen nationalen Polizeiindex wegen der vorgezogenen Inkraftsetzung von Art. 17a DSG ein Sonderfall sei. Wir erwähnten auch, dass im Rahmen der Revision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) Ausführungsbestimmungen betreffend Art. 17a DSG auszuarbeiten sein werden. Wir wiesen ausdrücklich darauf hin, dass unsere Stellungnahme zum Pilotprojekt für einen nationalen Polizeiindex Ausnahmecharakter habe und nicht als Präzedenzfall dienen könne. Gewisse Punkte könnten in Zukunft anders beurteilt werden, so zum Beispiel die Liste der Teilnehmer an dem Pilotprojekt oder die im Rahmen des Pilotprojekts verwendeten Daten. Schliesslich teilten wir fedpol mit, dass wir einen Augenschein bei einem Benutzer innerhalb des Bundesamtes, bei einem Benutzer des Grenzwachtkorps und, in Zusammenarbeit mit der kantonalen Datenschutzbehörde, bei einem kantonalen Benutzer vor Ort vornehmen werden.

1.3.3 Indirektes Auskunftsrecht

In einem Entscheid vom 31. August 2006 hielt die Eidgenössische Datenschutz- und Öffentlichkeitskommission fest, dass das so genannte indirekte Auskunftsrecht den Anforderungen der Europäischen Menschenrechtskonvention (EMRK) nicht genüge. Gerade in Fällen, in denen eine Gefährdung der freiheitlich-demokratischen Verfassungsordnung der Schweiz oder des Bestandes, der Unabhängigkeit und Sicherheit des Bundes und der Kantone ausgeschlossen werden könne, seien Informationen der betroffenen Personen über die Datenbearbeitung zwingend. Gestützt auf diesen Entscheid haben wir unsere Auskunftspraxis angepasst.

In Zusammenhang mit dem so genannten indirekten Auskunftsrecht hat die Eidgenössische Datenschutz- und Öffentlichkeitskommission (EDÖK) ein weiteres Urteil gefällt. Vorab ist darauf hinzuweisen, dass hier kein eigentliches Auskunftsrecht vorliegt, weil die betroffene Person, die ein Auskunftsgesuch gestellt hat, von uns in der Regel nur eine stets gleich lautende Antwort erhält, die keinen Aufschluss darüber gibt, ob sie erfasst ist oder nicht (vgl. auch unseren 7. Tätigkeitsbericht 1999/2000, Ziff. I. 1.2). Im erwähnten Entscheid der EDÖK ging es allerdings um die Anwendung der Ausnahmeregelung Art. 18 Abs. 3 des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS). Nach diesem Artikel können wir von der erwähnten, gesetzlich vorgesehenen Standardantwort abweichen und ausnahmsweise der gesuchstellenden Person in angemessener Weise Auskunft erteilen, wenn damit keine Gefährdung der inneren oder der äusseren Sicherheit verbunden ist und wenn der gesuchstellenden Person sonst ein erheblicher, nicht wieder gut zu machender Schaden erwächst.

In ihren Erwägungen stellte die EDÖK zunächst fest, dass Art. 18 BWIS grundsätzlich kein Auskunftsrecht der betroffenen Person vorsehe, sondern nur eine besondere und unabhängige Verwaltungskontrolle, in erster Instanz durch den EDÖB und in zweiter Instanz durch die EDÖK. Nur ausnahmsweise sei eine Information nach Art. 18 Abs. 3 BWIS vorgesehen. Zudem sollten registrierte Personen nachträglich über die Datenbearbeitung informiert werden, allerdings nach Art. 18 Abs. 6 BWIS und nur, „sofern dies nicht mit unverhältnismässigem Aufwand verbunden" sei.

Die EDÖK bemängelte sodann, dass wir in unseren Empfangsbestätigungen, die wir den betroffenen Personen nach Erhalt des indirekten Auskunftsgesuchs standardmässig zustellen, nicht ausdrücklich auf die Tatsache hinweisen, dass bei Darlegung eines erheblichen, nicht wieder gut zu machenden Schadens eine angemessene Information möglich sei. Dies führe dazu, dass die meisten gesuchstellenden Personen keinerlei Chance hätten, ausnahmsweise beschränkte Auskunft nach Art. 18 Abs. 3 BWIS zu erhalten.

Sodann beurteilte die EDÖK die Bestimmung von Art. 18 Abs. 3 BWIS auch aus verfassungsrechtlicher und völkerrechtlicher Sicht unter Beizug von Urteilen des Bundesgerichts sowie des Europäischen Gerichtshofs für Menschenrechte. Aus diesen ergebe sich klar, dass auch der blosse Verdacht oder eine Falschauskunft eines Polizeibeamten eine schwere Beeinträchtigung darstellen, die durch die pauschale Mitteilung nach Art. 18 BWIS höchstens noch verschärft werden. Gerade in Fällen, in denen eine Gefährdung der freiheitlich-demokratischen Verfassungsordnung der Schweiz oder des Bestandes, der Unabhängigkeit und Sicherheit des Bundes und der Kantone ausgeschlossen werden könne, seien Informationen der betroffenen Personen über die Datenbearbeitung zwingend. Die EDÖK kam daher zum Schluss, dass Art. 18 Abs. 1 und 2 BWIS den Anforderungen der Europäischen Menschenrechtskonvention (EMRK) nicht genüge.

Die Ausnahmeregelung von Art. 18 Abs. 3 BWIS sei derart irrational und zweckwidrig, dass sie offensichtlich dem EDÖB keine vernünftige Praxis erlaube, die dem Grundrechtsschutz und den Zwecken von Art. 1 BWIS Rechnung trage. Es sei festzuhalten, dass es mit den in EMRK und Bundesverfassung vorgesehenen Sicherungen der Grundrechte nicht vereinbar sei, eine Auskunft praktisch auszuschliessen.

Gestützt darauf empfahl uns die EDÖK, im vorliegenden Fall die gesuchstellende Person gemäss Art. 18 Abs. 3 BWIS darüber zu informieren, dass sie nicht registriert sei. Weiter wurde uns empfohlen, die Modalitäten der Information von Personen, die um eine Auskunft im Bereich polizeilicher Datenbearbeitung des Bundes ersuchen, so zu modifizieren, dass wir im Sinne dieses Entscheides der EDÖK auch Auskunft erteilen könnten. Dem Bundesamt für Polizei empfahl die EDÖK, im Rahmen der laufenden Revision des BWIS eine EMRK-konforme Regelung des datenschutzrechtlichen Auskunftsrechts im BWIS einzuleiten.

Wir haben nun unsere Empfangsbestätigungen zum indirekten Auskunftsrecht entsprechend geändert. So machen wir die gesuchstellende Person ausdrücklich darauf aufmerksam, dass sie der gesetzlich vorgesehenen Standardantwort nicht werde entnehmen können, ob über sie im Informationssystem Einträge vorhanden sind oder nicht. Gleichzeitig weisen wir sie ausdrücklich auf die Ausnahmebestimmung von Art. 18 Abs. 3 BWIS und die Möglichkeit hin, uns innert 30 Tagen darzulegen, aus welchen Gründen ihr durch das Ausbleiben angemessener Information ein nicht wieder gut zu machender Schaden erwachse. Schliesslich haben wir die Erwägungen der EDÖK zu Art. 18 Abs. 3 BWIS in unsere Praxis aufgenommen und entscheiden jeweils im Einzelfall, ob die Voraussetzungen dieser Bestimmung erfüllt sind oder nicht.

1.3.4 Verlängerung der Aufbewahrungsdauer von Telekommunikations-Verkehrsdaten

Im Rahmen eines Berichts des Bundesrates im Anschluss an ein Postulat zum Thema einer wirksameren Bekämpfung des Terrorismus und der organisierten Kriminalität wurden wir zu einer Stellungnahme aufgefordert, die sich namentlich auf eine mögliche Verlängerung der Aufbewahrungsdauer der Verkehrsdaten von sechs auf zwölf Monate beziehen sollte. Wir halten eine solche Massnahme für unverhältnismässig.

Die sicherheitspolitische Kommission des Ständerats ersuchte den Bundesrat, die in der Gesetzgebung vorzunehmenden Änderungen für einen wirksameren Kampf gegen den Terrorismus und die organisierte Kriminalität zu prüfen. Die Kommission war namentlich der Auffassung, dass die für die Datenaufbewahrung im Hinblick auf eine rückwirkende Kontrolle der Kommunikationen geltende Frist von sechs Monaten zu kurz sei. Im Rahmen seines Berichts zur Beantwortung dieses Postulats schlug der Bundesrat vor, anlässlich einer späteren Anpassung der Gesetzgebung (Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)) die Frist von sechs auf zwölf Monate zu verlängern. Wir wurden um eine Stellungnahme zu den Schlussfolgerungen dieses Berichts ersucht.

Die systematische und obligatorische Aufbewahrung der Daten bedeutet eine erhebliche Einschränkung des Schutzes der Privatsphäre und bedarf einer vollumfänglichen Rechtfertigung. Unseres Erachtens ist die bisherige Frist von sechs Monaten bei weitem ausreichend, und wir sind daher der Auffassung, dass eine Verlängerung dieser Frist unverhältnismässig wäre. Namentlich in Fällen der internationalen Rechtshilfe wäre es denkbar, dass sofort nach Eingang des Gesuchs die Blockierung der Daten bei dem zuständigen Organ beantragt würde, damit die gesamte Frist bestehen bleibt.

Darüber hinaus haben wir auch auf die Stellungnahme der Arbeitsgruppe „Artikel 29" vom 21. Oktober 2005 zum Vorschlag für eine Richtlinie des europäischen Parlaments und des Europarates über die Vorratsspeicherung von Daten Bezug genommen (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_de.pdf).

Für den Fall, dass die Dauer der Datenaufbewahrung dennoch auf zwölf Monate verlängert werden sollte, betonten wir, dass es zumindest angebracht wäre, die Anwendung dieser Massnahme zeitlich zu begrenzen und nach einer bestimmten Zeitspanne ihre Wirksamkeit einer Beurteilung zu unterziehen.

1.3.5 Aktivitäten des EDÖB im Zusammenhang mit der Euro 08

Im Rahmen der Vorbereitungen der EURO 08 wurden wir von verschiedenen Seiten um Stellungnahmen gebeten. Nebst dem Bundesratsbeschluss zum Assistenzdienst der Armee sind dabei die Themenbereiche Akkreditierung und Trittbrettfahrermarketing zu erwähnen.

Im Sommer 2006 hat uns das Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) um Stellungnahme zum Entwurf für den Bundesratsbeschluss zum Assistenzdienst der Armee angefragt. In unserer Stellungnahme haben wir darauf hingewiesen, dass die Angaben zum Schutz des Luftraums sehr unpräzise seien und dass eine detailliertere Regelung erforderlich sei, wenn im Assistenzdienst Drohnen eingesetzt würden. Weil der Zweck des Einsatzes von Drohnen und Helikoptern mit Infrarot-Aufklärungssystem einzig darin besteht, den Einsatz von Sicherheits- und allenfalls Rettungskräften zu steuern, gibt es keine Notwendigkeit, die Bildinformationen zu speichern oder gar weiterzuleiten. Dementsprechend wird die Aufzeichnung der Informationen im Bundesratsbeschluss untersagt, was dem Grundsatz der Verhältnismässigkeit entspricht (vgl. auch Ziffer 1.2.2).

Ebenfalls im Sommer 2006 haben wir dem Staatssekretariat für Wirtschaft (SECO) unsere Bemerkungen zur damals aktuellen Revision des Bundesgesetzes gegen den unlauteren Wettbewerb (UWG) vorgelegt. Dabei ging es um neu zu schaffende Bestimmungen gegen das so genannte Schmarotzer- oder Trittbrettfahrer-Marketing. Für den Datenschutz war an der mittlerweile beerdigten Vorlage relevant, dass die mit dem Gesetz einzuführenden Datenflüsse in keiner Weise bestimmt waren. Vielmehr wollte man die verschiedenen am Vollzug beteiligten Stellen mittels allgemeiner Formulierungen zu einer Vielzahl von Datenbekanntgaben ermächtigen, ohne konkrete Angaben zu den Datenflüssen zu machen. Das Ganze wurde in einem Artikel formuliert, welcher den Randtitel „Amtshilfe in der Schweiz" hätte tragen sollen. Die Bestimmungen jedoch hätte dem Wesen der Amtshilfe grundlegend widersprochen, weil mit ihr nicht blosse Einzelfälle geregelt werden sollten, sondern die Gesamtheit der für den Vollzug erforderlichen Datenflüsse.

Im Herbst 2006 haben wir uns auf Anfrage des Bundesamtes für Polizei (fedpol) zu Sicherheitsüberprüfungen im Rahmen des Akkreditierungsverfahrens anlässlich der EURO 08 geäussert. Dabei ging es um die staatliche Mitwirkung an diesem Verfahren der UEFA in der Form, dass Bundesbehörden bestimmte staatliche Datenbanken abfragen und der UEFA für die betroffenen Personen Empfehlungen abgeben. Für die Abfrage waren folgende Datenbanken vorgesehen: Das informatisierte Staatsschutz-Informationssystem ISIS, das zu schaffende Hooliganismus-Informationssystem HOO-

GAN, das automatisierte Strafregister VOSTRA, das automatisierte Fahndungssystem RIPOL, das so genannte Schengener Informationssystem SIS sowie das zentrale Migrationsinformationssystem ZEMIS. Betreffend die Anzahl der vom Akkreditierungsverfahren Betroffenen ging man von etwa 25'000 Personen aus. Dabei handelt es sich in erster Linie um Mitarbeitende der UEFA und des Organisationskomitees EURO 08, Gäste der UEFA, Angehörige der Mannschaften und Begleitpersonen sowie um Medienschaffende und Mitarbeitende des Sicherheits- und Servicepersonals.

Zu prüfen war, ob die staatlichen Tätigkeiten – d.h. die Datenbankabfrage und die Bekanntgabe von Empfehlungen an die UEFA – in der Einwilligung der betroffenen Personen eine genügende Grundlage finden könnten.

Wir haben zunächst die Einwilligung im vorliegenden Zusammenhang als problematisch bezeichnet. Denn eine Einwilligung muss erstens freiwillig erfolgen und zweitens in Kenntnis aller wesentlichen Konsequenzen, welche sich daraus ergeben. Gerade die Freiwilligkeit dürfte aber bei der Akkreditierung von angestellten Personen nicht immer gegeben sein. Darüber hinaus droht diesen Personen der Nachteil, dass ihr Arbeitgeber sie im Falle eines negativen Bescheids nicht weiter beschäftigen will. Aus diesen Gründen und aufgrund der beträchtlichen Anzahl betroffener Personen haben wir in Übereinstimmung mit dem Bundesamt für Justiz gefolgert, dass für die beschriebene staatliche Mitwirkung im Akkreditierungsverfahren die Einwilligung der Betroffenen nicht genügt und somit eine besondere Rechtsgrundlage erforderlich ist. Diese muss auf der Stufe eines Gesetzes angesiedelt sein, weil die Abfrage der erwähnten Informationssysteme eine Bearbeitung von besonders schützenswerten Personendaten darstellt. Eine derartige Rechtsgrundlage für Datenbekanntgaben an Private besteht aber nur für den Fall des Informationssystems HOOGAN.

Neben diesen Stellungnahmen haben wir im Zusammenhang mit der EURO 08 unsere Kontakte betreffend die geplanten Datenbearbeitungen mit den verschiedenen an der Organisation dieser Veranstaltung Beteiligten fortgeführt. Zu erwähnen sind dabei die UEFA, das Bundesamt für Sport (BASPO) und fedpol.

1.3.6 Änderung der Verordnungen für den Datenaustausch mit Europol

Im Rahmen der Ämterkonsultation haben wir zur Inkraftsetzung von Art. 351^{novies} des Strafgesetzbuchs und zur Änderung der Verordnungen betreffend den Datenaustausch mit Europol Stellung genommen. Unseres Erachtens ist eine blosse Änderung der Verordnungen nicht ausreichend.

Im Rahmen der Ämterkonsultation hatten wir Gelegenheit zu einer Stellungnahme betreffend den Entwurf für eine Änderung verschiedener Verordnungen, die einer Anpassung bedürfen, um den Datenaustausch mit dem Europäischen Polizeiamt (wie im Europol-Abkommen vorgesehen) zu ermöglichen. Wir gaben zu bedenken, dass die formelle gesetzliche Grundlage, auf der alle betroffenen Datenbanken beruhen, zu allgemein sei (vgl. unseren 12. Tätigkeitsbericht 2004/2005, Ziffer 3.1.2). Laut DSG erfordert die Bearbeitung von besonders schützenswerten Daten sowie von Persönlichkeitsprofilen nämlich eine formelle gesetzliche Grundlage, in der zumindest die Zweckbestimmung der Bearbeitung und ihre Bedeutung genau umschrieben werden müssen. Wir haben darauf hingewiesen, dass eine blosse Änderung der Verordnungen über die betreffenden Datenbanken nicht ausreicht. Diese Bemerkung wurde nicht berücksichtigt, sie wurde aber im Bundesratsantrag als Divergenz aufgeführt. Den meisten unserer übrigen Bemerkungen wurde hingegen Rechnung getragen.

1.3.7 Gesetzesentwurf über die polizeilichen Informationssysteme

Der Entwurf für ein Gesetz über die Informationssysteme vereint die Rechtsgrundlagen für die bestehenden Polizeidatensammlungen wie RIPOL, IPAS und JANUS im selben Regelwerk. Er führt lediglich ein einziges neues Datenbearbeitungssystem ein: den nationalen Polizeiindex, ein Verzeichnis der bestehenden Datenbanken. Obwohl insgesamt unseren Bemerkungen Rechnung getragen worden ist, bedauern wir doch die Beibehaltung des Systems des so genannten „indirekten Auskunftsrechts". Dieses gestattet es einem Antragsteller nicht in Erfahrung zu bringen, ob Daten, die ihn betreffen, in den einem solchen System unterstellten Datensammlungen des Bundesamtes für Polizei enthalten sind, und gegebenenfalls Zugriff darauf zu bekommen.

Wir wurden seit 2003 im Rahmen der Ausarbeitung des Gesetzesentwurfs über die polizeilichen Informationssysteme wiederholt konsultiert und konnten so unsere Bemerkungen und Vorschläge einbringen. Dieser Entwurf verbessert die Transparenz im komplexen Bereich der polizeilichen Informationssysteme des Bundes, Systeme, auf die auch die Kantone immer mehr Zugriff erhalten. Die Transparenz ist auch ein wesentliches Element der Achtung des Rechts auf Datenschutz. Mit Ausnahme des nationalen Polizeiindexes, eines Verzeichnisses der bestehenden Datenbanken (vgl. dazu auch Ziffer 1.3.2), schafft der Entwurf keine neuen Datenbearbeitungssysteme. Er ermöglicht die Vereinigung der Rechtsgrundlagen für die bestehenden Datensammlungen, insbesondere RIPOL, IPAS und JANUS, in ein und demselben Regelwerk. Insgesamt wurde unseren Bemerkungen zwar Rechnung getragen, wir haben uns jedoch entschieden gegen die Beibehaltung des Systems des so genannten „indirekten Auskunftsrechts" ausgesprochen. Dieses System ist derzeit im Gesetz über die kriminalpolizeilichen Zentralstellen des Bundes (ZentG) und im Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) vorgesehen. Es lässt einem Antragsteller keine Möglichkeit zu erfahren, ob ihn betreffende Daten in den einem solchen Verfahren unterstellten Datensammlungen des Bundesamtes für Polizei enthalten sind, und gegebenenfalls Zugriff darauf zu bekommen. Das System des „indirekten Auskunftsrechts" befähigt ihn lediglich, ein Gesuch an uns zu richten, damit wir überprüfen, ob Daten, die ihn betreffen, vom Bundesamt für Polizei in den Informationssystemen ISIS, JANUS und GEWA rechtskonform bearbeitet werden. Wir erteilen dem Gesuchsteller eine immer gleich lautende Antwort, die besagt, dass keine ihn betreffende Daten rechtswidrig bearbeitet wurden, oder dass wir dem für die Bearbeitung Verantwortlichen empfohlen haben, einen bei der Datenbearbeitung begangenen Fehler zu be-

heben. Der Gesuchsteller erfährt ausser in seltenen Ausnahmefällen nie, ob er in den fraglichen Systemen registriert ist und welche ihn betreffenden Daten gegebenenfalls bearbeitet werden. Die Rechte des Betroffenen werden somit ausgeklammert, und unter diesen Bedingungen kann nicht von einem „indirekten Auskunftsrecht" gesprochen werden. Es handelt sich lediglich um ein Recht, bei einer Kontrollbehörde die Überprüfung der Rechtmässigkeit der Bearbeitung zu beantragen. Dieses System ist unter dem Gesichtspunkt des Datenschutzes unbefriedigend. Einerseits haben unsere Überprüfungen nur eine begrenzte Tragweite, und eine Information der Betroffenen gibt es praktisch nicht. Andererseits ist die heutige Praxis nicht in Übereinstimmung mit Artikel 13 der Bundesverfassung und mit den Artikeln 8 und 13 der Europäischen Menschenrechtskonvention, welche den Schutz der Privatsphäre garantieren (vgl. zu diesem Thema auch Ziffer 1.3.3). Abgesehen von dieser erheblichen Divergenz kritisierten wir auch die Tatsache, dass eine nachträgliche Information der Betroffenen nur dann vorgesehen ist, wenn die Daten direkt (und ohne ihr Wissen) von der Bundeskriminalpolizei erhoben worden sind (vgl. Ziffer 1.3.8). Wir äusserten auch Zweifel betreffend den Online-Zugriff der eidgenössischen Spielbankenkommission auf das automatisierte Polizeifahndungssystem und denjenigen der Meldestelle für Geldwäscherei auf das Staatsschutz-Informations-System (ISIS). Schliesslich sprachen wir uns auch gegen die Angabe des Grundes für die erkennungsdienstliche Behandlung einer Person im nationalen Polizeiindex sowie gegen die Benennung des Informationssystems oder des Systemtyps aus, aus denen die Daten stammen.

1.3.8 Kontrollen im Bereich der nachträglichen Information der betroffenen Personen

Das EJPD hat im Zusammenhang mit der nachträglichen Information der betroffenen Personen den Entscheid getroffen, dass Art. 14 Abs. 1 ZentG nur dann anwendbar sei, wenn das Bundesamt für Polizei selber Daten beschafft hat, ohne dass es für die betroffene Person erkennbar war.

Im Zusammenhang mit der nachträglichen Information der betroffenen Personen im Polizeibereich und unseren entsprechenden Empfehlungen haben wir die Angelegenheit dem Eidgenössischen Justiz- und Polizeidepartement (EJPD) zum Entscheid vorgelegt (vgl. unseren 13. Tätigkeitsbericht 2005/2006, Ziff. 3.1.4). Dabei geht es um die Auslegung von Art. 14 Abs. 1 des Bundesgesetzes über kriminalpolizeiliche Zentralstellen des Bundes (ZentG) und des dafür vom Bundesamt für Polizei (fedpol) entworfenen Konzepts für die Informationssysteme JANUS und GEWA. Hauptdivergenz war Test 4 des Konzepts. Es besagt, Art. 14 Abs. 1 ZentG sei nur dann anwendbar, wenn die Datenbeschaffung originär, das heisst direkt durch fedpol resp. durch die Bundeskriminalpolizei (BKP) und nicht durch eine andere Behörde, erfolgt sei. Wir hatten uns auf den Standpunkt gestellt, dass die Voraussetzungen von Art. 14 Abs. 1 ZentG auch bei einer nicht originären Datenbeschaffung zu prüfen seien. Das EJPD hielt am erwähnten Test 4 fest mit der Begründung, keine Gesetzesbestimmung verpflichte zur nachträglichen Information der betroffenen Personen bei Daten, die nicht direkt von fedpol beschafft worden seien. Daher müsse man aufgrund von Indizien entscheiden, ob diese These begründet sei oder nicht. Folglich bleibt gemäss EJPD Art. 14 Abs. 1 ZentG nur im Falle der originären Datenbeschaffung anwendbar. Für das Informationssystem GEWA führt dies dazu, dass Art. 14 Abs. 1 ZentG gar keine Anwendung findet, da hier überhaupt keine originäre Datenbeschaffung durch fedpol erfolgt. Weiter sprach sich das EJPD darüber aus, dass fedpol darum besorgt sein müsse, die Gesetze in den nächsten Revisionen entsprechend anpassen zu lassen.

1.3.9 Datenschutz im Rahmen der Schengen-Evaluation

Der Datenschutz ist ein wichtiges Element der von den europäischen Sachverständigen im Rahmen von Schengen durchgeführten Evaluation. Diese beruht auf einem Fragebogen und auf örtlichen Inspektionen und betrifft die eidgenössische und die kantonalen Datenschutzbehörden.

Die Anwendung des Schengener Abkommens ist von einem Ratsbeschluss der Europäischen Union abhängig. Dieser muss von den Staaten, die Schengen anwenden, nach einer Beurteilung der Fähigkeit der Schweiz zur Umsetzung dieses Abkommens einstimmig gefasst werden. Mit der Evaluation sind Teams bestehend aus Sachverständigen des europäischen Rates, der europäischen Kommission und der Mitgliedstaaten betraut. Ihr Zweck ist nicht in erster Linie, Sanktionen auszusprechen, sondern den neuen Staaten zu helfen, ihre Institutionen mit den Abkommen und dem Besitzstand von Schengen in Einklang zu bringen. Die Beurteilung ermöglicht auch einen Vergleich und eine Verbesserung der einzelstaatlichen Praktiken. Sie erstreckt sich zunächst auf die Polizeizusammenarbeit, den Datenschutz, die Kontrolle an den Aussengrenzen, die Visa, die konsularische Zusammenarbeit, und danach auf das Schengener Infomformationssystem (SIS) – wenn dieses einmal operationell ist. Die Evaluation beruht auf einem Fragebogen und auf örtlichen Inspektionen. Spätere Evaluationen werden auch in den Ländern erfolgen, die bereits Mitglieder von Schengen sind.

Die Evaluation des Datenschutzes bezieht sich auf die Bestimmungen des Abkommens betreffend den Datenschutz und insbesondere auf die Kontrollbehörde. Sie umfasst einen an die eidgenössische und an die kantonalen Kontrollbehörden gerichteten Fragebogen und danach einen Besuch bei diesen Behörden. Die für diese Behörden geltenden Rechtsgrundlagen werden analysiert; es werden namentlich ihre Unabhängigkeit, ihre Kompetenzen im Bereich Untersuchungen und Sanktionen sowie ihre Rolle als Aufsichtsorgan, insbesondere bei der Kontrolle des SIS und der darin einbezogenen Dienste, geprüft. Die Rechte der betroffenen Personen und die Datensicherheit sind ebenfalls Bestandteil der Evaluation. Das Interesse der Experten gilt auch den Kontakten, welche die Kontrollbehörden mit den ausländischen Behörden im Rahmen der internationalen Zusammenarbeit pflegen, sowie den Beziehungen zur Öffentlichkeit. Eine besondere Bedeutung wird der Existenz einer Sensibilisierungspolitik und von Verhaltensrichtlinien für die betroffenen Personen beigemessen.

1.3.10 Rückübernahmeabkommen

Das Bundesamt für Migration ist mit der Ausarbeitung zahlreicher Rückübernahmeabkommen beschäftigt, in denen Datenschutznormen eingeführt werden. Da diese unterschiedlich ausgestaltet werden können, wendet sich das Bundesamt zwecks Stellungnahme an uns.

Wir wurden in den letzten fünf Jahren in zahlreichen Fällen zu Rückübernahme- und Transitabkommen konsultiert. Diese Abkommen sind einerseits mit Staaten abgeschlossen worden, die über eine angemessene Gesetzgebung über den Datenschutz verfügen, wie etwa die Staaten der Europäischen Union und Staaten, die das Übereinkommen 108 des Europarates ratifiziert haben, und andererseits mit Staaten, die keine ausreichende Gesetzgebung haben, wie die afrikanischen und asiatischen Staaten. Die wichtigsten Probleme betrafen die Bekanntgabe von besonders schützenswerten Daten im Zusammenhang mit administrativen oder strafrechtlichen Verfahren oder Massnahmen. Diese Probleme sind in unserem 10. Tätigkeitsbericht 2002/2003 (Ziffer 3.2.2) ausführlich erläutert.

1.4 Gesundheit

1.4.1 Vorentwurf zu einer Verfassungsbestimmung und einem Bundesgesetz über die Forschung am Menschen

Wir begrüssen die Schaffung einer Verfassungsbestimmung und eines Bundesgesetzes über die Forschung am Menschen. Der Vorentwurf statuiert als Grundsatz für jede Forschungstätigkeit die Einwilligung der betroffenen Person nach hinreichender Aufklärung. Wir haben bezüglich des Aufklärungsinhalts einige Anpassungen gefordert, welche für die betroffenen Personen die Transparenz der Datenbearbeitung erhöhen sollen. Ferner haben wir unsere Bedenken bezüglich der geplanten Abschaffung der Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung ausgedrückt und die Beschneidung unserer Aufsichts- und Beschwerdebefugnis kritisiert.

Im Rahmen des Vernehmlassungsverfahrens haben wir zum Vorentwurf zu einer Verfassungsbestimmung und einem Bundesgesetz über die Forschung am Menschen (HFG) Stellung genommen. Die Bestimmungen regeln in umfassender Weise das gesamte Gebiet der Forschung am Menschen im Gesundheitsbereich.

Wir haben es sehr begrüsst, dass nebst den Richtlinien der Schweizerischen Akademie der medizinischen Wissenschaften (SAMW) nun eine gesamtschweizerische Reglementierung zur Forschung am Menschen und insbesondere zum Umgang mit Personendaten und biologischen Materialien in Angriff genommen wurde. Diese für die Persönlichkeitsrechte der Datenspenderinnen und -spender äusserst wichtige Thematik bedarf klarer verfassungsrechtlicher und gesetzlicher Regelungen, welche die datenschutzrechtlichen Aspekte berücksichtigen und ernst nehmen. Als Schlüsselprinzip der Bearbeitung von Personendaten und biologischen Materialien gilt dabei der so genannte „informed consent", also die freie Zustimmung nach hinreichender Aufklärung. Demnach sind Einwilligung und Aufklärung unabdingbare Voraussetzungen für jegliche Forschungstätigkeit.

Vorweg haben wir angeregt, im Zweckartikel des Gesetzesentwurfes den Persönlichkeitsschutz stärker zu betonen; dies in Anlehnung an den neu formulierten verfassungsrechtlichen Auftrag, unter Beachtung der Forschungsfreiheit für den Schutz der Menschenwürde und Persönlichkeit zu sorgen. Ausgangspunkt einer gesetzlichen Regelung der Forschung am Menschen muss die Wahrung der Rechte der Probanden und Spender sein. Angesichts der Sensibilität der Forschungsdaten, welche grösstenteils besonders schützenswerte Personendaten im Sinne des DSG darstellen, hätten wir es zudem begrüsst, wenn bei der Ausarbeitung des HFG spezifischere Datenschutzbestimmungen in den Gesetzestext eingeflossen wären. Der im Vorentwurf enthaltene generelle Verweis auf das DSG erschien uns zu pauschal und ohne Konturen.

Das HFG erklärt die Einwilligung nach hinreichender Aufklärung und angemessener Bedenkzeit bei der medizinischen Forschung zum Grundprinzip. Somit darf grundsätzlich ohne Einwilligung des Betroffenen keine medizinische Forschung mit seinen Daten oder biologischen Materialien betrieben werden. Diesen Grundsatz haben wir sehr begrüsst, trägt er doch dem Erfordernis der Transparenz und der Rechtfertigung der Datenbearbeitung Rechnung. Abgelehnt haben wir in diesem Zusammenhang die im HFG vorgesehene Möglichkeit einer irreführenden Aufklärung für Forschungsprojekte, bei denen dies aus methodischen Gründen zwingend wäre. Eine irreführende Aufklärung widerspricht dem Grundsatz des informed consent fundamental und ist daher keinesfalls zulässig. Des Weiteren haben wir angeregt, dass die Aufklärung immer auch das Widerspruchsrecht und das jederzeitige Widerrufsrecht umfassen muss. Sofern die betroffene Person von ihrem Widerrufsrecht Gebrauch macht, haben wir gefordert, dass die bereits erhobenen Personendaten entweder anonymisiert oder gelöscht und die biologischen Materialien vernichtet werden.

Das HFG sieht vor, dass biologische Proben und Personendaten zu Forschungszwecken auch ins Ausland ausgeführt werden dürfen. Da diese Ausfuhr mit einem erhöhten Risiko für Persönlichkeitsverletzungen der Spenderinnen und Spender einhergeht, haben wir es begrüsst, dass die Proben und Daten ausschliesslich in pseudonymisierter oder anonymisierter Form transferiert werden dürfen. Zudem haben wir gefordert, dass bei einer Ausfuhr ins Ausland zwingend entsprechende Vernichtungs- und Rückgaberegelungen für die Proben und Daten vorgesehen werden. Zur Erhöhung der Transparenz haben wir angeregt, dass die betroffenen Personen bei der Aufklärung bereits auf die Möglichkeit des Daten- und Probentransfers ins Ausland und das entsprechende Widerspruchsrecht aufmerksam gemacht werden. Ebenso müssen Personen, die an einem Forschungsprojekt teilnehmen, über allfällige gesetzliche Offenlegungs- und Mitteilungspflichten der Forschungsresultate ausserhalb des Forschungskontexts (bspw. an Versicherungen) sowie über gesetzliche Zugriffsrechte Dritter aufmerksam gemacht werden. Nur so erhält die betroffene Person umfassende Transparenz darüber, was mit ihren Daten und Proben geschieht.

Schliesslich bedauern wir die im HFG geplante Abschaffung der Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung. Dieses gestützt auf Art. 321bis StGB und Art. 32 DSG eingeführte Gremium erfüllt heute eine wichtige Aufgabe zur Gewährleistung der Einhaltung des Datenschutzes in der medizinischen Forschung. Es entscheidet über die Aufhebung des Arztgeheimnisses, wenn die Zustimmung der betroffenen Personen nicht (mehr) eingeholt werden kann, sowie über die Bedingungen und Auflagen bei der Weiterleitung der Daten an Dritte. Gemäss dem Vorentwurf soll diese Aufgabe nun von den zuständigen Ethikkommissionen übernommen werden. Wir haben ernsthafte Bedenken dazu geäussert, denn es ist fraglich, ob die datenschutzrechtlichen Aspekte mit der Abschaffung der Expertenkommission ausreichend berücksichtigt werden. Die Aufgaben der Ethikkommissionen sind nämlich anders gelagert und umfassen primär die Bewilligung und inhaltliche Beurteilung von Forschungsprojekten. Das HFG trägt diesem Umstand aus unserer Sicht zu wenig Rechnung. Insbesondere werden im HFG nicht alle Voraussetzungen übernommen, welche gemäss Art. 321bis StGB und gemäss der Verordnung über die Offenbarung des Berufsgeheimnisses (VOBG) für die Erteilung einer Forschungsbewilligung vorliegen müssen. Einhergehend mit der Abschaffung der Expertenkommission für das Berufsgeheimnis werden auch die bestehenden Aufsichts- und Beschwerdekompetenzen des EDÖB in der medizinischen Forschung beschnitten. Wir haben hier gefordert, dass gewisse dieser Kompetenzen (Aufsicht über die Einhaltung von Datenschutzauflagen und die Aufklärung der Patientinnen und Patienten durch die Ärzteschaft; Beschwerderecht gegen Entscheide der Ethikkommissionen, die den Datenschutz betreffen) in der medizinischen Forschung aufrecht erhalten bleiben und die materiellen Bestimmungen des HFG entsprechend geändert werden.

1.4.2 Bearbeitung von medizinischen Daten im Auftragsverhältnis

Der auch informatikseitig immer komplexer werdende Spitalalltag führt zu neuen Fragestellungen, etwa mit Blick auf die speicherintensiven Daten bildgebender Systeme. Infolge einer Anfrage aus der Privatwirtschaft haben wir die rechtlichen Rahmenbedingungen der Auslagerung medizinischer Daten durch Privatspitäler an Dritte zum Zweck der Datensicherung und der Fernwartung reflektiert.

Zahlreiche Spitäler nehmen beim Umgang mit den im Spitalalltag anfallenden Daten Unterstützung aus der Privatwirtschaft in Anspruch. Erstmals ist in diesem Berichtsjahr ein Unternehmen mit der Frage an uns herangetreten, ob Patientendaten ausserhalb der Spitalräumlichkeiten – namentlich auch im Ausland – bearbeitet werden dürften.

In diesem Zusammenhang gilt es vor allem festzuhalten, dass eine Übertragung der Patientendatenbearbeitung an Dritte infolge des strafrechtlich relevanten Berufsgeheimnisses des Arztes grundsätzlich nur bei vorliegender Einwilligung sämtlicher betroffenen Personen zulässig ist. Will man bei einem Outsourcing ausnahmsweise ohne Einwilligungserklärungen vorgehen, muss mittels technisch-organisatorischer Massnahmen sichergestellt werden, dass die beauftragten Dritten keinen Zugriff auf medizinische Daten erhalten. In der Praxis der Patientendatenbearbeitung zeigt sich, dass dies bei der Datenarchivierung und insbesondere bei der Fernwartung eine anspruchsvolle Aufgabe ist. Wird sie nicht umfassend gelöst, ist ein Outsourcing im Bereich der Patientendaten weder strafrechts- noch datenschutzkonform.

Sollen Daten ausserdem gar ins Ausland transferiert werden, ist zu prüfen, ob im Empfängerland ein gleichwertiger Datenschutz gegeben ist. Sollte dies nicht der Fall sein, sind entsprechende Vorsichtsmassnahmen erforderlich (näheres unter www.edoeb.admin.ch, Themen – Datenschutz – Übermittlung ins Ausland). Überdies stünden wir einer Bearbeitung von Patientendaten auf dem Hoheitsgebiet der USA angesichts der jüngeren amerikanischen Rechtsentwicklung tendenziell skeptisch gegenüber. Auf eine Prüfung, ob und wie ein unerwünschter Zugriff auf schweizerische Patientendaten auf der Grundlage der Anti-Terrorgesetzgebung verhindert werden kann, dürfte bei einem solchen Projekt nicht verzichtet werden; allein die Berufung auf das Safeharbour-Prinzip vermag an diesem Ergebnis nichts zu ändern.

1.4.3 Bekanntgabe von Diagnosedaten (DRG) an die Versicherer durch die Spitäler

Mit Hilfe von Codierungen können umfangreiche Informationen in kürzester Form dargestellt werden. Diagnosen sind solche Informationen. Durch die Diagnosis Related Groups (DRG) werden Diagnosen nach Fallgruppen codiert. Die Anwendung der DRG war Anlass für einige Anfragen an uns. Zur Zeit besteht keine genügende rechtliche Grundlage für die systematische Weitergabe detaillierter medizinischer Daten durch Leistungserbringer an Versicherer.

Für die Abgeltung der Aufenthalte im stationären akutsomatischen Bereich soll in Zukunft eine diagnosebezogene Fallkostenpauschale angewendet werden. Zu diesem Zweck wird in einer ersten Phase eine nationale Datenbank aufgebaut. In einer zweiten Phase werden Leistungen der Spitäler anhand der errechneten Fallkostenpauschale durch die Versicherer vergütet. In beiden Phasen sind detaillierte Diagnosen erforderlich.

Die datenschutzrechtlichen Anforderungen unterscheiden sich je nach Phase. Der Aufbau der Datenbank muss zwingend mit anonymisierten Daten erfolgen. In der zweiten Phase, also der eigentlichen Anwendung der DRG, sind die Daten personenbezogen. Es handelt sich um eine systematische Weitergabe sehr detaillierter medizinischer Daten vom Leistungserbringer an den Versicherer. Dies ist nach der geltenden gesetzlichen Regelung nicht zulässig. Wenn die diagnosebezogene Fallkostenpauschale in Zukunft als Grundlage für die Leistungsabrechnung angewendet werden soll, müssen zuerst die gesetzlichen Grundlagen erarbeitet werden.

1.4.4 Datenschutz in der Arztpraxis

Eine moderne Arztpraxis erfordert einen praktischen und wirksamen Schutz der Informatikinfrastruktur und vor allem der Patientendaten. Anfragen an uns und Reaktionen von Ärztinnen und Ärzten während Referaten zum Datenschutz im Gesundheitswesen lassen eine gewisse Verunsicherung bezüglich sinnvoller Massnahmen erkennen. Darum haben wir uns entschieden, einen Katalog für minimale Schutzmassnahmen zu veröffentlichen.

Vereinfacht kann eine Arztpraxis in vier Bereiche aufgeteilt werden:

Der erste Bereich ist der Server mit den zentralen Funktionen und Patientendaten. Hier gilt es, einerseits jeden ungewollten Zugriff auf das System durch einen wirksamen Passwortschutz zu verhindern, und andererseits, Datenverlusten durch gute Backupstrategien vorzubeugen.

Der zweite Bereich umfasst die gesamte Praxisinfrastruktur. Die Geräte sind mehrheitlich durch ein Netzwerk miteinander verbunden. Hier muss darauf geachtet werden, dass nicht überflüssige und in der Folge unkontrollierte Geräte mit dem Netz verbunden sind. Die peripheren Geräte müssen so konfiguriert sein, dass ein Fremdzugriff nicht möglich ist, und so aufgestellt werden, dass ein Einblick, z.B. über den Bildschirm, für Unbefugte verhindert wird.

Der nächste Bereich ist das private Büro des Arztes, z.B. zu Hause. Die Übertragung von Patientendaten über das Internet muss auf jeden Fall verschlüsselt erfolgen. Besser ist es, die benötigten Daten vorher in der Praxis auf den Laptop zu kopieren und zu verschlüsseln.

Den vierten Bereich bilden die öffentlichen Netze, insbesondere das Internet. Grundsätzlich müssen die Praxissysteme von den öffentlichen Netzen getrennt sein. Sowohl die Wartungsarbeiten an den Praxissystemen als auch der Zugriff von der Praxisinfrastruktur auf das Internet müssen kontrolliert erfolgen. Das bedeutet, dass alle Aktivitäten zwischen Praxis und den öffentlichen Netzen über eine Firewall geschützt werden müssen. Besonders sollten keine Dateien vom Internet auf die Praxissysteme herunter geladen werden. Die Fernwartung sollte nicht über das Internet, sondern über dedizierte Fernwartungsmodems erfolgen.

Trotz allen technischen Massnahmen dürfen grundsätzliche Voraussetzungen nicht vergessen werden: Der Umgang mit den Patientendaten soll nur wenn erforderlich und immer mit der nötigen Umsicht erfolgen. Und der Arzt muss jederzeit Kenntnis über den aktuellen Zustand seiner Praxisinformatik haben.

Ausführlichere Anforderungen sind auf unserer Homepage und auf einer CD der Schweizerischen Gesellschaft für Allgemeinmedizin (www.sgam.ch/informatics) zu finden.

1.4.5 Aufsicht über die Umsetzung der Auflagen der Expertenkommission im Bereich der medizinischen Forschung

In der medizinischen Forschung wird häufig der Begriff „anonymisierte Daten" verwendet. In den meisten Fällen handelt es sich dabei jedoch um pseudonymisierte Daten. Bei anonymisierten Daten ist es unmöglich oder unverhältnismässig schwierig, die jeweilige Person zu identifizieren. Im Gegensatz dazu ist bei pseudonymisierten Daten eine Identifikation möglich. Im Übrigen mussten wir auch in diesem Jahr feststellen, dass weitere Kontrollen im Bereich der medizinischen Forschung erforderlich sind.

Im Bereich der medizinischen Forschung mussten wir feststellen, dass der Begriff „anonymisierte Daten" nicht immer richtig angewendet wird. In vielen Fällen werden bei den Forschungsprojekten pseudonymisierte Daten verwendet. Von Pseudonymisierung spricht man, wenn die identifizierenden Daten von den restlichen Daten getrennt werden. Die Zuordnung der beiden Datenbereiche erfolgt beispielsweise durch eine bestimmte Nummer, die sowohl bei den identifizierenden als auch bei den restlichen Daten vorhanden sein muss. Somit ist eine Zusammenführung der beiden Datenteile wieder möglich (Depseudonymisierung). Es gibt Forschungsvorhaben, bei denen man zum Beispiel im Verlauf der Forschungsprojektes feststellt, dass man noch auf weitere Informationen angewiesen ist. In einem solchen Fall besteht bei pseudonymisierten Daten die Möglichkeit, die Identität der Person festzustellen, damit die zusätzlichen Informationen erhoben werden können. Dabei ist darauf zu achten, dass die Depseudonymisierung messbar (also nachvollziehbar) zu gestalten ist. Es darf nicht sein, dass der Forschende selbständig eine Depseudonymisierung vornehmen kann (Funktionstrennung). Im Gegensatz dazu sind Daten anonymisiert, wenn sie nur mit einem unverhältnismässig grossen Aufwand an Arbeit, Zeit und Kosten einer bestimmten oder bestimmbaren Person zugeordnet werden können.

Auch in diesem Jahr haben wir im Bereich der medizinischen Forschung Kontrollen durchgeführt, um festzustellen, wie die Auflagen der Expertenkommission umgesetzt werden (vgl. auch unseren 13. Tätigkeitsbericht 2005/2006, Ziffer 4.1.2). In den meisten Fällen war der räumliche Zugang zu den Informationssystemen gut abgesichert, so dass wir diesbezüglich keine Beanstandungen machen mussten. In einem Fall mussten wir allerdings darauf hinweisen, dass eine saubere Trennung zwischen den aktuellen und den archivierten Projektdaten vollzogen werden muss und dass ein Zugriff auf nicht anonymisierte Archivdaten entsprechend messbar zu gestalten ist. Im Weiteren konnten wir bei einem Spital feststellen, dass die Forschungsprojekte insbesondere mit Hilfe der Daten, die sich im zentralen Papierarchiv befinden, durchgeführt werden. Es konnte uns aber nicht mitgeteilt werden, ob auch aufgrund elektronischer Datensammlungen Forschungsvorhaben durchgeführt werden können, weil die entsprechenden Angaben nicht vorlagen. Leider mangelt es in diesem Umfeld an Transparenz, so dass eine befriedigende Umsetzung des Datenschutzes wohl kaum möglich ist.

Wir werden auch weiterhin Kontrollen im Bereich der medizinischen Forschung vornehmen.

1.5 Versicherungen

1.5.1 Datenschutzrechtliche Aspekte der Einführung einer Versichertenkarte

Die Erarbeitung der technischen Grundlagen und der Verordnungsentwurf sind die grossen Etappen des Projekts Versichertenkarte in der vergangenen Periode. Die Einführung der Versichertenkarte ist für unser Gesundheitswesen ein fundamentales Ereignis. Deshalb ist es auch von zentraler Bedeutung, dass die grundsätzlichen Anforderungen des Datenschutzes strikt eingehalten werden. Fehler in der Anfangsphase auf dem Weg zur Gesundheitskarte sind später nur mit einem hohen organisatorischen und finanziellen Aufwand zu beheben.

In der Erklärung zum Verordnungsentwurf zur Versichertenkarte erwähnt das Bundesamt für Gesundheit (BAG), dass der Art. 42a Abs. 4 des Bundesgesetzes über die Krankenversicherung (KVG) als ein erster Schritt hin zu einer Gesundheitskarte angelegt ist. Dieser erste Schritt bringt mit sich, dass neben rein administrativen Daten auch Daten mit medizinischer Aussagekraft über die versicherte Person auf der Karte gespeichert sein sollen (vgl. dazu unseren 13. Tätigkeitsbericht 2005/2006, Ziffer 5.1.1). Das Einverständnis des Versicherten bildet die dafür zwingende Voraussetzung; so lautet die Forderung des Gesetzgebers. Damit der Versicherte sein Einverständnis geben kann, ist er auf eine klare, verständliche und umfassende Information über die Bearbeitung seiner Daten angewiesen.

Im Verordnungsentwurf wird der Umfang der Daten abschliessend aufgezählt: Blutgruppen- und Transfusionsdaten; Immunisierungsdaten; Transplantationsdaten; Allergien; Krankheiten und Unfallfolgen; in medizinisch begründeten Fällen ein zusätzlicher Eintrag; Medikation; eine oder mehrere Kontaktadressen für den Notfall und Hinweise auf bestehende Patientenverfügungen. Diese Daten sollen zur Verbesserung der Effizienz, der Sicherheit und der Qualität der medizinischen Behandlung auf der Versichertenkarte abgespeichert werden.

Zugriff auf diese Daten haben Ärzte, Apotheker, Zahnärzte, Chiropraktiker, Hebammen, Physiotherapeuten, Ergotherapeuten, Pflegefachpersonal, Logopäden und Ernährungsberater. Die Speicherung und der Zugriff erfolgen nur mit dem Einverständnis der versicherten Person. Die Aufklärung des Patienten erfolgt, so sieht es der Verordnungsentwurf vor, durch die oben aufgezählten Leistungserbringer.

Diese Erweiterung von einer administrativen Karte für die Rechnungsstellung der Leistungen nach dem KVG zu einer Karte mit Gesundheitsdaten hat nicht zuletzt Folgen für die Persönlichkeitsrechte der Versicherten und muss daher datenschutzkonform gestaltet werden.

Es muss erstens sichergestellt sein, dass die Daten für den vom Gesetzgeber vorgesehen Zweck geeignet sind. Die uns vorliegenden Stellungnahmen von Leistungserbringern lassen indessen bislang auch bei einer grosszügigen Interpretation nicht erkennen, dass dem so ist. Das Gegenteil ist der Fall. Einige Daten, wie z.B. die Blutgruppen- und Transfusionsdaten, würden gemäss Ärztevereinigung FMH dem Patienten allenfalls höchstens ein Sicherheitsgefühl vermitteln. Die Angaben zu Krankheiten und zur Medikation ihrerseits sind besonders problematisch, denn es gibt keine Garantie dafür, dass sie tatsächlich immer vollständig und aktuell sind. Auch von Seiten des Schweizer Spitalverbands H+ gibt es keine klare Aussage zur Zweckmässigkeit der Gesundheitsdaten auf der Versichertenkarte. Er erachtet die Vermischung von Versicherungs- und Gesundheitskarte als unglücklich.

Zweitens muss sichergestellt sein, dass sich der Patient über die Konsequenzen seiner Einwilligung oder Nichteinwilligung im Klaren ist und er daher entsprechend informiert wird. Da die Daten über heikle und intime Ereignisse und Zustände des Patienten Auskunft geben können, muss die Information besonders umfassend und verständlich sein. Der Patient muss wissen, wer seine Angaben zu welchem Zweck nutzen wird. Nur so kann er zwischen Vor- und Nachteilen seiner Einwilligung abwägen. Es stellt sich indessen die Frage, wer ihm diese Information geben soll. Der grösste Teil der Leistungserbringer bzw. ihrer Vertreter verneinen die Zweckmässigkeit der Speicherung medizinischer Daten auf der Karte. Sie könnten demnach nur unter Vortäuschung eines Zwecks eine Einwilligung des Patienten herbeiführen. Das kann aber nicht das Ziel der Versichertenkarte sein.

Und schliesslich müssen die Rahmenbedingungen für die Bearbeitung der Gesundheitsdaten erfüllt sein. Es ist nur ungenügend oder gar nicht geregelt, was genau mit diesen Daten in der praktischen Anwendung geschieht und wer welche Verantwortungen für die einzelnen Angaben trägt. Gemäss Kommentar zum Verordnungsentwurf kann die versicherte Person aus der Liste die Datenkategorien auswählen, die sie auf der Versichertenkarte abspeichern lassen will. Offen bleibt aber, ob der Wunsch des Patienten verbunden mit der Einwilligung des Leistungserbringers oder aber umgekehrt der Vorschlag des Leistungserbringers verbunden mit dem Einverständnis des Patienten dafür ausschlaggebend ist, welche medizinischen Daten auf der Karte gespeichert werden.

Wenn einer dieser drei Punkte nicht erfüllt ist, bestehen grosse Zweifel an der Rechtmässigkeit der Versichertenkarte im vorgesehenen Umfang.

Viele datenschutzrechtlich relevanten Fragen sind also noch nicht geregelt. Bei den Leistungserbringern fehlt die Akzeptanz für die Bearbeitung der Gesundheitsdaten. Deshalb haben wir sowohl in der Fachgruppe zur Erarbeitung der technischen Standards als auch in Stellungnahmen zum Verordnungsentwurf vom BAG gefordert, auf die Speicherung medizinischer Daten zu verzichten. Das Risiko ist zu gross, dass Patienten einer Bearbeitung ihrer Gesundheitsdaten ausdrücklich zustimmen, ohne über den Zweck der Bearbeitung genügend informiert zu sein.

1.5.2 Transparenz der Datenbearbeitung im Verfahren der Unfallversicherung

Wir haben uns zur ersten Etappe der Revision des Unfallversicherungsgesetzes vernehmen lassen. Aus Sicht des Datenschutzes ist zu fordern, dass sich im Unfallversicherungsbereich die Transparenz der Datenbearbeitung nicht verschlechtert. Dies wäre der Fall, würde die Informationsbeschaffung durch die Unfallversicherung künftig ohne Ermächtigung der verunfallten Person geschehen.

Im Jahr 2003 trat das Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts in Kraft (ATSG). In Rahmen dieses Erlasses wurde für den gesamten Bereich der Sozialversicherungen zur Regel erhoben, dass Versicherte, die vom Sozialversicherer Leistungen beziehen wollen, diesen zur Informationsbeschaffung ermächtigen müssen (Artikel 28 Absatz 3 ATSG). Der Revisionsentwurf des Bundesgesetzes über die Unfallversicherung (UVG) sieht nun vor, diese Regel im Unfallversicherungsbereich künftig nicht mehr anzuwenden. Wir haben uns im Rahmen der Vernehmlassung dafür eingesetzt, dass dieses Vorhaben nicht umgesetzt wird.

Die im ATSG vorausgesetzte Ermächtigung zur Informationsbeschaffung ist von einiger Bedeutung. Wird sie nicht erteilt, kann die mangelnde Bereitschaft zur Mitwirkung für den Versicherten unangenehme Folgen haben. Gleichzeitig haben die Versicherten vom Erfordernis der Ermächtigungserklärung aber auch einen Gewinn: Bei ihrer Erteilung erhalten sie über den Umstand der Informationsbeschaffung und deren Adressaten gesicherte Kenntnisse; nur so wird für die betroffene Person die Datenbearbeitung des Sozialversicherers einigermassen transparent.

Auch wenn einzuräumen ist, dass die Unfallversicherer für die Abwicklung ihrer Versicherungsfälle ein vergleichsweise grosses Informationsbedürfnis haben, sollte am bisherigen System der Ermächtigungserklärung festgehalten werden. Der Anspruch auf transparente Datenbearbeitung darf ohne zwingenden Grund nicht geschmälert werden.

1.6 Arbeitsbereich

1.6.1 Datenschutzkontrolle bei der Firma ALDI SUISSE AG

Im Verlauf des Jahres 2006 haben wir eine Filiale der Firma ALDI SUISSE AG einer eingehenden Datenschutzkontrolle unterzogen. Hauptaugenmerk galt dem Bereich der Videoüberwachung im Detailhandel. Der Hauptzweck der Überwachung – Schutz gegen Diebstahl und Überfall – wurde dem Verhältnis und der Intensität des Eingriffs in die Persönlichkeitsrechte gegenüberstellt. Nach differenzierter Gesamtbeurteilung mussten aus datenschutzrechtlicher Sicht diverse Anpassungen empfohlen werden. Nebst diversen Verbesserungen und Verfeinerungen hat ALDI insbesondere die Kameras im Kassenbereich so zu fokussieren, dass Aufnahmen von Mitarbeitenden nicht mehr möglich sind. Zudem hat sich ALDI verpflichtet, bis spätestens Ende 2008 in der Videoüberwachung datenschutzfreundliche Technologien (Privacy-Filter) einzusetzen.

In der Konsumwelt herrscht ein reges Interesse, das Auftreten und Verhalten der Kundschaft im wahrsten Sinne des Wortes zu durchleuchten. Nachdem wir 2005 als Datenaufsichtsbehörde im Rahmen einer Kontrolle bei Migros und Coop geprüft haben, ob die Datenbearbeitung bezüglich M-CUMULUS resp. Supercard datenschutzkonform erfolgt (s. unseren 13. Tätigkeitsbericht 2005/2006, Ziffern 7.1 und 7.2), unterzogen wir 2006 die Firma ALDI SUISSE AG einer Kontrolle der Videoüberwachungsanlage.

ALDI hat in der letzten Zeit mehrere Verkaufsfilialen in der Schweiz eröffnet. Wie alle Detailhändler sieht sich auch ALDI mit dem Problemkreis von Überfall und Diebstahl konfrontiert. Zu deren Bekämpfung dient – nebst verschiedenen baulichen und organisatorischen Vorkehrungen – auch der Einsatz eines Videoüberwachungssystems. Die Filialen von ALDI sind standardisiert aufgebaut. Wo Videoüberwachungssysteme betrieben werden, tangieren diese eine Vielzahl von Personen (Mitarbeitende, Lieferanten, Kundinnen und Kunden). Die Durchführung unserer Kontrolle erfolgte insbesondere im Hinblick auf die allgemeine Problematik der Videoüberwachung im Detailhandel während der Arbeitszeit sowie der allgemeinen Öffnungszeiten. Die gewonnenen Erkenntnisse und die daraus erfolgten Empfehlungen sollen auch andere Anwender von Videoüberwachungsanlagen im erweiterten Bereich des Dienstleistungssektors dazu veranlassen, die notwendigen Korrekturen vorzunehmen, sofern daselbst Mängel bestehen.

Eine Videoüberwachungsanlage verfolgt mit der Sicherung der Ware sowie der Aufklärung allfällig erfolgter Diebstähle und Überfälle nachvollziehbare Zwecke. Vor dem Einsatz einer Videoüberwachungsanlage sind stets andere geeignete Massnahmen zu überprüfen, welche weniger in die Persönlichkeitsrechte der Betroffenen eingreifen. Drängt sich eine Videoüberwachung auf, ist bei der Umsetzung des angestrebten Zwecks die persönliche Integrität der Kundinnen und Kunden sowie der Mitarbeitenden in Relation zum angestrebten Zweck zu setzen. Dies betrifft insbesondere die Überwachung der Kassenzone und die Überwachung des Verkaufsraums. Kameras sind allesamt so auszurichten, dass nur die für den erfolgten Zweck notwendigen Bilder in ihrem Aufnahmefeld erscheinen (vgl. das Merkblatt „Videoüberwachung durch private Personen" auf unserer Website). Dies bedeutet, dass mit Kameras im Eingangsbereich keine Aussenräume ins Aufnahmefeld geraten dürfen, die von blossen Passanten beansprucht werden. Auf Augenhöhe angebrachte Plakate in angemessener Grösse müssen im Eingangsbereich klar ersichtlich darauf hinweisen, dass Überwachungskameras installiert sind, die alle Personen vom Betreten bis zum Verlassen der Filiale filmen. Für die Videoüberwachung im Verkaufsbereich sind die Kameras so auszurichten, dass primär Waren mit einem gewissen Geldwert fokussiert werden, die von Kunden unschwer in Taschen, Jacken oder Ähnlichem versteckt. Obschon ALDI in seinen Betriebsanweisungen explizit darauf hinweist, dass Kameras nicht zur Überwachung des Personals eingesetzt werden dürfen, hat die Datenschutzkontrolle ergeben, dass die Kameras in der Kassenzone auch die Kassenmitarbeiter in ihren Blickwinkel miteinbezogen haben. Damit soll ALDI keineswegs unterstellt werden, dass je die Absicht bestanden hat, Mitarbeitende zu überwachen. Allein die Möglichkeit dazu muss ausgeschlossen sein. Im Bereich des Arbeitsgesetzes gilt als unumstössliche Gesundheitsvorsorge, dass Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmenden am Arbeitsplatz überwachen sollen, nicht eingesetzt werden dürfen. Wenn sich Überwachungs- oder Kontrollsysteme aus anderen Gründen als erforderlich erweisen, so sind sie insbesondere so zu gestalten und anzuordnen, dass die Gesundheit und die Bewegungsfreiheit der Arbeitnehmenden dadurch nicht beeinträchtigt werden.

Die Auswertung der Videoüberwachung ist bei ALDI nicht allen Mitarbeitenden zugänglich. Sie ist streng reglementiert und bei begründetem Verdacht nur berechtigten Personen mittels Passwort zur Überprüfung zugänglich. Wir haben im Zuge der Kontrolle geltend gemacht, dass im Bereich der verhältnismässigen und „erlaubten", d.h. gesetzeskonformen Videoüberwachung demnächst datenschutzfreundliche Technologien (Privacy-Filter) zum Standard des Datenschutzes werden. Diesen Technologien ist eigen, dass überwachte Personen nicht persönlich erkennbar sind. Erst bei be-

gründetem Verdacht können Personen von berechtigten Aufsichtspersonen kenntlich gemacht werden. Beim Einsatz dieser datenschutzfreundlichen Technologien können Bildschirme stets eingeschaltet bleiben. Der Einsatz solch datenschutzfreundlicher Technologien wurde ALDI bis spätestens Ende 2008 empfohlen. Es ist uns ein zentrales Anliegen, dass bei Videoüberwachungen im Bereich des Dienstleistungssektors aus datenschutzrechtlichen Gründen nur noch solche Technologien zum Einsatz gelangen.

Die ALDI SUISSE AG hat sämtliche im Schlussbericht aufgeführten Empfehlungen des EDÖB vollumfänglich akzeptiert (der Kontrollbericht findet sich auf unserer Website www.edoeb.admin.ch). Nebst verschiedenen Neuausrichtungen von Kameras werden insbesondere diejenigen im Kassenbereich aller Filialen bis Ende März 2007 so fokussiert, dass Aufnahmen von Mitarbeitenden an der Kasse ausgeschlossen sind. ALDI hat sich ausserdem dazu verpflichtet, zur Überwachung ihrer Filialen datenschutzfreundliche Technologien (Privacy-Filter) einzusetzen, sobald diese von ihrem System-Lieferanten lieferbar sind, spätestens aber bis Ende 2008.

1.6.2 Voraussetzungen für das Einholen von Strafregisterauszügen im Unternehmen

Um die eigenen Sicherheitsinteressen zu schützen und internationalen Standards zu genügen, holt ein Transportunternehmen Strafregisterauszüge seiner Angestellten ein. Wir haben diese Massnahme auf ihre Datenschutzkonformität hin geprüft und sind zum Schluss gekommen, dass sie grundsätzlich gerechtfertigt ist. Gleichzeitig haben wir das Unternehmen darauf hingewiesen, dass sie einen schweren Eingriff in die Persönlichkeit der Angestellten darstellt und daher in transparenter und verhältnismässiger Weise zu erfolgen hat.

Infolge verschiedener Anfragen von Angestellten einer Transportfirma haben wir uns mit der Frage befasst, unter welchen Umständen ein Arbeitgeber Strafregisterauszüge eines Angestellten einholen darf. Im vorliegenden Fall hatte sich die Transportfirma aufgrund des Warenwertes, des Anstiegs von Warenverlusten, aber auch infolge internationaler Frachtsicherheitsstandards und zur Verbesserung der Wettbewerbsfähigkeit für die Einholung des Strafregisterauszugs entschieden. Die zu schützende Ware umfasst unter anderem Gefahrengut und Hochpreisgüter. Laut Angaben der Firma bildet die Einholung des Strafregisterauszugs nur eine Massnahme eines umfassenden Sicherheits- und Massnahmenpaketes, welches die Unversehrtheit und Erhaltung der umgeschlagenen Güter und Waren sicherstellen soll.

Wir haben zur angesprochenen Problematik Folgendes festgehalten: Jede Bearbeitung von Personendaten bedarf gemäss Datenschutzgesetz einer Rechtfertigung. Als solche gelten die Einwilligung der betroffenen Person, ein überwiegendes Interesses oder ein Gesetz. Da im vorliegenden Fall weder das Gesetz noch die Einwilligung der betroffenen Person als Rechtfertigungsgrund in Frage kommen, haben wir geprüft, ob ein überwiegendes privates oder öffentliches Interesse die Einholung der Strafregisterauszüge der Angestellten des Unternehmens rechtfertigen kann.

Obwohl der Eingriff in die Persönlichkeit der betroffenen Personen schwer sein kann, sind wir im vorliegenden Fall davon ausgegangen, dass die Sicherheitsinteressen des Unternehmens überwiegen. Dazu ist aber anzumerken, dass das Strafregister besonders schützenswerte Daten – nämlich solche, die strafrechtliche Verfolgungen und Sanktionen betreffen – im Sinne des Datenschutzgesetzes enthält. Die Einsicht in den Strafregisterauszug durch Dritte stellt einen schweren Eingriff in die Persönlichkeit der betroffenen Person dar. Sie setzt neben einem Rechtfertigungsgrund auch eine Notwendigkeit sowie ein vernünftiges Verhältnis zwischen Bearbeitungszweck und Persönlichkeitsbeeinträchtigung voraus.

Zunächst galt es also zu prüfen, ob nicht andere Massnahmen, die weniger tief in die Persönlichkeit der Angestellten eingreifen, den verfolgten Zweck erfüllen würden. Diesbezüglich hat das Unternehmen eine Reihe von Sicherheitsmassnahmen aufgelistet, welche u. a. vom Zutrittsmanagement, Rampenüberwachung, Arealsicherung bis hin zu Fahrzeug- und Personenkontrollen gehen. Diese Massnahmen gewährleisteten zwar eine umfassende Sicherheit. Ein absoluter Schutz für die Güter besteht jedoch bei weitem nicht. Einige zum Teil tief in die Persönlichkeit der Angestellten eingreifende Sicherheitsmassnahmen wie z. B. die Personenkontrollen können nämlich nicht systematisch, sondern nur stichprobenweise durchgeführt werden. Andere wiederum können durch das Personal womöglich umgangen werden. Aus dieser Optik und in Anbetracht des Wertes der zu schützenden Güter haben wir festgestellt, dass die Einholung des Strafregisterauszugs nicht nur als eine nützliche, sondern auch als eine nötige Ergänzung des Sicherheitskonzepts zu betrachten ist.

Ein vernünftiges Verhältnis zwischen Bearbeitungszweck und Persönlichkeitsbeeinträchtigung scheint ebenfalls gegeben zu sein. Das Einholen von Strafregisterauszügen darf jedoch nur diejenigen Mitarbeiterkategorien betreffen, welche in irgendeiner Form (d. h. direkt oder durch Informatikmittel/Dokumente) Zugang zur Ware haben.

Weiter gilt es zu beachten, dass nur eine minimale Anzahl Personen in die Strafregisterauszüge der Angestellten Einsicht nehmen darf. Das Unternehmen hat uns mitgeteilt, dass die Personalabteilung nach Einholung der Strafregisterauszüge eine erste Triage durchführt. Wir haben festgehalten, dass nicht die gesamte Personalabteilung, sondern nur eine beschränkte Anzahl Angestellte dieser Abteilung auf die Strafregisterauszüge Zugriff haben dürfen. Idealerweise ist die Triage direkt durch die Personalleiterin durchzuführen, ohne Einbezug weiterer Mitarbeitenden der Personalabteilung. Die im Auswertungsprozess involvierten Personen sind überdies auf ihre Vertraulichkeitspflichten aufmerksam zu machen. Der Strafregisterauszug darf nur so lange aufbewahrt werden, bis der Bearbeitungszweck erfüllt ist. Die erfassten Daten dürfen unberechtigten Dritten nicht zugänglich sein.

Wir haben uns schliesslich noch mit der Frage befasst, ob die Massnahme für die Angestellten in angemessen transparenter Weise erfolgt. Je einschneidender die Datenbearbeitung in Bezug auf die Persönlichkeitsrechte ist, desto höhere Anforderungen werden an die Transparenz gestellt, die sich aus dem Prinzip von Treu und Glauben ableitet. Da im vorliegenden Fall die Angestellten durch ein Zustimmungsformular informiert wurden, erachteten wir dieses Prinzip als respektiert. Selbstverständlich ist für die betroffenen Personen das Auskunftsrecht zu gewährleisten.

1.6.3 Der Einsatz von Testkunden in Transportbetrieben

Transportbetriebe, die Testkunden zur versteckten Beurteilung ihres Fahrpersonals einsetzen, haben dafür zu sorgen, dass der Schutz der Persönlichkeit der betroffenen Angestellten gewährleistet wird. So muss etwa ein Grossteil der Arbeitszeit unüberwacht bleiben, und die Angestellten müssen die Möglichkeit erhalten, zu den Beurteilungen Stellung zu nehmen und im Streifall mit den betreffenden Testkunden konfrontiert zu werden.

Eine Gewerkschaft bat uns, die Praxis eines Transportbetriebs, seine Chauffeure durch anonyme Testkunden versteckt bewerten zu lassen, aus datenschutzrechtlicher Sicht zu beurteilen. Sie machte im Wesentlichen geltend, die fragliche Datenbearbeitung bezwecke nicht wie offiziell angegeben die Qualitätssicherung und Qualitätssteigerung, sondern die Überwachung und Beurteilung der Chauffeure. Weiter führte sie aus, die betroffenen Personen würden über den Zeitpunkt der Beurteilungen nicht informiert. Dies führte dazu, dass sich die betroffenen Angestellten ständig überwacht fühlten. Schliesslich wurde beanstandet, dass die betroffenen Personen keinen Zugang zu ihren Daten hätten. Die Gewerkschaft kam folglich zum Schluss, dass die fraglichen Beurteilungsdaten auf datenschutzwidrige Art und Weise beschafft würden.

Das Transportunternehmen versicherte seinerseits, die versteckte Überwachung diene in erster Linie der gezielten Qualitätssicherung und Qualitätssteigerung aus Kundensicht. Die Beurteilungsdaten würden nach seinen Angaben nur in bestimmten Regionen als Grundlage und Hilfsmittel für die jährlichen Mitarbeitergespräche des Personals verwendet.

Zunächst gilt es festzuhalten, dass die vom Transportunternehmen angegebenen Zwecke der Qualitätssicherung und Qualitätssteigerung sowie der Mitarbeiterbeurteilung gegenüber den Interessen der betroffenen, beurteilten Personen am Schutz ihrer Persönlichkeit als überwiegend betrachtet werden können. Somit liegt grundsätzlich ein Rechtfertigungsgrund für die Datenbearbeitung im Sinne des Datenschutzgesetzes vor. Um aber als datenschutzkonform erachtet zu werden, muss die Datenbearbeitung auch verhältnismässig sein.

Die Durchführung von verstecken Beurteilungen durch Testkunden stellt je nach Ausgestaltung und Inhalt im konkreten Einzelfall einen mehr oder weniger intensiven Eingriff in die Persönlichkeitsrechte der Betroffenen dar. Wir sind zum Schluss gekommen, dass hier ein Persönlichkeitsprofil vorliegt. Wir haben folglich unterstrichen, dass die versteckte Beurteilung durch Testkunden nur dann verhältnismässig ist und daher durchgeführt werden darf, wenn sich andere Massnahmen, die die Persönlichkeit weniger beeinträchtigen, als ungenügend oder undurchführbar erweisen. Ist dies der Fall, darf die versteckte Beurteilung durchgeführt werden, allerdings nur während einer beschränkten Periode. Dabei dürfen nur die für den verfolgten Zweck absolut notwendigen Daten bearbeitet werden.

Den Fragenkatalog für die Testkunden haben wir grundsätzlich als nötig und geeignet erachtet, um die Beurteilung der Chauffeure in zweckdienlicher Art und Weise durchführen zu können. Allerdings mussten wir feststellen, dass bestimmte Fragen des Beurteilungsbogens subjektive Werturteile auslösen können. Nun ist es so, dass sich die Richtigkeit von Daten nur auf Tatsachen beziehen kann, die auch objektiv festgestellt werden können. Subjektive Werturteile lassen sich indessen nur schwerlich als richtig oder unrichtig einordnen. Richtig sind Personendaten dann, wenn sie die Umstände und Tatsachen, bezogen auf die betroffene Person, sachgerecht wiedergeben. Das Datenschutzgesetz sieht eine Pflicht des Datenbearbeiters vor, sich über die Richtigkeit der von ihm bearbeiteten Personendaten zu vergewissern. Entsprechend ist ein Berichtigungsanspruch vorgesehen. Die betroffene Person kann nämlich durch die Bearbeitung von unrichtigen Daten erheblich in ihrer Persönlichkeit verletzt werden, etwa wenn eine Firma aufgrund falscher Beurteilungsdaten eine Person entlässt.

Gegen die Objektivität der Beurteilungsdaten bzw. gegen deren Richtigkeit spricht im vorliegenden Fall zudem die Tatsache, dass die Testkunden anonym bleiben können. Die Anonymität schützt sie zwar beispielsweise gegen Drohungen, versetzt sie aber gleichzeitig in die Lage, aus einer völlig geschützten Position über einen Chauffeur falsche Tatsachenbehauptungen zu äussern. Die beurteilte Person befindet sich demgegenüber in einer verwundbaren, ungeschützten Position. Der angeschuldigte Arbeitnehmer kann möglicherweise zwar ein Gegendarstellungsrecht gegenüber der Firma geltend machen, eine faire und transparente Konfrontation mit dem eigenen Beurteiler, dem Testkunden, ist aber nicht möglich. Es wird beispielsweise auch nicht möglich sein, den Testkunden wegen eventueller Verleumdung oder übler Nachrede erfolgreich verfolgen zu lassen. Die Gleichbehandlung von Testkunde und betroffenem Arbeitnehmer wird aufgrund des Kräfteungleichgewichts somit offensichtlich nicht gewährleistet.

Problematisch in Bezug auf die Objektivität der Beurteilungsdaten ist ebenfalls die kurze Ausbildungsdauer der Testkunden. Auch der Anstellungsvertrag weist nicht bzw. nur ungenügend auf die Datenschutzproblematik, speziell auf das Bedürfnis der Richtigkeit und Objektivität der Daten, hin.

Anlass zur Kritik gab uns auch der Umstand, dass die Beurteilungen während des ganzen Jahres stattfinden sollen. Dem Chauffeur sind weder der Testkunde noch der genaue Zeitpunkt der Beurteilungen bekannt. Das kann dazu führen, dass er das ganze Jahr unter ständigem Überwachungsdruck steht. Dieser Druck kann zu gesundheitlichen Problemen führen. Obwohl es sich im vorliegenden Fall nicht um eine verbotene Verhaltens-, sondern primär um eine zulässige Leistungsüberwachung handelt, welche nicht durch den Einsatz eines Überwachungssystems im engen Sinne des Wortes durchgeführt wird, ist die Grundproblematik des Gesundheits- und Persönlichkeitsschutzes offensichtlich. Obwohl die besagte Überwachung als geeignet bezeichnet werden kann, die angestrebten Zwecke zu erfüllen, fehlt es sowohl an einer Notwendigkeit des entsprechenden zeitlichen Umfangs als auch an einem vernünftigen Verhältnis zwischen ganzjähriger Überwachung und Persönlichkeitsbeeinträchtigung.

Die Datenbeschaffung und jede weitere Datenbearbeitung muss grundsätzlich für die betroffene Person erkennbar sein. Der Betroffene muss also aus den Umständen heraus damit rechnen oder er muss entsprechend informiert werden. Aus den Unterlagen entnahmen wir, dass sowohl über die Zwecke der Überwachung als auch über die bearbeiteten Daten und die Dauer der Überwachungsperiode informiert wurde. Eine Aufklärung über das Auskunftsrecht und die Auskunftsstelle fehlte jedoch. Ebenfalls war eine Information über die gewählten Kontrollperioden nicht vorhanden.

Aufgrund unserer Beurteilung des Einsatzes von Testkunden haben wir dem Transportunternehmen einige Verbesserungsvorschläge unterbreitet. So haben wir ihm nahe gelegt, diejenigen Fragen zu streichen, deren Beantwortung zu stark von subjektiven Empfindungen des Testkunden abhängt. Wir haben dem Unternehmen in Erinnerung gerufen, dass das Prinzip der Richtigkeit der Daten als eine Grundanforderung gilt, die ein Datenbearbeiter zu beachten hat.

Um die Position des beurteilten Angestellten zu stärken, ist gegebenenfalls eine persönliche Konfrontation des Chauffeurs mit dem Testkunden zu ermöglichen. Sowohl die Chauffeure als auch die Testkunden sind vorgängig darüber zu informieren. Wir haben das Transportunternehmen diesbezüglich aufgefordert, dafür zu sorgen, dass der Chauffeur seine Gegendarstellung unverzüglich machen darf. Dies setzt voraus, dass er nicht erst Wochen später mit einer negativen Beurteilung konfrontiert wird, sondern spätestens zwei Tage nach deren Einreichung.

Mit Blick auf das Verhältnismässigkeitsprinzip haben wir folgende Verbesserungsvorschläge formuliert: Gelegentliche versteckte Beurteilungen sollten in der Regel jeweils vorher angekündigt werden. Um den Interessen des Arbeitgebers, insbesondere der Wirksamkeit der Beurteilung, besser gerecht zu werden, ist es mit dem Persönlichkeitsschutz nicht unvereinbar, wenn die Angestellten nur über die ausgewählte Beurteilungsperiode informiert werden. Es muss jedenfalls dafür gesorgt werden, dass der Arbeitnehmer mit Sicherheit davon ausgehen kann, dass ein wesentlicher Teil seiner Arbeitszeit unüberwacht bleibt. Eine verhältnismässige Lösung könnte beispielsweise darin bestehen, die Dauer der Kontrollperioden auf vier von einander getrennte Monate pro Jahr zu reduzieren und die betroffenen Personen über die gewählten Kontrollperioden vorgängig zu informieren.

Des Weiteren haben wir angemerkt, dass Beurteilungsdaten ein Persönlichkeitsprofil darstellen und in aller Regel nur durch Vorgesetzte eingesehen werden dürfen. Im vorliegenden Fall sollten hingegen die Personaldienstangestellten die von den Testkunden gelieferten Daten im entsprechenden System erfassen. Wir haben das Transportunternehmen ersucht, speziell ausgebildete Vertrauenspersonen innerhalb des Unternehmens mit der Einsicht und Erfassung der Daten zu betrauen. Die Anzahl dieser Personen ist überdies klein zu halten. Technisch soll dafür gesorgt werden, dass die erfassten Daten unberechtigten Dritten nicht zugänglich sind.

Die Testkunden sind speziell auf die Vertraulichkeit der Fragebögen aufmerksam zu machen sowie vertraglich zur sofortigen Vernichtung allfälliger Kopien nach Abgabe des Originals an das Transportunternehmen zu verpflichten. Auf dem Übertragungsweg sind die Fragebögen mit geeigneten Schutzmassnahmen zu sichern. Erfolgt die Übertragung beispielsweise via Internet, so ist an eine Verschlüsselung zu denken.

Jede angestellte Person des Transportunternehmens muss Auskunft über die sie betreffenden bearbeiteten Daten verlangen können. Dieses Recht ermöglicht den Betroffenen, die Daten zu kontrollieren mit dem Ziel, die Einhaltung der datenschutzrechtlichen Grundsätze wie rechtmässige Datenbeschaffung, Treu und Glauben, Richtigkeit der Daten und Verhältnismässigkeit zu überprüfen und deren Durchsetzung zu verlangen.

1.6.4 Revision der Verordnung über den Schutz von Personaldaten in der Bundesverwaltung

In unserer Stellungnahme zur Verordnung über den Schutz von Personaldaten in der Bundesverwaltung sind wir im Wesentlichen zum Schluss gekommen, dass im Bundespersonalgesetz die gesetzlichen Grundlagen für die Verordnung noch zu schaffen sind. Wir haben ebenfalls beantragt, die Regelungen betreffend Zugriffsberechtigungen restriktiver auszugestalten. Infolge einer Sitzung mit verschiedenen Bundesämtern haben wir nach der Ämterkonsultation festgestellt, dass die Revision der Verordnung zurzeit verfrüht ist.

Wir wurden im Rahmen der Ämterkonsultation zur Revision der Verordnung über den Schutz von Personaldaten in der Bundesverwaltung eingeladen, Stellung zu nehmen. In unserer Stellungnahme haben wir insbesondere beantragt, im Rahmen der Revision des Bundespersonalgesetzes die erforderlichen gesetzlichen Grundlagen für die Verordnung zu schaffen. Weiter haben wir festgehalten, dass die in der Verordnung enthaltenen, wichtigen Recht setzenden Bestimmungen auf Gesetzesstufe anzuheben sind. Zur Regelung der Zugriffsberechtigungen haben wir festgehalten, dass der Kreis von Personen und Stellen, welche Zugriff auf die Gesamtheit der Daten im Verwaltungssystem der Personaldaten BV-PLUS erhalten sollen, zu gross ist. Folglich haben wir beantragt, die Regelungen betreffend Zugriffsberechtigungen restriktiver auszugestalten. Wir haben ebenfalls gefordert, in der Verordnung zu regeln, zu welchem Zweck die berechtigten Personen ein Zugriffsrecht auf die Gesamtheit der Daten in BV-PLUS erhalten sollen.

Infolge einer Sitzung mit dem federführenden Eidgenössischen Personalamt (EPA), dem Bundesamt für Justiz, der Bundeskanzlei sowie anderen Datenschutzberatern der Bundesverwaltung sind wir nach der Ämterkonsultation zum Schluss gekommen, dass eine Revision der Verordnung verfrüht ist. Das Konzept zur Automatisierung der Bearbeitung der Personaldossiers befindet sich nämlich noch in einer frühen Phase. Es gilt also zu verhindern, dass mit einer provisorischen Verordnung vollendete Tatsachen geschaffen werden, über deren Notwendigkeit man sich noch nicht eingehend auseinandergesetzt hat. Dasselbe gilt in Zusammenhang mit der Einführung der Beurteilungen und Zielvereinbarungen im BV-PLUS. Wir haben noch festgehalten, dass die einzige zurzeit notwendige Revision der Verordnung die Regelung der Nebenbeschäftigungen betrifft. Diese Gesetzeslücke kann aber vorläufig toleriert werden, sofern die Revisionsarbeiten an das Bundespersonalgesetz demnächst aufgenommen werden. Das EPA hat folglich die Revision der Verordnung suspendiert, bis die entsprechenden Grundlagen im Bundespersonalgesetz geschaffen werden.

1.6.5 Verordnung zum Bundesgesetz über Massnahmen zur Bekämpfung der Schwarzarbeit

Wir haben im Rahmen der Ämterkonsultation zur Schaffung einer Vollzugsverordnung zum Bundesgesetz über Massnahmen zur Bekämpfung der Schwarzarbeit Stellung genommen. Dabei haben wir den Bestimmtheitsgrad der datenschutzrechtlich relevanten Normen, vor allem jene über den Informationsaustausch unter Behörden und über ihre Zugriffsrechte, als ungenügend beanstandet.

Daten im Bereich der Schwarzarbeit sind besonders schützenswert. Deshalb ist für die Normen der Bearbeitung dieser Daten ein hoher Bestimmtheitsgrad erforderlich, der aus unserer Sicht bei der Vollzugsverordnung zum Bundesgesetz über Massnahmen zur Bekämpfung der Schwarzarbeit nicht gegeben ist. So haben wir im Rahmen der Ämterkonsultation zu dieser Verordnung kritisiert, dass die Normen zu allgemein formuliert seien; die Bearbeitung besonders schützenswerter Daten verlange jedoch nach einer Rechtsgrundlage mit hohem Bestimmtheitsgrad. Wir haben diesbezüglich ausgeführt, dass von einer gesetzlichen Grundlage im materiellen Sinne Konkretes in Bezug auf bearbeitete Personendaten, Zugriffsrechte und deren Umfang sowie Bekanntgaben erwartet wird.

Speziell haben wir kritisiert, dass insbesondere die gegenseitige Information der beteiligten Behörden im Verordnungstext nicht konkret umschrieben wird. Die vorgeschlagene Formulierung überlässt es dem Gutdünken der beteiligten Behörden zu entscheiden, wer wem wann welche Daten zu welchem Zweck bekannt gibt. Wir haben das federführende Staatssekretariat für Wirtschaft (SECO) aufgefordert, den Informationsaustausch unter Behörden im Verordnungstext fassbar zu regeln

Auch die Regelung des Zugriffsrechts der beteiligten Behörden haben wir beanstandet. Nach dem Wortlaut der Verordnung kann jede beteiligte Behörde aufgrund eines umfangreichen Zugriffsrechts auf die Datenbearbeitungen der anderen Behörden direkt Einfluss nehmen. Die Verantwortung für ein und dieselbe Datenbearbeitung tragen somit mehrere Behörden im gleichen Umfang. Demzufolge haben wir verlangt, dass in der Verordnung klar angegeben werde, welche Behörde in welchem Umfang Zugriff auf welche Daten hat. Gegebenenfalls sei eine Zugriffsmatrix vorzusehen.

Anlässlich einer Sitzung hat das SECO in der Folge unsere Einwände akzeptiert und sich engagiert, die Verordnung im Sinne unserer Einwände zu überarbeiten. Wir mussten aber nachträglich feststellen, dass der neue Verordnungsentwurf unsere damaligen Einwände nur teilweise berücksichtigte und dass wir nicht auf der Adressatenliste der zweiten Ämterkonsultation standen.

1.7 Handel und Wirtschaft

1.7.1 Auskunfts- und Berichtigungsrecht im Bereich Wirtschafts- und Kreditauskunft

Wie im letzten Tätigkeitsbericht erwähnt, haben wir im Jahr 2005 bei vier Unternehmen des Sektors Kredit- und Wirtschaftsauskunft geprüft, wie diese den betroffenen Personen ihre Rechte gemäss Datenschutzgesetz gewähren. Dabei sind wir zu insgesamt positiven Beurteilungen gekommen, was indes nicht bedeutet, dass für die betroffenen Personen keine Probleme existieren.

Wir haben geprüft, wie die einzelnen Kredit- und Wirtschaftsauskunfteien den betroffenen Personen gegenüber auf Auskunfts-, Berichtigungs- und Löschungsbegehren reagieren. Als Informationsquellen haben dabei nebst der angeforderten Dokumentation ein Augenschein sowie Gespräche und Schriftenwechsel gedient. Gemäss den von uns festgestellten Sachverhalten ist in formeller Hinsicht davon auszugehen, dass sowohl betreffend die Identitätsprüfung als auch betreffend Fristen und Kosten die rechtlichen Vorgaben eingehalten werden. Das bedeutet, dass die untersuchten Unternehmen vor Erteilung einer Auskunft nach Datenschutzgesetz die Identität der antragstellenden Person prüfen und dass sie die Auskünfte abgesehen von den gesetzlich vorgesehenen Ausnahmefällen kostenlos und innert maximal 30 Tagen erteilen. Auch materiell werden die Vorgaben des Datenschutzes eingehalten, da die gewährten Auskünfte nach unseren Beobachtungen vollständig und verständlich sind. Betreffend die Behandlung von Löschungs- und Berichtigungsbegehren haben wir ebenfalls keine Feststellungen gemacht, welche darauf hindeuten würden, dass rechtliche Vorgaben nicht eingehalten werden. Trotz dieser positiven Beurteilung der festgestellten Sachverhalte gelangen aber immer wieder Betroffene an uns aufgrund von Schwierigkeiten, die sie mit Unternehmen aus dem Sektor haben. Über mögliche Ursachen dafür können wir nur Vermutungen anstellen. Wir gehen davon aus, dass die bei uns eintreffenden Anfragen in zwei Gruppen unterteilt werden können: Erstens gehören dazu all diejenigen Fälle, in welchen Probleme beim Matching vorgekommen sind. Mit anderen Worten geht es hier um die Fälle der Verwechslung von zwei Personen, z.B. Personen mit beinahe identischen Namen, welche an derselben Strasse wohnen. Und zweitens kommt es im Falle von Löschungs- und Berichtigungsbegehren vor, dass der dem Eintrag zugrunde liegende Sachverhalt nicht eindeutig geklärt ist. In diesen Fällen gibt es einen offensichtlichen Gegensatz zwischen den Interessen der Kreditauskunftfirmen bzw. ihrer Kundinnen und Kunden einerseits und denjenigen der Betroffenen andererseits.

1.8. Finanzen

1.8.1 Datenschutz im internationalen Zahlungsverkehr (SWIFT)

Der überwiegende Teil des internationalen Zahlungsverkehrs wird über die in Belgien ansässige Society for Worldwide Interbank Financial Telecommunication (SWIFT) abgewickelt. Entsprechend brisant war die im Juni 2006 in den Medien verbreitete Meldung, wonach die US-Administration im Rahmen ihrer Anstrengungen zur Terrorbekämpfung Zugriff auf die Transaktionsdaten der SWIFT hat. Wir haben nach Kenntnisnahme dieses Vorgangs bei den wichtigsten Akteuren des schweizerischen Bankensektors Informationen eingeholt und auf verschiedenen Ebenen zur Bewältigung der SWIFT-Affäre beigetragen.

Die in Belgien domizilierte SWIFT ist bei der Abwicklung des internationalen Zahlungsverkehrs die weltweit wichtigste Akteurin. Sie verfügt über zwei Archive, welche sämtliche Transaktionsdaten je während 124 Tagen aufbewahren. Die amerikanische Presse konnte aufdecken, dass die US-Administration über das in den USA gelegene Archiv der SWIFT – und in Kooperation mit dieser – auf Transaktionsdaten Zugriff nahm; über den genauen Umfang des Zugriffs bestehen bis heute keine gesicherten Kenntnisse.

Der Datenschutz ist bei der juristischen Aufarbeitung der so genannten SWIFT-Affäre unzweifelhaft einer der zentralen Aspekte. Deshalb haben Datenschutzbehörden zahlreicher Länder Abklärungen vorgenommen. Da die SWIFT in Belgien domiziliert ist, kam der Untersuchung der dort zuständigen Commission de la protection de la vie privée herausragende Bedeutung zu. Sie stellte in ihrem Bericht verschiedene Verstösse gegen belgisches und europäisches Datenschutzrecht durch die SWIFT fest.

Auf der Grundlage des belgischen Berichts und eigener Nachforschungen haben wir festgestellt, dass die SWIFT in der Schweiz keine Personendaten bearbeitet. Zu beantworten blieb die Frage nach der datenschutzrechtlichen Verantwortung der hierzulande ansässigen Finanzdienstleister. Den zu dieser Frage verfassten Bericht des EDÖB finden Sie in Anhang 4.1.

Zusammenfassend ist auf zwei problematische Punkte hinzuweisen: Einerseits informierten die Finanzdienstleister auch nach Kenntnisnahme der SWIFT-Affäre ihre Kunden nicht über die Zugriffsrisiken beim Vorgang der internationalen Zahlung (mangelhafte Transparenz der Datenbearbeitung); andererseits besteht durch die Einsichtnahme in Transaktionsdaten durch die US-Administration das Problem eines Datentransfers in ein Land ohne gleichwertigen Datenschutz.

Die Aufarbeitung der Datenschutzprobleme rund um die SWIFT geschah in Zusammenarbeit mit zahlreichen ausländischen Datenschutzbehörden, namentlich mit der Artikel 29 Datenschutzgruppe; wir werden uns (auch) in diesem Rahmen weiterhin für eine datenschutzkonforme Lösung einsetzen. Schliesslich haben wir in dieser Angelegenheit auch der Geschäftsprüfungskommission des Nationalrates (Subkommission EFD/EVD) rapportiert, die sich der Bewältigung des Problems angenommen hat.

Aus Sicht des schweizerischen Datenschutzes besteht in der SWIFT-Affäre weiterhin Handlungsbedarf: Dabei gilt es, auf dem Weg politischer Aushandlung eine Lösung zu erarbeiten, die dem Anliegen der Terrorbekämpfung gerecht wird, aber auch die Datenschutzordnungen sämtlicher Länder respektiert, also auch das schweizerische Datenschutzgesetz. Soweit es in ihrer Handlungsmacht liegt, stehen ausserdem vorgängig die schweizerischen Finanzdienstleister in der Pflicht; sie haben namentlich die Transparenz über die Zugriffsrisiken beim Vorgang internationaler Zahlungen zu gewährleisten.

1.9 International

1.9.1 Internationale Konferenz der Datenschutzbeauftragten

Die 28. Konferenz der Datenschutzbeauftragten fand am 2. und 3. November 2006 in London statt. Als Hauptthema standen die Gefahren der Überwachungsgesellschaft im Mittelpunkt der Beratungen. Die Datenschutzbeauftragten stellten fest, dass die Überwachungsgesellschaft bereits Realität ist, und betonten die Bedeutung des Rechts auf Datenschutz in diesem Kontext. Es handelt sich dabei um ein für die Wahrnehmung der übrigen Rechte und Grundfreiheiten in einer demokratischen Gesellschaft notwendiges Grundrecht. Ausserdem verabschiedeten die Datenschutzbeauftragten eine Entschliessung zum Datenschutz bei Suchmaschinen. Sie unterstützten einstimmig eine Initiative der CNIL (der französischen Datenschutzkommission) für eine bessere und effektiver gestaltete Vermittlung des Datenschutzes.

Auf Einladung des britischen Datenschutz- und Informationsbeauftragten kamen 58 Datenschutzbehörden aus der ganzen Welt und Vertreter der internationalen Organisationen, der Wirtschaft und der Wissenschaft in London zusammen, um anlässlich der 28. Internationalen Konferenz der Datenschutzbeauftragten über die Überwachungsgesellschaft zu debattieren. Die Schweiz war durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten sowie durch die Datenschutzbeauftragten der Kantone Basel-Land, Zug und Zürich vertreten.

Der zentrale Teil der Konferenz war den Auswirkungen der Überwachungsgesellschaft gewidmet. Der britische Datenschutz- und Informationsbeauftragte hatte eine umfassende Studie zum Phänomen der Überwachungsgesellschaft in Auftrag gegeben, um eine öffentliche Debatte über die beunruhigenden Entwicklungen, mit denen sich die demokratischen Gesellschaften heute auseinandersetzen müssen, in Gang zu bringen (die Studie ist auf der Website der Konferenz abrufbar: www.privacyconference2006.co.uk). Die Überwachungsgesellschaft ist Realität geworden, und wenn ihr nicht klare Grenzen gesetzt werden, sind Auswüchse unvermeidlich.

Die im Rahmen der Überwachungsgesellschaft vorgenommenen Datenbearbeitungen haben einen wachsenden Einfluss im Leben des Einzelnen, auf unsere Verhaltensweisen und unseren Lebensstil. Sie lassen Risiken für den Datenschutz und die Achtung der grundlegenden Rechte und Freiheiten und namentlich der Privatsphäre entstehen. Gewisse Überwachungstätigkeiten sind indessen notwendig, zum Beispiel zur Bekämpfung von Terrorismus und Schwerkriminalität oder zur Verbesserung des

Gesundheitswesens. Sie können für den Einzelnen und für die Gesellschaft positive Auswirkungen haben. Es ist allerdings zu prüfen, was vom Standpunkt eines demokratischen, den Rechten und Grundfreiheiten verschriebenen Staates aus tragbar ist, und der Überwachung sind Grenzen zu setzen. Die unkontrollierte Überwachung wirkt sich nicht nur unter dem Gesichtspunkt des Rechtes auf Datenschutz und Schutz der Privatsphäre negativ aus, sie kann auch andere Werte eines Rechtsstaates in Gefahr bringen. Eine übermässige Überwachung kann namentlich dazu beitragen, ein Misstrauensklima zu schaffen und zu schüren, das Vertrauen der Bürgerinnen und Bürger in die bestehenden Institutionen untergraben und sich im Wesen der Gesellschaft selbst niederschlagen. Überdies ist ein wachsendes Risiko der Diskriminierung und der sozialen Ausgrenzung vorhanden. Ohne die Notwendigkeit gewisser Massnahmen bestreiten zu wollen, betonten die Datenschutzbeauftragten daher die besondere Bedeutung des Rechts auf Datenschutz und Schutz der Privatsphäre als Menschenrecht. Die Vorschriften für diesen Schutz ermöglichen die Durchsetzung legitimer Einschränkungen der Überwachung. Solche Regeln sind jedoch unzulänglich, wenn sie nicht mit Massnahmen einhergehen, die Gewähr für die Einhaltung der Datenschutzgrundsätze und insbesondere des Transparenzprinzips bieten können. Auch müssten die Einwirkungen der geplanten oder eingeführten Überwachungstechniken auf die Privatsphäre systematisch ausgewertet werden. Die Vorschriften müssen zudem danach beurteilt werden, ob sie eine angemessene Antwort auf die konkrete Herausforderung darstellen. Die Überwachungsgesellschaft muss Gegenstand weit reichender Debatten in der Öffentlichkeit sein. Sämtliche betroffenen Akteure müssen bei der Eindämmung der negativen Folgen dieser sicherheitsorientierten Entwicklung zusammenarbeiten. Sie müssen sich darum bemühen, das Vertrauen der Öffentlichkeit zu gewinnen und zu verstärken. Die Bürger müssen überzeugt sein, dass jeder Eingriff in ihre Privatsphäre jeweils notwendig und verhältnismässig ist. Missbräuche müssen aufgedeckt und Sanktionen (namentlich strafrechtlicher Art) verhängt werden können, wenn eine Verletzung der Privatsphäre vorliegt. In diesem Kontext haben die Datenschutzbehörden eine wesentliche Rolle zu spielen, um Exzesse in der Überwachung unter Kontrolle zu bringen und abzuwenden. Die Datenschutzbeauftragten unterstützten daher eine Initiative der französischen nationalen Kommission für Informatik und Freiheitsrechte (Commission nationale de l'informatique et des libertés, CNIL), die darauf abzielt, die grundlegende Bedeutung des Datenschutzes und des Schutzes der Privatsphäre in einer in ständigem Wandel befindlichen Welt zu bekräftigen. Die Erklärung „Datenschutz vermitteln und effektiver gestalten" (s. Anhang 4.4) ist ein Manifest für eine bessere Effektivität des Datenschutzes. Angesichts der mit den kollektiven Sicherheitsanforderungen und den technologischen Entwicklungen (Biometrie, Geolokalisierung, Videoüberwachung, Internet, RFID, usw.) verbundenen Risiken müssen die

Datenschutzbehörden, wie A. Türk, der Vorsitzende der CNIL betonte, „ein gesteigertes kollektives Bewusstsein wecken und gemeinsam koordinierte Initiativen ergreifen, die hauptsächlich auf einer neuen Kommunikationsstrategie, einer Erweiterung der Fachkapazitäten, einer Beurteilung und Verstärkung ihrer Handlungsmittel, und auf der Unterstützung von Arbeiten beruhen, die zur Anerkennung eines universellen Rechts auf Datenschutz führen. Das Kapital unserer Identität und unseres Privatlebens ist tagtäglich bedroht. Es muss dringend erhalten werden. Wie das Umweltkapital der Menschheit ist es in Gefahr, so schweren Schaden zu nehmen, dass es nicht mehr erneuert werden kann." Der Bewusstseinsbildung in der Öffentlichkeit wird besondere Aufmerksamkeit zuzuwenden sein.

Die Datenschutzbeauftragten verabschiedeten ausserdem zwei Entschliessungen. Die eine betrifft die Achtung der Privatsphäre bei Suchmaschinen (s. Anhang 4.6). Sie fordert insbesondere die Anbieter von Suchmaschinen auf, die Datenschutzerfordernisse einzuhalten und namentlich die Benutzer transparent über die bei der Beanspruchung ihrer Dienstleistungen vorgenommenen Datenbearbeitungen zu informieren und die Zahl der erfassten Personendaten zu beschränken (Grundsatz der Datenminimierung). Die zweite Entschliessung betrifft die praktischen Organisationsmodalitäten der Konferenz (s. Anhang 4.5). Die Datenschutzbeauftragen genehmigten auch die Akkreditierung der Datenschutzbehörden von Andorra, Liechtenstein, Estland, der kanadischen Provinzen New Brunswick, Northwest Territories und Nunavut, sowie von Gibraltar. Schliesslich zogen sie eine erste positive Bilanz der Folgemassnahmen zur Erklärung von Montreux (vgl. unseren 13. Tätigkeitsbericht 2005/2006, Ziffer 9.2.1 und Anhang 11.2). Im Besonderen fand die Aufforderung der Datenschutzbeauftragten zur Ausarbeitung einer Rechtsurkunde ein positives Echo, namentlich bei der Völkerrechtskommission der UNO, die dieses Thema in ihr Arbeitsprogramm aufgenommen hat. Ebenso verpflichtete sich das Generalsekretariat des Europarates, die Massnahmen für den Beitritt von Nichtmitgliedstaaten des Europarates zum Übereinkommen 108 zu unterstützen. Schliesslich geht die Notwendigkeit einer Verstärkung der Universalität des Rechts auf Datenschutz auch aus den Dokumenten des Weltgipfels zur Informationsgesellschaft in Tunis (16.-18. November 2005, http://www.itu.int/wsis/documents/doc_multi.asp?lang=fr&id=2331|2304) und aus der Erklärung des Gipfeltreffens der Staats- und Regierungschefs der französischsprachigen Länder in Bukarest (28.-29 September 2006, http://www.francophonie.org/doc/txt-reference/decl-bucarest-2006.pdf) hervor.

1.9.2 Europäische Konferenz der Datenschutzbeauftragten

Die europäische Konferenz der Datenschutzbeauftragten fand vom 24. bis 25. April 2006 in Budapest statt. Die europäischen Datenschutzbeauftragten verabschiedeten einstimmig eine Erklärung betreffend die Einführung des Grundsatzes der Datenverfügbarkeit im Rahmen der Verstärkung der Zusammenarbeit von Polizei- und Justizbehörden innerhalb der Europäischen Union.

Auf Einladung des Datenschutz- und Informationsbeauftragten Ungarns hielten die europäischen Datenschutzbeauftragten ihre Frühjahrskonferenz vom 24. bis 25. April 2006 in Budapest ab. Die Datenschutzbeauftragten aus 34 europäischen Staaten, der europäische Datenschutzbeauftragte und die Vertreter der gemeinsamen Kontrollinstanzen Europol und Schengen nahmen an der Konferenz teil. Die Schweiz war durch den Eidgenössischen Datenschutzbeauftragten und die Datenschutzbeauftragten der Kantone Basel-Land, Zug und Zürich vertreten.

In seiner Begrüssungsbotschaft erinnerte der Präsident der Republik Ungarn, László Sólyom, an die Bedeutung des Rechts auf Datenschutz in der heutigen Welt und hob insbesondere hervor, dass der Kampf gegen den Terrorismus nicht zu Lasten des informationellen Selbstbestimmungsrecht gehen dürfe. Die Konferenz bot den Datenschutzbeauftragten die Möglichkeit zu einer Bestandesaufnahme zu verschiedenen aktuellen Themen, darunter namentlich die Bearbeitung von Personendaten auf dem Gebiet der polizeilichen und justiziellen Zusammenarbeit, die Herausforderungen der neuen invasiven Technologien, die „Whistleblowing"-Warnsysteme in den Unternehmen, die Entwicklung der elektronischen Patientenakte, die Bearbeitung genetischer Daten, die wissenschaftliche Geschichtsforschung.

Die Datenschutzbeauftragten beschäftigten sich auch mit der Effektivität ihrer Tätigkeit. Ausgehend von der Feststellung, dass derzeit die meisten nationalen Datenschutzbehörden nicht über ausreichende Mittel für die Erfüllung ihrer Aufgaben verfügen, waren sich die europäischen Datenschutzbeauftragten darin einig, dass Prioritäten gesetzt und vorzugsweise Absprachen und eine Zusammenarbeit mit anderen Akteuren der Zivilgesellschaft (Verbraucherschutzorganisationen, Bürgerrechtsorganisationen usw.) angestrebt werden sollten. Sie betonten auch, wie wichtig es sei, ihre Massnahmen und die damit verfolgten Ziele sichtbar zu machen. Ebenfalls wichtig ist es, die Erfüllung ihrer Aufgaben einer Evaluation zu unterziehen. Die Behörden sind nicht in der Lage, sämtliche an sie gerichtete Gesuche zu behandeln und auf jede eingereichte Beschwerde hin einzuschreiten. Es ist wünschenswert, Kriterien für ein

behördliches Eingreifen festzulegen und vorrangig die Fälle zu behandeln, in denen sich die Betroffenen gegenüber dem Verantwortlichen der Datenbearbeitung in einer Position der Schwäche befinden, in denen die Bearbeitung von Personendaten erhebliche Folgen haben kann und in denen das informationelle Selbstbestimmungsrecht in ungerechtfertigter Weise eingeschränkt werden könnte. Um zu entscheiden, ob ihr Eingreifen angebracht ist, richtet sich die britische Datenschutzbehörde namentlich nach folgenden Kriterien: erhebliches Risiko für den Einzelnen, Zahl der betroffenen Personen, notwendige Klärung der Gesetzesbestimmungen oder der Datenschutzgrundsätze, Gefahr einer Wiederholung oder Fortdauer der Beeinträchtigung, Notwendigkeit, ein „Exempel" zu statuieren, Verhältnis zwischen den Kosten einer gesetzeskonformen Anpassung für die beteiligte Organisation und der erwarteten Wirkung, absichtliche Rechtsverletzung.

Die Konferenz akkreditierte drei neue Staaten: die ehemalige jugoslawische Republik Mazedonien, Rumänien und Slowenien. Andorra wurde der Beobachterstatus zuerkannt. Die Datenschutzbeauftragten verabschiedeten schliesslich einstimmig eine Erklärung zur Zusammenarbeit zwischen Polizei- und Justizbehörden, insbesondere zum Entwurf eines Rahmenbeschlusses der Europäischen Union betreffend das Verfügbarkeitsprinzip. Die Konferenz erinnerte insbesondere daran, dass der Austausch von personenbezogenen Informationen zwischen den Strafverfolgungsbehörden nur unter Einhaltung der Datenschutzvorschriften erfolgen darf. Nach Auffassung der europäischen Datenschutzbeauftragten ist es unerlässlich, den gesamten Bereich der polizeilichen und justiziellen Zusammenarbeit durch harmonisierte Vorschriften zu regeln, welche ein hohes Datenschutzniveau gewährleisten. Am Rande der 28. Internationalen Konferenz der Datenschutzbeauftragten (s. Ziffer 1.9.1) verabschiedete die europäische Konferenz eine zweite Erklärung zum Entwurf für einen Rahmenbeschluss der Europäischen Union über den Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit (vgl. unseren 13. Tätigkeitsbericht 2005/2006, Ziffer 9.1.2). In dieser Erklärung erinnern die Datenschutzbeauftragten daran, dass die Einführung des Verfügbarkeitsprinzips mit der Annahme eines angemessenen Datenschutzrahmens für sämtliche Bearbeitungen zum Zwecke der polizeilichen und justiziellen Zusammenarbeit verbunden sein muss. Dieser Rahmen hat ein hohes Datenschutzniveau zu gewährleisten, das im Einklang mit den Bestimmungen der europäischen Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr steht. Es darf insbesondere keine unterschiedliche Behandlung zwischen den Daten aus innerstaatlicher Verarbeitung und den von einer ausländischen Behörde stammenden Daten geben.

1.9.3 Case Handling Workshop

Die von der Europäischen Konferenz der Datenschutzbeauftragten eingerichtete Arbeitsgruppe „Case Handling Workshop" hat die Aufgabe, Mittel und Wege für eine Zusammenarbeit und gemeinsame Tätigkeiten der Datenschutz-Kontrollbehörden zu prüfen und auszugestalten. Bei ihren letzten Sitzungen beschäftigte sich die Arbeitsgruppe mit den Methoden, welche verschiedene nationale Behörden für die Behandlung von jeweils ähnlichen Fällen anwenden.

Aufgrund des Auftrags, den die Europäische Konferenz der Datenschutzbeauftragten ihm erteilt hatte, widmete der Case Handling Workshop seine beiden Tagungen im Jahre 2006 in Madrid und Athen der Umsetzung der im Vorjahr beschlossenen Neuorientierung.

Anlässlich ihrer ersten Tagungen hatte sich nämlich die Arbeitsgruppe – die damals noch die Bezeichnung „Complaints Handling Workshop" trug – auf die Kontrollmethoden konzentriert, die die Datenschutzbehörden gemäss ihren jeweiligen gesetzlichen Kompetenzen verwenden. Dieser Informationsaustausch über die in den verschiedenen Staaten durchgeführten Kontrollen vermittelte eine bessere Kenntnis der Rollen, der Sanktionsbefugnisse, der Instrumente und der Kompetenzen der anderen nationalen Kontrollbehörden.

Bei seinen Tätigkeiten stellte sich dem Workshop jedoch ein zweifaches Problem: die wachsende Zahl der Teilnehmenden einerseits und die schwierige Konkretisierung des Informationsaustausches andererseits. Mit seinen annähernd sechzig Teilnehmenden unterzog der Workshop seine Arbeitsweise einer eingehenden Prüfung. Ohne auf ihren informellen Rahmen zu verzichten, der den Erfahrungsaustausch erleichtern sollte, beschloss die Arbeitsgruppe, die verschiedenen Beiträge der Teilnehmenden effizienter zu organisieren, die Wahl der Tagungsthemen besser zu koordinieren (namentlich mit den laufenden Arbeiten der Gruppe Artikel 29 der Europäischen Union) und ihre Arbeiten auf konkrete Fälle zu konzentrieren. In diesem Sinne wurde die Gruppe in „Case Handling Workshop" umbenannt.

Nachdem diese Änderungen von der Europäischen Konferenz der Datenschutzbeauftragten, die im Frühjahr 2005 in Krakau stattfand, genehmigt worden waren, richtete der Workshop die Arbeiten seiner beiden Tagungen im Jahre 2006 auf konkrete Fälle aus. So lag der Schwerpunkt der Tagung im März 2006 in Madrid auf der Art der Behandlung der Datenschutzfälle im öffentlichen Sektor. Aus diesem Anlass erläuterten wir die Probleme, auf die wir in den verschiedenen Etappen unserer Kontrolle beim

Bundesamt für Polizei gestossen waren, als es darum ging, die nachträgliche Information der betroffenen Personen zu prüfen (vgl. unseren 12. Tätigkeitsbericht 2004/2005, Ziffer 3.1.1 und 13. Tätigkeitsbericht 2005/2006, Ziffer 3.1.4). Anhand der Vorstellung dieses konkreten Falls konnten zahlreiche Ähnlichkeiten mit den von anderen einzelstaatlichen Behörden im öffentlichen Sektor durchgeführten Kontrollen festgestellt werden (Schwierigkeiten bei der Feststellung des Sachverhalts und bei der Suche nach Verbesserungslösungen, Ablehnung der Empfehlungen, Nutzung der Rechtsmittel). Die Novembertagung 2006 in Athen wiederum war der Behandlung konkreter Fälle in Sachen E-Government einerseits und der Videoüberwachung andererseits gewidmet. Letzteres Thema bot die Gelegenheit zu einem ergiebigen Informationsaustausch über die zahlreichen Probleme (Rechtsgrundlagen, Verhältnismässigkeit, Datenzugriff, Rolle der verschiedenen Akteure, Wiederverwendung der Daten, Löschung der Daten, usw.), welche bei der Einrichtung von Videoüberwachungskameras im Rahmen von sportlichen Grossveranstaltungen wie den Olympischen Sommerspielen 2004 in Athen oder der in der Schweiz und in Österreich im Jahre 2008 stattfindenden Fussball-Europameisterschaft (EURO 2008) auftreten.

Der Workshop, dessen nächste Tagung im Jahre 2007 in Helsinki geplant ist, wird seine Tätigkeiten fortführen mit dem Ziel, die Zusammenarbeit zwischen den nationalen Kontrollbehörden zu verbessern. Zu diesem Zweck wird er einen Vergleich der Methoden für den Umgang mit jeweils ähnlichen Fällen und der dabei angewendeten Lösungen vornehmen, sei es im Rahmen von Beschwerden, Inspektionen, Analysen oder Kontrollen, die von Amtes wegen durchgeführt werden.

1.9.4 Internationale Arbeitsgruppe Datenschutz im Telekommunikationsbereich

Anlässlich der 40. Sitzung der Internationalen Arbeitsgruppe Datenschutz im Telekommunikationsbereich in Berlin wurden unter anderem die Themen Trusted Computing und digitale Rechteverwaltung sowie Internet-Telefonie (VoIP) diskutiert

Im September 2006 hat die Internationale Arbeitsgruppe Datenschutz im Telekommunikationsbereich (International Working Group on Data Protection in Telecommunications) in Berlin ihre 40. Sitzung durchgeführt, an der wir teilgenommen haben. Die Gruppe hat sich unter anderen mit folgenden Themen beschäftigt:

Trusted Computing (TC) /Technologien der digitalen Rechteverwaltung (DRM): In einem Arbeitspapier (http://www.datenschutzberlin.de/doc/int/iwgdpt/WP_Trusted_Computing_en.pdf) empfiehlt die Gruppe, dass Regierungen die Datenschutzrisiken, die bei der Implementierung solcher Technologien entstehen können, beachtet. Die Regierungen sollen Regelungen gegen die Beeinträchtigung der Privatsphäre durch TC/DRM erlassen. Überdies richtet die Gruppe Empfehlungen an die Softwareentwickler und Anbieter von TC/DRM-Produkten, die in ihrem Einflussbereich liegenden Datenschutzmassnahmen zu ergreifen.

Ein weiteres Papier wurde zum Thema Internet-Telefonie (VoIP) verabschiedet und publiziert (http://www.datenschutz-berlin.de/doc/int/iwgdpt/WP_VoIP_en.pdf): Die Nutzung von VoIP hat in letzter Zeit enorm zugenommen. Damit die Sicherheit und die Privatsphäre nicht auf der Strecke bleiben, sind Regulierungen zu treffen, die garantieren, dass bei der Internet-Telefonie mindestens die Datenschutz und -sicherheitsanforderungen implementiert werden, wie sie bei der herkömmlichen Festnetz- und Mobiltelefonie gelten. Unter anderem haben die VoIP-Anbieter bzw. -Hersteller ihre Kundinnen und Kunden auf die Risiken und deren Behebung hinzuweisen, interoperable end-to-end Verschlüsselung anzubieten und nur diejenigen Daten zu bearbeiten, die für die Erbringung des Dienstes oder für gesetzliche Anforderungen notwendig sind.

Alle publizierten Papiere der Gruppe sind auf der Website www.iwgdpt.org abrufbar.

2 Öffentlichkeitsprinzip

2.1 Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung

In der Bundesverwaltung wurde auf den 1. Juli 2006 das Öffentlichkeitsprinzip eingeführt. Es schafft ein einklagbares Recht auf Zugang zu amtlichen Dokumenten. Und es überträgt dem Eidgenössischen Datenschutzbeauftragten neuen Aufgaben: Er wird Beratungs- und Schlichtungsorgan fürs Öffentlichkeitsprinzip und heisst neu Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB).

Das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung, kurz Öffentlichkeitsgesetz (BGÖ) genannt, ist auf den 1. Juli 2006 in Kraft getreten. Damit wird der Wandel vom Geheimhaltungs- zum Öffentlichkeitsgrundsatz vollzogen. Neu können amtliche Dokumente, die seit Inkrafttreten des Gesetzes angefertigt worden sind, auf Gesuch eingesehen werden – vor Ort oder als Kopien. Ein besonderes Interesse muss dabei nicht geltend gemacht werden, ein formloses Gesuch an die zuständige Behörde genügt. Wird der Zugang abgelehnt, kann der Gesuchsteller beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten den Antrag auf ein Schlichtungsverfahren stellen. In seiner Funktion als Schlichtungsstelle strebt der Beauftragte in einem mündlichen oder schriftlichen Verfahren eine rasche Einigung zwischen der betroffenen Behörde und dem Gesuchstellenden an. Kommt es zu keiner Schlichtung, kann der Beauftragte eine Empfehlung abgeben, und dem Gesuchstellenden steht der Rechtsweg offen.

Neben dieser Funktion als Schlichtungsorgan hat der Beauftragte auch Beratungsaufgaben: Er wirkt als Kompetenzzentrum für Behörden und Private für alle Fragen in Zusammenhang mit dem Öffentlichkeitsprinzip und dem Zugang zu amtlichen Dokumenten.

Gemäss Öffentlichkeitsgesetz muss der Beauftragte den Vollzug und die Wirksamkeit dieses Gesetzes sowie insbesondere die durch seine Umsetzung verursachten Kosten überprüfen und dem Bundesrat 3 Jahre nach Inkrafttreten (d.h. auf den 1. Juli 2009) Bericht erstatten. In den ersten 7 Monaten seit Inkrafttreten des Öffentlichkeitsgesetzes sind bei uns 6 Schlichtungsanträge eingegangen. Im Folgenden werden die 3 abgeschlossenen Schlichtungsverfahren kurz erläutert.

2.2 Schlichtungsverfahren im Rahmen des Öffentlichkeitsprizips

2.2.1 Empfehlung an das Bundestrafgericht: „Bericht zu den Vorwürfen betreffend die geringe Anzahl der von der Bundesanwaltschaft erhobenen Anklagen"

Das Öffentlichkeitsgesetz gewährt dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten im Schlichtungsverfahren umfassende Einsichts- und Auskunftsrechte. Das Bundesstrafgericht weigerte sich indessen, uns Einsicht in einen Bericht zu gewähren. Wir mussten die Frage, ob der Bericht unters Öffentlichkeitsgesetz fällt und damit zugänglich ist, offen lassen.

Eine Person beantragte Zugang zu dem vom Bundesstrafgericht erstellten „Bericht zu den Vorwürfen betreffend die geringe Anzahl der von der Bundesanwaltschaft erhobenen Anklagen". Auf ein mündliches Zugangsgesuch wurde ihr geantwortet, dass keine weiteren Angaben gemacht würden, die über die Pressemitteilung zu dieser Sache hinausgingen. Auf ein weiteres, nun schriftliches Gesuch hin wurde ihr mitgeteilt, dass sie zu gegebener Zeit eine Antwort erhalten werde. Nachdem das Bundesstrafgericht die im Öffentlichkeitsgesetz vorgesehene Frist von 20 Tagen zur Stellungnahme ungenutzt hatte verstreichen lassen, reichte die Antragstellerin bei uns einen Schlichtungsantrag ein.

Wir forderten das Bundesstrafgericht auf, uns den besagten Bericht zur Beurteilung der Angelegenheit auszuhändigen. Das Gericht weigerte sich, dies zu tun, und teilte uns u.a. mit, dass der Bericht keinen administrativen Charakter aufweise und daher nicht in den Anwendungsbereich des Öffentlichkeitsgesetzes falle. Somit seien wir in dieser Sache nicht zuständig.

Zur Frage der Zuständigkeit führten wir in unserer Empfehlung u.a. aus, dass wir in Fällen, in denen nicht bereits von Beginn weg zweifelsfrei feststeht, dass das Öffentlichkeitsprinzip nicht zur Anwendung gelangt, auf jeden form- und fristgerecht eingereichten Schlichtungsantrag eintreten. Der Grund dafür liegt in der Konzeption des Öffentlichkeitsgesetzes: Es sieht vor, dass das Schlichtungsverfahren zwingend durchlaufen werden muss, bevor eine Person, welcher der Zugang verweigert worden ist, von der zuständigen Behörde eine Verfügung erwirken und diese in der Folge vor einer gerichtlichen Instanz anfechten kann. Träten wir in Fällen, in denen streitig

ist, ob das Öffentlichkeitsgesetz überhaupt zur Anwendung gelangt, nicht auf einen Schlichtungsantrag ein, so würden wir der antragstellenden Person die Ausübung der ihr nach Öffentlichkeitsgesetz zustehenden Rechte und damit letztlich auch das in der Bundesverfassung vorgesehene rechtliche Gehör (Art. 29 Abs. 2 BV) verweigern.

Die Frage, ob der besagte Bericht unter das Öffentlichkeitsgesetz fällt, konnten wir nicht abschliessend beurteilen, weil sich das Bundesstrafgericht geweigert hatte, uns ein Exemplar des Berichts auszuhändigen. Dies stellt einen klaren Verstoss gegen das Öffentlichkeitsgesetz dar, denn dieses gesteht dem Beauftragten im Rahmen des Schlichtungsverfahrens umfassende Auskunfts- und Einsichtsrechte zu. „Eine Behörde ist verpflichtet, dem Beauftragten alle erforderlichen Dokumente zur Verfügung zu stellen; sie kann sich dieser Verpflichtung nicht unter Berufung auf die Vertraulichkeit oder die geheime Natur der Informationen entziehen" heisst es dazu in den Erläuterungen zur Verordnung zum Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung. Folgerichtig unterstehen der Beauftragte und sein Sekretariat dem Amtsgeheimnis im gleichen Ausmass wie die Behörden, in deren amtliche Dokumente sie Einsicht nehmen oder die ihnen Auskunft erteilen (Art. 20 des Öffentlichkeitsgesetzes).

Der Gesetzgeber hat mit dem Erlass des Öffentlichkeitsgesetzes seinen klaren Willen zum Ausdruck gebracht, dass die Bürgerin und der Bürger Zugang zu amtlichen Dokumenten erhalten sollen. Er hat dem Beauftragten eine wichtige Funktion als eine Art Verbindungs- und Vermittlungsstelle mit entsprechenden Kompetenzen übertragen und ihm damit eine fundamentale Rolle im Verfahren um den Zugang zu Dokumenten zugesprochen (BBl 2003 2029). Der Beauftragte kann diese Aufgabe nicht wahrnehmen, wenn ihm – trotz klarer Gesetzgebung betreffend seiner Einsichts- und Auskunftsrechte – keine Einsicht in besagte Dokumente gewährt wird. Verweigern die dem Öffentlichkeitsprinzip unterliegenden Bundesbehörden und Bundesgerichte dem Beauftragten sein Einsichtsrecht, so bleibt letztlich das Öffentlichkeitsgesetz toter Buchstabe.

Wir empfahlen dem Bundesstrafgericht, das Zugangsgesuch zum besagten Bericht nochmals unter Berücksichtigung aller Aspekte des Öffentlichkeitsgesetzes zu prüfen. Die Empfehlung finden Sie in Anhang 4.7.

2.2.2 Empfehlung an das Bundesamt für Verkehr: „Jahresberichte der Seilbahnbetreiber"

Das Öffentlichkeitsgesetz findet nur Anwendung auf Dokumente, die nach seinem Inkrafttreten erstellt worden sind. Der Zugang zu früher erstellten Dokumenten muss nicht gewährt werden.

Eine Person beantragte beim Bundesamt für Verkehr (BAV) Zugang zu „Meldungen von Seilbahnbetreibern", „bei denen Seilbahnanlagen durch auftauenden Permafrost in Gefahr gerieten und danach dahingehend saniert werden mussten". Sie wünschte Zugang zu allen Dokumenten aus dem Zeitraum von 1991 bis 2006. Das BAV teilte dem Antragsteller mit, dass es keine Listen von gefährdeten Anlagen besitze und im Amt nach dem 1. Juli 2006 keine Dokumente zur „Sanierung von Seilbahnanlagen infolge auftauendem Permafrost" erstellt worden sind. Aus diesen Gründen könne es dem Zugangsgesuch des Antragsstellers nicht nachkommen.

Der Antragsteller reichte bei uns einen Schlichtungsantrag ein und führte an, dass das BAV ihm den Zugang zu den gewünschten amtlichen Dokumenten verweigert hätte.

In unserer Empfehlung stellten wir fest, dass das Öffentlichkeitsgesetz nur auf amtliche Dokumente Anwendung findet, die nach seinem Inkrafttreten, d.h. nach dem 1. Juli 2006, von einer Behörde erstellt oder empfangen wurden. Zudem gilt es zu beachten, dass das Öffentlichkeitsgesetz der gesuchstellenden Person lediglich ein einklagbares Recht auf Einsicht in amtliche Dokumente verschafft. Sie kann gestützt auf das Öffentlichkeitsgesetz jedoch nicht verlangen, dass eine Bundesbehörde ein nicht existierendes Dokument eigens für sie erstellt.

Wir kamen zum Schluss, dass das BAV unter den angeführten Umständen den Zugang zu den gewünschten Dokumenten in Übereinstimmung mit Art. 21 des Öffentlichkeitsgesetzes nicht gewähren musste. Die Empfehlung finden Sie in Anhang 4.8.

2.2.3 Empfehlung an das Eidgenössische Departement für auswärtige Angelegenheiten: „Früherkennung von Risiken im Visabereich"

Wir erachten die vom Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) erstellte Liste betreffend die Früherkennung von Risiken im Visabereich als grundsätzlich zugänglich. Das EDA folgte unserer Empfehlung und gewährte den Zugang.

Das EDA erstellte im Rahmen der Massnahmen gegen den Visamissbrauch in schweizerischen Auslandvertretungen unter anderem eine Liste, um Länder mit besonderen Risiken in diesem Bereich zu identifizieren. Die Liste sollte dazu dienen, besondere Schutzmassnahmen gezielt treffen zu können. Ein Gesuch um Zugang zu dieser Liste lehnte das EDA mit der Begründung ab, dass „eine Veröffentlichung der Liste die Beziehung der Schweiz zu bestimmten Staaten belasten und den aussenpolitischen Spielraum der Schweiz einschränken könnte." Es stützte sich dabei auf eine Ausnahmebestimmung von Art. 7 des Öffentlichkeitsgesetzes. Der Gesuchsteller reichte darauf einen Schlichtungsantrag bei uns ein.

Beim besagten Dokument handelte es sich um eine Liste mit allen schweizerischen Auslandvertretungen, die Visa erteilen. Anhand von sieben Kriterien wurde für jede Vertretung eine Einschätzung der Risiken missbräuchlicher Erschleichung von Visa erstellt. Wir stellten fest, dass die meisten Kriterien der Liste einen Bezug zur öffentlich bereits zugänglichen Visastatistik aufweisen respektive in Zusammenhang mit der Visaerteilung stehen. Anhand dieser Kriterien wurde eine Einstufung der einzelnen schweizerischen Vertretungen, nicht aber einzelner Staaten vorgenommen. Da weder die einzelnen Kriterien noch deren Einstufung Aussagen oder Wertungen über andere Staaten beinhalteten, erachteten wir die Verweigerung des Zugangs hinsichtlich dieser Kriterien als Verstoss gegen das Öffentlichkeitsgesetz.

Lediglich ein Kriterium basierte auf Einschätzungen und Beurteilungen der aktuellen Situation in jenen Staaten, in denen sich die Auslandvertretung befindet. Wir vertraten die Ansicht, die Zugänglichmachung dieses Kriteriums könnte dazu führen, dass die betroffenen Länder darin ein offizielles Werturteil der Schweiz betreffend die Situation in ihren Ländern sehen könnten. Damit bestand zumindest eine erhebliche Wahrscheinlichkeit, dass die Beziehung mit einem oder mehreren Staaten negativ belastet und in der Folge beeinträchtigt werden könnte, wenn das EDA die Liste zugänglich machen würde. Das EDA hatte den Zugang in diesem Punkt zu Recht verweigert.

Wir haben die Empfehlung (Anhang 4.9) erlassen, dass die Liste mit Ausnahme dieses Kriteriums zugänglich gemacht werden sollte. Das EDA folgte dieser Empfehlung.

3 Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte

3.1 Neuer Internetauftritt des EDÖB

Der Bundesrat hat Ende 2003 beschlossen, das Erscheinungsbild aller Bundesstellen zu vereinheitlichen mit dem Ziel, die Identität der Bundesverwaltung zu stärken, deren Transparenz zu verbessern, das Vertrauen in den Staat zu fördern sowie zur Glaubwürdigkeit und Sicherheit der öffentlichen Dienstleistungen des Bundes beizutragen. Auch wir haben unser Erscheinungsbild den neuen Vorgaben angepasst.

Gleichzeitig mit dem Inkrafttreten des Öffentlichkeitsgesetzes (BGÖ) am 1. Juli 2006 und der damit verbundenen Umbenennung von EDSB zu EDÖB haben wir unsere neu gestaltete Website aufgeschaltet. Sie folgt nun den Richtlinien, die die Fachstelle CD Bund im Zuge der Vereinheitlichung des Erscheinungsbildes der Bundesverwaltung ausgearbeitet hat. Selbstverständlich mussten wir uns auch eine neue Internetadresse geben, die die neue Bezeichnung unseres Dienstes enthält und den Vorgaben des CD Bund folgt. So wurde aus www.edsb.ch neu www.edoeb.admin.ch. Alternativ dazu kann die Adresse www.derbeauftragte.ch verwendet werden.

Wir haben die Gelegenheit genutzt, unser Informationsangebot im Internet auszubauen und zu verbessern. Gleichzeitig wollten wir uns aber nicht allzu sehr von der inhaltlichen Struktur unserer alten Website entfernen, um die Benutzerinnen und Benutzer nicht übermässig zu verwirren. Die formale Struktur der Website (Navigation) entspricht derjenigen der übrigen Bundesstellen, ein barrierefreier Zugang zu den Informationen sollte weitestgehend gewährleistet sein.

Eine weitere Neuerung stellt das News-Portal der Bundesverwaltung dar. Die Seite www.news.admin.ch bietet Zugriff auf die Medienmitteilungen und Referate der Bundeskanzlei, der Departemente und deren Dienststellen, also auch des EDÖB. Datenschutzinteressierte können den E-Mail-Abodienst des News-Portals nutzen, um gezielt informiert zu werden, wenn der EDÖB eine Medienmitteilung, Stellungnahme, Ankündigung oder neue Ausgabe des Newsletters datum herausgibt.

Nebst der Website wurde auch unsere gesamte Geschäftskorrespondenz dem neuen Erscheinungsbild des Bundes angepasst.

3.2 Dokumente zum Öffentlichkeitsprinzip auf der Website des EDÖB

Im Juli 2006 trat das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (BGÖ) in Kraft. Das Gesetz fördert die Transparenz in der Bundesverwaltung und sieht umfassende Rechte für Privatpersonen und Firmen zur Einsicht in amtliche Dokumente vor. Im Rahmen dieses Gesetzes hat der EDÖB neue Funktionen übernommen und die Dokumentation auf seiner Website erweitert.

In seiner Botschaft zum Öffentlichkeitsgesetz umriss der Bundesrat die Funktion des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten als die „eines Kompetenzzentrums in Sachen Zugang zu Dokumenten". Um dieser Aufgabe gerecht zu werden und also sowohl Private als auch Bundesämter und Departemente zu beraten, hat der EDÖB eine umfassende Dokumentation zusammengestellt.

Abgesehen von den rechtlichen Grundlagen wie Gesetz und Verordnung und der allgemeinen Einführung ins BGÖ (unter „Themen") bieten wir ein Merkblatt für Gesuchstellerinnen und Gesuchsteller ebenso wie Musterschreiben für das Zugangsgesuch und allfällige Schlichtungsanträge. Zahlreiche FAQs beleuchten verschiedene Aspekte des Zugangs zu amtlichen Dokumenten und helfen zudem, Fragen rund um das Zugangs- oder das Schlichtungsverfahren präzis zu klären. Für die betroffenen Bundesorgane stellen wir zur Vereinfachung der Gesuchsbeantwortung die Leitfäden und Ablaufschemata des Bundesamts für Justiz zur Verfügung.

Kommt es im Rahmen eines Schlichtungsverfahrens nicht zu einer Einigung, erlässt der EDÖB eine Empfehlung. Ganz im Sinne der Transparenz wird diese – anonymisiert – auf der Website veröffentlicht.

3.3 Publikationen des EDÖB - Neuerscheinungen

Wir haben im vergangenen Jahr das Informationsangebot auf unserer Website weiter ausgebaut. Zum Thema Ticketing in Skigebieten haben wir einige Erläuterungen verfasst (unter Themen – Datenschutz – Sonstige Themen, vgl. auch Anhang 4.3). Unter Themen – Datenschutz – Arbeitsbereich wird dargelegt, welche Kompetenzen der Arbeitgeber in der Handhabung von Beweismaterial hat, falls eine angestellte Person unter Verwendung von Internet oder E-Mail gegen das Strafgesetzbuch verstossen hat oder ein entsprechender Verdacht besteht.

Daneben finden sich auf unserer Website neu auch unsere Stellungnahmen zur Übermittlung von SWIFT-Transaktionsdaten an US-Behörden (Themen – Datenschutz – Finanzen sowie Anhang 4.1 dieses Berichts) und zur Verwendung der AHV-Versichertennummer in den Kantonen (Themen – Datenschutz – Sonstige Themen – Ausweise und Register).

Weiter sind im vergangenen Berichtsjahr auch zwei Ausgaben des Newsletters datum erschienen.

Zum Öffentlichkeitsprinzip haben wir auf unserer Website eine umfangreiche Dokumentation zusammengestellt. Vgl. dazu Ziffer 3.2.

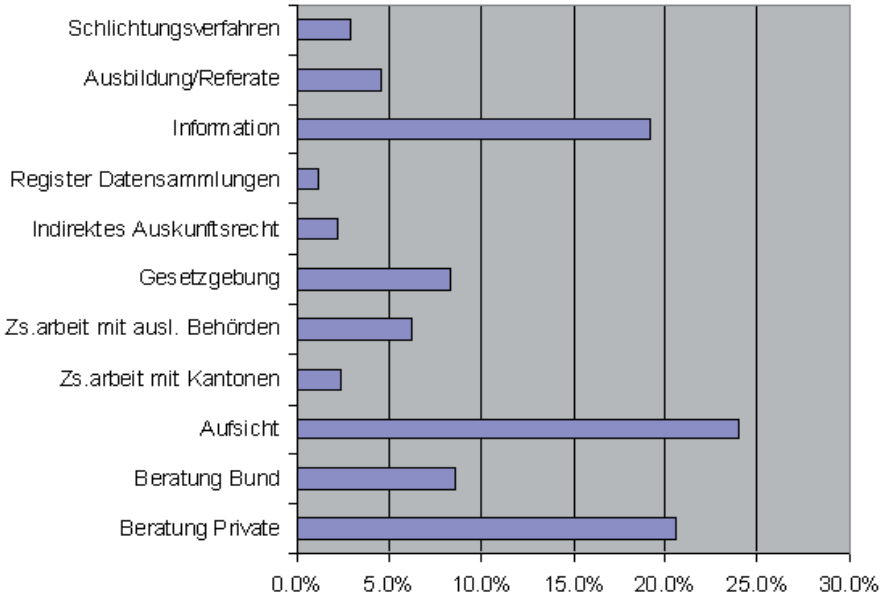
3.4 „Übertreiben wir den Datenschutz?"

Aus Anlass des 1. Europäischen Datenschutztages veranstalteten wir zusammen mit dem Europainstitut an der Universität Zürich (EIZ) am 26. Januar 2007 eine Podiumsdiskussion zum Thema „Übertreiben wir den Datenschutz?" Vor einem grossen Publikum diskutierte Hanspeter Thür mit drei Gästen über aktuelle Fragen des Datenschutzes.

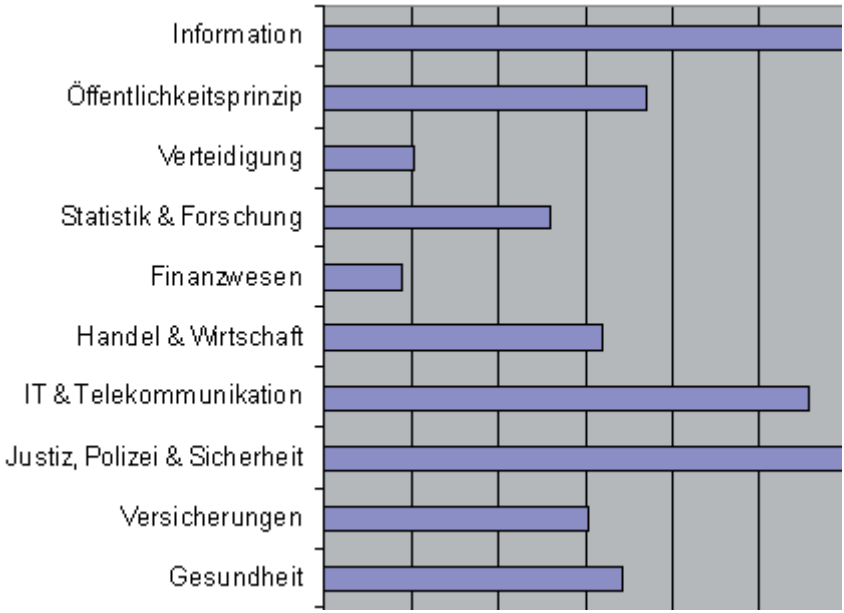
Casper Selg, Leiter der Nachrichtensendung „Echo der Zeit" des Schweizer Radio DRS, führte durch die Veranstaltung mit Anita Thanei, Nationalrätin SP/ZH, Filippo Leutenegger, Nationalrat FDP/ZH, Thomas Pletscher, Geschäftsleitungsmitglied economiesuisse, und Hanspeter Thür, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter. Einigkeit herrschte darüber, dass die technologische Entwicklung und die Terrorbekämpfung auch in den kommenden Jahren grosse datenschützerische Herausforderungen darstellen werden. Während einerseits betont wurde, die Wirtschaft sollte in ihren Datensammlungen möglichst frei sein, dem Staat jedoch müssten enge Grenzen gesetzt werden, forderte Thür anderseits im wirtschaftlichen Bereich mehr Transparenz und plädierte für privatwirtschaftliche Datenschutzzertifizierung. Der EDÖB wies zudem auf die Gefahren hin, die von der Miniaturisierung der Technik ausgehen. Nicht nur der Staat werde künftig von immer besseren und billigeren Mitteln profitieren; mit Minidrohnen, Handykameras, RFID-Chips und anderen Mitteln könne bald jeder jeden überwachen.

3.5 Statistik über die Tätigkeit des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten vom 1. April 2006 bis 31. März 2007

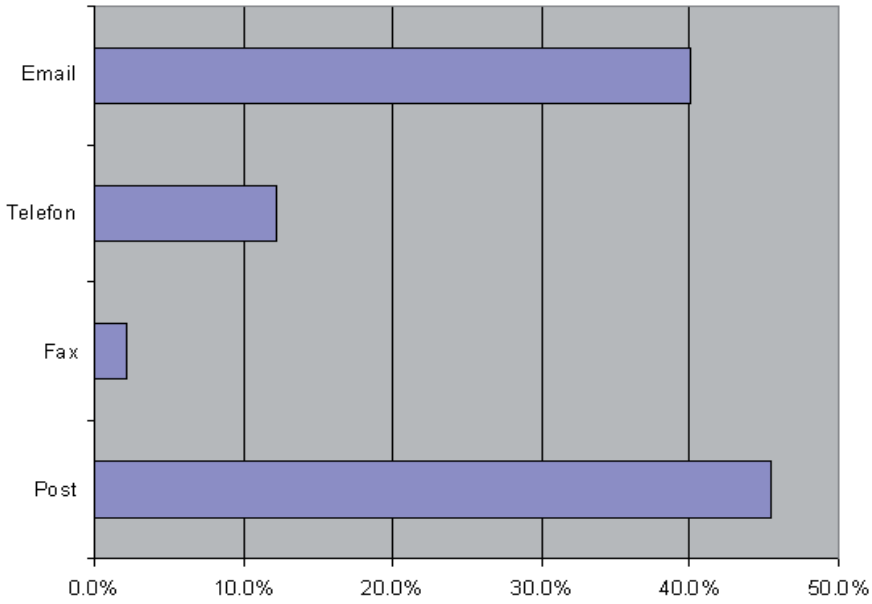
Aufwand nach Aufgabengebiet



Aufwand nach Sachgebiet



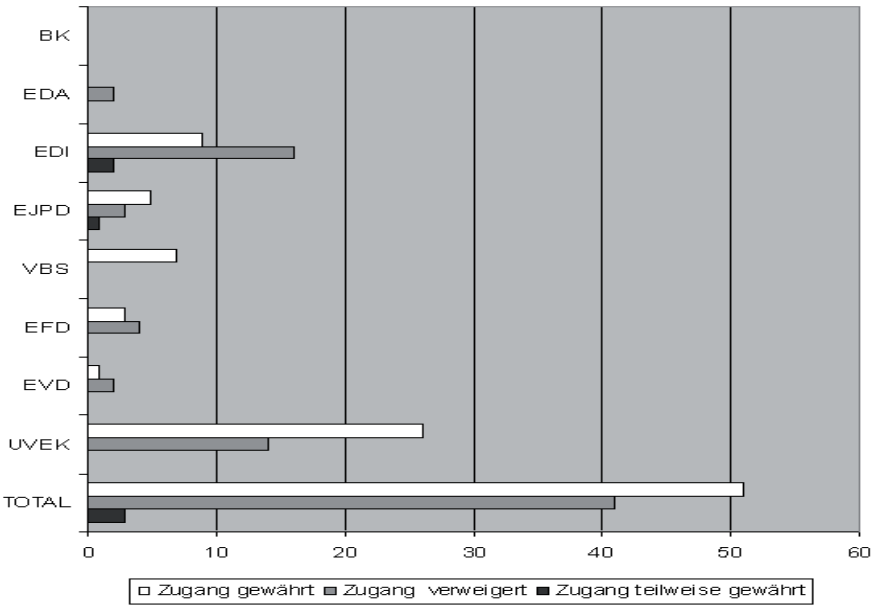
Herkunft der Anfragen



3.6 Statistik über die bei den Departementen eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Juli 2006 bis 31. Dezember 2006)

Departement	Anzahl Gesuche	Zugang gewährt	Zugang verweigert	Zugang teilweise gewährt
BK	0	0	0	0
EDA	2	0	2	0
EDI	27	9	16	2
EJPD	9	5	3	1
VBS	7	7	0	0
EFD	7	3	4	0
EVD	3	1	2	0
UVEK	40	26	14	0
TOTAL	95	51	41	3

Behandlung der Zugangsgesuche



3.7 Das Sekretatiat des EDÖB

Eidgenössischer Datenschutz-und Öffentlichkeitsbeauftragter:

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: 11 Personen

Kanzlei: 3 Personen

4 Anhänge

4.1 Der Zugriff auf Transaktionsdaten der SWIFT – Stellungnahme des EDÖB

I. Einleitung

Der überwiegende Teil des internationalen Zahlungsverkehrs wird über die in Belgien ansässige *Society for Worldwide Interbank Telecommunication* (SWIFT) abgewickelt. Entsprechend ist die seit Juni dieses Jahres in den Medien verbreitete Meldung äusserst brisant, wonach die US-Administration im Rahmen ihrer Anstrengungen zur Terrorbekämpfung Zugriff auf die Transaktionsdaten der SWIFT hat.

Der Datenschutz ist bei der rechtlichen Erfassung dieser Angelegenheit unzweifelhaft einer der zentralen Aspekte. Es haben deshalb die Datenschutzbehörden zahlreicher Länder Abklärungen vorgenommen. Da die SWIFT in Belgien domiziliert ist, kommt namentlich der Untersuchung der dort zuständigen *Commission de la protection de la vie privée* herausragende Bedeutung zu. Die Kommission hat die Resultate ihrer Arbeit am 27.9.2006 veröffentlicht.

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) hat nach Kenntnisnahme der Vorgänge durch die Presse bei den wichtigsten Akteuren des schweizerischen Bankensektors Informationen eingeholt. Die vorliegende Stellungnahme basiert auf der Grundlage der so erlangten Kenntnisse, des Berichtes aus Belgien[1] sowie der Stellungnahme des Bundesrates zuhanden der Geschäftsprüfungskommission des Nationalrates vom 4.7.2006.

Der Bundesrat hat in seinem Papier nicht nur die wichtigsten Fakten aufgearbeitet, sondern im Hinblick auf die Rechtmässigkeitsprüfung der Vorgänge auch die Zuständigkeiten sortiert: Während eine Prüfung auf der Grundlage des Datenschutzgesetzes in der Verantwortung des EDÖB liegt, wäre eine allfällige Verletzung des Bankkundengeheimnisses durch Gerichte zu prüfen[2].

[1] *Avis n° 37 / 2006 du 27 septembre 2006 relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST*. Nachfolgend als ‚*Bericht Belgien*' zitiert und im Volltext abrufbar unter www.privacycommission.be.

[2] Nicht zuständig sind für die Rechtmässigkeitsprüfung im vorliegenden Zusammenhang dagegen gemäss Aussage des Bundesrates die Schweizerische Nationalbank (SNB) sowie die Eidgenössische Bankenkommission (EBK).

Eine weitere Einschränkung des Gegenstandes dieser Stellungnahme ergäbe sich streng juristisch aus dem Territorialitätsprinzip. Gemäss den uns vorliegenden Informationen erfolgt in der Schweiz keine Bearbeitung von Personendaten durch die SWIFT[3]. Damit ist nicht die schweizerische, sondern die belgische Datenschutzgesetzgebung auf die SWIFT anwendbar. Die *Commission de la protection de la vie privée* hat allerdings zu Recht festgestellt, dass angesichts des Zusammenspiels der Akteure (SWIFT und Finanzdienstleister) für die Datenbearbeitung eine geteilte Verantwortung besteht[4].

Konkret stellt sich uns als nationaler Behörde in erster Linie die Frage nach der datenschutzrechtlichen Verantwortung der Finanzdienstleister in der Schweiz. Allerdings gilt es dabei den Gesamtzusammenhang nicht aus den Augen zu verlieren. Es ist daher zum einen vorgängig auf das Verhalten der SWIFT einzugehen. Zum anderen können die Schlussfolgerungen nicht allein auf die Situation in der Schweiz fokussieren. Die Angelegenheit hat eine internationale Dimension; allein auf das Landesrecht beschränkte Forderungen des Datenschutzes sind zur Bewältigung des Problems also nicht ausreichend.

II. Zur Verantwortung der SWIFT

Die SWIFT war im Nachgang zu den Anschlägen in New York mit der Kollision von (letztlich unvereinbaren) Pflichten verschiedener Rechtsordnungen konfrontiert (Belgien, EU, USA). Wie der Bericht aus Belgien aufzeigt, hat die SWIFT entschieden, den Ansprüchen der amerikanischen Rechtsordnung weitgehend stattzugeben. Wiewohl sich die SWIFT in Verhandlungen mit der US-Administration – genauer dem *US Department of the Treasury* – Kontroll- und Einflussmöglichkeiten zu sichern wusste[5], verletzte sie im Ergebnis dennoch in mehreren Punkten belgisches und europäisches Datenschutzrecht[6].

Vor dem Hintergrund der gemeinsamen Verantwortung der SWIFT und der Finanzdienstleister für die Datenschutzkonformität des Zahlungssystems ist der festgestellte Umfang der Pflichtverletzungen der SWIFT auch für die Analyse der Situation in der Schweiz von entscheidender Bedeutung.

[3] Weder die *SWIFT Switzerland GmbH* noch die *SWIFT Switzerland National Member and User Group* haben Aufgaben, die mit der Bearbeitung von Transaktionsdaten der belgischen SWIFT zusammenhängen.
[4] Vgl. *Bericht Belgien*, S. 14 f.
[5] Vgl. *Bericht Belgien*, S. 6 f.
[6] Vgl. *Bericht Belgien*, S. 16 ff.

Der Umstand des Zusammenwirkens mehrerer Akteure spielt namentlich im Kontext der Informationspflichten eine Rolle. Sieht man von der allgemeinen Fragestellung der Rechtmässigkeit des Datenzugriffs durch die US-Administration einmal ab, präsentiert sich als vordergründiges datenschutzrechtliches Problem die fehlende Transparenz dieses Vorgangs für die von der Datenbearbeitung betroffenen Personen. In diesem Punkt muss die gemeinsame Verantwortung für die Datenbearbeitung für SWIFT und Finanzdienstleister auseinander gehalten werden.

Im Zusammenhang mit der Verpflichtung zu transparenter Datenbearbeitung kommt die belgische Behörde zum Schluss, dass die SWIFT die Finanzdienstleister sowie die Datenschutzbehörden über die Anwendung amerikanischer *subpoenas* auf die SWIFT, mithin über die Möglichkeit eines Datenzugriffs durch die US-Behörden, hätte informieren müssen[7].

Vor diesem Hintergrund ist die Frage einer allfälligen Verletzung der Informationspflicht durch die Finanzdienstleister zu prüfen. Dabei darf nicht vergessen werden, dass es innerhalb des Zahlungssystems der SWIFT ausschliesslich die Finanzdienstleister sind, die mit den betroffenen Personen überhaupt in Kontakt stehen. Will man einzelfallweise Transparenz gewährleisten, müssen die Finanzdienstleister also zwingend in die Pflicht genommen werden.

III. Zur Verantwortung der Finanzdienstleister in der Schweiz

Bei der Abwicklung eines Zahlungsvorgangs über ein Finanzinstitut müssen sowohl der Urheber wie auch der Empfänger der Zahlung bekannt sein. Sind in der Schweiz Finanzdienstleister an einem Zahlungsvorgang beteiligt, liegt ohne Weiteres eine Bearbeitung von Personendaten im Sinne des Schweizerischen Datenschutzgesetzes vor (Art. 3 lit. a und e DSG). Damit obliegen den betroffenen Finanzdienstleistern auch sämtliche Pflichten, welche die Datenschutzgesetzgebung für Privatpersonen statuiert (DSG und VDSG).

Wie bereits aufgezeigt, steht innerhalb der denkbaren Pflichtverletzung die Frage nach einer Verletzung der Informationspflicht im Vordergrund. Genauer stellt sich hier die Frage, ob die Finanzdienstleister dem Grundsatz von Treu und Glauben der Datenbearbeitung (Art. 4 Abs. 2 DSG) Genüge tun, beziehungsweise getan haben.

[7] Vgl. *Bericht Belgien*, S. 23 f.

Wie wir bereits zu einem früheren Zeitpunkt betont haben, ist in dieser Frage der Kenntnisstand der Finanzinstitute von entscheidender Bedeutung. Soweit Finanzdienstleister Kenntnis von der Datenweitergabe durch die SWIFT hatten, verpflichtet sie das Datenschutzgesetz dazu, die betroffenen Personen zu informieren. Das gesetzlich statuierte Erfordernis nach transparenter Datenbearbeitung erfüllt nur, wer die betroffenen Personen über nachgelagerte Bearbeitungsschritte informiert[8]. Angesichts der Chronologie eines Zahlungsvorgangs kann die Informationspflicht dabei nur dem überweisenden Finanzdienstleister obliegen.

Wohlgemerkt löst bereits die Kenntnis der *blossen Möglichkeit* der Zugriffnahme auf die SWIFT-Daten durch Dritte eine Informationspflicht aus. Weitergehende Kenntnisse sind dafür nicht nötig, aber offenbar auch nicht möglich. Selbst die Untersuchung der *Commission de la protection de la vie privée* vermochte im Einzelnen nicht zu erhellen, in welchem Umfang die US-Administration Zugriff auf Transaktionsdaten genommen hat[9].

Die Verpflichtung zu transparenter Datenbearbeitung besteht weiterhin. Dass die Öffentlichkeit über die Weitergabe von Daten der SWIFT an die US-Behörden informiert wurde, spielt hier keine Rolle. Es kann nicht als allgemein bekannt vorausgesetzt werden, dass auch nach Aufdeckung der Angelegenheit durch die Medien ein Datentransfer durch die SWIFT weiterhin stattfindet.

Hingegen ist seit der Publikation des Berichts der belgischen Kommission autoritativ festgestellt[10], dass die SWIFT ihre Daten auch in den USA bearbeitet. Damit findet eine Datenweitergabe in ein Land statt, das keinen Datenschutz gewährleistet, der dem schweizerischen gleichwertig ist (Art. 6 Abs. 1 DSG). Die Finanzdienstleister können sich heute nicht mehr darauf berufen, von diesem Umstand keine Kenntnis zu haben.

[8] Die Pflicht zur Schaffung von Transparenz muss auch vor dem Hintergrund gesehen werden, dass zur Abwicklung internationaler Zahlungen Alternativen zum Zahlungssystem der SWIFT bestehen. Vgl. dazu *Bericht Belgien*, S. 3.
[9] Vgl. insbes. Bericht Belgien, S. 6.
[10] In den Medien wurde dieser Umstand bereits früher verschiedentlich erwähnt.

IV. Schlussfolgerungen

- Die belgische Kommission hat auf der Grundlage ihrer Abklärungen mehrere Verletzungen von belgischem und europäischem Datenschutzrecht festgestellt. Vor dem Hintergrund dieser Erkenntnisse ist festzustellen, dass auch das schweizerische Datenschutzrecht verletzt wird. Zum einen wird der Pflicht nach transparenter Datenbearbeitung nicht Genüge getan, zum anderen sind die in Artikel 6 DSG statuierten Erfordernisse nicht erfüllt.
- Wir unterstützen die von der *Commission de la protection de la vie privée* in ihrem Bericht gezogenen Schlussfolgerungen. Eine Lösung, die dem Anliegen der Terrorbekämpfung gerecht wird, aber auch die Datenschutzordnungen der Länder respektiert, die das SWIFT-System nutzen, hätte politischer Verhandlungen bedurft. Aus Sicht des schweizerischen Datenschutzes besteht solcher Handlungsbedarf bis heute.
- Die Forderung nach Schaffung von Transparenz durch die Finanzdienstleister in der Schweiz ist in Anbetracht der Gesamtsituation unzureichend. Analog zur Angelegenheit mit den Flugpassagierdaten muss auch hier auf dem Verhandlungsweg eine Optimierung der Situation angestrebt werden: Anzustreben ist eine Lösung, die sowohl der US-Gesetzgebung Rechnung trägt als auch die europäischen Datenschutznormen respektiert.
- Wir würden es begrüssen, wenn auch die Schweizer Banken, über deren Vertreter in der *SWIFT Ländergruppe Schweiz und Liechtenstein*, die Bemühungen zur Erreichung dieses Resultats nach Kräften unterstützten.
- Im Rahmen unserer Zusammenarbeit mit den europäischen Datenschutzbehörden, namentlich mit der *Artikel 29 Datenschutzgruppe*, werden wir darauf hinwirken, dass eine datenschutzkonforme Lösung erreicht wird, die insbesondere auch den Anforderungen von Artikel 6 DSG gerecht wird.

4.2 Erläuterungen über das Öffnen von privaten E-Mails am Arbeitsplatz

Ausgangslage

Der Arbeitgeber wird häufig mit der Frage konfrontiert, welches seine Kompetenzen in der Handhabung von Beweismaterial sind, falls eine angestellte Person unter Verwendung des Internet oder von E-Mail gegen das Strafgesetzbuch verstossen hat oder ein entsprechender Verdacht besteht. Ein häufig genanntes Beispiel ist dasjenige eines Angestellten, der verdächtigt wird, via E-Mail Fabrikationsgeheimnisse an Dritte weitergegeben zu haben. In diesem Fall muss sich der Arbeitgeber nicht nur die Frage stellen, wie er die Beweisstücke physisch sichern soll, sondern auch, ob er auf diese überhaupt zugreifen darf, um seinen Verdacht zu erhärten. Diese Frage ist insofern von Belang, als Beweise, die unter Verletzung der Persönlichkeit gesammelt worden sind, vom Gericht als unzulässig beurteilt werden können.

Da weder das Fernmeldegeheimnis (Art. 43 Fernmeldegesetz, FMG, SR 784.10) noch die Bestimmungen des Strafgesetzbuches, welche die Verletzung des Schriftgeheimnisses betreffen (Art. 179 Strafgesetzbuch, StGB, SR 311.0), anwendbar sind, kommen zur Klärung der Ausgangsfrage allein das Datenschutzgesetz (DSG, SR 235.1) und das Arbeitsrecht (Art. 328, 328b und 362 Obligationenrecht, OR, SR 220) in Frage.

Zuerst ist festzuhalten, dass es dem Arbeitgeber wegen seiner Pflicht, die Persönlichkeit des Angestellten zu achten (Art. 328 und 328b OR), grundsätzlich nicht zusteht, dessen private E-Mails zu öffnen. Zur geschäftlichen Korrespondenz hat der Arbeitgeber hingegen jederzeit Zugang.

In bestimmten Fällen, insbesondere wenn ein Verdacht auf Verletzung des Strafgesetzbuches unter Verwendung von E-Mail besteht (beispielsweise ein Verdacht auf Verletzung des Berufsgeheimnisses, Art. 320 StGB und Art. 35 DSG), hat der Arbeitgeber das Recht, Beweismaterial zu sichern. Er darf dieses namentlich auf geeignete Weise speichern, insbesondere durch das Erstellen einer physischen Kopie mittels Backup oder Mirroring; der Arbeitgeber stellt also eine Kopie der Originaldateien mit einer zu diesem Zweck geschaffenen Software her.

In einem solchen Fall ist das Sichern von Beweisstücken aber nur durch das überwiegende Interesse des Arbeitgebers und durch das Vorliegen konkreter Anhaltspunkte gerechtfertigt. Solche sind insbesondere dann gegeben, wenn Beweise oder zumindest ein begründeter Verdacht auf eine Verletzung des Strafgesetzbuches vorliegen. Vage Gefühle, Eindrücke, Vermutungen oder der blosse Mangel an Vertrauen gegenüber den Angestellten stellen in der Regel keine ausreichende Grundlage dar, um eine Untersuchung einzuleiten.

Für den Arbeitgeber ist es unbestreitbar schwierig, einzig auf der Grundlage von blossen Vermutungen – und seien diese noch so konkret – zu entscheiden, ob die Einleitung einer Untersuchung angebracht sei. Deshalb hat der Arbeitgeber häufig den Wunsch, zur Überprüfung seines Verdachts private E-Mails der verdächtigten Person zu öffnen, um in Kenntnis des Sachverhalts über die Einleitung einer Untersuchung zu entscheiden. Dass der Arbeitgeber diese Briefe liest, kann übrigens auch im Interesse des verdächtigten Angestellten sein, vermag ihn dies doch unter Umständen vom geäusserten Verdacht zu entlasten und ihm eine (ungerechtfertigte oder schlecht begründete) Anfeindung zu ersparen.

Der Arbeitgeber sollte folglich Zugang zu den privaten E-Mails des Angestellten haben, wenn dies zwingend notwendig ist, um den Verdacht besser zu begründen oder – im Gegenteil – zu zerstreuen und wenn der Einsichtnahme keine überwiegenden Interessen der betroffenen Person entgegenstehen. In diesem Fall ist die betroffene Person jedoch vorgängig zu informieren; sie muss dem Arbeitgeber ihr Einverständnis zum Öffnen privater E-Mails erteilen. Auch das Prinzip der vier Augen muss beachtet werden. Sollte sich die betroffene Person gegen diese Vorgehensweise aussprechen, empfehlen wir, die Verantwortung für das Aufnehmen von Beweisen, insbesondere für das Öffnen privater E-Mails, den Untersuchungsbehörden zu überlassen. Diese gewährleisten eine professionelle und neutrale Untersuchung, die Integrität des Beweismaterials dank der beteiligten Spezialisten (forensic computing scientists) sowie die Respektierung des Rechts, namentlich der Bestimmungen, welche die Überwachung am Arbeitsplatz betreffen (insbesondere Art. 59 Abs. 1 Bst. a Arbeitsgesetz, ArG, SR 822.11, sowie Art. 26 der Verordnung 3 zum Arbeitsgesetz, ArGV3, SR 822.113). Beweismaterial, das der Arbeitgeber unter Missachtung dieser Normen gesammelt hat, wird vom Gericht möglicherweise nicht zugelassen.

Wir sind ferner der Ansicht, dass Beweismaterial, welches der Arbeitgeber durch seinen Zugriff auf private E-Mails des verdächtigten Angestellten gesammelt hat, vor Gericht ausnahmsweise in den folgenden Fällen zugelassen werden kann: wenn überwiegende Interessen des Arbeitgebers dies erfordern (z.B. im Fall eines Notstands, Art. 34 StGB) oder wenn eine superprovisorische Massnahme des Richters nicht ausreichen würde, damit das Beweismaterial sichergestellt werden kann.

Falls das kantonale Recht die alleinige Kompetenz der Untersuchungsbehörden zum Öffnen privater E-Mails vorsieht, so ändert das Einverständnis des Angestellten nichts an dieser Tatsache. Die Wirkungslosigkeit der Willensbekundung seitens des Angestellten ergibt sich einerseits aus dem Vorrang des kantonalen Rechts vor einer privaten Willensbekundung; andererseits könnte ein derartiges Einverständnis, zumindest im hier besprochenen Fall, dem Angestellten schaden. Auch aus diesem Grund ist das Einverständnis des Arbeitnehmers als juristisch nicht zwingend einzustufen (siehe Art. 362 und 328 OR).

4.3 Erläuterungen zum Ticketing in Skigebieten

Zunehmend ausgeklügeltere Zugangskontrollsysteme in Wintersportgebieten wecken datenschützerische Bedenken. Wo die Snowboarderinnen und Skifahrer vor Jahren noch mittels einfacher Lochkarten kontrolliert wurden, kommen heute elektronische Kontrollsysteme zum Einsatz. Im Umgang mit den Personendaten der Wintersportlerinnen und -sportler müssen die Datenschutzprinzipien eingehalten werden.

Beim Kauf eines Abonnements für die Benutzung von Wintersportanlagen müssen Kundinnen und Kunden ein Passfoto ab- und Personalien bekannt geben. Dies sind so genannte Personendaten. Die Sammlung und Weiterverarbeitung dieser Daten durch den Betreiber der Anlagen stellt eine Datenbearbeitung im Sinne des Datenschutzgesetzes (DSG) dar, dessen rechtliche Grundsätze berücksichtigt werden müssen. Nun bedienen sich die Betreiber von Wintersportanlagen zunehmend elektronischer Zugangskontrollsysteme, installiert jeweils an den Talstationen der Bahnen. Passiert der Kunde die Schranke, erscheint das Foto des Abonnementsinhabers auf einem Bildschirm. Einerseits ermöglicht dieses System zu kontrollieren, ob Inhaber und Träger des Abonnements identisch sind, anderseits kann so die Gültigkeit der Abonnemente geprüft werden. Diese Kontrolle wird im Normalfall vom Personal der Wintersportstation vorgenommen. In einigen Skigebieten jedoch ist dieser Bildschirm auch für Dritte sichtbar, die sich in der Nähe des Kontrollpunktes aufhalten. Die persönlichen Daten des Abonnementsinhabers erscheinen auf dem Bildschirm und sind bei gewissen Anlagen so lange zu sehen, bis der nächste Kunde den Kontrollpunkt passiert. Das kann mehrere Minuten dauern.

Zunächst hält der EDÖB fest, dass jede Person prinzipiell ein Recht auf Achtung ihrer Privatsphäre und insbesondere auf den Schutz ihrer Identität gegenüber Dritten hat, auch und gerade im Rahmen ihrer Freizeitaktivitäten. Eine allfällige Bearbeitung von Personendaten erfordert deshalb einen Rechtfertigungsgrund. Als solcher gilt ein Gesetz, aber auch ein überwiegendes privates oder öffentliches Interesse oder die Einwilligung der betroffenen Personen. Selbst bei Vorliegen eines Rechtfertigungsgrundes müssen zudem die allgemeinen Prinzipien des Datenschutzes (Zweckbindung, Treu und Glauben, Verhältnismässigkeit) gewährleistet sein. Dazu gehört, gemäss Transparenzprinzip, auch die Information der Abonnementsinhaberinnen und -inhaber über den Zweck und die Modalitäten der Bearbeitung ihrer Personendaten.

Nun stellt sich die Frage, ob der Betreiber einer Wintersportstation für die Anzeige von Personendaten auf einem Bildschirm, der auch für Dritte sichtbar ist, einen Rechtfertigungsgrund geltend machen kann – ob eine solche Zurschaustellung also gemäss Datenschutzgesetz rechtmässig ist. Dazu hält der EDÖB folgendes fest: Im vorliegenden Fall existiert kein Gesetz, und es kann auch kein überwiegendes öffentliches Interesse geltend gemacht werden. Bleiben als Rechtfertigungsgründe ein überwiegendes privates Interesse oder die Einwilligung der Betroffenen.

Zweifellos hat der Betreiber einer Wintersportanlage ein legitimes und prinzipiell überwiegendes Interesse daran, die Gültigkeit der Abonnemente zu prüfen und insbesondere zu kontrollieren, dass Dritte nicht unerlaubterweise nicht-übertragbare Abonnemente benutzen. Zu diesem Zweck darf er ein elektronisches Zugangskontrollsystem einsetzen, wobei die allgemeinen Grundsätze des Datenschutzes respektiert werden müssen. Folgende Überlegungen sind entscheidend:

- Der EDÖB bezweifelt, dass die öffentliche Anzeige auf dem Bildschirm der Kontrolle der Gültigkeit der Abonnemente dienlich ist. Es ist nicht Sache der anderen Kundinnen und Kunden, anstelle des Personals zu kontrollieren, dass kein Missbrauch stattfindet. Vielmehr scheint der Einsatz solcher Systeme darauf abzuzielen, eventuelle Missetäter abzuschrecken.
- Grundsätzlich muss im Rahmen des Möglichen die Massnahme gewählt werden, die den Schutz der Privatsphäre am wenigsten gefährdet (Verhältnismässigkeitsprinzip). Die öffentliche Anzeige von Personendaten kann eine nicht vernachlässigbare Beeinträchtigung der Privatsphäre der Betroffenen bedeuten. Im vorliegenden Fall ist eine solche Massnahme nicht verhältnismässig, denn es existieren mindestens ebenso effiziente und zudem datenschutzkonforme Kontrollmöglichkeiten, so z.B. die systematische oder sporadische Kontrolle durch Angestellte. Dazu dürfen Bildschirme jedoch nur dem Personal zugänglich sein.
- Zudem muss bedacht werden, dass auch im Falle eines Missbrauchs nicht die Personendaten des Missetäters gezeigt werden, sondern die des Abonnementsinhabers, der unter Umständen mit dem Missbrauch gar nichts zu tun hat, also unschuldig exponiert wird.

Die Betreiber von Wintersportanlagen können sich also auch nicht auf ein überwiegendes privates Interesse als Rechtfertigung für die Zurschaustellung von Personendaten vor unbeteiligten Dritten berufen. Bleibt als Rechtfertigungsgrund einzig die Zustimmung der betroffenen Personen. Hierzu betont der EDÖB, dass die Zustimmung frei und aufgeklärt erfolgen muss. D.h., der Kunde oder die Kundin muss ein Recht haben, die Bearbeitung der eigenen Personendaten abzulehnen, ohne Nachteile zu erfahren. Die Kommunikation der Personendaten müsste also fakultativ sein, was technisch möglich wäre, praktisch aber den Kontrollabsichten der Betreiber zuwiderläuft.

Fazit: Die öffentliche Anzeige von Foto und Identität der Benutzerinnen und Benutzer von Wintersportanlagen ist nicht mit dem Eidgenössischen Datenschutzgesetz vereinbar. Es gibt andere Mittel, die nicht so tief in die Privatsphäre einschneiden, um die Gültigkeit von Abonnementen zu prüfen und Missbräuche zu verhindern, so z.B. systematische oder sporadische Abonnementskontrollen, wie wir sie von öffentlichen Verkehrsmitteln kennen. Unter den gegebenen Umständen ist die Kommunikation von Personendaten an Drittpersonen nicht nötig und unverhältnismässig.

Im Falle einer widerrechtlichen Persönlichkeitsverletzung haben Betroffene Klagemöglichkeiten nach Art. 15 DSG.

4.4 Erklärung von London

„Datenschutz vermitteln und effektiver gestalten“

Ursprung dieser Initiative

Dieser Bericht hat seinen Ursprung in der Rede von Alex Türk, dem Vorsitzenden der französischen Datenschutzbehörde (CNIL), anlässlich einer im Mai 2006 vom polnischen Generalinspektor für Datenschutz in Warschau abgehaltenen Konferenz zum Thema „Öffentliche Sicherheit und Schutz der Privatsphäre“. Alex Türk sprach über seine ernste Besorgnis angesichts der Herausforderungen, denen die Datenschutzbehörden zurzeit gegenüberstehen. Er betonte, dass die Datenschutzbehörden ihre Aktivitäten dringend auf diese Herausforderungen ausrichten müssten, da andernfalls Gefahr bestehe, dass die den Datenschutzbestimmungen zugrunde liegende Philosophie in kürzester Zeit an Gehalt verliere.

Im Anschluss an die Konferenz lud der Europäische Datenschutzbeauftragte (EDPS) den CNIL ein, eine gemeinsame Initiative ins Leben zu rufen, um die Notwendigkeit dieser dringlichen Maßnahmen bei der Konferenz in London zu präsentieren. Der britische Datenschutzbeauftragte gab der Initiative sofort volle Unterstützung. Vorliegender Bericht wurde in enger Zusammenarbeit der drei genannten Datenschutzbehörden erstellt.

Durch ihren Beitritt zu dieser Initiative verpflichten sich die teilnehmenden Datenschutzbehörden, ihre Aktivitäten im Hinblick auf die folgenden Ziele zu koordinieren:

- Entwicklung von Kommunikationsaktivitäten auf der Grundlage gemeinsamer Ideen, von denen einige in beigefügtem Text zum Ausdruck gebracht werden
- Anpassung der eigenen Verfahrensweisen und Methoden durch eingehende Beurteilung ihrer Effektivität und Effizienz sowie durch Ausweitung ihrer Kapazitäten in den Bereichen technische Kompetenz, Trendprognose und Intervention im technologischen Bereich
- Beitrag zur institutionellen Anerkennung von Datenschutzbehörden auf internationaler Ebene und Förderung der Einbeziehung anderer relevanter Interessenvertreter auf nationaler und internationaler Ebene.

Zum gegenwärtigen Zeitpunkt haben die folgenden Datenschutzbehörden bestätigt, diese Initiative grundsätzlich zu unterstützen:

- Commission nationale de l'informatique et des libertés (Frankreich)
- European Data Protection Supervisor (Europäische Union)
- Information Commissioner (Großbritannien und Nordirland)
- Privacy Commissioner of Canada (Kanada)
- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (Deutschland)
- Agencia Española de Protección de Datos (Spanien)
- Garante per la Protezione dei Dati Personali (Italien)
- College Bescherming Persoonsgegevens (Niederlande)
- Privacy Commissioner (Neuseeland)
- Préposé fédéral à la protection des données et à la transparence (Suisse) / Eidgenössische Datenschutz und Öffentlichkeitsbeauftragte (Switzerland)

Die gemeinsame Initiative wird während der geschlossenen Sitzung der Internationalen Konferenz der Datenschutzbeauftragten in London am 2.-3. November präsentiert. Sie ist nicht als Beschluss formuliert. Das Dokument wird als gemeinsame Initiative des französischen, europäischen und britischen Datenschutzbeauftragten präsentiert, unterstützt von den oben genannten Datenschutzbehörden, die sich auf diese Weise verpflichten, die Initiative in ihren Aktivitäten zu berücksichtigen. Die anderen bei der Konferenz vertretenen Datenschutzbehörden werden eingeladen, ihre Unterstützung der Initiative zum Ausdruck zu bringen oder auch beizutreten, wenn sie dies wünschen. Sie werden nicht aufgefordert, dieses Dokument offiziell zu verabschieden.

Nach einer einführenden Erinnerung, warum Datenschutz für unsere Gesellschaften unerlässlich ist (I), analysiert der Text im Einzelnen die Bedrohungen, denen persönliche Freiheiten und Datenschutz heute weltweit ausgesetzt sind und die ebenso viele Herausforderungen für die Aufsichtsbehörden darstellen (II). Aus den Ausführungen werden verschiedene Vorschläge für koordinierte Aktivitäten und Initiativen hergeleitet (III), wie auch für die Entwicklung einer neuen Kommunikationsstrategie (IV).

I. DATENSCHUTZ IST FÜR DIE GESELLSCHAFT UNERLÄSSLICH

1. Für die Gesellschaft ist der Schutz der Personendaten ihrer Bürger unerlässlich. Er steht auf gleicher Ebene wie die Presse- und die Bewegungsfreiheit. Da unsere Gesellschaften zunehmend auf Informationstechnologie angewiesen sind und immer mehr Personendaten erhoben oder erstellt werden, ist es wichtiger als je zuvor, dass individuelle Freiheiten und andere legitime Interessen der Bürger durch geeignete Datenschutzpraktiken auf angemessene Weise respektiert werden.

2. Datenschutz ist kein abstraktes, theoretisches, ganz zu schweigen ein „theologisches" Thema und darf nicht als solches betrachtet werden. Bestimmungen zum Datenschutz dienen dem Schutz des Einzelnen. Sie zielen auf die Wahrung des Rechts ab, nicht auf missbräuchliche oder unkontrollierte Weise erfasst oder überwacht zu werden. Sie zielen auf die Verteidigung der menschlichen Würde ab und sollen den Einzelnen in die Lage versetzen, seine Rechte auszuüben und seine legitimen Interessen zu schützen.

3. Datenschutz kann nur dann Realität werden, wenn Datenschutzbestimmungen in der Praxis befolgt werden. Datenschutzbehörden spielen eine wichtige Rolle, indem sie dafür sorgen, dass die Bestimmungen eingehalten werden. Sie können aber nur dann erfolgreich sein, wenn sie das Thema Datenschutz auf effektive Weise vermitteln, andere relevante Interessenvertreter involvieren und – falls nötig – ihre Ermittlungs- und Durchsetzungsrechte auf effektive Weise ausüben.

II. ZWEI GEFAHRENWELLEN, DREI HERAUSFORDERUNGEN

4. Die Freiheit des Einzelnen, aber auch die Datenschutzbehörden selbst sind bislang nicht da gewesenen Risiken ausgesetzt. Sie sind der Bedrohung unterworfen, von zwei Gefahrenwellen überrollt zu werden, stehen aber zusätzlich noch vor einer dritten Herausforderung.

A. Die erste Herausforderung gründet sich auf viele unterschiedliche Faktoren, die mit dem Tempo technologischer Veränderungen in Zusammenhang stehen

5. **Beschleunigung:** Internet, RFID, Nanotechnologien etc. Datenschutzbehörden sind Innovation und technologischem Fortschritt gegenüber nicht feindlich eingestellt. Aber der Zeitraum von der Entdeckung eines Phänomens bis zu dessen technischer Umsetzung, von einer Innovation zur nächsten, von der Entwicklung eines Prototyps bis zu dessen industrieller Anwendung wird kürzer und kürzer. Versuche zur Gesetzesanpassung und Gesetzgebung können immer weniger mit

der technologischen Entwicklung Schritt halten. Das Tempo der technologischen Entwicklung wird immer schneller, während das Tempo der Gesetzgebung nach wie vor sehr langsam ist, da es an den von demokratischen Verfahrensweisen auferlegten Rhythmus angepasst ist.

6. **Globalisierung:** Die örtliche Verlagerung der Datenverarbeitung steht in voller Blüte. Es lässt sich wohl kaum bestreiten, dass der internationale Datentransfer sehr schwer zu kontrollieren ist. Dieser Trend hin zur Globalisierung steht im Konflikt mit einem der Hauptmerkmale der Rechtsstaatlichkeit – ihrer geografisch beschränkten Anwendbarkeit.

7. **Ambivalenz:** Technologische Innovation bringt sowohl Fortschritt als auch Gefahren mit sich. Für den Einzelnen mögen die aus Technologie erwachsenden Vorteile und Bequemlichkeiten eine große Verlockung darstellen, die Risiken werden ihm vielleicht jedoch erst dann bewusst, wenn er oder jemand anders zu Schaden gekommen und es zu spät ist. Vielen Menschen ist es egal, dass alle ihre Bewegungen, Aktivitäten und Beziehungen nachvollzogen und potenziell überwacht werden können. Diese Zwiespältigkeit gegenüber der Technologie lässt sich nur schwer mit der Rechtsstaatlichkeit vereinbaren, die definitionsgemäß fest umrissene Antworten geben möchte.

8. **Unvorhersehbarkeit:** Die Anwendung neuer Technologien entwickelt sich manchmal in Richtungen, die anfangs selbst von den Entwicklern der Technologie nicht vorhergesehen wurden. Diese nicht vorhersehbaren Einsatzmöglichkeiten können schwer zu kontrollieren sein, insbesondere wenn die Anwendung einer Technologie von den ursprünglich geplanten Einsatzmöglichkeiten – auf die das Gesetz einfach anwendbar erschien – völlig abweicht.

9. **Unsichtbarkeit** (virtuelle Unsichtbarkeit/körperliche Unsichtbarkeit): Die Datenverarbeitung ist immer weniger sichtbar und greifbar, gleichzeitig auch immer weniger kontrollierbar. Moderne Technologien tendieren zu Unsichtbarkeit, erstens, weil ein großer Teil der Datenverarbeitung stattfindet, ohne dass sich der Einzelne ihrer Existenz bewusst ist (z. B. Nachverfolgbarkeit der Nutzung öffentlicher Verkehrsmittel, des Surfverhaltens im Internet, der elektronischen Kommunikation, der Telefonkommunikation usw.). Da die Prozesse unsichtbar sind, kann man hier von virtueller Unsichtbarkeit sprechen. Technologie wird aber auch unsichtbar aufgrund ihrer extremen Miniaturisierung, die man als körperliche Unsichtbarkeit bezeichnen kann. In ein paar Jahren wird die Entwicklung von Nanotechnologien dazu führen, dass man die in einem Gegenstand enthaltene Technologie mit dem bloßen Auge nicht mehr erkennen kann. Wie will man Verarbeitungsprozesse überwachen, die von unsichtbaren Technologien ausgeführt werden?

10. **Irreversibilität**: Technologischer Fortschritt lässt sich nicht umkehren: Wir werden nie wieder in einer Welt ohne Computer, Internet, Handys, biometrischer Identifizierung, Geolokalisierung und Videoüberwachung leben. In dem Maße, wie diese Technologien konvergieren und immer stärker miteinander verwoben werden, können sie in ihrer Gesamtheit eine echte Gefahr für unsere Gesellschaft darstellen.

B. Die zweite Herausforderung ist gesetzlicher Art, insbesondere in Bezug auf die neuen Antiterrorgesetze

11. Der Erlass von Antiterrorgesetzen bedeutet eine Herausforderung für die Datenschutzbehörden, die in diesem Zusammenhang Fallen vermeiden, Illusionen aufgeben und Mythen bekämpfen müssen.

12. **Die Notwendigkeit von Ausgewogenheit:** Unabhängige Datenschutzbehörden sind weder Gesetzgeber noch Gerichtshöfe noch Aktivisten, spielen aber dennoch eine äußerst spezifische Rolle. In den seltensten Fällen ist es ihnen möglich, Probleme auf klar umrissene Weise zu lösen. Alle Datenschutzbehörden erkennen die Legitimität von Antiterrorgesetzen an, wie sie in den vergangenen Jahren entwickelt wurden. Vor dem Hintergrund des Auftrags, den die Datenschutzbehörden vom Gesetz erhalten haben, und im Auftrag der Gesellschaft insgesamt ist es jedoch ihre Pflicht, kontinuierlich nach dem richtigen Gleichgewicht zwischen den Erfordernissen der öffentlichen Sicherheit einerseits und der Notwendigkeit des Datenschutzes und des Schutzes der Privatsphäre andererseits zu streben. Sie müssen diese Rolle vollkommen unabhängig erfüllen und die inakzeptablen Anschuldigungen verantwortungslosen Handelns von sich weisen, die gelegentlich gegen sie vorgebracht werden.

13. **Die Gefahr, in einen Teufelskreis zu geraten:** Dieses Risiko – eine Art „schleichende Funktionsausweitung" – sieht folgendermaßen aus: Eine Datenbank wird zu einem bestimmten Zeitpunkt in einer bestimmten Situation angelegt. Die Aufsichtsbehörde ist in die Entwicklung der Datenbank involviert. Zu einem späteren Zeitpunkt erweitert sich der Wirkungsbereich dieser Datenbank. Beispielsweise werden zunächst die Kategorien der erfassten Personen erweitert, dann die Gründe, warum jemand registriert werden kann, später wiederum die Kategorien der Personen, die Zugriff auf die Datenbank haben. In diesen späteren Phasen steht die Behörde dem Argument gegenüber, dass sie eine einfache Erweiterung nicht verweigern kann, da sie das Prinzip zur Erstellung der ursprünglichen Datenbank akzeptiert hat, und so weiter. Und dies, obwohl der ursprünglich akzeptierte Umfang des Systems zwischen der ersten und der letzten Entwicklungsphase so stark vergrößert wurde, dass er nicht länger akzeptabel ist.

14. **Das Trugbild der mustergültigen Natur von Präzedenzfällen in anderen Ländern:** Landesregierungen bringen als Angriff auf die landeseigene Datenschutzbehörde häufig das Argument vor, dass ein anderes Land bereits ein bestimmtes System eingeführt hat, wenn diese sich sträubt, ein in anderen Ländern verwendetes System diskussionslos zu akzeptieren. Dies führt zu ernsten Harmonisierungsproblemen und dazu, dass die Datenschutzbehörden einen gemeinsamen Nenner finden und gemeinsam nachdenken müssen.

15. **Die Illusion der Datenbank als Allheilmittel:** Die Datenschutzbehörden müssen Öffentlichkeit und Regierung fortwährend daran erinnern, dass durch die Schaffung von Datenbanken mit immer mehr Personendaten nicht alle Probleme gelöst werden können. Der „Glorienschein" der angeblich unfehlbaren Computerdatei erweist sich häufig als Illusion. Außerdem steigt mit der Verarbeitung von immer mehr Personendaten auch das Risiko falscher Zuordnungen, veralteter Informationen und anderer Fehler. Dies kann den Lebenschancen, der Gesundheit, dem Wohlstand und selbst der Freiheit des Einzelnen ernstlich schaden.

16. **Der Mythos der unfehlbaren Datei (das „Mehrheits-/Minderheitsproblem"):** Nur allzu häufig wird völlig unfundiert angenommen, dass wir alle aus gutem Grund in einer Datenbank erfasst werden – mit dem Ergebnis, dass sich Personen, die unnötig oder unangemessen erfasst werden („die Minderheit"), gelegentlich in unmöglichen Situationen wiederfinden, da jeder der Ansicht ist, es sei praktisch unmöglich, in einem derart effizienten System grundlos erfasst zu werden. Aus diesem Grund ist es aus ethischer Sicht äußerst wichtig, immer wieder darauf hinzuweisen, dass Technologie nicht unfehlbar ist, und die automatische Entscheidungsfindung, insbesondere in Bereichen wie Sicherheit und Recht, zu verbieten.

C. Bei der dritten Herausforderung geht es um den Ruf

17. Zumindest in einigen Ländern genießen Datenschutz und Datenschutzbehörden nicht den guten Ruf, den sie verdienen. Es kann die Auffassung herrschen, dass die Bestimmungen komplex sind und sich in der Praxis nur schwer auf konsequente, vorhersehbare und realistische Weise umsetzen lassen. Manche kritisieren die Kontrolle des Datenschutzes als übertrieben abstrakt und nicht ausreichend auf tatsächliche und potenzielle Gefahren ausgerichtet, die sowohl für den Einzelnen als auch für die Gesellschaft insgesamt erwachsen, wenn die Bestimmungen nicht beachtet werden. Andere kritisieren die Art und Weise, in der diese Bestimmungen umgesetzt und durchgesetzt werden, und den Mangel an positiven oder negativen Anreizen zur Einhaltung der Bestimmungen oder zur Investition in angemessene Maßnahmen. Negative Auffassungen wie diese werden von Politi-

kern, Verwaltungsbeamten, Unternehmen, den Medien und manchmal auch von Privatpersonen vertreten. Es ist wichtig, gegen derartige Ansichten vorzugehen, die praktische Bedeutung des Datenschutzes aufzuzeigen, die viel besprochenen Grundrechte und Grundfreiheiten zur Realität zu machen und die derzeitigen Praktiken – sofern angemessen – zu überdenken.

III. AUFGABEN UND INITIATIVEN FÜR DATENSCHUTZBEHÖRDEN

18. Die Datenschutzbehörden müssen dringend Maßnahmen ergreifen, um in ihren Bürgern ein gesteigertes Bewusstsein und ein besseres Verständnis der ernsten Risiken zu wecken, die ihre persönlichen Freiheiten in ihrem jeweiligen Land bedrohen. Sie müssen ferner ihre Arbeitsmethoden und ihre Effizienz und Effektivität überdenken.

A. Die Datenschutzbehörden müssen gemeinsam Änderungen und koordinierte Strategien vorbringen, um so auf neue, effektivere und sachdienlichere Weise zu handeln

19. **Stärkung der Kapazitäten in den Bereichen Fachwissen, fortgeschrittene Studien und Intervention im Technologiesektor:** Der Datenschutz leidet zurzeit unter seinem übermäßig „rechtsbetonten" Image. Die Glaubwürdigkeit unserer Institutionen hängt jedoch schon heute und auch in Zukunft immer mehr von unserer Fähigkeit ab, technologische Entwicklungen zu verstehen, zu analysieren und vorherzusehen.

20. Zur Analyse dieser neuen Trends müssen die Datenschutzbehörden Strategien erarbeiten, um sich die Arbeit abhängig vom jeweiligen Fall, ihren Erfahrungen, Zuständigkeiten und praktischen Maßnahmen zu teilen.

21. Sie müssen überlegen, welche Beziehungen sie im Bereich neue Technologien zu Forschung und Industrie aufbauen wollen. Sie müssen die Vorteile eines guten Datenschutzes gegenüber Wirtschaft und öffentlichen Körperschaften betonen.

22. **Beurteilung unserer Effektivität und Änderung unserer Praktiken:** Wir müssen unbedingt eine detaillierte und ehrliche Beurteilung der Effektivität einer jeden Behörde durchführen. Zeigt die Arbeit der jeweiligen Behörde wirklich Auswirkungen, erreicht sie etwas in der Praxis? Werden Worte in Taten umgesetzt? Durch derartige Beurteilungen lernen wir, wie wir unsere Ergebnisse verbessern können.

23. Die Beurteilung der Effektivität aller Behörden wird sicherlich dazu führen, dass einige von ihren Gesetzgebern verlangen, sie mit ausreichend Befugnissen und Mitteln auszustatten. Möglicherweise werden auch Fragen zu den Praktiken einiger Behörden aufgeworfen. Wir alle müssen Prioritäten setzen, insbesondere was Gefahr und Schwere eines möglichen Unheils anbelangt. Wir müssen uns primär auf die Hauptrisiken konzentrieren, denen der Einzelne ausgesetzt ist, und vorsichtig sein, dass wir bei Angelegenheiten, die es nicht verdienen, nicht übermäßig puristisch und rigide vorgehen. Wir müssen zu größerem Pragmatismus und mehr Flexibilität bereit sein.

B. Datenschutzbehörden müssen gemeinsam überlegen, wie sie auf internationaler Ebene eine bessere institutionelle Anerkennung ihrer Aktivitäten erzielen und andere Interessenvertreter involvieren können

24. **Eine notwendige Umstrukturierung der Internationalen Konferenz:** Globale Herausforderungen brauchen globale Lösungen. Die Internationale Konferenz der Datenschutzbeauftragten muss an der Spitze unserer Aktivitäten auf internationaler Ebene stehen. Wir müssen für die Lebens- und Existenzfähigkeit der Konferenz sorgen, ihre Funktionsweise verbessern, sie sichtbarer und effizienter machen und einen Aktionsplan – ein Kommunikationsprogramm – erarbeiten. Dazu gehört möglicherweise, dass wir darüber nachdenken, ein permanentes Sekretariat für die Konferenz einzurichten. Die Konferenz muss zu einem unvermeidbaren Gesprächspartner bei allen internationalen Initiativen werden, die einen Einfluss auf den Datenschutz haben. Sie muss Raum für Gespräche bieten und Vorschläge aufkommen lassen, damit internationale Initiativen besser verfolgt, Praktiken aufeinander abgestimmt und gemeinsame Standpunkte bezogen werden.

25. **Ausarbeitung einer internationalen Konvention und anderer globaler Instrumente:** In der Erklärung von Montreux (2005) forderten die Datenschutzbeauftragen eine universelle Konvention für den Datenschutz. Diese Initiative muss von den Datenschutzbehörden mit den zuständigen Institutionen unterstützt werden, mit gebührlichem Respekt für deren institutionelle Position und ggf. für die notwendigen Vorbedingungen einer landesinternen Koordination. Innerhalb dieses Rahmenwerks sollten sich die Datenschutzbehörden bemühen, die Initiative in ihrem jeweiligen Einflussbereich voranzutreiben, vor allem innerhalb der regionalen Organisationen und der Sprachzonen, in denen sie tätig sind. In bestimmten Sektoren (z. B. Internetkontrolle, Finanztransaktionen, Flugverkehr) kann die Notwendigkeit globaler Lösungen zur Respektierung von Privatsphäre und Datenschutz entstehen, worauf die Datenschutzbehörden mit allen geeigneten Mitteln eingehen müssen.

26. **Involvierung anderer Interessenvertreter (Einrichtungen der Zivilgesellschaft, Nichtregierungsorganisationen usw.):** Zurzeit sind sowohl national als auch international diverse andere Interessenvertreter für den Datenschutz und den Schutz der Privatsphäre aktiv, auf unterschiedlichen Ebenen und in unterschiedlichen Sektoren. Derartige Organisationen können als strategische Partner agieren und wesentlich dazu beitragen, dass die Datenschutzbehörden effektiver werden. Die Kooperation mit anderen geeigneten Interessenvertretern sollte daher gefördert oder aktiv entwickelt werden.

IV. EINER NEUEN KOMMUNIKATIONSSTRATEGIE ENTGEGEN

27. Kommunikation ist eine Hauptvoraussetzung, um Datenschutz effektiver zu machen. Eine Botschaft, die nicht ankommt und nicht verstanden wird, ist im Grunde genommen nicht existent. Eine Meinung oder Entscheidung, auf die sich nicht zugreifen lässt, ist in ihrer Wirkung begrenzt und möglicherweise nicht die auf ihre Ausarbeitung verwendete Mühe wert.

A. Wir müssen dringend eine neue Kommunikationsstrategie entwickeln, sowohl auf nationaler als auch auf internationaler Ebene

28. **Kommunikation als Ziel.** Eine sehr viel bessere Kommunikation mit der Öffentlichkeit muss eines der Hauptziele aller Datenschutzbehörden sein. Es ist inakzeptabel, dass in einigen Ländern, in denen das Recht auf Datenschutz – ebenso wie die Bewegungs- und Pressefreiheit - zu den Grundrechten gehört, die große Mehrheit unserer Mitbürger sich dieser Rechte und ihrer Bedeutung nicht bewusst ist. Noch viel weniger akzeptabel ist dies, wenn eine negative Einstellung gegenüber dem Datenschutz herrscht.

29. Wir müssen wirkungsvolle Kampagnen zur langfristigen Bewusstseinssteigerung ins Leben rufen, die den Einzelnen über die Existenz und den Inhalt seiner Rechte informieren. Die Wirksamkeit dieser Maßnahmen muss gemessen werden. Dabei gibt es zwei spezifische Ziele:

    - Gewählte Vertreter auf landesweiter und kommunaler Ebene – die meisten von ihnen sind nicht besser informiert als der Durchschnittsbürger.
    - Junge Menschen, die wenig Interesse an diesen Fragen haben, da sie so sehr an neue Technologien gewohnt sind. Wir müssen so bald wie möglich im Bereich der Bildung und Aufklärung aktiv werden.

30. **Kommunikation als wirkungsvolles Hebelwerkzeug.** Es ist wichtig und dringlich, dass unsere Datenschutzbehörden bessere Handlungsmittel erhalten und Anerkennung auf internationaler Ebene zugesichert bekommen. Öffentliches Vertrauen und Unterstützung sind unerlässlich. Datenschutz muss konkreter gemacht werden. Nur Organisationen, die kommunizieren – normalerweise über die Medien und auf eine Art und Weise, die für die Öffentlichkeit insgesamt **bedeutungsvoll, zugänglich und relevant** ist – werden die Macht erhalten, die erforderlich ist, um die öffentliche Meinung zu beeinflussen, und somit von den Staaten und der internationalen Gemeinde gehört und ernst genommen zu werden. Nur wenn diese Bedingung erfüllt wird, können die Datenschutzbehörden unverzichtbare Handlungsmittel erhalten.

31. Das bedeutet, dass wir in allen unseren Behörden professionelle Kommunikationspartner einsetzen, und dass die vermittelten Botschaften in allen Datenschutzbehörden möglichst einheitlich sind.

B. Eine interessante Kommunikationsbotschaft könnte im Aufzeigen einer Parallele zwischen dem Schutz der persönlichen Freiheiten und dem Schutz der Umwelt liegen

32. Was die Umwelt anbelangt, so werden wir nicht ungestraft davonkommen. Auf die gleiche Weise müssen wir im Bereich des Datenschutzes bei jeder unkontrollierten technologischen Entwicklung und jedem Gesetz, das ohne klare Vision der potenziellen Risiken erlassen wird, höchste Vorsicht walten lassen. In einem solchen Fall besteht die Gefahr, dass unser „Kapital" in Form von Freiheit und Identität reduziert oder sogar zunichte gemacht wird. Auch kann es nicht wiedergewonnen werden, und zwar genau deshalb, weil technologische Innovation irreversibel ist.

33. Möglicherweise sind Datenschutz und der Schutz der Privatsphäre genauso kostbar wie die Luft, die wir atmen. Beide sind unsichtbar, aber ihr Verlust ist gleichermaßen mit katastrophalen Folgen verbunden.

V. PROGRAMM ANSCHLIESSENDER AKTIVITÄTEN

34. Die Besprechung dieser Initiative bei der geschlossenen Sitzung der Internationalen Konferenz der Datenschutzbeauftragten in London sollte als erster Schritt in Richtung eines wachsenden Konsenses gesehen werden – eines Konsenses über die Notwendigkeit zur Ausarbeitung von Mitteln für bessere Kommunikation und effektiveren Datenschutz.

35. Datenschutzbehörden, die diese Initiative unterstützen, verpflichten sich zur Weiterentwicklung von und übernehmen ggf. die Verantwortung für eine Reihe von Aktivitäten, die bei der nächsten Konferenz in Montreal vorgestellt und weiter verfolgt werden, z. B.:

- Workshop zu strategischen Themen: Bedingungen, um Datenschutzbehörden effektiver zu machen; mögliche Entwicklung von „Prinzipien einer gutenÜberwachung" beim Datenschutz; Informationen zu Best Practice (Datenschutzbeauftragte und strategische Mitarbeiter); Überlegungen hinsichtlich der Entwicklung einer internationalen Konvention
- Workshop zum Thema Kommunikation: Verfügbares Expertenwissen im Bereich der Datenschutzkommunikation (z. B. Kampagnen, Meinungsforschung); Entwicklung einer gemeinsamen Botschaft und wirksamer Hilfsmittel für deren Verbreitung (professionelle Kommunikationspartner)
- Workshop zum Thema Durchsetzung: Verfügbares Expertenwissen im Bereich Überwachung und Gewährleistung der Vorschriftenbefolgung; wirksame Mechanismen zur Inspektion (z. B. Audits) und Intervention (Datenschutzbeauftragte und Personal von Durchsetzungsbehörden)
- Workshop zur internen Organisation: Jüngste Erfahrungen mit organisatorischen Veränderungen; Projekte zur Verbesserung von Effizienz und Effektivität (Datenschutzbeauftragte und organisatorisches Personal)
- Alle sonstigen Aktivitäten, die für diese Initiative als relevant erachtet werden

4.5 Entschliessung betreffend die praktischen Organisationsmodalitäten der Konferenz

Siehe Abschnitt 4.5 im französischen Teil des Berichtes

4.6 Resolution zum Datenschutz bei Suchmachinen[1]

673.18.2 (Übersetzung aus dem englischen, 27. Oktober 2006)

28. Internationale Konferenz der Datenschutzbeauftragten
London, Vereinigtes Königreich
2. und 3. November 2006

Vorgeschlagen von: Berliner Beauftragter für Datenschutz und Informationsfreiheit, Deutschland

Unterstützer: Deutschland (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit), Irland (Datenschutzbeauftragter), Norwegen (Datatilsynet), Polen (Generaldirektor für den Schutz personenbezogener Daten)

Resolution[2]

Heutzutage sind Suchmaschinen zum Schlüssel zum „cyberspace" geworden, um in der Lage zu sein, Informationen im Internet aufzufinden, und damit ein unverzichtbares Werkzeug.

[1] Diese Resolution bezieht sich nicht auf Suchfunktionen, die von Inhalteanbietern für ihre eigenen Angebote angeboten werden. Für den Zweck dieser Resolution wird „Suchmaschine" definiert als ein Service zum Auffinden von Ressourcen im Internet über verschiedene Websites hinweg und basierend auf nutzerdefinierten Suchbegriffen.

[2] Diese Resolution betrifft nicht Probleme, die durch die Praxis vieler Betreiber von Suchmaschinen aufgeworfen werden, Kopien des Inhalts von Internetseiten einschließlich darauf enthaltener personenbezogener Daten, die dort legal oder illegal veröffentlicht werden, zu speichern und zu veröffentlichen („caching").

Anbieter von Suchmaschinen haben die Möglichkeit, detaillierte Interessenprofile ihrer Nutzer aufzuzeichnen. IP-Protokolldaten, besonders wenn sie mit den entsprechenden Daten kombiniert werden, die bei Zugangsdiensteanbietern gespeichert sind, erlauben die Identifikation von Nutzern. Da die Nutzung von Suchmaschinen heutzutage unter den Internet-Nutzern eine gängige Praxis ist, erlauben die bei den Anbietern populärer Suchmaschinen gespeicherten Verkehrsdaten, ein detailliertes Profil von Interessen, Ansichten und Aktivitäten über verschiedene Sektoren hinweg zu erstellen (z. B. Berufsleben, Freizeit, aber auch über besonders sensible Daten, z. B. politische Ansichten, religiöse Bekenntnisse, oder sogar sexuelle Präferenzen).

Die Datenschutzbeauftragten sind bereits in der Vergangenheit hinsichtlich der Möglichkeit zur Erstellung von Profilen über Bürger besorgt gewesen[3] Die im Internet verfügbare Technologie macht diese Praxis jetzt in einem gewissen Umfang auf globaler Ebene technisch möglich.

Jüngste Entwicklungen haben noch einmal ein Schlaglicht auf die wachsende Bedeutung der gesammelten Daten geworfen, sowie auf ihre Eigenschaft als personenbezogene oder zumindest personenbeziehbare Daten: Im Frühjahr 2006 forderte das Justizministerium der Vereinigten Staaten von Amerika von Google, Inc. die Herausgabe von Millionen von Suchanfragen für ein Gerichtsverfahren, das unter anderem den Schutz vor der Verbreitung von kinderpornographischen Inhalten im Internet zum Gegenstand hatte. Google weigerte sich, dieser Aufforderung nachzukommen und gewann letztendlich das Verfahren. Im weiteren Verlauf desselben Jahres publizierte AOL eine Liste von beinahe 20 Millionen scheinbar anonymisierten Suchanfragen, die ungefähr 650.000 AOL-Nutzer über einen Zeitraum von drei Monaten in die AOL-Suchmaschine eingegeben hatten. Laut Presseberichten konnten daraus einzelne Nutzer auf der Basis des Inhalts ihrer Suchanfragen identifiziert werden. Diese Liste war – obwohl sie von AOL nach harscher Kritik, die ihre Veröffentlichung unmittelbar zur Folge hatte, zurückgezogen wurde – zum Zeitpunkt des Zurückziehens Berichten zufolge bereits vielfach heruntergeladen und neu publiziert, und in suchbarer Form auf einer Anzahl von Websites verfügbar gemacht worden.

Es muss darauf hingewiesen werden, dass nicht nur Verkehrsdaten personenbezogene Informationen darstellen können, sondern auch der Inhalt von Suchanfragen.

[3] Vgl. z. B. den gemeinsamen Standpunkt zu Datenschutz und Suchmaschinen (zuerst verabschiedet auf der 23. Sitzung in Hongkong SAR, China ,15. April 1998, überarbeitet und aktualisiert bei der 39. Sitzung, 6. – 7. April 2006, Washington D. C.) der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation; http://www.datenschutzberlin.de/doc/int/iwgdpt/search_engines_de.pdf. Vgl. ebenfalls Kapitel 5: „Surfen und Suchen" des Arbeitsdokuments der Artikel-29-Gruppe „Privatsphäre im Internet" – ein integrierter EU-Ansatz zum Online-Datenschutz"; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpddocs/2000/wp37de.pdf.

Diese Entwicklung unterstreicht, dass Daten über zurückliegende Suchvorgänge, die von Anbietern von Suchmaschinen gespeichert werden, bereits jetzt in vielen Fällen personenbezogene Daten darstellen. Insbesondere in Fällen, in denen Anbieter von Suchmaschinen gleichzeitig auch andere Dienste anbieten, die zur einer Identifikation des Einzelnen führen (z. B. E-Mail), können Verkehrsund Inhaltsdaten über Suchanfragen mit anderen personenbezogenen Informationen kombiniert werden, gewonnen aus diesen anderen Diensten innerhalb derselben Sitzung (z. B. auf der Basis des Vergleichs von IP-Adressen). Der Prozentsatz von Daten über Suchanfragen, die auf Einzelpersonen zurückgeführt werden können, wird vermutlich in der Zukunft weiter ansteigen wegen der Zunahme der Nutzung fester IP-Nummern in Hochgeschwindigkeits-DSL oder anderen Breitbandverbindungen, bei denen die Computer der Nutzer ständig mit dem Netz verbunden sind. Er wird noch weiter ansteigen, sobald die Einführung von Ipv6 abgeschlossen ist.

Dies und die zunehmende Bedeutung von Suchmaschinen für das Auffinden von Informationen im Internet führt zunehmend zu erheblichen Gefährdungen der Privatsphäre der Nutzer von Suchmaschinen.

Empfehlungen

Die Internationale Konferenz fordert die Anbieter von Suchmaschinen auf, die grundlegenden Regeln des Datenschutzes zu respektieren, wie sie in der nationalen Gesetzgebung vieler Länder sowie auch in internationalen Politikdokumenten und Verträgen (z. B. den OECD-Richtlinien zum Datenschutz, der Konvention 108 des Europarates, dem APEC Regelungsrahmen zum Datenschutz, und den Datenschutzrichtlinien der Europäischen Union) niedergelegt sind:

1. Unter anderem sollten Anbieter von Suchmaschinen ihre Nutzer im Vorhinein in transparenter Weise über die Verarbeitung von Daten bei der Nutzung der jeweiligen Dienste informieren.

2. Im Hinblick auf die Sensibilität der Spuren, die Nutzer bei der Nutzung von Suchmaschinen hinterlassen, sollten Anbieter von Suchmaschinen ihre Dienste in einer datenschutzfreundlichen Art und weise anbieten. Insbesondere sollten sie keine Informationen über eine Suche, die Nutzern von Suchmaschinen zugeordnet werden können, oder über die Nutzer von Suchmaschinen selbst aufzeichnen. Nach dem Ende eines Suchvorgangs sollten keine Daten, die auf einen einzelnen Nutzer zurückgeführt werden können, gespeichert bleiben, außer der Nutzer hat seine ausdrückliche, informierte Einwilligung dazu gegeben, Daten, für die Erbringung eines Dienstes die notwendig sind, speichern zu lassen (z. B. zur Nutzung für spätere Suchvorgänge).

3. In jedem Fall kommt der Datenminimierung eine zentrale Bedeutung zu. Eine solche Praxis würde sich auch zugunsten der Anbieter von Suchmaschinen auswirken, die sich zunehmend Forderungen nach der Herausgabe nutzerspezifischer Informationen durch Dritte ausgesetzt sehen.[4]

4. Die Internationale Konferenz fordert die Betreiber von Suchmaschinen auf, den international anerkannten Standard für den Schutz personenbezogener Daten Folge zu leisten (z. B. die OECD-Datenschutzrichtlinien von 1980, Konvention 108 des Europarates, oder die EU-Richtlinie 95/46) und gegebenenfalls ihre Praktiken entsprechend zu ändern.

[4] Für den Zweck dieser Erklärung bedeutet „Dritter" jede natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle außer der betroffenen Person, dem für die Verarbeitung Verantwortliche, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsdatenverarbeiters befugt sind, die Daten zu verarbeiten.

4.7 Empfehlung an das Bundestrafgericht: „Bericht zu den Vorwürfen betreffend die geringe Anzahl der von der Bundesanwaltschaft erhobenen Anklagen“

Bern, den 22. September 2006

Empfehlung

gemäss

Art. 14 des
Bundesgesetzes über das
Öffentlichkeitsprinzip der Verwaltung
vom 17. Dezember 2004

zum Schlichtungsantrag von

X

(Antragstellerin)

gegen

Schweizerisches Bundesstrafgericht, Bellinzona

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Die Beschwerdekammer des Bundesstrafgerichts hat am 17. Juli 2006 in einer Medienmitteilung darüber informiert, dass sie ihren „Bericht zu den Vorwürfen betreffend die geringe Anzahl der von der Bundesanwaltschaft erhobenen Anklagen" abgeschlossen hat. In der kurzen Medienmitteilung heisst es unter anderem, dass der Bericht „die aufgrund der getroffenen Abklärungen dafür massgeblichen Gründe" aufzeigt und sämtlichen Behörden zugestellt wurde, die für die Bereinigung der Situation zuständig sind. Am Ende der Medienmitteilung wird darauf hingewiesen, dass weitere Auskünfte zum Bericht seitens der Beschwerdekammer nicht erteilt werden.

2. Die Antragstellerin bittet das Generalsekretariat des Bundesstrafgerichts am 17. Juli 2006 (Tag der Publikation der Pressemitteilung) „mündlich um genauere Auskunft über den Inhalt des Berichts" (Zitat aus dem Zugangsgesuch, Beilage zum Schlichtungsantrag vom 13. August 2006 an den Beauftragten, s. unten Ziffer 5). Das Generalsekretariat antwortet darauf, dass keine Angaben gemacht werden, „die über den kurzen Inhalt des Communiqués" (Zitat Schlichtungsantrag) hinausgehen.

3. Am gleichen Tag richtet die Antragstellerin eine E-Mail an das Generalsekretariat des Bundesstrafgerichts mit der Bitte, ihr Einblick in den Bericht zu gewähren, da die Erkenntnisse der Beschwerdekammer „von einem eminenten öffentlichen Interesse" (Zitat Zugangsgesuch) sind. Die Antragstellerin verweist in ihrer E-Mail auch auf das am 1. Juli 2006 in Kraft getretene Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ, SR 152.3) und beruft sich insbesondere auf Art. 8 Abs. 5 BGÖ, gemäss dem der Zugang zu Berichten über die Evaluation der Leistungsfähigkeit der Bundesverwaltung und die Wirksamkeit ihrer Massnahmen gewährleistet ist.

4. Das Generalsekretariat des Bundesgerichts teilt der Antragstellerin umgehend per E-Mail mit, dass sie auf ihre „Anfrage betreffend Einsicht in den Bericht (…) zu gegebener Zeit eine Antwort erhalten" wird.

5. Die Antragstellerin hat mit Schreiben vom 13. August 2006 beim Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) einen Schlichtungsantrag nach Art. 13 BGÖ eingereicht (eingegangen am 15. August 2006). Die Antragstellerin führt an, dass das Bundesstrafgericht die im Öffentlichkeitsgesetz vorgesehene Frist von 20 Tagen zur Stellungnahme unbenutzt hat verstreichen lassen, und dass Art. 8 Abs. 5 BGÖ den Zugang zu Berichten über die Evaluation der Leistungsfähigkeit der Bundesverwaltung und die Wirksamkeit ihrer Massnahmen gewährleist.

6. Am 17. August 2006 informiert der Beauftragte das Bundesstrafgericht über den Schlichtungsantrag und fordert von ihm die Zustellung des „Berichts zu den Vorwürfen betreffend die geringe Anzahl der von Bundesanwaltschaft erhobenen Anklagen" und eine schriftliche Begründung, weshalb das Bundesstrafgericht der Gesuchstellerin den Zugang zum Bericht verweigert hat.

7. Mit Schreiben vom 21. August 2006 teilt das Bundesstrafgericht dem Beauftragten Folgendes mit:

   - Das Bundesstrafgericht vertritt die Ansicht, dass der Bericht keinen administrativen Charakter aufweist („questo rapporto non sia di carattere amministrativo") und somit das Öffentlichkeitsgesetz nicht anwendbar ist.
   - Das Reglement vom 20. Juni 2006 des Bundesstrafgerichts (Inkrafttreten am 1. Januar 2007) sieht vor, dass kein Schlichtungsverfahren durch den Beauftragten durchgeführt wird und dass bis zu seinem Inkrafttreten Art. 18 des Reglements über die Archivierung beim Bundesstrafgericht (SR 152.12) analog zur Anwendung gelangt.
   - Das Bundesstrafgericht erachtet daher den Beauftragten in dieser Angelegenheit als nicht zuständig.
   - Das Bundesstrafgericht hat die Antragstellerin mehrmals mündlich auf diese Sachlage aufmerksam gemacht und aufgefordert, ein formelles, schriftliches Gesuch einzureichen.

8. In Telefongesprächen, die der Beauftragte am 21. August 2006 und 8. September 2006 mit dem Bundesstrafgericht geführt hat, hielt letzteres an seiner Haltung (oben Ziffer 7) fest und bekräftigte, dass es stets die Absicht des Bundesstrafgerichts gewesen ist, das Schlichtungsverfahren durch den Beauftragten auszuschliessen. Im Anschluss an das Telefonat vom 8. September 2006 stellt das Bundesstrafgericht dem Beauftragten das auf den 1. Januar 2007 in Kraft tretende Reglement über das Bundesstrafgericht per E-Mail zu, das namentlich den Ausschluss des Schlichtungsverfahrens durch den Beauftragten vorsieht.

II. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte zieht in Erwägung:

A. Schlichtungsverfahren gemäss Art. 14 BGÖ

1. Gemäss Art. 13 BGÖ kann eine Person einen Schlichtungsantrag beim Beauftragten einreichen, wenn die Behörde den Zugang zu amtlichen Dokumenten einschränkt, aufschiebt oder verweigert, oder wenn die Behörde innert der vom Gesetz vorgeschriebenen Frist keine Stellungnahme abgibt.

   Der Beauftragte wird nicht von Amtes wegen, sondern nur auf Grund eines schriftlichen Schlichtungsantrages tätig (BBl 2003 2023). Berechtigt, einen Schlichtungsantrag einzureichen, ist jede Person, die an einem Gesuchsverfahren um Zugang zu amtlichen Dokumenten teilgenommen hat. Für den Schlichtungsantrag genügt einfache Schriftlichkeit. Aus dem Begehren muss hervorgehen, dass sich der Beauftragte mit der Sache befassen soll. Der Schlichtungsantrag muss innert 20 Tagen nach Empfang der Stellungnahme oder nach Ablauf der der Behörde für die Stellungnahme zur Verfügung stehenden Frist schriftlich eingereicht werden.

2. Die Antragstellerin hat ein Zugangsgesuch nach Art. 6 BGÖ beim Bundesstrafgericht eingereicht und innert der vom Gesetz vorgeschriebenen Frist keine Stellungnahme erhalten. Als Teilnehmerin an einem vorangegangenen Gesuchsverfahren ist sie zur Einreichung eines Schlichtungsantrags berechtigt. Der Schlichtungsantrag wurde formgerecht (einfache Schriftlichkeit) und fristgerecht (innert 20 Tagen nach Ablauf der der Behörde für die Stellungnahme zur Verfügung stehenden Frist) beim Beauftragten eingereicht.

3. Im Rahmen des Schlichtungsverfahrens werden beide Seiten angehört und es kommt idealtypisch zu einer gegenseitigen Annäherung der Positionen. Das Anhörungsverfahren kann auf schriftlichem Weg oder konferenziell unter Leitung des Beauftragten stattfinden. Die Festlegung des Verfahrens im Einzelnen obliegt alleine dem Beauftragten (BBl 2003 2024).

4. Aus dem Schlichtungsantrag der Antragstellerin geht klar hervor, dass sie Zugang zum Bericht haben möchte. Währenddessen beharrt das Bundesstrafgericht auf der Position, dass der Beauftragte in der vorliegenden Angelegenheit nicht zuständig ist und die Erstellung des besagten Berichts nicht als Teil der administrativen Aufgabenerfüllung zu bewerten ist.

   Der Beauftragte gelangt im Rahmen der Abklärungen zum Schluss, dass eine Schlichtung aufgrund der unvereinbaren Positionen aussichtslos ist. Gemäss Art. 14 BGÖ ist der Beauftragte somit gehalten, aufgrund seiner Einschätzung und Beurteilung der Angelegenheit eine Empfehlung abzugeben.

5. In Fällen, in denen nicht bereits von Beginn weg zweifelsfrei feststeht, dass das Öffentlichkeitsprinzip nicht zur Anwendung gelangt, tritt der Beauftragte auf jeden form- und fristgerecht eingereichten Schlichtungsantrag ein und prüft, ob die Bearbeitung des Zugangsgesuchs durch die Behörde angemessen und rechtmässig erfolgt ist (Art. 12 der Verordnung über das Öffentlichkeitsprinzip der Verwaltung VBGÖ, SR 152.31).

6. Die Konzeption des Öffentlichkeitsgesetzes sieht vor, dass das *Schlichtungsverfahren zwingend durchlaufen* werden muss, bevor eine Person, welcher der Zugang verweigert worden ist, von der zuständigen Behörde eine Verfügung erwirken und diese in der Folge vor einer gerichtlichen Instanz anfechten kann. Tritt der Beauftragte in Fällen, in denen streitig ist, ob das Öffentlichkeitsgesetz überhaupt zur Anwendung gelangt, nicht auf einen Schlichtungsantrag ein, so verweigert er der antragstellenden Person die Ausübung der ihr nach Öffentlichkeitsgesetz zustehenden Rechte (insbes. Art. 15f. BGÖ) und damit letztlich auch das rechtliche Gehör (Art. 29 Abs. 2 BV).

B. Anwendung des Öffentlichkeitsprinzips durch das Bundesstrafgericht

1. Der Geltungsbereich des Öffentlichkeitsgesetzes umfasst die Bundesverwaltung, die Parlamentsdienste und Personen des öffentlichen oder privaten Rechts, die nicht der Bundesverwaltung angehören, soweit sie Erlasse oder erstinstanzlich Verfügungen im Sinn von Art. 5 des Bundesgesetzes über das Verwaltungsverfahren (Verwaltungsverfahrensgesetz, SR 172.021) erlassen (Art. 2 BGÖ).

2. Das Bundesgesetz über das Bundesstrafgericht (Strafgerichtsgesetz SGG, SR 173.71) wurde auf Inkrafttreten des Öffentlichkeitsgesetzes folgendermassen ergänzt:

Art. 25a Grundsatz der Öffentlichkeit
[1] Das Öffentlichkeitsgesetz vom 17. Dezember 2004 gilt sinngemäss für das Bundesstrafgericht, soweit dieses administrative Aufgaben erfüllt.
[2] Das Bundesstrafgericht bezeichnet ein Beschwerdeorgan, das über Beschwerden gegen seine Verfügungen betreffend den Zugang zu amtlichen Dokumenten entscheidet. Es kann vorsehen, dass kein Schlichtungsverfahren durchgeführt wird; in diesem Fall gilt seine Stellungnahme zu einem Gesuch um Zugang zu amtlichen Dokumenten als beschwerdefähige Verfügung.

Das Öffentlichkeitsgesetz findet auf die Bundesstrafgerichte sinngemäss Anwendung. So hat der Gesetzgeber entschieden, dass die Verwaltungstätigkeit der Bundesgerichte (Justizverwaltung) ebenfalls dem Öffentlichkeitsprinzip unterstellt ist. Ausgenommen bleiben davon aber amtliche Dokumente, welche die Rechtsprechung betreffen.

Aufgrund der besonderen Stellung der Bundesgerichte hat der Gesetzgeber in Bezug auf das Schlichtungsverfahren eine Ausschlussmöglichkeit und in Bezug auf Streitfälle eine vom Öffentlichkeitsgesetz abweichende Regelung vorgesehen.

Mit Inkrafttreten der neuen Bundesrechtspflegegesetze auf den 1. Januar 2007 wird die Bestimmung erneut eine Anpassung erfahren. Künftig ist das Bundesgericht Beschwerdeorgan für Verfügungen des Bundesstrafgerichts. Konsequenterweise entfällt damit der erste Satz des aktuellen Absatzes 2. Im Übrigen erfährt der Wortlaut der Bestimmung keine Änderung.

C. Administrative Aufgabenerfüllung

1. Das Öffentlichkeitsprinzip findet nur Anwendung, soweit das Bundesstrafgericht administrative Aufgaben erfüllt (Art. 25a SGG). Nicht dem Öffentlichkeitsprinzip unterworfen sind demnach amtliche Dokumente wie Akten aus einem Strafverfahren und Urteile des Gerichts. Zentral im vorliegenden Schlichtungsverfahren ist daher die Beurteilung der Frage, ob der besagte Bericht dem Bereich der administrativen Aufgabenerfüllung oder der Rechtsprechung des Bundesstrafgerichts zuzuordnen ist.

2. Das Bundesstrafgericht vertritt die Meinung, dass es sich beim Bericht um ein Dokument aus dem Bereich seiner Aufsichtstätigkeit über die Bundesanwaltschaft handelt und verweist in diesem Zusammenhang auf Art. 28 SGG. Diese Bestimmung regelt die Zuständigkeit der Beschwerdekammer. Sie entscheidet u.a. über Beschwerden gegen Amtshandlungen oder Säumnis des Bundesanwalts und der eidgenössischen Untersuchungsrichter in Bundesstrafsachen (Art. 28 Bst. a SGG). Die Beschwerdekammer ist demnach Aufsichtsorgan über die Bundesanwaltschaft.

3. Da der Beauftragte vom Bundesstrafgericht keine weiteren Ausführungen zum Bericht erhalten hat, muss er eine Einschätzung aufgrund der wenigen ihm zur Verfügung stehenden Informationen vornehmen.

4. Das besagte Dokument trägt den Titel „Bericht zu den Vorwürfen betreffend die geringe Anzahl der von der Bundesanwaltschaft erhobenen Anklagen". Gemäss Medienmitteilung stellt das Bundesstrafgericht im Bericht fest, „dass die heutige Situation unbefriedigend ist und (es) zeigt die aufgrund der getroffenen Abklärungen dafür massgeblichen Gründe auf".

Für den Beauftragten weist die Bezeichnung „Bericht" sowie der Titel als Ganzes darauf hin, dass sich der Inhalt des Dokuments nicht in erster Linie auf einzelne Gerichtsverfahren bezieht, sondern sich grundsätzlich mit der Tätigkeit der Bundesanwaltschaft im Zusammenhang mit den von ihr erhobenen Anklagen auseinandersetzt. Denkbar ist, dass der Bericht auch Informationen und Ausführungen enthält, die nicht in einem direkten Zusammenhang mit gerichtlichen Verfahren stehen.

5. Alleine der Systematik des Strafgerichtsgesetzes folgend muss festgehalten werden, dass Art. 28 nicht in den Bereich der Organisation und Verwaltung des Gerichts (Art. 13 – 25 SGG), sondern ins Kapitel „Zuständigkeiten und Verfahren" fällt und somit in einen Bereich, der die Rechtsprechung durch das Gericht regelt.

   Selbst wenn die Beschwerdekammer als Rechtsprechungsbehörde den Bericht verfasst hat, bedeutet dies nicht, dass alle der von ihr erstellten Dokumente nie dem Öffentlichkeitsprinzip unterliegen. Bei der Beantwortung der Frage der Zugänglichkeit muss einzig darauf abgestellt werden, ob ein Dokument, welches das Gericht verfasst hat, im Einzelfall administrativer oder gerichtlicher Natur ist.

6. Ebenso wenig ist die Tatsache ausschlaggebend, dass das Bundesstrafgericht den besagten Bericht als (gesetzliches) Aufsichtsorgan über die Bundesanwaltschaft erstellt hat. Vielmehr sind zwei Anwendungsfälle von Aufsichtstätigkeiten auseinander zu halten: Einerseits die Aufsicht des Gerichts über die Verwaltung einer bestimmten Institution und anderseits die Aufsichtstätigkeit des Gerichts in den Belangen der Rechtsprechung.

7. In den auf den 1. Januar 2007 in Kraft tretenden Gesetzen zu den neuen Bundesgerichten (Totalrevision der Bundesrechtspflege, BBl 2001 4202) finden sich auch zwei Bestimmungen, die sich mit der Anwendung des Öffentlichkeitsprinzips im Bereich der Aufsichtstätigkeit des Bundesgerichts[1] und des Bundesverwaltungsgerichts[2] befassen.

   So sieht Art. 28 des künftigen Bundesgerichtsgesetzes (BGG) vor, dass das Öffentlichkeitsprinzip zur Anwendung gelangt, soweit das Gericht administrative Aufgaben oder *Aufgaben im Zusammenhang mit der Aufsicht* über das Bundesverwaltungsgericht und das Bundesstrafgericht erfüllt.

[1] Art. 28 des Bundesgesetzes vom 17. Juni 2005 über das Bundesgericht (Bundesgerichtsgesetz, BGG), BBl 2005 4045

[2] Art. 30 des Bundesgesetzes vom 17. Juni 2005 über das Bundesverwaltungsgericht (Verwaltungsgerichtsgesetz, VGG), BBl 2005 4093

Die in Art. 28 BGG angesprochene Aufsicht des Bundesgerichts meint also nicht die gerichtliche Aufsicht im Einzelfall, sondern die allgemeine Aufsichtstätigkeit administrativer Natur über die anderen Gerichte.

8. Der Beauftragte gelangt zum Schluss, dass für jeden konkreten Einzelfall neu geklärt werden muss, welcher Natur die Aufsichtstätigkeit, die das Gericht ausübt, ist. Erst nach dieser Bewertung kann beurteilt werden, ob das in Frage stehende Dokument dem Öffentlichkeitsprinzip untersteht.

   Ausschlaggebend ist letztlich das materielle Kriterium, ob das Gericht im Rahmen der Aufgabenerfüllung eine administrative Tätigkeit ausübt. Unerheblich bleibt dabei, von wem innerhalb des Gerichts diese Tätigkeit ausgeübt wird. Es kann sich dabei um Sekretariatspersonal, Gerichtsschreiber oder sogar, wie im vorliegenden Fall, um die Beschwerdekammer handeln.

9. Um diese Prüfung im Einzelfall vornehmen zu können, hat der Beauftragte beim Bundesstrafgericht das Einsichtsrecht nach Art. 20 BGÖ geltend gemacht. Das Gericht ist dieser Aufforderung nicht nachgekommen. Der Beauftragte hatte somit keine Möglichkeit, den Bericht einzusehen und zu prüfen, ob der im Rahmen der Aufsichtstätigkeit erstellte Bericht administrativer Natur ist und damit dem Öffentlichkeitsprinzip unterliegt. Deshalb muss auch die Frage, ob der Bericht administrativer Natur ist, offen bleiben.

10. Ebenfalls offen muss die Frage bleiben, ob der Bericht ein Evaluationsdokument im Sinne von Art. 8 Abs. 5 BGÖ darstellt. Diese Bestimmung garantiert einen *absoluten* Zugang zu Berichten über die Evaluation der Leistungsfähigkeit der Bundesverwaltung (BBl 2003 2015). Art. 8 Abs. 5 BGÖ gilt analog auch für Evaluationen der Leistungsfähigkeit des Bundesstrafgerichts, soweit sie dessen Verwaltungstätigkeit betreffen. Explizit führt der Bundesrat in seiner Botschaft zum Öffentlichkeitsgesetz denn auch aus, dass Evaluationen administrativer Belange der Bundesgerichte dem Öffentlichkeitsprinzip unterstehen (BBl 2003 1985).

11. Der Beauftragte bedauert, dass er diese beiden Fragen nicht eingehender klären konnte. Das Öffentlichkeitsgesetz gesteht dem Beauftragten im Rahmen des Schlichtungsverfahrens *umfassende* Auskunfts- und Einsichtsrechte zu. „Eine Behörde ist verpflichtet, dem Beauftragten alle erforderlichen Dokumente zur Verfügung zu stellen; sie kann sich dieser Verpflichtung nicht unter Berufung auf die Vertraulichkeit oder die geheime Natur der Informationen entziehen" (Erläuterungen zur VBGÖ). Folgerichtig unterstehen der Beauftragte und sein Sekretariat dem Amtsgeheimnis im gleichen Ausmass wie die Behörden, in deren amtliche Dokumente sie Einsicht nehmen oder die ihnen Auskunft erteilen (Art. 20 BGÖ).

Der Gesetzgeber hat mit dem Erlass des Öffentlichkeitsgesetzes seinen klaren Willen zum Ausdruck gebracht, dass die Bürgerin und der Bürger Zugang zu amtlichen Dokumenten erhalten sollen. Als eine Art Verbindungs- und Vermittlungsstelle hat er dem Beauftragten eine wichtige Funktion mit entsprechenden Kompetenzen übertragen und ihm damit eine fundamentale Rolle im Verfahren um den Zugang zu Dokumenten zugesprochen (BBl 2003 2029). Der Beauftragte kann diese Aufgabe nicht wahrnehmen, wenn ihm – trotz klarer Gesetzgebung betreffend seiner Einsichts- und Auskunftsrechte (Art. 20 BGÖ) – keine Einsicht in besagte Dokumente gewährt wird. Verweigern die dem Öffentlichkeitsprinzip unterliegenden Bundesbehörden und Bundesgerichte dem Beauftragten sein Einsichtsrecht, so bleibt letztlich das Öffentlichkeitsgesetz toter Buchstabe.

D. Durchführung des Schlichtungsverfahrens

1. Art. 25a SGG gibt dem Bundesstrafgericht die Möglichkeit vorzusehen, dass kein Schlichtungsverfahren durchgeführt werden soll. In seinem Schreiben an den Beauftragten führt das Bundesstrafgericht aus, dass das am 20. Juni 2006 erlassene Reglement über das Bundesstrafgericht, das auf den 1. Januar 2007 in Kraft treten soll, das Schlichtungsverfahren ausschliesst, und dass in der Übergangsphase bis zum 31. Dezember 2006 Art. 18 des Reglements über die Archivierung beim Bundesstrafgericht (SR 152.12) analog angewendet werden soll. Gemäss Ansicht des Bundesstrafgerichts ist der Beauftragte aus diesen Gründen nicht zuständig, auf den Schlichtungsantrag der Antragstellerin einzutreten.

   Im Folgenden gilt es zu prüfen, ob das Bundesstrafgericht das Schlichtungsverfahren ausdrücklich und rechtsgültig ausgeschlossen hat.

2. Es steht ausser Frage, dass das Bundesstrafgericht entscheiden kann, dass kein Schlichtungsverfahren durch den Beauftragten stattfinden soll. Allerdings enthält das *geltende Reglement vom 11. Februar 2004 für das Bundesstrafgericht (SR 173.710)* keine Bestimmung, welche die Anwendung des Öffentlichkeitsprinzips in der Justizverwaltung regelt. Auch zum Schlichtungsverfahren äussert sich das aktuelle Reglement nicht[3].

[3] Anders das Reglement für das Schweizerische Bundesgericht (SR 173.111.1): Das Bundesgericht hat mit Blick auf das Inkrafttreten des Öffentlichkeitsgesetzes bereits im Februar 2006 sein Reglement entsprechend ergänzt. Ein neuer Art. 31bis mit dem Titel „Öffentlichkeitsprinzip der Verwaltung" sieht vor, dass kein Schlichtungsverfahren durchgeführt wird (Abs. 3).

Es gilt festzuhalten, dass das neue, *auf den 1. Januar 2007 in Kraft tretende Reglement für das Bundesstrafgericht* von der Durchführung eines Schlichtungsverfahrens absieht. Für die Beurteilung des vorliegenden Falles ist das künftige Reglement unbeachtlich, denn „noch nicht in Kraft stehendes Recht vermag nicht die Grundlage für ein staatliches Handeln abzugeben" (BGE 89 I 472). Eine Vorwirkung von werdendem Recht ist einzig dann möglich und zulässig, wenn besondere gesetzliche Vorschriften diese Möglichkeit explizit einräumen. Letzteres ist vorliegend nicht der Fall.

3. Einziger Anknüpfungspunkt für die Beurteilung der Frage, ob ein Schlichtungsverfahren durchgeführt wird, bleibt damit der Entscheid des Bundesstrafgerichts, als *Übergangsregelung Art. 18 des Archivierungsreglements analog* anzuwenden. Diese Bestimmung besagt, dass ein Entscheid des Generalsekretärs oder der Generalsekretärin über die Abweisung oder die Beschränkung der Akteneinsicht innert 30 Tagen seit der Eröffnung bei der Gerichtsleitung angefochten werden kann.

4. Das Bundesstrafgericht vertritt die Ansicht, dass mit Entscheid der analogen Anwendung von Art. 18 des Archivierungsreglements grundsätzlich auch das Schlichtungsverfahren durch den Beauftragten ausgeschlossen worden ist.

5. Dieser Haltung kann der Beauftragte aus folgenden Gründen nicht folgen:

   - Mit dem Entscheid, das Archivierungsreglement in der Übergangsphase bis Ende 2006 anzuwenden, ist das Bundesstrafgericht lediglich der Forderung von Art. 25a SGG nachgekommen und hat das zuständige Beschwerdeorgan festgelegt.

   - Zum Ausschluss des Schlichtungsverfahrens äussert sich das Bundesstrafgericht nicht explizit. Das Archivierungsreglement selber enthält keine Ausführungen über Schlichtungsverfahren.

   - Das Schlichtungsverfahren und das sich daran anschliessende Verfahren zum Erlass einer Verfügung bilden keine Einheit, sondern sind in der Konzeption des Öffentlichkeitsgesetzes zwei eigenständige Verfahrensabschnitte (BBl 2003 2018).

   - Nach Art. 25a SGG kann das Bundesstrafgericht vorsehen, dass kein Schlichtungsverfahren durchgeführt werden soll. Dabei handelt es sich um eine Kann-Bestimmung. Macht das Bundesstrafgericht von dieser Möglichkeit ausdrücklich keinen Gebrauch, hat dies zur Folge, dass das im Öffentlichkeitsgesetz vorgesehene Schlichtungsverfahren zur Anwendung gelangt.

Gestützt auf die vorausgegangenen Ausführungen kommt der Beauftragte zum Schluss, dass das Bundesstrafgericht das Schlichtungsverfahren nicht ausdrücklich ausgeschlossen hat. Der Beauftragte erachtet sich als zuständig, in der vorliegenden Angelegenheit das Schlichtungsverfahren durchzuführen.

6. Hinzu kommt, dass die Verfahrensvorschriften, die in der Übergangsphase im Falle eines abgelehnten Zugangsgesuchs zur Anwendung gelangen, nicht in dem dafür erforderlichen Erlass (Reglement für das Bundesstrafgericht) ergangen sind. Überdies hätte dieses Reglement entsprechend den klaren Vorgaben des Bundesgesetzes über die Sammlungen des Bundesrechts und das Bundesblatt (PublG, SR 170.512) in der Amtlichen Sammlung des Bundesrechts veröffentlicht werden müssen, damit es überhaupt seine Rechtswirkungen entfalten kann. Diese Kriterien sind nach Ansicht des Beauftragten durch das Bundesstrafgericht nicht eingehalten worden.

   Zudem ist es für den Beauftragten nicht nachvollziehbar, weshalb das Bundesstrafgericht nicht rechtzeitig sein geltendes Reglement angepasst hat, zumal es kurz (d.h. 10 Tage) vor Inkrafttreten des Öffentlichkeitsgesetzes sein künftiges (auf den 1. Januar 2007 in Kraft tretendes) Reglement erlassen und darin eine entsprechende Bestimmung zum „Öffentlichkeitsprinzip in Bezug auf die Justizverwaltung" (Art. 18) vorgesehen hat.

E. Schriftlichkeit des Zugangsgesuchs

1. Das Bundesstrafgericht verlangt von den Gesuchstellenden, die Einsicht in ein amtliches Dokument nehmen wollen, dass sie ein schriftliches Gesuch einreichen. Es stützt sich dabei auf das Archivierungsreglement und auf das ab dem 1. Januar 2007 geltende Reglement für das Bundesstrafgericht, die beide diese Formvorschrift vorsehen.

2. Gemäss Art. 10 Abs. 3 BGÖ muss ein Gesuch hinreichend genau formuliert sein. Die Bestimmung sieht keine weiteren Formvorschriften vor, insbesondere legt sie nicht fest, dass ein Gesuch schriftlich eingereicht werden muss. Im Gegenteil: In der Botschaft des Bundesrates zum Öffentlichkeitsgesetz heisst es dazu ausdrücklich, dass „Ein Gesuch (…) formlos eingereicht werden (kann), das heisst, mündlich, durch Faxübermittlung, per E-Mail oder aber auch auf schriftlichem Weg" (BBl 2003 2019).

3. Das Bundesstrafgericht muss das Öffentlichkeitsgesetz sinngemäss anwenden. In welchen Bereichen es notwendige Anpassungen vornehmen darf, hat der Gesetzgeber in Art. 25a SGG normiert. Die Forderung, dass ein Zugangsgesuch in schriftlicher Form eingereicht werden muss, gehört nicht dazu und stellt eine zusätzliche Zugangsvoraussetzung dar, die das Öffentlichkeitsgesetz so nicht vorgesehen hat.

4. Der Beauftragte ist der Ansicht, dass die Forderung nach einer schriftlichen Gesucheinreichung einen Verstoss gegen das Öffentlichkeitsgesetzes darstellt.

5. Überdies darf nicht ausser Acht gelassen werden, dass die Antragstellerin ihr Zugangsgesuch zuerst per E-Mail beim Bundesstrafgericht eingereicht hat. Die E-Mail wurde an das für die Gesuchseinreichung zuständige Generalsekretariat gesandt (analoge Anwendung von Art. 15 Archivierungsreglement).

   Selbst wenn man den Überlegungen des Bundesstrafgerichts folgt und das Archivierungsreglement analog anwendet, darf das Bundesstrafgericht an die Schriftlichkeit eines Gesuchs keine über das Öffentlichkeitsgesetz hinausgehenden Ansprüche stellen. Das Öffentlichkeitsgesetz anerkennt, dass Zugangsgesuche auch per E-Mail eingereicht werden können. Demnach hätte das Bundesstrafgericht die E-Mail der Antragstellerin als schriftliches Gesuch entgegennehmen und im Falle der Verweigerung des Zugangs eine Verfügung erlassen müssen.

F. Schlussfolgerungen

Gestützt auf die vorangegangenen Ausführungen ergeben sich für den Beauftragten folgende Schlussfolgerungen:

1. Die Frage, ob der „Bericht zu den Vorwürfen betreffend die geringe Anzahl der von der Bundesanwaltschaft erhobenen Anklagen" dem Öffentlichkeitsprinzip unterliegt, muss offen gelassen werden, weil das Bundesstrafgericht dem Beauftragten den Bericht nicht zur Einsicht überlassen wollte.

2. Aus dem gleichen Grund muss der Beauftragte die Frage offen lassen, ob der Bericht als Evaluationsdokument nach Art. 8 Abs. 5 BGÖ zu qualifizieren und demnach der Zugang zu gewährleisten ist.

3. Das Bundesstrafgericht hat das Schlichtungsverfahren durch den Beauftragten nicht rechtsgültig ausgeschlossen.

4. Das Verlangen eines schriftlichen Zugangsgesuchs stellt ein Verstoss gegen das Öffentlichkeitsgesetz dar.

5. Obwohl aufgrund des verweigerten Einsichtsrechts keine abschliessende, materielle Beurteilung des Schlichtungsgesuchs durchgeführt werden konnte, gelangt der Beauftragte zum Schluss, dass das Bundesstrafgericht der Antragstellerin die Einsicht in den „Bericht zu den Vorwürfen betreffend die geringe Anzahl der von der Bundesanwaltschaft erhobenen Anklagen" verweigert hat, indem es weder auf ihr schriftliches noch auf ihr mündliches Zugangsgesuch eingetreten ist. Bei analoger Anwendung der Archivierungsverordnung hätte das Bundesstrafgericht eine Verfügung zuhanden der Antragstellerin erlassen müssen, um dieser zumindest die Möglichkeit einzuräumen, den Rechtsweg zu beschreiten.

III. Aufgrund dieser Erwägungen empfiehlt der Datenschutz- und Öffentlichkeitsbeauftragte:

1. Nochmalige Prüfung des Zugangsgesuch zum „Bericht zu den Vorwürfen betreffend die geringe Anzahl der von der Bundesanwaltschaft erhobenen Anklagen"

   Das Bundesstrafgericht überprüft nochmals, ob der Antragstellerin der Zugang zum „Bericht zu den Vorwürfen betreffend die geringe Anzahl der von der Bundesanwaltschaft erhobenen Anklagen" nach Öffentlichkeitsgesetz gewährt werden kann.

   Im Falle einer Verweigerung oder Aufschiebung des Zugangs informiert das Bundesstrafgericht die Antragstellerin schriftlich und begründet seine Stellungnahme summarisch (Art. 12 Abs. 4 BGÖ).

2. Erlass einer Verfügung durch das Bundesstrafgericht

   Das Bundesstrafgericht erlässt eine Verfügung nach Art. 5 des Verwaltungsverfahrensgesetzes, wenn es in Abweichung dieser Empfehlung das Zugangsgesuchs zum „Bericht zu den Vorwürfen betreffend die geringe Anzahl der von der Bundesanwaltschaft erhobenen Anklagen" nicht nochmals überprüft.

   Das Bundesstrafgericht erlässt die Verfügung innert 20 Tagen nach Empfang dieser Empfehlung (Art. 15 Abs. 3 BGÖ).

   Die Antragstellerin ihrerseits kann innerhalb von zehn Tagen nach Erhalt der Empfehlung den Erlass einer Verfügung nach Artikel 5 des Verwaltungsverfahrensgesetzes verlangen (Art. 15 Abs. 1 BGÖ).

3. Veröffentlichung des Ausschlusses eines Schlichtungsverfahrens und des Beschwerdeorgans

   Das Bundesstrafgericht veröffentlicht in einer allgemein zugänglichen Form (z.B. im Internet) den Entscheid, welche Verfahrensvorschriften betreffend die Beurteilung von Zugangsgesuchen nach dem Öffentlichkeitsgesetz in der Übergangsphase bis zum 31. Dezember 2006 gelten.

   Der Entscheid beantwortet die Frage nach dem Beschwerdeorgan im Sinne von Art. 25a SGG und nach der Durchführung eines externen Schlichtungsverfahrens.

4. Mündlich eingereichte Zugangsgesuche

   Behält das Bundesstrafgericht in der Übergangsphase den Ausschluss des Schlichtungsverfahrens bei, so erlässt es auch bei einem mündlich eingereichten Zugangsgesuch zu amtlichen Dokumenten eine Verfügung, sofern es den Zugang aufschieben, beschränken

   oder verweigern will.

5. Anpassung des Reglements vom 20. Juni 2006 für das Bundesstrafgericht

   Das Bundesstrafgericht sieht davon ab, nur auf schriftlich eingereichte Zugangsgesuche eine Verfügung zu erlassen, und passt sein auf den 1. Januar 2007 in Kraft tretendes Reglement entsprechend an.

6. Veröffentlichung der Empfehlung

   Diese Empfehlung wird veröffentlicht (Art. 13 Abs. 3 VBGÖ). Zum Schutz der Personendaten der am Schlichtungsverfahren Beteiligten wird der Name der Antragstellerin anonymisiert.

Jean-Philippe Walter

Kopie an: X

4.8 Empfehlung an das Bundesamt für Verkehr: „Jahresberichte der Seilbahnbetreiber“

Bern, den 27. November 2006

Empfehlung

gemäss

Art. 14 des
Bundesgesetzes über das
Öffentlichkeitsprinzip der Verwaltung
vom 17. Dezember 2004

zum Schlichtungsantrag von

X
(Antragsteller)

gegen

Bundesamt für Verkehr (BAV), Bern

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Der Antragsteller reichte am 27. September 2006 beim Bundesamt für Verkehr (BAV) ein schriftliches Zugangsgesuch ein. Er wollte Zugang zu allen „Meldungen von Seilbahnbetreibern", „bei denen Seilbahnanlagen durch auftauenden Permafrost in Gefahr gerieten und danach dahingehend saniert werden mussten" (Zitate Zugangsgesuch).

2. Das BAV teilte dem Antragsteller am 17. Oktober 2006 mit, dass innerhalb der Bundesverwaltung zwar eine Arbeitsgruppe zum Thema Permafrost bestehe, das BAV jedoch keine Listen von gefährdeten Anlagen besitze und nach dem 1. Juli 2006 keine Dokumente zur „Sanierung von Seilbahnanlagen infolge auftauendem Permafrost" erstellt worden sind. Aus diesen Gründen könne das BAV dem Zugangsgesuch des Antragsstellers nicht nachkommen.

3. Der Antragsteller reichte mit Schreiben vom 24. Oktober 2006 beim Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) einen Schlichtungsantrag nach Art. 13 des Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ; SR 152.3) ein (eingegangen am 26. Oktober 2006). Der Antragsteller führte an, dass das BAV ihm den Zugang zu besagten amtlichen Dokumenten verweigert hatte.

4. Am 7. November 2006 traf sich der Beauftragte mit den in dieser Angelegenheit zuständigen Mitarbeitern des BAV zu einer Sitzung. Er wollte dabei insbesondere wissen, ob seit dem Inkrafttreten des Öffentlichkeitsgesetzes „Meldungen" im Sinne des Antragstellers eingegangen seien. Zudem nahm er Einblick in einzelne Dokumente und liess sich über Aufgabe und Tätigkeit der angesprochenen Arbeitsgruppe informieren.

5. Mit Schreiben vom 13. November 2006 präzisierte das BAV gegenüber dem Beauftragten, dass die Arbeitsgruppe den Titel „Permafrost-Problematik" trage. Dabei soll es sich um eine BAV-interne Arbeitsgruppe handeln, in der Mitarbeitende des Bundesamtes für Umwelt BAFU als Berater mitwirken. Die erste und bisher einzige Sitzung der Arbeitsgruppe hat am 11. Oktober 2006 stattgefunden. Dabei informierte das BAFU über die von ihm erstellten Permafrostkarten. Es wurde diskutiert, wie diese Karten für die Bedürfnisse des BAV genutzt werden könnten. Das BAV hielt in seinem Schreiben an den Beauftragten fest, dass die Arbeitsgruppe bis anhin keine Dokumente, die einen inhaltlichen Bezug zum Zugangsgesuch des Antragstellers aufweisen, erstellt hat.

Im gleichen Schreiben versichert das BAV, dass bei den Neuanlagen und den zugehörigen Akten der Plangenehmigungsverfahren „zurzeit keine Meldungen vor(liegen), dass man auf Permafrost stossen könnte oder bei Sondierungen gestossen wäre." Bei den bestehenden Anlagen gebe es „aus diesem Jahr (…) keine Meldungen und Hinweise bezüglich Permafrost."

II. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte zieht in Erwägung:

A. Schlichtungsverfahren gemäss Art. 14 BGÖ

1. Gemäss Art. 13 BGÖ kann eine Person einen Schlichtungsantrag beim Beauftragten einreichen, wenn die Behörde den Zugang zu amtlichen Dokumenten einschränkt, aufschiebt oder verweigert, oder wenn die Behörde innert der vom Gesetz vorgeschriebenen Frist keine Stellungnahme abgibt.

   Der Beauftragte wird nicht von Amtes wegen, sondern nur auf Grund eines schriftlichen Schlichtungsantrags tätig (BBl 2003 2023). Berechtigt, einen Schlichtungsantrag einzureichen, ist jede Person, die an einem Gesuchsverfahren um Zugang zu amtlichen Dokumenten teilgenommen hat. Für den Schlichtungsantrag genügt einfache Schriftlichkeit. Aus dem Begehren muss hervorgehen, dass sich der Beauftragte mit der Sache befassen soll. Der Schlichtungsantrag muss innert 20 Tagen nach Empfang der Stellungnahme der Behörde schriftlich eingereicht werden.

2. Der Antragsteller hat ein Zugangsgesuch nach Art. 6 BGÖ beim BAV eingereicht und eine ablehnende Antwort erhalten. Als Teilnehmer an einem vorangegangenen Gesuchsverfahren ist er zur Einreichung eines Schlichtungsantrags berechtigt. Der Schlichtungsantrag wurde formgerecht (einfache Schriftlichkeit) und fristgerecht (innert 20 Tagen nach Empfang der Stellungnahme der Behörde) beim Beauftragten eingereicht.

3. Das Schlichtungsverfahren kann auf schriftlichem Weg oder konferenziell (mit einzelnen oder allen Beteiligten) unter Leitung des Beauftragten stattfinden. Die Festlegung des Verfahrens im Einzelnen obliegt alleine dem Beauftragten (BBl 2003 2024).

   Kommt keine Einigung zu Stande oder besteht keine Aussicht auf eine einvernehmliche Lösung, ist der Beauftragte gemäss Art. 14 BGÖ gehalten, aufgrund seiner Einschätzung und Beurteilung der Angelegenheit eine Empfehlung abzugeben.

B. Zeitlicher Geltungsbereich des Öffentlichkeitsgesetzes

1. Der Antragsteller beantragte Zugang zu den „Meldungen von Seilbahnbetreibern". Dabei interessierte er sich für „alle Fälle" in der Zeit von 1991 bis 2006, „bei denen Seilbahnanlagen durch auftauenden Permafrost in Gefahr gerieten und danach dahingehend saniert werden mussten".

2. Seilbahnbetreiber müssen jedes Jahr ein Formular mit dem Titel „Bericht über die Instandhaltung im Jahr …" (Jahresberichte) ausfüllen und beim BAV einreichen. Das Formular enthält keine Rubriken, die sich explizit auf die Auswirkungen des auftauenden Permafrosts auf Seilbahnanlagen beziehen. In der Rubrik „Verschiedenes" können die Betreiber u. a. ihre „Besondere(n) Feststellungen" und „Bemerkungen/Mitteilungen" festhalten. Denkbar ist, dass ein Betreiber an dieser Stelle Ausführungen zu allfälligen Auswirkungen des auftauenden Permafrosts auf die Anlage anbringt.

3. Das Öffentlichkeitsgesetz findet nur auf amtliche Dokumente Anwendung, die nach seinem Inkrafttreten, d.h. nach dem 1. Juli 2006, von einer Behörde erstellt oder empfangen wurden (Art. 21 BGÖ). Der Vollständigkeit halber sei darauf hingewiesen, dass das Öffentlichkeitsgesetz der gesuchstellenden Person lediglich ein einklagbares Recht auf Einsicht in amtliche Dokumente verschafft. Sie kann gestützt auf das Öffentlichkeitsgesetz jedoch nicht verlangen, dass eine Bundesbehörde ein nicht existierendes Dokument extra für sie erstellt.

4. Das BAV hält fest, dass seit dem 1. Juli 2006 keine Jahresberichte mit dem vom Antragsteller angeführten Kontext eingereicht worden sind. Gemäss Ausführungen des BAV werden die Jahresberichte für bestehende Anlagen in der Regel im Frühling eingereicht. Das BAV hat überdies versichert, dass es seit dem 1. Juli 2006 keine anderen Dokumente fertig erstellt oder von Dritten empfangen hat, die sich mit den Auswirkungen des auftauenden Permafrosts auf Seilbahnanlagen befassen.

5. *Der Beauftragte kommt zum Schluss, dass das BAV unter den angeführten Umständen den Zugang zu den gewünschten Dokumenten in Übereinstimmung mit Art. 21 BGÖ nicht gewähren musste.*

C. Dokumente mit Personendaten Dritter

1. Die Jahresberichte enthalten u.a. Angaben zu den Seilbahnbetreibern und den von diesen für verschiedene Arbeiten beigezogenen Fachunternehmen. Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, sind Personendaten nach Art. 3 Ziff. a des Bundesgesetzes über den Datenschutz (DSG, SR 235.1).

2. Der Schutz von Personendaten als Aspekt des verfassungsmässig garantierten Persönlichkeitsschutzes (Art. 13 Abs. 2 BV) geht dem Recht auf Zugang zu amtlichen Dokumenten grundsätzlich vor (BBl 2003 2016). Konsequenterweise hat der Gesetzgeber daher in Art. 9 BGÖ festgelegt, dass amtliche Dokumente, welche Personendaten Dritter enthalten, vor der Einsichtnahme grundsätzlich anonymisiert werden müssen. Erweist sich dies als nicht möglich, so kann der Zugang nur gewährt werden, wenn die Zustimmung der betroffenen Drittperson eingeholt worden ist oder eine spezialgesetzliche Bestimmung die Bekanntgabe ihrer Personendaten explizit vorsieht (Art. 9 Abs. 2 BGÖ in Verbindung mit Art. 19 des Bundesgesetzes über den Datenschutz DSG; SR 235.1). Ist eine Anonymisierung nicht möglich und liegt weder eine Zustimmung der betroffenen Drittperson(en) noch eine entsprechende spezialgesetzliche Bekanntgabenorm vor, so muss der Zugang in der Regel verweigert werden.

3. Mit anderen Worten muss der Zugang zu amtlichen Dokumenten eingeschränkt, aufgeschoben oder verweigert werden, wenn durch seine Gewährung die Privatsphäre Dritter beeinträchtigt werden kann (Art. 7 Abs. 2, erster Satzteil BGÖ). Nur in Ausnahmefällen, d.h. wenn die öffentlichen Interessen den Schutz der Privatsphäre Dritter überwiegen, dürfen amtliche Dokumenten, die Personendaten enthalten, zugänglich gemacht werden (Art. 7 Abs. 2, zweiter Satzteil BGÖ). Das öffentliche Interesse am Zugang kann namentlich überwiegen, wenn die Zugänglichmachung einem besonderen Informationsinteresse der Öffentlichkeit oder dem Schutz spezifischer öffentlicher Interessen (z.B. Schutz der öffentlichen Ordnung und Sicherheit oder der öffentlichen Gesundheit) dient (Art. 6 VBGÖ). Gelangt die Behörde im Rahmen der Gesuchsprüfung zur Überzeugung, dass im konkreten Fall das öffentliche Interesse am Zugang das Interesse der Betroffenen am Schutz der Privatsphäre überwiegt, so muss sie die Personen, die in ihrer Privatsphäre beeinträchtigt werden (vorliegend: Seilbahnbetreiber, beauftragte Unternehmen), über das Zugangsgesuch informieren, und ihnen die Möglichkeit zur Stellungnahme einräumen (Art. 11 BGÖ). Sind die Betroffenen in der Folge mit dem Absicht der Behörde, den Zugang zu gewähren, nicht einverstanden, können sie ein Schlichtungsverfahren einleiten (Art. 13 BGÖ).

4. *Abschliessend sei noch darauf hingewiesen, dass der Antragsteller jederzeit ein neues Zugangsgesuch in der gleichen Sache einreichen kann. Ist das BAV dann im Besitz von Jahresberichten, in denen der Permafrost thematisiert wird, muss die Frage des Zugangs nach den vorangegangenen Ziffern 1 bis 3 geprüft werden.*

III. Aufgrund dieser Erwägungen empfiehlt der Datenschutz- und Öffentlichkeitsbeauftragte:

1. Das Bundesamt für Verkehr hält an der Zugangsverweigerung fest.
2. Der Antragsteller kann innerhalb von 10 Tagen nach Erhalt dieser Empfehlung beim Bundesamt für Verkehr den Erlass einer Verfügung nach Artikel 5 des Verwaltungsverfahrensgesetzes verlangen (Art. 15 Abs. 1 BGÖ).

   Gegen diese Verfügung kann der Antragsteller bei der Eidgenössischen Datenschutz- und Öffentlichkeitskommission Beschwerde führen (Art. 16 BGÖ).
3. Diese Empfehlung wird veröffentlicht (Art. 13 Abs. 3 VBGÖ). Zum Schutz der Personendaten der am Schlichtungsverfahren Beteiligten wird der Name des Antragstellers anonymisiert.

Hanspeter Thür

Kopie an X

4.9 Empfehlung an das Eidgenössische Departement für auswärtige Angelegenheiten: „Früherkennung von Risiken im Visabereich“

Bern, den 27. November 2006

Empfehlung

gemäss

Art. 14 des
Bundesgesetzes über das
Öffentlichkeitsprinzip der Verwaltung
vom 17. Dezember 2004

zum Schlichtungsantrag von

X
(Antragsteller)

gegen

Eidg. Departement für auswärtige Angelegenheiten (EDA), Bern

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Der Antragsteller reichte am 23. September 2006 beim Eidg. Departement für auswärtige Angelegenheiten (EDA) ein schriftliches Zugangsgesuch ein. Er ersuchte um Zugang zur „Korruptionsliste des EDA" (Zitat Zugangsgesuch), welche das EDA „im vergangenen Sommer erstellen liess". Das Papier zeige, so die Ausführungen des Antragstellers weiter, die Korruptionsanfälligkeit der schweizerischen Auslandvertretungen auf.

2. In seinem Antwortschreiben vom 16. Oktober 2006 teilte das EDA dem Antragsteller mit, dass sich die Liste nicht auf die Korruptionsanfälligkeit der Vertretungen beziehe. Sie enthalte vielmehr „eine Einschätzung der Situation" in jenen Staaten, in denen die Schweiz eine Vertretung unterhalte. Mit der Liste werde das Ziel verfolgt, „mögliche Risiken für den Visabereich unserer Vertretungen frühzeitig erkennen zu können."

   Das EDA verweigerte den Zugang zum besagten Dokument mit der Begründung, dass „eine Veröffentlichung der Liste die Beziehung der Schweiz zu bestimmten Staaten belasten und den aussenpolitischen Spielraum der Schweiz einschränken könnte." Es stützte sich dabei auf Art. 7 Abs. 1 Bst. d Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ; 152.3).

3. Der Antragsteller reichte mit Schreiben vom 24. Oktober 2006 beim Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) einen Schlichtungsantrag nach Art. 13 BGÖ ein (eingegangen am 27. Oktober 2006). Der Antragsteller führte an, dass das EDA ihm den Zugang zu besagtem amtlichen Dokument verweigert hat.

4. Am 1. November 2006 traf sich der Beauftragte mit der in dieser Angelegenheit zuständigen Mitarbeiterin des EDA zu einem Gespräch über die Verweigerungsgründe und liess sich das besagte Dokument aushändigen. In einer schriftlichen Stellungnahme vom 13. November 2006 an den Beauftragten begründete das EDA seinen Standpunkt in dieser Sache.

II. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte zieht in Erwägung:

A. Schlichtungsverfahren gemäss Art. 14 BGÖ

1. Gemäss Art. 13 BGÖ kann eine Person einen Schlichtungsantrag beim Beauftragten einreichen, wenn die Behörde den Zugang zu amtlichen Dokumenten einschränkt, aufschiebt oder verweigert, oder wenn die Behörde innert der vom Gesetz vorgeschriebenen Frist keine Stellungnahme abgibt.

   Der Beauftragte wird nicht von Amtes wegen, sondern nur auf Grund eines schriftlichen Schlichtungsantrags tätig (BBl 2003 2023). Berechtigt einen Schlichtungsantrag einzureichen, ist jede Person, die an einem Gesuchsverfahren um Zugang zu amtlichen Dokumenten teilgenommen hat. Für den Schlichtungsantrag genügt einfache Schriftlichkeit. Aus dem Begehren muss hervorgehen, dass sich der Beauftragte mit der Sache befassen soll. Der Schlichtungsantrag muss innert 20 Tagen nach Empfang der Stellungnahme der Behörde schriftlich eingereicht werden.

2. Der Antragsteller hat ein Zugangsgesuch nach Art. 6 BGÖ beim EDA eingereicht und eine ablehnende Antwort erhalten. Als Teilnehmer an einem vorangegangenen Gesuchsverfahren ist er zur Einreichung eines Schlichtungsantrags berechtigt. Der Schlichtungsantrag wurde formgerecht (einfache Schriftlichkeit) und fristgerecht (innert 20 Tagen nach Empfang der Stellungnahme der Behörde) beim Beauftragten eingereicht.

3. Das Schlichtungsverfahren kann auf schriftlichem Weg oder konferenziell (mit einzelnen oder allen Beteiligten) unter Leitung des Beauftragten stattfinden. Die Festlegung des Verfahrens im Einzelnen obliegt alleine dem Beauftragten (BBl 2003 2024).

   Kommt keine Einigung zu Stande oder besteht keine Aussicht auf eine einvernehmliche Lösung, ist der Beauftragte gemäss Art. 14 BGÖ gehalten, aufgrund seiner Einschätzung und Beurteilung der Angelegenheit eine Empfehlung abzugeben.

B. Ausnahmefall nach Art. 7 BGÖ

1. Der Antragsteller ersuchte um Zugang zur „Korruptionsliste des EDA". Das EDA verweigerte den Zugang, da durch dessen Gewährung die schweizerischen Beziehungen zu bestimmten Staaten belastet und der aussenpolitische Spielraum des Landes eingeschränkt werden könnte.

2. Mit Inkrafttreten des Öffentlichkeitsgesetzes besteht ein Recht auf Einsichtnahme in amtliche Dokumente und auf Erhalt behördlicher Auskünfte über den Inhalt amtlicher Dokumente (Art. 6 BGÖ). Das Öffentlichkeitsprinzip gilt jedoch nicht absolut. Der Gesetzgeber hat in Art. 7 BGÖ eine abschliessende Auflistung von Ausnahmefällen aufgeführt, in denen die Bundesverwaltung keine Einsicht gewähren muss. Im vorliegenden Fall berief sich das EDA auf die Ausnahme von Art. 7 Abs. 1 Bst. d BGÖ, gemäss dem der Zugang zu einem amtlichen Dokument eingeschränkt, aufgeschoben oder verweigert werden kann, wenn durch seine Gewährung die aussenpolitischen Interessen oder die internationalen Beziehungen der Schweiz beeinträchtigt werden können.

3. Der Beauftragte hat im Rahmen des Schlichtungsverfahrens auch Zugang zu amtlichen Dokumenten, die der Geheimhaltung unterliegen (Art. 20 BGÖ). Es versteht sich von selbst, dass der Beauftragte im Schlichtungsverfahren respektive in seiner Empfehlung keine vertraulichen oder geheimen Informationen und Details aus dem fraglichen Dokument bekannt geben darf. Anders verhält es sich mit Angaben beschreibender Natur zum Inhalt und Aufbau des Dokuments, soweit diese für das Verständnis der Empfehlung notwendig sind.

   Das EDA händigte dem Beauftragten das zu beurteilende Dokument umgehend aus. Es enthält eine Auflistung aller schweizerischen Auslandvertretungen, die Visa erteilen. Anhand von 7 Kriterien wird für jede Vertretung eine Einschätzung der Risiken missbräuchlicher Erschleichung von Visa erstellt. Laut Ausführungen des EDA sagt die Auflistung nichts über eine mögliche Korruptionsanfälligkeit der einzelnen schweizerischen Vertretungen aus. Es bedeute auch nicht, dass bei auf der Liste aufgeführten schweizerischen Vertretungen Fehler aufgetreten seien.

4. Im Zusammenhang mit dieser Auflistung stellte sich für den Beauftragten die Frage, wie der Beauftragte mit Teilinformationen aus dem vertraulichen oder geheimen Dokument zu verfahren hat, wenn diese von einer Bundesbehörde früher bereits einmal zugänglich gemacht worden sind.

   Das Öffentlichkeitsprinzip garantiert eine so genannte *kollektive Information:* Wird der Zugang zu einem amtlichen Dokument einer Person gewährt, so muss er allen gewährt werden (BBl 2003 2001). Enthält ein amtliches Dokument, das nach Willen

der Behörde aufgrund des Vorliegens eines Ausnahmefalls von Art. 7 BGÖ dem Zugang entzogen bleiben soll, *bereits früher zugänglich gemachte Informationen, so rechtfertigt sich eine Geheimhaltung in Bezug auf diese (Teil-)Informationen nicht.* Daher sieht sich der Beauftragte frei, dieses Kriterium der Liste im Folgenden bekannt zu geben.

Die Auflistung des EDA enthält u.a. auch die aktuelle Visastatistik (erteilte und verweigerte Visa nach schweizerischer Auslandvertretung). Diese Visastatistik kann auf Anfrage beim Bundesamt für Migration bezogen werden und ist in der Vergangenheit bereits verschiedentlich zugänglich gemacht worden.

Der Beauftragte kommt daher zum Schluss, dass der Zugang zur Visastatistik als solche nicht verweigert werden darf.

5. Art. 7 BGÖ hält jene Ausnahmefälle fest, in denen der Zugang zum Dokument eingeschränkt, aufgeschoben oder verweigert werden kann. Eine Ausnahme kann zum Schutz von öffentlichen (Abs. 1 Bst. a – f) oder privaten (Abs. 1 Bst. h und g, Abs. 2) Interessen geltend gemacht werden. Das EDA ist der Ansicht, dass die Gewährung des Zugangs zu einer Beeinträchtigung der aussenpolitischen Interessen oder der internationalen Beziehungen der Schweiz führen würde.

   Enthält ein Dokument Informationen mit aussenpolitischem oder internationalem Bezug, so bedeutet dies nicht, dass das ganze Dokument oder die entsprechenden Informationen unbesehen und stets als Ausnahmefall von Art. 7 BGÖ zu betrachten sind. Vielmehr müssen die fraglichen Passagen „ein gewisses Gewicht"[1] aufweisen, um überhaupt eine reelle Beeinträchtigung der angerufenen Interessen hervorrufen zu können.

   Zudem müssen die entsprechenden Informationen geeignet sein, bei einer Bekanntgabe die aussenpolitischen Interessen oder internationalen Beziehungen verletzen zu können. Für den Einzelfall bedeutet dies hingegen nicht, dass es in der Folge tatsächlich zu einer Verletzung der Beziehungen kommen muss. *Die Verletzung muss jedoch zumindest „mit einer hohen Wahrscheinlichkeit eintreten, also nicht lediglich denkbar bzw. entfernt möglich sein."*[2]

[1] Votum BR Blocher zu Art. 7, Amtliches Bulletin 2004 N 1962
[2] Brunner, Interessenabwägung im Vordergrund, digma 4/2004, S. 163

6. Das Verhältnismässigkeitsprinzip verlangt, dass die Behörde stets prüft, ob anstelle einer vollumgänglichen Verweigerung allenfalls ein teilweiser[3] Zugang gewährt werden kann. Die Behörde muss dabei abklären, ob die sensiblen Teilbereiche des Dokuments abgedeckt, entfernt oder verschlüsselt werden können. Erst wenn diese Massnahmen dazu führen, dass die offenen Passagen des Dokuments keinen Sinn mehr ergeben, kann der Zugang (gänzlich) verweigert werden. Nachfolgend gilt es die Frage zu beurteilen, ob und in welchem Umfang das EDA allenfalls einen teilweisen Zugang zur Auflistung hätte gewähren müssen.

7. Fünf der sechs Kriterien (Kriterien 1 – 4 und 6) weisen einen direkten oder indirekten Bezug zur Visastatistik auf respektive stehen in Zusammenhang mit der Visaerteilung. Anhand dieser Kriterien wird eine Einstufung der einzelnen schweizerischen Vertretungen, nicht aber einzelner Staaten vorgenommen. Weder die einzelnen Kriterien noch deren Einstufung beinhalten somit Aussagen oder Wertungen über andere Staaten. Den Kriterien erfüllen die in Ziffer 5 ausgeführten Anforderungen nicht, wonach bereits die Offenlegung zu einer erheblichen Beeinträchtigung der Beziehungen der Schweiz zum jeweiligen Land führen könnte.

   Der Beauftragte vertritt daher die Meinung, dass diese Kriterien nicht unter die Ausnahme von Art. 7 Abs. Bst. d BGÖ fallen und damit eine Verweigerung des Zugangs hinsichtlich dieser Kriterien gegen das Öffentlichkeitsgesetz verstösst.

8. Lediglich ein Kriterium (Kriterium 5) basiert auf Einschätzungen und Beurteilungen der aktuellen Situation in jenen Staaten, in denen sich die Auslandvertretung befindet. Es ist nicht von der Hand zu weisen, dass diese Staaten ein Interesse an den schweizerischen Einschätzungen und Beurteilungen bekunden könnten. Der Beauftragte ist der Ansicht, dass die Zugänglichmachung dieses Kriteriums dazu führen kann, dass die betroffenen Länder darin ein offizielles Werturteil der Schweiz betreffend die Situation in ihren Ländern sehen könnten. Nach Ansicht des Beauftragten besteht zumindest eine erhebliche Wahrscheinlichkeit, dass dadurch die Beziehung mit einem oder mehreren Staaten negativ belastet und in der Folge beeinträchtigt werden könnte.

   Nach Meinung des Beauftragten sind die Voraussetzungen nach Art. 7 Abs. 1 Bst. d BGÖ für jenes Kriterium (Kriterium 5) gegeben, das sich über die aktuelle Situation in anderen Staaten ausspricht. In diesem Punkt kann das EDA den Zugang zum fraglichen Dokument einschränken. Im Übrigen sollte die Auflistung samt der Einstufung der einzelnen Vertretungen dem Antragsteller zugänglich gemacht werden.

[3] Art. 7 Abs. 1 BGÖ spricht in diesem Zusammenhang von „einschränken" oder „aufschieben".

III. Aufgrund dieser Erwägungen empfiehlt der Datenschutz- und Öffentlichkeitsbeauftragte:

1. Das Eidg. Departement für auswärtige Angelegenheiten gewährt dem Antragsteller einen teilweisen Zugang zur Auflistung. Der Zugang wird eingeschränkt in Bezug auf das Kriterium, das sich über die aktuelle Situation in anderen Staaten ausspricht (Kriterium 5).

2. Das Eidg. Departement für auswärtige Angelegenheiten erlässt eine Verfügung nach Art. 5 des Verwaltungsverfahrensgesetzes, wenn es in Abweichung dieser Empfehlung dem Antragsteller den teilweisen Zugang nicht gewährt.

   Das Eidg. Departement für auswärtige Angelegenheiten erlässt die Verfügung innert 20 Tagen nach Empfang dieser Empfehlung (Art. 15 Abs. 3 BGÖ).

3. Der Antragsteller kann innerhalb von 10 Tagen nach Erhalt dieser Empfehlung beim Eidg. Departement für auswärtige Angelegenheiten den Erlass einer Verfügung nach Artikel 5 des Verwaltungsverfahrensgesetzes verlangen, wenn er mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 1 BGÖ).

4. Gegen die Verfügung kann bei der Eidgenössischen Datenschutz- und Öffentlichkeitskommission Beschwerde geführt werden (Art. 16 BGÖ).

5. Diese Empfehlung wird veröffentlicht (Art. 13 Abs. 3 VBGÖ). Zum Schutz der Personendaten der am Schlichtungsverfahren Beteiligten wird der Name des Antragstellers anonymisiert.

Hanspeter Thür

Kopie an: X